جامعـــــة دمشـــــق
كليـــــة الحقـــــوق
قسم القانون الجزائي

الإرهاب بالوسائل الإلكترونية

بحث أعد لنيل درجة الماجستير في القانون الجزائي

إعداد الطالب

نور اللّه تلـــه

بإشراف

أ.د. بارعة القدسي

رئيسة قسم القانون الجزائي

٢٠١٥-٢٠١٦

تألفت لجنة الحكم على الرسالة من السادة الأساتذة:

د. بارعة القدسي ..... عضواً مشرفاً

أستاذ في قسم القانون الجزائي بكلية الحقوق _ جامعة دمشق

د. صفاء أوتاني ..... عضواً

أستاذ في قسم القانون الجزائي بكلية الحقوق _ جامعة دمشق

د. عيسى المخول ..... عضواً

أستاذ مساعد في قسم القانون الجزائي بكلية الحقوق _ جامعة دمشق

بسم الله الرحمن الرحيم

" مازال المرء عالماً ما طلب العلم فإذا ظن أنه علم فقد جهل"

علي بن أبي طالب

إهـــــــــداء

إلى القلبين الكبيرين ومن اتشرف بهما .. مثلي الأعلى في الحياة .. والدي ووالدتي

إلى القلوب البيضاء .. بسمة الحياة .. إخوتي

إلى صاحبة اليد الفضلى في إنجاز هذا العمل .. الأستاذة الدكتورة بارعة القدسي

إلى أساتذتي في قسم القانون الجزائي .. شكراً وتقديراً ووفاء

إلى جميع الأصدقاء ..

إلى جميع زملاء العمل ..

إلى كل من ساعدني وشجعني في إنجاز هذا العمل المتواضع ..

إلى من يشاركني حلو الحياة ومرها .. رفيقة دربي

شكر وتقدير

أتوجه بخالص الشكر والتقدير لأعضاء لجنة المناقشة الموقرين بقبول مناقشة هذه الرسالة والحكم عليها رغم كثرة مشاغلهم وأعبائهم الأكاديمية.

وأتوجه بالشكر الجزيل للأستاذة الدكتورة بارعة القدسي المشرف على هذه الرسالة حيث بفضل جهودها الكبيرة وتوجيهاتها السديدة ورحابة صدرها أثناء فترة البحث تم إنجاز هذا العمل فلها مني خالص التقدير.

وأتوجه بالشكر إلى الدكتورة منال مروان منجد رغم ظروف سفرها لما قدمته من جهد في إنجاز هذا العمل.

كما أتوجه بخالص الشكر إلى جميع الأساتذة في قسم القانون الجزائي.

وفي الختام أتقدم بالشكر الجزيل لكل من أسهم في إنجاز هذا العمل.

الإرهاب بالوسائل الإلكترونية

المقدمة

يعد الإرهاب من الظواهر القديمة، التي اتفقت الدول على تجريمها، واختلفت في تعريفها، وإن المتتبع لتاريخ الإرهاب بصفة عامة يلاحظ أنه قد عرف تطورات عدة خصوصاً في النصف الثاني من القرن الماضي، فقد كان الإرهاب كثيراً ما يفاجئ الدول بمهاجمة أهداف لم يكن يمسها من قبل.[١]

إن الإرهاب كصورة من صور العنف، تطور مع تطور المجتمع، فالإرهاب الذي كان يعتمد على الاغتيالات والتفجيرات واحتجاز الرهائن، أصبح وثيق الصلة بالتكنولوجيا،[٢] حيث يشهد العالم تطوراً هائلا في تكنولوجيا المعلومات والاتصالات، حتى أصبح يُطلق على هذا العصر–عصر ثورة المعلومات والاتصالات–[٣]حيث إن الانتشار الواسع للحاسب الآلي ودخوله مجالات الحياة كافة، وظهور شبكة الإنترنت، والتطور الهائل في عالم البرمجيات، وتزايد الاعتماد على بنوك المعلومات، أدى إلى وصول هذه التقنية إلى أيدي الخير والشر معاً.

استغل الإرهابيون هذه الثورة التقنية، سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث ابتكار أساليب وطرق

---

[١] عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، المغرب–القنيطرة، خلال الفترة ١١–١٥/٣/١٤٢٧هـ الموافق ٩–١٣/٤/٢٠٠٦م، ص ٥.

٢ سهير عثمان عبد الحليم، الإرهاب والإنترنت، دراسة حالة في ضوء التجربة المصرية، ورقة عمل مقدمة للمؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، المنعقد في القاهرة ٢–٤ يونيو ٢٠٠٨، ص ١.

٣ عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى مؤتمر الدولي الأول حول حماية الأمن والمعلومات والخصوصية في قانون الإنترنت، القاهرة، مصر، ٢–٤ يونيو ٢٠٠٨م، بحث منشور على الإنترنت. منتدى كلية الحقوق، جامعة المنصورة، مصر، متاح على الرابط: www.f-law.net، لا يوجد رقم صفحة.

إجرامية متقدمة، فإذا كان للإنترنت مزايا كثيرة، فإن الإرهابيين وجدوا في هذه الوسيلة التكنولوجية ضالتهم، لأنها طريقة آمنة للأعمال غير المشروعة، فظهر تبعاً لذلك مصطلحات ومفاهيم جديدة للإرهاب، فظهر ما يعرف بالإرهاب بالوسائل الإلكترونية.

وهذه الصورة الحديثة للإرهاب، استهدفت الأمن القومي للدول خصوصاً في مجال التكنولوجيا، فوجدت أن المعادلة التي تجمع قطاعات الكهرباء والماء والاتصالات والحاسب هي الركائز الضرورية للأمن الاجتماعي والقومي، وبالنتيجة إن هذه المعادلة: كهرباء + اتصالات + حاسوب معرضة لتهديد ما يسمى (الإرهاب بالوسائل الإلكترونية).[١]

حيث يستفيد الإرهابيون مما توفره شبكة الإنترنت من خدمات عبر العناوين الإلكترونية أو ما يسمى بغرف الدردشة من أجل الدعاية ونشر أفكارهم، كما أنهم يستعملونها في التجنيد وجمع التبرعات ووضع الخطط والأهداف، فضلا عن مهاجمة البنية التحتية المعلوماتية التي تعتمد على شبكة الإنترنت بهدف تدميرها أو وقفها عن العمل أو السيطرة عليها.

وبالتالي فإن المصادر التي يَعتمد عليها من يريد القيام بهجوم إرهابي إلكتروني متوافرة ومنتشرة بين الناس عامة، وتتألف من جهاز الحاسوب ونقطة اتصال بالإنترنت، حيث أن معظم الجرائم الإرهابية ارتبطت بالإنترنت، المسرح المفضل لها، فالفريق الإرهابي يقتل والثاني يبرر ويحرض ويجند، مما جعل الإنترنت وسيلة فعالة وسهلة الاستخدام وسريعة الوصول إلى الجمهور، ورخيصة الثمن وساحة حرة بلا رقيب.[٢]

---

١ أ.د. عبد الله بن ناصر الحمود، وسائل الإعلام المعاصرة والإرهاب المعلوماتي، الدورة التدريبية: مكافحة الجرائم الإرهابية المعلوماتية، خلال فترة ٩-٢٠٠٦/٤/١٣، المغرب، القنيطرة. ص ٢٦.

٢ أ.د. عبد الله بن ناصر الحمود، المرجع السابق. ص ٢٦.

حيث تَعد تكنولوجيا المعلومات من أرخص الوسائل التي يمكن استخدامها في الهجمات الإرهابية، على الرغم من أن تكنولوجيا المعلومات وتشغيل الشبكة والحماية اللازمة لها مكلفة جداً، في حين أن الوسائل اللازمة لمهاجمتهم رخيصة.[١]

وإن محاولة تأصيل ظاهرة الإرهاب بالوسائل الإلكترونية يعود إلى نهايات القرن الماضي، خاصة بعد بروز فكرة حرب المعلومات،[٢] فبعد أحداث ١١ أيلول ٢٠٠١م، ظهر بوضوح الدور الذي لعبته شبكة الإنترنت في دعم الأنشطة الإرهابية لتنظيم القاعدة، الأمر الذي دفع الباحثين إلى وضع ظاهرة توظيف قنوات الإعلام الجديد وإمكانات الإنترنت من قبل الجماعات المتطرفة والإرهابية في مركز الاهتمام.[٣]

ويمكن الجزم بأن مصطلح الإرهاب بالوسائل الإلكترونية هو وليد أحداث ١١ أيلول ٢٠٠١م، فالاتفاقيات الدولية والإقليمية، التي أعقبت الأحداث المذكورة كان لها عظيم الأثر في تبني الكثير من الدول مصطلح الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) وأن تتضمنه قوانينها الجزائية.[٤]

---

١ محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد في الرياض، المملكة العربية السعودية: خلال الفترة ٢١-٢٢ ربيع الثاني ١٤٣١هـ، ٦-٧ ابريل ٢٠١٠م، ص ٣.

٢ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من ١١-١٤٢٧/٣/١٥هـ لموافق ٩-٢٠٠٦/٤/١٣م، المغرب، القنيطرة، الموافق ١٤٢٧هـ-٢٠٠٦م، ص٦.

٣ د. مها عبد المجيد صلاح، استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الإنترنت، دراسة تحليلية، الندوة العلمية، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، القاهرة، مصر، ١٧-١٤٣١/١١/١٩هـ الموافق ٢٥-٢٠١٠/١٠/٢٧م، ص٩.

٤ عبد الحق باسو، المرجع السابق، ص١٨.

وبالتالي أصبح الإرهاب بالوسائل الإلكترونية، هاجساً يخيف العالم الذي بات عرضة لهجمات الإرهابيين عبر الإنترنت، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة غير قادرة على حماية الناس من العمليات الإرهابية التي سببت أضراراً جسيمة للأفراد والمنظمات والدول.[١]

وقد تنبه الغرب إلى قضية الإرهاب بالوسائل الإلكترونية منذ مدة طويلة، واتخذت الدول الإجراءات التشريعية والتقنية العديدة.[٢]

وبالعودة إلى الواقع التشريعي في الدول العربية بشكل عام، وفي الجمهورية العربية السورية بشكل خاص، يبرز عدم مواكبته لهذا النوع الجديد من الجرائم الإرهابية التي تتطور بسرعة، وترتبط بالإرهاب من جهة، وتكنولوجيا المعلومات من جهة أخرى.

وقد ابتلت الجمهورية العربية السورية في الآونة الأخيرة بالإرهاب، بصوره وأشكاله كافة، التقليدي منها والإلكتروني، والذي طال كل نواحي وأشكال الحياة، وأمام هذا الإرهاب، أصدر المشرع السوري عدة مراسيم تشريعية تهدف إلى مكافحة الإرهاب، منها المرسوم التشريعي رقم /١٩/ الصادر في ٢٠١٢/٧/٢م والمتضمن قانون مكافحة الإرهاب.[٣]

---

١ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية: سوسيولوجية، مجلة كلية الآدب بقنا، جامعة جنوب الوادي، مصر، العدد ٢٧، ٢٠٠٩م، ٢٢٢.

٢ إرهاب إلكتروني، ويكيبيديا، الموسوعة الحرة، متاح على الرابط التالي:

/إرهاب- إلكتروني/https://ar.wikipedia.org/wik، تاريخ الزيارة: ٢٠١٤/٥/٢٤م.

٣ حيث كان المشرع السوري يعالج جرائم الإرهاب ضمن أحكام المواد /٣٠٤ إلى ٣٠٦/ من قانون العقوبات السوري الصادر بالمرسوم التشريعي رقم ١٤٨ لعام ١٩٤٩م، ضمن زمرة الجرائم الواقعة على أمن الدولة الداخلي.

فضلاً عن صدور تشريع خاص هو المرسوم التشريعي **رقم /١٧/ لعام ٢٠١٢م**، المتضمن قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، الذي ينظم البيئة الإلكترونية ويكافح الإجرام المعلوماتي.

وتكمن خطورة الإرهاب بالوسائل الإلكترونية في استغلاله واستخدامه لأساليب متطورة للغاية، مما يحتم مواجهتها بوسائل لا تقل تطوراً عن أساليب ارتكابها، لذا أضحى من واجب الدول أن تتعاون فيما بينها لإرساء قواعد قانونية ملائمة تستجيب لمتطلبات الحياة الرقمية لمواجهة الأنشطة الإجرامية العصرية، لأنه بات مؤكدا أن الدول منفردةً عاجزة عن مكافحتها.

حيث تشكل مواجهة الإرهاب بالوسائل الإلكترونية تحدياً أمنياً خطيراً، فلم يعد من المقبول في ظل السياق الثقافي والتكنولوجي والمعلوماتي الجديد أن تواجه عمليات الإرهاب بالوسائل الإلكترونية بطرق وأساليب قانونية تقليدية. فقد أثبت الواقع أن التنظيمات الإرهابية لديها متخصصون على مستوى عالٍ في مجال أنظمة المعلومات، واستطاعت هذه التنظيمات الإرهابية استخدام شبكة الإنترنت وتمرير أفكارها عبرها، وتتحدى العالم بإعلان ما ترتكبه من جرائم عبر شبكة الإنترنت،[١] إذ يكفي أن يتمكن إرهابيون ضالعون في وسائل الاتصالات الحديثة من الدخول إلى نظام معلوماتي استراتيجي لبث فيروس لشل المصادر الأساسية في قطاعات حساسة كالقطاع العسكري، أو السياسي، أو الاقتصادي، أو الاجتماعي في بلد واحد أو قارة بأكملها، وإذا صحّ هذا الكلام فإن حجم الأضرار الناجمة عن مثل هذه الاعتداءات

---

١ د. نايف بن محمد المرواني، تمويل الإرهاب إلكترونياً التحديات وطرق المواجهة، التجربة السعودية، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٩، العدد ٥٨، محرم ١٤٣٥هـ، الرياض، المملكة العربية السعودية، نوفمبر/ديسمبر ٢٠١٣، ص ٦.

الإرهابية الإلكترونية سيفوق بإضعاف مضاعفة الأضرار الناجمة عن أي عمل إرهابي آخر من حيث قدرته على بث الفوضى والتشويش والشلل.[١]

[١] أ.د. عبد الله بن ناصر الحمود، المرجع السابق. ص ٣٠.

أولاً: مشكلة البحث

لا يبدد الواقع التشريعي في الدول العربية بشكل عام، وفي **سورية** بشكل خاص، المخاوف من الإرهاب بالوسائل الإلكترونية، حيث أن النصوص الجزائية لم تتدخل بوضعها الراهن بنصوص خاصة لحماية الأفراد والمنظمات الحكومية التي تستخدم شبكة الاتصال وتعتمد عليها من خطر الإرهاب بالوسائل الإلكترونية الذي يستخدم شبكة الإنترنت وسيلةً حرة له.

لا تكمن **المشكلة الرئيسية** في استغلال الإرهابيين لشبكة الإنترنت، وإنما في عدم ملاحقة القانون لهم، وعدم مسايرت تشريعاته للتكنولوجيا الجديدة، فهذا الفراغ التشريعي ظهر نتيجة عدم التجاوب القانوني مع الاحتياجات التي تولدها متغيرات العصر، مما يستدعي تعديل القوانين لتواكب هذه المتغيرات، بما يتلاءم مع ما استجد في الحياة من تقنيات حديثة وأنماط حياة وسلوكيات بشر تختلف اختلافاً جذرياً وجوهرياً عن تلك السلوكيات التي عاصرت القوانين المعمول بها.

وعانت الجمهورية العربية السورية في ظل الأزمة التي تحيط بها، ولازالت تعاني، من توظيف الإرهابيين لشبكة الإنترنت لخدمة مشاريعهم الإرهابية، حيث استخدم الإرهابيون شبكة الإنترنت في تنفيذ أعمال إرهابية عدة من خلال (مهاجمة المواقع الإلكترونية الحكومية، مهاجمة مواقع الإعلام الرسمي على شبكة الإنترنت، تجنيد الإرهابيين عبر وسائل التواصل الاجتماعي، حملات التحريض والدعاية، نشر التطرف والنعرات الطائفية، توثيق العمليات الإرهابية من خلال مقاطع الفيديو أو الصور ونشرها على شبكة الإنترنت واظهار منفذيها بمظهر الأبطال، إصدار البيانات الإلكترونية، التهديد بالقيام بعمليات إرهابية، ... إلخ).

أمام هذا كله، ليس من الواقع في شيء مواجهة الإرهاب بالوسائل الإلكترونية بالوسائل التقليدية قانونياً أو فنياً، من هنا تأتي مشكلة هذه الدراسة وهي كيفية توفير الحماية اللازمة للبيئة الإلكترونية من الإرهاب بالوسائل الإلكترونية.

فقد أصدر المشرع السوري في ظل ظروف الأزمة الحالية، مراسيم تشريعية عدة لمكافحة الإرهاب وتنظيم البيئة الإلكترونية، **(القانون رقم /١٩/ لمكافحة الإرهاب لعام ٢٠١٢م، والمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية)**، وعلى أساس أن الإرهاب بالوسائل الإلكترونية يرتبط بالإرهاب من جهة وتكنلوجيا المعلومات من جهة أخرى.

- فهل ما جاء به القانون رقم /١٩/ لعام ٢٠١٢م الخاص بمكافحة الإرهاب، يجرم الإرهاب بصورته الإلكترونية؟
- وهل المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م الخاص بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، بما يحتويه من مواد قانونية، قادر على حماية البيئة الإلكترونية السورية سواء الحكومية أو الخاصة أو حتى على مستوى الأفراد، من خطر الإرهاب بالوسائل الإلكترونية؟

ثانياً: أهمية البحث

تكمن أهمية البحث في أنه يقدم دراسة نظرية تتمثل في إلقاء الضوء على جريمة الإرهاب بالوسائل الإلكترونية، من خلال تحديد ماهية هذه الجريمة، وخصائصها وآثارها، وحجم الأضرار التي تخلفها، والجرائم ذات الصلة،

مثل الجرائم المعلوماتية، التي تمخض عنها عصر التقنية الرقمية، والإطار القانوني لها، وآليات مكافحتها والوقاية منها سواء فنياً / تقنيا ً / أو قانونياً، سواء على صعيد تجارب الدول أو على الصعيد الدولي، لأن هذه الجريمة من أخطر جرائم الإرهاب وأكثرها استحداثاً وانتشاراً، في ظل التطور التكنولوجي وتنامي استخدام شبكة الإنترنت.

وتأتي أهمية البحث أيضاً في ضوء ما تتعرض له الجمهورية العربية السورية من إرهاب بصوره وأشكاله كافة، ومنها الإرهاب بالوسائل الإلكترونية.

فضلاً عن حداثة كل من قانون مكافحة الإرهاب في سورية، والمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م الخاص بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، في مواجهة جريمة الإرهاب بالوسائل الإلكترونية.

ثالثاً: أهداف البحث

تسعى هذه الدراسة إلى محاولة استكشاف وتحديد معالم ظاهرة جريمة الإرهاب بالوسائل الإلكترونية، التي تعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصالات وشبكة المعلومات، بهدف الوقوف على السبل والوسائل الناجعة لمكافحة هذه الظاهرة الإجرامية، وذلك من خلال:

- التعرف على جريمة الإرهاب بالوسائل الإلكترونية من حيث ماهيتها وتعريفها وأهم خصائصها وأخطارها وآثارها.
- إلقاء الضوء على أهم طرق وأساليب الإرهاب بالوسائل الإلكترونية في الاستفادة من التقنية الرقمية.

- دراسة الإطار القانوني للإرهاب بالوسائل الإلكترونية في الجمهورية العربية السورية.
- الوقوف على كيفية مكافحة الإرهاب بالوسائل الإلكترونية على المستوى الرقمي.
- عرض تجارب بعض الدول في مواجهة الإرهاب بالوسائل الإلكترونية، بالإضافة إلى الجهود الدولية لمكافحة الإرهاب بالوسائل الإلكترونية.
- محاولة وضع مشروع قانون لتجريم الإرهاب بالوسائل الإلكترونية.

رابعاً: منهجية البحث

اتبعت في بحثي المنهج التحليلي الذي يقوم على رصد الجريمة وتحليلها للوقوف على جوانبها كلها، ودراسة الإطار القانوني للإرهاب بالوسائل الإلكترونية في الجمهورية العربية السورية، بالإضافة إلى عرض تجارب بعض الدول العربية والأجنبية في مواجهة الإرهاب بالوسائل الإلكترونية والجهود الدولية لمكافحة الإرهاب بالوسائل الإلكترونية، معتمداً على بعض الدراسات والبحوث والتشريعات المتعلقة بالموضوع، فضلاً عن المؤتمرات والندوات التي تطرقت لها.

وقد قسمت بحثي إلى الفصلين التاليين:

الفصل الأول: ماهية الإرهاب بالوسائل الإلكترونية.

الفصل الثاني: مكافحة الإرهاب بالوسائل الإلكترونية.

مخطط البحث:

الإرهاب بالوسائل الإلكترونية

الفصل الأول: ماهية الإرهاب بالوسائل الإلكترونية

المبحث الأول: الإطار العام للإرهاب بالوسائل الإلكترونية

المطلب الأول: تعريف الإرهاب بالوسائل الإلكترونية

الفرع الأول: تعريف المصطلحات

الفرع الثاني: تصنيف الإرهاب بالوسائل الإلكترونية وميزاته

المطلب الثاني: مظاهر الإرهاب بالوسائل الإلكترونية

الفرع الأول: أشكال الإرهاب بالوسائل الإلكترونية

الفرع الثاني: النماذج التطبيقية للإرهاب بالوسائل الإلكترونية

المبحث الثاني: الإطار القانوني للإرهاب بالوسائل الإلكترونية (سورية)

المطلب الأول: قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية

الفرع الأول: **الجرائم المستحدثة**

الفرع الثاني: **الجرائم الاعتيادية**

المطلب الثاني: قانون مكافحة الإرهاب

الفرع الأول: جريمة العمل الإرهابي

الفرع الثاني: الجرائم المستحدثة في قانون مكافحة الإرهاب

الفصل الثاني: مكافحة الإرهاب بالوسائل الإلكترونية

المبحث الأول: مكافحة الإرهاب بالوسائل الإلكترونية تشريعياً

المطلب الأول: التشريعات الوطنية

الفرع الأول تشريعات بعض الدول العربية

الفرع الثاني: تشريعات بعض الدول الأجنبية

المطلب الثاني: الآليات الدولية لمكافحة الإرهاب بالوسائل الإلكترونية

الفرع الأول: الاتفاقيات الدولية

الفرع الثاني: التعاون الدولي

المبحث الثاني: مكافحة الإرهاب بالوسائل الإلكترونية فنياً

المطلب الأول: إجراءات الحماية الفنية الأساسية

المطلب الثاني: أنظمة الحماية الفنية من الاعتداءات الإلكترونية

الإرهاب بالوسائل الإلكترونية

الفصل الأول

ماهية الإرهاب بالوسائل الإلكترونية

مع بزوغ الثورة المعلوماتية، وتطور الاتصالات ودخول الحاسب الآلي إلى مجالات الحياة كافة وظهور شبكة الإنترنت وما يسمى بالحكومات الإلكترونية وانتقال المجتمعات الإنسانية من مجتمعات معاصرة إلى مجتمعات ما بعد الحداثة،[١] توسعت استخدامات التقنيات الإلكترونية الحديثة في مجالات كثيرة، وأفادت في نواحي حياتية كثيرة، وساعدت على توصيل المعلومات وسهلت العديد من الخدمات، إلا أن هذه الاستخدامات لا تخلو من الانحرافات والتجاوزات عن الاستخدامات المفيدة والمثلى لهذه التقنيات.

والأمر الذي لم يعد خافياً على أحد، هو العلاقة بين التقنية الحديثة والإرهاب إجراماً ومكافحة، إذ إن استخدام الإرهابيين للتقنيات الحديثة يسهل تنفيذ جرائمهم ويوفر فرص ارتكاب الجرائم عن بعد، ويزيد من عدد الضحايا ويوسع من دائرة الدمار التي تصيب المرافق والممتلكات، ويصعب مهمة أجهزة مكافحة الإرهاب.[٢] فالإرهاب لا وطن له ولا دين، واستخدام الإرهابيين للتقنيات الحديثة زاد من أخطار الإرهاب وأضراره.[٣]

---

١ د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٧هـ-٢٠٠٦م، ص١١.

٢ اللواء د. محمد فتحي عيد، الأساليب والوسائل التقنية التي يستخدمها الإرهابيون وطرق التصدي لها ومكافحتها، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٢ هـ _ ٢٠٠٢، ص ٥.

٣ اللواء د. محمد فتحي عيد، الأساليب والوسائل التقنية التي يستخدمها الإرهابيون وطرق التصدي لها ومكافحتها، المرجع السابق، ص٦.

وبالتالي أدى انتقال المجتمعات من الحالة التقليدية إلى حالة الحداثة المعاصرة إلى ظهور نمط جديد من الجرائم أطلق عليها **الجرائم المستحدثة**، والتي تتسم بأنها عابرة ومتجددة وتعتمد على منتجات الحداثة،[١] وظهرت تبعاً لذلك مصطلحات ومفردات ومفاهيم جديدة للإرهاب، ولعل من الصور الحديثة للإرهاب استخدام الوسائل الإلكترونية فيه.[٢]

حيث استخدم الإرهاب، كنظام قائم على الرعب، الشبكة الدولية (الإنترنت) في تنفيذ الكثير من الأعمال الإرهابية، واستعار الإرهابيون هذه الوسيلة الآمنة في نشر ما يعرف بالرعب الإلكتروني، أحد الأبعاد الجديدة للإرهاب التقليدي،[٣] وإذا كان الإرهاب بالوسائل الإلكترونية مفهوماً جديداً فإنه يبقى مع ذلك مجرد تطور نوعي للإرهاب بصفة عامة أو صورة جديدة لما يمكن أن يسمى بالإرهاب التقليدي.[٤]

فتكنولوجيا المعلومات وشبكة الإنترنت مفيدة للجماعات الإرهابية في ناحيتين:[٥]

أولاً يمكن لهم أن يستخدموا أجهزة الحاسب والإنترنت بوصفها أدوات مفيدة لتعزيز النشاط الإرهابي التقليدي، مثل استخدام الإنترنت في التجنيد والتدريب وتبادل المعلومات بين المنظمات الإرهابية المختلفة.

ثانياً البنية التحتية للمعلومات، يمكن أن تشكل هدفاً جذاباً للأعمال الإرهابية التي يمكن من خلالها التأثير في الرأي العام العالمي.

---

١ د. أحمد فلاح العموش، المرجع السابق، ص ٦٠.

٢ د. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها وطرق مكافحتها، المملكة العربية السعودية، جامعة الأمام محمد بن سعود الإسلامية، اللجنة العلمية للمؤتمر العالمي عن موقف الإسلام من الإرهاب، ٢٠٠٤م، ص٣.

٣ أ.د. محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير وأساليبها، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٧هـ -٢٠٠٦م، ص ١١٩.

٤ عبد الحق باسو، المرجع السابق، ص ٥.

٥ محمد سيد سلطان، المرجع السابق. ص ٦.

وبالتالي نحن مع القول بأن العصر الجديد للإرهاب تميز بالدور المركزي الذي تلعبه شبكة الإنترنت في تشكيله ونقل الأفكار والخبرات عبرها، وقد أصبح الإرهاب وثيق الصلة بالتكنولوجيا، لدرجة أنه يمكن معه القول إن بث الإرهاب عبر الإنترنت أصبح من سمات الألفية الثالثة.[١]

وبالتالي سنقسم هذا الفصل إلى مبحثين:

المبحث الأول: الإطار العام للإرهاب بالوسائل الإلكترونية.

المبحث الثاني: الإطار القانوني للإرهاب بالوسائل الإلكترونية(سورية).

---

١ أ.د جميل عبد الباقي الصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الإنترنت، الحلقة العلمية، الإنترنت والإرهاب. خلال الفترة ١٥-٢٠٠٨/١١/١٩بالتعاون مع جامعة عين شمس، القاهرة-مصر، ص٣.

المبحث الأول

الإطار العام للإرهاب بالوسائل الإلكترونية

بدء الإرهابيون في توظيف الفضاء الالكتروني لخدمة أغراضهم الإرهابية، مع انتشار الحاسب والإنترنت والتوسع في توظيف شبكات المعلومات، ونجم عن ذلك ما يعرف بالإرهاب بالوسائل الإلكترونية، ومن المصطلحات المرادفة والدالة على المعنى ذاته أيضاً الإرهاب الالكتروني أو المعلوماتي أو الشبكي أو الافتراضي أو التخيلي أو الفضائي، الذي أصبح واقعاً فرضته الحوادث اليومية، التي كانت تقنيات الاتصال الحديثة طرفاً فيها أو ضحية لها.

وإن معالم ظاهرة الإرهاب بالوسائل الإلكترونية، لم تبرز إلى الوجود بشكل جلي إلا بعد أحداث ١١ أيلول ٢٠٠١ التي ضربت الولايات المتحدة الأمريكية، خصوصاً بعد أن أثبتت الدراسات الاستراتيجية المنجزة عقب تلك الأحداث بداية الانتقال من المواجهة المباشرة إلى حرب فضاء المعلومات، وعزم التنظيمات الأصولية المتشددة على استهداف الأنظمة الإلكترونية الحساسة في الدول المتقدمة لتحقيق أكبر خسارة ممكنة، من دون الحاجة إلى المواجهة المباشرة والمفتوحة مع أجهزة الأمن والاستخبارات.[١]

لذلك سنقوم بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: تعريف الإرهاب بالوسائل الإلكترونية.

المطلب الثاني: مظاهر الإرهاب بالوسائل الإلكترونية.

---

١ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص٦.

المطلب الأول

تعريف الإرهاب بالوسائل الإلكترونية

يتكون لفظ الإرهاب بالوسائل الإلكترونية من عنصرين أساسيين هما: البيئة الرقمية (الفضاء الإلكتروني) والإرهاب.[١] ولا بد لتعريف الإرهاب بالوسائل الإلكترونية من تحديد ماهية البيئة الإلكترونية، والجرائم التي ترتكب ضمنها /الجرائم المعلوماتية/، ومفهوم الإرهاب، ليتم بمقتضاه التوصل إلى تعريف الإرهاب بالوسائل الإلكترونية.

لذلك لابد من تقسيم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: تعريف المصطلحات.

والفرع الثاني: تصنيف الإرهاب بالوسائل الإلكترونية وميزاته.

الفرع الأول

تعريف المصطلحات

أولاً: البيئة الإلكترونية أو العالم الافتراضي

تحتوي البيئة الإلكترونية على كل ما يتصل بتكنولوجيا المعلومات من أدوات وخدمات[٢]، وتشير إلى التمثيل الرمزي والزائف والمجازي للمعلومات أو هو المكان الذي تعمل فيه برامج أجهزة الحاسوب وتنتقل فيه البيانات.[٣]

---

١ محمد سيد سلطان، المرجع السابق، ص ١٠.

٢ محمد سيد سلطان، المرجع السابق، ص ١٠.

٣ د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، المرجع السابق، ص ٩٠.

وينطلق الإرهاب بالوسائل الإلكترونية من عالمين، العالم المادي والعالم الافتراضي، ويشير **العالم المادي** إلى قضايا وظواهر متعددة مثل الطاقة، الضوء، الظلام، البرودة، الأمور المادية جميعها، والحيز الذي نعيش فيه ونمارس الوظائف من خلاله، ويمثل التقاء هذين العالمين وسيلةً أو أداةً للإرهاب بالوسائل الإلكترونية.[١]

والإنترنت[٢] كأهم تطبيق تنتسب للبيئة الإلكترونية وتعبر عنها وأحيانا تختصرها، مثلت بيئة حاضنة لأنشطة الإرهاب بالوسائل الإلكترونية أو للاستخدام في الأغراض الإرهابية،[٣]ويعود أصل كلمة إنترنت إلى الكلمة الإنجليزية (internet)، وهي منقسمة إلى قسمين الأول وهو (inter)

---

١ د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، المرجع السابق، ص ٩١.

٢ بدأ الانترنت " في أواخر الستينات عندما شكلت وزارة الدفاع الأمريكية لجنة من الخبراء، أوكلت إليهم مهمة إنشاء شبكة تربط بين الحاسبات، وسميت اللجنة (وكالة مشروع الأبحاث المتقدمة) عام ١٩٥٧م، ونجحت اللجنة في مهمتها، وبذلك أنشئت أول شبكة للإنترنت في الولايات المتحدة الأمريكية تحت أسم (ARBANET)، وهي اختصار لعبارة (شبكة وكالة مشروع الأبحاث المتقدمة)، وكان الغرض من هذه الشبكة هو خدمة الاستخبارات العسكرية، وبدأت الشبكة تخرج من الخصوصية إلى العالمية تدريجياً، ففي عام ١٩٨٣م انقسمت الشبكة إلى شبكتين، كانت الأولى هي (ARBANET) فاحتفظت باسمها وبغرضها الأساسي، أما الثانية فهي (MILNET) وهذه الشبكة خصصت للاستخدامات المدنية.

وفي عام ١٩٨٦م أمكن للأمريكيين ربط شبكات خمسة مراكز عملاقة بشبكة واحدة سميت (NSFNET)، والتي أصبحت فيما بعد بمثابة العمود الفقري لنمو وازدهار الإنترنت في أمريكا ومن ثم باقي دول العالم، فانتشر الإنترنت في أرجاء المعمورة، بعد أن كان يربط في البداية ثلاثة حواسيب، ويصل الآن لكي يربط مئات الملايين في مختلف دول العالم". أنظر: محمد سيد سلطان، المرجع السابق ص٤.

٣ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت لأغراض إرهابية، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢ م. ص ١٥٧.

ويعني البينة، والثاني (net) ويعني الشبكة، وعليه فتكون الترجمة الحرفية هي الشبكة البينية.[١]

ومن المصطلحات المرادفة والدالة على نفس المعنى: الشبكة العنكبوتية، الشبكة العالمية، شبكة الويب، النسيج العنكبوتي.[٢]

وأكثر التعريفات شيوعاً لشبكة الإنترنت هو: نظام المعلومات العالمي، الذي يتصل بعضه ببعض بواسطة عناوين متفردة، معتمدة على بروتوكول الإنترنت ip أو لواحقه وتوابعه الفرعية، ويكون قادراً على دعم الاتصالات بواسطة بروتوكول التحكم في الإرسال tcp/ip ، أو أي بروتوكول إنترنت متوائم.[٣]

لا تخضع هذه الأداة التكنولوجية الجديدة لملكية أية جهة كانت، فهي ساحة عالمية حرة سمحت بظهور مجتمع الإنترنت الذي يحظى بتمويل من أطراف متعددة حكومية وغير حكومية، وتجارية.[٤]

وتتألف شبكة الإنترنت من عدد كبير من المواقع، فقد وصل عدد المواقع على شبكة الإنترنت حتى شهر أكتوبر ٢٠١٠م إلى أكثر من ٢٣٢ مليون موقع،[٥] وتحتوي على بنوك معلومات ضخمة تتراوح بين الموسوعات إلى قواعد المعطيات، مرورا بمختلف البيانات، وذلك بسرعة اتصال مذهلة

---

١ محمد سيد سلطان، المرجع السابق، ص٤.

٢ د. نايف بن محمد المرواني، المرجع السابق، ص١٠.

٣ د. نايف بن محمد المرواني، المرجع السابق، ص١٠-١١.

٤ د. أخام بن عودة زواوي ملكية، تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس / ليبيا، ٢٧-٣٠ أكتوبر ٢٠٠٩، بحث منشور على الإنترنت، لا يوجد رقم صفحة.

٥ أ.د. وليد محمد أبو ريه، التعرف على الإرهاب الإلكتروني، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٧-١٩/١١/١٤٣١هـ الموافق ٢٥-٢٧/١٠/٢٠١٠م، ص٥٣.

وآنية، ومن أهم خصائص شبكة الإنترنت: التفاعلية والآنية وخدمة الوسائط المتعددة. [١]

وإذا كانت الشبكة قد أحدثت ثورة معلوماتية كوسيلة اتصال وأداة معرفية تثقيفية وتعليمية جديدة، فإنها كانت مصحوبة بأشكال مستحدثة من الجرائم التقنية نسبة للآلة المستعملة في ارتكابها، حيث تعد شبكة المعلومات (الإنترنت) اليوم من الوسائط القوية الأثر في خدمة الإرهاب والجريمة. [٢]

ثانياً: الجريمة المعلوماتية[٣](الإلكترونية)

هي ظاهرة إجرامية مستجدة نسبياً رافقت نشوء وتطور نظم الحاسوب والشبكات وثورة تكنولوجيا المعلومات، [٤] ومصطلح الجريمة المعلوماتية مصلح قانوني ذو دلالة واسعة يكون مراعياً لمستجدات الاختراعات الإلكترونية ووسائل الاتصال أي كل ما يخدم المعلومة، إذ لا نعلم ما سيأتي به الغد القريب من تطور وتقدم، هذا من جانب ومن جانب آخر فإن استخدام

---

١ د. فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصالات الجديدة. دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٠، العدد ٣٩، الرياض، المملكة العربية السعودية، محرم ١٤٢٦هـ-فبراير ٢٠٠٥، ص ١٤١-١٤٢.

٢ أ.د علي علي فهمي، دور الشبكات الاجتماعية في تمويل وتجنيد الإرهابيين، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢ م، ص ٨٩.

٣ حيث بدأ الحديث عن هذه الظاهرة في أواخر الستينات من القرن العشرين تحت عبارة جرائم الحاسب الآلي، وتم تطوير هذا المصطلح إلى جرائم الحاسب الآلي والإنترنت في الثمانينات. ومن ثم ظهرت مصطلحات أخرى منها (الجرائم الإلكترونية، جرائم تقنية المعلومات، جرائم التقنية العالية، جرائم الإنترنت، جرائم السايبر، جرائم السايبر الفضائية). أنظر: د. محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، جامعة نايف العربية للعلوم الأمنية، القاهرة ١٤٢٩هـ/٢٠٠٨م.الحلقة العلمية (الإنترنت والإرهاب) خلال الفترة من ١٧-١٤٢٩/١١/٢١هـ الموافق ٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، القاهرة-مصر، ص٨.

٤ د. يونس عرب، مشروع قانون نموذجي عربي، لجرائم الكمبيوتر والإنترنت أو للجرائم الإلكترونية، ورشة عمل: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ٢-٤ نيسان، ٢٠٠٦، عمان - الأردن، لا يوجد رقم صفحة.

هذا المصلح يكون ضامناً لاستيعاب جرائم الحاسوب وغيرها من السلوكيات الضارة بالفرد والمجتمع.

وتنطوي الجرائم المعلوماتية على مخاطر جمة، وتُلحِق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (البيانات والمعلومات والبرامج بأنواعها كافة)، وتَطال المعطيات المخزنة والمعلومات المنقولة عبر النظم وشبكات المعلومات، هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة.[١]

وقد عرف المشرع السوري الجريمة المعلوماتية في مادته الأولى من الفصل الأول من المرسوم التشريعي رقم /١٧/ لعام **٢٠١٢م بأنها: "جريمة ترتكب باستخدام الأجهزة الحاسوبية[٢] أو الشبكة[٣] أو تقع على المنظومة المعلوماتية[٤] أو الشبكة."**

---

١ د. يونس عرب، مشروع قانون نموذجي عربي، لجرائم الكمبيوتر والإنترنت أو للجرائم الإلكترونية، المرجع السابق، لا يوجد رقم صفحة.

٢ عرف المشرع السوري الجهاز الحاسوبي في المادة الأول من المرسوم التشريغي رقم /١٧/ لعام ٢٠١٢م بأنه: "أي جهاز يستخدم التقانات الإلكترونية أو الكهرطيسية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها." ويدل الجهاز الحاسوبي على أي جهاز، سلكي لاسلكي، مهما كان نوعه أو شكله، يملك معالجاً للمعلومات، مثل: المخدم، الحاسوب الشخصي، والمساعد الرقمي الشخصي، الهاتف الذكي.....الخ. أنظر: ت١/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٣ عرف المشرع السوري الشبكة في المادة الأولى من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م بأنه: "ترابط من الأجهزة الحاسوبية والمنظومات المعلوماتية يسمح بتبادل المعلومات أو التشارك فيها بين مرسل ومستقبل أو مجموعة من المستقبلين وفق إجراءات محددة." ومن الأمثلة على الشبكات: الإنترنت، شبكات المعلومات الداخلية، شبكات تبادل المعطيات، الشبكات النقالة، الشبكات الهاتفية الذكية ...الخ. أنظر: ت٤/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٤ عرّف المشرع السوري المنظومة المعلوماتية في المادة الأولى من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م بأنها: "مجموعة متسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها." ومن الأمثلة على المنظومة المعلوماتية: مخدم تتصل به حواسيب طرفية، حاسوب مع المعدات الملحقة به، كالمودم،

يتضح من هذا التعريف أن الجريمة المعلوماتية لا يمكن أن تجري بالاستخدام المنفرد والأوحد للحاسوب، وبمعزل عن الشبكة، فلابد من حدوث اتصال بين جهاز حاسوب وآخر، هذا يعني أنه لا يمكن ارتكاب جريمة إلكترونية بالعمل على جهاز منفرد مهما كان نوع الجرم المفتعل.[١]

حيث يمكن استخدام الحاسب في ارتكاب جرائم كثيرة، لكن ليس بالضرورة أن يجري توصيفها على أنها جرائم إلكترونية، كجريمة التزوير بالمستندات والوثائق، أو التلاعب بصورة الأفراد وتشويهها بقصد إهانة الكرامة، كل تلك الجرائم ربما لا يمكن لها أن تقع لولا استخدام الحاسوب في ارتكابها، إلا أنه لا يمكن أن تصنف كجريمة إلكترونية بل ترد إلى أصل الفعل.[٢]

في الوقت ذاته يجري توصيف تلك الجرائم جميعها كجرائم إلكترونية تلقائياً بمجرد إرسالها من جهاز حاسوبي إلى أخر، كتزوير مستندات وإرسالها/استقبالها من/إلى الإنترنت، أو إرسال صور بالبريد الإلكتروني، جرت معالجتها ببرامج الحاسوب بقصد إهانة الكرامة، وجميع تلك الجرائم

والطابعة والماسح الضوئي. أنظر: ت٣/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

كما عرف أيضاً البرمجيات الحاسوبية في المادة نفسها بأنها: "سلسلة متسقة من التعليمات المرمزة التي يمكن تنفيذها على جهاز حاسوبي بغية تمكينه من أداء الوظائف والتطبيقات المطلوبة." والبرمجيات الحاسوبية قد تكون مضمنة في الجهاز الحاسوبي عند تصنيعه، وقد تكون أساسية أو تطبيقية يمكن تصميمها وتطويرها على الجهاز الحاسوبي. أنظر: ت٢/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

١ إياد علي الدرة، المناعة التشريعية في مواجهة الوباء المعلوماتي، المرجع السابق.

٢ إياد علي الدرة، المناعة التشريعية في مواجهة الوباء المعلوماتي، المرجع السابق.

لا تجري إذا لم يحدث الاتصال بين أجهزة الحاسوب، وهو شرط مهم في توصيف الجريمة وتصنيفها (كجريمة إلكترونية).[١]

وتنقسم الجرائم المعلوماتية (أو جرائم الفضاء السبراني) عموماً إلى نوعين أساسيين: **الأول** هو الذي يكون فيه الحاسب الآلي أو الشبكة مجرد وسيلة تسمح بارتكاب الجريمة، وهي غالباً جرائم اعتيادية (مثل جريمة التهديد عن طريق الإنترنت)، ولكن الضرر منها عادة ما يكون أعظم.[٢]

والنوع **الثاني** من الجرائم المعلوماتية، هو الذي تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة (مثل اختراق المنظومة المعلوماتية وتخريبها)، وهي غالباً جرائم مستحدثة لا بد من النص على أركانها ومعاقبتها.[٣]

نلاحظ من التقسيم السابق، أن الجرائم المعلوماتية بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م لا تحدث إلا في حالتين هما:

١- عندما يكون جهاز الحاسوب أو الشبكة أداة تنفذ بواسطتها الجريمة وتصنف على أنها جرائم اعتيادية.

٢- عندما تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة، وتصنف على أنها جرائم مستحدثة.

---

١ إياد علي الدرة، المناعة التشريعية في مواجهة الوباء المعلوماتي، المرجع السابق.

٢ ت١٥/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢.

٣ ت١٥/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

حيث قام المشرع السوري بموجب المرسوم **رقم /١٧/** لعام **٢٠١٢م**، بوضع تعريف عام للجريمة المعلوماتية يستند إلى معيارين، معيار الوسيلة المستخدمة بارتكاب الجريمة، ومعيار موضوع الجريمة أو المحل، واشترط حدوث اتصال بين جهاز حاسوب وآخر، خلاف ذلك لا يمكن ارتكاب جريمة معلوماتية بالعمل على جهاز منفرد مهما كان نوع الجرم المفتعل.

وبما أنه لا جريمة ولا عقوبة إلا بنص قانوني، قام المشرع بتحديد الأفعال المعاقب عليها في الفصل الثالث من المرسوم التشريعي ذاته تحت عنوان مكافحة الجريمة المعلوماتية.

ثالثاً: الإرهاب

لقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه، وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه، فما يراه البعض إرهابا يراه البعض الآخر عملاً مشروعاً.

وقد ظهرت أول محاولة لتعريف الإرهاب على يد عصبة الأمم عام ١٩٣٧م على إثر اغتيال الملك ألكسندر الثالث ملك يوغسلافيا ووزير خارجية فرنسا في مرسيليا عام ١٩٣٤م، حيث تم إبرام اتفاقية جنيف،[١] التي عرّفت الإرهاب بأنه: (الأفعال الإجرامية الموجهة ضد إحدى الدول والتي يكون

---

١ اللواء د. نشأت عثمان الهلالي، تجارب عربية ناجحة في تنظيم وتجهيز مكافحة الإرهاب (التجربة المصرية)، قدرات الأجهزة الأمنية وأثرها في مكافحة الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣١هـ -٢٠١٠م، ص ٥٥.

هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة).[١]

كما عرّفت الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م **الإرهاب** بأنه: (كل فعل من أفعال العنف أو التهديد به أياً كانت دوافعه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر).

