لمملكـة العربية السعوديـة
وزارة التعليم العالي
جامعة الإمام محمد بن سعود الإسلامية

وسائل الإرهاب الإلكتروني

حكمها في الإسلام وطرق مكافحتها

إعـداد

د. عبدالرحمن بن عبدالله السند

اللجنة العلمية

للمؤتمر العالمي عن موقف الإسلام

من الإرهاب

١٤٢٥هـ / ٢٠٠٤م

بسم الله الرحمن الرحيم

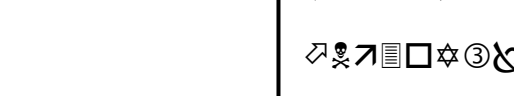
البحوث والأوراق المنشورة في المؤتمر
تعبر عن وجهـــة نظـر كاتبيها ، ولا تعبر بالضرورة عن رأي الجامعـــة .

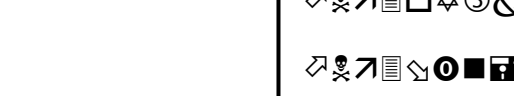
مقدمـــة :

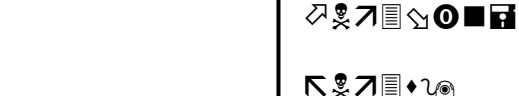
الحمد لله رب العالمين ، والعاقبة للمتقين ، والصلاة والسلام على أشرف الأنبياء و أشرف المرسلين ، نبينا محمد وعلى آله وصحبه أجمعين .

أما بعد :

فإن الشريعة الإسلامية جاءت كاملة شاملة ، صالحة لكل زمان ومكان محققة لسعادة البشرية في الآجل والعاجل فقد جاءت من عند الله – سبحانه وتعالى – خالق الناس ، والعالم بما يصلحهم في دنياهم وأخراهم ، قال الله تعالى : ↓  ↑ (١).

وقال الله تعالى: ↓ 





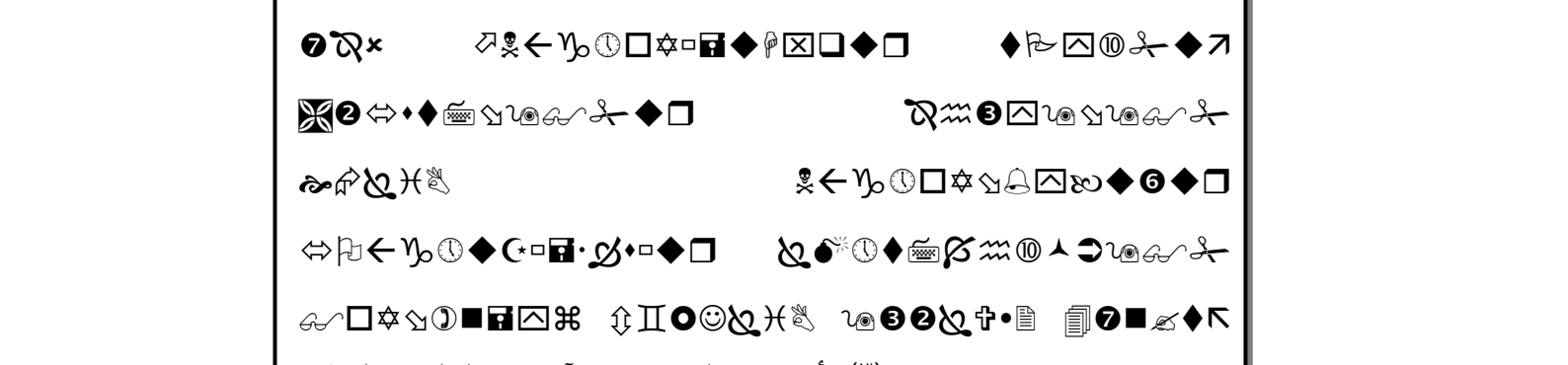
↑ (٢) .

لقد خلق الله الإنسان فأكرمه ، قال الله سبحانه: ↓

---

(١) سورة الأنعام ،آية : ٣٨ .

