بحث بعنوان

جريمة الإرهَابُ الإلكَتْرُونيُّ في التَّشْرِيعاتِ الجنائيَّة
دراسةٌ تحليليَّة مُقارنةٌ

إعداد

د. لورنس سعيد الحوامدة

أستاذ مُشارك في القانون الجنائي

جامعة طيبة – كلية الحقوق- قسم القانون العام

المملكة العربية السعودية

٢٠٢١/ ٢٠٢٢

جريمة الإرهاب الإلكتروني في التَّشريعات الجنائيَّة
دراسةٌ تحليليَّة مُقارنةٌ

لورنس سعيد الحوامدة.

قسم القانون العام، كلية الحقوق، جامعة طيبة، المملكة العربية السعودية.

البريد الإلكتروني: loooowww@yahoo.com :

مُلخَّص البحث :

تُعدُّ جريمة الإرهاب الإلكتروني مِنْ الجرائم الخطيرة والمؤثرة على أمن المجتمعات والدَّول، سيَّما مع ازدياد ارتكاب جرائم الإرهاب الإلكتروني في العصر الحديث في ظل اتساع استخدام شبكة الاتصالات وتكنولوجيا المعلومات، ولسهولة ارتكاب هذه الجرائم مِنْ قِبَلِ الجماعات الإرهابية عبر الوسائط الإلكترونية والتي تُعاني مِنْ ضعف الرقابة الأمنيَّة عليها مِنْ قِبَلِ الأجهزة الأمنيَّة، لذلك توصلت الدراسة إلى مجموعة مِنْ التوصيات يمكن أن تشكل حلولاً لمعالجة جميع الإشكاليات ذات الصلة بجرائم الإرهاب الإلكتروني ومنها ضرورة إيجاد تشريع مُستقل يُعنى بمُكافحة جرائم الإرهاب الإلكتروني، كذلك استحداث مركز عربي لمُكافحة الإرهاب الإلكتروني تابعاً لجامعة الدَّول العربية، وتعديل بعض التشريعات القائمة (كتشريعات مُكافحة الإرهاب وتشريعات الجرائم المعلوماتية) لشمولها بصور وأفعال جرائم الإرهاب الإلكتروني بما يضمن مُكافحة هذه الظاهرة المؤثرة في أمن الدَّول والمجتمعات.

الكلمات المفتاحيَّة: الإرهاب الإلكتروني، التعاون الدَّولي، التَّشريعات، الجرائم المعلوماتيَّة، الركن المادي التنظيمات الإرهابيَّة.

Cyberterrorism offence in criminal legislation Comparative analytical study

Lourance.S. Al-Hawamdeh

Department of Public Law, Faculty of Law, Taibah University , Kingdom Saudi Arabia .

E-mail: looooww@yahoo.com

Abstract:

The crime of cyber terrorism is one of the serious crimes that affect the security of societies and countries, especially with the increase in the commission of cyber terrorism crimes in the modern era in light of the wide use of the communication and information technology network. And also, with the ease of committing these crimes by terrorist groups through electronic media, which suffer from weak security oversight over them by the security services. So, the study concludes a set of recommendations that could constitute solutions to address all the problems related to cyber-terror crimes, including the need to find independent legislation concerned with fighting cyber-terror crimes. As well as the creation of an Arab Center to fight cyber-terrorism affiliated with the League of Arab States. And the study concludes the amendment of some legislation that already exists (such as anti-terrorism legislation, and cybercrime legislation) to include images and actions of cyber-terror crimes to ensure fighting this phenomenon affecting the security of countries and societies.

Keywords: Cyber Terrorism, International Cooperation, Legislation, InformationC, Physical Pillar.

المُقدِّمة:

تولى الدَّول لجريمة الإرهاب الإلكتروني اهتماماً كبيراً لما تشكله هذه الجريمة كظاهرة مِنْ خطرٍ على المجتمع والمدنيين، وزعزعة لاستقرار وأمن الدّول يترتب عليه تدمير للممتلكاتِ، وانتهاك للحرمات والمقدسات، وخطف وقتل للمدنيين الآمنين. (الجابري،٢٠١٢، ص١٥٩).

لذلك فإنَّ جرائم الإرهاب الإلكتروني تُعدُّ مِنْ أخطر الجرائم على المستوى الوطني والدّولي، حيث أصبحت البيانات والمعلومات الحكومية والأشخاص أهدافاً للتنظيمات الإرهابية نظراً لسهولة استخدام الشبكات وتدمير البنية الإلكترونية الحكومية عنْ طريق شلّ أنظمة القيادة والاتصال أو قطع شبكات الاتصالات بين القيادات المركزية والوحدات الفرعية أو التحكم والسيطرة على خطوط الملاحة الجوية والبحرية أو اختراق النظام المصرفي أو تجنيد أشخاص عنْ طريق استقطابهم مِنْ خلال وسائل التواصل الاجتماعي، لذلك سارعت الدّول إلى مكافحة جرائم الإرهاب الإلكتروني مِنْ خلال سن وتشريع قوانين خاصة تُجرم جميع الأفعال ذات الصلة بجرائم الإرهاب الإلكتروني، كما عقدت الدّول العديد مِنْ الاتفاقيات الدّولية الثنائية أو الجماعية لتأطير التعاون بينها في سبيل مكافحة هذه الظاهرة المؤثرة على الجانب الاقتصادي والسياسي والاجتماعي للدّول والمجتمعات. (الزعابي، بني إبراهيم، ٢٠١٩، ص٢١).

لذلك فإنَّ الدراسة ستناقش مجموعة مِنَ المحاور يتناول الأوَّل مفهوم الإرهاب الإلكتروني ، كما سيتم دراسة الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني، أما المحور الثاني مِنَ الدراسة سيتناول أركان جريمة الإرهاب الإلكتروني وفقاً للتَّشريعات الجنائيَّة (الركن المادي، الركن المعنوي)، بالإضافة إلى الإشارة بالشرح والتحليل إلى سُبل ووسائل مُكافحة جرائم الإرهاب الإلكتروني على المستوى الوطني والدّولي مِنْ خلال إبراز دور التَّشريعات الجنائيَّة ذات الصلة بجرائم الإرهاب والتَّشريعات ذات الصلة بالجرائم الإلكترونية في مكافحة جرائم الإرهاب الإلكتروني، وبيان دور الاتفاقيات الدّولية كنوع مِنْ مظاهر التعاون بين الدول في مكافحة جرائم الإرهاب الإلكتروني على المستوى العربي والدَّولي.

▪مُشكلة الدراسة:

تتلخص مُشكلة الدراسة في أنَّ معظم التَّشريعات الجنائيَّة ذات الصلة بجرائم الإرهاب التقليدية والإلكترونية تخلط بين جرائم الإرهاب الإلكترونية وجرائم الإرهاب التقليدية ممّا سبب ذلك قصوراً في التَّشريعات الجنائيَّة أدى إلى عدم مكافحة هذا النوع مِنَ الجرائم بالصورة الصحيحة، فضلاً على أنّ القانون الدّولي العام ممثلاً بالاتفاقيات الدّولية لم يتوصل إلى اتفاق موحد لتحديد مفهوم الإرهاب الإلكتروني منصرفاً ذلك على عدم الاتفاق بين فقهاء القانون على تعريف موحد للإرهاب على وجه العموم، بالإضافة

إلى ندرة الاتفاقيات الدّولية وشح التعاون بين الدّول في مجال مُكافحة جرائم الإرهاب الإلكتروني، لذلك فإنَّ الدراسة ستجيب على مجموعة مِنْ الأسئلة نجملها على النحو الآتي:

١- ما أوجه القصور في التَّشريعات الجنائيَّة ذات الصلة بجرائم الإرهاب الإلكتروني والإرهاب التقليدي؟
٢- ما الطبيعة القانونيَّة لجرائم الإرهاب الإلكتروني؟ وهل تختلف عنْ غيرها مِنْ جرائم الإرهاب التقليدية؟
٣- ما أركان جريمة الإرهاب الإلكتروني؟ وهل تناولت التَّشريعات الجنائيَّة صور السلوك المادي المكون لجريمة الإرهاب الإلكتروني ضمن نصوصها؟
٤- ما وسائل مُكافحة جرائم الإرهاب الإلكتروني على المستوى الوطني؟ وما مدى فاعلية التَّشريعات ذات الصلة بالإرهاب الإلكتروني في مكافحة هذه الظاهرة؟
٥- ما مدى فاعليَّة الاتفاقيات الدّولية ممثلة بالقانون الدّولي العام في مكافحة جرائم الإرهاب الإلكتروني على المستوى الدّولي؟
٦- هل يوجد تشريعات جنائيَّة خاصة لمُكافحة جرائم الإرهاب الإلكتروني أم عولجت ضمن التَّشريعات ذات الصلة بجرائم الإرهاب التقليدي أو الإلكتروني؟

▪أهداف الدراسة:

تتلخص أهداف الدراسة بما يلي:

١- بيان أوجه القصور في التَّشريعات الجنائيَّة ذي الصلة بالإرهاب الإلكتروني إن وجدت والإرهاب التقليدي.
٢- الوصول إلى تعريف مُوحد لمصطلح الإرهاب الإلكتروني.
٣- شرح وتوضيح الأركان الخاصة لجريمة الإرهاب الإلكتروني.
٤- التعرف على الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني.
٥- توضيح سُبل مكافحة جريمة الإرهاب الإلكتروني على المستوى الدّولي والوطني.
٦- التأكد مِنْ مدى فاعلية القانون الدّولي العام ممثلاً بالاتفاقيات الدّولية في مُكافحة جرائم الإرهاب الإلكتروني.

▪ أهمية الدراسة:

تبرز أهمية الدراسة لجريمة الإرهاب الإلكتروني في تسليط الضوء على مدى خطورة جريمة الإرهاب الإلكتروني على أمن الفرد والمجتمعات، مِنْ خلال استهداف شبكات الاتصالات للدول والبنية المعلوماتيَّة الحكومية وسرقة المعلومات، وتجنيد

الأشخاص عبر وسائل التواصل الاجتماعي للقيام بعمليات إرهابية تنال مِنْ أمن الدول والمجتمعات، وغيرها مِنْ المظاهر والسلوكيات التي تُعدُّ مِنْ عناصر جريمة الإرهاب الإلكتروني، لذلك فإنَّ أهمية الدراسة تكمن في الإشارة إلى دور التَّشريعات الجنائيَّة الوطنية، والاتفاقيات الدّولية، والتعاون بين الدّول في مكافحة هذا النوع مِنْ الجرائم بالأدوات التَّشريعية، والأمنية، والفكرية المتاحة مِنْ أجل التغلب على جميع المعيقات التي تعرقل سُبل مكافحة جريمة الإرهاب الإلكتروني على المستوى الدّولي والوطني، وبيان جوانب القصور في التَّشريعات الجنائيَّة ذات الصلة في الإرهاب الإلكتروني إن وجدت.

▪منهجيَّة الدراسة:

تتلخص منهجيَّة الدراسة باعتماد المنهج الوصفي والتحليلي والمقارن لظاهرة الإرهاب الإلكتروني، مِنْ خلال شرح وتحليل التَّشريعات الجنائيَّة ذات الصلة ومقارنتها ببعضها البعض مِنْ أجل الخروج بتوصيات تُعدُّ حلولاً لمشكلة الدراسة، كما سيتم الإشارة إلى الاتفاقيات الدّولية المُتخصصِّة في الإرهاب الإلكتروني مِنْ خلال تحليلها ومناقشتها بصورة علميَّة ومنهجيَّة للوقوف على مدى فاعليتها في مُكافحة ظاهرة الإرهاب الإلكتروني وبيان مدى تعاون الدَّول في تبادل المعلومات، وعقد الاتفاقيات الدَّولية، وكلّ المسائل القضائيَّة ذات الصلة بالإرهاب الإلكتروني .

▪خطة الدراسة:

▪المبحثُ الأوَّل: ماهية الإرهاب الإلكتروني.
▪المطلبُ الأوَّل: مفهوم الإرهاب الإلكتروني.
▪المطلبُ الثّاني: الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني.
▪المبحثُ الثّاني: أركان جريمة الإرهاب الإلكتروني وسُبل مكافحتها.
▪المطلبُ الأوَّل: العناصر المكونة لجريمة الإرهاب الإلكتروني.
▪المطلبُ الثّاني: جهود مكافحة جريمة الإرهاب الإلكتروني على المستوى الوطني والدّولي.

المبحثُ الأوَّل

ماهية الإرهاب الإلكتروني

تمهيد وتقسيم:

يُعدُّ الإرهاب الإلكتروني مِنَ الجرائم الخطيرة على المستوى الوطني والإقليمي والدّولي، سيَّما وأنَّ الفقه القانوني والمُختصين في مجال القانون الدَّولي لم يتفقوا إلى الوقت الحالي على تعريف موحد للإرهاب بمفهومه العام والشامل. (الجابري، ٢٠١٢، ص٦). لذلك وقبل الخوض في دراسة هذه الظاهرة المؤثرة، لا بد مِنْ تعريف وتوضيح مفهوم الإرهاب الإلكتروني، ودراسة الطبيعة القانونيَّة للإرهاب الإلكتروني، على النحو الآتي:

- المطلبُ الأوَّل: مفهوم الإرهاب الإلكتروني.
- المطلبُ الثّاني: الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني.

