

الفصل السادس عشر

الإرهاب الإلكتروني

وطرق مكافحته

obeikan.com

المطلب الأول: المقصود بالإرهاب الإلكتروني^{٣٤}

يشكل الإرهاب إحدى أخطر الظواهر الإجرامية التي عرفتتها المجتمعات الحديثة لما يمثله من تهديدات خطيرة للفكر والعقيدة والكيان السياسي للشعوب، وهو باتساع مفهومه أضحى من أبرز المهددات الأمنية لما له من تأثيرات بعيدة المدى والخطورة على الإنسانية كافة.

كما أن الإرهاب يعد من الظواهر البارزة وذات الصلة القوية بمستحدثات العصر (من تقدم تكنولوجيا) في مجال المعلومات والاتصالات. هذا ويصنف الإرهاب من حيث محل وقوعه إلى نوعين هما:

- ١- الإرهاب الداخلي: وهو يقع داخل الدولة وتتحصر نتائجه داخل نطاقها.
 - ٢- الإرهاب الدولي: وهو يمس العلاقات الدولية.
- ومن ناحية الشكل ينقسم الإرهاب إلى الآتي^{٣٥}:
- ١- الإرهاب السياسي: وهو يتعلق بالنزاعات السياسية بين القوى الخارجية.
 - ٢- الإرهاب الاقتصادي: وهو يتمثل في احتكار فئة معينة بالدولة للامتيازات الاقتصادية.
- ٣- الإرهاب الاجتماعي: الذي يكون نتيجة للتمييز بين فئات المجتمع.
 - ٤- الإرهاب العسكري: الناتج عن التهديد عبر القوة العسكرية لإحداث الخوف والفرع.
 - ٥- الإرهاب الديني: الذي تنتهجه بعض الجماعات المتطرفة.

34- د. عبد الرحمن بن عبد الله السند، الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها،

35- مجلة الأمن، العدد (٣٢١) - ٢٠٠٩م، جامعة نايف العربية للعلوم الأمنية، الرياض.

وهناك أشكال أخرى للإرهاب مثل:

- ١- الإرهاب الإعلامي: وهو يتمثل فيما تبثه وسائل الإعلام من تغطية الأعمال الإرهابية أو ما يبيث من خلالها من حرب نفسية ورسائل ترويع.
- ٢- الإرهاب الفكري: وهو يستهدف تسميم العقول عبر بث الفكر الإرهابي الهدام.

يعني الإرهاب في اللغات الأجنبية القديمة مثل اليونانية: حركة من الجسد تفرع الآخرين^{٣٦}.

وقد أطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم^{٣٧} فكلمة إرهاب تستخدم للرعب أو الخوف الذي يسببه فرد، أو جماعة، أو تنظيم سواء كان لأغراض سياسية أو شخصية أو غير ذلك، فتطور ظاهرة الإرهاب جعلها لا تقتصر على الناحية السياسية فقط بل شملت نواحي قانونية، وعسكرية، وتاريخية، واقتصادية، واجتماعية. وقد وضع وزراء الداخلية والعدل العرب في الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م تعريفاً للإرهاب بأنه: كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه وأغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو اختلاسها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر^{٣٨}.

36- انظر: الإرهاب السياسي والقانون الجنائي، عبد الرحيم صدق، دار النهضة العربية -

القاهرة، ١٩٨٥م، ص ٨١.

37- انظر: المعجم الوسيط ١، ٣٧٦.

38- انظر: الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م.

من هذه التعاريف نتوصل إلى أن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

إن ما يتميز به الإرهاب الإلكتروني عن الإرهاب التقليدي بالطريقة المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات، فالأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين. ويشير الإرهاب الإلكتروني إلى عنصرين أساسيين هما:

الفضاء الافتراضي. أو العالم الإلكتروني، وهو المكان الذي تعمل به أجهزة وبرامج الحاسوب والحواسب المعلوماتية كما تنتقل فيه المعلومات الإلكترونية، والإرهاب. وقد استفادت تلك المنظمات الإرهابية من تلك التقنية واستغلتها في إتمام عملياتها الإجرامية، مما زاد من خطورتها. كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والشركات الاقتصادية الكبرى.

المطلب الثاني: خطر الإرهاب الإلكتروني

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أو المرافق العامة، أو المجال التعليمي، أو الأمني أو غير ذلك، إلا أنه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإن الوجه الآخر والمتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره، إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق.

