قضايا قانونية

في أمن المعلومات وحماية البيئة الإلكترونية

محمد سيد سلطان

ناشرون

نشر إلكترونيًّا في ربيع الأول،١٤٣٣/يناير، ٢٠١٢.

التدقيق اللغوي: آمال المطيري
الإخراج الفني والغلاف: شيماء رضوان
صورة خلفية الكتاب نقلًا عن: http://wallpapers-hq.ru/en

محتـــويات الكتـــــاب

المقدّمة

إن التقدم الكبير الذي تم إحرازه في مجال تكنولوجيا المعلومات والاتصالات له تأثير غير مسبق على مجتمعنا وحياتنا إليومية في وقتنا الحالي، فالنسبة الكبيرة من أنشطتنا اليومية تعتمد اعتمادًا كبيرًا على تكنولوجيا المعلومات. هذا الاعتماد واضح كل الوضوح على مستوى القطاعين العام والخاص على حدٍ سواء. فالعوامل الحيوية في الحياة العامة مثل النقل الجوي والبري والبحري وخطوط السكك الحديد والمرور، والطاقة والكهرباء والغاز، والاتصالات السلكية واللاسلكية، والهواتف النقالة، والشرطة، وطلب الإغاثة، والمستشفيات، والمكاتب الحكومية، والعديد من الخدمات العامة، تنظم وتراقب من خلال استخدام أجهزة الحاسب الآلي وشبكات الاتصال.

والوضع لا يختلف كثيرًا في القطاع الخاص، فالعديد من المعاملات والأعمال التجارية تتم عن طريق أجهزة الحاسب الآلي، فهناك البيع الإلكتروني والشراء الإلكتروني، والأسهم، والبنوك، وغيرها الكثير من المؤسسات التي تستثمر مليارات الدولارات من خلال البيئة الإلكترونية.

هذا الاعتماد الكبير على تكنولوجيا المعلومات خلق شكلًا جديدًا من أشكال الضعف، الذي يواجه المجتمع والحياة العامة والخاصة، ويضع الجميع في قبضة يد الإرهابيين لتحقيق أغراضهم الغير مشروعة. فمع مرور الوقت ظهرت الكثير من الجرائم التي تستهدف البيئة الإلكترونية، هذه الجرائم هي واحدة من أسرع القطاعات نموًا في الأنشطة الإجرامية على وجه الأرض، فهي تغطي مجموعة واسعة من الأنشطة غير القانونية بما في ذلك الاحتيال المالي، والقرصنة، وتحميل الصور الإباحية من

الإنترنت، والفيروس، والمطاردة، والحرمان من الخدمة، والتشجيع على الكراهية العنصرية. وهذا أدى بدوره إلى تآكل في الحماية القانونية التي توفرها القوانين الوطنية لمكافحة هذه الجرائم.

والحرب العالمية التي تسود العالم اليوم هي الحرب على الإرهاب، فمواجهة الإرهاب آخذة في التغير، في حين أن الدوافع لا تزال هي نفسها. فالعالم يواجه الآن أسلحة جديدة للإرهاب غير مألوفة، منها الإرهاب الإلكتروني، الذي يعتمد في هجماته على أهداف إلكترونية من خلال إتلافها أو تدميرها. فسوف يكون الضغط على لوحة المفاتيح للوصول إلى غرض إرهابي أسهل مما يمكن، ما لم تكون هناك إجراءات أمنية وضعت لمنع هذا الغرض.

فتكنولوجيا المعلومات تعتبر من أرخص الوسائل التي يمكن استخدامها في الهجمات الإرهابية، فبالرغم من أن تكنولوجيا المعلومات وتشغيل الشبكات والحماية اللازمة لهم مكلفة جدًّا، فحين أن الوسائل اللازمة لمهاجمتهم رخيصة، فكل ما يحتاج إليه المرء هو جهاز حاسب إلى ومودم.

ومنذ فترة من الزمن، كان العديد من الخبراء يتوقعوا بنسبة ضئيلة جدًّا أن أنظمة الكمبيوتر والإنترنت يمكن أن تكون هدفًا لهجوم إرهابي من شخص أو جماعة أو دولة، ولكن بعد لحظة معينة من الزمن تضخمت هذه النسبة الضئيلة تدريجيًّا لتصل إلى ذروتها، خصوصًا بعد أحداث ١١ سبتمبر، ليتيقن الجميع بأن الإرهاب الإلكتروني تهديد حقيقي يهدد المجتمع الدولي بأكمله.

فهذا البحث يقوم على فرضية أساسية وهي أن أمن المعلومات والبيئة الإلكترونية تواجه العديد من التحديات الأمنية لا سيما الجريمة والإرهاب الإلكتروني اللذان يشكلا تهديدًا حقيقيًّا لنظم وأمن المعلومات، فبعيدًا عن البحث المعقد للأسباب التي تدعم هذه الفرضية، يمكن أن نسندها إلى التأكيدات التالية:

- أن التهديدات الإرهابية لا تزال قائمة، ولا تزال تهدد المجتمع الدولي.
- البني التحتية لنظم المعلومات عرضة للهجوم الإرهابي وللجريمة الإلكترونية.
- من السهولة مهاجمة الهياكل الأساسية والحيوية للدول وتعطيل الكثير من مصالحها العامة والخاصة.
- قدرة الحاسب الآلي الفائقة على تنفيذ أغراض الإرهابيين الغير مشروعة.

لذلك فمن المعقول أن تكون الأمة كلها عرضة للإرهاب الإلكتروني وللهجوم في أي وقت، فالبحث في تاريخ الجريمة الإرهابية عبر الإنترنت يبين أن هناك أسباب عديدة تدعو إلى توفير المزيد من الحماية.

من هذه النقطة، تأتي مشكلة هذه الدراسة وهي بيان أهم القضايا القانونية التي يُثيرها موضوع أمن المعلومات، وكيفية توفير الحماية القانونية اللازمة لحماية البيئة الإلكترونية من الجريمة والإرهاب على الصعيد الوطني والدولي، ويمكن أن نتناول حل تلك المشكلة عن طريق الإطار النظري للدراسة وهو كالآتي:

أولًا: البيئة الإلكترونية: حياة بلا جدار.

ثانيًا: أمن المعلومات: التهديدات والمخاطر.

ثالثًا: الآليات القانونية لحماية البيئة الإلكترونية.

***

أولًا: البيئة الإلكترونية: عالم بلا جدار

يوصف العصر الحالي بأنه العصر التكنولوجي، حيث أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات في العقود الثلاثة الأخيرة، ثورة الكترونية لا يمكن الاستغناء عنها. فبدأت بإنتاج الحاسب الآلي ومن ثم العمل على تطويره من خلال صناعة البرامج والبيانات التي انتشرت في جميع أرجاء المعمورة في وقت قصير نسبيًّا. وأخذ التقدم العلمي في الازدهار والانتشار، من خلال ربط أجهزة الحاسب الآلي المنتشرة في جميع الدول عن طريق شبكة الإنترنت، التي ساعدت على وضع العديد من الخدمات المتميزة منها على سبيل المثال البريد الإلكتروني **(E-mail)** الذي يعتبر من أكثر وسائل الإنترنت استخدامًا على المستوي العالمي، وأيضًا إنشاء شبكة النسيج العالمي **(WWW)** التي تتيح يوميًّا لملايين المستخدمين دخول المواقع الإلكترونية والصفحات باستخدام متصفحات وبوابات الإنترنت، كل ذلك وغيره الكثير، ساعد على تأسيس البيئة الإلكترونية التي تعمل بشكل مستمر لنمو وازدهار الحياة التجارية والعامة ولتخدم جميع دول العالم.

وفيما يلي سوف نتحدث عن نشأة الإنترنت وكيفية خروجه من النطاق الضيق إلى النطاق العالمي، وبعد ذلك نتناول موضوع الصفات الأساسية للبيئة الإلكترونية في الوطن العربي، وأيضًا نتحدث عن تلاقي الجريمة مع البيئة الإلكترونية، وأخيرًا نتحدث عن الإنترنت بوصفه مسرحًا للإرهابيين.

١-١ الإنترنت: من الخصوصية إلى العالمية

يعود أصل كلمة إنترنت إلى الكلمة الإنجليزية (INTERNET) وهي منقسمة إلى قسمين الأول وهو INTER ويعني البينية، والثاني NET ويعني الشبكة، وعليه فتكون الترجمة الحرفية هي الشبكة البينية[١].

وتنوعت وتعددت التعريفات الخاصة بالإنترنت، وظهرت العديد من المصطلحات الدالة عليه مثل شبكة الشبكات، الشبكة العنكبوتية، وشبكة الويب.

بدأ الإنترنت في أواخر السيتينات عندما شكلت وزارة الدفاع الأمريكية لجنة من الخبراء، أوكلت إليهم مهمة إنشاء شبكة تربط بين الحاسبات، وسميت اللجنة باسم "وكالة مشروع الأبحاث المتقدمة" عام ١٩٥٧م، ونجحت اللجنة في مهمتها، وبذلك أنشئت أول شبكة للإنترنت في الولايات المتحدة الأمريكية تحت اسم "ARBANET"، وهي اختصار لعبارة (شبكة وكالة مشروع الأبحاث المتقدمة)[٢]، وكان الغرض من هذه الشبكة هو خدمة الاستخبارات العسكرية. وبدأت الشبكة تخرج من الخصوصية إلى العالمية تدريجيًّا. ففي عام ١٩٨٣م انقسمت الشبكة إلى شبكتين، كانت الأولى هي "ARBANET" فاحتفظت باسمها وبغرضها الأساسي، أما الثانية في "MILNET" وهذه الشبكة خصصت للاستخدامات المدنية. وفي عام ١٩٨٦م تمكن الأمريكيون من ربط شبكات خمس مراكز عملاقة بشبكة واحدة سميت "NSFNET" والتي أصبحت فيما بعد بمثابة العمود الفقري لنمو وازدهار الإنترنت في أمريكا ومن ثم باقي دول العالم[٣]. فانتشر الإنترنت في أرجاء المعمورة، بعد أن كان

١- الحجاج أسامة، دليلك الشخصي إلي عالم الانترنت، دار النهضة العربية، القاهرة، ١٩٩٨م، ص١٨,

٢- عبد القادر الفنتوخ، الإنترنت للمستخدم العربي، مكتبة العبيكان، الرياض، ١٤٢١هـ، ص٢١-٢٤,

٣- سمير السيد، محاضرات في شبكة المعلومات العالمية، مكتبة عين شمس، القاهرة، ١٩٩٧م، ص١٥.

يربط في البداية ثلاثة حواسيب فقط، ليصل الآن ويربط مئات الملايين في مختلف دول العالم.

١-٢ الصفات الأساسية للبيئة الإلكترونية في الوطن العربي

لم تختلف البيئة الإلكترونية العربية عن البيئات الأخرى بكثير، ولم نكن قد أخطأنا إذا ما قلنا أنها تقل الكثير والكثير عن البيئات الإلكترونية الأخرى في المستوى الأمني والتقني. فالبيئة الإلكترونية العربية لم تكن بمنأى من الجريمة والإرهاب الإلكتروني، بل يمكن القول إنها أقرب إلى أيدي الإرهابيين، فقد يأتي إليوم الذي تستضيف الدول العربية فيه دورة الألعاب الإرهابية، وسوف يشهد العالم جميع جولات الدورة دون أي تشفير. خلاصة القول في هذا المقام هو أن البيئة الإلكترونية العربية لم تصل إلى مستوى أمني مرتفع يصل بها إلى درجة عالية من الأمان، وهذه المشكلة سوف تتضاعف مع نمو فكر التطرف في الوطن العربي.

١-٣ تلاقي الجريمة مع البيئة الإلكترونية

بعد ما رأينا كيف تطورت البيئة الإلكترونية وكيف وصلت إلى مكانة عالية في الحياة العامة، فإليوم لا يستطيع الإنسان العيش بدون الحاسب الآلي، ولا أن تتراقص أصابع يداه على لوحة المفاتيح لتعزف ألحان التفوق والمستقبل والنمو والتقدم. ولكن لوحة المفاتيح لا تعزف دائمًا ألحان الحياة، فكثيرًا أيضًا ما تتسلل بعض الأصابع لتصنع ألحان موت وتدمير وخراب. فتلاقت الجريمة مع البيئة الإلكترونية عند نقطة الارتكاز وفي حيز بسيط للغاية وهي لوحة المفاتيح. ففي ظل هذه البيئة تكمن المشكلة في معرفة من الذي يقف خلف لوحة المفاتيح، فمرونة تكنولوجيا المعلومات والحاسب والإنترنت هي التي ساعدت الأصابع الخبيثة لكي تنشر العنف والخوف ولكي تخطط وتنفذ الهجمات الإرهابية. فتكنولوجيا المعلومات تكون مفيدة للجماعات الإرهابية في ناحيتين:

١. يمكن لهم أن يستخدموا أجهزة الحاسب والإنترنت بوصفها أداة مفيدة لتعزيز النشاط الإرهابي التقليدي مثل استخدام الإنترنت في التجنيد والتدريب وتبادل المعلومات بين المنظمات الإرهابية المختلفة.
٢. البنية التحتية للمعلومات يمكن أن تشكل هدفًا جذابًا للأعمال الإرهابية التي يمكن من خلالها التأثير على الرأي العام العالمي.