المطلبُ الأوَّل

مفهوم الإرهاب الإلكتروني

تعدَّدت المفاهيم الفقهية للإرهاب الإلكتروني، فقد عرَّف جانب مِنَ الفقه الإرهاب الإلكتروني بأنَّه" سلوك إجرامي يتم بواسطة بث أو إشاعة الأفكار المتطرفة عبر الوسائل الإلكترونية سواءً كانت دينية، أو سياسيَّة، أو اجتماعيَّة، أو عنصرية مِنْ أجل السيطرة على وجدان الأفراد والمجتمعات وأفساد عقائدهم وتنمية تمردهم واستغلال معاناتهم، بهدف تحقيق مآرب خاصة تتعارض مع مصالح المجتمع وأمن الدَّول". (بوادي، حسنين ٢٠٠٦، ص٥٤).

جانبٌ أخر مِنَ الفقه عرَّفه بأنَّه" استخدام الأجهزة الإلكترونية بنظمها وبرامجها وملحقاتها مِنْ أجل ارتكاب الجرائم الإرهابية سواءً كانت هذه التقنية هي محل الجريمة أو كانت وسيلة في ارتكابها". (موسى، مصطفى، ٢٠٠٥، ص٧٤).

وعرِّف ايضاً بأنَّه " جريمة يترتب عليها عدوان أو تهديد أو تخويف مادياً كان أم معنوياً ويتم عبر الوسائط الإلكترونية الصادرة عنْ الدَّول أو الكيانات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق وبشتى صور الإفساد في الأرض". (العذار، أنيس بن علي، الشافعي، خالد بن عبد الله، ٢٠١٧، ص٢٢٦).

لذلك فإنَّ الإرهاب الإلكتروني أصبح يستهدف أنظمة وبرامج الكمبيوتر والمعلومات الموجودة فيها، حيث بات يُعدُّ ذلك نمطاً مُستحدثاً مِنْ أنماط الإرهاب الإلكتروني، سيَّما وأنَّه لا يعتمد على الأسلحة والمتفجرات التقليدية إنما يقوم على استغلال المجرمين للثغرات المتوفرة في أنظمة المعلومات والبيانات للأجهزة الإلكترونية. (العموش، أحمد فلاح، ١٤٢٧هـ، ص٩٠).

ويرى الباحث - بعد استعراض مفاهيم الإرهاب الإلكتروني السابقة أنَّ الإرهاب الإلكتروني كسلوك إجرامي غير مشروع يستند على مجموعة مِنَ المحاور تتلخص بما يلي:

١- إنَّ جريمة الإرهاب الإلكتروني ترتكب بواسطة الأجهزة الإلكترونية بحيث تكون هذه الأجهزة وسيلة أو محلاً للجريمة ولا ترتكب بوسائل تقليدية.
٢- يستغل الإرهابين حاجات الناس ومطالبهم مِنْ أجل إشاعة الرعب، أو الفتنة، أو الخوف، أو العنصرية، أو ارتكاب الخطف، أو القتل بقصد تحقيق مآرب خاصة بهم تستهدف أمن الدَّول والمجتمعات.

المطلبُ الثّاني

الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني

اختلف فقهاء القانون الجنائي والدّولي حول مسألة التكييف القانوني لجريمة الإرهاب الإلكتروني وانقسموا إلى اتجاهين: الأوَّل قال إنَّ جريمة الإرهاب الإلكتروني هي جريمة جنائية وطنية ومِنْ اختصاص القضاء الجنائي الوطني، أمَّا الاتجاه الثاني فاعتبر أنَّ جريمة الإرهاب الإلكتروني هي جريمة دولية ذات طابع سياسي وتتطلب صدور قرار سياسي بمحاربتها ومكافحتها عنْ طريق المجتمع الدَّولي. (الجابري، مرجع سابق، ص٦٢). لذا ستتم مناقشة ودراسة هذه الاتجاهات على النحو الآتي:

الفرعُ الأوَّل: جريمة الإرهاب الإلكتروني (جريمة وطنية)

يرى الاتجاه الأوَّل مِنَ الفقه أنَّ الإرهاب الإلكتروني هي جريمة جنائيَّة وطنية نظراً لما يتوافر فيها مِنْ عناصر كالجرائم الوطنية (كالقتل، والاغتصاب، والسرقة، والسطو وغيرها....) لذلك فإنَّ الطبيعة القانونيَّة لجريمة الإرهاب الإلكتروني تتطلب تعريفاً قانونيَّاً للجريمة يُحدد أركانها ويأخذ فيه المُشرِّع وفقاً لمبدأ شرعية الجرائم والعقوبات " لا جريمة ولا عقوبة إلاَّ بنص" وهذا ما أخذت به بعض التَّشريعات العربية كالتَّشريع المصري والذي عرَّف الإرهاب في المادة (٣) مِنْ قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥ وتعديلاته بالقانون رقم ١٥ لسنة ٢٠٢٠م بقوله" يقصد بتمويل الإرهاب كلّ جمع أو تلقٍّ أو حيازة أو إمداد أو نقل أو توفير أموال أو أصول أخرى أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها لأي نشاط إرهاب فردي أو جماعي مُنظم أو غير مُنظم في الداخل أو الخارج ، بشكل مباشر أو غير مباشر أيَّاً كان مصدره وبأي وسيلة كانت بما فيها الشكل الرقمي أو الإلكتروني، وذلك بقصد استخدامها كلها أو بعضها في ارتكاب جريمة إرهابية أو العلم باستخدامها سواء وقع الفعل الإرهابي أو لم يقع، أو بتوفير مكان للتدريب أو مكان آمن لإرهابي أو أكثر أو تزويده بأسلحة أو مستندات أو غيرها أو بأي وسيلة مساعدة أخرى مِنْ وسائل الدعم أو التمويل الخ...." (الجابري، مرجع سابق، ٦٣).

كما اعتبر المُشرِّع المصري الجريمة الإرهابية جريمة وطنية بامتياز وهذا واضح مِنْ نص المادة (١/ج) مِنْ قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م وتعديلاته بقوله" كل جريمة منصوص عليها في هذا القانون، وكذا كل جناية أو جنحة ترتكب باستخدام إحدى وسائل الإرهاب، أو بقصد تحقيق، أو تنفيذ غرض إرهابي، أو بقصد الدعوة إلى ارتكاب أو التهديد بها"

ويرى الباحث - أنَّ المُشرِّع المصري اعتبر جميع الأفعال ذات الصلة بالإرهاب التقليدي والإرهاب الإلكتروني وتمويله وطنية حتى لو كان بعض صور التمويل للإرهاب له ارتباط خارجي ما دام أنَّ الأفعال والسلوكيات ذات الصلة بالجريمة الإرهابية بدأت مِنْ داخل حدود الدَّولة، وهذا واضح مِنْ خلال قراءة نص المادة ١/ج

والمادة ٣ مِنْ قانون مكافحة جريمة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م وتعديلاته بالقانون رقم ١٥ لسنة ٢٠٢٠م، لذا فإنني أؤيد الاتجاه الأوَّل والذي اعتبر أنَّ الإرهاب الإلكتروني أو التقليدي جريمة وطنية بامتياز على اعتبار أنَّ آثار الجريمة تكون مباشرة على الأمن الوطني للدّولة ولو امدت بعض آثارها خارج حدود الدّولة ومهما اختلفت وسائل ارتكاب جرائم الإرهاب سواء أكانت وسائل إلكترونية أو تقليدية.

الفرعُ الثّاني: جريمة الإرهاب الإلكتروني (جريمة دولية)

يرى أنصار الاتجاه الثاني أنَّ الإرهاب الإلكتروني والإرهاب التقليدي جريمة دولية، إذا كان السلوك المرتكب فيه مخالفة للقواعد القانونيَّة الدّولية المنصوص عليها في الاتفاقيات الدّولية أو القانون الدّولي العرفي وترتب على ارتكاب هذه الجرائم المسؤولية الجنائيَّة الشخصية. (سرور، أحمد فتحي، ٢٠٠٨، ص١١٠).

ويرى جانبٌ مِنَ الفقه أنَّ جريمة الإرهاب الإلكتروني وحتى تكون جريمة دولية لا بد أن تتوافر فيها مجموعة مِنَ الشروط تتلخص بما يلي:

١- ألاَّ تكون حدود جريمة الإرهاب الإلكتروني مقتصرة فقط على دولة بعينها، بل تتجاوز الحدود الوطنية للدولة.
٢- أن ترتكب جريمة الإرهاب الإلكتروني بدعم دولة أجنبية، أو تشجيعها، أو موافقتها، أو استخدام بعض وسائل الإعلام لخدمة أهداف هذه الدَّولة والتي تنتهج الإرهاب سلوكاً، وهذا ما نصَّت عليه بعض الاتفاقيات الدَّولية ذات الصلة بجرائم الإرهاب الإلكتروني.
٣- أن تُهدد الجريمة الإرهابية الأمن والسلم للمجتمع الدّولي بأسره.
٤- أن تكون الأفعال والسلوكيات المكونة لجريمة الإرهاب الإلكتروني على درجة عالية مِنْ الجسامة، مِنْ خلال استعمال وسائل التكنولوجيا الحديثة لارتكاب الجريمة. (الجابري، مرجع سابق، ص٦٤-٦٥).

ويرى جانبٌ أخر مِنَ الفقه أنَّ جريمة الإرهاب الإلكتروني يُطلق عليها وصف " الجريمة الدَّولية" وفقاً للقانون الدّولي إذا تم ارتكابها بوصفها جريمة حرب أو جريمة ضد الإنسانية. (إبراهيم، ثامر، ١٩٩٨، ص٥٥).

لكن السؤال الذي يُطرح هو: هل جريمة الإرهاب الإلكتروني تُعدُّ جريمة منظمة أم لا؟

تختلف الجريمة المنظمة عنْ جريمة الإرهاب الإلكتروني، فمِنْ حيث الهدف تهدف الجريمة المنظمة إلى جمع أكبر كمية مِنْ الأموال وبكافة الوسائل الممكنة، أمّا جريمة الإرهاب الإلكتروني فهدفها سياسي ولا تهدف إلى كسب أو جمع المال إلاَّ في حالات محدودة، وفيما يتعلق بالآثار التي تترتب على الجريمة المنظمة عند وقوعها فإنَّها لا تتعدى ضحاياها، بعكس جريمة الإرهاب الإلكتروني والتي يمكن أن تمتد آثارها إلى

المجتمع كله، إلاَّ أنَّ كلا الجريمتين تشتركان في بث سياسة الخوف والرعب بين الناس والدّول بشكل أساسي وهذا واضح مِنْ خلال الجرائم التي تم ارتكابها في فترات زمنية متعدِّدة.(كوران، يوسف، ٢٠٠٧، ص ٧٣-٧٤).

الخلاصة: يمكن القول - أنَّ جريمة الإرهاب الإلكتروني هي جريمة وطنية ولو كان لها امتداد دولي، وبالتالي فإنّه يقع على عاتق الدّول مسؤولية مُكافحة هذا النوع مِنْ الجرائم عنْ طريق عقد الاتفاقيات الدّولية، وسن التَّشريعات، والتنوير الفكري للمجتمع مِنْ مخاطر وسلبيات هذه الجرائم، ويرى الباحث ومِنْ خلال قراءة ومطالعة نصوص نظام روما الأساسي للمحكمة الجنائية الدَّولية والصادر عام ١٩٩٨م خلوها مِنْ الإشارة إلى جرائم الإرهاب الإلكتروني باعتبارها جرائم دولية، وهذا يؤكد أنَّ هذه الجرائم تمتاز بأنَّها وطنية ولو كان لها امتداد دولي، سيَّما وإنَّ نصَّ المادة (٥) مِنْ نظام روما الأساسي للمحكمة الجنائية الدَّولية حدَّد اختصاص المحكمة بالجرائم على سبيل الحصر كما يلي:

١- جريمة الإبادة الجماعية.
٢- الجرائم ضد الإنسانية.
٣- جرائم الحرب.
٤- جريمة العدوان.

المبحثُ الثّاني

أركان جريمة الإرهاب الإلكتروني وسُبل مكافحتها

تمهيد وتقسيم:

أجمع الفقهاء على أنَّ جريمة الإرهاب الإلكتروني تختلف مِنْ حيث أركانها (المادي، والمعنوي) عنْ جرائم الإرهاب التقليدي. (الكساسبة، فهد، ٢٠١٥، ص١٥١)، لذا سيناقش هذا المبحث مجموعة مِنَ المحاور نجملها على النحو الآتي:

- المطلبُ الأوَّل: العناصر المكونة لجريمة الإرهاب الإلكتروني.
- المطلبُ الثّاني: جهود مكافحة جريمة الإرهاب الإلكتروني على المستوى الوطني والدّولي.

المطلبُ الأوَّل

العناصر المكونة لجريمة الإرهاب الإلكتروني

تتكون جريمة الإرهاب الإلكتروني كغيرها مِنَ الجرائم في القانون الجنائي مِنْ الركن المادي والذي يتكون مِنْ السلوك الإيجابي والسلبي، والنتيجة الجرمية، والعلاقة السببية، أمَّا الركن المعنوي لجريمة الإرهاب الإلكتروني فإنَّه يتكون مِنَ القصد الجرمي بعنصريه العلم، والإرادة، لذا سندرس هذه العناصر المكونة لجريمة الإرهاب الإلكتروني بالبحث والتحليل على النحو الآتي:

- الفرعُ الأوَّل: الركن المادي لجريمة الإرهاب الإلكتروني
- الفرعُ الثّاني: الركن المعنوي لجريمة الإرهاب الإلكتروني

الفرعُ الأوَّل: الركن المادي لجريمة الإرهاب الإلكتروني

ويتكون الركن المادي لجريمة الإرهاب الإلكتروني مِنْ سلوك، ونتيجة، وعلاقة سببيَّة وسنبين ذلك بالمناقشة والتحليل على النحو الآتي:

أ- (السلوك):

يُعرِّف جانبٌ مِنَ الفقه السلوك بأنَّه " الفعل المادي الخارجي الذي يصدر عنْ الجاني ويترتب على حدوثه وقوع نتيجة جرميَّة يُعاقب عليه القانون، ويُعدُّ السلوك أو الفعل عنصراً ضرورياً لكلِّ جريمة". (المجالي، توفيق نظام، ٢٠١٠، ص٢١١).

