الجريمة الإرهابية الإلكترونية

أمجد الكوش

مقدمة

لا شك أن الثورة التكنولوجية أحدثت نقلة نوعية في أسلوب حياة الأفراد والمجتمعات نحو الأفضل، من خلال الاستفادة من وسائل الاتصالات المتطورة التي وضعتها في متناول الأفراد في مختلف المجتمعات عبر العالم. غير أن التوظيف السلبي لهذه الوسائل أصبح يشكل خطراً على حياة الأفراد واستقرار المجتمعات والدول، فقد أصبحت الجماعات الإجرامية والإرهابية تستخدم وسائل الاتصال خصوصاً شبكة الأنترنت بشكل احترافي للتخطيط وتنفيذ أعمال إجرامية حيث يلاحظ وبشكل ملحوظ استعمال مكثف للعديد من التطبيقات لنشر أفكارها والدعاية لمبادئها، وكذلك تجنيد العناصر الجديدة أو تدريبها على صنع المتفجرات واستخدام الأسلحة، فضلاً عن الاتصال والتخطيط للهجمات الإرهابية وهذا ما طرح تحديات كبيرة بالنسبة إلى الحكومات والدول في مواجهة هذه الجرائم الإرهابية الإلكترونية الجديدة.

عرفت بعض المفاهيم والظواهر تحولات جوهرية بعد نهاية الحرب الباردة ويرجع ذلك بالأساس إلى جملة التغيرات التي شهدتها البيئة الدولية، ويمكن اعتبار الثورة التكنولوجية والمعلوماتية في مجال وسائل الإعلام والاتصال، أو ما يصطلح عليه الثورة الصناعية الثالثة، أهم هذه التغيرات التي انعكست بدورها على عدد من المجالات الأخرى، حيث تحولت إلى مجتمعات رقمية تربط أفرادها علاقات.

ومن أبرز هذه المجالات الجريمة بمختلف أشكالها، حيث أصبحت الجماعات الإجرامية تستخدم مختلف وسائل الاتصال والمعلومات في هذا الإطار لتحقيق أهدافها، فاستطاعت من خلال ذلك تطوير أساليبها الإجرامية لخدمة أغراضها وتهديد أمن المجتمعات والدول فأصبح هذا الإجرام يعرف بالجريمة الإلكترونية. وقد تكون الجريمة الإرهابية الإلكترونية أخطر أشكال الجريمة، حيث أصبحت التنظيمات الإرهابية تستخدم الأنترنت في تجنيد العناصر الإرهابية وتدريبها، وكذلك في تنفيذها وعرضها للرأي العام.

القسم الأول
الجريمة الإرهابية الإلكترونية
بين المفهوم العام والتطبيق

المبحث الأول
الإطار العام للجريمة الإرهابية الإلكترونية

إن مصطلح «الإرهاب السيبراني» هو مصطلح مثير للجدل لا يظهر في أي معاهدة دولية، ويثير صعوبات حقيقية من حيث التعريف. ومع ذلك، جرت محاولات في الثمانينيات، بما في ذلك المحقق الرئيسي لمعهد الأمن والاستخبارات في كاليفورنيا، باري كولين، ووفقا له، فإن الإرهاب السيبراني هو العلاقة بين الإرهاب والفضاء الإلكتروني، والذي يعرفه بأنه «المكان الذي تعمل فيه برامج الكمبيوتر وحيث يتم تداول البيانات». أحد التحديات هو الحد الفاصل بين الجريمة السيبرانية والإرهاب السيبراني. وبينما تتميز الجريمة السيبرانية بتنفيذ أعمال أو أنشطة غير مشروعة باستخدام أدوات حاسوبية لأغراض اقتصادية في كثير من الأحيان، فإن الإرهاب السيبراني، من ناحية أخرى، يعتمد أكثر على الدوافع السياسية والإيديولوجية. وفقا لتعريف مجلس أوروبا، الإرهاب السيبراني هو «استخدام الإنترنت لأغراض إرهابية»[١].

المطلب الأول: مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية أو السيبرانية (Cybercriminalité) هي مصطلح حديث يتألف من مصطلحين، الأول إجرام أو جريمة (Crime) والمصطلح الثاني سيبراني أو الكتروني (Cyber)، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسوب أو عصر المعلومات. وهي من "**الجرائم الهادئة**" التي لا تتطلب القوة أو العنف أو السلاح[٢]. فالجريمة الإلكترونية هي فعل غير مشروع يرتكب بواسطة نظام حاسوبي مرتبط بشبكة الأنترنت[٣].

ورغم تعدد الميزات الإيجابية لتطور وسائل الاتصال الحديثة، غير أن هذا التطور صاحبه توظيف مكثف لهذه الوسائل في مجال الجريمة بمختلف أنواعها، فأصبحت بذلك الجريمة الإلكترونية ظاهرة إجرامية جديدة تتميز بعديد من الخصائص التي تجعلها مختلفة عن الجرائم التقليدية، حيث إن المجرمون في هذا المجال أو كما يسمون " الهاكرز / Pirates " يتميزون بالذكاء في استخدام وسائل تقنية متطورة، وتنفيذ جرائمهم بكل دقة وسرية بعيداً من الخطر والمتابعات الأمنية والقضائية، سواء في عمليات إرسال الفيروسات المخربة للأنظمة والمواقع، أم سرقة الأموال والسطو على المصارف وتحويل الأموال، أم سرقة البيانات المهمة أم إتلافها، كما تتميز الجريمة الإلكترونية بالسرعة في التخطيط والتنفيذ، وبجهد وتكاليف أقل بكثير من الجهد والأموال الكبيرة التي كانت تنفق في تنفيذ الجرائم التقليدية، إضافة الى أنها تتخطى قدرات الدولة وحدودها السيادية فيمكن تنفيذها من الخارج وفي أي منطقة من العالم، فالجريمة الإلكترونية أقرب الى مفهوم الجريمة الدولية أكثر منها إلى مفهوم الجريمة المحلية[٤].