إن أكثر الأنظمة التقنية تقدماً وأسرعها تطوراً هي الأنظمة الأمنية، وعلى رغم سرعة تطورها إلا أنها أقل الأنظمة استقراراً وموثوقية، نظراً لتسارع وتيرة الجرائم الإلكترونية وأدواتها والثغرات الأمنية التي لا يمكن أن يتم الحد منها على المدى الطويل، فمجال أمن المعلومات في الإنترنت أخذ في التطور بشكل كبير تماشياً مع التطور في الجريمة الإلكترونية.

لقد أصبح الإرهاب الإلكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازمات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

المطلب الثالث: أسباب الإرهاب الإلكتروني

إنها متعددة ومتنوعة ومتشابكة، وهي عينها أسباب ظاهرة الإرهاب عموماً، حيث تتداخل الدوافع الشخصية مع الدوافع الفكرية والسياسية والاقتصادية والاجتماعية، ونعرض هذه الأسباب على النحو التالي:

أولاً: الأسباب العامة للإرهاب :

تختلف أسباب الإرهاب ودوافعه تبعاً لاختلاف الجهات السياسية والظروف الاقتصادية والأحوال الاجتماعية، والاختلاف الديني والعقائدي. ولذلك فإن ما يصدق على مجتمع قد لا يصدق بالضرورة على غيره من المجتمعات.

١ - الدوافع الشخصية مثل:

أ - الرغبة في الظهور وحب الشهرة.

ب - الإحباط في تحقيق بعض الرغبات أو الوصول إلى المكانة المنشودة، وإحساس الشخص بأنه أقل من غيره وينظر إليه نظرة متدنية، فيلجأ إلى الإرهاب للمخروج على النظام.

ت - فشل الشخص في الحياة الأسرية، مما يؤدي إلى الجنوح وعدم الشعور بالانتماء والولاء للوطن.

ث - الإخفاق الحياتي، الذي قد يكون إخفاقاً في الحياة العلمية أو العملية، أو النواحي الوظيفية، أو التجارب العاطفية، مما يجعله يشعر بالفشل في الحياة.

٢ - الدوافع الفكرية مثل:

أ - الفراغ الفكري، والفهم الخاطئ للدين ومبادئه وأحكامه وآدابه، وسوء تفسيره.

ب - التطرف وخاصة في الأمور الفكرية.

٣ - الدوافع السياسية ونذكر منها:

أ - غياب العدالة الاجتماعية في بعض الدول، وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق الأساسية، والاستيلاء على الأموال العامة.

ب - اعتقاد الإرهابي بانتهاك حقوقه وحرماته، وخرق القوانين والمواثيق الدولية، حيث أدى ذلك إلى التشدد والتطرف.

٤ - الدوافع الاقتصادية مثل:

أ - تفاقم الأزمات الاقتصادية في المجتمعات الدولية، بالإضافة إلى المتغيرات الاقتصادية العالمية، والاستغلال غير المشروع للموارد الاقتصادية لبلد معين.

ب - عدم إقامة تعاون دولي جدي من قبل الأمم المتحدة، وعدم إيجاد تنظيم عاجل ودائم لعدد من المشاكل العالمية، مثل اغتصاب الأراضي والاضطهاد.

ت - معاناة الأفراد من المشاكل الاقتصادية المتعلقة بالإسكان والفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية، وعدم تحسن دخل الفرد، مما يؤدي إلى تفشي روح التذمر ودفع الشباب إلى التطرف والإرهاب.

ث - انتشار البطالة في المجتمعات المختلفة وعدم توفر فرص العمل، مما ساهم في ظهور جرائم السرقات والإرهاب.

ج - التقدم التقني للأنظمة المصرفية العالمية وما أدى إليه من سهولة انتقال الأموال وتحويلها بين جميع أرجاء العالم عن طريق شبكة النت، مما ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أهدافهم غير المشروعة.

٥- الدوافع الاجتماعية مثل:

أ - التفكك الأسري، مما يؤدي إلى انتشار الأمراض النفسية والانحراف والإرهاب، خاصة وأن الترابط الأسري يحيط الأشخاص بشعور التعاون والتماسك.

ب - الفراغ النفسي والروحي والعقلي جعل الفرصة سانحة لقبول كل فكر هدام ومتطرف.