أمَّا عنْ مفهوم السلوك الإيجابي فقد عرَّفه بعض الفقهاء بأنَّه" قيام الجاني بحركة أو فعل إرادي يترتب عليه حدوث تغيير في العالم الخارجي" أمَّا السلوك السلبي فهو امتناع الجاني عنْ القيام بعمل أوجب القانون عليه القيام بهذا العمل، حيث شكل امتناع

الجاني حدوث النتيجة الجرمية" وفيما يتعلق بالأفعال والسلوكيات المكونة لجريمة الإرهاب التقليدي فإنَّها تقوم على قيام الجاني بأفعال واستخدام أدوات ومواد تشكل خطراً عاماً وتثير الرعب والذعر بين الناس، وتحدث ضرر جسيم لأمن المجتمع والدَّول، أمَّا بالنسبة لجريمة الإرهاب الإلكتروني فإنَّ سلوكها يتضمن استخدام جهاز الحاسوب ووجود بيئة رقميَّة يقوم بواسطتها الجاني بارتكاب جريمة الإرهاب الإلكتروني.(الكساسبة، فهد، مرجع سابق، ص١٥٢).

أمَّا في التَّشريعات الجنائية فقد تعدَّدت صور الأفعال المكونة لجريمة الإرهاب الإلكتروني، ففي التَّشريع الأردني نجد أنَّ المُشرِّع الأردني قد جرَّمَ الأنشطة والأفعال المكونة لجريمة الإرهاب الإلكتروني في المادة ٣ مِنْ قانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦م بقوله" ه- استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو اعلام أو إنشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل مِنْ شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم" [١].

كما نصَّت المادة (١٥) مِنَ الاتفاقية العربيَّة لمُكافحة جرائم تقنيَّة المعلومات والصادرة عام ٢٠١٢م على جميع السلوكيات غير المشروعة لجريمة الإرهاب الإلكتروني تحت مسمى " الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنيَّة المعلومات" وعلى النحو الآتي:

١- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
٢- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
٣- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
٤- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

ويمكن القول - أنَّ الأفعال المكونة لجريمة الإرهاب الإلكتروني تتطلب بيئة رقميَّة أو إلكترونية يستطيع مِنْ خلالها الجاني ارسال بياناته ومعلوماته مِنْ أجل القيام بأعمال إرهابية أو تسهيل الإجراءات لجماعة أو منظمة إرهابية أو مساعدة الجماعات الإرهابية في نشر أفكارها أو تسهيل تمويلها، كما إنَّ نص المادة ١٥ مِنْ الاتفاقية خلا

١- كما جرَّم الأفعال ذات الصلة بجريمة الإرهاب الإلكتروني عبر شبكة تقنية المعلومات المُنظم السعودي، حيث عاقب المُنظم كل شخص "أنشاء أو استخدم موقعاً على الشبكة المعلوماتية أو برنامجاً على أجهزة الحاسب الآلي أو أي مِنْ الأجهزة الإلكترونية أو نشر أيَّاً منهما وذلك بهدف إرتكاب جرائم إرهابية أو لتسهيل الاتصال بأحد القيادات أو الأفراد التابعين لأي كيان إرهابي، أو لترويج أفكار أي منظمة أو كيان أو تمويله" الخ.... (انظر المادة ٤٣) مِنْ نظام مكافحة الإرهاب وتمويله السعودي رقم م/٢١ تاريخ ١٤٣٩/٢/١٢هـ.

مِنْ الإشارة إلى جميع الأفعال والسلوكيات غير المشروعة المكونة لجريمة الإرهاب الإلكتروني، وهذا قصور في التَّشريع ينعكس على مُكافحة هذا النوع مِنَ الجرائم المؤثرة على أمن المجتمعات والدَّول.

ويرى بعض الفقهاء أنَّ هنالك وسائل عامة تستخدم في جميع أشكال جريمة الإرهاب الإلكتروني، حيث تتنوع هذه الوسائل وتتطور تبعاً لتطور البيئة الرقميَّة أو الإلكترونية وتتلخص هذه الوسائل بما يلي:

أ- مرحلة الشروع في جريمة الإرهاب الإلكتروني:

ومِنْ خصائص هذه المرحلة أنَّ الإرهابيون يقومون بالتلقين الإلكتروني لمؤيديهم والمتعاطفين معهم في المجتمع خصوصاً فئة الشباب منهم، كما تقوم هذه الجماعات ببث أفكارها ووسائلها مِنْ أجل تجنيد واستقطاب إرهابين جُدد، وهذا واضح مِنْ خلال الاف المواقع الإرهابية والتي تساهم في نشر الفكر والمعتقدات لهذه الجماعات، كذلك التخطيط والتنسيق للعمليات الإرهابية المنوي القيام فيها مستقبلاً. (نظمي، رانيا محمد عزيز، ٢٠١٩، ص٢٠).

وقد جرَّم المُشرِّع الأردني الشروع في الجرائم الإرهابية ومنها جرائم الإرهاب الإلكتروني، حيث ساوى المُشرِّع مِنْ حيث العقوبة بين الجريمة التامة والشروع في الجرائم الإرهابية ومنها الإلكترونية أو الاشتراك فيها مِنْ باب تشديد العقوبة في هذا النوع مِنْ الجرائم والتي لها تأثير على أمن الأفراد والدَّول. (انظر نص المادة ٧/ومِنْ قانون منع الإرهاب الأردني رقم ٥٥ لسنة ٢٠٠٦م).

وحسناً فعل المُشرِّع الأردني بالمساواة في العقوبة بين الجريمة التامة في الجرائم الإرهابية ومنها جرائم الإرهاب الإلكتروني وبين الشروع فيها، وفي ذلك ردع للمنظمات الإرهابية والإرهابيين مِنْ أن تسوِّل لهم أنفسهم بالأقدام على ارتكابِ هذا النوع مِنْ الجرائمِ والتي لها آثار مدمرة على أمن الدَّول والمجتمعات.

ويرى الباحث - أنَّ مرحلة التحضير للجرائم الإرهابية لا عقوبة عليها انسجاماً مع القواعد العامة في القانون الجنائي إلاَّ إذا شكل العمل التحضيري جُرماً مستقلاً، أمَّا البدء في التحضير للقيام بارتكاب الفعل غير المشروع فيُعدُّ شروعاً وقد بينا أحكامه في القانون سابقاً، سيَّما وإنَّ بعض التَّشريعات عاقبت على مرحلة التحضير والإعداد للجريمة الإرهابية، ومِنْ هذه التَّشريعات قانون مكافحة الإرهاب المصري حيث نصَّ في المادة (٣٤) مِنْ قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م على ما يلي" يُعاقب بالحبس مدة لا تقلَ عن سنة كل من قام بأي عمل من أعمال الإعداد أو التحضير لارتكاب جريمة إرهابية حتى ولو لم يتعدَّ عمله هذا الإعداد أو التحضير".

ب-الدخول إلى المواقع الإلكترونية مِنْ أجل تدميرها:

تُعدُّ مِنْ ضمن الأهداف للمنظمات والجماعات الإرهابية تدمير المواقع الإلكترونية، حيث تقوم هذه الجماعات بالدخول لهذه المواقع مِنْ أجل تدميرها واتلاف محتوياتها، سيَّما وإنَّ هذه الجماعات تمتلك مِنْ الوسائل ما لا يمتلكه بعض الخبراء في المجال التقني والأفراد العاديين، سيَّما وإنَّ الأفراد المنتمين لهذه الجماعات يتصفون بالخبرة في المجال التقني والتكنولوجي ممَّا يؤهلهم لاختراق المواقع الإلكترونية مِنْ أجل الحصول على الاسرار والمعلومات بداخلها، وتدمير ما تريد تدميره مِنْ البيانات والمعلومات بهدف تحقيق غاياتها المتمثلة بزعزعة استقرار الدَّول والمجتمعات.(الكساسبة، فهد، مرجع سابق، ص١٥٤).

وقد جرَّمة بعض التَّشريعات العربية فعل الدخول إلى المواقع الإلكترونية بطريقة غير مشروعة، ومِنْ هذه التَّشريعات نظام مكافحة الجرائم المعلوماتية السعودي حيث اعتبر النظام أنَّ فعل الدخول إلى المواقع الإلكترونية أو أي نظام معلوماتي أو عن طريق الشبكة المعلوماتية أو أجهزة الحاسوب بطريقة غير مشروعة وبقصد الحصول على بيانات تمس الأمن الوطني الداخلي أو الخارجي يُعدُّ فعلاً غير مشروع ويعاقب الجاني بالسجن مدة لا تزيد عن عشر سنوات وبغرامة لا تزيد على خمس ملايين ريال أو بإحدى هاتين العقوبتين، كما جرَّم المُنظم السعودي فعل الدخول إلى المواقع الإلكترونية مِنْ أجل حذف البيانات أو تدميرها أو تسريبها أو إتلافها أو إعادة نشرها وعاقب على ذلك بالسجن مدة لا تقل عن أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين.(انظر المواد ١/٥، ٢/٧ مِنْ نظام مُكافحة جرائم المعلوماتية السعودي رقم م/١٧ تاريخ ١٤٢٨/٣/٨ه).

وحسناً فعل المُنظم السعودي بتشديد العقوبات على كلِّ شخص قام بالدخول إلى المواقع الإلكترونية بطريقة غير مشروعة، لخطورة هذا الفعل على أمن الدَّول والأفراد على حدٍ سواء.

كذلك جرَّم المُشرِّع المصري فعل الدخول إلى أي موقع إلكتروني بصورة غير مشروعة سواء أكان الدخول للموقع الإلكتروني عمداً أو بصورة الخطأ وعاقب على ذلك بالسجن مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنية ولا تتجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين، وإذا ترتب على الدخول للموقع الإلكتروني تعديل البيانات أو حذفها أو تغييرها أو نسخها أو إعادة نشر المعلومات، فقد شدَّد المُشرِّع المصري العقوبة لتصبح الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنية ولا تزيد عن مائتي ألف جنية أو بإحدى هاتين العقوبتين.(انظر المادة ١٤ مِنْ قانون تقنيَّة المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م).

ويمكن القول - إنَّ المُشرِّع المصري قد وقع في خطأ تشريعي يستدعي تعديل نص المادة ١٤ مِنْ قانون تقنيَّة المعلومات عندما ساوى في العقوبة بين الدخول إلى المواقع الإلكترونية بصورة عمدية أو خطأ، وهذا يخالف المبادئ العامة في القانون الجنائي والتي تفترض أنَّ عقوبة الفعل الخاطئ أقلُّ جسامةً مِنْ عقوبة الفعل القصدي أو العمدي وهذا متفق عليه في الفقه والقضاء ومعظم التَّشريعات الجنائية.

ويرى جانب مِنَ الفقه أنَّ مِنْ صور تدمير المواقع الإلكترونية مِنْ قِبَلِ الجماعات الإرهابية محاولة تعديل البيانات أو التلاعب فيها أو الغائها أو تحويلها بطريقة غير صحيحة بواسطة المعالجة الآلية للبيانات والمعلومات داخل المواقع الإلكترونية دون إذن مِنْ مالك الموقع الإلكتروني وبصورة تشكل فعلاً جُرميَّاً مخالف للقوانين المعمول بها. (الشوابكة، محمد أمين،٢٠٠٤، ص١).

ويرى جانبٌ أخر مِنَ الفقه أنَّ الدخول إلى المواقع الإلكترونية بوسائل غير مشروعة يسمى" القرصنة" ويقصد بذلك الدخول إلى أجهزة الحاسوب المملوكة للغير بوسائل غير مشروعة مِنْ أجل مهاجمة المعلومات والبيانات داخل جهاز الحاسوب والمساس بالسرية التامة لأمن المعلومات أو المحتوى أو تعطيل القدرة والكفاءة للأنظمة بقصد شلّ قدرتها على القيام بأعمالها. (محمود، جميل زكريا، ٢٠٠٥، ص١٤٧).

ج- التجسس على المواقع الإلكترونيَّة:

يُعرَّف التجسس الإلكتروني بأنَّه " الاطلاع على المعلومات الخاصة بالغير، والمؤمنة في جهاز الحاسوب أو الموقع الإلكتروني، حيث لا يجوز لغير المعنيين الاطلاع على هذه المعلومات أو البيانات. (العلماء، محمد عبد الرحيم سلطان، ٢٠٠٤، ص٨٨٠).

ويعتاد مجرمي المنظمات والجماعات الإرهابية ومرتكبي الجرائم المنظمة على الإقدام وبشكل مستمر لسلوك التجسس على المواقع الإلكترونية مِنْ أجل الحصول على المعلومات والبيانات لإتمام وارتكاب جرائمهم، وذلك مِنْ خلال زرع حصان طروادة في جهاز المجني عليه بطرق ووسائل مختلفة، وهذا ما أكدت عليه المباحث السرية الأمريكية (the us secret service) بأنَّ هذه الجماعات تمتهن التسلل للمواقع الإلكترونية لارتكاب جرائمها وتحقيق غاياتها المتمثلة في زعزعة استقرار الدّول والمجتمعات. (داود، حسن ظاهر، ٢٠٠٠، ص٨٩-٩٣).