والحاسب الآلي هو أيضًا عاملًا جذابًا للإرهابيين لأسباب عديدة منها[٤]:

- إنه أرخص سعرًا من الأساليب الإرهابية التقليدية، فكل ما يحتاج إليه الإرهابي هو الحاسب وطريق من طرق الاتصال بالإنترنت. فالأعمال الإرهابية الإلكترونية لا تحتاج إلى أسلحة مثل البنادق والمتفجرات لتنفيذ أهدافها الإجرامية، فيمكنها أن تخلق فيروس مدمر من خلال خط الهاتف أو كابل الاتصال، أو الاتصال اللاسلكي (**wireless**).

- مرتكب الإرهاب الإلكتروني مجهول أكثر من مرتكب الإرهاب التقليدي، فمثلًا العديد من المتصفحين يستخدموا الأسماء المستعارة على شبكة الإنترنت، وهذا يجعل من الصعب تعقب هوية الإرهابيين، وأيضًا في الفضاء الإلكتروني لا توجد حواجز مادية مثل نقاط التفتيش للتنقل، أو العبور عبر الحدود.

- تنوع وتعدد الأهداف التي يمكن للإرهابيين استهدافها من خلال الحاسب.

- التعامل مع الحاسب يكون من بعد، وهي سمة جذابة للإرهابيين.

٤-Weimann.G،(2004 may) Cyber terrorism, How Real Is the Threat?
http://www.usip.org/resources/cyberterrorism-how-real-threat

- الحاسب الآلي يتطلب قدرًا أقل من التدريب البدني.

وإذا كانت تكنولوجيا المعلومات والحاسب عوامل جذابة للإرهابيين فإن الإنترنت أكثر مرونة وأكثر جاذبية لعوامل عدة منها[٥]:

- سهولة الوصول إلى شبكة الإنترنت.
- ضآلة أو معدومة التنظيم والرقابة، وانعدام السيطرة الحكومية في أغلب الأحيان.
- الانتشار الجماهيري الكبير من جميع أنحاء العالم.
- سهولة استخدام الإنترنت، وتوفير بيئة جيدة للوسائط المتعددة، فيسهل الجمع بين النصوص والرسوم وبين الصوت والفيديو، كما يسهل تحميل الأفلام والأغاني والكتب والملفات المتعددة.
- القدرة على التأثير عن طريق التغطية الإعلامية.

وبالإضافة إلى مرونة الإنترنت والحاسب الآلي، هناك العديد من العوامل التي تعتبر بمثابة دوافع (سياسية، اقتصادية، اجتماعية، فكرية) للإرهاب الإلكتروني، أذكر منها على سبيل المثال لا الحصر:

○ الحرب والاحتلال:

تساعد الحروب على ولادة الكثير من العنف الذي يصاحبه حالة من الغضب وحب الانتقام. ففي الحروب لم تقتصر المسألة على حرب الجيوش والجنود وإنما تمتد إلى

5-Weimann .G. (2004، march) www.terror.net:How 5-modern terrorism uses the Internet.

حروب أخرى كثيرة مثل الحرب الإعلامية والنفسية وأيضًا ما يسمى بالحرب الإلكترونية، فمثلًا الاحتلال الإسرائيلي لفلسطين العربية ساعد على ولادة الكثير من عمليات الإرهاب الإلكتروني[٦]، ففي أكتوبر ٢٠٠٠ شهدت مواقع القيادات الفلسطينية لحزب الله وحماس هجمات من قبل مراهقين إسرائيليين.

وأيضًا الصراع بين باكستان والهند أدى إلى العديد من الهجمات الإلكترونية على مواقع حيوية، فنمت هذه الهجمات سنويًا بمعدل: ٤٥ في عام ١٩٩٩م، ١٣٣ في عام ٢٠٠٠، ٢٧٥ في عام ٢٠٠١[٧].

وأيضًا في سنة ١٩٩٩م أثناء حرب كوسوفو كانت حواسيب حلف شمال الأطلسي عرضة لطرد متفجر ولمحاولات إنكار الخدمة من طرف المعارضين لهجوم الحلف، مما أدى إلى إيقاف الشبكات عن الخدمة لعدة مرات خلال عدة أيام[٨].

○ الصراع السياسي والدبلوماسي:

يساعد أيضًا الصراع السياسي والدبلوماسي بين بلدين أو أكثر على ولادة هجمات إرهابية الكترونية، فمثلًا عندما اصطدمت طائرة أمريكية للمراقبة مع طائرة صينية مقاتلة في الهواء عام ٢٠٠١م، نشاء بين البلدين صراع سياسي. هذا الصراع رافقه حملة على الإنترنت لهجمات قراصنة الكمبيوتر، كان نتيجتها تعرض أكثر من ١٢٠٠ موقع

6- Kraft، D. (2000، October 26). Islamic groups 'attack' Israeli web sites. Retrieved November 10، 2003 ،fromhttp://www.landfield.com/isn/mail-archive/2000/Oct/0137.html

7-Vatis، M. (2002، June). Cyber attacks: Protecting America's security against digital threats. Discussion paper،ESDP-2002-04، John F. Kennedy School of Government، Harvard University.

٨– عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، أبحاث الدورة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف للعلوم الأمنية، ٢٠٠٦، ص١٠

أمريكي للتشويه ولهجمات من نوع إنكار الخدمة الموزعة، بما فيها موقع البيت الأبيض وموقع القوات الجوية الأمريكية ووزارة الطاقة[٩].

وأيضًا خلال القصف الذي تعرضت له السفارة الصينية في بلغراد، قام مهاجمون صينيون بإيداع رسائل تحمل عنوان "لن نتوقف عن الهجوم إلَّا عندما تتوقف الحرب"، وذلك عبر مواقع حكومية أمريكية.

٤-١ الإنترنت مسرح الإرهابيين

أصبح الإنترنت مسرح مفتوح لارتكاب الجريمة الإرهابية بسبب مرونة الاستخدام والوصول السهل إلى الشبكة، وضآلة التنظيم والرقابة، وغيرها الكثير من عيوب الإنترنت التي كانت في السابق مزاياه. وفيما يلي يمكن أن نعرض طرق وصور استخدام الإرهابيين للإنترنت:

المشهد الأول: بث ثقافة الإرهاب

قد يؤدي الإرهاب في نهاية المطاف إلى موت مرتكبي الجريمة أو نبذهم أو ملاحقتهم دوليًّا، لذلك وكما يقول الدكتور على العسيري إنه لا يقدم على الجريمة الإرهابية "إلا من ترسخ لديه مبادئ ومواقف متطرفة لا تؤمن بالحلول الوسط أو المرحلية وترفض الآخرين بل تلغي وجودهم معنويًّا ومن ثم حسيًّا، وهذا ما يحوج الإرهابيين إلى منابر لبث فكرهم وتوفير أكبر عدد ممكن من المستعدين لتبنيه"[١٠].

9- McWethy، J. & Starr، B. (2001، April 26). Hacker alert: Pentagon braces for Chinese computer attacks. Retrieved November 2، 2003 ، from،http://abcnews.go.com/sections/world/DailyNews/chinahackers_010426.html.

١٠- د.علي بن عبد الله العسيري، الإرهاب والانترنت، بحث منشور ضمن كتاب الإرهاب والقرصنة البحرية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٨، ص ٢٢٣,

ويتم بث ثقافة الإرهاب عبر الإنترنت عن طريق تأسيس مواقع تمثل المنظمات الإرهابية، وهو يكون بمثابة موقع افتراضي للمنظمة، وهذه المواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، فيتم نشر المقالات والبيانات التي تحتوي على تهديدات ووعيد بتنفيذ عمليات إرهابية، أو تعلن عن تحملها مسئولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة عن منظمات أو جهات دولية أخرى.

المشهد الثاني: التجنيد والتدريب

من خلال الإنترنت يمكن للجماعات الإرهابية أن تجند عناصر إرهابية تساعدهم على تنفيذ أعمالهم الإجرامية، وهم في ذلك يعتمدون على فئة الشباب، خصوصًا ضعاف العقل والفكر. فتعلن الجماعات الإرهابية عبر مواقعها على الإنترنت عن حاجتها إلى عناصر انتحارية، كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني. فدائمًا ما تصف الأهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوى الشباب إلى الجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة.

وأيضًا تقوم الجماعات الإرهابية بتدريب عناصرها عن طريق الإنترنت، من خلال نشر فيديو وصور تساعد على كيفية صناعة القنابل وكيفية التخطيط للهدف والهجوم عليه. ففي حادث الأزهر بمصر (٧ ابريل ٢٠٠٥)، والذي نفذه حسن بشندي طالب بكلية الهندسة[١١]، أثبتت التحقيقات الأولية أن منفذ العملية حصل على معلومات عبر شبكة الإنترنت، ساعدته على تصنيع قنبلة بدائية الصنع استخدمها في الحادث.

المشهد الثالث: استخدام الإنترنت في إعداد وتنفيذ الهجمات الإرهابية

١١- د. سهير عثمان عبد الحليم، الإرهاب والإنترنت، أبحاث المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، ٢٠٠٨، ص١.

يستخدم الإرهابيين الإنترنت في إعداد وتنفيذ الهجمات الإرهابية، فإعداد وتخطيط الهجمات الإرهابية يتم من خلال جمع المعلومات المطلوبة حول الهدف. فيمكن للإرهابيين الحصول وبكل سهولة على مواعيد إقلاع ووصول الطائرات والشاحنات والقطارات، كما يمكن لهم الحصول على خرائط وصور ملتقطة من الفضاء عبر الأقمار الصناعية للهدف المطلوب.

أما تنفيذ الهجمات الإرهابية فهي نوعان: هجمات إرهابية تستهدف الواقع المادي وتعزز الإرهاب التقليدي مثل الدخول إلى شبكة الطيران وتغير مواعيد إقلاع وهبوط الطائرات مما يؤدي إلى تصادمهم. أما النوع الثاني فهي هجمات إرهابية تستهدف شبكة الإنترنت ذاتها وهي متعددة ومتنوعة مثل هجوم المعلومات، وتدمير البنية التحتية للمعلومات، وغيرها الكثير من الجرائم التي سوف نتناولها فيما بعد.

***

ثانيًا: أمن المعلومات: التهديدات والمخاطر

هناك الآن الملايين من أجهزة الحاسب الآلي تسكن الأرض في هذا العصر، وملايين الأميال من الأسلاك الضوئية والألياف التي تلتف حول العالم لكي تصله ببعض في أقل من الثانية. فمجتمعنا هو حقًّا مجتمع المعلومات، وعصرنا هو عصر المعلومات. فالنقلة النوعية في حياة البشر جلبت العديد من المشكلات الأخلاقية والقانونية التي ترتبط بالعديد من الحقوق والحريات. فهناك العديد من التحديدات الفريدة التي نواجهها إليوم في عصر المعلومات، وهي تنبع من طبيعة المعلومات ذاتها. فالمعلومات هي الوسيلة التي من خلالها تتوسع العقول وتزيد من قدرتها على تحقيق أهدافها، فالمعلومات تشكل رأس المال الفكري للبشر ومصدر حياتهم[١٢].

فالتكنولوجيا الحديثة أثرت تصاعديًّا في مختلف مجالات الحياة الاجتماعية والاقتصادية والسياسية والأمنية. وانتشرت الجرائم والإنتهاكات في جميع دول العالم، حتى أصبح أمن المعلومات من أولويات الدول المتقدمة والنامية والمجتمع الدولي بأكمله. وهناك العديد من أسباب الضعف في النظام الأمني للمعلومات، أذكر منها:

- عدم وجود سياسة موحدة في مجال أمن المعلومات.
- القصور التشريعي في القوانين الخاصة التي تنظم أمن المعلومات، لا سيما في الدول العربية.
- عدم وجود رقابة كافية على المعلومات من جانب السلطة والمجتمع.

12 - Richard O. Mason،Management Information Systems Quarterly ، Volume 10، Number 1، March، 1986pp. 5-12

- تدني المستوى الأمني للأشخاص الطبيعيين والاعتباريين في مجال المعلومات.
- الحصول على المعلومات الشخصية من قبل المخابرات وأجهزة الدولة.

كما أن موضوع أمن المعلومات تحيط به العديد من التهديدات التي تهدد أمنه واستقراره منها:

- الوصول غير المشروع للمعلومات الشخصية.
- تسرب المعلومات واختراق الخصوصية.
- تدمير أو إتلاف أو سرقة أجهزة الحاسب الآلي.
- اعتراض المعلومات في شبكات البيانات وخطوط الاتصالات.
- التعدي على القيود القانونية المفروضة على توزيع البيانات.

قضايا قانونية

يثير موضوع أمن المعلومات العديد من القضايا القانونية الهامة والتي تؤثر على الحياة العامة والخاصة. فأمن المعلومات يؤثر على حقوق الملكية الفكرية، والسرية والخصوصية، وحماية البيانات، والحق في حرمة الحياة الخاصة. كما أن أمن المعلومات والتكنولوجيا الحديثة قد استحدثت العديد من الجرائم مثل الجريمة المعلوماتية، والإرهاب الإلكتروني، والاحتيال المالي، والسرقة، والقرصنة، والفيروسات، والعديد من الجرائم الأخرى التي ترتكب داخل البيئة الإلكترونية. ولعل تناول موضوع التدابير القانونية لبعض القضايا المرتبطة بالبيئة الإلكترونية موضوع في غاية الأهمية. ونظرًا لحدود حجم هذه الورقة، سوف نقتصر الحديث على تناول ثلاث قضايا رئيسية لأمن المعلومات وهم الخصوصية والجريمة المعلوماتية والإرهاب الإلكتروني.

