دولة الإمارات العربية المتحدة

جامعة أبو ظبي- كلية القانون

ماجستير القانون العام

السياسة الجنائية في مواجهة الإرهاب الإلكتروني

Criminal Policy in the Face of Terrorism

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

إعداد الطالبة/ ميثاء محمد المنصوري

الرقم الجامعي: 1076596

إشراف الدكتور/ حسين عيسى المحمد

العام الدراسي 2020-2021

إقرار الباحثة

أقر أنا الموقعة أدناهالطالبة/ ميثاء محمد المنصوري ، المقيدة ببرنامج الماجستير أن هذا البحث المقدم مني للحصول على درجة الماجستير في القانون العام، هو من نتاج عملي وجهدي الخالص، وأنه لم يسبق لي التقدم به لأي جهة علمية،أو إدارية، أو غيرها داخل الدولة أو خارجها للحصول على أي درجة علمية أخرى، أو لأي سبب من الأسباب، وأن مضمون هذه الرسالة يعكس آراء الباحث الخاصة؛ وهي ليست بالضرورة الآراء التي تتبناها الجهة المانحة للدرجة العلمية، كما أقر بقيام قبول الجامعة في حال إجازة الرسالة من قبل لجنة المناقشة والحكم بطباعة الرسالة ونشرها بالكيفية التي تراها محققه لأغراضهاوأهدافها، دون أن يكون لي حق العدول عن هذا الإقرار بعد إجازة الرسالة.

اسم الباحث: ميثاء محمد المنصوري.

الرقم الجامعي: 1076596

توقيع الباحثة:

إجازة أطروحة الماجستير

عنوان الرسالة: (السياسة الجنائية في مواجهة الإرهاب الإلكتروني)

نوقشت هذه الرسالة وتم إجازتها من قبل أعضاء لجنة المناقشة المشار إليهم أدناه بتاريخ:

المشرف: الدكتور/ حسين عيسى المحمد أستاذ القانون الجنائي المساعد.

كلية- قسم القانون العام- جامعة أبوظبي.

التاريخ التوقيع

عضو لجنة المناقشة : الدكتورة / دينا جنبلاط - أستاذ القانون الجنائي المساعد.

كلية القانون- قسم القانون العام- جامعة أبوظبي.

التاريخ التوقيع

الآية القرآنية

بسم الله الرّحمن الرّحيم

«منْ قتَلَ نفْساً بغيْر نفْسٍ أو فَسَادٍ في الأرضِ فكأنّما قتلَ النَّاسَ جميعاً، ومَنْ أحْياها فكأنّما أحيا الناسَ جميعاً» (سورة المائدة/الآية 32).

الإهداء

إلى من جرع الكأس فارغًا ليسقيني قطرة حب، إلى من كلَّت أنامله ليقدم لنا لحظة سعادة (روح والدي)

إلى من أرضعتني الحب، إلى رمز الحنان، إلى القلب الناصع البياض (والدتي الحبيبة)

إلى القلوب الطاهرة الرقيقة والنفوس البريئة، إلى رياحين حياتي (أخواتي)

إلى سندي وعضدي، إلى من سكن قلبي وأسر حبي... زوجي الغالي.

إلى كل من أشعل شمعة في دروب علمنا، إلى مَن وقف على المنابر وأعطى من حصيلة فكره لينير دربنا، إلى

الأساتذة الكرام في كلية القانون في جامعة إبوظبي، وأخص بالشكر الأستاذ الدكتور حسين عيسى المحمدالذي

كان لتوجيهاته وإرشاداته الأثر الكبير في إنجاز هذه الدراسة.

الشكر والتقدير

الحمدلله العلي القدير على توفيقه لأخراج هذه الرسالة على هذه الصورة، التي أتمنى ان تعود بالنفع لمن أعدها ولكل من قرأها، وأن تكون لبنة متواضعة في صرح هذا العلم.

كما أتوجه بالشكر الجزيل الى كل من وجهني، وساعدني خلال فترة إعداد هذه الرسالة، سائلة الله عز وجل أن يجزيهم عني خير الجزاء، وأن يكون في ميزان حسناتهم.

وأخص بالشكر والتقدير والعرفان الدكتور **حسين عيسى المحمد** لتكرمه بالإشراف على هذه الرسالة، وبما غمرني به من دعم وعون، وأكرمني به من غهتمام وسعة صدر، طيلة فترة كتابة الرسالة بالرغم من كثرة انشغالاته، فجزاه الله خيراً ونفع به كل طالب علم.

والشكر موصول لوطن أكرمنا الله به، شيوخاً وحكومة وشعباً، يُجِلُّ العلم والعلماء، ويشجع أبناءه على البحث وطلب العلم تحقيقاً لإرادة وطن يسعى إلى الريادة في كل المجالات.

ميثاء محمد مبارك المنصوري

السياسة الجنائية في مواجهة الإرهاب الإلكتروني

ميثاء محمد مبارك المنصوري

الملخص

تتناول الدراسة ظاهرة من الجرائم المستحدثة ألا وهي الإرهاب الإلكتروني، بوصفها ظاهرة من الظواهر الناجمة عن التقدم التقني والتكنولوجي في العديد من مجالات الحياة، الأمر الذي يتطلب البحث في مدى إمكانية تطبيق القوانين والاتفاقيات الدولية المتعلقة بمكافحة الإرهاب على الجرائم الإرهابية التي تتم باستخدام الوسائل الإلكترونية.

انطلاقا من ذلك قسمت الدراسة إلى فصلين،تناول الأول منهما مفهوم الإرهاب االإلكتروني وسبل مواجهته، وتناول الثاني الإشكاليات القانونية في مواجهة الإرهاب الإلكتروني.

وخلصت الدراسة إلى أن جرائم الإرهاب الإلكتروني جرائم ذات خصائص منفردة، تختلف عن الجرائم التقليدية من حيث طرق ووسائل ارتكابها، الأمر الذي ينعكس على طبيعة الإجراءات التي يجب على السلطات المختصة اتخاذها في مواجهتها، فضلا عن نهج أساليب خاصة في مكافحة هذا النوع من الإجرام المستحدث.

وخلصت الدراسة أيضًا إلى ضرورة تكثيف الجهود على الصعيد الدولي لصياغة اتفاق شامل حول جرائم الإرهاب الإلكتروني تلتزم الدول الأطراف بتضمين أحكامه في قوانينها الوطنية، لما يمثله هذا النوع من الجرائم من خطورة على السلم والأمن الدوليين.

السياسة الجنائية في مواجهة الإرهاب الإلكتروني

Criminal Policy in the Face of Terrorism

Abstract

This Study aimed to search about new created crime which is the cyber terrorism and it`s considered caused by the technical and technological development in many fields and، it`s required to search regarding the possibility of following the laws to the international agreements which is related to the Confronirtation of the cyber terrorism generally on the cyber terrorism crimes.

According to that، this study have been divided to two chapters، to the concept of the cyber terrorism and it`s properties in the first chapter and the second chapter was concerned to clarify the legal issues which is related to the cyber terrorism. And one of the most important results in this study that، the cyber terrorism has a special properties differs it from the traditional terrorism crimes in the ways and implementation methods in it so، which is reflect to the nature of procedures that required to be done by the concerned authorities and the confrontation methods in this kind of crimes.

The researcher has concluded to the nessicty for intensification of the international cooperation to create comprehensive agreement concerned to the cyber terrorism crimes that، can be followed by countries to include it to their nation laws، because that kind of crimes considers as real threaten of the international peace and security.

المقدمة:

تمتد جذور ظاهرة الإرهاب إلى زمن بعيد، فبالرجوع إلى تاريخ الإرهاب ونشأته في العصور القديمة نجد أن الجرائم الإرهابية كانت موجودة في الحضارات والمجتمعات القديمة، وذلك بكافة أركانها، كما نجد أنها قد امتدت في هذه الحقبة الزمنية ولم تختفي إلا بشكل نسبي، وذلك باختلاف العوامل التي تساهم في زيادة الجرائم الإرهابية في كل مكان وزمان، وأيضا بحسب الظروف والأوضاع المحيطة.

وفيما يتعلق بالعصور الوسطى فقد ظهر الإرهاب فيها بطريقه وشكل أكثر تميزا ووضوحا عن العصور القديمة، حيث شهدت هذه الحقبة الزمنية أبشع أنواع وصور للعنف، والأحداث الإرهابية، وذلك ابتداء من محاكم التفتيش الخاصة بالباباوات والتي كان يعاقب فيها كل من لا يدين للكنسية البابوية، وقتل واغتيال الملوك بهدف الوصول إلى الحكم، كما قد كان يواجه العديد بأنواع متعددة من العقوبات والتي تتمثل في الإعدام والمصادرة وغيرها من العقوبات، ومن أكبر العمليات الإرهابية في هذه الحقبة الحملة الصليبية والتي كانت بغرض القضاء على الأثرياء والنبلاء للجنوب الفرنسي وقتل خمسه عشر ألف من السكان[1].

وبالتالي فإن ظاهره الإرهاب في العصر الحديث، تعبر امتداد للإرهاب في العصور القديمة والوسطى، كما أنها ترافق المجتمعات البشرية، حيث كان لتطور المجتمعات الأثر الكبير في انتشار العديد من العمليات والجرائم الإرهابية في العصر الحديث، بالإضافة إلى أن تطور وسال تكنولوجيا المعلومات والاتصالات قد أدى إلى تطور الأعمال والجرائم الإرهابية.

حيث يشهد العالم اليوم ثوره واسعة وتقدما ملحوظا في مجال الأنظمة المعلوماتية، و يعرف هذا التقدم بثوره المعلومات، والتي قد نشأت من جماع طفرتين وهما طفرة تقنية المعلومات وطفرة

---

(1) سلطان عناد إبراهيم العدينات، **الآلية الدولية لمكافحة الإرهاب**، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2018م، ص17/10.

الاتصالات، وانعكست على أنظمة الاتصالات الحديثة، الأمر الذي أتاح عمليه تبادل المعلومات والبيانات بين هذه الأجهزة، وبالتالي عدم الاعتراف بالحدود الجغرافية، بما يعرف بالطابع الدولي، وتلاشي الحدود السياسية بين الدول المتعددة، مما أدى إلى اعتبار العالم قرية عالمية واحدة، أو قرية كونية صغيرة تسبح في الفضاء الالكتروني[2].

وقد أضحت المعلوماتية تهيمن على العديد من جوانب حياتنا المعاصرة، بأبعادها القانونية والاقتصادية والثقافية والاجتماعية، وحلت تكنولوجيا الاتصالات محل الوسائل التقليدية والدعامات الورقية[3]

كما قد أفرز التطور والتقدم المستمر في مجال تكنولوجيا الاتصالات والمعلومات أنواعا جديدة من الجرائم المستحدثة والتي يتم ارتكابها من خلال الوسائل الإلكترونية الحديثة، بحيث اتسع الإطار الخاص بالجرائم الإلكترونية في ظل التطور الهائل والثورة الرقمية في وسائل الاتصال الحديثة، ومن أهم المظاهر المستحدثة للجرائم الإلكترونية، الأعمال الإرهابية التي يتم ارتكابها في الفضاء الإلكتروني، والتي يعبر عنها بالإرهاب الإلكتروني [4].

---

(2) إيمان مأمون أحمد سليمان، **إبرام العقد الإلكتروني وإثباته، الجوانب القانونية لعقد التجارة الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2008م، ص 7.

(3) عمرو عبد الفتاح على يونس، **جوانب قانونيه للتعاقد الإلكتروني في إطار القانون المدني**، دراسة مقارنه، مدعمه بأحدث الأحكام القضائية الأجنبية والعربية ، ط1، 2009م، ص13.

(4)عبد الله دغش العجمي، **المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنه**، رسالة ماجستير، جامعه الشرق الأوسط، 2012م، ص12.

- عبد الله نوار شعت، **الإثبات والالتزامات في العقود الإلكترونية**، ط1، مكتبه الوفاء القانونية، الإسكندرية، 2017م، ص 3.

فقد أصبح الإرهاب آفة تهدد أمن واستقرار المجتمعات، حيث لم يعد يسلم أي مجتمع من المجتمعات من العديد من الأفعال الإرهابية ، كما أنه لم يعد محصورا في نطاق معين، أو مرتبطا بجماعه أو أشخاص أو ثقافة معينة، بل أصبح هذا الخطر يتضاعف مع التطور والتقدم الهائل في مجال تكنولوجيا المعلومات والاتصالات، من خلال ما يعرف بالإرهاب الإلكتروني، والذي يتم باستخدام هذه الوسائل والاعتماد عليها في ارتكاب العديد من الأفعال الإرهابية، باعتبارها مجالا خصبا للإرهابيين من حيث ممارسه الجرائم الخاصة بهم ضد نظم التحكم والسيطرة [5].

ويعتبر الإرهاب عبر شبكه الإنترنت واحدا من أحد الصور والأشكال الخاصة بالإرهاب، والذي يتمثل في استخدام الموارد المعلوماتية بهدف التخويف أو الإرغام لتحقيق أهداف سياسيه، فهو يرتبط بمستوى التقدم والتطور الذي تلعبه تكنولوجيا المعلومات والاتصالات في مختلف مجالات الحياة، وذلك من خلال الدور الذي تلعبه الجماعات الإرهابية من التسلح بوسائل الإعلام المتعددة بغرض تسويق أهدافهم وأغراضهم، واكتساب السيطرة على الرأي العام، من خلال المعلومات والأخبار التي يتم نشرها، أو بهدف تضليل الأجهزة الأمنية، وتجنيد وتدريب الأعضاء على مقاومه السلطات وغير ذلك من الأفعال التي يتم استخدام وسائل التواصل الاجتماعي ووسائل تكنولوجيا المعلومات في ارتكابها [6].

فالإرهاب ظاهرة خطيرة تهدد حياة الناس على امتداد العالم، ويظهر ذلك جليًّا في انتشار العمليات الإرهابية وتنوع صورها وأشكالها والأساليب المستحدثة في تنفيذها، التي يصعب ضبطها والسيطرة

---

(5) سليمان أحمد فضل، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكه المعلومات الدولية، الإنترنت**، دار النهضة العربية، القاهرة، 2013م، ص128.

(6) محمود صالح العادلي، **الإرهاب الرقمي في القانون البحريني المقارن بالنظام السعودي والقانون المصري، (ماهيته – الجماعات المتطرفة والإرهابية– صور استخدام الإنترنت في الإرهاب– البحث والتحقيق الجنائي المتصل بالإرهاب الرقمي**، دار النهضة العربية، القاهرة، ط1، 2016م، ص7.

عليها؛ رغم الجهود الكبيرة التي تبذلها الدول والحكومات للحد منها، والإرهاب الإلكتروني في حقيقته سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية وشبكة المعلومات الإنترنت، ويهدد بالقيام بأعمال عنف موجهة ضد المجتمع، أو تسهيل القيام بهذه الأعمال، أو دعم الجماعات والتنظيمات التي تمارس الأعمال الإرهابية، أو الترويج لأفكارها، أو تمويلها.

وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكة المعلوماتية عبر الاختراق والقرصنة، وتضم كذلك الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت؛ كالجرائم التي تهدد أمن الدولة وسلامتها المالية، كما تشمل انتهاك حقوق التأليف، ونشر الصور والأفلام الإباحية، والتغرير بالأطفال واستغلالهم في الأعمال الإجرامية، وكذلك جرائم الاتجار غير المشروع بالمخدرات، وغسيل الأموال، والاحتيال الإلكتروني.

إزاء انتشار هذه الظاهرة سعت دول العالم إلى وضع التشريعات المتنوعة لمنعها أو الحد منها، وفي هذا السياق بذلت دولة الإمارات العربية المتحدة جهودًا كبيرة بهدف الوصول إلى آلية مناسبة تحد من عمليات الإرهاب الإلكتروني، ومواجهتها بالعقوبات والتدابير المناسبة؛ حيث صدر القانون رقم (7) لسنة 2014م في شأن مكافحة الجرائم الإرهابية الذي ألغى المرسوم بقانون اتحادي رقم 1 لسنة 2004 بشأن مكافحة الجرائم الإرهابية[7].

أهمية البحث:

يمثل الإرهاب جريمة العصر، وقد انقسم العالم إزاء الجرائم الإرهابية إلى فسطاطين؛ قسم لا يتخذ أي إجراءات جدية لمواجهة الإرهاب ويصنف على أنه بيئة حاضنة وداعمة للإرهاب، وقسم آخر اتخذ إجراءات وتدابير حاسمة لمواجهة مختلف أشكال الإرهاب،ومع انتشار تقنية الاتصالات الحديثة

(7) القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية، والذي تم نشره في الجريدة الرسمية بتاريخ 2014/8/31م.

وشيوع استخدام شبكة الإنترنت؛ نشأت مفاهيم وأبعاد جديدة للإرهاب تعتمد على التقنية والتكنولوجيا وشبكة المعلومات؛ مما أدى إلى ظهور أسلوب جديد للإرهاب يتمثل في الإرهاب الالكتروني.

وتبرز أهمية البحث من خطورة جريمة الإرهاب الإلكتروني؛ حيث لم تعد التقنية والتطور التكنولوجي قادران على حماية المجتمع والأفراد من عمليات الإرهاب الإلكتروني؛ الذي بات ظاهرة تهدد أمن وسلامة الأفراد والمجتمعات، الأمر الذي يستوجب تدخل المشرع على الصعيدين الدولي والمحلي لسن التشريعات واتخاذ الإجراءات والتدابير المناسبة لمواجهه هذه الظاهرة الخطيرة.

مشكلة البحث:

يتطلب التطور التقني في أساليب ارتكاب الجريمة؛ خاصة تلك التي ترتكب عبر الإنترنت وأجهزة الحاسوب تطورًا في القوانين والتشريعات، تحدد أركان هذه الجرائم وعناصرها والعقوبات المناسبة لها، وتوفير المناخ الآمن والمناسب لاستخدام التكنولوجيا المتطورة من خلال تتبع وملاحقة الأفراد والجماعات الذين يوظفون التكنولوجيا لأغراض إجرامية؛ وبناءً على ذلك فإن مشكلة الدراسة تتمثل في: بيان مدى كفاية الحماية الجنائية في التشريع الاتحادي لمواجهة جريمة الإرهاب الإلكتروني على الصعيدين الإجرائي والموضوعي.

تساؤلات البحث:

يثير البحث التساؤلات التالية:

1- ما المقصود بالإرهاب الإلكتروني؟

2- ما أسباب الإرهاب الإلكتروني وسبل مواجهته؟

3- ما مدى ملاءمة القواعد العامة في التشريع الاتحادي لمواجهة الإرهاب الإلكتروني؟

4- ما مدى ملاءمة القواعد الخاصة فيالتشريع الاتحادي لمواجهة الإرهاب الإلكتروني؟

5- ما الصعوبات التي تواجهها السلطات فيجمع الأدلة وتتبع المجرمين بصدد جرائم الإرهاب الإلكتروني؟

6- ما مدى مراعاة مبدأ مشروعية الدليل في إثبات جرائم الإرهاب الإلكتروني؟

أهدف البحث:

تهدف الدراسة إلى ما يلي:-

1- التعرف على مفهوم الجريمة الإلكترونية والإرهاب الإلكتروني.

2- تحديد أسباب انتشار ظاهرة الإرهاب الإلكتروني .

3- البحث في مدى كفاية القواعد العامة والخاصة في مواجهه جرائم الإرهاب الإلكتروني

4- الوقوف على التشريعات الخاصة بمكافحه جرائم الإرهاب بوجه عام، والإرهاب الإلكتروني بوجه خاص

5- البحث في الاتفاقيات الدولية الخاصة بمكافحه الإرهاب، وجرائم تقنيه المعلومات

6- الصعوبات التي تواجهها السلطات في جمع الأدلة وتتبع المجرمين بصدد جرائم الإرهاب الإلكتروني.

7- مدى مراعاة مبدأ مشروعية الدليل في إثبات جرائم الإرهاب الإلكتروني.

منهج البحث:

اعتمدت الباحثة في هذه الدراسة على المنهجين الوصفي والتحليلي؛ حيث اعتمدت على المنهج الوصفي لملاءمة أدواته للدراسة من حيث وصف ظاهرة الإرهاب الإلكتروني وتفسيرها، من خلال تحديد المفاهيم القانونية التي تتعلق بها، والوقوف على المعلومات والحقائق التي تتعلق بأسباب انتشارها، كما اعتمدت على المنهج التحليلي؛ من خلال عرض النصوص القانونية والتشريعات الخاصة

بجرائم الإرهاب، وجرائم تقنية المعلومات،والاتفاقيات والمؤتمرات الدولية والإقليمية الخاصة بمكافحة الإرهاب والجرائم الإلكترونية، وتحليل العناصر والمكوناتالخاصة بهذه الظاهرة، ومعالجة الإشكاليات التي تثيرها الجريمة فيما يتعلق بإثباتها، والكشف عنها، وملاحقة مرتكبيها.

الدراسات السابقة:

الدراسة الأولى- دراسة إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية وفقًا للمرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات وتعديلاته،جامعه الإمارات العربية المتحدة، 2018م[8]:

تطرق الباحث في هذه الدراسة إلى جريمة الدخول غير المشروع التي تعد من الجرائم المعلوماتية المستحدثة، والتي تقع على النظام المعلوماتي؛ هدفها الوصول والاطلاع على البيانات والمعلومات المخزنة.

وقد توصل الباحث إلى أن الجريمة محل الدراسة من الجرائم التي عالجها المشرع في قانون مكافحة جرائم تقنية المعلومات الاتحادي،حيثتتمثل هذه الجريمة في ثلاث صور هي؛ تجاوز حدود تصريح الدخول غير المشروع، والدخول إلى النظام المعلوماتى بدون تصريح، والبقاء بصورة غير مشروعةفي النظام المعلوماتى.

تناولت هذه الدراسة الجريمة بوصفها من جرائم تقنية المعلومات، وليس بوصفها أحد صور النشاط الذي يتم ارتكاب جرائم الإرهاب الإلكتروني من خلاله،حيث أشارت إلى أنه يمكن ارتكاب عدد من الجرائم من خلال جريمة الدخول غير المشروع، ولم تتخصص في جرائم الإرهاب التي يتم ارتكابها

---

(8)إبراهيم محمد القاسمي،**جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، وفقًا للمرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات وتعديلاته،** رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018م.

عبر وسائل تقنية المعلومات كما في شأن دراسة الباحثة الحالية؛التي تناولتُ فيها الإرهاب الإلكتروني بجميع صوره وأركانهوطرق مكافحته من خلال القانون الاتحادي رقم 5 لسنه 2012م في شأن مكافحة جرائم تقنية المعلومات[9]، والقانون الاتحادي رقم 7 لسنه 2014م بشأن مكافحة الجرائم الإرهابية.

الدراسة الثانية– دراسةمحمد صلاح محمد عبدالمنعم، بعنوان الجرائم الإلكترونية وتحدياتها، دراسة مقارنة، جامعة المنصورة، مصر، 2017م[10]:

تناول الباحث في هذه الدراسة ماهيَّة الجرائم الإلكترونية، وتحديد الأركان الخاصة بها، ومعايير تقسيمها، والأنواع الخاصة بها والتي يعد منها جرائم الإرهاب الإلكتروني، كما بيّن الباحث طرق وأساليب مكافحة الجرائم الإلكترونية، سواء من خلال المواجهة التقنية، أو المواجهة التشريعية والاتفاقيات الدولية والتعاون الدولي.

وتختلف دراسة الباحثة الحالية عن الدراسة السابقة في أنها تناولت الجرائم الإلكترونية بوجه عام من خلال القواعد العامة، ولم تتطرق إلى جريمة الإرهاب الإلكتروني بوجه خاص؛ بل أشارت إليها فقط،فيما تناولت الدراسة الحالية الإرهاب الإلكتروني بجميع صوره وأركانه وطرق مكافحته من خلال المرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحةتقنية المعلومات والمعدل بالقانون الاتحادي رقم 2 لسنة 2018 م، والقانون الاتحادي رقم 7 لسنة 2014 بشأن مكافحة الجرائم الإرهابية،فالدراسة الحالية متخصصة في هذا النوع من الجرائم الإلكترونية،يتم ارتكابها من خلال وسائل تقنية المعلومات، وطرق مكافحتها من خلال القواعد الخاصة بهذه الجريمة.

تقسيم الدراسة:

---

(9) القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، صادر بتاريخ 8/13/ 2012م.

(10)محمد صلاح محمد عبدالمنعم،**الجرائم الإلكترونية وتحدياتها**، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2017م.

قسمت الدراسة إلى فصلين، حيث جاء **الفصل الأول** تحت عنوان **ماهية الإرهاب الإلكتروني و أسبابه وسبل مواجهته،** وقسّم بدوره إلى مبحثين، تناول المبحث الأول بيان مفهوم الإرهاب الإلكتروني من خلال تعريف الإرهاب الإلكتروني وبيان الأركان المشتركة لجرائم الإرهاب الإلكتروني، فيما تناول المبحث الثاني أسباب جرائم الإرهاب الإلكتروني وسبل مواجهتها.

أما **الفصل الثاني** فجاء تحت عنوان **الإشكاليات القانونية في مواجهة الإرهاب الإلكتروني،** حيث قسّم إلى مبحثين، تناول الأول منهما الإشكاليات التي تثيرها مواجهة الإرهاب الإلكتروني في جانب النصوص الموضوعية، لبيان مدى ملاءمة القواعد الجنائية العامة والخاصة في مواجهة الإرهاب الإلكتروني، فيما تناول المبحث الإشكاليات الإجرائية التي تثيرها مواجهة الإرهاب الإلكتروني ويأتي على رأسها صعوبة جمع الأدلة وتتبع المجرمين، ومدى التقيد بمبدأ شرعية الأدلة في إثبات جرائم الإرهاب الإلكتروني.ثم ختمت الباحثة دراستها بمجموعة من النتائج والتوصيات.

الفصل الأول

ماهية الإرهاب الإلكتروني وأسبابه وسبل مواجهته

تمهيد وتقسيم:

أدى التقدم التكنولوجي الكبير، والتزايد المستمر في مجال الاتصالات؛ فضلًا عن اتساع شبكة الإنترنت، وسهولة الدخول إليها، والطبيعة السرية التي تتسم بها نظم المعلومات التي تتم من خلالها، إلى تطور الجريمة بوجه عام، وظهور أشكال جديدة منها على جميع المستويات الإقليمية والدولية والمحلية[11].

فقد تعددت الجرائم المرتبطة بشبكات المعلومات والاتصالات، وزادت معاناة دول العالم من الأنشطةالخاصة بالإرهاب الإلكتروني، التي تعد من الجرائم ذات الطابع السياسي المرتبط بالأمن العسكري أو القومي،لأن الهدف من ارتكابها هو تهديد الأمن العسكري والقومي،في إطار مايعرف بحرب المعلومات[12].

حيث استغلت الجماعاتالمتطرفة الطبيعةالاتصالية لشبكة المعلوماتمن أجل بث أهدافها ومعتقداتها، والقيام ببعض الممارسات التي تهدد أمن الدولة؛ حيثأصبح الإرهاب ظاهرة عالمية مرتبطة بعوامل سياسية، وثقافية، واجتماعية، وتكنولوجية، أفرزتها التطورات السريعة والمتلاحقة في العصر

(11) شمسان ناجي صالح الخيلي،**الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت**، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009م، ص35.

(12) نائله عادل محمد فريد قوره،**جرائم الحاسب الآلي الاقتصادية**، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية،2004م، ص37.

الحديث[13].

بناءً عليه قُسِّم هذا الفصل إلى مبحثين؛ يتناول المبحث الأول مفهوم الإرهاب الإلكتروني، فيما يستعرض المبحث الثاني الأسباب الخاصة بالإرهاب الإلكتروني وسبل مواجهته على النحو التالي.

المبحث الأول: مفهوم الإرهاب الإلكتروني.

المبحث الثاني: أسباب الإرهاب الإلكتروني وسبل مواجهته.

المبحث الأول

ماهية الإرهاب الإلكتروني وأركانه

تمهيد وتقسيم:

تعد ظاهرة الإرهاب الإلكتروني من الظواهر الأكثر خطورة على مستوى العالم، حيث أصبحت ظاهرة عالمية تشكل تهديدًا وخطرًا على المجتمع الدولي، وللتعرف على ظاهرة الإرهاب الإلكتروني والوقوف على الجوانب التي تحيط بها، لا بد من دراسة مفهوم هذه الظاهرة؛ من حيث تعريفها، وتحديد طبيعتها القانونية، ومعرفة الأركان المشتركة لها؛ من خلال تخصيص مطلبين لدراسة الجوانب المتعلقة بمفهوم هذه الظاهرة:

المطلب الأولـتعريف الإرهاب الإلكتروني.

المطلب الثانيـالأركان المشتركة لجرائم الإرهاب الإلكتروني.

---

(13) مها محمد أحمد عنانزه، **وعي طلبة جامعة اليرموك بمخاطر الإرهاب الإلكتروني ودور التربية الوطنية والإسلامية والقانونية في التصدي لها**، رسالة دكتوراه، كليه التربية، جامعة اليرموك، 2018م، ص2/1.

المطلب الأول

تعريف الإرهاب الإلكتروني

تقسيم:

لا بد لفهم ظاهرة الإرهاب الإلكتروني من الوقوف علىمفهوم الإرهاب التقليدي بوجه عام؛ من خلال الإشارة إلى التعريف اللغوي، والفقهي، والقانوني له،ثم تعريف الجريمة الإلكترونية والإرهاب الإلكتروني بوجه خاص في الفرعين التاليين:

الفرع الأول

تعريف الإرهاب التقليدي

هناك اتفاق بين الفقهاء والخبراء على أن الإرهاب يعد مشكلة في حد ذاته، إلا أنه لا يوجد اتفاق بينهم بشأن تعريفه؛ حيث تعددت التعريفات التي تناولته بالشرح والتفصيل، كما تنوعت في شأنه الاجتهادات دون التوصل إلى تعريف موحد ومتفق عليه، وللبحث في تعريف الإرهاب التقليديلا بد من توضيح المعنى اللغوي والفقهي والقانوني للإرهاب، وبيان المقصود به في الاتفاقيات والمواثيق الدولية؛ وفق الآتي:

أولًا- التعريف اللغوي للإرهاب:

الإرهاب لغةً: مصدر الفعل (رهب)، فالراء والهاء والباء، أصلان أحدهما على دقة وخفة، والآخر على خوف،فالأول الرهب وهو الناقة المهزولة، والرهاب عظم في الصدر مشرف على البطن،

والأصل الآخر الرهبة تقول: رهبت الشيء رهبًا ورهبةً، ومن الباب الإرهاب، بمعنى قدع الإبل من الحوض[14].

ويقال: أرهب فلانًا بمعنى أفزعه وأخافه، وترهّب: أي انقطع للعبادة في صومعته.أما الإرهابيون فهو وصف يطلق على الذين يسلكون سبل الإرهاب والعنف في سبيل تحقيق أهدافهم السياسية[15].

وجاء في لسان العرب في تعريف الفعل رهب بالكسر ومصدره الإرهاب، من رهب الشيء رهبًا ورهبه أي أخافه، والاسم الرهب والرهبوت، ويقال: رجل رهبوت خير من رحموت، وترهب غيره أي توعده، ويقال: رهباها الذي ترهبه، كقوله هالك وهلكى، وإذا ترهبا أي توعدا، وتقول الرهباء من الله والرغباء إليه[16].

ثانيًا– التعريف الفقهي للإرهاب:

اختلفت الآراء الفقهية وتضاربت حول تحديد تعريف الإرهابتبعًا لاختلاف المعايير التي اعتمدها أصحابها في تحديد تعريف الإرهاب، وقد بذل فقهاء القانون الدولي جهودًا فقهية كبيرة، على الصعيدين العربي أو الغربي لوضع تعريف محدد للإرهاب، واعتمدوا في تعريفاتهم على أحد المعيارين؛ المعيار الموضوعي الذي يعتمد على الغاية أو الهدف من العمل الإرهابي، والمعيار الماديالذي يعتمد على طبيعة العمل الإرهابي كأساس لتعريف الإرهاب؛ على النحو التالي:

1– المعيار الموضوعي لتعريف الإرهاب:

يرى أنصار هذا الاتجاه أن مدلول الإرهاب لا بد أن يتسم بالنظرة الموضوعية، والاهتمام بالغاية

---

(14) أبو الحسين أحمد بن فارس بن زكريا القزويني الرازي، **معجم مقاييس اللغة**، ج2، دار الفكر، 1979م، ص447.

(15) **مجمع اللغة العربية، المعجم الوجيز**، وزاره التربية والتعليم، 2006م، ص279.

(16) أبو الفضل جمال الدين محمد بن مكرم ابن منظور الأنصاري الرويفعي الأفريقي، **لسان العرب**، ج1، دار المعارف، 2007م، ص436/437.أبو عبدالله محمد بن أبي بكر بن عبدالقادر الحنفي الرازي، **مختار الصحاح**، ج2، المكتبة العصرية، الدار النموذجية، ط5، 1999م، ص130.

التي يسعى إليها مرتكبو الأعمال الإرهابية؛ ومن هؤلاء **الفقيه إيريك دافيد**[17]: الذي ربط بين أعمال العنف المسلح وتحقيق أهداف معينة مسبقة، وعرف الإرهاب بأنه: "كل عمل من أعمال العنف المسلح يتم ارتكابه من أجل هدف اجتماعي، أو سياسي، أو ديني، أو مذهبي، من خلال انتهاك قواعد القانون الدولي الإنساني المحظور فيه استخدام الوسائل البربرية والوحشية، أو مهاجمة أهداف معينة دون أية ضرورة عسكرية، أو مهاجمة الضحايا الأبرياء".

كما عرف الفقيه ريمون أرون؛ الإرهاب بأنه: "كل فعل من أفعال العنف الذي تتجاوز الأهمية الخاصة بتأثيراتها السيكولوجية الأهمية التي تتعلق بنتائجه المادية البحتة"[18].

إضافة إلى الفقيه أحمد جلال عز الدين الذي ذهب إلى أن:"الإرهاب هو العنف المتصل والمنظم الذي يهدف إلى التهديد العام الموجه لجماعة سياسية، أو دولة معينة، وتقوم بارتكابه جماعة منظمة بغرض تحقيق أهداف سياسية"[19].

