" جرائم الإرهاب الإلكتروني كأحد جرائم السلم الاجتماعي وسبل مواجهتها "

تحت إشراف

السيد الأستاذ الدكتور / أكمل يوسف السعيد

أستاذ القانون الجنائى المساعد

كلية الحقوق – جامعة المنصورة

الباحث / طه صباح المحمودى

مسجل دكتوراه بقسم القانون الجنائى

كلية الحقوق جامعة المنصورة

المقدمة

مما لا شك فيه أن العالم اليوم يشهد تطوراً هائلاً في وسائل الاتصالات وتقنية المعلومات؛ حتى أصبح يطلق على هذا العصر (عصر الثورة المعلوماتية)، ذلك لان التغيرات السريعة المترتبة على التقدم العلمي والتقني شملت معظم جوانب الحياة، وكانت اشبه ما تكون بالثورة في حياة البشرية.

لقد ترتب على هذه الثورة الكبيرة والطفرة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات بروز مصطلح الارهاب الالكتروني (الارهاب الرقمي) وشيوع استخدامه، وزيادة خطورة الجرائم الارهابية وتعقيدها، سواء من حيث تسهيل الاتصال بين الجماعات الارهابية وتنسيق عملياتها، وهو الأمر الذي دعا ثلاثين دولة الى التوقيع على أول اتفاقية دولية لمكافحة الاجرام المعلوماتي في العاصمة المجرية بودابست عام ٢٠٠١م، عقب الهجمات الارهابية التي تعرضت لها الولايات المتحدة الامريكية في الحادي عشر من سبتمبر من العام نفسه، وفي ظل أجواء ترقب وتحسب دوليين من هجمات إرهابية متوقعة[١].

يعد "الإرهاب الإلكتروني" أو كما يسميه البعض "الإرهاب المعلوماتي" أو "الإرهاب السيبراني". الذي يقابله في اللغة الفرنسية مصطلح "Le Cyberterrorisme" من أخطر جرائم الفضاء الإلكتروني المعاصرة، التي أصبحت تشكل تهديداً حقيقياً على أمن واستقرار المجتمع الدولي برمته نتيجة توظيف المنظمات الإرهابية لتقنية المعلومات في تنفيذ مخططاتها الإرهابية ونشر أفكار التطرف والكراهية والتحريض على القتل والتخريب وتجنيد الإرهابيين وتمويل أعمالها الإرهابية بل والأخطر من ذلك سعي هذه المنظمات لاختراق النظم المعلوماتية للأجهزة الأمنية ومختلف المؤسسات الاقتصادية والمرافق الإدارية من أجل إتلاف أو تعديل أو تغيير البيانات التي تحتويها أو التحكم عن بعد في أسلحة الدمار الشامل[٢].

وفي ظل تنامي المخاطر الأمنية والاقتصادية والفكرية لجرائم البيئة الرقمية في الدول العربية، وقصور تشريعاتها الجنائية في مواجهة هذا النمط من الإجرام العابر للحدود الوطنية وافق وزراء الداخلية ووزراء العدل العرب في اجتماعهما المشترك في ٢١ ديسمبر ٢٠١٠ بمدينة القاهرة على الاتفاقية العربية

---

(١) Daniel Ventre, Cyberattaque et cyberdéfense. Paris ; La Voisier, 2011, p158.

(٢) د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، مجلة العلوم القانونية والسياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد ٩، العدد ٣، ٢٠١٨، ص٧٧.

لمكافحة جرائم تقنية المعلومات من أجل توحيد السياسة الجنائية لحماية المجتمع العربي من خطر وآثار هذه الجرائم بما فيها جريمة الإرهاب الإلكتروني.

إشكالية البحث

لقد أضحت مواقع التنظيمات الإرهابية مصدراً لهجمات إلكترونية يصعب صدها، ويكمن الإشكال فيما يتعلق بالإرهاب الإلكتروني، في صعوبة التنبؤ بما يستجد من صوره ومساراته، ومن ثم صعوبة مكافحته، إذ يصعب عملياً مراقبة كل المواقع الإلكترونية عبر العالم وحجب المواقع ذات النزعة الإرهابية.

لذا تثور مشكلة البحث حول بيان ما مفهوم جريمة الإرهاب الإلكتروني وما هي أركانها وصورها ؟ وصولاً إلى توضيح ما هي الجهود الدولية والإقليمية المبذولة في مكافحة هذه الجريمة ؟.

أهمية البحث.

يهتم هذا البحث بدراسة الإرهاب الإلكتروني الذي أضحى اليوم ظاهرة عالمية خطيرة، ولا يخفى ما تشكله هذه الآفة من خطورة على السلم الاجتماعي والأمن الفكري، فإذا كان الإرهاب التقليدي لا يعترف بالحدود الدولية بالنسبة للأضرار التي يسببها، فإن الإرهاب الإلكتروني يحقق انتشاراً أوسع على مستوى العالم نظراً لاعتماده على الإنترنت ووسائل الاتصال الحديثة. فجاءت هذه الدراسة لإلقاء الضوء على خطورة الإرهاب الإلكتروني الذي يعتبر وليد التطور التكنولوجي الذي نعيشه اليوم، ومحاولة إيجاد مفهوم واضح للإرهاب الإلكتروني وصوره وسبل مواجهته.

منهجية البحث.

اتبعنا المنهج التحليلي والمنهج الوصفي، من خلال وصف الآراء الفقهية والنصوص القانونية الوطنية والدولية ذات العلاقة بموضوع الدراسة ومن ثم القيام بتحليلها وإبداء وجهة النظر حولها.

خطة البحث.

نتناول هذا البحث من خلال مبحثين متتاليين، الأول بعنوان ماهية جريمة الارهاب الالكتروني وأركانها، والثاني بعنوان جهود المنظمات الدولية والإقليمية في مكافحة الإرهاب الإلكتروني.

المبحث الأول

ماهية جريمة الإرهاب الإلكتروني وأركانها

يعتبر الإرهاب الإلكتروني أحد أخطر أشكال الإرهاب الدولي المعاصر، نظراً لتعدد وتنوع جرائمه وسهولة ارتكابها وصعوبة البحث والتحري عنها في عالم افتراضي جعل العالم بمساحته الشاسعة رقعة جغرافية صغيرة لا تعترف بالحدود السياسية للدول.

لذلك سنتطرق الى بيان تعريف هذه الظاهرة ومن ثم أركان جريمة الإرهاب الإلكتروني وصورها، وذلك من خلال المطالب التالية: –

المطلب الأول

مفهوم الارهاب الالكتروني

لقد تعددت تعاريف الارهاب واختلفت وتباينت في شأنه الاجتهادات. ولم يصل المجتمع الدولي حتى الان الى تعريف جامع مانع متفق عليه للارهاب، ويرجع ذلك إلى تنوع اشكاله ومظاهره، وتعدد اساليبه وانماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله وتباين العقائد والايديولوجيات التي تعتنقها الدول تجاهه[٣]، فما يراه البعض أرهاباً يراه الآخر عملاً مشروعاً.

وعلى أساس ذلك، نتناول هذا المطلب من خلال الفروع التالية: –

الفرع الأول

مشكلة تعريف الإرهاب

لقد انقسم فقهاء القانون حول مسألة تعريف الإرهاب إلى اتجاهين اتجاه يرفض أنصاره تعريف هذه الظاهرة، مستندين في ذلك إلى عدة حجج، بينما يرى أنصار الاتجاه الثاني أن تعريف الإرهاب أمر حتمي لتمييزه عن باقي ظواهر العنف المشابهة له، وهذا ما سيتم تفصيله فيما سيتبع.

---

[٣] د. أمل يازجي، الإرهاب الدولي والنظام العالمي الراهن، دار الفكر، دمشق، ٢٠٠٢، ص١٢.

أولاً: الاتجاه الفقهي الرافض لتعريف الإرهاب: يرى أنصار هذا المذهب أن الإرهاب غير قابل للتعريف وحجتهم ذلك أن أي محاولة لتعريفه لن تكون ملمة بكل أشكاله وأساليبه[٤]، وأن أي تعريف لهذه الظاهرة إما أن يكون عاماً يحتاج إلى تفسيرات أخرى أو يكون حصريا يشمل مجموعة من الجرائم الإرهابية، فيكون بذلك جامدا لا يستطيع مواكبة التطور المستمر لأشكال وأساليب الإرهاب[٥].

كما أسس أنصار هذا المذهب رأيهم في رفض تعريف الإرهاب على اختلاف وجهات النظر الفكرية والسياسية والعقائدية للمهتمين بدراسة هذه الظاهرة، التي أصبح يفسرها كل واحد من الجهة أو الزاوية التي تخدم مصالحه، وأن الدخول في موضوع تعريف الإرهاب يعتبر من المسائل غير المجدية في الفقه القانوني، مادام مفهومه غير مستقرا في الأذهان[٦].

وفي هذا الصدد يرى الفقيه "ولتر" لكور" "Walter Laqueur" بأنه لا يوجد حاليا تعريف للإرهاب ولا يمكن تعريفه في المستقبل، ويقول في هذا الشأن أيضا الفقيه دنبال ستيفن" "Daniel Stephen" "إني لن أحاول تعريف الإرهاب لاعتقادي بأن مناقشة التعريف لن تحقق تقدما في دراسة المشكلة التي تتعامل معها"[٧]. وقد تأثرت أيضا بهذا المذهب العديد من الدول المشاركة في المؤتمر الثامن المتعلق بمنع الجريمة ومعالجة المجرمين، المنعقد بهافانا سنة ١٩٩٠ والمؤتمر التاسع المنعقد بالقاهرة سنة ١٩٩٥، بتركيزها على ضرورة تعزيز التعاون الدولي لمكافحة الإرهاب والبحث في أسبابه والعمل على إيجاد السبل الكفيلة والفعالة لمعالجتها عوض تضييع الوقت في مشكلة تعريف الإرهاب[٨].

ثانياً: الاتجاه الفقهي المؤيد لتعريف الإرهاب: على عكس الاتجاه الفقهي الرافض لتعريف الإرهاب يرى أنصار هذا الاتجاه كما أشرنا إليه سابقا بضرورة تعريف الإرهاب لوضع الحدود الفاصلة بينه وبين ظواهر

)4(Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p166.

[٥] د. نادية شرايرية، إشكالية تعريف الإرهاب في القانون الدولي، مجلة التواصل في العلوم الاجتماعية والإنسانية، جامعة باجي مختار، بجاية، الجزائر، المجلد ١٩، العدد ٢، ٢٠١٣، ص١٥٣.

[٦] د. أسامة حسين محيي الدين، جرائم الإرهاب على المستوى الدولي، المكتب العربي الحديث، الإسكندرية، ٢٠٠٩، ص٥٧.

)7(Gabriel Weimann, Terror on the Internet, United States Institute of Peace, Washington, April 2006, P.12.

[٨] د. إمام حسنين عطا الله، الإرهاب والبنيان القانوني للجريمة، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٥، ص١٠٤.