على الرغم من أن هذا التعريف يَبرز مظاهر وطبيعة النشاط الإرهابي، إلا أنه لم يتطرق إلى الوسائل والأساليب المستخدمة من طرف الإرهابيين وهي عديدة ومتنوعة، بل قد تأخذ أشكالاً حديثة.[٢]

وتتجه التشريعات الجزائية في دول العالم مختلفة نحو معالجة مشكلة الإرهاب، غير أن غالبيتها يقف عاجزاً عن وضع تعريف محدد لهذه الظاهرة، وتكتفي بالنص على أفعال معينة تمثل صوراً من الجرائم الإرهابية يتم إخضاعها لنظام قانوني خاص لمواجهة أثارها الخطيرة على المجتمع وردع مرتكبيه.

ولقد تناول التشريع السوري موضوع الإرهاب وعدّها جريمة مستقلة، بموجب المواد **٣٠٤** و**٣٠٥** و**٣٠٦** من قانون العقوبات السوري الصادر بالمرسوم التشريعي رقم /١٤٨/ لعام ١٩٤٩م، والتي ألغيت بموجب قانون مكافحة الإرهاب الصادر بالمرسوم التشريعي رقم /١٩/ لعام **٢٠١٢م**،

---

١ اللواء د. محمد فتحي عيد، الإجرام المعاصر، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤١٩هـ -١٩٩٩م، ص١٤٢.

٢ أ.د. محمد مسعود قيراط، الإرهاب، دراسة في البرامج الوطنية واستراتيجيات مكافحته، مقاربة إعلامية، الطبعة الأولى، جامعة نايف العربي للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٢ هـ -٢٠١١م، ص ٦٢.

والذي صدر نتيجة الحاجة الملحة والظروف الاستثنائية التي تمر بها سورية، وقد تضمن تعريفاً بالعمل الإرهابي والمنظمة الإرهابية وتمويل الإرهاب وعقوبة القيام بالعمل الإرهابي أو الترويج للأعمال إرهابية.

فقد عرف المشرع السوري في المادة **الأولى** من هذا القانون **العمل الإرهابي** بأنه: **(كل فعل يهدف إلى إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الإضرار بالبنى التحتية أو الأساسية للدولة ويُرتكب باستخدام الأسلحة أو الذخائر أو المتفجرات أو المواد الملتهبة أو المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية مهما كان نوع الوسائل أو باستخدام أي أداة تؤدي الغرض ذاته).** وعاقب المشرع على جريمة العمل الإرهابي في المادة **السابعة** من القانون نفسه.

رابعاً: الإرهاب بالوسائل الإلكترونية

كما أنه لا يوجد تعريف واحد لمصطلح الإرهاب حظي بقبول عالمي، فإنه لا يوجد تعريف واحد لمصطلح الإرهاب بالوسائل الإلكترونية تم قبوله عالمياً، وتعريف الإرهاب بالوسائل الإلكترونية ينطلق من تعريف الإرهاب،[١] فكلمة إرهاب تعني الخوف، وإذا ركزنا على المفهوم القانوني الذي نُجَرِّم به الفعل المرتكب في الجرائم الإرهابية، لوجدنا أن الفكرة الأساسية للتجريم تكمن في الخوف المترتب على استخدام العنف، والإرهاب دائماً يسعى لنشر الخوف والفزع داخل المجتمع، ولكن الأمر يكون أكثر تعقيداً عندما نحاول الجمع بين الإرهاب والبيئة الإلكترونية.[٢]

---

١ إياد علي الدرة، الإرهاب الإلكتروني، المجلة المعلوماتية، أمن المعلومات، تصدر عن الجمعية العلمية السورية للمعلومات، العدد ٨١، تشرين الثاني، ٢٠١٢م. متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢٠١٣/٥/٢م.

٢ محمد سيد سلطان، المرجع السابق، ص١٠.

يعتمد الإرهاب الإلكتروني على العنف الإلكتروني باستخدام تطبيقات الإنترنت والخدمات المتصلة بها،[١] الذي يرتكب من أجل إثاره الخوف، فهو نفس الإرهاب التقليدي إلا أنه يستخدم الحاسب كمصدر للهجمات،[٢] فالذي يميز الإرهاب الإلكتروني عن الإرهاب التقليدي هو الطريقة العصرية في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات.[٣]أما بالنسبة للأهداف المتوخاة من الفعل الإرهابي والقائمين عليه وممارسة العنف كأداة للضغط فتبقى مشتركة بين كل أنواع الإرهاب سواء كان تقليدياً أو معلوماتياً.[٤]

إن تعريف الإرهاب بالوسائل الإلكترونية لا بد أن يأخذ في الحسبان الأدوات التي يستخدمها الإرهابيون لتنفيذ جرائمهم وأهدافهم.[٥]

أ- التعريف الفقهي

إذ يرى بعض الفقهاء أن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد.

---

١ د. فايز عبد الله الشهري، ثقافة التطرف والعنف على الشبكة الإنترنت: الملامح والاتجاهات، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢ م. ص٩.

٢ محمد سيد سلطان، المرجع السابق، ص١٠.

٣ أ.د. جميل عبد الباقي الصغير، المرجع السابق، ص٦.

٤ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٢.

٥ د. فراس طحان، المرجع السابق، ص٣٦٥.

فالإرهاب الإلكتروني يعتمد على استغلال وسائل الاتصال والإنترنت من أجل تهديد الآخرين والإضرار بهم.[١]

ويُعّرفه البعض الآخر بأنه: (التقاء للإرهاب مع الفضاء التخيلي، وهو يعني التهديدات غير القانونية ضد الحاسبات والشبكة والمعلومات المخزنة، وذلك لإخافة أو إجبار الحكومات أو الناس لتعزيز أهداف سياسية أو اجتماعية، وهو العنف ضد الأفراد أو الممتلكات أو أنه مؤذ لدرجة كافية لخلق الخوف، والتعديات المفضيه للموت أو الإصابة أو الانفجاريات أو الخسارة الاقتصادية وهذه ما هي إلا أمثلة للتعديات على الإرهاب التخيلي. ويمكن تصنيف الجمهور المستهدف في ثلاثة فئات هي: الأفراد والممتلكات والحكومات).[٢]

كما عرفت المادة١.٢ من اقتراح وضع اتفاقية دولية بشأن الجريمة والإرهاب الإلكتروني، الذي أعدها مركز الأمن والتعاون الدولي، الإرهاب بالوسائل الإلكترونية بأنه: (الاستخدام المتعمد أو التهديد باستخدام العنف دون سلطة معترف بها قانونياً، أو أي تدخل ضد تكنولوجيا المعلومات، عندما يكون من المحتمل أن مثل هذا الاستخدام من شانه أن يسفر عن وفاة أو إصابة شخص أو أشخاص، أو يلحق الضرر بالممتلكات المادية، أو يؤدي إلى ضرر اقتصادي كبير).[٣]

---

١ د. فراس طحان، المرجع السابق، ص٣٦٥.

٢ أ.د. ذياب موسى البداينة، الإرهاب المعلوماتي (التعريف-المفهوم-المجالات-النتائج)، الحلقة العلمية، الإنترنت والإرهاب خلال الفترة من ١٧-١٤٢٩/١١/٢١هـ الموافق ١٥-٢٠٠٨/١١/١٩م، جامعة نايف العربية للعلوم الأمنية، بالتعاون مع جامعة عين شمس، القاهرة، مصر، ١٤٢٩هـ/٢٠٠٨م، ص١٢.

٣ محمد سيد سلطان، المرجع السابق، ص١١.

ويعرفه جانب من الفقه بأنه: (الإرهاب التخيلي أي فعل إرهاب يستخدم نظم المعلومات أو التقنية الرقمية (الحواسيب أو الشبكات) وسيلة أو هدف).[١]

ونجد أن القانون البريطاني ٢٠٠٠ terrorism act، عندما عرّف الإرهاب أدخل في هذا التعريف "كل نشاط أنشئ لعرقلة نظام إلكتروني مع نية الضغط على الحكومة أو إحداث الذعر بين السكان بدافع سياسي أو ديني أو إيديولوجي مع إدماج الأنشطة الممارسة خارج المملكة".[٢]

ويعرف أيضاً بأنه:(سوء الاستخدام المتعمد لنظام المعلومات الرقمي، والشبكات، أو المكونات تجاه هدف يدعم أو يسهل حملة إرهابية أو فعل إرهابي).[٣] فالشرطيون في أوربا يعتبرون أن مجرد استخدام الإرهابيين للإنترنت للاتصال فيما بينهم أو تبني أعمالهم أو لغاية الدعاية أو التمويل، إرهاباً إلكترونياً.[٤]

وعرَّف أيضاً بأنه: كل فعل يهدف إلى زعزعة استقرار الدولة أو الضغط على حكومتها السياسية لحملها على الاستجابة لمطالب معينة وذلك عن طريق ارتكاب جرائم متصلة بالمعلومات.[٥]

---

١ أ.د. ذياب موسى البداينة، الإرهاب المعلوماتي (التعريف–المفهوم–المجالات–النتائج)، الحلقة العلمية، المرجع السابق، ص١٣.

٢ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص١٢.

٣ أ.د. ذياب موسى البداينة، الإرهاب المعلوماتي (التعريف–المفهوم–المجالات–النتائج)، المرجع السابق، ص١٣.

٤ الإرهاب الإلكتروني تهديد لم يتبلور بعد لكن لابد من أن يؤخذ على محمل الجد، صحيفة الراكوبة، أخبار السودان لحظة بلحظة، تاريخ النشر: ٢٠١٣/١٠/٢، متاح على الرابط التالي: www.alrakoba.net/news–action–show–id–٨٦٧٢٦.htmK، تاريخ الزيارة: ٢٠١٤/٧/٧.

٥ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص٩.

٢- نتائج تعريف الإرهاب بالوسائل الإلكترونية

أ- نلاحظ من خلال كل هذه التعريفات، الارتباط الوثيق للإرهاب بالوسائل الإلكترونية بالمستوى المتقدم لتكنولوجيا المعلومات، فكل من حاول تعريف الإرهاب بالوسائل الإلكترونية قد انطلق من زاويته ليعطي صفة الإرهاب بالوسائل الإلكترونية لأنشطة عدّها كذلك، إما من حيث الوسيلة المستعملة أو الهدف المتوخى أو الآثار المحدثة أو الدافع السياسي، مما يعبر عن الغموض الذي يكتنف الظاهرة والذي يؤثر بالتالي على سن القوانين أو الاستراتيجيات لمحاربتها، فنجد البعض وسع تعريف الإرهاب بالوسائل الإلكترونية ليشمل جميع الأفعال التي تستخدم النظم الرقمية أو التقنية كهدف أو وسيلة، والبعض قصره على الأفعال التي ترمي إلى التخريب والسيطرة على النظم المعلوماتية.

ب-وهناك من يُميز بين الإرهاب الإلكتروني وبين استعمال الإنترنت لأغراض إرهابية أو استخدام الإرهابيين للإنترنت، حيث عدّ أن استخدام الإرهابيين للإنترنت أو استخدام الانترنت لأغراض إرهابية، هو مفهوم أوسع بكثير، إذ قد يشير إلى طائفة معتبرة من أنشطة الإرهاب الإلكتروني خاصة عندما تستخدم الإنترنت وسيلة لارتكاب جرائم الإرهاب الإلكتروني، لكنه يشمل بشكل رئيسي سائر الأنشطة التي تستخدم فيها الإنترنت كبيئة للجريمة الإرهابية بما في ذلك نشر وتوفير المعلومات والتمويل والربط الشبكي لأغراض إرهابية، وتجنيد الإرهابيين، وجمع المعلومات.[١]

---

١ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت لأغراض إرهابية، المرجع السابق، ص ١٩٥.

ج- ونجد أيضاً أن بعض من عرّف الإرهاب بالوسائل الإلكترونية قد وسع دائرته ليشمل أفعالاً قد تصنف بالأحرى في دائرة الجريمة المعلوماتية، فالقانون الانكليزي مثلا لا يفرق بين القراصنة الشباب الذين يقومون بأفعالهم بدافع التحدي واللهو وبين القراصنة ذوي الدوافع السياسية والإيديولوجية.[١]

د- لذلك من الضروري **التمييز بين الجرائم المعلوماتية والإرهاب بالوسائل الإلكترونية**، وكما يقول ASHISH PANDEY وهو الباحث في قانون الانترنت في الهند: (بأن جميع الأعمال الإرهابية الإلكترونية هي جرائم إلكترونية، ولكن ليست جميع الجرائم الإلكترونية تدخل ضمن الأعمال الإرهابية).

فالإرهاب الإلكتروني مفهوم يشمل على الجريمة الإلكترونية،[٢] ويكمن الفارق بين الإرهاب بالوسائل الإلكترونية والجريمة المعلوماتية، في الدافع على ارتكاب الجريمة، كما يكمن الفرق في الغالب بنتائج هذه الجرائم،[٣] فقد ذهب بعض الفقه إلى أنه لا يقع الإرهاب الإلكتروني إلا إذا تحقق شرط واحد وهو الهجوم الذي يسبب الضرر الكبير ويمكن في نهاية المطاف أن يؤدي إلى تصاعد الخوف والموت والدمار، ودون هذه العوامل لا يمكن أن يعد الهجوم إرهاباً إلكترونياً.[٤]

---

١ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص١٣.

٢ محمد سيد سلطان، المرجع السابق، ص١٢.

٣ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق، ص ١٦٣.

٤ محمد سيد سلطان، المرجع السابق، ص١٣.

وفي كتاب حول الإرهاب المعلوماتي الذي أنجزه باتريك كالي ضمّن فيه الخلاصة التالية " سأبقى مقتنعاً بأن الضربات الإرهابية التقليدية هي الأكثر تأثيراً في الرأي العام، لكن فداحة الخسائر ستحملها الهجمات الإرهابية المعلوماتية."[١]

٣_ التعريف في التشريع السوري

إن جل التشريعات العربية لم تتصدى لتعريف (الإرهاب الإلكتروني، الإرهاب بالوسائل الإلكترونية) بصورة مستقلة عن العمل الإرهابي (الجريمة الإرهابية)، وكذلك حال المشرع السوري الذي عدد الأفعال التي يمكن أن تعد إرهاباً على سبيل المثال لا الحصر .. في القانون رقم /١٩/ لعام **٢٠١٢**م الخاص بمكافحة الإرهاب، وكذلك الحال بالنسبة إلى المرسوم التشريعي رقم /١٧/ لعام **٢٠١٢**م الخاص بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية الذي لم يتطرق لتعريف الإرهاب بالوسائل الإلكترونية، وبالتالي إذا أردنا أن نعرف الإرهاب بالوسائل الإلكترونية في ضوء التعريفات السابقة، فيمكننا أن نعرف الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) بأنه:

"**كل فعل يهدف إلى نشر حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الإضرار بالبنية التحتية أو الأساسية أو المعلوماتية، ويستخدم نظم المعلومات أو التقنية الرقمية (الحواسيب أو الشبكات) كهدف أو وسيلة.**"

أي يمكننا القول إن الإرهاب بالوسائل لإلكترونية، هو كل فعل يستخدم النظم الرقمية أو التقنية كهدف أو وسيلة، فالنظرة إلى الإرهاب بالوسائل الإلكترونية لا تنحصر في الأعمال التخريبية مثل اختراق المواقع

---

١ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص٧.

الإلكترونية العسكرية والمدنية والسيطرة عليها أو تدميرها، بل تمتد لتشمل أنشطة أكثر خطورة، وهي الاستخدام اليومي للإنترنت من قبل الإرهابيين والجماعات الإرهابية، **وهذا التعريف يستند بشكل كبير إلى تعريف المشرع السوري للعمل الإرهابي في المادة الأولى من القانون رقم /١٩/ لعام ٢٠١٢م، الذي لم يحدد صورة الفعل الجرمي، واكتفى بتحديد العناصر المميزة له.**

ولا بد أن نشير إلى أن الاعتداءات التي تَطال الأجهزة والمواد ذات الوظيفة التكنولوجية أو الإلكترونية، كالاعتداءات التي تستهدف ماديات نظم الحاسب والشبكات تخرج عن نطاق الجرائم المعلوماتية وجرائم الإرهاب بالوسائل الإلكترونية لأنها محل صالح لانطباق نصوص التجريم المختلفة التي تستهدف المال المادي المنقول،[١] فالاعتداء المادي على الأنظمة والأجهزة المعلوماتية بالسرقة أو التخريب أو الأتلاف أو التفجير، تخضع للقواعد التقليدية في التجريم والعقاب.

بعد تبيان العناصر التي ينضوي عليها مصطلح الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) وتعريفه، سننتقل إلى تبيان تصنيفاته وأهم خصائصه والخطر الذي ينطوي عليه في الفرع التالي.

---

١ د. يونس عرب، مشروع قانوني نموذجي عربي لجرائم الكمبيوتر والإنترنت أو للجرائم الإلكترونية، المرجع السابق، لا يوجد رقم صفحة.

الفرع الثاني

تصنيف الإرهاب بالوسائل الإلكترونية وميزاته

أولاً: تصنيف الإرهاب بالوسائل الإلكترونية

تتعدد تصنيفات الإرهاب بالوسائل الإلكترونية، وتختلف باختلاف الأيدلوجيات المتعددة.

١- التصنيف الثلاثي

ومن هذه التصنيفات تصنيف "Collin" الذي قسم الإرهاب الإلكتروني إلى ثلاثة أنواع من الأفعال وهي: الدمار، والتعديلات، واقتناء وإعادة الإرسال.[١] كما صُنف الإرهاب الإلكتروني تصنيفاً آخر، وفقاً لهذا التصنيف يوجد ثلاثة أنواع من الأنشطة الهجومية يمكن للإرهابيين استخدامها: **أولاً**، يمكن للإرهابيين أن يستخدموا تكنولوجيا المعلومات لغرض الدعاية، **ثانياً**، استخدام شبكة الإنترنت لشن هجمات تخريبية، **وأخيراً**، يمكن استخدام هذه الشبكات لأغراض تدميرية.[٢]

٢- التصنيف الرباعي

ويُعد من أفضل التصنيفات المختلفة للإرهاب الإلكتروني التصنيف الذي جاء به "ballard" وهو عالم سلوك أمريكي، الذي صنفه إلى أربع أنواع وهي كالتالي:[٣]

هجوم المعلومات: يركز الإرهابيون على تغيير أو تدمير محتوى الملفات الإلكترونية، وأنظمة الحاسب أو أي مواد أخرى متصلة بالبيئة الإلكترونية.

---

١ محمد سيد سلطان، المرجع السابق، ص١٣.

٢ محمد سيد سلطان، المرجع السابق، ص١٣.

٣ محمد سيد سلطان، المرجع السابق، ص١٤.

هجمات البنية التحتية: هي الهجمات التي تستهدف تعطيل أو تدمير الأجهزة الفعلية، أو أنظمة التشغيل، أو البرمجيات، في بيئة محوسبة مما يؤدي إلى تدمير أو تعطيل البنية التحتية المعلوماتية.

تيسير التكنولوجيا: يتم من خلاله استخدام الحاسب الآلي وأنظمة الاتصال على التخطيط للهجمات الإرهابية، والتحريض عليها، أو تسهيل الإرهاب التقليدي.

جمع التبرعات: يستخدم الإرهابيون شبكة الإنترنت لجمع التبرعات من أجل قضية سياسية معينة، أو لجلب المساعدات/ أو لتعزيز أيديولوجية بديلة في التوجيه.

٣- تصنيف الدكتور يوسف بن أحمد الرميح رئيس قسم الاجتماع والخدمة الاجتماعية /جامعة القصيم/ السعودية

حيث قسم الإرهاب الإلكتروني إلى ثلاثة مجموعات هي:[١]

المجموعة الأولى: الجرائم التي تستهدف النظم والمعلومات كهدف.

المجموعة الثانية: الجرائم التي تستخدم وسائل التكنولوجيا المعلومات كوسائل لارتكاب الجرائم.

المجموعة الثالثة: الجرائم التي ترتبط بمحتوى مواقع المعلومات وبياناتها.

وبعد العرض السابق للتصنيفات المختلفة للإرهاب الإلكتروني، يمكننا أن نصنف الإرهاب الإلكتروني إلى ثلاث أنواع هي:

هجوم المعلومات: يقوم على تغيير أو تدمير محتوى الملفات الإلكترونية، وأنظمة الحاسب أو أي مواد أخرى متصلة بالبيئة الإلكترونية.

هجمات البنية التحتية: التي تستهدف تعطيل أو تدمير الأجهزة الفعلية، أو أنظمة التشغيل، أو البرمجيات، مما يؤدي إلى تدمير أو تعطيل البنية التحتية

---

١ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية: سوسيولوجية، المرجع السابق، ص ٢٢٣.

المعلوماتية أو السيطرة عليها من قبل الإرهابيين **وهي الصورة الرئيسية للإرهاب بالوسائل الإلكترونية.**

تيسير التكنولوجيا: يتم من خلاله استخدام الحاسب الآلي وشبكة الإنترنت وأنظمة الاتصال على التخطيط للهجمات الإرهابية، والتحريض عليها، وإنشاء مواقع إلكترونية، وجمع التبرعات والتمويل، والتجنيد والتدريب، أو تسهيل الإرهاب بصورتيه التقليدية أو الإلكترونية.

ثانياً: خصائص الإرهاب بالوسائل الإلكترونية

يتميز الإرهاب بالوسائل الإلكترونية بالعديد من الخصائص والسمات التي يختلف فيها عن بقية الجرائم، وتحول دون اختلاطه بالإرهاب التقليدي، ومن بين الخصائص الأساسية للإرهاب بالوسائل الإلكترونية هي:

١- استهداف النظم المعلوماتية، فهذه الخاصية هي التي تشكل الخط الفاصل بينه وبين باقي الصور الأخرى للظاهرة.[١]

حيث تشكل المنظومات المعلوماتية الهدف المباشر لمخططاته التخريبية، والوسيلة المحققة لأهدافه غير المباشرة، المتمثلة في خلق حالة من الرعب في أوساط المجتمع،[٢] وعدم تطلب عملياته لموارد مالية وبشرية مرتفعة الكلفة والعدد، مقارنةً مع متطلبات الإرهاب التقليدي،[٣] واستخدام التقنيات الحديثة أو الأساليب المبتكرة في كل عملية من مراحل الجريمة، والأمر الأبرز أن عملية الاستحداث ذاتها متطورة ومتجددة مع كل تطور تقني.[٤]

---

[١] عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص١٠.

٢ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص١٠.

٣ عبد الحق باسو، المرجع السابق، ص١٤.

٤ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي: رؤية سوسيولوجية، المرجع السابق، ص ٢٢٤.

٢- يتم الإرهاب بالوسائل الإلكترونية في حالة من المتعة والسرور بعيداً عن الخوف والقلق، وبعيداً عن أعين الناظرين، ويتم عن بعد دون اللجوء إلى العنف المادي أو الجسدي،[١] فهو لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.[٢]

٣- ويتسم أيضاً بأنه عابر للدول والقارات،[٣] أي تدويل الجريمة وإخراجها من الحدود الوطنية والإقليمية سواء في مرحلة الإعداد أو التنفيذ أو الآثار المترتبة عليها،[٤]وتخلق هذه الخاصية كثيراً من التحديات القانونية في مواجهتها والتصدي لها فيما يتعلق بمدى إمكانية تطبيق التشريعات الوطنية على هذه الجرائم ومبدأ إقليمية القانون الجزائي،[٥] وصعوبة اكتشاف جرائم الإرهاب بالوسائل الإلكترونية ونقص الخبرة لدى بعض الجهات الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم، وصعوبة إثبات هذه الجريمة، لغياب الدليل الرقمي من ناحية، وسهولة إتلافه وتدميره من ناحية أخرى.[٦]

٤- كما أن مرتكب هذه الجريمة يكون من المختصين في مجال تقنية المعلومات.[٧]

٥- وتتسم هذه الجريمة أيضاُ بارتفاع تكلفتها وتعاظم أثارها على البنية الاجتماعية وذلك من حيث حجم الضحايا والمصابين مادياً ونفسياً.[١]

---

١ د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، المرجع السابق، ص ٩٤.

٢ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٣ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ١٠.

٤ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي: رؤية سوسيولوجية، المرجع السابق، ص٢٢٤.

٥ د. فراس طحان، المرجع السابق، ص ٣٦٧.

٦ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ١٠.

٧ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

علماً أن الخسائر الناجمة عن الإرهاب الإلكتروني تتجاوز أحياناً الخسائر الناجمة عن الإرهاب التقليدي خاصةً في الدول التي تعتمد بشكل رئيسي على تقنية المعلومات.[٢]

ثالثاً: خطر الإرهاب بالوسائل الإلكتروني

يتميز الإرهاب بالوسائل الإلكترونية عن غيره من أنواع الإرهاب، بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف للإرهابيين.[٣]

١- نظراً لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية، فقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة.

٢- أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وهناك ما يشير إلى إمكانية انهيار البنى التحتية للأنظمة والشبكات المعلوماتية في العالم كله، وليس في بعض المؤسسات والشركات الكبرى أو في بعض الدول المستهدفة.

---

١ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية سوسيولوجية، المرجع السابق، ص ٢٢٤.

٢ د. فراس طحان، المرجع السابق، ص ٣٦٨.

٣ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ٦.

٣- والإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره،[١] حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخٍ في منزله أو في مكتبه أو غرفته الفندقية، وبعيداً عن أنظار السلطة والمجتمع.

٤- وتجدر الإشارة إلى أن تدمير شبكة معلوماتية تقدر خسائرها اليومية بأضعاف مضاعفة لانهيار مبنى أو قصف منشأة أو تفجير جسر أو اختطاف طائرة.[٢]

٥- وإن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة والتي تُدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات، حيث تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق أثار تدميرية تفوق مثيلتها في التفجيرات، حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية

---

١ د. عبد الرحمن عبد الله السند، المرجع السابق، ص٥.

٢ قُدرت الخسائر التي لحقت بقطاع الاتصالات والتعاملات الإلكترونية بمئات الملايين من الدولارات، وذلك عند انقطاع الكيبل البحري الذي يربط أوروبا بالشرق الأوسط في نهاية شهر يناير عام ٢٠٠٨، وما أعقبه من انقطاع أخر للكيبل القريب من ساحل دبي وخليج عُمان، ، ولا تزال الأسباب مجهولة من وراء ذلك الانقطاع المفاجئ. أنظر: عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية.[١]

وقد لخصت الدكتورة Solange Ghenaout المسؤولة عن شعبة الأمن المعلوماتي وأستاذة التعليم العالي بجامعة لوزان، المخاطر التي يمكن أن تحملها الجريمة الإرهابية الإلكترونية فيما يلي: **إن السيطرة والتحكم في البنى التحتية الحساسة هي أهم أولويات الإرهاب الإلكتروني.**[٢]

ونحن مع القول بإن الإرهاب بالوسائل الإلكترونية هو إرهاب الغد، نظراً لتعدد أشكاله وتنوع أساليبه، واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها، مع توفير قدر كبير من السلامة والأمان للإرهابيين.[٣]

وبعد تعريف مصطلح الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) وتبيان أهم تصنيفاته وخصائصه والخطر الذي ينضوي عليه في المطلب الأول، سننتقل إلى دراسة مظاهر الإرهاب بالوسائل الإلكترونية وذلك في المطلب الثاني.

---

[١] أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ٦.

٢ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص٧.

٣ د. يوسف بن أحمد الرميح، الإرهاب الإلكتروني. وشبكات التواصل (٢-٢)، نقلا عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ١٧ أغسطس ٢٠١٣م، متاح على الرابط: www.assakina.com/news/news١/٢٧١٤٥.html، تاريخ الزيارة: ٢٠١٤/١١/٩م.

المطلب الثاني

مظاهر الإرهاب بالوسائل الإلكترونية

أصبح الإرهاب بالوسائل الإلكترونية حقيقةً واقعية، فمرونة تكنولوجيا المعلومات والحاسب والإنترنت هي التي ساعدت الأصابع الخبيثة كي تنشر العنف والخوف ولكي تخطط وتنفذ جرائمها، لذلك لابد لنا من تقسيم هذا المطلب إلى فرعين:

الفرع الأول: أشكال الإرهاب بالوسائل الإلكترونية

الفرع الثاني: النماذج التطبيقية للإرهاب بالوسائل الإلكترونية

الفرع الأول

أشكال الإرهاب بالوسائل الإلكترونية

من الصعب تحديد أشكال الإرهاب بالوسائل الإلكترونية جميعها، فطبيعته تتطلب اللامحدودية لأنه يستخدم تكنولوجيا تتطور يوماً بعد يوم، لكن يمكن أن نذكر بعضها والتي يتمثل أبرزها في:

أولاً: إنشاء المواقع الإلكترونية[١] الإرهابية

تسعى المؤسسات والشركات والجهات الرسمية وحتى الأفراد إلى امتلاك مواقع على شبكة الإنترنت للتعريف بأنفسهم وإتاحة خدماتهم لمستخدمي

---

١ الموقع الإلكتروني هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل (HTML) / HYPER TEXT MARK UP LANGUAGE ولأجل عرض هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (WWW BROWSER) ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة. أنظر: عبد الرحمن عبد الله السند، المرجع السابق، ص ١٣.

والمقصود بالنطاق أو الموقع هو الاسم الذي يشير إلى الحيز الذي يملكه شخص طبيعي أو اعتباري معين من فضاء الإنترنت، ويمكن ترجمته إلى عنوان معين في الشبكة. أنظر: اللواء د. مصطفى محمد موسى، التنظيمات الإرهابية وشبكة الإنترنت، الندوة العلمية استشراق التهديدات الإرهابية، الرياض، المملكة العربية السعودية، ٧-١٤٢٨/٨/٩هـ الموافق ٢٠-٢٠٠٧/٨/٢٢م، ص٣٩.

الإنترنت، فقد وصل عدد مواقع الإنترنت حتى شهر تشرين الأول ٢٠١٠ إلى أكثر من ٢٣٢ مليون موقع.

وقد وجد الإرهابيون ضالتهم في هذه الوسيلة الرقمية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة الإنترنت، فغدت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب بالوسائل الإلكترونية.[١]

ويقوم الإرهابيون بإنشاء وتصميم مواقع على شبكة الإنترنت لنشر الأفكار والدعوات الإرهابية، بل وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغيرها.[٢]

ولابد من الإشارة إلى إن المواقع الإلكترونية الإرهابية يستضيفها مزود خدمات الإنترنت الغربية بصورة مباشرة أو غير مباشرة، وهذه المواقع تطورت من أربعة مواقع عام ١٩٩٨م إلى قرابة العشرة عام ٢٠٠١م، وبعد أحداث ١١ أيلول ٢٠٠١م حصل تزايد في هذه المواقع بحيث تم افتتاح أربعة آلاف موقع في غضون أربع سنوات، وزادت بعد ذلك زيادة أكبر مما يدل على خطورة هذه الجرائم وتناميها.[٣]

---

١ عبد الرحمن عبد الله السند، المرجع السابق، ص١٥.

٢ د. محمد بن عبد الله آل فايع العسيري و د.حسن بن أحمد الشهري، الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، المرجع السابق، ص٢٢٧.

٣ د. فراس طحان، المرجع السابق، ص٣٧٠.

ثانياُ: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم الجماعات الإرهابية بشن هجمات إلكترونية من خلال شبكة الإنترنت بقصد تدمير المواقع والبيانات الإلكترونية، والنظم المعلوماتية، وإلحاق الضرر بالبنية التحتية المعلوماتية وتدميرها.[١]

ويقصد **بالتدمير:** الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بشبكة الإنترنت من خلال نظام آلي (server – pc) أو مجموعة نظم مترابطة شبكياُ بهدف تخريب نقطة الاتصال أو النظام،[٢] وليس هناك وسيلة تقنية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم، فالمتغيرات التقنية وإلمام المخترق بالثغرات في التطبيقات التي بنيت بمعظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source) سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة أو البرمجة، جعلت الحيلولة دون الاختراقات صعبة جداً.[٣]

وسنشير إلى أبرز الوسائل التي يتم فيها الاختراق أو التدمير من قبل الجماعات الإرهابية:

١- **الاقتحام أو التسلل:** تتم عملية الاقتحام من خلال برامج يتم تصميمها لهذا الغرض، ولا يتم كشفها بواسطة برامج مكافحة الفيروسات، ويقوم هذا البرنامج بالتجسس على أعمال المستخدم للجهاز المُخَترق وتسجيل كل تحركاته على الحاسب الآلي وبياناته السرية وحساباته المالية ومحادثاته الخاصة عبر شبكة الإنترنت ورقم بطاقة الائتمان الخاصة به، وحتى كلمات المرور المستخدمة لدخول البريد الإلكتروني، خاصة أن

---

[١] د. فراس طحان، المرجع السابق، ص٣٧٠.

٢ عبد الرحمن عبد الله السند، المرجع السابق، ص ١٤.

٣ أ.د. جميل عبد الباقي الصغير، المرجع السابق، ص١٥.

مرتكبي هذه الجرائم يملكون الكفاءة في استخدام الحاسب الآلي، وليس للبعد الجغرافي أي أهمية في الحد من الاختراقات الإلكترونية.[١]

فقد دمرت منظمة إرهابية أسترالية عام ٢٠٠٠ شبكة الصرف الصحي بواسطة عملية إلكترونية، وفي العام نفسه اخترقت منظمة أدم شيريكو اليابانية الإرهابية البرامج المتحكمة بمسار سيارات الخدمة العامة.[٢]

وفي إحدى الهجمات الإرهابية تمكن الإرهابيون من السيطرة على نظام الحاسب الآلي في أحد المطارات الأمريكية الصغيرة، وتمكنت من إطفاء مصابيح إضاءة ممرات هبوط الطائرات.[٣]

٢-الفيروسات: تعد الفيروسات من أخطر آفات الشبكة، حيث يستخدمها الإرهابي في تدمير المواقع وتعطيلها، كما يمكن استخدامها في الاختراق والتجسس.[٤]

والفيروسات هي عبارة عن برنامج حاسوبي يُلحق الضرر بنظم المعلومات والبيانات ولها قدرة على التكاثر والانتقال من جهاز إلى أخر وتغيير شكلها، وقد تمّكن فيروس Blaster عام ٢٠٠٣م من تدمير نصف مليون جهاز حاسوب.[٥]

٣-الإغراق في الرسائل /القصف الإلكتروني/[٦]: يتم تدمير المواقع الإلكترونية من خلال ضخ مئات آلاف الرسائل الإلكترونية من جهاز الحاسوب الخاص بالإرهابي إلى الموقع الإلكتروني المستهدف للتأثير

---

١ د. فراس طحان، المرجع السابق، ص ٣٧١.

٢ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، لا يوجد رقم صفحة.

٣ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ١٥.

٤ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ١٦.

٥ د. فراس طحان، المرجع السابق، ص٣٧٠.

٦ الإرهاب الإلكتروني، جولة في عقل متطرف، نقلاً عن صحيفة العرب الإلكترونية، موقع السكينة، تريخ النشر: ١٧ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com/awareness-net/terrorism-net/٤٤٦٥٧.html، تاريخ الزيارة: ٢٠١٥/٢/٢م.

على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة، وتشتيت البيانات والمعلومات المخزنة في الموقع، فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من معلومات وبيانات خاصة بالموقع المعتدى عليه.[١]

لذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة (تدفق أعداد كبيرة منها).[٢]

ثالثاً: نشر وتبادل المعلومات الإرهابية من خلال شبكة المعلومات

يصعب في الواقع الملموس على المنظمات العاملة في حقل الإرهاب الاجتماع في نقطة مكانية وزمانية محددة نظراً إلى الرقابة الأمنية المشددة، لكن بفضل الطرق المعلوماتية السريعة أصبح الأمر ميسوراً، إذ يمكن من خلال غرف الدردشة والمنتديات جمع في وقت محدد عدد من الأشخاص في أماكن جغرافية متفرقة، للتشاور وتبادل المعطيات والاستراتيجيات، فضلاً عن البريد الإلكتروني الذي يسمح من جهة بنقل الملفات والمعلومات بسرعة مذهلة وآمنة، ومن جهة أخرى بنشر الأفكار المتطرفة والترويج لها لكسب الدعم والأتباع.[٣]

ويعد البريد الإلكتروني من أهم الوسائل المستخدمة في الإرهاب بالوسائل الإلكترونية، حيث إن كثيراً من العمليات الإرهابية ارتكبت نتيجة لاستخدام

---

١ د. سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجية الأمن القومي، مؤتمر الجرائم المستحدثة-كيفية إثباتها ومواجهتها، ١٥-١٦ ديسمبر ٢٠١٠م، القاهرة، مصر، ٢٠١٠م، ص٥.

٢ اللواء. عبد الحميد ابراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، ما هو دور القطاع الخاص، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، ١١-١٤٢٧/٣/١٥هـ الموافق ٩-٢٠٠٦/٤/١٣م، المغرب-القنيطرة،١٤٢٧هـ-٢٠٠٦م، ص٤٦.

٣ عبد الرحمن عبد الله السند، المرجع السابق، ص٩.

البريد الإلكتروني في تبادل المعلومات بين القائمين بالعمليات الإرهابية والمخططين لها.[١]

ومما يقوم به الإرهابيون أيضًا اختراق البريد الإلكتروني للآخرين (أفراد، مؤسسات)، وهتك أسرارهم، والاطلاع على معلوماتهم وبياناتهم، والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم التخريبية.[٢]

إن النظرة إلى الإرهاب بالوسائل الإلكترونية كانت تنحصر في الأعمال التخريبية مثل اختراق المواقع الإلكترونية العسكرية والمدنية، وأغفلت تماماً أنشطة أكثر خطورة، وهي الاستخدام اليومي للإنترنت من قبل الإرهابيين والجماعات الإرهابية،[٣] فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة، حيث يمكن للإرهابيين استخدام الشبكة في:

١- **الاتصال والتخفي:** تستخدم الجماعات والمنظمات الإرهابية المختلفة شبكة الإنترنت في الاتصال والتنسيق فيما بينهم، نظراً إلى قلة تكاليف الاتصال باستخدام الشبكة مقارنةً بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال والتخفي، ولذا يشارك العديد من الإرهابيين في حساب واحد للبريد الإلكتروني، ولا يبعث الشخص الذي يكتب الرسالة بها، بل يحتفظ بها في ملف المسودات، ثم يدخل الشخص الأخر الشبكة ويطلع على المسودة دون إرسالها على الإطلاق.[٤]

---

١ عبد الرحمن عبد الله السند، المرجع السابق، ص٩.

٢ د .محمد بن عبد الله آل فايع العسيري و د.حسن بن أحمد الشهري، الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، المرجع السابق، ص٢٢٦.

٣ كتاب الإرهاب على الشبكة العالمية، موقع السكينة، تاريخ النشر: ١٦ يناير ٢٠١٠م، متاح على الرابط:www.assakina.com/ceuter/red-book/٤٦٦٨.html، تاريخ الزيارة: ٢٠١٣/٦/٥م.

٤ أ.د. عبد الله بن ناصر الحمود، المرجع السابق، ص ٦٠.

وبالمثل فإن الإرهابيين يتصلون ببعضهم البعض عبر منتديات الألعاب الإلكترونية، وفي بعض الأحيان يستخدمون الدردشة على الهواء في مواقع الألعاب الإلكترونية اليابانية، التي لا يتنصت عليها إلا المراهقون.[١]

٢- **جمع المعلومات الإرهابية:** تعد شبكة الإنترنت موسوعةً شاملة، متنوعة المصادر، غنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية والمواقع العسكرية، وأماكن السيطرة والقيادة، ومصادر توليد الطاقة، والخرائط، ومواعيد الرحلات الجوية الدولية، وغالباً ما تكون مدعمة بالصور الضوئية،[٢] وبذلك يكون ٨٠% من مخزونهم المعلوماتي معتمداً في الأساس على مواقع إلكترونية متاحة للكل، دون أي خرق لقوانين الشبكة وبروتوكولاتها.[٣]

٣- **التخطيط والتنسيق للعمليات الإرهابية:** إن العمليات الإرهابية على جانب من التعقيد والصعوبة، فهي تحتاج إلى تخطيط محكم، وتنسيق شامل للمعلومات، وتُعد الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية، حيث تتيح لهم حرية التخطيط والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيداً عن أعين الناظرين، مما يسهل للإرهابيين ترتيب تحركاتهم، وتوقيت هجماتهم.[٤]

---

١ أ.د. عبد الله بن ناصر الحمود، المرجع السابق، ص ٦٠.

٢ د. فراس طحان، المرجع السابق، ص ٣٧٥.

٣ كتاب الإرهاب على الشبكة العالمية، المرجع السابق.

٤ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٤- **التعبئة وتجنيد الإرهابيين:** تستخدم الجماعات الإرهابية شبكة الإنترنت بشكل مكثف لتجنيد وتدريب وتلقين المجندين،[١] حيث تبث الجماعات الإرهابية في شبكة الإنترنت الأفكار والفلسفات التي تنادي بها، وبالتالي تتمكن هذه الجماعات من تكوين قاعدة فكرية لدى ذوي الميول والاستعداد للانخراط في الأعمال التخريبية، ويمكنها تجنيدهم لتنفيذ هجمات إرهابية،[٢] إذ إن استقدام عناصر جديدة داخل التنظيمات الإرهابية، يحافظ على بقائها واستمرارها.[٣]

كولين روز مواطنة أمريكية مواليد ١٩٦٣، تعرف بالاسم الحركي **جهاد جين** من أكثر النساء المتطرفات فاعلية وتأثيراً ومقدرة على نشر المواد الداعمة للإرهاب، وعلى تسهيل وصول هذه المواد للباحثين عن التطرف. استطاعت تكوين خلية افتراضية وجعلت منهم نشطاء، وحولتهم إلى قادرين على تنفيذ عمليات ميدانية، امرأة عادية تعيش حياة

---

١ Patrick chambet,le cyber-terrorisme, DISPONIBLE SUR LE LIN: www.chambet.com/publications/ le cyber-terrorisme.pdf, Date de la visite: ١٢/٤/٢٠١٥.

٢ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص١٣.

٣ حيث لم يمض الكثير من الوقت لتغيب عن الذاكرة حادثة الشاب السعودي سليمان السبيعي /السمبتيك/ أشهر السعوديين الذين ذهبوا للقتال في سورية، الذي عاد عبر شاشة القناة الأولى السعودية في برنامج "همومنا" ليكشف قصة ذهابه وتجنيده عن طريق الإنترنت. أنظر: الكاتب تركي تركي، وسائل التواصل الاجتماعي..تسويق الإرهاب وإعادة تدويره، نقلاً عن الاقتصادية، موقع السكينة، تاريخ النشر: ١٣ يوليو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٣/٢م.

وقال "السمبتيك" ٢٥ عاماً إن ذهابه إلى القتال في سورية بعد مقتل أخيه عبد العزيز الذي كان يقاتل في سورية في تلك الفترة. أما وصوله لساحات القتال فكان مساعدة مهرب سوري تعرف عليه عن طريق "تويتر". أنظر: الكاتب تركي تركي، وسائل التواصل الاجتماعي.. تسويق الإرهاب وإعادة تدويره، المرجع السابق.

أمريكية لم تلتق أياً من رموز الإرهاب لكنها تبنت أفكارهم عبر الإنترنت.[١]

ويذكر الغرب أن سبعمائة أوربي ذهبوا للجهاد في سورية بسب التأثر بوسائل التواصل الاجتماعي، خاصة أن المشكلة تفاقمت بعد قيام القاعدة بالترجمة إلى لغات عديدة كالفرنسية والإنكليزية والروسية وغيرها، ويكاد العالم أجمع يتفق على هذه المعضلة.[٢]

٥- **الحصول على التمويل (التمويل الإلكتروني):** لا تستطيع الجماعات الإرهابية القيام بعملياتها الإرهابية دون توافر التمويل الكافي الذي يُمَكّنها من القيام بذلك، وتتعدد وتتنوع مصادر التمويل للإرهاب والإرهابين، وفي ظل التطور التقني والمعلوماتي الهائل استفاد الإرهابيون من شبكة الإنترنت في تمويل ودعم انشطتهم، بل أضحت شبكة الإنترنت من أهم مصادر التمويل،[٣]حيث يقوم الإرهابيون من خلال شبكة الإنترنت وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون إلى الشبكة المعلوماتية،[٤] بالتعرف على الأشخاص واستجدائهم بدفع تبرعات لأشخاص اعتبارية أو مؤسسات خيرية تكون واجهة لتنظيمات إرهابية، بصورة لا يشك فيها المتبرع بقيامه بمساعدة أحد التنظيمات الإرهابية.[٥] كما يتم استخدام الحوالات الإلكترونية بمبالغ صغيرة لتجنب الوصول إلى الحد المقرر للعمليات المقررة والتي قد توقع المودع تحت طائلة

---

١ جهاد جين (سيدة الإرهاب الإلكتروني)، موقع السكينة، تاريخ النشر: ١٠ يناير ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٤/٢م.

٢ الإرهاب الإلكتروني جولة في عقل متطرف، المرجع السابق.

٣ د. نايف بن محمد المرواني، المرجع السابق، ص١٠.

٤ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٥ د. فراس طحان، المرجع السابق، ص ٣٧٤.

القانون، الحوالات الإلكترونية من وإلى شخص ما في الوقت الذي لا تتوافر فيه المعلومات كافية عن المحول أو المستفيد.[١]

ويتبع في بعض الحالات غسل الأموال عن طريق الإنترنت، إذ يمكن غسل الأموال باستخدام البطاقة الذكية التي تسمح بتحويل الأموال عبر شبكة الإنترنت مع ضمان أمنها.[٢]

٦- **التدريب الإرهابي الإلكتروني أو التلقين الإلكتروني:** نظراً إلى أن معسكرات التدريب الإرهابية التقليدية يكون من الممكن اكتشافها ومداهمتها، فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات، أصبحت وسيلةً مهمةً للتدريب الإرهابي، بعيداً عن أعين رجال الأمن، حيث قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وهذه الأدلة يمكن نشرها عبر شبكة الإنترنت لتصل إلى الإرهابيين في أنحاء العالم المختلفة.[٣]

فقد استغل الإرهاب الحاسب والكاميرا إلى أقصى حد ممكن فأصبحت تقدم أدلة عسكرية على شكل كتب وأفلام وسلايدات تتضمن معلومات شتى عن الأسلحة والاغتيالات وصنع المتفجرات والسموم.[٤]

لقد أصبحت شبكة الإنترنت وكأنها معسكر افتراضي للإرهابيين،[٥] وقد نشرت مجلة النيويورك تايمز تقرير يؤكد أن ٩٠% من الهجمات

---

١ د. نايف بن محمد المرواني، المرجع السابق، ص١٠-١١.