2- المعيار المادي لتعريف الإرهاب:

اهتم أنصار هذا الاتجاه في تعريفهم للإرهاب بالوسائل التي يتم استخدامها في العمليات الإرهابية والفزع والرعب كنتيجة له،دون الاهتمام بالهدفوالغرض منه؛ ومن هؤلاء الفقهاء؛ **الفقيه سلدانا** الذي وضع تعريفين للإرهاب أحدهما ضيق؛ ويتمثل في الأعمال الإجرامية والإرهابية التي يكون الهدف الأساسي منها نشر الرعب والخوف كعنصر شخصي،من خلال استخدام الوسائل التي يكون من شأنها

---

(17) شريف عبد الحميد حسن رمضان،**الإرهاب الدولي، أسبابه وطرق مكافحته في القانون الدولي والفقه الإسلامي،** دراسة مقارنة،ج3، ع31، مجله كليه الشريعه والقانون، طنطا، 2016م، ص1116.

(18) علي لونيسي،**آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الانفرادية،** رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، 2012م، ص23.

(19) على لونيسي، **آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الانفرادية،** مرجع سابق، ص24.

إحداث حالة من الخطر العام كعنصر من العناصر المادية. والمعنى الواسع المتمثل في كل جنحة، أو جناية اجتماعية، أو سياسية ينتج عن التعبير عنها أو تنفيذها ما يثير الفزع العام أو الخطر العام[20].

بدوره **الفقيه سوتيل** الذي عرف الإرهاب بأنه العمل الإجرامي المقترن بالعنف والرعب أو الفزع؛ وذلك بغرض تحقيق هدف معين.**والفقيه عبدالعزيز سرحان** الذي ذهب إلى تعريف الإرهاب بأنه كلاعتداء على الأموال والأرواح والممتلكات الخاصة أو العامة؛ خلافًا لأحكام القانون الدوليبجميع مصادره بما في ذلك المبادئ العامة للقانون،وفق المعني الذي حددته المادة 38 من النظام الأساسي الخاص بمحكمة العدل الدولية،بأنه جريمة دولية أساسها مخالفة القانون الدولي[21].

وترى الباحثة أن التعريفات السابقة وصفت الأعمال الإرهابية ولم تعرف الجريمة الإرهابية، رغم أن الإرهاب وصف عام مرن، كما أن وصف البعض من الأعمال على أنها إرهابية قد يؤدي إلى إخراج البعض من الأعمال الإجرامية الأخرى من الدائرة الخاصة بالإرهاب؛ لعدم ذكرها ضمن هذه الأعمال المحددة وليس لكونها ليست إرهابية، مما يترتب عليه إفلات الكثير من الجناة من العقاب.

وبناءً عليه يمكن تعريف الإرهاب من **وجهة نظر الباحثة** بأنه كل فعل سواء باستخدام القوة، أو العنف، أو التهديد بهما، أو التحريض باستخدام القوة أو العنف،أو أي تحريض من خلال استخدام الوسائل الإعلامية المقروءة، أو المسموعة، أو المرئية، أو من خلال استخدام وسائل التواصل الاجتماعي في تهييج المشاعر والتحريض على العنف، سواء كانت هذه الأفعال صادرة من دولة أو فرد أو جماعة، ضد دولةأو جماعة أو ممتلكات خاصة أو عامة، بغرض تحقيق أهداف أيدلوجية أو

---

(20) شريف عبد الحميد حسن رمضان، **الإرهاب الدولي، أسبابه وطرق مكافحته في القانون الدولي والفقه الإسلامي**، دراسة مقارنة، مرجع سابق، ص1115/1118.

(21) على لونيسي،**آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الانفرادية**، مرجع سابق، ص19/21.

سياسية أو اجتماعية، أو دينية، أو غيرها من الأسباب.

ثالثًا– التعريف القانوني للإرهاب:

دخلت فكرة الإرهاب الفكر القانوني لأول مرة في المؤتمر الأول الخاص بتوحيد القانون العقابي المنعقدفي مدينة وارسو عام 1930م[22].

وفيما يتعلق بموقف المشرع الاتحادي من تعريف الإرهاب الإلكتروني، فلم يعرف المشرع الإرهاب الإلكتروني ولكنه عرف الجريمة الإرهابية، حيث نص القانون الاتحادي رقم 7 لسنة 2014م بشأن مكافحة الجرائم الإرهابية في المادة الأولى منه على تعريف الجريمة الإرهابية بأنها:"كل فعل أو امتناع عن فعل مجرم بموجب هذا القانون، وكل فعل أو امتناع عن فعل يشكل جناية أو جنحة واردة في أي قانون آخر، إذا ارتكب لغرض إرهابي"[23].

وعرف الشخص الإرهابي بأنه: "كل شخص ينتمي إلى تنظيم إرهابي، أو ارتكب جريمة إرهابية، أو شارك مباشرة أو بالتسبب في ارتكابها، أو هدد بارتكابها، أو يهدد أو يخطط أو يسعى لارتكابها، أو روَّج أو حرَّض على ارتكابها"[24].

وترى الباحثة من جماع النصوص السابقة أن المشرع الاتحادي تناول تعريف الجريمة الإرهابيةمن باب الأفعال المجرمة وفقًا لهذا القانون،أو التي تشكل جناية أو جنحة وفقًا لأي قانون آخر،إذا ارتكبت بقصد إحداث نتيجة إرهابية مباشرة أو غير مباشرة؛ تتمثل في إزهاق الأرواح، أو إثارة الرعب بين مجموعة من الناس، أو إلحاق ضرر ذي شأن بالممتلكات أو البيئة، أو التسبب في أذى

(**22**)غزاله حميدة،**الإرهاب البيولوجي وآليات مكافحته دوليًا**، رسالة ماجستير، جامعه العربي التبسي، 2016/2015م، ص10.

(**23**)المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية، والذي تم نشره في الجريدة الرسمية بتاريخ 2014/8/31م.

(24) المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

بدني جسيم، أو الإخلال بأمن المجتمع الداخلي أو الدولي، أو معاداة الدولة، إلى غير ذلك من النتائج التي نص عليها المشرع فيما يتعلق بتعريف النتيجة الإرهابية.

رابعًا- تعريف الإرهاب في المواثيق والاتفاقيات الدولية:

تناولتبعض الاتفاقيات والمواثيق الدولية تعريف الإرهاب؛ منها:

1- الاتفاقية العربية لمكافحة الإرهاب الموقعة بتاريخ 1998م:

عرفت هذه الاتفاقية الإرهاب بأنه: "أي جريمة أو شروع فيها ترتكب تنفيذًا لغرض إرهابي في أي دولة متعاقدة، أوعلى ممتلكاتها، أومصالحها، أو على رعاياهاأو ممتلكاتهم؛ يعاقب عليها قانونها الداخلي، وكذلك التحريض على الجرائم الإرهابية، أو الإشارة لها، أو نشر أو طبع أو إعداد محررات أو مطبوعات أو تسجيلات أيًّا كان نوعها للتوزيع أو جمع الأموال لتمويل الجرائم الإرهابية مع العلم بذلك[25].

ويعد من الجرائم الإرهابية الجرائم المنصوص عليها في الاتفاقيات التالية، التي أشارت إليها هذه الاتفاقيةعدا ما استثنته منها تشريعات الدول المتعاقدة أو لم تصادق عليها"(26).

- اتفاقية طوكيو الخاصة بالجرائم والأفعال التي ترتكب على متن الطائرات والموقعة بتاريخ 1963/9/14.
- اتفاقية لاهاي بشأن مكافحةالاستيلاء غير المشروع على الطائرات والموقعة بتاريخ 1970/12/16.
- اتفاقية مونتريال الخاصة بقمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني والموقعة في 1971/9/23، والبروتوكول الملحق بها والموقع في مونتريال بتاريخ 1984/5/10.

(25) المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة بتاريخ 1998/4/22م.

(26) المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة بتاريخ 1998/4/22م.

- اتفاقية نيويورك الخاصة بمنع ومعاقبة الجرائم المرتكبة ضد الأشخاص المشمولين بالحماية الدولية بمن فيهم الممثلون الدبلوماسيون والموقعة في 1973/12/14.
- اتفاقية اختطاف واحتجاز الرهائن والموقعة في 1979/12/17.
- اتفاقية الأمم المتحدة لقانون البحار لسنة 1983 والتي تتعلق بالقرصنة البحرية.

2- الاتفاقية الدولية لقمع تمويل الإرهاب 1999م:

أشارت هذه الاتفاقية إلى الجرائم الإرهابية في مادتها الأولى التي تضمنت النص على أنه "يرتكب جريمة بمفهوم هذه الاتفاقية كل شخص يقوم بأية وسيلة كانت مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادته بتقديم أو جمع أموال بنية استخدامها وهو يعلم أنها ستستخدم كليًّا أو جزئيًّا للقيام بعمل يشكل جريمة في نطاق إحدى المعاهدات الواردة في المرفق وبالتعريف المحدد في هذه المعاهدات، والتي أشارت إليها هذه الاتفاقية"(27).

3- اتفاقيه دول مجلس التعاون لدول الخليج العربية لمكافحه الإرهاب 2004م:

أشارت هذه الاتفاقية إلى تعريف الإرهاب و الجريمة الإرهابية وذلك في مادتها الأولى حيث تضمنت النص على تعريف الإرهاب بأنه " كل فعل من أفعال العنف أو التهديد به، أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الممتلكات العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر".

كما تضمنت النص على تعريف الجريمة الإرهابية بأنها أي جريمة أو شروع فيها ترتكب تنفيذا لغرض إرهابي في أي دوله متعاقدة أو على ممتلكاتها أو مصالحها أو على رعاياها أو ممتلكاتهم

(27) المادة الثانية من الاتفاقية الدولية لقمع تمويل الإرهاب عام 1999م، والتي دخلت حيز النفاذ بتاريخ 2002/4/10م.

يعاقب عليها قانونها الداخلي، وكذلك لتحريض على الجرائم الإرهابية أو الإشادة بها ونشر أو طبع أو إعداد محررات أو مطبوعات أو تسجيلات يا كان نوعها للتوزيع أو لإطلاع الغير عليها بهدف تشجيع ارتكاب تلك الجرائم، ويعد جريمة إرهابيه تقديم أو جمع الأموال أيا كان نوعها لتمويل الجرائم الإرهابية مع العلم بذلك"(28).

الفرع الثاني

تعريف الجريمة الإلكترونية والإرهاب الإلكتروني

تأخذ جرائم الإرهاب الإلكتروني أشكالًا وأنواعًا مختلفةً، ويرجع ذلك إلى البيئة والظروف التي يتم ارتكاب الجريمة فيهاأو نوعية الأعمال التي تقوم بها الدول أو الأشخاص؛ حيث إنها تعدّ نوعًا من أنواع الجرائم الإلكترونية، وللوقوف على تعريف ظاهرة الإرهاب الإلكتروني لابد من الإشارة إلى تعريف الجريمة الإلكترونية، ثم التطرق لبيان تعريف الإرهاب الإلكتروني؛ وفقًا لما يلي:

أولًا- تعريف الجريمة الإلكترونية:

إن الحداثة التي تتميز بها الجرائم التي يتم ارتكابها عبر شبكة الإنترنت، واختلاف النظم الثقافية والقانونية بين الدول، والتطور التاريخي الذي مرَّ به مفهوم الجريمة الإلكترونية؛ أدى إلى صعوبة الاتفاق على تعريف عام وشامل لها؛ ويمكن الإشارة إلى أهم التعاريف الفقهية والقانونية التي وردت بشأنها على النحو التالي:

أ- التعريف الفقهي للجريمة الإلكترونية:

انقسم فقهاء القانون حول تحديد مدلول الجريمة الإلكترونية إلى أربع اتجاهات؛ هي[29]:

---

(28) المادة الأولى من اتفاقيه دول مجلس التعاون لدول الخليج العربية لمكافحه الإرهاب عام 2004م، تاريخ النشر 2008/7/24م.

(29) إبراهيم رمضان إبراهيم عطايا، **الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية**، دراسة تحليلية تطبيقية، 2015م، ص370.

1- موضوع الجريمة:

ذهب أنصار هذا الاتجاه إلى أن الجريمة التي يتم ارتكابها عبر شبكة الإنترنت ليست هي الجريمة التي يكون النظام المعلوماتي أداة ارتكابها؛ بل هي الجريمة التي تقع في نطاقة أو تقع عليه، حيث عرفها البعض من فقهاء القانون، بأنها النشاط غير المشروع الموجه لحذف أو تغيير أو نسخ أو للوصول إلى المعلومات التي يتم تخزينها داخل الحاسب أو التي تحول عن طريقه[30].

2- توافر المعرفة بتقنية المعلومات:

استند أنصار هذا الاتجاه في تعريف الجريمة الإلكترونية إلى شخصية الفاعل، الذي لا بد أن يكون ملمًا بتقنية المعلومات، والتعامل مع تقنية أجهزة الحاسب الآلي؛ فعرفها البعض بأنها الجريمة التي يتطلباقترافهامعرفة فنية بتقنية الحاسبات تمكن الفاعل من ذلك[31].

3- وسيلة ارتكاب الجريمة:

يعتمد أنصار هذا الاتجاه في تعريف الجريمة الإلكترونية على وسيلةارتكاب الجريمة،التي تتمثل في الحاسوب أو إحدى وسائل التقنية الحديثة المرتبطة به، فعرفها البعض بأنها النشاط الإجرامي الذي تستخدم فيه التقنية الإلكترونيةوالحاسوب الآلي الرقمي بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ النشاط الإجرامي[32].

4- دمج أكثر من تعريف:

عمد أصحاب هذا الاتجاه إلى وضع تعريف شامل للجريمة التي يتم ارتكابها عبر شبكة الإنترنت،

---

(30) شمسان ناجي صالح الخيلي،مرجع سابق، ص34.

(31) عبد الرحيم محمد، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، مجلس البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، الأمانة العامة لمجلس التعاون لدول الخليج العربية، 2016م، ص22.

(32) داود سليمان علي الحمادي، **أحكام جريمة التزوير الإلكتروني وفقًا لأحكام قانون مكافحة جرائم تقنية المعلومات الإماراتي**، دار النهضة العربية، القاهرة، د.ت، ص22/20.

يتضمن جميع أركانها؛ وذلك من خلال دمج أكثر من تعريف[33]، حيث عرفت بأنها الجريمة التي يتم فيها استخدام الحاسب الآلي كأداة أو وسيلة لارتكابها، أو جريمة من الجرائم التي يكون الحاسب نفسه ضحيتها، فهي بذلك تشمل كل أشكال السلوكغير المشروع الذي يتم من خلال الحاسب، واستخدام التقنية الإلكترونية[34].

وترجح الباحثة المعيار الأخير المتمثل في دمج أكثر من تعريف، لأنهالأساس الأنجح من الناحية العملية في تعريف الجريمة الإلكترونية؛ لاعتماده على دمج عدة معايير، فضلًا عنأنه يوفر إحاطة شاملة بالظاهرة الخاصة بجرائم التقنية، و إمكانية التعامل مع التطورات التقنية المستقبلية.

ب-التعريف التشريعي للجريمة الإلكترونية:

أصدر المشرع الإماراتي القانون الاتحادي رقم 2 لسنة 2006م بشأن مكافحة جرائم تقنية المعلومات، إلا أنه لم يتضمن تعريفًا محددًا للجريمة الإلكترونية[35]، وقد أُلْغِيَ هذا القانون بموجب المرسوم الخاص بمكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012م، ولم يرد في هذاالقانون أيضًا تعريف لجريمة تقنية المعلومات أو الجريمة الإلكترونية،لكنه أشار إليها من خلال تجريم عدد من الأفعال ترتبط بوسيلة تقنية المعلومات، حيث عرفها بأنها " أداة إلكترونية مغناطيسية بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية، وأداء العمليات المنطقية

(33) قد أجري استبيان من قبل منظمة التعاون الاقتصادي والتنمية، تم توزيعه على دول الأعضاء حول تحديد مدلول للجريمة المرتكبة عبر الإنترنت، وقد ورد في الإجابة البلجيكية أنها هي: "كل امتناع أو فعل يكون من شأنه الاعتداء على الأموال المعنوية أو المادية يكون ناتجًا عن تدخل التقنية المعلوماتية، بطريقة مباشرة أو غير مباشرة". شمسان ناجي صالح الخيلي، مرجع سابق، ص34.

(34) عبد الله دغش العجمي،**المشكلات العلمية والقانونية للجرائم الإلكترونية**، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2012م، ص12.

(35) القانون الاتحادي رقم 2 لسنة 2006م بشأن مكافحة جرائم تقنية المعلومات الملغى. منشور في العدد رقم 442 من الجريدة الرسمية بتاريخ 2006/1/30م.

والحسابية،أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية، أو إيصالها للآخرين"[36].

ج- **التعريف القضائي للجريمة الإلكترونية**

وفيما يتعلق بالتعريف القضائي للجريمة الإلكترونية فقد أشارت محكمة تمييز دبي إلى تعريف وسيلة تقنية المعلومات والتي يمكن ارتكاب الجرائم من خلالها وذلك وفق الآتي: "لما كان ذلك وكانت وسيلة تقنية المعلومات تعد أداة إلكترونية مغناطيسية بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية، وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلةموصلة أو مرتبطة بشكل مباشر تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية، أو إيصالها للآخرين، من خلال تخزين بيانات أو اتصالات تعمل أو تتعلق بالاقتران مع مثل هذه الأداة من خلال الارتباط بين أكثر من وسيلة وذلك للحصول على معلومات وبيانات وتبادلها، حيث إن المشرع لم يقم بتحديد تقنية المعلومات بوسيلة محددة ومعينة، فقد تشمل الشبكة المعلوماتية، والحاسب الآلي،والبلوتوث، وأجهزة الموبايل، وجهاز إلكتروني منقول أو ثابت، سلكي أو لاسلكي، يحتوى على نظام معالجة البيانات، أو استرجاعها، أو تخزينها أو استقبالها، أو إرسالها؛ مثل (الواتس آب)، ومواقع التواصل الاجتماعي، والرسائل القصيرة، والفيس بوك، ويؤدي وظائف محددة ومعينة حسب الأوامر المعطاة له والبرامج، ويمكن أن يكون ذلك من خلال الكتابة، أو الصوت، أو الصور، أو الحروف، أو الأرقام، أو الإشارات أو غيرها، وأيضًا أية وسيلة يمكن أن تنشأ في المستقبل تحت هذه المعطيات، وذلك باعتبارها ذات طابع مادي، تتحقق بكل سلوك أو فعل غير مشروع يرتبط بأي شكل من

(36) المادة الأولى من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات. صادر بتاريخ 2012 /8/13م.

الأشكال، أو أي وجه بالشبكة المعلوماتية السلكية أو اللاسلكية بالحاسب الآلي، أو الهواتف الذكية والنقالة"[37].

د- تعريف الجريمة الإلكترونية في الاتفاقيات الدولية:

عرفت اتفاقية مجلس أوروبا لسنة 2001م جرائم الحاسب الآلي من خلال الإشارة إلى الجرائم التي تتعلق بالحاسب الآلي؛ وهي على الترتيب: الجرائم التي تمس خصوصية وسلامة بيانات ونظم الكمبيوتر،التي تتمثل في النفاذ غير المشروع، والتدخل في البيانات، والاعتراض غير المشروع، والتدخل في النظام، وأيضًا إساءة استخدام الأجهزة، والجرائم ذات الصلة بالكمبيوتر،وتتمثل في الاحتيال، والتزوير المرتبط بالكمبيوتر، والجرائم ذات الصلة بالمحتوى، وهي التي تتعلق بمواد إباحية عن الأطفال، وأيضًا الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة[38].

ثانيًا- تعريف الإرهاب الإلكتروني:

برز مصطلح الإرهاب الإلكتروني وشاع استخدامه عقب الطفرة الكبيرة التي حققتهااستخدامات الإنترنت والحواسيب الآلية وتكنولوجيا المعلومات، وبغية الوقوف على تعريف الإرهاب الإلكتروني لا بدَّ من توضيح التعريف الفقهي والقانوني للإرهاب؛ على النحو التالي:

أ- التعريف الفقهي للإرهاب الإلكتروني:

يلاحظ عدم وجود تعريف موحد أو متفق عليه للإرهاب الإلكتروني، حيث حاول كل اتجاه أن يقوم بتعريف الجريمة حسب منظوره الخاص لها؛ فقد عرفه البعض بأنه الهجماتغير المشروعة، أو التهديد بهجمات ضد الشبكات أو الحاسبات، أو المعلومات المخزنة إلكترونيًّا، توجه بهدف الابتزاز، أو

---

(37) طعن جزائي رقم 895 لسنة 2015م، الأحكام الجزائية، جلسة 18/ 1 / 2016 محكمه تمييز دبي، موقع المحامون العرب, موسوعة الأحكام القضائية للدول العربية، https://mohamoon.co/mwswaa-l-hkm-lqdy-y-laarby.html تاريخ الدخول 2021/1/15.

(38) الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، مجموعة المعاهدات الأوربية، مجلس أوروبا، 2001م، ص6/4.

الإجبار، أو الانتقام، أو التأثير في الشعوب أو الحكومات أو المجتمع الدولي بأسره، بغرض تحقيق أهداف دينية، أو سياسية، أو اجتماعية.ولكي يعدّ الشخص إرهابيًّا على شبكة الإنترنتوليس مخترقًا فقط؛ لا بد أن تؤدي الهجمات التي يشنها إلى عنف ضد الممتلكات أو الأشخاص، أو أن تحدث على الأقل ضررًا كافيًا من أجل نشر الرعب والخوف(39).

وعرفه البعض الآخر بأنه الجريمة ذات الطابع المادي، التي تتمثل في السلوك غير القانوني باستخدام الأجهزة الإلكترونية، الذي ينتج عنه الحصول على فوائد معنوية ومادية للمتهم، وتحميل الضحية الخسارة المقابلة لهذه الفوائد، وتهدف هذه الجريمة إلى ابتزاز الأشخاص باستخدام المعلومات الموجودة في الأجهزة، أو القرصنة من أجل إتلاف أو سرقة هذه المعلومات(40).

ب-**التعريف القانوني للإرهاب الإلكتروني:**

أطلق مكتب التحقيقات الفيدرالي تعريفًا على الإرهاب الإلكتروني بأنه "الهجوم المخطط ذو الدوافع والأهداف السياسية، الذي يستهدف الأنظمة والمعلومات الإلكترونية وبياناتها وبرامجها، ويؤدي إلى استخدام العنف ضدالأهدافغير القتالية، من خلال عملاء سريّين، أو مجموعات وطنية فرعية"(41).

كما عرف مجمع الفقة الإسلامي الدوليالتابع لمنظمة المؤتمر الإسلامي الإرهاب الإلكتروني بأنه: "التخويف أو العدوان أو التهديد المعنوي أو المادي الصادر من الجماعات، أو الدول، أو الأفراد على الإنسان، أو نفسه، أو عِرْضه، أو دينه، أو ماله، أو عقله بغير حق، باستخدام الوسائل الإلكترونية

---

(39) سليمان أحمد فضل،**المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدوليةالإنترنت،** دار النهضة العربية، القاهرة، 2013م، ص128.

(40) أحمدي بوجلطيه بوعلي،**الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي،** دراسة للتجربتين السعودية والقطرية، أكاديمية الدراسات الاجتماعية والإنسانية، قسم العلوم الاقتصادية والقانونية، ع16، 2016م، ص183.

(41) بيتر سينجر، **الإرهاب الإلكتروني، خرافات وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجهة،** سلسلة محاضرات الإمارات 215، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2018م، ص3.

والموارد المعلوماتية، بمختلف أشكال العدوان، وصور الفساد؛ حيث إن الإرهاب الإلكتروني يعتمد على استخدام الإمكانيات التقنية و العلمية، واستغلالا لشبكات المعلوماتية و وسائل الاتصال، من أجل ترويع و تخويف الآخرين لإلحاق الضرر بهم"[42].

وقد أشار المرسوم الخاص بمكافحة جرائم تقنية المعلومات الاتحادي رقم 5 لسنة 2012م إلى جرائم الإرهاب التي يمكن ارتكابها عبر شبكة الإنترنت باستخدام وسائل التقنية الحديثة، من خلال تجريم العديد من الأفعال التي ترتبط بوسيلة تقنية المعلومات، و تتمثل في "إدارة وإنشاء مواقع إلكترونية أو نشر معلومات بهدف التجنيد، أو الترويج لأفكار من شأنها إثارة الفتنة أو الطائفية، أو الإخلال بالآداب العامة، أو الإضرار بالوحدة الوطنية، وإدارة وإنشاء مواقع إلكترونية أو نشر معلومات لهيئة غير مشروعة أو جماعة إرهابية بقصد الترويج لها، وتسهيل الاتصال بقياداتها، أو لاستقطاب عضوية لها، أو تحبيذ أو ترويج أفكارها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية، أو استخدام إحدى وسائل تقنية المعلومات بقصد الترويج والاتجار بالذخائر، والأسلحة النارية، والمتفجرات في غير الأحوال المصرح بها قانونًا"[43].

وترى الباحثة مما تقدم أن الإرهاب الإلكتروني لا يختلف عن مفهوم الإرهاب التقليدي إلا من حيث الوسيلة المستخدمة؛ وهي تكنولوجيا المعلومات في مجال الإنترنت والحاسب الآلي، وغير ذلك من وسائل التواصل الاجتماعي، فرغم المزايا العديدة التي تقدمها الشبكة الإلكترونية وما تحتوي عليه من معلومات يسهل وصولها للملايين من الناس في آن واحد، إلا أنها تفسح مجالًا واسعًا للإرهابيين المحترفين في استغلال الشبكة المعلوماتية بغرض تحقيق أهدافهم في العديد من المجالات من خلال

---

(42) بوقرين عبدالحليم،**المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي**، دراسة مقارنة، المجلد 16، ع1، مجلة جامعة الشارقة للعلوم القانونية، 2019م، ص384.

(43) المواد 24، 25، 26 من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات.

توجيه الرسائل والتهديدات الإلكترونية، والتهديد بنظم المعالجة الآلية الخاصة بالمعلوماتعبر تقنية الاتصالات الحديثة.

أما فيما يتعلق بالمفهوم الخاص بكلٍّ منهما فكلاهما ذو طابع تدميري، من خلال التهديد والترهيب الذي يحقق الأهداف ذاتها والأضرار عينها،في المجالات الاجتماعية أو العسكرية أو السياسية أو الاقتصادية،أوغيرها من المجالات.

المطلب الثاني

الأركان المشتركة لجرائم الإرهاب الإلكتروني

تمهيد وتقسيم:

تتخذ الجريمة التي يتم ارتكابها عبر شبكة الإنترنت ووسائل التواصل الاجتماعي الفضاء الافتراضي مسرحًا لها،مما يجعلها تتميز بالعديد من الخصائص، إلا أن ذلك لا يعني أنها تختلف عن الجريمةالتي يتم ارتكابهابالوسائل التقليدية، فهي تتطلب لتحققها العناصر والأركان اللازمة والمتفق على ضرورة توافرها في أي جريمة.

ستوضح الباحثة الركن الشرعي أو الصفةغير المشروعة للفعل،ثم تتناول كُلًّا من الركنين المادي والمعنوي للجريمة؛ من خلال الفروع الآتية:

الفرع الأول

الرُّكن الشرعي

الركن الشرعي هو الصفة غير المشروعة للفعل؛ من خلال وجود النص الذي يجرم الفعل، ويبيّن العقاب الذي يترتب عليه، فلا قيام للجريمة إذا كان الفعل مشروعًا، والركن الشرعي يتجرد من

الكيان المادي نظرًا لكونه مجرد تكييف قانوني، فيختلف بذلك عن الركن المادي للجريمة، كما أن للركن الشرعي طابعًا موضوعيًّا يتمثل بتطبيق قواعد قانون العقوبات على الفعل، فوجوده غير مرتهن باتجاه خاص لإرادة الجاني، ومن هذه الزاوية يختلف أيضًاعن الركن المعنوي للجريمة[44].

فالنص الشرعي هو النص الذي يضفي على الامتناع أو الفعل الصفةغير المشروعة،ففي حالة وجود النص القانوني الذي يجرم الفعل أو الامتناع، وهو ما يعرف بمبدأ شرعية الجرائم والعقوبات، وأنه لا جريمة ولا عقوبة إلا بنص، والذي يتمثل في وجود نص قانونيساري المفعول يفصح عن مضمون الجريمة،من خلال توضيح السلوك المجرم والعناصر المحددة له وعقوبته، فإذا انتفى النص التشريعي الذي يجرم الفعل أو الامتناع انتفت الصفة غير المشروعة للفعل[45].

وقد اخلتف الفقهاء حول طبيعة النص الشرعي الذي يجرم الفعل أو الامتناع؛ فذهب البعض إلى أأنه يعدّ ركنًا من أركان الجريمةإلى جانب كُلٍّ من الركنين المادي والمعنوي للجريمة،وذهب البعض الآخر إلى اعتباره صفة غير مشروعة تكون مقترنة بالسلوك وتجعله مجرمًا ومعاقبًا عليه[46].إلا أن المتفق عليه أن مبدأ شرعية الجرائم والعقوبات يعدّ من أهم المبادئ التي تحمي حقوق الأفراد وحرياتهم، وقد حرصت المواثيق الدولية والدساتير الخاصة بالدول على النص عليه صراحة، كما ورد في المادتين العاشرة و الحادية عشر من الإعلان العالمي لحقوق الإنسان الصادر عام 1948م [47]، والمادتين

---

(44) محمود نجيب حسني،**شرح قانون العقوبات القسم العام**، ط8، دار المطبوعات الجامعية، الإسكندرية،2017م، ص71.

(45) سالم بن حامد بن على البلوي،**التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة**، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2009م، ص17/16.

(46) نبيلة هبه هروال، **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات**، دار الفكر الجامعي، الإسكندرية، 2006م، ص42/41.

(47) الإعلان العالمي لحقوق الإنسان الصادر عام 1948م، بموجب قرار الجمعية العامة للأمم المتحدة، المؤرخ في 1948/12/10م.

الخامسة و الثامنة من الإعلان الخاص بحقوق الإنسان الصادر عام 1948م[48].

أما فيما يتعلق بالصفة غير المشروعة والركن الشرعي لجرائم الإرهاب الإلكتروني، التي تكون شبكة الإنترنت قد استخدمت كوسيلة في ارتكابها، فإنها تتمثل في وجود فعل إجرامي تم النص عليه في قانون مكافحة جرائم تقنية المعلومات.

أما بالنسبة لدولة الإمارات فقد نص القانون الاتحادي رقم 7 لسنة 2014 بشأن مكافحة الجرائم الإرهابية في المادة الأولى منه على ذلك فيما يتعلق بالإرهاب التقليدي[49].

كما نص في قانون مكافحة جرائم تقنية المعلومات رقم 2012/5م على تجريم العديد من الأفعال التي تعتبر جرائم إرهاب يمكن ارتكابها عبر شبكة الإنترنت باستخدام وسائل التقنية الحديثة؛ كجرائم إدارة وإنشاء مواقع إلكترونية، أو نشر معلومات بهدف التجنيد، أو الترويج لأفكار من شأنها إثارة الفتنة أو الطائفية، أو الإضرار بالوحدة الوطنية، وإدارة وإنشاء مواقع إلكترونية،حيث نص المشرع على تجريم هذه الأفعال وبيَّن العقوبات المقررة لها فيما يعرف بالصفة غير المشروعة والركن الشرعي لهذه الجرائم[50].

الفرع الثاني

الركن المادي

الأصل أن لكل جريمة من الجرائم ركنًا ماديًّا، يتمثل في المظهر الخارجي لها، فهو الواقعة المجرمة بالمعنى الضيق؛ أي ماديات الجريمة التي يعاقب عليها النظامالتي تكشف عن ارتكابها،

---

(48) الإعلان العالمي لحقوق الإنسان الصادر عام 1948م، بموجب قرار الجمعية العامة للأمم المتحدة، المؤرخ في 1948/12/10م.

- أمين مصطفى محمد، **قانون العقوبات، القسم العام**، دار المطبوعات الجامعية، الإسكندرية، 2016م، ص16.

(49) المادة الأولى من القانون الاتحادي رقم 7 لسنه 2014م، بشأن مكافحة الجرائم الإرهابية.

(50) المواد 24، 25، 26 من القانون الاتحادي رقم 5 لسنة 2012 م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون الاتحادي رقم 2 لسنة 2018م الصادر بتاريخ 2018/7/24م.

وتجعل إقامة الدليل عليها والتوصل إلى مرتكبها أمرًا ممكنًا، وأهم ما يميز الركن المادي عناصره الثلاثة التي يتكون منها؛ التي تتمثل في السلوك الإجراميالذي يصدر من الفاعل، والذي يعبر عنه بالنشاط الإجرامي الذي يقوم به مرتكب الجريمة، سواء كان إيجابيًّا أم سلبيًّا، والنتيجة الإجرامية التي تتمثل في الضرر الذي يصيب الحق أو المصلحة المحمية قانونًا، وعلاقة السببية التي تربط بين هذا السلوك والنتيجة الإجرامية التي تحققت(51).

وحيث إن جريمة الإرهاب الإلكتروني لها طبيعة خاصة، فقد اشترط المشرع لها ركنًا مفترضًا لا بد من تحققه حتى يقع عليه السلوك الإجرامي في هذه الجريمة، يتمثل في وجود الكيان المادي للنظام المعلوماتي و المكونات المادية له؛ كالآلات والأجهزة والمعدات والمواقع الإلكترونية، وغيرها من وسائل تقنية المعلومات. فتثير هذه الجريمة ما يعرف بمصطلح الشرط المفترض، الذي يسبق تحقق الركن المادي للجريمة، فهو ليس من الأركان العامة للجريمة، إلا أنه يمثل ركنًا خاصًّا لها، ومن ثمَّ فإنَّ تحديد الركن المادي في جريمة الإرهاب الإلكتروني يثير جملةً من الصعوبات التي تفرضها طبيعة الوسط التقني الذي تقع فيه الجريمة(52).

وتجدر الإشارة أيضًا إلى أن السلوك الإجرامي في الجرائم الإرهابية لا يمكن أن يتخذ في جميع الحالات سوى المظهر الإيجابي، فالسلوك الإيجابي وحده هو الذي ينطوي على قدر من الشدة والقوة، أو التهديد والعنف، فهذه الجرائم ينعدم فيها السلوك السلبي المتمثلبالامتناع عن القيام بعمل(53).