العنف الأخرى التي يتقاطع معها في العديد من الخصائص. فقد عرف الفقيه "توم مالكيسون" " Tom Malkison" الإرهاب بأنه "الاستعمال المنسق للعنف أو التهديد به من أجل بلوغ أهداف سياسية"[٩]. وما يؤخذ على هذا التعريف أنه يحصر مفهوم الإرهاب في استعمال العنف من أجل تحقيق أهداف سياسية فقط، بينما أهداف الإرهاب قد تكون سياسية أو اقتصادية أو اجتماعية أو عقائدية أو إعلامية من أجل لفت انتباه الرأي العام الداخلي والعالمي... إلخ[١٠].

وعرفه الفقيه "إريك دافيد Eric David" بأنه "عمل من أعمال العنف المسلح الذي يرتكب التحقيق أهداف سياسية أو فلسفية أو إيديولوجية أو دينية وهو كل اعتداء على الأرواح والأموال والممتلكات العامة أو الخاصة بالمخالفة لأحكام القانون الدولي العام بما في ذلك الأحكام الأساسية المحكمة العدل الدولية أو هو الاستخدام غير المشروع للعنف أو التهديد بواسطة مجموعة أو دولة ضد فرد أو جماعة أو دولة بنتج عنه رعب يعرض للخطر أرواحا بشرية أو يهدد حريات أساسية ويكون الغرض منه الضغط على الجماعة أو الدولة لكي تغير سلوكها تجاه موضوع ما"[١١].

فيما عرفه الدكتور محمود شريف بسيوني بأنه: "استراتيجية عنف محرمة دولياً تحفزها بواعث عقائدية، وتتوخى أحداث عنف مرعبة داخل شريحة خاصة من مجتمع معين لتحقيق الوصول إلى السلطة أو القيام بدعاية لمطلب أو لمظلمة بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم أو نيابة عنهم أو نيابة عن دولة من الدول"[١٢]. وقد تم الأخذ بهذا التعريف من طرف لجنة الخبراء الإقليميين التي نظمت اجتماعاتها في الأمم المتحدة في فينا من ١٤ إلى غاية ١٨ مارس ١٩٨٨، إلا أنه انتقد أيضا كونه يركز على الدوافع السياسية للإرهاب فقط، كما هو الشأن بالنسبة لتعريف الفقيه "توم مالكيسون"[١٣].

---

[٩] د. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، السليمانية، العراق، ٢٠٠٧، ص١٤.

[١٠] د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٨٠.

[11] Gabriel Weimann, Terror on the Internet, ,op.cit, p15.

[١٢] د. منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ص٣٨.

[١٣] د. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها، مرجع سابق، ص١٦.

وفي التشريع، عرف قانون الارهاب العراقي رقم ١٣ لسنة ٢٠٠٥ في المادة الأولى منه الإرهاب بأنه: (ادخال الرعب أو الخوف والفزع بين الناس أو اثارة الفوضى تحقيقا لغايات ارهابية بالممتلكات العامة أو الخاصة بغية الاخلال بالوضع الأمني أو الاستقرار الوحدة الوطنية).

كما عرفه القانون المصري للإرهاب لسنة ٢٠١٥ في المادة الثانية منه بأنه: (كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ اليه الجاني تنفيذاً لمشروع اجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وامنه للخطر إذا كان من شأن ذلك ابناء الاشخاص او إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم او أمنهم للخطر وإلحاق الضرر بالبيئة او بالاتصالات أو المواصلات أو بالأموال أو المباني أو بالاملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة او معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح).

الفرع الثاني

تعريف الإرهاب الإلكتروني

في ظل غياب تعريف موحد للإرهاب العادي، تعددت أيضا تعريفات الإرهاب الإلكتروني، فقد عرفه قاموس "لاروس" "Larousse" بأنه "مجموعة من الهجمات الخطيرة (فيروسات، فرصنة. الخ) على حواسيب شبكات وأنظمة الإعلام الآلي لمؤسسة أو هيئة ترتكب لخلق فوضى عامة بهدف بث الرعب"(١٤).

وعرفه قاموس كورد بال" "Cordial" بأنه: "مجموعة من الهجمات على شبكة الإنترنت باستخدام الفيروسات والبرامج المحرمة للبيانات"(١٥). وبإمعان النظر في هذا التعريف نجد أنه لم يحدد الهدف من الأفعال الإجرامية التي ترتكب عن طريق الإنترنت مقارنة بتعريف قاموس "لاروس"، وبذلك يخلط هذا التعريف بين الأفعال التي يرتكها قراصنة المعلوماتLes Hackersبدافع الشهرة أو من أجل تحقيق مكاسب مادية، والأفعال التي يرتكبها الإرهابيون من أجل بث الرعب والخوف بين الناس.

---

(١٤) د. إمام حسنين عطا الله، الإرهاب والبنيان القانوني للجريمة، مرجع سابق، ص١١١.

)15(Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p171.

وتجدر الإشارة إلى أن الإرهاب التقليدي ظاهرة إجرامية قديمة قدم المجتمعات البشرية، غير أن الإرهاب الإلكتروني لم يظهر إلا حديثا بقلم الخبير "باري كولين" "Barry Collin" سنة ١٩٩٦، والذي عرفه بأنه التقاء العالم المادي مع العالم الافتراضي[١٦]. ولكن ما يؤخذ على هذا التعريف أنه قد يشمل كل أنواع الإجرام المعلوماتي، في حين أن الإرهاب الإلكتروني له العديد من السمات التي تميزه عن باقي أنواع الجريمة الإلكترونية الأخرى.

فيما عرفه الدكتور أحمد فلاح العموش بأنه: "الإرهاب الناجم عن منتجات الحداثة الغربية وموجه لتدمير تلك المنجزات الحضارية والثقافية بأساليب إجرامية متطورة ويستهدف المعلومات وأنظمة وبرامج الكمبيوتر والبيانات والتي ينتج عنها ارتكاب عنف ضد أهداف مدنية والتي تقوم بها مجموعات أو عملاء سريون"[١٧]. وعرفه البعض بأنه: "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد"[١٨]. كما عرفه البعض بأنه: "هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو المعلومات المخزنة إلكترونيا من أجل الانتقام أو ابتزاز أو إجبار الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية"[١٩].

وعلى ضوء ما سبق ذكره، يمكننا تعريف الإرهاب الإلكتروني بأنه كل فعل إجرامي يرتكب ضد تقنية المعلومات أو بواسطتها لأغراض إرهابية أو التهديد بذلك من أجل تحقيق أهداف محددة: قد تكون سياسية أو اقتصادية أو اجتماعية أو عقائدية أو إعلامية للفت انتباه الرأي العام لقضية معينة.

---

[١٦] د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٨٠.

[١٧] د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مرجع سابق، ص٩٠.

[١٨] د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، ط١، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١١، ص٢١٩.

[١٩] د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص١٢٨.

المطلب الثاني

أركان جريمة الارهاب الالكتروني

لجريمة الارهاب الالكتروني ركن مادي يتمثل بالسلوك الذي يلجأ اليه الجاني عند ارتكاب الجريمة واخر معنوي يمثل توجيه الفاعل ارادته نحو السلوك المكون للركن المادي للجريمة، وتشترك جريمة الارهاب الالكتروني مع جميع الجرائم بهذين الركنين، الا ان ما يميزها هو الركن الخاص المتمثل بوسيلة ارتكبها والتي يجب أن تكون بالوسائل الالكترونية الحديثة.

وهذا ما سنبحثه في الأفرع الثلاثة التالية: –

الفرع الأول

الركن المادي

يعتبر الركن المادي في الجريمة الارهابية العنصر الأكثر عملية في قيام هذا النوع من الجرائم، فإذا كانت القاعدة العامة تبرر زجر الجريمة الارهابية لما تخلفه هذه الاخيرة من اضطرابات سواء في شكل عمل أو في شكل امتناع يتمثل الركن في اعمال ارهابية ويشير كل من الفقه والاتفاقيات الدولية على أن هذه الافعال تتجلى في تخويف المقترن بالعنف مثال: أفعال تفجيرية وتدمير منشأت العامة: وتحطيم السكك الحديدية والقتل الجماعي والخطف[٢٠]. فمعيار الارهاب ينحصر في موضوع الجريمة او الغرض الذي يبتغيه الجاني سواء كان للحصول على مغنم أو فرض مذهب سياسي أو تغيير شكل الدولة[٢١].

وفي الحالتين يمكن اعتباره ارهابا داخليا أو دوليا حسب موضوع الجريمة، إذا انصب على نظام اجتماعي وسياسي داخلي كان ارهابا داخليا، اما إذا امتد الى العلاقات الدولية فهو ارهاب دولي، وبموجب قانون الارهاب العراقي رقم ١٣ لسنة ٢٠٠٥ فأن الفعل المادي للجريمة يتكون من مجمل الافعال التي نصت عليها المادة الأولى من القانون المذكور، وتمثل هذه الأفعال: –

---

[٢٠] د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، ط١، دار النهضة العربية، القاهرة، ٢٠٠٨، ص١١٢.

[21] Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p173.

١. العنف أو التهديد الذي يهدف الى القاء الرعب بين الناس أو تعرض حياتهم وحرياتهم وأمنهم للخطر وتعريض امولهم وممتلكاتهم للتلف ايا كانت بواعثه واغراضه يقع تنفيذا لمشروع ارهابي منظم فردي أو جماعي.

٢. العلم بالعنف والتهديد على تخريب او هدم او اتلاف او اضرار عن عمد مباني او املاك عامة او مصالح حكومية أو مؤسسات أو هيئات حكومية أو دوائر الدولة والقطاع الخاص او المرافق العامة والاماكن العامة المعدة للاستخدام العام او الاجتماعات العامة لارتياد الجمهور أو مال عام ومحاولة احتلال او الاستيلاء عليه أو تعريضه للخطر أو الحيلولة دوة استعماله للغرض المعد له بباعث زعزعة الأمن والاستقرار.

٣. من نظم او تراس او تولي قيادة عصابة مسلحة ارهابية تمارس وتخطط له وكذلك الاسهام والاشتراك في هذا العمل بالعنف والتهديد على اثارة فتنة طائفية أو حرب اهلية او اقتتال طائفي وذلك بتسليح المواطنين او حملهم على تسليح بعضهم بعضا أو بالتحريض او التمويل الاعتداء بالاسلحة النارية على دوائر الجيش او الشرطة أو مراكز التطور او الدوائر الأمنية أو الاعتداء على القطاعات العسكرية الوطنية او امتداداتها او خطوط اتصالاتها او معسكراتها او قواعدها بدافع إرهابي.

٤. الاعتداء بالاسلحة النارية وبدافع ارهابي على السفارات والهيئات الدوبلوماسية في العراق كافة وكذلك المؤسسات العراقية كافة والمؤسسات والشركات العربية والاجنبية والمنظمات الدولية. الحكومية وغير الحكومية العاملة في العراق وفق اتفاق نافذ.

