مكافحة الإرهاب الإلكتروني

ضرورة بشرية وفريضة شرعية

https:\\www .

د. بن يحيى الطاهر ناعوس

الألوكة
www.alukah.net

مكافحة الإرهاب الإلكتروني

ضرورة بشرية وفريضة شرعية

تمهيد:

أصبح الأمن الإلكتروني ضرورة لأن حياتنا مرتبطة ارتباطاً وثيقاً بوسائل الاتصال الحديثة التي سهلت طرق التواصل بكل أشكالها "السمعي – البصري – المكتوب"، ومن هنا فإن الحفاظ على الخصوصية في حياة كل شخص أضحى من المستحيلات، لوجود ما يهدد هذه الخصوصية عن طريق ما يسمى بالإرهاب الالكتروني فكثير من المواقع العالمية المشهورة تنصح مرتاديها والمنتسبين إليها من خطر التهديد الإلكتروني.

حذرت موسوعة ويكيبيديا زوارها من وجود برمجيات خبيثة في الموقع قد تصيب أجهزتهم عن طريق متصفحات الانترنت.

وتتمثل هيئة البرمجيات الخبيثة على شكل إعلانات موجودة في الشبكة وهي بالأصل برمجيات خبيثة كون موسوعة ويكيبيديا لا تنشر إعلانات أبدا، حيث لو ظهر أمامك إعلان في موسوعة ويكيبيديا فأنت الآن مصاب ببرمجيات خبيثة.

ونصحت ويكيبيديا مستخدميها الذين تظهر لديهم الإعلانات بتعطيل جميع إضافات متصفحاتهم، وذلك كمحاولة مبدئية لمعرفة مصدر المشكلة، لكن هذا غير كافٍ إذ قد تمتلك البرمجية الخبيثة أجزاء أخرى تعمل على النظام وبالتالي فالحل الأفضل هو استخدام برنامج لمكافحة الفيروسات وتحديثه بشكل دائم بحسب المؤسسة.

على غرار مصير خدمتي ستريت فيو Street View و Friend Finderفقد أمرت محكمة ألمانية بإيقاف خدمة Bing Streetside من مايكروسوفت في ألمانيا وجاء هذا

القرار بعد اتهامات من قبل مواطنين ألمان بانتهاك الخدمة الأخير لخصوصياتهم حيث أنها تقوم بتصوير منازلهم الأمر الذي لا يريده هؤلاء.

وتأسيسا على ما سبق، فإنه لا يمكن لأي بلد في هذا العصر أن يعيش معزولًا 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 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، فكيف يمكن مكافحة المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق؟ وما هو الأسلوب الأنجع والنافع لكي لا يعرض الإنسان نفسه للفتن والشرور؟

ماهية الإرهاب الإلكتروني:

جاء في المعاجم العربية أن كلمة الإرهاب كلمة مشتقة من "أَرْهَبَه ورَهَّبَه واسترْهَبَه: أَخافَه وفَزَّعه. واسْتَرْهَبَه: اسْتَدْعَى رَهْبَتَه حتى رَهِبَه الناسُ؛ وبذلك فسر قوله عز وجل: واسْتَرْهَبُوهُم وجاؤُوا بسحْرٍ عظيمٍ؛ أَي أَرْهَبُوهم، وفي حديث بَهْز بن حَكِيم: إِني لأَسمع الرَّاهِبةَ. قال ابن الأَثير: هي الحالة التي تُرْهِبُ أَي تُفْزِعُ وتُخَوِّفُ؛ وفي رواية: أَسْمَعُك راهِباً أَي خائفاً"[1].

[1]-لسان العرب، ابن منظور، مادة رهب.

و يعني الإرهاب في اللغات الأجنبية القديمة مثل اليونانية: حركة من الجسد تفزع الآخرين [2]، ويُعرف، أيضا، بأنه "أسلوب من اساليب الصراع الذي تقع فيه الضحايا جزافا كهدف عنف فعال، وتشترك هذه الضحايا الفعالة في خصائصها مع جماعة أو طبقة في خصائصها مما يشكل أساساً لانتقائها من أجل التضحية بها"[3].

وقد أطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم [4] 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 1998م تعريفا للإرهاب بأنه: كل فعل من أفعال العنف أو التهديد أيًا 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 [5].

ويُعتبر تعريف مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي من أفضل التعاريف الاصطلاحية للإرهاب من حيث الشمولية وتحديد سلوك الإرهاب فقد عرف الإرهاب

---

[2]- ينظر: الإرهاب السياسي والقانون الجنائي، عبد الرحيم صدق، دار النهضة العربية – القاهرة، 1985 م، ص81.