---

(١) Alina B. pour le club Risques AEGE, < https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2020/le > cyberterrorisme-menace-du-siecle-depuis-son-utilisation-jusquaux-attaques/.

(٢) طارق عبد الوهاب سليم، الجرائم المرتكبة بواسطة الأنترنت وسبل مكافحتها، تونس، ١٩٩٧، ص ١٥٠.

(٣) سمير ابراهيم جميل العزاوي، "المسؤولية الجنائية الناتجة عن استخدام الأنترنت"، كلية القانون جامعة بغداد، ٢٠٠٥، ص٩.

(٤) صخري محمد، ٢٠٢١/٨/٢٩: https://www.politics-dz.com

المطلب الثاني: مفهوم الإرهاب

في اللغة العربية مصطلح إرهاب مشتق من الفعل "رهب" بمعنى خاف وفزع ورعب وهي مصدر للفعل "أرهب"، وأرهبه بمعنى خوفه وفي المعاجم العربية القديمة عرف الفعل "رهب" يرهب رهبة ورهباناً أي خاف ورهبه أي أخافه وأفزعه، والرهبة هي الخوف والفزع والرعب(٥).

ويعتبر جناية اجتماعية وسياسية يكون تنفيذها أو التعبير عنها بمختلف الوسائل طريقاً لنشر الفزع العام وعدم الاستقرار في المجتمع والنظام السياسي، فالإرهاب خطر حقيقي يهدد أمن الفرد والمجتمع والدولة. والإرهاب هو طريقة لإثارة البلبلة والاضطراب عن طريق العنف المستخدم بواسطة فرد أو جماعة أو دولة أو ممثلين سريين، ويكون هذا العنف لأسباب سياسية أو خاصة، فالضحايا هم الأهداف المباشرون للعنف، ويكون هؤلاء الضحايا مختارين بشكل عشوائي من السكان وهذا يحمل رسالة معينة، فالعنف والتهديد والتخويف ما هما إلّا وسيلة لاتصال المنظمات الإرهابية بالإعلام، والضحايا هنا هم الجمهور الذين تحولوا الى أهداف ولكنهم في الحقيقة وسيلة وليس غاية(٦).

وأخذ الإرهاب في نهاية القرن العشرين البعدين السياسي والدولي، فأصبح وسيلة أساسية لتحقيق الأهداف السياسية (الإرهاب السياسي / Terrorisme Politique)، كما أصبح أيضاً يحمل الطابع الدولي (الإرهاب الدولي Le / Terrorisme International) حيث تجاوز نشاط الجماعات الإرهابية الحدود السيادية للدولة، وهذا ما جعل منه جريمة دولية وليست داخلية فحسب.

شهدت السنوات الأخيرة نوعاً جديداً من الجرائم الإرهابية وبالأحرى تحولاً نوعياً في أساليب تنفيذ الجرائم الإرهابية وأدواتها، على غرار اختطاف الطائرات المدنية وتفجيرها واستخدام المتفجرات والأحزمة الناسفة وتخريب شبكات الاتصال ومواقع الأنترنت الخاصة بالمصالح الأمنية، أو استخدامها لتجنيد عناصر جديدة ونشر الفكر الجهادي والتكفيري، وحتى تنفيذ هجمات إرهابية فائقة الدقة،

حيث أصبح امتلاك الدولة لوسائل التكنولوجيا والمعلومات من أهم عناصر القوة في السياسة الدولية، ويكتسي أهمية أكثر من القوة العسكرية والاقتصادية وذلك في ظل التطور الكبير في وسائل الإجرام واستخدامها بكفاءة عالية من طرف الارهابيين، وهذا ما يؤكده المفكر الأمريكي الجنسية (Joseph Nye) جوزف ناي(٧).

المطلب الثالث: مفهوم الإرهاب الإلكتروني

المقصود بالإرهاب الإلكتروني هو استخدام التقنيات الرقمية لإخافة الآخرين وإخضاعهم أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية(٨) فالإرهاب

(٥) علي بن عبد العزيز بن علي العميريني، مفهوم الإرهاب في الفقه الاسلامي والقانون الوضعي (جزء ١) الرياض، ٢٠٠٧، ص ٦٧، ٦٨.

(٦) Joseph S. Tuman, Communicating Terror (the Rhetorical Dimensions of Terrorism), San Francisco: SAG Publications, p.13.(2016).

(٧) ريهام مقبل، "مركب القوة – عناصر وأشكال القوة في العلاقات الدولية"، ملحق مجلة السياسة الدولية،مصر، العدد ١٨٨، المجلد ٤٧، نيسان٢٠١٢، ص٧،

(٨) بن يحيى الطاهر ناعوس: "مكافحة الارهاب الالكتروني ضرورة بشرية وفريضة شرعية"، http://www.alukah.net/ / library

الإلكتروني في دوافعه لا يختلف عن الإرهاب، حيث تبقى الدوافع السياسية المحرك الأساسي لهذا النشاط الإجرامي، غير أن وسائله تختلف عن الإرهاب التقليدي من خلال استخدام وسائل متطورة كنظم المعلومات والوسائل التكنولوجية والرقمية المتطورة، وقد تكون خطورتها أكبر بالنسبة إلى الشركات الاقتصادية الكبرى والبنوك ونظم المعلومات التابعة للأجهزة الأمنية للدول، وبالتالي فإن ضرر الإرهاب الإلكتروني يتجاوز بكثير الضرر الذي يخلفه الإرهاب التقليدي.

تتضاعف خطورة الإرهاب الإلكتروني إذا نظرنا إلى سهولة استخدام هذا السلاح، حيث يقوم الإرهابي بعمله التخريبي من منزله أو غرفته في الفندق أو من مقهى عمومي، وهذا ما جعل هذا النوع من الإرهاب هاجساً حقيقياً، فكل منطقة من العالم أصبحت عرضة لهجمات الإرهابيين عبر الأنترنت. ورغم سعي العديد من الدول إلى مواجهة ضرر هذه الهجمات الإرهابية وتفاديها، إلا أنها لا تزال بعيدة عن المستوى المطلوب.