٥. استخدام بدوافع ارهابية اجهزة متفجرة أو حارقة مصممة لازهاق الأرواح وتمتلك القدرة على ذلك او بث الرعب بين الناس او عن طريق التفجير او اطلاقه او نشر او زرع او تفخيخ اليات او اجسام أي كان شكلها أو بتأثير المواد الكيماوية السامة أو العوامل البايلوجية او المواد المماثلة أو المواد المشعة او التوكسنات.

٦. خطف او تقييد حريات الأفراد او احتجازهم او للابتزاز المالي لاغراض ذات طابع سياسي او طائفي او قومي او ديني أو عنصر نفعي من شأنه تهديد الأمن والوحدة الوطنية والتشجيع على الارهاب[٢٢].

ويتمثل النشاط العادي الخاص بكل صورة من الصور اعلاه الركن المادي المكون لجريمة الارهاب الالكتروني على ان تكون الوسيلة المستخدمة فيها هي وسيلة الكترونية كالحاسبة الالكترونية او الهواتف الالكترونية.

---

[٢٢] المادة (٢) من قانون الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥.

ويظل القاسم المشترك للنشاط المادي الصادر عن المجرم في الجريمة الارهابية متمحور حول عنصرين رئيسيين:

أ. تعلق الفعل الارهابي بمشروع فردي أو جماعي باجتماعي صورته ترويع عامة الناس وإفزاعهم وإشاعة جو من اللاطمأنينة وألااستقرار، فأن هذا الاضطراب ومن باب الموازنة يعتذر قيامه أو تحققه على ارض الواقع العملي مالم يصدر نشاط مادي عن الفاعل الارهاب سواء بشكل خطير بالنظام العام وزعزعة الأمن العمومي[٢٣].

ب. ارتباط الغاية من هذا النشاط المادي بأشاعة الخوف والترهيب عن طريق اعتماد العنف او التهديد به، وما دام ان القانون السابق قد عدد صور الجرائم التي تعتبر ارهابية متى اقترنت بالعنصرين المشار اليهما اعلاه فأننا سنرجيء الحديث عن تجليات الركن المادي في الجريمة الارهابية الى غاية التطرق في فقرة لاحقة لهذه الصور وتناوله بالرصد والبيان والمناقشة القانونية[٢٤].

الفرع الثاني

الركن المعنوي

لا يشترط لقيام الجريمة الارهابية مجرد قيام مشروع فردي أو جماعي يستهدف المس الخطير بالنظام العام بواسطة التخويف او التهريب او العنف ولو تحققت الصور الاجرامية المنصوص عليها في هذا الشق، بل يتعين توافر عنصر العمد لدى الفاعل الإجرامي وهو ما يصطلح على تسميته بالركن المعنوي في الجريمة الارهابية، فما هو مضمون هذا الركن وماهي تجلياته ؟، يمكن القول ان القصد الجنائي عامة، يتجلى مفهومه في واقع الأمر كترجمة ميدانية للارادة التي تخالج مخيلته الفاعل الإجرامي وتتسخ بعقليته فتتحكم في توجيه نشاطه الإجرامي الذي يستهدف به بصفة ادارية وتلقائية[٢٥]، قيامه مالم يعمد الفاعل الاجرامي الى توجيه ارادته نحو تحقيق الفعل المادي للجرم المزمع اقترافه فيتمثل الركن المعنوي في قصد اشاعة الارهاب لدى شخصيات معينة أو مجموعة من الاشخاص او لدى الشعب، ويتحقق ذلك بتوفر علم

---

[٢٣] د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، مرجع سابق، ص١١٢–ص١١٣.

[24] Gabriel Weimann, Terror on the Internet, ,op.cit, p.22.

[٢٥] د. علي عسيري، الإرهاب والإنترنت، ط١، بلا دار نشر، الرياض، ٢٠٠٦، ص١٧٦.

الجاني بأن من شأنه فعله تحقيق هذا الارهاب وبأنصراف ارادته الى ذلك ويعتبر افعاله كقرينة على توفر القصد الجنائي، ولاعبرة بالبواعث اذا كانت شخصية أو سياسية أو حتى كان يعتقد الجاني حدودها في اصلاح المجتمع، أن الجريمة الارهابية لا تشد على هذا النسق وهو ما عبر عنه المشرع في المادة الأولى كانت لها علاقة عمدا ...."

والعنصر المعنوي في الجرائم الارهابية يقع عبر مستويين رئيسيين هما:

- أولهما:- توجيه المجرم الإرهابي لنشاطه الارادي من اجل واقعة مجرمة مصنفة في عداد الجرائم الإرهابية.
- اما ثانيها:- فيمثل في الاحاطة والعلم عند الجاني بواقعة الجريمة من الناحية الواقعية والقانونية[٢٦].

وعليه فأنه ينتفي القصد الجنائي لدى المجرم ولو ارتكب جريمة ارهابية في حالة عدم الاحاطة بالواقعة الجرمية نتيجة الجهل المادي حيث ينعدم لديه العلم بحقيقة الواقعة الإجرامية، كما هو الشأن بالنسبة للشخص الذي يعمد الى اخفاء أموال أو منافع مادية أخرى متحصلة من جريمة ارهابية دون أن يعلم بماهيتها أو بمصدر تحصيلها[٢٧]. رغم ان اخفاء الأشياء المتحصل عليه من جراء جريمة ارهابية يندرج ضمن التعداد القانوني للافعال الارهابية التي عددها المشرع في المادة الثانية من قانون الارهاب فأن فعله هذا وان كان يرتب في حقه مسؤولية مدنية أو جنائية، فإن رغم ذلك يتعذر وصف ما اقدم عليه بالجريمة الارهابية واخيرا تمثل لهذه الحالة بمن يعمد الى نقل اسلحة او ادوات متفجرة معباة بشكل محكم في علبة مخصصة لاغراض الخرى اعتقادا منه انه يحمل مواد غذائية او استهلاكية مروجا اياها لفائدة طالبيها.

الفرع الثالث

الركن الخاص (وسيلة ارتكاب الجريمة)

يعد هذا الركن العامل المميز لجريمة الارهاب الالكتروني عن جريمة الارهاب العادية حيث بمقتضاه فأن الجريمة لا يمكن اكتمال وصفها ان لم تتميز بوسيلتها وهذه الوسيلة لاتعدو عن كون ان الجريمة يجب ان ترتكب بأحدى الوسائل المعلوماتية الحديثة، ويعتبر الحاسوب الالكتروني الوجه الاغلب الذي ترتكب

---

[٢٦]د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مجلة القانون للبحوث القانونية، جامعة ذي قار، العراق، المجلد ١، العدد ١٣، ٢٠١٦، ص١٩.

[27] Gabriel Weimann, Terror on the Internet, ,op.cit, p.٢٣.

الجريمة من خلاله، الا انها ليست بالوسيلة الوحيدة بل من الممكن أن ترتكب بوسائل أخرى، فالعبرة في الوسيلة هو مدى كونها من الوسائل المعلوماتية (الالكترونية) [٢٨]، وبالتالي من الممكن تصور ارتكاب الجريمة بواسطة اجهزة الهاتف النقال خصوصا وان بعض هذه الاجهزة تتمتع بنفس البرامجيات الموجودة في الحواسيب الالكترونية كما ان هناك أجهزة أخرى لديها شبكات توصل خاصة بها مثل اجهزة هواتف البلاك بيري وبالتالي فأن وسيلة الجريمة لا تعدو عن كونها التقنية الالكترونية الحديثة التي لجأ اليها الجاني لارتكاب جريمته الارهابية [٢٩].

من هذا التعريف يمكننا ملاحظة أن الحاسب ما هو الا الة وليس عقلا كما يحلو للبعض تسميته العقل الالكتروني. ويمكننا ايضا ملاحظة أن جهاز الحاسوب بمفرده لا يكفي لأداء عمل مفيد ولكن الاستفادة الحقيقية تأتي من استخدام ما يسمى البرنامج والبرنامج يعد بمثابة الروح التي تبعث الحركة في الة الكومبيوتر فالكومبيوتر بدون برنامج يصبح جثة هامدة. ويطلق على البرنامج بوجه عام Software بينما يطلق على جهاز الكومبيوتر واي من ملحقاته التي يمكن رؤيتها ولمسها لفظ Hardware، ويدون هذه الوسيلة فأن الجريمة لا تعدو عن كونها جريمة ارهابية اعتيادية[٣٠].

المطلب الثالث

صور جريمة الارهاب الالكتروني

يرتبط الارهاب الالكتروني بالمستوى المتقدم للغاية الذي باتت وسائل الاتصال وتقنية المعلومات تلعبه في جميع مجالات الحياة وفي العالم بأسره، ومن خلال الانظمة الالكترونية وشبكات المعلوماتية اتخذ الارهاب ابعاد جديدة، وازدادت خطورته على المجتمعات الدولية. وينطلق الارهاب الالكتروني من عالمين: العالم المادي (physical world) والعالم الافتراضي (Virtual World) والذي من خلاله تتم عمليات

---

(28) Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p177.

[٢٩] د. عبد الرحمن المسند، وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ج١، الرياض، ٢٠٠٤، ص٢٢٢–ص٢٢٣.

[٣٠] د. علي عسيري، الإرهاب والإنترنت، مرجع سابق، ص١٨١.

الارهاب الالكتروني والتدمير والتخريب ويشير العالم المادي الى قضايا وظواهر متعددة منها[٣١]: الطاقة، والضوء، والظلام. البرودة والحرارة، وجميع الأمور المادية والحيز الذي يعيش فيه المجتمع، ويمارس الوظائف والادوار من خلاله، اما العالم الافتراضي فيشير الى التمثيل الرمزي والمجازي للمعلومات، وهو المكان الذي تعمل به البرامج والانظمة الالكترونية تنتقل فيه البيانات.

ولعل ابرز صور الارهاب الالكتروني نتناولها في الفروع التالية: –

الفرع الأول

تبادل المعلومات الارهابية ونشرها من خلال شبكة المعلوماتية

اذا كان التقاء الارهابيين والمجرمين في مكان معين لتعلم طرق الاجرام والإرهاب وتبادل الآراء والأفكار والمعلومات صعباً في الواقع، فأنه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيراً، اذ يمكن ان يلتقي عدة اشخاص في اماكن متعددة وفي زمن معين، ويتبادلون الحديث والاستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم اتباعا وانصارا غير نشر افكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الالكتروني[٣٢]، على الرغم من أن البريد الالكتروني (E-mail) اصبح من اكثر الوسائل استخداما في مختلف القطاعات، وخاصة قطاع الاعمال: لكونه أكثر سهولة وامنا وسرعة لايصال الرسائل ؛ الا انه يعد من اعظم الوسائل المستخدمة في الأرهاب الالكتروني[٣٣]، وذلك من خلال استخدام البريد الالكتروني في التواصل بين الارهابيين وتبادل المعلومات فيما بينهم، بل أن كثيراً من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين في العمليات الارهابية والمخططين لها[٣٤]، يقوم الارهابيين كذلك باستغلال البريد الالكتروني والاستفادة منه في نشر افكارهم والترويج لها، والسعي لتكثير الاتباع والمتعاطفين معهم عبر الرسائل الالكترونية فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الارهابية نشر افكارها المتطرفة،

---

(٣١) د. عبد الرحمن المسند، وسائل الإرهاب الإلكتروني، مرجع سابق، ص٢٢٧.