هذا وقد حددت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الأفعال التي تعد من الجرائم

---

(51) أمين مصطفى محمد،**قانون العقوبات، القسم العام**، مرجع سابق، ص199.

(52) إبراهيم محمد القاسمي،**جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، وفقًا للمرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات وتعديلاته**، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018م، ص11/10.

(53) سليمان أحمد فضل، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت**، مرجع سابق، ص126.

الإرهابية المتعلقة بتقنية المعلومات؛ وتتمثل في: "نشر أفكار ومبادئ جماعات إرهابية والدعوة إليها، تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر طرق صناعة المتفجرات التي تستخدم في عمليات إرهابية، ونشر النعرات والفتن والاعتداء على الأديان والمعتقدات"[54].

كما نص المرسوم بقانون اتحادي رقم 5 لسنة 2012م المعدل بشأن مكافحة جرائم تقنية المعلومات على الأفعال الإرهابية التي تتم عبر شبكة الإنترنت، و وسائل التكنولوجيا الحديثة،حيث يمكن تحديدالسلوك الإرهابي الذي يتم باستخدام وسائل التقنية الحديثة بصفته أحد عناصر الركن المادي في جريمة الإرهاب الإلكتروني.

وتعليقًا على السلوك الإجرامي الذي نصت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمرسوم بقانون اتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات؛ أن الجماعات الإرهابية والمتطرفة تستهدف من إنشاء وإدارة المواقع الإلكترونية على شبكة الإنترنت عدة أهداف؛ أبرزها الاستطلاع، ونشر الفكر والدعاية، والاتصال وإنشاء مجتمع إلكتروني، والدعم المالي، والتجنيد والقرصنة؛ بالإضافة إلى تدمير المواقع والنظم المعلوماتية والبنية التحتية لتحقيق أغراضهم الإرهابية، ويمكن توضيح هذه الأهداف على النحو التالي:

- **تدمير المواقع والنظم المعلوماتية والبنية التحتية**

قد تسهدف الجماعات الإرهابية والمتطرفة من إنشاء وإدارة المواقع الإلكترونية عبر شبكة الإنترنت تدمير المواقع والنظم المعلوماتية والبنية التحتية، وذلك من خلال النفاذ و الدخول إلى شبكات التحكم في المرافق العامة؛ مما يؤدي إلى حدوث شلل تام في البنية التحتية الأساسية، وشيوع الفوضى

(54) المادة (15) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

و الخراب في جميع أرجاء البنية التحتية؛ بل واحتمال تدميرها بالكامل[55].

إضافة إلى ما تمثله المواقع الإباحية من خلال الدور الذي تقوم به في انتشار الإرهاب الإلكتروني، من تجميع أكبر قدر من المعلومات والبيانات عن الشركات المستهدفة والمؤسسات واختراقها عبر استغلال الهاكرز لغرف الدردشة الخاصة بالمواقع الإباحية؛ لجمع الأسرار واختراق الأجهزة الحساسة وتدمير المواقع والنظم المعلوماتية [56].

- **التجنيد:**

تستغل الجماعات والمنظمات الإرهابية شبكة الإنترنت ومواقع التواصل الإلكتروني لتجنيد الشباب ممن تتوافر لديهم بذور الفكر والتطرف؛ حتى تضمن المحافظة على استمرارها وبقائها، وتسعى هذه المواقع المتطرفة إلى استقطاب دماء جديدة لضمها إلى التنظيمات الإرهابية، مستغلة في ذلك تعاطف الآخرين منمستخدمي الإنترنت في القضايا الخاصة بهم، تحت ستار المبادئ البرَّاقة، أو التفسير التعسفي للدين[57].

- **نشر الفكر والدعاية:**

تلجأ الجماعات الإرهابية والمتطرفة إلى نشر الأفكار والدعاية على مواقعها على الإنترنت في العالم الواسع دون عوائق مادية تحول دون نقل معتقداتها وأفكارها إلى المجتمعات البشرية، وذلك على مدار الساعة.

حيث يعمل قادة التنظيمات والجماعات الإرهابية والمتطرفة على تزويد مؤيديهم بمجموعة من الكتيبات السياسية والدينية والفكرية، لدرجة أصبحت فيها الشبكة العنكبوتية مكتبة افتراضية للمواد

---

(55)سليمان أحمد فضل، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الإنترنت**، دار النهضة العربية القاهرة، 2013م، ص128.

(56) مها محمد أحمد عنانزه، مرجع سابق، ص14.

(57) مها محمد أحمد عنانزه،مرجع سابق، ص14.

الإرهابية والمتطرفة، تتناول فتاوى إلكترونية مشددة، والتهديد والتهجم على علماء الدين والنيل منهم، الأمر الذي يؤدي إلى وجود فجوة وعدم ثقة بين أبناء المجتمع؛ خاصة الشباب منهم وعلماء الدين[58].

فالإرهاب الإلكتروني ينتشر من خلال مواقع ترويج الأفكار التكفيرية والمتطرفة التي أنشأتها جهات أو منظمات سياسية أو دينية أوأشخاص؛ بهدف نشر أفكارهم المتطرفة، والسيطرة على محدودي الثقافة. [59]

حيث تأخذ هذه المواقع بظواهر النصوص الدينية دون العلم بمقاصدها، لدرجة الغلو في الدين، وتحول الشخص المتطرف إلى إرهابي، واتخاذه منهجًا معاكسًا ومخالفًا للواقع.، كما تؤدي الفتاوى الإلكترونية التكفيرية المشددة إلى الكراهية والانفعال الحاد وسلوك العنف، من خلال الدعوة إلى نشر الشائعات والفتن التي تؤدي إلى الانقسام والفرقة[60].

بناءً على ما سبق يمكن الإشارة إلى بعض المواد التي تنشرها المواقع الإرهابية عبر شبكة الإنترنت ووسائل التواصل الاجتماعي؛ وتتمثل في[61]:

- المواد الإخبارية المتعلقة بأنشطة التنظيم، والإنجازات البطولية، وأيضًا التصريحات الإعلامية حول النشاط الخاص بالتنظيم.
- الحوارات المفتوحة بين أعضاء المنتديات الإلكترونية حول العديد من الموضوعات.

---

(58) محمود صالح العادلي،**الإرهاب الرقمي في القانون البحريني المقارن بالنظام السعودي والقانون المصري، (ماهيته الجماعات المتطرفة والإرهابية، صور استخدام الإنترنت في الإرهاب، البحث والتحقيق الجنائي المتصل بالإرهاب الرقمي**"،دار النهضة العربية، القاهرة، ط1، 2016م، 103/102.

(59) محمود صالح العادلي،**الإرهاب الرقمي في القانون البحريني المقارن بالنظام السعودي والقانون المصري**،ص 103 ومابعدها.

(60) مها محمد أحمد عنانزه، مرجع سابق، ص14.

(61) المرجع السابق، ص14.

- المواد الدعوية التي تشمل الخطب الخاصة بقيادات الجماعات الإرهابية و المقالات، التي تهدف إلى حشد أكبر عدد من الجمهور؛ من خلال إخراج هذه المواد بصورة جذابة.
- الدراسات والكتب و المواد الخاصة بكيفية صنع المتفجرات والقنابل، ونشر المواد الوثائقية، وكيفية الهروب من الأجهزة الأمنية.
- **القرصنة والدخول غير المشروع على البيانات:**

تستهدف الجماعات الإرهابية والمتطرفة اختراق البريد الإلكتروني، أو ما يسمى بالهاكرز، والدخول غير المشروع للمعلومات الشخصية والسرية التي تتميز بالخصوصية، من خلال اختراق البريد الإلكتروني ونشر الفيروسات، فالمعلومات والبيانات المبرمجة والمتصلة فيما بينها من خلال شبكة اتصالات تكون عرضة للوصول غير المشروع إليها.

حيث إنها تمثل صندوق مغلق يحتوى على بيانات وموجودات في مكان عام، فلا يتعدى الأمر إيجاد مفتاح هذا الصندوق المغلق، فقابلية المعلومات والبيانات للوصول غير المشروع إليها أصبحت تفوق كثيرًا ما كان عليه الأمر سابقًا قبل وجود الحاسبات الآلية.

فغالبية الجرائم التي يتم ارتكابها عبر شبكة الإنترنت تستهدف جهات أو أشخاص معينة، وقد يتم ارتكابها بطريقة مباشرة كالتهديد والتشهير، أو بطريقة غير مباشرة كالدخول غير المشروع، والحصول على المعلومات والبيانات الخاصة بالأشخاص أوالجهات، واستخدامها في ارتكاب العديد من الجرائم[62].

انطلاقًا من ذلك جرّم المشرع الاتحادي الدخول على الموقع الإلكتروني، أو شبكة المعلومات، أو النظام المعلومات الإلكتروني، أو وسيلة تقنية المعلومات بدون تصريح أو إذن أو تجاوز الحدود

(62)شمسان ناجي صالح الخيلي،مرجع سابق، ص40.

الخاصة بالتصريح، كما جرم البقاء فيه بطريقة غير مشروعة[63].

كما يوجد العديد من التطبيقات القضائية التي وردت بشأن جرائم الدخول غير المشروع، حيث جاء في قضاء محكمة النقض بأبو ظبي:"لما كان الثابت في مدونات الحكم الذي طُعن فيه، والذي أدانت فيه المحكمة المطعون ضده بالجريمة الخاصة بالدخول إلى وسيلة تقنية المعلومات، حيث إن المطعون ضده وهو هندي الجنسية يعد أجنبيًّاعن الدولة، وأن محكمة أول درجة قد أدانته وعاقبته بالحبس مدة أربعة أشهر وقضت بإبعاده، وأن الحكم المستأنف قد قضى بتعديل الحكم والاكتفاء بحبس المتهم مدة شهر واحد ولم تتبع ذلك بعقوبة الإبعاد، ويفيد ذلك أنه قد تم إسقاط عقوبة الإبعاد، طبقًا لهذا التعديل الذي قد أجراه الحكم المستأنف، و بالتالي يكون قد أخطأ في تطبيق القانون الذي يجب إعماله؛ مما يوجب نقض هذا الحكم وتصحيحه بإضافة عقوبة الإبعاد إلى العقوبة التي قد قضي بها[64].

وترى الباحثة أن فعل الدخول لا يكون غير مشروع في حد ذاته؛ بل يتخذ الوصف الإجرامي إذا كان هذا الدخول بدون تصريح و بغير وجه حق، وقد يتم استخدام طرق وأساليب عديدة للدخول إلى النظام والوصول إلى البيانات والمعلومات المخزنة، دون رضاء الشخص المسؤول عن هذه المعلومات أو النظام، ومن ثمَّ يمكن تطبيق ذلك على جرائم الإرهاب الإلكتروني التي يمكن تحققها من خلال الدخول غير المشروع إلى البيانات، وإساءة استخدام النظام، والحصول على البيانات والمعلومات واستغلالها في تحقيق العديد من الأغراض الإرهابية، وترويج ونشر الأفكار الطائفية بواسطة شخص غير مرخص أو مصرح له باستخدامه".

ويؤكد ذلك ما نص عليه المشرع الاتحادي في قانون مكافحة جرائم تقنية المعلومات من تجريم

---

(63)المادة (2) منالقانون الاتحادي رقم5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات.

(64) الطعن رقم 769 لسنه 2010م س4 ق.أ جزائي، مجموعه الأحكام والمبادئ القانونيه الصادره عن محكمه النقض في الدائره الجزائيه، السنه القضائيه الرابعه 2010، ج3، ص1086.

الحصول بدون تصريح على رقم سري أو شيفرة أو كلمة مرور، أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع إلكتروني، أو شبكة معلوماتية، أو نظام معلومات إلكتروني، أو معلومات إلكترونية[65].

- **الاتصال وإنشاء مجتمع الكتروني:**

تساعد شبكة الإنترنت ومواقع التواصل الاجتماعي المنظمات الإرهابية والجماعات المتطرفة في الاتصال والتنسيق فيما بينها، ويرجع ذلك لوفرة المعلومات والبيانات التي يمكن تبادلها من خلال شبكة الإنترنت، والخدمات العامة ذات الطابع العام المتاحة للجميع؛ كتصفح مواقع الويب.

بالإضافة إلى قلة تكاليف الاتصال باستخدام شبكة الإنترنت مقارنة بوسائل الاتصال الأخرى، فضلًا عن كونها تتيح لهذه الجماعات العديد من وسائل الاتصال السريعة؛ كالبريد الإلكتروني، والمواقع، والمنتديات، وبرامج الصورة والصوت سكايب، وإيمو، وفايبر، والمواقع الخاصة ببث مواقع الفيديو.

وذلك بهدف التأثير على الشباب، ونشر مقاطع لعناصرها أثناء العمليات الإرهابية، وبعد القيام بها؛ مما يدفع الشباب إلى الانخراط والاتصال معها، فضلًا عن قيامها بتوظيف المنتديات البعيدة عن الشبهة؛ مثل المواقع النسائية والجنسيةوالرياضيةلتبادل المعلومات بين أعضائها[66].

- **الدعم المعنوي والمالي:**

يدخل ضمن السلوك الإجرامي لجرائم الإرهاب الإلكتروني؛ عمليات دعم المنظمات والجماعات

---

(65) المادة (14) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات.

(66)محمود صالح العادلي،مرجع سابق، ص106/105. أيضًا: محمود أحمد طه،المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، 2017/2016م، ص170.

الإرهابية عبر المواقع الإلكترونية، سواء تم ذلك من قبل المخابرات الدولية، أو من خلال مؤيديها، عن طريق إرسال أموال إليهم، أو نشر العمليات الخاصة بهم على الشبكة، وتمويل التنظيمات غير المشروعة.

وقد جرم المشرع الاتحادي جريمة تمويل الإرهاب و التنظيمات غير المشروعة، في القانون الخاص بمواجهة جرائم غسل الأموال، و مكافحة تمويل الإرهاب والتنظيمات غير المشروعة[67]؛ بالنص على أنه "مع عدم الإخلال بأحكام القانون الاتحادي رقم (3) لسنة 1987م المشار إليه، والقانون الاتحادي رقم 7 لسنة 2014م المشار إليه:

1- يعد مرتكبًا لجريمة تمويل الإرهاب كل من ارتكب عمداً أيًّا مما يأتي:

أ- أحد الأفعال المحددة في البند (1) من المادة (2) من هذا المرسوم بقانون؛ التي تتمثل في:

1- تحويل المتحصلات، أو نقلها، أو إجراء أي عملية بها بقصد إخفاء أو تمويه مصدرها غير المشروع.

2- إخفاء أو تمويه حقيقة المتحصلات أو مصدرها أو مكانها، أو طريقة التصرف فيها، أو حركتها، أو ملكيتها، أو الحقوق المتعلقة بها.

3- اكتساب أو حيازة أو استخدام المتحصلات عند تسلمها.

4- مساعدة مرتكب الجريمة الأصلية على الإفلات من العقوبة إذا كان عالمًا بأن المتحصلات كلها أو بعضها مملوكة لتنظيم إرهابي، أو لشخص إرهابي، أو معدة لتمويل تنظيم إرهابي، أو شخص إرهابي أو جريمة إرهابية، ولو كان ذلك دون قصد إخفاء أو تمويه مصدرها غير المشروع).

---

(67)المواد 2، 3، المرسوم بقانون اتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية رقم 10 لسنه 2019، الصادر بتاريخ 2018/9/23م.

ب- قدم المتحصلات، أو جمعها، أو أعدها، أو حصلها، أو سهل للغير الحصول عليها بقصد استخدامها، مع علمه بأنها سوف تستخدم كلها أو بعضها في ارتكاب جريمة إرهابية، أو ارتكب تلك الأفعال لصالح تنظيم إرهابي، أو لشخص إرهابي مع علمه بحقيقتهما أو غرضهما.

2 - يعد مرتكبًا لجريمة تمويل التنظيمات غير المشروعة كل من ارتكب عمدًا أيًّا مما يأتي:

أ- أحد الأفعال المحددة في البند (1) من المادة (2) من هذا المرسوم بقانون، إذا كان عالمًا بأن المتحصلات كلها أو بعضها مملوكة لتنظيم غير مشروع أو لأحد المنتمين له، أو معدة لتمويل أي منهما، ولو كان ذلك دون قصد إخفاء أو تمويه مصدرها غير المشروع.

ب-قدم المتحصلات، أو جمعها، أو أعدها، أو حصلها،أو سهل للغير الحصول عليها بقصد استخدامها، مع علمه بأنها سوف تستخدم كلها أو بعضها لصالح تنظيم غير مشروع، أو لأحد المنتمين له مع علمه بحقيقتهما أو غرضهما".

- **التدريب والاستطلاع:**

تستخدم الجماعات الإرهابية و المتطرفة شبكة الإنترنت كمصدر مهم للبيانات و المعلومات، حيث يقوم عدد من الشركات و الأفراد و غيرهم بوضع معلومات حساسة وهامة على الشبكة بقصد أو بدون قصد منهم، يمكن استخدامها في تحقيق الأغراض الإرهابية الخاصة بهم.

كما أن المواقع الموجودة على شبكة الإنترنت قد تستخدمها الجماعات المتطرفة و الإرهابية في تدريب الإرهابيين و المتطرفين، من خلال إرشادات وكتيبات تشرح كيفية صنع الأسلحة الكيماوية والقنابل والمتفجرات، بغرض الإعداد والتدريب للقتال، والتدريب على تنفيذ العمليات الانتحارية[68].

أما فيما يتعلق بعنصري النتيجة وعلاقة السببية فقد أدخل المشرع الاتحادي في عداد الإرهاب كل فعل من الأفعال المحددة في المادتين (29 ، 30) من القانون الاتحادي رقم 7 لسنة 2014م[69]، الذي

(68) محمود صالح العادلي، مرجع سابق، ص108/107.

يتمثل في:"كل فعل أو امتناع عن فعل مجرم بموجب هذا القانون، وكل فعل أو امتناع عن فعل يشكل جناية أو جنحة واردة في أي قانون آخر، إذا ارتكب لغرض إرهابي".

أي أنَّ المشرع تطلب في هذا الفعل أو الامتناع أن يكون بهدف تحقيق نتيجة إرهابية عبّر عنها "بإثارة الرعب بين مجموعة من الناس، أو إزهاق الأرواح، أو التسبب في أذى بدني جسيم، أو إلحاق ضرر ذي شأن بالممتلكات أو البيئة، أو الإخلال بأمن المجتمع الداخلي أو الدولي، أو معاداة الدولة، أو التأثير على السلطات العامة في الدولة، أو دولة أخرى، أو منظمة دولية في أدائها لأعمالها، أو الحصول من الدولة، أو دولة أخرى، أو منظمة دولية على منفعة، أو ميزة من أي نوع"[70].

وأشار أيضًا إلى علاقة السببية التي تربط بين السلوك الإجرامي والنتيجة التي تحققت، عندما نص على تعريف الغرض الإرهابي"بأنه اتجاه إرادة الجاني إلىارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع مجرمًا قانونًا، بقصد إحداث نتيجة إرهابية مباشرة أو غير مباشرة، أو علم الجاني بأن من شأن الفعل أو الامتناع عن الفعل تحقيق نتيجة إرهابية"[71].

وترى الباحثة أن النتيجة الإجرامية في جرائم الإرهاب عمومًا؛ تتمثل في حالة الفزع والترويع المواكبة لإحداث ضرر شديد أو خطر عام يصيب الأموال والأشخاص؛ بهدف تحقيق أغراض سياسية، أو أيدلوجية أو أسباب أخرى، من خلال استهداف الأشخاص والأموال العامة، أو إسقاط عدد كبير من الضحايا. وأن جريمة تمويل الجماعات والمنظمات الإرهابية كإحدى صور جريمة الإرهاب الإلكترونيتعدّمن الجرائم الشكلية التي تتحقق بمجرد وقوع الفعل، دون أن تتطلب وقوع نتيجة جرمية، فتقع بمجرد وضع المال تحت تصرف الجماعات الإرهابية.

---

(69) المادة الأولى من المرسوم بقانون اتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة.

(70) المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(71) المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

الفرع الثالث

الركن المعنوي

يتمثل الركن المعنوي للجريمة بالإرادة الإجرامية، التي تنصرف إلى إرادة النشاط وإرادة النتيجة الإجرامية، فالجاني يريد تحقق النشاط الذي نسب إليه، ويريد تحقيق النتيجة الإرهابية، وهذا العنصر الذي يتمثل في إرادة تحقيق النتيجة هو الذي يفرق بين الجرائم العمدية والجرائم غير العمدية؛ ونظرًا لأن الجرائم الإرهابية جرائم عمدية فإن الركن المعنوي فيها يتخذ صورة القصد الجنائي بعنصريه العلم والإرادة؛ لذا يجب أن تتوفر لدى الجاني نية ارتكاب الجريمة وعزمه على تحقيق نتيجتها، فإذا ثبت أن الفاعل أراد تحقيق النتيجة لكن توقف فعله عند حد الشروع لأسباب خارجة عن إرادته؛ فإنه يسأل في هذه الحالة عن شروع في جريمة إرهابية[72].

وقد تطرق المشرع الاتحادي في قانون العقوبات إلى بيان مكونات الركن المعنوي[73]، حيث نص على أن "يتكون الركن المعنوي للجريمة من العمد أو الخطأ، ويتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرمًا قانونًا بقصد إحداث نتيجة مباشرة، أو أية نتيجة أخرى مجرمة قانونًا يكون الجاني قد توقعها. ويتوافر الخطأ إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواء أكان هذا الخطأ إهمالًا، أم عدم انتباه، أم عدم احتياط، أو طيشًا، أو رعونة، أم عدم مراعاة القوانين، أو اللوائح، أو الأنظمة، أو الأوامر".

ويمكن توضيح الركن المعنوي لجرائم الإرهاب الإلكتروني من خلال الحالة النفسية للجانيالتي تربط بين شخصية الجاني وماديات الجريمة، حيث يقوم الركن المعنوي لجرائم الإرهاب التي ترتكب عبر

---

(72) إبراهيم محمد القاسمي، مرجع سابق، ص33.

(73) المادة (38) من قانون القانون الاتحادي رقم 3 لسنة 1987م، بشأن إصدار قانون العقوبات، نشر في الجريدة الرسمية العدد 182 السنة السابعة، بتاريخ 1987/12/20م.

شبكة الإنترنت على أساس توافر الإرادة لدىمرتكب الجريمة، وتوجيه هذه الإرادة للقيام بفعل غير مشروع نص القانون على تجريمه[74].

ولما كانت جرائم الإرهاب الإلكتروني تعد من جرائم التقنية التي تتطلب التعليم التخصصي، والتعليم من قبل من يمارس هذا النوع من الأنواع الخاصة بوسائل الاتصال،فإنهلا يتصور وقوعها إلا في صورة العمد، أي أن يكون مرتكب الجريمة قد دبر وخطط لارتكابها بهدف الحصول على المعلومات والبيانات، أو لاختراق حاسوب آخر، أو استخدام الشبكة لتحقيق أغراض إرهابية[75].

ومن ثمّ فإن الركن المعنوي في الجريمة يتخذ صورة القصد الجنائي القائم على العلم والإرادة، ويتحقق باتجاه إرادة الجاني إلى ارتكاب الركن المادي للجريمة، مع إحاطة العلم به و بكافة العناصر التي يتطلبها القانون، وفقًا لمبدأ الشرعية الذي يتطلب أن يكون مرتكب الجريمة عالمًا بأن السلوك الذي يأتيه مجرمًا وفقًا لنص القانون، ويجب أن يتوافر العلم بجميع عناصرها حين دخول مرتكب الجريمة إلى النظام المعلوماتي و الشبكة المعلوماتية، وإنشاء و إدارة المواقع التي يسهل القيام بالعمليات الإرهابية من خلالها[76].

أما الإرادة فهي العنصر الثاني من عناصر القصد الجنائي، وهي تعبر عن الموقف النفسي أو الحالة النفسية لدى مرتكب الجريمة، من السلوك الإجرامي الذي يرتكبه والنتيجة التي تترتب عليه، فإذا كانت الجريمة من الجرائم الشكلية التي لا تتطلب لتحققها حدوث نتيجة معينة؛ مثل جريمة تمويل الإرهاب، والدخول غير المشروع للبيانات والمعلومات، واختراق الأجهزة، فإن الإرادة تقتصر فقط على

---

(74)أحمد محمود مصطفى،**جرائم الحاسبات الآلية في التشريع المصري**، دراسة مقارنة، دار النهضة العربية، القاهرة،، ط1، 2010م، ص113.

(75)نبيلة هبه هروال،**الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات**، مرجع سابق، ص50.

(76) أمين مصطفى محمد، قانون العقوبات، القسم العام، مرجع سابق، ص342.

السلوك الإجرامي دون أن تمتد للنتيجة، ووفقًا لهذه الجريمة لا بد أن تتجه إرادة الجاني إلى إحداث الفعل والسلوك الإرهابي دون إكراه[77].

فإذا ما توافرت جميع عناصر الجريمة، واتجهت إرادة الجاني إلى ارتكاب السلوك الإجرامي وإحداث النتيجة التي تترتب عليه،يتوافر القصد الجنائي العام المتمثل في العلم والإرادة، والذي يكفي لقيام المسئولية العمدية؛ إلا أن هناك بعض الجرائم التي تتطلب إضافة للقصد العام، غاية معينة يستهدف الجاني تحقيقها من السلوك الإجرامي الذي ارتكبه، وهو ما يعرف بالقصد الخاص؛ الذي يتطلب البحث فيه بعد توافر القصد الجنائي العام.

وفيما يتعلق بجريمة الإرهاب الإلكتروني فإنه لا يكفي القصد العام لقيام الركن المعنوي بالنسبة لها؛ بل لا بد من توافر القصد الخاص الذي يتمثل في الهدف والغاية من ارتكاب السلوك الإجرامي وهي تحقيق النتيجة الإرهابية، أو أحد الأغراض الإرهابية؛ أي لا بد من توافر النية لدى مرتكب الجريمة وهو يستخدم الشبكة المعلوماتية أنه يهدد أويقوم بأحد الأعمال الإرهابية وفقًا لما ورد في القانون الاتحادي في شأن الجرائم الإرهابية، من ضرورة اتجاه إرادة الجاني إلىارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع مجرمًا قانونًا بقصد إحداث نتيجة إرهابية، وعلم الجاني بأن من شأن هذا الفعل أو الامتناع تحقيق هذه النتيجة[78].

وهو ما تبنته الاتفاقية الدولية لمكافحة تمويل الإرهاب عام 1999م[79]؛ بنصها على"وجوب توافر نية خاصةإضافة إلى القصد الجنائي العام، يتمثل في علم مرتكب الجريمة بعدم مشروعية الفعل

---

(77) خالد سليمان عبدالله الحمادي،**جريمة الدخول غير المشروع إلى النظام المعلوماتى في القانون القطري**، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019م، ص85/84.

(78) المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(79) زياد محمد سلامة جفال، **مكافحة جريمة تمويل الإرهاب في القانون الدولي والإماراتي، دراسة في مدى مواءمة التشريع الإماراتي لأحكام الاتفاقية الدولية لمكافحة تمويل الإرهاب لعام 1999**م، دراسات، علوم الشريعة والقانون، المجلد 46، ع3، الجامعة الأردنية، 2019م، ص190.

الذي يأتيه، وأن تتجه إرادته إلى ارتكاب السلوك وإحداث النتيجة، ثم يأتي القصد الجنائي الخاص الذي يتمثل في علم الجاني واتجاه نيته بأن هذه الأموال سوف يتم استخدامها كليًّا أو جزئيًّا للقيام بالعمليات الإرهابية، ومن ثمَّ يكون قصده دعم وتمويل الجماعات والمنظمات الإرهابية بالأموال التي يعلم أنها ستستخدمها في تحقيق أغراض وجرائم إرهابية".

المبحث الثاني

أسباب الإرهاب الإلكتروني وسبل مواجهته

تمهيد وتقسيم:

أصبح الاعتماد على الوسائل الحديثة لتقنية المعلومات والاتصالات يزداد يومًا بعد يوم، سواء في المرافق العامة والمؤسسات المالية والتعليمية والأمنية وغير ذلك...، وإذا كان لهذه الوسائل كثير من الفوائد، إلا أنها قد تستخدم استخداماتضارة تمثل تهديدًا للمجتمع؛ كالإرهاب الإلكتروني.

انطلاقًا من ذلك وبغية التعرف على أسباب الإرهاب الإلكتروني وسبل مواجهته؛ خصصت الباحثة المطلبين التاليين:

المطلب الأول- أسباب الإرهاب الإلكتروني.

المطلب الثاني-أساليب مواجهة الإرهاب الإلكتروني.

المطلب الأول

أسباب الإرهاب الإلكتروني

لا يكفي التنديد بالإرهاب الإلكتروني دون بحث أسبابه ودوافعه المتعددة، فهناك العديد من الأسباب والدوافع لارتكاب الجرائم الإرهابية بوجه عام، والإرهاب الإلكتروني بوجه خاص، إلا أنه

يصعب حصرها على وجه الدقة،ولتحديد الدوافع والأسباب الكامنة وراء تصاعد العمليات الإرهابية الإلكترونية، وللوقوف على أسباب الإرهاب الإلكتروني يمكن تصنيف هذه الأسباب إلى أسباب اقتصادية، وأسباب سياسية، وأسباب تكنولوجية، وأسباب شخصية وفكرية، وأسباب اجتماعية؛ على النحو التالي:

أولًا- الأسباب السياسية:

لا شك في أن هناك دوافع سياسية تقف وراء الأعمال الإرهابية، خاصة في الحالات التي تعجز فيها بعض الجهات أو الأفراد عن تحقيق مكاسب بالطرق السلمية.

حيث تلجأ إلى الأعمال الإرهابية كوسيلة عنيفة لنشر مظلمة، أو التعبير عن قضية، أو الاحتجاج على سياسية معينة؛ كاعتماد الدولة واستخدامها للأساليب القهرية في التعامل مع المواطنين، وغياب الحوار الوطني حول القضايا المصيرية والرئيسة، وعجز الحكومات وفشلها في تلبية الحقوق والمصالح الأساسية للمواطنين؛ كالسكن والعمل، وعدم المساواة في توزيع الثروة الوطنية، وغياب العدالة الاجتماعية، و التفاوت في توزيع الخدمات والمرافق العامة.

فضلًا عن معاناة بعض الشعوب والمجتمعات من الظلم والاضطهاد، والسيطرة الاستعمارية، وخرق القوانين والمواثيق الدولية، وسلب الأموال، مما يدفع الشعوب إلى التطرف والتشدد بقصد إحداث الفوضى والإضرار بصالح الدولة.

كما أن ضعف النظام السياسي الدولي في الرد على الانتهاكات التي تتعرض لها المواثيق الدولية، والتناقض بين ما تحث عليه المواثيق والمعاهدات الدولية من قيم إنسانية ومبادئ، مع ما تتبعه الدولة من ممارسات؛ أدى إلى انتشار العمليات الإرهابية، ولجوء بعض الجماعات والمنظمات إلى تنفيذ عمليات إرهابية ضد بعض الدول[80].

(80) سلطان عناد إبراهيم العدينات، **الآلية الدولية لمكافحة الإرهاب**، رسالة ماجستير، مرجع سابق، ص29/27.

إضافة لما تقدم هناك العديد من الأسباب والدوافع السياسية التي تنتج الإرهاب كضعف الأحزاب السياسية وعدم قيامها بدور فاعل في المساهمة في حل المشاكل المختلفة التي تواجهها الدولة، وعدم قيامها بتقديم تصورات واقتراحات لحل المشكلات التي تواجه المجتمع، والذي يعد من أهم الأسباب والدوافع الداخلية للإرهاب(81).

بالإضافة للإعلان عن القضايا السياسية على المستوى العالمي في إطار وسائل الإعلام واستعطاف المؤيدين من بعض القوى الدولية، وإحداث الضغوط على النظام السياسي في دولة معينة للتراجع عن بعض القرارات التي ستقدم على اتخاذها، أو لتعديل سلوك معين تقوم به.

واستنادًا إلى ما تقدم يمكن القول بأن الأسباب السياسية لها دور مهم في ظهور وانتشار العمليات الإرهابية عبر وسائل التقنيات الحديثة، سواء كانت هذه الأسباب خارجية؛ كالتسلط، و الهيمنة و الاستعمار و استغلال الشعوب، أو كانت أسبابًا داخلية؛ كالمحاكمات غير العادلة، وكبت الحريات، وغياب الديمقراطية التي تؤدي بدورها إلى التعبير والاحتجاج على الأوضاع السياسية غير المقبولة(82).

ثانيًا– الأسباب الاجتماعية:

الجرائم الإرهابية –كغيرها من الجرائم– وليدة عوامل اجتماعية تؤثر تأثيرًا سلبيًّا على المجتمع، فهناك العديد من العوامل والأسباب الاجتماعية تدفع لارتكاب الجرائم الإرهابية، وتؤثر على أفراد المجتمع، كاقتصار العديد من المؤسسات التعليمية على تقديم خدمات لطبقة معينة دون غيرها، وانخفاض مستوى التعليم، وعدم التوعية والرقابة على الكتب المعروضة على أفراد المجتمع، وعدم الاهتمام بالبنية التحتية، وانعدام الخدمات الصحية وغيرها؛ كالطاقة الكهربائية، والمياه، وانخفاض مستوى الدخل، وقلة الاهتمام بالجوانب الاجتماعية، فضلًاعن العنصرية في المجتمعات، فهذه العوامل تولد الإحساس

(81) على لونيسي،**آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الإنفرادية**، مرجع سابق،ص64/66.

(82) مها محمد أحمد عنانزه، مرجع سابق،ص16.

والشعور بالظلم، وتجعل الشخص ضعيفًا وفريسة للجماعات والمنظمات الإرهابية، فالأشخاص الذين يفقدون الأمل ويشعرون بعدم القدرة على تلبية احتياجاتهم المادية والمالية، يتولد لديهم إحساس بالكراهية والرغبة في الانتقام من خلال القيام بالأعمال الإرهابية[83].

وتجدر الإشارة إلى أن الدوافع الاجتماعية للإرهاب قد تعود بصفة عامة إلى التفكك الأسري فالمشكلات الاجتماعية والنفسية تؤدي إلى الخلل والاضطراب في جو الأسرة، والعجز عن إقامة علاقات اجتماعية سويه كالعلاقات العاطفية وعلاقات الصداقة.