٢ د. فراس طحان، المرجع السابق، ص ٣٧٤.

٣ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٤ د. يوسف بن أحمد الرميح، الإرهاب الإلكتروني. وشبكات التواصل (٢-٢)، المرجع السابق.

٥ أصبح الإنترنت شبه بديل لمعسكرات التدريب لهذه الجماعات ووفقاً لتقرير أصدره الجيش الأمريكي في في شهر أيار ٢٠٠٧م تم العثور في حواسيب منفذي العملية الإرهابية بمحطات القطار في مدريد على نحو ٥٠ كتاباً من تأليف مفكرين راديكاليين تم تنزيلها من شبكة الإنترنت، وشكلت للإرهابيين مصدراً استمدوا منه إيحاءهم وغني عن البيان ما تشتمل شبكة المعلوماتية من كم هائل من المواقع والمنتديات التي تحتوي

الإرهابية استخدم فيها متفجرات صناعة يدوية من تلك التي توجد وصفاتها بكثرة على الإنترنت.[١]

٧- **إصدار البيانات الإلكترونية:** تستخدم المنظمات الإرهابية شبكة الإنترنت في نشر بياناتها وذلك من خلال المواقع الإلكترونية أو بواسطة البريد الإلكتروني أو من خلال منتديات الحوار، [٢] وتأخذ البيانات الصادرة من قبل المنظمات الإرهابية اتجاهات متنوعة، فتارةً ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي، وأحياناً تكون للتهديد والوعيد بشن هجمات إرهابية معينة، في حين تصدر معلنة عن تبني عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار أو تصريحات صادرة من جهات أخرى.[٣]

رابعاً: التهديد الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد باستخدام شبكة الإنترنت، وتتعدد أساليب التهديد وتتنوع طرقه سواء بالقتل أو بتفجير منشآت، أو نشر فيروسات، أو تدمير بنى تحتية،[٤] من أجل نشر الخوف والرعب بين الأفراد والدول والشعوب في محاولة للضغط عليهم للرضوخ لأهداف تلك

على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة المدمرة. أنظر: د. فراس طحان، المرجع السابق، ص ٣٧٤.

١ د. يوسف بن أحمد الرميح، معركتنا ضد الإرهاب على الساحة الافتراضية الإلكترونية، نقلاً عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ١١ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٥/١م.

٢ أ.د. جميل عبد الباقي الصغير، المرجع السابق، ص١٣.

٣ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٤ د. فراس طحان، المرجع السابق، ص ٣٧٥.

التنظيمات من ناحية، ومن أجل الحصول على التمويل المالي، ولإبراز قوة التنظيم الإرهابي من ناحيةٍ أخرى.[١]

خامساً: التجسس الإلكتروني

في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدول مستباحة بأقمار التجسس والبث الصناعي، ولقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وانتشاره عالمياً.[٢]

والتجسس الإلكتروني هو التلصص وسرقة المعلومات،[٣] حيث يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الوطنية أو الدولية، وذلك باستخدام الأنظمة الإلكترونية بهدف تحقيق التجسس العسكري أو السياسي أو الاقتصادي.[٤]

وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق، ومن أشهرها البريد الإلكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، كما يمكن للإرهابي استخدام الفيروسات في الاختراق والتجسس المعلوماتي.[٥]

---

١ أياد علي الدرة، الإرهاب الإلكتروني، المرجع السابق.

٢ اللواء. عبد الحميد ابراهيم محمد العريان، المرجع السابق، ص٣١.

٣ د. يوسف بن أحمد الرميح، الإرهاب والاعلام الجديد (الإرهاب الرقمي) ١-٢، صحيفة الجزيرة الإلكتروني، العدد ١٥٥٠٠، ٢٠١٥/٣/٧م، متاح على الرابط: www.al-jazirah.com/٢٠١٥/٢٠١٥٠٣٠٧/ar.ihtm، تاريخ الزيارة: ٢٠١٥/٥/٥م.

٤ أ.د جميل عبد الباقي الصغير، المرجع السابق، ص ١٧.

٥ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

كما يقوم الإرهابيون باختراق البريد الإلكتروني للأشخاص وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة في عملياتهم الإرهابية.[١]

وتجدر الإشارة إلى أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس وتم الحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن.[٢]

الفرع الثاني
النماذج التطبيقية للإرهاب بالوسائل الإلكترونية

تزداد التهديدات الإرهابية يوماً بعد يوم، خصوصاً بعد أن أصبح الإنترنت جزء أساسياً من حياتنا اليومية، فالإنترنت يستخدم في (المفاعلات النووية، الكهرباء، المياه، خطوط الملاحة الجوية والبرية والبحرية، البنوك، البورصة..) وغيرها الكثير، فتعطيل مثل هذه المجالات يؤدي إلى نتائج مادية خطيرة.

وفيما يلي سنتحدث عن الهجمات الإرهابية الإلكترونية التي قد تستهدف الأهداف العسكرية والسياسية، أو الأهداف الاقتصادية والمالية.

---

١ د. سعد عطوة الزنط، المرجع السابق، ص٤.

٢ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

أولاً: الهجوم على الأهداف العسكرية والسياسية

يستهدف هذا النوع من الهجوم عادةً الأهداف العسكرية غير المدنية والسياسية، المرتبطة بشبكة المعلومات، ويعد هذا الهجوم من أخطر الهجمات التي قد تعصف بمجتمعنا المعاصر،[١] فبالنسبة للأهداف العسكرية هو نادر الحدوث عادةً لأسباب عدة أهمها أن الدولة تفصل بين معلوماتها العسكرية والواقع الافتراضي، ولا تقوم بتوصيل الأجهزة التي تحمل المعلومات بالعالم الخارجي بأي شكل من الأشكال.[٢]

وقد أتاح برنامج غوغل إيرث Google earth الشهير الموجود على الإنترنت والذي جعل الدول كتاباً مفتوحاً، من خلال عرض صور للكرة الأرضية وخرائط الدول بتفاصيل دقيقة جداً إلى حد عرض أسماء الشوارع والأزقة بأسمائها الشعبية أحياناً، فما على مستخدم البرنامج سوى الضغط على منطقة ذات دلالة معينة، وحينئذ ستنبثق إحدى نوافذ ديسكفري التي تضم روابط لملفات الفيديو كلها ومعلومات الموسوعة حول هذه المنطقة، وعرض الصور لها بما فيها المناطق العسكرية أيضاً، وهي الخدمة التي أحدثت هزة في العالم نتيجة خوضها في المحظور، وانتهاك خصوصية الدول، ولربما خدمة للإرهابيين لمراقبة العالم عبر الإنترنت.[٣]

ومن الأمثلة التطبيقية على أنواع الجرائم التي تمس الأمن الاستراتيجي والعسكري، تلك الجريمة التي قام بها "ريتشارد برايس"، والذي يبلغ من العمر ستة عشر عاماً وهو بريطاني الجنسية حيث استخدم شبكة الإنترنت

---

١ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٢ د. سعد عطوة الزنط، المرجع السابق، ص ٦.

٣ سهير عثمان عبد الحليم، المرجع السابق، ص ٨.

لاختراق محطة الأبحاث النووية لكورية الشمالية، وشبكة القوات الجوية الأمريكية، مما كان سيعرض هذه المجتمعات لكارثة نووية وعسكرية خطيرة.[١]

أما الهجمات التي تستهدف مواقع سياسية فهي منتشرة وكثيراً ما حدثت على أرض الواقع، منها نجاح الإنكليزي (نيكولاس أندرسون) في اختراق موقع البحرية الأمريكية وسرقة كلمات السر والأكواد الخاصة المستخدمة في الهجوم النووي.[٢]

وفي مايو ٢٠٠٧م تعرضت استونيا لهجوم إلكتروني كبير بعد إزالة النصب التذكاري للحرب العالمية الثانية، وكان الهجوم هجوم حرمان من الخدمة، وخرجت الشبكات الحكومية الاستونية كلها تقريباً عن الخدمة.[٣]

---

١ د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية سوسيولوجية، المرجع السابق، ص ٢٣٣.

٢ محمد سيد سلطان، المرجع السابق ص١٥.

٣ Cyberterrorisme, DISPONIBLE SUR LE LIN:

https:fr.wikipedia.org/wiki/cyberterrorisme, Date de la visite: ١١/٥/٢٠١٥.

ثانياً: الهجوم على الأهداف الاقتصادية والمالية[١]

أصبح الاعتماد على شبكات الحاسوب شبه مطلق في عالم المال والأعمال، مما جعل هذه الشبكات نظراً لطبيعتها المترابطة، وانفتاحها على العالم، هدفاً مغرياً، ومما يزيد من إغراء الأهداف الاقتصادية والمالية، هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات أو تخريبها يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي.[٢]

ويسعى الإرهابيون إلى مهاجمة الأهداف الاقتصادية والمالية لسببين: الأول، أنهم بحاجة للأموال، والثاني هو أن الهجمات الموجهة ضد نظم المعلومات الاقتصادية والمالية لها تأثير كبير في الرأي العالمي.[٣]

ثالثاً: استهداف محطات توليد الطاقة والماء

أصبح الاعتماد على شبكات المعلومات وخصوصاً في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربائية، ويمكن لهجمات على مثل هذا

---

[١] ومن الأمثلة على الهجمات الاقتصادية، العملية التي قام بها مجموعة من الإرهابيين، أطلقوا على أنفسهم اسم (نادي الفوضى)، في عام ١٩٩٧م حيث قام هؤلاء الشباب بإنشاء برنامج تحكم لغة (أكتف إكس) مصمم للعمل عبر شبكة الإنترنت، ويمكنه أن يخادع برنامج (Quicken) الذي يقوم بتحويل الأموال من الحساب المصرفي إلى المستخدمين، وباستخدام هذا البرنامج أصبح بإمكانهم سرقة الأموال من أرصدة مستخدمي برنامج (Quicken) في جميع أنحاء العالم. أنظر: محمد سيد سلطان، المرجع السابق، ص١٦.
ومن الأمثلة التطبيقية على الهجمات الاقتصادية نذكر أيضاً، جريمة لصبي يبلغ من العمر ستة عشرة سنة من أصل استرالي، والذي استطاع الدخول إلى أحد المواقع البولندية على شبكة الإنترنت، وقام بتحميل البرامج التي تستخدمها البنوك، لكي يتوصل إلى الترتيب العشوائي لترقيم بطاقات الائتمان. وبعد أن توصل إلى الأرقام الصحيحة لهذه البطاقات، استخدمها في شراء أجهزة الحاسوب التي بلغت قيمتها ٣٧ ألف دولار استرالي، وتبرع لأحد الجمعيات الخيرية بمبلغ ٥.٧٠٠ دولار. أنظر: د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية سوسيولوجية، المرجع السابق، ص ٢٣٣.
٢ د. سعد عطوة الزنط، المرجع السابق، ص٦.
٣ محمد سيد سلطان، المرجع السابق، ص١٦.

النوع من شبكات المعلومات أن تؤدي إلى نتائج خطيرة، وخصوصاً في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية، وتعد شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني، وكذلك بالنسبة لشبكات مصادر المياه وطرق توزيعها.[١] ففي فبراير عام ٢٠٠١م تم ترك الشبكة التابعة لممول الكهرباء بكاليفورنيا مربوطا بالشبكة العنكبوتية لمدة أحد عشر يوم حيث تمت قرصنته.[٢]

رابعاً: استهداف نظم المواصلات[٣]

يتضمن هذا النموذج اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج الطائرات وإقلاعها، مما قد ينجم عنه تصادم فيما بينها، أو تعطيل نظام الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات، وتغيير مواعيد الانطلاق بحيث تسود الفوضى، وكذلك بالنسبة للسفن والناقلات والغواصات البحرية.[٤]

---

١ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٢ عبد الحق باسو، المرجع السابق، ص١٠.

٣ في أبريل عام ٢٠٠٠م نشرت المجلة البريطانية new scientist أن الاتصالات عبر الأقمار الصناعية بما فيها المواصلات العسكرية وأجهزة GPS قد يشوش عليها بالقليل من المعدات الإلكترونية بإتباع طرق سهلة موجودة على مواقع في الإنترنت. وبما أن نظام GPS مستخدم بطريقة كثيفة في مجال النقل الجوي فلنتخيل ما يمكن أن يحدث من خلال المس بهذه الأنظمة. أنظر: عبد الحق باسو، المرجع السابق، ص١١.

٤ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

خامساً: استهداف نظم الاتصالات

يشمل هذا النموذج اختراق الشبكات المعلوماتية، والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية، وقد تَمارس سلسلة من الهجمات على خطوط الهواتف المحمولة، ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية، الأمر الذي ينشر حالةً من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية.[١]

ففي فلوريدا قام أشخاص بتحويل المكالمات الموجهة للرقم ٩١١ الخاص بالشرطة في الولايات المتحدة الأمريكية نحو متجر لبيع البيتزا.[٢]

وبذلك نكون قد انتهينا من عرض الإطار العام للإرهاب للوسائل الإلكترونية، الذي تناولنا فيه تعريف الإرهاب بالوسائل الإلكترونية ومظاهره في المبحث الأول، وسننتقل إلى دراسة الإطار القانوني للإرهاب بالوسائل الإلكترونية في الجمهورية العربية السورية في المبحث الثاني.

---

١ عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق.

٢ عبد الحق باسو، المرجع السابق، ص٩.

المبحث الثاني

الإطار القانوني للإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني)

إن التصدي للإرهاب بالوسائل الإلكترونية يجد إطاره القانوني ضمن طائفتين من تشريعات الدولة، الأولى تشريعات الفضاء الإلكتروني وبشكل خاص الجرائم الإلكترونية، والطائفة الثانية تشريعات مكافحة الإرهاب (التقليدية)المناط بها تحديد المفاهيم، وجهات الإشراف والاختصاص، وإنفاذ القانون.[١]

فالعلاقة بين تشريعات الإرهاب بالوسائل الإلكترونية وتشريعات الجرائم الإلكترونية، هي أن الصور التقنية لسلوكيات الجرائم الإلكترونية ذاتها هي التي تتبع بارتكابها، حيث أن كل منهما جرائم ومحل الجريمة في كلاهما واحد وهو البيئة الإلكترونية،[٢] لكن يكمن الفارق في الدافع على ارتكاب الجريمة (وهو في الغالب ليس عنصراً في الجريمة إلا إذا عبر عنه المشرع السوري ضمن النص صراحة وفي الأحوال التي عينها القانون)،[٣] والقصد الجرمي، كما يكمن الفرق غالباً بنتائج هذه الجرائم.[٤]

وبما أن صور جرائم الإرهاب الإلكتروني وقواعد المسؤولية المتصلة بها وعقوباتها تنتمي إلى ذات الخصائص والقواعد الخاصة بالجرائم الإلكترونية،

---

١ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، المرجع السابق، ص٢١٩.

٢ محمد سيد سلطان، المرجع السابق، ص١٢.

٣ أ.د. محمد الفاضل، المبادئ العامة في قانون العقوبات، الطبعة الثانية، دمشق، ١٩٦٣م، ص ٤٧٤.

٤ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق، ص١٦٣.

لهذا فإن موطن تنظيمها الملائم من بين تشريعات الدولة هو قوانين الجرائم الإلكترونية.[١]

والعلاقة بين تشريعات الإرهاب بالوسائل الإلكترونية وتشريعات مكافحة الإرهاب، هي أن تشريعات مكافحة الإرهاب العادية هي من يضطلع بتحديد مفهوم الإرهاب والعمل الإرهابي، ويمتد هذا التحديد لوصف نتائج وغايات أنشطة الإرهاب بالوسائل الإلكترونية لأن هذه الأخيرة إما استغلالاً لتطبيقات ووسائل البيئة الرقمية أو تنطوي على أفعال تحقق نتائج موصوفة ضمن تعريف العمل الإرهابي، أي أن التشريعات العادية هي التي تحدد جهات تولي أنشطة مكافحة الإرهاب سواء من حيث أجهزة الضبط العدلي أم أجهزة التحقيق أم جهة المحاكمة.[٢]

وبالتالي تستوجب دراسة الإرهاب بالوسائل الإلكترونية (الإرهاب المعلوماتي) في سورية، تسليط الضوء على تشريعين قانونيين خاصين هما المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، والقانون رقم /١٩/ لعام ٢٠١٢م الخاص بمكافحة الإرهاب.[٣]

لذلك لابد من دراسة هذين القانونين من الناحية الموضوعية، وبالتالي سنقسم هذا المبحث إلى مطلبين:

---

١ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق ص١٧٢.

٢ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق ص١٨٩-١٩٠.

٣ لابد لنا من أن نشير أن كل من المرسوم التشريعي رقم ١٧ لعام ٢٠١٢م والقانون رقم ١٩ لعام ٢٠١٢/٧/٢م، قد صدرا بعد اختيار موضوع البحث "الإرهاب بالوسائل الإلكترونية".

المطلب الأول: قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

المطلب الثاني: قانون مكافحة الإرهاب.

المطلب الأول

قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية

إن طرح موضوع التنظيم القانوني للعالم الافتراضي، بشكل أكثر دقة وتحديد معالمه من الموضوعات الجديدة في عالمنا العربي، وأمام الاستخدام الواسع والمتزايد للشبكة العنكبوتية في سورية، والتحسن النسبي لجودة الخدمة أيضاً، إضافة إلى الحاجة اليومية إليها في المراسلات العقدية والتجارية وكذلك الإعلامية، وخاصة في الأعوام المنصرمة (إعلامياً) على وجه الخصوص، ساهم بشكل كبير في ازدياد عدد مستخدمي الإنترنت، والطلب على بوابات النفاذ في كل مراكز الخدمة في سورية.[١]

إضافة إلى وجود فراغ تشريعي في مجال مكافحة الجريمة المعلوماتية، هذا الأمر اقتضى صدور تشريع خاص هو المرسوم التشريعي **رقم /١٧/** لعام **٢٠١٢م** المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، مستفيدين من تجارب الدول التي سبقتنا في هذا المجال، حتى لو افتقرنا إلى البينية التحتية، الفنية والتشغيلية والتطبيقية ذات

---

١ إياد علي الدرة، المناعة التشريعية في مواجهة الوباء المعلوماتي، مجلة المعلوماتية والقانون، الجمعية العلمية السورية المعلوماتية، العدد (٧٣)، شهر آذار، ٢٠١٢م، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢٠١٣/٥/٢م.

الصلة، فبعد مضي ما يقارب نصف قرن على ظهور أول تشريع إلكتروني، نجد أنه من غير المقبول أن نُحَمِّل القانون التقليدي مالا يطاق في معاقبة الجرائم المعلوماتية.[١]

والمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م لم يكن الخطوة الأولى في مجال تنظيم البيئة الإلكترونية في سوريا،[٢] فقد جاء قبله وبعده خطوات عديدة.[٣]

وسنتناول في هذا المطلب المرسوم التشريعي رقم /١٧/ لعام **٢٠١٢م**، من حيث الصور الجرمية التي تضمنها، في إطار إن تنظيم مكافحة جرائم الإرهاب بالوسائل الإلكترونية هو جزء من تشريع الناظم للجرائم الإلكترونية سواء بقواعده الموضوعية أو الإجرائية، سواء أفرد لها قانون

---

١ إياد علي الدرة، التجربة السورية في مجال التشريع الإلكتروني، مجلة المعلوماتية والقانون، الجمعية العلمية السورية المعلوماتية، العدد (٦١)، شهر آذار، ٢٠١١، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢٠١٣/٤/٥م.

٢ وجاء المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م ليتوج كل الخطوات السابقة، وهو يتألف من /٣٦/ مادة، تقع ضمن خمسة فصول، تتناول تنظيم التواصل على المواقع الإلكترونية وتحديد المسؤوليات والعقوبات المقررة في حال مخالفة تلك المسؤوليات، بعد تصنيف الجرائم مع إحداث ضابطة عدلية متخصصة مهمتها التقصي الإلكتروني والتفتيش والضبط وغيرها من القضايا القانونية.

٣ أولاً: قانون حماية حق المؤلف والحقوق المجاورة رقم ٦٢ لعام ٢٠١٣ م.

ثانياً: القانون رقم ٢٦ لعام ٢٠٠٧م المتعلق بالأحوال المدنية.

ثالثاً: قانون التوقيع الإلكتروني وخدمات الشبكة رقم ٤ لعام ٢٠٠٩ م.

رابعاً: قانون الإعلام الإلكتروني المرسوم التشريعي رقم /١٠٨/ تاريخ ٢٠١١م.

خامساً: القانون رقم ٣ لعام ٢٠١٤م الناظم للمعاملات الإلكترونية بتاريخ ٢٠١٤/٣/٤، وهذا القانون جاء مكملاً لقانون التوقيع الإلكتروني وقانون تنظيم التواصل عبر الشبكة.

مستقل أو أفرد كقسم أو فصل ضمن قانون العقوبات، باعتبار أن صور جرائم الإرهاب بالوسائل الإلكترونية تنتسب إلى الجرائم الإلكترونية.[١]
وقد بينا سابقاً، أن الجرائم المعلوماتية بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م لا تحدث إلا في حالتين هما:

١- عندما تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة، وتصنف على أنها جرائم مستحدثة.

٢- عندما يكون جهاز الحاسوب أو الشبكة أداة تنفذ بواسطتها الجريمة وتصنف على أنها جرائم اعتيادية.

لذلك سنقسم هذا المطلب إلى فرعين:

الفرع الأول: الجرائم المستحدثة والذي تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة.

الفرع الثاني: الجرائم الاعتيادية (التقليدية) والتي يكون فيه الحاسب الآلي أو الشبكة مجرد وسيلة تسمح بارتكاب الجريمة.

الفرع الأول

الجرائم المستحدثة

جاء في الفصل الثالث من المرسوم التشريعي **رقم /١٧/ لعام ٢٠١٢م،** تحت عنوان **مكافحة الجريمة المعلوماتية،** الأفعال الجرمية التي تشكل جرائم معلوماتية، وسنحاول أن نحلل بشيء من الإيجاز، بعض من هذه الجرائم مبينين أركانها الأساسية والعقوبة المستحقة لمرتكبيها، والتي يمكن أن ترتكب في إطار عمل إرهابي إلكتروني يستهدف أحد البنى التحتية

---

١ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق، ص١٧٩.

المعلوماتية الحيوية، من أجل نشر الخوف والفزع، والتي يمكن إجمالها بما يلي:

١- الدخول غير المشروع إلى منظومة معلوماتية.

٢- إعاقة الوصول إلى الخدمة.

٣- اعتراض المعلومات.

٤- تصميم البرمجيات الخبيثة واستخدامها.

في ضوء كما أسلفنا سابقاً، بأن جميع الأعمال الإرهابية الإلكترونية هي جرائم إلكترونية، ولكن ليست جميع الجرائم الإلكترونية تدخل ضمن الأعمال الإرهابية.

فالإرهاب بالوسائل الإلكترونية مفهوم يشمل على الجريمة الإلكترونية، ويكمن الفارق بين الإرهاب بالوسائل الإلكترونية والجريمة الإلكترونية، في الدافع على ارتكاب الجريمة، والقصد الجرمي، كما يكمن الفرق في الغالب بنتائج هذه الجرائم.

أولاً: الدخول غير المشروع إلى منظومة معلوماتية

نصت المادة **الخامسة عشرة** من المرسوم التشريعي **رقم /١٧/** لعام ٢٠١٢م على أنه:

أ- **يعاقب بالغرامة من عشرين ألف إلى مائة ألف ليرة سورية كل من دخل قصداً بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك.**

فجريمة الدخول غير المشروع كغيرها من الجرائم، يتطلب قيامها ركناً مادياً وركناً معنوياً، فأركان الجريمة هي مكوناتها الأساسية التي تعطيها عند توافرها وجوداً قانونياً.[١]

١- الركن المادي في جريمة الدخول غير المشروع

لا بد في كل جريمة من ركن مادي يعكس ما يُعرف بمبدأ ماديات الجريمة، والركن المادي يتكون من ثلاث عناصر: السلوك، والنتيجة، وعلاقة السببية.[٢]

يتمثل النشاط الجرمي في هذه الجريمة، بفعل الدخول إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني دون أن يكون له الحق في ذلك أو يملك الصلاحية، ويُعاقب المشرع على مجرد الدخول، وبأي وسيلة كانت، ولم يشترط المشرع السوري أن يكون النظام محمياً أو لا، ولم يشترط حدوث نتيجة جرمية معينة، وبالتالي يعاقب المشرع على فعل الدخول فقط بغض النظر عن الوسيلة المستخدمة، لأن علة التجريم هي حماية النظام ذاته من الدخول إليه بصورة غير مشروعة.

وتنطبق هذه الفقرة بوجه خاص على كل من يخترق جهازاً حاسوبياً أو منظومة معلوماتية أو موقع إلكتروني، سواء أكان ذلك عن بعد، أو عن طريق الشبكة، بأي وسيلة كانت، أم مباشرة، أي بالدخول كمستخدم لا يملك

---

١ أ.د. عبود السراج، قانون العقوبات-القسم العام، المرجع السابق، ص١٨٩.

٢ د. سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٠م، ص ٤٧٠-٤٧١.

الحق أو الصلاحية أو التصريح اللازم للقيام بذلك، ومن ذلك سرقة بيانات الدخول.[١]

٢- الركن المعنوي

هو الركن الثاني في الجريمة، من دونه لا تعد الجريمة قائمة، ويتحقق الركن المعنوي في إحدى صورتين: صورة القصد الجرمي، فتكون الجريمة مقصودة وصورة الخطأ فتكون الجريمة غير مقصودة.[٢]

وتعد جريمة **الدخول غير المشروع** من الجرائم المقصودة، يتمثل فيها الركن المعنوي في صورة القصد الجرمي، فهي لا تقع عن طريق الخطأ، ويكفي فيها القصد الجرمي العام، وبالتالي لا ينطبق الحكم المذكور في هذه الفقرة على الدخول غير المقصود الذي لا ينطوي على إجراءات يقوم بها الفاعل بهدف تجاوز الحمايات الموضوعة أو الالتفاف عليها.[٣]

٣- العقوبة

عاقب المشرع السوري على جريمة الدخول غير المشروع، بعقوبة جنحية وهي الغرامة من عشرين ألف إلى مائة ألف ليرة سورية، وشدد المشرع العقوبة في الفقرة /**ب**/ من المادة **الخامسة عشرة** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢ م والتي نصت على الآتي:

---

١ ت١الفقرة أ/ م١٥، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٢ د. معن أحمد محمد الحياري، الركن المادي للجريمة، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، ٢٠١٠م، ص ٥٧.

٣ ت١الفقرة أ/ م١٥، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

"وتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها."

وتشدد العقوبة في حال أضيف إلى الإختراق المذكور في الفقرة السابقة نسخ أي شكل من أشكال المعلومات التي جرى الحصول عليها، أو تغييرها أو تزويرها بأي صورة كانت، أو استخدامها أو إفشائها، وتنطبق هذه الفقرة، على سبيل المثال، على من يشوه تصميم موقع إلكتروني على الوب، أو يقتحم قاعدة بيانات، سواء كان ذلك عند بعد أم مباشرة بغرض استغلال المعطيات الموجودة فيها.[١]

وبالتالي فإن الركن المعنوي المطلوب لتطبيق الظرف المشدد، يجب فيه توافر القصد الجرمي الخاص إلى جانب القصد الجرمي العام، ويتمثل القصد الجرمي الخاص هنا بأن يقوم بأحد الأفعال المذكورة سابقاً وأن تتجه إرادته إلى ارتكاب هذه الأفعال.

ومن الجدير بالذكر أن الأفعال الجرمية المتعلقة بالتوقيع الإلكتروني وتزوير البيانات المعلوماتية معاقب عليها بموجب أحكام قانون التوقيع الإلكتروني وخدمات الشبكة النافذة.[٢]

لكن هنا يثور السؤال التالي: ما هو حكم من بقي في منظومة معلوماتية أو موقع إلكتروني، كان قد دخل إليها عن طريق الخطأ، دون استخدام أي

---

١ ت١الفقرة ب/ م١٥، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢.

٢ ت١الفقرة ب/ م١٥، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢.

إجراءات بهدف تجاوز الحمايات الموضوعة أو الالتفاف عليها، حبذا لو أن المشرع السوري، اضاف فقرة إلى المادة الخامسة عشرة السابقة عاقب بموجبها على البقاء في منظومة معلوماتية أو موقع إلكتروني، كان دخل إليها عن طريق الخطأ، هذا من جهة.

ثانياً: إعاقة الوصول إلى الخدمة

عالج المشرع السوري تحت عنوان "إعاقة الوصول للخدمة" بموجب نص المادة **السابعة عشرة** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م إعاقة الوصول إلى الخدمة على النحو الآتي:

"**يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة إلف إلى خمس مائة ألف ليرة سورية كل من أعاق أو منع قصدا بأي وسيلة كانت الدخول إلى منظومة معلوماتية أو الشبكة أو عطلها أو أوقفها عن العمل أو منع قصداً بأي وسيلة كانت الوصول إلى الخدمات أو البرامج أو المواقع الإلكترونية أو مصادر البيانات أو المعلومات عليها**".

هذه المادة خاصة بجمهور المستخدمين، وتتضمن ثلاث صور جرمية:

أ- كل من أعاق أو منع قصداً بأي وسيلة كانت الدخول إلى منظومة معلوماتية أو الشبكة أو عطلها.

ب-عطل أو أوقف منظومة معلوماتية أو الشبكة عن العمل، أي التعطيل الكلي للخدمة.

ج-منع قصداً بأي وسيلة كانت الوصول إلى الخدمات أو البرامج أو المواقع الإلكترونية أو مصادر البيانات أو المعلومات على منظومة معلوماتية أو الشبكة.

وتنطبق هذه الفقرة على إعاقة الدخول إلى أي منظومة معلوماتية أو إلى الشبكة أو تعطيل وظائفها كلياً أو جزئياً، سواء أكان ذلك بتخريب البرمجيات أو البيانات أم بإغراق المنظومة بما يفوق طاقتها، أم بقطع الاتصال عنها، بأية وسيلة معلوماتية أخرى، ويفترض توافر القصد لدى الفاعل، لكن تستثنى الحالات العرضية التي تحدث بطريق الخطأ.[١]

لم يحدد المشرع في كلا الصور الجرمية، الوسيلة المستخدمة، وإنما جاء النص عام بأي وسيلة معلوماتية كانت، ولا تحتاج إلى قصد خاص بل يكفي فيها القصد العام.

و**العقوبة** واحدة في كل الصور الجرمية، وهي الحبس من ثلاث أشهر إلى سنتين والغرامة من مائة إلف إلى خمس مائة ألف، وهي عقوبة جنحوية الوصف.

وفي رأينا كان أكثر ملائمة لو أن المشرع شدد العقوبة في حال تعطيل أو إيقاف منظومة معلوماتية أو الشبكة عن العمل، نتيجة جسامة الضرر وكونها أشد خطورة على البنية التحتية المعلوماتية.

ثالثاً: اعتراض المعلومات

تضمنت المادة **الثامنة عشرة** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، صورتين جرميتين لاعتراض المعلومات، تتمثل **الأولى** في اعتراض أو التقاط أو التنصت على المعلومات المتداولة على منظومة معلوماتية، في حين تتمثل **الصورة الثانية** في استخدام الخداع للحصول على

---

١ ت١، م١٧، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢.

معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة.

١- اعتراض أو التقاط أو التنصت على المعلومات المتداولة على منظومة معلوماتية.

نصت الفقرة /أ/ من المادة **الثامنة عشرة** من المرسوم ذاته على الآتي:

"**يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة ألف إلى خمس مائة ألف ليرة سورية كل من اعترض أو التقط قصداً بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها**".

تنطبق هذه الفقرة على كل من أقدم قصداً، بوجه غير مشروع، على اعتراض أو التقاط المعلومات المتداولة على منظومة معلوماتية أو على الشبكة، أو التنصت عليها بوسائل معلوماتية، وذلك عند نقلها من أو إلى منظومة معلوماتية، سواء جرى استغلال هذه المعلومات لاحقاً أو لا.

ويفترض في هذا الفعل أيضاَ أن تكون المعلومات المعنية غير متاحة أصلاً لاطلاع عامة الجمهور عليها، أي لا يمكن الوصول إليها إلا من قبل المخولين بذلك،[١] ولا تنطبق هذه المادة في حالة التقاط المعلومة لأغراض إحصائية فقط، على ألا يؤدي ذلك إلى التقاط معلومة سرية تنتهك الخصوصية.[٢]

---

١ ت١الفقرة أ/ م١٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٢ ت٢الفقرة أ/ م١٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢.

وجريمة اعتراض المعلومات لابد فيها من ركن مادي وركن معنوي.

أ- **الركن المادي**، يتمثل النشاط الجرمي فيه ب (اعتراض، التقاط، التنصت) بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة، ولم يشترط المشرع وسيلة معينة في اعتراض المعلومات، ولتطبيق هذه الفقرة يجب توافر شرطين:

- أن يكون التقاط أو اعتراض المعلومة تم بوجه أو بطريقة غير مشروعة.
- أن تكون المعلومات محل هذه الجريمة غير متاحة للجمهور.

ب-**الركن المعنوي في جريمة اعتراض المعلومات**، تعد هذه الجريمة من الجرائم القصدية، التي تتطلب القصد الجرمي العام، ويتمثل في قصد اعتراض أو التقاط أو التنصت على معلومات متداولة على الشبكة أو منظومة معلوماتية غير متاحة للجمهور.

ج- **العقوبة**، حدد المشرع للجاني عقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة ألف إلى خمس مائة ألف ل.س.

لكن **السؤال** هنا ما هي الحالات المشروعة لاعتراض المعلومات أو التنصت عليها؟ وهل يمكن اعتراض المعلومات بطريقة مشروعة؟ حبذا لو أن المشرع بين هذه الحالات، وحبذا أيضاً لو أنه قام بتعريف أو تحديد المقصود بكل من الاعتراض، الالتقاط، التنصت، حرصاً على وضوح النص.

٢-استخدام الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة.

نصت الفقرة /ب/ من المادة **الثامنة عشرة** من المرسوم التشريعي سالف الذكر على الآتي:

" **يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مائة ألف إلى خمس مائة ألف ليرة كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة يمكن استغلالها لأغراض إجرامية**".

وقد عرف المشرع السوري الخصوصية في **المادة الأولى** من المرسوم ذاته، حيث نصت على أن:" **الخصوصية، حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة وفي عدم اختراقها أو كشفها دون موافقته.**"

هذا يعني أن الفقرة /ب/ من المادة **الثامنة عشرة**، تنطبق على كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة. سواء أكان ذلك باستخدام البريد الإلكتروني، أم بانتحال أسماء أو محتوى مواقع الإلكترونية، أم بأي وسيلة أخرى.[١]

وفي حال الحصول على المعلومات الشخصية أو السرية عن طريق اعتراضها أو التنصت عليها، فتطبق الفقرة السابقة من هذه المادة.[٢]

وكل جريمة لا بد فيها من ركنين، ركن مادي وركن معنوي.

---

١ ت١الفقرة ب/ م١٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٢ ت٢الفقرة ب/ م١٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

أ- **الركن المادي** في هذه الصورة، يتمثل السلوك الجرمي بفعل خداع المستخدمين على منظومة معلوماتية أو الشبكة للحصول على معلومات شخصية بأي وسيلة كانت.

ب-**الركن المعنوي**، تتطلب هذه الصورة قصداً خاصاً إضافة إلى القصد العام، يتمثل القصد العام في قصد خداع المستخدمين في الحصول على معلومات شخصية، والقصد خاص استخدام هذه المعلومات لأغراض إجرامية.

ج- **العقوبة**، هي الحبس من شهر إلى ستة أشهر والغرامة من مائة ألف إلى خمس مائة ألف ليرة سورية.

نجد أن العقوبة في الصورة الأولى (اعتراض أو التقاط أو التنصت على المعلومات المتداولة على منظومة معلوماتية) أشد من العقوبة في الصورة الثانية (استخدام الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة)، وهذا يعود إلى القدرة التقنية التي يمتلكها المجرم في جريمة **اعتراض أو التقاط أو التنصت على المعلومات المتداولة على منظومة معلوماتية** إضافة إلى الوسائل المعلوماتية المتطورة التي يستخدمها.

رابعاً: تصميم البرمجيات الخبيثة واستخدامها

نصت المادة **التاسعة عشرة** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، على أنه:

"/أ/ يعاقب بالحبس من ثلاث سنوات والغرامة من خمس مائة ألف إلى مليونين ونصف المليون ليرة سورية كل من يقوم بتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية."

"/ب/ يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مائتي ألف إلى مليون ليرة سورية كل من استخدم البرمجيات الخبيثة أياً كان نوعها وبأي وسيلة كانت بقصد الإضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة."

نستنتج من هذه المادة أنها تضمنت صورتين جرميتين، **الأولى:** تتمثل في تصميم البرمجيات الخبيثة وترويجها، في حين تتمثل **الثانية:** في استخدام البرمجيات الخبيثة بقصد الأضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة.

وعرّف المشرع السوري **البرمجيات الخبيثة** في المادة **الأولى** من هذا المرسوم بأنها: "**برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية المعلوماتية أو المواقع الإلكترونية أو الشبكة أو تعطيل عملها أو تبطئته أو تخريب محتوياته أو مواردها أو جمع معلومات عنها أو عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة.**"

ومن أكثر أصناف البرمجيات الخبيثة شيوعاً: الفيروسات، الديدان، أحصنة طروادة، والبرمجيات التي تتيح التحكم في جهاز حاسوبي أو منظومة معلوماتية من دون علم صاحبها، سواء أكان بغرض سرقة المعلومات

الموجودة، أو استخدامها في مهاجمة أجهزة حاسوبية أخرى أو منظومة معلوماتية أخرى.[١]

١- الصورة الأولى، **تصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية.**

أ- يتمثل **الركن المادي** في هذه الصورة بفعل تصميم البرمجيات الخبيثة، والتصميم هو اختراع هذه البرمجيات.

ب-في حين يتمثل **الركن المعنوي** بصورة القصد الجرمي، ولا يكفي القصد الجرمي العام بل تحتاج هذه الصورة إلى قصد جرمي خاص، فالقصد العام هو قصد تصميم البرمجيات الخبيثة، والقصد الجرمي الخاص هو ترويجها لأغراض جرمية.

ج-و**العقوبة** هي الحبس من ثلاث إلى خمس سنوات والغرامة من خمس مائة ألف إلى مليونين ونصف المليون ليرة سورية.

٢- الصورة الثانية، **استخدام البرمجيات الخبيثة بقصد الأضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة.**

وتنطبق الفقرة /**ب**/ من المادة /**١٩**/، على كل من استخدم البرمجيات الخبيثة، أياً كان نوعها، وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة، أي أن استخدام البرمجيات

---

١ ت١١/ م١، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

الخبيثة أو دراستها لأغراض البحث والتطوير، أو بهدف التصدي لها. لا يدخل في نطاق تطبيق هذه الفقرة.[١]

وهذه الصورة تتكون من:

أ- **ركن مادي**، في صورة استخدام البرمجيات الخبيثة، أياً كان نوعها، وبأي وسيلة كانت.

ب-**وركن معنوي**، حيث أن هذه الجريمة مقصودة، وتحتاج إلى قصد خاص هو قصد الأضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة، إضافة إلى القصد العام الذي يتمثل بصورة استخدام البرمجيات الخبيثة.

ج- أما **العقوبة** فهي الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مائتي ألف إلى مليون ليرة سورية.

نلاحظ أن العقوبة في الصورة الأولى (تصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية) أشد من العقوبة في الصورة الثانية (استخدام البرمجيات الخبيثة بقصد الأضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة)، وهي عقوبة تتناسب والخطورة الإجرامية للجاني الذي يقوم بتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية، لأن هذا الجاني خطره اشد من الشخص الذي يقوم فقط باستخدام البرمجيات الخبيثة لأغراض إجرامية.

---

١ ت١ الفقرة أ/ م١٩، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

وحبذا لو أن المشرع أفرد فقرة عاقب بموجبها الشخص الذي يقوم بتصميم البرمجيات الخبيثة ويستخدمها لأغراض إجرامية، بعقوبة أشد من العقوبة الواردة في الصورتين السابقتين، نظراً لخطورته الإجرامية.

لكن السؤال الذي يطرح نفسه، هل تعد حيازة البرمجيات الخبيثة دون نية استخدامها، جريمة معاقب عليها؟ حبذا لو أن المشرع أشار إلى هذه الناحية، وعاقب على حيازة البرمجيات الخبيثة، نظراً لخطورة هذه البرمجيات على البنية التحتية المعلوماتية.

وبعد عرض بعض الجرائم المستحدثة التي تكون فيها المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، والتي يمكن أن ترتكب في إطار عمل إرهابي إلكتروني، سننتقل إلى دراسة الجرائم التي يكون فيها جهاز الحاسوب أو الشبكة أداة تنفذ بواسطتها الجريمة وتصنف على أنها جرائم اعتيادية في الفرع التالي.

الفرع الثاني

الجرائم الاعتيادية (التقليدية)

نص المشرع السوري في الفصل الخامس، من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، تحت عنوان (أحكام عامة وختامية) على الجرائم التقليدية و**التي** يكون فيه الحاسب الآلي أو الشبكة مجرد وسيلة تسمح بارتكاب الجريمة، في موضعين، هما: تطبيق القوانين الجزائية، والأعمال الدعائية والتحريض على ارتكاب الجرائم.

أولاً: تطبيق القوانين الجزائية

نصت المادة **الثامنة والعشرون** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م على أنه:

"/أ/ إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون تطبق العقوبة التي هي أشد.

/ب/ يضاعف الحد الأدنى للعقوبة المقررة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين:

١- إذا ارتكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة.

٢- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو المعلومات أو البيانات المخزنة عليها."

١- **أم الغرض من الفقرة /أ/ من المادة الثامنة والعشرين** هو ما يُعرف باجتماع الجرائم المعنوي أو التعدد الصوري،[١] ويكون عند ارتكاب الجاني فعلا إجرامياً واحداً، نجمت عنه نتيجة واحدة، ألا أن هذا الفعل له عدة أوصاف قانونية أو ينطبق عليه أكثر من نص من نصوص القوانين الجزائية.[٢]

٢- **أما الغرض من الفقرة /ب/ من المادة /٢٨/** هو النص على معاقبة الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى، إذا

---

١ خص المشرع السوري اجتماع الجرائم المعنوي بقاعدتين نصت عليها المادة /١٨٠/ من قانون العقوبات السوري الصادر بالمرسوم التشريعي ١٤٨ لعام ١٩٤٩م، وهما:

إذا كان للفعل عدة أوصاف قانونية، ذكرت جميعها في الحكم، على أن يحكم القاضي بالعقوبة الأشد.

على أنه إذا انطبق على الفعل نص عام ونص خاص أخذ بالنص الخاص.

٢ أ.د. بارعة القدسي، أصول المحاكمات الجزائية، الجزء الأول، الدعوى العامة-الدعوى المدنية، جامعة دمشق، ١٤٣٠-١٤٣٢هـ، ٢٠١٠-٢٠١١م، ص٩٢.

ارتكب النشاط الجرمي باستخدام الشبكة أو وقع على الشبكة أو إذا وقع النشاط الجرمي على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة فيها.

ولا ينطبق هذا النص على الحالات التي لا يكون فيها لاستخدام الشبكة دور إيجابي في وقوع الجريمة، كأن تستخدم لمجرد التواصل، والهدف من ذلك توحيد النص التشريعي وعدم تكرار أشكال الجرائم الاعتيادية عندما ترتكب بالوسائل المعلوماتية أو تقع على المنظومة المعلوماتية.[١]

أ- ومن أهم أشكال هذه الجرائم، على سبيل المثال لا الحصر:[٢]

١- ترويج المواد المخدرة على الشبكة.

٢- المقامرة على الشبكة.

٣- الذم والقدح.

٤- تهديد الأشخاص على الشبكة.

٥- التعرض للآداب والأخلاق العامة.

٦- إنتاج محتوى يتعلق بإباحية القاصرين على منظومة معلوماتية أو توزيعه أو حيازته.

٧- التحرش الجنسي بالقاصرين بوسيلة معلوماتية.

٨- التحريض على ارتكاب الجرائم بوسيلة معلوماتية.

٩- الترويج لجرائم الاتجار بالأشخاص.

---

١ ت١ الفقرة ب/ م٢٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

٢ت١ الفقرة ب/ م٢٨، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

١٠- المساعدة أو التحريض بوسيلة معلوماتية على ارتكاب جرائم ضد الإنسانية.

١١- نشر وتوزيع المحتوى العنصري بوسيلة معلوماتية.

١٢- نشر بيانات تهدد الأمن والسلامة العامة بوسيلة معلوماتية.

١٣- الترويج للإرهاب بوسيلة معلوماتية.

ب-علاقة الجرائم المذكورة بالإرهاب بالوسائل الإلكترونية

وبالعودة إلى الإرهاب بالوسائل الإلكترونية، فكما أسلفنا سابقاً بأنه هو كل فعل يستخدم النظم الرقمية أو التقنية كهدف أو وسيلة، وبالتالي في حال ارتكاب عمل إرهابي تنص عليه القوانين الجزائية المعمول بها حالياً (القانون /١٩/ لعام ٢٠١٢م قانون مكافحة الإرهاب)، باستخدام الشبكة أو وقع على الشبكة أو وقع النشاط الجرمي على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة فيها، فإننا نقول بإمكانية تطبيق الفقرة /ب/ من المرسوم رقم /١٧/ سالف الذكر، على الإرهاب بالوسائل الإلكترونية، والتي تنص على مضاعفة الحد الأدنى للعقوبة المقررة.

