رابطة العالم الإسلامي

الأمانة العامة

الإدارة العامة للمؤتمرات والمنظمات

طبيعة
الإرهاب الإلكتروني

إعداد

الدكتور عبد القادر الشيخلي

المستشار في رابطة العالم الإسلامي

مقدم إلى

المؤتمر الإسلامي العالمي

مكافحة الإرهاب

الذي تنظمه

رابطة العالم الإسلامي

تحت رعاية خادم الحرمين الشريفين

الملك سلمان بن عبد العزيز آل سعود

مكة المكرمة

٣ - ٦ / جمادى الأولى / ١٤٣٦ هـ، الموافق: ٢٢ - ٢٥ / فبراير / ٢٠١٥ م

رابطة العالم الإسلامي

مكة المكرمة – المملكة العربية السعودية

صندوق البريد (٥٣٧) أو (٥٣٨) مكة المكرمة (٢١٩٥٥)

هاتف: ٠٠٩٦٦١٢٥٦٠٠٩١٩ – الفاكس: ٥٦٠١٣١٩ – ٥٦٠١٢٦٧

برقياً: رابطة – مكة، تلكس: ٥٤٠٠٠٩ و٥٤٠٣٩٠

www.themwl.org

البريد الإلكتروني للإدارة العامة للمؤتمرات والمنظمات

conferences@themwl.org

واتس أب: ٠٠٩٦٦٥٠٣٣٩٦٣٢٠ :whatsApp

بسم الله الرحمن الرحيم

مقدمة

الحمد لله الذي هدانا للبحث العلمي، وما كنا لنهتدي لولا أن هدانا الله رب العالمين، والصلاة والسلام على سيد المرسلين، محمد النبي الأمين، وعلى أصحابه الغر الميامين وأمهات المؤمنين، ومن تبعهم جميعاً إلى يوم الدين، أما بعد:

فإن الإرهاب فعل قائم على العنف، أخذ يستشري بعد انتهاء الحرب الباردة بين المعسكرين الرأسمالي والشيوعي، إذ لم يعُد ثمة شيء يشغل بعض الأطراف الدولية ذات المصالح الاقتصادية والسياسية، فأخذ التنازع صيغة الإرهاب باعتباره الأداة الجديدة لإضعاف دول ومجتمعات أخرى، والتركيز على العامل الدولي للإرهاب مسألة في غاية الأهمية، كي يكون تفكير الباحث عن الموضوع متكاملاً، فالمصالح الدولية لها أولوية في عالم اليوم، والعلاقات الدولية تفتقر إلى الأخلاق، وأن مكانة الأخلاق نظرياً موجودة ضمن بنود القانون الدولي ومن ثم المواثيق الدولية التي تشكل النصوص الرسمية الواضحة، والعلاقات الدولية لا تسير ضمن ضوابط نظامية دائماً، وإنما مصلحة هذه الدولة الكبرى أو تلك تقتضي انتهاك سيادة هذه الدولة أو تلك وذلك بتشجيع الجماعات الإرهابية عن طريق ممارسة العنف ضد النظام السياسي القائم في الدولة، فتُمَد هذه الجماعات بالمال والسلاح، وقد توفر لها المأوى الآمن. فإذا انتقلنا إلى حالة الفقر في دولة ما فإن جماعات الإرهاب تجد فيه الفرصة الكبيرة للانطلاق والحركة، فوأد بؤَر الفقر والبطالة هي من أولويات الوقاية من الإرهاب، وحينما

ينحرف الفكر المذهبي لدى هذه الطائفة أو الأخرى، وتشعر نفسها بالدونية أو التهميش فتضع يدها بيد الإرهاب، ولعل ترويج ثقافات التسامح والحوار والمشاركة هي من أكثر الطرق فعالية لوأد الفكر الطائفي المنغلق.

إن الإرهاب هو كيان موجود في جميع الدول حتى تلك التي تتغنى بديمقراطياتها وحقوق الإنسان فيها، ولكن ثمة عوامل خارجية أو داخلية هي التي تحرك هذا الكيان الخبيث للعمل على إرهاق المجتمع بتخويفه وإلحاق الضرر فيه على مستويات الجماعات والأفراد إضافة إلى الأضرار التي يسببها الإرهاب في كيان الدولة ذاتها وسمعتها وسلطاتها وأجهزتها.