"وقد جرَّمت العديد مِنَ التَّشريعات الجنائيَّة فعل التجسس على البيانات والمعلومات لخطورته وأثره على أمن الدَّول والأفراد، ومِنْ هذه التَّشريعات قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م والذي عاقب بالسجن مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن مائتي دينار ولا تزيد عن ١٠٠٠ دينار أو بكلتا هاتين العقوبتين كل شخص تنصَّت أو اعترض أو التقط كل ما هو مُرسل عنْ

طريق الشبكة المعلوماتيَّة بطريقة غير مشروعة".(انظر المادة ٥ مِنْ قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م).

د- نشر الفيروسات الإلكترونية:

ويقصد بها " برامج مِنْ نوع خاص " خارجية" صُنعت قصداً بهدف تغيير خصائص الملفات التي تستهدفها مِنْ أجل أن تقوم بتنفيذ بعض الأوامر بالإزالة، أو التعديل، أو الإلغاء، أو التخريب بُغية إلحاق الضرر بجهاز الحاسوب أو السيطرة عليه وأخذ المعلومات والبيانات منه أو تدميرها أو غيرها مِنَ الأفعال والتي تُعدُّ مِنْ صور جرائم الإرهاب الإلكتروني". (نقلاً عنْ مجاهد، توفيق، عباسة، طاهر، مرجع سابق، ص٨٥).

ومِنَ الفيروسات والتي يمكن أن تخترق الأجهزة الإلكترونية وتقوم بتدمير المعلومات والبيانات فيها أو تحذفها أو تُحرفها ما يلي:

أ-فيروسات الجزء التشغيلي للأسطوانة (Brain)

ب-الفيروسات المتطفلة وتسمى (Cascade)

ج- الفيروسات المتعدِّدة الأنواع (Flip)

د- أحصنة طروادة. (مقابلة، حسن يوسف، ٢٠١١، ص١٠٩).

ب- (النتيجة الجرميَّة):

تتلخص النتيجة الجرميَّة في جرائم الإرهاب الإلكتروني، في أنَّها تتصل بشكل واسع بعنصر الخطر والمتمثل بترويع الناس وتخويفهم، وتستخدم لتحقيق هذه النتيجة في جرائم الإرهاب الإلكتروني وسائل نفسيَّة تختلف عنْ الوسائل المستعملة في الجرائم الجنائيَّة التقليدية. (العفيف، محمد عبد الكريم، ٢٠١١، ص١٤٠-١٤٤).

ويزداد ارتكاب جرائم الإرهاب الإلكتروني في الدَّول المتقدِّمة والتي تعتمد بنيتها التحتيَّة على استخدام الأجهزة الإلكترونية والتقنيات المتطورة، ممَّا يجعلها هدفاً سهلاً مِنْ قِبَلِ المنظمات والجماعات الإرهابية، حيث تستطيع هذه الجماعات ومِنْ خلال الضغط على لوحة المفاتيح إحداث تدمير واسع النطاق يفوق بشكل كبير استخدام الأسلحة التقليدية كالمتفجرات، أو قطع شبكات الاتصال أو شل أنظمة السيطرة أو أنظمة الدفاع الجوي أو التحكم في خطوط الملاحة الجوية أو التحكم والسيطرة في أعمال البنوك أو القطاع المصرفي وبالتالي فإنَّ النتائج المترتبة على هذه السلوكيات والأفعال تُعدُّ نتائج ضاره وخطيرة على أمن الدَّول والمجتمعات، وهذا ما تتميَّز به جريمة الإرهاب الإلكتروني عنْ غيرها مِنْ الجرائم التقليدية.(عسيري، علي بن عبد الله، ٢٠٠٦، ص٩١).

وتطبيقاً لذلك قضت محكمة التمييز الأردنية في أحد قراراتها بأنَّه " تتمثل النتيجة الجرميَّة في جرائم الإرهاب الإلكتروني في تطبيق نص المادة ٦/٧ من قانون منع الإرهاب الأردني والذي بموجبه يجب على النيابة العامة أن تتثبت في جرائم الإرهاب

الإلكتروني مِنْ أنَّ المتهم استخدم نظام المعلومات أو شبكة المعلوماتية أو أي وسيلة نشر أو إعلان أو موقع إلكتروني لتسهيل القيام بأعمال إرهابية وتحقيق النتيجة الجرميَّة" (انظر تمييز جزاء أردني رقم ١٣٧٨ لسنة ٢٠١٧م، محكمة التمييز الأردنية).

ج- (العلاقة السببيَّة):

تُعدُّ العلاقة السببيَّة الأساس لتحديد المسؤولية الجزائية، وهي مِنْ العناصر المهمة المكونة للركن المادي للجريمة، سيَّما وإنَّ العلاقة السببيَّة تقوم على الربط بين السلوك الجرمي وتحقيق النتيجة الجرميَّة. وهل أنَّ السلوك الجرمي أدى فعلاً إلى حدوث النتيجة الجرميَّة أم لا؟ لذلك لا تثور الصعوبة إذا كان السلوك الجرمي قد أدى فعلاً إلى حدوث النتيجة الجرميَّة مباشرة دون أن يتداخل مع فعل الجاني عوامل آخرى، أمَّا إذا تتداخل مع فعل الجاني عوامل آخرى نتج عنها حدوث النتيجة الجرميَّة فقد انقسم الفقه الجنائي إلى ثلاث نظريات على النحو الآتي:

- نظرية تعادل الأسباب: ويرى أنصار هذه النظرية أنَّ جميع العوامل تُعدُّ متساوية في إحداث النتيجة الجرميَّة، حيث يربط بين السلوكيات والعوامل علاقة سببيَّة متساوية.
- نظرية السببيَّة الملائمة: ويرى أنصار هذه النظرية أنَّ السبب الملائم والكافي هو المسؤول عنْ النتيجة الجرميَّة ولا علاقة للأسباب والعوامل الأخرى المتداخلة مع السبب الكافي بالمسؤولية الجزائية.
- نظرية السبب المباشر: ويرى أنصار هذه النظرية أنَّ الجاني لا يسأل عنْ فعله غير المشروع إلاَّ إذا كان فعله هو المباشر والرئيسي لأحداث النتيجة الجرميَّة، حتى لو تتداخل مع فعل الجاني عوامل آخرى. (إبراهيم، أكرم نشأت، ١٩٩٨، ص٩٠).

وبإسقاط العلاقة السببيَّة وربط ذلك بما ذكرناه سابقاً بجرائم الإرهاب الإلكتروني، نجد بأنَّ العلاقة السببيَّة في هذا النوع مِنْ الجرائم تكمن بالبحث عنْ الصلة بين استخدام شبكة الإنترنت أو الشبكة المعلوماتية كوسيلة لارتكاب جرائم الإرهاب الإلكتروني بصورها المتعدِّدة (كالتحريض على الدَّولة أو تعطيل النظام المصرفي أو تعطيل خطوط الملاحة الجوية والبحرية مِنْ خلال الدخول إلى الأنظمة الإلكترونية الخاصة بها أو التجسس على البيانات الخاصة والعامة الخ...) حيث يكون لهذه الوسائل أو السلوكيات غير المشروعة صلة بالنتيجة الضارة المترتبة على قيام الجاني بارتكاب الأفعال غير المشروعة والتي خالف بموجبها الجاني القوانين المعمول بها وأثر على أمن الدَّول والمجتمعات وأحدث الرعب والفزع بين الناس.(الجابري، إسراء طارق، مرجع سابق، ص٧٥-٧٦).

ويرى الباحث - أنَّ اثبات الصلة بين قيام الجاني بالأفعال غير المشروعة المكونة لجريمة الإرهاب الإلكتروني وحدوث النتيجة الجرميَّة يقع على عاتق النيابة

العامة ومحكمة الموضوع بما يُقدم إليهما مِنْ أدلة ووقائع وبما لمحكمة الموضوع مِنْ صلاحية في وزنِ البينات.

الفرعُ الثَّاني: الركن المعنوي لجريمة الإرهاب الإلكتروني

تتكون الجريمة بالإضافة إلى الكيان المادي العنصر النفسي، فالجريمة ليست عنصراً مادياً فقط، بل تتكون ايضاً مِنْ عنصر نفسي، لذلك يُعدُّ الكيان النفسي للجريمة مكون أساسي للركن المعنوي ويمثل الأصول النفسيَّة لماديات الجريمة، فكلما سيطرت الإرادة على ماديات الجريمة أدى ذلك إلى تعدُّدِ صور الركن المعنوي، لذلك فإنَّ الإرادة كعنصر مِنْ عناصر الركن المعنوي صورتان هما (الخطأ، القصد) لنكون أمام جرائم قصدية أو جرائم خطأ. (المجالي، نظام توفيق، مرجع سابق، ص٣٢٥).

كما عرَّفها جانبٌ أخر مِنَ الفقه بأنَّها" الأصول النفسيَّة لماديات الجريمة". (حسني، محمود نجيب، ١٩٦٤، ص٣٣).

نستنتج ممَّا سبق - أنَّ مفهوم الركن المعنوي للجريمة يتمثل في " الكيان النفسي للجريمة والذي يتكون مِنْ عنصري العلم، والإرادة المسيطرين على ماديات الجريمة واحداث النتيجة الجرميَّة".

لذا فإنَّ الركن المعنوي للجريمة يتكون مِنْ عنصري (العلم، والإرادة) وسنناقش هذه المحاور على النحو الآتي:

١-العلم: أي علم الجاني بوقائع الجريمة، والعناصر المكونة لها، وبأنَّ كلّ الأفعال والسلوكيات التي سيرتكبها الجاني هي مخالفة للقانون، وهذا ينصرف على جرائم الإرهاب الإلكتروني كجريمة مستحدثة والتي يجب أن ينصَّب علم الجاني فيها على الوقائع والأفعال غير المشروعة والمتمثلة على سبيل المثال لا الحصر في الدخول إلى المواقع الإلكترونية لحذف البيانات أو تحوير المعلومات أو تعديلها أو تعطيل حركة الملاحة البحرية أو الجوية، أو التجسس على البيانات المدنيَّة أو العسكرية للدَّول، أو تفجير بعض المواقع الحكومية أو الخاصة عنْ طريق استخدام الأجهزة الإلكترونية وغيرها مِنَ السلوكيات والأفعال المكونة لجريمة الإرهاب الإلكتروني.

٢-الإرادة: وتعني انصراف إرادة الجاني إلى الفعل والنتيجة الجرميَّة، بمعنى إرادة القيام بالفعل غير المشروع وتحقيق النتيجة الجرميَّة المترتبة على القيام بالفعل. (الكساسبة، فهد يوسف، مرجع سابق، ص١٦١). "كما يجب أن تتجه إرادة الجاني إلى القيام بالسلوك الإجرامي، والنتيجة الجرميَّة المتمثلة في إلحاق ضرر فعلي بحياة الناس وأموالهم، كما يجب أن تتوجه إرادة الجاني إلى إرعاب الناس وتخويفهم، والتعرض لحقوقهم التي يحميها القانون". (كوران، يوسف، مرجع سابق، ص٩٤).

ويرى جانب مِنَ الفقه أنَّ بعض التَّشريعات الجنائية كالتَّشريع الأردني اشترطت لتوافر القصد العام بعنصريه العلم والإرادة في جرائم الإرهاب الإلكتروني توافر القصد الخاص والمتمثل في الاخلال بالنظام العام، وتعريض سلامة المجتمع وأمنه للخطر، واحداث الفزع والخوف بين الناس. (العفيف، محمد عبد الكريم، مرجع سابق، ص١٤٨).

ويرى بعض الفقهاء أنَّ القصد الخاص في جرائم الإرهاب الإلكتروني له غايتان: الأولى غاية قريبة، وتتمثل في القتل أو تدمير الممتلكات والأموال العامة والخاصة، أو تعطيل حركة الملاحة البحرية أو الجوية أو التجسس على البيانات والمعلومات الحكومية أو الخاصة أو محاولة حذف هذه البيانات أو تعديلها أو تحويرها بطريقة غير مشروعة وعبر الوسائط الإلكترونية، أمَّا الثانية: فهي الغاية البعيدة وتتمثل في زرع الرعب والخوف في قلوب الناس وإحداث الفزع بينهم، وتعطيل الحياة العامة بهدف تحقيق غايات خاصة لهذه الجماعات والمنظمات الإرهابية.(كوران، يوسف، مرجع سابق، ص٩٦).

وتطبيقاً لذلك قضت محكمة أمن الدَّولة في الأردن في أحد قراراتها بأنَّه" أمَّا فيما يتعلق بالقصد الخاص لجريمة الإرهاب الإلكتروني فإنَّه يتمثل في قصد الاخلال بالنظام العام، وتعريض سلامة المجتمع وأمنه للخطر المستفاد مِنْ نصِّ المادة (١٤٧) مِنْ قانون أصول المحاكمات الجزائية وهو ثابت للمحكمة مِنْ خلال ظروف وملابسات هذه الدعوى والبينات المقدَّمة فيها وبخاصة إفادة المتهم لدى المدعي العام الذي اعترف مِنْ خلالها أنَّه عقد العزم على محاربة الأنظمة العربيَّة ومِنْ ضمنها الدوائر الحكومية الأردنية وذلك مِنْ خلال إرسال الرسائل التهديدية الإلكترونية قاصداً بذلك الاخلال بالنظام العام وإثارة الخوف والفزع لدى العاملين فيها". (قرار صادر عنْ محكمة أمن الدَّولة في الأردن رقم ٢٠٠٥/١٣١م تاريخ ٢٠٠٥/٥/١١م منشورات مركز عدالة، الأردن).