ولكن إمكانية تطبيق هذه الفقرة على الإرهاب بالوسائل الإلكترونية، لا تغني عن تجريم الإرهاب بالوسائل الإلكترونية، بنصوص جزائية صريحة وواضحة ومستقلة، لأن الهدف من الفقرة /ب/ من المادة /٢٨/ السالفة الذكر، كما جاء في التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، هو توحيد النص التشريعي وعدم تكرار أشكال الجرائم الاعتيادية عندما ترتكب بالوسائل المعلوماتية أو تقع على المنظومة المعلوماتية، وليس الهدف منها التصدي للإرهاب بالوسائل الإلكترونية، فالإرهاب بالوسائل

الإلكترونية ليس من الجرائم الاعتيادية، بل هو صورة جديدة من صور الإرهاب وأكثرها خطورة واستحداثاً وانتشاراً.

ثانياً: الأعمال الدعائية والتحريض على ارتكاب الجرائم

نصت المادة **التاسعة والعشرين** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م على أنه:

/أ/ يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات والغرامة من مائة ألف إلى خمس مائة ألف ليرة سورية كل من قام بالتحريض أو الترويج لارتكاب أي جريمة من الجرائم المنصوص عليها في القوانين الجزائية النافذة باستخدام الشبكة.

/ب/ ولا تقل العقوبة الحبس عن سنة والغرامة عن مائتين وخمسين ألف ليرة سورية إذا ارتكب الفعل المنصوص عليه في الفقرة /أ/ من هذه المادة باستخدام الانترنت."

والتحريض حسب ما هو منصوص عليه في المادتين /٢١٦/ و /٢١٧/ من قانون العقوبات السوري، هو حمل أو محاولة حمل شخص أخر على ارتكاب جريمة، فالغرض من المادة **التاسعة والعشرين** السالفة الذكر، هو تجريم فعل التحريض على ارتكاب الجرائم باستخدام الشبكة، وذلك مع مراعاة العقوبات المنصوص عليها في المادة **الثامنة والعشرين** من هذا المرسوم.[١]

---

١ ت١ الفقرة أ/ م٢٩، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

ونلاحظ هنا أن المشرع خرج عن القاعدة العامة، والتي تنص عليها المادة /٢١٧/ من قانون العقوبات، والتي تُعَرِّض المحرض لعقوبة الجريمة التي أراد أن تقترف، سواء كانت ناجزة أو مشروعاً فيها أو ناقصة.[١]

ويقصد بالترويج النشر والقبول والاستساغة،[٢] أي الدعاية، فالدعاية فلا ترقى إلى مستوى التحريض، ولكن الشبكة قد تكون وسيطاً ملائماً لأعمال الدعاية على ارتكاب الجرائم أو التعريف بطريقة ارتكابها (الدعاية لتصنيع المتفجرات).[٣]

وشدد المشرع السوري العقوبة المنصوص عليها في الفقرة /أ/ من المادة /٢٩/، إذا أرتكب فعل من الأفعال المنصوص عليها في الفقرة /أ/ باستخدام الإنترنت.

وبالتالي إن التحريض على ارتكاب الجرائم الإرهابية باستخدام الشبكة معاقب عليه بموجب الفقرة /أ/ من المادة /٢٩/ سالفة الذكر، وهذه الحالة تعد جانب أو مفردة من مفردات الإرهاب بالوسائل الإلكترونية.

في نهاية الحديث عن المرسوم **رقم /١٧/** لعام ٢٠١٢م **(قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية)**، وبعد أن استعرضنا بشيء من الإيجاز بعض الأحكام والنصوص القانونية الواردة فيه، **نجد أن المشرع السوري خطا خطوات إيجابية في مجال سن تشريعات حديثة لمواجهة الجريمة المعلوماتية، وبالتالي أصبح للقاضي آليات للبت في**

---

١ أ.د. عبود السراج، المرجع السابق، ص٢٨٠.

٢ د. منال مروان منجد، المواجهة الجنائية لجرائم الإرهاب في القانون السوري دراسة تحليلية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد٣٠، العدد الثاني، ٢٠١٤، ص١٢٣.

٣ ت٢ الفقرة أ/ م٢٩، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

قضايا الجريمة المعلوماتية، لكن لا يمكن الجزم بأن الرصيد التشريعي السوري في هذا الصدد كافٍ لمكافحة كل صور الجرائم المعلوماتية، بل لا بد من استكماله، بحيث يشمل جرائم لم يشملها المرسوم رقم /١٧/ لعام ٢٠١٢م، **فظاهرة الإجرام المعلوماتي حديثة ومتجددة، وقطاع تكنولوجيا الاتصال في تطور مستمر، مما يعني أنه يمكن ان تظهر في المستقبل أنواع أخرى من الجرائم المعلوماتية، مما يجعل المشرع السوري ملزم بمواكبة التطورات المتلاحقة عبر سن تشريعات جديدة أو تعديل التشريعات الحالية.**

نجد في المقابل، أن المشرع السوري لم يتعرض للإرهاب بالوسائل الإلكترونية ولم يشر إليه أبداً في نص المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، سواء من حيث (التعريف، الخصائص، الصور الجرمية للإرهاب بالوسائل الإلكترونية....إلخ) أو من حيث امكانية ارتكاب أعمال إرهابية بوسائل معلوماتية، وأشار بشكل ضمني إلى حالة تعد جانب أو مفردة من مفردات الإرهاب بالوسائل الإلكترونية، في الفصل الخامس (أحكام عامة وختامية) من المرسوم السالف الذكر في الفقرة /أ/ من المادة /٢٩/ منه والتي نصت على أعمال الدعاية والتحريض على ارتكاب الجرائم باستخدام الشبكة.

إضافة إلى إمكانية تطبيق الفقرة /ب/ من المادة /٢٨/ من المرسوم التشريعي رقم /١٧/ سالف الذكر، على الإرهاب بالوسائل الإلكترونية، والتي تنص على مضاعفة الحد الأدنى للعقوبة المقررة.

لكن يمكن الاستفادة من هذا المرسوم، في إطار كون جرائم الإرهاب بالوسائل الإلكترونية هي جرائم معلوماتية لكن تختلف من حيث القصد

الجرمي والضرر، والصور التقنية لسلوكيات الجرائم الإلكترونية هي التي تتبع بارتكابها.

وبعد البحث في المرسوم التشريعي /١٧/ لعام ٢٠١٢م (قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية)، سننتقل إلى بحث القانون /١٩/ لعام ٢٠١٢م الخاص بمكافحة الإرهاب، لأن هذا التشريع كما أسلفنا سابقاً هو من يضطلع بتحديد مفهوم الإرهاب والعمل الإرهابي، ويمتد هذا التحديد لوصف نتائج وغايات أنشطة الإرهاب بالوسائل الإلكتروني كون الأخيرة إما استغلالاً لتطبيقات ووسائل البيئة الرقمية أو تنطوي على أفعال تحقق نتائج موصوفة ضمن تعريف العمل الإرهابي.

المطلب الثاني

قانون مكافحة الإرهاب

عمد المشرع السوري نتيجة الظروف الاستثنائية التي تمر بها سورية، وتفشي ظاهرة الإرهاب في الآونة الأخيرة والتي امتدت إلى مناحي الحياة كلها، بأساليب وأشكال لم تكن معروفة سابقا، على إصدار قانون مكافحة الإرهاب ومجموعة قوانين أخرى تهدف معه إلى مكافحة الإرهاب،[١] وإلى إلغاء المواد (٣٠٤ – ٣٠٥ – ٣٠٦) من قانون العقوبات ضمن زمرة الجرائم الواقعة على أمن الدولة الداخلي.

حيث كانت المواد (٣٠٤ – ٣٠٥ – ٣٠٦) تكتفي بتجريم العمل الإرهابي والمؤامرة التي تهدف إلى ارتكاب عمل إرهابي، وجريمة إنشاء جمعية بقصد تغيير كيان الدولة الاقتصادي أو الاجتماعي أو أوضاع المجتمع الأساسية، بينما قانون مكافحة الإرهاب الجديد توسع فيه المشرع في التجريم والعقاب، ولم يكتفِ بالعقاب على الجرائم الإرهابية، وإنما شمل القانون أفعال كثيرة كانت تعد من قبيل المساهمة الجرمية فيما لو تركت للقواعد العامة.[٢]

---

١ نتيجة الظروف الاستثنائية التي تمر بها سورية، أصدر المشرع الجزائي السوري عدة مراسيم تشريعية لمكافحة الإرهاب، وهي:

المرسوم التشريعي رقم /١٩/ الصادر في ٢٠١٢/٧/٢ والمتضمن قانون مكافحة الإرهاب والمرسوم التشريعي رقم /٢٠/ الصادر في ٢٠١٢/٧/٢ المتعلق بالعاملين في الدولة والذين يثبت تورطهم بجرائم الإرهاب، والمرسوم التشريعي /٢١/ الصادر في ٢٠١٢/٧/٢ والذي عدل المشرع السوري بموجبه المادة /٥٥٦/ من قانون العقوبات الصادر بالمرسوم التشريعي رقم /١٤٨/ لعام ١٩٤٩ والمعدل بالمرسوم التشريعي رقم /١/ لعام ٢٠١١ والمتعلقة بجرم الحرمان من الحرية، والمرسوم التشريعي رقم /٢٢/ الصادر في ٢٠١٢/٧/٢٦ والقاضي بإنشاء محكمة خاصة بقضايا الإرهاب.

٢ د. منال مروان منجد، المرجع السابق، ص١٠٦.

وسنقوم في هذا المطلب بتناول القانون رقم /١٩/ الخاص بمكافحة الإرهاب،[١] وتحليل الجريمة الإرهابية كونها الجريمة الأساسية ومن ثم الجرائم المستحدثة في قانون مكافحة الإرهاب، بحيث نستطيع الإجابة على السؤال الآتي: هل تكفي الأحكام التشريعية التي جاء بها المرسوم التشريعي رقم /١٩/ لعام ٢٠١٢ لمواجهة الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني)؟

وبالتالي سنقسم هذا المطلب إلى فرعين:

الفرع الأول: جريمة العمل الإرهابي.

الفرع الثاني: الجرائم المستحدثة في قانون مكافحة الإرهاب.

الفرع الأول

جريمة العمل الإرهابي

جريمة العمل الإرهابي هي الجريمة الأساسية التي يسعى المشرع السوري لمواجهتها، وقد عالج المشرع جريمة العمل الإرهابي في المادة **السابعة** من قانون مكافحة الإرهاب رقم /١٩/ لعام ٢٠١٢م حيث نصت على الآتي:

"**عقوبة العمل الإرهابي:**

١- يعاقب بالأشغال الشاقة المؤبدة والغرامة ضعفي قيمة الضرر من ارتكب عملاً إرهابياً نجم عنه عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الإضرار بالبنية التحتية أو الأساسية للدولة.

---

١ والقانون /١٩/ الخاص بمكافحة الإرهاب لعام ٢٠١٢م، من التشريعات الجزائية الخاصة التي صدر في ظل ظروف الأزمة التي تحيط بسورية، ونظراً لحداثته، وندرة الدراسات والأبحاث حول هذا القانون، واجهنا صعوبات في إعداد هذا البحث.

٢- وتكون العقوبة الأشغال الشاقة المؤقتة خمس سنوات على الأقل إذا كانت الوسائل المستخدمة في العمل الإرهابي تحدث تفجيراً صوتياً فقط."

ولابد لنا من تحليل هذه الجريمة إلى أركانها وعناصرها الأساسية.

أولاً: أركان جريمة العمل الإرهابي

أركان الجريمة هي مكونات الجريمة الأساسية، التي تعطيها عند توافرها وجوداً قانونياً،[١] والجريمة الإرهابية كغيرها من الجرائم يتطلب قيامها ركناً مادياً وركناً معنوياً، وهي أركان عامة لا يتصور قيام أي جريمة بدونها.

١- الركن المادي لجريمة العمل الإرهابي

يتكون الركن المادي للجريمة، من حيث المبدأ، من ثلاث عناصر هي: السلوك، والنتيجة، وعلاقة السببية.

أ- **السلوك الإجرامي**، لقد عاقب المشرع السوري على العمل الإرهابي في المادة **السابعة** من قانون مكافحة الإرهاب، في حين عَرّف المشرع العمل الإرهابي في المادة **الأولى** منه بأنه:

"كل فعل يهدف إلى إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الأضرار بالبنى التحتية أو الأساسية للدولة، ويُرتكب باستخدام الأسلحة والذخائر أو المتفجرات أو المواد الملتهبة أو المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية مهما كان نوع هذه الوسائل أو باستخدام أي أداة تؤدي الغرض ذاته."

---

١ أ.د. عبود السراج، المرجع السابق، ص١٤٣.

لم يحدد المشرع صورة السلوك الجرمي المكون للركن المادي لجريمة العمل الإرهابي، وإنما اكتفى بتحديد الهدف منه ووسائله والنتيجة المترتبة عليه، فالمادة السابعة جاءت عامة، حيث نص المشرع على أنه:

" **يعاقب بالأشغال الشاقة المؤبدة والغرامة ضعفي قيمة الضرر من ارتكب عملاً إرهابيا...**"

لم يحدد المشرع السوري بدقة صورة الفعل الجرمي المكون لجريمة العمل الإرهابي واكتفى بتحديد العناصر المميزة له، ويعود ذلك لسببين:[١] الأول رغبة المشرع في ترك سلطة تقديرية واسعة للقاضي الجزائي في تكييف طبيعة العمل الإرهابي، والثاني صعوبة حصر الأعمال الإرهابية وحصر صورها وأدواتها.

ب-**النتيجة الإجرامية:** فقد حدد المشرع السوري النتيجة الجرمية المترتبة على العمل الإرهابي بأنها عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الإضرار بالبنية التحتية أو الأساسية للدولة.

وهكذا نجد أن المشرع حدد النتيجة الجرمية على سبيل الحصر، وبالتالي تنتفي جريمة العمل الإرهابي إذا أدت إلى نتيجة جرمية مغايرة للنتيجة التي حددها المشرع في المادة السابعة من قانون مكافحة الإرهاب،[٢] في حين أنه كان فيما سبق يعاقب على العمل الإرهابي دون تحديد النتيجة الجرمية المترتبة عليه بموجب نص المادة /٣٠٥/ الملغاة من قانون العقوبات السوري.

---

١ د. منال مروان منجد، المرجع السابق، ص ١٠٨.

٢ د. منال مروان منجد، المرجع السابق، ص١١٠.

وبالتالي كان حري بالمشرع السوري أن يعاقب على جريمة العمل الإرهابي أياُ كانت النتيجة الجرمية المترتبة.

ج- **الوسيلة الجرمية:** ويجب لقيام جريمة العمل الإرهابي أن يلجأ الفاعل إلى وسائل حددها المشرع في نص المادة **الأولى** من قانون مكافحة الإرهاب وهذه الوسائل هي: "**الأسلحة والذخائر أو المتفجرات أو المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية مهما كان نوع هذه الوسائل أو باستخدام أي أداة تؤدي الغرض ذاته.**"

أي أن المشرع السوري لم يحدد وسائل ارتكاب العمل الإرهابي على سبيل الحصر، وإنما استعمل مصطلحاً مرناً واسع الدلالة بقوله "..... أو باستخدام أي أداة تؤدي الغرض ذاته."

وبالعودة إلى الإرهاب بالوسائل الإلكترونية ومدى كفاية النص القانوني في قانون مكافحة الإرهاب، نجد أن المشرع لم يُشر صراحة إلى الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) أو إلى إمكانية ارتكاب العمل الإرهابي باستخدام الوسائل الإلكترونية، سواء في المادة الأولى عندما عرف العمل الإرهابي أو في المادة السابعة عندما عاقب على العمل الإرهابي.

لكنه في الوقت نفسه لم يحدد صور السلوك الجرمي المكون لجريمة العمل الإرهابي وإنما جاء النص القانوني عاماً، حيث اكتفى المشرع بتحديد العناصر المميزة له، ولم يحدد الوسائل التي ترتكب بها هذه الجريمة فقد استعمل مصطلحاً مرناً واسعاً بقوله " أي أداة تؤدي الغرض ذاته"، آخذاً بالحسبان الوسائل التي قد يفرزها التطور التكنولوجي والعلمي المستمر، وبالتالي يمكننا القول إن التعريف الذي جاء به قانون مكافحة الإرهاب للجريمة العمل الإرهابي شمل في طياته الإرهاب بالوسائل الإلكترونية.

ولكننا نجد في الوقت نفسه أن المشرع قد حدد النتيجة الجرمية وذكرها على سبيل الحصر بأنها عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الأضرار بالبنية التحتية أو الأساسية للدولة.

وبالتالي نستطيع القول في عدم إمكانية تطبيق نص المادة السابعة على جريمة الإرهاب بالوسائل الإلكترونية إلا في حال كانت النتيجة الجرمية هي النتيجة الجرمية ذاتها التي حددها المشرع السوري على سبيل الحصر، وهذا التضييق في النتيجة الجرمية وبالتالي في نطاق التجريم، ينال من الإرهاب بصورتيه التقليدية الإلكترونية.

٢-الركن المعنوي في جريمة العمل الإرهابي

جريمة العمل الإرهابي من الجرائم المقصودة، يتمثل الركن المعنوي فيها بصورة القصد الجرمي، فهي لا تقع عن طريق الخطأ، إلا أن القصد الجرمي العام لا يكفي لقيام هذه الجريمة بل لابد من توافر القصد الجرمي الخاص المتمثل بإيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الأضرار بالبنى التحتية أو الأساسية للدولة.

وبالنسبة لجريمة الإرهاب بالوسائل الإلكترونية (الإرهاب المعلوماتي)، فيما يتعلق بالركن المعنوي، هي أيضاً جريمة مقصودة، لا تقع عن طريق الخطأ، ولا يكفي القصد العام وتحتاج إلى قصد خاص، لأن هذا القصد الخاص هو الذي يميزها عن غيرها من الجرائم وخاصة الجرائم الإلكترونية.

ثانياً: عقوبة جريمة العمل الإرهابي

عاقب المشرع السوري بموجب الفقرة الأولى من المادة **السابعة** من قانون مكافحة الإرهاب على جريمة العمل الإرهابي بالأشغال الشاقة المؤبدة والغرامة ضعفي قيمة الضرر، وتكون العقوبة خمس سنوات على الأقل إذا كانت الوسائل المستخدمة في العمل الإرهابي تحدث تفجيراً صوتياً فقط.

وكان المشرع السوري يعاقب على هذه الجريمة بموجب نص المادة /٣٠٥/ الملغاة بالأشغال الشاقة من خمس عشر سنة إلى عشرين سنة، ويشدد عقوبة الجاني إلى الإعدام إذا نتج عنه التخريب ولو جزئياً في بناية عامة أو مؤسسة صناعية أو منشآت أخرى أو التعطيل في سبل المخابرات والمواصلات والنقل أو إذا أفضى الفعل إلى موت إنسان.

وقد جاء قانون مكافحة الإرهاب بعقوبة واحدة محددة لجريمة العمل الإرهابي مهما كانت جسامة النتيجة المترتبة على هذا العمل أو الوسيلة المستخدمة في تنفيذ هذا العمل الإرهابي باستثناء أنه خفف العقوبة في حال كانت الوسائل المستخدمة في العمل الإرهابي تحدث تفجيراً صوتياً، كما جاء خالياً من ظروف التشديد، وبالتالي يمكننا القول أنه يجب على المشرع أن يعيد النظر في عقوبة العمل الإرهابي لجهة تشديد العقوبة حسب جسامة النتيجة الجرمية والوسيلة المستعملة في تنفيذ العمل الإرهابي، لأنه من المنافي للعدالة، المساواة بالعقوبة بين الجناة جميعهم دون الأخذ في الحسبان النتيجة الجرمية المترتبة والوسيلة المستعملة.

وبعد تحليل جريمة العمل الإرهابي إلى أركانها وعناصرها الأساسية في ضوء إمكانية تطبيقها على جريمة الإرهاب بالوسائل الإلكترونية في الفرع الأول، سننتقل إلى تحليل الجرائم المستحدثة في الفرع الثاني.

الفرع الثاني

الجرائم المستحدثة في قانون مكافحة الإرهاب

تضمن قانون مكافحة الإرهاب إضافةً إلى جريمة العمل الإرهابي، مجموعةً من الجرائم الأخرى التي ترتبط برباط وثيق مع جريمة العمل الإرهابي، ولم يكن المشرع السوري يجرم هذه الأفعال سابقاً بنصوص مستقلة، وإنما كانت تخضع للقواعد العامة المتعلقة بالمساهمة الجرمية.[١]

وبالعودة إلى قانون مكافحة الإرهاب نجد أن الجرائم المستحدثة بموجب هذا القانون هي: المنظمة الإرهابية – تمويل الإرهاب – التدريب على الأعمال الإرهابية – وسائل الإرهاب – التهديد بعمل إرهابي – الترويج للأعمال الإرهابية.

وسنتناول هذه الجرائم بشيء من الإيجاز، في ضوء إمكانية ارتكابها باستخدام الوسائل الإلكترونية (المعلوماتية).

أولاً: المنظمة الإرهابية

عالج المشرع السوري "**المنظمة الإرهابية**" بموجب نص المادة **الثالثة** من قانون مكافحة الإرهاب والتي نصت:

"**١–يعاقب بالأشغال الشاقة من عشر سنوات إلى عشرين سنة كل من أنشأ أو أدار منظمة إرهابية.**

٢–وتكون العقوبة الأشغال الشاقة المؤقتة سبع سنوات على الأقل لكل من انضم إلى منظمة أو أكره شخص بالعنف أو التهديد على الانضمام إلى منظمة إرهابية.

---

١ د. منال مروان منجد، المرجع السابق، ص ١١٢.

٣-تشدد العقوبة الواردة في هذه المادة وفق القواعد العامة المنصوص عليها في قانون العقوبات إذا كان القصد من إنشاء المنظمة الإرهابية تغيير نظام الحكم في الدولة أو كيان الدولة."

نلاحظ أن هذه المادة **تضمنت** ثلاث صور جرمية هي:

- إنشاء أو تنظيم أو إدارة منظمة إرهابية.
- الانضمام إلى منظمة إرهابية.
- إكراه شخص بالعنف أو التهديد على الانضمام إلى منظمة إرهابية.

وقد عرّف المشرع السوري المنظمة الإرهابية في المادة **الأولى** من قانون مكافحة الإرهاب بأنها: "**جماعة مؤلفة من ثلاثة أشخاص أو أكثر بهدف ارتكاب عمل إرهابي أو أكثر**".

١- **العقوبة**، نستنتج من نص المادة الثالثة من القانون رقم /١٩/ الخاص بمكافحة الإرهاب، أن المشرع السوري ميّز في العقوبة بين الشخص الذي يقوم بدور أساسي أو قيادي في منظمة إرهابية وبين الشخص الذي ينضم إلى تلك المنظمة، ويقصد بإنشاء منظمة إرهابية إيجادها أو خلقها من العدم، أي تأسيسها وتشكيلها، في حين أن المقصود بتنظيم المنظمة الإرهابية أو إدارتها هو قيام الجاني بدور أساسي وهام في المنظمة الإرهابية.

وقد ساوى المشرع في العقوبة بين جريمة الانضمام إلى منظمة إرهابية وجريمة إكراه شخص بالعنف أو التهديد على الانضمام إلى منظمة إرهابية. وكان حري بالمشرع السوري أن يشدد عقوبة الجاني الذي يكره شخص بالعنف والتهديد على الانضمام إلى منظمة إرهابية، نظراً للخطورة الإجرامية التي يمثلها، ويعاقب المشرع السوري الجناة حتى لو

لم تباشر المنظمة الإرهابية العمل أو الأعمال الإرهابية التي أُنشئت بهدف ارتكابها،[١] حتى أنه يُعاقب على هذه الجريمة دون تحديد الأعمال الإرهابية التي سيقوم الجناة بارتكابها، ويكتفي باجتماع أعضاء المنظمة الإرهابية على هدف محدد هو القيام بأعمال إرهابية دون تحديدها على وجه الدقة،[٢] وهو بذلك يسجل خروجاً على القواعد العامة التي تتطلب للعقاب على الجريمة بلوغها مرحلة التنفيذ.

٢- **الركن المعنوي**، وبالنسبة للركن المعنوي لهذه الجرائم الثلاث هي جرائم مقصودة يتمثل الركن المعنوي فيها في صورة القصد الجرمي العام، وعناصره العلم والإرادة، وقد شدد المشرع السوري العقوبة وفقاً للأحكام العامة في حال توافر قصد جرمي خاص من إنشاء المنظمة الإرهابية هو "تغيير نظام الحكم في الدولة أو كيان الدولة."

وبالعودة إلى الإرهاب بالوسائل الإلكترونية، نجد المشرع السوري عاقب على إنشاء أو إدارة المنظمة الإرهابية أو الانضمام إلى منظمة إرهابية أو إكراه شخص بالعنف أو التهديد على الانضمام إلى منظمة إرهابية دون أن يشير صراحةً إلى إمكانية ارتكاب هذه الصور الجرمية بالوسائل الإلكترونية أو المعلوماتية.

فالمشرع السوري عاقب على مجرد الإنشاء أو الإدارة أو الانضمام حتى لو لم تباشر المنظمة العمل أو الأعمال الإرهابية التي أُنشأت بهدف ارتكابها، ولم يحدد المشرع بموجب نص المادة **الثالثة** من قانون مكافحة الإرهاب آلية

---

١ د. منال مروان منجد، المرجع السابق، ص١١٤.

٢ د. منال مروان منجد، المرجع السابق، ص ١١٤.

أو كيفية أو وسائل إنشاء هذه المنظمة الإرهابية أو إدارتها أو آلية الانضمام إليها، بل ترك الباب مفتوحاً.

فقد يتم إنشاء المنظمة الإرهابية في الفضاء الإلكتروني (إنشاء مواقع إلكترونية إرهابية)، أو يتم إدارة هذه المنظمة وتوزيع الأدوار فيها من خلال شبكة الإنترنت، أو يكون الانضمام إلى هذه المنظمة الإرهابية عن طريق الفضاء الإلكتروني (المواقع على شبكة الإنترنت، شبكات التواصل الاجتماعي، غرف الدردشة ..).

ثانياً: تمويل الإرهاب

نصت المادة **الرابعة** من قانون مكافحة الإرهاب في فقرتها **الأولى** على أنه: "**مع عدم الإخلال بالأحكام المتعلقة بتجميد وحجز الأموال المنقولة وغير المنقولة وتتبعها المنصوص عليها بقانون مكافحة غسيل الأموال وتمويل الإرهاب وتعديلاته والتعليمات والقرارات ذات الصلة .. يعاقب كل من قام بتمويل عمل إرهابي أو أكثر بالإشغال الشاقة من خمس عشر سنة إلى عشرين سنة وبالغرامة ضعفي قيمة الأموال المنقولة وغير المنقولة أو الأشياء التي كانت محلا للتمويل.**"

تتكون جريمة تمويل العمل الإرهابي من ركنين ركن مادي وركن معنوي.

١- **الركن المادي** يتمثل في صورة تمويل عمل إرهابي أو أكثر بأي مال منقول أو غير منقول.

ولقد عَرّف المشرع السوري **تمويل الإرهاب** في المادة **الأولى** من قانون مكافحة الإرهاب بأنه: "**كل جمع أو إمداد بشكل مباشر أو غير مباشر بالأموال أو الأسلحة أو الذخائر أو المتفجرات أو وسائل الاتصال أو**

المعلومات أو الأشياء الأخرى بقصد استخدامها في تنفيذ عمل إرهابي يرتكبه شخص أو منظمة إرهابية."

يشمل موضوع الإمداد (أموال، أسلحة، ذخائر، متفجرات، وسائل الاتصال، معلومات، والأشياء الأخرى)، جاءت هذه المادة شاملة لكل أوجه الدعم المالي والمعنوي مباشر أو غير مباشر لأي عمل إرهابي سيقوم به شخص أو منظمة إرهابية، سواء كان العمل الإرهابي تقليدياً أو إلكترونياً، حتى أنه ذكر وسائل الاتصال والمعلومات بشكل صريح في صلب تعريف تمويل الإرهاب في المادة الأولى من قانون مكافحة الإرهاب، كما جاء المشرع بعبارة ذات مدلول واسع (..أو الأشياء الأخرى ..).

ويمكن القول إن تمويل الإرهاب عملية تهدف إلى إمداد الجماعات الإرهابية بالأموال والمعدات والأدوات اللازمة لتنفيذ مخططاتهم الإرهابية، وذلك أياً كان مصدرها، مشروع أو غير مشروع.[١] وقد يكون ممول الإرهاب شخصاً طبيعياً أو شخصاً اعتبارياً (شركة، مؤسسة) سواء كانت تمارس عملها في داخل الدولة أو خارجها.[٢]

ومن أهم خصائص عملية تمويل الإرهاب بصورة عامة هي: **خاصية الخفاء**، ذلك أن هذه العمليات تتم بسرية تامة، ولهذا من الصعب إثبات تورط ممولي الإرهاب بأية أنشطة إجرامية محددة.[٣]

ولا تقتصر عمليات التمويل على الإمداد الداخلي للجماعات الإرهابية بل أصبحت تأخذ بعداً دولياً، وذلك بقيام أشخاص أو جماعات يقيمون في دول

---

١ د. محمد السيد عرفة، تجفيف مصادر الإرهاب، الطبعة الأولى، الرياض، المملكة العربية السعودية، ١٤٣٠هـ -٢٠٠٩م، ص٢٦.

٢ د. محمد السيد عرفة، المرجع السابق، ص ٢٨.

٣ د. محمد السيد عرفة، المرجع السابق، ص ٥١-٥٢.

أخرى بإمداد الجماعات الإرهابية بالأموال والمعدات اللازمة لتنفيذ عملياتهم الإرهابية[١].

٢- **الركن المعنوي:** فيتمثل بصورة القصد الجرمي العام وعناصره العلم والإرادة، فلا بد أن يعلم الجاني بأنه يقدم المال لدعم عمل إرهابي أو أكثر وأن تتجه إرادته إلى ذلك.

٣- **العقوبة:** وقد حدد المشرع **عقوبة** هذه الجريمة بالأشغال الشاقة من خمس عشر سنة إلى عشرين سنة وبالغرامة ضعفي قيمة الأموال المنقولة وغير المنقولة أو الأشياء التي كانت محلا للتمويل.

ولابد أن نشير إلى الفقرة الأخيرة من المادة **الرابعة** والتي نصت على أنه:" **لا تخل أحكام هذه المادة بتطبيق قواعد الاشتراك الجرمي عند توافرها المنصوص عليها في قانون العقوبات العام.**"

بحيث نستطيع طرح **السؤال التالي:** إذا قام شخص عن علم ودراية بدفع مبالغ مالية وتأمين مواد متفجرة للقيام بعمل إرهابي، ثم نجحت المجموعة الإرهابية في تنفيذ هدفها ونجم عنه قتلى وجرحى ودمار في البنية التحتية والممتلكات العامة والخاصة، هل يطبق بحق ممول العمل الإرهابي نص الفقرة الأولى من المادة الرابعة ويعد فاعلاً في جريمة تمويل عمل إرهابي، أم يعد متدخلاً أساسيا عملاً بأحكام الفقرة /د/ من المادة /٢١٨/ من قانون العقوبات العام؟[٢]

نلاحظ أن المشرع السوري في المادة **الرابعة** السالفة الذكر، عاقب على جريمة تمويل العمل الإرهابي الذي يرتكبه إرهابي أو منظمة إرهابية، ولم

---

١ د. نايف بن محمد المرواني، المرجع السابق، ص١٤.

٢ د. منال مروان منجد، المرجع السابق، ص١١٦.

يعاقب على تمويل الإرهابيين أو المنظمة الإرهابية، وكان حري بالمشرع السوري لو توسع وعاقب على تمويل الإرهابيين والمنظمة الإرهابية أيضاً.

ثالثاً: التدريب على الأعمال الإرهابية

نصت الفقرة **الثانية** من المادة **الرابعة** من قانون مكافحة الإرهاب على أنه:

" **يعاقب الأشغال الشاقة من عشر سنوات إلى عشرين سنة كل من تدرب أو درب شخصاً أو أكثر على استعمال المتفجرات أو الأسلحة بمختلف أنواعها أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية وذلك بقصد استعمالها في تنفيذ عمل إرهابي.**"

نلاحظ أن هذه الفقرة تتضمن صورتين جرميتين خصص لهما المشرع عقوبةً واحدةً، هاتان الجريمتان هما:

١-الجريمة الأولى:

(التدرب على استعمال المتفجرات أو الأسلحة بمختلف أنواعها أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية وذلك بقصد استعمالها في تنفيذ عمل إرهابي).

فالنشاط الجرمي هو التدرب، فالجاني هو متلقي التدريب، وهو مشروع إرهابي، حيث أن الجاني يتدرب لدى جهة غير شرعية وهدفه من التدريب هو استعمال خبراته المكتسبة في تنفيذ أعمال إرهابية.

٢-الجريمة الثانية:

(تدريب شخص أو أكثر على استعمال المتفجرات أو الأسلحة أنواعها أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية وذلك بقصد استعمالها في تنفيذ عمل إرهابي).

يقوم الجاني بتدريب أشخاص وإعطائهم خبراته لاستخدامها في تنفيذ عمل إرهابي.

٣-أوجه التشابه بين الجريمتين:

أ- وتشترك كلا الجريمتين في موضوع التدريب، إذا لابد أن ينصب موضوع التدريب على استعمال المتفجرات أو الأسلحة بأنواعها أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية.

ب-كما تشتركان في الركن المعنوي، حيث أن كلا الجريمتين تتطلبان قصد جرمي خاص، وهو قصد استخدام هذه الخبرات في تنفيذ عمل إرهابي أو أكثر، ولا يشترط أن يتم العمل الإرهابي أو يشرع به بل يكفي أن يكون القصد هو استخدام هذه المعارف مستقبلاً في تنفيذ عمل إرهابي.[١]

ج- وقد حدد المشرع عقوبة واحدة لكلا الجريمتين هي الأشغال الشاقة من عشر سنوات إلى عشرين سنة، وكان حرياً به أن يميز في العقوبة بين من يدرب وبين من يتلقى التدريب لأن من يدرب شخص أو أكثر من شخص أشد خطورة، كما لم يميز المشرع بالنسبة للعقوبة أيضاً بالنسبة للخبرات التي يتم التدرب أو التدريب عليها بين مثلا من يدرب أو يتدرب على استعمال سلاح ناري أو يدرب أو يتدرب على تفخيخ السيارات.

أما بالنسبة للإرهاب بالوسائل الإلكترونية، فقد اقتصر نص الفقرة **الثانية** من المادة **الرابعة** من قانون مكافحة الإرهاب على التدرب أو التدريب على أمور محددة وهي "استعمال المتفجرات أو الأسلحة بمختلف أنواعها أو

---

١ د. منال مروان منجد، المرجع السابق، ص ١١٧.

الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية" بقصد استعمالها في تنفيذ عمل إرهابي، ولم يشر المشرع صراحة إلى التدرب أو التدريب على المهارات المستعملة بالإرهاب بالوسائل الإلكترونية، كالتدريب أو التدرب على (أعمال القرصنة أو صناعة الفيروسات واستخدامها، اختراق المواقع الإلكترونية، تدمير البنى التحتية المعلوماتية بوسائل معلوماتية....)، فقد أشار إلى التدرب أو التدريب على وسائل الاتصالات دون تحديد، فقد تكون هذه الوسائل وسائل اتصال تقليدية وقد تكون وسائل اتصال حديثة متطورة معلوماتية عن طريق شبكة الإنترنت.

لكن المشرع في الوقت نفسه لم يحدد المكان الذي يتم فيه التدريب أو التدرب، سواء كان التدرب أو التدريب يتم بصورة تقليدية (معسكرات)، أو في الفضاء الإلكتروني أو ما يسمى بالتلقين الإلكتروني.

رابعاً: وسائل الإرهاب

نصت المادة **الخامسة** من قانون مكافحة الإرهاب على أنه:

"١-**يعاقب بالأشغال الشاقة من خمس عشرة سنة وبالغرامة ضعفي قيمة المضبوطات كل من قام بتهريب أو تصنيع أو حيازة أو سرقة أو اختلاس الأسلحة أو الذخائر أو المتفجرات مهما كان نوعها بقصد استخدامها في تنفيذ عمل إرهابي.**

٢-وتكون العقوبة الإعدام إذا رافق هذه الأفعال قتل شخص أو إحداث عجز به."

بالنسبة لأركان هذه الجريمة فتتمثل:

١- **بركن مادي** تتعدد صور السلوك الجرمي المكون له، حيث تقع الجريمة بتهريب أو تصنيع أو حيازة أو سرقة أو اختلاس الأسلحة أو الذخائر أو المتفجرات مهما كان نوعها.

ونلاحظ أن المشرع السوري حصر محل الجريمة بالأسلحة والذخائر والمتفجرات وعاقب على تهريبها وتصنيعها وحيازتها وسرقتها واختلاسها، في الوقت الذي عَدّ من وسائل الإرهاب بموجب المادة **الأولى** من قانون مكافحة الإرهاب: الأسلحة والذخائر والمتفجرات والمواد الملتهبة والمنتجات السامة والمحرقة والعوامل الوبائية والجرثومية مهما كان نوعها، بل وأي وسيلة تؤدي الغرض ذاته أي إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الأضرار بالبنى التحتية أو الأساسية للدول، وهذا تناقض يؤدي إلى نتائج غير مقبولة.

وبالتالي كان حرياً بالمشرع السوري أن يتوسع في صور السلوك الجرمي، لتشمل أفعال أخرى كالبيع، الشراء، الإخفاء..إلخ، هذا من جهة، ويتوسع في وسائل الإرهاب بحيث تشمل إضافة إلى الأسلحة والذخائر والمتفجرات وسائل الإرهاب الأخرى التي تضمنتها المادة الأولى من قانون مكافحة الإرهاب وهي" **المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية مهما كان نوع هذه الوسائل أو أي أداة تؤدي إلى إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الأضرار بالبنى التحتية أو الأساسية للدولة.**"

٢- وبالنسبة **للركن المعنوي** لهذه الجريمة يتمثل في صورة القصد الجرمي، إلا أنه لا يكفي القصد العام وإنما تحتاج هذه الجريمة إلى قصد جرمي

خاص والذي عبر عنه المشرع السوري بقوله "بقصد استخدامها في تنفيذ عمل إرهابي"،[١] وقد عاقب المشرع على هذه الجريمة بالأشغال الشاقة من خمس عشرة سنة إلى عشرين وبالغرامة ضعفي قيمة المضبوطات لمرتكب هذا الجرم.

أخيراً نلاحظ أن المشرع السوري، إضافة إلى التناقض الذي وقع فيه بين نص المادة **الأولى** والمادة **الخامسة** من قانون مكافحة الإرهاب بالنسبة للوسائل المستعملة في تنفيذ الأعمال الإرهابية، نلاحظ تضييق نطاق التجريم بالنسبة لوسائل الإرهاب إذ حصرها بالأسلحة والذخائر والمتفجرات مهما كان نوعها، ولم يتطرق نهائياً إلى الوسائل المعلوماتية أو الوسائل التي أفرزتها التكنولوجيا الحديثة والتي تستخدم سواء في تعزيز النشاط الإرهابي التقليدي أو تستخدم في تنفيذ الهجمات الإرهابية الإلكترونية عبر الفضاء الإلكتروني.

خامساً: التهديد بعمل إرهابي

نصت المادة **السادسة** من قانون مكافحة الإرهاب على أنه:

١"-يعاقب بالأشغال الشاقة المؤقتة من هدد الحكومة بالقيام بعمل الإرهابي بهدف حمل الحكومة على القيام بعمل أو الامتناع عنه.

٢-وتكون العقوبة الأشغال الشاقة من خمس عشرة سنة إلى عشرين سنة إذا رافق التهديد خطف إحدى وسائل النقل الجوي أو البحري أو البري العامة أو الخاصة أو الاستيلاء على عقار مهما كان نوعه أو الاستيلاء على الأشياء العسكرية أو خطف شخص ما.

---

١ د. منال مروان منجد، المرجع السابق، ص ١٢٠.

٣-وتكون العقوبة الإعدام إذا أدى الفعل إلى موت الشخص."

الأصل أن المشرع الجزائي السوري يعاقب على جرم التهديد ضمن الجرائم الواقعة على الأشخاص،[١] فالتهديد يوجه إلى شخص، أما في قانون مكافحة الإرهاب فالتهديد يوجه إلى دولة وموضوعه القيام بعمل إرهابي.

أركان هذه الجريمة تتمثل في:

١- **ركن مادي** يقوم على **فعل التهديد** الموجه للحكومة و**موضوع التهديد** هو توعد الجاني القيام بأفعال إرهابية تجاه الحكومة.

أما بالنسبة لموضوع التهديد الموجه للحكومة: فالمقصود بالتهديد هو الوعيد بالشر، فالجاني يهدد الحكومة بالقيام بعمل إرهابي إذا هي لم ترضخ لطلباته والمتمثل بقيام الحكومة بعمل أو امتناعها عن عمل.

أما بالنسبة **لوسيلة التهديد** فيعاقب المشرع على تهديد الحكومة بعمل إرهابي أياً كانت وسيلته، فقد يكون التهديد كتابياً أو شفوياً سرياً أو علنياً، مباشراً أو بالواسطة، ومع تطور وسائل الاتصالات والإنترنت أصبح ارتكاب هذه الجريمة من السهولة بمكان حيث ظهرت على شاشات التلفزيون ومواقع التواصل الاجتماعي العديد من التسجيلات التي تضمنت تهديد الحكومة بالقيام بعمل إرهابي بهدف حملها على القيام بعمل ما أو الامتناع عنه.[٢]

٢- أما **الركن المعنوي** لهذه الجريمة فيتمثل في قصد جرمي خاص، إذا لا يكفي القصد الجرمي العام المتمثل بعلم الجاني أنه يهدد الحكومة بالقيام

---

١ نص المشرع الجزائي السوري على جرم التهديد الواقع ع الأشخاص في المواد من ٥٥٩ إلى ٥٦٤ من قانون العقوبات السوري الصادر بالمرسوم التشريعي رقم /١٤٨/ لعام ١٩٤٩م، ضمن الفصل الثاني من الباب الثامن في الجنايات والجنح التي تقع على الأشخاص.

٢ د. منال مروان منجد، المرجع السابق، ص ١٢١.

بعمل إرهابي واتجاه إرادته لذلك، بل يجب أن يكون قصده من وراء التهديد حمل الحكومة على القيام بعمل أو الامتناع عنه.

وبالتالي تنتفي مسؤولية من يهدد الحكومة بعمل إرهابي دون أن يتوافر لديه هذا القصد الخاص، وحبذا لو أن المشرع عاقب على جريمة تهديد الحكومة بعمل إرهابي في جميع الأحوال، وشدد العقوبة في حال اقتران التهديد بقصد حمل الحكومة على القيام بعمل أو الامتناع عنه.

٣- **العقوبة، عاقب** المشرع السوري على هذه الجريمة بعقوبة الأشغال الشاقة المؤقتة، وشدد المشرع العقوبة لتصبح الأشغال الشاقة من خمس عشر سنة إلى عشرين سنة إذا رافق التهديد خطف إحدى وسائل النقل الجوي أو البحري أو البري العامة أو الخاصة أو الاستيلاء على عقار مهما كان نوعه أو الاستيلاء على الأشياء العسكرية أو خطف شخص ما، كما شدد المشرع العقوبة إلى الإعدام إذا أدى الفعل إلى موت الشخص.

وبما أن المشرع السوري ترك الباب مفتوحاً بموجب نص المادة **السادسة** من قانون مكافحة الإرهاب، بالنسبة لموضوع التهديد وبالنسبة للوسيلة التي يتم بها التهديد، فيمكن أن يتم تهديد الحكومة بالقيام بالإعمال الإرهابية التقليدية (تفجيرات – اغتيالات ..) أو بالأعمال الإرهابية الإلكترونية (مهاجمة المواقع الإلكترونية الحكومية أو نشر الفيروسات أو تدمير البنى التحتية المعلوماتية ..إلخ) على حد سواء، عن طريق شبكة الإنترنت من خلال إصدار بيانات إلكترونية أو عن طريق مواقع التواصل الاجتماعي أو ترك رسائل على المواقع الإلكترونية الحكومية بعد اختراقها أو قرصنتها على سبيل المثال.

سادساً: الترويج للأعمال إرهابية

نصت المادة **الثامنة** من قانون مكافحة الإرهاب على أنه:

"**يعاقب بالأشغال الشاقة المؤقتة كل من قام بتوزيع المطبوعات أو المعلومات المخزنة مهما كان شكلها بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية وتنزل العقوبة نفسها بكل من أدار أو استعمل موقعاً الكترونيا لها الغرض.**"

تضمنت المادة **الثامنة** صورتين لترويج الأعمال الإرهابية:

الصورة الأولى توزيع المطبوعات أو المعلومات المخزنة مهما كان شكلها بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.

الصورة الثانية إدارة أو استعمال موقع الكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.

١- في الصورة الأولى

أ- **الركن المادي** يتمثل بقيام الجاني بتوزيع مطبوعات ورقية أو معلومات مخزنة على وسائط إلكترونية مثلاً.

ب-و**الركن المعنوي** يتمثل بقصد النشر والترويج لوسائل الإرهاب أو الأعمال الإرهابية.

٢- في الصورة الثانية

أ- **الركن المادي** يتمثل بإدارة أو استعمال موقع الكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية، ويطلق الفقه على هذا النوع من الجرائم "الإرهاب الإلكتروني".[١]

---

١ د. منال مروان المنجد، المرجع السابق، ص ١٢٣.

حيث تستخدم وسائل الاتصال والمعلومات وتوظف لنشر وترويج وسائل الإرهاب أو الأعمال الإرهابية.

ب-**ركن معنوي** يتمثل بقصد النشر والترويج لوسائل الإرهاب أو الأعمال الإرهابية.

تعد هذه الصورة جانباً من جوانب الإرهاب الإلكتروني، وهي الإشارة الوحيدة من المشرع السوري، للإرهاب بالوسائل الإلكترونية (الإرهاب المعلوماتي)، وهي إدارة أو استعمال موقع إلكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية، وقد أشار المشرع إلى استعمال الموقع الإلكتروني أو إدارته فقط في حال الترويج لوسائل الإرهاب أو الأعمال الإرهابية دون التطرق إلى الصور الأخرى لاستخدام المواقع الإلكترونية في تعزيز النشاط الإرهابي التقليدي أو الإلكتروني مثل (تمويل – تجنيد – تدريب ..) أو استخدامها لتنفيذ هجمات إرهابية إلكترونية مثل (نشر فيروسات – إرسال بريد واغل ..).