إن إلقاء الأضواء إلى حد الاكتفاء على موضوعات الإرهاب من حيث النشأة والاستقلال والقوى الفاعلة في توجيهه لهي من الدراسات والبحوث العلمية ذات المطلب الآني المُلحّ.

وجدير بالذكر أن المجرمين يستفيدون فائدة مباشرة من التقدم العلمي والتكنولوجي في عالم اليوم، وذلك بتطوير وسائلهم وأساليبهم الإجرامية بطرق تستثمر هذا التقدم لبلوغ مآربهم غير المشروعة، ولعل الإرهاب الإلكتروني في الوقت الحاضر هو الإرهاب الأحدث في العالم، إذ تهيء التكنولوجيا وشبكة المعلومات الدولية «الانترنت» والحاسب الآلي مجالاً أوسع لعمل جماعات الإرهاب والتطرف والفكر المنحرف في ضوء هذا الإدراك أصبحت مهمة مكافحة الإرهاب أكثر صعوبةً وتعقيداً، لأن حركة الإجرام الإلكتروني اتسعت بحيث أصبحت مواجهتها أكثر من شاقة، لذلك فإن جلالة مهمة المكافحة تحفز على ملاحقة فاعلي الإرهاب الإلكتروني كيلا تُترك ساحة العمل دون رقيب أو حسيب، ومن هنا تبدو المهمة آنية ومستقبلية ودون منظور واضح.

ومن الله الرشاد والسداد وإليه حسن المعاد.

المبحث الأول
معنى الإرهاب الإلكتروني

تعريف جريمة الإرهاب:

يُعرّف قانون العقوبات المصري الصادر سنة ١٩٣٧م الإرهاب بأنه كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأَمْنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو المواصلات أو بالأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح[١].

بينما تُعرّف الاتفاقية العربية لمكافحة الإرهاب بأنه كل فعل من أفعال العنف أو التهديد به أيًا كانت دوافعه أو أغراضه،يقع تنفيذاً لمشروع إجرامي فردي أو جماعي،ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر[٢].

---

(١) عُدل قانون العقوبات المصري الصادر في سنة ١٩٣٧م، بالقانون رقم (٩٧) لسنة ١٩٩٢م، وذلك لإيراد نص حديث لتجريم الإرهاب.

(٢) هي الاتفاقية الصادرة في القاهرة من مجلس وزراء الداخلية العرب في سنة ١٩٩٨م.

في حين عرَّف مجمع البحوث الإسلامية بالأزهر الإرهاب بأنه ترويع الآمنين، وتدمير مصالحهم ومقومات حياتهم، والاعتداء على أموالهم وأعراضهم وحرياتهم، وكرامتهم الإنسانية، بغياً وإفساداً في الأرض[١].

ولجأ الاتحاد الأوروبي في سنة ٢٠٠٢م إلى تعريف الإرهاب بأنه أعمال ترتكب بهدف ترويع الأهالي أو إجبار حكومة أو هيئة دولية على القيام بفعل أو الامتناع عن القيام بفعل ما، أو تدمير الهياكل الأساسية السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو هيئة دولية، أو زعزعة استقرارها[٢].

أما مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فقد عرّف في سنة ١٤٢٢هـ الإرهاب بأنه العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان في دينه ودمه وعقله وماله وعِرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصور الحرابة وإخافة السبيل وقطع الطريق، وكل فِعلٍ من أفعال العنف أو التهديد، يقع تنفيذاً لمشروع إجرامي فردي أو جماعيٍ، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أموالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة، أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها[٣].

---

(١) بيان مجمع الفقه الإسلامي بالأزهر، بشأن ظاهرة الإرهاب صدر في ١٥/ ٨/ ١٤٢٢هـ.

(٢) د. أحمد فتحي سرور: المواجهة القانونية للإرهاب، القاهرة، دار النهضة العربية، ٢٠٠٨م، ص١٦.

(٣) رابطة العالم الإسلامي - مجمع الفقه الإسلامي: بيان مكة المكرمة، الدورة السادسة عشرة، ١٤٢٢هـ.