(٢) سورة المائدة ، آية : ٣ .



واعتدال الخلق وغير ذلك ومنه طهارتهم بعد الموت "وحملناهم في البر" على الدواب "والبحر" على السفن "ورزقناهم من الطيبات وفضلناهم على كثير ممن خلقنا" كالبهائم والوحوش "تفضيلا" فمن بمعنى ما أو على بابها وتشمل الملائكة والمراد تفضيل الجنس ولا يلزم تفضيل أفراده إذ هم أفضل من البشر غير الأنبياء [٤] . ولقد ميز الله الإنسان بالعقل والفهم ليعمل على إسعاد نفسه وبيئته ويسعى في عمارة الكون بما يصلح الخلق والأرض ، وإذا انحرف الإنسان عن هذه المهمة ونزع إلى الشر والفساد فهو مصادم للفطرة السليمة التي فطر الله الإنسان عليها ، إن من أبرز مظاهر الانحراف عن الفطرة السليمة في هذا العصر الإرهاب ولاسيما استغلال الوسائل الحديثة في ذلك، ولعل من الصور الحديثة للإرهاب استخدام الوسائل الإلكترونية فيه، فكان هذا البحث لبيان (الإرهاب

(٣) سورة الإسراء ، آية : ٧٠ .
(٤) تفسير الجلالين آية ٧٠ من سورة الإسراء.

الإلكتروني وموقف الإسلام منه) وقد جعلته في المباحث الآتية :

تمهيد :

المطلب الأول : المقصود بالإرهاب الإلكتروني

المطلب الثاني : خطر الإرهاب الإلكتروني

المبحث الأول : وسائل الإرهاب الإلكتروني

المطلب الأول : البريد الإلكتروني

المطلب الثاني : إنشاء مواقع على الإنترنت

المطلب الثالث: تدمير المواقع

المبحث الثاني : طرق مكافحة الإرهاب الإلكتروني

المطلب الأول : ترشيح الدخول على الإنترنت

المطلب الثاني : أنظمة التعاملات الإلكترونية

المطلب الثالث : أنظمة الحماية من الاعتداءات الإلكترونية

المبحث الثالث : جهود التصدي للإرهاب الإلكتروني

المطلب الأول : جهود المملكة العربية السعودية في التصدي للإرهاب الإلكتروني

المطلب الثاني : الجهود الدولية في التصدي للإرهاب الإلكتروني

الخاتمة.

تمهيـد

المطلب الأول - المقصود بالإرهاب الإلكتروني :

الإرهاب بعني في اللغات الأجنبية القديمة مثل اليونانية : حركة من الجسد تفزع الآخرين(١).

وقد أطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم(٢) ، 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 تعريفا 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

---

(١) انظر : الإرهاب السياسي والقانون الجنائي ، عبدالرحيم صدق ، دار النهضة العربية - القاهرة ،١٩٨٥ م ، ص٨١.

(٢) انظر : المعجم الوسيط ٣٧٦/١.

الخاصة أو اختلاسها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر(١).

ولعل من أفضل التعاريف الاصطلاحية للإرهاب من حيث الشمولية وتحديد سلوك الإرهاب ما توصل إليه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فقد عرف الإرهاب بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً 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 تنفيذاً 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 و الأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها(٢).(٣)

وقد أصدر مجمع الفقه الإسلامي الدولي قراراً في دورته

---

(١) انظر : الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م.

(٢) انظر : بيان مكة المكرمة الصادر عن المجمع الفقهي لرابطة العالم الإسلامي ، الدورة السادسة عشرة ، مكة المكرمة ، رابطة العالم الإسلامي ١٤٢٢هـ ، ص : ٨ .

(٣) انظر : الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي ، الدكتور/ حسن بن محمد سفر ، بحث مقدم لمجمع الفقه الإسلامي الدولي ، ص : ٩–١١ .