(32) Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p184.

(٣٣) د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٢.

(٣٤) د. عبد الرحمن المسند، وسائل الإرهاب الإلكتروني، مرجع سابق، ص٢٢٨.

والدعوى الى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من اجل تحقيق اغراضهم غير المشروعة والتي تتعارض مع مصلحة المجتمع[٣٥].

ويستخدم الارهابيون الشبكة العلمية للمعلومات (Internet) بشكل يومي لنشر افكارهم الهادمة وتحقيق اهدافهم السيئة ومن الممكن ابراز أهم استخداماتهم للشبكة فيما يلي: [٣٦]

١. الاتصال والتخفي: تستخدم الجماعات والمنظمات الارهاربية المختلفة الشبكة عالمية للمعلومات في الاتصال والتنسيق فيما بينهم، نظرا لقلة تكاليف الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للارهابيين فرصة ثمينة في الاتصال والتخفي[٣٧]، وذلك عن طريق البريد الالكتروني أو المواقع والمنتديات وغرف الحوار الالكتروني، حيث يمكن وضع وسائل مشفرة تأخذ طابعا لا يلفت الانتباه، من دون ان يضطر الارهابي الى الافصاح عن هويته كما انها لاتترك اثرا واضح يمكن ان يدل عليه[٣٨].

٢. جمع المعلومات الارهابية: تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما انها تعتبر موسوعة الكترونية شاملة متعددة الثقافات ومتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الارهابيون للحصول عليها، كمواقع المنشأة النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية، والمعلومات المختصة بسبل مكافحة الارهاب، ونحو ذلك من المعلومات التي تعتبر بمثابة الكنز الثمين بالنسبة للارهابيين نظراً لما تحتويه من معلومات تفصيلية مدعمة بالصورة الضوئية[٣٩].

٣. التخطيط والتنسيق للعمليات الارهابية: العمليات الارهابية عمل على جانب من التعقيد والصعوبة، فهي تحتاج الى تخطيط محكم، وتنسيق شامل، تعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة

)35(Gabriel Weimann, Terror on the Internet, ,op.cit, p.١٨.

(٣٦) أنظر تفصيلاً: د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، مرجع سابق، ص١٢١–ص١٢٤.

)37(Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p201.

(٣٨) د. علي عسيري، الإرهاب والإنترنت، مرجع سابق، ص١٦٣.

(٣٩) د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٣.

الأهمية للجماعات الاهابية، حيث تتيح لهم هوية التخطيط الدقيق والتنسيق الشامل لشن الهجمات الارهابية المحددة في جو مريح، وبعيدا عن اعين الناظرين مما يسهل على الارهابيين ترتيب تحركاتهم، وتوقيت هجماتهم(٤٠).

٤. التعبئة وتجنيد الارهابيين: تستخدم الجماعات والمنظمات الارهابية الشبكة المعلوماتية العالمية في نشر ثقافة الارهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي به، كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الارهابيين في تبني افكارها ومبادئها(٤١).

الفرع الثاني

إنشاء المواقع الإرهابية الإلكترونية

يقوم الإرهابيون بأنشاء وتصميم مواقع لهم عن طريق الشبكة العالمية للمعلومات (Internet) لبث أفكارهم الضالة، والدعوة الى مبادئهم المنحرفة، ولابراز قوة التنظيم الارهابي، وللتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الالكتروني، وللتدريب الالكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات ارهابية، فقد انشأت مواقع ارهابية الكترونية لبيان كيفية صناعة القنابل والمتفجرات، والاسلحة الكيمياوية الفتاكة، والشرح طرق اختراق البريد الالكتروني وكيفية اختراق وتدمير المواقع الالكترونية، والدخول الى المواقع المحجوبة، لتعليم طرق نشر الفيروسات ونحو ذلك(٤٢).

واذا كان الحصول على مواقع افتراضية او وسائل اعلامية كالقنوات التلفزيونية والاذاعية صعبا بالنسبة للارهابيين، فأن انشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات (Internet) لخدمة اهدافهم ترويج افكارهم الضالة اصبح سهلا وممكننا، ولذا فأن معظم التنظيمات الارهابية لها مواقع الكترونية، وهي بمثابة مقر افتراضي لها(٤٣).

---

(٤٠) د. عبد الرحمن المسند، وسائل الإرهاب الإلكتروني، مرجع سابق، ص٢٣٠.

(٤١) د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٤.

(42) Gabriel Weimann, Terror on the Internet, ,op.cit, p.206.

(43) Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p158.

وتتم عملية اختراق النظم المعلوماتية في غالب الأحيان عن طريق الأفعال التالية:

أ. التسلل: يشمل هذا الفعل كل الاختراقات للمواقع الرسمية للمؤسسات الحكومية أو المواقع الشخصية أو اختراق البريد الإلكتروني أو الاستيلاء على الأرقام السرية للمستخدمين. وتتم هذه العملية عن طريق تشغيل برنامج إلكتروني صغير يعرف باسم "حصان طروادة" في الحاسب الآلي للتجسس على كل ما يقوم به صاحبه، حيث يقوم هذا البرنامج بتسجيل كل بياناته السرية كرقم بطاقة الائتمان الخاصة به والمكالمات التي يجريها مع غيره بواسطة هذا الحاسوب بل وحتى كلمات السر التي يستعملها للدخول للإنترنت التي تمكن المجرم المعلوماتي من استخدامها. ومن أبرز الأمثلة على هذه العمليات في العالم. قيام مراهقين بالتسلل إلى الصفحة العنكبوتية للقواعد العسكرية للولايات المتحدة الأمريكية أثناء حرب الخليج مما أرعب الحكومة الأمريكية التي اعتقدت في بداية الأمر أنها تعرضت لعمل إرهابي[٤٤].

ب. الإغراق بالرسائل الإلكترونية: تتم هذه العملية عن طريق إرسال عدد كبير من الرسائل الإلكترونية ذات الحجم الكبير غير المفيدة دفعة واحدة وفي وقت متقارب قصد التأثير على السعة التخزينية للحواسيب الآلية المستهدف، مما يؤدي إلى توقفها عن العمل بسبب امتلاء منافذ الاتصال وكذا قوائم الانتظار، الأمر الذي ينتج عنه انقطاع الخدمة التي توفرها هذه الحواسيب[٤٥].

ج. نشر الفيروسات الإلكترونية: يقصد بالفيروسات الإلكترونية برامج خارجية صنعت عمدا بغرض تغيير خصائص الملفات التي تصيبها، لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات الغرض منها إلحاق الضرر بحاسوب أو السيطرة عليه[٤٦]. وقد سميت هذه البرامج الإلكترونية بهذا الاسم، نظرا لتشابيها الكبير مع لفيروسات البيولوجية من حيث الانتقال والانتشار والقوة التدميرية، وقدرتها على تعديل مختلف البرامج، واستطاعتها التمييز بين البرامج السليمة والبرامج المصابة بالفيروس[٤٧].

---

[٤٤] د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية، مرجع سابق، ص٢٠٢.

[٤٥] د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٨٥.

[٤٦] د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مرجع سابق، ص١١٢.

[47] Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p211-p212.

الفرع الثالث

تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية

تقوم التنظيمات الارهابية بشن هجمات الكترونية من خلال الشبكات المعلوماتية، يقصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية، والحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الارهابية في عصر المعلومات ثلاثة اهداف اساسية غالبا، وهي الاهداف العسكرية والسياسية والاقتصادية[٤٨] في عصر ثورة المعلومات تجد الاهداف الثلاثة نفسها، وعلى رأسها مراكز القيادة والتحكم العسكري، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والاسواق المالية، وذلك لاخضاع ارادة الشعوب والمجتمعات الدولية المقصود بالتدمير هنا: الدخول غير المشروع على نقطة ارتباط اساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام الي (Server) او مجموعة نظم مترابطة شبكيا (Internet)بهدف تخريب نقطة الاتصال او النظام[٤٩].

أما جريمة تدمير أنظمة المعلومات، يقصد بها الدخول العمدي إلى الأنظمة المعلوماتية سواء كان النظام محميا أو غير محمي، وسواء مرتبط بأجهزة أخرى أو غير مرتبط وذلك بهدف الحصول على معلومات أو يهدف تحقيق الضرر من خلال فصخ المعطيات المعلوماتية أو اتلافها أو تعديلها أو إعدامها[٥٠]. وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول دون تدمير المواقع او اختراقها بشكل دائم، فالمتغيرات التقنية، والمام المخترق بالثغرات في التطبيقات التي بينت في معظمها على اساس التصميم المفتوح ولمعظم الاجزاء (source open)، سواء كان ذلك في مكونات نقطة الاتصال او في النظم أو في الشبكة او في البرمجة، جعلت الحيلولة دون الاختراقات صعبة جدا، بالاضافة الى ان هناك منظمات ارهابية

---

[٤٨] د. علي عسيري، الإرهاب والإنترنت، مرجع سابق، ص١٦٧.

[٤٩] د. إمام حسنين عطا، البنيان القانوني لجريمة الإرهاب، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٤، ص٦٩.

[٥٠] د. حسين بن سعيد الظافري، السياسة الحديثة في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٣٧٨.

يدخل من ضمنها عملها ومسؤلياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الامكانات والقدرات ما ليس لدى الافراد[٥١].

ويستطيع قراصنة الحاسب الالي (Hackers) التوصل الى المعلومات السرية والشخصية، واختراق خصوصية سرية المعلومات بسهولة، وذلك يرجع الى ان التطور المذهل في عالم الحاسب الالي والشبكات المعلوماتية يصحبه تقدم اعظم في الجرائم المعلوماتية وسبل ارتكابها، ولاسيما أن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الالي[٥٢]. وإن عملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة وبرامج شبكة الانترنيت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا اهمية له في الحد من الاختراقات المعلوماتية، ولاتزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الالي والشبكات المعلوماتية[٥٣].

كما يتم نشر ثقافة الارهاب من خلال تأسيس مواقع الكترونية تمثل التنظيمات الإرهابية، وكذلك من خلال صفحات التواصل الاجتماعي والتي تعتبر سوق مفتوح لترويج الفكر الإرهابي ونشره بين عامة الناس، وخلال العقد الماضي اخدت تلك المواقع بالازدياد حيث يتم من خلالها نشر المقالات والبيانات ومقاطع الفيديو التي تحتوي على تهديدات وعمليات إرهابية وتحريض على النظام السياسي. كذلك النشر الإلكتروني المتمثل في المواقع الإلكترونية وصفحات التواصل الاجتماعي، مثل Twitter و Facebook، والتي تعد أبرز الساحات التي تستعملها التنظيمات الإرهابية لنشر ثقافتها، وكذلك تشمل تطبيقات الميديا الخاصة لنشر مقاطع الفيديو مثل You Tube[٥٤].

---

(٥١) د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٦.

(52) Gabriel Weimann, Terror on the Internet, ,op.cit, p.٢٦.