فالمشرع السوري كان مقتضباً إلى أبعد الحدود في جريمة الترويج للأعمال الإرهابية، ونحن مع الرأي الذي يقول بأنه يفضّل لو أن المشرع السوري توسع في تجريم الإرهاب الإلكتروني.[١]

ج- العقوبة، وقد حدد المشرع السوري للجاني في كلا الصورتين **عقوبة واحدة** هي الأشغال الشاقة المؤقتة من ٣ إلى ١٥ سنة.

مما تقدم نلاحظ ما يلي: وبعد البحث في قانون مكافحة الإرهاب ومدى إمكانية تطبيق نصوصه على الإرهاب بالوسائل الإلكترونية (الإرهاب

---

١ د. منال مروان منجد، المرجع السابق، ص١٤٢.

المعلوماتي)، نلاحظ أن المشرع السوري لم يشر صراحةً إلى الإرهاب بالوسائل الإلكترونية أو إمكانية ارتكاب عمل إرهابي باستخدام وسائل معلوماتية، باستثناء المادة **الثامنة** تحت عنوان **"الترويج للأعمال الإرهابية"** التي أشارت بشكل ضمني إلى جانب من جوانب الإرهاب بالوسائل الإلكترونية، وهو **إدارة أو استعمال موقع إلكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.**

وبالتالي ندعو المشرع السوري إلى عدم الاكتفاء بالمادة الثامنة من قانون مكافحة الإرهاب السالفة الذكر، والتوسع في تجريم الإرهاب بالوسائل الإلكترونية، وذلك إما بالنص عليه صراحةً كجريمةٍ مستقلة بذاتها أو التوسع في تعريف العمل الإرهابي بموجب المادة الأولى من قانون مكافحة الإرهاب لتشمل في طياتها الإرهاب بالوسائل الإلكترونية، نظراً لخطورة هذه الجريمة وحداثتها، وانتشارها الكبير في الفضاء الإلكتروني.

وحبذا لو توسع المشرع السوري في صور استخدام المواقع الإلكترونية في الأنشطة الإرهابية مثل (التجنيد –التدريب–التهديد–جمع معلومات–..)، حيث أن المادة الثامنة من قانون مكافحة الإرهاب، أشارت إلى صورةٍ واحدةٍ لاستخدام المواقع الإلكترونية وهي **إدارة أو استعمال موقع إلكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.**

كما يجدر التنويه إلى ضرورة مد نطاق نصوص مواد قانون مكافحة الإرهاب وذلك بالنسبة للجرائم المستحدثة (المنظمة الإرهابية – تمويل الإرهاب – التدريب على الإعمال الإرهابية – وسائل الإرهاب – التهديد بعمل إرهابي) التي نص عليها قانون مكافحة الإرهاب والتي كانت تخضع سابقاً للقواعد العامة المتعلقة بالمساهمة الجرمية، بالنص صراحة على

إمكانية ارتكابها بوسائل إلكترونية، لتشمل أوجه وأنشطة الإرهاب بالوسائل الإلكترونية كلها من جهة، وحرصاً على وضوح النص من جهة أخرى.

وبذلك نكون قد انتهينا من عرض الإطار القانوني للإرهاب بالوسائل الإلكترونية في التشريع السوري، في ضوء المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، والقانون رقم /١٩/ لعام ٢٠١٢م، والقصور التشريعي الذي يعتري كل من هذين النصين القانونيين في معالجة الإرهاب بالوسائل الإلكترونية، وتضمنهما بعض الثغرات التي نقترح على المشرع السوري إعادة النظر فيها للقضاء على الإرهاب بأشكاله كلها سواء كان تقليدياً أو معلوماتياً، وذلك بالنص على الإرهاب بالوسائل الإلكترونية كجريمة مستقلة بذاتها، سواء في قانون مكافحة الإرهاب أو قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية أو التوسع في تعريف العمل الإرهابي بموجب المادة الأولى من قانون مكافحة الإرهاب ليشمل الإرهاب بالوسائل الإلكترونية.

وبعد البحث في ماهية الإرهاب بالوسائل الإلكترونية في الفصل الأول، سننتقل إلى دراسة كيفية مكافحة الإرهاب بالوسائل الإلكترونية في الفصل الثاني من هذه الدراسة.

الفصل الثاني

مكافحة الإرهاب بالوسائل الإلكترونية

تتزايد مخاطر الإرهاب بالوسائل الإلكترونية، في ظل ثورة الاتصالات واعتماد الدول بشكل رئيسي على تقنية المعلومات وشبكة الإنترنت، مما يُوجب العمل للحد من هذه الجرائم إن لم يكن القضاء عليها، وتواجه مكافحة الإرهاب بالوسائل الإلكترونية تحديات كبيرة، نظراً للأساليب التقنية التي يستخدمها من ناحية وتنوع أشكاله من ناحية أخرى.[١]

ويعد الفراغ التنظيمي والقانوني لدى دول عديدة، حول الجريمة المعلوماتية والإرهاب بالوسائل الإلكترونية، من الأسباب الرئيسية في انتشار الإرهاب بالوسائل الإلكترونية،[٢] كما أن عدم وجود جهة مركزية موحدة تتحكم بما يعرض على شبكة الإنترنت وتسيطر على مدخلاتها ومخرجاته، يعد سبباً في تفشي هذه الظاهرة، وكل ما تملكه الجهات التي تحاول فرض الرقابة، هو المنع من الوصول إلى بعض المواقع المحجوبة، أو إغلاقها وتدميرها،[٣] لكل هذه الأسباب أصبح الإرهاب بالوسائل الإلكترونية هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية.[٤]

---

[١] د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية سوسيولوجية، المرجع السابق، ص ٢٣٣.

٢ الإرهاب الإلكتروني مفهومه ووسائل مكافحته، شبكة ضياء للمؤتمرات والدراسات، تاريخ النشر: ٢٩ أكتوبر ٢٠١٤، متاح على الرابط: diae.net/١٦٢٤٣ ، تاريخ الزيارة: ٢٠١٥/٧/١.

٣ الإرهاب الإلكتروني مفهومه ووسائل مكافحته، المرجع السابق.

٤ الإرهاب الإلكتروني الثوابت والمتغيرات، مدير البحث العلمي في وزارة الأوقاف، حزب البعث العربي الاشتراكي–القطر السوري–القيادة القطرية، تاريخ النشر: ٢٠١٤/١٢/١٤، متاح على الرابط: baathparty.sy/Arabic/index.php?node=٥٥٢&cat=١٢٦٩&، تاريخ الزيارة: ٢٠١٥/٥/٣.

ولما كان للإرهاب بالوسائل الإلكترونية هذا القدر من الخطورة، كان لزاماً على الجهات الأمنية والتشريعية أن تطور أساليبها ووسائلها حتى يمكنها التعامل مع جرائم ثورة المعلومات ومواجهة هذه الجرائم بأسلوب علمي وغير تقليدي ليمكنها أن تقف أمام تحديات عصر العولمة،[١] من خلال الاعتماد على آخر ما توصل إليه العلم، لأن مطوري تكنولوجيا المعلومات وخبراء الإنترنت، مُطالبون باستمرارية العمل على أنشطة الحماية وسد الثغرات لحماية هذا الفضاء المعلوماتي من أن يصبح ساحة إرهاب دامية،[٢] كما يتوجب على الحكومات تطوير قدراتها للتصدي للتهديدات الإلكترونية بتوفير التقنيات اللازمة للحماية، وتقنين القواعد والتشريعات على المستوى الوطني والدولي، حيث يضفي البعد الدولي للظاهرة تعقيداً في شأن المواجهة الدولية خاصةً مع عدم وجود إطار قانوني دولي واضح لتناول هذه الظاهرة المستحدثة، ما يستلزم إيجاد قانون دولي جديد أو محاولة عقد اتفاقيات مكملة للاتفاقيات الدولية، أو تفعيل اتفاقيات أخرى قائمة،[٣] وتنمية الوعي لدى المجتمع بخاصة في أوساط الشباب، في ظل التقدم التقني الذي فتح آفاقاً جديدة وجلب معه مشكلات ومخاطر جديدة.

---

[١] د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية سوسيولوجية، المرجع السابق، ص ٢٣٣

٢ د. حسين بن سعيد بن سيف الغافري، الإرهاب الإلكتروني، هيئة تقنية المعلومات، سلطنة عمان، متاح على الرابط: itaportal=ar/pags/page.aspx&nid=١&pid=٩٨lid=seoman@ita.gov.com/، تاريخ الزيارة: ٢٠١٣/٥/١م.

٣ د. سعد عطوة الزنط، المرجع السابق، ص ٢٤.

تتطلب مكافحة الإرهاب بالوسائل الإلكترونية اتخاذ إجراءات، منها يتعلق بالوقاية والمنع، وإجراءات تتعلق بالتجريم والعقاب،[١] وعلى ذلك فإننا نقسم هذا الفصل إلى مبحثين:

المبحث الأول: نتناول فيه مكافحة الإرهاب بالوسائل الإلكترونية تشريعياً، على المستوى التشريعي، سواء على الصعيد المحلي /الوطني/ أو الدولي.

والمبحث الثاني: نتناول فيه مكافحة الإرهاب بالوسائل الإلكترونية فنياً، على المستوى الرقمي عبر إجراءات الوقاية التقنية /الفنية/.

[١] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، الملتقى العلمي، الجرائم المستحدثة في ظل المتغيرات والمتحولات الإقليمية والدولية، خلال الفترة من: ٢-٢٠١٤/٩/٤م، عمان، المملكة الأردنية الهاشمية، ٢٠١٤م، ص ٢٤.

المبحث الأول

مكافحة الإرهاب بالوسائل الإلكترونية تشريعياً

بغية الحديث عن مكافحة الإرهاب بالوسائل الإلكترونية على المستوى التشريعي، ارتأينا بدايةً التعاطي مع موضوع الإرهاب بالوسائل الإلكترونية داخل النظم القانونية للدول سواء العربية أو الأجنبية، وثانياً، التطرق للإرهاب بالوسائل الإلكترونية في إطار الاتفاقيات الدولية، والتعاون الدولي. بالتالي سنقسم هذا المبحث إلى مطلبين:

المطلب الأول: الإرهاب بالوسائل الإلكترونية في التشريعات الوطنية.

المطلب الثاني: الإرهاب بالوسائل الإلكترونية على الصعيد الدولي.

المطلب الأول

الإرهاب بالوسائل الإلكترونية في التشريعات الوطنية

انتشر الإرهاب بالوسائل الإلكترونية بصورة ملحوظة في السنوات الأخيرة، بحيث لم تستطع التشريعات الوطنية مواجهته أو الحّد منه، فلا تزال التشريعات الوطنية في أغلب دول العالم تنظر إلى الجرائم الإلكترونية على أنها جرائم تقليدية، ويبدو أن الفراغ التشريعي الوطني يعد من الأسباب الرئيسية في عدم الحد من هذه الجرائم، مما يوجب سد هذا الفراغ بعقوبات رادعة، والتركيز على الإرهاب بالوسائل الإلكترونية، حتى لا يستغل الإرهابيون ذلك لتنفيذ جرائمهم في دول لا تجرم هذه الأفعال بصورة واضحة،[١] هذا من جهة، ومن جهةٍ أخرى، فإن الدول التي تصدت لهذه

---

١ د. فراس طحان، المرجع السابق، ص ٣٧٥.

الظاهرة المستجدة بموجب قوانينها الوطنية، تراوحت بين من تستحضر نصوصها مصطلح الإرهاب بالوسائل الإلكترونية دون إعطائه تعريفاً محدداً، وقوانين جزائية أخرى تتضمن المصطلح وتقدم تعريفات قانونية له،[١] ومنها من تعطي مفهوم ضيقاً للإرهاب بالوسائل الإلكترونية ، ومنها من توسع في دائرة الأنشطة التي تعد إرهاباً إلكترونياً.[٢]

وهناك تقرير عن الجريمة الإلكترونية والقوانين الوطنية، تناول الوضع القانوني ل ٥٢ دولة، وبين أن هناك عشر دول فقط هم الذين أصدروا تشريعات لمواجهة الجرائم الإلكترونية، وأن تسعة دول قد عدّلوا تعديلاً جزئياً في قوانينهم، وأن ثلاثة ثلاثين دولة لم تقم بأي تعديل أو تحديث للقوانين الوطنية.[٣]

وسنتطرق انسجاماً مع متطلبات الدراسة أولاً لتشريعات الدول العربية، وسنأخذ مثالاً عليها تشريعات كل من المملكة العربية السعودية والإمارات العربية المتحدة والمغرب والأردن، ثم نتطرق بعدها لتشريعات بعض الدول الأجنبية كتشريع الولايات المتحدة الأمريكية وبريطانيا وفرنسا.

لذلك لابد من تقسيم هذا المطلب إلى فرعين:

الفرع الأول: الإرهاب بالوسائل الإلكترونية في تشريعات الدول العربية.

الفرع الثاني: الإرهاب بالوسائل الإلكترونية في تشريعات الدول الأجنبية.

---

١ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٠.

٢ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٠.

٣ محمد سيد سلطان، المرجع السابق، ص ١٧.

الفرع الأول

الإرهاب بالوسائل الإلكترونية في تشريعات الدول العربية

رغم صدور تشريعات عديدة بشأن جرائم الإنترنت، إلا أن مكافحة هذه الجرائم في عدد كبير من الدول العربية لا يزال دون غطاء تشريعي يحددها ويجرم صورها كلها،[١] فالبيئة الإلكترونية العربية ليست بمنأى من الجريمة الإلكترونية والإرهاب بالوسائل الإلكترونية، بل يمكن القول إنها أقرب إلى أيدي الإرهابيين،[٢] فقد درجت المنشآت الرسمية وغير الرسمية في العالم العربي على عدم الإفصاح عن ظاهرة الجرائم الإلكترونية، وذلك لدواعي أمنية وغيرها لكن هذا لا يعني عدم وقوعها.[٣]

لذا نحن مع القول بأن البيئة الإلكترونية العربية لم تصل بعد إلى مستوى أمني مرتفع يصل بها إلى درجة عالية من الأمان، وهذه المشكلة سوف تتضاعف مع نمو فكر التطرف في الوطن العربي.[٤]

ويجد المتتبع للتشريعات الجزائية العربية أن موقف هذه التشريعات متباين من الإرهاب بالوسائل الإلكترونية، فهي لم تدرج الإرهاب بالوسائل الإلكترونية كجريمة مستقلة بذاتها، فالبعض من هذه التشريعات العربية نص على تجريم الإرهاب بمفهومه العام ولم يعالج الإرهاب بالوسائل

---

١ د. فراس طحان، المرجع السابق، ص ٣٧٦.

٢ محمد سيد سلطان، المرجع السابق، ص ٥.

٣ أ.د. عبد الرحمن عبد العزيز الشنيفي، المواجهة الأمنية للإرهاب الإلكتروني، الحلقة العلمية، الإرهاب والإنترنت، خلال الفترة من ١٥-٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، القاهرة، مصر، ١٤٢٩هـ/٢٠٠٨م، ص٣.

٤ محمد سيد سلطان، المرجع السابق، ص ٥.

الإلكترونية، والبعض الآخر -أي التشريعات- وسعت من نطاق تعريف الإرهاب ليشمل الإرهاب بالوسائل الإلكترونية.[١]

لذلك سنقوم في هذا الفرع بدراسة الإرهاب بالوسائل الإلكترونية في تشريعات بعض الدول العربية.

أولاً: الإرهاب بالوسائل الإلكترونية في تشريع المملكة العربية السعودية

١- الإرهاب بالوسائل الإلكترونية في بعض الأنظمة واللوائح والقرارات

أصدرت المملكة العربية السعودية بعض الأنظمة واللوائح والقرارات لمواجهة الجرائم الإلكترونية والإرهاب بالوسائل الإلكترونية، فقد أصدر مجلس الوزراء السعودي القرار /١٦٣/ تاريخ ١٤١٧/١٠/٢٤هـ الذي نص فيه على الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها وتضمن:[٢]

أ- الامتناع عن الوصول أو محاولة الوصول إلى أنظمة الحواسيب الألية الموصولة بشبكة الإنترنت أو أي معلومات خاصة دون الحصول على موافقة المالكين أو من يتمتعون بحقوق ملكية لها.

ب-الامتناع عن إرسال معلومات مشفرة أو استقبالها إلا بترخيص من إدارة الشبكة المعنية.

ج-الامتناع عن الدخول إلى حسابات الأخرين أو محاولة استخدامها دون تصريح.

---

١ د. أيسر محمد عطية، المرجع السابق، ص ٣٤.

٢ د. عبد الرحمن بن عبد الله السند، المرجع السابق، ص٣٦.

د- الامتناع عن اشراك الآخرين في حسابات الاستخدام واطلاعهم على الرقم السري للمستخدم.

ه- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.

و- الامتناع عن تعريض الشبكة الداخلية للخطر عن طريق فتح ثغرات أمنية عليها.

ز- الامتناع عن استخدام المكثف للشبكة بما يشغلها ويمنع الأخرين من الاستفادة من خدماتها.

ح- الالتزام بما تصدره وحدة خدمات الإنترنت بمدينة الملك عبد العزيز من ضوابط لاستخدام الشبكة.

٢- الإرهاب بالوسائل الإلكترونية في نظام مكافحة الجرائم المعلوماتية رقم م/١٧ لعام ٢٠٠٧م

كما أصدرت هيئة الاتصالات وتقنية المعلومات نظام مكافحة الجرائم المعلوماتية رقم م/١٧ ١٤٢٨هـ، ٢٠٠٧/٣/٢٥، حيث اشتمل على ستة عشرة مادة تنظم استخدام الإنترنت وكان من ضمن تلك المواد، مواد تعالج وبشكل مباشر إساءة استخدام الإنترنت من قبل المنظمات الإرهابية.

وبذلك تكون السعودية من أوائل الدول العربية التي أصدرت قانوناً يجرم استخدام التنظيمات الإرهابية، وكل شخص تسول له نفسه استخدام التكنولوجيا في ارتكاب الجرائم الإرهابية.[١]

---

١ اللواء د. مصطفى محمد موسى، التنظيمات الإرهابية وشبكة الإنترنت، الندوة العلمية استشراق التهديدات الإرهابية، الرياض، المملكة العربية السعودية، ٧-١٤٢٨/٨/٩هـ الموافق ٢٠-٢٠٠٧/٨/٢٢م، ص ٥٢.

أ- فقد نصت **المادة السادسة** في **الفقرة الأولى**، من نظام مكافحة الجرائم المعلوماتية لعام ٢٠٠٧م على أنه:

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

- **انتاج ما من شانه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده أو إرساله، أو تخزينه عن طريق الشبكة العنكبوتية، أو أحد أجهزة الحاسب الآلي.**

نستنتج من المادة السابقة أن المشرع السعودي جرم استخدام الشبكة العنكبوتية في إنتاج أو إعداد أو إرسال أو تخزين ما من شأنه المساس بالنظام العام.

ب-كما نصت **المادة السابعة** من النظام نفسه على أنه:

يعاقب بالسجن مدة لا تزيد عن عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أي من الجرائم المعلوماتية الآتية:

- **إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.**

- **الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي او الخارجي للدولة، أو اقتصادها الوطني.**

نلاحظ إن المادة السابعة تضمنت صورتين جرميتين:

- الصورة الأولى: إنشاء موقع لمنظمة إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لجهة:
  - تسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها.
  - ترويج أفكارها.
  - أو تمويلها.
  - نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات.
  - أي أداة تستخدم في الأعمال الإرهابية.
- الصورة الثانية: الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي او الخارجي للدولة، أو اقتصادها الوطني، وهذا ما يسمى بالتجسس الإلكتروني وهو جانب من جوانب الإرهاب بالوسائل الإلكترونية.

ج- كما تضمنت **المادة الثامنة** من النظام نفسه الظروف المشددة، والتي نصت على أنه:

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترفت الجريمة بإحدى الحالات الآتية:

- **ارتكاب الجاني الجريمة من خلال جريمة منظمة.**

- **شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكاب الجريمة مستغلاً سلطاته ونفوذه.**
- **التغرير بقاصر ومن في حكمهم، واستغلالهم.**
- **صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.**

نستنتج مما سبق، أن نظام مكافحة الجريمة المعلوماتية في المملكة العربية السعودية، لم يتطرق للإرهاب بالوسائل الإلكترونية بشكل مستقل، لكنه تضمن مواد تعالج وبشكل مباشر إساءة استخدام شبكة الإنترنت من قبل المنظمات الإرهابية، فقد أشار إلى إمكانية استخدام الشبكة العنكبوتية في إنتاج أو إعداد أو إرسال أو تخزين ما من شأنه المساس بالنظام العام، وإلى إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، وجرّم الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي او الخارجي للدولة، أو اقتصادها الوطني (التجسس الإلكتروني).

وتمثل هذه الصور الجرمية كلها مفردات من الإرهاب بالوسائل الإلكترونية ولا تشمل سائر أنشطته.

فالصور الأساسية للإرهاب بالوسائل الإلكترونية المتمثلة بتدمير البنية التحتية المعلوماتية أو السيطرة عليها لم تلحظ في النظام السالف الذكر، كما أن هناك صور أخرى لاستخدام الجماعات الإرهابية للمواقع الإلكترونية لم ينص عليها المشرع السعودي لها مثل التجنيد والتدريب (التلقين الإلكتروني) أو استخدامها لتنفيذ هجمات إرهابية إلكترونية.

ولا بد إن نشير إلى الأمر الملكي الذي أصدره خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز، بالسجن مدة لا تقل عن ثلاثة أعوام ولا تزيد عن عشرين عاماً، لكل من يشارك في أعمال قتالية خارج السعودية، أو ينتمي إلى التيارات والجماعات الدينية أو الفكرية المتطرفة، أو المصنفة داخلياً أو إقليمياً أو دولياً منظمات إرهابية، مع شمول العقوبة من يؤيدون تلك الجماعات والتيارات ومن يفصحون عن التعاطف معها " بأي وسيلة كانت"، أثراً كبير في قص أجنحة "القاعدة" على "تويتر" من داخل السعودية.[١]

٣- الإرهاب بالوسائل الإلكترونية في نظام (مكافحة الإرهاب وتمويله) لعام ٢٠١٤م

نجد أن نظام (مكافحة الإرهاب وتمويله) لعام ٢٠١٤م، والذي يضم أربعين مادة قانونية، لم يتطرق نهائياً إلى الإرهاب بالوسائل الإلكترونية، حتى إنه لم يشر أبداً إلى إمكانية استخدام الوسائل الإلكترونية أو الشبكة في القيام بالأعمال الإرهابية.

أ- فقد عَرّف نظام (مكافحة الإرهاب وتمويله)، الجريمة الإرهابية في مادته الأولى الفقرة /أ/، بأنه:

"**كل فعل يقوم به الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بشكل مباشر أو غير مباشر، يقصد به الإخلال بالنظام العام، أو زعزعة أمن المجتمع واستقرار الدولة أو تعريض وحدتها الوطنية للخطر، أو تعطيل**

---

١ الكاتب زبير الأنصاري، معسكر "تويتر" يعوض " القاعدة" عن "الفاروق" وتلال "الرقة ، نقلاً عن الحياة، موقع السكينة، تاريخ النشر: ١٢ مايو ٢٠١٤، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٣/١م.

النظام الأساسي للحكم أو بعض مواده، أو الإساءة إلى سمعة الدولة أو مكانتها، أو إلحاق الضرر بأحد مرافق الدولة أو مواردها الطبيعية، أو محاولة إرغام إحدى سلطاتها على القيام بعمل أو الامتناع عنه، أو التهديد بتنفيذ أعمال تؤدي إلى المقاصد المذكورة أو التحريض عليها."

نستنتج من التعريف السابق، أن المشرع السعودي قد توسع بشكل كبير في تعريف الجريمة الإرهابية، واستخدم مصطلحات وعبارات واسعة فضفاضة، مثال ذلك عبارة: زعزعة أمن المجتمع واستقرار الدولة، أو عبارة الإساءة إلى سمعة الدولة أو مكانتها، ويؤدي هذا التوسع إلى التضييق على الحريات الفردية وإدخال جرائم تقليدية في إطار العمل الإرهابي، فضلاً عن ذلك لم يشير إلى الوسائل التي يمكن أن تستخدم في الجريمة الإرهابية هذا من جهة، ومن جهة أخرى، إن علة تجريم العمل الإرهابي تقوم بالدرجة الأولى على نشر الخوف والفزع والرعب باستخدام العنف، وهذا لم يُلحظ في تعريف المشرع السعودي للجريمة الإرهابية.

ب-كما عرف النظام السالف الذكر، جريمة تمويل الإرهاب في المادة الأولى الفقرة /ب/ بأنها:

كل فعل يضمن جمع أموال، أو تقديمها، أو آخذها، أو تخصيصها، أو نقلها، أو تحويلها – أو عائداتها- كلياً أو جزئياً لأي نشاط إرهابي فردي أو جماعي، منظم أو غير منظم، في الداخل أو الخارج، سواء أكان ذلك بشكل مباشر أو غير مباشر من مصدر مشروع أو غير مشروع.

أو القيام لمصلحة هذا النشاط أو عناصره بأي عملية بنكية أو مصرفية أو مالية أو تجارية، أو الحصول مباشرة أو بالوساطة على أموال لاستغلالها

لمصلحته، أو للدعوة والترويج لمبادئه، أو تدبير أماكن للتدريب، أو إيواء عناصره، أو تزويدهم بأي نوع من الأسلحة أو المستندات المزورة، أو تقديم أي وسيلة مساعدة أخرى من وسائل الدعم والتمويل مع العلم بذلك، وكل فعل يشكل جريمة في نطاق إحدى الاتفاقيات الواردة في مرفق الاتفاقية الدولية لقمع وتمويل الإرهاب، وبالتعريف المحدد بالاتفاقيات.

نلاحظ أن المشرع السعودي قد توسع في تعريف تمويل الإرهاب ليشمل أوجه الدعم والتمويل كلها، لأي عمل إرهابي سواء كان تقليدياً أو إلكترونياً، فاستعمل مصطلح مرناً بقوله: ".. أو تقديم أي وسيلة مساعدة أخرى من وسائل الدعم والتمويل مع العلم بذلك .."

فنظام (مكافحة الإرهاب وتمويله) تضمن أربع صور جرمية فقط، وهي:

أ- الجريمة الإرهابية، والتهديد بها والتحريض عليها، المادة الأولى الفقرة /أ/.

ب-جريمة تمويل الإرهاب، المادة الأولى الفقرة /ب/.

ج- الجريمة الإرهابية المرتكبة من قبل شخص سعودي أو أجنبي خارج المملكة العربية السعودية، المادة الثالثة.

ذ- التآمر بين أثنين أو أكثر لتنفيذ جريمة من الجرائم المنصوص عليها في هذا النظام والذي يعد ظرف مشدد للعقوبة، المادة الثانية والعشرين.

لم يجرم المشرع السعودي بموجب نظام (مكافحة الإرهاب وتمويله)، إنشاء منظمة إرهابية، أو التدريب على الأعمال الإرهابية، ولم يتطرق إلى وسائل الإرهاب، ولم يجرم الترويج للأعمال الإرهابية، ولم يشر إلى الإرهاب بالوسائل الإلكترونية أو استخدام الوسائل الإلكترونية في الأعمال الإرهابية،

فقد كان مقتضب جداً في الصور الجرمية التي تضمنها، هذا من جهة، إضافة إلى التوسع وعدم الوضوح في تعريف الجريمة الإرهابية.

٤- المقارنة مع التشريع السوري

أ_ بالنسبة لتشريعات مكافحة الجريمة المعلوماتية

إن المشرع السعودي وبموجب نظام مكافحة الجريمة المعلوماتية رقم م/١٧ لعام ٢٠٠٧، لم ينص على جريمة الإرهاب بالوسائل الإلكترونية كجريمة مستقلة، لكنه تضمن مواد تعالج وبشكل مباشر إساءة استخدام شبكة الإنترنت من قبل المنظمات الإرهابية، وهي:

- جريمة استخدام الشبكة العنكبوتية في إنتاج أو إعداد إرسال أو تخزين ما من شأنه المساس بالنظام العام، المادة السادسة من نظام مكافحة الجريمة المعلوماتية.
- جريمة إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، لتسهيل الاتصال بين أعضائها، او ترويج أفكارها، أو تمويلها ...، الفقرة /أ/ من المادة السابعة من نظام مكافحة الجريمة المعلوماتية.
- جريمة التجسس الإلكتروني، الفقرة /ب/ من المادة السابعة من نظام مكافحة الجريمة المعلوماتية.

نجد في المقابل، أن المشرع السوري بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، لم ينص صراحةً على استخدام الشبكة المعلوماتية من قبل الإرهابيين، باستثناء المادتين /٢٨/ و /٢٩/ المرتبطتين بالإرهاب بالوسائل الإلكترونية وبشكل غير مباشر.

ب- بالنسبة لتشريعات مكافحة الإرهاب

إن نظام (مكافحة الإرهاب وتمويله) السعودي، وكما أسلفنا سابقاً، لم يشر إلى الإرهاب بالوسائل الإلكترونية أو استخدام الوسائل الإلكترونية في الأعمال الإرهابية، فقد كان مقتضب جداً في الصور الجرمية التي تضمنها، هذا من جهة، إضافة إلى التوسع وعدم الوضوح في تعريف الجريمة الإرهابية.

ثانياً: الإرهاب بالوسائل الإلكترونية في تشريع الإمارات العربية المتحدة

١- الإرهاب بالوسائل الإلكترونية بموجب نص قانون اتحادي رقم /٥/ لسنة ٢٠١٤م

فيما يتعلق بمكافحة الإرهاب بالوسائل الإلكترونية، فقد نص قانون اتحادي رقم /٥/ لسنة ٢٠١٤م في شأن مكافحة جرائم تقنية المعلومات،[١] في:

أ- مادته **السادسة والعشرين** على **أنه: " يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مليون درهم ولا تجاوز مليوني درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد التسهيل 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**

---

١ القانون الاتحادي رقم ٥ لسنة ٢٠١٤م في شأن مكافحة جرائم تقنية المعلومات، تم بموجب المادة /٥٠/ منه، إلغاء القانون الاتحادي رقم ٢ لسنة ٢٠٠٦م في شأن مكافحة جرائم تقنية المعلومات.

الأجهزة الحارقة أو المتفجرات، أو أية أدوات أخرى تستخدم في الأعمال الإرهابية ".

نستنتج من النص القانوني أن المشرع الإماراتي، عاقب كل من إنشء أو أدار أو أشرف على موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية بقصد:

- التسهيل الاتصال بقياداتها أو أعضائها.
- استقطاب عضوية لها.
- ترويج أو تحبيذ أفكارها.
- تمويل أنشطتها.
- توفير المساعدة الفعلية لها.
- بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أية أدوات أخرى تستخدم في الأعمال الإرهابية.

وكما أسلفنا سابقاً فإن صور استخدام المواقع الإلكترونية جميعها أو النشر على شبكة الإنترنت من قبل الجماعات الإرهابية ماهي إلا جوانب أو مفردات من الإرهاب بالوسائل الإلكترونية.

ب- كما نصت المادة **السادسة والأربعون** من قانون اتحادي رقم ٥ لسنة ٢٠١٤م على أنه:

"**يعد ظرفاً مشدداً استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون.**

كما يعد ظرفاً مشدداً ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة."

إن قصد المشرع الإماراتي من **الفقرة الأولى** من المادة السابقة، هو عدم تكرار الجرائم التقليدية في حال ارتكبت بواسطة شبكة الإنترنت أو أي وسيلة معلوماتية أخرى، وبالتالي نستنتج أن استخدام (شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات) لارتكاب عمل إرهابي مجرم بموجب القوانين الجزائية الإماراتية، يعد ظرفاً مشدداً.

وبالنسبة **للفقرة الثانية** من المادة السادسة والأربعين من القانون نفسه، فقد نص المشرع الإماراتي، على أن ارتكاب أي جريمة معلوماتية نص عليها القانون الاتحادي /٥/ لعام ٢٠١٤م، لصالح جماعة إرهابية، يعد ظرفاً مشدداً، وهذه إشارة ضمنية من المشرع الإماراتي إلى الإرهاب بالوسائل الإلكترونية، لأن الصورة الأساسية للإرهاب بالوسائل الإلكترونية هي إرتكاب جرائم معلوماتية بقصد نشر الخوف والفزع.

٢- الإرهاب بالوسائل الإلكترونية بموجب نص قانون اتحادي رقم /١/ لعام ٢٠٠٤م

أ- عرف المشرع الإماراتي العمل الإرهابي في المادة الأولى من قانون اتحادي رقم /١/ لعام ٢٠٠٤م، بأنه: "**كل فعل أو امتناع عن فعل يلجأ إليه الجاني، تنفيذاً لمشروع إجرامي فردي أو جماعي، بهدف نشر الرعب بين الناس أو ترويعهم، إذا كان من شأن ذلك الإخلال بالنظام**

العام أو تعريض سلامة المجتمع وأمنه للخطر أو إيذاء الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر بمن في ذلك ملوك ورؤساء الدول والحكومات والوزراء وافراد عائلاتهم وأي ممثل أو موظف رسمي لدولة أو منظمة دولية ذات صفة حكومية وأفراد أسرهم الذين يعيشون في كنفهم المقررة لهم الحماية وفقاً للقانون الدولي أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الطبيعية للخطر".

فالمشرع الإماراتي بتعريفه للعمل الإرهابي، لم يحدد صورة الفعل الجرمي المكون لجريمة العمل الإرهابي، وإنما جاء النص عاماً فقد اكتفى بتحديد العناصر المميزة له، ولم يحدد وسائل ارتكاب العمل الإرهابي، لكنه في المقابل حدد النتيجة الجرمية المترتبة على العمل الإرهابي وتوسع بها، بالتالي يمكننا القول أن هذا التعريف يشمل بطياته الإرهاب بالوسائل الإلكترونية بشكل ضمني.

ب- ولابد إن نشير إلى المادة السابعة من قانون اتحادي رقم /١/ **لعام ٢٠٠٤**م المتعلق بمكافحة الجريمة الإرهابية، والتي تنص على أنه:

"**يعاقب بالحبس المؤبد أو المؤقت كل من درب شخصاً أو أكثر على استعمال الأسلحة التقليدية أو غير التقليدية أو وسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية أو أية وسيلة اتصال أخرى أو علمه فنوناً حربية أو أساليب قتالية أياً كانت، بقصد الاستعانة به لتنفيذ عمل إرهابي**"

فالمشرع الإماراتي نص صراحة بموجب القانون رقم ٢٠٠٤/١م، على جريمة تدريب شخص أو أكثر على وسائل الاتصال الإلكترونية، بقصد الاستعانة بها لتنفيذ عمل إرهابي.

٣- المقارنة مع التشريع السوري

أ_ بالنسبة لتشريعات مكافحة الجريمة المعلوماتية

إن المشرع الإماراتي وبموجب نص قانون اتحادي رقم /٥/ لسنة **٢٠١٤م** لم ينص على جريمة الإرهاب بالوسائل الإلكترونية كجريمة مستقلة، لكنه خطا خطوات إيجابية في مجال مكافحة الإرهاب بالوسائل الإلكترونية، من خلال:

- عاقب كل من إنشء أو أدار أو أشرف على موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية بقصد ...، المادة السادسة والعشرون من نص قانون اتحادي رقم /٥/ لسنة ٢٠١٤م.
- يعد ظرفاً مشدداً، استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة تقليدية، الفقرة /أ/ من المادة السادسة والأربعين من نص قانون اتحادي رقم /٥/ لسنة ٢٠١٤م.
- يعد ظرفاً مشدداً، ارتكاب أي جريمة معلوماتية نص عليها القانون الاتحادي /٥/ لعام ٢٠١٤م، لصالح جماعة إرهابية، الفقرة /ب/ من المادة السادسة والأربعين من نص قانون اتحادي رقم /٥/ لسنة ٢٠١٤م.

نجد في المقابل، وكما أسلفنا سابقاً أن المشرع السوري بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، لم ينص صراحةً على استخدام الشبكة المعلوماتية من قبل الإرهابيين، باستثناء المادتين /٢٨/ و /٢٩/ المرتبطتين بالإرهاب بالوسائل الإلكترونية وبشكل غير مباشر.

ب-بالنسبة لتشريعات مكافحة الإرهاب

أن المشرع الإماراتي والمشرع السوري اتبعا السياسة نفسها تقريباً في تعريفهما للعمل الإرهابي، من حيث عدم تحديد صورة الفعل الجرمي المكون لجريمة العمل الإرهابي، وإنما جاء النص عاماً فقد اكتفيا بتحديد العناصر المميزة له، ولم يحددا وسائل ارتكاب العمل الإرهابي، لكن المشرع الإماراتي على عكس المشرع السوري توسع في النتيجة الجرمية.

ثالثاً: الإرهاب بالوسائل الإلكترونية في القانون المغربي

إن دراسة الإرهاب المعلوماتي في القانون المغربي يقوم على نصين مهمين هما: القانون رقم ٠٣-٠٧ لعام ٢٠٠٣م الخاص بالجرائم المتعلقة بنظام المعالجة الآلية للمعطيات، والقانون رقم ٠٣-٠٣ لعام ٢٠٠٣م المتعلق بمكافحة الإرهاب.

وقبل صدور القانون ٠٣-٠٧ الخاص بالجرائم المتعلقة بنظام المعالجة الآلية للمعطيات، كان هناك جدل فقهي حول تكييف الأفعال التي تشكل جريمة معلوماتية، ولقد جاء القانون المذكور أعلاه ليضع حداً لكل هذه الجدالات.

١- القانون رقم ٠٣-٠٣ لعام ٢٠٠٣م المتعلق بمكافحة الإرهاب

وإذا نحن انتقلنا إلى القانون رقم ٠٣-٠٣ المتعلق بمكافحة الإرهاب، فإننا نجد أن فصله ١-٢١٨ قد نص على الآتي:

"**تعتبر الجرائم الأتية أفعالاً إرهابية إذا كانت لها علاقة عمداً بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف**".

ثم عمد المشرع المغربي إلى ذكر الأفعال التي تشكل أفعالاً إرهابية،[١] كان **سابعها** هو المتعلق **بنظام المعالجة الألية للمعطيات**، مع الإشارة إلى أن المشرع المغربي لم يعرفّ نظام المعالجة الآلية للمعطيات وأوكل مهمة تعريفه لكل من الفقه والقضاء.[٢]

إن إدراج الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات ضمن الأفعال التي تعد أفعالاً إرهابية، إذا كانت تهدف للمس الخطير بالنظام العام بواسطة

---

١ عدد المشرع المغربي الجرائم التي تعد أفعالاً إرهابية بموجب القانون ٠٣-٠٣ المتعلق بمكافحة الإرهاب، في الفصل ١-٢١٨ منه، وهي: ١- الاعتداء عمداً على حياة الأشخاص أو على سلامتهم أو على حرياتهم أو اختطافهم أو احتجازهم. ٢- تزييف أو تزوير النقود أو سندات القرض العام، أو تزييف أختام الدولة والدمغات والطوابع والعلامات، أو التزوير أو التزييف المنصوص عليه في الفصول ٣٦٠ و٣٦١ و٣٦٢ من هذا القانون.٣- التخريب أو التعييب أو الإتلاف. ٤- تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل أو إتلافها أو إتلاف منشآت الملاحة الجوية أو البحرية او البرية أو تعييب أو تخريب أو إتلاف وسائل الاتصال. ٥- السرقة وانتزاع الأموال. ٦- صنع أو حيازة أو نقل أو ترويج أو استعمال الأسلحة أو المتفجرات أو الذخيرة خلافاً لأحكام القانون. ٧- الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات. ٨- تزوير أو تزييف الشيكات أو وسيلة أداء أخرى المشار إليها على التوالي في المادتين ٣١٦ و ٣٣١ من مدونة التجارة. ٩- تكوين عصابة أو اتفاق لأجل إعداد أو ارتكاب فعل من أفعال الإرهاب. ١٠- إخفاء الأشياء المتحصل عليها من جريمة إرهابية مع علمه بذلك.

٢ د. سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، الملتقى العلمي، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من ٢-٢٠١٤/٩/٤م، عمان، المملكة الأردنية الهاشمية، ١٤٣٥هـ-٢٠١٤م، ص ٥.

التخويف أو الترهيب أو العنف يغطي جل إن لم يكن كل الأفعال التي تقترف في إطار ما يسمى بالإرهاب بالوسائل الإلكترونية.[١]

لكن الإشارة في الفقرة السابعة من الفصل ٢١٨-١ إلى الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات كنمط من أنماط الجرائم الإرهابية طرح في ذلك التساؤل حول الأساس القانوني للجرائم المتعلقة بنظام المعالجة الآلية للمعطيات، حيث أن القانون المغربي لم يكن يحتوي على تكييفات خاصة بهذا النوع من الجرائم، لذلك سارع المشرع المغربي إلى تبني قانون خاص بهذا النوع من الجرائم، هو القانون ٠٣-٠٧ المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات.

٢- القانون ٠٣-٠٧ المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات

إن الأفعال التي جرمها القانون ٠٣-٠٧، هي:

أ- **الفصل ٦٠٧-٣:** الدخول إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال، وكذلك من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق الدخول. وقد شدد المشرع المغربي العقوبة، إذا نتج عن الفعلين حذف أو تغيير في المعطيات التي يحتوي عليها النظام أو أحدث اضطراباً في سيره.

ب-**الفصل ٦٠٧-٤:** نفس الأفعال السابقة، إذا ارتكبت في حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات يفترض أنه يتضمن معلومات

---

١ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٧.

تخص الأمن الداخلي أو الخارجي للدولة أو أسرار تهم الاقتصاد الوطني، وشدد العقوبة إذا نتج عن هذه الأفعال حذف أو تغيير للمعطيات المحتواة في النظام أو إذا ارتكبت الأفعال من طرف موظف أو مستخدم أثناء مزاولة مهامه أو سهل للغير القيام بها.

ج- **الفصل ٦٠٧-٥:** الأفعال التي تعمد إلى عرقلة سير النظام المعالجة الآلية للمعطيات أو أحدث خلل فيها.

د- **الفصل ٦٠٧-٦:** خصص لمن أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها أو غير المعطيات المدرجة أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال.

ه- **الفصل ٦٠٧-٧:** يخص كل من زور أو زيف وثائق المعلومات أيا كان شكلها إذا كان من شأن التزوير إلحاق ضرر بالغير، وكذلك كل من استعمل هذه الوثائق المزورة مع علمه بتزييفها او تزويرها.

و- الفصل **٦٠٧-١٠:** عالج صنع تجهيزات أو أدوات أو إعداد برامج للمعلومات أو أية معطيات أعدت أو اعتمدت خصيصاً لأجل ارتكاب الجرائم المذكورة أعلاه أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير.

وإذا كان المشرع المغربي قد تصدى للجريمة الإلكترونية من خلال مجموعة من القوانين الخاصة فإنه لم يعمد إلى وضع إطار واضح أو تعريف محدد للجريمة المعلوماتية، وقد أحسن باتباع هذه السياسة التشريعية لأن ذلك يبقى من صنيعة الفقه والقضاء من جهة، وبغية عدم حصر القاعدة

التجريمية في إطار أفعال معينة تحسبا للتطور العلمي والتقني في المستقبل، من جهة ثانية.[١]

٣- ومما تجدر الإشارة إليه أيضاً أن القانون المغربي رقم ٠٣-٠٣ المتعلق بمكافحة الإرهاب في الفصل ٢-٢١٨ منه، عاقب على استعمال وسائل الإعلام ومنها الإلكترونية في الإشادة بالأعمال الإرهابية، لأن وسائل الإعلام الإلكترونية متعددة، من أبرزها الشبكة الدولية للمعلومات الإنترنت، والذي ينص على أنه "**يعاقب بالحبس من سنتين إلى ست سنوات وبغرامة تتراوح بين ١٠٠٠٠ و٢٠٠٠٠٠ درهم كل من أشاد بأفعال تكون جريمة إرهابية بواسطة الخطب أو الصياح أو التهديدات المفوه بها في الأماكن او الاجتماعات العمومية أو بواسطة المكتوبات أو المطبوعات المبيعة أو الموزعة أو المعروضة للبيع أو المعروضة في الأماكن أو الاجتماعات العمومية أو بواسطة الملصقات المعروضة على أنظار العموم بواسطة مختلف وسائل الإعلام السمعية والبصرية والإلكترونية**".

وهكذا بمفعول هذين القانونين يكون التشريع المغربي قد غطى ما يمكن تغطيته من الأفعال الواجب محاربتها في ميدان الإرهاب المعلوماتي.[٢]

٤- المقارنة مع التشريع السوري

لم ينص المشرع المغربي على الإرهاب بالوسائل الإلكترونية كجريمة مستقلة بذاتها، إلا أنه نص على إمكانية إرتكاب إعمال إرهابية بوسائل إلكترونية، وإمكانية وقوع إعمال إرهابية على البينة التحتية المعلوماتية،

---

١ د. سومية عكور، المرجع السابق، ص ٣.

٢ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٧.

فبموجب نص القانون ٠٣-٠٣ الخاص بمكافحة الإرهاب اعتبر أن الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات جرائم إرهابية إذا ارتكبت في إطار مشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو العنف.

وبالعودة إلى التشريع السوري، فإن قيام المشرع السوري بالنص بصورة مستقلة على أن الجرائم المعلوماتية جرائم إرهابية إذا إرتكبت في إطار عمل إرهابي يهدف إلى نشر الخوف أو الفزع أو الإضرار بالبنية التحتية أو الأساسية للدولة، يغنيه عن تطبيق نص المادتين /٢٨/ و/٢٩/ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بموجب المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، أو مد نطاق تعريف العمل الإرهابي ليشمل الإرهاب بالوسائل الإلكترونية بموجب المادة الأولى من قانون مكافحة الإرهاب رقم /١٩/ لعام ٢٠١٢م.