الرابعة عشرة المعقودة في الدوحة في شهر ذي القعدة من عام ١٤٢٣هـ ذكر فيه تعريف مصطلح الإرهاب بأنه: العدوان أو التخويف أو التهديد مادياً أو معنوياً 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[١] .

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.

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

(١) انظر : قرارات وتوصيات الدورة الرابعة عشرة لمجلس مجمع الفقه الإسلامي ، الدوحة – قطر ، ٨–١٣ ذو القعدة ١٤٢٣هـ.

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 آخذ في التطور بشكل كبير تماشياً مع التطور في الجريمة الإلكترونية.

لقد أصبح الإرهاب الإلكتروني هاجسا 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 والاحترازات لمواجهة الإرهاب الإلكتروني ، إلا أن هذه الجهود قليلة ولا نزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

المبحث الأول
وسائل الإرهاب الإلكتروني

المطلب الأول – 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 المرسلة بمكان معين ، بل يمكن الاطلاع 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 وأمنا 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 وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

لقد نهى الله – جل جلاله – عن التجسس ، فقال سبحانه: ↓ ❐◆•• ✍❐♌■○○○❍❑✂☎ ↑ [1] ، ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرماتهم ، ففي الحديث أن النبي ε قال : (إنك إن اتبعت عورات المسلمين أفسدتهم أو كدت أن تفسدهم) [2] ، واختراق البريد الإلكتروني هو خرق لخصوصية الآخرين وهتك لحرماتهم وتجسس على معلوماتهم وبياناتهم التي لا يرغبون أن يطلع عليها غيرهم ، والنبي ε يقول : (ولا تحسسوا ولا تجسسوا) [3] .

فالشريعة الإسلامية كفلت حفظ الحقوق الشخصية للإنسان

---

(١) سورة الحجرات ، الآية : ١٢ .

(٢) رواه أبو داود ، حديث رقم (٤٨٨٨) ، وقال عنه النووي : إسناده صحيح . (انظر : رياض الصالحين باب النهي عن التجسس ، ص٥٩٦).

(٣) رواه البخاري في كتاب الأدب ، باب ما ينهى عن التحاسد والتدابر ، ورواه مسلم في كتاب البر و الصلة والآداب ، باب : تحريم الظن والتجسس والتنافس برقم (٢٥٦٣) . .

وحرمت الاعتداء عليها بغير حق ، وهؤلاء الذين يعتدون على بيانات الآخرين ومعلوماتهم عبر اختراق رسائلهم البريدية الإلكترونية آثمون لمخالفة أمر الشارع الحكيم ومستحقون للعقاب التعزيري الرادع لهم ، ولا بد من إشاعة هذا الحكم بين الناس وتوعية المتعاملين بشبكة المعلومات العالمية (الإنترنت) بخطورة انتهاك خصوصية الآخرين وحكم ذلك في الشريعة الإسلامية ، وأن هذا الأمر مما استقرت الشريعة على تحريمه والنهي عنه ، وقد تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها ، بل قد تنادت الدول إلى تجريم مخترقي البريد الإلكتروني لما فيه من ضياع للحقوق واعتداء على خصوصيات الآخرين وأسرارهم، ولاسيما إذا كان ذلك لاستغلالها في الجرائم الإرهابية والعدوان على الآخرين .

واستثناء من ذلك فقد يكون التجسس مشروعاً في أحوال معينة كالتجسس على المجرمين، فقد لا يعرفون إلا بطريق التجسس، وقد أجاز الفقهاء التجسس على اللصوص وقطاع الطريق، وطلبهم بطريق التجسس عليهم وتتبع أخبارهم(١)، وكذلك يجوز التجسس في حال الحرب بين المسلمين وغيرهم لمعرفة أخبار جيش الكفار وعددهم وعتادهم ومحل إقامتهم وما إلى ذلك .

أما الجاسوس الذي يتجسس على المسلمين فقد ذهب الحنفية إلى

---

(١) انظر : تبصرة الحكام لابن فرحون ١٧١/٢ .