[3]-جاء في الطبعة الأولى من كتاب الإرهاب السياسي(Political Terrorism) سجل" شميد "مئة وتسعة تعريفا من وضع علماء متنوعين من جميع العلوم الاجتماعية بما في ذلك علماء القانون واستناداً إلى هذه التعريفات المائة وتسعة فقد أقدم" شميد "على مغامرة تقديم تعريف في رأيه جمع العناصر المشتركة في غالبية التعريفات.

[4] -ينظر: المعجم الوسيط 1 376.

[5]-ينظر: الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998م.

بأنه: "العدوان الذي يمارسه أفراد أو جماعات أو دول بغيًا على الإنسان دينه، ودمه، وعقله، وماله، وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذًا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو المرافق العامة والأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها" [6] [7].

وقد أصدر مجمع الفقه الإسلامي الدولي قرارًا في دورته الرابعة عشرة المعقودة في الدوحة في شهر ذي القعدة من عام 1423هـ ذكر فيه تعريف مصطلح الإرهاب بأنه: العدوان أو التخويف أو التهديد ماديًا أو معنويًا 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 "[8].

إذن؛ فالإرهاب الإلكتروني هو "العدوان أو التخويف أو التهديد مادياً أومعنوياً باستخدام الوسائل الإلكترونية الصادرة عن الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني، أو أن يكون هدفاً لذلك العدوان، بما يؤثر على الاستخدام السلمى له"[9].

---

[6] ينظر: بيان مكة المكرمة الصادر عن المجمع الفقهي لرابطة العالم الإسلامي، الدورة السادسة عشرة، مكة المكرمة، رابطة العالم الإسلامي 1422هـ، ص: 8.

[7] ينظر: الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، الدكتور حسن بن محمد سفر، بحث مقدم لمجمع الفقه الإسلامي الدولي، ص: 9-11.

[8] ينظر: قرارات وتوصيات الدورة الرابعة عشرة لمجلس مجمع الفقه الإسلامي، الدوحة – قطر، 8-13 ذو القعدة 1423هـ.

[9]- الإرهاب الإلكتروني. نمط جديد وتحديات مختلفة، المؤلف: عادل عبدالصادق الناشر: المركز العربي لأبحاث الفضاء الإلكتروني، 2013م.

و على ما سبق، فإن "الإرهاب الإلكتروني هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية" [10].

ويُستخلص من التعاريف السابقة، بأن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد ماديًا أو معنويًا 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 الذي نهت عنه الشريعة الإسلامية.

نجملها في هذا المخطط البياني ليسهل فهمه:

---

[10]- من كتاب Business Informatin Systems ، الطبعة الثانية 2003.

خطورته على الفرد والمجتمع.

أضحى الإرهاب الإلكتروني خطرًا يهدد العالم بأسره، نتيجة ظهور الحاسبات الآلية التي غيَّرتْ شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يومًا بعد يوم، سواء في المؤسسات المالية، أو المرافق العامة، أو المجال التعليمي، أو الأمني أو غير ذلك، إلا إنَّه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإن الوجه الآخر والمتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة، ذلك أنَّ خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في مترله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق[11].

إنَّ مجال أمن المعلومات في الإنترنت آخذ في التطور بشكل كبير تماشيًا مع التطور في الجريمة الإلكترونية، وهو من أكثر الأنظمة التقنية تقدمًا وأسرعها تطورًا هي الأنظمة الأمنية، وعلى رغم سرعة تطورها إلا أنها أقل الأنظمة استقرارًا وموثوقية، نظرًا لتسارع وتيرة الجرائم الإلكترونية وأدواتها والثغرات الأمنية التي لا يمكن أن يتم الحد منها على المدى الطويل.

لقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم[12]، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضرارًا جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب

---

[11]- ينظر: الإرهاب الدولي، د.محمد عزيز شكري، دار العلم للملايين/بيروت/ط /أولى/1991.