١-٢ الخصوصية المعلوماتية

تعتبر الخصوصية حق أساسي من حقوق الإنسان وحجر الزاوية في المجتمعات الديمقراطية. فهي تكمن في أساس سيادة القانون وحرمة انتهاك الحياة الخاصة. ومع تطور التكنولوجيا الجديدة للمعلومات والاتصالات أصبحت الخصوصية من أكثر حقوق الإنسان انتهاكًا في البيئة المعلوماتية.

١-١-٢ تعريف الخصوصية

تعتبر الخصوصية من أكثر التعريفات صعوبة في التحديد[١٣] فهي تختلف باختلاف السياق والغرض، وتختلف من دولة إلى أخرى. فالخصوصية قد تنصهر مع مفهوم حماية البيانات، وقد تدخل تحت نطاق حرمة الحياة الخاصة، وقد ترى دولة بأنها وسيلة لرسم الخط الذي يمكن للمجتمع أن يتعداه ويتدخل في شؤون الأفراد[١٤]. ولكن عدم وجود تعريف واحد لا يعني أن قضية الخصوصية تفتقر إلى الأهمية، فجميع حقوق الإنسان هي جوانب من الحق في الخصوصية[١٥]. وهي أيضًا تعتبر الحق الطبيعي الذي يوفر الأساس للحصول على حق قانوني محمي بموجب الدستور. والحق القانوني في الخصوصية محمي دستوريًّا في معظم المجتمعات الديمقراطية. وأعرب عن هذا الحق الدستوري في مجموعة متنوعة من الأشكال التشريعية الغربية والعربية.

13 - James Michael، Privacy and Human Rights 1 (UNESCO 1994).
14 - Simon Davies، Big Brother: Britain's Web of Surveillance and the New Technological Order 23 (Pan 1996).
15 - Volio، Fernando، "Legal personality، privacy and the family" in Henkin (ed)، The International Bill of Rights (Columbia University Press 1981).

وهناك من اعتبر الخصوصية مزيج من ثلاثة مفاهيم وهم: القيود في الوصول إلى عالم الشخصية، والسيطرة على المعلومات الشخصية، والتحرر من مراقبة الآخرين[١٦].

ومفهوم الخصوصية يشتمل على العديد من المفاهيم المتنوعة والمتداخلة معًا في الوقت ذاته وهي[١٧]:

- خصوصية المعلومات، وهي التي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقة الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي في العادة كل ما يتصل بحماية البيانات.
- الخصوصية الجسدية أو المادية، وهي التي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوصات الجينات، وفحص المخدرات، والتجارب الطبية.
- خصوصية الاتصالات، وهي التي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الإلكتروني وغيرها من الاتصالات.
- الخصوصية الإقليمية، وهي تختص بالإقليم المكاني وهي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية والتوثق من بطاقات الهوية.

16 - Privacy and the computer: Why we need privacy in the information society"، L. Introna، Metaphilosophy (http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp96/abstracts/introna.html.

17 - Cedric Laurant، Privacy & Human Rights، Electronic Privacy Information Center، USA، 2003.

والخصوصية هي حق مهم وشرط ضروري لإقامة العديد من الحقوق الأخرى مثل الحرية والاستقلال الشخصي. فهناك علاقة بينها وبين الحرية والكرامة والديمقراطية، فاحترام خصوصية الشخص هو اعتراف بحق هذا الشخص في الحرية والاعتراف بأن هذا الشخص مستقل بذاته[١٨]. ولكن هذا الحق ليس مطلق، فله العديد من الاستثناءات نذكر منها:

- حق الشرطة في التجسس على المجرمين والاستيلاء على الوثائق الشخصية[١٩].
- حق الدولة في جمع المعلومات الخاصة والشخصية عن مواطنيها بهدف الحفاظ على النظام العام[٢٠].

٢-١-٢ تهديدات الخصوصية

تتعرض الخصوصية في ظل النطاق الواسع للبيئة الإلكترونية إلى العديد من التهديدات المختلفة، ويمكننا تقسيم تلك التهديدات وفقًا للغرض من هذه الدراسة كالتإلى:

- تهديدات الأجهزة: مثل أجهزة التصنت، والدوائر التلفزيونية المغلقة، والكاميرات الخفية، وميكروفونات، وأجهزة الاستشعار عن بعد وغير ذلك الكثير.

18 - J. J. BRITZ، TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession، http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html.

19 - McGarry، K. (1993). The Changing Context of Information. An Introductory Analysis. 2nd ed. London: Library Association Publishing.

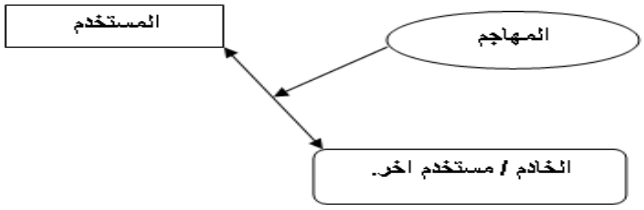
20 - Ware، W.H. (1993). The new faces of privacy. The Information Society، 9 (3): 195-211.

- تهديدات البرمجيات: منها البرامج الخبيثة مثل الفيروسات وأحصنة طروادة وبرامج التجسس وغيرها من البرامج التي يمكنها أن تكشف عن البيانات الشخصية والحساسة.
- تهديدات المحتويات الرقمية: يدخل ضمن هذا النوع التهديدين السابقين، بالإضافة إلى استخراج البيانات، وتحليل البيانات، والتسريبات الغير قانونية لقواعد البيانات.

ولعل تهديدات المحتويات الرقمية للخصوصية هو موضوع دراستنا، وهذا النوع من التهديدات يعتبر من أكثر أنواع التهديدات انتشارًا. فالجميع يستخدموا المحتويات الرقمية والبرمجيات وشبكة الإنترنت، من خلال التصفح وإرسال البريد الإلكتروني والمشاركة في المحادثات والمنتديات، دون أن يدركوا مدى السهولة التي يمكن لطرف ثالث الحصول على البيانات والمعلومات الخاصة بهم. ويمكننا أن نقسم التعدي على الخصوصية عبر المحتويات الرقمية إلى ثلاث أقسام وهما كالتإلى[٢١]:

✓ الإلتقاط:

جميع البيانات الشخصية تمر عبر خطوط مختلفة في طريقها إلى الخادم (**Web Server**). فأولًا تنتقل البيانات عبر خطوط التليفون ومن ثم إلى خطوط خدمة الإنترنت، وفي النهاية تصل إلى الخادم. وخلال طريقها إلى الخادم يمكن للعديد من الأشخاص الحصول عليها في الوقت الذي يجري فيه نقلها (انظر الشكل التإلى).



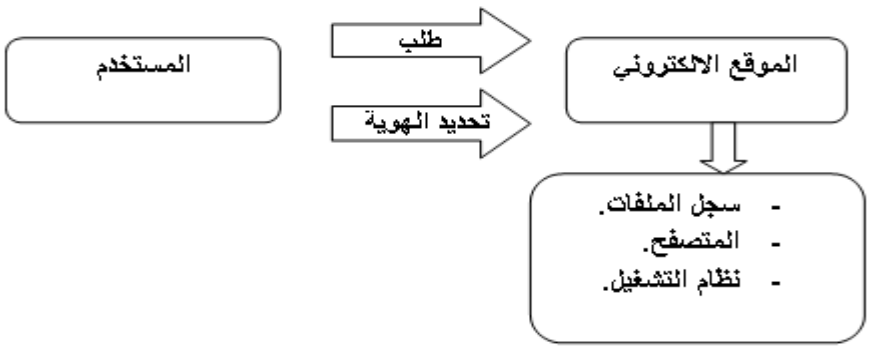
21 - S. Wehner، Privacy and Anonymity on the Net، http://www.r4k.net/cyfem/.

✓ البريد الإلكتروني:

يسافر البريد الإلكتروني حول الإنترنت في وضوح تام، تمامًا كبطاقة بريدية دون مغلف. ويمكن الحصول على البريد الإلكتروني من أي شخص عن طريق الخادم الخاص به أو الخادم الخاص بالطرف المتلقي، كما يمكن التقاطه في الوقت الذي يجري نقله.

✓ المواقع الإلكترونية:

تميل المواقع الإلكترونية على وجه الخصوص إلى خلق المزيد من الأخطار على الخصوصية. وهذا لأن المتصفح ينقل عادة الكثير من المعلومات الشخصية عبر المواقع الإلكترونية.



ومع توفر لغات البرمجة وأدواتها وبصورة مجانية أدى بدوره إلى خلق سلوك ضار إلى حد جعل الخصوصية فريسة سهلة المنال للأفراد العاديين لأداء الأنشطة غير المشروعة على نطاق واسع. فقضايا الخصوصية أصبحت الآن أكثر خطورة من مجرد اختصارها في أعمال المراقبة الحكومية على البيانات بل أصبح من الممكن الحصول على البيانات الشخصية الحساسة، والصور المخزنة على الأقراص الخاصة، وتفاصيل البطاقات الائتمانية، وكلمات السر، من قبل أشخاص عاديين.

٣-١-٢ حماية الخصوصية

١-٣-١-٢ التشريعات

يمكننا تناول التشريعات من خلال تناول التوجيهات الدولية والقوانين الوطنية، وهذا على النحو التإلى:

- **التوجيهات الدولية:**

نص الإعلان العالمي لحقوق الإنسان على الحق في الخصوصية بوجه عام فقد كفل حماية الأماكن والاتصالات. والعهد الدولي للحقوق المدنية والسياسية واتفاقية الأمم المتحدة للعمال المهجرين واتفاقية الأمم المتحدة لحماية الطفولة قد نص صراحة على الحق في الخصوصية. وأيضًا على المستوى الإقليمي هناك العديد من الاتفاقيات التي اعترفت بالحق في الخصوصية نذكر منها، الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، والاتفاقية الأمريكية لحقوق الإنسان، والإتفاقية الأفريقية لحقوق الإنسان، والميثاق العربي، وغيرها العديد من الاتفاقيات الإقليمية التي نصت صراحة على الحق في الخصوصية بوجه عام.

أما عن التوجيهات الدولية بشأن حماية الخصوصية في مجال تكنولوجيا المعلومات، فقد ظهرت أول اتفاقية دولية لحماية الخصوصية المعلوماتية في عام ١٩٨١ عندما وضع الإتحاد الأوروبي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية وهي تعتبر بمثابة أول صك دولي ملزم قانونًا لحماية البيانات. وبعد ذلك أصدرت منظمة التعاون الاقتصادي والتنمية دليلًا إرشاديًا لحماية الخصوصية ونقل البيانات الخاصة، والذي بموجبه قرر مجموعة من القواعد التي تحكم عمليات المعالجة الإلكترونية للبيانات. وفي عام ١٩٨٩ تبنت الأمم المتحدة دليلاً يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية[٢٢]، وأطلقت مجموعة دول الثمانية مجموعة من التوصيات لحماية الخصوصية في عام ١٩٩٥. ومن خلال عرض التوجيهات الدولية الخاصة بالخصوصية يتضح لنا عدم وجود اتفاقية دولية لحماية الخصوصية المعلوماتية. كما أن هناك عجز تشريعي دولي في وضع إطار عام لحماية البيانات الشخصية عبر الإنترنت. كما أن المبادئ التوجيهية لمنظمة التعاون والتنمية تعتبر بمثابة مبادئ إرشادية للدول وغير ملزمة قانونيًا.

- **التشريعات الوطنية:**

مع تعارض الخصوصية بتقنية المعلومات وبسبب المخاطر المتزايدة للخصوصية الشخصية، تطورت التشريعات الوطنية لكي تواكب الجرائم المستحدثة المتصلة بالخصوصية. ففي عام ١٩٧٠ ظهرت أول معالجة تشريعية في ميدان حماية البيانات والخصوصية في مقاطعة هيس بألمانيا، ثم اتسعت دائرة سَن التشريعات الخاصة بالخصوصية المعلوماتية فمن قانون هيس إلى قانون وطني متكامل في السويد عام ١٩٧٣، إلى الولايات المتحدة عام ١٩٧٤، ثم إلى ألمانيا على المستوى الفيدرإلى عام ١٩٧٧، ثم

22 - United Nations، GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES. Adopted by the General Assembly on 14 December 1990.

فرنسا عام ١٩٧٨. وبذلك أخذت الدائرة في الاتساع شيئًا فشيء إلى أن أصبحت حماية البيانات مطلبًا أساسيًا من مطالب حقوق الإنسان. وأصبحت كلًا من النمسا، بلجيكا، التشيك، الدنمارك، فنلندا، فرنسا، ألمانيا، المجر، أيسلندا، أيرلندا، إيطاليا، لوكسمبورج، هولندا، النرويج، البرتغال، أسبانيا، السويد، المملكة المتحدة، لديهم قوانين عامة لحماية الخصوصية والبيانات(٢٣).

وبالنسبة للدول العربية، فإنه لا يوجد دستور عربي ينص على حماية الخصوصية المعلوماتية، فجميع الدساتير العربية نصت على الحق في حرمة المسكن والمراسلات بصفة عامة، وبعض الدول نصت على حرمة الحياة الخاصة. أما بالنسبة للقوانين الوطنية العربية الخاصة بالخصوصية وحماية البيانات فقد جاءت متأخرة فأول تشريع عربي لحماية البيانات كان في سنة ٢٠٠٧ في دولة الإمارات، وبعد ذلك أخذت بعض الدول العربية تصدر مشاريع قانونية خاصة بحماية البيانات والخصوصية مثل مشروع قانون حماية البيانات والخصوصية ومكافحة الجريمة الإلكترونية بمصر في سنة ٢٠٠٨.