أن يوجع عقوبة ويطال حبسه حتى يحدث توبة [١]، وذهب المالكية إلى أنه يقتل ولا يستتاب ولا دية لورثته كالمحارب لإضراره بالمسلمين وسعيه بالفساد في الأرض، وقيل : يجلد نكالاً ويطال حبسه وينفى من الموضع الذي كان فيه ، وقيل : يقتل إلا أن يتوب، وقيل : يقتل إلا أن يعذر بجهل ، وقيل : يقتل إن كان معتاداً لذلك [٢]. وذهب الشافعية [٣] إلى أن الجاسوس المسلم يعزر ولا يجوز قتله، وإن كان ذا هيئة – أي سلف كريم في خدمة الإسلام– عفي عنه لحديث حاطب بن أبي بلتعةت [٤] ، وذهب الحنابلة إلى أن الجاسوس يقتل لضرره على المسلمين[٥] .

وكذلك يجوز اختراق البريد الإلكتروني للمجرمين المفسدين في الأرض واللصوص وقطاع الطريق ، لتتبعهم ومعرفة خططهم وأماكن وجودهم ، لقطع شرهم ودفع ضررهم عن المسلمين وهذا موافق لمقاصد الشريعة الإسلامية التي جاءت بحفظ الدين والعرض والمال والنفس والعقل .

المطلب الثاني – إنشاء مواقع على الإنترنت :

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم ،

---

(١) انظر : الخراج لأبي يوسف ٢٠٥ .
(٢) انظر : تبصرة الحكام لابن فرحون ١٧٧/٢ ، وتفسير القرطبي ٥٢/١٨ .
(٣) انظر : حاشية القليوبي ٢٢٦/٤.
(٤) حديث حاطب بن أبي بلتعة أخرجه البخاري ١٤٣/٦ ، وأخرجه مسلم ١٩٤١/٤ .
(٥) انظر : شرح منتهى الإرادات ١٣٨/٢ .

بل تعليم 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 (HTML) Hyper text mark up language. ولأجل رؤية هــذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (WWW Browser) ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة .[١]

وتسعى الجهات الرسمية ، والمؤسسات ، والشركات ، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الإنترنت في شهر ١٠ / ٢٠٠٠م إلى أكثر من ٢٢مليون موقع .[٢]

إن الشبكة العنكبوتية (World Wide Web) أو نظام الويب الذي ابتكره العالم الإنجليزي تم بيرنرس عام ١٩٨٩م ، يرتكز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات

---

(١) انظر : التجارة على الإنترنت ،سايمون كولن ، نقله إلى العربية يحيى مصلح ، بيت الأفكار الدولية بأمريكا ١٩٩٩م ، ص٢٦.

(٢)انظر موقع : www.yahoo.com

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، من خلال برامج التصفح.

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام ، وتبادل الآراء والأفكار والمعلومات صعبا 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 صعبا ، 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 على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن 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.

ولا شك أن إنشاء المواقع للعدوان وتضليل الآخرين ونشر الأفكار الهدامة محرم ولا يجوز يقول سماحة مفتي عام المملكة الشيخ عبد العزيز بن عبد الله آل الشيخ : (شبكة الإنترنت من وسائل الاتصالات الحديثة السريعة في إيصال المعلومات الواسعة من حيث الانتشار وسهولة الوصول إليها وهي إن استغلت في الخير والدعوة إلى الله ونشر دين الله في أصقاع الأرض من قبل الأفراد والمؤسسات الإسلامية المختلفة ، فلا شك أنها من الجهاد في سبيل الله بالبيان واللسان ويجب على المسلمين استغلالها وتسخيرها لهذا الغرض الخير ، أما المواقع الفاسدة المخلة والمضرة بعقائد المسلمين من خلال التلبيس والتشكيك والمضرة بأخلاقهم كذلك من خلال ما يعرض فيها من الدعوة إلى الفساد وتيسير طرقه وتعليم الناشئة لهذه الأمور ، وتربيتهم عليها من خلال ما يعرض فيها ... فلا ريب أن هذا من أعظم المنكرات التي يجب التصدي لها وإنكارها وفق قواعد إنكار المنكر التي جاء بها النص من الكتاب والسنة ، وبينها وفصلها علماء الأمة ، والله تعالى يقول :

