تدابير و آليات مكافحة الإرهاب الإلكتروني

الباحثة نجاري بن حاج علي فايزة
جـامعة مولـود معمري تيزي وزو.

الملخص

التطور التكنولوجي وتقنية المعلومات ساهما فعلا بانتشار الشبكة المعلوماتية الانترنيت، وهو ما أدى إلى زيادة استخدام الحاسب الآلي وتطبيقاته في الحوكمة الإلكترونية وكل مجالات الحياة خاصة السياسية والاقتصادية من جهة، لكن من جهة أخرى التطور التكنولوجي وتقنية المعلومات ساهما أيضا في عولمة الكثير من الجرائم، خاصة الإرهاب الذي خطى خطوة جد رهيبة بتنازله عن استعمال الأساليب التقليدية وتحوله إلى إرهاب إلكتروني يتطلب إتحاد جميع الدول للتصدي لهذه الظاهرة.

تعد دراسة الإرهاب الإلكتروني والتطرق إلى وسائله وأساليبه، خصائصه و صوره نظرة تحليلية اتجاه ظاهرة إرهابية معاصرة ومعقدة وذات أبعاد تدميرية مكلفة للبشرية والعالم، لأننا أمام إرهاب صامت وغير ظاهر للعيان، يقتل ويدمر في جو لا يمكن رصده وهذا ما يوفر الراحة والسلامة والوقت للجماعة الإرهابية.

الكلمات المفتاحية: الانترنيت، الإرهاب الإلكتروني، تقنيات الاتصال، الأمن والاستقرار، آليات المكافحة.

المقدمة

بعد ان عاشت البشرية ثورتين غيرتا طبيعة الحياة البشرية: الثورة الصناعية والثورة الزراعية ، يعيش العالم اليوم ثورة جديدة قوامها المعلوماتية، زيادة الإنتاج وسرعة اتخاذ القرارات آلا وهي الثورة التكنولوجية، حيث يأتي في مقدمتها شبكة المعلومات العالمية الانترنيت، أبرز مجهود نتج عن تلاحم تكنولوجيا المعلومات بوسائل الاتصال و الحواسيب كما أنها – أي الإنترنت- تمثل أبرز النماذج العالمية في الاستفادة من خدمات الشبكة الرقمية المتكاملة (Integrated Digital Network).

بتقدم التكنولوجيا تقدمت الصناعة ووسائل الاتصال بين الدول والشعوب، الأمر الذي ساعد على معرفة المستهلكين ورغباتهم بفضل وسائل الإعلام المختلفة وهذا ما دفع الإنسان إلى الرغبة في اقتناء هذه التكنولوجيا الحديثة، قصد الوصل بين البائع والمستهلك وهو السبب الفعلي لوجود ما يعرف بالاقتصاد الرقمي.

إلا أن هذه الثورة التكنولوجية، كانت لها سلبيات – كغيرها من الثورات الأخرى- في ظهور مجموعة من الأفراد يسيئون استخدامها لخدمة الإرهاب، سواء عن طريق الاتصال بشبكة الانترنيت لتجنيد عدد من الإرهابيين والتواصل معهم وتدريبهم، أو من أجل عرض أفكارهم الهدامة، ونشر ثقافة الرعب والإرهاب، أو من خلال الاتصالات السلكية واللاسلكية عبر الأقمار الصناعية وما يتبعه من عمليات تجسس، وكذا خرق الأنظمة الإلكترونية للمواقع الحساسة للأجهزة الأمنية، التجسس على المؤسسات الاقتصادية العملاقة في تعاملاتها التجارية الإلكترونية، ضرب البنى التحتية للاقتصاد العالمي... الخ، وهو الأمر الذي دعا ثلاثين دولة للتوقيع على أول اتفاقية دولية لمكافحة الإجرام المعلوماتي، والتي وصفت هذا النوع من الإرهاب بـ «الإرهاب الإلكتروني» بالعاصمة المجرية بودابست، عقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر 2001.[1]