وقضت أيضاً محكمة التمييز الأردنية في أحد قراراتها بانَّه " يتمثل القصد العام في جرائم الإرهاب أنَّ الهدف الأساسي للنشاط الإرهابي سواءً اكان تقليدي أو إلكتروني يكمن في إرادة إحداث الخوف في نفس الخصوم والناس، سيَّما وأنَّ العمل الإرهابي لا يعني فقط النتيجة المادية البحتة والمتمثلة بقيام الجاني بالعمل الإرهابي (قتلاً أو اعتداءً على الحرية أو تخريباً) أمَّا القصد الخاص فيكمن في الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر الهادف إلى إلقاء الرعب بين الناس" (انظر تمييز جزاء أردني رقم ٢٠٧٠ لسنة ٢٠٢٠م ، محكمة التمييز الأردنية).

المطلبُ الثّاني

جهود مُكافحة جريمة الإرهاب الإلكتروني على المُستوى الوطني والدَّولي

سارعت العديد مِنَ الدَّول سواء على المستوى الوطني أو الدَّولي إلى عقد الاتفاقيات الثنائية أو الجماعية لمُكافحة ظاهرة الإرهاب الإلكتروني، أو سن تشريعات تُجرم الأفعال المكونة لجريمة الإرهاب الإلكتروني، إلاَّ أنَّ الجهود الدَّولية في مكافحة هذا النوع مِنَ الجرائم ما زالت دون المستوى المطلوب، والسبب في ذلك يعود إلى التباين في مواقف وسياسات بعض الدَّول في كيفية التعاطي مع جرائم الإرهاب الإلكتروني، وهذا السبب حال دون عقد اتفاقية دولية موحدة تُعنى بمكافحة هذا النوع مِنْ الجرائم على المستوى الوطني والدَّولي، سيَّما وإنَّ هذا التباين في مواقف بعض الدَّول في التعاطي مع جرائم الإرهاب الإلكتروني دفع التنظيمات الإرهابية إلى توسيع دائرة جرائمها في العديد مِنْ دول العالم، لذلك سيناقش هذا المطلب محورين أساسين على النحو الآتي:

- الفرعُ الأوَّل: سُبل مُكافحة جرائم الإرهاب الإلكتروني وفقاً للتَّشريعات الجنائية الوطنية.
- الفرعُ الثّاني: سُبل مُكافحة جرائم الإرهاب الإلكتروني وفقاً للاتفاقيات الدَّولية.

الفرعُ الأوَّل: سُبل مُكافحة جرائم الإرهاب الإلكتروني وفقاً للتَّشريعات الجنائية الوطنية

سارعت اغلب الدَّول وعبر تشريعاتها بمُكافحة جرائم الإرهاب الإلكتروني، لكن الملاحظ أنَّ الدَّول وخصوصاً العربية لم تسن تشريعات خاصة لمُكافحة ظاهرة الإرهاب الإلكتروني، بل تم معالجة هذه الجريمة ضمن تشريعات مُكافحة جرائم الإرهاب التقليدي، أو التَّشريعات الخاصة بالجرائم المعلوماتية أو الإلكترونية على اعتبار أنَّ جرائم الإرهاب الإلكتروني تُعدُّ مِنْ ضمن الجرائم المعلوماتية أو الإلكترونية.

وفي التَّشريع الأردني عالج المُشرِّع الأردني جريمة الإرهاب الإلكتروني في قانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦م حيث اعتبر المُشرِّع الأردني مِنْ جرائم الإرهاب الإلكتروني استخدام أي شخص لنظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو اعلام أو إنشاء موقع الكتروني لتسهيل القيام بأعمال إرهابية أو دعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية، أو الترويج لأفكار جماعة إرهابية أو تمويلها أو القيام بأي أعمال تعرض حياة الناس وأمن المجتمع للخطر، ومِنْ باب مُكافحة ظاهرة الإرهاب الإلكتروني شدَّد المُشرِّع الأردني العقوبة بحيث تصبح الأشغال الشاقة المؤبدة إذا قام أي شخص بأحد الأفعال المكونة لجريمة الإرهاب الإلكتروني وهي على النحو الآتي:

١-إلحاق الضرر في ممتلكات عامة، أو خاصة، أو سفينة، أو طائرة، أو أي مِنْ وسائل النقل ولو كان الضرر جزئي.
٢-تعطيل الاتصالات وأنظمة الحاسوب واختراق شبكاتها بطريقة غير مشروعة.
(انظر المواد ٣/ه ٧/أ/١/٢ مِنْ قانون منع الإرهاب الأردني رقم ٥٥ لسنة ٢٠٠٦م).

ويرى الباحث - أنَّ التَّشريع الأردني في قانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦م لم يعالج ويجرِّم جميع الأفعال التي تنطوي تحت مفهوم الإرهاب الإلكتروني بشكل شمولي، فهنالك أفعال كان يجب على المُشرِّع ذكرها في النصِّ وتجريمها ومنها على سبيلِ المثال ما يلي:

١- جريمة التجسس على المواقع الإلكترونية العامة والخاصة باستخدام الأجهزة التقنيَّة مِنْ قِبَلِ المنظمات الإرهابية.
٢- جريمة الدخول للمواقع الإلكترونية مِنْ أجل حذف البيانات، أو المعلومات، أو تعديلها، أو تحويرها.
٣- جريمة تعطيل النظام المصرفي والبنكي بواسطة استخدام الأجهزة الإلكترونية.
٤- جريمة استهداف وتعطيل محطات الطاقة باعتبار الطاقة مِنْ الضرورات الأساسية لاستقرار الدَّول والمجتمعات.

لكن المُشرِّع الأردني جرَّم بعض الأفعال المكونة لجريمة الإرهاب الإلكتروني في قانون جرائم أنظمة المعلومات رقم ٣٠ لسنة ٢٠١٠م، حيث عاقب القانون كل شخص استخدم الشبكة المعلوماتية أو أنظمة المعلومات أو أنشأ موقعاً إلكترونيَّاً بهدف تسهيل العمل للقيام بجرائم إرهابية، أو مساعدة منظمات، أو جماعات إرهابية، أو الترويج لأفكارها، أو تمويلها بالأشغال الشاقة المؤقتة. (انظر المادة ١٠ مِنْ قانون جرائم أنظمة المعلومات رقم ٣٠ لسنة ٢٠١٠م).

ويمكن القول - أنَّ المُشرِّع الأردني لم يجمع جميع السلوكيات والأفعال المكونة لجريمة الإرهاب الإلكتروني تحت مظلة تشريع واحد بل شتت تجريم هذه الأفعال في العديد مِنْ القوانين ذات الصلة بصورةٍ يصعب فيها على القضاء الرجوع إلى النص الواجب التطبيق على الواقعة المعروضة عليه، وهذا واضح مِنْ تعدد المرجعيات القانونية للنصوص التي تُجرِّم جريمة الإرهاب الإلكتروني في التَّشريع الجنائي الأردني والذي جرَّم هذه الأفعال إمَّا في قانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦م أو في قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥م أو في قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م. لذا فإنني أتمنى على المُشرِّع الأردني تجريم جميع الأفعال المكونة لجريمة الإرهاب الإلكتروني في قانون منع الإرهاب أو سن تشريع

خاص يُعني بتجريم كل الأفعال المكونة لجريمة الإرهاب الإلكتروني لتكون الصورة واضحة للقضاء وللجهات المنفذة للقانون.

أمَّا في النظام السعودي فقد جرَّم المُنظم السعودي بعض الأفعال ذات الصلة في الإرهاب الإلكتروني مثل استخدام الأجهزة الإلكترونية أو التقنيَّة لتسهيل الاتصال بإحدى القيادات أو الأفراد ذات الصلة بالجماعات الإرهابية أو ترويج أفكارهم أو تمويلهم أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أسلحة لاستخدامها في تنفيذ جريمة إرهابية، أو تعطيل حركة الملاحة الجوية أو البحرية أو البرية أو نشر أي أخبار كاذبة أو مُغرضة عبر وسائل تقنيَّة المعلومات مِنْ أجل تنفيذ جريمة إرهابية.(انظر المواد ٤٢/٤٣/٤٤ مِنْ نظام مُكافحة جرائم الإرهاب وتمويله السعودي والصادر بالمرسوم الملكي رقم م/٢١ تاريخ ١٤٣٩/٢/١٢ه).

ونلاحظ أنَّ المُنظم السعودي تميَّز عنْ المُشرِّع الأردني بإضافة وصف " استخدام الأجهزة التقنيَّة لتصنيع الأسلحة والمتفجرات بكافة أنواعها لتنفيذ عمليات إرهابية" وحسناً فعل المُنظم السعودي بتجريم هذا الفعل، سيَّما وإنَّ المنظمات الإرهابية اعتادت في الفترة الأخيرة على تصنيع الأسلحة وبيعها بكافة أنواعها عبر الوسائط الإلكترونية وهذا يتطلب مِنَ الدَّول وعبر تشريعاتها تشديد العقوبات على هذا الفعل غير المشروع، والتعاون بينها على المستوى الأمني بحيث يكون التعاون والتنسيق " إلكتروني عالي المُستوى " لمُكافحة هذه الظاهرة الخطيرة على أمن الدَّول والمجتمعات.

ويرى جانب مِنَ الفقه أنَّ بيع الأسلحة يخضع لإجراءات صارمة مِنْ قِبَلِ الدَّول، غير أنَّ ثورة تكنولوجيا المعلومات والاتصالات "الإنترنت" سمحت ببيع هذه الأسلحة بالخفاء مِنْ قِبَلِ المنظمات الإرهابية عبر وسطاء مُتخصِّصين في مجال بيع الأسلحة. (مظلوم، محمد جمال، ٢٠١٣، ص٢٠).

ومِنْ جانب تشديد الرقابة والإجراءات على المنظمات الإرهابية ومرتكبي جرائم الإرهاب الإلكتروني أصدر مجلس الوزراء السعودي قراره رقم ١٦٣ تاريخ ١٤١٧/١٠/٢٢ه والمتضمن وضع الضوابط الخاصة والمنظمة لاستخدام شبكة الإنترنت وقد نصَّ القرار على ما يلي:

١- "الامتناع عنْ الدخول إلى أي موقع إلكتروني أو أنظمة حاسب آلي دون الحصول على موافقة المالكين.
٢- الامتناع عن إرسال أو استقبال معلومات مشفرة إلاَّ بعد الحصول على التراخيص اللازمة مِنْ إدارة الشبكة المعنية.
٣- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية عند النفاذ إليها.
٤- الامتناع عنْ الدخول إلى حسابات الآخرين أو محاولة استخدامها بدون تصريح.
٥- الامتناع عنْ تعريض الشبكة الداخلية للخطر وذلك بواسطة فتح ثغرات أمنية عليها.

٦- الالتزام بما تصدره وحدة خدمات (الإنترنت) بمدينة الملك عبد العزيز للعلوم والتقنيَّة مِنْ ضوابط وسياسات لاستخدام الشبكة". (الزعابي، ناصر محمد البكر، مرجع سابق، ص٤٣).

وحسناً فعل مجلس الوزراء السعودي لوضع هذه الضوابط والتي مِنْ شأنها تشديد الرقابة على الجماعات الإرهابية ومرتكبي جرائم الإرهاب الإلكتروني.

وفي هذا الاطار كانت الإمارات العربية المتحدة ايضاً مِنْ أوائل الدَّول في وضع قواعد قانونية وإجرائية صارمة لمُكافحة جرائم الإرهاب التقليدي، والإرهاب الإلكتروني وتمويله، حيث خصَّصت لائحة مستقلة تُعنى بوضع الضوابط القانونية والإجرائية لمراقبة الأموال مِنْ أجل مُكافحة جرائم غسل الأموال وتمويل الإرهاب للمنظمات والجماعات الإرهابية تحت مسمى "اللائحة التنفيذية للمرسوم بقانون اتحادي رقم ٢٠ لسنة ٢٠١٨م" في شأن مكافحة جرائم غسل الأموال وتمويل الإرهاب والصادرة بقرار مجلس الوزراء الإماراتي رقم ١٠ لسنة ٢٠١٩م، حيث تكونت اللائحة مِنْ ٦١ مادة معظمها ركزت على تجفيف الأصول المالية للمنظمات والجماعات الإرهابية، ومراقبة تداول الأموال داخل حدود الدَّولة مِنْ أجل ضمان عدم وصول هذه الأموال للمنظمات الإرهابية.

وفي باب مُكافحة جرائم الإرهاب الإلكتروني، نجد أيضاً بأنَّ المُشرِّع المصري شدَّد العقوبات والرقابة على المنظمات الإرهابية مِنْ حيث متابعة تصرفات هذه الجماعات، والرقابة المالية الصارمة على تمويل هذه المنظمات، والأفراد والجهات المتعاملين معها.