(٥٣) د. إمام حسنين عطا، البنيان القانوني لجريمة الإرهاب، مرجع سابق، ص٧٢.

(54) Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p221.

الفرع الرابع

التجسس الالكتروني

يقوم الارهابيون بالتجسس على الاشخاص أو الدول او المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الالكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والانظمة الالكترونية التي جلبتنا حضارة التقنية في عصر المعلومات وتستهدف عمليات التجسس الارهابي في عصر المعلومات ثلاثة اهداف رئيسية، وهي: التجسس العسكري، التجسس السياسي، التجسس الاقتصادي[٥٥].

وفي عصر المعلومات مع وجود وسائل التقنية الحديثة فأن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الالكترونية، وخاصة مع ظهور الشبكات المعلوماتية وانتشارها عالميا، ومع توسع التجارة الالكترونية عبر الشبكة العالمية للمعلومات (Internet) تحولت مصادر المعلومات التجارية الى اهداف للتجسس الاقتصادي[٥٦].

ان محاولة اختراق الشبكات والمواقع الالكترونية من قبل العابثين من مخترقي الانظمة المعلوماتية (hackers)، لا بعد ارهابا، فمخاطر هولاء محدودة وتقتصر غالبا على العبث او اتلاف المحتويات التي يمكن التغلب عليها باستعادة نسخة أخرى مخزونة في موقع امن ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية واجهزة الاستخبارات المختلفة من اجل الحصول على أسرار ومعلومات الدولة، ومن ثم افشائها لدول اخرى معادية أو استغلالها بما يضر المصلحة العامة للوحدة الوطنية للدولة[٥٧].

وتتم عملية ارسال نظم للتجسس الالكتروني بعدة طرق ومن اشهرها البريد الالكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، من الاساليب الحديثة للتجسس الالكتروني اسلوب اخفاء المعلومات داخل المعلومات[٥٨]. ويتلخص هذا الاسلوب في لجوء المجرم الى اخفاء المعلومة الحساسة والمستهدفة داخل المعلومات الأخرى العادية داخل الحاسب الآلي، ومن ثم يجد وسيلة ما لتهريب

---

[٥٥] د. علي عسيري، الإرهاب والإنترنت، مرجع سابق، ص١٦٨–ص١٦٩.

[٥٦] د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٧.

[57] Daniel Ventre, Cyberattaque et cyberdéfense., op.cit, p.226.

[٥٨] د. علي عسيري، الإرهاب والإنترنت، مرجع سابق، ص١٧١.

تلك المعلومة العادية، ولا يشك أحد في أنّ هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً، كما قد يلجأ الى وسائل غير تقليدية للحصول على المعلومات السرية. ومما يقوم به الارهابيون من اختراق البريد االلكتروني للاخرين وهتك اسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الارهابية، أو تهديدهم لحملهم على إتيان افعال معينة يخططون لاقترافها[٥٩].

وتجدر الاشارة من قبل الباحث الى ان الطرق الفنية للتجسس المعلومات سوف تكون أكثر الطرق استخداما في المستقبل من قبل التنظيمات الارهابية، نظراً لاهمية المعلومات الخاصة بالمؤسساتوالقطاعات الحكومية، وخصوصا العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من اجل الاضرار بمصلحة المجتمع والوطن.

المبحث الثاني

جهود المنظمات الدولية والإقليمية في مكافحة الإرهاب الإلكتروني

أدركت الدول والمنظمات الدولية والإقليمية أهمية التعاون الدولي وأحست بأنه أمر ملح لمواجهة تحديات الجرائم الإلكترونية، فعمدت الكثير منها إلى عقد اتفاقيات لتسهيل مهمة التحقيق في جرائم الكمبيوتر والأرهاب الإلكتروني[٦٠]. وعلى أساس ذلك، نتناول هذا المبحث من خلال المطلبين التاليين:-

المطلب الأول

جهود المنظمات الدولية في مكافحة الإرهاب الإلكتروني

سنتناول هذا الفرع من خلال النقاط التالية:-

أولاً: جهود منظمة الأمم المتحدة: - في إطار الجهد المبذول فإن هناك العديد من الهيئات الدولية التي تلعب دوراً ملحوظاً في هذا المجال على رأسها منظمة الأمم المتحدة التي بذلت جهوداً لا يستهان بها، مؤكدة على

---

[٥٩] د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٢٧-ص٢٨.

[٦٠] د. السيد عوض، الجريمة في مجتمع متغير، مرجع سابق، ص٢٠٦.

وجوب تعزيز العمل المشترك بين أعضاء المنضمة من أجل التعاون على الحد من انتشار الجريمة المعلوماتية والإرهاب الإلكتروني، وهذا من خلال مؤتمراتها لمنع الجريمة ومعاملة المجرمين بدءاً بالمؤتمر السابع عام ١٩٨٥ إلى غاية المؤتمر الثاني عشر عام ٢٠١٠، إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات وذلك تحت إشراف الأمم المتحدة عام ١٩٩٤، الذي نتج عنه عدة توصيات و قرارات ذات صلة بالجرائم المعلوماتية، وقد تضمنت شقين اثنين واحد موضوعي بتناول الأفعال التي تقع تحت طائلة الإحرام للمعلوماتي، وثاني إجرائي يتضمن الإجراءات الواجب إتباعها لتطبيق القواعد الموضوعية[٦١].

وفيما يخص مؤثرات الأمم المتحدة في هذا المجال؛ نجد المؤتمر السابع المنعقد بميلانو عام ١٩٨٥ الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلي وإعداد تقرير يعرضه على المؤتمر الثامن، وقد عقد هذا الأخير إلى هافانا عام ١٩٩٠ وقد خرج بالعديد من التوصيات أهمها التأكيد على ضرورة الاستفادة من التطورات العلمية والتكنولوجية في مواجهة الجريمة اللاكترونية، وأشار إلى مسألة الخصوصية واختراقها بالإطلاع على البيانات الشخصية المحزنة داخل النظام المعلوماتي. كما أكد على ضرورة تحديث القوانين التي تناول هذه الجرائم وتحسين تدابير الأمن والوقاية المتعلقة بها تدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة فيها، وكذا التعاون مع المنظمات المهتمة بهذا الموضوع. كما عقد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في القاهرة عام ١٩٩٥ والذي أوصى بوجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة، كما أوصى كذلك المؤتمر العاشر المنعقد في بودابست عام ٢٠٠٠ بوجوب العمل الجاد من أجل الحد من جرائم تقنية المعلومات المتزايدة والتي اعتبرت نمطاً من الجرائم والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة[٦٢].

بالإضافة إلى مؤتمرات الأمم المتحدة؛ نذكر في هذا المجال المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في ريو دي جانيرو عام ١٩٩٤ وقد خرج بالعديد من التوصيات منها: –

– وضع قائمة بالحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبل الجرائم المعلوماتية.

---

[٦١] صباح كزيز وآمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مرجع سابق، ص٣١٦.

[٦٢] د. السيد عوض، الجريمة في مجتمع متغير، مرجع سابق، ص٢١٤–ص٢١٥.

- وجوب تحديد الجهات التي تقوم بإجراء التفتيش والضبط، وضرورة وضع القواعد المتعلقة بالإثبات الإلكتروني ومصداقية الأدلة[١].

ثانياً: الإتحاد الدولي للاتصالات: هناك جهد كبير مبذول من قبل الاتحاد الدولي للاتصالات في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبل الأمين العام للإتحاد عام ٢٠٠٧، والذي يرمي إلى تحقيق عدة أهداف أبرزها استحداث تشريع نموذجي لمكافحة الجريمة المعلوماتية يمكن تطبيقه عالميا ويكون قابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي[٢].

ثالثاً: جهود منظمة الشرطة الجنائية الدولية (الانتربول): يبرز دور الانتربول – المنظمة الشرطية– في العالم كبيراً في مكافحة الجرائم الالكترونية بما فيها الإرهاب الإلكتروني والتي يعتبرها أحد مجالات الإجرام الأسرع نمواً، نظراً للتسهيلات والسرعة التي تقدمها التقنيات الحديثة وخصائصها أي مميزات الطابع العالمي للإنترنت في إخفاء الهوية لمرتكبيها الذي يساعد على تزايد الأنشطة الإجرامية[٣]. ولقد مرت جهود المنظمة في هذا المجال مراحل عديدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا نيوي، أذريحان بيونس أيرس لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك[٤].

على مستوى الجهود الدولية أيضا صدر في عام ٢٠٠٠ مسودة اتفاق عالمي حول الجريمة والإرهاب الإلكتروني من جامعة "ستاند فورد " فيما عرف خطة ستاند فورد وحملت تلك الخطة العديد من النقاط حول هدف الوصول إلى تعاون دولي أوسع في مقاومة هجمات الفضاء الإلكتروني، وذلك على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين، وخاصة مع التطور المستمر في التكنولوجيا وجهود الأطر القانونية الحالية في مواجهة الأخطار والهجمات، وفي المادة ١٢ تلك الخطة اقترح بإقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات[٥].

---

[١] صباح كزيز وآمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مرجع سابق، ص٣١٧.

[٢] د. السيد عوض، الجريمة في مجتمع متغير، مرجع سابق، ص٢١٧.

[3] Daniel Ventre, Cyberattaque et cyberdéfense., op.cit,p244.

[٤] صباح كزيز وآمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مرجع سابق، ص٣١٧–ص٣١٨.

[٥] د. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، ص٦، تاريخ النشر ٢٠١٦/١٢/١٢، تاريخ الإطلاع ٢٠٢٣/٥/٦، منشور على الرابط الإلكتروني الآتي: –

وبعد أحداث ١١ سبتمبر ٢٠٠١ طلب من مكتب الأمم المتحدة للمخدرات والجريمة في فينا وضع ارشادات للدول عند تشريع وتطبيق وسائل محاربة الإرهاب وتنفيذاً لذلك وضع للمكتب سنة ٢٠٠٦ قائمة بالإرشادات تضمنت أربعة أقسام: الأول في الأعمال المجرمة، والثاني في الوسائل التي تضمن التجريم الفعال والثالث في القانون الإجرائي، والرابع في وسائل التعاون الدولي في المسائل الجالية، ووضع المكتب في نهاية الإرشادات مشروع قانون ضد الإرهاب[١].

المطلب الثاني

جهود المنظمات الإقليمية في مكافحة الإرهاب الإلكتروني

لعب المجلس الأوروبي دوراً مهماً في محاولة الحد من الجرائم الالكترونية والإرهاب الإلكتروني، من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الإستخدام وحماية تدفق المعلومات، وفي ١٩٨١/١/٢٨، تم توقيع اتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية. وفي عام ١٩٨٩ نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون في مواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام ١٩٩٥ حول الإجراءات الجنائية في مجال الجرائم المعلوماتية وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام ١٩٩٧ بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد تفاقية في هذا الإطار[٢].