(١). وقال ε كما في الحديث الذي رواه أبو سعيد الخدري τ : «من رأى منكم منكراً فليغيره بيده ، فإن لم يستطع فبلسانه ، فإن لم يستطع فبقلبه ، وذلك أضعف الإيمان»)(٢). (٣)

المطلب الثالث : تدمير المواقع :

تدمير المواقع 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 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

---

(١) سورة آل عمران الآية (١٠٤) .

(٢) أخرجه الإمام مسلم في باب : بيان كون النهي عن المنكر من الإيمان ، من كتاب الإيمان ٦٩/١ .

(٣) جريدة الرياض ، العدد ١٢٠٥١ ، يوم الجمعة ١ / ربيع أول / ١٤٢٠هـ.

ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانات 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 ، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين ، بل قد يكونون خبراء في مجال الحاسب الآلي. (١)

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة 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 لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي.(٢)

يمكن لمزود خدمات الإنترنت (ISP) من الناحية النظرية أن

---

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

(٢) انظر : الاختراقات الإلكترونية خطر كيف نواجهه ، موزة المزروعي ، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة ، العدد التاسع ، سبتمبر ٢٠٠٠م ، ص٥٤ .

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، وتأريخ وزمن الاتصال والانفصال عن الشبكة ، وبعض البيانات الأخرى، إن معرفة البيانات التفصيلية للمستخدم تجعل الإقدام على الاعتداء الإلكتروني أقل ، وذلك لأن بعض الذين يحصل منهم الاعتداء الإلكتروني يتم منهم ذلك بسبب ظنهم أن بياناتهم التفصيلية لا يمكن الاطلاع عليها، فيظن أنه بمجرد دخوله على الشبكة باسم وهمي تصبح بياناته غير معلومة ، وهذا خطأ .[1]

(١) انظر : جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظور أمني ، للعقيد الدكتور / ممدوح عبدالحميد عبدالمطلب ، ص٤٢ ، 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 ٢٠٠٠م .

إن من الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (mails–e) 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. (١)

وفي الواقع إن هناك أسباباً لوقوع عملية تدمير المواقع ومن 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 المخترق .

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.

---

(١) انظر : التكييف 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 ، ص٤.

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(١) 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 ، ويعد عام ٢٠٠٢م من أكثر الأعوام اختراقاً، فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل

(١) 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 حرجة ، ودعت المستخدمين إلى تركيب برنامج ترقيعي لحل المشكلة . (جريدة الرياض ، العدد ١٢٥٤٢ ، السبت ٢٠ / ٨ / ١٤٢٣هـ ، ص١٩) .

والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات.(١)

حكم تدمير المواقع :

لقد جاءت الشريعة الإسلامية بحفظ حقوق الآخرين وصيانتها ، قال الله – عز وجل – في النهي عن الاعتداء : ﴿ ... ﴾(٢) ، فنهى الله عز وجل عن الاعتداء ، وإن المواقع على شبكة المعلومات العالمية حق للآخرين لا يجوز الاعتداء عليه بأي وجه من الاعتداء ، وتدمير المواقع نوع اعتداء فهو محرم ولا يجوز ، وقد صدر قرار مجمع الفقه الإسلامي في دورته الخامسة سنة ١٤٠٩هـ بأن حقوق التأليف والاختراع أو الابتكار مصونة شرعاً ، ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها(٣).

فالاعتداء على مواقع الإنترنت ممنوع شرعاً من باب أولى ، فإذا كان حق الاختراع والابتكار مصوناً شرعاً ، فكذلك الموقع على شبكة الإنترنت مصون شرعاً ولا يجوز الاعتداء عليه.