أما مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي فقد عرّفه في سنة ١٤٢٧هـ بأنه العدوان أو التخويف أو التهديد ماديـًا أو معنويـًا الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، بشتى صنوف العدوان وصور الإفساد في الأرض[١].

خصائص الإرهاب الإلكتروني:

يتميز الإرهاب الإلكتروني بعددٍ من الخصائص والسمات التي يختلف فيها عن بقية الجرائم، وتحول دون اختلاطه بالإرهاب العادي، ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يلي:

أ- يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متجاوزة للحدود، وعابرة للدول والقارات، إذ أنها غير خاضعة لنطاق إقليمي محدود.

ب- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، لنقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم[٢].

ج- إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية الدولية ومزود ببعض البرامج اللازمة.

---

(١) منظمة المؤتمر الإسلامي - مجمع الفقه الإسلامي، قرار رقم ١٢٨ (٢/ ١٤) بشأن حقوق الإنسان والعنف الدولي، صادر في ١١-١٦/ ١/ ٢٠٠٣م، قطر، الدوحة ٢٠٠٣م.

(٢) د. السيد عتيق: جرائم الانترنت، القاهرة، دار النهضة العربية، ٢٠٠٤م، صادر ١٣.

د- صعوبة الإثبات في الإرهاب الإلكتروني، نظراً لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.

هـ- يتميز الإرهاب الإلكتروني بأنه يتم عادة بتعاون أكثر من شخص على ارتكابه.

و- أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية[١].

أغراض الإرهاب الإلكتروني:

أبرز أغراض عصابات الإرهاب الإلكتروني هي:

١- أغراض إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم، وإثارة الفوضى ونشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة.

٢- تعطيل الأداء الطبيعي لنظم السيطرة والرقابة الإلكترونية، وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الاستراتيجية في الدولة.

٣- الإخلال بالنظام العام، والأمن المعلوماتي، وزعزعة الطمأنينة، وتعريض سلامة المجتمع وأمنه للخطر، وإثارة الرأي العام.

---

(١) د. حسن مظفر الرزو: الفضاء المعلوماتي، بيروت، مركز دراسات الوحدة العربية، ٢٠٠٧م، صادر ٢٨.

٤- إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

٥- تهديد السلطات العامة والمنظمات الدولية وابتزازها.

٦- جمع الأموال والاستيلاء عليها[١].

(١) انظر: - د. عبدالله بن عبدالعزيز العجلان: الإرهاب الإلكتروني في عصر المعلومات، القاهرة ٢٠١٣م، ص١٤.

- يونس محمد عرب: الإطار القانوني للإرهاب الإلكتروني واستخدام الانترنت للأغراض الإرهابية، الرياض، جامعة نايف العربية للعلوم الأمنية، ١٤٣٣هـ ٢٠١٢م ص١٥٨.

المبحث الثاني
وسائل وأساليب الإرهاب الإلكتروني

يمكن للمجرم الإلكتروني أن يخترق البريد الإلكتروني، وأن ينشئ ويدمر المواقع القائمة[١]، وفيما يلي بيان ذلك بثلاثة مطالب مستقلة:

المطلب الأول: اختراق البريد الإلكتروني:

جرى استخدام البريد الإلكتروني بصورة واسعة جداً وهذا مما سهل نقل المعلومات بين الدول، ولكن نجد في الآونة الأخيرة إساءة استخدام هذا البريد حيث أصبح يمثل إرهاباً إلكترونياً عالمياً يهدد العالم بأَسره، ويكمُن خطر استخدام ذلك - سهولة استخدامه - فيقوم بذلك الإرهابي وهو في مكتبه أو غرفة نومه سواء أكان في بيته أم في فندقه، أم في مكان آخر، ويعتبر البريد الإلكتروني من أهم الوسائل في التواصل بين الإرهابيين وتبادل المعلومات لذلك يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية، وما يقوم به الإرهابيون أيضاً من اختراق البريد الإلكتروني للآخرين، وهتك أسرارهم.

---

(١) في التوسع انظر:

- د. عبدالرحمن بن عبدالله السند: وسائل الإرهاب الإلكتروني، حكمها في الإسلام، وطرق مكافحتها، بحث للمؤتمر العالمي عن موقف الإسلام من الإرهاب.
- د. عبدالرحمن بن عبدالله السند: الأحكام الفقهية للمعاملات الإلكترونية، الرياض، دار الوراق، ١٤٢٤هـ - ٢٠٠٤م ص٢٧٧ وما بعدها.