وقد أثمرت جهود الإتحاد عن ميلاد أولى المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية والإرهاب الإلكتروني بالعاصمة المجرية بودابست عام ٢٠٠١، وقد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية بعضها البعض، وتعزيز قدرات القضاء وكذا لتحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات الجرائم المعلوماتية في إطار القوانين المحلية، وما قام به المجلس في هذا المجال هو إشرافه

---

http://repository.nauss.edu.sa/bitstream/hand

[١]د. السيد عوض، الجريمة في مجتمع متغير، المكتبة المصرية، الإسكندرية، ٢٠٠٤، ص٢٢٢.

[٢]صباح كزيز وآمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، دراسة تحليلية، مجلة التراث، الجزائر، المجلد ٨، العدد ١، ٢٠١٨، ص٣١٨.

على اتفاقية بودابست الموقعة ورغم أن هذه الاتفاقية هي في الأصل أوروبية الميلاد إلا أنها دولية المنابع، حيث أعّد مجلس أوروبا هذه الاتفاقية بالتعاون مع اليابان وجمهورية جنوب إفريقيا والولايات المتحدة الأميركية وعرضت للتوقيع في بودابست في ٢٠٠١/١١/٢٣ ودخلت حيز التنفيذ في ٢٠٠٤/٠٧/٠١، تهدف الاتفاقية إلى إرساء نظام سريع وفعال للتعاون الدولي. وبالتالي تتضمن الاتفاقية أحكاماً تهدف إلى استحداث هكذا إطار في سبيل تعاون دولي سريع وموثوق وتطلب من الدول الأطراف من بعضها البعض بمختلف أشكال التعاون[١].

وقد حددت الاتفاقية (بودابست) الجرائم الالكترونية وصنفتها في خمسة عناوين في القسم الأول من الاتفاقية:-

- العنوان الأول: ويضم جوهر جرائم الحاب أو الجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات والنظم.
- العنوان الثاني: ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.
- العنوان الثالث ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى، وهي التي تخص الإنتاج والنشر غير المشروع، في المادة التاسعة من الاتفاقية.
- العنوان الرابع: ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة العاشرة من الاتفاقية.
- العنوان الخامس: وهو يشتمل على أحكام إضافية بخصوص الشروع والاشتراك وأيضا الجزاءات والإجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية.

وفي ١١ ماي ٢٠٠٤ أصدرت دول الثمانية بيانا مشتركا صدر بعنوان مواصلة تعزيز القوانين المحلية، الذي أوصى جميع الدول أن تواصل تحسين القوانين التي تجرم اساءة استخدام الشبكات الالكترونية والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالأنترنت وفي ١٧ نوفمبر ٢٠٠٤ انعقد الاجتماع الوزاري لمنظمة الأبيك في شيلي، وصدر بيان مشترك من زعماء الابيك لتعزيز اقتصاديات الدول الأعضاء

---

[١] د. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، ص١٠، تاريخ النشر ٢٠١٦/١٢/١٢، تاريخ الإطلاع ٢٠٢٣/٥/٦، منشور على الرابط الإلكتروني الآتي: - http://repository.nauss.edu.sa/bitstream

للقدرة على مكافحة الجريمة الالكترونية والإرهاب الإلكتروني من خلال سن تشريعات محلية مما يتفق مع أحكام الصكوك القانونية الدولية بما في ذلك اتفاقية الجرائم الالكترونية[1].

المطلب الثالث

موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠

من الإرهاب الإلكتروني

لقد ألزمت الاتفاقية العربية جميع الدول الأطراف بأن تجرم في قوانينها الداخلية كل الأفعال التي نصت عليها في الفصل الثاني منها، بما في ذلك الأفعال المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وتبنيا أيضا لحزمة من التدابير الإجرائية، وكذا تعزيزها لجهود التعاون القانوني والقضائي بينها المكافحة كافة هذه الأفعال الخطيرة بصورة فعالة. ولتوضيح ذلك نتناول هذا المطلب كما يلي:-

الفرع الأول

صور الإرهاب الإلكتروني التي نصت عليها الاتفاقية العربية لمكافحة

جرائم تقنية المعلومات

بإلقاء نظرة فاحصة على المادة ١٥ من هذه الاتفاقية نجد أنها قد حضرت الإرهاب الإلكتروني ثلاث صور تتمثل الأولى في نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والنعرات والاعتداء على الديانات، والثانية في تمويل الأعمال الإرهابية والتدريب عليها. أما الثالثة فتتمثل في تسهيل الاتصال بين المنظمات الإرهابية.

أولاً: نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والاعتداء على الديانات والمعتقدات: يتميز النشر في العالم الافتراضي بالسرعة والحرية المطلقة غير المقيدة بإجراءات معينة ما عدا تلك المتعلقة

---

[1] د. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، مرجع سابق، ص١٢.

بحجز نطاق الاسم والمساحة الضرورية لدى أحد مقدمي الخدمات، على عكس النشر في العالم المادي الذي يتطلب إجراءات محددة كإيداع المصنف والالتزام باحترام النظام العام والآداب العامة .. إلخ[١].

ونظرا لسهولة النشر الإلكتروني على شبكة الإنترنت الزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف في المادة ١٥ منها بتجريم نشر فكر التطرف والغلو الذي يعتبر أحد أهم العوامل المغذية للعنف والإرهاب سواء أكان عن طرق الفتاوى المسموعة أم السمعية البصرية أو المقروءة، وطرق صناعة المتفجرات وكيفية استعمالها في الأعمال الإرهابية، وكذا نشر الفتن الطائفية والسياسية والاعتداء على الديانات بالسب والتحقير والسخرية أو غير ذلك من الأفعال التي تمس بحرية المعتقد.

وفي ظل التزايد المستمر لعدد مستخدمي الإنترنت في العالم الذين فاق عددهم ٣,٤٢ مليار مستخدما في العالم خلال سنة ٢٠١٦، لجأت المنظمات الإرهابية إلى إنشاء العديد من هذه المواقع الإلكترونية المتطرفة. فقد أحصى الخبيران في الدراسات الإعلامية فيليب سيب" و"دانا "جانبك". كتابهما الإرهاب الدولي والإعلام الجديد: ٢٠٠٠ موقعا إلكترونيا إرهابيا سنة ١٩٩٧، و٤٣٥٠ موقعا في مطلع سنة ٢٠٠٥، و٦٠٠٠ موقعا في سنة ٢٠٠٨، ليتجاوز حاليا ٦٠ ألف موقعا إلكترونيا إرهابيا[٢].

ولا يقف الأمر عند صور النشر التي عددها المادة ١٥ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بل أن المنظمات الإرهابية أصبحت تستخدم هذه التقنية أيضا لنشر فيديوهات وصور عن أبشع الجرائم التي يرتكيا الإرهابيون لبث الرعب والخوف بين الناس والظهور بمظهر القوة.

ثانياً: تمويل الأعمال الإرهابية والتدريب على ارتكابها بواسطة تقنية المعلومات: يعرف تمويل الإرهاب بأنه: "أي دعم مالي في مختلف صوره يقدم إلى الأفراد أو المنظمات التي تدعم الإرهاب أو تقوم بالتخطيط لعمليات إرهابية، وقد يأتي هذا التمويل من مصادر مشروعة كالجمعيات الخيرية مثلا أو مصادر غير مشروعة مثل تجارة البضائع التالفة أو تجارة المخدرات"[٣]. وعرفته الاتفاقية العربية لمكافحة غسيل الأموال

---

[١] د. عبد العال الديربي ود. محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢، ص٢٧٠.

[٢] د. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مرجع سابق، ص١١٤.

[٣] د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٩، ص٢٢.

وتمويل الإرهاب لعام ٢٠١٠ بأنه "جمع أو تقديم أو نقل الأموال بأي وسيلة مباشرة أو غير مباشرة لاستخدامها كليا أو جزئيا لتمويل الإرهاب وفقا لتعريفات الإرهاب الواردة في الاتفاقية العربية مع العلم بذلك".

أما عن استعمال المنظمات الإرهابية لهذه التقنية لتدريب الإرهابيين، فيمكننا القول بأن الإنترنت أصبح مركزا افتراضيا لتدريب الإرهابيين عن بعد عن كيفيات استعمال الأسلحة ومختلف أساليب القتل والعنف والتخريب والتفجير لبث الرعب والخوف بين الناس كقطع الرؤوس واختطاف الطائرات واستعمال الأحزمة الناسفة وتلغيم السيارات وزراعة المتفجرات في الأماكن العمومية، بل وحتى طرق اختراق النظم المعلوماتية للمرافق الحكومية والمؤسسات المصرفية.

ثالثاً: تسهيل الاتصال بين المنظمات الإرهابية: إلى جانب إلزام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتجريم نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والنعرات والاعتداء على الديانات وتمويل الأعمال الإرهابية والتدريب عليها ألزمتها أيضا بتجريم كل الأفعال التي من شأنها تسهيل الاتصال بين المنظمات الإرهابية عن طريق مختلف وسائل الاتصال لمنعها من تبادل الأفكار والتنسيق والتعاون بينها لتنفيذ مخططاتها الإجرامية[١].

ويبدو من الوهلة الأولى أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أغفلت تجريم العديد من الأفعال الأشد خطورة من الأفعال التي نصت علها في المادة ١٥ منها التي ترتكب بواسطة تقنية المعلومات لأغراض إرهابية كاختراق النظم المعلوماتية للأجهزة الحكومية ومختلف المؤسسات الحيوية كالمرافق النووية والمطارات ومحطات المياه والطاقة الكهربائية والتجسس الإلكتروني، وإنشاء المواقع الإلكترونية المتطرفة، واستعمال أجهزة الاتصال المحمولة لتفجير القنابل عن بعد. إلخ، غير أنه وبالرجوع إلى المادة ٢٢ من هذه الاتفاقية تجدها تلزم الدول الأطراف بتطبيق الصلاحيات والإجراءات المحددة في الفصل الثالث منها المتعلق بالأحكام الإجرائية على الجرائم التي نصت عليها في المواد من ٠٦ إلى ١٩ أو أي جريمة أخرى ترتكب بواسطة تقنية المعلومات، الأمر الذي يسوقنا للقول بأن هذه الاتفاقية وسعت من مجال تطبيق أحكامها لتشمل جميع الجرائم التي ترتكب بواسطة هذه التقنية بما في ذلك مختلف جرائم الإرهاب الإلكتروني التي لم تنص عليها المادة ١٥ منها.

---

[١] د. عبد العال الديربي ود. محمد صادق إسماعيل، الجرائم الإلكترونية، مرجع سابق، ص٢٨١.

الفرع الثاني

آليات مكافحة الإرهاب الإلكتروني التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إن مكافحة الإرهاب الإلكتروني باعتباره من أخطر الجرائم العابرة للحدود التي أصبحت تهدد الأمن المعلوماتي تقتضي تبني الدول في قوانينها الداخلية لمجموعة من الأحكام الإجرائية، وتكثيفاً لجهود التعاون القانوني والقضائي والتقني فيما بين الدول.