ثانياً - الأسباب الخاصة بالإرهاب الإلكتروني وهي:

١- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: حيث أن شبكات المعلومات مصممة بحسب الأصل بشكل مفتوح دون حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين. ويمكن للمنظمات الإرهابية استغلال الثغرات المتواجدة في الأنظمة الإلكترونية والشبكات المعلوماتية، في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية.

٢- عدم وضوح الهوية الرقمية للمستخدم يجعل الفرصة سانحة للإرهابيين، حيث يستطيع محترف الحاسوب أن يتخفى تحت شخصية وهمية، ويشن بالتالي هجومه الإلكتروني بعيداً عن مراقبة السلطات العامة.

٣- سهولة استخدام شبكة المعلومات وقلة التكلفة مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون حاجة إلى مصادر تمويل. فشن

هجوم إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب إلى متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة. فصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب الإرهاب الإلكتروني، لأنها تساعد المجرم على الإفلات من العقوبة.

٤- صعوبة اكتشاف وإثبات الجريمة الإرهابية ، خاصة في مجال جرائم الاختراق، مما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.

٥- غياب السيطرة والرقابة على الشبكات المعلوماتية، ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى.

المطلب الرابع: خصائص الإرهاب الإلكتروني وأهدافه

ينفرد الإرهاب الإلكتروني بعدد من الخصائص التي تميزه عن الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق بعض الأغراض غير المشروعة، وذلك على النحو التالي:

أولاً: خصائص الإرهاب الإلكتروني التي تميزه عن الإرهاب العادي:

١- لا يحتاج الإرهاب الإلكتروني في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب إلى متصل بالشبكة المعلوماتية فقط ومزود ببعض البرامج اللازمة.

٢- يتسم الإرهاب الإلكتروني بأنه عابر للدول والقارات، وغير خاضع لدولة معينة.

٣- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الجهات الأمنية والقضائية في التعامل مع مثل ذلك النوع من الجرائم.

٤- صعوبة إثبات جرائم الإرهاب الإلكتروني، لغياب الدليل الرقمي من ناحية، وسهولة إتلافه وتدميره من ناحية أخرى.

٥- يكون مرتكب الإرهاب الإلكتروني في العادة من المتخصصين في مجال تقنية المعلومات ، أو لديه - على الأقل - قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية.

ثانياً: أهداف الإرهاب الإلكتروني هي:

- ١- نشر الخوف والرعب بين الأشخاص والدول، وتعريض سلامة المجتمع وأمنه للخطر.
- ٢- الإخلال بالأمن المعلوماتي وزعزعة الطمأنينة.
- ٣- تدمير البنى التحتية المعلوماتية، والإضرار بوسائل الاتصالات وتقنية المعلومات.
- ٤- الدعاية والإعلان وإثارة الرأي العام.
- ٥- الاستيلاء على الأموال.

المطلب الخامس: وسائل الإرهاب الإلكتروني

١ - البريد الإلكتروني :

البريد الإلكتروني خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وتعد هذه الخدمة من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما تمثله من سرعة في إيصال الرسالة وسهولة الإطلاع عليها في أي مكان، فلا ترتبط الرسالة الإلكترونية المرسله بمكان معين، بل يمكن الإطلاع عليها وقراءتها في أي مكان من العالم.

وعلى الرغم من أن البريد الإلكتروني (E-mail) أصبح أكثر الوسائل استخداماً في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمناً وسرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيراً من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

وكذلك يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية.

ومما يقوم به الإرهابيون أيضاً اختراق البريد الإلكتروني للآخرين وھتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس علیها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

٢- إنشاء مواقع على الإنترنت :

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك.

والموقع هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل Hyper text mark up language (HTML) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (WWWBrowser) ويقوم بحل رموز (HTML) وإصدار التعليقات لإظهار الصفحات المتكونة^{٣٩}.

إن الشبكة العنكبوتية (World Wide Web) أو نظام الويب الذي ابتكره العالم الإنجليزي تم بيرنرس عام ١٩٨٩م، يركز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت، ومن هنا أطلقت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجاناً عبر شبكة الإنترنت في عام ١٩٩١م، واعتمد في المرحلة الأولى عام ١٩٩٣م على برامج التصفح.