المطلب الثاني: إنشاء مواقع على الإنترنت:

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات الدولية (الإنترنت) لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أُنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك، وتسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الإنترنت في شهر أكتوبر سنة ٢٠٠٠م إلى أكثر من (٢٢) مليون موقع.

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادُل الآراء والأفكار والمعلومات صعباً في الواقع، فإن الإنترنت تسهل هذه العملية كثيراً، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، ويتبادلوا الحديث والاستماع لبعضهم عبر الإنترنت، بل يمكن أن يجمعوا لهم أتباعاً وأنصاراً عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الإنترنت، ومنتديات الحوار، وما يسمى بغرف الدردشة، فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلاً ممكناً، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمنوا انتشاراً أوسع، وحتى لو تم منع الدخول إلى بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها، ولقد وجد الإرهابيون بغيتهم في تلك الوسائل الرقمية في ثورة المعلوماتية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة المعلومات الدولية (الإنترنت)، فغدَت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب الإلكتروني.

المطلب الثالث: تدمير المواقع القائمة:

يقصد به: الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (Server-PC)، أو مجموعة نظم مترابطة شبكياً (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراق المواقع بشكل دائم، فالمتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source) سواء أكان ذلك في مكونات نقطة الاتصال أم النظم أم الشبكة أم البرمجة، جعلَت الحيلولة دون الاختراقات صعبة جداً، إضافة إلى أن هناك منظمات إرهابية تُدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع، ومن المعلوم أن لدى المؤسسات من الإمكانات والقدرات ما ليس لدى الأفراد.

إن من الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه.

أسباب وقوع عملية تدمير المواقع: من هذه الأسباب ما يأتي:

١ - ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية

كسر وتخمين الكلمات السرية من المخترِق.

٢- عدم وضع برامج حماية كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق للموقع.

٣- استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج وأنظمة غير موثوقة أمنيًا ولا يتم تحديثها باستمرار.

٤- عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.

٥- عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة فيه، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في المواقع للضياع وعدم إمكانية استرجاعها، ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في الآونة الأخيرة، ويعد عام ٢٠٠٢م من أكثر الأعوام اختراقًا، فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات[1].

(١) د. عبدالرحمن بن عبدالله السند: الأحكام الفقهية للمعاملات الإلكترونية، مرجع سبق ذكره، ص٢٩٤.

المبحث الثالث
أسباب سهولة اقتراف الإرهاب الإلكتروني

فيما يلي الأسباب المغرية لاقتراف هذه الجريمة:

أولاً: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها؛ رغبة في التوسع وتسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية.

ثانيًا: غياب الحدود الجغرافية وتدني مستوى المخاطرة: إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعدُّ فرصة مناسبة للإرهابيين، حيثُ يستطيع محترف الحاسوب أن يقدِّم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ومن ثم يشنُّ هجومَه الإلكتروني وهو مسترخٍ في منزله من دون مخاطرة مباشرة، وبعيداً عن أعين الناظرين.

ثالثا: سهولة الاستخدام وقلة التكلفة: إن السمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام، طيعة الانقياد، قليلة الكلفة، لا تستغرق وقتًا ولا جهداً كبيراً، مما هيَّأ للإرهابيين فرصةً ثمينةً للوصول إلى أهدافهم غير المشروعة، ومن دون الحاجة إلى مصادر تمويل ضخمة، فالقيام بشن هجوم إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية الدولية ومزود بالبرامج اللازمة.

رابعًا: صعوبة اكتشاف وإثبات الجريمة في هذا النوع من الإرهاب: في كثير من أنواع الجرائم المعلوماتية لا يُعلم بوقوع الجريمة أصلاً وخاصة في مجال جرائم الاختراق، وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفّذ جريمته، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تعطي المجرم أملاً في الإفلات من العقوبة.