وقد جرَّم المُشرِّع المصري جميع الأفعال غير المشروعة والتي تشكل خطراً على أمن الدَّول والمجتمعات، وعاقب كل شخص قام بإعداد أو تدريب فرد أو أفراد على صناعة أسلحة تقليدية، أو حديثة، أو وسائل اتصالات لاسلكية، أو إلكترونية، أو أي وسيلة تقنيَّة أخرى أو التعليم على فنون حربيَّة أو استخدام وسائل تقنيَّة حديثة بقصد ارتكاب جرائم إرهاب إلكتروني أو تقليدي، وعاقب على هذه الأفعال بالسجن المؤبد أو السجن المُشدَّد بمدة لا تقل عنْ عشرين سنة. (انظر المادة ١٥ مِنْ قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م).

كما شدَّد المُشرِّع المصري العقوبة على المنظمات الإرهابية إذا دخلت بطريقة غير مشروعة على المواقع الإلكترونية الحكومية مِنْ أجل الحصول على البيانات أو التجسس عليها أو القيام بتعديلها، أو إتلافها، أو حذفها، أو تغيير الحقيقة فيها بطريقة غير مشروعة وعاقب على هذه السلوكيات غير المشروعة بالسجن مدة لا تقل عنْ عشرين سنة. (انظر المادة ٢٩ مِنْ قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م).

وفي مجال مُكافحة تمويل جرائم الإرهاب الإلكتروني والتقليدي، فقد اغلق المُشرِّع المصري الباب على المنظمات الإرهابية والأفراد والجهات التي تتعامل معها،

مِنْ خلال تشديد العقوبات على كل شخص أو جهة قامت بجمع أو حيازة أو امداد أو أخذ أو نقل ذخائر أو أسلحة أو مفرقعات أو الآت أو بيانات أو معلومات لأي منظمة إرهابية داخليا أو خارجياً بصورة مباشرة أو غير مباشرة وباستخدام وسائل سواء رقميَّة أو تقنيَّة بقصد وبغرض ارتكاب جرائم إرهاب إلكتروني أو تقليدي وعاقب على هذه الأفعال بالإعدام وبغرامة لا تقل عنْ مائة ألف جنيه ولا تتجاوز ثلاثة ملايين جنيه.(انظر المواد ٣، ١٣ مِنْ قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م).

وكإجراء استباقي لملاحقة المنظمات الإرهابية ومُكافحة جرائم الإرهاب الإلكتروني، "أجاز المُشرِّع المصري للنيابة العامة أن تأذن وبصورة مُسببة لرجال الشرطة ولمدة لا تزيد عنْ ثلاثين يوماً بمراقبة المحادثات والرسائل التي ترد على وسائل الاتصال السلكي واللاسلكي أو وسائل الاتصال الحديثة وتصوير ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها وضبط المكاتبات والرسائل العادية أو الإلكترونية".(انظر المادة ٤٦ مِنْ قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م).

وتطبيقاً للك قضت محكمة النقض المصرية في أحد قراراتها بأنَّه " إذا كان إذن النيابة العامة صادر مِنْ أجل تفتيش خط نت مملوك لشخص معين بهدف ضبط جهاز الحاسب الآلي، وكذلك لتتبع أي وصلات مِنَ الجهاز المربوط بالسنترال لبيان فيما إذا كان استخدامها له علاقة بالجريمة المرتكبة، وعند انتقال مأمور الضبط الجنائي مِنْ أجل مقابلة مالك المنزل تبين أنَّ مالك المنزل لدية وصلة إنترنت مأخوذة منه، فتتبع رجال الضبط الجنائي الوصلة المأخوذة مِنْ مالك المنزل وقاموا بالدخول للشقة التي أخذت الوصلة مِنْ مالكها وتم طرق باب الشقة وتفتيشها مِنْ قِبَلِ رجال الضبط الجنائي وفحص جهاز الحاسوب الذي هو في حوزة المتهم وتبين وجود عبارات تحريضية ضد مؤسسات الدولة، وبعد ذلك قاموا رجال الضبط الجنائي بالقبض على المتهم متلبساً بالجريمة، كما قررت المحكمة أنَّ دخول الضابطين مسكن الطاعن وضبط جهاز الكمبيوتر المستخدم يُعدُّ صحيحاً ومشروعاً". (انظر قرار محكمة النقض المصرية رقم ٢٢٩٥٣/ ٨٦ جلسة مجموعة أحكام محكمة النقض المصرية، الدائرة الجنائيَّة، تاريخ ٢٠١٧/٤/٢٧م).

ويمكن القول - أنَّ المُشرِّع المصري عالج في قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م جميع الأفعال ذات الصلة في الإرهاب الإلكتروني والتقليدي (الشق الموضوعي) بشكل شمولي، كما نصَّ المُشرِّع المصري على جميع الإجراءات الشكلية ذات الصلة في جرائم الإرهاب الإلكتروني كضبط الأشياء والأجهزة الإلكترونية ومراقبتها، ومراقبة جميع وسائل الاتصال السلكية واللاسلكية عكس باقي قوانين مُكافحة الإرهاب الإلكتروني والتي اكتفت بتحديد الأفعال التي تُعد جرائم إرهاب إلكتروني أي الجانب الموضوعي دون الإشارة إلى الإجراءات الشكلية كالضبط، وتتبع الإرهابين، ومراقبة أجهزتهم، بل احالت ذلك إلى قوانين الإجراءات الجنائية باعتبارها قوانيين شكلية ترسم الاطار الشكلي للجريمة وليس الموضوعي.

ويرى الباحث - أنَّ إيجاد تشريع مستقل لمُكافحة جرائم الإرهاب الإلكتروني سيكون له الأثر على مكافحة هذا النوع مِنَ الجرائم، سيَّما في ظلِّ ازدياد استعمال المنظمات الإرهابية لشبكات الاتصالات وتكنولوجيا المعلومات لتنفيذ اجنداتها ومخططاتها الإجراميَّة بحق الدَّول والمجتمعات، أمَّا النص على جرائم الإرهاب الإلكتروني في ثنايا قوانين مكافحة الإرهاب أو الجرائم الإلكترونية أو المعلوماتية سيؤدي إلى تشعب النصوص القانونية الناظمة لمُكافحة جرائم الإرهاب الإلكتروني، وعدم توحيد المرجعيات المتخصِّصة في الرقابة على جرائم الإرهاب الإلكتروني.

الفرعُ الثّاني: سُبل مُكافحة جرائم الإرهاب الإلكتروني وفقاً للاتفاقيات الدَّولية

سارعت معظم دول العالم إلى تعزيز التعاون الدَّولي بينها مِنْ أجل مُكافحة جرائم الإرهاب الإلكتروني سواء كان ذلك بعقد الاتفاقيات الدَّولية أو الثنائية بين الدَّول، أو مِنْ خلال التعاون الأمني وتبادل المعلومات بشأن الإرهابين أو الجماعات المرتكبة لهذه الجرائم، لذا سنسلط الضوء على الجهود الدَّولية والعربية ذات الصلة بمكافحة ظاهرة الإرهاب التقليدي والإلكتروني على وجه العموم في محورين أساسين على النحو الآتي:

أ-الجهود الدَّولية لمُكافحة الإرهاب الإلكتروني والتقليدي

"بدأت أولى الجهود الدَّولية لمُكافحة جرائم الإرهاب في العصر الحديث عندما استضافت المملكة العربية السعودية في شباط ٢٠٠٥م المؤتمر الدَّولي لمُكافحة الإرهاب في الرياض، وقد تمخَّض عنْ المؤتمر اعتماد وإقرار الجمعية العامة للأمم المتحدة أنشاء "المركز الدَّولي لمُكافحة الإرهاب " وقد كان هذا الإجراء هو البادرة الأولى لمُكافحة جرائم الإرهاب ومنها ظاهرة الإرهاب الإلكتروني، وبناء على ذلك تم تأسيس المركز الدَّولي لمُكافحة الإرهاب في ١٨ تشرين الثاني نوفمبر لعام ٢٠١١م، وبدأ تشغيل المركز والعمل به في شهر نيسان عام ٢٠١٢م، وقد تبرعت المملكة العربية السعودية بمبلغ ١٠٠ مليون دولار أمريكي للجنة مُكافحة الإرهاب كما قدمت أكثر مِنْ ثلاثين دولة الدعم المالي وذلك لاستمرار دعم المركز وتحقيق أهدافه، وفي شهر حزيران من عام ٢٠١٧م انشات الجمعية العامة للأمم المتحدة "مكتب الأمم المتحدة لمُكافحة الإرهاب" بموجب القرار رقم A/RESL/٢٩١ ، كما شكلت الأمم المتحدة في عام ٢٠١٨م مجلس استشاري تابع للمركز الدَّولي لمُكافحة الإرهاب ويتكون مِنْ ٢٢ عضواً ويترأس المجلس الاستشاري المملكة العربية نظراً لجهودها في مُكافحة الإرهاب على المستوى الدَّولي".(انظر الموقع الإلكتروني للأمم المتحدة – المركز الدَّولي لمُكافحة الإرهاب التابع للأمم المتحدة www.un.org).

وحسناً فعلت المملكة العربية السعودية بتوحيد الجهود الدَّولية لمُكافحة جرائم الإرهاب التقليدي والإلكتروني في ظل غياب وعدم اتفاق الدَّول على وضع آلية موحدة

للقضاء على ظاهرة الإرهاب ومنها الإلكتروني، وقد تبلورت مظاهر توحيد الجهود الدَّولية بإنشاء " المركز الدَّولي لمُكافحة الإرهاب" والذي سيكون له الدور الأساسي على المستوى الدَّولي للقضاء على هذه الظاهرة المؤثرة على أمن الدَّول والمجتمعات.

وفي مجال مُكافحة الإرهاب الإلكتروني صدر قرار مجلس الأمن الدَّولي رقم ٢٠١٧/٢٣٤١م والذي يقضي بأنَّه على الدَّول التعاون فيما بينها مِنْ تبادل الخبرات والمعلومات، والإستمرار في عمليات التدريب بهدف مُكافحة جرائم الإرهاب الإلكتروني، وقد أُتخذ هذا القرار بعد مراجعة الدَّول الأعضاء في مكتب الأمم المتحدة لمُكافحة الإرهاب (un counter – Terrorism center UNCCT) للاستراتيجية العالمية لمُكافحة الإرهاب (A/RES/٧٢/٢٨٤) والتي عبَّرت بموجبها الدَّول عنْ قلقها نتيجة تزايد استخدام المنظمات الإرهابية لشبكات الإنترنت والوسائط الإلكترونية لتنفيذ مخططاتها الإجرامية.(انظر الموقع الإلكتروني للأمم المتحدة www.un.org).

وفي شهر نوفمبر لعام ٢٠٠٢م اتخذت الجمعية العامة للأمم المتحدة قرار يقضي بمراقبة ميدان الاتصالات السلكية واللاسلكية، وقد تم الخروج بتوصية لإرساء ثقافة عالميَّة لأمن الفضاء الإلكتروني مِنْ خلال تشجيع الدَّول على زيادة التعاون فيما بينها لمُكافحة جرائم الإرهاب الإلكتروني. (شفيق، نوران، ٢٠١٥، ص١٠٨).

كما أنشأت الولايات المتحدة الأمريكية مركزاً يُعنى بمراقبة الفضاء الإلكتروني يسمى - مركز حماية البنيَّة الأساسية القومي. ومقره مكتب التحقيقات الفيدراليَّة الأمريكي بهدف وضع جميع شبكات الأمن الإلكتروني تحت رقابة المخابرات الأمريكية ومجلس الأمن القومي ومركز حماية البنيَّة الأساسية القومي وذلك مِنْ أجل توحيد الجهود لمُكافحة جرائم الإرهاب الإلكتروني. (موسى، مصطفى محمد، ٢٠٠٩، ص٢٩٨).

وفيما يتعلّق بالجهود الدّولية لمُكافحة جرائم الإرهاب التقليدي والإلكتروني على مستوى عقد الاتفاقيات الدَّولية تم التوقيع على الاتفاقية الأوربية لقمع الإرهاب عام ١٩٧٧م بهدف مُكافحة ظاهرة الإرهاب والتي اجتاحت اوروبا في مطلع السبعينات مِنْ القرن الماضي. (الجزولي، علاء الدين محمد موسى، ٢٠١٩، ص١٠٨).

كما وقعت نحو (٣٠) دولة مِنْ دول الاتحاد الأوربي في العاصمة المجرية الاتفاقية الدَّولية لمُكافحة الجرائم المعلوماتيَّة " اتفاقية بودابست" بتاريخ ٢٠٠١/١١/٢٣م ، وقد تكونت الاتفاقية مِنْ مُقدِّمة وأربعة أبواب ناقشت بموجبها الدَّول الاطار الموضوعي للجرائم المعلوماتيَّة، وكيفية مُكافحتها، كما تمَّ وضع الأسس الخاصة بالتعاون بين الدَّول الأعضاء لمُكافحة الجرائم المعلوماتيَّة والإرهاب الإلكتروني، وتضمنت الاتفاقية كذلك النص على القواعد الإجرائيَّة وجهات الاختصاص المُكلفة بتنفيذ وتطبيق بنود الاتفاقية.(أحمد، هلالي عبد الله، ٢٠١١، ص٣).

كما اهتمت منظمة الأمم المتحدة بمُكافحة الإرهاب بكافة اشكاله، حيث أصدرت ما بين عام ١٩٦٣م إلى عام ٢٠٠٥م (١٣) اتفاقية في مجال مُكافحة الإرهاب، كما ألزم

مجلس الأمن الدَّولي التابع للأمم المتحدة الدَّول على تجريم كل الأفعال ذات الصلة بالإرهاب ومنها الإرهاب الإلكتروني بموجب القرار الصادر عنه رقم ١٥٦٦/ ٢٠١٤م. (العذار، أنيس بن علي، الشافعي، خالد بن عبد الله، ٢٠١٧، ص٢٤٣).