المطلب الرابع: مفهوم الجريمة الإرهابية الإلكترونية

هي نوع من الإرهاب الحديث الذي وظف واستثمر تقنيات المعلومات والاتصال بشكل يلائم متطلباته وأهدافه، وذلك بغرض إثارة الخوف وزعزعة استقرار المجتمعات، فهو يعتمد في التخطيط والتنفيذ للعمليات الإجرامية الإرهابية على وسائل الاتصال الإلكترونية، فخلال العقود الأخيرة أصبحت التنظيمات الإرهابية تعتمد في نشاطها على هذه الوسائل الإلكترونية بشكل مكثف، وهو ما أنتج شكلاً جديداً من الإرهاب وهو ما أطلق عليه الجيل الثاني من الإرهاب أو الإرهاب الإلكتروني وهو "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادرة عن الدول والجماعات أو الأفراد عبر الفضاء الإلكتروني، أو أن يكون هدفاً لذلك بما يؤثر على الاستخدام السلمي له"(٩). ويعرفه جميل عبد الباقي أيضاً بأنه: "ذلك النوع من الإرهاب الحديث الذي يعتمد بصورة كلية على استخدام كل الوسائل والإمكانيات العلمية والتقنية لشبكات الأنترنت وشبكات الاتصالات المعلوماتية في سبيل إدخال الخوف والرعب وإلحاق الضرر بالأفراد أو الجماعات المدنية أو المؤسسات الحكومية"(١٠).

إن تطور وسائل الاتصال وشبكات المعلومات ومختلف الإمكانيات العلمية والتقنية جعل استغلالها في تنفيذ العمليات الإرهابية أكثر سهولة حيث يمكن تنفيذها على الأهداف الحكومية بدقة كبيرة تقل فيها نسبة الخطأ، وذلك بفضل التوجيه والتحكم في وسائل نقل المتفجرات والاتصال بين العناصر الإرهابية أثناء عملية التنفيذ بوسائل اتصال جد متطورة، كما أن استهداف البنية التحتية لشبكة المعلومات الحكومية أو العامة للمؤسسات الاقتصادية والشركات وتخريبها أو تدميرها قد يتم بسرعة فائقة ويكلف خسائر كبيرة جداً تتجاوز الخسائر التي تكون نتيجة العمليات الإرهابية بالشكل التقليدي. والأخطر من كل ذلك أن الجماعات الإرهابية قد تنفذ هذه

(٩) عادل عبد الصادق، الإرهاب الإلكتروني نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الالكتروني، ٢٠١٣.

(١٠) حسن تركي عمير، "الإرهاب الالكتروني ومخاطره في العصر الراهن" مجلة العلوم القانونية والسياسية جامعة ديالي عدد خاص ص٣٢٧.

العمليات وهي في أماكن بعيدة وآمنة عن الشرطة فقد أصبحت فواعل إلى جانب الدول فبإمكانها تهديد أمن الدول وتغيير مجرى الأحداث الدولية، فهذه الأخيرة لم تعد اللاعب الوحيد في العلاقات الدولية، ومنه لم تعد تتمتع بالسيادة المطلقة مثلما كانت سابقاً[١١].

لقد أصبحت التنظيمات الإرهابية في السنوات الأخيرة تمتلك قدرات كبيرة في توظيف الوسائل التكنولوجية، حتى أصبح استخدام مصطلح "الإرهاب التكنولوجي" موضوعياً إلى أبعد الحدود، كما توضح الدراسة التي نشرها مركز الأبحاث لدراسات الصراع والإرهاب[١٢]، "التكنولوجيا والارهاب التهديد الجديد للألفية الجديدة" (ستيفن أرباورز & كمبرلي أركيز)، حيث أكدت هذه الدراسة أن التنظيمات الإرهابية أصبح بإمكانها حالياً الحصول على كل ما تريد من معلومات عبر الاستخدام المقنن للكمبيوتر ومن خلال استغلال ثغرات شبكات المعلومات أو باللجوء إلى عمليات القرصنة المعلوماتية والدخول إلى بنوك المعلومات العسكرية والأمنية للدول، واستغلالها في التخطيط للعمليات الإرهابية، كما يمكنها أيضاً الدخول إلى شبكات البورصة والأسواق المالية وتدميرها بقصد المساس بالقوة الاقتصادية للدول المستهدفة.

المبحث الثاني: دور الأنظمة الإلكترونية في تجنيد الإرهابيين وتدريبهم

وظفت التنظيمات المتطرفة وسائل التقنية الحديثة لتحقيق مآربها التخريبية، وأهدافها الإرهابية، وإن الإرهابيين ينظرون إلى الإنترنت بتِقاناته المختلفة ومواقعه وصفحات التواصل الاجتماعي فيه، بوصفه وسيلةً مهمَّة وميسَّرة لممارسة نشاطاتهم المتطرفة غير المشروعة، ولاستهداف بعض المواقع الإلكترونية والأنظمة الحاسوبية للجهات المعادية لهم، لتحقيق مآربهم وأهدافهم.

المطلب الأول: دور الأنظمة الإلكترونية في تجنيد الإرهابيين وتدريبهم

الفقرة الأولى: العوامل المساعدة على توظيف الإرهاب للأنظمة الإلكترونية[١٣]

ساهمت بعض العوامل في نجاح التنظيمات الإرهابية في استغلال الأنظمة الالكترونية والمعلوماتية لتنفيذ أهدافها الإجرامية ومن أهمها:

– الانفتاح الذي تتميز به أنظمة المعلومات عموماً والأنترنت على وجه الخصوص، فالبنية الخاصة بالشبكة المعلوماتية تفتقد للقيود والحواجز والرقابة الأمنية، وهي الثغرة التي تتسلل من خلالها التنظيمات الإرهابية لتحقيق أهدافها التخريبية.