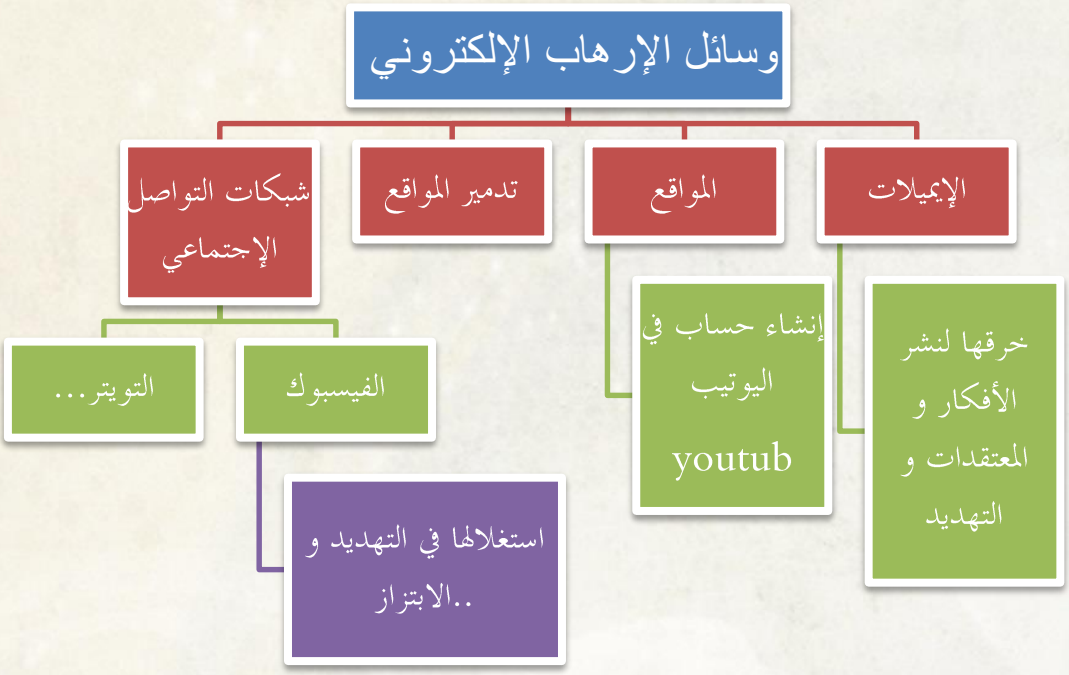
[12]- ينظر :جريدة عكاظ، الثلاثاء 1429/09/16هـ، 16/ سبتمبر/2008 العدد: 2648

الإلكتروني، إلا أن هذه الجهود قليلة ولا نزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

و في هذا الجدول نلاحظ جانبا من جوانب خطورة الإرهاب الإلكتروني في شكل نشر المواقع الإباحية التي تهدم القيم والمبادئ لدى الأفراد والجماعات :

أرقام وحقائق	
عدد المواقع الإباحية	4.2 مليون (12% من مجموع المواقع)
عدد الصفحات الإباحية	420 مليون
عدد مرات البحث عن الإباحية على موقع بحث	68 مليون بحث (25% من مجموع البحوث)
عدد الرسائل الإباحية اليومية	2.5 مليون (8% من مجموع الرسائل الإلكترونية)
نسبة مستعملي الإنترنت الذين يشاهدون موادا إباحية	42.7%
عدد مرات استقبال مواد إباحية غير مرغوب فيها	34%
متوسط الرسائل الإلكترونية الإباحية التي يتلقاها كل مستعمل للنت	4.5 رسالة.
عدد مرات تحميل مواد إباحية شهريا	1,5 بليون تحميل (35% من مجموع التحميلات)
المواقع التي تعرض الشذوذ مع الأطفال	100,000
عدد الزوار للمواقع الإباحية في العالم	72 مليون زائر شهريا
مبيعات الإباحية على النت	4.9$ مليار دولار

ومن هنا، وجب أن ندقّ ناقوس الخطر ليعلم الخاص والعام خطورة الإرهاب الإلكتروني، ومن المعلوم، فإن الإرهاب الإلكتروني له وسائل كثيرة ومتعددة نجملها في هذا المخطط البياني:


وسائل الإرهاب الإلكتروني
الإيميلات
المواقع
تدمير المواقع
شبكات التواصل الإجتماعي
خرقها لنشر الأفكار و المعتقدات و التهديد
إنشاء حساب في اليوتيب youtub
الفيسبوك
التويتر...
استغلالها في التهديد و الابتزاز..