39- انظر: التجارة على الإنترنت، سايمون كولن، نقله إلى العربية يحيى مصلح، بيت

الأفكار الدولية بأمريكا ١٩٩٩م، ص ٢٦.

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادل 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 غداً سهلاً ممكناً، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمّنوا انتشاراً أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها.

لقد وجد الإرهابيون بغيتهم في تلك الوسائل الرقمية في ثورة المعلوماتية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة المعلومات العالمية الإنترنت، فغدت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب الإلكتروني.

٣- تدمير المواقع

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

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

يستطيع قراصنة الحاسب الآلي (Hackers) التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولاسيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي^{٤٠}.

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات غير مكتشفة بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي^{٤١}.

يمكن لمزود خدمات الإنترنت (ISP) من الناحية النظرية أن يكتشف كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة، ويشمل ذلك: عناوين المواقع التي زارها، ومتى كان ذلك، والصفحات التي اطلع عليها، والملفات التي جلبها، والكلمات التي بحث عنها، والحوارات التي شارك فيها، والبريد الإلكتروني الذي أرسله أو استقبله، وفواتير الشراء للسلع التي طلب شراءها، والخدمات التي شارك فيها، لكن تختلف من الناحية الفعلية كمية المعلومات التي يجمعها مزود خدمات الإنترنت عن مستخدم الشبكة باختلاف التقنيات والبرمجيات التي يستخدمها، فإذا لم يكن مزود الخدمة يستخدم مزودات (بروكسي) تتسلم وتنظم كل الطلبات، ويستخدم برامج تحسس الرقم الخاص (IP) التي تحلل حركة المرور بتفصيل كبير، فقد لا يسجل سوى البيانات الشخصية للمستخدم،

40- انظر: التهديدات الإجرامية للتجارة الإلكترونية، د سهير حجازي، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد (٩١).

41- انظر: الاختراقات الإلكترونية خطر كيف نواجهه، مؤزة المزروعي، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر ٢٠٠٠م، ص ٥٤.

وتاريخ وزمن الاتصال والانفصال عن الشبكة، وبعض البيانات الأخرى، إن معرفة البيانات التفصيلية للمستخدم تجعل الإقدام على الاعتداء الإلكتروني أقل، وذلك لأن بعض المعتدين يقومون بالاعتداء الإلكتروني بسبب ظنهم أن بياناتهم التفصيلية لا يمكن الاطلاع عليها، فيظن أنه بمجرد دخوله على الشبكة باسم وهمي تصبح بيانات المعتدي غير معلومة، وهذا خطأ^{٤٢}.

من الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (E-mails) 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 وتشتت 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^{٤٣}.

وفي الواقع إن هناك أسباباً لوقوع عملية تدمير المواقع ومن هذه الأسباب ما يأتي:

١ - ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجدون أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمونها، مما يسهل عملية كسر وتخمين الكلمات السرية من المخترق.

-
- 42 - انظر: جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظور أمني، للعقيد الدكتور ممدوح عبد الحميد عبد المطلب، ص ٤٢، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة ١- ٣ مايو ٢٠٠٠
- 43 - انظر: التكيف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، د عماد علي الخليل، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة ١- ٣ مايو ٢٠٠٠م، ص ٤.

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

٣ - استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج وأنظمة غير موثوقة أمنياً 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^{٤٤} 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 الموقع للضياع وعدم إمكانية استرجاعها، ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في الآونة الأخيرة.

44- حذرت شركة مايكروسوفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجية، ودعت المستخدمين إلى تركيب برنامج ترقيعي لحل المشكلة. (جريدة الرياض، العدد ١٢٥٤٢، السبت ٢٠ ١٤٢٣هـ، ص ١٩).

المطلب السادس: طرق مكافحة الإرهاب الإلكتروني

١- ترشيح الدخول على الإنترنت :

لا يمكن لأي بلد في هذا العصر أن يعيش معزولاً عن التطورات التقنية المتسارعة، والآثار الاقتصادية، والاجتماعية، والأمنية الناجمة عنها. 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 أفراد 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 جميعاً 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 وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، فهذا الأسلوب يعد من الأساليب المجدية والنافعة، فالإنسان لا يعرض نفسه للفتن والشرور.