أولاً: الآليات الإجرائية التي نصت علها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

يمكننا إيجاز الآليات الإجرائية التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فيما يلي:

١. **الحفظ العاجل للبيانات المعلوماتية المخزنة والأمر بتسليمها:** تعرف البيانات المعلوماتية حسب هذه الاتفاقية بأنها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها. أما التحفظ العاجل للبيانات المعلوماتية: فيقصد به توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية[١].

ويعد، هذا الإجراء من أهم الإجراءات التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة ٢٣ منها التي الزمت بموجها الدولة الأطراف باتخاذ التدابير التشريعية اللازمة لما تقتضيه إجراءات التحقيق في الجريمة الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني لتمكين السلطات المختصة من توجيه الأمر لشخص بحفظ البيانات المعلوماتية المخزنة التي في حوزته أو تحت سيطرته لمدة أقصاها ٩٠ يوما تكون قابلة للتجديد خاصة إذا كانت هذه الأخيرة معرضة للفقدان أو التعديل، واتخاذ الإجراءات الضرورية التي من شأنها الحفاظ على سرية المعلومات المخزنة طيلة الفترة القانونية المنصوص عليها في قوانينها الداخلية[٢]. كما تلزم هذه الاتفاقية الدول المتعاقدة باعتماد إجراءات تستطيع من خلالها

---

[١] د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، مرجع سابق، ص١١٦.

[٢] المادة ٢٣ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

السلطات المختصة من توجيه الأمر إلى أي شخص كان على إقليمها قصد تقديم البيانات التي بحوزته سواء أكانت المخزنة في تقنية معلومات أم في دعامة تخزين كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية .. إلخ. أو إلى أي مزود خدمة لتسليم معلومات المشتركين في الخدمة المقدمة التي بحوزته أو تحت سيطرته[١].

٢. **تفتيش المعلومات المخزنة:** يعتبر تفتيش البيانات المخزنة في تقنية المعلومات أحد أهم الإجراءات للكشف عن ملابسات الجريمة والوصول إلى مرتكبيها، ولهذا تلزم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف باتخاذ التدابير التشريعية اللازمة حتى تتمكن سلطاتها المختصة من تفتيش تقنية معلومات أو جزء منها أو إحدى وسائط تخزين المعلومات الإلكترونية[٢].
٣. **ضبط المعلومات المخزنة (الحجز):** يعرف الضبط بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والحفظ على هذه الأدلة والضبط هو الغاية من التفليش ونتيجته المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه القواعد نفسها التي تنطبق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط[٣].

غير أنّ محل الضبط في مجال الجرائم الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني أثار جدلا كبيرا وانقسم بشأنه فقهاء القانون إلى اتجاهين: الاتجاه الأول يرى أنصاره أن المعلومات المعالجة إلكترونيا في عالم افتراضي غير مادي لا يمكن أن تكون محلا للضبط إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير، أو ينقلها بواسطة مختلف دعائم التخزين الإلكترونية، فيما ذهب أنصار الاتجاه الثاني إلى أن المعلومات المعالجة الكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية قابلة للتسجيل والحفظ والتخزين، يمكن نقلها وبثيا واستقبالها وإعادة إنتاجها، وبذلك لا يمكن إنكار وجودها المادي[٤].

ونظراً لأهمية هذا الإجراء في مكافحة الجريمة الإلكترونية نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ٢٧ منها على ضرورة اعتماد الدول الأطراف الإجراءات تمكن السلطات المختصة من

---

[١] المادة ٢٥ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٢] المادة ٢٦ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٣] د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٩١.

[٤] د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، مرجع سابق، ص١١٧.

ضبط وتأمين تقنية المعلومات أو جزء منها أو وسائط تخزين المعلومات كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية... إلخ، ونسخ المعلومات والاحتفاظ بها ومحوها أو إزالتها من التقنية التي اكتشفت فيها أو منع أي شخص آخر من الوصول إلها. وتمكين هذه السلطات من الاستعانة بالأشخاص الذين لهم خبرة ومعرفة في هذا المجال[١].

٤. **الجمع الفوري لمعلومات تتبع المستخدمين:** إلى جانب الإجراءات السابق ذكرها الزمت هذه الاتفاقية الدول الأطراف باتخاذ التدابير اللازمة التي من شأنها أن تمكن السلطات المختصة من جمع أو تسجيل المعلومات المتعلقة بتقيع المستخدمين عن طريق مختلف الوسائل الفنية وتلزم مزودي الخدمة في حدود اختصاصهم أيضا للقيام بذلك مع الحفاظ على سرية هذه المعلومات. ولكنها لم تحدد الشروط القانونية الواجب اتخاذه الجمع وتسجيل المعلومات ما عدا الزامها الدول الأطراف ينبني إجراءات الإلزام مزودي الخدمة بالحفاظ على سرية المعلومات[٢].
٥. **اعتراض بيانات المحتوى:** تنص المادة ٢٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الزامية تبني الدول الأطراف في تشريعات الداخلية للتدابير اللازمة لتمكين السلطات المختصة من اعتراض بيانات المحتوى في ما يتعلق ببعض الجرائم المنصوص عليا في قوانينها الداخلية.

ثانياً: آليات التعاون القانوني والقضائي لمكافحة جرائم الإرهاب الإلكتروني: يقصد بالتعاون القضائي الدولي محمل الإجراءات التي تتخذها السلطات القضائية داخل الدولة بصدد جريمة محددة أو مجرمين محددين (مهمين أو محكوم عليم) والمنصوص عليها في الاتفاقيات الدولية التي تكون الدول طرفا فيها بمقتضى التشريعات الوطنية النافذة.

١. **تسليم المجرميين:** يعرف تسليم المجرمين بأنه ذلك الإجراء القانوني الذي تقوم به دولة ما لتسليم شخص متواجد على إقليمها إلى دولة أخرى تطلب تسليمه لمحاكمته أو لتنفيذ العقوبة المحكومة بها

---

[١] المادة ٢٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٢] المادة ٢٨ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

أو كإجراء وقائي[١]. وعرفه نظام روما الأساسي بأنه "نقل دولة ما شخصا إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني"[٢].

٢. **المساعدة المتبادلة بين الدول الأطراف:** نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جملة من الإجراءات لتنظيم طلبات المساعدة المتبادلة بين الدول الأطراف يمكننا أن نوجزها في ما يلي:

- يتعين على كل دولة طرف أن تقوم بتعين سلطة مركزية تعنى بإرسال ودراسة طلبات المساعدة المتبادلة والإجابة عليها وتنفيذها أو تقديمها إلى السلطات المختصة لتنفيذها على أن يتم قيد هذه السلطة في سجل خاص تعده الأمانة العامة لوزراء الداخلية العرب والأمانة الفنية لوزراء العدل العرب لهذا الغرض. غير أنه في الحالات المستعجلة يمكن أن توجه أي دولة طرف طلب المساعدة مباشرة إلى السلطة القضائية للدولة المطلوب منها المساعدة مع التزام الدولة الطالبة بإرسال نسخة من هذا الطلب إلى السلطة المركزية للدولة المطلوب منها المساعدة وفي وحالة عدم اختصاص السلطة القضائية تحيل هذه الأخيرة طلب المساعدة إلى السلطة المختصة شريطة إعلاميا للدولة الطالبة بذلك فورا، كما أجازت هذه الاتفاقية للدول الأطراف إرسال طلبات المساعدة إلى بعضها البعض عن طريق المنظمة الدولية للشرطة الجنائية "INTERPBOL""[٣].

- توجه طلبات المساعدة المتبادلة من الدولة الطرف الطالبة للمساعدة إلى الدولة المطلوب منها بشكل خطي كقاعدة عامة، غير أنه يجوز أن ترسل هذه الطلبات في الحالات المستعجلة عن طريق وسائل الاتصال الحديثة كالفاكس أو البريد الإلكتروني مع مراعاة أمن وسرية الاتصالات بين الأجهزة المختصة للدول التي تقدمت بطلب المساعدة والدولة التي تلقت هذا الطلب كاستعمال طريقة تشفير المعلومات مثلاً [٤].

---

[١] د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني، مرجع سابق، ص٩٣.

[٢] المادة ١٠٢ من نظام روما الأساسي لعام ١٩٩٨.

[٣] المادة ٣٤ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٤] المادة ٣١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

وإن هذه التقنية تعتبر من أهم التقنيات المستعملة لحماية المعلومات السرية المخزنة في الحاسب الآلي أو نقلها عبر الشبكات غير المأمونة كشبكة الإنترنت حتى لا يتمكن الأشخاص غير المرخص لهم من الاطلاع عليا، حيث تتم هذه العملية إما عن طريق التشفير التقليدي أو المتماثل الذي يعتمد على مفتاح واحد لعملية التشفير وفك التشفير للبيانات أو عن طريق تشفير المفتاح العام الذي يُستخدم فيه مفتاحان مفتاح عام لتشفير الرسائل ومفتاح خاص لفتح الرسائل المشفرة.

ثالثاً: مجالات المساعدة المتبادلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: تتمثل مجالات المساعدة المتبادلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ما يلي:

١. التقديم التلقائي للمعلومات بين الدول الأطراف: أجازت هذه الاتفاقية على غرار اتفاقية بودابست لسنة ٢٠٠١ للدول الأطراف أن تقدم لبعضها البعض بصفة تلقائية المعلومات تحصلت عليها من خلال التحقيقات التي تقوم بها مصالحها المختصة بدون طلب مسبق للمساعدة في إطار التعاون من أجل مواجهة الجريمة الإلكترونية والإرهاب الإلكتروني[١]. كما أجازت هذه الاتفاقية للدولة التي تحيل المعلومات بصفة عرضية أن تطلب من الدول التي أحالت لها المعلومات أن تحافظ على سريتها في حالة ما إذا كانت هذه المعلومات حساسة أو إذا ما تم الكشف عنها قد تتعرض المصالح الجوهرية للدولة المقدمة للمعلومات للخطر. وإذا كشف التحقيق المسبق أن الدولة الطرف المتلقية للمعلومات لا تستطيع الالتزام بالسرية كما لو كانت هذه المعلومات مطلوبة كدليل في محاكمة علنية، فيتعين عليها إعلام الدولة التي أحالت إليها هذه المعلومات، أما إذا قبلت المعلومات بشرط الحفاظ على سريتها فيجب عليا التقيد بهذا الشرط[٢].