– صعوبة تحديد هوية وملاحقة مرتكبي الجريمة الإرهابية الإلكترونية.

– سهولة التواصل بين العناصر الإرهابية والتخطيط لتنفيذ الجريمة دون الحاجة إلى الاجتماع في مكان واحد ما يعرضها للخطر، فهي لا تتطلب موارد مالية ضخمة مثل العمليات الإرهابية التقليدية.

– سهولة استخدام شبكة المعلومات والدخول إليها في أي منطقة من العالم فهي تتجاوز الحدود الجغرافية للدول ويمكن تنفيذها

(١١) Thomas Quiggin, Seeing the Invisible National Security Intelligence in an Uncertain Age, London World ScientificPublishing, 2007. p13.

(١٢) www.europarabct.com

(١٣) https://www.bayancenter.org/2019/09/5458/

من دولة بعيدة وبهوية وهمية أو انتحال شخصية غير موجودة أصلاً.

– ضعف التشريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول، خاصة في البلدان النامية.

الأمر الذي يفسر تنامي التنظيمات الإرهابية وتزايدها، حيث أصبح نشاط الجماعات الإرهابية على شبكة الأنترنت مكثفاً ومؤثراً بشكل كبير في توجيه نشاطاتها الإجرامية، سواء في التواصل بين فروعها وخلاياها، أم في تنفيذ جرائم التخريب ضد المواقع الحكومية أم التجسس عليها أم في تجنيد العناصر الجديدة في صفوفها ونقل رسائلها التهديدية، وفي هذا الإطار نشرت قناة DW الألمانية بتاريخ: ١٥/ ٢٠١٦/١٠ تقريراً يؤكد وجود حوالي ٤٥٠٠ موقع إلكتروني على الشبكة العنكبوتية له نشاطات ذات طابع إرهابي(١٤).

وتوفر شبكة الأنترنت كل المعلومات الثمينة التي يحتاجها الإرهابيون لتنفيذ أعمالهم الإجرامية، مثل مواعيد الرحلات الجوية، وتحديد أماكن مراكز توليد الطاقة الكهربائية وتوزيعها والمواقع الرئيسية للتحكم في أنظمة الاتصالات والمعلومات ومواقع المنشآت النووية وغيرها من المواقع والمراكز الحساسة.

الفقرة الثانية: وسائل تنفيذ الجريمة الإرهابية الإلكترونية:

تعتمد الجريمة الإرهابية الإلكترونية على ثلاث وسائل أساسية(١٥):

١) خدمة البريد الإلكتروني: البريد الالكتروني (E-mail) الذي يسمح بإرسال الرسائل وتبادل المعلومات على الأنترنت في أي منطقة من العالم حيث أصبحت من أهم الوسائل التي تستخدمها التنظيمات الإرهابية في التواصل بين الإرهابيين وتبادل المعلومات والتخطيط للعمليات الإرهابية الإلكترونية من بلدان مختلفة، كما تستخدم لنشر أفكار التنظيم والترويج لها، وأيضاً في اختراق البريد الإلكتروني للموظفين الحكوميين أو رجال الأمن والاطلاع على معلوماتهم وبياناتهم والتجسس على مراسلاتهم والاستفادة منها في عملياتهم الإرهابية.

٢) استحداث مواقع على الأنترنت: تقوم التنظيمات الإرهابية بإنشاء مواقع وصفحات على شبكة الأنترنت تكون بمثابة نافذة على العالم لنشر أفكارهم والدعوة لمبادئهم من أجل كسب أكبر قدر ممكن من المجندين والمتعاطفين، كما أنها وسيلة تساعد عناصرهم في القيام بتنفيذ عمليات إرهابية من خلال تعليمهم طريقة صنع المتفجرات والتحكم في تفجيرها عن بعد وكيفية اختراق وتدمير المواقع الإلكترونية وتدميرها ونشر الفيروسات وطرق اختراق البريد الإلكتروني وغيرها، وبالتالي فهي طريقة لتبادل الأفكار والآراء والمعلومات بين الإرهابيين.

٣) خرق المواقع الإلكترونية وتخريبها: ويقصد بها الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بشبكة الأنترنت، وذلك بهدف تخريبها من خلال الثغرات المتعددة في التطبيقات التي تستخدمها

(١٤) إبراهيم فؤاد عباس: الإرهاب (المعالجة المواجهة ـ الظاهرة)، القاهرة: دار الكتب العلمية للنشر والتوزيع، ٢٠١٧، ص ١٧١ و ١٧٠.

(١٥) سعد عطوة الزنط، "الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي"، أعمال مؤتمر دولي بعنوان: الجرائم المستحدثة كيفية اثباتها ومواجهتها" المركز القومي للبحوث الاجتماعية والجنائية، المنعقد بالقاهرة في ١٥ و ١٦ كانون الأول ٢٠١٠.

التنظيمات الإرهابية غالباً لتخريب الأنظمة الأمنية أو أنظمة الاتصالات، وذلك من أجل إفشال عمليات المراقبة والتتبع التي تفرضها الأجهزة الحكومية لكشف مخططاتهم، وتتبع اتصالاتهم ومشاريعهم أو أماكن تحركهم وغيرها.

المطلب الثاني: توظيف الأنظمة الإلكترونية لتجنيد الارهابيين وتدريبهم

الفقرة الأولى: أساليب التجنيد

أصبح الإرهاب يوظف الأنترنت لتجنيد العناصر الإرهابية وتدريبهم وذلك من خلال بث الأفكار والخطابات المضللة بطرق وأساليب ذكية ومغرية وتغذية الشباب المتحمس ببعض الفتاوى المحرضة وإثارة مشاعر الغيرة والتعصب للقيم والمبادئ الدينية، واعتماد بعض الأساليب الخاطئة في نشر سير السلف الصالح، خاصة ما تعلق منها بالجهاد وتأويلها بطرق مختلفة، وكذلك استخدام أساليب تحريضية ضد الحكومات وسياساتها، والدعوة إلى الخروج عليها ومحاربتها بالأسلحة والمتفجرات. وتمنح شبكة الأنترنت تأمين عمليات الاتصال والتخفي وذلك عن طريق مختلف المواقع والبريد الإلكتروني وغرف الحوار الإلكتروني ومنتديات الدردشة وغيرها من التطبيقات التي تسمح لهم بوضع رسائل مشفرة تحميهم من الرقابة والتتبع الأمني.