كما أن افتقاد الشخص لأهمية دوره في مجال الأسرة والمجتمع وشعوره بالفشل في الحياة الأسرية، يؤدي إلىعدم الشعور بالولاء والانتماء للوطن،كدافع من الدوافع الشخصية لارتكاب العديد من الجرائم والعمليات الإرهابية[84]

إضافة إلى تدهور الظروف والأحوال المعيشية لدى أفراد المجتمع، وانتشار الجهل، فضلاً عن الشعور بالملل والفراغ من أهم الأسباب والدوافع التي تؤدي ارتكاب الجرائم، والانضمام إلى الجماعات والمنظمات الإرهابية، ففي ظل الظروف القاسية من بطالة وفقر....

حيث يصبح الفراغ والملل سببًا في انحراف العديد من الشباب وانضمامهم إلى الجماعات المتطرفة، فالشاب الذي لا يستغل أوقات فراغه ويستثمرها في إشباع حاجاته، مهددٌ بالانحراف والانخراط في الجماعات التي يشعر بأنها تعمل على تحقيق ذاته[85].

ثالثًا- الأسباب النفسية:

---

(83) سلطان عناد إبراهيم العدينات، مرجع سابق، ص35.

(84) مها محمد أحمد عنانزه،**وعي طلبة جامعة اليرموك بمخاطر الإرهاب الإلكتروني ودور التربية الوطنية والإسلامية والقانونية في التصدي لها**، مرجع سابق،ص16.

(85) على لونيسي،**آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الانفرادية**، مرجع سابق،ص68/67.

يرجع ارتكاب العديد من الجرائم الإرهابية والانضمام إلى الجماعات والمنظمات الإرهابية إلى دوافع شخصية، فهناك العديد من الأسباب والدوافع الشخصية التي تؤدي إلى انتشار الإرهاب بوجه عام، والإرهاب الإلكتروني بوجه خاص، كالرغبة في الشهرة والظهور، بحيث لا يكون الشخص مؤهلًا فيلجأ إلى البحث عما يؤهله بطريقة خاطئة، فيلجأ إلى التخريب والعدوان.

وقد ترجع بعض الجرائم الإرهابية إلى تحقيق أهداف معينة؛ كابتزاز الأموال من خلال بعض الشركات، كشركات الطيران، أو قد تستند إلى دوافع شخصية في شخص مرتكب الجريمة؛ كإصابته بمرض نفسي أو خلل عقلي يوجهه لارتكاب العديد من الجرائم الإرهابية(86).

فضلًا عن أن العديد من الجماعات الإرهابية قد تستهدف ذوي المستويات التعليمية المختلفة من خلال المواقع الإلكترونية للتأثير على حالتهم النفسية، والتحريض على الكراهية وحرب الأفكار، ونشر الصور والمقاطع الصوتية أو مقاطع الفيديو، وإظهار الانتحاريين بصورة الأبطال في عيون الشباب؛ لاستقطابهم و التأثير عليهم، أو القيام بحرب نفسية تستهدف السيطرة على الرأي العام، وتحقيق الأهداف الرئيسة لها في نشر الفوضى، والترويع، وتخريب المجتمعات(87).

رابعًا- الأسباب الاقتصادية:

تعدُّ الأسباب الاقتصادية القاسم المشترك بين كافة الجرائم، حيث يساهم الفقر وارتفاع الأسعار، وانتشار البطالة و انهيار العملة، في العجز عن تلبية العديد من الحاجات الضرورية للأفراد-مقابل وجود طبقة ثرية تمتلك الأموال الطائلة وتتمتع بالامتيازات سواء في إطار المشروعية أو غير ذلك، فينعكس الشعور بالظلم واليأس والاحباط على الأفراد بالعزلة، والشعور بالحقد والاندفاع إلى الانتقام من

(86) شريف عبدالحميد حسن رمضان،مرجع سابق، ص1150.

(87) مها محمد أحمد عنانزه،مرجع سابق،ص16.

خلال الجرائم الإرهابية[88].

كما أن تكريس الوضع الدولي القائم على عملية التفاوت بين عالم الجنوب وعالم الشمال، وإغراق البلدان الفقيرة بالمشاكل الاقتصادية للسيطرة عليها وضمان تبعيتها، وعدم التوازن في العلاقات الاقتصادية الدولية، واتباع سياسة العقوبات الاقتصادية التي تفرضها الدول الكبرى على الدول الفقيرة، وسياسات الحصار والحرمان والافقار تعدُّ من أهم الأسباب والدوافع للقيام بالأعمال الإرهابية[89].

واستنادًا لما تقدم يكون الدافع لارتكاب جرائم الإرهاب الالكتروني الإضرار باقتصاديات ومصالح دول معينة، من خلال تدمير منشآتها التجارية والصناعية، أو مهاجمة المنشآت السياحية التابعة لها، أو مكاتب وشركات الطيران؛ باستخدام وسائل التقنية الحديثة، واختراق شبكات هذه المؤسسات وإلحاق الضرر بها، إضافة إلى إثارة الرعب بين المتعاملين[90].

خامسًا- الأسباب التكنولوجية والإعلامية:

إن عولمة منظومة الحقوق واعتبار المجال المعلوماتي حقًّا من الحقوق المكرسة طبقًا للقوانين والاتفاقيات العالمية، واعتبار أي تعطيل للوصول إلى الشبكة المعلوماتية يشكل جريمة التعدي على الحريات العامة، أدى إلى انتشار العديد من الجرائم التي ترتكب عبر المواقع الإلكترونية.

كما أن السرية التي يتضمنها الإنترنت تمكن أي شخص من الحصول على المعلومة عن طريق ظهوره كل مرة بشكل مختلف دون التعريف عن نفسه، حيث يمكنه أن يخفي جميع المعلومات المتعلقة به من وضعه العائلي، وسنه، وغير ذلك من الأمور الخاصة به، فيتمكن من التجربة والاكتشاف بشكل سري عبر الإنترنت.

و يعدُّ من أسباب انتشار ظاهرة الإرهاب الإلكتروني ضعف البنية الخاصة بالشبكات المعلوماتية

---

(88) على لونيسي،مرجع سابق،ص70/69.

(89) سلطان عناد إبراهيم العدينات، **مرجع سابق** ص30/29.

(90) شريف عبدالحميد حسن رمضان،مرجع سابق، ص1146.

ووسائل التكنولوجيا الحديثة، وقابليتها للاختراق؛ مما يمكن المنظمات الإرهابية من التسلل إليها والعمل على تخريبها؛ نتيجة لاتسام هذه الشبكات الخاصة بالبيانات والمعلومات بالانفتاح، وغياب الحواجز والقيود الأمنية لاحتوائها على كثير من الثغرات المعلوماتية بغرض التوسع وتسهيل الدخول، فضلًا عن قلة التكلفة، وسهولة الاستخدام، وسهولة إنشاء مواقع وبرامج للتجسس، فضلًا عن صعوبة اكتشاف الجرائم الإلكترونية وإثباتها بشكل عام[91].

وتجدر الإشارة إلى الدور السلبي للشبكة المعلوماتية في تجنيد الشباب، مما أكسب الإرهاب أهمية كبيرة في العصر الحاضر، من خلال استخدام وسائل التكنولوجيا الحديثة في نقل الأخبار، وسرعة انتشار العمليات الإرهابية؛ لصعوبة اكتشافها وإثباتها، وغياب الهوية الرقمية.

مما مكَّن الجماعات الإرهابية من شنِّ العديد من الهجمات الإلكترونية بشخصيات وهمية، إذ لا يلزم للقيام بالهجمات الإلكترونية سوى توافر حاسب آلي متطور وشبكة معلوماتية متطورة، كما أن غياب الآليات القانونية المختصة بالرقابة على شبكات الاتصالات والمعلومات أدى بدوره إلى انتشار الإرهاب الإلكتروني[92].

وقد استغلت الجماعات الإرهابية الوسائل الإعلامية في نشر ونقل الأخبار كوسيلة لتسويق جرائمها، ونشر الرعب والفزع بين أفراد المجتمع، لتحقيق أغراضها الإرهابية، فقد استغل تنظيم داعش وسائل الدعاية والإعلام، ووسائل التكنولوجيا الحديثة للمعلومات والاتصالات في تجنيد الشباب بهدف القيام بالعمليات الإرهابية، ونشر مقاطع الفيديو التي ترغّب وتحث على الانضمام إليه؛ الأمر الذي انعكس على زيادة الأعمال الإرهابية من خلال استخدام شبكة الإنترنت في تجنيدهم وتدريبهم على

(91) مها محمد أحمد عنانزه، مرجع سابق،ص17.

(92) سلطان عناد إبراهيم العدينات، مرجع سابق، ص33.

استخدام المتفجرات والأسلحة[93].

سادسًا- الأسباب الفكرية والدينية:

إن الفهم الخاطئ للدين، والجهل بمقاصد الشريعة الإسلامية، وتفسير النصوص تفسيرًا خاطئًا،من أهم العوامل التي ساعدت على انحراف الشباب، وحدوث الانقسامات الدينية والفكرية بين التيارات المختلفة، فتلقي الخطاب الديني من غير المتخصصين، والفهم الخاطئ للأمور، والتعصب الديني والمذهبي والطائفي، أدى إلى انتشار الإرهاب، وكان دافعًا لانتشار ظاهرة الإرهاب الإلكتروني[94]. ناهيك عن أن للتطرف والإرهاب روافد خارجية توفير الدعم المالي لهلتحقيق أغراض سياسية، والنيل من أمن البلدان واستقرارها السياسي،ومن ثمَّ فلا رابط بين الإسلام والإرهاب؛ لأن الإرهاب ظاهرة عالمية منتشرة في كافة بلدان العالم، ليس لها دين أو مذهب[95].

وترى الباحثة أن المنظمات الإرهابية قد استغلت المميزات العديدة للشبكة العنكبوتية في تجنيد الشباب ونشر أفكارها؛ من خلال التخفي والسرية وسهولة الاتصال والاستخدام، فالإرهابي لا يخاطر بنفسه؛ بل يجند عددًا كبيرًا من الشباب باستخدام وسائل التقنية الحديثة، ومواقع التواصل الاجتماعي، ويدربهم على صنع القنابل والمتفجرات، وكيفية الهروب من الأجهزة الأمنية، وأساليب الدعاية الإعلامية للإرهاب عبر شبكة المعلومات،إضافة إلى استخدام الجماعات والمنظمات الإرهابية مواقع التواصل الاجتماعي للحصول على المعلومات عن الأماكن المستهدفة، حيث تساعد شبكة الإنترنت على تحقيق الترابط التنظيمي بين الجماعات الإرهابية وبين الخلايا التي تزودها بالبيانات والمعلومات الأفكار بمنتهى السرية؛ الأمر الذي يحول دون اكتشافها وملاحقتها.

---

(93) على لونيسي، مرجع سابق،ص70/69. سلطان عناد إبراهيم العدينات، مرجع سابق، ص33.

(94) شريف عبدالحميد حسن رمضان، **مرجع** سابق، ص1147.

(95) على لونيسي، مرجع سابق،ص73/70.

المطلب الثاني

أساليب مواجهة الإرهاب الإلكتروني

تمهيد وتقسيم:

أضحت جرائم الإرهاب الإلكتروني تمثل تهديدًا مباشرًا للاستقرار والسلام في العالم، فضلًا عن كونها عائقًا للتنمية والتقدم في المجتمع،فتنامي ظاهرة الإرهاب الإلكتروني، وعدم اقتصار آثارها وأضرارها على بعض الجماعات والأفراد، باتت تهدد دول العالم أجمع، الأمر الذي يؤكد على ضرورة التنسيق والتعاون الدوليين بشأن مكافحة هذه الجرائم بصفة عامة، وجريمة الإرهاب الإلكتروني بصفة خاصة.

استنادًا إلى ذلك، وسعيًا للوقوف على أساليب مواجهة هذه الجرائم لا بد من البحث في المواجهة التقنية لجرائم الإرهاب الإلكتروني، ثم بيان دور المشرع الإماراتي والتعاون الدولي في مواجهة هذه الجرائم،من خلال الفروع الثلاثة التالية:

الفرع الأول

المواجهة التقنية لجرائم الإرهاب الإلكتروني

يمكن الوقوف على المواجهة التقنية لجرائم الإرهاب الإلكتروني من خلال البحث في المواجهة التي ترتكز على التقنية الرقمية، وتساهم في رسم السياسة الوقائية للحد من هذه الجرائم، التي لا بد من تدعيمها بإنشاء شبكة طوارئ، بغرض تقديم المساعدة الفورية والتدخل السريع والفعال في جمع الأدلة الإلكترونية، واتخاذ الإجراءات اللازمة للمواجهة.

حيث تتم المواجهة التقنية في المرحلتين الوقائية والعلاجية؛ فالمواجهة في المرحلة الوقائية تتمثل في تكريس الجهود والأدوات الخاصة بالأمن والحماية من خلال مجموعة برامج يتم تحميلها وتثبيتها على

الحاسبات، حتى تكون النظم المعلوماتية آمنة من الاختراقات والمخاطر التي تتعلق بالأنشطة الإجرامية.

وهذه البرامج تنقسم إلى مجموعات تظهر من خلال برامج تشفير المعلومات، والبرامج النارية أو جدران النار، وبرامج مضادات الفيروسات أو الحماية من الفيروسات.

كما يمكن تقسيمها من حيث القدرة والإمكانات إلى برامج أمنية خاصة بحماية أمن الشبكات تستهدف البنوك والشركات وقطاعات الأعمال ومقاهي الإنترنت، وبرامج عادية تستهدف الشركات الصغيرة والمستخدم العادي[96].

كما تتمثل السياسة الوقائية أيضًا في حماية تكامل وخصوصية الأنظمة من خلال تأمين شبكة النظام الخارجية والداخلية، التي تطبق من خلال تقسيم الحزم المارة في شبكة النظام الخارجية والداخلية إلى مجموعات طبقية من الحزم، وحمايتها من الاختراقات والهجوم من قبل المخترقين باستخدام وسائل وأجهزة حماية للشبكات؛ مثل تشفير المعلومات والبيانات التي ترسلها وتستقبلها أنظمة المعلومات عن طريق شبكتها الداخلية والخارجية، كما تتمثل في تأمين الحاسبات الرئيسية من خلال ما يلي[97]:

- استخدام وسائل وأساليب الذكاء الاصطناعي للقيام في استخدام موارد النظام بما لها من قدرة على الاحتفاظ بالتأمينات السابقة للنظام، وتحديد السياسات الخاصة بالدخول.
- تصنيف وتحديد المعلومات والبيانات التي تتيحها التطبيقات الخاصة بالنظام للمستخدمين له، سواء كانوا من خارج المؤسسة أو داخلها، وأيضًا وضع الإجراءات التأمينية لها.
- مراجعة جميع الخدمات الخاصة بالشبكات التي تقدمها نظم التشغيل المختلفة للمستخدمين؛ لمنع استغلال مخترقي أنظمة المعلومات من الدخول بدون ترك أي أثر لهم.

---

(96) محمد صلاح محمد عبدالمنعم، **مرجع سابق**، ص118/117.

(97) المرجع السابق، ص117. سليمان أحمد فضل، مرجع سابق،ص388/387.

- وضع العديد من الإجراءات الصارمة على خروج الأجهزة الخاصة بالحاسبات الآلية عن المواقع الخاصة بها بأنظمة المعلومات.
- المراجعة الدورية والمستمرة للنظام الخاص بالبريد الإلكتروني في المؤسسة وفصلها عن القواعد الخاصة بالبيانات الموجودة بالمؤسسة، وإجراء النسخ الاحتياطي لنظام المعلومات بصفة منتظمة ودورية.

أما المواجهة العلاجية فتلعب دورًا مزدوجًا في مواجهة جرائم الإرهاب الإلكتروني، حيث تتتبَّع الوسائل التي يستخدمها القراصنة في الاختراق والحصول على المعلومات من شبكة الإنترنت، فهناك العديد من الأساليب التي يمكن من خلالها التخلص من الفيروسات التي قد تخترق الأجهزة، ومن ناحية أخرى تقوم بتتبع القراصنة من خلال الوسائل التي قاموا باستخدامها عبر برامج الجدران النارية، التي تتتبع محاولات الاختراق التي تتعرض لها النظم المعلوماتية، كما يوفر جدار النار معلومات عن المكان القائم بالقرصنة، ومعرفة العنوان الخاص بمزود الإنترنت الذي بدأت عنده محاولات القرصنة[98]. ويمكن تلخيص المواجهة العلاجية والإجراءات التي يجب اتخاذها في حالة اختراق نظام المعلومات في الخطوات التالية[99]:

- القدرة على تحديد الثغرات الموجودة في النظم الخاصة بالحماية الموضوعة لتأمين نظام المعلومات والبيانات، التي يمكن من خلالها اختراق النظام.
- إعادة تحميل المعلومات والبيانات وخدمات النظام من الملفات التأمينية للنظام الذي يحتفظ بها.
- مراجعة ملفات الدخول للنظام المعلوماتي حتى يمكن تحديد اسم الدخول وكلمة السر المستخدمة لاختراق النظام، وتحديد وقت وأسلوب إتمام الاختراق، وهناك العديد من سياسات الفحص الواجب

(98) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص121/120.
(99)سليمان أحمد فضل، مرجع سابق،ص389.

القيام بها، تتمثل في عملية إدارة الدخول الخاص بالنظام، ودخول مستخدمي النظام، والأهداف الخاصة بالنظام والعمليات التي يقوم بها، وحقوق مستخدمي النظام،إضافة إلى التغيير الذي يتم في السياسات الخاصة بالنظام، وتتبع العمليات التشغيلية التي يقوم بها.

الفرع الثاني

مواجهة جرائم الإرهاب الإلكتروني على المستوى الوطني والدولي

إن الحديث عن مواجهة جرائم الإرهاب الإلكتروني على المستوى الوطني والدوليتطلب البحث في مواجهة هذا النوع من الجرائم على المستوى الوطني، ثم مواجهته على المستوى الدولي من خلال الاتفاقيات والمعاهدات الدولية وفق التالي:

أولًا- مواجهة جرائم الإرهاب الإلكتروني على المستوى الوطني:

يمكن الوقوف على مواجهة جرائم الإرهاب الإلكتروني على المستوى الوطني في دولة الإمارات، من خلال القوانين والنصوص التشريعية التي وضعها المشرع للمعاقبة على الجرائم الإرهابية بوجه عام، والإرهاب الإلكتروني وجرائم تقنية المعلومات بوجه خاص، ثم التطرق لمكافحة المشرع الاتحادي للخطورة الإرهابية على النحو التالي:

أ- مواجهة جرائم الإرهاب الإلكتروني والجرائم الإرهابية من خلال النصوص التشريعية:

لا يوجد خلاف بالنسبة للجرائم التي تقع على المكونات المادية للأجهزة التقنية، حيثت يطبق عليها النصوص العامة لقانون العقوبات في الإتلاف والسرقة وغيرها من الجرائم الخاصة بالأموال، أما فيما يتعلق بالجرائم التي تقع على المكونات غير المادية فلا بد من مواجهتها بنصوص خاصة تتوافق مع طبيعتها، وقد عالج المشرع الاتحادي الجرائم الإرهابية في العديد من النصوص التشريعية، ووضع لها العديد من العقوبات على النحو التالي:

- **النصوص التشريعية الخاصة بمواجهة الجرائم الإرهابية بوجه عام:**

تناول المشرع الاتحادي في القانون رقم 7 لسنة 2014 بشأن مكافحة الجرائم الإرهابية تجريم الأعمال الإرهابية، ووضع لها العديد من العقوبات، حيث نصت المادة الثامنة من القانون أعلاه على أن "يعاقب بالإعدام أو السجن المؤبد لكل من استخدم مرفقًا نوويًّا أو كيميائيًّا أو بيولوجيًّا أو أحدث أضررًا به بطريقة من شأنها إطلاق الإشعاع، أو النشاط الإشعاعي، أو السموم أو المواد الكيميائية السامة، أو الكائنات أو الوسائط البيولوجية المرضية، وكان ذلك لغرض إرهابي".

كما نصت المادة (12) من القانون ذاته على أن"ويعاقب بالسجن المؤبد أو المؤقت كل من حاول أو شرع في الاعتداء على سلامة أو حرية شخص مشمول بالحماية الدولية لغرض إرهابي، وتكون العقوبة السجن المؤبد إذا وقعت الجريمة، ويعاقب بالسجن المؤبد أو المؤقت كل من اعتدى بالقوة لغرض إرهابي على المقر الرئيسي، أو محل إقامة، أو وسيلة مواصلات شخص مشمول بالحمايةالدولية".

و"يعاقب بالسجن المؤبد أو المؤقت كل من أعلن بإحدى طرق العلانية عداءهللدولة، أو لنظام الحكم فيها، أو عدم ولائه لقياداتها".

ونصت المادة (31) من القانون سالف البيان بصدد التعاون مع التنظيمات أوالجماعات الإرهابية على أن على أن:

"1- يعاقب بالسجن المؤبد أو المؤقت الذي لا تقل مدتة عن خمس سنوات كل من تعاون مع تنظيم إرهابي مع علمه بحقيقته أو بغرضه.

2- يعاقب بالسجن المؤبد أو المؤقت الذي لا تقل مدته عن خمس سنوات كل من أعان شخص إرهابي على تحقيق غرضه مع علمه بحقيقته أو بغرضه.

3- تكون العقوبة الإعدام أو السجن المؤبد إذا كان الفاعل في البندين السابقين من أفراد القوات المسلحة، أو الشرطة، أو الأمن، أو سبق له تلقي تدريبات عسكرية أو أمنية".

- **النصوص الواردة بشأن مواجهة جرائم تمويل الإرهاب بوجة عام باعتبارها إحدى صور الإرهاب الإلكتروني**

يلاحظ أن المشرع الاتحادي نص على الأفعال التي تتعلق بتمويل الإرهاب، ووضع تعريفًا شاملًا لها في القانون رقم 7 لسنة 2014م بشأن مكافحة الجرائم الإرهابية، والمرسوم بقانون رقم 20 لسنة 2018م الخاص بمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، وفق ما أشارت إليه الباحثة سابقًا لدراسة الركن المادي لجريمة الإرهاب الإلكتروني. حيث نص المشرع الاتحادي على عدد من العقوبات لمكافحة هذه الجرائم سواء تم ارتكابها بصفة مستقلة، أو بصفة مرتبطة مع جريمة غسل الأموال، حيث تنص المادة المادة (30) من القانون رقم 7 لسنة 2014م بشأن مكافحة الجرائم الإرهابية على أن: "يعاقب بالسجن المؤبد أو المؤقت الذي لا تقل مدته عن عشر سنوات كل من كان عالمًا بأن الأموال كلها أو بعضها متحصلة من جريمة إرهابية، أو مملوكة لتنظيم إرهابي، أو كانت غير مشروعة ومملوكة لشخص إرهابي، أو معدة لتمويل تنظيم إرهابي أو شخص إرهابي، أو جريمة إرهابية، وارتكب أحد الأفعال الآتية: 1- حوَّل، أو نقل، أو أودع، أو استبدل الأموال بقصد إخفاء، أو تمويه حقيقتها أو مصدرها، أو غرضها غير المشروع.2- أخفى أو موَّه حقيقة الأموال غير المشروعة، أو مصدرها، أو مكانها، أو طريقة التصرف فيها، أو حركتها، أو ملكيتها، أو الحقوق المتعلقة بها.3- اكتسب الأموال، أو حازها، أو استخدمها، أو أدارها، أو حفظها، أو استثمرها، أو بدَّلها، أو تعامل فيها بقصد إخفاء أو تمويه حقيقتها، أو مصدرها، أو غرضها غير المشروع".

كما نص المشرع على عقوبة المصادرة كعقوبة تكميلية لعقوبة تمويل الإرهاب، حيث أوجب على المحكمة المختصة مصادرة الأموال محل الجريمة أو أي أموال يملكها الجاني تعادل قيمة الأموال أو المتحصلات من الجريمة في حال ثبوت الجريمة، حيث تنص المادة (26) من المرسوم بقانون

اتحادي رقم 20 لسنة 2018 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب على أن: "تحكم المحكمة في حال ثبوت ارتكاب الجريمة بمصادرة ما يلي:

1- الأموال محل الجريمة، والمتحصلات والوسائط المستخدمة، أو التي كان يراد استخدامها فيها. 2- أي أموال يملكها الجاني تعادل قيمة الأموال والمتحصلات المنصوص عليها في الفقرة (أ) من هذا البند في حال تعذر ضبطها.3- تتم المصادرة بصرف النظر عما إذا كانت تلك الأموال أو المتحصلات في حيازة أو ملكية الجاني أو طرف آخر، دون الإخلال بحقوق الغير حسنالنية.4-لا تحول وفاة المتهم، أوكونه مجهولًا في جريمة معاقب عليها بموجب أحكام هذا المرسوم بقانون دون أن يكون للنيابة العامة رفع الأوراق للمحكمة المختصة؛ لإصدار حكمها بمصادرة الأموال، والمتحصلات، والوسائط المضبوطة إذا أثبتت صلتها بالجريمة".

فضلا عن ذلك تشدد المشرع بشأن ارتكاب الجرائم الإرهابية في نص المادة (39) من قانون مكافحة الجرائم الإرهابية سالف البيان التي ورد نصها وفق الآتي: "فيما لم يرد به نص في هذا القانون، وهو القانون الخاص بمكافحة الجرائم الإرهابية، تعتبر الجنح والجنايات المنصوص عليها في قانون العقوبات أو أي قانون آخر جرائم إرهابية إذا ارتكبت لغرض إرهابي؛ وتوقع العقوبة على النحو التالي:

1- إذا كانت العقوبة المقررة أصلًا للجريمة هي الحبس جاز مضاعفة حدها الأقصى.

2- إذا كانت العقوبة المقررة أصلًا للجريمة هي السجن المؤقت الذي يقل حده الأقصى عن خمس عشرة سنة جاز الوصول بالعقوبة إلى هذا الحد.

3- إذا كانت العقوبة المقررة أصلًا للجريمة هي السجن المؤقت الذي يصل حده الأقصى جاز الوصول بالعقوبة إلى السجن مدة عشرين سنة، أو يستبدل بها السجن المؤبد.

4- إذا كانت العقوبة المقررة أصلًا للجريمة جاز الحكم بالإعدام".

وترى الباحثة أن النصوص التقليدية للجرائم الإرهابية التي كانت سائدة قبل انتشار شبكة الإنترنت لم تعد قادرة على مواكبة التطورات الهائلة في مجال تكنولوجيا المعلومات، حيث أصبحت الجريمة أكثر صعوبةً وتعقيدًا في ظل هيمنة التكنولوجيا الحديثة، كما أصبحت القوانين غير كافيه لمواجهه جرائم الإرهاب الالكتروني التي يتم ارتكابها من خلال وسائل تكنولوجيا الاتصالات والمعلومات.

- **النصوص التشريعية الواردة بشأن مواجهة جرائم تقنية المعلومات،التي نص المشرع فيها على العديد من صور الإرهاب الذي يتم عبر وسائل تقنية المعلومات:**

تفيد نصوص قانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012م المعدل بالقانون رقم 2 لسنة 2018م بأن المشرع جرَّم العديد من الصور باعتبارها جرائم إرهاب إلكترونية مرتكبة عبر شبكة المعلومات أوبوسائل تقنية المعلومات، كما نص على العقوبات المقررة لها ومواجهتها، حيث "عاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم، ولا تجاوز مليون درهم كل منأنشأ أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات للترويج أو التحبيذ لأي برامج أو أفكار من شأنها إثارة الفتنة والكراهية، أو العنصرية أو الطائفية، أو الإضرار بالوحدة الوطنية، أو السلم الاجتماعي، أو الإخلال بالنظام العام أو الآداب العامة"(100).

"ويعاقب أيضًا بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل منأنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف

(100) المادة (24) من القانون الاتحادي رقم 5 لسنة 2012م، بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

عليه، أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار أو الترويج للأسلحة النارية، أو الذخائر أو المتفجرات، في غير الأحوال المصرح بها قانونًا"[101].

ونص أيضًا على أن "يعاقب بالسجن مدة لا تقل عن عشر سنوات ولا تزيد عن خمس وعشرين سنة والغرامة التي لا تقل عن مليوني درهم ولا تجاوز أربعة ملايين درهم، كل من أنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات، وذلك لجماعة إرهابية 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 الأجهزة الحارقة أو المتفجرات، أو أدوات أخرى تستخدم في الأعمال الإرهابية"[102].

إضافة إلى ما تقدم نص المشرع على "عقوبة الحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم لمن حمل محتوى أيٍّ من المواقع المذكورة في المادة 26، أو أعاد بثها أو نشرها بأي وسيلة كانت، أو تقرر دخوله إليها لمشاهدتها، أو نشر أي محتوى يتضمن التحريض على الكراهية، وللمحكمة في حالة العود بدلًا من الحكم بالعقوبة المشار إليها في الفقرة السابقة أن تحكم بإيداع المتهم إحدى دور المناصحة أو الحكم بوضعه تحت المراقبة الإلكترونية، ومنعه من استخدام أيًّا من وسائل تقنية المعلومات خلال فترة تقدرها المحكمة على ألا تتجاوز الحد الأقصى للعقوبة المقررة "[103].

---

(101) المادة (25) من القانون الاتحادي رقم 5 لسنة 2012م، بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(102) المادة (26) من القانون الاتحادي رقم 5 لسنة 2012م، بشأن مكافحة جرائم تقنية المعلومات، والتي استبدلت بموجب المادة الأولى من المرسوم بقانون اتحادي رقم 2 بتاريخ 24/7/ 2018م.

(103) المادة (26) من القانون الاتحادي رقم 5 لسنه 2012م، بشأن مكافحة جرائم تقنية المعلومات، والتي استبدلت بموجب المادة الأولى من المرسوم بقانون اتحادي رقم 2 بتاريخ 24/7/ 2018م.

ويجدر بالذكر أن المشرع قد "عاقب على الشروع في الجنح المنصوص عليها في القانون رقم (20) لسنة 2018م، والخاص بمكافحة جرائم تقنية المعلومات بنصف العقوبة المقررة للجريمة التامة"[104].

كما نص أيضًا على عقوبة المصادرة للأجهزة والبرامج التي تم ارتكاب هذه الجرائم من خلالها "مع عدم الإخلال بحقوق الغير حسني النية، يحكم في جميع الأحوال بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون، أو الأموال المتحصلة منها، أو محو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم؛ وذلك إما إغلاقًا كليًّا أو للمدة التي تقدرها المحكمة"[105].

وتجدر الإشارة أيضًا إلى أن المشرع جرَّم الدخول غير المشروع للبيانات، والعمل على اختراقها؛ حيث نص على عقوبة جريمة الدخول غير المشروع إلى النظام المعلوماتي في صورتها المجردة بعقوبة الحبس والغرامة؛ نظرًا لاختلاف وتدرج النشاط والفعل المكون للجريمة، حيث نصت المادة (2) من قانون تقنية المعلومات سالف البيان على أن "يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد عن ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح أو بالبقاء فيه بصورة غير مشروعة. وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى

(104) المادة (40) من القانون الاتحادي رقم 5 لسنة 2012م، بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(105)المادة (26) من القانون الاتحادي رقم 5 لسنة 2012م، بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

هاتين العقوبتين، إذا ترتب على هذا البقاء أو الدخول أي نشاط يؤدي إلى إلغاء،أو تدمير، أو حذف، أو إتلاف، أو إفشاء، أو نشر، أو نسخ، أو إعادة نشر أي معلومات أو بيانات.

ب-مواجهة الخطورة الإرهابية:

الفكر المتطرف أسلوب من الأساليب المغلقة في التفكير، يتسم بعدم قابليته وقدرته على تقبل أية آراء أو معتقدات تختلف عن معتقدات الجماعة أو الشخص المتطرف، ويتخذ موقفًا يتسم بالخروج عن حد الاعتدال، وتجاوز المعايير الفكرية، والبعد عن المألوف في القيم الأخلاقية والسلوك الذي يرضاه المجتمع.

وتعدُّ الخطورة الإرهابية نوعًا خاصًّا من أنواع الخطورة الإجرامية، وهي مصطلح حديث لم يتعرض الفقه لتعريفه؛ فهو مشتق من الخطورة الإجرامية، وقد تناول المشرع هذا المصطلح في قانون مكافحة الجرائم الإرهابية، حيث نص على أن: "تتوافر الخطورة الإرهابية في الشخص إذا كان متبنيًّا للفكر المتطرف أو الإرهابي؛ بحيث يخشى من قيامه بارتكاب جريمة إرهابية"[106].

يتضح من النص أعلاه أن المشرع الاتحادي ساوى بين كُلٍّ من الفكر الإرهابي، والفكر المتطرف مع اتساع المصطلح الأول وشموله للمصطلح الثاني، إلا أن المشرع ربط بينهما في أن كلًّا منهما إذا كان متوافرًا في الشخص يخشى من ارتكابه جرائم إرهابية، ويعبر عنه باحتمالية ارتكاب الشخص جرائم إرهابية في المستقبل، فتتوفر في شأنه حالة الخطورة الإرهابية[107].

وترى الباحثة أن المشرع اتبع سياسة عقابية تهدف إلى وقاية المجتمع من خطورة الجرائم الإرهابية بوجه عام ، وذلك بأن أورد نصًا خاصا لمواجهة الخطورة الإرهابية في قانون مكافحة الجرائم الإرهابية

---

(106) المادة (40) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(107) عبدالإله محمد النوايسة، **دور قانون مكافحة الجرائم الإرهابية الإماراتي في مكافحة الخطورة الإجرامية في جرائم الإرهاب**، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، ع1، 2018م، ص384/383.

سالف البيان، حيث نص على أنه: "إذا توافرت في الشخص الخطورة الإرهابية، أودع في أحد مراكز المناصحة بحكم من المحكمة وبناء على طلب من النيابة، ويقدم مركز المناصحة إلى النيابة تقريرًا دوريًّا كلثلاثة أشهر عن الشخص المودع، وعلى النيابة رفع هذه التقارير إلى المحكمة مشفوعة برأيها، وعلى المحكمة أن تأمر بإخلاء سبيل المودع إذا تبين لها أن حالتة تسمح بذلك"[108].

حيث ترى الباحثة أن المناصحة عبارة عن تدبير من التدابير الوقائية التي يخضع لها من تتوافر في شأنه الخطورة الإرهابية.