٢-٣-١-٢ الحلول التقنية:

هناك العديد من التقنيات الخاصة بحماية الخصوصية التي من شأنها أن تخفف من المخاطر التي تتعرض لها خصوصية البيانات، ونذكر منها:

- التشفير: يمكن لتقنيات التشفير حماية البيانات من الوصول إليها بطريقة غير مشروعة، فنقل البيانات بطريقة مشفرة له أهمية خاصة خصوصًا عند إرسال المعلومات الحساسة، مثل أرقام بطاقات الائتمان والمعلومات المالية عبر الإنترنت. ويمكن للمستخدم تحديد ما إذا كان موقع الإنترنت آمن بطريقتين: الأولي: أن مواقع الويب تشير إلى أن التحويلات مشفرة، والثانية: وجود رمز

23 - Flaherty، Protecting Privacy، and A.C.M Nugter، Transborder Flow of Personal Date Within the EC، Kluwer Law and Taxation Publishers، 1990.

التشفير وغالبًا ما يكون رمز القفل الصغير في أسفل الزاوية إليسرى أو إليمنى من الصفحة. وهناك أيضًا العديد من برامج التشفير المتاحة مجانًا على العديد من مواقع الإنترنت[٢٤].

- استخدام برامج حماية: تعتبر برامج الحماية فعالة في حماية الخصوصية كما إنها لا تكلف الكثير من المال والجهد كما أن هناك العديد من البرامج متاحة مجانًا للمستخدمين.

- استخدام عناوين بريد الكتروني يمكن التخلص منها: وهذا الحل يعتبر من أسهل الحلول لمشكلة خصوصية البريد الإلكتروني، فالكثير من المنتديات والمواقع تتطلب التسجيل لكي تستطيع التصفح عليه، وعند التسجيل ببريدك الإلكتروني الأساسي فيكون احتمال سرقته وانتهاك الخصوصية كبير، لذلك يمكن استخدم عناوين البريد الإلكتروني التي يمكن التخلص منها بسهولة.

٢-٢ الجريمة والإرهاب الإلكتروني

رأينا فيما سبق كيف تكونت البيئة الإلكترونية وتفاقمت أهميتها على المستوى الوطني والدولي، وكيف تلاقت الجريمة مع البيئة الإلكترونية لتصنع نوع من الجرائم المستحدثة التي يصعب مواجهتها على النطاق الضيق. وفيما يلي نتكلم عن الجريمة والإرهاب الإلكتروني من حيث التعريف والعلاقة.

١-٢-٢ تعريف الجريمة الإلكترونية

24 - Whitten and D. Tygar، "Why Johnny can't encrypt: A usability evaluation of PGP 5.0"، In Proceedings of the 8th USENIX Security Symposium، Washington، DC، 1999، p. 169-184.

هناك العديد من التعريفات المختلفة للجريمة الإلكترونية، ويمكن أن نتناولها بحسب التصنيف التإلى[٢٥]:

- تعريفات متمركزة حول وسيلة ارتكاب الجريمة:

ومن هذه التعريفات، تعريف الفقيه الألماني (**Tiedemann**) ويعرفها بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب"[٢٦]. ويعرفها أيضًا ضمن هذا التصنيف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًّا"[٢٧]. وقريب من ذلك التعريف، تعريف (**Ball**) للجريمة المرتبطة بالحاسب الآلي بأنها "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية". وهذا التصنيف لتعريف الجريمة الإلكترونية والذي يعتمد على الوسيلة المستخدمة في ارتكاب الجريمة ينتقده البعض وبشدة لأن الوسائل وحدها لا تكشف عن الجريمة وإنما يجب العمل على كشف المكون الأساسي للجريمة للوصول إلى تحديد هويتها ونطاقها.

- تعريفات متمركزة حول موضوع الجريمة:

هذا التصنيف يرتكز على بيان موضوع الجريمة وبموجبه تكون الجريمة إلكترونية عندما تقع على الحاسب أو داخل نظامه. ومن هذه التعريفات، تعريف (**Rosenblatt**) والذي يعرفها بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".

٢٥- تصنيف الأستاذ الدكتور/ هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، دار النهضة العربية، ٢٠٠٨، ص٢٩.

٢٦- د. هشام رستم، قانون العقوبات، مرجع سابق، ص ٢٩.

27 - Addressing the New Hazards of the High Technology Workplace، Harvard Law Review، Vol. 104، No. 8، Juin 1991، Notes، p، 1898.

- تعريفات مرتبطة بتوافر المعرفة بتقنية المعلومات:

ومنها، تعريف (David Thompson) للجريمة الإلكترونية بأنها "أية جريمة يكون متطلبًا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب الآلي". وأيضًا تعريف (Stein Schjolberg) بأنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[٢٨].

٢-٢-٢ تعريف الإرهاب الإلكتروني

قبل أن نتمكن من عرض ومناقشة تعريف الإرهاب الإلكتروني يجب علينا في البداية أن نشير إلى أن لفظ الإرهاب الإلكتروني يتكون من عنصرين أساسيين هما: البيئة الإلكترونية والإرهاب.

فالبيئة الإلكترونية سبق أن تكلمنا عنها في بداية البحث، ووضحنا أنها تحتوي على كل ما يتصل بتكنولوجيا المعلومات من أدوات وخدمات. أما كلمة الإرهاب "Terrorism" فهي تأتي من الكلمة اللاتينية "Terrere" وتعني الخوف. وبعيدًا عن الخوض في تعريف كلمة الإرهاب التي لم يتفق على تعريف دولي لها حتى الآن. فيمكننا أن نقول وبعبارات عامة جدًّا أن الإرهاب الإلكتروني مثله مثل أي فعل إجرامي (أو التهديد به) ما دام إنه ارتكب من أجل إثارة الخوف، فهو نفسه الإرهاب المادي إلا إنه يستخدم الحاسب كمصدر للهجمات.

وعلى الصعيد الدولي هناك فهم مشترك لهذا المفهوم تم التوصل إليه، خصوصًا أنه لا يوجد تعريف موحد للإرهاب على المستوى الدولي أو الإقليمي بل على المستوى الوطني. فداخل الدولة الواحدة تختلف التعاريف والمفاهيم الخاصة بالإرهاب. وإذا ركزنا على

٢٨- د. هشام رستم، مرجع سابق، ص ٣١.

المفهوم القانوني الذي نجّرم به الفعل المرتكب في الجرائم الإرهابية لوجدنا أن الفكرة الأساسية للتجريم تكمن في الخوف المترتب على استخدام العنف، ومن المتفق عليه عمومًا أن الإرهاب يسعى دائمًا إلى نشر الخوف والفزع داخل المجتمع، ولكن الأمر يكون أكثر تعقيدًا عندما نحاول الجمع بين الإرهاب والبيئة الإلكترونية.

فالإرهاب الإلكتروني يدور حول الاستخدام المتعمد والضار لتكنولوجيا المعلومات، مما يرتب على ذلك آثار ضارة ومدمرة تختلف من مجتمع إلى آخر، لذلك وصف بأنه إرهاب مناسب أو ملائم[٢٩] بسبب عدم إمكانية خلق خوف من الأذى البدني أو الوفاة، وكما يقول (جوشوا غرين) إن "هناك طرق عديدة يمكن للإرهابي أن يقتلك، الحواسيب ليست واحدة منهم"[٣٠].

ومن المهم أن نلاحظ أنه كما لا يوجد تعريف واحد لمصطلح الإرهاب حظي بقبول عالمي، فإنه لا يوجد تعريف واحد لمصطلح الإرهاب الإلكتروني تم قبوله عالميًّا. فهناك العديد من المفاهيم التي يمكن أن نتناولها بشيء من الإيضاح للوصول إلى تعريف عملي وعلمي للإرهاب الإلكتروني.

يعرف (دورثي دايينج) الإرهاب الإلكتروني بأنه "التقاء للإرهاب مع الفضاء التخيلي، وهو يعني التهديدات غير القانونية ضد الحاسبات والشبكات والمعلومات المخزنة، وذلك لإخافة أو إجبار الحكومات أو الناس لتعزيز أهداف سياسية أو اجتماعية، وهو العنف ضد الأفراد أو الممتلكات أو إنه مؤذٍ لدرجة كافية لخلق الخوف، والتعديات المفضية للموت أو الإصابة أو الانفجاريات أو الخسارة الاقتصادية وهذه ما

٢٩ - Cyber Terrorism- the Dark Side of the Web World - http://www.articlesbase.com/law-articles/cyber-terrorism-the-dark-side-of-the-web-world-331261.html.
30 - Joshua Green، the myth of cyberterrorism ، http://www.washingtonmonthly.com/features/2001/0211.green.html

هي إلا أمثلة للتعديات على الإرهاب التخيلي. ويمكن تصنيف الجمهور المستهدف في ثلاثة فئات هي: الأفراد والممتلكات والحكومات[٣١].

أما (كولنز) فيعرفه بأنه "سوء الاستخدام المتعمد لنظام المعلومات الرقمي والشبكات أو المكونات، تجاه هدف يدعم أو يسهل حملة إرهابية أو فعل إرهابي"[٣٢].

وهناك تعريف للإرهاب الإلكتروني يعتبر من أقرب التعريفات، وهو للأمريكي (**mark pollitt**) من مكتب التحقيقات الفيدرإلى، الذي عرف من خلاله الإرهاب الإلكتروني على النحو التإلى "هجوم ذات دوافع سياسية مسبق ضد المعلومات، ونظم الحاسب، وبرامج الحاسب، والبيانات، والذي نتج عنه عنف ضد أهداف غير محاربة، من قبل مجموعات فرعية أو عملاء سريون"[٣٣].

وتعرف المادة ١,٢ من اقتراح وضع اتفاقية دولية بشأن الجريمة والإرهاب الإلكتروني، الذي أعدها مركز الأمن والتعاون الدولي بأنه "الاستخدام المتعمد أو التهديد باستخدام العنف دون سلطة معترف بها قانونيًّا، أو أي تدخل ضد تكنولوجيا المعلومات، عندما يكون من المحتمل أن مثل هذا الاستخدام من شأنه أن يسفر عن وفاة أو إصابة شخص أو أشخاص، أو يلحق الضرر بالممتلكات المادية، أو يؤدي إلى ضرر اقتصادي كبير".

31– راجع في التعريف كلا من:(د. ذياب موسي البداينة، الإرهاب المعلوماتي، أبحاث الحلقة العلمية حول "الإنترنت والإرهاب"، كلية التدريب جامعة نايف للعلوم الأمنية بالتعاون مع جامعة عين شمس، ٢٠٠٨م، ص١٣.

-Denning، Dorothy E..Activism، Hacktivism، and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.، http://www.nautilus.org/info-policy /workshop/papers/denning.html.، February ،٤ 2000

-Stark، Rod. "Cyber Terrorism: Rethinking New Technology،" Department of Defense and Strategic Studies، 1999.)

32 - White، Col. Kenneth C.١٩٩٨ Cyber-Terrorism: Modem Mayhem." Carlisle Barracks، Pennsylvania: U.S. Army War College.

33 - Mark M.pollitt، " cyberterrorism: fact or fancy?" proceedings of the 20th National Information Systems Security Conference، October 1997، pp. 285-289.

وهناك تعريف آخر يعرف الإرهاب الإلكتروني بأنه "استخدام لتكنولوجيا المعلومات لتنظيم وتنفيذ الهجمات ضد الشبكات والنظم الحاسوبية والهياكل الأساسية للاتصالات السلكية واللاسلكية، أو لتبادل المعلومات إلكترونيًّا، أو توجيه تهديدات."[٣٤].

ويعرفه (كوليجيوم سيفيتاس) بأنه "العمل الإجرامي الذي ارتكب من خلال أجهزة الكمبيوتر مما يؤدي إلى العنف والموت و / أو الدمار، وخلق الرعب لغرض إجبار الحكومة على تغيير سياساتها"[٣٥].

وبعد العرض السريع للتعريفات المختلفة للإرهاب الإلكتروني، يمكن أن نعرفه بأنه "الاستخدام المتعمد لنظم المعلومات، لأغراض تخريبية، أو التهديد باستخدامها، مع تواجد نِيَّة القيام بهذا الفعل، وذلك لتحقيق هدف سياسي أو اجتماعي أو ديني".

فالإرهاب الإلكتروني يتكون من عناصر أساسية وهي أداة وهدف وغرض: فأداة الجريمة الحاسب والإنترنت، والهدف البيئة الإلكترونية ونظم المعلومات، والغرض هو تحقيق هدف سياسي أو اجتماعي أو ديني.

٣-٢-٢ العلاقة بين الجريمة الإلكترونية والإرهاب الإلكتروني

العلاقة المشتركة بين الجريمة الإلكترونية والإرهاب الإلكتروني تتمحور في نقطتين: الأولى أن كل منهما جرائم، والثانية: أن محل الجريمة في كلاهما واحد وهو البيئة الإلكترونية. ويمكن أن نفهم العلاقة بينهم من خلال تحديد نطاق الإرهاب

34 - Cyberterrorism، available at http://www.ncsl.org/programs/lis/cip/cyberterrorism.htm accessed on 15th May 2008.