ولقد جاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم، ولقد سعت بعض الدول إلى حجب المواقع الضارة، ففي تركيا قررت شركة الاتصالات التركية التي تزود جميع أنحاء البلاد بخدمات الإنترنت حجب بعض المواقع الضارة على شبكة المعلومات العالمية الإنترنت، ولذلك عمدت إلى تركيب الأجهزة والأدوات التي تقوم بتتقية المواقع وحجب المواقع الضارة ومنع ظهورها^٥ وهناك دول عدة إسلامية وغير إسلامية تعتمد إلى ترشيح شبكة الإنترنت وحجب المواقع التي ترى أنها ضارة أخلاقياً أو فكرياً.

٢ - أنظمة التعاملات الإلكترونية

مع التوجه المتنامي نحو تقنية المعلومات، تبرز بوضوح الحاجة الملحة إلى إيجاد أنظمة لضبط التعاملات الإلكترونية بشتى صورها، فعلى الرغم من محدودية ما أنجز في هذا السياق فإن الجهات التي تضطلع بهذه المهام تعاني من البطء الشديد في إنجاز هذه الأنظمة لكثرة الجهات الممثلة في لجان الصياغة، وتعدد الجهات المرجعية التي تقوم بمراجعة الأنظمة واعتمادها، لذا فلا بد من إعداد الأنظمة اللازمة لتحقيق الاستفادة القصوى من تقنية المعلومات، وحماية المتعاملين من المخاطر التي تتطوي عليها تلك التقنيات، ولقد أظهرت استبانة أجريت للتعرف على مدى الحاجة إلى وجود تطبيقات ولوائح تحكم قضايا تقنية المعلومات أن ٧٠٪ يرون الحاجة إلى ذلك^{٤٦}.

إن المخاطر الكامنة في تغلغل تقنية المعلومات الحديثة في واقعنا تتطلب من المجتمع والدول جميعاً الحيلولة دون حصول تلك المخاطر بشتى أنواعها، ومن أهم ما يجب توفيره في هذا الصدد الأحكام والأنظمة واللوائح المنظمة لسلوك الأفراد والمؤسسات حيال التعامل مع تقنية المعلومات مهما كان نوع التعامل وأياً كانت مقاصده، دون تقييد حرية المجتمع عن الاستثمار البناء لتلك التقنية، فحسب دراسة أجراها مشروع الخطة الوطنية لتقنية المعلومات على ما يزيد عن ٧٠٠ شخص في المملكة العربية السعودية، اتضح أن ٩٪ من أفراد العينة يقومون بمحاولات اختراق مواقع وأجهزة الأفراد والمؤسسات، بالإضافة إلى ما يقرب من ٧٪ يقومون بهذا العمل بشكل نادر، وهذه النسبة عالية بكل المقاييس، وتزيد هذه النسبة في نوع آخر من المخالفات كإغراق أجهزة الخادمت بالرسائل البريدية، حيث وصلت النسبة إلى ما يزيد عن ١٥٪ بالإضافة إلى ١٢٪ من أفراد العينة يقومون بهذا العمل بشكل نادر (أي سبق أن قاموا به).

إنه وبالرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة

46 - انظر: دراسة الوضع الراهن في محور أحكام في المعلوماتية، ص ١٣.

واللوائح الجزئية التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات، كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة^{٤٧}.

وفي المملكة العربية السعودية يجري العمل لإصدار عدد من الأنظمة التي تضبط التعاملات الإلكترونية وتجرم الاعتداء والعدوان الإلكتروني، ومن أمثلة ذلك مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية^{٤٨} فقد نصت المادة (٢٠) من مشروع النظام على أنه: يعد مرتكباً جناية أي شخص يدخل عن عمد منظومة حاسوب، أو جزءاً منها بدون وجه حق، وذلك بالتعدي على إجراءات الأمن، من أجل ارتكاب عمل يعد جناية حسب الأنظمة المرعية وحسب ما تحدده اللائحة التنفيذية.

ونصت المادة (٢١) من مشروع النظام على أنه يعد مرتكباً جناية أي شخص يعترض عمداً وبدون وجه حق وعن طريق أساليب فنية، إرسال البيانات الحاسوبية غير المصرح بها للعموم من منظومة حاسوب أو داخلها.