خامسًا: الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية: يعتبر الفراغ التنظيمي والقانوني لدى بعض المجتمعات الدولية حول الجرائم المعلوماتية والإرهاب الإلكتروني من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، وكذلك لو وُجِدت قوانين تجريمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة، ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق، كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يُعرَض على الشبكة، وتسيطر على مُدخلاتها ومُخرجاتها يعدُّ سببًا مهمًا في تفشي ظاهرة الإرهاب الإلكتروني، حيثُ يمكن لأي شخص الدخول ووضع ما يريد على الشبكة، وكل ما تَملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة، أو إغلاقها وتدميرها بعد نشر المجرم لما يريده فيها، لكلِّ هذه الأسباب والدوافع أصبح الإرهاب الإلكتروني هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية[١].

---

(١) د. عبدالله العجلان، مرجع سبق ذكره، ص٤٨.

المبحث الخامس
مكافحة الإرهاب الإلكتروني

لا يمكن لأيّ دولة في هذا العصر خاصة من بداية هذا القرن أن تعيش بمعزل عن التكنولوجيا، لأنها أصبحت من أهم وسائل التواصل العالمي، وأداة ترابط بين دول العالم، وفي ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والاتصالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات، بات من الضروري لكل بلد حماية أفراده ومؤسساته ومقدراته وحضارته من آثار هذا الانفتاح، ومع إدراك الجميع اليوم للفوائد الجمة لتقنية المعلومات، فإن المخاطر الكامنة في تغلغل هذه التقنية في بيوتنا ومؤسساتنا تتطلب من المجتمع والدولة جميعًا الحيلولة دون حصول تلك المخاطر بشتى أنواعها، ومن أهم ما يجب توفيره في هذا الصدد حجب المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلّم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، فهذا الأسلوب يعد من الأساليب المجدية والنافعة، فالإنسان لا يعرّض نفسه للفتن والشرور، بل المسلِم يسأل ربَّه أن يحفظَه من التعرض للفتن.

وجاء في بعض الدراسات أنَّ الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم؛ ولذلك سعت مدينة الملك عبدالعزيز للعلوم والتقنية إلى حجب المواقع الإباحية عن مستخدمي (الإنترنت) في المملكة العربية السعودية حفاظًا على الأخلاق وصيانة للأمَّة من عبثِ العابثين وإفساد المجرمين، فقد صدر في عام ١٤١٧هـ قرار مجلس

الوزراء رقم (١٦٣) الذي أناط بمدينة الملك عبدالعزيز للعلوم والتقنية مهمة إدخال خدمة (الإنترنت) الدولية للمملكة، وتولي جميع الإجراءات اللازمة بما في ذلك ترشيح المحتوى[١].

وتتم الحماية الفنية بعدة وسائل منها:

أولاً: تشفير البيانات المهمة المنقولة عبر الإنترنت.

ثانيًا: إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

ثالثًا: توفير برامج الكشف عن الفيروسات والمقاومة لها لحماية الحاسب الآلي والبيانات والمعلومات من الإضرار بها.

رابعًا: عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، مع عمل وسائل التحكم في الدخول إلى المعلومات والمحافظة على سريتها.

خامسًا: توزيع مهام العمل بين العاملين، فلا يعطى المبرمج مثلاً وظيفة تشغيل الحاسب الآلي عمله، ففي هذه الحالة سوف يكون قادراً على كتابة برامج قد تكون غير سليمة، ومن ثمَّ تنفيذها على البيانات الحقيقية، كما يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين، مما يجعلُ كتابة برامج ضارة أمراً صعبًا.

إن المحافظة على المعلومات من أهم ما تحرص عليه الهيئات والمنظمات والدول، وحتى على مستوى الأفراد، إذ يمكن تعويض فقدان الأجهزة

---

(١) مجموعة من المؤلفين: موقف المملكة العربية السعودية من الإرهاب، الرياض ١٤٢٦هـ - ٢٠٠٦م.