كما ترى الباحثة أيضا أن المشرع الاتحادي ضمّن المرسوم بقانون رقم 5 لسنة 2012م العديد من مظاهر التشدد لمواجهه جرائم الإرهاب الالكتروني ؛ سواء فيما يتعلق بالعقوبات السالبة للحرية، أو الغرامات المالية، تحقيقًا للردع العام والردع الخاص

ثانيًا- مواجهة جرائم الإرهاب الإلكتروني على الصعيد الدولي:

يقتضي الوقوف على أساليب مواجهة الإرهاب الإلكتروني على المستوى الدولي البحث في الصكوك الإقليمية، والاتفاقيات الثنائية، إضافة إلى الصكوك الدولية التي صادقت عليها دولة الإمارات العربية المتحدة بشأن مكافحة الإرهاب، والتدابير التي اتخذت في هذا الشأن، ثم التطرق للبحث في أساليب المكافحة المنصوص عليها في الاتفاقيات الدولية؛ وفق التفصيل التالي:

أ- الصكوك والاتفاقيات التي صادقت عليها أو انضمت إليها دولة الإمارات العربية المتحدة بشأن مكافحة الإرهاب:

- **الاتفاقيات الثنائية[109]:**

أبرمت دولة الإمارات العربية المتحدة العديد من الاتفاقيات الثنائيةالخاصة بمجالات التعاون

(108) المادة (40) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(109) **دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن**، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، الأمم المتحدة، نيويورك، 2009م، ص68.

القانوني والقضائي، مع العديد من الدول؛ مثل الجمهورية التونسية مرسوم رقم 32 عام 1975م[110]، المملكة الأردنية مرسوم رقم 106 لسنة 1999م [111]، والمملكة المغربية مرسوم رقم 80 لسنة 1978م[112]، وجمهورية الهند مرسوم رقم 33 لسنة 2000م[113]، والجمهورية الجزائرية مرسوم رقم 12 لسنة 1984م[114]، والجمهورية الفرنسية مرسوم رقم 31 لسنة 1992م[115]، وأيضًا الجمهورية الصومالية مرسوم رقم 95 لسنة 1982م[116].

الاتفاقيات الدولية:

انضمت دولة الإمارات العربية المتحدة إلى العديد من الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإرهابية؛ والتي تتمثل فيما يلي[117]:

1- اتفاقية مكافحة الاستيلاء غير المشروع على الطائرات، الموقعة في لاهاي في 16 ديسمبر 1970م والتي تم الانضمام إليها عام 1981م[118].

---

(110) المرسوم الاتحادي رقم 32 لسنه 1975م، بالموافقة على اتفاقيه التعاون القضائي وتنفيذ الأحكام وتسليم المجرمين بين دولة الإمارات العربية المتحدة والجمهورية التونسية.

(111) مرسوم اتحادي رقم 106 لسنه 1999م، بشأن اتفاقيه التعاون القانوني والقضائي بين دولة الإمارات العربية المتحدة والمملكة الأردنية، بتاريخ 1999/11/24.

(112) المرسوم الاتحادي رقم 80 لسنه 1978م، بالموافقة على اتفاقيه التعاون القضائي والإعلانات و الانابات وتسليم المجرمين بين دولة الإمارات العربية المتحدة والمملكة المغربية.

(113) المرسوم الاتحادي رقم 33 لسنه 2000م، بشأن اتفاقيه التعاون القانوني والقضائي في المسائل المدنية والتجارية، واتفاقيه حول المساعدة القانونية المتبادلة في المسائل الجنائية واتفاقيه في شأن تسليم المجرمين بين حكومة دولة الإمارات العربية المتحدة وحكومة جمهوريه الهند.

(114) المرسوم الاتحادي رقم 12 لسنه 1984م، بالموافقه على اتفاقية التعاون القضائي بين دولة الامارات العربية المتحدة والجمهوريه الجزائرية.

(115) المرسوم الاتحاد رقم 31 لسنه 1992م، بالتصديق على اتفاقيه التعاون القضائي والإعتراف بالأحكام وتنفيذها في الشئون المدنيه والتجارية بين حكومة دولة الامارات العربية المتحدة وحكومة الجمهورية الفرنسية.

(116) المرسوم الاتحادي رقم 95 لسنه 1982م، بشأن اتفاقيه التعاون القانوني والقضائي المعقوده بين دولة الإمارات العربية المتحدة وجمهورية الصومال.

(117) **دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن**، مرجع سابق، ص69.

2- الاتفاقية الخاصة بالجرائم وبعض الأفعال الأخرى المرتكبة على متن الطائرات،التي انضمت إليها الإمارات عام 1981م[119].

3- اتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني، الموقعة في مونتريال في 23 سبتمبر 1971م، والتي انضمت إليها الإمارات عام 1981م[120].

4- برتوكول قمع أعمال العنف غير المشروعة في المطارات التي تخدم الطيران الدولي الملحق باتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني،التي صدقت عام 1989م[121].

5- اتفاقية منع الجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية، بما فيهم الموظفون الدبلوماسيون، والمعاقبة عليها، التي اعتمدتها الجمعية العامة في 14 ديسمبر 1973م، التي انضمت إليها الإمارات عام 2003م[122].

6- الاتفاقية الدولية لمناهضة أخذ الرهائن، التي اعتمدتها الجمعية العامة في 17 ديسمبر 1979م، وانضمت إليها الإمارات عام 2003م[123].

7- اتفاقية الحماية المادية للمواد النووية، المعتمدة في فيينا في 3 مارس 1980م،وانضمت إليها الإمارات عام 2003م[124].

---

(118) اتفاقية لاهاي بشأن مكافحة الاستيلاء غير المشروع على الطائرات لعام 1970م.

(119) اتفاقية طوكيو الخاصة بالجرائم والأفعال التي ترتكب على متن الطائرات والموقعة بتاريخ 1963/9/14.

(120)اتفاقية مونتريال الخاصة بقمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني والموقعة في 1971/9/23، والبروتوكول الملحق بها والموقع في مونتريال بتاريخ 1984/5/10م.

(121)البروتوكول المتعلق بقمع أعمال العنف غير المشروعة في المطارات التي تخدم الطيران المدني الدولي، المكمل لاتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني،والموقع في مونتريال في 24 فبراير 1988م.

(122)اتفاقية نيويورك الخاصة بمنع ومعاقبة الجرائم المرتكبة ضد الأشخاص المشمولين بالحماية الدولية بمن فيهم الممثلون الدبلوماسيون والموقعة في 1973/12/14.

(123)اتفاقية اختطاف واحتجاز الرهائن والموقعة في 1979/12/17.

(124) اتفاقية الحماية المادية للمواد النووية، المعتمدة في فيينا في 3 /3/ 1980م.

8- اتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الملاحة البحرية، الموقعة في روما في 10 مارس 1988م[125].

9- البروتوكول المتعلق بقمع أعمال العنف غير المشروعة الموجهة ضد سلامة المنصات الثابتة الواقعة على الجرف القاري، الموقع في روما في 10 مارس 1988م، والتي دخلت حيز النفاذ بالنسبة لدولة الإمارات العربية المتحدة عام 2005م[126].

10- الاتفاقية الدولية لقمع الهجمات الإرهابية بالقنابل التي اعتمدتها الجمعية العامة في 15 ديسمبر 1997م، التي انضمت إليها الإمارات عام 2005م[127].

- **الاتفاقيات الإقليمية:**

صادقت دولة الإمارات العربية المتحدة على العديد من الاتفاقيات الإقليمية بشأن مكافحة الإرهاب[128]:

- اتفاقية الرياض للتعاون القضائي، وذلك بالمرسوم الاتحادي رقم 53 لعام 1999م[129].
- الاتفاقية الخاصة بدول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب، وتم التصديق عليها بالمرسوم رقم 54 لعام 2004م"[130].
- معاهدة منظمة المؤتمر الإسلامي الخاصة بمكافحة الإرهاب الدولي عام 1999م[131].

---

(125)اتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الملاحة البحرية، الموقعة في روما في 10 مارس 1988م.

(126)البروتوكول المتعلق بقمع أعمال العنف غير المشروعة الموجهة ضد سلامة المنصات الثابتة الواقعة على الجرف القاري، الموقع في روما في 10 مارس 1988م.

(127)الاتفاقية الدولية لقمع الهجمات الإرهابية بالقنابل التي اعتمدتها الجمعية العامة في 15 ديسمبر 1997.

(128) **دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن**، مرجع سابق، ص68.

(129) المرسوم الاتحادي رقم 53 لسنه 1999م، بشأن اتفاقية الرياض للتعاون القضائي.

(130) اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب عام 2004م، تاريخ النشر 24/7/ 2008م.

(131) معاهدة منظمة المؤتمر الإسلامي الخاصة بمكافحة الإرهاب الدولي عام 1999م، بتاريخ 1 يوليو 1999م.

- الاتفاقية العربية لمكافحة الإرهاب لعام 1998م، التي صدقت عليها الإمارات بموجب القانون رقم 103 لعام 1998م[132].

- أما فيما يتعلق بالتدابير التي اتخذتها دولة الإمارات بشأن مكافحة الجرائم الإرهابية وآليات التعاون القضائي الدولي؛ فقد أصدرت دولة الإمارات القانون الاتحادي بشأن التعاون القضائي الدولي في المسائل الجنائية[133].

، الذي تناول الأحكام الخاصة بتسليم الأشياء والأشخاص من حيث حالات وشروط التسليم وحالات الرفض، والإجراءات والجهات المختصة بالأمر، وكيفية الطعن على القرارات، كما عالج أحكام استرداد الأشياء والأشخاص، وأحكام النقل الخاصة بالمحكوم عليه وإبعاده إلى دول أجنبية، والمساعدة القضائية المتبادلة في المسائل الجنائية.

كما أصدر مجلس الوزراء قرارًا "بإنشاء اللجنة الوطنية بهدف تنفيذ قرار مجلس الأمن رقم 1373، عام 2001م، حيث منحت هذه اللجنة اختصاصات واسعة لوضع التصورات والخطط، واقتراح الأنظمة التنفيذية والإدارية، لتوحيد الجهود المبذولة على المستوى الدولي لمكافحة الإرهاب"[134].

ب-أساليب مكافحة الإرهاب الإلكتروني المنصوص عليها في الاتفاقيات والمؤتمرات الدولية والإقليمية:

تعد المعاهدات والاتفاقيات الدولية من أهم صور التعاون الدولي في مجال مكافحة جرائم الإرهاب الإلكتروني؛ ومن أهم المعاهدات والاتفاقيات الدولية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م، التي صادق عليها مجلس وزراء الداخلية، ومجلس وزراء العدل العرب، في

(132) الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة بتاريخ 1998/4/22م.

(133) القانون الاتحادي رقم 39 لسنه 2006م، بشأن التعاون القضائي الدولي في المسائل الجنائية، نشر بتاريخ 2006/11/14م.

(134) دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن، مرجع سابق، ص69.

الاجتماعالمنعقد بمقر الأمانة العامة لجامعة الدول العربية عام 2010م، وقد تناولت هذه الاتفاقية جرائم الإرهاب الإلكتروني من خلال النص الوارد في المادة الثانية منها، الذي أشار إلى"أن الجرائم المتعلقة بالإرهاب والمرتكبة من خلال وسائل تقنية المعلومات؛ هي نشر مبادئ وأفكار جماعات إرهابية، والدعوة إليها، وتمويل العمليات الإرهابية، وتسهيل الاتصالات بين المنظمات الإرهابية، وأيضا نشر الطرق الخاصة بصناعة المتفجرات التي يتم استخدامها في عمليات إرهابية بوجه خاص، ونشر الفتن والنعرات، والاعتداء على الأديان والمعتقدات" [135].

ويمكن الإشارة في ضوء الحديث عن الجهود والمؤتمرات والاتفاقيات الدولية والإقليمية الخاصة بمواجهة جرائم الإرهاب الإلكتروني، إلى جهود مجموعة الدول الثمانية، بالإضافة إلى العديد من الإعلانات والبيانات التي تم إصدارها بشأن الجرائم الإرهابية؛ تتمثل في[136]:

- البيان الصادر عام 2004م، وتم الاتفاق فيه على مواصلة تعزيز القوانين المحلية لبناء القدرات العالية والخاصة بمكافحة الاستخدامات الإجرامية والإرهابية للإنترنت، ومواصلة الدول تحسين القوانين التي تعمل على تجريم إساءة استخدام الشبكات المعلوماتية والحاسوبية، والتي تسمح بسرعة التعاون الخاص بالتحقيقات التي تتصل بالإنترنت.
- بيان موسكو عام 2006م، الذي أكد على ضرورة اتخاذ التدابير اللازمة لمنع الأعمال الإرهابية المحتملة، التي تتضمن مجالات الاتصالات السلكية واللاسلكية، والعمل ضد بيع المعلومات والبيانات المزيفة، وبرامج الكمبيوتر وتطبيقات الفيروسات الضارة.
- البيان الصادر عام 2006م في سانت بطرسبرغ، الذي أكدَّ على التعاون مع الشركاء الدوليين بشأن مكافحة التهديد الإرهابي، وتضمن القيام بتحسين وتنفيذ الإطار القانوني الدولي الخاص

(135) المادة (15) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م.

(136)عبد الرحيم محمد، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**،مرجع سابق، ص69/67.

بمكافحة الإرهاب، والتصدي بفاعلية لمحاولات إساءة استخدام الفضاء الإلكتروني لتحقيق أغراض إرهابية،كما تضمن مكافحة التحريض على ارتكاب الجرائم الإرهابية، وتجنيد الإرهابيين وعمليات صنع الخطط الإرهابية.

وتجدر الإشارة في هذا المجال إلى العديد من المؤتمرات التي عقدت بهدف مكافحة الجرائم التي يتم ارتكابها عبر الفضاء الإلكتروني[137]:

- مؤتمر الأمم المتحدة 12 بشأن منع الجريمة والعدالة الجنائية عام 2010م، الذي انعقد في سلفادور تحت عنوان (إستراتيجيات شاملة لتحديات عالمية)، حيث تناول تنظيم العدالة الجنائية وتطورها في عالم متغير ومنع الجريمة، كما تضمن جدول أعمال خاص بمناقشة ثمانية بنود من ضمنها التعاون الدولي في مكافحة الجريمة، وجرائم الإنترنت، أو الشبكة العنكبوتية.
- مؤتمر قمة الأمن السيبراني في الولايات المتحدةالأمريكية عام 2014م، الذي تضمن مناقشة التدابير المضادة للتهديدات الإلكترونية، وقياس مدى تأمين البرامج الخاصة بالحاسب الآلي ضد العديد من الهجمات.
- مؤتمر قمة الأمن السيبراني بالبحرين، الذي ناقش العديد من الموضوعات؛منهاإعادة تعريف المخاطر، واستراتيجية مواجهة التهديدات المتنقلة، والبحث في إعادة الأمن، واستراتيجية تكنولوجيا المعلومات، والتخفيف من المخاطر الخاصة بأدوات التواصل الاجتماعي، إضافة إلى تنفيذ أفضل الممارسات بهدف تحقيق مدونة التهديدات.
- مؤتمر الأمن السيبراني الذي انعقد في جامعة نيويورك عام 2014م، وشارك فيه عدد من الشركات، وخبراء الإنترنت، والحكومات، وناقش عددًا من الموضوعات؛ منها: الابتكارات في

(137)عبد الرحيم محمد، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، مرجع سابق، ص72/70

المؤسسات الأجنبية والخصوصية، وحماية البنية التحتية الحساسة، والأفراد، والمنظمات من الهجمات الإلكترونية، وأنظمة الأمن والإنترنت.

الفصل الثاني

الإشكاليات القانونية في مواجهة الإرهاب الإلكتروني

تمهيد وتقسيم:

يرتبط مفهوم الإرهاب ارتباطًا وثيقًا بوسائل تقنية المعلومات، والتطور التكنولوجي، حيث ساهم التقدم التكنولوجي في ظهور أشكال وأساليب جديدة لارتكاب جرائم الإرهاب من خلال الوسائل الإلكترونية؛ فترتبعلى ذلك اتساع نطاق التجريم الخاص بهذه الجرائم،مما أدى إلى إحداث تغيرات مستمرة في صورها وأشكالها عن النماذج التقليدية الخاصة بها(138).

ونظرًا لكون جرائم الإرهاب الإلكتروني تعدنوعًا من أنواع الجرائم التي ترتكب عبر الفضاء الإلكتروني، فإنها تتميزبخصائص تنفرد عن غيرها من جرائم الإرهاب الأخرى التي تتم باستخدام الوسائل التقليدية،ومن ثمَّ فهي تحتاج إلى قواعد قانونية متطورة موازية لتلك الظاهرة، فضلًا عن أنها تثير العديد من الإشكاليات حول صعوبة اكتشافها وإثباتها، ومدى كفاية القوانين العامة والخاصة في مواجهتها(139).

بناء على ما سبق ستقسم الباحثة هذا الفصل إلى مبحثين؛ يتناول المبحث الأول الإشكاليات الموضوعية في مواجهة الإرهاب الإلكتروني، بينما يتناول الثاني الإشكاليات الإجرائية في مواجهة الإرهاب الإلكتروني.

المبحث الأول–الإشكاليات الموضوعية في مواجهة الإرهاب الإلكتروني.

المبحث الثاني–الإشكاليات الإجرائية في مواجهة الإرهاب الإلكتروني.

---

(138) حابس يوسف زيدات، مدى استيعاب النصوص **التقليدية للسرقة الإلكترونية**، دراسة مقارنة، مجلة مركز حكم القانون ومكافحة الفساد، دار جامعة حمد بن خليفة لنشر، 2019م، 2/1.

(139) شمسان ناجي صالح الخيلي، مرجع سابق، ص38.

المبحث الأول

الإشكاليات الموضوعية في مواجهة الإرهاب الإلكتروني

تمهيد وتقسيم:

إذا كانت الجرائم التي ترتكبعبر الفضاء الإلكتروني تتسم بخصائص تثير العديد من الإشكاليات الموضوعية في مواجهتها، فإن جرائم الإرهاب الإلكتروني ترتكب من خلال جماعات منظمة ترسم خطواتها وتسعى لتحقيق أغراضها بدقة عالية، الأمر الذي يجعلها تتسم بخصائص تفوق غيرها من جرائم الإرهاب الأخرى، وذلك من حيث الإشكاليات الموضوعية التي تثار في مواجهتها، وبغية الإحاطة بالجوانب المختلفة لهذه الإشكاليات، لا بد من دراسة القواعد العامة في مواجهة الإرهاب الإلكتروني، ثم دراسة القواعد الخاصة لمواجهة الإرهاب الإلكتروني؛ من خلال المطلبين التاليين:

المطلب الأول–القواعد الموضوعية العامة في مواجهة الإرهاب الإلكتروني.

المطلب الثاني– القواعد الموضوعية الخاصة في مواجهة الإرهاب الإلكتروني.

المطلب الأول

القواعد الموضوعية العامة والصعوبات في مواجهة الإرهاب الإلكتروني

تتسم جرائم الإرهاب الإلكتروني بالسرية والتعقيد، حيث يتصف مرتكبو هذه الجرائم بصفات تختلف عن تلك التي يتصف بها مرتكبو جرائم الإرهاب التقليدية، فهم على درجة عالية من الدقة والكفاءة التكنولوجية، من حيث الإلمام بمعارف ومهارات فنية واسعة في مجال الإنترنت والحاسب الآلي، ونظرًا لأنالتطور السريع في مجال التكنولوجيا لا يقابله تطور سريع في النصوص القانونية التي تواجهه هذا النوع من الجرائم؛ فإن النصوص الجنائية العامة الحالية لا تكون كافية لمواجهة هذه

الصور المستحدثة من جرائم الإرهاب؛ مما يؤدي إلى خروج هذه الفئة من تحت طائلة القانون[140].

بناء عليه ستعمد الباحثة إلبيان القواعد العامة التي وردت في قانون مكافحةالجرائم الإرهابية رقم 7 لسنة 2014م، ثم بيان صعوبات مواجهة جرائم الإرهاب الإلكتروني من خلال تطبيق القواعد العامة؛ على النحو التالي:

الفرع الأول

القواعد الموضوعية العامة في قانون مكافحةالجرائم الإرهابية

يلاحظ من خلال الاطلاع على النصوص الواردة في قانون مكافحة الإرهاب، أن المشرع قد نص على تجريم الأعمال الإرهابية بوجه عام، من خلال وضع تعريف لها وتقرير العديد من العقوبات لمواجهتها، حيث عرَّف الجريمة الإرهابية بأنها: "كل فعل أو امتناع عن فعل مجرم بموجب هذا القانون، وكل فعل أو امتناع عن فعل يشكل جناية أو جنحة واردة في أي قانون آخر، إذا ارتكبت لغرض إرهابي"[141].

هذا وقد أحسن المشرع عندما جمع بين كُلٍّ من الجريمة الإرهابية والجريمة المنظمة في تعريف التنظيم الإرهابي، وحدد المقصود بالشخص الإرهابي في الجرائم الإرهابية، وجرائم تمويل الإرهاب باعتبارها نوعًا من أنواع الجرائم الإرهابية، سواء كان شخصًا عاديًا أو تنظيمًا إرهابيًّا؛ حيث عرف الشخص الإرهابي بأنه: "كل شخص ينتمي لتنظيم إرهابي، أو ارتكب جريمة إرهابية، أو شارك مباشرة

(140)طارق فوزي الفقي، **الجوانب الإجرائية في الجرائم المعلوماتية**، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية، 2011م، ص34.

(141) المادة الأولى من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

أو بالتسبب في ارتكابها، أو هدد بارتكابها، أو يهدد أو يخطط أو يسعى لارتكابها، أو روَّج أو حرَّض على ارتكابها"(142).

كما عرف التنظيم الإرهابي بأنه "مجموعة مكونة من شخصين أو أكثر، تكتسب الشخصية الاعتبارية بحكم القانون أو توجد بحكم الواقع، ارتكبت جريمة إرهابية أو شاركت مباشرة أو بالتسبب في ارتكابها، أو هددت بارتكابها، أو تهدف أو تخطط أو تسعى لارتكابها، أو روَّجت أو حرَّضت على ارتكابها، أيًّا كان مسمى هذه المجموعة، أو شكلها، أو المكان الذي أسست فيه، أو تتواجد فيه، أو تمارس فيه نشاطها، أو جنسية أفرادها، أو مكان تواجدهم"(143).

أما بالنسبة للعقوبات فقد قرر المشرع عددًا من العقوبات على ارتكاب الجرائم الإرهابية؛ حيث نص المشرع على "معاقبة كل من خطط، أو سعى لارتكاب جريمة إرهابية بالعقوبة المقررة للجريمة التي خطط أو سعى لارتكابها"(144)، وأيضًا "معاقبة كل من حرَّض على ارتكاب جريمة إرهابية بالعقوبة المقررة للشروع في الجريمة التي حرَّض على ارتكابها، ولو لم ينتج عن التحريض أثر"(145).

ونص أيضًا على تطبيق "عقوبتي الإعدام أو السجن المؤبد لكل من استخدم مرفقًا نوويًّا أو كيميائيًّا، أو بيولوجيًّا أو أحدث أضررًا به، بطريقة من شأنها الإطلاق الإشعاعي، أو النشاط الإشعاعي، أو السموم أو المواد الكيميائية السامة، أو الكائنات أو الوسائط البيولوجية المرضية، وكان ذلك لغرض إرهابي"(146).

كما فرض "عقوبة السجن المؤبد أو المؤقت على كل من حاول، أو شرع في الاعتداء على سلامة، أو حرية شخص مشمول بالحماية الدولية لغرض إرهابي، وفي حالة وقوع الجريمة تكون العقوبة السجن

---

(142) المادة الأولى من القانون الاتحادي رقم 7 لسنه 2014م، بشأن مكافحة الجرائم الإرهابية.
(143) المادة الأولى من القانون الاتحادي رقم 7 لسنه 2014م، بشأن مكافحة الجرائم الإرهابية.
(144) المادة (19) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.
(145) المادة (20) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.
(146) المادة (8) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

المؤبد، و أيضًا على عقوبة السجن المؤبد أو المؤقت لكل من اعتدى بالقوة لغرض إرهابي على المقر الرئيسي، أو محل إقامة، أو وسيلة مواصلات شخص مشمول بالحماية الدولية"[147].

كما قرر "عقوبتي الإعدام أو السجن المؤبد لكل من ارتكب فعلًا، أو امتنع عن فعل من شأنه أو قصد به تهديد استقرار الدولة، أو سلامتها، أو وحدتها، أو سيادتها، أو أمنها، أو كان مناهضًا للمبادئ الأساسية التي يقوم عليها نظام الحكم، أو قصد به قلب نظام الحكم فيها، أو الاستيلاء عليه، أو تعطيل بعض أحكام الدستور بطريقة غير مشروعة، أو منع إحدى مؤسسات الدولة أو إحدى السلطات العامة من ممارسة أعمالها، أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي"[148].

إضافة إلى ذلك عاقب المشرع على جرائم التعاون مع تنظيم إرهابي مع العلم بحقيقة هذا التنظيم وغرضه، أو التعاون مع شخص إرهابي على تحقيق غرضه مع العلم أيضًا بحقيقته وغرضه، حيث قرر عقوبة السجن المؤبد أو المؤقت الذي لا تقل مدته عن خمس سنوات،وتشديد هذه العقوبة إلى الإعدام أو السجن المؤبد في الحالة التي يكون فيها الفاعل من أفراد القوات المسلحة، أو الشرطة، أو الأمن، أو سبق له تلقي تدريبات عسكرية أو أمنية[149].

كما تطرق المشرع إلى الوسائل الإلكترونية في مجال جرائم الإرهاب، ويتضح ذلك من العقاب على عمليات الترويج للجرائم الإرهابية بأي وسيلة من هذه الوسائل؛ حيث نص على أنه:" 1- يعاقب بالسجن المؤقت الذي لا تزيد مدته على عشر سنوات كل من روَّج، أو حَبَّذَ بالقول أو الكتابة أو بأي طريقة أخرى لأي تنظيم إرهابي، أو شخص إرهابي، أو جريمة إرهابية؛ مع علمه بذلك. 2- يعاقب بالسجن المؤقت الذي لا تزيد مدته على عشر سنوات كل من: أ- حاز بالذات أو بالواسطة، أو أحرز أي محررات، أو مطبوعات، أو تسجيلات أيًّا كان نوعها تتضمن ترويجًا أو تحبيذًا لتنظيم إرهابي، أو

(147) المادة (12) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.
(148) المادة (14) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.
(149) المادة (31) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

لشخص إرهابي، أو لجريمة إرهابية، إذا كانت معدة للتوزيع أو لاطلاع الغير عليها؛ مع علمه بذلك.

ب- حاز أو أحرز أي وسيلة من وسائل الطباعة، أو التسجيل، أو العلانية، استعملت أو أعدت للاستعمال ولو بصفة مؤقتة لطبع، أو تسجيل، أو إذاعة، أو نشر شيء مما ذكر؛ مع علمه بذلك"[150].

هذا ولم يغفل المشرع عن تجريم إعلان العداء أو عدم الولاء للدولة أو لنظام الحكم فيها "يعاقب بالسجن المؤبد أو المؤقت كل من أعلن بإحدى طرق العلانية عداءه للدولة، أو لنظام الحكم فيها، أو عدم ولائه لقياداتها"[151].

كما بين المقصود بالخطورة الإرهابية التي تتمثل في تبني الفكر المتطرف أو الإرهابي، حيث يخشى من ارتكاب هذا الشخص لجرائم إرهابية، كما أنه يعتبر عنصرًا دخيلًا على المجتمع، ويهدد استقراره وأمنه؛ ومن ثم يقتضي الأمر إضافة للعقوبات المقيدة للحرية أن يتم معالجته وتقويمه فكريًّا، من خلال السلطة التي أعطاها المشرع للنائب العام بإيداع المحكوم عليه في إحدى مراكز المناصحة؛ حيث نص المشرع على أنه: " للمحكمة بناء على طلب من النيابة أن تحكم بإخضاع من توافرت فيه الخطورة الإرهابية، وللمدة التي تحددها المحكمة، لتدبير أو أكثر من التدابير الآتية: المنع من السفر، المراقبة، حظر الإقامة في مكان معين أو منطقة محددة، تحديد الإقامة في مكان معين، حظر ارتياد أماكن أو محال معينة، ومنع الاتصال بشخص أو أشخاص معينين، وتشرف المحكمة على تنفيذ التدابير التي أمرت بها، وعلى النيابة عرض تقرير على المحكمة عن مسلك الخاضع للتدبير في فترات دورية لا تزيد أي فترة منها على ثلاثة أشهر، وللمحكمة أن تأمر بإنهاء التدبير، أو تعديله، أو إنقاص مدته؛ بناء على طلب من النيابة أو الخاضع للتدبير، وإذا رفض طلب الخاضع للتدبير فلا يجوز له

(150) المادة (34) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(151) المادة (15) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

تقديم طلب جديد إلا بعد ثلاثة أشهر من تاريخ رفضه، ويعاقب الخاضع للتدبير بالحبس مدة لا تزيد عن سنة إذا خالف التدبير الذي أمرت به المحكمة".

ونص المشرع على أنه "إذا توافرت في الشخص الخطورة الإجرامية أودع في أحد مراكز المناصحة بحكم من المحكمة وبناء على طلب من النيابة، ويقدم مركز المناصحة إلى النيابة تقريرًا دوريًّا كل ثلاثة أشهر عن الشخص المودع، وعلى النيابة رفع هذه التقارير إلى المحكمة مشفوعة برأيها، وعلى المحكمة أن تأمر بإخلاء سبيل المودع إذا تبين لها أن حالته تسمح بذلك"[152].

وتخلص الباحثة من النصوص السابقة أن المشرع اتبع سياسة عقابية تهدف إلى وقاية المجتمع من خطورة الجرائم الإرهابية بوجه عام، سواء من خلال تحقيق الردع العام؛ الذي يتمثل في إنذار الكافة بسوء العاقبة التي ستلحق بهم، من خلال تطبيق العقوبات المقررة عند ارتكاب أي من الجرائم الإرهابية المنصوص عليها في هذا القانون، أو من خلال الردع الخاص؛ الذي يتمثل في مخاطبة فرد معين، لم يتحقق معه الردع العام قبل ارتكابه لهذه الجرائم؛ فتطبيق العقوبة عليه لإصلاحه، والقضاء على الدوافع التي أدت إلى ارتكابه الجرائم، كما تطبق التدابير الاحترازية لمن تتوافر فيه الخطورة الإجرامية؛ حتى يتم تأهيله وتهذيبه وإصلاحه، وتنمية الشعور لديه بالمسؤولية تجاه نفسه وتجاه المجتمع.

يلاحظ على المشرع مما سبق أنه تشدد في العقاب على الجرائم الإرهابية بشكل عام، ومن مظاهر هذا التشدد النص على أنه"فيما لم يرد به نص في هذا القانون ... تعتبر الجنح والجنايات المنصوص عليها في قانون العقوبات أو أي قانون آخر جرائم إرهابية إذا ارتكبت لغرض إرهابي؛ وتوقع العقوبة على النحو الآتي:

(152) المادة (40) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

1- إذا كانت العقوبة المقررة أصلًا للجريمة هي الحبس جاز مضاعفة حده الأقصى.

2- إذا كانت العقوبة المقررة أصلًا للجريمة هي السجن المؤقت الذي يقل حده الأقصى عن خمس عشرة سنة جاز الوصول بالعقوبة إلى هذا الحد.

3- إذا كانت العقوبة المقررة أصلًا للجريمة هي السجن المؤقت الذي يصل إلى حده الأقصى جاز الوصول بالعقوبة إلى السجن مدة عشرين سنة، أو يستبدل بها السجن المؤقت.

4- إذا كانت العقوبة المقررة أصلًا للجريمة هي السجن المؤبد جاز الحكم بالإعدام"[153].

كما قرر المشرع عدم انقضاء الدعوى الجزائية أو سقوط العقوبة المحكوم بها في الجرائم الإرهابية إلا بالتنفيذ التام، أو العفو الشامل، أو بالعفو الخاص،وعدم خضوع العقوبات المقيدة للحرية المحكوم بها في أي جريمة إرهابية للإفراج المبكر المنصوص عليها في أي قانون نافذ[154].

أما فيما يتعلق بجرائم تمويل الإرهاب، قد أورد المشرع عددا من النصوص بشأن مكافحته جرائم تمويل الإرهاب بصفتها نوعًا من أنواع الجرائم الإرهابية؛ من ذلك النص على أنه"مع عدم الإخلال بأحكام القانون الاتحادي رقم (3) لسنة 1987م المشار إليه، والقانون الاتحادي رقم 7 لسنة 2014م المشار إليه:

1- يعد مرتكبًا لجريمة تمويل الإرهاب كل من ارتكب عمدًا أيًّا مما يأتي[155]:

أ- أحد الأفعال المحددة في البند (1) من المادة (2) من هذا المرسوم بقانون،(التي تتمثل في أ- حول المتحصلات، أو نقلها، أو أجرى أي عملية بها بقصد إخفاء، أو تمويه مصدرها غير

(153) المادة (39) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(154) المادة (53) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(155) المواد 2، 3، المرسوم بقانون اتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل، الإرهاب وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية رقم 10 لسنه 2019م، صادر بتاريخ 2018/9/23م.

المشروع. ب- أخفى، أو موه حقيقة المتحصلات، أو مصدرها، أو مكانها، أو طريقة التصرف فيها، أو حركتها، أو ملكيتها، أو الحقوق المتعلقة بها.ج- اكتسب، أو حاز، أو استخدام المتحصلات عند تسلمها.د- مساعدة مرتكب الجريمة الأصلية على الإفلات من العقوبة) إذا كان عالمًا بأن المتحصلات كلها أو بعضها مملوكة لتنظيم إرهابي، أو لشخص إرهابي، أو معدة لتمويل تنظيم إرهابي، أو شخص إرهابي، أو جريمة إرهابية، ولو كان ذلك دون قصد إخفاء، أو تمويه مصدرها الغير مشروع.

ب-قدم المتحصلات، أو جمعها، أو أعدها، أو حصلها، أو سهّل للغير الحصول عليها بقصد استخدامها، أو مع علمه بأنها سوف تستخدم كلها أو بعضها في ارتكاب جريمة إرهابية، أو ارتكب تلك الأفعال لصالح تنظيم إرهابي، أو لشخص إرهابي، مع علمه بحقيقتهما أو غرضهما.