أما المادة (٢٢) فقد نصت على أنه يعد مرتكباً جناية كل شخص يقوم عن عمد أو بإهمال جسيم وبدون وجه حق بإدخال فيروس حاسوبي أو يسمح بذلك في أي حاسوب أو منظومة حاسوب، أو شبكة حاسوب.

كما جاءت المادة (٢٣) لتجريم إلحاق الضرر بالبيانات الحاسوبية بالمسح أو التحويل أو الكتمان.

ونصت المادة (٢٥) على أنه يعد مرتكباً جناية أي شخص يقوم عن عمد وبدون وجه حق وبقصد الغش بإدخال بيانات حاسوبية أو تحويلها أو محوها وينتج عنها بيانات غير صحيحة بقصد اعتبارها معلومات صحيحة.

47 - دراسة الوضع الراهن في مجال أحكام في المعلوماتية، إعداد: د محمد القاسم، د رشيد الزهراني،

د عبد الرحمن السند، عاطف العمري، مشروع الخطة الوطنية لتقنية المعلومات، ص ٦، ٧.

48 - وقد كلف الباحث من قبل وزارة التجارة بالمشاركة في إعداد هذا النظام، فشارك في صياغته، وقد تم رفع المشروع للجهات العليا لاعتماده.

كما نصت المادة (٢٨) على العقوبات المترتبة على التجاوزات التي حددها النظام^{٤٩} كما يجري العمل لإصدار نظام للحد من الاختراقات الإلكترونية، وهذا النظام يحدد العقوبات المترتبة على الاختراقات الإلكترونية، وتقوم بإعداده وزارة الداخلية للتصدي لمخترقي شبكة المعلومات في المملكة، ويشمل هذا النظام تحديد الجناة القائمين بالاختراق سواء كانوا أفراداً أو مؤسسات، وكذلك العقوبات النظامية التي يتم تطبيقها بحقهم^{٥٠}.

٣- أنظمة الحماية الفنية من الاعتداءات الإلكترونية

منذ أول حالة لجريمة موثقة ارتكبت عام ١٩٥٨م في الولايات المتحدة الأمريكية بواسطة الحاسب الآلي وحتى الآن كبر حجم هذه الجرائم وتنوعت أساليبها وتعددت اتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومي للدول، خصوصاً تلك التي تركز مصالحها الحيوية على المعلوماتية، وتعتمد عليها في تسيير شؤونها، فقد تحولت هذه الجرائم من مجرد انتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة، ينخرط فيها الكثير ممن تتوافر لديهم القدرات في مجال الحاسب الآلي والاتصال بشبكات المعلومات.

إن المقاومة للجرائم والاعتداءات الإلكترونية على نوعين:

النوع الأول: المقاومة الفنية.

النوع الثاني: المقاومة النظامية.

وتتم الحماية الفنية التقنية بعدة وسائل منها:

أولاً: تشفير البيانات المهمة المنقولة عبر الإنترنت.

ثانياً: إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

49- انظر: مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية، في المملكة العربية

السعودية ١٧ ٤٢٣ ١هـ، إعداد: وزارة التجارة، إدارة التجارة الإلكترونية.

50- جريدة المدينة، العدد: ١٤٤٨٩، ٢٠ ١٠ ٤٢٣ ١هـ، ص ١٧.

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

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

خامساً: توزيع مهام العمل بين العاملين، فلا يعطى المبرمج مثلاً وظيفته تشغيل الحاسب الآلي إضافة إلى عمله، ففي هذه الحالة سوف يكون قادراً على كتابة برامج قد تكون غير سليمة، ومن ثم تنفيذها على البيانات الحقيقية، كما يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين، مما يجعل كتابة برامج ضارة أمراً صعباً.

الإنترنت ميدان لكل ممنوع، ولا نغالي إذا قلنا: إن التقدم التقني الذي يشهده العالم اليوم، كما أن له من الجوانب الإيجابية ما يصعب حصره، إلا أن جوانبه السلبية تكاد تكون مدمرة، ما لم تكن هناك مقاومة لهذه السلبيات، فمن خلال شبكة الإنترنت يمكن معرفة كيفية صناعة المتفجرات، وغسيل الأموال، وصناعة القنبلة النووية، وسرقة البطاقات الائتمانية، ولقد أظهر تقرير لمركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على المؤسسات الأمنية في إجراءات معالجة المعلومات والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر مع رجال الأمن، إلى جانب الحاجة إلى التعاون الدولي المتبادل للبحث الجنائي والنظامي في مجال مكافحة جرائم الكمبيوتر، وفي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تتمحور حول عدد من النقاط منها المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه للتحقيق، والطبيعة العالمية لبعض جرائم الكمبيوتر، وتحديد معايير لوسائل الأمن المعلوماتي، والوقاية من جرائم الكمبيوتر، الأمر الذي ينبه إلى المعضلة الأساسية في هذا النوع من جرائم الكمبيوتر وهي عدم الارتباط بالحدود الجغرافية، وأيضاً كون التقنية المستخدمة في هذه الجرائم متطورة جداً، فالأموال التي يتم استحصالها لعصابة في