٢. المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة: وتتمثل المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة حسب هذه الاتفاقية في الحفظ العاجل للبيانات المحزنة في تقنية معلومات والكشف العاجل للبيانات المتعلقة بتتبع المستخدمين، وهذا ما ستكتشفه في ما يلي:

- الحفظ العاجل للبيانات المخزنة في تقنية معلومات: تجيز المادة ٣٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لأي دولة طرف أن تقدم طلبا للحصول على الحفظ العاجل للبيانات المخزنة في تقنية المعلومات الموجودة على إقليم الدولة الطرف للطلب على أن يشتمل هذا طلب اسم البيئة المصدرة له نوع الجريمة الإلكترونية محل التحقيق. ملخصا للوقائع البيانات التي يتعين حفظها

---

[١] المادة ١/٣٣ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٢] المادة ٢/٣٣ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

وبيان علاقتها بهذه الجريمة المعلومات المتعلقة بالمسؤول عن البيانات المخزنة وموقعها وكذا الهدف المتوخى من طلب المساعدة والذي يكون إما للوصول أو البحث أو ضبط أو كشف عن البيانات المخزنة، كما تلزم هذه الاتفاقية في المادة نفسها الدول الأطراف التي تتلقى طلب الحفظ العاجل للبيانات المخزنة في تقنية معلومات اتخاذ التدابير والإجراءات الضرورية لحفظ البيانات المذكورة في الطلب وفقا لقانونها الداخلي وعدم تمسكها بمبدأ ازدواجية التجريم كشرط لحفظ البيانات في الجرائم المنصوص عليها في الفصل الثاني منها، غير أنها أجازت للدول الأطراف المطلوب منها المساعدة أن ترفض هذا الطلب إذا كان تنفيذه يعرض سيادتها أو أمن مصالحها الجوهرية للخطر أو إذا كانت الجريمة موضوع التحقيق تعتبر من قبيل الجرائم السياسية في قوانينها الداخلية[1].

والجدير بالملاحظة أن هذه الاتفاقية حددت المدة الدنيا للحفظ العاجل للبيانات المخزنة في تقنية معلومات المترتب على طلب المساعدة في الفقرة ٠٧ من المادة ٣٧ منها بستين (٦٠) يوما، دون أن تحدد المدة القصوى لذلك.

- الكشف العاجل لبيانات تقبع المستخدمين: يتعين على الدولة المتلقية لطلب المساعدة إذا ما اكتشفت أن بيانات الحركة التي تم التطرق إليه سابقا، تفيد بأنه تم توجيه الإرسال من مزود خدمة في دولة ثالثة أو من الدولة الطالبة للمساعدة أن تقدم إلى هذه الأخيرة قدرا كافيا من بيانات تتبع المستخدمين لتمكينها من معرفة مزود الخدمة وتحديد. مساريث الاتصال، أما إذا كان ذلك يمس بأمنها أو سيادتها أو مصالحها أو من قبيل الجرائم السياسية فيجوز لها رفض طلب الكشف عن بيانات المستخدمين[2].

٣. المساعدة المتبادلة للوصول إلى البيانات المخزنة واعتراض بيانات المحتوى: في إطار تعزيز التعاون بين الدول الأطراف في مجال مكافحة الإجرام المعلوماتي تجيز المادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات للدول الأطراف أن تطلب من بعضها البعض القيام بأي إجراء من شأنه البحث أو النفاذ أو الضبط أو التأمين أو الكشف عن البيانات المخزنة في تقنية معلومات موجودة داخل أراضيا مع مراعاة الدول المطلوب منها المساعدة للأحكام المنصوص عليها في هذه الاتفاقية التي تنظم المساعدة القانونية المتبادلة، وكذا التزامها بالتعجيل بالرد على طلب

---

[1] المادة ٣٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[2] المادة ٣٨ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

المساعدة للدولة الطالبة في الأحوال التي تكون فيها البيانات المخزنة معرضة للحذف أو التغيير أو التعدي[١].

كما أجازت المادة ٤٠ من هذه الاتفاقية أيضا للدول الأطراف أن تحصل على المعلومات المتوفرة للعامة في أي مكان دون حصولها على تفويض من دولة أخرى طرف والتزامها أيضا بتقديم المساعدة لبعضها البعض بالجمع الفوري لبيانات تقبع المستخدمين التي تتم عن طريق إحدى تقنية المعلومات[٢].

ونظرا لخطورة التدخل التي تتسم بها عملية الاعتراض، قيدت هذه الاتفاقية على غرار اتفاقية بودابست المساعدة المتبادلة لاعتراض بيانات المحتوى في حدود ما تسمح به المعاهدات والقوانين الداخلية السارية المفعول للدول الأطراف[٣].

الخاتمة

وجدنا أن الإرهاب الإلكتروني من الجرائم المستحدثة بالغة التعقيد فهو وليد عوامل عديدة ومتضافرة (اجتماعية أيديولوجية ثقافية) ورغم أهمية النصوص القانونية، فإن القضاء على هذا النوع من الإجرام يستدعي حلولا نتجاوز فكرة العقاب وتكرس ما يمكن تسميته بمكافحة الإرهاب "الإقناعية" التي تقوم على كسب القلوب والعقول في مكافحة الإرهاب. وإن تنامي ظاهرة الجرائم المعلوماتية عبر الوطنية بما فيها الإرهاب الإلكتروني، وتخطي آثارها حدود الدول، أفرز حملة من التحديات على الصعيد الدولي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل يشأها باعتبارها لا تترك أثراً مادياً ملموسا، كما هو الحال في الجرائم التقليدية. وبالرغم من الجهود التي بذلت ولا تزال تبدل على المستوى الدولي، فإن هذه التحديات تبقى عصية على الحل في كثير من الأحيان في غياب إستراتيجية واضحة للتعامل مع هذه الصنف من الجرائم ومرتكبيها لاسيما في الدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تناسب مع متطلبات هذا العصر.

وقد توصلنا في الختام لعدة نتائج وتوصيات هي: –

أولاً: نتائج البحث.

---

[١] المادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٢] المادة ٤١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٣] المادة ٤٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

١. عدم اتسام النموذج القانوني للإرهاب الإلكتروني في قانون العقوبات بالدقة والوضوح .
٢. يستهدف الإرهاب الالكتروني بعدين هامين يتمثل أولهما في أنه أصبح عاملاً مساعداً للإرهاب التقليدي، من خلال توفير المعطيات عن الأماكن المستهدفة أو المساهمة في تنفيذ العملية الإرهابية. والبعد الثاني معنوي يتمثل في بث الكراهية ونشر الأفكار الهدامة عبر خطاب إعلامي منهجي.

٣. استطاعت المنظمات الإرهابية توظيف شبكة الإنترنت في الحصول على كم هائل من المعلومات ومن ثم تبادلها بين أفردها بصورة خفية لتحقيق أهدافها الإجرامية.

٤. هناك إمكانية لشن الجماعات والمنظمات الإرهابية هجوما إرهابيا مدمرا بواسطة تعطيل الأجهزة الإلكترونية ما يترتب عنه إغلاق المواقع الحيوية والحاق 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 والبحرية، أو شل النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية.
٥. أسهمت شبكة الإنترنت في توسع الأعمال التجسسية بشكل كبير، حيث تقوم المنظمات الإرهابية بالتجسس على الأشخاص والدول والمنظمات والهيئات أو المؤسسات الدولية، وتستهدف عملية التجسس المجال العسكري والسياسي والاقتصادي والأمني.

ثانياً: توصيات البحث.

١. ضرورة وضع نظام وقواعد إجرائية خاصة موحدة لجرائم الإرهاب الإلكتروني.

٢. ضرورة التوسع في صور التعاون الأمني بعقد المزيد من الاتفاقيات والتعاون مع الدول المختلفة وذلك لمواجهة مخاطر تزايد احتمالات ارتكاب الجرائم الماسة بأمن الدولة والجرائم الإرهابية، خاصة بعد ثورات الربيع العربي التي لم تجني الدول منها إلا مشكلات ما زالت تبحث عن حلول.

٣. ضرورة حماية الشبكات وأجهزة الحاسب الآلي من خلال تشفير المعطيات الحساسة المتبادلة عبر الإنترنت وتعزيز أعلى قدرة لأمن المعلومات. مع ضرورة تعقب وحجب المواقع ذات الخلفية الإرهابية، كطريقة وقائية لتجفيف منابع الاستقطاب والتجنيد الإرهابي وقطع الطريق أمام توظيف الإرهابيين للإنترنت للدعاية لأعمالهم الإرهابية.

٤. أهمية التكامل والتنسيق بين التشريعات الدولية والإقليمية من جهة، والتشريعات والقوانين الوطنية من جهة أخرى للتصدي للإرهاب الإلكتروني بجميع أشكاله وصوره.

٥. التأكيد على أهمية دور وسائل الاعلام والمؤسسات المدنية ونظم التعليم في بلورة استراتيجيات للتصدي لمزاعم الإرهابيين، وتشجيع وسائل الاعلام لوضع قواعد ارشادية للتقارير الاعلامية والصحفية بما يحول دون استفادة الإرهابيين منها في الاتصال أو التجنيد أو غير ذلك.

قائمة المصادر والمراجع

أولاً: المراجع العربية

أ. الكتب القانونية.

١. د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، ط١، دار النهضة العربية، القاهرة، ٢٠٠٨.

٢. د. أسامة حسين محيي الدين، جرائم الإرهاب على المستوى الدولي، المكتب العربي الحديث، الإسكندرية، ٢٠٠٩.

٣. د. إمام حسنين عطا الله، الإرهاب والبنيان القانوني للجريمة، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٥.

٤. د. إمام حسنين عطا، البنيان القانوني لجريمة الإرهاب، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٤.

٥. د. أمل يازجي، الإرهاب الدولي والنظام العالمي الراهن، دار الفكر، دمشق، ٢٠٠٢.

٦. د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، ط١، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١١.

٧. د. حسين بن سعيد الظافري، السياسة الحديثة في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩.

٨. د. السيد عوض، الجريمة في مجتمع متغير، المكتبة المصرية، الإسكندرية، ٢٠٠٤.

٩. د. عبد العال الديربي ود. محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢.

١٠. د. علي عسيري، الإرهاب والإنترنت، ط١، بلا دار نشر، الرياض، ٢٠٠٦.

١١. د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٩.
١٢. د. منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨.
١٣. د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١.
١٤. د. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، السليمانية، العراق، ٢٠٠٧.

ب. الأبحاث المنشورة.

١. د. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، تاريخ النشر ٢٠١٦/١٢/١٢، تاريخ الإطلاع ٢٠٢٣/٥/٦، منشور على الرابط الإلكتروني الآتي: –
http://repository.nauss.edu.sa/bitstream
٢. صباح كزيز وآمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، دراسة تحليلية، مجلة التراث، الجزائر، المجلد ٨، العدد ١، ٢٠١٨.
٣. د. صلاح هادي الفتلاوي، جريمة الإرهاب الإلكتروني، مجلة القانون للبحوث القانونية، جامعة ذي قار، العراق، المجلد ١، العدد ١٣، ٢٠١٦.
٤. د. عباسة طاهر ود. مجاهد توفيق، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، مجلة العلوم القانونية والسياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد ٩، العدد ٣، ٢٠١٨.
٥. د. عبد الرحمن المسند، وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ج١، الرياض، ٢٠٠٤.
٦. د. نادية شرايرية، إشكالية تعريف الإرهاب في القانون الدولي، مجلة التواصل في العلوم الاجتماعية والإنسانية، جامعة باحي مختار، بجاية، الجزائر، المجلد ١٩، العدد ٢، ٢٠١٣.

ثانياً: المراجع الأجنبية.

- Daniel Ventre, Cyberattaque et cyberdéfense. Paris ; La Voisier, 2011.
- Gabriel Weimann, Terror on the Internet, United States Institute of Peace, Washington, April 2006.