2-يعد مرتكبًا لجريمة تمويل التنظيمات غير المشروعة كل من ارتكب عمدًا أيًّا مما يأتي:

أ- أحد الأفعال المحددة في البند (1) من المادة (2) من هذا المرسوم بقانون، إذا كان عالمًا بأن المتحصلات كلها أو بعضها مملوكة لتنظيم غير مشروع، أو لأحد المنتمين له، أو معدة لتمويل أي منهما، ولو كان ذلك دون قصد إخفاء أو تمويه مصدرها الغيرالمشروع.

ب-قدم المتحصلات، أو جمعها، أو أعدها، أو حصلها، أو سهّل للغير للحصول عليها بقصد استخدامها، أو مع علمه بأنها سوف تستخدم كلها أو بعضها لصالح تنظيم غير مشروع، أو لأحد المنتمين له، مع علمه بحقيقتهما أو غرضهما".

كما عرف المشرع المتحصلات بأنها هي "الأموال الناتجة بطريق مباشر أو غير مباشر من ارتكاب أي جناية أو جنحة، ويشمل ذلك الأرباح، والامتيازات، والفوائد الاقتصادية، وأي أموال مماثلة محولة

كليًّا أو جزئيًّا إلى أموال أخرى"[156].

كما قرر المشرع عددًا من العقوبات بشأن مكافحة جرائم تمويل الإرهاب، سواء وقعت بصوره مستقلة، أو مرتبطة بغسيل الأموال حيث نص على أنه: "يعاقب بالسجن المؤبد أو المؤقت كل من كان عالمًابأن الأموال كلها أو بعضها متحصلة من جريمة إرهابية، أو مملوكة لتنظيم إرهابي، أو كانت غير مشروعة ومملوكة لشخص إرهابي، أو معدة لتمويل تنظيم إرهابي، أو شخص إرهابي، أو جريمة إرهابية، وارتكب أحد الأفعال الآتية[157]:

1- حوَّل، أو نقل، أو أودع، أو استبدل الأموال بقصد إخفاء أو تمويه حقيقتها، أو مصدرها، أو غرضها غير المشروع.

2- أخفى، أو موَّه حقيقة الأموال غير المشروعة، أو مصدرها، أو مكانها، أو طريقة التصرف فيها، أو حركتها، أو ملكيتها، أو الحقوق المتعلقة بها.

3- اكتسب الأموال، أو حازها، أو استخدمها، أو أدارها، أو حفظها، أو استثمرها، أو بدَّلها، أو تعامل فيها بقصد إخفاء أو تمويه حقيقتها، أو مصدرها، أو غرضها غير المشروع".

كما نص على أنه" 1- يعاقب بالإعدام أو بالسجن المؤبد كل من أمدَّ تنظيمًا إرهابيًّا، أو شخصًا إرهابيًّا بأسلحة تقليدية، أو غير تقليدية، أو غيرها من المواد التي تعرض حياة الناس أو أموالهم للخطر، مع علمه بحقيقة أو بغرض التنظيم أو الشخص.2- يعاقب بالسجن المؤبد أو المؤقت الذي لا تقل مدته عن عشر سنوات كل من أمدَّ تنظيمًا إرهابيًّا أو شخصًا إرهابيًّا بمهمات، أو مستندات صحيحة أو مزورة، أو وسائل اتصال، أو أي أدوات، أو معلومات، أو مشورة، أو سكن، أو مأوى، أو

(156)المادة الأولى من المرسوم بقانون اتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية رقم 10 لسنه 2019م.

(157) المادة (30) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

مكان للاجتماع، أو غير ذلك من التسهيلات التي تعينه على تحقيق غرضه، مع علمه بحقيقة أو بغرض التنظيم أو الشخص.

4- يعاقب بالسجن المؤبد أو المؤقت الذي لا تقل مدته عن عشر سنوات كل من أخفى، أو أتلف، أو سرق، أو اختلس مستندًا أو محررًا خطيًّا، أو إلكترونيا؛ لمنع الكشف عن جريمة إرهابية، أو إقامة الدليل عليها"[158].

كما نص المشرع على عقوبة تمويل الإرهاب المرتبطة بغسل الأموال "يعاقببالسجن المؤبد أو المؤقت الذي لا تقل مدته عن عشر سنوات وبالغرامة التي لا تقل عن 300000 ثلاثمائة ألف درهم ولا تزيد على 10000000 عشرة ملايين درهم كل من استخدم المتحصلات في تمويل الإرهاب"[159].

وكذلك نص على أن "يعاقببالسجن المؤقت أو الغرامة التي لا تقل عن 300000 ثلاثمائة ألف درهم ولا تزيد على 10000000عشرة ملايين درهم كل من استخدم المتحصلات في تمويل تنظيمات غير مشروعة"[160].

إضافة إلى ما تقدم أكد المشرع في القانون الاتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة،على التزام دولة الإمارات العربية المتحدة بتنفيذ القرارات الدولية التي تتعلق بمكافحة جرائم تمويل الإرهاب، وفرض العديد من العقوبات الجسيمة على مخالفتها؛ من خلال النص على أنه "يعاقب بالحبس أو الغرامة التي لا تقل عن 50000 خمسين ألف درهم ولا تزيد عن 5000000 خمسة ملايين درهم كل من يخالف التعليمات الصادرة من قبل السلطة المعنية في الدولة، بشأن تنفيذ القرارات الصادرة من مجلس الأمن

---

(158) المادة (32) من القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية.

(159) المادة (22) من المرسوم بقانون اتحادي رقم 20 لسنة 2018م، في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية رقم 10 لسنه 2019م.

(160) المادة (22) من المرسوم بقانون اتحادي رقم 20 لسنة 2018م، في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية رقم 10 لسنه 2019م.

التابع للأمم المتحدة، تحت الفصل السابع من ميثاق الأمم المتحدة، بشأن منع وقمع الإرهاب، وتمويله، ومنع وقمع ووقف انتشار أسلحة الدمار الشامل، وتمويلها، وغيرها من القرارات ذات الصلة".

وتخلص الباحثة مما سبق أنه على الرغم من العقوبات السالبة للحرية التي قررها المشرع في مواجهة الجرائم الإرهابية، فضلًا عن النصوص التي هدف من ورائها معالجته الخطورة الإرهابية؛ فإن القواعد العامة والنصوص التقليدية غير كافية لمواجهة جرائم الإرهاب الإلكتروني؛ حيث تتطلب القواعد العامة الصفة المادية في الشيء محل الجريمة، وهذا يتنافى مع الطبيعة المعلوماتية للجرائم التي ترتكب عبر شبكة الإنترنت، ووسائل الاتصالات والمعلومات. ويرجع ذلك لاختلاف جرائم الإرهاب التي تستخدم الوسائل التقليدية في ارتكابها، عن جرائم الإرهاب الإلكتروني التي تستخدم في ارتكابها الوسائل الإلكترونية؛ نظرًا لارتباطها بشبكةَ الإنترنت بصفة عامة، ووسائل التواصل الاجتماعي بوجه خاص.

الفرع الثاني

صعوبات مواجهة جرائم الإرهاب الإلكتروني من خلال تطبيق القواعد العامة

تنفرد جرائم الإرهاب الإلكتروني عن غيرها من جرائم الإرهاب التقليدية بعدد من السمات والخصائص،مما يجعل النصوص التقليدية غير كافية لمواجهتها، تتمثل هذه الصعوبات فيما يلي:

اولا:- يتم ارتكاب جرائم الإرهاب الإلكتروني عبر الفضاء الإلكتروني من خلال الحاسب الآلي:

تعدُّ هذه الخاصية أهم الخصائص التي تميز جرائم الإرهاب الإلكتروني عن غيرها من جرائم الإرهاب التقليدية، فعادة ما تتطلب هذه الجريمة وجود حاسب آلي يكون متصل بالشبكة المعلوماتية [161]. فشبكة الإنترنت هي الفضاء الإلكتروني الذي يمكن من خلاله ارتكاب جرائم الإرهاب الإلكتروني، وتعتبر أيضًا حلقة الوصل بين كافة الأهداف والأغراض المحتملة لهذا النوع من الجرائم،

(161)نبيلة هبه هروال، **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات**، مرجع سابق، ص37.

فقد أتاحت شبكة الإنترنت الفرصة للعديد من المنظمات الإرهابية بفتح مواقع تعتبر بمثابة المقر المركزي لها، بهدف الترويج عن المنتجات الخاصة بها، ونشر أفكارها بغرض تجنيد الأفراد الذين يتعاطفون مع تلك الأعمال[162].

ثانيا:- تعتبر جرائم الإرهاب الإلكتروني من الجرائم العابرة للحدود الدولية:

تتسم جرائم الإرهاب الإلكتروني بالطابع الدولي،فهي جرائم عابرة للقارات لا تعترف بالحدود والحواجز القائمة بين الدول سواء كانت حدود سياسية، أو جغرافية؛ لذا فهي تصنف في نطاق الجرائم الدولية، ولا تخضع لنطاق إقليمي محدد[163].

وتعتبر جريمة الإرهاب جريمة عابرة للحدود وجريمة دولية في الحالة التي يكون أحد أطرافها شخص من الأشخاص الدولية، أو في حالة امتداد العمل الإرهابي لأكثر من دولة،حيث تمكنت الجماعات الإرهابية من استغلال الفضاء الإلكتروني في عدد من الأغراض؛كالإشهار، وذلك لبيان المخططات الخاصة بها، أو لإصدار بياناتها، أو لتبني عملياتها المنفذة، أو إنجازاتها[164].

وانطلاقًا من ذلك يعترض مواجهة جرائم الإرهاب الإلكتروني عدد من المشكلات والصعوبات القانونية والعملية، بصفتها جرائم عابرة للحدود؛ يمكن إيجاز هذه الصعوبات فيما يلي[165]:

1- عدم تجريم بعض الدول لبعض الأفعال التي ترتكب من خلال الوسائل الإلكترونية ووسائل تقنية المعلومات، في حين أنها مجرمة في دول أخرى.

---

(162)محمود صالح العادلي، مرجع سابق،ص96.

(163)غنام محمد غنام، **دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت**، دار الفكر والقانون، المنصورة، 2017/2016م، ص217.

(164)نبيلة هبه هروال، **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات**، مرجع سابق، ص96.

(165) سليمان أحمد فضل، مرجع سابق، ص384/383.غنام محمد غنام، مرجع سابق، ص219.

2- صعوبة وتعقد المشاكل الفنيةوالقانونيةالخاصة بتنفيذ النظام المعلوماتى خارج حدود الدولة، أو الأمر بتسليم المعلومات المخزنة فيه، أو ضبطها.

3- صعوبة معرفة الفاعل والمرتكب الحقيقي لجرائم الإرهاب الإلكتروني.

4- عدم كفاية المعاهدات الجماعية أو الثنائية بين الدول، أو المعاهدات الخاصة بالتسليم، التي تسمح بالتعاون الدولي، لمواجهة المتطلبات الخاصة بمكافحة جرائم الإرهاب الإلكتروني.

5- عدم وجود مفهوم وتعريف عام مشترك بين الدول فيما يتعلق بجرائم الإرهاب والإرهاب الإلكتروني، ونماذج النشاط المكونة لتلك الجرائم.

6- عدم التناسق بين القوانين الخاصة بالدول فيما يتعلق بالإجراءات الجنائية بشأن مواجهة جرائم الإرهاب الإلكتروني

ثالثا:- السرعة والتطورفي ارتكاب جرائم الإرهاب الإلكتروني:

ألقى التطور السريع الذي شهده المجال الخاص بتكنولوجيا المعلومات والاتصالات بظلاله على جرائم الإرهاب الإلكتروني، حيث إن الأساليب الخاصة بارتكابها في تطور دائم ومستمر، حيث يستفيد المجرمون من شبكة الإنترنت في تبادل المعلومات والأفكار الإجرامية، حيث تقدمالجماعات الإرهابية على تدريب من يرغب في الإنخراط في الأنشطة الإرهابية، من خلال التعليمات والكتابات والمعلومات التي توضح طرق ووسائلتصنيع المتفجرات، والقنابل، والأسلحة المدمرة، والمواد الحارقة، فتوفر شبكة الإنترنت المعلومات التي يصعب الحصول عليها في الواقع، فتتيح الفرصة للتعرف على مصادر توليد الكهرباء والطاقة، ومواقع المنشآت النووية، ومواعيد الرحلات الجوية الدولية، وغير ذلك

من المعلومات التي تكون مدعومة بالصور، والتي تسمح بالتخطيط الدقيق والمحكم من خلالها[166].

رابعا:- سهولة ارتكاب جرائم الإرهاب الإلكتروني:

جرائم الإرهاب الإلكتروني التي ترتكب باستخدام الوسائل الإلكترونية لا تحتاج إلى عنف أثناء ارتكابها أو تنفيذها، حيث إنها تتم باستخدام الشبكة المعلوماتية، فالمجرم فيها يعتمد في ارتكابها على خبرته في مجال تكنولوجيا المعلومات، فهو مجرم غير عنيف، ولا يلجأ إلى استخدام العنف في ارتكاب الجرائم الخاصة به؛ خلافًا لجرائم الإرهاب التقليدية التي تعتمد على استخدام التهديد والعنف، وإثارة الرعب؛ من خلال استخدام أداة ضغط عسكرية أو سياسية[167].

خامسا:- خصوصية مرتكبي جرائم الإرهاب التي ترتكب باستخدام الوسائل الإلكترونية:

إن مرتكبي جرائم الإرهاب الإلكتروني ذوي اختصاص ومعرفة في مجال تقنية المعلومات والاتصالات، ولديهم المعرفة والقدرة على التعامل مع مختلف الوسائل الإلكترونية؛ خلافًا لمرتكبي جرائم الإرهاب التقليدية[168].

سادسا:- نقص الخبرة لدى الأجهزة القضائية والأمنية في التعامل مع جرائم الإرهاب الإلكتروني:

تتطلب جرائم الإرهاب الإلكتروني إلمام أجهزة النيابة العامة والشرطة والقضاء بعدد من الأمور التقنية والفنية؛ بغية معرفة مرتكبي هذه الجرائم، كما تتطلب أسلوبًا خاصًّا في التعامل مع هذا النوع من الجرائم التي تحتاج لوسائل فنية تقنية متطورة في ارتكابها،حيث وجدت العديد من هذه الجهات أنها

---

(166) محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة المعلومات**، دراسة مقارنة، ط2، دار النهضة العربية، 2009م، ص39.

(167) المرجع السابق، ص39.

(168) عبدالله بن عبدالعزيز بن فهد العجلان، **الإرهاب المعلوماتى**، بحوث ومقالات،المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، 2015، ص56. أيضا- عبدالله دغش العجمي،مرجع سابق،ص22/21. شمسان ناجي صالح الخيلي، سابق، ص43/42.

غير قادرة على اكتشاف هذا النوع من الجرائم والتعامل معه، فلجأت إلى فئة من المجرمين يسمون بالهاكرز لمعرفة بعض الأمور الغامضة الخاصة بجرائم الإرهاب الإلكتروني[169].

إزاء ذلك قامت هذه الجهات بالعمل على تطوير أجهزتها المختصة، وإنشاء مراكز متخصصة لهذا الغرض وهذا النوع من التقنية، وهناك محاولات جادة في استيعاب رجال القضاء والأمن، ضمن تطبيقات الحاسب الآلي، إلا أن هذه المحاولات لم تحقق الأهداف والأغراض المرجوة منها لعدد من الأسباب؛ أهمها[170]:

- انتشار الحاسب الآلي والإنترنت على نطاق واسع وتعدد البرامج والأنظمة الخاصة به، والتطور المتلاحق والسريع عليه؛ أدى إلى صعوبة تدريب وإعداد الجهات القضائية والأمنية ومواكبتها لهذا التطور.
- ضعف الميزانية المالية لدى أجهزة القضاء والأمن، قياسًا بتكاليف الخبرة الخاصة في تطبيقات وعلوم الحاسب الآلي، إضافة إلى أنها لا تصل إلى المبالغ التي تسددها شركات ومؤسسات القطاع الخاص.
- إن الخبرة الإجرائية لدى الجهات والسلطات العامة بشأن جرائم الإرهاب الإلكتروني لا زالت حديثة، رغم انتشار التقنيات المتطورة والحديثة في الحكومة والقطاع الخاص، والحياة العامة والخاصة؛ نظرًا لعدم وضوح الرؤية الخاصة بنصوص التجريم، كما أن الخبرة العلمية لدى هذه الجهات تأتي من الممارسة، الأمر الذي يستلزم أن يتم وقوع الجرائم بنفس الشكل والعدد الذي تقع به الجرائم التقليدية.

سابعا:- تتسم جرائم الإرهاب الإلكتروني بالخفاء:

---

(169) محمد عبيد الكعبي،مرجع السابق، ص44/43.

(170) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص44/43.

تتسم جرائم الإرهاب الإلكتروني بالخفاء فهي من الجرائم المستترة التي لا يمكن ملاحظتها، تقع بعد تدبير وتخطيط مسبق أثناء التواجد على شبكة الإنترنت وغرف الدردشة وتبادل المعلومات في المنتديات،فلا ينتبه لها ولا تلاحظ إلا بعد فترة من وقوعها؛ نتيجة تعامل الجناة مع نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا من خلال الحاسب، كما يؤدي توافر الخبرة الفنية والمعرفة التقنية لدى الجاني إلى صعوبة اكتشافها، إضافة إلى أن المجرمين الذين يرتكبون جرائم الإرهاب الإلكتروني، يكونون على درجة عالية من الذكاء؛ لتذليل الصعوبات والعقبات التي يمكن تواجههم أثناء ارتكاب جرائمهممن خلال عدد من البرامج التي تساعدهم على إخفاء شخصياتهم أثناء تصفح الموقع أو إرسال البريد[171]، حيث يعد انتحال الشخصية من خلال البريد الإلكتروني من أكثر الوسائل استخدامًا من طرف المجرمين لتزييف الرسائل لتبدو كأنها صادرة من أشخاص وأسماء أخرى[172].

المطلب الثاني

القواعد الموضوعية الخاصة في مواجهة الإرهاب الإلكتروني

لم تعد النصوص التقليدية التي كانت سائدة قبل انتشار شبكة الإنترنت قادرة على مواكبة التطورات الهائلة في مجال تكنولوجيا المعلومات، حيث أصبحت الجريمة أكثر صعوبةً وتعقيدًا في ظل هيمنة التكنولوجيا الحديثة، كما ظهرت أشكال وصور عديدة للجرائم الإرهابية، ومن بينها جرائم الإرهاب التي يتم ارتكابها عبر الفضاء الإلكتروني، حيث لعب التطور التكنولوجي والتقدم العلمي في وسائل الاتصال والمعلومات دورًا بارزًا فيها، كما أصبحت أجهزة المعلومات والاتصالات متاحة على

(171) شمسان ناجي صالح الخيلي،مرجع سابق، ص41.محمد عبيد الكعبي، مرجع سابق ص40.

(172) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص125. محمود صالح العادلي،مرجع سابق،ص94.شمسان ناجي صالح الخيلي،مرجع سابق، ص41.

مستوى واسع، الأمر الذي أدى إلى ابتكار طرق جديدة في ارتكابها، فبدا جليًا عجز القوانين والقواعد العامة التقليدية عن مواجهتها، الأمر الذي يقتضي وجود قواعد قانونية خاصة وتشريعات جديدة لمواجهة جرائم الإرهاب الإلكتروني؛ منعًا من اللجوء إلى القياس، والتوسع في تفسير النصوص التقليدية لمواجهة تلك الجرائم؛ حفاظًا على مبدأالشرعية الجنائية[173]، الذي يستوجب اتخاذ خطوات سريعة نحو مواكبة هذه التطورات التي تشهدها وسائل التكنولوجيا الحديثة[174].

وترى الباحثةُ أن المشرع الاتحادي أدرك أهمية وضع تشريع خاص بمكافحة جرائم تقنية المعلومات،حيث كانت دولة الإمارات من أوائل الدول العربية التي أصدرت تشريعات خاصة بمكافحة جرائم تقنية المعلومات، بما فيها الجرائم الإرهابية التي يتم ارتكابها بوسائل تقنية المعلومات.

وانطلاقًا مما سبق ستوضح الباحثة ما تضمنه المرسوم رقم 5 لسنة 2012م المعدل بالقانون رقم 2 لسنة 2018م من قواعد خاصة بشأن مواجهة جرائم الإرهاب الإلكتروني، فضلا عن أنها ستطرق إلى بعض المؤتمرات التي انعقدت في دولة الإمارات بشأن مكافحة جرائم تقنية المعلومات؛ على النحو التالي:

الفرع الأول

ما تضمنه المرسوم رقم 5 لسنة 2012م المعدل بالقانون رقم 2 لسنة 2018م من قواعد خاصة بشأن مواجهة جرائم الإرهاب الإلكتروني

واكب المشرع الاتحادي التغيرات المعلوماتية، والتكنولوجية، والاجتماعية، والاقتصادية التي أدت إلى ظهور جرائم الإرهاب الإلكتروني، والتي تعد من الجرائم ذات الخطورة العالية باستخدام وسائل تكنولوجيا المعلومات والاتصالات، من حيث الاستقطاب والاتصالوالإشراف والإدارة وغيرذلك في

(173) شمسان ناجي صالح الخيلي، مرجع سابق، ص44.محمد عبيد الكعبي، مرجع سابق، ص44.

(174) شمسان ناجي صالح الخيلي، المرجع السابق، ص44.محمد عبيد الكعبي، المرجع السابق، ص44.

العصرالخاص بالازدهار الإلكتروني، كما تغيرت أشكال وأنماط ارتكاب هذا النوع من الجرائم، واختلفتعن جريمة الإرهاب في صورتها التقليدية، كما أصبح اقتحام المواقع، والعبث بمحتوياتها، والدخول غير المشروع على شبكة المعلومات بهدف ارتكاب الجرائم هو أسلوب الإرهاب في صورته المستحدثة،الذي واكبه المشرع من خلال البحث في المستجدات الإقليمية والمحلية والدولية، لتحديد الأفعال والسلوكيات الخاصة بارتكابه، مع وضع العقوبات الرادعة بشأنه(175).

حيث نص المشرع على أن: "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم كل من أنشأ، أو أدار، موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات، للترويج أو التحبيذ لأي برامج أو أفكار من شأنها إثارةالفتنة، أو الكراهية والعنصرية، أو الطائفية، أو الإضرار بالوحدة الوطنية، أو السلم الاجتماعي، أو الإخلال بالنظام العام، أو الآداب العامة"(176).

كما "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم، أو بإحدى هاتين العقوبتين كل من أنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات، بقصد الاتجار أو الترويج

---

(175)رحيمة الطيب عيساني، **أخلاقيات استخدام وسائل الاتصال الجديدة وتشريعاتها في دولة الإمارات العربية المتحدة، قراءة تحليلية لقانون مكافحة تقنية المعلومات**، مجلة جامعة العين للأعمال والقانون، ع2، 2020م، ص79/77.

- عبدالمجيد مراد داد محمد أحمد، **المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي، دراسة وصفية تحليلية للقانون والقضاء الإماراتي**، كلية القانون، جامعة الشارقة، دولة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، 2020/2019م، ص28/26.

(176) المادة (24) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

للأسلحة النارية، أو الذخائر، أو المتفجرات في غير الأحوال المصرح بها قانونًا"[177].

و "يعاقب بالسجن مدة لا تقل عن عشر سنوات ولا تزيد عن خمس وعشرين سنة والغرامة التي لا تقل عن مليوني درهم ولا تجاوز أربعة ملايين درهم، كل من أنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات لمجموعة أو جماعة إرهابية، أو منظمة، أو جمعية، أو لهيئة غير مشروعة، أو جماعة إرهابية بقصد الترويج لها، وتسهيل الاتصال بقياداتها، أو لاستقطاب عضوية لها، أو تحبيذ أو ترويج أفكارها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة، أو المتفجرات،أو أي أدوات أخرى تستخدم في الأعمال الإرهابية. وتكون العقوبة الحبس مدة لا تزيد عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم، لمن حمل محتوى أيّا من المواقع المذكورة في المادة 26، أو أعاد بثها أو نشرها بأي وسيلة كانت، أو تقرر دخوله إليها لمشاهدتها، أو نشر أي محتوى يتضمن التحريض على الكراهية. وللمحكمة في غير حالات العود بدلًا من الحكم بالعقوبة المشار إليها في الفقرة السابقة أن تحكم بإيداع المتهم إحدى دور المناصحة، أو الحكم بوضعه تحت المراقبة الإلكترونية، ومنعه من استخدام أيّا من وسائل تقنية المعلومات خلال فترة تقدرها المحكمة، على ألا تتجاوز الحد الأقصى للعقوبة المقررة"[178].

و "يعاقب بالسجن المؤبد كل من أنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على الشبكة المعلوماتية، أو وسيلة تقنية معلومات، تهدف أو تدعو إلى قلب أو تغيير نظام الحكم في الدولة، أو الاستيلاء عليه، أو إلى تعطيل أحكام الدستور، أو القوانين السارية في البلاد، أو المناهضة

---

(177) المادة (25) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(178) المادة (26) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، والتي استبدلت بموجب المادة الأولى من المرسوم بقانون اتحادي رقم 2 بتاريخ 2018/7/24م.

للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة،ويعاقب بالعقوبة ذاتها كل من روَّج أو حرَّض على أي من الأفعال المذكورة أو سهلها للغير"[179]. و"يعاقب بالحبس والغرامة التي لا تقل عن مئتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من دعا، أو حرَّض عن طريق نشر معلومات على الشبكة المعلوماتية، أو وسيلة تقنية معلومات إلى عدم الانقياد إلى القوانين والأنظمة المعمول بها في الدولة"[180].

كما "يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ، أو أدار موقعًا إلكترونيًّا، أو أشرف عليه، أو استخدم الشبكة المعلوماتية، أو وسيلة تقنية معلومات؛ للتخطيط، أو التنظيم، أو الترويج، أو الدعوة لمظاهرات، أو مسيرات، أو ما في حكمها بدون ترخيص من السلطة المختصة" [181].

و ترى الباحثة أن المشرع قد شدد العقوبات على جرائم الإرهاب التي ترتكب باستخدام الوسائل الإلكترونية، بوصفها من الجرائم الماسة بالنظام والأمن العام، كالنص على عقوبة السجن المؤبد على كل من أنشأ، أو أدار، موقعًا إلكترونيًّا، أو أشرف عليه، أو نشر معلومات على الشبكة المعلوماتية، أو وسيلة تقنية معلومات، تهدف أو تدعو إلى قلب أو تغيير نظام الحكم في الدولة، أو الاستيلاء عليه، أو إلى تعطيل أحكام الدستور، أو القوانين السارية في البلاد، أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة؛ مراعيًا في ذلك التطور في استخدام وسائل التكنولوجيا والاتصالات

---

(179) المادة (30) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(180) المادة (31) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(181) المادة (32) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

الحديثة في ارتكاب هذه الأفعال التي تهدد الاستقرار والأمن المجتمعي، وهو مظهر من مظاهر التشدد في العقوبات السالبة للحرية، يمكن من خلالها تحقيق أهداف العقوبة في الزجر والردع.

إضافة إلى ما تضمنه المرسوم بقانون رقم 5 لسنه 2012م بشأن المصادرة للأجهزة والبرامج التي ارتكبت الجرائم من خلالها، حيث نصت المادة (41) منه على أنه "مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادره الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون، أو الأموال المتحصله منها، أو محو المعلومات أو البيانات،أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم؛ وذلك إما إغلاقًا كليًّا، أو للمدة التي تقدرها المحكمة"[182].

مفاد ذلك أن الحكم الخاص بالمصادرة لا يطبق إلا على شخص الجاني؛ طبقًا لمبدأ شخصية العقوبة، فلا تطبق المصادرة على الغير من حسني النية، وقد نص قانون العقوبات الاتحادي بشأن المصادرة على أن "تحكم المحكمة عند الحكم بالإدانة بمصادرة الأشياء والأموال المضبوطة التي استعملت في الجريمة، أو كان من شأنها أن تستعمل فيها، أو كانت محلًا لها، أو التي تحصلت منها، فإذا تعذر ضبط أي من تلك الأشياء أو الأموال حكمت المحكمة بغرامة تعادل قيمتها؛ وذلك كله دون الإخلال بحقوق الغير حسن النية"[183].

وتأييدًا لذلك قضت المحكمة الاتحادية العليا بأن: "المصادرة هي نقل ملكية مال أو أكثر إلى الدولة، وذلك بعد ضبط تلك الوسائل المعينة على ارتكاب الجريمة، وبالتالي فإنها عقوبة لا يقضي بها

(182) المادة (41) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

(183) المادة (82) من قانون القانون الاتحادي رقم 3 لسنة 1987م، بشأن إصدار قانون العقوبات

بحسب القاعدة العامة إلا إذا كان الشيء موضوع المصادرة قد سبق ضبطه على ذمة الفصل في الدعوى"[184].

وقضت أيضًا: "بتغريم كل متهمة عشرة آلاف درهم ومصادرة جهاز البلاك بيري الخاص بها"[185].

وترى الباحثة أن المشرع الاتحادي ضمّن المرسوم بقانون رقم 5 لسنة 2012م العديد من مظاهر التشدد في كل ما من شأنه أن يمس ويهدد سلامة واستقرار الأمن الداخلي؛ سواء فيما يتعلق بالعقوبات السالبة للحرية، أو الغرامات المالية، تحقيقًا للردع العام والردع الخاص، حيث أشار المشرع إلى أن هناك طائفة من مرتكبي هذه الجرائم ليست لديهم أهداف إرهابية أو خطورة إجرامية، وإنما يسعون لارتكاب هذه الجرائم من باب إثبات الذات والتحدي، الأمر الذي يقتضي معالجتهم فكريًّا ونفسيًّا، من خلال تدابير الخدمة المجتمعية، وذلك عندما أجاز للمحكمة في غير حالات العود بدلًا من الحكم بالعقوبة المشار إليها في الفقرة الثانية من المادة (26) أن تحكم بإيداع المتهم إحدى دور المناصحة، أو الحكم بوضعه تحت المراقبة الإلكترونية، ومنعه من استخدام أيّا من وسائل تقنية المعلومات خلال فتره تقدرها المحكمة، على ألا تتجاوز الحد الأقصى للعقوبة المقررة.

كما ترى أنه أشار أيضا إلى مظاهر التشدد في عقوبة الغرامة المالية، وذلك فيما ورد في المادة (26) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، والتي استبدلت بموجب المادة الأولى من المرسوم بقانون اتحادي رقم 2 بتاريخ 2018/7/24م.

حيث تجاوز فيها المشرع ما نصت عليه القواعد العامة في الغرامة المالية، في شأن الجنايات حيث

---

(184) الطعنان 289، 307 لسنة 2011م جزائي، جلسة 2012/2/21م، المحكمة الاتحادية العليا، أحدث إجتهادات المحكمة الإتحادية العليا، (https://www.moj.gov.ae/ar/about-moj/union-supreme-court/e-) ، تاريخ الإطلاع 2021/4/10.

(185) الطعن رقم 345 لسنة 2013م جزائي، جلسة 10 /2013/12م، المحكمة الاتحادية العليا، أحدث إجتهادات المحكمة الإتحادية العليا، (https://www.moj.gov.ae/ar/about-moj/union-supreme-court/e-) ، تاريخ الإطلاع 2021/4/10.

وضع حدًّا أعلى لا يجاوز أربعة ملايين درهم، وحدًّا أدنى لا يقل عن مليوني درهم،وهذا التجاوز في حدود ما هو منصوص عليه في قانون العقوبات الاتحادي، حيث تنص المادة (71 ق.ع)على أنَّ: "عقوبة الغرامة هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى علىمليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح؛ وذلك كله ما لم ينص القانون على خلافه".

الفرع الثاني

الإجراءات الخاصة التي اتخذتها الإمارات بصدد مكافحة جرائم تقنية المعلومات وجرائم الإرهاب

اتخذت دولة الإمارات عددًا من التدابير الخاصة بنظام الذخائر والأسلحة، حيث تشددت في الرقابة على المتعاملين والأسلحة والذخائر وجميع الموادالخطرة، من حيث التصدير والاستيراد والاستعمال والنقل والتداول والاتجار، فأصدرت المرسوم بقانون رقم 5 لسنة2013م بشأن الأسلحة والمتفجرات والذخائر والعتاد العسكري، مبينًا ضوابط تصديرها، واستيرادها، ونقلها، وتخزينها، واستعمالها،والاتجار بها؛ فلا يجوز لأي شخص معنوي أو طبيعي اقتناء أي سلاح ناري، أو مواد متفجرة، أو ذخائر،أو الاتجار بها، بأي صورة إلا بناء على ترخيص صادر له من السلطةالمختصة بمنح الترخيص وفقًا للقانون.

وقد أفاد التقرير الخاص بدولة الإمارات إلى لجنة الإرهاب والمتابعة في مجلس الأمن، أن الدولة قد اتخذت العديد من التدابير اللازمة لتقييد جميع المواد الخطرة التي تتضمن المتفجرات بجميع أنواعها وأشكالها لدى سلطات الجمارك في الدولة، وشددت الرقابة على تصدير واستيراد المواد الكيماوية التي يمكن استخدامهافي أسلحةالدمار الشامل[186].

(186) عبدالمجيد مراد داد محمد أحمد، **المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي**، مرجع سابق، ص66/65.

كما أنشأت السلطات الإماراتية قاعدة بيانات ومعلومات متطورة؛ لحصر العناصر الإرهابية والمتطرفة في الخارج والداخل، ومعرفة الخلايا والجماعات التي تدعمها ومخططاتها وأهدافها، كما تعمل السلطات على تسهيل الإجراءات الخاصة بتبادل المعلومات، بصورة سرية وعاجلة بين الأجهزة الأمنية المعنية على مختلف الأصعدة، وتشجيع ودعم البحوث الأمنية ومراكز الدراسات والبحوث، وحثها على دراسة الإرهاب؛ للتعرف على أساليبه، وأسبابه، والآثار الناجمة عنه، وكيفية مواجهته، ودراسة ما يقع من أعمال إرهابية؛ لاستخلاص أوجه القصور في المواجهة، والاستعداد لتحقيق التطور والتقدم المستمر في هذاالمجال[187].

(187)المرجع السابق، ص66/65.