35 - Collegium Civitas" Foreign Policy of the United States of America how to prevent and fight international and domestic CYBERTERRORISM AND CYBERHOOLIGANISM prepared by Lukasz Jachowicz Warsaw"، January 2003، honey.7thguard.net/essays/cyberterrorism-policy.pdf

الإلكتروني الذي يمكن أن نعتبره فكرة مستقلة عن الجريمة الإلكترونية، فكلاهما يدخلا ضمن الأعمال الإجرامية المعاقب عليها بالقانون كما سبق أن أوضحنا، ومع ذلك هناك حاجة ملحة للتفريق بينهم لتحديد نطاق التجريم. فالجرائم الإلكترونية قد تكون ضد فرد أو منظمة أو دولة، أما الإرهاب الإلكتروني فهو ضد المجتمع الدولي بأكمله، فعندما يقع الهجوم على دولة معينة فيعتبر هجوم ضد المجتمع الدولي برمته، فتتحرك جميع الدول من أجل ملاحقة المجرمين. فكما يقول (**Ashish Pandey**) وهو باحث في قانون الإنترنت في الهند "بأن جميع الأعمال الإرهابية الإلكترونية هي جرائم إلكترونية، ولكن ليست جميع الجرائم الإلكترونية تدخل ضمن الأعمال الإرهابية"، فالإرهاب الإلكتروني مفهوم يشمل على الجريمة الإلكترونية[٣٦].

وكما سبق أن ذكرنا أن الإرهاب الإلكتروني هو استخدام العنف وممارسة الأنشطة التخريبية أو التهديد باستخدامها في مجال البيئة الإلكترونية، من أجل تعزيز أهداف اجتماعية وأيديولوجية وسياسية. فالإرهاب الإلكتروني يتضمن أنشطة تخريبية تؤدي إلى التدمير أو التخويف على المستوى الدولي، فهو قضية تتعدى الحدود الوطنية والإقليمية، وهذا يرجع إلى طبيعة شبكة الإنترنت التي لا تعترف بالحدود الإقليمية والحدود الجغرافية[٣٧] وهذا بعكس الجرائم الإلكترونية التي قد تشكل مضايقة للأفراد عن طريق رسائل البريد الإلكتروني، أو التشهير بهم، أو قرصنتهم، أو التحايل والنصب عليهم، أو إيقاعهم في الغش والاحتيال. فكما يقول (دينيغ) "لا يقع الإرهاب الإلكتروني إلا إذا تحقق شرط واحد وهو الهجوم الذي يسبب الضرر الكبير ويمكن في

36 - Ashish Pandey، Cyber Crimes – Detection and Prevention، p 5.4

37 - Nagpal، Rohas. Defining Cyber Terrorism. 2004. Asian School of Cyber Laws. 04 June 2006. <http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm>

نهاية المطاف أن يؤدي إلى تصاعد الخوف والموت والدمار ودون هذه العوامل لا يمكن أن يعتبر الهجوم إرهابًا إلكترونيًّا)[٣٨].

ومع تزايد الدور الذي تؤديه أجهزة الحاسب الآلي في جميع مجالات الحياة يزداد تهديد الإرهاب الإلكتروني، ويهدد المستوى الأمني الدولي. فالإرهابيون يستخدموا تكنولوجيا المعلومات لوضع الخطط وجمع الأموال ونشر الأفكار السامة، وكل هذا سوف يؤدي إلى نوع من عدم الاستقرار الإلكتروني، وزعزعة الأمن المعلوماتي، فالإرهاب الإلكتروني ما هو إلا هجمات خطيرة ضد البنى التحتية لأنظمة المعلومات.

٤-٢-٢ تصنيفات الإرهاب الإلكتروني

تتعدد تصنيفات وأنواع الإرهاب الإلكتروني، وتختلف باختلاف الأيديولوجيات المتعددة، فهناك سبل مختلفة لتصنيف الإرهاب الإلكتروني منها: تصنيف (**Collin**) عام ١٩٩٩ الذي قسم الإرهاب الإلكتروني إلى ثلاثة أنواع من الأفعال وهم: الدمار، والتعديلات، واقتناء وإعادة الإرسال. وأيضًا اتجه إلى هذا التقسيم الثلاثي (**grabosky**) في دراسة نشرت عام ١٩٩٨ حدد من خلالها ثلاثة أشكال رئيسية للأعمال الإرهابية التي تستهدف البيئة الإلكترونية وهي: تدمير الملفات، إعاقة الوصول إلى ملفات البيانات عن طريق تشفيرها، إضعاف قدرة النظام على القيام بمهامه.

وهناك تصنيف آخر للإرهاب الإلكتروني قدمها كلًا من (**zanini** & **Edwards**) عام ٢٠٠١، ووفقًا لهذا التقسيم هناك ثلاثة أنواع من الأنشطة الهجومية يمكن للإرهابيين استخدامها: أولًا، يمكن للإرهابيين أن يستخدموا تكنولوجيا

38 - Denning، Dorothy. Is cyber terror next? 1 November 2001. Social Science Research Council. 05 June 2006. < http://www.ssrc.org/sept11/essays/denning.htm>

المعلومات لغرض الدعاية، ثانيًا، استخدام شبكة الإنترنت لشن هجمات تخريبية، وأخيرًا، يمكن استخدام هذه الشبكات لأغراض تدميرية[٣٩].

ويعتبر التصنيف الذي جاء به (**Ballard**) من أفضل التصنيفات المختلفة للإرهاب الإلكتروني وصنفه إلى أربع أنواع وهي كالتإلى[٤٠]:

- هجوم المعلومات:

يركز الإرهابيون من خلال هذا النوع على تغيير أو تدمير محتوى الملفات الإلكترونية، وأنظمة الحاسب، أو أي مواد أخرى متصلة بالبيئة الإلكترونية.

- هجمات البنية التحتية:

هي الهجمات التي تستهدف تعطيل أو تدمير الأجهزة الفعلية، أو أنظمة التشغيل، أو البرمجيات، في بيئة محسوبة مما يؤدي إلى تدمير أو تعطيل البنية التحتية للمعلومات.

- تيسير التكنولوجيا:

يتم من خلالها استخدام الحاسب وأنظمة الاتصالات على التخطيط للهجمات الإرهابية، والتحريض عليها، أو تسهيل الإرهاب التقليدي.

- جمع التبرعات والترويج:

39 - راجع في التصنيفات السابقة Human and Societal Dynamics، Responses to Cyber Terrorism، IOS Press، 2008، p 73.

40 - Ballard، J.D، Tlomik،J . G ، & mekenzie D. 2000، "Technological facilitation of terrorism: Definitional، legal and policy issues " American Behavioral scientist، 45،(6)، 989- 1016.

يستخدم الإرهابيون شبكة الإنترنت لجمع التبرعات من أجل قضية سياسية معينة، أو لجلب المساعدات، أو لتعزيز أيديولوجية بديلة في التوجيه.

٥-٢-٢ سيناريوهات التهديدات الإلكترونية

تزداد التهديدات الإرهابية الإلكترونية يومًا بعد يوم، خصوصًا بعد أن أصبح الإنترنت جزء أساسي من حياتنا إليومية. فالآثار العنيفة للإرهاب الإلكتروني لم نراها ولم نسمع دوي انفجارها بعد، ولكن مؤشرات الخطر تتصاعد وترتفع إلى القمة. فالإنترنت يستخدم في جميع مجالات الحياة، في المفاعلات النووية، الكهرباء، المياه، خطوط الملاحة الجوية والبرية والبحرية، المجالات الطبية، الإغاثة، البنوك، البورصة، وغيرها الكثير. فتعطيل مثل هذه المجالات سوف يؤدي إلى نتائج مادية خطيرة. فإليوم، لا ننادي فقط بمهاجمة أسلحة الدمار الشامل، بل يجب أن نرفع أصواتنا لمحاربة أسلحة التعطيل الشامل، فتعطيل الإنترنت يؤدي إلى تعطيل شامل للعديد من مجالات الحياة الضرورية. وفيما يلي يمكن أن نتحدث عن سيناريوهات التهديدات الإلكترونية من خلال الحديث عن الهجمات الإرهابية المتوقعة التي قد تستهدف المحتوى المعلوماتي أو الأهداف العسكرية والسياسية، أو الأهداف الاقتصادية والمالية، وهذه التهديدات في غاية الخطورة، خصوصًا بعد أن ظهر الدور المهم والميزة الأساسية للتكنولوجيا وهي الكفاءة في إنجاز الهدف.

١ ٥ ٢ ٢ الهجوم على المحتوى المعلوماتي والبنية التحتية للمعلومات:

يستهدف هذا الهجوم الإنترنت ذاته بحيث يتوقف عن العمل لعدة ساعات مما يؤدي إلى آثار مادية واقتصادية وسياسية واجتماعية خطيرة بالمجتمع الدولي، بحيث يبدأ الهجوم بتسليط كم هائل من المعلومات على الخوادم التي يعمل الإنترنت من خلالها بمقدار يفوق قدرة الخادم على الاستقبال مما يؤدي إلى تعطيله. ومثال على ذلك، الهجوم

الذي استمر ساعة واحدة وسلط بيانات تفوق البيانات التي يستقبلها الخوادم بـ ٤٠ ضعفًا، مما أدى إلى تعطيل ٩ أجهزة خوادم من أصل ١٣ جهاز منتشر حول العالم. ويمكن أيضًا للإرهابيين تدمير البنية التحتية للمعلومات من خلال استهداف كابلات الاتصالات عن طريق قطعها أو إتلافها، مما يؤدي إلى توقف الاتصال بالإنترنت عدة أيام.

٢ ٢ ٥ ٢ الهجوم على الأهداف العسكرية والسياسية:

يستهدف هذا النوع من الهجوم الأهداف العسكرية (غير المدنية) والسياسية، فبالنسبة للأهداف العسكرية فهذا النوع نادر الحدوث عادة لعدة أسباب أهمها أن الدولة تفصل بين معلوماتها العسكرية والواقع الافتراضي، ولا تقوم بوصل الأجهزة التي تحمل المعلومات بالعالم الخارجي بأي شكل من الأشكال. أما الهجمات الإرهابية التي تستهدف مواقع سياسية فهي منتشرة وكثيرًا ما وقعت على أرض الواقع، منها نجاح الإنجليزي (نيكولاس أندرسون) في اختراق موقع البحرية الأمريكية وسرقة كلمات السر والأكواد الخاصة المستخدمة في الهجوم النووي، وأيضًا نجاح الألماني (هيس لأندر) في اختراق قاعدة بيانات شبكة البنتاجون واستطاع الحصول على ٢٩ وثيقة متعلقة بالأسلحة النووية[٤١].

وأيضًا قام مراهق أمريكي يبلغ ١٦ عامًا من فلوريدا بسرقة برمجيات خاصة بوكالة الفضاء الأمريكية ناسا بقيمة تبلغ ٧،١ مليون دولار والخاصة بإقامة محطة فضاء عالمية وتكلفت ناسا ٤١ ألف دولار لإعادة تصميم النظام وقد تم ضبط المواطن وهو يحاول اختراق نظم وزارة الدفاع الأمريكية[٤٢]، كما استطاع الأمريكي (ايريل برنس) اختراق الموقع الرسمي للبيت الأبيض، وتم القبض عليه ومحاكمته في نوفمبر ١٩٩٩م.

٣ ٢ ٥ ٢ الهجوم على الأهداف الاقتصادية والمالية:

٤١- د.على بن عبد الله العسيري، الإرهاب والإنترنت، مرجع سابق، ص٢٣٠.

٤٢- ذات المرجع، وذات المؤلف، ص٢٣١.

أصبح الإنترنت الآن عبارة عن سوق حرة مفتوحة لجميع دول العالم، فتتم من خلاله معاملات تجارية مختلفة بمليارات الدولارات، مما أصبح الجانب الاقتصادي للإنترنت أكثر إغراءًا للإرهابيين، فدائمًا ما يسعوا إليه لسببين: الأول، إنهم بحاجة إلى الأموال، والثاني، هو أن الهجمات الموجهة ضد نظم المعلومات الاقتصادية والمالية لها تأثير كبير في الرأي العالمي. ومن الأمثلة على الهجمات الاقتصادية العملية التي قام بها مجموعة من الإرهابيين، أطلقوا على أنفسهم اسم "نادي الفوضى" في عام ١٩٩٧م حيث قام هؤلاء الشباب بإنشاء برنامج تحكم لغة "أكتف اكس" مصمم للعمل عبر شبكة الإنترنت، ويمكنه أن يخادع برنامج "**Quicken**" الذي يقوم بتحويل الأموال من الحساب المصرفي إلى المستخدمين، وباستخدام هذا البرنامج أصبح بإمكانهم سرقة الأموال من أرصدة مستخدمي برنامج "**Quicken**" في جميع أنحاء العالم.