ويعتبر تدمير الموقع من باب الإتلاف وعقوبته أن يضمن ما

---

(١) انظر : المرجع السابق ، العدد ١٢٤٦٠ ، يوم الاثنين ٢٦ / ٥ / ١٤٢٣هـ ، ص٣٢ .

(٢) سورة البقرة ، الآية : ١٩٠ .

(٣) مجلة مجمع الفقه الإسلامي ، العدد الخامس ، المجلد الثالث ، ص٢٢٦٧ .

أتلفه ، فيحكم عليه بالضمان.

المبحث الثاني
طرق مكافحة الإرهاب الإلكتروني

المطلب الأول – 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 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 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 والشـــرور ، بل المسلم يسأل ربه أن يحفظه من التعرض للفتن ، والله – عز وجل – يقول عن يوسف عليه السلام

(١) سورة يوسف ، الآية :٣٣ .

والأدوات التي تقوم بتنقية المواقع وحجب المواقع الضارة ومنع ظهورها(١)، وهناك دول عدة إسلامية وغير إسلامية تعمد إلى ترشيح شبكة الإنترنت وحجب المواقع التي ترى أنها ضارة أخلاقياً أو فكرياً.

المطلب الثاني – 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 تنطوي عليها تلك التقنيات ، ولقد أظهرت استبانة أجريت للتعرف على مدى الحاجة إلى وجود تنظيمات ولوائح تحكم قضايا تقنية المعلومات أن ٧٠٪ يرون الحاجة إلى ذلك(٢).

إن المخاطر الكامنة في تغلغل تقنية المعلومات الحديثة في واقعنا تتطلب من المجتمع والدول جميعاً الحيلولة دون حصول تلك

(١) انظر : جريدة الرياض ، العدد : ١٢٣٢٨ ، الثلاثاء ١٢ /١/ ١٤٢٣هـ .
(٢) انظر : دراسة الوضع الراهن في محور أحكام في المعلوماتية ، ص١٣ .

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 لحرية 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 الخادمات 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 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 [١].

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[٢] ، 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

---

(١) 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 ، ص٦،٧.

(٢) وقد كلف الباحث من قبل وزارة التجارة بالمشاركة في إعداد هذا النظام ، فشارك في صياغته ، و قد تم رفع المشروع للجهات العليا لاعتماده .

شبكة حاسوب .

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

ونصت المادة (٢٥) على أنه يعد مرتكباً 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 (٢٨) على العقوبات المترتبة على التجاوزات التي حددها النظام[١].

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 [٢].

المطلب الثالث – أنظمة الحماية الفنية من الاعتداءات الإلكترونية:

---

(١) انظر : مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية ، في المملكة العربية السعودية ١٤٢٣/٣/١٧هـ ، إعداد : وزارة التجارة ، إدارة التجارة الإلكترونية .

(٢) جريدة المدينة ، العدد : ١٤٤٨٩ ، ١٤٢٣/١٠/٢٠هـ ، ص١٧ .

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 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 :

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.

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 وظيفة 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(١).

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

---

(١) انظر : جريدة الشرق الأوسط ، العدد ٨١٩٦ ، يوم الاثنين ٢٠٠١/٥/٧ ، ص ٥١ .

، 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 مثلا ، أو الهجـــوم على بريد إلكتروني ، أو موقـــع 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 الســـري حتى لا يستغل من قبل الآخرين ، وينطبق هذا أيضـــاً على أصحاب الشبكات كالجامعات 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- استخـــدام 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 أخـــرى, 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

وتأريخها 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 تخزن 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[1].

(١) انظر : مقدمة في الحاسب الآلي وتقنية المعلومات طارق بن عبد الله الشدي ، دار الوطن للنشر الرياض ، الطبعة الثانية ، ١٤١٦هـ ، ص١٨٨ .

المبحث الثالث
جهود التصدي للإرهاب الإلكتروني

المطلب الأول – جهود المملكة العربية السعودية في التصدي للإرهاب الإلكتروني:

تتميز المملكة العربية السعودية 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.