طوكيو، يمكن تحويلها في ثانية واحدة إلى أحد البنوك في نيويورك، دون إمكانية ضبطها^{٥١}.

إن أجهزة الأمن تحتاج إلى كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها، وتطوير إجراءات الكشف عن الجريمة، خاصة في مسرح الحادث، وأن يكون رجل التحقيق قادراً على تشغيل جهاز الحاسب الآلي، ومعرفة المعدات الإضافية فيه، ومعرفة البرمجيات اللازمة للتشغيل، بحيث يتمكن من تقديم الدليل المقبول للجهات القضائية، وأيضاً يلزم نشر الوعي العام بجرائم الكمبيوتر، والعقوبات المترتبة عليها، واستحداث الأجهزة الأمنية المختصة القادرة على التحقيق في جرائم الكمبيوتر، والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

إن معظم أدوات الجريمة الإلكترونية تكون متوافرة على الشبكة، وهذا الأمر لا تمنعه الأنظمة في معظم الدول، إما لعدم القدرة على السيطرة عليه، أو لأن هناك استخدامات مفيدة لهذه البرامج، فمثلاً هناك عدة برامج لكسر كلمة السر لدخول الأجهزة المحمية بكلمة مرور وهو ما يطلق عليه (CRACKING) وهذه البرامج تكون مفيدة لمن نسي كلمة السر للدخول على الجهاز، أو الدخول على أحد الملفات المحمية، وفي الوقت نفسه يمكن للمعتدي أن يستغل هذه البرامج في فتح جهاز معين بعد معرفة كلمة السر، والدخول على الإنترنت واستغلاله في الاستخدام السيئ، إذن أدوات القرصنة والإجرام متوافرة، لكن الإجرام يكون في الاستغلال السيئ لهذه الأدوات، ويوجد لدى معظم الدول الكبرى أدوات تعقب لمعرفة مصدر مطلق الفيروس مثلاً، أو الهجوم على بريد إلكتروني، أو موقع رسمي لإحدى هذه الدول، ولذلك يحرص هؤلاء المعتدون على أن يتم هذا العمل الإجرامي عن طريق أجهزة الآخرين، وهذا يبين أهمية أن يحمي كل واحد جهازه، وأن يحرص على رقمه السري حتى لا يستغل من قبل الآخرين، وينطبق هذا أيضاً

51 - انظر: جريدة الشرق الأوسط، العدد ٨١٩٦، يوم الاثنين ٥٧ ٢٠٠١، ص ٥١.

على أصحاب الشبكات كالجوامع والمعاهد التي توفر الإنترنت لمنسوبيها، فقد يستغلها بعضهم لإطلاق الفيروسات أو غيرها من الاعتداءات الإلكترونية.

إن المحافظة على المعلومات من أهم ما تحرص عليه الهيئات والمنظمات والدول، وحتى على مستوى الأفراد، إذ يمكن تعويض فقدان الأجهزة 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 اتباع مجموعة من الإجراءات التي تضمن سلامة هذه المعلومات منها ما يأتي:

١ - عدم إلقاء مخرجات الحاسب الآلي، أو شريط تحبير الطابعة، لأن 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 أن 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 تحكم داخل النظام تساعد على منع 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 للتأكد من أنها تعمل بشكل صحيح، وخاصة البرامج المالية التي غالباً ما يكون التلاعب بها من قبل المبرمجين أو المستخدمين، وذلك عن طريق أخذ عينات عشوائية لمخرجات البرنامج في فترات مختلفة، كما يقومون بفحص ملف المتابعة للتعرف على الأشخاص الذين وصلوا إلى البيانات، أو حاولوا الوصول إليها.