***

ثالثًا: الآليات القانونية لحماية البيئة الإلكترونية

١-٣ القوانين الوطنية وإليات الدفاع

إن الخطر المتزايد من الجرائم التي ترتكب ضد أجهزة الحاسب الآلي أو ضد نظم وأمن المعلومات، يمثل تحدي كبير أمام حكومات الدول. فهذه الأخيرة وجدت نفسها مطالبة بالتصدي لجريمة تعتبر من أكثر جرائم العصر صعوبة من حيث مكافحتها أو ملاحقة مرتكبيها. وبإجماع الخبراء يمكن للحكومات حماية البيئة الإلكترونية من خلال العمل على وضع سد منيع وحاجز قوي من القوانين والتشريعات الوطنية، والعمل على إصدار قوانين خاصة بهذه الجرائم، أو تعديل القوانين القائمة بحيث تلائم متطلبات مكافحتها. فالقوانين الحالية قد تكون غير قابلة للتنفيذ لمكافحة مثل هذه الجرائم، بالإضافة إلى أن هناك نقص موجود في الحماية القانونية ضد مخاطر الإرهاب والجريمة الإلكترونية في أغلب دول العالم ولا سيما الدول النامية، مما أدى ببعض الشركات والمنظمات على أن تعتمد على التدابير التقنية لحماية أنفسهم من هذه الجرائم.

ولكن هذه الحماية الذاتية بالرغم من أهميتها وضرورة تواجدها، إلا إنها لا تكفي لجعل الإنترنت مكانًا آمنًا لممارسة المعاملات التجارية، وعقد الصفقات التجارية التي تدر مليارات الدولارات، فلا بد من سيادة القانون.

ومن المعلوم أن الإرهاب والجريمة الإلكترونية لا تقف عند حدود جغرافية معينة، بل تمتد من أقصى المشرق إلى أقصى المغرب، دون أن يعترضها حاجز. لذلك يجب على حكومات الدول أن تدرس وضعها الراهن لتحديد ما إذا كانت قوانينها الداخلية

كافية لمكافحة الجريمة والإرهاب الإلكتروني أم لا، وأيضًا يتعين على الحكومات أن تعمل على اعتماد أفضل الممارسات من الدول الأخرى، والعمل على سن الحماية القانونية ضد هذه الجرائم.

وهناك تقرير عن الجريمة الإلكترونية والقوانين الوطنية[٤٣]، الذي تناول الوضع القانوني لـ ٥٢ دولة، وبين أن هناك ١٠ دول[٤٤] فقط هم الذين أصدروا تشريعات لمواجهة الجرائم الإلكترونية، وأن ٩ دول[٤٥] قد عدلوا تعديل جزئي في قوانينهم، وأن ٣٣ دولة[٤٦] لم تفعل أي تعديل أو تحديث لقوانينها الوطنية. ومن بين مجموعة الدول الأخيرة هناك خمس دول عربية هم مصر، ولبنان، والسودان، والأردن، والمغرب. مما يدعونا إلى بحث الوضع القانوني المصري الخاص بحماية البيئة الإلكترونية.

١-١-٣ الوضع القانوني في مصر:

في مصر لا يوجد قانون خاص بحماية البيئة الإلكترونية من الجريمة والإرهاب، لذلك فإنه يتم حمايتها بإحدى الطريقتين:

- حماية البيئة الإلكترونية بموجب الدستور المصري.
- حماية البيئة الإلكترونية بموجب قوانين أخرى.

وفيما يلي نعرض بإيجاز كيف تناولت تلك القوانين حماية البيئة الإلكترونية:

43- Cyber crime and punishment? Archaic laws threaten global information, A report prepared by McConnell, December 2000, www.mcconnellinternational.com.

44- الدول العشرة هم: استراليا وكندا واستونيا والهند واليابان وموريشيوس وبيرو والفلبين وتركيا والولايات المتحدة الأمريكية.

45- التسعة دول هم: البرازيل وتشيلي والصين والتشيك وكوريا والدنمارك وماليزيا وبولندا وأسبانيا والمملكة المتحدة.

46- هم: ألبانيا وبلغاريا وبوروندي والدومينيكان ومصر و إثيوبيا وفيجي وفرنسا وغامبيا وهنغاريا وأيسلندا وإيران وايطاليا والأردن وكازاخستان ولاتفيا ولبنان وليسوتو ومالطا ومولدوفا والمغرب ونيوزيلندا و نيكاراغوا ونيجريا والنرويج ورومانيا وجنوب أفريقيا والسودان وفيتنام ويوغوسلافيا وزامبيا وزيمبابوي.

١-١-١-٣ حماية البيئة الإلكترونية بموجب الدستور المصري:

من المعروف أن الحماية التي تتاح بموجب الدستور تكون هي الأقوى والأكثر أمانًا، لأنه هو الوثيقة العليا في الدولة والمصدر الرئيسي لجميع القوانين الأخرى، ولكن للأسف لم ينص الدستور المصري ١٩٧١م، على الجرائم المعلوماتية ولم يتعرض لها، ويرجع ذلك إلى حداثة هذه الجرائم.

٢-١-١-٣ حماية البيئة الإلكترونية بموجب قوانين أخرى:

تتعدد القوانين الفرعية وتختلف باختلاف الغرض من إصدارها، ولكننا سوف نقتصر في هذا المقام على عرض القوانين المتعلقة بالبيئة الإلكترونية، بالإضافة إلى قانون العقوبات المصري.

٣-١-١-٣ حماية البيئة الإلكترونية بموجب قانون العقوبات المصري:

لم ينص قانون العقوبات المصري على تجريم خاص بالجرائم الإلكترونية، مما جعل منه قانون يصاحبه القصور، خصوصًا أن نصوص قانون العقوبات القائمة حاليا لا تنطبق على الجرائم المعلوماتية استنادًا لأن محل الجرائم المعلوماتية ذو طبيعة معنوية تختلف عن الجرائم التقليدية، التي يتكفل قانون العقوبات الحالي بتجريمها ومعاقبة مرتكبيها. لذلك يجب على المشرع المصري إجراء التعديلات المناسبة على قانون العقوبات لكي يواكب الجرائم المستحدثة.

٤-١-١-٣ حماية البيئة الإلكترونية بموجب قانون الأحوال المدنية:

نظرًا لقيام قطاع الأحوال المدنية بمصر باستخدام تكنولوجيا المعلومات في العديد من المهام التي يقوم بها، فقد صدر القانون رقم ١٤٣ لسنة ١٩٩٤م والذي يتضمن بعض النصوص التي تعالج بصورة ما بعض الجرائم الإلكترونية، منها[٤٧]:

م ٧٢ تنص على "إنه في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز الأحوال المدنية ومحطات الإصدار الخاصة بها والمستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية فإذا وقع التزوير في المحرارت السابقة أو غيرها من المحررات الرسمية تكون العقوبة السجن المشدد أو السجن لمدة لا تقل عن خمس سنوات".

م ٧٤ تنص على "إنه مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع أو شرع في الإطلاع أو حصل منه شروع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو إذاعتها أو إفشاءها في غير الأحوال التي نص عليها القانون وفقًا للإجراءات المنصوص عليها فيه فإذا وقعت الجريمة على البيانات أو الإحصاءات المجمعة تكون العقوبة السجن".

م٧٥ تنص على "إنه يعاقب بالحبس مدة لا تجاوز ستة أشهر وغرامة لا تقل عن مائتي جنيه ولا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزء منها وكان ذلك ناشئًا عن إهماله

٤٧- القانون رقم ١٤٣ لسنة ١٩٩٤م قانون الأحوال المدنية، انظر الجريدة الرسمية العدد ٤٣ الصادر بتاريخ ١٩٩٤/٦/٩، وانظر أيضًا: د.أحمد خليفة الملط، الجرائم المعلوماتية، رسالة دكتوراه، جامعة بني سويف، ٢٠٠٥، ص١٨٣ وما بعدها.

أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة. فإذا وقع الفعل عمدًا تكون العقوبة السجن المشدد مع عدم الإخلال بحق التعويض في الحالتين".

م٧٦ تنص على "إنه يعاقب بالسجن المشدد كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصائيات المجمعة بأي صورة من الصور، تكون العقوبة السجن المشدد إذا وقعت الجريمة في زمن الحرب".

ومن خلال الإطلاع على النصوص السابقة يتبين أن المشرع في هذا القانون قد قصر محل الجريمة على البيانات والمعلومات الخاصة فقط بمصلحة الأحوال المدنية، دون أن يعتبر الجريمة الإلكترونية فعل معاقب عليه مهما كان محل الجريمة، فهو بذلك قصر الحماية على البيئة الإلكترونية لمصلحة الأحوال المدنية فقط، دون أن يتعدى هذا النطاق الضيق.

٥-١-١-٣ حماية البيئة الإلكترونية بموجب قانون حماية حق المؤلف:

يعتبر قانون حماية حق المؤلف بمثابة الخطوة الأولى لإصدار قانون خاص لحماية البيئة الإلكترونية في مصر، حيث اعترف المشرع بأن الحاسب الآلي كيان ينقصه الحماية، ومن ثم يجب العمل على حمايته، ففي التعديل الأخير لقانون حق المؤلف رقم ٣٥٤ لسنة ١٩٥٤م، الذي عدل بالقانون رقم ٢٩ لسنة ١٩٩٤م، تم إدراج مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها، ضمن المصنفات المشمولة بالحماية.

وفي نهاية عرض الوضع القانوني في مصر، والذي تبين من خلاله نقص البيئة التشريعية فيما يخص الجرائم الإلكترونية، يجب علينا أن نطالب المشرع المصري بسرعة التعرض للجرائم الإلكترونية ومواجهة الأشكال المستحدثة من الجرائم الاقتصادية والمالية وجرائم النصب والاحتيال، والجرائم الإرهابية، التي ترتكب عن طريق النظام الإلكتروني.

فمن المعلوم أن للقوانين الوطنية أهمية كبرى في ردع الجرائم، خصوصًا الجرائم الإلكترونية التي لا يمكن أن نتخطى خطورتها إلا بالقوانين الوطنية الرادعة التي تكون بمثابة إليات للدفاع، وفيما يلي سوف نعرض بإيجاز تجارب بعض الدول في التغلب على الجريمة والإرهاب الإلكتروني من خلال قوانينها واستراتيجيتها الوطنية:

- **الولايات المتحدة الأمريكية:**

تعتبر الولايات المتحدة الأمريكية أولى الدول التي أصدرت قانون لمكافحة الإرهاب الإلكتروني، ففي أكتوبر ٢٠٠١، أصدرت اتفاقية لمكافحة الإرهاب الإلكتروني[٤٨]، التي وسعت من خلالها سلطات البحث والتحقيق والمراقبة الإلكترونية. وهناك أيضًا العديد من الخطوات التي اتخذتها الولايات لمكافحة الجريمة والإرهاب الإلكتروني منها:

- إصدار قانون تعزيز أمن المعلومات ٢٠٠٢م[٤٩].
- وضع الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني ٢٠٠٣م.
- أنشأت وزارة العدل الأمريكية لجنة لمكافحة الإرهاب الالكتروني.
- دعوة البنتاغون ٢٠٠٥ إلى إنشاء لجنة تضم مجموعة من عباقرة الاختراق، لتأمين وتحصين الفضاء الإلكتروني، والشبكات الحساسة في الولايات المتحدة[٥٠].

٤٨– عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، مرجع سابق، ص٢٢.

٤٩– جمال محمد غيطاس، أمن المعلومات والأمن القومي، دار نهضة مصر، القاهرة، ٢٠٠٧، ص,٢٣٣

٥٠– عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، أبحاث الدورة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف للعلوم الأمنية، ٢٠٠٦، ٢٣.

- اليابان:

أنشأت الحكومة اليابانية العديد من دروع الحماية اللازمة للنظم المعلوماتية، خصوصًا بعد الهجمات المتتالية على مواقعها الإلكترونية من قبل كوريا الجنوبية، واعتمدت العديد من السياسات لمكافحة الإرهاب والجريمة الإلكترونية، نذكر منها[٥١]:

- وضع خطة عمل لحماية أنظمة المعلومات ضد تهديدات الإنترنت، ٢٠٠٠م.
- وضع المبادئ التوجيهية لسياسة أمن تكنولوجيا المعلومات، ٢٠٠٠م.
- وضع خطة للعمل بشأن التدابير المضادة للإرهاب الإلكتروني لحماية الهياكل الأساسية والحيوية، ٢٠٠٠م.
- إعلان الاستراتيجية الشاملة لأمن المعلومات، ٢٠٠٣م.
- وضع خطة عمل للهياكل الحكومية للرد على التهديدات الإلكترونية.

٢-٣ الآليات الدولية لمكافحة الجريمة والإرهاب الإلكتروني: الإستراتيجية والنهج

تتعدد إليات وطرق مكافحة الجريمة والإرهاب الإلكتروني على المستوى الدولي، وتختلف من منظمة إلى أخرى. وسوف نلقي الضوء على الآليات الدولية داخل الإطار القانوني الدولي، وبعد ذلك نتحدث عن التعاون الدولي، وأخيرًا عن مقترح لوضع الاستراتيجية العربية لتأمين البيئة الإلكترونية من الجريمة والإرهاب.

51- Status and Requirements of Counter-Cyberterrorism، Jeong-Tae Kim, and Tchanghee Hyun World Academy of Science، Engineering and Technology 6 2005, www.waset.org/journals/waset/v6/v6-6.pdf.