الفقرة الثانية: مراحل التجنيد

بموجب أساليب التجنيد، فقد أصبح استخدام التنظيمات الإرهابية للأنترنت بشكل مكثف في إطار نشر ثقافة الإرهاب والترويج لها، وتوظيف كل الأفكار والمبادئ والفلسفات التي تصب في تحقيق هذا الهدف، فتعمل على تكوين قاعدة فكرية تضم كل من لهم استعداد للانخراط في الأعمال الإرهابية[١٦]، وتعمل على تجنيدهم وتحضيرهم نفسياً لتنفيذ عمليات إرهابية في المستقبل. وتمر عملية التجنيد بأربع مراحل أساسية هي:

١ – **مرحلة العزل**:وتقوم على استراتيجية عزل العنصر المستهدف للتجنيد عن محيطه من الأصدقاء والأقارب، فتعطى له نصائح وتعليمات عبر الأنترنت لمقاطعة الجميع والاتصال الدائم بالتنظيم.

٢ – **مرحلة الملازمة**: وتعتمد على ملازمة المجند للتنظيم وتعزيز الانتماء له وإعلانه عضواً مهماً ومؤثراً في التنظيم، وحثّه على تبني بعض الشعارات الخاصة بالتنظيم وترديدها باستمرار وإقناعه بمشروع التنظيم، مع العمل على إقناعه بأن يكره ويكفر كل من هو خارج التنظيم.

٣ – **مرحلة المشاركة**: حيث يقدم التنظيم مطالب صغيرة للمجند لاختبار انتمائه، كبعض المهمات الثانوية.

٤ – **مرحلة الانخراط العملي**: يطلب من المجند إعلان انتمائه إلى التنظيم عن طريق وسائل التواصل الاجتماعي أو على وسائل الإعلام وهي المرحلة التي تجعله غير قادر على التراجع عن الالتزام تجاه التنظيم.

وقد نجح في هذا الإطار كل من تنظيم القاعدة وتنظيم الدولة الإسلامية في العراق والشام "داعش" في تجنيد عدد كبير من العناصر من خلال الدعوة عبر الأنترنت، فالتنظيم الأول يضم قسماً خاصاً بالمعلومات يمثل شركة إعلام نشطة جداً تسمى "شركة السحاب"، أما التنظيم الثاني فيعمل من خلال

(١٦) المنتدى العالمي للوسطية: الإرهابُ الإلكترونىّ مفهومه ووسائل مكافحته، ٢٠١٦/١٢/٢١ https://www.wasatyea.net/ar

خلايا للإعلام توظف قناتي "الفرقان" و"الفجر" وعدد من الشركات الإعلامية المستقلة الأخرى، التي كانت تبث الرسائل التي يتبنى فيها التنظيم مسؤوليته عن العمليات الإرهابية[١٧]. كما كان يستخدم تنظيم القاعدة عدد من الأساليب كاستخدام مقاهي الأنترنت لإرسال المواد الإعلامية والدعائية، فيقوم العناصر المكلفون بذلك بالتنقل إلى مقاهي أنترنت تكون بعيدة جداً عن مقار سكنهم، ويقومون بإرسال هذه الرسائل في شبكة الأنترنت عبر هذه المقاهي، مع الحرص على أن لا تتجاوز مدة مكوثهم بالمكان أكثر من خمس دقائق ثم مغادرة المكان فوراً حتى لا يقعوا في قبضة أجهزة الأمن[١٨].

من جهة أخرى أتاحت شبكة الأنترنت للتنظيمات الإرهابية أسلوباً جديداً من التدريب النمطي لأفرادها، فعوض إقامة معسكرات تدريب قابلة للاكتشاف من طرف الأجهزة الأمنية، أصبحت تقوم باستغلال شبكة الأنترنت في تقديم تدريب نوعي لعناصرها، حيث أن الاطلاع على بعض المواقع يتيح لنا اكتشاف الكم الهائل من المعلومات المتعلقة بكيفية عمل المتفجرات واستخدام مختلف أنواع الأسلحة وطريقة والتدريب على العديد من طرق القتل المختلفة[١٩]. فقد أصبحت التنظيمات الإرهابية في السنوات الأخيرة تقدم دروساً على الأنترنت تعتبر بمثابة ميدان للتدريب، وذلك من خلال نشر كتيبات عن أنواع الأسلحة وطرق استخدامها، وتقديم دورات في طرق صنع المتفجرات وإرشادات حول كيفية صناعتها محلياً في المنازل، وموضوعات أخرى ذات صلة على غرار مجلة "معسكر البتار" التابعة لتنظيم القاعدة والمنشورة على الأنترنت من طرف "جماعة المقاتلين في الجزيرة العربية"[٢٠]. وهناك أيضاً عدد من المواقع الأخرى التي تعتبر نوافذ إعلامية لهذه التنظيمات الإرهابية، مثلما هو الحال لموقع "النداء" الذي استخدمه تنظيم القاعدة بعد أحداث ١١ سبتمبر ٢٠٠١ لإصدار بياناته الإعلامية أو صوت "الجهاد" الذي كان يستخدمه تنظيم القاعدة في جزيرة العرب.

القسم الثاني
التشريع الدولي وسبل التصدي للجريمة الإرهابية الإلكترونية

يُعد التشريع الدولي أداة مهمة لمكافحة الجريمة الإرهابية الإلكترونية، حيث يوفر إطارًا قانونيًا مشتركًا للدول للتعاون في التحقيق في هذه الجرائم ومحاكمة مرتكبيها.