والبرامج، ولكن تعويض فقدان البيانات والمعلومات أو التلاعب بها يعد من الأمور الصعبة والمكلفة، فالمعلومات والبيانات تعد من أهم ممتلكات أي منظمة، لذا يتم السعي للمحافظة على البيانات والمعلومات قدر الإمكان حتى لا يصل إليها أشخاص غير مصرح لهم، ويتم اتّباع مجموعة من الإجراءات التي تضمن سلامة هذه المعلومات منها ما يأتي:

١- عدم إلقاء مخرجات الحاسب الآلي، أو شريط تحبير الطابعة؛ لأنّ مثل هذه المخرجات قد تحتوي على معلومات مهمة تصل إلى أشخاص غير مصرح لهم الاطلاع عليها، لذا يجب تمزيق المخرجات بواسطة آلات خاصة قبل إلقائها.

٢- استخدام كلمات السر للدخول إلى الحاسب الآلي، وتغييرها كل فترة بحيث تعتمد طول الفترة على أهمية البيانات بالنسبة للمنظمة، كما أنّ بعض أنظمة التشغيل لا تسمح باستخدام كلمة السر نفسها مرة أخرى، وتجبرك على تغييرها بعد فترة محددة من قبل المشرف على نظام التشغيل.

٣- عمل طرق تحكّم داخل النظام تساعد على منح محاولات الدخول غير النظامية مثال ذلك: عمل ملف يتم فيه تسجيل جميع الأشخاص الذين وصلوا أو حاولوا الوصول إلى أي جزء من البيانات: يحوي رقم المستخدم، ووقت المحاولة وتاريخها ونوع العملية التي قام بها وغير ذلك من المعلومات المهمة.

٤- توظيف أشخاص تكون مهمتهم المتابعة المستمرة لمخرجات برامج الحاسب الآلي للتأكّد من أنها تعمل بشكل صحيح، وخاصة البرامج

الماليـة التـي غالبـاً مـا يكـون التلاعـب بهـا مـن قبـل المبرمجـين أو المستخدمين، وذلـك عـن طريـق أخـذ عينـات عشـوائية لمخرجـات البرنـامج في فـترات مختلفـة، كمـا يقومـون بفحـص ملـف المتابعـة للتعـرف علـى الأشـخاص الـذين وصـلوا إلـى البيانـات، أو حـاولوا الوصول إليها[١].

(١) د. سليمان بن عبدالله أبا الخيل: موقف المملكة العربية السعودية من الإرهاب، الرياض ١٤٣٣هـ، ص٢٩٩.

خاتمة
في النتائج والتوصيات

بعد الانتهاء من بحث طبيعة الإرهاب الإلكتروني، توصلت إلى جملة نتائج وكذلك جملة توصيات، وفيما يلي بيان ذلك:

أولاً: النتائج:

١- يعد الإرهاب الإلكتروني، الشكل الأحدث للإرهاب، وهو إرهاب الحاضر والمستقبل، توسل بالتقنيات والمعلومات لإيجاد أهداف جديدة للعمليات الإرهابية، وأصبح هذا الإرهاب مهدِّدا للسِّلم والأمن الدوليين فخطره غير محصور في منطقة جغرافية دون أخرى.

٢- ظهَر أن تقنيات المعلومات غير قادرة على حماية الناس من العمليات الإرهابية.

٣- سعت دول العالم إلى اتخاذ تدابير احترازية لمواجهة الإرهاب الإلكتروني، إلا أن هذه الوسائل مازالت قليلة وضعيفة.

٤- دعت المملكة العربية السعودية دول العالم إلى مكافحة الإرهاب أيـًا كان مصدره ونوعه، ومعاقبة مقترفيه عقابـًا صارمـًا، كما رفضت المملكة إلصاق الإرهاب بالإسلام والمسلمين، لأن ديننا هو دين الإسلام والعدالة والحق والتسامح.

٥- إن ضعف بنية الشبكات المعلوماتية، وقابليتها للاختراق، وسهولة استخدام الحاسب الآلي، وقلة تكلفة هذا الاستخدام، وغياب الحدود الجغرافية، وصعوبة اكتشاف المجرمين، سهّل كل ذلك من انتشار جرائم الانترنت التجارية والاجتماعية وكذلك الجرائم الإرهابية.

ثانياً: التوصيات:

١- ضرورة خضوع جميع المعاملات الإلكترونية للأحكام الشرعية والقانونية من خلال قوانين تحدِّد ما هو مباح وما هو محظور، ويجب مراجعة هذه القوانين كل فترة زمنية لأن المجرمين يستفيدون من بعض الثغرات أو الخلل في هذه القوانين، وذلك لتقويمها من قبل السلطة العامة، وإجراء التعديلات عليها بالزيادة أو الحذف.