ولقد صدرت 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 (١٦٣) في ١٤١٧/١٠/٢٤هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها ، ومن ذلك :

١- 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 .

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

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

٤- الامتناع عن إشراك الآخرين في حسابات الاستخدام ، أو إطلاعهم على الرقم السري للمستخدم .

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

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

٧- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دوماً ، ويمنع الآخرين من الاستفادة من خدماتها.

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

٩- 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 عبدالعزيز 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.

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 ٦٠٠ مليون دولار ، ٢٥٪ من هذه الجرائم تعرض لها أفراد ومؤسسات من السعودية خلال عام

٢٠٠٠م فقط ، وفيما تعمل لجنة سعودية حكومية مكونة من وكلاء الوزارات المعنية بهذا الموضوع على الانتهاء من إنجاز مشروع نظام التجارة الإلكترونية ، فهي مكلفة أيضاً بوضع النظم والبيانات ، وتقييم البنية التحتية ، وجميع العناصر المتعلقة بالتعاملات الإلكترونية ، وتأتي هذه الاستعدادات للحد من انتشار هذا النوع من الجريمة محلياً 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 .

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 البطاقات الائتمانية والأرقام السرية ونشرها أحياناً 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 قادراً على التعامل مع الأدوات الإلكترونية من أجهزة وبرامج(١).

وكما ذكرنا سابقاً يجري العمل في المملكة العربية السعودية لإصدار عدد من الأنظمة التي تضبط التعاملات الإلكترونية وتجرم الاعتداء والعدوان الإلكتروني.

المطلب الثاني – 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

(١) انظر : السعودية تعقد دورات لمكافحة جرائم الكمبيوتر بعد خسائر تقدر بأكثر من ١٥٠ مليون دولار لحقت بمؤسساتها الوطنية ، عمر الزبيدي ، جريدة الشرق الأوسط ، العدد : ٨١٩٦ ، يوم الاثنين ٢٠٠١/٥/٧م ، ص١٥ .

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 ١٥٠,٠٠٠دولار ماليزي(١)، مع السجن مدة تصل إلى عشر سنوات .

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 .

---

(١) انظر : دراسة تجارب الدول في مجال أحكام في المعلوماتية ، إعداد : د/ محمد القاسم ،د/رشيد الزهراني د/عبدالرحمن السند ، عاطف العمري ، مشروع الخطة الوطنية لتقنية المعلومات ١٤٢٣/١١/١٠هـ

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 ، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة ، مما قد يسبب لبعض الدول أو الأفراد أضراراً فادحة ، يغدو التعاون الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمراً متحتماً ، ومع 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.

وسعياً 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 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 [1].

(١) 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 ، ص٤٨،٤٩ .

الخاتـــمة:

الحمد لله الذي بنعمته تتم الصالحات ، والصلاة والسلام على من ختمت ببعثته الرسالات نبينا محمد وعلى آله وصحبه وسلم تسليما كثيراً . أما بعد : فلقد أصبح الإرهاب الإلكتروني هاجسا 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 والاحترازات لمواجهة الإرهاب الإلكتروني ، إلا أن هذه الجهود قليلة ولا نزال 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.

إن من أبرز ما توصلت إليه في البحث الآتي:

أولاً : أن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة يجب أن تخضع 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.

ثانياً : أن من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني 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.

ثالثاً : اختراق البريد الإلكتروني خرق لخصوصية الآخرين وهتك لحرمة معلوماتهم وبياناتهم والله – عز وجل – نهى عن التجسس، والشريعة الإسلامية كفلت حفظ الحقوق الشخصية للإنسان وحرمت الاعتداء عليها بغير حق. كما أن الاعتداء على مواقع الإنترنت بالاختراق أو التدمير ممنوع شرعاً، ويعد تدمير المواقع من باب الإتلاف وعقوبته أن يضمن ما أتلفه فيحكم عليه بالضمان.

رابعاً : يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم ، 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.

خامساً : 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.

سادساً : على الرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية والتي تعتبر وسيلة من وسائل مكافحة الإرهاب الإلكتروني، 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.