المبحث الأول: الجريمة الإرهابية الإلكترونية في التشريعات الدولية

التشريع الدولي للإرهابية الإلكترونية هو مجموعة من الاتفاقيات والمعاهدات الدولية التي تجرم الأعمال الإرهابية التي يتم تنفيذها من خلال وسائل إلكترونية أو رقمية. وقد تم تطوير هذا التشريع في السنوات الأخيرة استجابة لزيادة انتشار الإرهاب الإلكتروني، والذي يشكل تهديدًا خطيرًا للأمن الدولي.

(١٧) هشام الهاشمي، عالم داعش – من النشأة الى اعلان الخلافة، لندن: دار الحكمة للنشر والتوزيع، ٢٠١٥، ص٨٨، ٨٩.
(١٨) عبد الله حسين علي محمود: سرقة المعلومات المخزنة في الحاسب الآلي، القاهرة: دار النهضة العربية، ٢٠٠٢، ص ٣٠٨.
(١٩) عدنان هاشم سلطان صناعة الإرهاب، مصر: المكتب المصري الحديث، ٢٠٠٨، ص ١٣١.
(٢٠) هشام الهاشمي، مرجع سابق، ص ٨٨.

المطلب الأول: الاتفاقيات والمعاهدات الدولية التي تجرم الإرهاب الإلكتروني

ومن أبرز هذه الإتفاقيات وربما أهمها هي:

١) اتفاقية الأمم المتحدة لمكافحة الإرهاب (١٩٩٩)[٢١]

٢) اتفاقية مجلس أوروبا بشأن مكافحة الإرهاب[٢٢] (٢٠٠٥)

٣) اتفاقية الاتحاد الأوروبي لمكافحة الإرهاب[٢٣] (٢٠٠٢)

٤) اتفاقية منظمة التعاون الإسلامي لمكافحة الإرهاب[٢٤] (١٩٩٩)

تجرم هذه الاتفاقيات والمعاهدات مجموعة واسعة من الأعمال الإرهابية التي يتم تنفيذها من خلال وسائل إلكترونية أو رقمية، بما في ذلك عدد من الأمور الأخرى:

١) الهجمات الإلكترونية على البنية التحتية الحيوية.

٢) نشر المعلومات المضللة أو التحريضية.

٣) تمويل الإرهاب.

٤) التدريب على الإرهاب.

كما تتضمن هذه الاتفاقيات والمعاهدات تدابير قانونية وأمنية لمكافحة الإرهاب الإلكتروني، بما في ذلك:

١ – تبادل المعلومات الاستخباراتية بين الدول.

٢ – تعزيز التعاون الدولي في التحقيق في جرائم الإرهاب الإلكتروني.

٣ – تعزيز الوعي العام بمخاطر الإرهاب الإلكتروني.

بالإضافة إلى الاتفاقيات والمعاهدات الدولية، فقد وضعت بعض الدول تشريعات وطنية تجرم الإرهاب الإلكتروني .على سبيل المثال، فقد وضعت الولايات المتحدة قانون مكافحة الإرهاب الإلكتروني (٢٠١٨)[٢٥]، والذي يجرم مجموعة واسعة من الأعمال الإرهابية التي يتم تنفيذها من خلال وسائل إلكترونية أو رقمية.

المطلب الثاني:

التحديات التي تواجه التشريع الدولي

يُعد التشريع الدولي للإرهاب الإلكتروني أداة مهمة لمكافحة هذا التهديد المتزايد .ومع ذلك، لا يزال هناك حاجة إلى المزيد من الجهود لتعزيز هذا التشريع وتنفيذه على النحو الأمثل. فيما يلي بعض التحديات التي تواجه التشريع الدولي للإرهاب الإلكتروني[٢٦]:

١) التحدي التقني: يواجه التشريع الدولي صعوبة في مواكبة التطورات السريعة في مجال التكنولوجيا.

٢) التحدي القانوني: يختلف التشريع الوطني للإرهابية الإلكترونية من دولة إلى أخرى، ما يعقد التعاون الدولي في التحقيق في هذه الجرائم.

٣) التحدي السياسي: قد يكون من الصعب على الدول الاتفاق على إجراءات قانونية وأمنية مشتركة لمكافحة الإرهاب الإلكتروني.

من أجل مواجهة هذه التحديات، من المهم مواصلة تطوير التشريع الدولي لمكافحة الجريمة الإرهابية الإلكترونية وتعزيز التعاون الدولي في هذا المجال. وفيما يلي بعض المقترحات لتعزيز التشريع الدولي لمكافحة

---

(٢١) https://www.un.org/counterterrorism/ar/international-legal-instruments

(٢٢) https://www.europarabct.com

(٢٣) https://www.dw.com/ar

(٢٤) http://hrlibrary.umn.edu/arab/b207.html

(٢٥) www.washingtoninstitute.org

الجريمة الإرهابية الإلكترونية[ٓ]:

١ – مراجعة الاتفاقيات والمعاهدات الدولية لمكافحة الجريمة الإرهابية الإلكترونية بشكل دوري لضمان مواكبتها للتطورات السريعة في مجال التكنولوجيا.

٢ – تعزيز التعاون الدولي في مجال مكافحة الجريمة الإرهابية الإلكترونية من خلال تبادل المعلومات الاستخباراتية والتعاون في التحقيق في هذه الجرائم.

٣ – تطوير برامج توعية عامة بمخاطر الجريمة الإرهابية الإلكترونية في جميع الدول.

أيضاً وبهدف مواجهة هذه التحديات، من المهم مواصلة تطوير التشريع الدولي للإرهاب الإلكتروني وتعزيز التعاون الدولي في هذا المجال.