رابعاً: الإرهاب بالوسائل الإلكترونية في القانون الأردني

١- الإرهاب بالوسائل الإلكترونية بموجب نص قانون منع الإرهاب

قامت الحكومة الأردنية بتاريخ ٢٠٠٦/١١/١م بإصدار قانون منع الإرهاب، الذي شمل تعريف شمل في طياته، الإرهاب بالوسائل الإلكترونية،[١] حيث عَرّف هذا القانون العمل الإرهابي بأنه: "**كل عمل مقصود يُرتكب بأي وسيلة كانت يؤدي إلى قتل أي شخص أو التسبب بإيذائه جسدياً أو إيقاع أضرار في الممتلكات العامة أو الخاصة أو في وسائط النقل أو البيئة أو البنية التحتية أو في مرافق الهيئات الدولية أو البعثات الدبلوماسية، إذا**

١ د. رائد العدوان، المرجع السابق، ص ٢٣.

كانت الغاية منه الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر أو تعطيل تطبيق أحكام الدستور أو القوانين أو التأثير على سياسة الدولة او الحكومة أو إجبارها على عمل ما أو الامتناع عنه أو الإخلال بالأمن الوطني بواسطة التخويف أو الترهيب أو العنف".

فالمشرع الأردني بتعريفه للعمل الإرهابي، لم يحدد صورة الفعل الجرمي المكون لجريمة العمل الإرهابي، وإنما جاء النص عاماً فقد اكتفى بتحديد العناصر المميزة له، ولم يحدد وسائل ارتكاب العمل الإرهابي على سبيل الحصر، إنما استعمل مصلحاً مرناً واسع الدلالة بقوله "... بأي وسيلة كانت ..، لكنه في المقابل حدد النتيجة الجرمية المترتبة على العمل الإرهابي وتوسع بها، بالتالي يمكننا القول أن هذا التعريف يشمل بطياته الإرهاب بالوسائل الإلكترونية بشكل ضمني.

أي أن المشرع الأردني والمشرع السوري اتبعا السياسة نفسها في تعريفهما للعمل الإرهابي، لكن المشرع الأردني على عكس المشرع السوري توسع في النتيجة الجرمية.

٢- الإرهاب بالوسائل الإلكترونية بموجب نص قانون جرائم أنظمة المعلومات رقم /٣٠/ لسنة ٢٠١٠م

جَّرم المشرع الأردني الإرهاب بالوسائل الإلكترونية، حين أفرد نصاً خاصاً في قانون جرائم أنظمة المعلومات رقم /٣٠/ لسنة ٢٠١٠م للإرهاب بالوسائل الإلكترونية،[١] فقد نصت المادة **العاشرة** من هذا القانون على أنه: "**كل من استخدم نظام المعلومات أو الشبكة أو أنشأ موقعاً إلكترونياً لتسهيل**

---

١ د. أيسر محمد عطية، المرجع السابق، ص ٣٥.

القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لاتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة".

وبإمعان النظر فيما تضمنته هذه المادة نجد أنها حصرت مواجهة الإرهاب بالوسائل الإلكترونية بإنشاء مواقع تروج وتدعم الأعمال الإرهابية أو تستخدم وسيلة لتمويلها، وهذه لا تمثل سائر مفردات وصور أنشطة الإرهاب بالوسائل الإلكترونية.[١]

وبالتالي يجب على المشرع الأردني أن يتوسع في صور تجريم استخدام نظم المعلومات أو الشبكة أو المواقع الإلكترونية للقيام بأعمال إرهابية ليشمل جوانب الإرهاب بالوسائل الإلكترونية كلها.

وفي نهاية هذا الفرع لا بد أن نشير، إلى أن التشريعات العربية (محل الدراسة) لم تعالج الإرهاب بالوسائل الإلكترونية بصورة مستقلة بذاتها، فجميع هذه التشريعات قامت بالتوسع في تعريف العمل الإرهابي أو الجريمة الإرهابية في قوانينها الخاصة بمكافحة الإرهاب، والإشارة إلى جوانب أو صور من الإرهاب بالوسائل الإلكترونية بموجب قوانينها الخاصة بتنظيم البيئة الرقمية، باستثناء المشرع المغربي، فهو المشرع العربي الوحيد الذي نص بشكل صريح على أن الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات هي جرائم إرهابية إذا وقعت في إطار مشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو العنف.

---

١ د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، المرجع السابق، ص ١٩١.

وكذلك المشرع الإماراتي الذي لم يشر إلى الإرهاب بالوسائل الإلكتروني كجريمة مستقلة بذاتها، لكنه خطا خطوات إيجابية في مجال مكافحة الإرهاب بالوسائل الإلكترونية، فهو من جهة توسع في صور استخدام موقع إلكتروني أو نشر معلومات على الشبكة الجرمية لخدمة جماعات إرهابية، ومن جهة أخرى نص على ارتكاب جرائم معلوماتية لصالح جماعات إرهابية.

وندعو المشرع السوري إلى الاستفادة من التجارب التشريعية للدول العربية في مجال مكافحة الإرهاب بالوسائل الإلكترونية بشكل عام، لتجريم الإرهاب بالوسائل الإلكترونية بصوره وأشكاله كافة، في ضوء ما تتعرض له سورية من إرهاب خطير سواء بصورته التقليدية أو الإلكترونية.

وبعد أن انتهينا من دراسة دور المشرع في الدول العربية في مكافحة الإرهاب بالوسائل الإلكترونية، لا بد من إلقاء الضوء على الخطوات التي اتبعها المشرع في الدول الغربية وذلك في الفرع التالي.

الفرع الثاني

الإرهاب بالوسائل الإلكترونية في تشريعات الدول الأجنبية

سنعرض فيما يلي بإيجاز تجارب بعض الدول الغربية في مواجهة الإرهاب بالوسائل الإلكترونية من خلال قوانينها واستراتيجياتها الوطنية.

أولاً: الولايات المتحدة الأمريكية

قررت الإدارة الأمريكية في عهد الرئيس بيل كلينتون إجراء خطوات تنفيذية لمكافحة ظاهرة الإرهاب الإلكتروني،[١] حيث تميزت الاستراتيجية الأمريكية لمكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة، وانصبت هذه الاستراتيجية في بادئ الأمر على المجال العسكري، حيث عمد البنتاغون سنة ٢٠٠٥ إلى إنشاء وحدة عسكرية متخصصة، عُهد إليها بمهمة تحصين الفضاء المعلوماتي الأمريكي، وتأمين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة.[٢]

وتعد الولايات المتحدة الأمريكية من أولى الدول التي أصدرت قوانين لمكافحة الإرهاب الإلكتروني، ففي أكتوبر ٢٠٠١م، أصدرت اتفاقية لمكافحة الإرهاب المعلوماتي، والتي وسعت من خلالها سلطات البحث والتحقيق والمراقبة الإلكترونية،[٣] وتعمل الحكومة الفيدرالية الأمريكية جاهدةً على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث

---

١ د. رائد العدوان، المرجع السابق، ص ١١.

٢ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص ٢٢.

٣ محمد سيد سلطان، المرجع السابق، ص ١٩.

تحاول تقنين استخدام محرك البحث Google – msn – yahoo في مجموعة من الشركات.[١]

وهناك خطوات عديدة اتخذتها الولايات المتحدة لمكافحة الجريمة والإرهاب الإلكتروني منها:[٢]

١- إصدار قانون تعزيز أمن المعلومات ٢٠٠٢.

٢- وضع الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني ٢٠٠٣.

٣- أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الإلكتروني.

٤- كما تم إنشاء " لجنة حماية البنية التحتية الحساسة" في الولايات المتحدة، والتي أسست مجموعة خاصة تتناول جوانب الإرهاب الإلكتروني وأطلقت عليها اسم: "مركز حرب المعلومات".[٣]

٥- كما تم إنشاء "المركز القومي لحماية البنية التحتية" ومركز تحليل وتبادل المعلومات، وبرنامج " حراسة البنية التحتية" وغيرها من المبادرات.[٤]

وبالنتيجة، تعد الولايات المتحدة من الدول السباقّة في محاربة ظاهرة الإرهاب بالوسائل الإلكترونية، من خلال قوانينها الوطنية، أو من خلال سعيها لعقد اتفاقيات دولية بهذا الخصوص، أو من خلال إنشاء الأجهزة المختصة بمكافحة الإرهاب بالوسائل الإلكترونية.

---

١ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص ٢٢.

٢ محمد سيد سلطان، المرجع السابق، ص١٩-٢٠.

٣ د. رائد العدوان، المرجع السابق، ص١١.

٤ د. رائد العدوان، المرجع السابق، ص ١١.

ثانياً: بريطانيا

يعطي القانون البريطاني لمكافحة الإرهاب والمعروف ب terrorism act ٢٠٠٠ الذي دخل حيز التنفيذ في فبراير ٢٠٠١م، للإرهاب تعريفاً موسعاً، ليشمل أفعال القرصنة المعلوماتية التي من شأنها إزعاج أو خلق اضطراب داخل النظام الإلكتروني.[١]

وتضمن القانون terrorism act ٢٠٠٠ ثماني أقسام، وبهذا القانون وضعت قوانين مكافحة الإرهاب في مدونة واحدة،[٢] وقد طرأ عليه مجموعة من التعديلات منها:[٣] في سنة ٢٠٠٦م صدر تعديل لقانون مكافحة الإرهاب تضمنً أفعال جديدة عدّت تشجيعاً للإرهاب، حيث عدّ تشجيعاً للإرهاب نشر التصريحات التي يمكن أن تفهم من الجمهور بأنها تشجيع مباشر أو غير مباشر، أو تحريض على ارتكاب الإرهاب، أو التجنيد لأعمال إرهابية، كما تضمن هذا القانون جرائم التدريب على الإرهاب والتحضير له.

وقرر مجلس النواب البريطاني في أوائل نيسان ٢٠١٢م طرح ومناقشة قانون يسمح بموجبه لأحد وكالات المخابرات البريطانية بمراقبة كل الاتصالات الهاتفية والرسائل الإلكترونية والنصية والأنشطة التي تمارس

---

١ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ٢١.

٢ د. أحمد فتحي سرور، حكم القانون في مواجهة الإرهاب، القاهرة، ٢٠٠٧م، بحث منشور على الإنترنت، متاح على الرابط: hccourt.gov.eg/pages/elmglacut/mkat/١٢/Makala-html. ، تاريخ الزيارة: ٢٠١٤/١١/٩م.

٣ د. أحمد فتحي سرور، حكم القانون في مواجهة الإرهاب، المرجع السابق.

على شبكة الإنترنت لمعالجة ظاهرة الإرهاب الإلكتروني، مما أثار جدلاً واسعاً حول انتهاك الحرية الشخصية سواء في بريطانيا أو في العالم.[١]

ثالثاً: فرنسا

أصدرت الحكومة الفرنسية قانوناً لمكافحة الإرهاب عام ٢٠٠٦م يسمح، بمراقبة الهواتف والإنترنت، وزرع كاميرات مراقبة في الأماكن العامة، وملاحقة أي فرنسي يسافر للتدرب على أعمال إرهابية خارج البلاد حتى ولو لم يرتكب أي عمل مسيء في فرنسا، وحتى لو لم يمضِ شبابه على الأراضي الفرنسية، وذلك بتهمة تشكيل عصابة إجرامية تهدف لارتكاب عمل إرهابي، وهي جريمة يعاقب عليها بالسجن عشر سنوات والغرامة ٢٢٥ ألف أورو.[٢]

وشهد القانون الفرنسي تعديلاً في نوفمبر ٢٠١٤م، قبل الهجوم على صحيفة شارلي إيبدو الساخرة، وقد نص التعديل على منع الفرنسيين من السفر للانضمام للجماعات الجهادية في سورية بعد انضمام مئات الفرنسيين لتنظيم "داعش"، ومصادرة جواز سفر وبطاقة هوية كل من أمضى بين ستة أشهر وعامين بها، ومنع المشتبه بانضمامهم لتنظيم "داعش" من دخول فرنسا،

---

١ د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، أراء حول الخليج، متاح على الرابط: araa.ea/index.pbp?optton=com-content&view=article&i٨=٢٤٤:٢٠١٤-٠٦-١٣-١٦، تاريخ النشر: ٣١-١٢١، تاريخ الزيارة: ٢٠١٥/٧/٢٨م.

٢ أماني عزام، تعرف على أشهر الدول التي تطبق "قوانين مكافحة الإرهاب"، الوطن، بوابة إلكترونية شاملة، متاح على الرابط: www.elwatannews.com.com/news/details/٧٦٢٧٥٣/، تاريخ النشر: ٢٠١٥/٧/٣م، تاريخ الزيارة: ٢٠١٥/٧/٩م.

ومراقبة السلطات للمواقع الإلكترونية التي تدعو للتطرف، ومطالبة مديرها بمسح المحتويات المتشددة وحظر المواقع التي تدافع عن الإرهاب.[١]

وبعد تسع سنوات من العمل بالقانون القديم، خرج إلى النور في أذار الماضي قانون جديد باسم "تعزيز مكافحة الإرهاب"، طرحته الحكومة الفرنسية ووافق عليه البرلمان، وينص القانون على جواز اختراق من وصفهم ب"الإرهابيين المحتملين" ومراقبتهم من خلال أذونات إدارية دون الحاجة إلى موافقة قضائية،" اللجوء إلى أجهزة لتسجيل كلام الأشخاص وصورهم، أو لبرامج معلوماتية تلتقط البيانات المعلوماتية"، ما سيسمح لعناصر الاستخبارات بوضع ميكروفونات وكاميرات تجسس وغيرها أينما يرون ذلك ضرورياً، بما في ذلك إقامة مراكز تتبع هواتف المشتركين التي تسمح باعتراض الاتصالات في مربع معين، سواء من اتصالات مشتبه بهم أو المقربين منهم والتنصت عليهم، ويلزم القانون مشغلو خطوط الهواتف ومزودو الإنترنت بتسليم السلطات كل ما يمكن أن يجمعوه من بيانات.[٢]

وجرى في ٢٣ نيسان ٢٠١٥م اتفاق بين الحكومة الفرنسية وكبار مشغلي الإنترنت لمكافحة الإرهاب الإلكتروني والتصدي للمواقع الجهادية، ويهدف الاتفاق إلى التصدي لمحاولات نشر التطرف والتعصب على الإنترنت، ووضع آلية سريعة لسحب المضامين ذات الطابع الإرهابي، فضلاً عن

---

١ أحمد إمام، قانون "مكافحة الإرهاب" في فرنسا..١٤ تعدلاً خلال ٩ سنوات، تاريخ النشر: ٢٠١٣/٧/٩م، الوطن بوابة إلكترونية شاملة، متاح على الرابط: www.almustagbal.com/news/detailes/٧٦٦٧٤٥، تاريخ النشر: ٢٠١٣/٧/٩م، تاريخ الزيارة: ٢٠١٤/١/١م.

٢ أحمد إمام، قانون "مكافحة الإرهاب" في فرنسا..١٤ تعدلاً خلال ٩ سنوات، .المرجع السابق.

تشكيل مجموعة عمل مشتركة بين وزارة الداخلية الفرنسية ومشغلي الإنترنت.[١]

وانضم إلى الاتفاق كل من شركات غوغل وفيس بوك وميكروسوفت وآبل وتويتر، إضافة إلى الجمعية الفرنسية للشركات المزودة لخدمة الإنترنت لهذا الاتفاق.[٢]

وقد حجبت وزارة الداخلية الفرنسية خمسة مواقع تمجد الإرهاب عبر الإنترنت، في سابقة منذ تبني قانون "تعزيز مكافحة الإرهاب"، وصدر أمر الحجب عن مكتب الجريمة المرتبطة بتكنولوجيا المعلومات والاتصال.[٣]

وأخيراً، بعد استعراض العديد من التشريعات الوطنية للدول، نجد أن الدول العربية والأجنبية في سباق تشريعي جميعها، لسن تشريعات لمواجهة الإرهاب بصوره وأشكاله كلها ولا سيما الإرهاب بالوسائل الإلكترونية، وإنشاء الأجهزة المختصة لذلك، نتيجة تفشي ظاهرة الإرهاب في الآونة الأخيرة في دول العالم جميعها وخاصة في البيئة الإلكترونية، مما يدل على الخطر الكبير والمتنامي لهذه الظاهرة الإجرامية المستحدثة.

وبعد أن انتهينا من دراسة الإرهاب بالوسائل الإلكترونية في التشريعات الوطنية لبعض الدول العربية والأجنبية، لابد من إلقاء الضوء على الآليات الدولية لمكافحة الإرهاب بالوسائل الإلكترونية وذلك في المطلب التالي.

---

١ فرنسا تشدد الرقابة على الإنترنت بحجة: مكافحة الإرهاب، رصد-وكالات، تاريخ النشر: ٢٣ نيسان ٢٠١٥م، القاهرة، متاح على الرابط rassd.com/١٣٩٤٢٦.htm، تاريخ الزيارة: ٢١٥/٥/٤م.

٢ فرنسا توقع اتفاقية لمحاربة الإرهاب الإلكتروني، المستقبل، موقع اخباري، تاريخ النشر: ٢٠١٥/٤/٢٣م، متاح على الرابط: www.almustagbal.com، تاريخ الزيارة: ٢٠١٥/٥/٦م.

٣ فرنسا تحجب المواقع الإرهابية، تاريخ النشر: ١٧ مارس ٢٠١٥م، موقع السكينة، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٤/١م.

المطلب الثاني

الآليات الدولية لمكافحة الإرهاب بالوسائل الإلكترونية

من الضروري تكثيف الجهود الدولية بهدف تحصين الفضاء الإلكتروني، وتتعدد آليات وطرق مكافحة الجريمة والإرهاب الإلكتروني على المستوى الدولي، لذلك لابد لنا من تقسيم هذا المطلب إلى فرعين:

الفرع الأول: الاتفاقيات الدولية

الفرع الثاني: التعاون الدولي في مجال مكافحة الإرهاب بالوسائل الإلكترونية

الفرع الأول

الاتفاقيات الدولية

وضع المجتمع الدولي ثلاث عشر صكاً قانونياً وثلاثة بروتوكولات لمكافحة الأعمال الإرهابية، وتلك الصكوك أُعدّت تحت إشراف الأمم المتحدة ووكالاتها المختصة، وباب الاشتراك فيها مفتوح للدول الأعضاء جميعها.[١]

كما عملت الأمم المتحدة على وضع استراتيجية لمواجهة الإرهاب بمقتضى القرار الذي اتخذته جمعيتها العمومية في ٨ سبتمبر ٢٠٠٦م وملحق هذا القرار الذي يتضمن خطة العمل، وتمثل هذه الاستراتيجية الإطار العالمي الأول لمواجهة الإرهاب.[٢]

---

١ الأمم المتحدة في مواجهة الإرهاب، الصكوك الدولية لمكافحة الإرهاب، الموقع الرسمي للأمم المتحدة، متاح على الرابط: www.un.org/ar/terrorism/instuments.shtml، تاريخ الزيارة: ٢٠١٣/٩/١١م.

٢ د. محمد فتحي سرور، جريدة الأهرام، قضايا وآراء، الخميس ٢٧ شوال ١٤٢٧هـ، ٨ نوفمبر ٢٠٠٧م، العدد ٤٤١٦٦.

واكتفت هذه الاتفاقيات والبروتوكولات جميعها بذكر الأفعال التي طالبت الدول بتجريمها لأنها تمثل أعمالاً إرهابية تهدد الأمن والسلم الدوليين، وتثير الفزع والرعب في شعوب العالم، وتوسعت هذه الاتفاقيات في ذكر الوسائل التي ترتكب بها هذه الأعمال فبعد ذكر عدة وسائل، تذكر عبارة (بأي صورة) أو (بأي وسيلة).[١]

علاوة على ما تقدم، أصدرت الأمم المتحدة عبر جمعيتها العامة العديد من القرارات التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداماً غير سلمي، ومن هذه القرارات قرار الجمعية العامة في الدورة ٥٥/٢٨ في ديسمبر ٢٠٠٠م والدورة ٥٦/١٩ في ١٩ ديسمبر ٢٠٠١م بشأن إرساء الأساس القانوني لمكافحة إساءة استعمال التكنولوجيا الاتصال والمعلومات في أعمال إجرامية.[٢]

وفي المقابل ليس هناك حتى الآن مفهوم دولي موحد حول الإرهاب بالوسائل الإلكترونية، فالقانون الدولي لم يعطي تعريفاً واضحاً ومنهجاً معيناً للتعامل مع هذه الصورة الجديدة من الإرهاب،[٣] حتى أن الأمم المتحدة لم تعالج إلى الوقت الراهن حالة يمكن الاستناد إليها في تعريف الإرهاب بالوسائل الإلكترونية، والتعامل معه من الناحية القانونية والتجريمية،[٤] وتعد

---

[١] د. محمد فتحي عيد، تقويم قواعد مكافحة الإرهاب الواردة في الاتفاقيات الدولية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، المجلد ٢٩، العدد ٥٧، رجب ١٤٣٤هـ-مايو/يونيو ٢٠١٣م، ص ٣٦.

[٢] د. رائد العدوان، المرجع السابق، ص١٠

٣ د. أيسر محمد عطية، المرجع السابق، ص ٣٧.

٤ علي مطر، الإرهاب الإلكتروني في القانون الدولي: نوع جديد لم يتم التعامل معه بعد، موقع الأنباء الاخباري، تاريخ النشر: ٢٠١٣/٢/٢٥م، متاح على الرابط:/الإرهاب-الإلكتروني-في-القانون-الدولي www.inbaa.com/، تاريخ الزيارة: ٢٠١٤/٣/١م.

الاتفاقيات الدولية حول الجريمة المعلوماتية بمثابة المصدر القانوني الدولي الأول للاتفاقيات الدولية والإقليمية كلها، والتشريعات الوطنية التي لها علاقة بموضوع الإرهاب بالوسائل الإلكترونية.[١]

صحيح أن الاتفاقيات المذكورة تعالج الجوانب المتعلقة بالجريمة الإلكترونية، إلا أن ارتباط الإرهاب بالوسائل الإلكترونية بهذا النوع من الإجرام سيجعل من بنود الاتفاقية ملهمة وموجهة لكل المصادر القانونية التي ستحاول الحد من استعمال المعلومات لأهداف إرهابية.[٢]

وبالتالي سنقوم بدراسة هذه الاتفاقيات، أولاً: المستوى العربي، ثانياً: على المستوى الدولي.

أولاً: على المستوى العربي

لا يوجد على مستوى الدول العربية، اتفاقية خاصة تعالج الإرهاب بالوسائل الإلكترونية، لكن يوجد عدد من الاتفاقيات الخاصة بمكافحة الإرهاب وتنظيم البيئة الإلكترونية، لأن تشريعات مكافحة الإرهاب بالوسائل الإلكترونية بصورة عامة ترتبط بكل من تشريعات مكافحة الإرهاب من جهة، وتشريعات مكافحة الجريمة الإلكترونية من جهة أخرى.

وسنعالج على المستوى العربي كل من الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة في ٢٢ نيسان لعام ١٩٩٨م كونها عرفت كل من الإرهاب والجريمة الإرهابية، وقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣م، والاتفاقية

---

١ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٩.

٢ عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٩.

العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة أيضاً بتاريخ ٢٠١٠/١٢/٢١م والتي تناولت تنظيم البيئة الإلكترونية العربية، وأخيراً وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليج العربية لعام ٢٠١٣م.

١- الاتفاقية العربية لمكافحة الإرهاب لعام ١٩٩٨م

لم تتطرق هذه الاتفاقية للإرهاب بالوسائل الإلكترونية، ولعل أبرز المقتضيات التي حفلت بها هذه الاتفاقية، هو التعريف الموحد الذي أعطته للإرهاب والجريمة الإرهابية، ونصها الصريح على ضرورة تعهد الدول بعدم تنظيم أو تمويل أو ارتكاب الأعمال الإرهابية، أو الإشتراك فيها بأي صورة من الصور، بالإضافة إلى مطالبتها بضرورة تفعيل التعاون الأمني والقضائي بين البلدان العربية المختلفة، لاسيما في مجال تبادل المعلومات حول النشاطات الإرهابية، والهياكل التنظيمية للخلايا المتطرفة وأساليبها الإجرامية واتصالاتها المحتملة فوق أراضي باقي الدول الأعضاء.[١]

وتتكون الاتفاقية العربية لمكافحة الإرهاب من **اثنتين وأربعين** مادة موزعة على أربعة أبواب:[٢]

---

١ عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، المرجع السابق، ص ٦.

٢ د. على بن فايز الجحني، أضواء على الاتفاقية العربية لمكافحة الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤١٩هـ -١٩٩٩م، ص٢٧٤.

أ- **الباب الأول**

يشتمل على تعريف وأحكام عامة، حيث يركز على تعريف الإرهاب وتعريف الجريمة الإرهابية، ويفصل بين الإرهاب وحالات الكفاح المسلح ضد الاحتلال الأجنبي وفق المواثيق الدولية.

ب-**الباب الثاني**

يشتمل على أسس التعاون العربي لمكافحة الإرهاب، ويتكون من فصلين.

ج_ الباب الثالث

يشمل آليات تنفيذ القانون من حيث إجراءات تسليم المجرمين، وإجراءات الإنابة القضائية، وحماية الشهود، ويتكون هذا الباب من ثلاث فصول.

د_ الباب الرابع

يتعلق بالأحكام الختامية من حيث التصديق وسريان الاتفاقية، وعدم جواز مخالفة الاتفاقية، والانسحاب وأصوله.

وعرفت الاتفاقية الإرهاب في المادة الأولى منها بأنه: "**كل فعل من أفعال العنف أو التهديد به أياً كانت بواعثه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، يهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر**".

نلاحظ من التعريف السابق، أن الاتفاقية قد توسعت في تعريف الإرهاب، والقيد الوحيد الذي وضعته الاتفاقية هو أن تكون الأفعال وليدة مشروع

إجرامي،[١] ونلاحظ أيضاً، أن الاتفاقية لم تتطرق للوسائل التي يمكن أن يستخدمها الإرهابيين في ارتكاب أعمالهم الإرهابية.

كما عرفت هذه الاتفاقية الجريمة الإرهابية في المادة نفسها بأنها: "**هي أي جريمة أو شروع فيها ترتكب تنفيذاً لغرض إرهابي في أي من الدول المتعاقدة، أو على رعاياها أو ممتلكاتها أو مصالحها يعاقب عليها قانونها الداخلي**".

٢- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣م.

اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم ٤٩٥-د١٩-٢٠٠٣/١٠/٨م، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم ٤١٧-د٢١/٢٠٠٤م، وصدر هذا القانون في ضوء تعميمه على وزارات الداخلية العربية في الدول العربية للاستفادة منه في تنظيم البيئة الإلكترونية، ووضع ملاحظاتها بهذا الشأن.

ويتألف القانون من سبعة وعشرين مادة، تعالج تنظيم البيئة الإلكترونية، ولم يتطرق القانون الاسترشادي للإرهاب بالوسائل الإلكترونية بشكل صريح، ولكنه أشار إليه بصورة ضمنية في نص المادة الواحدة والعشرين من القانون المذكور، والتي تنص على أنه:

"**كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية**

---

١ د. محمد فتحي عيد، تقويم قواعد مكافحة الإرهاب الواردة في الاتفاقيات الدولية، المرجع السابق، ص ٤٩-٥٠.

لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن ...."

وبإمعان النظر في المادة السابقة، نستنتج أنها حصرت الإرهاب بالوسائل الإلكترونية في إنشاء موقع إلكتروني على الشبكة المعلوماتية لجماعة إرهابية، لتسهيل الاتصالات بقياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، وهذه الصور لاستخدام الموقع الإلكتروني لا تشمل كل جوانب الإرهاب بالوسائل الإلكترونية.

٣- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١م

تتألف هذه الاتفاقية من **ثلاثة وأربعين** مادة تقع في خمس فصول، **الفصل الأول:** الأحكام العامة، **الفصل الثاني:** التجريم، **الفصل الثالث:** الأحكام الإجرائية، **الفصل الرابع:** التعاون القانوني والقضائي، **الفصل الخامس:** أحكام ختامية.

وتهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.[١]

والأفعال التي جرمتها هذه الاتفاقية والخاصة بالبيئة الإلكترونية، بموجب الفصل الثاني منها، هي:

---

١ المادة /١/ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أ- جريمة الدخول غير مشروع.

ب-جريمة الاعتراض غير المشروع.

ج-الاعتداء على سلامة البيانات.

د-جريمة إساءة استخدام وسائل تقنية المعلومات.

هـ- جريمة التزوير.

و- جريمة الاحتيال.

ح-جريمة الإباحية.

ط- الجرائم الأخرى المرتبطة بالإباحية.

ك-جريمة الاعتداء على الحياة الخاصة.

ل- الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات.

م- الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات.

ن- الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.

ش-الاستخدام غير المشروع لأدوات الدفع الإلكترونية.

لم تشر هذه الاتفاقية إلى الإرهاب بالوسائل الإلكترونية بشكل صريح وواضح، لكنها تناولت الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، فقد جاء في الفصل الثاني في المادة **الخامسة عشرة** منه تحت عنوان الجرائم المتعلقة **بالإرهاب والمرتكبة بواسطة تقنية المعلومات،** الآتي:

١-نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

٢-تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

٣-نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

٤- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

نلاحظ من المادة الخامسة عشرة السابقة، أنها توسعت في صور استخدام تقنية المعلومات في جرائم الإرهابية، وأشارت بشكل صريح إلى استخدام تقنية المعلومات في تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، لكن تمثل هذه الصور الجرمية حول (الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات)، مفردات من الإرهاب بالوسائل الإلكترونية، ولا تغطي جوانب الإرهاب بالوسائل الإلكترونية كلها، فالصور الأساسية للإرهاب بالوسائل الإلكترونية والمتمثلة بالتدمير والسيطرة على البنية التحتية المعلوماتية لم تلحظ في هذه الاتفاقية.

كما نصت المادة **الواحدة والعشرون** تحت عنوان تشديد الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات على أنه: "**تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات**".

ومما يؤخذ على هذه الاتفاقية استخدامها مصطلحات فضفاضة وغير محددة، وتحتمل التأويل، سواء فيما يتعلق بالتجريم أو بجمع البيانات والمعلومات عن المستخدمين أو حتى في المبادئ العامة التي استندت إليها، لكن يمكن الاستفادة من هذه الاتفاقية، في إطار أن جرائم الإرهاب بالوسائل الإلكترونية مفهوم يشتمل على الجريمة الإلكترونية.

وقد وقعت الجمهورية العربية السورية على كل من الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة في ٢٢ نيسان لعام ١٩٩٨م، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة أيضاً بتاريخ ٢٠١٠/١٢/٢١م، في إطار تعزيز التعاون العربي وتبني سياسة جنائية مشتركة تهدف على خلق مظلة عربية واحدة لمكافحة كل من الإرهاب والجرائم الإلكترونية.

٤_ وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليج العربية لعام ٢٠١٣م

يأتي هذا النظام (القانون) استكمالاً لسلسلة الأنظمة (القوانين) الاسترشادية التي تم إنجازها في إطار مسيرة التعاون العدلي والقضائي بين دول مجلس التعاون الخليجي، كنظام استرشادي لمدة أربع سنوات يتجدد تلقائياً حال عدم ورود ملاحظات عليه من الدول الأعضاء، ويتكون هذا النظام (القانون) من تسعة وثلاثين مادة اشتملت على صور جرائم تقنية المعلومات وعقوبات مرتكبيها.

وقد أشار النظام (القانون) إلى الإرهاب بالوسائل الإلكترونية بصورة ضمنية في نص المادة **التاسعة والعشرين** من القانون المذكور، والتي تنص على أنه:

"**كل من أنشأ موقعاً أو نشر على الشبكة المعلوماتية أو أحد وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع**

الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالسجن مدة لا تقل عن (....) والغرامة التي لا تقل عن (....)".

وبإمعان النظر في المادة السابقة، نستنتج أنها مشابهة لنص المادة الواحدة والعشرين من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣م، والتي حصرت أيضاً الإرهاب بالوسائل الإلكترونية في إنشاء موقع إلكتروني على الشبكة المعلوماتية لجماعة إرهابية، لتسهيل الاتصالات بقياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية.

في النهاية، لا بد لنا من دعوة الدول العربية لوضع اتفاقية عربية واستراتيجية شاملة لمكافحة الإرهاب بالوسائل الإلكترونية، على غرار الاتفاقيات السابقة، تحدد صور النشاط المجرم، وأوجه التعاون الأمني والقضائي والمعلوماتي العربي، وإنشاء الأجهزة المختصة، لحماية البيئة الإلكترونية العربية من مخاطر الإرهاب بالوسائل الإلكترونية.

ثانياً: على المستوى الدولي

يوجد بعض الاتفاقيات الدولية المتعلقة بجرائم الحاسب الآلي بشكل عام، من بينها اتفاقية فينا عام ١٩٨٨م والتي حثت دول العالم الدخول في اتفاقيات ثنائية ضد الإرهاب الإلكتروني،[١] ومعاهدة حماية الأفراد المتعلقة بالمعالجة

[١] د. رائد العدوان، المرجع السابق، ص٩.

الآلية للبيانات الشخصية المنعقدة في ستراسبورغ لعام ١٩٨١م وتعديلاتها لعام ١٩٩٩م وبروتوكولها الإضافي لعام ٢٠٠١م.[١]

كما عملت دول المجلس الأوربي على التصدي لمكافحة الإرهاب الإلكتروني والجريمة المعلوماتية، فوقّع وزراء خارجية دول أعضاء مجلس أوربا،[٢] في ٥ نوفمبر ٢٠٠١م، على الاتفاقية الدولية للجريمة المعلوماتية، والتي تعد أول معاهدة دولية لمكافحة الجريمة الإلكترونية، وهي نتيجة لعمل استمر أربع سنوات وشارك فيها خبراء ٤٥ دولة عضو، وأيضاً من الدول غير الأعضاء.[٣]

وتسمى هذه الاتفاقية باتفاقية، بودابست لعام ٢٠٠١م، وبروتوكولها لعام ٢٠٠٣م أبرز اتفاقية تختص بالجرائم الإلكترونية ودخلت حيز التنفيذ عام ٢٠٠٤م، ووقعت عليها فضلاً عن الدول الأوربية كندا واليابان وجنوب إفريقية والولايات المتحدة الأمريكية.

وأكدت الاتفاقية ضرورة التزام الدول الأعضاء بتسليم المجرمين والمساعدة المتبادلة في التحقيق وجمع الأدلة واتخاذ التدابير التشريعية التي تمكنها من الوفاء بالالتزامات.[٤]

وتتكون هذه الاتفاقية من ثمان وأربعين مادة، وقد كان الهدف من هذه الاتفاقية وضع سياسة جنائية مشتركة بين دول المجلس تهدف إلى حماية

---

١ د. فراس طحان، مرجع سابق، ص ٣٧٩. عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، المرجع السابق، ص ١٩.

٢ تأسس مجلس أوروبا في العام ١٩٤٩م ويتكون من ٤٦ دولة، من دول الاتحاد الأوربي وعدد آخر من الدول خارج القارة، الولايات المتحدة وكندا واليابان وغيرها من دول أمريكا اللاتينية مراقبين. يقوم هذا المجلس بدور مهم في محاولة الحد من جرائم الحاسب الآلي.

٣ محمد سيد سلطان، المرجع السابق، ص ٢٢.

٤ د. فراس طحان، المرجع السابق، ص ٣٧٩.

ممتلكاته من الجريمة الإلكترونية من خلال اعتماد التشريعات الملائمة وتقرير التعاون الدولي.[١]

وتتألف الاتفاقية من مقدمة وأربع أقسام: القسم الأول فقد عرفت الاتفاقية بعض المفاهيم منها نظام الحاسوب وبيانات الحاسوب.

أما القسم الثاني فقد تضمن التدابير الواجب اتخاذها على الصعيد الوطني، وجاء في الباب الأول منه تحت عنوان القانون الجنائي الموضوعي، تعداد للجرائم المعلوماتية والتي تم تقسيمها إلى أربع مجموعات:

١- **المجموعة الأولى**

وتتضمن الجرائم التي تمس الخصوصية، وتجانس وتوافر بيانات الحاسوب ومنظوماته وهي الدخول غير المشروع، الاعتراض غير المشروع، التدخل في البيانات، التدخل غير المشروع في منظومة، إساءة استخدام الأجهزة.

٢- **المجموعة الثانية**

وتتضمن الجرائم المتعلقة بالحاسوب، وهي جريمة التزوير المتعلقة بالحاسوب، وجريمة النصب المتعلقة بالحاسوب.

٣- **المجموعة الثالثة**

وتتضمن الجرائم المتعلقة بالمحتوى، وقد تضمنت صورة جرمية واحدة هي الجرائم المتعلقة بالصور الفاضحة للأطفال.

---

١ د. حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية (تصور مفتوح)، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، ٢٠١١م/١٤٣٢هـ، المجلد ٢٧، العدد ٥٣، ص ٤١.

٤- المجموعة الرابعة

تضمنت الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المجاورة، أما القسم الثالث فقد تضمن التعاون الدولي.

وقد صدرت مسودة اتفاق عالمي حول الجريمة والإرهاب الإلكتروني من جامعة "ستاندفورد" وعرف بخطة ستاندفولرد في عام ٢٠٠٠م، وشملت تلك الخطة نقاط عدة حول هدف الوصول إلى تعاون دولي أوسع في مقاومة هجمات الفضاء الإلكتروني، وذلك لأن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين، وخاصةً مع التطور المستمر في التكنولوجيا، وجمود الأطر القانونية الحالية في مواجهة الأخطار والهجمات، واشتملت المادة الثانية عشرة من تلك الخطة اقتراح بإقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات.[١]

وتدرس كوريا الجنوبية بهدف إيجاد آلية عالمية لمكافحة الإرهاب الإلكتروني خطة لإنشاء منظمة دولية لمكافحة الإرهاب الإلكتروني تتخذ من سيؤول مقراً لها.[٢]

وبعد أن انتهينا من عرض الاتفاقيات الدولية ودورها في مكافحة الإرهاب بالوسائل الإلكترونية، لابد لنا من إلقاء الضوء على التعاون الدولي في مكافحة الإرهاب بالوسائل الإلكترونية وذلك في الفرع التالي.

---

١ د. رائد العدوان، المرجع السابق، ص١٠.

٢ د. فراس طحان، المرجع السابق، ص ٣٨٠.

الفرع الثاني

التعاون الدولي في مجال مكافحة الإرهاب بالوسائل الإلكترونية

بما إن جغرافية أفعال الإرهاب بالوسائل الإلكترونية هي عبارة عن فضاء غير محدد مادياً، ولأن الفعل يشكل جريمةً عابرة للحدود، فإن أي نشاط للحد من تداعيات الإرهاب بالوسائل الإلكترونية، يمر حتماً عبر آلية التعاون الدولي، فالتعاون بين الدول جميعها هو جزء أساسي من مواجهة الإرهاب بالوسائل الإلكترونية.[١]

فالتعاون الدولي هو اللبنة الأساسية لمواجهة الرهاب بالوسائل الإلكترونية الذي ينفّذ غالباً في دولة، وتحصل أثاره في دولة أخرى، فلا يمكن لأي دولة أن تحد من هذه الجريمة بجهودها المنفردة،[٢] كما لا يمكن للتشريعات الوطنية وحدها الوقوف أمام مجرم دون وطن، وفي وجه إجرام يتعدى حدود الدولة الوطنية، ومع الحاجة الماسة لهذا التعاون إلا أن عقبات عدة تقف في سبيله أبرزها:[٣]

١- عدم وجود اتفاقيات دولية تنظم هذا التعاون.

٢- عدم وجود مفهوم عام موحد للنشاط المجرم.

٣- عدم وجود معاهدات دولية تنظّم هذا التعاون.

٤- وتعقد مشكلات تفتيش نظام معلوماتي خارج حدود الدولة، وجمع الأدلة.

حتى أن الأمم المتحدة كما أسلفنا سابقاً، لم تعالج إلى الأن أية حالة يمكن الاستناد إليها في تعريف الإرهاب بالوسائل الإلكترونية وإمكانية التعامل من

---

١ محمد سعيد سلطان، المرجع السابق، ص ٢٣.

٢ د. فراس طحان، المرجع السابق، ص٣٨٠.

٣ د. عبد الرحمن بن عبد الله السند، المرجع سابق/ د. فراس طحان، المرجع سابق، ص ٣٨٠.

الناحية القانونية والجرمية، فالقانون الدولي لم يعطِ تعريفاً واضحاً ومنهجاً للتعامل مع هذا النوع الجديد من الإرهاب.[١]

وأخيراً تمثل عملية إدارة الإنترنت واحتكاره من جانب الولايات المتحدة إشكالية مهمة عند استخدام شبكة الإنترنت في بث الكراهية الدينية والإرهاب، ومن هنا تثور قضية عد الإنترنت مرفقاً عالمياً يحق للبشرية المشاركة في إدارته وبين رغبات الولايات المتحدة في الاحتفاظ به كجزء من الهيمنة على النظام الدولي.[٢]

من هنا يتوجب على الدول تكثيف آليات التعاون في مجال صد الإرهاب بالوسائل الإلكترونية، من خلال تخصيص الأطر القانونية للتدخل في إطار تعاون دولي إقليمي وثنائي الأطراف، فالتعاون الثنائي والمتعدد ثبت أنه أنجح وسيلة للرد على الإرهاب بالوسائل الإلكترونية، لسببين:[٣]

الأول: هو أن بعض الدول لم تشهد الإرهاب الإلكتروني حتى الآن، في حين أن بعض الدول شهدت هجمات إلكترونية عديدة.

والثاني: هو أن بعض الدول لديها قوانين وطنية تجّرم الجريمة والإرهاب الإلكتروني، في حين أن البعض الآخر لم يكن لديه أي نوع من أنواع القوانين التي تعاقب أو تجرّم هذه الجرائم، فقد يكون من أنسب أنواع التعاون بين الدول هو التعاون الثنائي أو المتعدد.

---

١ علي مطر، الإرهاب الإلكتروني في القانون الدولي: نوع جديد لميتم التعامل معه بعد، المرجع السابق.

٢ د. سعيد عطوة الزنط، المرجع السابق، ص٢٥.

٣ محمد سيد سلطان، المرجع السابق، ص ٢٢.

كما يجب العمل على خلق مؤسسات وأجهزة دولية مكلّفة بتتبع الإرهاب بالوسائل الإلكترونية، إضافة إلى إيجاد على مستوى كل دولة جهاز مكلف بتنسيق أنشطة التعاون الدولي.

فليس من المقبول اليوم الانكفاء داخل الحدود الوطنية في مكافحة الإرهاب بالوسائل الإلكترونية، فقد أعد المجتمع الدولي مجموعةً من الطرائق والآليات للتعاون الدولي في المسائل الجنائية، منها ما يتعلق بتسليم المجرمين، والمساعدة القانونية المتبادلة، ونقل الأشخاص المحكوم عليهم، والاعتراف بقرارات المحاكم الأجنبية، وتتعلق هذا الطرائق بأنواع الإجرام جميعها، من دولي وعابر للحدود الوطنية، بما في ذلك الإرهاب بالوسائل الإلكترونية.

ففي سياق التعاون الدولي في مكافحة الإرهاب بالوسائل الإلكترونية، يمكن أن تبرم معاهدات ثنائية وإقليمية، أو التصديق على اتفاقيات دولية خاصة بالإرهاب بالوسائل الإلكترونية في حال وجودها، أو مبدأ المعاملة بالمثل.

وبالتالي يجب العمل على وضع اتفاقية أممية شاملة لمكافحة الإرهاب بالوسائل الإلكترونية، وتتضمن هذه الاتفاقية تعريف موحد بالإرهاب بالوسائل الإلكترونية، وتحديد صور النشاط الجرمي، وآليات التعاون في المجال القضائي والأمني وتبادل المعلومات والخبرات، والتحقيق والتفتيش وجمع الأدلة، والملاحقة وتسليم الإرهابيين، وإنشاء مراكز لمراقبة الاتصالات وشبكة الإنترنت ومتابعة وملاحقة المجرمين.

وبعد أن انتهينا من دراسة مكافحة الإرهاب بالوسائل الإلكترونية تشريعياً، سننتقل إلى دراسة مكافحة الإرهاب بالوسائل الإلكترونية فنياً وذلك في المبحث التالي.

المبحث الثاني

مكافحة الإرهاب بالوسائل الإلكترونية فنياً

مع تعميم الرقمية، واعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات، وانخراط جميع القطاعات، العلمية، والاجتماعية، والأكاديمية، والاقتصادية والحكومية، في مجتمع المعلومات، إضافةً إلى توفر التكنولوجيا بسهولة، وانتشار البرامج والتطبيقات بشكل غير مسبوق، وبكلفة زهيدة، وبروز الوسائط المتعددة واستعمالها بشكل مكثف، نجد أنفسنا أمام حاجة ملحة إلى الأمن في الفضاء الإلكتروني.[١]

ويعد الأمن في الفضاء الإلكتروني، الهم الأول الذي تسعى إليه الحكومات، التي تهدف إلى الإفادة من إمكانات تكنولوجيا المعلومات والاتصالات في دعم التنمية والتطور والتجارة والاقتصاد،[٢] حيث أن الدول الأكثر اعتماداً على الإنترنت وعلى الشبكات المعلوماتية تعد الأكثر عرضة في المقابل للنتائج الكارثية لأي هجوم إرهابي إلكتروني،[٣] ولأن الأفضلية في مجال الإنترنت هي للمهاجم وليس للمتحصن، حيث يمثل عنصر المباغته الذي يتميز بها الإرهاب بالوسائل الإلكترونية وخاصة في بعده الرقمي تحدياً أمنياً ليضع الطرف الأخير في موقف ضعيف حيث يقتصر دوره في تلك الحالة على رد الفعل مع إصابة الإجراءات الوقائية في مقتل،[٤] لذلك تعمل الدول على

---

١ د. منى الأشقر جبور، د. عزيز ملحم بربر، أمن الشبكات والإنترنت، الحلقة العلمية الإنترنت والإرهاب، خلال الفترة: ١٧-١٤٢٩/١١/٢١هـ الموافق ١٥-٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، جامعة نايف العربية للعلوم الأمنية، القاهرة، مصر، ٢٠٠٨م، ص ١.

٢ د. منى الأشقر جبور، د. عزيز ملحم بربر، المرجع السابق، ص ١.

٣ الإرهاب الإلكتروني الثوابت والمتغيرات، المرجع السابق.