تعد دراسة الإرهاب الإلكتروني والتطرق إلى وسائله و خصائصه نظرة تحليلية اتجاه ظاهرة إرهابية معاصرة ومعقدة وذات أبعاد تدميرية مكلفة للبشرية والعالم، لأننا أمام إرهاب صامت وغير ظاهر للعيان، يقتل ويدمر في جو لا يمكن رصده وهذا ما يوفر الراحة والسلامة والوقت للجماعة الإرهابية، خاصة مع استخدامهم الحاسب الآلي وتطبيقاته في مجال الحوكمة الإلكترونية والاقتصاد الرقمي بكل أنشطته وخدماته، كما هو الحال في الدول الأوروبية وبعض الدول العربية كدولة الإمارات العربية المتحدة، لكن من جهة أخرى التطور التكنولوجي وتقنية المعلومات ساهما أيضا في عولمة الكثير من الجرائم، خاصة الإرهاب الذي خطى خطوة جد رهيبة بتنازله عن استعمال الأساليب التقليدية وتحوله إلى إرهاب إلكتروني يتطلب إتحاد جميع الدول للتصدي لهذه الظاهرة.

على ضوء ما تقدم، فإن إشكالية دراستنا تنحصر في: **الآليات الدولية والوطنية لمحاربة خطر الإرهاب الإلكتروني الذي يهدد أمن واستقرار العالم بطريقة مباشرة وخطيرة؟**

للإجابة على هذه الإشكالية نركز في دراستها على محورين أساسيين هما:

أولا: محاولة تحديد مفهوم الإرهاب الإلكتروني.

ثانيا: التطرق الى التدابير التقنية والتشريعية المقررة لمكافحة الإرهاب الإلكتروني.

المحور الأول: مفهوم الإرهاب الإلكتروني

بسبب طبيعة شبكة الانترنيت وانفتاحها غير المحكوم، وعدم ارتباطها بدولة واحدة أو حدود جغرافية معينة، وبسبب صعوبة الرقابة أو المحاسبة على ما ينشر عليها، أصبحت مسرحا سهلا للاعتداءات كنشر الأفكار المتطرفة التي تتعارض ومصالح المجتمع بشكل يخفي هوية الفاعل، مقارنة بالمجرم التقليدي الذي يحتاج إلى أسلحة وتحركات سريعة جدا قد تصيب وقد تخفق، ناهيك عن التكاليف المادية لإنجاح العمليات بينما يحتاج المجرم الذي ينشط في المجال الإلكتروني إلى بعض المعلومات ليستطيع اقتحام كل التعاملات الإلكترونية، كما أن التكاليف لا تتجاوز جهاز حاسوب موصول بشبكة الانترنيت.

بناءًا على ذلك فقد جرى توظيف التقنيات الرقمية من قبل الأفراد، المنظمات والدول للإضرار بالغير والقيام بأعمال إجرامية سميت بـ "الإرهاب الإلكتروني".

أولا: مفهوم الدولي للإرهاب الإلكتروني

يعتبر الإرهاب الإلكتروني نوع من الإرهاب الحديث الذي وظّف واستثمر تقنيات المعلومات والاتصالات في العصر الراهن بشكل يلائم متطلباته، إذ يصعب رصده أو حصره، وهذا أدى أيضا إلى وجود صعوبة في تحديد تعريف صريح وواضح، بل هناك مفاهيم له سيتم عرضها كالتالي:

أ - الولايات المتحدة الأمريكية

ظهر الإرهاب الإلكتروني بصورة علنية عندما قام الرئيس الأمريكي "بيل كلينتون" سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية، وكان أول استنتاج لهذه اللجنة هو أن مصادر الطاقة الكهربائية والاتصالات، إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة الأمريكية، وبما أنّ هذه المنشآت تعتمد بشكل

كبير على المعلومات الرقمية، فإنّها ستكون الهدف الأول لأي هجمات إرهابية، تستهدف أمن الولايات المتحدة الأمريكية، وعليه قامت كافة الوكالات الحكومية في هذه الأخيرة – الولايات المتحدة الأمريكية – بإنشاء هيئات ومراكز خاصة للتعامل مع هجمات الإرهاب الإلكتروني.[2]