وقد دعت منظمة الأمم المتحدة الدول الأعضاء في مؤتمرها الثامن المتعلق بمنع الجريمة، إلى ضرورة اتخاذ إجراءات فعالة لمحاربة الجريمة الإرهابية الالكترونية، وذلك من خلال العمل على تحديث القوانين والتشريعات من جهة، وتفعيل التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من جهة ثانية، وذلك في ظل مراعاة حريات وحقوق الإنسان الأساسية وإشراك المجتمع المدني في محاربة هذه الجرائم، وتدعم هذا المؤتمر باتفاقية أخرى عقدتها هيئة الأمم المتحدة سنة ٢٠٠٠، والتي حملت عنوان "مكافحة اساءة استعمال التكنولوجيا لأغراض إجرامية"[٢٨].

وقد أكدت خلاله على الحاجة لتعزيز التعاون والتنسيق بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية أو إرهابية. أما على مستوى الدول، فتعتبر السويد أولى الدول التي وضعت قوانين لمحاربة الجريمة الإلكترونية وذلك سنة ١٩٧٣[٢٩]. وتبعتها الولايات المتحدة الأمريكية وبقية الدول الأوروبية تدريجياً، حيث طورت الدول الأوروبية تشريعاتها تماشياً مع تطور الجريمة الإلكترونية، ثم مع ظهور الجريمة الإرهابية الإلكترونية.

المبحث الثاني: سبل التصدي للجريمة الإرهابية الإلكترونية وآلياتها

المطلب الأول: طرق محاربة الجريمة الإرهابية الإلكترونية ومنافذها

تعتبر السبل القانونية المتمثلة في التشريعات الدولية والعمل على تطويرها بما يتناسب مع تطور الجريمة الإرهابية الإلكترونية من بين أهم سبل التصدي وآلياته لهذه الجريمة[٣٠]. فلا بد من إعادة النظر في طرق ومناهج عمل الشبكة المعلوماتية وخلق أنظمة مراقبة ومتابعة متطورة للقضاء على ظاهرة الجريمة الإرهابية الإلكترونية أو الحد من خطورتها.

ويعتبر تطوير التشريعات القانونية باستمرار، وذلك لمواكبة التطور المستمر للجرائم الإرهابية الإلكترونية وتماشياً مع تطور

(٢٦) د. عبد الوهاب كريم: الامن السيبراني– القيود والتحديات في ضوء قواعد القانون الدولي، دراسة منشورة في مجلة العقد الإجتماعي، العدد ٩، سلطنة عمان، ٢٠٢١.

(٢٧) د. جورج لبكي: المعاهدات الدولية للإنترنت – حقائق وتحدّيات، مجلة الجيش (لبنان)، العدد ٨٣، كانون الثاني ٢٠١٣.

(٢٨) اتفاقية هيئة الأمم المتحدة، رقم ٦٣/٥٥ – ٢٠٠٠، حول مكافحة اساءة استعمال المعلومات لأغراض إجرامية، كانون الأول ٢٠٠٠.

(٢٩) عبد الله حسين علي محمود: مرجع سابق، ص ٣٠٨.

(٣٠) خلفوني فايزة: سبل وآليات مكافحة الجرائم الالكترونية: قراءة في التجربة القطرية (٢٠٠٥–٢٠١٤)، مجلة التميز الفكري للعلوم الاجتماعية والإنسانية، العدد الثالث، ص. ١١–٢٤، ٢٣/١/٢٠٢١.

استخدام مختلف تقنيات التكنولوجيا الحديثة، عنصراً مهماً في مجال التصدي ببجريمة الإرهابية الإلكترونية. كما أن استخدام نفس الأساليب التي تعتمدها التنظيمات الإرهابية في هذا المجال، مثل التجسس والقرصنة واختراق المواقع واستخدام العملاء وغيرها...، تعتبر طريقة مهمة للغاية.

إن التواصل عبر شبكة الأنترنت مع هؤلاء المجرمين والحوار معهم بغرض إقناعهم لتغيير مبادئهم وأفكارهم، فالحوار كما يعتبره (Jacques Bourrinet) وسيلة ونداء للعمل العقلاني السلمي الهادف إلى تغيير الوضع نحو الأحسن(٣١).

المطلب الثاني: خطوات التصدي للجريمة (الإرهابية الإلكترونية) من خلال التشريع الدولي

يجب تطوير أنظمة التكوين والتدريب والتوعية بالنسبة لفئة الشباب من أجل تفادي استغلالهم من طرف المجرمين على شبكة الأنترنت، واستخدام وسائل الإعلام لنشر ثقافة التبليغ لدى المواطنين على كل حالات الاستخدام غير القانوني أو الأخلاقي لشبكة الانترنت خاصة في الأماكن العمومية مثل مقاهي الأنترنت من الوسائل المساندة والمساعدة في التصدي للجريمة الإرهابية الإلكترونية

ويمكننا تلخيص سبل التصدي للجريمة الإرهابية الإلكترونية من خلال التشريع الدولي فيما يأتي(٣٢):

* التشريع الدولي الموحد: الذي يُعد أداة مهمة لمكافحة الجريمة الإرهابية الإلكترونية، حيث يوفر إطارًا قانونيًا مشتركًا للدول بهدف التعاون في التحقيق في هذه الجرائم ومحاكمة مرتكبيها.

* التعاون الدولي: وهو أمر أساسي لمكافحة الجريمة الإرهابية الإلكترونية، حيث تتطلب هذه الجرائم عادةً جهودًا متعددة الأطراف من أجل التحقيق فيها ومحاكمة مرتكبيها.

* التوعية العامة: التي تعتبر أمرًا مهمًا للوقاية من هذه الجرائم، حيث يمكن للأفراد والمجتمعات أن يؤدوا دورًا مهمًا من خلال التعرف عليها واتخاذ الإجراءات المناسبة للوقاية منها.