ويرى الباحث - أنَّ الاتفاقيات الدَّولية ساهمت إلى حدٍّ مُعين في مُكافحة ظاهرة الإرهاب الإلكتروني، لكن التعاون بين الدَّول ما زال دون المستوى المطلوب، وهذا يتطلب زيادة التعاون الأمني وتبادل المعلومات بين الدَّول، وتفعيل عقد الاتفاقيات الثنائية مِنْ أجل القضاء على هذه الظاهرة المؤثرة على أمن المجتمعات والدَّول، ويقع ذلك على عاتق المركز الدَّولي لمُكافحة الإرهاب والتابع للأمم المتحدة والذي بدوره عليه مسؤولية حثّ الدَّول على التنسيق فيما بينها مِنْ أجل عقد الاتفاقيات الثنائية وتبادل المعلومات حول أمن المعلومات ومُكافحة الإرهاب الإلكتروني.

ب- الجهود العربيةَ لمُكافحة الإرهاب الإلكتروني والتقليدي

سارعت الدَّول العربية إلى مُكافحة جرائم الإرهاب الإلكتروني بعقد مجموعة مِنْ الاتفاقيات على المستوى العربي، ومِنْ الملاحظ أنَّ مُكافحة جرائم الإرهاب الإلكتروني كانت ضمن الاتفاقيات العربية ذات الصلة بجرائم تقنيَّة المعلومات أو جرائم الإرهاب التقليدي، بمعنى أنَّ جامعة الدَّول العربية لم تبادر إلى أنشاء اتفاقية عربية تُعنى بمُكافحة هذا النوع مِنْ الجرائم بشكلٍ مستقل، بل عالجتها ضمن الاتفاقية العربية لمكافحة جرائم الإرهاب أو ضمن النصوص الخاصة بالاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات.

وفي باب مُكافحة جرائم الإرهاب الإلكتروني على المستوى العربي، أقرت جامعة الدَّول العربية الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات والصادرة بتاريخ ٢١ ديسمبر عام ٢٠١٢م، وتتكون الاتفاقية مِنْ ٤٣ مادة عالجت معظم المواد فيها الأحكام الموضوعية والإجرائية لجرائم تقنيَّة المعلومات، وخصص جزء منها ايضاً لمُكافحة جرائم الإرهاب الإلكتروني. (محمود مدين، عبد الرحمن، ٢٠١٧، ص٦٤).

ويرى جانبٌ مِنَ الفقه أنَّ الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات جاءت متوافقة مع اتفاقية بودابست والتي تم توقيعها في اطار الاتحاد الأوربي بتاريخ ٢٠٠١/١/٢٢م مِنْ حيث القواعد الإجرائية، وقواعد الاختصاص القضائي، كما ألزمت الاتفاقية الدَّول الأطراف فيها على تعديل تشريعاتها بما يتلاءم مع نصوص الاتفاقية، كما نصَّت الاتفاقية على تشديد الإجراءات ذات الصلة بتفتيش البيانات والمعلومات داخل الأجهزة الإلكترونية والحجز عليها وصلاحية التجميع الفوري لها بما يضمن مُكافحة جرائم الإرهاب الإلكتروني وجرائم تقنيَّة المعلومات، وقد نصَّت الاتفاقية على تلك الصلاحيات في المواد مِنْ ٢٣ إلى ٢٩ مِنْ الاتفاقية، كذلك نصَّت المادة ٣٠ مِنْ الاتفاقية على تحديد الاختصاص القضائي عند وقوع جريمة إرهابية على إقليم إحدى الدَّول الأطراف في الاتفاقية سواء وقعت الجريمة على إقليم دولة جزئياً أو كلياً، وبذلك يتحدد الاختصاص القضائي وفقاً للضوابط التالية:

١- في إقليم دولة طرف في المعاهدة.
٢- على متن سفينة تحمل علم دولة طرف.
٣- على متن طائرة مسجلة لقوانين دولة طرف في المعاهدة.
٤- إذا كانت الجريمة تمس أحد مصالح الدَّولة العليا.

وينصرف ذلك على تحديد الاختصاص القضائي بجرائم الإرهاب الإلكتروني الواقعة على إقليم أي مِنْ الدَّول الأطراف في المعاهدة. (الزعابي، ناصر محمد البكر، بني إبراهيم، سلطان راشد، مرجع سابق، ص٤١-٤٢).

كما جرَّمت الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات والصادرة عام ٢٠١٢م بعض صور الإرهاب الإلكتروني والتي ترتكب عبر الوسائط الإلكترونية، ونصَّت على ذلك خلافاً لأحكام المادة (١٥) مِنْ الاتفاقية بما يلي:

١- نشر أفكار جماعات ومبادئ إرهابية والدعوة لها.
٢- تمويل العمليات الإرهابية والتدريب عليها، وتسهيل الاتصالات بين التنظيمات الإرهابية.
٣- نشر طرق وصناعات الأسلحة والتي تستخدم بشكلٍ خاص في تنفيذ العمليات الإرهابية.
٤- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

ويرى الباحث - أنَّ الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات جانبها الصؤاب والقصور في عدم النص على جميع السلوكيات والأفعال المكونة لجرائم الإرهاب الإلكتروني وهي كثيرة ومتعدِّدة نذكر منها على سبيل المثال ما يلي:

١- تعطيل الملاحة البحرية والجوية بفعل استخدام تقنيَّة المعلومات بطرقٍ غير مشروعة.
٢- تعطيل العمل بوسائل الطاقة وهي مِنْ ضرورات الحياة الرئيسية بفعل استخدام تقنيَّة المعلومات بطرقٍ غير مشروعة.
٣- التجسس على البياناتٍ والمعلومات العسكرية والأمنية للدول عنْ طريق الدخول غير المشروع للمواقع العسكرية والأمنيَّة بوسائل غير مشروعة.

كما صادقت الدَّول العربية على الاتفاقية العربية لمُكافحة جرائم الإرهاب والصادرة بقرار مجلس وزراء العدل والداخلية العرب في الاجتماع الذي عُقد في مقر الأمانة العامة للجامعة العربية بتاريخ ١٩٩٨/٤/٢٢م، وقد بدأ نفاذ الاتفاقية والعمل بها بتاريخ ١٩٩٩/٥/٧م، وتكونت الاتفاقية مِنْ ٤٢ مادة، خُصص الباب الأول للأحكام العامة والمفاهيم لمصطلح الإرهاب، أمَّا المادة الثانية مِنْ الاتفاقية فنصَّت على صور الإرهاب التقليدي نذكر منها على سبيل المثال (التعدي على ملوك ورؤساء الدول، التعدي على الأشخاص المتمتعين بحماية دولية، القتل العمد والسرقة المصحوبة بالإكراه،

أعمال التخريب للممتلكات العامة والخاصة الخ...) أمَّا باقي أبواب الاتفاقية فناقشت مسائل شكلية وإجرائية (كالتعاون الدَّولي في مُكافحة الإرهاب، والتعاون العربي، وتسليم المجرمين، والاختصاص القضائي).

ويمكن القول - وبعد مطالع نصوص الاتفاقية العربية لمُكافحة الإرهاب تبين أنَّها عالجت مُكافحة جرائم الإرهاب التقليدي مِنْ الجانب الشكلي فقط ولم تتناول صور الإرهاب التقليدي مِنْ الجانب الموضوعي إلاَّ في المادة (٢) مِنْ الاتفاقية، كما أنَّ الاتفاقية لم تنص على مُكافحة الإرهاب الإلكتروني وصورة في نص المادة (٢) مِنْ الاتفاقية، ولم تُعرِّف الاتفاقية كذلك في المادة الأولى منها الإرهاب الإلكتروني، وهذا قصور يتطلب معالجة الإرهاب بشتى صورة، سيَّما وإنَّ الإرهاب الإلكتروني كظاهرة يُعدُّ مِنْ الظواهر الخطيرة والمؤثرة في أمن المجتمعات والدَّول.

"وفي إطار مجلس التعاون الخليجي وافقت دول مجلس التعاون الخليجي على الإستراتيجية الأمنيَّة لمُكافحة التطرف والإرهاب في عام ٢٠٠٢م، ثم وافقت دول مجلس التعاون الخليجي واستكمالاً للإستراتيجية الأمنيَّة لمُكافحة الإرهاب والتطرف على " اتفاقية دول مجلس التعاون الخليجي لمُكافحة الإرهاب" والصادرة عام ٢٠٠٤م وقد كانت الاتفاقية نقطة تحول لمُكافحة هذه الظاهرة من عدة جوانب وعلى النحو الآتي:

١- الإبلاغ عنْ العناصر الإرهابية أو التي يشتبه بعلاقتها مع هذه العناصر ضمن منظومة دول مجلس التعاون الخليجي.
٢- انشأت دول مجلس التعاون الخليجي اللجنة الخليجية الدائمة للقائمة الإرهابية الموحدة، وتختص هذه اللجنة بأدراج، أو تعديل، أو رفع أسماء الجماعات، أو المؤسسات، أو الكيانات، أو الأفراد الذين ينتمون للمنظمات الإرهابية أو المنشقين عنها أو المتعاونين معها، بحيث تكون أسماؤهم في قائمة خليجية موحدة.
٣- إعداد تقرير سنوي يُلخص جهود مجلس التعاون الخليجي في مجال مُكافحة الإرهاب بشتى صوره سواء الإرهاب التقليدي أو الإلكتروني". (انظر الموقع الإلكتروني لمجلس التعاون الخليجي www.gcc-sg.org) .

ويرى الباحث - ضرورة تفعيل التعاون بين الدَّول العربية بصورة أوسع بحيث يتم أنشاء مركز عربي لمُكافحة الإرهاب التقليدي والإلكتروني على المستوى العربي يتبع للجامعة العربية قياساً على المركز الدَّولي والذي انشأته منظمة الأمم المتحدة ومقره فيها بهدف مُكافحة الإرهاب على المستوى الدَّولي، ويكون الهدف مِنْ أنشاء المركز ما يلي:

١- تفعيل التعاون العربي في مجال مُكافحة الإرهاب مِنْ خلال مراجعة الاتفاقيات الثنائية التي تُعقد بين الدَّول العربية في مجال الإرهاب، ومتابعة تنفيذ الدَّول العربية لبنود الاتفاقية العربية لمُكافحة الإرهاب والتي وقعت عليها مُعظم الدَّول العربية.
٢- عقد المؤتمرات والندوات في مجال مُكافحة ظاهرة الإرهاب التقليدي والإلكتروني.
٣- متابعة الدَّول العربية بخصوص تعديل تشريعاتها الوطنية بما يتوافق مع الاتفاقيات ذات الصلة بالإرهاب وخصوصاً الإلكتروني.
٤- تدريب الكوادر الأمنيَّة والقضائية على كيفية التعامل مع ظاهرة الإرهاب الإلكتروني.
٥- وضع الضوابط التَّشريعية لمراقبة الفضاء الإلكتروني العربي لضمان أمنة مِنْ عبثِ الجماعات الإرهابية.

الخاتمة :

تُعدُّ جرائم الإرهاب الإلكتروني مِنْ الجرائم المؤثرة على أمن الدَّول والمجتمعات مِنْ الجانب الاقتصادي والاجتماعي، والسياسي، سيَّما مع ازدياد ارتكاب هذه الجرائم مِنْ قِبَلِ المنظمات الإرهابية عبر وسائل الاتصالات وتكنولوجيا المعلومات، مُستغلين بذلك سهولة التعامل مع الوسائط الإلكترونية، وسرعة إخفاء الأدلة المتحصلة مِنْ خلال تعديلها أو حذفها أو تزويرها، ممَّا يسهل بالنتيجة على الجماعات الإرهابية سهولة ارتكاب الجرائم الإلكترونية بصورةٍ يصعب على الدَّول والأجهزة الأمنيَّة اكتشاف هذا النوع مِنْ الجرائم كما يحصل عند ارتكاب الجرائم التقليدية، لذلك سارعت الدَّول إلى إيجاد الحلول لمُكافحة ظاهرة الإرهاب الإلكتروني على المستوى (التَّشريعي، الأمني، الفكري). وقد انتهت الدراسة بمجموعة مِنَ النتائج والتوصيات نجملها على النحو الآتي:

- **النتائج:**

١- لم يجمع الفقه والتَّشريعات والمنظمات الدَّولية على مفهوم يُعدُّ جامعاً مانعاً لمصطلح الإرهاب التقليدي والإلكتروني.
٢- يزداد الإقبال على ارتكاب جرائم الإرهاب الإلكتروني مِنْ قِبَلِ المنظمات الإرهابية لسهولة التعامل مع الوسائط الإلكترونية، وضعف الرقابة الأمنية.
٣- يرتكب الإرهابين جريمة الإرهاب الإلكتروني في دول غير مستقرة سياسيَّاً واجتماعيَّاً واقتصادياً أو تعاني مِنْ حروب أهلية.
٤- تُعدُّ جريمة الإرهاب الإلكتروني جريمة وطنية ومِنْ اختصاص القضاء الوطني حتى ولو كان لها امتداد دولي.
٥- تتطلب جريمة الإرهاب الإلكتروني بالإضافة للقصد العام بعنصرية العلم والإرادة توافر القصد الخاص والمتمثل في تخويف الناس، واثارة الرعب والفزع بينهم.
٦- نصَّت التَّشريعات على جميع الأفعال غير المشروعة المكونة لجريمة الإرهاب الإلكتروني ضمن قوانين مُكافحة الإرهاب أو الجرائم المعلوماتية أو الإلكترونية دون سن تشريع خاص يُعالج جميع المسائل ذات الصلة بالإرهاب الإلكتروني.
٧- مُكافحة الإرهاب الإلكتروني على المستوى العربي لم يكن بالمستوى المطلوب مِنَ الجانب الأمني وعقد الاتفاقيات الثنائية، وتبادل المعلومات بين الدَّول.
٨- لم تنص بعض التَّشريعات والاتفاقيات العربية ذات الصلة بمُكافحة الإرهاب التقليدي أو الإلكتروني على جميع الأفعال غير المشروعة المكونة لجرائم الإرهاب الإلكتروني، فكانت التَّشريعات قاصرة مَّا أثر على مُكافحة ظاهرة الإرهاب الإلكتروني.