سبل مكافحة الإرهاب الإلكتروني

في ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والاتصالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات لا يمكن لأي بلد في هذا العصر أن يعيش معزولًا عن التطورات التقنية المتسارعة، والآثار الاقتصادية، والاجتماعية، والأمنية الناجمة عنها، وبات 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 وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، فهذا الأسلوب يعد من الأساليب المجدية والنافعة، فالإنسان لا يعرض نفسه للفتن والشرور، بل المسلم يسأل ربه أن يحفظه من التعرض للفتن، والله تعالى يقول عن يوسف عليه السلام: {قَالَ رَبِّ السِّجْنُ أَحَبُّ إِلَيَّ مِمَّا يَدْعُونَنِي إِلَيْهِ وَإِلَّا تَصْرِفْ عَنِّي كَيْدَهُنَّ أَصْبُ إِلَيْهِنَّ وَأَكُنْ مِنَ الْجَاهِلِينَ} [13].

كما هو معلوم، فإنَّ مدينة الملك عبد العزيز للعلوم والتقنية، على سبيل المثال، سعت إلى حجب المواقع الإباحية عن مستخدمي الإنترنت في المملكة العربية السعودية حفاظًا على الأخلاق وصيانة للأمة من عبث العابثين وإفساد المجرمين، فقد صدر في عام 1417هـ قرار مجلس الوزراء رقم (163) الذي أناط بمدينة الملك عبد العزيز للعلوم والتقنية مهمة

---

[13] سورة يوسف آية: 33.

إدخال خدمة الإنترنت العالمية للمملكة[14]، وتولي جميع الإجراءات اللازمة بما في ذلك ترشيح المحتوى.

أثبتت بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم، لهذا 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 بتنقية المواقع وحجب المواقع الضارة ومنع ظهورها [15] وهناك دول عدة إسلامية وغير إسلامية تعمد إلى ترشيح شبكة الإنترنت وحجب المواقع التي ترى أنها ضارة أخلاقيًا أو فكريًا[16].

تبرز بوضوح الحاجة الملحة، مع التوجه المتنامي نحو تقنية المعلومات، 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 تنطوي عليها تلك التقنيات، ولقد أظهرت استبانة أجريت للتعرف على مدى الحاجة إلى وجود تنظيمات ولوائح تحكم قضايا تقنية المعلومات أن 70% يرون الحاجة إلى ذلك [17].

---

[14]- جولة حرة في الرقابة العربية على الإنترنت،
http://articles.islamweb.net/media/index.php?page=article&lang=A&id=83671

([15]) ينظر: جريدة الرياض، العدد: 12328، الثلاثاء 12 1 1423هـ.

[16]- ينظر: الإرهاب الدولي، د.محمد عزيز شكري، دار العلم للملايين/بيروت/ط /أولى/1991.

([17]) ينظر: دراسة الوضع الراهن في محور أحكام في المعلوماتية، ص13.

إنَّ تغلغل تقنية المعلومات الحديثة يجر مخاطر كثيرة في واقعنا، تتطلب من المجتمع والدول جميعًا 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 وأيًا كانت مقاصده، دون تقييد لحرية المجتمع عن الاستثمار البناء لتلك التقنية، فحسب دراسة أجراها مشروع الخطة الوطنية لتقنية المعلومات على ما يزيد عن 700 شخص في المملكة العربية السعودية، اتضح أن 9% من أفراد العينة يقومون بمحاولات اختراق مواقع وأجهزة الأفراد والمؤسسات، بالإضافة إلى ما يقرب من 7% يقومون بهذا العمل بشكل نادر، وهذه النسبة عالية بكل المقاييس، وتزيد هذه النسبة في نوع آخر من المخالفات كإغراق أجهزة الخادمات بالرسائل البريدية، حيث وصلت النسبة إلى ما يزيد عن 15% بالإضافة إلى 12% 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 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 [18].

ويجري العمل في المملكة العربية السعودية لإصدار عدد من الأنظمة التي تضبط التعاملات الإلكترونية وتجرم الاعتداء والعدوان الإلكتروني، ومن أمثلة ذلك مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية [19] فقد نصت المادة (20) من مشروع النظام

([18]) 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، ص7، 6.

([19])جولة حرة في الرقابة العربية على الإنترنت،
http://articles.islamweb.net/media/index.php?page=article&lang=A&id=8367
.1

على أنه: يعد مرتكبًا جناية أي شخص يدخل عن عمد منظومة حاسوب، أو جزءًا 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 (21) من مشروع النظام على أنه يعد مرتكبًا جناية أي شخص يعترض عمدًا وبدون وجه حق وعن طريق أساليب فنية، إرسال البيانات الحاسوبية غير المصرح بها للعموم من منظومة حاسوب أو داخلها[20].

أما المادة (22) فقد نصت على أنه يعد مرتكبًا 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 (23) لتجريم إلحاق الضرر بالبيانات الحاسوبية بالمسح أو التحوير أو الكتمان.