وقد ركز مجلس الأمن اهتمامه على مكافحة استغلال تكنولوجيا المعلومات والاتصالات للأغراض الإرهابية لأكثر من ٢٠ عاما واتخذ ١٥ قرارا تتعلق بمكافحة الإرهاب وأصدر أربع وثائق سياسية بشأن هذه المسألة. ولاحظ المجلس في قراره ٢٠١٣/٢١٢٩ تطور الصلة بين الإرهاب وتكنولوجيات المعلومات والاتصالات، ولا سيما شبكة الإنترنت، واستخدام هذه التكنولوجيات لارتكاب أعمال إرهابية وتيسير ارتكابها. وأشار المجلس في قراره ٢٠٢١/٢٦١٧، إلى استخدام الإنترنت والأشكال الأخرى من تكنولوجيا المعلومات والاتصالات وسائر التكنولوجيات الناشئة لأغراض إرهابية(٣٣).

أيضاً، أوعز مجلس الأمن في قراره

(٣١) Jacques Bourrinet, Le Dialogue Euro-Arabe, Paris: Economica, 1979, p.16-17.

(٣٢) بشريف وهيبة: أساليب الجريمة الإلكترونية، مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الالكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي الجزائرية، العدد ٨، ص. ٥٤-٦٥، ٢٠١٩/١/١.

(٣٣) https://www.un.org/counterterrorism/ar

٢٠١٧/٢٣٤١ إلى لجنة مكافحة الإرهاب، مدعومةً بالمديرية التنفيذية للجنة مكافحة الإرهاب، أن تدرس جهود الدول الأعضاء المبذولة من أجل حماية البنى التحتية الحيوية من الهجمات الإرهابية، بوصفها ذات صلة بتنفيذ القرار ٢٠٠١/١٣٧٣ ومن أجل تحديد الممارسات الجيدة والثغرات ومواطن الضعف في هذا الميدان. وفي عام ٢٠١٨، قامت المديرية التنفيذية والإنتربول ومكتب مكافحة الإرهاب بوضع الخلاصة المعنونة" حماية البنى التحتية الحيوية من الهجمات الإرهابية: خلاصة وافية للممارسات الجيدة، والتي يمكن استكمالها في الوقت المناسب بإضافة تتناول المسائل السيبرانية على نحو أكثر تحديداً[٣٤].

الخاتمة

يمكن القول إن التطور الذي شهدته الجريمة الإرهابية الإلكترونية، جعل منها شكلاً جديداً من الجرائم التي تختلف اختلافاً جذرياً عن أشكال الجريمة الأخرى التي عرفها التاريخ، فهي تشكل تهديدات أمنية خطيرة جداً غير ظاهرة وغير ملموسة بإمكانها إحداث انهيار في الاقتصاد العالمي، وهذا ما أصبح يطرح تحديات كبيرة بالنسبة إلى المجتمعات والدول على حد سواء، ويتطلب ضرورة تطوير سبل وآليات التصدي لها.

إن دور الدولة وحده أصبح غير كافٍ في ظل اتساع دائرة هذا النوع من الجريمة، وهو ما يتطلب تعاون وتحالف على المستوى الدولي بين الدول والمنظمات الدولية هذا من جهة، ومن جهة ثانية تعاون على المستوى المحلي بين الأجهزة الأمنية للدولة الواحدة ومنظمات المجتمع المدني والمواطنين، كما أنه من الضروري العمل على تطوير التشريعات القانونية الدولية والمحلية لمعاقبة مثل هذه الجرائم، وتطوير الوسائل والآليات الرقابية على استخدام الأنظمة الالكترونية بصفة عامة.

لا شك بأن الأساليب المتبعة والجهود المبذولة من أجل التصدي للجريمة الإرهابية الإلكترونية هي جهود جبارة إن كان على المستوى الدولي أو المحلي، فضلاً عن مساعي الأمم المتحدة والاتحاد الأوروبي والأنتربول الدولي والعديد من المنظمات الدولية والإقليمية. غير أن كل هذه المساعي والجهود بإمكانها أن تتعزز عبر المقترحات الآتية:

١) ضرورة السعي إلى عقد مؤتمر دولي، بشكل دوري، بإشراف الأمم المتحدة لتحديد الخطط العملية الدولية لمكافحته الجريمة الإرهابية الإلكترونية بجميع صورها وأشكالها مع احترام سيادة الدول الأعضاء.

٢) التشديد من قبل المجتمع الدولي على أن الإرهاب ليس له دين معين أو جنس أو جنسية أو منطقة جغرافية محددة.

٣) التأكيد على أهمية دور وسائل الإعلام (لا سيما العالمية منها) والمؤسسات المدنية ونظم التعليم في بلورة إستراتيجيات للتصدي للمزاعم الإرهابيين.

٤) تشجيع كل دولة والدول في العالم ودفعها نحو زيادة التعاون على المستوى الوطني والإقليمي والدولي للتنسيق بين الأجهزة المختصة بمكافحة الإرهاب الإلكتروني، لتبادل الخبرات والتجارب والمعلومات.

٥) الدعوة إلى تطوير القوانين والإجراءات الوطنية والدولية الجنائية الكفيلة بمنع الإرهابيين من استغلال قوانين اللجوء والهجرة للحصول على ملاذ آمن أو استخدام أراضي الدول

(٣٤) https://www.un.org/counterterrorism/ar

كقواعد للتجنيد أو التدريب أو التخطيط أو التحريض أو الانطلاق منها لشن الهجمات وتنفيذ الجرائم الإرهابية الإلكترونية ضد الدول الأخرى.

٦) حث الدول إلى الإسراع والانضمام إلي الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب الإلكترونية والسعي الى تطويرها وتحديث بنودها كلما دعت الحاجة.

ختاماً، مع انتشار ظاهرة الذكاء الإصطناعي التي تغزو العالم بوتيرة متسارعة، يلاحظ أن هذه الظاهرة تستخدم لأغراض صحية وتربوية واقتصادية وصناعية وصحية وعسكرية وغيرها كثير من المجالات، فهل سيكون للجريمة الإرهابية الإلكترونية وافر النصيب من ظاهرة الذكاء الإصطناعي في المستقبل القريب أو البعيد؟