سابعاً : 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،

بحيث تتمكن 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.

ثامناً : تضطلع المملكة العربية السعودية بجهود جبارة في مكافحة الإرهاب الإلكتروني ، ولقد أصدرت مجموعة من الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني ، إضافة إلى عقد دورات تدريبية، هي الأولى من نوعها حول موضوع مكافحة جرائم الحاسب الآلي بمشاركة مختصين دوليين.

تاسعاً : 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.

وختاماً فإني أحمد المولى عز وجل على ما منّ به عليّ من إكمال هذا البحث والذي أرجو أن ينال القبول منه سبحانه وأن يبارك فيه ، وأن ينفع به ، وأن يرزقني الإخلاص في القول والعمل وأن يجعل هذا العمل خالصاً لوجهه الكريم.

والحمد لله من قبل ومن بعد ، واستغفر الله من الزلل والخطأ ،

فجل من لاعيب فيه وعلا ، وصلى الله وسلم على نبينا محمد وعلى آله وصحبه أجمعين.

المراجــع

- الإرهاب السياسي والقانون الجنائي . عبد الرحيم صدق ، دار النهضة العربية – القاهرة ،١٩٨٥ م .
- الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي. الدكتور/ حسن بن محمد سفر ، بحث مقدم لمجمع الفقه الإسلامي الدولي ، الدورة الرابعة عشرة ، الدوحة– قطر ٢٠٠٣/١/١١م .
- تبصرة الحكام في أصول الأقضية ومناهج الأحكام . برهان الدين إبراهيم بن محمد بن فرحون اليعمري المالكي ، تخريج / جمال مرعشلي ، دار الكتب العلمية ، بيروت، لبنان.
- تجارب الدول في مجال أحكام في المعلوماتية . د/ محمد بن عبدالله القاسم ، د/ رشيد الزهراني ، عبد الرحمن بن عبد الله السند ، عاطف العمري ، مشروع الخطة الوطنية لتقنية المعلومات ، ١٤٢٣هـ .

- التجارة على الإنترنت . سايمون كولن ، نقله إلى العربية ، يحيى مصلح ، بيت الأفكار الدولية بأمريكا ١٩٩٩م .
- التدمير المتعمد لأنظمة المعلومات الإلكترونية . د / عباده أحمد عبادة ، مركز البحوث والدراسات ، شرطة دبي بدولة الإمارات العربية المتحدة .
- التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية . د/ خالد بن محمد الطويل ، مركز المعلومات الوطني ، وزارة الداخلية ، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات ١٩ / ١٠ / ١٤٢٣هـ الرياض .
- التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت . عماد علي الخليل ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، الذي نظمته كلية الشريعة والقانون ، بجامعة الإمارات العربية المتحدة ، عام٢٠٠٠م.
- التهديدات الإجرامية للتجارة الإلكترونية . د / سهير حجازي ، مركز البحوث والدراسات ، شرطة دبي بدولة الإمارات العربية المتحدة .
- جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت). د / ممدوح عبدا لحميد عبد المطلب ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، بجامعة الإمارات العربية المتحدة ، عام ٢٠٠٠م .
- 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 كلية الشريعة والقانون ، بجامعة الإمارات العربية المتحدة ، عام ٢٠٠٠م .
- حاشية قليوبي على شرح المحلى . شهاب الدين أحمد بن محمد بن

سلامة قليوبي ، شركة مكتبة ومطبعة مصطفى البابي الحلبي ، مصر .

- شرح منتهى الإرادات . منصور بن يونس البهوتي ، تحقيق ونشر / مكتبة نزار الباز .
- قرارات وتوصيات مجمع الفقه الإسلامي . منظمة المؤتمر الإسلامي ، جدة ، دار القلم ، دمشق .
- مقدمة في الحاسب الآلي وتقنيات المعلومات . طارق بن عبد الله الشدي ، دار الوطن للنشر ، الرياض ، الطبعة الثانية ، ١٤١٦هـ .