ونصت المادة (25) على أنه يعد مرتكبًا جناية أي شخص يقوم عن عمد وبدون وجه حق وبقصد الغش بإدخال بيانات حاسوبية أو تحويرها أو محوها وينتج عنها بيانات غير صحيحة بقصد اعتبارها معلومات صحيحة.

كما نصت المادة (28) على العقوبات المترتبة على التجاوزات التي حددها النظام [21].

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 أفرادًا أو مؤسسات، وكذلك العقوبات النظامية التي يتم تطبيقها بحقهم [22].

---

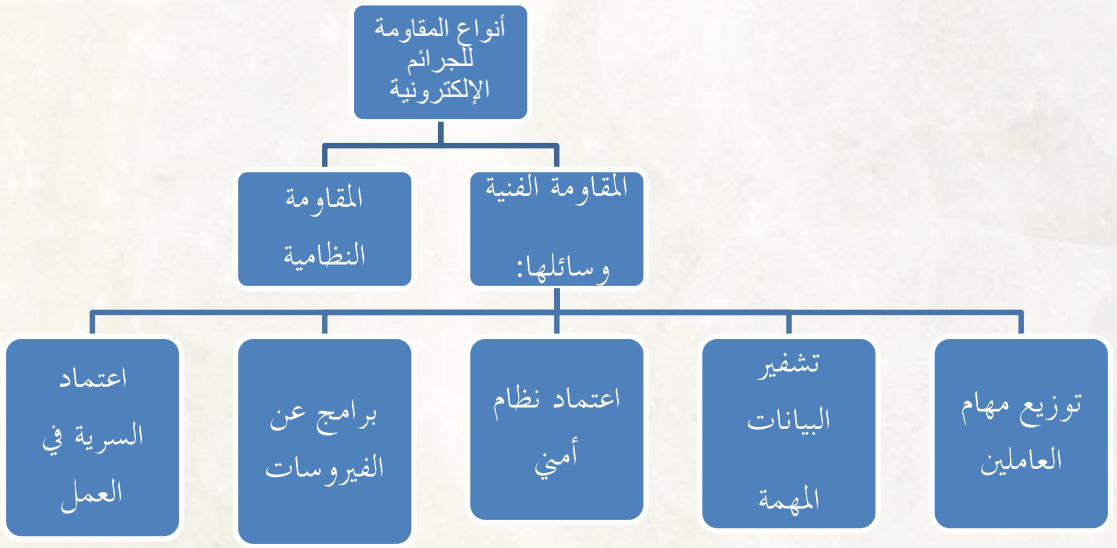
[20]-المرجع السابق.

[21] يُنظر: مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية، في المملكة العربية السعودية 17 3 1423هـ، إعداد: وزارة التجارة، إدارة التجارة الإلكترونية.

[22] جريدة المدينة، العدد: 14489، 20 10 1423هـ، ص17.

منذ أول حالة لجريمة موثقة ارتكبت عام 1958م 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، خصوصًا تلك التي ترتكز 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 كما يبينها هذا المخطط:



يشهد العالم اليوم تقدما تقنيا مذهلا، وهذا يستدعي يقظة على جميع الأصعدة، رغم أن له من الجوانب الإيجابية ما يصعب حصره، إلا أن جوانبه السلبية تكاد تكون مدمرة، ما لم تكن هناك مقاومة لهذه السلبيات، كما يبينا، 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، وأيضًا كون التقنية المستخدمة في هذه الجرائم متطورة جدًا، فالأموال التي يتم استحصالها لعصابة في طوكيو، يمكن تحويلها في ثانية واحدة إلى أحد البنوك في نيويورك، دون إمكانية ضبطها (23).

على الرغم من عدم وجود تعريف محدد لجرائم الإرهاب الإلكتروني إلا أن أحد القانونيين العرب عرفها بأنها "جرائم تبعث الذعر وتنشئ خطراً عاماً يهدد عدداً غير محدد من الأشخاص وتعتمد على أساليب وحشية لا يتناسب ضررها مع الغرض المستهدف بها مثال على ذلك نسف المباني وبصفة خاصة قاعات الاجتماع في وقت يجتمع فيه الناس، وإتلاف الخطوط الحديدية وتسميم المياه"[24] كل ذلك انطلاقا من استخدام المواقع الإلكترونية.