قامت في السنة نفسها (1996) المدرسة الحربية التابعة لوزارة الدفاع الأمريكية، بتقديم تعريف للحرب الإلكترونية دون الإرهاب الإلكتروني بأنها «إنّ الحرب الإلكترونية هي الإجراءات التي يتم اتخاذها بشكل سلبي على المعلومات والنظم الإلكترونية، لتخريبها وتخريب النظم الإلكترونية التي تحتويها»، حسب تعريف المدرسة الحربية، فإنّ الحرب الإلكترونية تتضمن أنشطة مثل تخريب أمن المعلومات، الهجمات على النظم الإلكترونية وكذا الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم أو النقاط الهامة ضمن شبكاته.

قامت المكاتب الفيدرالية باتخاذ إجراءات أمنية في المجال نفسه، حتى تتمكن بالرد السريع والفعال إزاء المتغيرات السريعة لعمليات الإرهاب الإلكتروني.[3]

كما أظهرت دراسة أمريكية أن الإرهابيين لديهم شغف في استخدام شبكة الانترنيت في عملياتهم الإرهابية، مظهرين بذلك مستوى براعتهم في تحطيم أو التفوق على أي تقنية مستخدمة.[4]

وعليه يمكن القول أن الولايات المتحدة الأمريكية لم تعط أي تعريف للإرهاب الإلكتروني، بل اهتمت بدراسة الظاهرة محاولةً فهم سياسة تفكير الإرهاب الإلكتروني والطرق التي يتخذها في تنفيذ عملياته، مشيرة إلى الرابط الذي يجمع هذا الأخير بحرب المعلومات أما مجموع التعاريف المقدمة سابقا، فهي عبارة عن محاولة لبعض الأجهزة والإدارات التابعة للولايات المتحدة الأمريكية في تحديد معنى الإرهاب بما يخدم أغراضها، وبدلا من إيجاد تعريف واحد، هناك أكثر من تعريف.[5]

ب – الاتحاد الأوروبي

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر، ذلك منذ عام 1976، ثم في عام 1996 أنشأت اللجنة الأوروبية (ECCP) للتعامل مع مشاكل الإجرام والتي يدخل تحت رايتها الجرائم الإلكترونية[6]، عملت اللجنة منذ سنة 1997 إلى غاية سنة

2000 على مشروع اتفاقية بودابست والتي اعتمدها البرلمان الأوروبي في الجزء الثاني من الجلسة العامة في شهر أفريل 2001، ثم تم التصديق على المعاهدة رسميا من قبل 30 دولة في 23 نوفمبر من السنة نفسها.

تم تجديد مدونة اتفاقية عمل بودابست ضد الجرائم المعلوماتية بمختلف أشكالها وأنواعها، محددة في ذلك التعاون بين الدول الأعضاء، في تبني التشريعات الأساسية في هذا المجال، لكن ما يلاحظ أن هذه الاتفاقية لم تأتِ بتعريف لمرتكبي هذه الجرائم التي تدخل ضمن الإرهاب الإلكتروني؟

دفع هذا الفراغ ببعض الدول الأعضاء مثل فرنسا في تبني مفهوم الإرهاب الإلكتروني على أنه «كل هجوم الغرض منه الحصول على المعلومات المرتبطة بالغير، وإمكانياته واستراتيجياته التي يتخذها للدفاع عن نفسه، أو تدمير نظم معلوماته أو نشر معلومات زائفة من أجل تضليله بتوظيف تكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنيت».[7]

الملاحظ في هذا التعريف أنه لم يحدد الفئة التي يحدث ضدها الهجوم، فالقول كل هجوم ضد الغير مبهم، لكن بالمقابل حدد تماما الأسباب التي تدفع بوجود إرهاب إلكتروني مع تحديد الوسائل التكنولوجية المختلفة، الحاسب الآلي أي الكمبيوتر، الانترنيت، تكنولوجيا المعلومات مثل الأقمار الصناعية... الخ.