١-٢-٣ الآليات الدولية لمكافحة الجريمة والإرهاب الإلكتروني:

لم يكن هناك اتفاق أو إجماع دولي لمكافحة الإرهاب والجريمة الإلكترونية، بخلاف الاتفاقية الأوربية للجريمة الإلكترونية. وبما أن الاعتماد على تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية آخذة في الازدياد، وهذه التكنولوجيا تحمل في طياتها الكثير من الجرائم المستحدثة، فيجب علينا مناقشة الإطار القانوني الدولي الحالي، ومعرفة الآليات الدولية التي تم اعتمادها لمكافحة الإرهاب الإلكتروني:

- الأمم المتحدة:

هناك العديد من الاتفاقيات الدولية التي أصدرتها الأمم المتحدة والتي تتناول مختلف أنواع الأنشطة الإرهابية منها: الجرائم التي ترتكب على متن الطائرات، والاستيلاء غير المشروع على الطائرات والجرائم المرتكبة ضد سلامة الطيران المدني، والجرائم المرتكبة ضد الأشخاص المحمية، وأخذ الرهائن، والاستخدام غير المشروع للمواد النووية، والأعمال غير المشروعة ضد سلامة الملاحة البحرية، والإرهاب النووي.

بالإضافة إلى ذلك، فإن الأمم المتحدة أطلقت استراتيجية عالمية لمكافحة الإرهاب. والتي تعمل على مساعدة الدول الأعضاء وتطور من قدراتها على مكافحته.

وبالنسبة لمكافحة الإرهاب الإلكتروني بالتحديد، فقد قررت الأمم المتحدة في عام ٢٠٠٠م من قبل الجمعية العامة لبحث سبل مكافحة إساءة استعمال تكنولوجيا المعلومات، واعتمد القرار على توصية الدول باتخاذ تدابير معينة والتي تضمنت:

- ينبغي على الدول الأعضاء أن تنص في قوانينها على عدم توفير الملاذ الآمن لأولئك الذين يسيئون استخدام تكنولوجيا المعلومات جنائيًّا.

- النص في النظم القانونية على حماية سرية وسلامة وتوافر البيانات ونظم الحاسب من عرقلة غير مأذون بها والتأكد من معاقبة مرتكبها جنائيًّا.

وأيضًا في عام ٢٠٠٠م، انعقد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين في فيينا بالنمسا، حيث تم التأكيد على أهمية بذل جهود منسقة على الصعيد الدولي تجاه منع التهديدات ضد أمن نظم المعلومات والإنترنت، بالإضافة إلى ذلك، تم التأكيد على أهمية تبادل الخبرات التقنية بين السلطات الوطنية.

- دول مجلس أوربا:

عملت دول المجلس الأوربي على التصدي لمكافحة الإرهاب الإلكتروني والجريمة المعلوماتية، فوقَّع وزراء خارجية دول أعضاء مجلس أوربا، في ٥ نوفمبر ٢٠٠١، على الاتفاقية الدولية للجريمة المعلوماتية، والتي تعتبر أول معاهدة دولية لمكافحة الجريمة الإلكترونية، وهي نتيجة لعمل استمر أربع سنوات وشارك فيها خبراء من ٤٥ دولة أوربية، وأيضًا خبراء من دول أخرى مثل إليابان والولايات المتحدة الأمريكية وكندا.

كانت هذه الاتفاقية ثمرة تقرير أعده مجلس أوربا وتم اعتماده في ٢ أكتوبر ٢٠٠٠م بسراسبورغ، وحظي هذا التقرير أيضًا قبول دول مجموعة الثمانية في الاجتماع الذي انعقد في برلين ٢٤ أكتوبر ٢٠٠٠م. وتعد هذه الاتفاقية الثمرة الناجحة على المستوى الدولي لمحاربة الجريمة الإلكترونية.

- الإنتربول:

للإنتربول جهود كبيرة في مجال مكافحة الإرهاب والجريمة المعلوماتية، ففي ظل هذه المنظمة الدولية يتم التعاون بين ١٧٨ دولة عضو في المنظمة يعملون على مكافحة

الجريمة وملاحقة المجرمين، وهي تساعد جميع الدول الأعضاء وتقوم بتدريب موظفيها، والعمل على حمايتها ضد مختلف الجرائم.

وهناك أيضًا العديد من الخطوات التي تم اتخاذها على الساحة الدولية لمكافحة الجريمة والإرهاب الإلكتروني، منها:

- في ١٩٦٨م، انعقد المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان بطهران، والتي تبنت الجمعية العامة للأمم المتحدة توصياته.
- في ١٩٩٦م، اعتمدت لجنة الأمم المتحدة قانون الانسيترال النموذجي بشأن التجارة الإلكترونية، والذي يعتبر من الجهود الدولية الأساسية في مكافحة الجريمة والإرهاب الإلكتروني.
- في اجتماع دول الثمانية الذي عقد في واشنطن، في عام ١٩٩٧م، تم اعتماد عشرة مبادئ لمكافحة جرائم الحاسب الآلي في أي مكان في العالم.
- في ديسمبر ١٩٩٩م، عقدت جامعة ستانفورد في ولاية كإليفورنيا، مؤتمرًا دوليًّا حول التعاون الدولي لمكافحة الجريمة الإلكترونية والإرهاب، وعلى أساس ذلك قدم مقترحًا لوضع اتفاقية دولية بشأن الجريمة الإلكترونية والإرهاب.
- في مايو ٢٠٠٢م، اجتمع وزراء دول الثمانية بمدينة ترومبلن بكندا، لإصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدودية، من أجل مكافحة الأعمال الإرهابية.

- في ١١ مايو ٢٠٠٤م، أصدرت دول الثمانية بيانًا مشتركًا صدر بعنوان "مواصلة تعزيز القوانين المحلية"، الذي وصَّي جميع الدول أن تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الإلكترونية، والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالإنترنت.

- في ١٧ نوفمبر ٢٠٠٤، انعقد الاجتماع الوزاري لمنظمة "الأبيك" في شيلي، وصدر بيان مشترك من زعماء الأبيك لتعزيز اقتصاديات الدول الأعضاء للقدرة على مكافحة الجريمة الإلكترونية من خلال سن تشريعات محلية بما يتفق مع أحكام الصكوك القانونية الدولية، بما في ذلك اتفاقية الجرائم الإلكترونية.

- في ٢٨ أبريل ٢٠٠٤م، انعقد الاجتماع الخامس لوزراء العدل في واشنطن، وقدموا توصيات إلى الجمعية العامة لمنظمة الدول الأمريكية، تحثها على تنفيذ المبادئ الواردة في اتفاقية أوربا بشأن الجريمة الإلكترونية، والنظر في إمكانية الانضمام إلى الاتفاقية.

- في ٢٠٠٥م، وضعت رابطة أمم جنوب شرق آسيا "آسيان" خطة لتبادل المعلومات حول أمن الحاسب الآلي.

٢-٢-٣ التعاون الدولي كأداة لمواجهة تهديد الإرهاب الإلكتروني:

التعاون بين جميع الدول هو جزء أساسي من مواجهة الإرهاب الإلكتروني، ومع ذلك البيئة الإلكترونية لا تملك خطة من التعاون الدولي لحمايتها ضد مخاطر الجريمة والإرهاب. فهناك أسباب وراء عدم التعاون هذا، أولًا، أن هذه الجرائم جديدة في بعض

الدول، وثانيًا، لا تعرف الكثير من الدول ما يجب أن يتخذ، وأخيرًا، إنها تمس قضايا حساسة تتراوح ما بين المنافسة الاقتصادية والخصوصية والوصول إلى الأمن القومي[٥٢].

هذه الصعوبة التي تكمن فيما يتعلق بالأمن القومي والخصوصية، تعتبر من أهم الأسباب التي تمنع الدول من التعاون فيما بينها بشأن حماية البيئة الإلكترونية، خصوصًا أن هذا التعاون قد يفضي إلى الإعلان عن نقاط الضعف الخاصة بدولة معينة. فمع التقدم التكنولوجي وتزايد النظم المالية والمصرفية، وشبكات الاتصالات السلكية واللاسلكية، وأنظمة الطيران، ومراقبة الحركة الجوية، كل ذلك يعتمد اعتمادًا كبيرًا على الحواسيب وتكنولوجيا المعلومات، وفي حين إنها تخدم العديد من الدول، فإنها لا تسيطر عليها دولة واحدة. لذلك فإنه قد يكون من المعقول أن تتعاون الدول فيما بينها لخدمة المجتمع الدولي بأكمله. فالتعاون الثنائي والمتعدد ثبت إنه أنجح وسيلة للرد على الإرهاب الإلكتروني، لسببين، الأول وهو أن بعض الدول لم تشهد الإرهاب الإلكتروني حتى الآن، في حين أن بعض الدول الأخرى شهدت العديد من الهجمات الإلكترونية، والثاني، هو أن بعض الدول لديها قوانين وطنية تجرم الجريمة والإرهاب الإلكتروني، في حين أن البعض الآخر لم يكن لديه أي نوع من أنواع القوانين التي تعاقب وتجرم هذه الجرائم. لذلك فقد يكون من أنسب أنواع التعاون بين الدول هو التعاون الثنائي أو المتعدد، ونعطي بعض الأمثلة للتعاون الثنائي الذي ساعد على مكافحة الجريمة الإلكترونية:

- في فبراير ٢٠٠٠م، تلقى المركز القومي الأمريكي تقارير تفيد بأن موقع السي إن إن، وياهو، والأمزون، وغيرها من المواقع قد تعرضت للهجوم من خلال رفض الخدمة الموزعة (الحرمان الموزع)، ومن خلال التحقيقات تم إرجاع الهجمات إلى كندا، وتم التعاون بين المركز القومي

٥٢- Responses to Cyber Terrorism,Center of Excellence Defence Against Ter, IOS Press, 2008,p74.

الأمريكي، والمركز القومي للشرطة الملكية الكندية، ومن ثم تم تحديد مرتكب الهجوم وكانوا مجموعة تطلق على نفسها اسم "مافيا الأولاد" وتم القبض عليهم.

- في مايو ٢٠٠٠، تم هجوم الشركات والأفراد في جميع أنحاء العالم من قبل فيرس "I LOVE YOU" أنا أحبك، والذي تسبب في خسائر فادحة، فقام المركز القومي الأمريكي بالتحقيق في الحادث وتم التعرف على المشتبه فيه من خلال تعقب الهجوم، وتم التعاون بين مكتب التحقيقات الفيدرإلى، ومكتب التحقيقات الوطني الفلبيني، وتم تحديد المشتبه فيه.

٣-٢-٣ الاستراتيجية العربية لتأمين البيئة الإلكترونية:

الحديث عن الاستراتيجية العربية لتأمين البيئة الإلكترونية في الوقت الحالي في غاية الأهمية، نظرًا لتزايد عدد الهجمات الإرهابية على النطاق الدولي. بالإضافة إلى أن الكثير من الدول العربية البنية التحتية لمعلوماتها تفتقد الحماية المطلوبة، لأسباب عديدة يأتي في مقدمتها، عدم وجود تشريع خاص بالجريمة الإلكترونية في أغلب الدول العربية. لذلك هناك حاجة ضرورية وملحة إلى وضع استراتيجية عربية لحماية البيئة الإلكترونية، من أجل حماية الوطن العربي من التهديدات الإرهابية، ومن الهجمات الإلكترونية التي قد تؤدي إلى خسائر فادحة تصل إلى مليارات الدولارات. لذلك يجب العمل في ظل جامعة الدول العربية على وضع تلك الاستراتيجية، والعمل على إشراك جميع الدول العربية في وضعها ومن ثم تعاونهم على تنفيذها. وتصوري لهذه الاستراتيجية يمكن أن يعتمد على ثلاثة محاور أساسية وهي الوعي والتعليم، والتنسيق للحماية ضد الإرهاب والجريمة الإلكترونية، وتقاسم المعلومات بين الدول العربية.

١-٣-٢-٣ توضيح الإطار الاستراتيجي:

✓ الوعي والتعليم:

يجب التركيز على توعية المواطن العربي من خلال التعليم أو القنوات الإعلامية أو من خلال الإنترنت نفسه، بمخاطر الإرهاب والجريمة المعلوماتية، والتركيز على فئة الشباب فهي الفئة المستهدفة من قبل الإرهابيين، وأيضًا توعيتهم بأنواع الجرائم الإلكترونية لكي لا يتعرضوا لجريمة نصب أو سرقة عبر الإنترنت. وأيضًا يجب حثهم على الاستخدام الأمثل والمفيد للإنترنت والابتعاد عن المواقع المشبوهة والإرهابية، فكما علمنا أن الذي قام بتفجيرات الأزهر هو شاب مصري استخدم الإنترنت في مساعدته على كيفية صناعة قنبلة بدائية.

✓ التنسيق للحماية ضد الإرهاب الإلكتروني:

يجب التنسيق بين كافة الدول العربية على حماية البيئة الإلكترونية، وذلك من خلال عقد اتفاقية عربية لمواجهة الجريمة والإرهاب الإلكتروني على غرار الاتفاقية الأوربية، أو عقد اتفاقيات ثنائية أو متعددة لتسهيل و تسريع التحقيقات وجمع الأدلة بين الوكالات المعنية بالجريمة والإرهاب، ويجب أيضًا التنسيق بشكل استراتيجي لمحاربة المجموعات الإرهابية الموجودة داخل الدول العربية.