لهذا كله؛ تحتاج أجهزة الأمن 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 قادرًا على تشغيل جهاز الحاسب الآلي، ومعرفة المعدات الإضافية

---

[23] ينظر: جريدة الشرق الأوسط، العدد 8196، يوم الاثنين 7 5 2001، ص 51.

[24]- سيكولوجية الإرهاب السياسي، د.خليل فاضل، ط/أولى، إصدارات خليل فاضل 1991.

فيه، ومعرفة البرمجيات اللازمة للتشغيل، بحيث يتمكن من تقديم الدليل المقبول للجهات القضائية، وأيضًا 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، فمثلًا 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.

و من هنا؛ فإنَّ أدوات القرصنة والإجرام متوافرة، لكن الإجرام يكون في الاستغلال السيئ لهذه الأدوات، ويوجد لدى معظم الدول الكبرى أدوات تعقب لمعرفة مصدر مطلق الفيروس مثلا، 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 أيضا على أصحاب الشبكات كالجامعات والمعاهد التي توفر الإنترنت لمنسوبيها، فقد يستغلها بعضهم لإطلاق الفيروسات أو غيرها من الاعتداءات الإلكترونية[25].

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

---

[25]- ينظر: جريدة الشرق الأوسط، العدد 8196، يوم الاثنين 7 5 2001، ص 51.

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:

1- 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.

2- 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.

3- 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 وتأريخها ونوع العملية التي قام بها وغير ذلك من المعلومات المهمة.

4- توظيف أشخاص تكون مهمتهم المتابعة المستمرة لمخرجات برامج الحاسب الآلي للتأكد من أنها تعمل بشكل صحيح، وخاصة البرامج المالية التي غالبًا 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.

5- 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.

6- عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة.

7- استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد، أو الصوت [26].

بعض التجارب العربية والدولية:

رأيت في البداية أن اتحدث عن جهود المملكة العربية السعودية في التصدي للإرهاب الإلكتروني وذلك لأنَّ المملكة العربية السعودية تتميز باعتمادها على القرآن الكريم والسنة النبوية المطهرة شريعة وحكما في جميع شؤون الحياة، ومن هذا المنطلق فإن التعاملات المرتبطة بتقنية المعلومات، كغيرها من مجالات الحياة، تخضع للأحكام الشرعية المستمدة من الكتاب والسنة، وفي ضوء تلك الأحكام تقوم الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الهيئات الأمنية والقضائية والحقوقية بتنزيل تلك الأحكام واللوائح على القضايا المختلفة.

فقد أنشأت المملكة، بناء على دعوة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز، مركزا دوليا لتبادل المعلومات والخبرات بين الدول وإيجاد قاعدة بيانات ومعلومات أمنية واستخباراتية تستفيد منها الجهات المعنية بمكافحة الإرهاب، تقدمت المملكة بمشروع قرار للجمعية العامة للأمم المتحدة يدعو لتشكيل فريق عمل لدراسة توصيات المؤتمر وما تضمنه «إعلان الرياض» بما في ذلك إنشاء مركز دولي لمكافحة الإرهاب وفق ما أعلنه الأمير سلطان بن عبد العزيز ولي العهد نائب رئيس مجلس الوزراء وزير الدفاع والطيران

([26]) يُنظر: مقدمة في الحاسب الآلي وتقنية المعلومات طارق بن عبد الله الشدي، دار الوطن للنشر الرياض، الطبعة الثانية، 1416هـ، ص188.

والمفتش العام في كلمته أمام الجمعية العامة للأمم المتحدة في 16 سبتمبر (أيلول) 2005م[27].

واعتمدت المملكة، على المستوى المحلي، استراتيجية شاملة لمحاربة الإرهاب، وحرصت على أن تشارك جميع مؤسسات المجتمع في تنفيذ هذه الاستراتيجية، كل في مجال اختصاصه، ونجح علماء المملكة في إيضاح منافاة الإرهاب لتعاليم الإسلام، وما تمثله الأعمال الإرهابية من اعتداء محرم على الأنفس المعصومة من المسلمين وغيرهم، وتفنيد مزاعم الفئة الضالة، التي تروجها التنظيمات الإرهابية لتبرير جرائمها أو كسب أي تعاطف معها. وحث علماء السعودية عموم المواطنين والمقيمين في البلاد على التعاون مع الجهات الأمنية في التصدي للفئة الضالة والإبلاغ عن المتورطين في الأعمال الإرهابية، كما كان للعلماء دور كبير في مناصحة بعض المتأثرين بدعاوى الفئة الضالة في الوقت الذي كانت فيه الجهات الأمنية تحقق نجاحات متتالية في ملاحقة أعضاء هذه الفئة المتورطين بارتكاب جرائم إرهابية وتوجيه عدد كبير من العمليات الاستباقية التي حققت نجاحا كبيرا في إفشال مخططات إرهابية في عدد من مناطق المملكة[28].

وأصدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء رقم (163) في 24 10 1417هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها، ومن ذلك:

---

[27]- ينظر: جريدة الشرق الأوسط، الخميس 05 ربيع الاول 1431 هـ 18 فبراير 2010 العدد 11405.

[28]- المرجع نفسه.

1- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين، أو من يتمتعون بحقوق الملكية لتلك الأنظمة والمعلومات أو المصادر.

2- الامتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.

3- الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح.

4- الامتناع عن إشراك الآخرين في حسابات الاستخدام، أو اطلاعهم على الرقم السري للمستخدم.

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

6- الامتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.

7- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دومًا، ويمنع الآخرين من الاستفادة من خدماتها.

8- الالتزام بما تصدره وحدة خدمات (الإنترنت) بمدينة الملك عبد العزيز للعلوم والتقنية من ضوابط وسياسات لاستخدام الشبكة.

9- نص القرار على تكوين لجنة دائمة برئاسة وزارة الداخلية وعضوية وزارات: الدفاع، والمالية، والثقافة والإعلام، والاتصالات وتقنية المعلومات، والتجارة، والشؤون الإسلامية، والتخطيط، والتعليم العالي، والتربية والتعليم، ورئاسة الاستخبارات، ومدينة الملك عبد العزيز للعلوم والتقنية، وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام (الإنترنت) والتنسيق فيما يخص الجهات التي يراد حجبها، ولها على الأخص ما يأتي:

أ - الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للإنترنت والتي تتنافى مع الدين الحنيف والأنظمة.

ب- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.

وهذا القرار يبين مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطها[29].

ولقد بدأت المملكة العربية السعودية في عقد دورات تدريبية، هي الأولى من نوعها حول موضوع مكافحة جرائم الحاسب الآلي بمشاركة مختصين دوليين، وتقدر تكلفة جرائم الحاسب الآلي في منطقة الشرق الأوسط بحوالي 600 مليون دولار، 25% من هذه الجرائم تعرض لها أفراد ومؤسسات من السعودية خلال عام 2000م فقط، وفيما تعمل لجنة سعودية حكومية مكونة من وكلاء الوزارات المعنية بهذا الموضوع على الانتهاء من إنجاز مشروع نظام التجارة الإلكترونية، فهي مكلفة أيضًا بوضع النظم والبيانات، وتقييم البنية التحتية، وجميع العناصر المتعلقة بالتعاملات الإلكترونية، وتأتي هذه الاستعدادات للحد من انتشار هذا النوع من الجريمة محليًا بعد فتح باب التجارة الإلكترونية فيها، خاصة أن العالم يعاني من انتشارها بشكل واسع بعد أن تطورت بشكل لافت للنظر فيما يخص ماهية هذا النوع من الجرائم، ومرتكبيها، وأنواعها ووسائل مكافحتها، إلى جانب الأحكام والأنظمة التي تحد من ارتكابها[30].

وتهدف الإجراءات في المملكة العربية السعودية إلى تنمية معارف ومهارات المشاركين في مجال مكافحة الجرائم التي ترتكب عن طريق الكمبيوتر، أو عبر شبكة الحاسب الآلي، وتحديد أنواعها ومدلولاتها الأمنية، وكيفية ارتكابها، وتطبيق الإجراءات الفنية لأمن المعلومات في البرمجيات وأمن الاتصالات في شبكات الحاسب الآلي، والإجراءات الإدارية لأمن استخدام المعلومات.

ويرتكب هذا النوع من الجرائم بواسطة عدة فئات مختلفة، ولعل الفئة الأخطر من مرتكبي هذا النوع من الجرائم هي فئة الجريمة المنظمة التي يستخدم أفرادها الحاسب الآلي لأغراض السرقة أو السطو على المصارف والمنشآت التجارية، بما في ذلك سرقة أرقام

---

[29]- ينظر: جريدة الشرق الأوسط، الخميس 05 ربيع الاول 1431 هـ 18 فبراير 2010 العدد 11405.

[30]- ينظر: جريدة الشرق الأوسط، الخميس 05 ربيع الاول 1431 هـ 18 فبراير 2010 العدد 11405.