أما إيطاليا فقد عرّفت الإرهاب الإلكتروني بأنه «كل جماعة إرهابية تستعمل الوسائل التكنولوجية كالانترنيت من أجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق وتبادل المهارات والخبرات والأساليب، أو جمع التبرعات من أجل تمويل عملياتهم الإرهابية»[8]، جاء تعريف إيطاليا للإرهاب الإلكتروني من خلال تحديد أسلوبه في العمل عن طريق الدعاية للأعمال الإرهابية باستعمال الوسائل التكنولوجية، التنسيق والتخطيط للعمليات وكذا تمويلها، ولكن بالرجوع إلى هذا التعريف الذي يحصر الإرهاب الإلكتروني كونه جماعة، فهل الشخص الذي ينشط بطريقة فردية متبعا الأساليب نفسها يُعتبر مجرما إلكترونيا لا يصنف كإرهابا إلكترونيا؟

نظرا للثغرات الموجودة في مجموع التعاريف المقدمة للإرهاب الإلكتروني من طرف الدول الأعضاء في الاتحاد الأوروبي، كان لابدّ على هذا الأخير "الاتحاد الأوروبي" من إيجاد تعريف شامل للإرهاب الإلكتروني، إلا أن الاتحاد تقدم بتعريف الإرهاب

بشكل عام سنة 2002 «كل عمل يرتكب بهدف ترويع الأهالي، أو إجبار حكومة أو هيئة دولية على القيام بعمل أو الامتناع عنه، أو تدمير الهياكل الدستورية أو الاقتصادية أو الاجتماعية لدولة ما أو هيئة دولية ما أو زعزعة استقرارها ».[9]

شمل تعريف الاتحاد الأوروبي للإرهاب كل أنواع الإرهاب سواء الإرهاب الفردي إرهاب الجماعة أو ذلك الذي يمس الدولة أو إحدى الهيئات الدولية، مع تحديد الغايات بتلك العمليات الإرهابية كالترويع، التهديد، إجبار الخصم بالقيام بعمل أو الامتناع عنه أو زعزعة الاستقرار.

إذا اعتبرنا أن الإرهاب الإلكتروني يدخل ضمن هذا التعريف، لأنه حتى وإن اختلفت وسائله يظل إرهابا، لماذا لم يتبنَ الاتحاد الأوروبي تعريفا صريحا للإرهاب الإلكتروني ما دام يقر بجرائمه من خلال اتفاقية بودابست؟ بل أكثر من ذلك لماذا بعض الدول الأعضاء ميزت بين إرهاب التقليدي والإلكتروني بينما يظل الاتحاد صامتا عن إعطاء تعريفا واضحا للإرهاب الإلكتروني؟

ج- تعريف الدول العربية للإرهاب الإلكتروني

حاولت الحكومات العربية مواكبة الثورة التكنولوجية، باعتماد العديد من الدول العربية كمصر، الإمارات العربية المتحدة والجزائر مؤخرا تبني فكرة التجارة الإلكترونية والتعاملات الإلكترونية، يقابلها تحديد الصعوبات التي تواجه هذه الدول، وأخرى في تجسيدها على أرض الواقع نظرا لوجود العديد من العراقيل، أهمها الخوف من ظاهرة الإرهاب الإلكتروني.

أقرت العديد من الدول العربية بالخطر الذي يواجهها على الصعيدين الداخلي والدولي للإرهاب الإلكتروني، إذ أن دولة قطر اعترفت بوجوده محددتا بذلك مفهومه على أنه «العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الفساد».[10]

وتعرّفه المملكة العربية السعودية على أنه «أي فعل يُرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية أو استخدام التقنيات الرقمية المخالفة لأحكام

النظام، ومن أنواعه: السب، التشهير والابتزاز والإباحة وكذلك الشائعات وما يتعلق بالأمور المالية كالاعتداء على البطاقات البنكية بأشكالها واختلاسها».[11]