التوصيات:

١- التوصية بسن تشريع مستقل لمُكافحة جرائم الإرهاب الإلكتروني بدلاً مِنْ ترك النصوص الخاصة بهذا النوع مِنْ الجرائم في ثنايا قوانين مُكافحة الإرهاب أو قوانين الجرائم الإلكترونية أو المعلوماتية.

٢- التوصية بتعديل نص المادة (١٥) مِنْ الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات والصادرة عام ٢٠١٢م، والمادة (٢) مِنْ الاتفاقية العربية لمُكافحة الإرهاب والصادرة عام ١٩٩٨م للنصِّ والإشارة إلى جميع الأفعال غير المشروعة المكونة لجريمة الإرهاب الإلكتروني بما نضمن مُكافحة هذه الظاهرة على المستوى العربي.

٣- التوصية بإنشاء مركز عربي لمُكافحة الإرهاب التقليدي والإلكتروني على المستوى العربي يتبع للجامعة العربية قياساً على المركز الدَّولي والذي انشأته منظمة الأمم المتحدة ومقره فيها بهدف مُكافحة الإرهاب على المستوى الدَّولي، ويكون الهدف مِنْ إنشاء المركز ما يلي:

أ- تفعيل التعاون العربي في مجال مُكافحة الإرهاب مِنْ خلال مراجعة الاتفاقيات الثنائية التي تُعقد بين الدَّول العربية في مجال الإرهاب، ومتابعة تنفيذ الدَّول العربية لبنود الاتفاقية العربية لمُكافحة الإرهاب والتي وقعت عليها مُعظم الدَّول العربية.

ب-عقد المؤتمرات والندوات في مجال مُكافحة ظاهرة الإرهاب التقليدي والإلكتروني.

ج- تابعة الدَّول العربية بخصوص تعديل تشريعاتها الوطنية بما يتوافق مع الاتفاقيات ذات الصلة بالإرهاب وخصوصاً الإلكتروني.

د- تدريب الكوادر الأمنيَّة والقضائية على كيفية التعامل مع ظاهرة الإرهاب الإلكتروني.

هـ - وضع الضوابط التَّشريعية لمراقبة الفضاء الإلكتروني العربي لضمان أمنة مِنْ عبثِ الجماعات الإرهابية.

٤- التوصية بتعديل نصوص قانون منع الإرهاب الأردني رقم ٥٥ لسنة ٢٠٠٦م للنصِّ على بعض الأفعال غير المشروعة المكونة لجريمة الإرهاب الإلكتروني (كالتجسس على المواقع الإلكترونية العامة والخاصة، وجريمة تعطيل النظام المصرفي عبر استخدام الأجهزة التقنيَّة، وجريمة تعطيل واستهداف محطات الطاقة عبر الوسائط الإلكترونية، وجريمة صناعة الأسلحة والمتفجرات عبر الأجهزة التقنيَّة لتنفيذ عمليات إرهابية).

٥- التوصية بعقد مؤتمر دولي سنوي تحت رعاية الأمم المتحدة لمُكافحة جرائم الإرهاب التقليدي والإلكتروني، للخروج بتوصيات يمكن أن تساعد الدَّول بحل جميع الإشكاليات التي تُعرقل مُكافحة جرائم الإرهاب بشتى صورة وأنواعه.

٦- التوصية بتعديل نصوص الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات والصادرة عام ٢٠١٢م والاتفاقية العربية لمُكافحة الإرهاب والصادرة عام ١٩٩٨م، وذلك بإضافة جميع الأفعال غير المشروعة المكونة لجريمة الإرهاب الإلكتروني في نصوص الاتفاقيات المذكورة بما يضمن مُكافحة ظاهرة الإرهاب الإلكتروني على المستوى العربي.

قائمة المراجع:

- **المراجع القانونيَّة العامة والمتخصِّصة:**

١.إبراهيم، أكرم نشأت (١٩٩٨). القواعد العامة في قانون العقوبات المُقارن. بغداد: مطبعة الفتيان (ط١) ٩١.

٢.إبراهيم، ثامر (١٩٩٨). مفهوم الإرهاب في القانون الدَّولي. دمشق: دار حوران للطباعة، ٥٥.

٣.أحمد، هلالي عبد الله (٢٠١١). اتفاقية بودابست لمُكافحة جرائم المعلوماتيَّة مُعلقاً عليها. القاهرة دار النهضة العربية (ط٨)،٣.

٤.بوادي، حسنين محمد (٢٠٠٦). إرهاب الإنترنت – الخطر القادم. الإسكندرية: دار الفكر العربي (ط١)، ٥٤.

٥.حسني، محمود نجيب (١٩٦٤). قانون العقوبات – القسم العام. القاهرة: دار النهضة العربية، ٣٣.

٦.داود، حسن الظاهر (٢٠٠٠). جرائم نظم المعلومات. الرياض: جامعة نايف العربية للعلوم الامنيَّة – مركز الدراسات والبحوث (ط١)، ٨٩-٩٣.

٧.سرور، أحمد فتحي (٢٠٠٨). حكم القانون في مواجهةِ الإرهاب. بيروت: الدار الجامعية، ١١٠.

٨.شفيق، نوران (٢٠١٥). أثر التهديدات الإلكترونية على العلاقات الدَّولية – دراسة في أبعاد الأمن الإلكتروني. القاهرة: دار المكتب العربي للمعارف،١٠٨.

٩.الشوابكة، محمد أمين (٢٠٠٦). جرائم الحاسوب والإنترنت " الجريمة المعلوماتيَّة ". عمَّان: دار الثقافة للنشر والتوزيع (ط١)، ١.

١٠.عبد الرحمن، محمود مدين (٢٠١٧). الجريمة الإلكترونية وتحديات الأمن القومي. القاهرة المصرية للنشر والتوزيع، ٦٤.

١١.العموش، أحمد فلاح (٢٠٠٦). مستقبل الإرهاب في هذا القرن. الرياض: جامعة نايف العربية للعلوم الأمنيَّة – مركز الدراسات والبحوث(ط١)، ٩٠.

١٢.كوران، يوسف (٢٠٠٧). جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدَّولي. العراق: مركز كردستان للدراسات الإستراتيجية، ٧٣-٧٤.

١٣.المجالي، نظام توفيق (٢٠١٠). شرح قانون العقوبات. الأردن: دار الثقافة للنشر والتوزيع (ط٣) ٢١١.

١٤.مقابلة، حسن يوسف (٢٠١١). الجرائم الدَّولية للإنترنت. القاهرة: المركز القومي للإصدارات القانونيَّة (ط١)، ١٠٩.

١٥.موسى، مصطفى (٢٠٠٥). أساليب إجراميَّة بالتقنيَّة الرقميَّة – ماهيتها ومُكافحتها. مصر: دار الكتب القانونيَّة، ٧٤.

١٦.موسى، مصطفى محمد (٢٠٠٩). الإرهاب الإلكتروني – دراسة قانونية (أمنيَّة، نفسيَّة، اجتماعيَّة) الأردن: دار الكتب والوثائق القوميَّة(ط١)، ٢٩٨.

- **الدوريات (رسائل الماجستير والدكتوراه والأبحاث القانونيَّة المنشورة في المجلات المتخصِّصة):**

١٧. الجابري، إسراء طارق. (٢٠١٢) " جريمة الإرهاب الإلكتروني – دراسة مُقارنة" رسالة ماجستير غير منشورة، جامعة النهرين، العراق. ١٥٩.
١٨.الجزولي، علاء الدين محمد موسى. (٢٠١٩). جريمة الإرهاب وآليات مُكافحتها. مجلة العلوم الاقتصادية والإدارية والقانونيَّة، ١٠، ١٠٨.
١٩.حليم، رامي. (٢٠٠٩) جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات. مجلة دراسات وأبحاث زيان عاشور، الجلفة – الجزائر،١، ٣٤٩.
٢٠.الزعابي، ناصر محمد، بني إبراهيم، راشد بني رشيد. (٢٠١٩). تداعيات جرائم الإرهاب على استقرار الدُّول وأمنها. مجلة الفكر الشرطي – قيادة شرطة الشارقة – مركز الدراسات والبحوث،٢٨، ٢١.
٢١.العذار، أنيس بن علي، الشافعي، خالد بن عبد الله. (٢٠١٧). الإرهاب الإلكتروني. مجلة العلوم القانونيَّة، جامعة عجمان، ٥، ٢٣٧.
٢٢.العفيف، محمد عبد الكريم. (٢٠١١) " جرائم الإرهاب في قانون العقوبات الأردني " رسالة دكتوراه غير منشورة، جامعة عمَّان العربية للدراسات العليا – الأردن. ١٤٠ – ١٤٤.
٢٣.الكساسبة، فهد يوسف. (٢٠١٥). الإرهاب الإلكتروني في التَّشريع الأردني – دراسة مُقارنة. مجلة العلوم القانونيَّة والسياسيَّة، المجلة العلميَّة للبحوث والدراسات الإستراتيجية – العراق، ١، ١٣٥.
٢٤.مجاهد، توفيق، عباسة، طاهر. (٢٠١٨). جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمُكافحة جرائم تقنيَّة المعلومات لعام ٢٠١٠م. مجلة القانونيَّة والسياسيَّة – الجزائر، .٥٣
٢٥.المعداوي، وليد سمير فهيم. (٢٠٢٠). مُكافحة جرائم تقنيَّة المعلومات والإرهاب الإلكتروني وفقاً لأحدث التَّشريعات المصرية. مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة – مركز بحوث الشرطة، ١١٤، ٢٣٦.
٢٦.نظمي، رانيا محمد عزيز. (٢٠١٩). الفراغ الفكري وتأثيراته على الاستخدام السيء لتقنيَّة الاتصالات الحديثة. المجلة العربية للعلوم التربوية والنفسيَّة – مصر، ٨، ٢٠.

المؤتمرات العلميَّة المتخصِّصة:

٢٧.العدوان، رائد. (٢٠١٣) دورة تدريبية عُقدت في الرياض بعنوان " توظيف شبكات التواصل الاجتماعي في مُكافحة الإرهاب" في الفترة ما بين ٢٣-٢٠١٣/٢/٢٧م، ١٤.

٢٨.عسيري، علي بن عبد الله. (٢٠٠٦) بحث منشور بعنوان" الإرهاب والإنترنت" والمُقدم في ندوة" الإرهاب والقرصنة البحرية" والتي عُقدت في جامعة نايف العربية للعلوم الأمنيَّة – مركز الدراسات والبحوث، ط١، ٩١.

٢٩.العلماء، محمد عبد الرحيم سلطان. (٢٠٠٤) بحث منشور بعنوان " جرائم الإنترنت والاحتساب عليها" والمُقدم في مؤتمر " القانون والكمبيوتر والإنترنت" والذي عُقد في جامعة الإمارات العربية المتحدة كلية الشريعة والقانون في الفترة ما بين ١-٢٠٠٤/٥/٣م، المجلد الثالث، ط٣، ٨٨٠.

٣٠.محمود، جميل زكريا. (٢٠٠٥) بحث منشور بعنوان " الجريمة المعلوماتية وأساليب التأمين" والمُقدم في المؤتمر الدَّولي والذي عُقد في سلطنة عُمان بعنوان " أمن المعلومات الإلكترونية" في عام ٢٠٠٥م، ١٤٧.

٣١.مظلوم، محمد جمال. (٢٠١٣) بحث منشور بعنوان " التجارة غير المشروعة للسلاح والإرهاب" والمُقدم في الحلقة العلميَّة بعنوان " تجارة السلاح غير المشروعة وغسيل الأموال" والتي عُقدت في جامعة نايف العربيَّة للعلوم الامنيَّة في الفترة ما بين ٣-٢٠١٣/٢/١١م الموافق ١-١٤٣٤/٤/٣هـ، ٢٠.

- **التَّشريعات والاتفاقيات الدَّولية:**

١.قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠م.

٢.قانون تقنيَّة المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م.

٣.قانون جرائم أنظمة المعلومات الأردني رقم ٣٠ لسنة ٢٠١٠م.

٤.قانون مُكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥م.

٥.قانون منع الإرهاب الأردني رقم ٥٥ لسنة ٢٠٠٦م.

٦.قرار مجلس الوزراء السعودي رقم ١٦٣ تاريخ ١٤١٧/١٠/٢٢هـ.

٧.لائحة مُكافحة جرائم غسل الأموال وتمويل الإرهاب الإماراتي رقم ٢٠ لسنة ٢٠١٨م.

٨.نظام مُكافحة الإرهاب وتمويله السعودي رقم م/٢١ تاريخ ١٤٣٩/٩/١٢هـ.

٩.نظام مُكافحة جرائم المعلوماتية السعودي رقم م/١٧ تاريخ ١٤٢٨/٣/٨هـ.