✓ تقاسم المعلومات:

يعد محور تقاسم المعلومات بين الدول من أهم محاور الاستراتيجية، فقد أثبتت جميع الإحصائيات العالمية أن الغالبية العظمى من الجرائم الإرهابية التي تتم في أي دولة إنما يساعد على وقوعها تمويل خارجي أو تسليح أو تدريب أو تسهيل أو تحريض على القيام بأعمال إرهابية من دولة أخرى. كما أن الجماعات الإرهابية تتعاون مع بعضها

ربما في معظم الحالات بفاعلية أكبر من تعاون الدول والمنظمات الدولية، وهي تستخدم تكنولوجيا المعلومات لتمرير المعلومات والبيانات للمنظمات الإرهابية الأخرى. لذلك يجب على الدول العربية تقاسم المعلومات فيما بينها لتفادي الوقوع تحت كلمة الإرهاب. فأكد على ذلك المشاركون في المؤتمر التاسع والعشرين لقادة الشرطة والأمن العرب المنعقد بعمان خلال الفترة ١٣-٢٠٠٥/١١/١٤م في البيان النهائي، على أهمية التعاون العربي لمواجهة الجريمة الإرهابية. وكما رأينا فيما سبق كيف ساعد التعاون الدولي بين الدول على التقليل من حوادث الإرهاب والجريمة الإلكترونية وكيف أصبح أداة فعالة لمواجهة تهديد الإرهاب والجريمة الإلكترونية.

***

الخاتمة

ليس هناك شك حول حقيقة أن الإرهاب عبر الإنترنت هو ظاهرة خطيرة وإن لم تصل التهديدات بعد إلى درجة عالية من الخطورة، فهو واقع لم تستطيع أي دولة أن تتجاهله، فالمشاكل المرتبطة باستخدام تكنولوجيا المعلومات تمثل خطر ذات طابع عالمي، فجميع الدول تواجه هذه المشكلة، ويبذلون كل ما في وسعهم للقضاء عليها.

وفي الوقت الحالي، لا توجد طرق مضمونة لحماية النظام الإلكتروني، ولا يوجد نظام آمن تمامًا بحيث يصعب على الإرهابيين الوصول إليه، مما جعل الكثير من الحكومات والمنظمات تتبع سياسة العزلة، مثلاً معظم الجيوش لا تحتفظ بالبيانات والمعلومات السرية على أجهزة متصلة بشبكة المعلومات، وإنما تحتفظ بها على أجهزة لا تتصل بالعالم الافتراضي، وسياسة العزلة بوصفها شكل من أشكال الوقاية من الإرهاب والجريمة الإلكترونية لا تصلح مع الواقع الذي تفرضه البيئة الإلكترونية على الحياة العامة. وبعيدًا عن سياسة العزلة يمكن اللجوء إلى التشفير، أو الجدران النارية. كل ذلك وغيره الكثير من وسائل الحماية التقنية، لا تستطيع أن تحدث الأثر الفعال لها دون تواجد للحماية الوطنية. ففي معظم الدول العربية لا توجد بها قوانين وطنية تحمي البيئة الإلكترونية من الجريمة والإرهاب، هذه البيئة التي يصعب ضبط وتوصيف وتعقب مرتكب الجريمة داخلها، فهي تتسم بالتغيير والانتشار الجغرافي الواسع والعابر للحدود، لذلك يجب وضع قانون وطني لحمايتها من خطر الجريمة والإرهاب.

وقبل عرض نتائج وتوصيات الدراسة يمكننا أن ندعو في نهاية هذه الدراسة حكومات الدول العربية في أن تعيد النظر في قوانينها الوطنية وأن تعدلها بحيث تناسب

الجرائم المستحدثة، وأن تعمل على سد الفراغ التشريعي. كما يجب عليها أيضًا أن تتعاون فيما بينها من خلال استراتيجية عربية لحماية البيئة الإلكترونية من الجريمة والإرهاب وأن تعيد النظر في مفاهيم الأمن القومي.

نتائج الدراسة:

- تدني المستوى الأمني والتقني للبيئة الإلكترونية العربية، فهي لم تكن بمنأى من الجريمة والإرهاب الإلكتروني.
- هناك مساحة مشتركة لتلاقي الجريمة مع البيئة الإلكترونية، هذه المساحة تتمثل في مرونة الحاسب الآلي والإنترنت، فهما أرخصا سعرًا من الأساليب الإرهابية التقليدية.
- من أهم الدوافع المؤدية للإرهاب والجريمة الإلكترونية في الوقت الحالي هي الحروب والصراعات السياسية والدبلوماسية، فالاحتلال الصهيوني لفلسطين والاحتلال الأمريكي للعراق والصراعات الداخلية والنزاعات السياسية بين الدول العربية بعضها البعض، قد ساعد على ولادة الكثير من الهجمات الإلكترونية العربية.
- أصبح الإنترنت مسرحًا للإرهابيين وبمثابة الموقع الافتراضي للعديد من المنظمات والجمعيات الإرهابية التي تبث من خلاله ثقافة الإرهاب والعنف والتطرف، وتحث الشباب العربي على الانضمام إليها مستخدمه في ذلك الجانب الديني، كما إنها تعمل على تجنيد وتدريب عناصرها الجديدة من خلال مواقعها الافتراضية.
- هناك نقص وفراغ تشريعي في موسوعة القوانين العربية فيما يختص بالجريمة الإلكترونية.

- عدم وجود تعاون بين الدول فيما يتعلق بحماية البيئة الإلكترونية على المستوى الإقليمي والدولي.

توصيات الدراسة:

- تعتبر الجريمة الإلكترونية من أكثر جرائم العصر صعوبة من حيث مكافحتها أو ملاحقة مرتكبيها، لذلك يجب على الدول وخصوصًا الدول العربية أن تتعاون فيما بينها لمكافحتها والقضاء عليها.
- التدخل التشريعي لمواجهة القصور في التشريعات والقوانين الحالية إما بإبرام قوانين خاصة بتجريم الجرائم الإلكترونية، أو بتحديثها والنص صراحة على تجريم الجرائم المتعلقة بالبيئة الإلكترونية.
- دعوة الدول العربية إلى إبرام الاتفاقيات الثنائية والمتعددة للتعاون فيما بينها لحماية البيئة الإلكترونية.
- التنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحة الإرهاب عبر البيئة الإلكترونية في كافة أنحاء العالم.
- تعزيز التعاون والتنسيق مع المؤسسات والمنظمات الدولية لمواجهة خطر الجريمة والإرهاب الإلكتروني.
- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.
- حث الدول العربية بقيادة جامعة الدول العربية على إبرام معاهدة أو اتفاقية خاصة بمكافحة الجرائم الإلكترونية، على غرار الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية.

- أهمية وضع استيراتيجية عربية لحماية البيئة الإلكترونية من الجريمة والإرهاب الإلكتروني.

***

قائمة المراجع

باللغة العربية:

١. د. أحمد خليفة الملط، الجرائم المعلوماتية، رسالة دكتوراه، جامعة بني سويف، ٢٠٠٥م.

٢. الحجاج أسامة، دليلك الشخصي إلى عالم الإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨م.

٣. جمال محمد غيطاس، أمن المعلومات والأمن القومي، دار نهضة مصر، القاهرة، ٢٠٠٧م.

٤. د. ذياب موسى البداينة، الإرهاب المعلوماتي، أبحاث الحلقة العلمية حول "الإنترنت والإرهاب"، كلية التدريب جامعة نايف للعلوم الأمنية بالتعاون مع جامعة عين شمس، ٢٠٠٨م.

٥. سمير السيد، محاضرات في شبكة المعلومات العالمية، مكتبة عين شمس، القاهرة، ١٩٩٧م.

٦. د. سهير عثمان عبد الحليم، الإرهاب والإنترنت، أبحاث المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، ٢٠٠٨م.

٧. عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي والدولي، أبحاث الدورة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف للعلوم الأمنية، ٢٠٠٦م.

٨. عبد القادر الفنتوخ، الإنترنت للمستخدم العربي، مكتبة العبيكان، الرياض، ١٤٢١هـ.

٩. عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، أبحاث الدورة التدريبية "مكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف للعلوم الأمنية، ٢٠٠٦م.

١٠. د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، دار النهضة العربية، ٢٠٠٨.

١١. د. علي بن عبد الله العسيري، الإرهاب والإنترنت، بحث منشور ضمن كتاب الإرهاب والقرصنة البحرية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٨م.

١٢. د. عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، ٢٠٠٠م.

١٣. د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة والنشر، ١٩٨٧م.

١٤. د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، دار النهضة العربية، القاهرة، ١٩٩٢م.

باللغة الإنجليزية:

1. **Addressing the New Hazards of the High Technology Workplace, Harvard Law Review, Vol. 104، No. 8، Juin 1991, Notes, p, 1898.**
2. **Ashish Pandey, Cyber Crimes – Detection and Prevention, p 5.4.**
3. **Ballard, J.D, Tlomik,J . G , & mekenzie D. 2000, "Technological facilitation of terrorism: Definitional, legal and policy issues " American Behavioral scientist, 45,(6), 989- 1016.**
4. **Cedric Laurant, Privacy & Human Rights, Electronic Privacy Information Center, USA, 2003.**
5. **Collegium Civitas" Foreign Policy of the United States of America how to prevent and fight international and domestic CYBERTERRORISM AND CYBERHOOLIGANISM prepared by Lukasz Jachowicz Warsaw", January 2003, honey.7thguard.net/essays/cyberterrorism-policy.pdf.**
6. **Cyber crime and punishment? Archaic laws threaten global information, A report prepared by McConnell, December 2000, www.mcconnellinternational.com.**
7. **Cyber Terrorism- the Dark Side of the Web World - http://www.articlesbase.com/law-articles/cyber-terrorism-the-dark-side-of-the-web-world-331261.html.**
8. **Cyberterrorism, available at http://www.ncsl.org/programs/lis/cip/cyberterrorism.htm accessed on 15th May 2008.**

9. Denning, Dorothy E..Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy., http://www.nautilus.org/info-policy /workshop/papers/denning.html., February ٤, 2000.
10. Denning, Dorothy. Is cyber terror next? 1 November 2001. Social Science Research Council. 05 June 2006. < http://www.ssrc.org/sept11/essays/denning.htm>.
11. Flaherty, Protecting Privacy, and A.C.M Nugter, Transborder Flow of Personal Date Within the EC, Kluwer Law and Taxation Publishers, 1990.
12. Human and Societal Dynamics, Responses to Cyber Terrorism, IOS Press, 2008, p 73.
13. J. J. BRITZ, TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession, http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html.
14. James Michael, Privacy and Human Rights 1 (UNESCO 1994).
15. Joshua Green, the myth of cyberterrorism, http://www.washingtonmonthly.com/features/2001/0211.green.html.
16. Kraft, D. (2000, October 26). Islamic groups 'attack' Israeli web sites. Retrieved November 10, 2003, fromhttp://www.landfield.com/isn/mail-archive/2000/Oct/0137.html.
17. Mark M.pollitt, " cyberterrorism: fact or fancy?" proceedings of the 20th National

Information Systems Security Conference, October 1997, pp. 285-289.

18. McGarry, K. (1993). The Changing Context of Information. An Introductory Analysis. 2nd ed. London: Library Association Publishing.

19. McWethy, J. & Starr, B. (2001, April 26). Hacker alert: Pentagon braces for Chinese computer attacks. Retrieved November 2, 2003, from,http://abcnews.go.com/sections/world/DailyNews/chinahackers_010426.html.

20. Nagpal, Rohas. Defining Cyber Terrorism. 2004. Asian School of Cyber Laws. 04 June 2006. http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm.

21. Privacy and the computer: Why we need privacy in the information society", L. Introna, Metaphilosophy (http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp96/abstracts/introna.html.

22. Responses to Cyber Terrorism,Center of Excellence Defence Against Ter, IOS Press, 2008,p74.

23. Richard O. Mason,Management Information Systems Quarterly , Volume 10, Number 1, March, 1986pp. 5-12

24. Ronczkowski, Michael. Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations. Boca, FL: CRC Press, 2004. 17-42.

25. S. Wehner, Privacy and Anonymity on the Net, http://www.r4k.net/cyfem/.

26. Savino, Adam. Cyber-Terrorism. 2001. University of Dayton School of Law: Cyber Crimes. 04 June 2006. http://www.cybercrimes.net/Terrorism/ct.html.

27. Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order 23 (Pan 1996).

28. Stark, Rod. "Cyber Terrorism: Rethinking New Technology," Department of Defense and Strategic Studies, 1999.

29. Status and Requirements of Counter-Cyberterrorism, Jeong-Tae Kim, and Tchanghee Hyun World Academy of Science, Engineering and Technology 6 2005, www.waset.org/journals/waset/v6/v6-6.pdf.

30. United Nations, GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES. Adopted by the General Assembly on 14 December 1990.

31. Vatis, M. (2002, June). Cyber attacks: Protecting America's security against digital threats. Discussion paper,ESDP-2002-04, John F. Kennedy School of Government, Harvard University.

32. Volio, Fernando, "Legal personality, privacy and the family" in Henkin (ed), The International Bill of Rights (Columbia University Press 1981).

33. Ware, W.H. (1993). The new faces of privacy. The Information Society, 9 (3): 195-211.

34. Weimann .G .(2004,march) www.terror.net:How 5-modern terrorism uses the Internet.

35. Weimann.G,(2004 may) Cyber terrorism, How Real Is the Threat? http://www.usip.org/resources/cyberterrorism-how-real-threat.

36. White, Col. Kenneth C.١٩٩٨ Cyber-Terrorism: Modem Mayhem." Carlisle Barracks, Pennsylvania: U.S. Army War College.

37. Whitten and D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", In Proceedings of the 8th USENIX Security Symposium, Washington, DC, 1999, p. 169-184.

***