المبحث الثاني

الإشكاليات الإجرائية في مواجهة الإرهاب الإلكتروني

تمهيد وتقسيم:

إن جرائم الإرهاب الإلكتروني التي يتم ارتكابها من خلال وسائل تقنية المعلومات، لها خصائص ذاتية وطبيعة خاصة، تختلف عن جرائم الإرهاب التقليدية من حيث طرق ووسائل ارتكابها؛ مما ينعكس على الإجراءات التي يجب على السلطات المختصة اتخاذها في سبيل ملاحقة مرتكبيها، الأمر الذي يقتضي الجوانب التي تحيط بهذه الإشكاليات كصعوبة جمع الأدلة وتتبع مرتكبي جرائم الإرهاب الإلكتروني، ثم دراسة القواعد الخاصة في الإثبات ومبدأ مشروعية الدليل؛ من خلال المطلبين التاليين:

المطلب الأول–صعوبة جمع الأدلة وتتبع المجرمين.

المطلب الثاني–الإثبات ومبدأ مشروعية الدليل.

المطلب الأول

صعوبة جمع الأدلة وتتبع المجرمين

يعدُّ مسرح الجريمة أو مكان وقوعها الميدان الأساسي لتحري وضبط الجريمة وملاحقة مرتكبيها، وينطبق ذلك على جرائم الإرهاب الإلكتروني، وإن كان مختلفًا عن مسرح الجريمة في صورتها التقليدية، حيث يعرف مسرح الجريمة عبر الفضاء الإلكتروني بأنه المسرح المعنوي أو التخيلي الذي يشمل كل مكان يتجول الشخص فيه بداخل الشبكة العنكبوتية، ويترك آثار بصماته المعنوية في الموقع الذي قام بزيارته، ويتم تحديد المكان الذي يدخل منه، والجهاز الذي يستخدمه، وتحديد العنوان IP الدائم له، ويتم من خلاله اكتشاف معلومات وبيانات المستخدم، ويكون بإمكان أي شخص تتبع

تحركات المجرم، حيث يقوم بذلك المتخصصون في مجال تقنية المعلومات، كما أن جهاز المجرم الشخصي يحتفظ بالملفات الخاصة بالكوكيز للمواقع التي دخلها [188].

إلا أن ذلك لا يكون بهذا القدر من السهولة، حيث يقوم المجرمون بوضع عدد من السياجات الأمنية على أفعالهم غير المشروعة، قبل ارتكابها حتى لا يقعون تحت طائلة الملاحقة والعقاب، من خلال التلاعب بالقوائم الموجودة في الأجهزة، وقواعد البيانات والبرامج؛ لأن البيانات تكون مكتوبة بطريقة رقمية لا يمكن معرفتها أورؤيتها، والقيام بالتشفير أو استخدام الرموز، كما يعمد المجرمون المتخصصون إلى محوالآثار الخاصة بهم؛ من خلال مسح ملفات الكوكيز الموجودة على الأجهزة الخاصة بهم[189].

ويعتمد الضبط الخاص بجريمة الإرهاب الإلكتروني على إجراءات جمع الأدلة الخاصة بها، حيث حدد المشرع الاتحادي الجهة المختصة بها في المادة (30) من قانون الإجراءات الجزائية الاتحادي رقم (35) لسنة 1992 وتعديلاته: "يقوم مأمورو الضبط القضائي بتقصيالجرائم، والبحثعن مرتكبيها، وجمع المعلومات والأدلة اللازمة للتحقيق والاتهام"[190].كما نصت المادة (49) من قانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012م المعدل على أن: "يكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفة مأموري الضبط القضائي في إثبات الأفعال التي تقع بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين؛ وذلك لتمكينهم من القيام بأعمالهم"[191].

---

(188) محمود صالح العادلي، مرجع سابق، ص142/141.

(189) شمسان ناجي صالح الخيلي، مرجع سابق، ص41. أيضًا محمد عبيد الكعبي، مرجع سابق،ص40.

(190) المادة (30) من قانون رقم 35 لسنة 1992م بشأن إصدار قانون الإجراءات الجزائية،

(191) المادة (49) من القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات، المعدل بالقانون رقم 2 لسنة 2018م.

وحيث إن هناك عددًا من القواعد والإجراءات الخاصة بجمع الأدلة في جرائم الإرهاب الإلكتروني؛ تشمل المعاينة، والضبط، والخبرة؛ لذا كان لزامًا على الباحثة بيانها على النحو التالي:

الفرع الأول

الخبرة والمعاينة في مجال جرائم الإرهاب الإلكتروني

انطلاقًا من التطور الحاصل في مجال تقنيه المعلومات تعدُّ الخبرة والمعاينة في مجال الإرهاب الإلكترونيمن أكبر العقبات والصعوبات التي تعترض غير المتخصصين في هذا المجال، وقد يؤدي ذلك إلى العجز عن كشف الغموض الخاص بهذا النوع من الجرائم الإرهابية، وجمع الأدلة المتعلقة بها،حيث إن المفهوم الخاص بالمعاينة يتمثل في الإجراء الذي يتم من خلاله الانتقال إلى مكان ارتكاب الجريمة لمشاهده آثارها، وتتضمن جمع أي شيء يفيد في كشف الجريمة والوصول إلى الجاني، ويتطلب ذلك إثبات حالة الأشياء والأشخاص الموجودة، ورفع الآثارالتي تتعلق بالجريمة، سواء كانت هذه المعاينة مكانية تتعلق بمكان ارتكاب الجريمة، أو شخصية تتعلق بشخص الجاني[192].

وتختلف المعاينة في جرائم الإرهاب الإلكتروني عن جرائم الإرهاب التقليدية، حيث إنها تواجه العديد من التحديات والصعوبات؛ فهي نادرًا ما تخلف آثارًا مادية بعد ارتكابها، فمرتكبو هذه الجرائم على درجة عالية من الدقة، كما أن الفترة الزمنية بين وقوع الجريمة وبين اكتشافها قد تطول؛ مما يعرضالدليل للتلف،إضافة إلى أن عملية استخلاصالدليل في مجال جرائم الإرهاب الإلكتروني قد تواجه نقص الخبرة المطلوبة من حيث الإلمام بالجرائم التي تتم عبر الفضاء الإلكتروني باستخدام وسائل التكنولوجيا الحديثة، وكيفية التعامل معها، كما قد يرجع إلى الثقافة الأمنية أو الحركة التشريعية بخصوص التي لا تسير بمعدل التطور والتقدم الخاص بهذا النوع من الجرائم[193].

---

(192)عبدالله دغش العجمي،مرجع سابق،ص78/77.

(193) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص127/126.

لذا يتعين عند اللجوء إلى المعاينة بعد وقوع جرائم الإرهاب الإلكتروني الالتزام بما يلي[194] :

اولا:–قصر المعاينة على المحققين والباحثين الذين تتوافر لديهم الخبرة الكافية في مجال تقنية المعلومات.

ثانيا:– تصوير جهاز الحاسب الآلي والأجهزة الطرفية التي تتصل به، على أن يُسجل مكان وتاريخ التقاط كل صورة من هذه الصور.

- إثبات حالة الكابلات والتوصيلات المتصلة بمكونات النظام؛ حتى يمكن إجراء عمليات التحليل والمقارنة عند عرض الأمر على المحكمة.

ثالثا:– ملاحظة الطريقة التي أعد النظام بها، والحرص على عدم نقل أي مواد معلوماتية أوبيانات من مسرح الجريمة، إلا بعد إجراء الاختبارات والتأكد من خلو المحيط الخارجي الخاص بموقع الحاسب من أي نطاق خاص بقوى مغناطيسية يمكن أن تكون السبب في محو جميع البيانات المسجلة.

رابعا:– التحفظ على المخرجات الورقية الخاصة بالحاسب ذات صله بالجريمة، فضلًا عن مستندات الإدخال؛ لرفع البصمات التي قد توجد عليها.

خامسا:–التحفظ على المعلومات الخاصة بسلة المهملات من أوراق الكربون المستعملة أو الأوراق الممزقة أو الملقاة أو الأقراص الممغنطة غير السليمة، والعمل على فحصها.

وقد يقتضي الأمر فيما يتعلق بالخبرة الاستعانة بخبير لتقديم المعلومات المطلوبة في مجال جرائم الإرهاب الإلكتروني وتشغيل النظام، وفقًا للطريقة التي تطلبها جهة التحقيق، فقد تريد إرسال المعلومات والبيانات على ورق، أو على أقراص ممغنطة، أو مسجلة على ديسك، من خلال إرسال الأشياءالتي يتطلب بيانها والكشف عنها إلى الخبير للبحث عنها، فالمعلومات الخاصة بجرائم الإرهاب الإلكتروني

(194) محمود صالح العادلي،مرجع سابق،ص48/47.

تكون مرسلة غالبًا بطريقة مختلفة عن الطرق العادية في الإرسال، وقد تكون مشتملة على ألغاز أو مشفرة؛ مما يتطلب نوعًا خاصًا من الخبرة بهذه الجرائم،إضافة إلى الخبرة التقنية.

وتعدّ الخبرة التقنية والفنية من أهم التحديات التي تواجه الخبراء في مجال جرائم الإرهاب الإلكتروني، كما يأتي عامل الوقت على رأس الصعوبات التي تواجه الخبرة في مجال الإرهاب الإلكتروني؛ لسرعة اتمامها، فقد تمحى البيانات والمعلومات الإلكترونية دون تحديد زمن معين، ومن ثمّ يتعيّن على الخبير إنجاز المهمة المكلف بها، باقتفاء أثر الجريمة؛ مثل معرفة عنوان البريدالإلكتروني الخاص بالجاني، أو معرفة (IP) الخاص بالحاسب الآلي الذي ارتكبت الجريمة من خلاله، إلى غير ذلك من الآثار الخاصة بارتكاب الجريمة، في الوقت المحدد وبسرعة فائقة.

وتجدر الإشارة إلى أن الالتزام الخاص بالخبير هو التزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة؛ نتيجة الصعوبات والعقبات التي واجهته،أو نتيجة ضعف خبرته،خلافًا لمسؤوليته في حالة إتلاف البيانات المسؤول عنها، أو رفض المهمة المكلف بها[195].

استنادًا لما تقدم يمكن إيجاز الإجراءات الخاصة ببرامج التتبع والإرشاد الجنائي عبر الحاسب الآلي، التي يمكن استخدامها في كشف جرائم الإرهاب الإلكتروني وفق الآتي:

- **نظام الإرشاد الجنائي:**

تستخدم عدد من المؤسسات الضبطية في العالم النظام الخاص بالإرشاد الجنائي عبرالإنترنت، عن طريق تجنيد الغير، أو دفع العناصر الخاصة بها للدخول في قاعات البحث وحلقات النقاش، أو استخدام برمجيات الاتصال المستقلة والمباشرة، والدخول إلى قاعات الدردشة، بأسماء وصفات وهمية؛ بحثًا عن مرتكبي تلك الجرائم، ويستطيع مأمور الضبط القضائي القيام بهذا الأمر بنفسه من خلال

(195)محمد عبدالفتاح عبدالمقصود علي، **القواعد الإجرائية للجرائم التي تقع عبر شبكة الإنترنت**، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، 2015م، ص334. أيضًا- عبدالله دغش العجمي، مرجع سابق،ص78/77.

الحصول على إذن رسمي بمباشرة مهامه الخاصة بذلك عبر الإنترنت، وهذا الإذن الرسمي الذي يحصل عليه مأمور الضبط لا بد أن يكون متضمنًا عددًا من المعلومات؛ تتمثل في رقم الحاسب، وصلاحيته للعمل، واحتوائه على البرمجيات الأصلية وليس المنسوخة، ورقم وتاريخ الترخيص، والجهةالخاصة بالإصدار، وغير ذلك من البيانات والمعلومات اللازمة لاكتشاف جرائم الإرهاب الإلكتروني.

وتجدر الإشارة إلى أن المهمة الخاصة بمأمورالضبط تكون حول التقصي عن المعلومات المباشرةوالخاصة بالجرائم أثناء التواصل مع الغير، وليس دفع الغير على ارتكاب الجرائم، حيث يقوم بالحديث عن بث الفيروسات والاختراق...وغيرذلك من الأفعال والسلوكيات الخاصة بمجال الإرهاب الإلكتروني، حتى يكتشف المشروع الإجرامي، حيث يقوم المرشد الجنائي بتوصيل المعلومات والبيانات التي حصل عليها، وتوصيلها إلى جهة الضبط القضائي؛ لمباشرة العمل الخاص بها في كشف الجريمة وضبط الجاني[196].

- **برامج التتبع وكشف الاختراق:**

يقصد ببرامج التتبع" البرامج التي يكون الغرض منها اقتفاء الأثر الخاص بالقراصنة الذين يحاولون اختراق الأجهزة والأنظمة المعلوماتية، والقيام بأفعال وجرائم إرهابية وتدميرية، من خلال معرفة (IP) الخاص بالحاسب الآلي الذي حاول اختراق النظام، والاسم الخاص بمزود الخدمة الذي قام المخترق من خلاله بالدخول، وهذه البرامج تساعدفي تحديد مخترقي الأنظمة المعلوماتية، والمواقع الإلكترونية، والتعرف على المحاولات الخاصة بالاختراق، إضافة إلى إشعار الجهة المتضررة من هذا الاختراق بهذه العملية، وتعمل هذه البرامج أثناء محاولة الاختراق أو القرصنة، حيث يسارع جهاز الحاسب الآلي

(196)طارق فوزي الفقي، مرجع سابق، ص54/53.

بإغلاق منافذ الدخول أمام المخترق، والبدء في عملية المطاردة واقتفاء أثرمرتكبي عمليات الاختراق؛ حتى يصل إلى الجهاز الذي تمت العملية من خلاله"[197].

أما فيما يتعلق ببرامج الاختراق فهذه البرامج تحلل وتراقب العمليات الخاصة بالتعامل الإلكتروني مع أجهزة الحاسبوشبكة الإنترنت؛ لتقوم بالرصد المبكرلأي إتلاف أو اختراق يمكن أن يمثل تهديدًا إلكترونيًّا،يتم من خلاله ارتكاب الجرائم الإرهابية، وتجري هذه العملية من خلال تحليل المعلومات والبيانات عند انتقالهاعبرشبكة الإنترنت، ومراقبة الملفات الخاصة بالتشغيل، وإجراء المقارنة الخاصة فيما يتعلق بنتائج التحليل، ومجموعة من الصفات التي تشترك في الاعتداء على الحاسب الآلي،حيث يوجه إخطارًاإلى مدير النظام في حالة حدوث اعتداء على النظام، وتسجيل البيانات والمعلومات الخاصة بهذا النظام في سجلات خاصة[198].

وترى الباحثة أن إجراءات المعاينة والخبرة الجنائية الخاصة بجرائم الإرهاب الإلكتروني التي ترتكب عبرشبكة الإنترنتلا تقتصر على تدريب الأشخاص القائمين على الخبرة الجنائية؛ بل يحتاج الأمر إلى إدارة خاصة يعمل بها أشخاص متخصصون في مجال تقنية المعلومات يتمتعون بالضبطية القضائية.

الفرع الثاني

التفتيش والضبط في مجال جرائم الإرهاب الإلكتروني

يقصد بالتفتيش البحث عن الشيء الذي يتصل بالجريمة التي وقعت، بما يفيد في كشف الحقيقة عنها، وعن شخص مرتكبها، كما يقصد بالتفتيش أيضًا الوسيلة الخاصة بالإثبات المادي؛ فالتفتيش

(197)المرجع السابق، ص331.

(198) المرجع السابق، ص331.

ليس غاية في حد ذاته، إنما هو إجراء يتخذ بهدف ضبط الأشياء المادية التي تتعلق بالجريمة التي ارتكبت[199].

وهناك شروط خاصة بالتفتيش تتضمن شروطًا موضوعية؛ تتمثل في وقوع جريمة بالفعل تعد جنحة أو جناية، وتوجيه اتهام للشخص الذي يراد تفتيشه، بهدف الحصول على أشياء تساعد في الكشف عن الجريمة.

كما يتضمن شروطًا شكلية تتمثل في أن يكون الإذن بالتفتيش مسببًا، وتحرير محضر بالتفتيش، وحضور المتهم أو من ينيبه، أو شخص من الغير، أو من ينيبه، كما تتضمن الإجراءات الخاصة بالتفتيش شبكات المعلومات، وقد يتجاوز هذا الأمر النظام المشتبه به ويمتد إلى نظام آخر، مما يثيرعددًا من التحديات؛ تتمثل في مدى مساس هذا الإجراء بحقوق الخصوصية المعلوماتية، ومدى قانونية هذا الإجراء[200].

أما فيما يتعلق بالتفتيش في مجال جرائم الإرهاب الإلكتروني فيواجه العديد من التحديات، حيث يثار التساؤلحول مدى صحة اعتبار البحث والتفتيش عن الأدلة الخاصة بجرائم الإرهاب الإلكتروني في شبكات الاتصال ونظم الحاسبات نوعًا من أنواع التفتيش؛ نظرًا لأن البيانات الإلكترونية لا يكون لها مظهر مادي ملموس،ومن ثمَّلا بد من التفرقة بين حالتين؛ تتمثل الأولى منهما في الحالة التي يكون فيها محل التفتيش المكونات المادية للحاسب، أما الثانية فيكون محل التفتيش فيها البيانات الإلكترونية؛ ويمكن تفصيل ذلك فيما يلي:

اولا:- مدى خضوع (مكونات الحاسب المعنوية)البيانات الإلكترونية للتفتيش في مجال جرائم الإرهاب الإلكتروني:

---

(199) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص127/126.

(200)عبدالله دغش العجمي،مرجع سابق،ص81.

ثار الخلاف حول مدى صحة أو جواز تفتيش(المكونات المعنوية للحاسب)البيانات الإلكترونية، فذهب البعض إلى القول بأنه إذا كان الغرض من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم الخاص بهذا الغرض وهو المفهوم المادي لا يشمل البيانات الإلكترونية الخاصة بالحاسب، بينما ذهب البعض الآخر إلى القول بأنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم الخاص بهذا الغرض وهو المفهوم المادي يشمل جميع البيانات الإلكترونية الخاصة بالحاسب بمختلف أشكالها(201).

ثانيا:- مدى خضوع مكونات الحاسب المادية للتفتيش في مجال جرائم الإرهاب الإلكتروني:

يتوقف القول بجواز تفتيش المكونات المادية الخاصة بالحاسب الآلي على طبيعة الحيّز أوالمكان الموجودة فيه، بوصف هذا المكان بأنه مكانعام أم خاص، فالصفة لها أهمية خاصة في مجال تفتيش المكونات المادية للحاسب الآلي، فيحكمها إذا كانت موجودة في مكانعاما يحكم المكان العام،ويتوقف مدى جواز التفتيش على الحالات التي يجوز فيها التفتيش وفق القيود المنصوص عليها في هذا النطاق، أما إذا كانت موجودة في مكان خاص تأخذ حكمه؛ فلا يمكن تفتيشها إلا في الحالات التي يجوز فيها تفتيش المكان الخاص، وفق الضمانات والقيود الواردة بشأنه، وتجدر الإشارة إلى أن الوسائل المادية؛ كالأقراص الصلبة، والأشرطة الممغنطة، والبيانات المخزنة في أوعية تخضع جميعها للتفتيش(202).

---

(201) محمد صلاح محمد عبدالمنعم، مرجع سابق، ص211 .سوزان عدنان الأستاذ، **انتهاك حرمة الحياة الخاصة عبر الإنترنت، دراسة مقارنة**، مجلة جامعة دمشق للعلوم الاقتصادي والقانونية، المجلد 29، ع3، 2013م، ص448.

(202) محمود صالح العادلي،مرجع سابق،ص149.محمد صلاح محمد عبدالمنعم، مرجع سابق، ص210.

وترى الباحثة أن البيانات الموجودة في الفضاء الإلكتروني المتمثلة في النبضات الإلكترونية تكون قابلة للتخزين على وسائط مادية؛ كالأشرطة الممغنطة، والأسطوانات، والأقراص، والتخزين على الأوعية،كما يمكن قياسها وتقديرها، وانطلاقًا من أن ليس لها مظهر مادي ملموس فإن التفتيش الخاص بها يرد على هذه البيانات ثم حفظها وتخزينها من خلال تحويلها إلى وسائط إلكترونية، ومن ثمَّ تصلح لإجراء التفتيش،حيث إن الهدف من التفتيش هو الوصول إلى الحقيقة والأدلة؛ من أجل حماية مصالح المجتمع الجديرة بالحماية.

أما فيما يتعلق بالضبط فيقصد بهالإجراء القانوني الذي يتمثل في الحصول على الأدلة الخاصة بالجريمة، ووضع كل ما يحتمل أن يكون قد نتج عن الجريمة أو استعمل في ارتكابها، أو أي شيء من الأشياء التي وقعت عليها الجريمة، التي يباشر التحقيق بشأنها والتحفظ عليها.

فالضبط هو الهدف من التفتيش والنتيجة المباشرة له، ويتمثل في الحصول على الأدلة التي تفيد في الكشف عن الجريمة، ومن ثمَّ لابد من توافر الشروط والضوابط القانونية بهذا الإجراء، كما يتعين على مأمور الضبط القضائي تسليم الشيء الذي يحصل عليه للمحقق؛ لاستكمال إجراءات التحقيق والكشف عن الجريمة، وهذا الإجراء لا يتوقف على جهاز الحاسب الآلي؛ بل يمتد أيضًا ليشمل مختلف الأجزاء الخاصة به[203].

وتجدر الإشارة إلى اختلاف الضبط في مجال جرائم الإرهاب الإلكتروني عن الضبط الذي يتم في مجال جرائم الإرهاب التقليدية، حيث تواجه هذا الأخير العديد من التحديات والصعوبات في مجال ضبط البيانات المعالجة إلكترونيًّا، تتمثل في[204]:

---

(203)عبدالله دغش العجمي، مرجع سابق،ص81.

(204)محمد صلاح محمد عبدالمنعم،مرجع سابق، ص241. عبدالله دغش العجمي، المرجع السابق،ص81.

- ضرورة وجود أدوات معينة تتناسب مع سرعة الإخفاء والمحو التي تواجه الدليل؛ ومن هذه الأدوات: أدوات المراجعة، وبرامج الحماية، وأدوات مراقبة المستخدمين للشبكة، والتقارير التي تنتجها نظم أمن البيانات والمعلومات، إضافة إلى أدوات التصنت على الشبكة، والمراجعة الخاصة بقاعدة البيانات، والتسجيل وبرامج النسخ، وغير ذلك من أدوات الضبط، كما أنه يمكن استخدام الأدوات التي تم استعمالها في الجريمة؛ مثل الأدوات الخاصة بجمع المعلومات والبيانات عن الزائرين للمواقع، كبرمجيات كوكيز وغيرها من البرامج،التي تتطلب خبرة تقنية في مجال جرائم الإرهاب الإلكتروني.

- وجود هذه البيانات في أجهزة أو شبكات تابعة لدولة أجنبية،مما يستدعي التعاون مع الجهات الخاصة بالتحقيق والشرطة، في العمليات الخاصة بالضبط والتفتيش والتحفظ.
- الحجم الخاص بالشبكة الذي يحتوى على المعلومات المعالجة إلكترونيًّا،التي يطلب ضبطها من خلال البحث في نظام إلكتروني خاص بشركات متعددة.
- إن الضبط والتفتيش في العديد من الأحيان قد يمثل اعتداء على حرمة الحياة الخاصة أو حقوق الغير، مما يقتضي مراعاة الضمانات والإجراءات اللازمة للحفاظ على حماية هذه الحقوق والحريات من الاعتداء عليها.

المطلب الثاني

الإثبات ومبدأ مشروعية الدليل

تعدّ المستندات من الأدلة الهامة التي يلجأ إليها القاضي الجنائي في الإثبات، ومن ثَمَّ فهي تخضع لتقدير المحكمة، وهناك نوعان من أدلة الإثبات؛ أحدهما يتمثل في الأدلة التقليدية وتشمل الخبرة، وشهادة الشهود، والأدلة المادية، وغير ذلك من أنواع الأدلة التقليدية، والنوع الثاني الأدلة الرقمية، وتختلف الأخيرة عن الأدلة التقليدية من حيث درجة قبولها وسلامتها، فجرائم الإرهاب الإلكتروني تترك آثارًا وبصماتٍ رقمية غير مرئية، أو تكون مرئية على وجه افتراضي، خلافًا للأدلة التقليدية لجرائم الإرهاب التقليدي،التي تترك آثارًا مادية(205).

وبغية التعرف على مبدأ مشروعية الدليل الرقمي، لا بد من تعريف الدليل الإلكتروني الرقمي،وبيان أنواعه، وتحديد طبيعته التي تختلف عن الأدلة التقليدية، ثم بيان التحديات والصعوبات التي تواجه الإثبات من خلاله في جرائم الإرهاب الإلكتروني،وبيان دوره ومشروعيته في إثبات هذا النوع من الجرائم.

الفرع الأول

تعريف الدليل الرقمي وأنواعه في مجال جرائم الإرهاب الإلكتروني

يُعرف الدليل الرقمي بأنه الدليل الذي يجد أساسه في العالم الافتراضي، ويدل على وقوع جريمة الإرهاب الإلكتروني، فهو ثمرة الاستعانة بالتكنولوجيا الخاصة بالمعالجة التقنيّة للمعلومات، ويؤدي إلى الاقتناع بارتكاب الشخص لجريمة محددة عبر شبكة الإنترنت أو تقنية المعلومات، حيث تحول الدليل

(205) مصطفى عبد الباقي، **التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين**، دراسة مقارنة، دراسات علوم الشريعة، المجلد 45، ع4، ملحق 2، 2018م، ص292.عبد الله دغش العجمي،مرجع سابق،ص76.

من الدليل الصامت الذي كان يشارإليه في مجال جرائم الإرهاب التقليدية كالوثائق، والمستندات، وغيرها، إلى الدليل الرقمي في مجال جرائم الإرهاب الإلكتروني الذي يقتضيه المنطق،ويعبر عن التطور الذي تنتجه وسائل تقنية المعلومات،فيما يمكن وصفه بالمظهر التقني المعلوماتي الذي يتسم بالذكاء والحركية[206].

كما عرفت المنظمة العالمية لدليل الكمبيوتر الدليل الرقمي عام 2001م، بأنه "المعلومات المنقولة أو المخزنة التي يمكن الاعتماد عليها أمام المحكمة، أو المعلومات ذات القيمة المخزنة، أو المحتملة، أو المنقولة في صورة رقمية"[207].

وتجدر الإشارة إلى أن الأدلة في مجال الإرهاب الإلكتروني تشمل نوعًا آخر من الأدلة غير الأدلة الرقمية، وهي الأدلة المادية المتمثلة في الجهاز الخاص بالحاسب الآلي وملحقاته؛ والطابعات التي تطور استخدامها،الأمر الذي يقتضي أن يكون لدى الخبير الفني أو مأمور الضبط الخبرة الكافية والإلمام الوافي ببياناتها وآلية عملها، كما تشمل الأدلة المادية المودم، وجهاز الهاتف النقال، والفلاش ميموري، والأوراق الخطية الخاصة بالإدخال في الحاسب، والبرامج التي توجد مع الحاسب الآلي الرقمي،إضافة إلى المستندات سواء كانت إدارية، أو قانونية محفوظة في النظام الخاص بالمعلومات الإدارية الدفترية، وغير ذلك من الأدلة المادية[208].

وتجدر الإشارة أيضًا إلى وجود نوعين من الأدلة الرقمية أحدهما يتمثل في الدليل الذي لا يمكن صنعه أو إنشاؤه؛ مثل ملفات تعريف الارتباط، وملفات التسجيل، وبيانات التعريف والعناوين،

---

(206)فتحي محمد أنور عزت، الأدلة الإليكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دون دار نشر، ط2، 2010م، ص635. مصطفى عبد الباقي، مرجع سابق، ص292.

(207)مصطفى محمد موسى، **التحقيق في الجرائم الإلكترونية**، دون دار نشر، 2009م، ص213.

(208)مصطفى محمد موسى، مرجع سابق، ص213/212.

وهذا النوع يتضمن معلومات وأشكال وبرامج عديدة؛ منها برامج الدردشة والمواقع الإلكترونية، والبريد الإلكتروني.

أما النوع الثاني فيتمثل في البيانات التي تكون مخزنة على الجهاز؛ وتتمثل في برامج العرض، وملفات الوورد، والصور، وهذا النوع من الأنواع المرئية التي يمكن عرضها وطباعتها[209].

الفرع الثاني

طبيعة الدليل الرقمي في جرائم الإرهاب الإلكتروني

هناك تمييز حقيقي بين طبيعة الدليل الرقمي في جرائم الإرهاب الإلكتروني وطبيعة الدليل المادي في جرائم الإرهاب التقليدي، فالأولى ليست سوى تعداد غير محدود لأرقام ثنائية، خلافًا للثانيةالتي تعبر عن وضعية ملموسة، يكون لها طابع مادي متميز، والدليل في القانون لا يتخذ طابعًا نموذجيًّا أو موحدًا يجب تطبيقه في جميع الأحوال؛ بل يتسم بالتنوع نظرًا لتوافقه مع الجريمة والواقعة المرتكبة، ومن ثمَّ تبقى الطبيعة الخاصة بالدليل عبر الإنترنت مثارًا للتساؤلات.

فطبيعة الدليل الرقمي لها طابع افتراضي لا يمكن أن يرتقي إلى المستوى الخاص بطبيعة الدليل المادي، الأمر الذي جعل النظام الاتهامي يبنى على قاعدة مدى إمكانية قبول الدليل الناتج عن جهاز الحاسب الآلي، ففي كثير من الحالات ترفض مخرجات الحاسوب عبر الطابعة؛ لكونها دليلًا يستمد من آلة تتمثل مهامها في إعداد تسلسل خاص بالأوراق، فضلًا عن أن الدليل الإلكتروني دليل

(209)مصطفى عبدالباقي، مرجع سابق، ص292.

مستوحى من قاعدة مجهولة، يمكن للجاني إزالته وإلغاؤه بطريقة أو بأخرى، ومن ثمَّ يكون ما تبقى منه هي النسخة المتحصل عليها من خلال المراقبة الإلكترونية[210].

الفرع الثالث

التحديات والصعوبات التي تواجه الإثبات في جرائم الإرهاب الإلكتروني

هناك العديد من التحديات والصعوبات التي تواجه عمليه الإثبات في مجال جرائم الإرهاب الإلكتروني؛ نظرًا لكونها من الجرائم التي ترتكب باستخدام الشبكات الإلكترونية من قبل أشخاص على درجة فائقة من الذكاء، إضافة إلى وجودعدد من الأسباب التي تؤدي إلى صعوبة الإثبات تتمثل فيما يلي[211]:

اولا:- فقدان وانعدام الآثار التقليدية لجرائم الإرهاب التي يتم ارتكابها عبر الفضاء الإلكتروني؛ نظرًا للطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم،حيث لا تترك أي آثار، فجرائم الإرهاب الإلكتروني لا تترك آثارًا مادية أو خارجية تدل على شخص مرتكب الجريمة، فتقع دون الشعور بارتكابها من خلال الأجهزة المعلوماتية؛ مثل جرائم التجسس التي تقع من خلال اعتراض النبضات الإلكترونية، وفيما يتعلق بالجماعات والمنظمات الإرهابية عبر شبكة الإنترنت فإن الشبكة توفر لهم من خلال البريد الإلكتروني، والمنتديات وغرف الدردشة مجالًا يمكن فيه إخفاء هويتهم بحيث يصعب التعرف على الأشخاص الذين يختفون وراء هذه الشخصيات، ويستفيدون من عدم وجود آثار تقليدية

---

(210)فتحي محمد أنور عزت، مرجع سابق، ص638/637.

(211) المختار لمجيدري، **الإرهاب الإلكتروني، إشكاليات الإثبات الجنائي والقضاء عليه**، مجلة العلوم السياسية والقانون، المجلد 3، المركز الديمقراطي العربي، ألمانيا، 2019م، ص276/266. نبيلة هبه هروال، مرجع سابق، ص40. سليمان أحمد فضل،مرجع سابق، ص383محمود صالح العادلي،مرجع سابق،ص94. شمسان ناجي صالح الخيلي، مرجع سابق، ص39.محمد عبيد الكعبي،مرجع سابق، ص41.

لارتكاب هذه الجرائم،فدليل ثبوت هذه الجرائم يعتمد على البيانات أو الأرقام التي يمكن محوها أو حذفها من السجلات المخزنة في الحاسوب؛ ومن ثمّ لا يكون لها آثار مادية ما يؤدي إلى صعوبة اكتشافها.

ثانيا:- سرعة غياب الدليل المرئي حيث تأخذ المعلومات والبيانات التي يتم تداولها عبر شبكة الإنترنت والوسائل الإلكترونية شكل رموز تخزن على وسائط ممغنطة لا يمكن أن تقرأ إلا من خلال الحاسب الآلي، مما يجعل الوصول إلى الدليل الذي يمكن من خلاله اكتشاف مرتكبي هذه الجرائم أمرًا غاية في الصعوبة.

حيث ينعدم الأثر المادي لتلك الجرائم، كما أنه لا يتخلف عنها أي كتابة، مما يؤدي إلى إخفاء الجريمة، وغياب الدليل المرئي، إضافة إلى وجود العديد من المكونات التقنية التي تمثل خطرًا كبيرًا على المعلومات والبيانات؛ مثل وجود مجال مغناطيسي يستخدم في محو وإزالة البيانات.

كما يتعمد مرتكبو جرائم الإرهاب الإلكتروني تدمير البيانات والمعلومات التي يمكن استخدامها كدليل في الإثبات، إضافة إلى ما يتطلبه موقع الجريمة من فحص دقيق من قبل الأشخاص المختصين في هذا المجال؛ للوقوف على أي دليل يمكن من خلاله معرفة مرتكبي هذه الجرائم، مما يقتضي فحصًا كاملًا لعدد من البيانات والوثائق، كما يتطلب تكلفة مادية عالية بسبب غياب أونقص الخبرة لدى الجهات القضائية والأمنية في هذا المجال.

ثالثا:- تتطلب جرائم الإرهاب الإلكتروني حرفية فائقة وتقنية عالية لاكتشافها،مما يؤدي إلى صعوبة التحقيق بشأنهامن خلال المحقق الذي اعتاد التحقيق بشأن جرائم الإرهاب التقليدية، إضافة إلى نقص الخبرة لديه فيالمجال الخاص بجرائم الإرهاب التي ترتكب عبر الفضاء الإلكتروني؛ لأن مجرمي الإرهاب الإلكتروني يغيرون آليات عملهم باستمرار.