٤ د. سعد عطوة الزنط، المرجع السابق، ص٢٤.

تطوير قدراتها الرقمية، والتي تهدف إلى حفظ الأمن بمنع وقوع الجريمة، عن طريق التدابير الاحترازية الوقائية أو العلاجية لمكافحة الجريمة قبل وقوعها.

ويمكن القول أن هذا الأسلوب هو من أكثر وسائل المكافحة أهميةً، فهو السبيل لتفادي الخسائر المحتملة، وبالتالي إن استخدام مجموعة من الإجراءات الفنية التقنية الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الإرهاب بالوسائل الإلكترونية، فيجب على الدول انتهاج سياسة تقنية في أمن المنشآت الحيوية، وتدريب المسؤولين عن مكافحة الإرهاب على استيعاب السياسات الأمنية الإلكترونية، مع مكافحة المواقع التي تحض على الإرهاب أو التي توفر معلومات تساعد على القيام بإعمال إرهابية.[١]

لذلك سنقوم بتقسيم هذا البحث إلى مطالبين:

المطلب الأول: إجراءات الحماية الفنية الأساسية

المطلب الثاني: أنظمة الحماية الفنية من الاعتداءات الإلكترونية

---

١ الإرهاب الإلكتروني جولة في عقل متطرف، المرجع السابق.

المطلب الأول

إجراءات الحماية الفنية الأساسية

إن استخدام مجموعة من الإجراءات الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الإرهاب بالوسائل الإلكترونية والجريمة المعلوماتية،[١] وتوفير بيئة إلكترونية آمنة نسبياً، وتشمل هذه الإجراءات التي يجب مراعاتها: التدريب ونشر الوعي الإلكتروني، وتفعيل الرقابة الإلكترونية وأنظمة الحجب والترشيح.

وفي هذا المطلب لا بد لنا أن نتناول في الفرعين التاليين:

الفرع الأول: التدريب والتوعية.

الفرع الثاني: تفعيل المراقبة الإلكترونية وأنظمة الحجب.

الفرع الأول

التدريب والتوعية

تتطلب مكافحة الإرهاب بالوسائل الإلكترونية في الفضاء الإلكتروني، مواجهته من خلال تدريب المسؤولين عن مكافحة الإرهاب على استيعاب السياسات الأمنية الإلكترونية،[٢] والتركيز على دحض أفكار الإرهابيين وعزلهم عن المجتمع، مع بث أفكار مضادة لما يروجون له، من خلال إنشاء مواقع التوعية العديدة،[٣] وعدم ترك الساحة الإعلامية ساحة حرة لهم.[١]

---

[١] سعد السبيعي، الهجمات الإلكترونية..تأثيرها على الاقتصاد الوطني، موقع السكينة، تاريخ النشر: ١١ فبراير ٢٠١٤م، متاح على الرابط:
www.assakina.com/awareness_net/rebunds/٣٨٠٧٤.htmi، تاريخ الزيارة: ٢٠١٥/٩/١م.

[٢] هيام الدهبي، الإرهاب الإلكتروني والقوة في العلاقات الدولية، موقع الحياة، تاريخ النشر: ٢ أذار ٢٠١٤م، متاح على الرابط التالي:
www.alhayat.com/articles/٨٣١٥١٠/الإرهاب_الإلكتروني_والقوة_في_العلاقات_الدولية/، تاريخ الزيارة: ٢٠١٥/٦/٥م.

٣ الإرهاب الإلكتروني جولة في عقل متطرف، المرجع السابق.

في هذا الفرع لابد أن نتناول في الدراسة:

أولاً: التدريب.

ثانياً: إنشاء مواقع التوعية.

ثالثاً: تفعيل دور الإعلام.

أولاً: التدريب

إن التدريب ضروري لبناء الخبرات والمهارات، خاصةً في ظل التقدم المتواصل لتكنولوجيا الحاسب الآلي والإنترنت، الأمر الذي يفرض على جهات إنفاذ القوانين، وخاصة المسؤولة عن مكافحة الإرهاب، أن تسير في خطوات متناسقة مع هذا التطور، حتى يتم التصدي للجرائم الإلكترونية والإرهاب بالوسائل الإلكترونية.

فيجب أن يكون رجال القضاء والنيابة العامة على درجة كبيرة من الإلمام بالحوسبة الرقمية والكفاءة والمعرفة والقدرة على متابعة الجرائم الإلكترونية والإرهاب الإلكتروني، واستخلاص الأدلة منها، وهذا لا يتم إلا بالتدريب الذي يشمل جوانب الجرائم الإلكترونية كلها، من حيث كيفية إنشاء المواقع وإدارة الشبكات ونقاط الضعف وأماكن الاختراق لشبكات المعلومات وطرق الحصول على أدلة والتعاون الدولي في هذا المجال.[٢]

ثانياُ: إنشاء مواقع التوعية

تدير الجماعات الإرهابية مواقع إرهابية عديدة على شبكة الإنترنت، وتبث جميعها الأفكار الضالة والسامة، وتعمل جاهدةً على استقطاب أكبر عدد من

---

[١] د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف، المرجع السابق

٢ د. فراس طحان، المرجع السابق، ص٣٧٩.

الشباب، وبالتالي تجدر الإشارة إلى أهمية عدم ترك الساحة الإلكترونية لتلك الجهات، أي ضرورة إيجاد البديل القوي والمنافس على شبكة الإنترنت،[١] والبدء بإنشاء المواقع والمنديات التي تخدم المجتمع وتنير أفكار الشباب وتحارب الجماعات الإرهابية وتكشف كذب ما يروجون له من أفكار هدامة،[٢] هذا من جهة، وتعمل على تثقيف المستخدمين الذين يستخدمون شبكة الإنترنت من جهة أخرى لتجنب مخاطر الإرهاب بالوسائل الإلكترونية والوصول للاستخدام الأمثل للشبكة، أي نشر الوعي التكنولوجي بكيفية التعامل مع الإنترنت والحاسوب.[٣]

فعادة لا يهتم المستخدم بحيثيات الحماية مما يتسبب بنتائج غير مرغوبة، بل علاوةً على ذلك غالباً ما يعد المستخدمين إجراءات الحماية ضرباً من الإزعاج أكثر منه مساعدة ووقاية.[٤]

أي أنه كما يستطيع الإرهابيين استخدام شبكة الإنترنت بكفاءة، كذلك يستطيع صانعو السلام، استخدام الإنترنت لمجابهتهم، والمقصود هو نشر الأفكار السامية والمتحضرة التي تدعو إلى السلام والمحبة والتعايش السلمي،[٥] أي ما يسمى المواجهة اللينة مع الإرهاب عبر دحض أفكاره، وعزله عن

---

١ د. محمد بن حمود الهدلاء، كثرة مواقع الجماعات الإرهابية، نقلاً عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ٢٩ أكتوبر ٢٠١٢م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٣/٩/١.

٢ د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف وآليات مواجهته، موقع السكينة، تاريخ النشر: ٢٦ يونيو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة ٢٠١٥/٦/١م.

٣ أ.د. وليد أبو ريه، المرجع السابق، ص١٠.

٤ المهندس زكريا أحمد عامر، حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، دراسة لنيل درجة الماجستير في تقانة المعلومات، جامعة النيلين، كلية الدراسات العليا، الخرطوم، السودان، ١٤٣٢هـ/٢٠١١م، ص ٣٠.

٥ كثرة مواقع الجماعات الإرهابية، المرجع السابق.

المجتمع، مع بث أفكار مضادة لما يروج له الإرهابيين، وإتاحة الفرصة أمام حرية التعبير.[١]

ثالثاً: تفعيل دور الإعلام

يجب التـــأكيد على أهمية دور وسائل الإعلام الرسمي وغير الرسمي في بلورة استراتيجية للتصدي لمزاعم الإرهابيين وتشجيع وسائل الإعلام على وضع قواعد إرشادية للتقارير الإعلامية والصحفية مما يحول دون استفادة الإرهابيين منها.[٢]

حيث يعمل الإرهاب بالوسائل الإلكترونية على خدمة البعد الإعلامي للجماعات الإرهابية، من خلال استخدام شبكة الإنترنت كحاضن لنشاطها الإعلامي، فالجماعات الإرهابية لا يهمها عدد الضحايا الذين قتلوا بقدر ما يهمها كم من الناس شاهدوا وتفاعلوا مع الحادثة الإرهابية، كما يعمل أيضاً على تضخيم الصورة الذهنية لقوة وحجم الجماعات الإرهابية.[٣]

ويلعب الإعلام دور محورياً مهماً في مكافحة الإرهاب بالوسائل الإلكترونية،[٤] فلا يجب أن يقتصر دور الإعلام على الإعلام الموجه ضد الجماعات الإرهابية، إنما يجب أن يمتد ليشمل وضع ضوابط خاصة بالتغطية الإعلامية للجماعات الإرهابية، مثل عدم التوسع والمبالغة في نشر التهديدات الصادرة عن الجماعات الإرهابية من خلال شبكة الإنترنت، نظراً

---

١ الإرهاب الإلكتروني جولة في عقل متطرف، المرجع السابق.

٢ د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، أراء حول الخليج، متاح على الرابط: araa.sa/index.pbp?optton=com-content&view=article&i٨=٢٤٤:٢٠١٤-٠٦-١٣-١٦-٣١-١٢١، تاريخ الزيارة: ٢٠١٥/٧/٢٨

٣ د. سعد عطوة الزنط، المرجع السابق، ص ٢٢.

٤ د. أيسر محمد عطية، المرجع السابق، ص ٢٥.

لما يتركه ذلك من أثار سلبية في نفوس الجمهور، وأيضاً عدم تسليم وسائل الإعلام بكل ما ينشر من قبل الإرهابيين على المواقع الإلكترونية، وعدم عدّها من مصادر الإعلام الموثوقة.[١]

الفرع الثاني

تفعيل المراقبة الإلكترونية وأنظمة الحجب

يجب على الحكومات والدول أن تقوم بفرض الرقابة والسيطرة على كل ما يقدم من خلال شبكة الإنترنت، في إطار إيجاد بيئة إلكترونية خالية من الجريمة والإرهاب.

ولا بد أن نتناول في هذا الفرع دراسة:

أولاً: المراقبة الإلكترونية.

وانياً: أنظمة الحجب والترشيح.

أولاً: المراقبة الإلكترونية

ينبغي على الدول فرض رقابة على كل ما يقدم عبر شبكة الإنترنت، لمنع الدخول للمواقع التي يتضمن محتواها مواد تتعلق بالإرهاب، فضلاً عن مراقبة الاتصالات عبر شبكة الإنترنت والبريد الإلكتروني بهدف ضبط المجرمين وتفتيشهم، وجمع الأدلة لإدانتهم وتقديمهم للمحاكمة.[٢]

ويجب أن تكون هذه المراقبة مشروعة وتحقق التوازن بين حق الأفراد في الخصوصية وحق المجتمع في مكافحة الجريمة.

---

١ د. أيسر محمد عطية، المرجع السابق، ص ٢٣.

٢ د. فراس طحان، المرجع السابق، ص ٣٧٨.

لا تعني الرقابة المنع من استخدام شبكة الإنترنت، لكنها تدبير وقائي، لمنع وقوع الجرائم، فالرقابة على الإنترنت هي التحكم في النشر والوصول إلى المعلومات على الإنترنت، وتستخدم الرقابة تقنية تعتمد على الجدار الناري أو البروكسي، ويتم ذلك من خلال إجبار المتعاملين مع الشبكة على المرور عبر خوادم البروكسي قبل الوصول إلى الشبكة.[١]

فمزودات خدمة الإنترنت تتسلم وتنظم كل الطلبات، وتستخدم برامج تحسس الرقم الخاص ip ، مما يعطي بعض البيانات عن المستخدم حتى لو استخدم اسم وهمي لدخول الشبكة، ويوجد برامج عدة للمراقبة الإلكترونية وبرامج متخصصة بجمع الأدلة والقرائن من رسائل البريد الإلكتروني.[٢]

فعلى سبيل المثال، توظف الصين مليوني شخص لمراقبة الأنشطة على شبكة الإنترنت، حيث تعد شبكة الإنترنت في الصين من أكثر الشبكات التي تشهد سيطرة ورقابة حكومية صارمة في العالم، حيث تعد مواقع الإنترنت تحت الرقابة الجبرية الدائمة، بل وصل الأمر إلى حد التدخل لحذف التعليقات ذات الحساسية بصورة روتينية على مواقع الشبكات الاجتماعية.[٣]

---

١ الرقابة على الإنترنت، ويكيبيديا، الموسوعة الحرة، متاح على الرابط: الرقابة –على–الإنترنت /Ar.wikipedia.org/wiki، تاريخ الزيارة: ٢٠١٤/١٢/١٢م.

٢ د. فراس طحان، المرجع السابق، ص ٣٧٨.

٣ الصين توظف مليوني شخص لمراقبة الأنشطة على شبكة الإنترنت، الأمة صحيفة إلكترونية مستقلة، تاريخ النشر: ٧ أكتوبر ٢٠١٣، متاح على الرابط: html–الصين –توظف –مليوني–شخص –لمراقبة –الأنشطة –على –شبكة –الإنترنت –www.al–omah.com/mis/٦١٧٣، تاريخ الزيارة: ٢٠١٤/٨/١م.

ثانياً: أنظمة الحجب

من أهم ما يجب توافره في هذا الصدد حجب المواقع الضارة التي تدعو إلى الشر والفساد، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، والقيام بالإجراءات كلها بما في ذلك ترشيح المحتوى.[١]

ولقد جاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم.[٢]

١- حجج مؤيدي آلية الحجب

ويظن البعض أن آلية الحجب غير مجدية ولا تحقق الأهداف المرجوة منها ويحتجون بانتشار وسائل تخطي هذا النظام، والحقيقة أن هذا الاعتقاد لا يستند إلى حقائق ولا أدلة ملموسة بسبب:[٣]

أ- إن تطبيقات تجاوز الحجب ليست منتشرة بالشكل الذي يتخيله بعض المختصين.

ب-إنها حتى لو توافرت، فليس كل المستخدمين لديهم التأهيل للازم لاستخدامها، رغم عدم تعقيد هذا الإجراء، الذي يكفل لهم التعامل معه.

ج- إن كثيراً من المواقع التي توفر خدمة تجاوز الحجب، يتم حجبها خلال ساعات أو أيام مما يجعل البحث عن مواقع أخرى توفر هذه الخدمة (خدمة تجاوز الحجب) عملية مملة تدعو المتصفح للتوقف عنها.

---

١ د. عبد الرحمن بن عبد الله السند، المرجع السابق، ص ٢٣.

٢ د. عبد الرحمن بن عبد الله السند، المرجع السابق، ص ٢٤.

٣ د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف، المرجع السابق.

د- إن هناك أعداد ليست بالقليلة من متصفحي الإنترنت يلجونها من خلال أجهزة لا تخصهم (كأجهزة الحاسوب في العمل الموصولة على شبكة الإنترنت، مقاهي الإنترنت) وليس لديهم القدرة أساساً على تنصيب برامج غير مشروعة.

٢- موقف الدول الأنكلوسكسونية

وفي هذا السياق اختلفت كل من بريطانيا وأمريكا في تشرين الأول ٢٠١٠م، إذ كانت بريطانيا تحث أمريكا على التعامل بحزم أكثر مع المواقع الإرهابية **/حظر مواقع الإنترنت التي تخدم الإرهاب وتحرض عليه/**، رغم قضايا حرية التعبير، إلا أن إدارة الرئيس الأمريكي أوباما دافعت، حينها، عن نهجها لأنه يعبر عن التوازن المناسب بين المصالح المتنافسة، ومنها استخدام مثل هذه المواقع كمصدر للمخابرات وكنموذج لحرية استخدام الإنترنت الذي يمكن أن يقلل في نهاية المطاف من التطرف السياسي العنيف، ولكن الوقائع والمؤتمرات والتقارير اليوم، تثبت فشل الرؤية الأمريكية، كما تثبت زيادة التطرف والإرهاب.[١]

٣- الرأي الشخصي

ونحن مع القول الذي يدعو إلى تطوير أنظمة الحجب لتصبح أكثر فعالية في حجب مواقع الشبكات الاجتماعية /الفيس بوك مثلا/، بحيث يصبح قادراً على انتقاء صفحة أو رابط بعينه وحجبه.[٢]

---

١ تركي تركي، (الجهاد الإعلامي) وخلايا (القاعدة الإلكترونية) .. أزمة عالمية، موقع السكينة، تاريخ النشر: ١١ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٣/١م.

٢ د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف وآليات مواجهته، المرجع السابق.

٤-خطوات عملية جديرة بالاهتمام

وهناك نقطة أخرى لابد من الإشارة إليها وهي حذف المواد التي تبثها الجماعات الإرهابية من مواقع الشبكات الاجتماعية ومواقع مشاركة الملفات، وهذه الطريقة أصعب بكثير من سابقتها، بل باستحالتها تقريبا لأسباب كثيرة يأتي على رأسها إمكانية رفع أعداد هائلة من المواد التي يصعب تحديد مكنونها.[١]

كذلك من الاستراتيجيات الفعالة، التنسيق مع محركات البحث أمثال جوجل، ياهو، يوتيوب، ووينـدوز لايف، ومكتوب، والفيس بوك، وغيرها لمنع دخول الإرهابيين لهذه المواقع وعدم استخدام مواقعهم كوسيلة لنشر الفكر الإرهابي.[٢]

٥-موقف المشرع السوري

وقد أخذ المشرع السوري بآلية حجب المواقع الإلكترونية بالنسبة لمقدمي خدمة التواصل على الشبكة، عن طريق موقع إلكتروني أو أكثر، أو أي منظومة معلوماتية مشابهة، ونص على ذلك في المادة **السابعة** من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م التي جاء فيها:

"**لا يحجب الموقع الإلكتروني، أو أي منظومة مشابهة يستخدمها مقدم خدمة التواصل على الشبكة، حجباً كلياً أو جزئياً، دائماً أو مؤقتاً، إلا في الحالتين التاليتين:**

---

١ د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف وآليات مواجهته، المرجع السابق.

٢ د. يوسف بن أحمد الرميح، معركتنا ضد الإرهاب على الساحة الافتراضية الإلكترونية، المرجع السابق.

١-بأمر من السلطة القضائية.

٢-في حال إخلال مقدم خدمة التواصل على الشبكة بالتزاماته بوضع بيانات التعريف عن الموقع الإلكتروني الخاص به مخالفاً أحكام المادة /٥/ من هذا القانون، وذلك إلى حين إزالة المخالفة."

وجاء في التعليمات التنفيذية للهيئة /**الهيئة الوطنية لخدمات الشبكة في وزارة الاتصالات والتقانة المحدثة بموجب قانون التوقيع الإلكتروني وخدمات الشبكة ذي الرقم ٤ لعام ٢٠٠٩**/ تنفيذاً للبند الثاني من هذه الفقرة، تقوم من تلقاء نفسها أو بناء على شكوى تردها، بالطلب من مقدمي خدمة النفاذ إلى الشبكة حجب الموقع الإلكتروني الذي يخل بالتزاماته بوضع بيانات التعريف المشار إليها في المادة الخامسة من هذا القانون، وذلك إلى حين إزالة المخالفة.[١]

لكن **السؤال** الذي يثور هنا، ماهي الحالات التي تأمر بها السلطة القضائية بحجب الموقع الإلكتروني، حبذا لو أن المشرع السوري بين هذه الحالات ولم يترك النص على اطلاقه، دون تحديد.

ولقد أعطى المشرع السوري بموجب المادة **السادسة** من المرسوم التشريعي **رقم /١٧/ لعام ٢٠١٢م**، كل شخص سواء كان طبيعياً أو اعتبارياً، يرى نفسه متضرراً، إبلاغ مقدم خدمات التواصل على الشبكة أو المضيف، بالطابع غير المشروع للمحتوى الذي يضعه مقدم الخدمات المعني على

---

١ ت١ الفقرة ٢/م٧، التعليمات التنفيذية للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، القرار رقم /٢٩٠/ أيار ٢٠١٢م.

الشبكة أو المخزن لدى المضيف المعني، والمطالبة بحذفه أو تعديله أو تصحيحه أو منع الوصول إليه.

المطلب الثاني

أنظمة الحماية الفنية من الاعتداءات الإلكترونية

تتم الحماية الفنية من الاعتداءات الإلكترونية سواء كانت إرهابية أو غيرها، بوسائل فنية عدة منها:[١] – تشفير البيانات المهمة المنقولة عبر الإنترنت، سواء كانت منقولة عبر وسائل الاتصالات أو عبر الألياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة، لأن عملية التشفير مكلفة.

– إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

– توفير برامج الكشف عن الفيروسات لحماية الحاسب والبيانات والمعلومات من الإضرار بها.

– عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية.

– توزيع مهام العمل بين العاملين، فلا يُعطى مثلاً المبرمج وظيفة تشغيل الحاسب الآلي إضافة إلى عمله، كما يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين، مما يجعل كتابة برامج ضارة أمراً صعباً.

– عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة.

– استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد أو الصوت.

---

١ د. عبد الرحمن بن عبد الله السند، المرجع السابق، ص ٢٩.

– استخدام كلمة مرور، حيث تعد كلمة المرور من أبسط أشكال الحماية، ويفضل اختيار كلمة مرور ذات بنية قوية، ويجب مراعاة تغييرها الدوري.[١] وسنتحدث في هذا المطلب عن بعض هذه الوسائل بشيء من الإيجاز.

الفرع الأول

نظام التحقق من الهوية

يشير مفهوم التعرف بالهوية إلى التعرف الإيجابي الدقيق بهوية مستخدمي الشبكة ومضيفاتها، وتطبيقاتها، وخدماتها، ومصادرها.[٢]

يوجد تقنيات عدة للتحقق من الهوية وخصوصاً أساليب التحقق البيولوجي من الهوية، بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص، حيث تعتمد هذه الأنظمة على تسجيل معلومات عن بصمات الأصابع والوجوه، والأصوات، وقزحية وشبكية العين، التوقيع اليدوي، وغيرها.[٣]

يمكننا أن ننظر إلى هذه التقنية على أنها تعتمد على شيء لا يمكن نسيانه أو فقده أو تركه في مكان غير آمن، مثل البطاقات الممغنطة أو كلمات السر.

لكن تبقى كلمة السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعاً للتحقق من الهوية، وهنالك وسائل كثيرة يمكن استخدامها، وتعتمد هذه الوسائل

---

١ هيئة التحرير، عشر نصائح أساسية لحماية الشبكات، أمن المعلومات، هيئة التحرير، مجلة المعلوماتية، الجمعية العلمية السورية، عدد ١٢، شباط، ٢٠٠٧، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢٠١٤/٧/١م.

٢ المهندس زكريا أحمد عامر، حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، المرجع السابق، ص ٢٧.

٣ أ.د عبد الناصر الحمود، وسائل الإعلام المعاصرة والإرهاب المعلوماتي، المرجع السابق، ص٢٣.

أساساً على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم.[١]

الفرع الثاني

خدمات الأدلة

برمجيات خدمات الأدلة هي عبارة عن قواعد بيانات خاصة، ذات مستوى عالٍ من الأمان عادة، ومصممة لجمع وإدارة المعلومات المتعلقة بمستخدمي الشبكة، ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين.[٢]

ويتم استخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بمكوناتها جميعها كالتطبيقات، والأجهزة الخادمة، والمجلدات، وحتى شكل الشاشة التي يستعملها المستخدم، وتدار كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة أو المستخدمين.[٣]

الفرع الثالث

استخدام التشفير لحماية المعلومات الهامة

يُعَرِّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة، تبدو غير ذات معنى، لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة.[٤]

---

١ د. سعيد عطوة الزنط، المرجع السابق، ص٨.

٢ د. سعيد عطوة الزنط، المرجع السابق، ص٨.

٣ د. سعيد عطوة الزنط، المرجع السابق، ص٨.

٤ د. محمد بن عبد الله آل فايع العسيري، د. حسن بن أحمد الشهري، المرجع السابق، ص ٩.

فكل معلومة يمكن قراءتها دون استخدام أي أدوات إضافية، يطلق عليها اسم النص الصريح، والتعمية هي نص معمى يطلق عليه اسم Cipher Text وهذا النص المعمى عصي على القراءة لقوة التعمية وخوارزمياته المستخدمة.[١]

وتجري عملية التعمية بواسطة استخدام خوارزميات التعمية التي هي تابع رياضي يستخدم مفتاح معين ومن ثم الحصول على النص المعمى.[٢]

وتعتمد هذه التقنية على علاقة رياضية خاصة تجمع ما بين مفتاحين أو بالأحرى كلمتين سريتين أحدهما عام والأخر خاص، فعند إرسال رسالة يقوم التطبيق الموجود على جهاز المرسل بتشفيرها أو بعثرة بياناتها، باستخدام كلمة سر غير معروفة لأحد سوى المرسل، ثم تشفيرها ثانية بمفتاح العام للمستقبل.

والسبيل الوحيد الذي يمكن به للمستقبل أن يتعامل مع هذه الرسالة يتمثل في فك تشفيرها، أو إعادة ترتيب بياناتها، باستخدام مفتاحه الخاص أو كلمته السرية أولاً، ومن ثم استخدام المفتاح العام للمرسل لفك شيفرته الخاصة.[٣]

وللتعمية أنواع عدة، منها التعمية الإصلاحية، والتعمية باستخدام المفتاح العمومي، ولا بد من أن يكون برنامج التعمية واحد بين المرسل والمستقبل.[٤]

---

١ د. سامر الدقاق، التعمية وحماية المعلومات على شبكة الإنترنت، مجلة المعلوماتية، الجمعية العلمية السورية، العدد ٨٠، تشرين الأول ٢٠١٢م، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢٠١٣/٩/٧م.

٢ د. سامر الدقاق، المرجع السابق.

٣ د. سعيد عطوة الزنط، المرجع السابق، ص٨.

٤ د. سامر الدقاق، المرجع السابق.

وهناك العديد من برامج التشفير، منها المجاني، والتجاري، والشخصي، ومنها على مستوى الشركات والمنظمات.

والتشفير سلاح ذو حدين، حيث أنه يوفر الحماية للبيانات، لكن إذا فقد المفتاح السري أو البرنامج الذي شفر المحتوى، فلا فائدة ترجى من المحتوى المشفر.[١]

الفرع الرابع

الجدار الناري

الجدار الناري هو فلتر يسمح بالتعاملات والتبادلات المرغوب فيها فقط،[٢] حيث تعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالاعتماد على مجموعة من السياسات، حيث تقوم بتصفية حركة حزم البيانات بالسماح بمرور الحزم الواردة من المصادر المعروفة والموثوق بها، ومنع الحزم الواردة من جميع المصادر الأخرى وكذلك السماح بتشغيل الخدمات اللازمة لأعمال المؤسسة ومنع تشغيل الخدمات الأخرى.[٣]

ويوجد ضمن فئة الجدران النارية صنفان، الأول: هو الجدران النارية المؤسسية التي تقوم بحماية تطبيقات المؤسسات، والثاني: هي الجدران

---

١ د. خالد بن سليمان الغثبر، د. المهندس محمد عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التميز لأمن المعلومات، جامعة الملك سعود، المملكة العربية السعودية، ١٤٢٩هـ-٢٠٠٩م، لا يوجد رقم صفحة.

٢ د. أغيد القطعان، مفاهيم ومصطلحات الأمن السيبراني، المجلة المعلوماتية، الجمعية العلمية السورية، العدد ٨٩، تموز، ٢٠١٣م، متاح على الرابط: www.infomag.news.com، تاريخ الزيارة: ٢٠١٤/٧/٦م.

٣ المهندس زكريا أحمد عامر، المرجع السابق. ص ٣٩.

النارية الشخصية،[١] والجدران النارية في تطور مستمر وذلك رداً على تطور القراصنة ومحاولات اختراقها أو تعطيلها.[٢]

الفرع الخامس

الشبكات الافتراضية الخاصة

لا توجد طريقة أكثر أمناً من الشبكات الافتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى الشبكة.

وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة، وفي هذه الحالة يمكن للمستخدمين المعينين النفاذ إلى الشبكة عبر الإنترنت، وإسقاط الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين.[٣]

مما تقدم نخلص إلى ما يلي:

في نهاية هذا المبحث، لابد من القول أنه على الرغم من أهمية إجراءات الحماية الأساسية وأنظمة الحماية الفنية من الاعتداءات الإلكترونية وضرورة تواجدها، إلا أنها لا تكفي لجعل الإنترنت مكاناً آمناً، فلا بد من سيادة القانون.[٤]

---

١ د. سعيد عطوة الزنط، المرجع السابق، ص٧.

٢ حماد حجازي، احتراف أمن وحماية الأجهزة الشخصية موجه للمستخدم العادي، الطبعة الأولى، فلسطين-غزة، ٢٠٠٨، متاح على الرابط: download-internet-pdf-ebooks.com/٤٥٦-free-book، ص٨٨.

٣ د. سعيد عطوة الزنط، المرجع السابق، ص٨.

٤ محمد سيد سلطان، مرجع سابق، ص ١٦.

على الرغم من أن تكنولوجيا المعلومات وتشغيل الشبكة والحماية اللازمة لها مكلفة جداً، في حين أن الوسائل اللازمة لمهاجمتهم رخيصة، فقد أثبتت التجربة أن المجرمين المعلوماتيين عموماً لهم قدرة فائقة على تجاوز أنظمة الأمان التي تزود بها الأنظمة المعلوماتية، وفي استحداث وسائل وطرق جديدة على الدوام لا تتمكن طرق أو وسائل الحماية الموجودة من استيعابها، وقد كشف الواقع أن أكبر الأنظمة المعلوماتية، وأكثرها توفيراً لهذه الحماية الفنية تم اختراقها.[١]

وبالتالي، لا يوجد حل جذري يُنصح به للوقاية من جرائم الإرهاب بالوسائل الإلكترونية نظراً لتنوع أشكالها وتعدد أساليب ارتكابها، نتيجة التطور التقني الذي يحدث بسرعة كبيرة، بالإضافة إلى عنصر المباغتة الذي يتميز به الإرهاب بالوسائل الإلكترونية في بعده الرقمي، والذي يعد تحدياً أمنياً يضع الطرف الأخير في موقف ضعيف، حيث يقتصر دوره في تلك الحالة على رد الفعل مع إصابة الإجراءات الوقائية في مقتل.

ولكن تبقى الخلاصة هي أنه لا يمكن تقديم حماية مطلقة وتامة لنظم المعلومات المرتبطة بشبكة الاتصالات، والسبيل الوحيد لتأمين المعلومات الحساسة حتى الوقت الراهن هي عزل الأجهزة التي تحتوي هذه المعلومات عن العالم، لكن مثل هذه الإجراءات يمكن لها أن تؤدي على المدى الطويل لحرمان المجتمع من وسائل زيادة الإنتاجية والفاعلية.[٢]

---

١ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية-مصر، ٢٠٠٧م، ص٣٠.

٢ د. سعيد عطوة الزنط، مرجع سابق، ص ٧.

الخاتمة

يأتي هذا البحث الذي عالج ظاهرة الإرهاب بالوسائل الإلكترونية، من باب الاهتمام بها، لتسليط الضوء على سلبيات العالم الرقمي وما جاء به من أخطار، وذلك للاهتمام بهذه الظاهرة الجرمية المستحدثة من الناحية القانونية والتقنية، ونحن كدول نامية تحملنا ونتحمل ثقل الآثار الاقتصادية والاجتماعية وحتى السياسية لهذا النوع من الجرائم، لأننا بقينا جاثمين أمام الاجتياح التكنولوجي الذي دخل حياتنا رغماً عنا، دون أن نتخذ ردة فعل مناسبة بوضع التشريعات الملائمة، وأجهزة المراقبة والمكافحة الميدانية، لحماية مجتمعنا تاركين المجال مفتوحاً للعبث بمستقبل ومصير أوطاننا.

وفي الوقت الحالي، لا توجد طرق مضمونة لحماية النظام الإلكتروني أو البنى التحتية الإلكترونية، ولا يوجد نظام آمن تماماً بحيث يصعب على الإرهابيين الوصول إليه، مما يجعل حكومات كثيرة تتبع سياسة العزلة، التي توصف بأنها أحد اشكال الوقاية من الإرهاب بالوسائل الإلكترونية والجريمة المعلوماتية.

وخلصنا من هذا البحث العلمي، والذي أوضحنا فيه ماهية الإرهاب بالوسائل الإلكترونية، سواء من حيث إطاره النظري أو القانوني، أو من حيث آليات مكافحة هذه الظاهرة سواء على المستوى الفني أو التقني أو على المستوى التشريعي، إلى مجموعة من النتائج والتوصيات.

أولاً: النتائج

١- إذا كان الإرهاب بالوسائل الإلكترونية مفهوماً جديداً، فإنه يبقى مع ذلك مجرد تطور نوعي للإرهاب بصفة عامة، أو صورة جديدة لما يمكن أن يسمى بالإرهاب التقليدي، وهذه الصورة الحديثة للإرهاب، باتت تستهدف الأمن القومي للدول، خصوصاً في مجال التكنولوجيا، وإن معالم ظاهرة الإرهاب بالوسائل الإلكترونية، لم تبرز إلى الوجود بشكل جلي إلا بعد أحداث ١١ أيلول ٢٠٠١م التي ضربت الولايات المتحدة الأمريكية.

٢- يعّرف الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) بأنه: "**كل فعل يهدف إلى نشر حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الإضرار بالبنية التحتية أو الأساسية أو المعلوماتية، ويستخدم نظم المعلومات أو التقنية الرقمية (الحواسيب أو الشبكات) كهدف أو وسيلة.**" أي إن الإرهاب بالوسائل الإلكترونية، هو كل فعل يستخدم النظم الرقمية أو التقنية كهدف أو وسيلة، فالنظرة إلى الإرهاب بالوسائل الإلكترونية لا تنحصر في الأعمال التخريبية مثل اختراق المواقع الإلكترونية العسكرية والمدنية والسيطرة عليها أو تدميرها، بل تمتد لتشمل أنشطة أكثر خطورة، وهي الاستخدام اليومي للإنترنت من قبل الإرهابيين والجماعات الإرهابية.

٣- تصنف أفعال الإرهاب بالوسائل الإلكترونية إلى ثلاث أنواع هي:

أ- **هجوم المعلومات:** الذي يقوم على تغيير أو تدمير محتوى الملفات الإلكترونية، وأنظمة الحاسب أو أي مواد أخرى متصلة بالبيئة الإلكترونية.

ب_ هجمات البنية التحتية: التي تستهدف تعطيل أو تدمير الأجهزة الفعلية، أو أنظمة التشغيل، أو البرمجيات، مما يؤدي إلى تدمير أو تعطيل البنية التحتية المعلوماتية أو السيطرة عليها من قبل الإرهابيين وهي الصورة الرئيسية للإرهاب بالوسائل الإلكترونية.

ج- تيسير التكنولوجيا: يتم من خلاله استخدام الحاسب الآلي وشبكة الإنترنت وأنظمة الاتصال على التخطيط للهجمات الإرهابية، والتحريض عليها، وإنشاء مواقع إلكترونية، وجمع التبرعات والتمويل، والتجنيد والتدريب، أي تسهيل الإرهاب بصورتيه التقليدية والإلكترونية.

٤- يجد الإرهاب بالوسائل الإلكترونية إطاره القانوني ضمن طائفتين من تشريعات الدولة، الأولى تشريعات الفضاء الإلكتروني وبشكل خاص الجرائم الإلكترونية، والطائفة الثانية تشريعات مكافحة الإرهاب (العادية)المناط بها تحديد المفاهيم وجهات الإشراف والاختصاص وإنفاذ القانون.

٥- خطى المشرع السوري خطوات إيجابية في مجال سن تشريعات حديثة لمواجهة الجريمة المعلوماتية بإصداره المرسوم التشريعي رقم ١٧ لعام **٢٠١٢م**، الخاص بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، وبالتالي أصبح للقاضي آليات للبت في قضايا الجريمة المعلوماتية، لكن لا يمكن الجزم بأن الرصيد التشريعي السوري في هذا الصدد كافٍ لمكافحة كل صور الجرائم المعلوماتية، بل لابد من استكماله، بحيث يشمل جرائم لم يشملها المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، فظاهرة الإجرام المعلوماتي حديثة ومتجددة، وقطاع تكنولوجيا الاتصال في تطور مستمر، مما يعني أنه يمكن أن تظهر في المستقبل أنواع أخرى من الجرائم المعلوماتية، مما يجعل المشرع

السوري ملزم بمواكبة التطورات المتلاحقة عبر سن تشريعات جديدة أو تعديل التشريعات الحالية.

٦- لم يتعرض المشرع السوري للإرهاب بالوسائل الإلكترونية ولم يشر إليه أبداً في نص المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، سواء من حيث (التعريف، الخصائص، الصور الجرمية للإرهاب بالوسائل الإلكترونية....إلخ) أو من حيث إمكانية ارتكاب أعمال إرهابية بوسائل معلوماتية، وأشار إلى حالة تعد جانباً أو مفردةً من مفردات الإرهاب بالوسائل الإلكترونية، في الفصل الخامس (أحكام عامة وختامية) من المرسوم السالف الذكر، وذلك في الفقرة /أ/ من المادة /٢٩/ منه والتي نصت على أعمال الدعاية والتحريض على ارتكاب الجرائم باستخدام الشبكة، إضافة إلى إمكانية تطبيق الفقرة /ب/ من المادة /٢٨/ من المرسوم التشريعي رقم /١٧/ سالف الذكر، على الإرهاب بالوسائل الإلكترونية، والتي تنص على مضاعفة الحد الأدنى للعقوبة المقررة.

أما الصور الأساسية للإرهاب الإلكتروني المتمثلة ب (هجمات بوسائل معلوماتية على مواقع أو بنى تحتية معلوماتية للتدمير أو السيطرة، أو إنشاء مواقع إلكترونية للتخطيط والتدريب والتمويل الإرهابي المعلوماتي....)، لم تلحظ بالتجريم في هذا المرسوم نهائياً، لكن يمكن الاستفادة من هذا المرسوم، في إطار كون جرائم الإرهاب بالوسائل الإلكترونية هي جرائم معلوماتية لكن تختلف من حيث القصد الجرمي والضرر، والصور التقنية لسلوكيات الجرائم الإلكترونية هي ذاتها التي تتبع بارتكابها.

٧- توسع المشرع في قانون مكافحة الإرهاب الجديد في التجريم والعقاب، ولم يكتفِ بالعقاب على الجرائم الإرهابية فقط، وإنما شمل القانون أفعال كثيرة كانت تعد من قبيل المساهمة الجرمية فيما لو تركت للقواعد العامة.

٨- لم يُشر المشرع السوري صراحةً إلى الإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني) أو إلى إمكانية ارتكاب العمل الإرهابي باستخدام الوسائل الإلكترونية، سواء في المادة الأولى عندما عرف العمل الإرهابي أو في المادة السابعة عندما عاقب على العمل الإرهابي.

لكنه في الوقت نفسه لم يحدد صور السلوك الجرمي المكون لجريمة العمل الإرهابي وإنما جاء النص القانوني عاماً، حيث اكتفى المشرع بتحديد العناصر المميزة له، ولم يحدد الوسائل التي ترتكب بها هذه الجريمة فقد استعمل مصطلحاً مرناً واسعاً بقوله " أي أداة تؤدي الغرض ذاته"، آخذاً بالحسبان الوسائل التي قد يفرزها التطور التكنولوجي والعلمي المستمر، وبالتالي يمكن أن ترتكب جريمة العمل الإرهابي باستخدام وسائل إلكترونية (معلوماتية)، ولكننا نجد في الوقت نفسه أن المشرع السوري قد حدد النتيجة الجرمية وذكرها على سبيل الحصر بأنها عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الأضرار بالبنية التحتية أو الأساسية للدولة، في حين أن النتائج التي قد تترتب على الإرهاب الإلكتروني مختلفة ومتنوعة (تدمير البنى التحتية المعلوماتية سواء عامة أو خاصة أو تدمير المواقع الإلكترونية الحكومية عسكرية أو سياسية أو تدمير نظم المعلومات الاقتصادية والمالية ...) ولا تتوقف عند النتائج التي أشار إليها المشرع السوري على سبيل الحصر.

وبالتالي نستطيع القول في عدم إمكانية تطبيق نص المادة السابعة على جريمة الإرهاب بالوسائل الإلكترونية إلا في حال كانت النتيجة الجرمية هي ذاتها النتيجة الجرمية التي حددها المشرع السوري على سبيل الحصر، وهذا التضييق في النتيجة الجرمية وبالتالي في نطاق التجريم، ينال من الإرهاب بصورتيه التقليدية الإلكترونية.

٩- عاقب المشرع السوري على جريمة العمل الإرهابي بموجب المادة السابعة من قانون مكافحة الإرهاب لعام ٢٠١٢م، بعقوبة واحدة، وجاء النص خالياً من الظروف المشددة.

١٠-إن المشرع السوري لم يعاقب بموجب الفقرة الأولى من المادة الرابعة من قانون مكافحة الإرهاب، على تمويل المنظمة الإرهابية أو شخص إرهابي.

لكنه حدد بموجب الفقرة الثانية من المادة نفسها، عقوبةً واحدةً لكلا الصورتين الجريمتين التي تضمنتهما، وهي الأشغال الشاقة من عشر سنوات إلى عشرين سنة، ولم يميز في العقوبة بين من يدرب وبين من يتلقى التدريب، لأن من يدرب شخص أو أكثر من شخص أشد خطورة، وكما لم يميز المشرع السوري في العقوبة أيضاً بين الخبرات التي يتم التدرب أو التدريب عليها بين مثلا من يدرب أو يتدرب على استعمال سلاح ناري أو يدرب أو يتدرب على تفخيخ السيارات.

١١-لقد اقتصر نص الفقرة **الثانية** من المادة الرابعة من قانون مكافحة الإرهاب، على التدرب أو التدريب على أمور محددة وهي "استعمال المتفجرات أو الأسلحة بأنواعها المختلفة أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية"، بقصد استعمالها بتنفيذ عمل

إرهابي، ولم يشر المشرع السوري صراحةً إلى التدرب أو التدريب على المهارات المستعملة بالإرهاب بالوسائل الإلكترونية، التدرب أو التدريب على (أعمال القرصنة أو صناعة الفيروسات واستخدامها، اختراق المواقع الإلكترونية، تدمير البنى التحتية المعلوماتية بوسائل معلوماتية....).

١٢-لم يحدد المشرع السوري الوسائل التي ترتكب بها الأعمال الإرهابية على سبيل الحصر بموجب المادة الأولى من قانون مكافحة الإرهاب، لكنه وقع بتناقض واضح مع المادة الخامسة من القانون نفسه، عندما عاقب على تهريب أو تصنيع أو سرقة أو اختلاس وسائل الإرهاب، وذكر منها فقط "الأسلحة والذخائر والمتفجرات".

١٣-إضافةً إلى التناقض الذي وقع فيه بين نص المادة **الأولى** والمادة **الخامسة** من قانون مكافحة الإرهاب بالنسبة للوسائل المستعملة في تنفيذ الأعمال الإرهابية، نلاحظ تضييق نطاق التجريم بالنسبة لوسائل الإرهاب، إذ حصرها بالأسلحة والذخائر والمتفجرات مهما كان نوعها، ولم يتطرق نهائياً إلى الوسائل المعلوماتية أو الوسائل التي أفرزتها التكنولوجيا الحديثة، والتي تستخدم سواء في تعزيز النشاط الإرهابي التقليدي، أو تستخدم في تنفيذ الهجمات الإرهابية الإلكترونية عبر الفضاء الإلكتروني.

١٤-لم يشر المشرع السوري صراحةً إلى الإرهاب بالوسائل الإلكترونية، أو إمكانية إرتكاب عمل إرهابي باستخدام وسائل معلوماتية بموجب القانون رقم /١٩/ لعام ٢٠١٢م، باستثناء المادة **الثامنة** منه تحت عنوان **"الترويج للأعمال الإرهابية"**، التي أشارت بشكل ضمني إلى

جانبٍ من جوانب الإرهاب بالوسائل الإلكترونية، وهو **إدارة أو استعمال موقع إلكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.**

١٥-بيّن البحث، أن مكافحة الإرهاب بالوسائل الإلكترونية تتطلب اتخاذ إجراءات، منها يتعلق بالوقاية والمنع (على المستوى الرقمي) وإجراءات تتعلق بالتجريم والعقاب (على المستوى التشريعي).

وعلى الرغم من أهمية مكافحة الإرهاب على المستوى الرقمي سواء من خلال إجراءات الحماية الأساسية أو أنظمة الحماية الفنية من الاعتداءات الإلكترونية وضرورة تواجدها، والتي يمكن لها أن تقلل بشكل كبير من مخاطر الإرهاب بالوسائل الإلكترونية، إلا أنها لا تكفي لجعل الإنترنت مكاناً آمناً، فلا بد من سيادة القانون.

١٦-إن موقف التشريعات الجزائية العربية متباين من الإرهاب بالوسائل الإلكترونية، فهي لم تدرج الإرهاب بالوسائل الإلكترونية كجريمة مستقلة بذاتها، فالبعض من هذه التشريعات العربية نص على تجريم الإرهاب بمفهومه العام ولم يعالج الإرهاب بالوسائل الإلكترونية، والبعض الآخر -أي التشريعات- وسعت من نطاق تعريف الإرهاب ليشمل الإرهاب بالوسائل الإلكترونية.

١٧-ليس هناك مفهوم دولي موحد حول الإرهاب بالوسائل الإلكترونية، فالقانون الدولي لم يعطِ تعريفاً واضحاً ومنهجاً معيناً للتعامل مع هذه الصورة الجديدة من الإرهاب، وتعد الاتفاقيات الدولية حول الجريمة المعلوماتية بمثابة المصدر القانوني الدولي الأول لكل الاتفاقيات الدولية والإقليمية والتشريعات الوطنية التي لها علاقة بموضوع الإرهاب بالوسائل الإلكترونية.

١٨-لا يوجد على مستوى الدول العربية، اتفاقية خاصة تعالج الإرهاب بالوسائل الإلكترونية، لكن يوجد عدد من الاتفاقيات الخاصة بمكافحة الإرهاب وتنظيم البيئة الإلكترونية.