البطاقات الائتمانية والأرقام السرية ونشرها أحيانًا على شبكة الإنترنت، كما تستخدم هذه الفئة الحاسب الآلي لإدارة أعمالها غير المشروعة كالقمار والمخدرات وغسيل الأموال، وعلى رغم تنوع الفئات التي ترتكب هذه النوعية من الجرائم إلا أن الطرق المستخدمة في الجريمة تتشابه في أحيان كثيرة.

ولذلك فإن أجهزة الأمن بحاجة إلى الكثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر، خاصة في مسرح الجريمة، حتى يكون رجل التحقيق قادرًا على التعامل مع الأدوات الإلكترونية من أجهزة وبرامج [31].

ويجري العمل في المملكة العربية السعودية، كما ذكرنا سالفاً، لإصدار عدد من الأنظمة التي تضبط التعاملات الإلكترونية وتجرم الاعتداء والعدوان الإلكتروني.

([31]) ينظر: السعودية تعقد دورات لمكافحة جرائم الكمبيوتر بعد خسائر تقدر بأكثر من 150 مليون دولار لحقت بمؤسساتها الوطنية، عمر الزبيدي، جريدة الشرق الأوسط، العدد: 8196، يوم الاثنين 7 5 2001م، ص15.

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 1997م 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 150.000دولار ماليزي [32] مع السجن مدة تصل إلى عشر سنوات.

وفي أيرلندا صدر نظام في عام 2001م 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.

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 أمنًا كاملًا، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضرارًا فادحة،

([32]) يُنظر: 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 10 11 1423هـ.

يغدو التعاون الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمرًا متحتمًا، ومع الحاجة الماسة لهذا التعاون إلا أن عقبات عدة تقف في سبيله أبرزها ما يأتي:

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

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

3- اختلاف مفاهيم الجريمة باختلاف الحضارات.

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

5- 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 أطرافًا 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 تنطوي 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 [33].

([33]) يُنظر: 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، 2000م، ص49، 48.

الخاتمة

من خلال المتابعة المتأنية لهذا الموضوع والدراسة العلمية الدقيقة توصلنا لجملة من النتائج نجملها في النقاط التالية:

- ✓ من الضروري بمكان، أن تخضع التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة للأحكام الشرعية المستمدة من الكتاب والسنة، وفي ضوء تلك الأحكام تقوم الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الهيئات القضائية والأمنية والحقوقية بتنزيل تلك الأحكام واللوائح على القضايا المختلفة، وفض النزاعات الناتجة عنها.
- ✓ إن كثيرًا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها[34].
- ✓ يُعتبر الاعتداء على مواقع الإنترنت بالاختراق أو التدمير ممنوع شرعًا، ويعد تدمير المواقع من باب الإتلاف وعقوبته أن يضمن ما أتلفه فيحكم عليه بالضمان.
- ✓ تصميم وإنشاء المواقع ذات الصبغة الإرهابية ينتشر انتشارا مذهلا، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك.
- ✓ حجب المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق من الأساليب المجدية والنافعة لمكافحة الإرهاب الإلكتروني.

---

[34]- ينظر: جريدة الشرق الأوسط، الخميس 05 ربيع الاول 1431 هـ 18 فبراير 2010 العدد 11405.

- ✓ لا تزال الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام في مراحلها الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة 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.
- ✓ تعليم وإعلام الرأي العام العربي حول الإرهاب الإلكتروني والخطر الإرهابي الذي يشكله عالم الإنترنت السلبي للأمن والمصالح العربية والتقاليد.
- ✓ يجب على الدول العربية أن تُضاعف من قيمة الميزانية المخصصة لمكافحة الإرهاب الإلكتروني واعتبار ذلك أولوية.
- ✓ إصدار مراسيم من أجل تنظيم تكوين محققين ورجال شرطة وقضاة على التقنية المعلوماتية والمعرفة الكافية لجرائم الانترنت.
- ✓ نظرا لخطورة الإرهاب الإلكتروني على الأفراد والجماعات 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.
- ✓ قامت المملكة العربية السعودية، ولازالت، بمجهودات جبارة في مكافحة الإلكتروني، عن كريق إنشاء أنظمة أمنية، وعقد الدورات التدريبة في مقاومة الإرهاب الإلكتروني.
- ✓ على مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سنت أنظمة لضبط التعاملات الإلكترونية، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الإلكترونية ومكافحة الإرهاب الإلكتروني.

و في ختام البحث نحمد الله الذي وقفنا لهذا، ونستغفره من كل زلل.