رابعا:- البعد الدولي لجرائم الإرهاب الإلكتروني، قد يجري النفاذ في أحد البلدان في العالم، بينما يتم التلاعب بالبيانات في بلد آخر، وفي بعض الأحيان تسجل النتائج في بلد ثالث، كما أنه يمكن تخزين البيانات والأدلة في حاسوب موجود في بلد غير البلد الذيارتكبت الجريمة فيه، مما يستطيع معه الجاني أن يخفي هويته، وينقل البيانات من خلال قنوات متعددة في بلدان مختلفة، الأمر الذي يصعب على الجهات الأمنية والقضائية إثبات جرائم الإرهاب الإلكتروني، حيث يلعب البعد المكاني والزمني والقانوني لهذا النوع من الجرائم دورًاهامًّا في عملية التشتيت فيما يتعلق بالتنسيق الدولي لجهود التحري في تعقب مثل هذه الجرائم.

خامسا:- تشفير البيانات المنقولة عبر شبكات الاتصال، أو المخزنة إلكترونيًّا.

سادسا:- نقص الخبرة الفنية والتقنية والدراية الكافية لدى رجال الضبط الجنائي لطبيعة جرائم الإرهاب الإلكتروني،إضافة إلى أن السلطات الخاصة بالتحقيق والبحث والتحري لا يمكنها تطبيق الإجراءات التقليدية في مجال جرائم الإرهاب الإلكتروني؛ نظرًا لطبيعتها المستحدثة، واتصالها المباشر بمجال تقنية المعلومات والاتصالات.

سابعا:- تعتمد الأدلة الرقمية في مجال الإرهاب الإلكتروني في نجاحها على التقنيات الخاصة بالحاسب الآلي في استنتاج الحقائق، وتحليل القرائن، وحصر الأسباب والاحتمالات والفرضيات، وتعرف النتائج من خلال معاملات حسابية مخصصة لهذا الغرض، الأمر الذي يحتاج إلى خبرات كافية في هذا المجال.

ثامنا:- التحدي الذي يتعلق بطبيعة إعداد نظام الجهاز، وإعداد البرامج والذي يمثل العديد من المخاطر الفنية وعاملًا مؤثرًا في الإثبات من حيث الكتابة والمحتوى.

الفرع الرابع

دور الدليل الرقمي ومشروعيته في إثبات جرائم الإرهاب الإلكتروني

ستسلط الباحثة الضوء على مشروعية الدليل الرقمي في جرائم الإرهاب الإلكتروني، ثم تنتقل إلى بيان الدور الإيجابي للقاضي وسلطته في الأخذ بهذا الدليل كأحد وسائل الإثبات في جرائم الإرهاب الإلكتروني،على النحو التالي:

اولا:- مشروعية الدليل الرقمي في إثبات جرائم الإرهاب الإلكتروني:

يعد الإثبات الجنائي نشاط إجرائي موجه بطريقة مباشرة للوصول إلى ما يعرف باليقين القضائي، ويتمثل في إقامة الدليل أمام القضاء من خلال الطرق التي يحددها القانون، والتي تثبت صحة الواقعة القانونية المتنازع بشأنها، مما يترتب على ذلك عدد من الآثار القانونية[212].

ووفقا لمبدأ حرية الإثبات الجنائي كمبدأ من المبادئ المستقرة الخاصة في نظرية الإثبات الجنائي، يجوز للأطراف اللجوء إلى جميع وسائل الإثبات التي تثبت صحة ما يدعونه، كما أن للجهات المختصة بالتحقيق اللجوء أيضا إلى أية وسيلة من وسائل الإثبات يمكن من خلالها إدانة المتهم، ويكون للقاضي الموازنة بينها وفقا للسلطة التقديرية التي يتمتع بها[213].

وطبقا لما استقر عليه القضاء الاتحادي حول مبدأ سلطة القاضي الواسعة في الإثبات الجنائي وتقدير القرائن والأدلة، وما تحمله هذه الوقائع من الدلالة على ارتكاب الجريمة، جاء في قضاء

([212])عبد الصبور عبد القوي على مصري، **المحكمة الرقمية والجريمة المعلوماتية**، دراسة مقارنة، مكتبة القانون والاقتصاد، ط1، 2012م، ص387.

([213])سالم بن حامد بن على البلوى، **التقنيات الحديثة ودورها في ضبط الجريمة**، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2009م، ص45.

المحكمة الاتحادية العليا "أن الأصل في المحاكمات الجزائية هو اقتناع القاضي بناء على الأدلة المطروحة عليه فله أن يكون عقيدته من أي قرينه أو دليل يطمئن إليه، إلا إذا قيده القانون بدليل معين ينص عليه، ومن المقرر أن تقدير الأدلة ووزن أقوال الشهود وتقديرها يعتبر من إطلاقات محكمه الموضوع تنزله المنزلة التي تراها"[214].

وانطلاقا من أن الدليل الإلكتروني يمكن استخلاصه عن طريق شبكات المعلومات أو الأجهزة الرقمية في المجال الخاص بجرائم الإرهاب الإلكتروني؛ فإنه يعتبر تطبيقًا من تطبيقات الدليل العلمي الذي يتميز بالكفاءة والموضوعية وفق قواعد علمية محكمة يقينية لا تقبل التأويل، وبالتالي يمكن الإثبات من خلاله شريطة أن يكون هذا الدليل مرتبطا بالوقائع الأساسية ومنسجما مع التسلسل المنطقيلها[215]. ولم يقيد المشرع الاتحادي القاضي برفض أو قبول أي دليل في الإثبات الجنائي بما فيها الدليل الإلكتروني، فلم ينص على قواعد خاصة للإثبات في قانون مكافحه الجرائم المعلوماتية، بل ترك ذلك للقواعد العامة في الإثبات المنصوص عليها في قانون الإجراءات الجزائية الاتحادي، التي تنص على أن" للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لإظهار الحقيقة"[216].

كما أن المشرع الاتحادي أقر بالدليل الإلكتروني في قانون المعاملات والتجارة الإلكترونية، حيث نص على أنه "لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات، أن

---

(214) الطعن رقم 101 لسنه 10ق، ع جزائي، جلسه 1/4/ 1989،المحكمة الإتحادية العليا، أحدث إجتهادات المحكمة الإتحادية العليا، (https://www.moj.gov.ae/ar/about-moj/union-supreme-court/e-) ، تاريخ الإطلاع (2021/3/25).

(215)سالم بن حامد بن على البلوى، مرجع سابق، ص45.

(216) الماده (179) من قانون الإجراءات الجزائيه الإتحادي رقم 29 لسنه 2005، بتعديل بعض أحكام قانون الإجراءات الجزائيه رقم 35 لسنه 1992، بتاريخ 23 ديسمبر 2005م، المعدل بالمرسوم بقانون الإتحادي رقم 28 لسنه 2020م.

تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني"[217].

كما أعطى المشرع للدليل الإلكتروني الحجية الكاملة في الإثبات وفقا لأحكام قانون الإثبات الاتحادي، حيث نص على أن"للكتابة الإلكترونية والمحررات الإلكترونية، والسجلات الإلكترونية والمستندات الإلكترونية ذات الحجة المقررة للكتابة والمحررات الرسمية والعرفية في أحكام هذا القانون متى استوفت الشروط والأحكام المقررة في قانون المعاملات والتجارة الإلكترونية"[218].

وينبغي الإشارة إلى أنه على الرغم من أن الدليل الإلكتروني في جرائم الإرهاب التي يتم ارتكابها عبر الفضاء الإلكتروني، يثير العديد من التحديات والصعوبات في إمكانية الحصول عليه من خلال الإجراءات التقليدية من المعاينة والتفتيش، إلا أنه يتبع المبادئ والشروط العامة في الحصول عليه،المتمثلة في مشروعيه وجوده والحصول عليه، فهو يخضع لمبدأ المشروعية الجنائية، التي تتطلب أن يكون قد استخلص بطريقه مشروعه ومقبولة في الإثبات، حتى يكون صالحا للنظر فيه، فالقاضي لا يحكم إلا استنادا على دليل مشروع، تم الحصول عليه طبقا لمبدأ المشروعية[219].

فرغم السلطة الواسعة الواسعة والحرية الممنوحة للقاضي في أن يستمد قناعته من أية دليل وبالوسيلة التي يمكن من خلالها الوصول إلى الحقيقة الفعلية، إلا أن هذه الحرية مقيدة بضرورة مشروعية مصدر دليل الإثبات،حيث لابد أن يكون الدليل الذي يمكن الاستناد إليه والأخذ به مقبولا في الدعوى، وهو لا يكون كذلك إلا بعد التأكد من أنه يتفق مع النظام القانوني ومبدأ المشروعية في

([217])المادة (10) من القانون الاتحادي رقم 1 لسنة 2006م، بشأن المعاملات والتجارة الإلكترونية، الجريدة الرسمية، العدد 442، السنة السادسة والثلاثون، 1محرم 1427هـ، 31 يناير 2006م.

([218])المادة (17) من القانون الاتحادي رقم 36 لسنة 2006م، بتعديل قانون الإثبات في المعاملات المدنيه والتجاريه، رقم 10 لسنه 1992م، الجريدة الرسمية، العدد 233،بتاريخ 15 يناير 1992م، المعدل بالمرسوم بقانون رقم 27 لسنه 2020م.

(219) محمد صلاح محمد عبد المنعم، مرجع سابق، ص277.

الإثبات،ويترتب على مخالفة هذا المبدأ إهدار قيمة الدليل الذي تم تقديمه، ويصف قضاءه بالبطلان،فلابد من مراعاة مبدأ المشروعية عند استخلاص الدليل الرقمي في جرائم الإرهاب الإلكتروني و كذلك الطريقة التي تم الحصول عليه من خلالها[220].

ثانيا:- الدور الإيجابي للقاضي وسلطته في الأخذ بالدليل الرقمي في جرائم الإرهاب الإلكتروني:

يتمتع القاضي الجنائي بسلطة واسعة في المجال الخاص بإثبات جرائم الإرهاب الإلكتروني، فله أن يطلب من سلطة الاتهام العديد من الأدلة الإلكترونية التي تثبت ارتكاب المتهم لهذه الجريمة، وله أن يسمح للمتهم بنفي مسؤوليته بتقديم الدليل المناسب، إضافة إلى أن سلطته في هذا المجال لا تقف عند الأدلة المقدمة إليه من أطراف الدعوى، حيث يتميز بدوره الإيجابي في توفير الدليل الرقمي،من خلال المبادرة باتخاذ العديد من إجراءات تحقيق الدعوى والكشف عن الحقيقة الفعلية، حيث إن الضرر الذي تمثله جرائم الإرهاب الإلكتروني لا يمس فقط المصلحة الفردية بل يمس مصلحة وأمن المجتمع واستقراره، بناء عليه لابد من منح القاضي السلطات الكافية للوصول إلى الحقيقة[221].

فيمكن للقاضي أن يوجه العديد من الأوامر إلى مزودي الخدمة بتقديم المعطيات اللازمة التي تسمح بتعرف المرسل إليهم أو إليه الاتصال،إضافة إلى عناوين المواقع التي تم الاطلاع عليها، والأدلة التي تثبت ارتكاب المتهم لجرائم الإرهاب الإلكتروني، فضلًا عن أنه يمكن للقاضي أن يطلب تتبع الاتصالات اللاسلكية والسلكية إن وجد ضرورة لهذا الإجراء وكان مفيدا في مجال الكشف عن هذا النوع من الجرائم[222].

حيث قضت المحكمة الاتحادية العليا بأنه "لما كان المقرر في قضاء هذه المحكمة أن لمحكمة

([220]) طارق فوزي ألفقي، مرجع سابق، ص224/222

([221]) سليمان أحمد فضل،مرجع سابق، ص363

([222]) طارق فوزي ألفقي، مرجع سابق، ص56/53.

الموضوع السلطة التامة في تكوين عقيدتها مما تطمئن إليه من أدله الدعوى، كما لها أن تأخذ باعتراف المتهم متى اطمأنت إلى صدوره عن إرادة حرة وأن تستخلص من ذلك الاعتراف الصورة الصحيحة للواقعة، ولا يشترط في الأدلة ومنها الاعتراف الذي اعتمدت عليه المحكمة في حكمها واتخذته سندا لقضائها أن ينبئ في كل جزيئاته عن الواقعة، بل يكون للمحكمة أن تعضده بأدلة وقرائن أخرى، ذلك أن الأدلة في المواد الجنائية متساندة بعضها يكمل البعض حيث تكون منها المحكمة عقيدتها ولا ينظر إلى دليل بعينه، دون باقي الأدلة الأخرى، بل يكفي أن تكون هذه الأدلة تؤدي في مجموعها إلى ما قصده الحكم منها"[223].

إضافة لما تقدم يمكن للقاضي أن يستعين بالخبراء في المجال الإلكتروني لتقديم تقارير أو لتوضيح أمور بشأن جرائم الإرهاب التي يتم ارتكابها عبر الفضاء الإلكتروني، فالخبير التقني له دور هام في مساعده القاضي للفصل في هذا النوع من القضايا، وهذا ما نصت عليه المادة (2) من القانون الاتحادي بشأن تنظيم الخبرة أمام المحاكم، بأن "للمحكمة عند الاقتضاء أن تحكم بندب خبير أو أكثر من بين موظفي الدولة أو من بين الخبراء المقيدين في جدول الخبراء للاستنارة برأيهم في المسائل المشار إليهافي المادة السابقة وتقدر المحكمة الأمانة التي يجب إيداعها خزانة المحكمة لحساب مصروفات الخبير وأتعابه، والخصم الذي يكلف إيداع هذه الأمانة، والأجل الذي يجب فيه الإيداع، والمبلغ الذي يجوز للخبير سحبه لمصروفاته"[224].

تطبيقا لما تقدم فإن الدليل الرقمي في مجال جرائم الإرهاب الإلكتروني يخضع للمبدأ العام في الإثبات الجنائي، وهو أن للقاضي الحرية التامة في الاقتناع به وفقا لقناعته الشخصية، فالقاضي يمتلك

([223]) الطعن رقم 416 لسنه 2014 جزائي، جلسه 2/ 2/ 2015م، المحكمه الإتحاديه العليا، أحدث إجتهادات المحكمة الإتحادية العليا، (https://www.moj.gov.ae/ar/about-moj/union-supreme-court/e-) ، تاريخ الإطلاع (2021/3/27).

([224]) المادة (2) من القانون الإتحادي رقم (8) لسنة 1978 بشأن تنظيم الخبرة أمام المحاكم.

الحرية الواسعة في تقدير الإثبات من خلاله، فيستمد قناعته وعقيدته من أي دليل تطمئن إليه نفسه،بدون قيود تغل يده في هذا المجال، سواء كانت الأدلة المقدمة إليه من الخصوم أو من النيابة العامة، أو التي يرى تقديمها، والحرية الواسعةللقاضي في هذا المجال ليس الهدف منهاتوسيع دائرة الاتهام أو البراءة، إنمايراعى فيها صعوبة الحصول على الدليل الرقمي في مجال جرائم الإرهاب الإلكتروني[225].

حيث قضت المحكمة الاتحادية العليا بأنه "لما كان من المقرر في قضاء هذه المحكمة أن فهم الوقائع في الدعوى وتقدير أدلتها والموازنة بينها موضوعي، والمحكمة غير ملزمة بتتبع أقوال الخصوم متى كان سائغا وترجيح ما تراه المحكمة راجحا وجديرا في مختلف حججهم للرد عليها، كفاية تبين الحقيقة التي اقتنعت بها المحكمة، وواحد من أهم الأدلة بتلك الدعوى هو حسب ما جاء بالنص: المستندات ومنها الرسائل المتبادلة بين المتهم (الطاعن) والشخص الموجود خارج الدولة،والاتصالات الهاتفية"[226].

وترى الباحثة أن للقاضي الجنائي الحرية التامة والواسعة في الاستعانه بكافه وسائل الإثبات بغرض تكوين عقيدته وقناعته للوصول إلى الحقيقة، وله الحرية في الأخذ بالأدلة الجنائية الرقمية في إثبات جرائم الإرهاب الإلكتروني، فالمشرع لم يحصر الأدلة التي يجب على القاضي الاستناد إليها والأخذ بها، بل له وفقا للمبادئ المستقر عليها الحرية في الإثبات ما لم يقيد المشرع حريته بنص، ومن ثمَّ فإن مسألة قبول المحكمة للدليل الإلكتروني ودوره في إثبات جرائم الإرهاب الإلكتروني لا يؤثر فيها سوى قناعه القاضي بالدليل الذي تم استخلاصه.

([225])محمد صلاح محمد عبد المنعم، ص515/514.

([226]) الطعن رقم 764 لسنة 2014، السنة الثامنة القضائية، جزائي، جلسة 2014/11/19، موقع المحامون العرب،

الخاتمة

تناولت الباحثة في هذه الدراسة موضوع السياسة الجنائية في مواجهة الإرهاب الإلكتروني،من حيث مفهوم الإرهاب الإلكتروني،وبيان أسبابه وأساليب وطرق مكافحته،إضافة إلى بيان الإشكاليات الموضوعية والإجرائية التي تعترض مواجهة الإرهاب الإلكتروني، وقد توصلت الباحثة في ختام الدراسة إلى عدد من النتائج والتوصيات؛ يمكن إجمالها فيما يلي:

أولًا- النتائج:

خلصت الدراسة إلى النتائج التالية:

أ- لا يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي من حيث المفهوم؛ لكن يختلفالإرهاب الإلكتروني عن الإرهاب التقليديمن حيث الوسيلة المستخدمة؛ وهي تكنولوجيا المعلومات في مجال الإنترنت والحاسب الآلي، وغير ذلك من وسائل التواصل الاجتماعي، التي ترتكب جرائم الإرهاب من خلالها، أما فيما يتعلق بالمفهوم الخاص بكل منهما فكلاهما له طابع تدميري، من خلال التهديد والترهيب، الذي يحقق الأهداف والأضرار ذاتها،سواء من الناحية الاجتماعية، أو الاقتصادية، أو السياسية، أو العسكرية ...

ب-تستهدف الجماعات الإرهابية والمتطرفة من إنشاء وإدارة المواقع الإلكترونية على شبكة الإنترنت عدة أهداف؛ أبرزها: الاستطلاع ونشر الفكر والدعاية، والاتصال وإنشاء مجتمع إلكتروني، والدعم المالي، والتجنيد والقرصنة؛ لتحقيق أغراض إرهابية.

ت-يمكن مواجهة جرائم الإرهاب الإلكترونيمن خلال المواجهة التقنية للجرائم الإلكترونية بوجه عام،التي تتمثل في السياسة الوقائية والعلاجية.

ث–تعد المعاهدات والاتفاقيات الدولية من أهمآليات التعاون الدولي في مجال مكافحة الجرائم الإلكترونية بوجه عام، وجرائم الإرهاب الإلكتروني بوجه خاص؛ ويأتي على رأس هذه المعاهدات والاتفاقيات؛ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م.

ج– تثير مواجهة جرائم الإرهاب الإلكتروني عددًا من الإشكاليات الموضوعية، تتمثل في عدم كفاية القواعد العامة والنصوص التقليدية، لمواجهة هذا النوع من الجرائم، حيث يقابل التطور والتقدم في المجال التكنولوجي استغلال الجناة لهذه التقنيات واستخدامها في ارتكاب جرائم الإرهاب الإلكتروني.

ح– تعدُّجرائم الإرهاب الإلكتروني جرائم لها خصائص منفردة وطبيعة خاصة، تختلف عن الجرائم التقليدية من حيث طرق ووسائل ارتكابها، وينعكس ذلك على طبيعة الإجراءات التي يجب اتخاذها من السلطات المختصة؛ كإجراءات الضبط، والتفتيش، والخبرة، والمعاينة، وغيرها...

خ– أضفى المشرع الاتحادي حجية قانونية كاملة على المحررات الإلكترونية في مجال الإثبات بشأن المعاملات والتجارة الإلكترونية، كما أضفى الحجية ذاتها على التوقيع الإلكتروني في مجال البيانات التي يتم معالجتها آليًّا من خلال شبكات الإنترنت والحاسب الآلي.

د– تنطبق الشروط الخاصة بالدليل التقليدي على الأدلة الجنائية الرقمية، التي تأتي على رأس الأدلة العلمية؛ بل قد تكون لها حجية أكبر في الإثبات؛ لأنها معالجة بوسائل تقنية المعلومات، فضلًا عن أنها مُحْكمة لا تقبل التأويل.

ثانيًا– التوصيات:

أ– توصي الباحثة بضرورة وجود جهاز ضبطية قضائية متخصص في مجال تقنية المعلومات؛ لأن إجراءات المعاينة والخبرة الجنائية الخاصة بجرائم الإرهاب الإلكتروني التي ترتكب عبر شبكة

الإنترنت لا يكفي معها التدريب التقليدي؛ بل تحتاج إلى تدريب فني تقني وكفاءة عالية في مجال الحاسب الآلي والإنترنت ووسائل الاتصال.

ب- تهيب الباحثة بالمشرع الاتحادي بضرورة النص على الضوابط والشروط الخاصة بإجراءات المعاينة والضبط والخبرة في مجال الجرائم الإرهابية، بما يتلاءم مع خصوصية وطبيعة هذه الجرائم التي ترتكب عبر الفضاء الإلكتروني.

ت- توصي الباحثة بتطوير الوسائل الخاصة بالإثبات في جرائم الإرهاب الإلكتروني، ضد مرتكبي هذه الجرائم، من خلال الأجهزة الحكومية وخبراء تقنية المعلومات.

ث- تقترح الباحثة عقد دورات تدريبية للقضاة في مجال جرائم الإرهاب الإلكتروني؛ لزيادة خبرة وإلمام القضاة بطرق ووسائل ارتكاب هذا النوع من الجرائم، ومعرفة المداخل القانونية التي يستغلها المتهم للتخفي وتدمير الأدلة في جرائم الإرهاب الإلكتروني.

ج- توصي الباحثة بإنشاء منظمة عربية لتنسيق الجهود الخاصة بمكافحة جرائم الإرهاب بشكل عام والإرهاب الإلكتروني على وجه التحديد، وتوفير قاعدة بيانات مشتركة عن العناصر التي لديها ميول إلى التطرف أو علاقات مشبوهة مع منظمات غير مشروعة لوضعها تحت المراقبة كإجراء استباقي قبل تورطهم في أي عمل إرهابي.

ح- توصي الباحثة بزيادة التعاون على المستوى الوطني والدولي للتنسيق بين الجهات والأجهزة المختصة بصدد مكافحة جرائم الإرهاب الإلكتروني،من خلال الإعدادوالتدريب وتبادل الخبرات؛ لضمان الفعالية في مكافحة هذه الجرائم.

خ- توصي الباحثة بتفعيل وتطوير قنوات التعاون الإقليمي والدولي في مجال تدريب المحامين، والقضاة، وأعضاء النيابة العامة، ورجال الضبط القضائي، على آليات تطبيق التشريعات الخاصة بجرائم الإرهاب الإلكتروني، وعلى كيفية التعامل مع هذه الجرائم.

د- تهيب الباحثة بالمشرع الاتحادي على تحديث التشريعات المتعلقة بجرائم الإرهاب الإلكتروني بشكل دوري ومستمر؛ لمواكبة القفزات الهائلة في المجال التكنولوجي، وما يتبعها من تطور مستمر في طرق وأساليب ارتكاب جرائم الإرهاب الإلكتروني، وذلك لعدم كفايه القواعد المنصوص عليها لمواجهه هذا النوع من الجرائم.

ذ- توصي الباحثة بمواصلة السعي وبذل مزيد من الجهد على المستوى الدولي وعلى مختلف القنوات؛ للوصول إلى مفهوم محدد ومتفق عليه للإرهاب بوجه عام، والإرهاب الإلكتروني بوجه خاص.

ر- توصي الباحثة بتكثيف الجهود على الصعيد الدولي؛ لصياغة اتفاق شامل حول جرائم الإرهاب الإلكتروني تلتزم الدول الأطراف بتضمين أحكامه في قوانينها الوطنية، وتشمل تعريفه وأساليبه وجميع الجوانب الخاصة بمكافحته؛ لما يمثله هذا النوع من الجرائم من خطورة على السلم والأمن الدوليين.

ز- تهيب الباحثة بالمشرع الاتحادي لإنشاء هيئة متخصصة للتحقيق في جرائم الإرهاب وكل ما يتفرع عنها أو يتصل بها من جرائم؛ كجرائم الإرهاب الإلكتروني، أو الجرائم التي ترتكب لغرض إرهابي، أو جرائم تمويل الإرهاب.

س- توصي الباحثة بفتح المجال أمام سلطات إنفاذ القانون -وفق ضوابط معينة- لتتبع الأعمال المريبة التي قد تنذر بأعمال إرهابية، دون التقيد بالقواعد التقليدية في الإثبات، التي قد تعيق اكتشاف هذه الجرائم قبل وقوعها؛ الأمر الذي يؤدي إلى نتائج كارثية على أمن البلاد واستقرارها، يفوق أي مصالح أو أضرار فردية.

ش- توصي الباحثة -على الصعيد المجتمعي- بتوفير منصات إعلامية عبر الوسائل السمعية والمرئية؛ تعنى بتثقيف وتوعية أفراد المجتمع وخاصة الشباب، بالأساليب الخبيثة الخادعة التي

تتبعها المنظمات والجماعات الإرهابية في تجنيد الشباب ونشر فكرها التدميري والمتطرف عبر شبكة الانترنيت ومنصات التواصل،لحماية المجتمع وتحصينه من مخاطر الإرهاب.

قائمة المراجع

1) إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، دراسة تحليلية تطبيقية، 2015م.
2) إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، وفقًا للمرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات وتعديلاته، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018م.
3) أبو الحسين أحمد بن فارس بن زكريا القزويني الرازي، معجم مقاييس اللغة، ج2، دار الفكر، 1979م.
4) أبو الفضل جمال الدين محمد بن مكرم ابن منظور الأنصاري الرويفعي الأفريقي، لسان العرب، ج1، دار المعارف، 2007م.
5) أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي الرازي، مختار الصحاح، ج2، المكتبة العصرية، الدار النموذجية، ط5، 1999م.
6) أحمدي بوجلطيه بوعلي، الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي، دراسة للتجربتين السعودية والقطرية، الأكاديمية للدراسات الاجتماعية والإنسانية، قسم العلوم الاقتصادية والقانونية ، ع16، 2016م.
7) القانون الاتحادي رقم 7 لسنة 2014م، بشأن مكافحة الجرائم الإرهابية، والذي تم نشره في الجريدة الرسمية بتاريخ 2014/8/31م.
8) القانون الاتحادي رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات. صادر بتاريخ 8/13/ 2012م.
9) القانون الاتحادي رقم 5 لسنة 2012 م بشأن مكافحة جرائم تقنية المعلومات،المعدل بالقانون الاتحادي رقم 2 لسنة 2018م الصادر بتاريخ 2018/7/24م.
10) القانون الاتحادي رقم 3 لسنة 1987م، بشأن إصدار قانون العقوبات، نشر في الجريدة الرسمية العدد 182 السنة السابعة، بتاريخ 1987/12/20م.
11) القانون الإجراءات الجزائية الاتحادي رقم 29 لسنه 2005م, بتعديل بعض أحكام قانون الإجراءات الجزائية رقم 35 لسنه 1992، بتاريخ 23 ديسمبر 2005م, المعدل بقانون اتحادي رقم 28 لسنه 2020م.

12) القانون الاتحادي رقم 1 لسنة 2006م، بشأن المعاملات والتجارة الإلكترونية، الجريدة الرسمية، العدد 442، السنة السادسة والثلاثون، بتاريخ 31 يناير 2006م.
13) القانون الاتحادي رقم 36 لسنة 2006م، بتعديل قانون الإثبات في المعاملات المدنية والتجارية، رقم 10 لسنه 1992م، الجريدة الرسمية، العدد 233،بتاريخ 15 يناير 1992م, المعدل بقانون اتحادي رقم 27 لسنه 2020م.
14) المختار لمجيدري، الإرهاب الإلكتروني، إشكاليات الإثبات الجنائي والقضاء عليه، مجله العلوم السياسية والقانون، المجلد 3، المركز الديمقراطي العربي، ألمانيا، 2019م.
15) المرسوم بقانون اتحادي رقم 20 لسنة 2018م في شأن مواجهة جرائم غسل الأموال، ومكافحة تمويل الإرهاب، وتمويل التنظيمات غير المشروعة, ولائحته التنفيذية رقم 10 لسنه 2019م.
16) أمين مصطفى محمد، قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، 2016م.
17) إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، الجوانب القانونية لعقد التجارة الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2008م.
18) بوقرين عبد الحليم، المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي، دراسة مقارنة، المجلد 16، ع1، مجلة جامعة الشارقة للعلوم القانونية، 2019م.
19) بيتر سينجر، الإرهاب الإلكتروني، خرافات وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجهة، سلسلة محاضرات الإمارات 215، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2018م.
20) حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية ، دراسة مقارنة، مجلة مركز حكم القانون ومكافحة الفساد، دار جامعة حمد بن خليفة لنشر، 2019م.
21) خالد سليمان عبد الله الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتى في القانون القطري، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019م.
22) داود سليمان علي الحمادي، أحكام جريمة التزوير الإلكتروني، وفقًا لأحكام قانون مكافحة جرائم تقنية المعلومات الإماراتي، دار النهضة العربية، القاهرة، د.ت.
23) دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، الأمم المتحدة، نيويورك، 2009م.
24) رانيا عزب، العقود الرقمية في قانون الإنترنت، دراسة تحليلية مقارنة في الفقه والتشريعات العربية والأمريكية والأوربية، دار الجامعة الجديدة،الإسكندرية، 2012م .

25) رحيمه الطيب عيساني، أخلاقيات استخدام وسائل الاتصال الجديدة وتشريعاتها في دولة الإمارات العربية المتحدة، قراءة تحليلية لقانون مكافحة تقنية المعلومات، مجلة جامعة العين للأعمال والقانون، ع2، 2020م.

26) زياد محمد سلامة جفال، مكافحة جريمة تمويل الإرهاب في القانون الدولي والإماراتي، دراسة في مدى مواءمة التشريع الإماراتي لأحكام الاتفاقية الدولية لمكافحة تمويل الإرهاب لعام 1999م، دراسات، علوم الشريعة والقانون، المجلد 46، ع3، الجامعة الأردنية، 2019م.

27) سالم بن حامد بن على البلوى، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2009م.

28) سلطان عناد إبراهيم العدينات، الآلية الدولية لمكافحة الإرهاب، رسالة ماجستير، كلية الحقوق ، جامعة الشرق الأوسط، 2018م.

29) سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت، دار النهضة العربية، القاهرة، 2013م.

30) سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنت، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادي والقانونية، المجلد 29، ع3، 2013م.

31) شريف عبد الحميد حسن رمضان، الإرهاب الدولي، أسبابه وطرق مكافحته في القانون الدولي والفقه الإسلامي، دراسة مقارنة، ج3، ع31، مجله كليه الشريعة والقانون، طنطا، 2016م.

32) شمسان ناجي صالح ألخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009م.

33) طارق فوزي ألفقي، الجوانب الإجرائية في الجرائم المعلوماتية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية، 2011م.

34) عبد الإله محمد النوايسة، دور قانون مكافحة الجرائم الإرهابية الإماراتي في مكافحة الخطورة الإجرامية في جرائم الإرهاب، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، ع1، 2018م.

35) عبد الرحيم محمد،الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، الأمانة العامة، مجلس التعاون لدول الخليج العربية، 2016م.

36) عبد الصبور عبد القوي على مصري، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، مكتبة القانون والاقتصاد، ط1، 2012م.

37) عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب المعلوماتى، بحوث ومقالات، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، 2015م.

38) عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2012م.

39) عبد الله نوار شعت، الإثبات والالتزامات في العقود الإلكترونية، ط1،مكتبة الوفاء القانونية، الإسكندرية، 2017م.

40) عبد المجيد مراد داد محمد أحمد، المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي، دراسة وصفية تحليلية للقانون والقضاء الإماراتي، كلية القانون، جامعة الشارقة، دولة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، 2020/2019م.

41) علي لونيسي، آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الانفرادية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، 2012م.

42) عمرو عبد الفتاح علي يونس، جوانب قانونية للتعاقد الإلكتروني في إطار القانون المدني، دراسة مقارنة، مدعمة بأحدث الأحكام القضائية الأجنبية والعربية ، ط1، 2009م.

43) غزاله حميدة، الإرهاب البيولوجي وآليات مكافحته دوليًّا، رسالة ماجستير، جامعة العربي التبسي، 2016/2015م.

44) غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، 2017/2016م.

45) فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتى، دون دار نشر، ط2، 2010م.

46) مجمع اللغة العربية، المعجم الوجيز، وزارة التربية والتعليم، 2006م.

47) محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2017م.

48) محمد عبد الفتاح عبد المقصود علي،القواعد الإجرائية للجرائم التي تقع عبر شبكة الإنترنت،رسالة دكتوراه، كلية الحقوق، جامعة طنطا، 2015م.

49) محمد عبيد ألكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة المعلومات، دراسة مقارنة، ط2، دار النهضة العربية، 2009م.

50) محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، 2017/2016م.

51) محمود صالح العادلي، الإرهاب الرقمي في القانون البحريني المقارن بالنظام السعودي والقانون المصري، (ماهيته – الجماعات المتطرفة والإرهابية– صور استخدام الإنترنت في الإرهاب– البحث والتحقيق الجنائي المتصل بالإرهاب الرقمي، دار النهضة العربية، القاهرة، ط1، 2016م.

52) محمود نجيب حسني، شرح قانون العقوبات القسم العام، ط4، دار النهضة العربية، القاهرة، 1977م.

53) مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، دراسة مقارنة، دراسات علوم الشريعة، المجلد 45، ع4، ملحق 2، 2018م.

54) مها محمد أحمد عنانزه، وعي طلبة جامعة اليرموك بمخاطر الإرهاب الإلكتروني ودور التربية الوطنية والإسلامية والقانونية في التصدي لها، رسالة دكتوراه، كلية التربية، جامعة اليرموك، 2018م.

55) ميثاء إسحاق عبد الرحيم الشيباني، المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية طبقًا للمرسوم رقم 5 لسنة 2012م بشأن قانون مكافحة جرائم تقنية المعلومات، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018م.

56) نائلة عادل محمد فريد قوره، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، 2004.

57) نبيلة هبه هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006م.

58) محمد علي عريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011م.

قائمة المحتويات