١٩-التعاون الدولي هو اللبنة الأساسية لمواجهة الرهاب بالوسائل الإلكترونية، إلا أن عقبات عدة تقف في سبيله أبرزها: عدم وجود اتفاق عام مشترك بين الدول حول نموذج إساءة استخدام نظم المعلومات، عدم وجود مفهوم عام موحد للنشاط المجرم، عدم وجود معاهدات دولية تنظم هذا التعاون، تعقّد مشكلات تفتيش نظام معلوماتي خارج حدود الدولة، وجمع الأدلة.

ثانياً: التوصيات

١- دعوة المشرع السوري، إلى أن يعيد النظر في قوانيننا الوطنية وتعديلها بحيث تتناسب مع الجرائم المستحدثة، وأن يعمل على سد الفراغ التشريعي، من خلال التدخل لمواجهة القصور في التشريعات والقوانين الحالية أو تحديثها بالنص صراحةً على الإرهاب بالوسائل الإلكترونية كجريمة مستقلة إما ضمن مواد قانون مكافحة الإرهاب أو ضمن مواد قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، أو التوسع في تعريف العمل الإرهاب في المادة الأولى من القانون رقم /١٩/ لعام ٢٠١٢م ليشمل في طياته الإرهاب بالوسائل الإلكترونية.

٢- التوسع في صور استخدام المواقع الإلكترونية في الأنشطة الإرهابية مثل (التجنيد –التدريب–التهديد–جمع معلومات–..)، حيث أن المادة الثامنة من قانون مكافحة الإرهاب، أشارت إلى صورة واحدة لاستخدام المواقع الإلكترونية وهي **إدارة أو استعمال موقع إلكتروني بقصد الترويج لوسائل الإرهاب أو الأعمال الإرهابية.**

٣- التوسع في نصوص مواد قانون مكافحة الإرهاب وذلك بالنسبة للجرائم المستحدثة (المنظمة الإرهابية – تمويل الإرهاب – التدريب على الإعمال الإرهابية – وسائل الإرهاب – التهديد بعمل إرهابي) والتي كانت تخضع سابقاً للقواعد العامة المتعلقة بالمساهمة الجرمية، بالنص صراحةً على إمكانية ارتكابها بوسائل إلكترونية، لتشمل أوجه، وأنشطة الإرهاب بالوسائل الإلكترونية كلها من جهة، وحرصاً على وضوح النص من جهة أخرى.

٤- حدد المشرع السوري النتيجة الجرمية المترتبة على العمل الإرهابي على سبيل الحصر بموجب المادة السابعة من القانون رقم/١٩/ لعام ٢٠١٢م بأنها (عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الأضرار بالبنية التحتية أو الأساسية للدولة).

وبالتالي ندعو المشرع السوري إلى العقاب على العمل الإرهابي أياً كانت النتيجة المترتبة عليه، وتشديد العقوبة في حال عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الأضرار بالبنية التحتية أو الأساسية للدولة.

٥- جاء قانون مكافحة الإرهاب بعقوبة واحدة محددة لجريمة العمل الإرهابي مهما كانت جسامة النتيجة المترتبة على هذا العمل أو الوسيلة المستخدمة في تنفيذ هذا العمل الإرهابي، باستثناء أنه خفف العقوبة في حال كانت الوسائل المستخدمة في العمل الإرهابي تحدث تفجيراً صوتياً، كما جاء خالياً من ظروف التشديد، وبالتالي ندعو المشرع إلى أن يعيد النظر في عقوبة العمل الإرهابي لجهة تشديد العقوبة حسب جسامة النتيجة الجرمية والوسيلة المستعملة في تنفيذ العمل الإرهابي، لأنه من المنافي للعدالة، المساواة بالعقوبة بين جميع الجناة دون الأخذ بالحسبان النتيجة الجرمية المترتبة والوسيلة المستعملة.

٦- دعوة المشرع السوري إلى المعاقبة على تمويل الإرهابيين والمنظمة الإرهابية، وعدم اكتفاءه بالعقاب على جريمة تمويل العمل الإرهابي الذي يرتكبه إرهابي أو منظمة إرهابية، بموجب المادة **الرابعة** من قانون مكافحة الإرهاب.

٧- إن المشرع بموجب الفقرة **الثانية** من المادة **الرابعة** من قانون مكافحة الإرهاب، قد حدد عقوبةً واحدةً لكل من تدرب أو درب شخصاً أو أكثر

على استعمال المتفجرات أو الأسلحة بأنواعها المختلفة أو الذخائر أو وسائل الاتصالات أو على فنون القتال الحربية وذلك بقصد استعمالها في تنفيذ عمل إرهابي.

دعوة المشرع السوري إلى التمييز في العقوبة بين من يدرب وبين من يتلقى التدريب لأن من يدرب شخص أو أكثر من شخص أشد خطورة، والتمييز أيضاً بالنسبة للعقوبة بالنسبة للخبرات التي يتم التدرب أو التدريب عليها، مثلا من يدرب أو يتدرب على استعمال سلاح ناري ليس بخطورة يدرب أو يتدرب على تفخيخ السيارات.

٨- بالنسبة لنص المادة الخامسة من قانون مكافحة الإرهاب رقم /١٩/ لعام ٢٠١٢م، نرى أن يتوسع المشرع السوري في وسائل الإرهاب، بحيث يشمل وسائل الإرهاب التي تضمنتها المادة الأولى من القانون نفسه، والنص صراحةً على الوسائل التي أفرزها التطور التكنولوجي والتقدم العلمي.

٩- بالنسبة لنص المادة **السادسة** من قانون مكافحة الإرهاب، دعوة المشرع إلى العقاب على جريمة تهديد الحكومة بعمل إرهابي في جميع الأحوال، وتشديد العقوبة في حال اقتران التهديد بقصد حمل الحكومة على القيام بعمل أو الامتناع عنه.

١٠- يجب على الدول انتهاج سياسة تقنية في أمن المنشآت الحيوية، واستخدام مجموعة من الإجراءات الفنية التقنية الأساسية والتي يمكن لها أن تقلل بشكل كبير من مخاطر الإرهاب بالوسائل الإلكترونية، وتدريب المسؤولين عن مكافحة الإرهاب على استيعاب السياسات الأمنية الإلكترونية.

١١- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال تكنولوجيا المعلومات، والتركيز على تنمية الوعي بالثقافة المعلوماتية وأمن المعلومات وحجم أخطار الثورة الرقمية، وذلك بالنسبة للعاملين بالمؤسسات الحساسة: الأمنية – العدالة – الإعلام.

١٢- فرض الرقابة الكافية _وليست الشاملة_ من قبل الحكومة عن كل ما يقدم ويعرض من خلال الشبكة، وحجب المواقع التي تدعو وتحرض على الإرهاب، إضافة إلى إنشاء المواقع الإلكترونية التي تقوم بنشر الوعي والأفكار السامية.

١٣- تفعيل دور الإعلام الرسمي وغير الرسمي، حيث يلعب الإعلام دوراً محورياً مهماً في مكافحة الإرهاب بالوسائل الإلكترونية.

١٤- العمل إلى إيجاد الهوية الرقمية لمستخدمي الإنترنت، والتي لا يمكن للمستخدمين النفاذ إلى شبكة الإنترنت إلا من خلال هذه الهوية.

١٥- نقل التقنية التي تستخدم في الدول المتقدمة في مكافحة الإرهاب بالوسائل الإلكترونية إلى الدول التي لا تتوافر فيها هذه التقنية.

١٦- دعوة الدول العربية لوضع اتفاقية عربية واستراتيجية شاملة لمكافحة الإرهاب بالوسائل الإلكترونية، تحدد صور النشاط الإجرامي، وأوجه التعاون الأمني والقضائي والمعلوماتي العربي، لحماية البيئة الإلكترونية العربية من مخاطر الإرهاب بالوسائل الإلكترونية.

١٧- التنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحة الإرهاب بالوسائل الإلكترونية في دول العالم كافة.

١٨- التأكيد على أن التعاون بين الدول جميعها هو جزء أساسي من مواجهة الإرهاب بالوسائل الإلكترونية، والدعوة إلى زيادة التعاون على المستوى الوطني والثنائي والإقليمي.

١٩- حثّ الدول على عقد الاتفاقيات الدولية الخاصة بمكافحة الإرهاب بالوسائل الإلكترونية، والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الإرهاب والجرائم المعلوماتية.

٢٠- العمل على وضع اتفاقية أممية شاملة لمكافحة الإرهاب بالوسائل الإلكترونية، وتتضمن هذه الاتفاقية تعريف موحد للإرهاب بالوسائل الإلكترونية، وتحديد صور النشاط الجرمي، وآليات التعاون في المجال القضائي والأمني وتبادل المعلومات والخبرات، والتحقيق والتفتيش وجمع الأدلة، والملاحقة وتسليم الإرهابيين، وإنشاء مراكز لمراقبة الاتصالات وشبكة الإنترنت ومتابعة وملاحقة المجرمين.

ثالثاً: الاقتراحات

مشروع قانون لبعض المواد التي يجب إضافتها بالنسبة للإرهاب بالوسائل الإلكتروني، إضافة إلى تعديل بعض مواد قانون مكافحة الإرهاب رقم /١٩/ لعام ٢٠١٢م:

إضافة مادة إلى الفصل الثالث (مكافحة الجريمة لمعلوماتية) من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، تحت عنوان الأعمال الإرهابية بالوسائل الإلكترونية، على النحو الآتي:

١- العمل الإرهابي بالوسائل الإلكترونية: كل فعل يهدف إلى نشر حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الإضرار بالبنية التحتية أو الأساسية أو المعلوماتية، ويُرتكب باستخدام وسائل معلوماتية.

٢- كل عمل إرهابي بالوسائل الإلكترونية يستوجب الأشغال الشاقة المؤقتة سبع سنوات على الأقل والغرامة ضعفي قيمة الضرر.

٣- وتكون العقوبة الأشغال الشاقة المؤبدة والغرامة ضعفي قيمة الضرر إذا نتج عنه عجز إنسان أو الإضرار بالبنية التحتية او الأساسية أو المعلوماتية.

٤- وتكون العقوبة الإعدام إذا افضى الفعل إلى موت إنسان.

إضافة مادة إلى الفصل الثالث (مكافحة الجريمة لمعلوماتية) من المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، تحت عنوان الأعمال المتعلقة بالإرهاب والمرتكبة بالوسائل الإلكترونية، على النحو الآتي:

١- يعاقب بالأشغال الشاقة المؤقتة والغرامة من مليون إلى مليونين ليرة سورية كل من أنشأ أو أدار موقعاً إلكترونيا أو أشرف عليه أو نشر معلومات على الشبكة، أو استخدم الشبكة، بقصد:

- تسهيل الاتصال بين الإرهابيين (قيادات أو أعضاء).
- جمع المعلومات لارتكاب الأعمال الإرهابية.
- الترويج لأفكار الإرهابيين ومبادئهم.
- الترويج لوسائل الإرهاب أو الأعمال الإرهابية.
- تجنيد عناصر للقيام بأعمال إرهابية.
- تمويل إرهابي أو منظمة إرهابية أو عمل إرهابي.
- التدريب الإلكتروني على ارتكاب أعمال إرهابية.
- التهديد الإلكتروني بارتكاب أعمال إرهابية.
- إصدار البيانات الإلكترونية (مرئية، مكتوبة، مسموعة) للجماعات الإرهابية.
- التخطيط والتنسيق لارتكاب أعمال إرهابية.
- التحريض على ارتكاب الأعمال الإرهابية.

٢- وتكون العقوبة الأشغال الشاقة من خمس عشرة سنة إلى عشرين سنة والغرامة من مليونين إلى مليونين ونصف مليون ليرة سورية، إذا ارتكبت الأفعال السابقة من خلال مواقع التواصل الاجتماعي.

تعديل تعريف العمل الإرهابي في المادة /١/ من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

كل فعل يهدف إلى إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الإضرار بالبنى التحتية أو الأساسية للدولة، ويُرتكب باستخدام الأسلحة والذخائر أو المتفجرات أو المواد الملتهبة أو المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية أو وسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية مهما كان نوع هذه الوسائل أو باستخدام أي أداة تؤدي الغرض ذاته.

تعديل الفقرة /١/ من المادة /٤/ (تميل الأعمال الإرهابية) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

يعاقب كل من قام بتمويل إرهابي أو منظمة إرهابية أو عمل إرهابي أو أكثر بالأشغال الشاقة من خمس عشر سنة إلى عشرين سنة وبالغرامة ضعفي قيمة الأموال المنقولة وغير المنقولة أو الأشياء التي كانت محلا للتمويل.

تعديل الفقرة /٢/ من المادة /٤/ (التدريب على الأعمال الإرهابية) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

يعاقب الأشغال الشاقة من عشر سنوات إلى عشرين سنة كل من تدرب أو دربّ شخصاً أو أكثر على استعمال المتفجرات أو الأسلحة بمختلف أنواعها أو الذخائر أو وسائل الاتصالات السلكية أو اللاسلكية أو الإلكترونية أو أي وسيلة اتصال أخرى أو على فنون القتال الحربية أياً كانت، وذلك بقصد استعمالها في تنفيذ عمل إرهابي.

تعديل الفقرة /ا/ من المادة /٥/ (وسائل الإرهاب) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

يعاقب بالأشغال الشاقة من خمس عشرة سنة إلى عشرين سنة وبالغرامة ضعفي قيمة المضبوطات كل من قام بتهريب أو بيع أو شراء أو تصنيع أو تحضير أو أحراز أو حيازة أو سرقة أو اختلاس أو نقل الأسلحة أو الذخائر أو المتفجرات أو المواد الملتهبة أو المنتجات السامة أو المحرقة أو العوامل الوبائية أو الجرثومية أو وسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية مهما كان نوع هذه الوسائل أو باستخدام أي أداة تؤدي الغرض ذاته، أو الأجزاء التي تستعمل في صنعها أو تحضيرها، بقصد استخدامها في تنفيذ عمل إرهابي.

تعديل المادة /٦/ (التهديد بعمل إرهابي) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

١- يعاقب بالأشغال الشاقة المؤقتة من هدد الحكومة بأي وسيلة كانت بالقيام بعمل الإرهابي.

٢- وتكون العقوبة الأشغال الشاقة من خمس عشرة سنة إلى عشرين سنة إذا كان القصد من التهديد حمل الحكومة على القيام بعمل أو الامتناع عنه، أو رافق التهديد خطف إحدى وسائل النقل الجوي أو البحري أو البري العامة أو الخاصة أو الاستيلاء على عقار مهما كان نوعه أو الاستيلاء على الأشياء العسكرية أو خطف شخص ما.

٣- وتكون العقوبة الإعدام إذا أدى الفعل إلى موت الشخص.

تعديل المادة /٧/ (عقوبة العمل الإرهابي) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

١- كل عمل إرهابي يستوجب الأشغال الشاقة المؤبدة والغرامة ضعفي قيمة الضرر.

٢- وتكون العقوبة الإعدام إذا نجم عنه وفاة أو عجز إنسان أو انهدام بناء جزئياً أو كلياً أو الإضرار بالبينية التحتية أو الأساسية للدولة.

٣- وتكون العقوبة الأشغال الشاقة المؤقتة خمس سنوات على الأقل إذا كانت الوسائل المستخدمة في العمل الإرهابي تحدث تفجيراً صوتياً فقط.

تعديل المادة /٨/ (الترويج للأعمال الإرهابية) من القانون رقم /١٩/ لعام ٢٠١٢م، بحيث تصبح على النحو الآتي:

يعاقب بالأشغال الشاقة المؤقتة كل من روّج لوسائل الإرهاب أو الأعمال الإرهابية، بطريقة مباشرة أو غير مباشرة بالقول أو الكتابة، أو قام بتوزيع المطبوعات أو المعلومات المخزنة مهما كان شكلها.

مراجع البحث

أولاُ: المراجع باللغة العربية

١- المراجع العامة

- أ.د. بارعة القدسي، أصول المحاكمات الجزائية، الجزء الأول، الدعوى العامة-الدعوى المدنية، جامعة دمشق، ١٤٣٠-١٤٣٢هـ، ٢٠١٠-٢٠١١م.
- د. سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٠م.
- أ.د. عبود السراج، قانون العقوبات، القسم العام، الطبعة الثانية عشر، جامعة دمشق، ١٤٢٥-١٤٢٦هـ الموافق٢٠٠٤-٢٠٠٥م.
- أ.د. محمد الفاضل، المبادئ العامة في قانون العقوبات، الطبعة الثانية، دمشق، ١٣٨٣هـ -١٩٦٣م.
- د. معن أحمد محمد الحياري، الركن المادي للجريمة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١٠م.

٢- المراجع المتخصصة

أ- الكتب

- د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٧هـ-٢٠٠٦م.

- حماد حجازي، احتراف أمن وحماية الأجهزة الشخصية موجه للمستخدم العادي، الطبعة الأولى، فلسطين غزة، ٢٠٠٨م، متاح على الرابط: download-internet-pdf-ebooks.com/٤٥٦-free-book
- د. خالد بن سليمان الغثبر، د. المهندس محمد عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التميز لأمن المعلومات، جامعة الملك سعود، المملكة العربية السعودية، ١٤٢٩هـ-٢٠٠٩م.
- اللواء د. محمد فتحي عيد، الأساليب والوسائل التقنية التي يستخدمها الإرهابيون وطرق التصدي لها ومكافحتها، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٢ هـ _ ٢٠٠٢م.
- أ.د. محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير وأساليبها، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٢٧هـ -٢٠٠٦م.
- اللواء د. محمد فتحي عيد، الإجرام المعاصر، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤١٩هـ - ١٩٩٩م.
- أ.د. محمد مسعود قيراط، الإرهاب، دراسة في البرامج الوطنية واستراتيجيات مكافحته، مقاربة إعلامية، جامعة نايف العربي للعلوم الأمنية، الطبعة الأولى، الرياض، المملكة العربية السعودية، ١٤٣٢ هـ -٢٠١١م.

- د. محمد السيد عرفة، تجفيف مصادر الإرهاب، الطبعة الأولى، الرياض، المملكة العربية السعودية، ١٤٣٠هـ -٢٠٠٩م.
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠٠٧م.
- اللواء د. نشأت عثمان الهلالي، تجارب عربية ناجحة في تنظيم وتجهيز مكافحة الإرهاب (التجربة المصرية)، قدرات لأجهزة الأمنية وأثرها في مكافحة الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣١هـ -٢٠١٠م.

ب- الرسائل العلمية

- المهندس زكريا أحمد عامر، حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، دراسة لنيل درجة الماجستير في تقانة المعلومات، جامعة النيلين، كلية الدراسات العليا، الخرطوم، السودان، ١٤٣٢هـ/٢٠١١م.

ج- الأبحاث والمقالات

- د. أحمد فتحي سرور، حكم القانون في مواجهة الإرهاب، القاهرة، ٢٠٠٧م، بحث منشور على الإنترنت، متاح على الرابط: hccourt.gov.eg/pages/elmglacut/mkat/١٢/Makala-html، تاريخ الزيارة: ٢٠١٤/١١/٩م.
- د. حسين بن سعيد بن سيف الغافري، الإرهاب الإلكتروني، هيئة تقنية المعلومات، سلطنة عمان، متاح على الرابط:

eoman@ita.gov.com
/itaportal=ar/pags/page.aspx&nid=١&pid=٩٨lid=s،
تاريخ الزيارة: ٢٠١٣/٥/١م.

- د. يوسف بن أحمد الرميح، الإرهاب والجريمة الإلكترونية بالمجتمع السعودي رؤية: سوسيولوجية، مجلة كلية الآدب بقنا، جامعة جنوب الوادي، مصر، العدد ٢٧، ٢٠٠٩م.
- أماني عزام، تعرف على أشهر الدول التي تطبق "قوانين مكافحة الإرهاب"، الوطن، بوابة إلكترونية شاملة، متاح على الرابط: www.elwatannews.com.com/news/details/٧٦٢٧٥٣/، تاريخ النشر: ٢٠١٥/٧/٣م، تاريخ الزيارة: ٢٠١٥/٧/٩م.
- أحمد إمام، قانون "مكافحة الإرهاب" في فرنسا..١٤ تعديلاً خلال ٩ سنوات، الوطن بوابة إلكترونية شاملة، تاريخ النشر: ٢٠١٣/٧/٩م، متاح على الرابط: www.almustagbal.com/news/detailes/٧٦٦٧٤٥/ ، تاريخ الزيارة: ٢٠١٤/١/١م.
- كتاب الإرهاب على الشبكة العالمية، موقع السكينة، تاريخ النشر: ١٦ يناير ٢٠١٠م، متاح على الرابط: www.assakina.com/ceuter/red-book/٤٦٦٨.htmlwww.assakina.com/ceuter/red-book/٤٦٦٨.html، تاريخ الزيارة: ٢٠١٣/٦/٥م.
- الإرهاب الإلكتروني تهديد لم يتبلور بعد لكن لابد من أن يؤخذ على محمل الجد، صحيفة الراكوبة، أخبار السودان لحظة بلحظة، تاريخ النشر: ٢٠١٣/١٠/٢، متاح على الرابط التالي: www.alrakoba.net/news-action-show-id-٨٦٧٢٦.htmK. تاريخ الزيارة: ٢٠١٤/٧/٧م.

- الإرهاب الإلكتروني، جولة في عقل متطرف، نقلاً عن صحيفة العرب الإلكترونية، موقع السكينة، تريخ النشر: ١٧ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com/awareness-net/terrorism-net/٤٤٦٥٧.html، تاريخ الزيارة: ٢٠١٥/٢/٢م.
- الإرهاب الإلكتروني مفهومه ووسائل مكافحته، شبكة ضياء للمؤتمرات والدراسات، تاريخ النشر: ٢٩ أكتوبر ٢٠١٤، متاح على الرابط: diae.net/١٦٢٤٣، تاريخ الزيارة: ٢٠١٥/٧/١.
- الإرهاب الإلكتروني الثوابت والمتغيرات، مدير البحث العلمي في وزارة الأوقاف، حزب البعث العربي الاشتراكي-القطر السوري-القيادة القطرية، تاريخ النشر: ٢٠١٤/١٢/١٤، متاح على الرابط: baathparty.sy/Arabic/index.php?node=٥٥٢&cat=١٢٦٩&، تاريخ الزيارة: ٢٠١٥/٥/٣.
- إرهاب إلكتروني، ويكيبيديا، الموسوعة الحرة، متاح على الرابط التالي:
https://ar.wikipedia.org/wik/إرهاب- إلكتروني/، تاريخ الزيارة: ٢٠١٤/٥/٢٤م.
- تركي تركي، وسائل التواصل الاجتماعي.. تسويق الإرهاب وإعادة تدويره، نقلاً عن الاقتصادية، موقع السكينة، تاريخ النشر: ١٣ يوليو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٣/٢م.
- تركي تركي، (الجهاد الإعلامي) وخلايا (القاعدة الإلكترونية) .. أزمة عالمية، موقع السكينة، تاريخ النشر: ١١ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٣/١م.

- جهاد جين (سيدة الإرهاب الإلكتروني)، موقع السكينة، تاريخ النشر: ١٠ يناير ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢/٤/٢٠١٥م.
- الرقابة على الإنترنت، ويكيبيديا، الموسوعة الحرة، متاح على الرابط: الرقابة –على–الإنترنت /Ar.wikipedia.org/wiki، تاريخ الزيارة ١٢/١٢/٢٠١٤م.
- زبير الأنصاري، معسكر "تويتر" يعوض " القاعدة" عن "الفاروق" وتلال "الرقة، نقلاً عن الحياة، موقع السكينة، تاريخ النشر: ١٢ مايو ٢٠١٤، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ١/٣/٢٠١٥م.
- سعد السبيعي، الهجمات الإلكترونية..تأثيرها على الاقتصاد الوطني، موقع السكينة، تاريخ النشر: ١١ فبراير ٢٠١٤م، متاح على الرابط: www.assakina.com/awareness_net/rebunds/٣٨٠٧٤. htmi، تاريخ الزيارة: ١/٩/٢٠١٥م.
- الصين توظف مليوني شخص لمراقبة الأنشطة على شبكة الإنترنت، الأمة صحيفة إلكترونية مستقلة، تاريخ النشر: ٧ أكتوبر ٢٠١٣، متاح على الرابط: html–الصين –توظف –مليوني–شخص – لمراقبة –الأنشطة –على –شبكة –الإنترنت –www.al –omah.com/mis/٦١٧٣، تاريخ الزيارة: ١٨/٢٠١٤م.
- علي مطر، الإرهاب الإلكتروني في القانون الدولي: نوع جديد لم يتم التعامل معه بعد، موقع الأنباء الاخباري، تاريخ النشر: ٢٠١٣/٢/٢٥م، متاح على الرابط:/الإرهاب–الإلكتروني–في– القانون–الدولي www.inbaa.com/، تاريخ الزيارة: ١/٣/٢٠١٤م.

- د. عبد الرحمن الهدلق، الجهاد الإلكتروني الزائف وآليات مواجهته، موقع السكينة، تاريخ النشر: ٢٦ يونيو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة ٢٠١٥/٦/١م.
- فرنسا تشدد الرقابة على الإنترنت بحجة: مكافحة الإرهاب، رصد- وكالات، تاريخ النشر: ٢٣ نيسان ٢٠١٥م، القاهرة، متاح على الرابط rassd.com/١٣٩٤٢٦.htm، تاريخ الزيارة: ٢١٥/٥/٤م.
- فرنسا توقع اتفاقية لمحاربة الإرهاب الإلكتروني، المستقبل، موقع اخباري، تاريخ النشر: ٢٠١٥/٤/٢٣م، متاح على الرابط: www.almustagbal.com، تاريخ الزيارة: ٢٠١٥/٥/٦م.
- فرنسا تحجب المواقع الإرهابية، تاريخ النشر: ١٧ مارس ٢٠١٥م، موقع السكينة، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٤/١م.
- د. محمد بن حمود الهدلاء، كثرة مواقع الجماعات الإرهابية، نقلاً عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ٢٩ أكتوبر ٢٠١٢م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٣/٩/١م.
- د. محمد فتحي سرور، جريدة الأهرام، قضايا وآراء، الخميس ٢٧ شوال ١٤٢٧هـ، ٨ نوفمبر ٢٠٠٧م، ٤٤١٦٦.
- د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، أراء حول الخليج، متاح على الرابط: araa.ea/index.pbp?optton=com-content&view=article&i٨=٢٤٤:٢٠١٤-٠٦-١٣-١٦-١٢١-٣١، تاريخ الزيارة: ٢٠١٥/٧/٢٨م.

- هيام الدهبي، الإرهاب الإلكتروني والقوة في العلاقات الدولية، موقع الحياة، تاريخ النشر: ٢ أذار ٢٠١٤م، متاح على الرابط التالي: /الإرهاب_الإلكتروني_والقوة_في_العلاقات_الدولية/ www.alhayat.com/articles/٨٣١٥١٠، تاريخ الزيارة: ٢٠١٥/٦/٥م.
- د. يوسف بن أحمد الرميح، الإرهاب الإلكتروني. وشبكات التواصل (٢-٢)، نقلا عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ١٧ أغسطس ٢٠١٣م، متاح على الرابط: www.assakina.com/news/news١/٢٧١٤٥.html، تاريخ الزيارة: ٢٠١٤/١١/٩م.
- د. يوسف بن أحمد الرميح، الإرهاب والاعلام الجديد (الإرهاب الرقمي) ١-٢، صحيفة الجزيرة الإلكتروني، العدد ١٥٥٠٠، تاريخ النشر: ٢٠١٥/٣/٧م، متاح على الرابط: www.al-jazirah.com/٢٠١٥/٢٠١٥٠٣٠٧/ar.ihtm، تاريخ الزيارة: ٢٠١٥/٥/٥م.
- د. يوسف بن أحمد الرميح، معركتنا ضد الإرهاب على الساحة الافتراضية الإلكترونية، نقلاً عن صحيفة الجزيرة السعودية، موقع السكينة، تاريخ النشر: ١١ مايو ٢٠١٤م، متاح على الرابط: www.assakina.com، تاريخ الزيارة: ٢٠١٥/٥/١م.

د-الندوات والمؤتمرات

- د. أيسر محمد عطية: دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، الملتقى العلمي، الجرائم المستحدثة في ظل المتغيرات والمتحولات الإقليمية والدولية،

خلال الفترة من: ٢-٢٠١٤/٩/٤م، عمان، المملكة الأردنية الهاشمية، ٢٠١٤م.

- د. أخام بن عودة زواوي ملكية: تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس / ليبيا، ٢٧-٣٠ أكتوبر ٢٠٠٩م، بحث منشور على الإنترنت.
- د. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، الدورة التدريبية: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، الرياض، المملكة العربية السعودية، خلال الفترة ٢٣-٢٠١٣/٢/٢٧م.
- د. سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، الملتقى العلمي، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من ٢-٢٠١٤/٩/٤م، عمان، المملكة الأردنية الهاشمية، ١٤٣٥هـ-٢٠١٤م.
- د. سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجية الأمن القومي، مؤتمر الجرائم المستحدثة-كيفية إثباتها ومواجهتها، القاهرة-مصر، ١٥-١٦ ديسمبر ٢٠١٠م.
- د. علي علي فهمي، دور الشبكات الاجتماعية في تمويل وتجنيد الإرهابيين، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢ م.

- أ.د جميل عبد الباقي الصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الإنترنت، الحلقة العلمية، الإنترنت والإرهاب، بالتعاون مع جامعة عين شمس، القاهرة-مصر، خلال الفترة ١٥-٢٠٠٨/١١/١٩م.
- أ.د. ذياب موسى البداينة، الإرهاب المعلوماتي (التعريف-المفهوم-المجالات-النتائج)، الحلقة العلمية، الإنترنت والإرهاب خلال الفترة من ١٧-١٤٢٩/١١/٢١هـ الموافق ١٥-٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، جامعة نايف العربية للعلوم الأمنية، القاهرة ١٤٢٩هـ/٢٠٠٨م.
- سهير عثمان عبد الحليم، الإرهاب والإنترنت، دراسة حالة في ضوء التجربة المصرية، ورقة عمل مقدمة للمؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، المنعقد في القاهرة ٢-٤ يونيو ٢٠٠٨.
- د. على بن فايز الجحني، أضواء على الاتفاقية العربية لمكافحة الإرهاب، تشريعات مكافحة الإرهاب في الوطن العربي، الندوة العلمية الخمسون، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤١٩هـ -١٩٩٩م.
- أ.د. عبد الله بن ناصر الحمود، وسائل الإعلام المعاصرة والإرهاب المعلوماتي، مكافحة جرائم الإرهاب عبر الإنترنت، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، المغرب، القنيطرة خلال الفترة ٩-٢٠٠٦/٤/١٣م.
- د. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها وطرق مكافحتها، المملكة العربية السعودية، جامعة الأمام محمد بن

سعود الإسلامية، اللجنة العلمية للمؤتمر العالمي عن موقف الإسلام من الإرهاب، ٢٠٠٤م.

- عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، القنيطرة-المغرب، خلال الفترة ١١-١٤٢٧/٣/١٥هـ الموافق ٩-٢٠٠٦/٤/١٣م.
- د. عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من ١١-١٤٢٧/٣/١٥هـ لموافق ٩-٢٠٠٦/٤/١٣م، المغرب، القنيطرة، الموافق ١٤٢٧هـ-٢٠٠٦م.
- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى مؤتمر الدولي الأول حول حماية الأمن والمعلومات والخصوصية في قانون الإنترنت، القاهرة، مصر، ٢-٤ يونيو ٢٠٠٨م، بحث منشور على الإنترنت. منتدى كلية الحقوق، جامعة المنصورة، مصر، متاح على الرابط: www.f-law.net.
- أ.د. عبد الرحمن عبد العزيز الشنيفي، المواجهة الأمنية للإرهاب الإلكتروني، الحلقة العلمية، الإرهاب والإنترنت، خلال الفترة من ١٥-٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، القاهرة-مصر، ١٤٢٩هـ/٢٠٠٨م.
- اللواء. عبد الحميد ابراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، ما هو دور القطاع الخاص، الدورة التدريبية، مكافحة الجرائم الإرهابية المعلوماتية، ١١-

١٤٢٧/٣/١٥هـ الموافق ٩-٢٠٠٦/٤/١٣م، المغرب-القنيطرة،١٤٢٧هـ-٢٠٠٦م.

- د. فايز عبد الله الشهري، ثقافة التطرف والعنف على الشبكة الإنترنت: الملامح والاتجاهات، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢م.
- د .محمد بن عبد الله آل فايع العسيري و د. حسن بن أحمد الشهري، الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢م.
- محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد في الرياض، المملكة العربية السعودية: خلال الفترة ٢١-٢٢ ربيع الثاني ١٤٣١هـ، ٦-٧ ابريل ٢٠١٠م.
- د. مها عبد المجيد صلاح، استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الإنترنت، دراسة تحليلية، الندوة العلمية، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، القاهرة، ١٧-١٩/١١/١٤٣١هـ الموافق ٢٥-٢٠١٠/١٠/٢٧م.
- د. محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، جامعة نايف العربية للعلوم الأمنية، القاهرة ١٤٢٩هـ/٢٠٠٨م.الحلقة العلمية (الإنترنت والإرهاب) خلال الفترة

من ١٧-١٤٢٩/١١/٢١هـ الموافق ٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس.

- اللواء د. مصطفى محمد موسى، التنظيمات الإرهابية وشبكة الإنترنت، الندوة العلمية استشراق التهديدات الإرهابية، الرياض، المملكة العربية السعودية، ٧-١٤٢٨/٨/٩هـ الموافق ٢٠-٢٠٠٧/٨/٢٢م.
- د. منى الأشقر جبور، د. عزيز ملحم بربر، أمن الشبكات والإنترنت، الحلقة العلمية الإنترنت والإرهاب، خلال الفترة: ١٧-١٤٢٩/١١/٢١هـ الموافق ١٥-٢٠٠٨/١١/١٩م، بالتعاون مع جامعة عين شمس، جامعة نايف العربية للعلوم الأمنية، القاهرة، مصر، ٢٠٠٨م.
- أ.د. وليد محمد أبو رية، التعرف الإرهاب الإلكتروني، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ -٢٠١٢ م.
- د. يونس محمد عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت لأغراض إرهابية، الندوة العلمية: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ١٤٣٣هـ - ٢٠١٢ م.
- د. يونس عرب، مشروع قانون نموذجي عربي، لجرائم الكمبيوتر والإنترنت أو للجرائم الإلكترونية، ورشة عمل: تطوير التشريعات

في مجال مكافحة الجرائم الإلكترونية، عمان – الأردن، ٢-٤ نيسان، ٢٠٠٦م.

ه-المجلات والدوريات

- د. أغيد القطعان، مفاهيم ومصطلحات الأمن السيبراني، مجلة المعلوماتية، الجمعية العلمية السورية للمعلومات، العدد ٨٩، تموز، ٢٠١٣م، متاح على الرابط: www.infomag.news.sy.
- إياد علي الدرة، المناعة التشريعية في مواجهة الوباء المعلوماتي، مجلة المعلوماتية والقانون، الجمعية العلمية السورية المعلوماتية، العدد (٧٣)، شهر آذار، ٢٠١٢م، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٢/٥/٢٠١٣م.
- إياد علي الدرة، التجربة السورية في مجال التشريع الإلكتروني، مجلة المعلوماتية والقانون، الجمعية العلمية السورية المعلوماتية، العدد (٦١)، شهر آذار، ٢٠١١م، متاح على الرابط: www.infomag.news.sy، تاريخ الزيارة: ٥/٤/٢٠١٣م.
- إياد علي الدرة، الإرهاب الإلكتروني، المجلة المعلوماتية، أمن المعلومات، الجمعية العلمية السورية للمعلومات، العدد ٨١، تشرين الثاني، ٢٠١٢م. متاح على الرابط: www.infomag.news.sy.
- د. حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية (تصور مفتوح)، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، ٢٠١١م/١٤٣٢هـ، المجلد ٢٧، العدد ٥٣.

- د. سامر الدقاق، التعمية وحماية المعلومات على شبكة الإنترنت، مجلة المعلوماتية، الجمعية العلمية السورية للمعلومات، العدد ٨٠، تشرين الأول، ٢٠١٢م، متاح على الرابط: www.infomag.news.sy.
- عشر نصائح أساسية لحماية الشبكات، أمن المعلومات، هيئة التحرير، مجلة المعلوماتية، الجمعية العلمية السورية للمعلومات، عدد ١٢، شباط، ٢٠٠٧م، متاح على الرابط: www.infomag.news.sy.
- د. فراس طحان، الإرهاب الإلكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٧، العدد الثاني،٢٠١١م.
- د. فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصالات الجديدة. دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٠، العدد ٣٩، الرياض، المملكة العربية السعودية، محرم ١٤٢٦هـ–فبراير ٢٠٠٥م.
- د. منال مروان منجد، المواجهة الجنائية لجرائم الإرهاب في القانون السوري دراسة تحليلية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٣٠، العدد الثاني، ٢٠١٤م.
- د. نايف بن محمد المرواني، تمويل الإرهاب إلكترونياً التحديات وطرق المواجهة، التجربة السعودية، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٩، العدد ٥٨، الرياض، المملكة العربية السعودية، محرم ١٤٣٥هـ، نوفمبر/ديسمبر ٢٠١٣م.

هـ-النصوص القانونية والاتفاقيات الدولية

- المرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، سورية.
- التعليمات التنفيذية، للمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢م، قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، القرار رقم /٢٩٠/ أيار ٢٠١٢م، سورية.
- القانون رقم /١٩/ لعام ٢٠١٢م، قانون مكافحة الإرهاب، سورية.
- نظام مكافحة الجرائم المعلوماتية، المملكة العربية السعودية، رقم م/١٧ ١٤٢٨هـ، ٢٠٠٧/٣/٢٥م.
- قانون اتحادي رقم ٢٠١٤/٥م لمكافحة جرائم تقنية المعلومات، الإمارات العربية المتحدة.
- قانون اتحادي رقم ٢٠٠٤/١م لمكافحة الجريمة الإرهابية، الإمارات العربية المتحدة.
- القانون رقم ٠٣-٠٧ لعام ٢٠٠٣م الخاص بالجرائم المتعلقة بنظام المعالجة الألية للمعطيات، المغرب.
- والقانون رقم ٠٣-٠٣ لعام ٢٠٠٣م المتعلق بمكافحة الإرهاب، المغرب.
- قانون جرائم أنظمة المعلومات رقم /٣٠/ لسنة ٢٠١٠م. الأردن.
- الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة في ٢٢ نيسان لعام ١٩٩٨م.
- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣م.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١م.
- وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليج العربية لعام ٢٠١٣م.
- اتفاقية بودابست لعام ٢٠٠١م، اتفاقية تختص بالجرائم الإلكترونية ودخلت حيز التنفيذ عام ٢٠٠٤م.

و-المواقع الإلكترونية

- الأمم المتحدة في مواجهة الإرهاب، الصكوك الدولية لمكافحة الإرهاب، الموقع الرسمي للأمم المتحدة، متاح على الرابط: www.un.org/ar/terrorism/instuments.shtml، تاريخ الزيارة: ٢٠١٣/٩/١١م.

ثانياً: المراجع باللغة الفرنسية

- Patrick chambet,le cyber-terrorisme, DISPONIBLE SUR LE LIN: www.chambet.com/publications/ le cyber-terrorisme.pdf, Date de la visite: ١٢/٤/٢٠١٥.
- Cyberterrorisme, DISPONIBLE SUR LE LIN: htts:fr.wikipedia.org/wiki/cyberterrorisme, Date de la visite: ١١/٥/٢٠١٥.

الفهرس

الموضوع	الصفحة
المقدمة	١
أولاً: مشكلة البحث	٧
ثانياً: أهمية البحث	٨
ثالثاً: أهداف البحث	٩
رابعاً: منهجية البحث	١٠
الفصل الأول **ماهية الإرهاب بالوسائل الإلكترونية**	١٣
المبحث الأول **الإطار العام للإرهاب بالوسائل** الإلكترونية	١٦
المطلب الأول **تعريف الإرهاب بالوسائل الإلكترونية**	١٧
الفرع الأول **تعريف المصطلحات**	١٧
أولاً: البيئة الإلكترونية أو **العالم الافتراضي**	١٧

ثانياً: الجريمة المعلوماتية (الإلكترونية)	٢٠
ثالثاً: الإرهاب	٢٤
رابعاً: الإرهاب بالوسائل الإلكترونية	٢٦
الفرع الثاني تصنيف الإرهاب بالوسائل الإلكترونية وميزاته	٣٤
أولاً: تصنيف الإرهاب بالوسائل الإلكترونية	٣٤
ثانياً: خصائص الإرهاب بالوسائل الإلكترونية	٣٦
ثالثاً: خطر الإرهاب بالوسائل الإلكتروني	٣٨
المطلب الثاني مظاهر الإرهاب بالوسائل الإلكترونية	٤١
الفرع الأول أشكال الإرهاب بالوسائل الإلكترونية	٤١
أولاً: إنشاء المواقع الإلكترونية الإرهابية	٤١
ثانياُ: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية	٤٣
ثالثاً: نشر وتبادل المعلومات الإرهابية من خلال شبكة المعلومات	٤٥
رابعاً: التهديد الإلكتروني	٥١
خامساً: التجسس الإلكتروني	٥٢

الفرع الثاني **النماذج التطبيقية للإرهاب بالوسائل الإلكترونية**	٥٣
أولاً: الهجوم على الأهداف العسكرية والسياسية	٥٤
ثانياً: الهجوم على الأهداف الاقتصادية والمالية	٥٦
ثالثاً: استهداف محطات توليد الطاقة والماء	٥٦
رابعاً: استهداف نظم المواصلات	٥٧
خامساً: استهداف نظم الاتصالات	٥٨
المبحث الثاني **الإطار القانوني للإرهاب بالوسائل الإلكترونية (الإرهاب الإلكتروني)**	٥٩
المطلب الأول **قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية**	٦١
الفرع الأول **الجرائم المستحدثة**	٦٣
أولاً: الدخول غير المشروع إلى منظومة معلوماتية	٦٤
ثانياً: إعاقة الوصول إلى الخدمة	٦٨
ثالثاً: اعتراض المعلومات	٦٩
رابعاً: تصميم البرمجيات الخبيثة واستخدامها	٧٣

الفرع الثاني **الجرائم الاعتيادية (التقليدية)**	٧٧
أولاً: تطبيق القوانين الجزائية	٧٨
ثانياً: الأعمال الدعائية والتحريض على ارتكاب الجرائم	٨١
المطلب الثاني **قانون مكافحة الإرهاب**	٨٥
الفرع الأول **جريمة العمل الإرهابي**	٨٦
أولاً: أركان الجريمة الإرهابية	٨٧
ثانياً: عقوبة جريمة العمل الإرهابي	٩١
الفرع الثاني **الجرائم المستحدثة في قانون مكافحة الإرهاب**	٩٢
أولاً: المنظمة الإرهابية	٩٢
ثانياً: تمويل الإرهاب	٩٥
ثالثاً: التدريب على الأعمال الإرهابية	٩٨
رابعاً: وسائل الإرهاب	١٠٠
خامساً: التهديد بعمل إرهابي	١٠٢

سادساً: الترويج للأعمال إرهابية	١٠٥
الفصل الثاني مكافحة الإرهاب بالوسائل الإلكترونية	١٠٩
المبحث الأول مكافحة الإرهاب بالوسائل الإلكترونية تشريعياً	١١٢
المطلب الأول الإرهاب بالوسائل الإلكترونية في التشريعات الوطنية	١١٢
الفرع الأول الإرهاب بالوسائل الإلكترونية في تشريعات الدول العربية	١١٤
أولاً: الإرهاب بالوسائل الإلكترونية في تشريع المملكة العربية السعودية	١١٥
ثانياً: الإرهاب بالوسائل الإلكترونية في تشريع الإمارات العربية المتحدة	١٢٤
ثالثاً: الإرهاب بالوسائل الإلكترونية في القانون المغربي	١٢٩
رابعاً: الإرهاب بالوسائل الإلكترونية في القانون الأردني	١٣٤
الفرع الثاني الإرهاب بالوسائل الإلكترونية في تشريعات الدول الأجنبية	١٣٨
أولاً: الولايات المتحدة الأمريكية	١٣٨
ثانياً: بريطانيا	١٤٠

ثالثاً: فرنسا	١٤١
المطلب الثاني **الآليات الدولية لمكافحة الإرهاب بالوسائل الإلكترونية**	١٤٤
الفرع الأول **الاتفاقيات الدولية**	١٤٤
أولاً: على المستوى العربي	١٤٦
١-الاتفاقية العربية لمكافحة الإرهاب لعام ١٩٩٨م	١٤٧
٢-قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام ٢٠٠٣م.	١٤٩
٣-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١م	١٥٠
٤_ وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليج العربية لعام ٢٠١٣م	١٥٣
ثانياً: على المستوى الدولي	١٥٤
الفرع الثاني **التعاون الدولي في مجال مكافحة الإرهاب بالوسائل الإلكترونية**	١٥٨
المبحث الثاني **مكافحة الإرهاب بالوسائل الإلكترونية فنياً**	١٦١

المطلب الأول **إجراءات الحماية الفنية الأساسية**	١٦٣
الفرع الأول **التدريب والتوعية**	١٦٣
أولاً: التدريب	١٦٤
ثانياُ: إنشاء مواقع التوعية	١٦٤
ثالثاً: تفعيل دور الإعلام	١٦٦
الفرع الثاني **تفعيل المراقبة الإلكترونية وأنظمة الحجب**	١٦٧
أولاً: المراقبة الإلكترونية	١٦٧
ثانياً: أنظمة الحجب	١٦٩
المطلب الثاني **أنظمة الحماية الفنية من الاعتداءات الإلكترونية**	١٧٤
الفرع الأول **نظام التحقق من الهوية**	١٧٥
الفرع الثاني **خدمات الأدلة**	١٧٦
الفرع الثالث **استخدام التشفير لحماية المعلومات الهامة**	١٧٦

الفرع الرابع **الجدار الناري**	١٧٨
الفرع الخامس **الشبكات الافتراضية الخاصة**	١٧٩
الخاتمة	١٨١
أولاً: النتائج	١٨٢
ثانياً: التوصيات	١٩٠
ثالثاً: الاقتراحات	١٩٥
مراجع البحث	٢٠١
الفهرس	٢١٩