٥- تشفير البيانات المهمة المنقولة عبر وسائل الاتصالات كالأقمار الصناعية أو عبر الألياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة، لأن عملية التشفير مكلفة.

٦- عمل نسخ احتياطية من البيانات تخزين خارج مبنى المنظمة.

٧- استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد، أو الصوت^{٥٢}.

المطلب السابع: جهود التصدي للإرهاب الإلكتروني

١- الجهود الدولية في التصدي للإرهاب الإلكتروني:

على مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سنت أنظمة لضبط التعاملات الإلكترونية، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الإلكترونية ففي ماليزيا صدر نظام في عام ١٩٩٧م للمخالفات الإلكترونية، وقد صنف المخالفات إلى: الوصول غير المشروع إلى الحاسب الآلي والدخول بنية التخريب أو التعديل غير المسموح به وتتراوح العقوبات المحددة بين غرامات مالية تصل إلى ١٥٠,٠٠٠ دولار ماليزي^{٥٣} مع السجن مدة تصل إلى عشر سنوات.

52- انظر: مقدمة في الحاسب الآلي وتقنية المعلومات طارق بن عبد الله الشدي، دار الوطن

للتشر الرياض، الطبعة الثانية، ١٤١٦هـ، ص ١٨٨.

53- انظر: دراسة تجارب الدول في مجال أحكام في المعلوماتية، إعداد: د محمد القاسم، د

رشيد الزهراني د عبد الرحمن السند، عاطف العمري، مشروع الخطة الوطنية لتقنية

المعلومات ١٠ ١١ ١٤٢٣هـ.

وفي أيرلندا صدر نظام في عام ٢٠٠١م للحماية من الجرائم المعلوماتية، يتيح معاقبة الاستخدام غير المسموح به لأجهزة وأنظمة الحاسب الآلي.

وفي مصر يجري العمل في وزارة الاتصالات والمعلومات لإصدار نظام عن الجريمة الإلكترونية، يتضمن عقوبات رادعة لمن يقوم من الأفراد أو المؤسسات بتزوير أو إفساد مستند إلكتروني على الشبكة، أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الإلكترونية.

أما في الأردن فيجري العمل لإعداد تنظيم يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر الشبكات العالمية للمعلومات، كما تساهم الأردن في إعداد مشروع حول قانون مكافحة جرائم تقنية المعلومات وما في حكمها، والمقدم إلى الإدارة العامة للشؤون القانونية في جامعة الدول العربية.

٢- صعوبة التعاون الدولي في مكافحة الجريمة الإلكترونية:

في عالم مزدحم بشبكات اتصال دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية متباعدة باستخدام تقنيات لا تكفل للمعلومات أمناً كاملاً، يتيح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضراراً فادحة، يغدو التعاون الدولي الواسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمراً متحتماً، وبالرغم من الحاجة الماسة لهذا التعاون إلا أن عقبات عدة تقف في سبيله أبرزها ما يأتي:

١- عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات الواجب تجريمها.

٢- عدم الوصول إلى مفهوم عام موحد حول النشاط الذي يمكن الاتفاق على تجريمه.

٣- اختلاف مفاهيم الجريمة باختلاف الحضارات.

٤- عدم وجود معاهدات دولية لمواجهة المتطلبات الخاصة بالجرائم الإلكترونية.

٥- تعقد المشكلات النظامية والفنية الخاصة بتفتيش نظام معلوماتي خارج حدود الدولة، أو ضبط معلومات مخزنة فيه، أو الأمر بتسليمها.

وسعيًا للتغلب على هذه المشكلات أو بعضها، أهاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا، في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي بالدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسب الآلي التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في:

أ) تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءات بشأن سلطات التحقيق وقبول الأدلة على نحو ملائم.

ب) النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.

كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات، بما في ذلك دخولها حسب الاقتضاء أطرافاً في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، وأن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاون الدولي في هذا المضمار ولاسيما فيما يتعلق بوضع أو تطوير ما يأتي:

أ - معايير دولية لأمن المعالجة الآلية للبيانات.

ب - تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.

ج - اتفاقيات دولية تتطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول^{٥٤}.

ختاماً، أصبح الإرهاب الإلكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت والذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازاات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

فالإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق.



54 - انظر: الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، د هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص ٤٩، ٤٨.