٢- ضرورة متابعة أرباب الأسر لأبنائهم، عند استخدامهم لتقنيات المعلومات وبخاصة شبكة المعلومات الدولية (الانترنت)، للتأكد من سلامة الاستخدام وشرعيته، وإفهام هؤلاء الأبناء أن الموضوع يخص أمن الوطن والمواطن، فلا مجال للعبث أو تجربة أفعال محظورة شرعاً وقانوناً.

٣- ضرورة تكثيف الدورات الفنية والعلمية لرجال الأمن المسؤولين بمكافحة النشاط الإرهابي، سواء داخل البلاد أو خارجها وذلك لتحديث معلوماتهم وتزويدهم بخبرات فنية جديدة من أجل إنجاح مهامهم الوقائية والمكافحية.

٤- ضرورة نشر الوعي العلمي بين أفراد المجتمع، ولاسيما الشباب، بمخاطر التعامل غير الشرعي بالمواقع الإلكترونية، وبيان النتائج المترتبة على هذا الاستخدام غير المشروع.

٥- ضرورة نشر طرق الوقاية من الإرهاب الإلكتروني والعمليات الإجرامية الإلكترونية عموماً وذلك بتخطيط دور الأسرة والمسجد والمدرسة والجامعة ضمن خطة استراتيجية علمية متكاملة يشد كل جانب فيها

الجانب الآخر، فيكمل المسجد دور الأسرة، وتكمل المدرسة دور المسجد، وتكمل الجامعة دور الجميع.

٦- للإعلام دور جوهري في هذا الشأن، إذ أنه يتعامل مع الأفراد مباشرة، سواء كان مسموعاً أو مقروءًا أو مشاهداً، الأمر الذي يتطلب منه إبداع برامج تبين مخاطر الإرهاب عموماً والإرهاب الإلكتروني خاصة، وأن تتبع وسائل الإقناع المنطقية، وأن تلهم زبون الإعلام بأن دوره أساسي في الوقاية والمكافحة، فالخطر محدق بالجميع.

المصادر والمراجع

١ - د. أحمد فتحي سرور: المواجهة القانونية للإرهاب، القاهرة دار النهضة العربية، ٢٠٠٨م.

٢ - د. السيد عتيق: جرائم الانترنت، القاهرة دار النهضة العربية ٢٠٠٤م.

٣- د. حسن مظفر الرزو: القضاء الإلكتروني، بيروت، دار دراسات الوحدة العربية، ٢٠٠٧م.

٤ - رابطة العالم الإسلامي - مجمع الفقه الإسلامي: بيان مكة المكرمة - الدورة (١٦) لسنة ١٤٢٢هـ.

٥ - د. سليمان بن عبدالله أبا الخيل: موقف المملكة العربية السعودية من الإرهاب ١٤٣٣هـ - الرياض.

٦ - قانون العقوبات المصري، المعدل بالقانون رقم (٩٧) لسنة ١٩٩٥م.

٧- د. عبدالعزيز بن عبدالله السند: الأحكام الفقهية للمعاملات الإلكترونية، الرياض دار الوراق ١٤٢٤هـ - ٢٠٠٤م.

٨- د. عبدالرحمن بن عبدالله السند: وسائل الإرهاب الإلكتروني وحكمها في الإسلام ومكافحتها، بحث للمؤتمر العالمي لمكافحة الإرهاب، الرياض ١٤٣٠هـ.

٩ - د. عبدالله بن عبدالعزيز العجلان: الإرهاب الإلكتروني في عصر المعلومات، القاهرة ٢٠١٣م.

١٠- مجمع الفقه الإسلامي بالأزهر: بيان بشأن ظاهرة الإرهاب في ١٤٢٢هـ (انترنت).

١١- مجموعة من المؤلفين في موقف السعودية من الإرهاب، الرياض ١٤٢٦هـ - ٢٠٠٦م.

١٢- يونس محمد عرب: الإطار القانوني للإرهاب الإلكتروني، واستخدام الانترنت للأغراض الإرهابية، الرياض جامعة نايف العربية للعلوم الأمنية ١٤٣٣هـ - ٢٠١٢م.