أما مصر فقد عرفت الإرهاب الإلكتروني بأنه «الاستخدام غير القانوني للقوة أو الضعف ضد الأفراد أو الممتلكات بغية الإرهاب والتهديد لإرغام الحكومة أو السكان المدنيين أو أي فئة أخرى على القبول بهدف سياسي أو اجتماعي أو اقتصادي».[12]

الملاحظ في التعريفات المقدمة من طرف بعض الدول العربية على غرار اعترافاتها بهذا التهديد الجديد، هناك عدة تسميات لهذه الظاهرة الإرهابية، فمرة يسمى الإرهاب المعلوماتي، الإرهاب الإلكتروني وتارة بإرهاب تكنولوجيا المعلومات، هذا الاختلاف في التسميات يرجع إلى كون هذه الظاهرة الإجرامية جديدة في المجتمع العربي، كما أن لكل دولة دوافعها من هذه التسميات، ولكن الأمر يتطلب وضع عنوان جامع وشامل تنطوي تحته كل التسميات السابقة الذكر حتى يمكن التفرقة بين هذا النوع من الإرهاب دون غيره.

ثانيا: خصائص الإرهاب الإلكتروني

بالرجوع إلى بعض خصائص الإرهاب القديم نجده يتمركز في مكان واحد، ضعيف البنيان وغير منظم، عكس الإرهاب الحديث وأشكاله الجديدة التي تعتمد على التكنولوجيا التي ساعدت المنظمات الإرهابية في التحكم الكامل في اتصالاتها ببعضها البعض، مما زاد من اتساع مسرح عملياتهم الإرهابية، والتي أصبح من الصعب حصرها والقضاء عليها لأنها تتمتع بالخصائص التالية:

أ- التعامل بالبريد الإلكتروني

يعتبر البريد الالكتروني من أعظم الوسائل والأدوات المستعملة في الإرهاب الإلكتروني من خلال استخدامه للتواصل بين الإرهابيين، بل إن الكثير من العمليات الإرهابية التي تمت في السنوات الأخيرة، كان البريد الإلكتروني السبب في نجاحها.[13]

غير أن الغرض الحقيقي من استعمال الإرهاب الإلكتروني للبريد الالكتروني هو سهولة نشر أفكارهم وتحقيق أهدافهم التخريبية من خلال الاتصال والتنسيق فيما بينهم نظرا لقلة التكاليف، كما أن الرسائل الالكترونية مقارنة بالوسائل الأخرى، توفر للإرهابيين التواصل والتخفي عن طريق البريد، بوضع رسائل مشفرة، تأخذ طابعا يلفت

الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته، كما أنها لا تترك أثر يمكن أن يدل عليه.[14]

كل هذه الأساليب التي يستخدمها الإرهاب الإلكتروني إن دلت على شيء فإنما تدل على وجود عيوب في البريد الإلكتروني أهمها دخول البرامج الضارة أو ما يسمى بالفيروسات، وهذه الأخيرة تقوم بإتلاف البرامج والملفات جزئيا أو كليا وبأساليب مختلفة، وقد تمت مواجهة الفيروسات بالفيروسات المضادة، تقوم باكتشاف الفيروسات المخبأة داخل الملفات أو البرامج وتمنعها من الدخول إلى النظام، وذلك لتأمين سلامة المعلومات والبيانات الموجودة في ذاكرة الحاسوب، لكن هذه البرامج المضادة للفيروسات تبقى غير نافعة جزئيا بحكم أن الإرهابي يجد دائما طرق أخرى سواء لاختراق البريد الإلكتروني أو لاستعماله كأداة تمهد أو تسهل أو تقوم بالغرض الإرهابي.

أضف إلى أن بعض رسائل البريد الإلكتروني لا تظهر توقيع صاحبها، ذلك لأن ارتباط البريد الإلكتروني بشبكة متشعبة كالأنترنيت، لا يمكن العلم مسبقا بالطريق الذي سوف تسلكه الرسالة أو التأكد من حسن استلامها أو إثبات استلامها، إذا أنكر الطرف الآخر الموجهة إليه هذه الرسالة.

ب- تعطيل الخدمات الإلكترونية

تعطيل الخدمات الإلكترونية، ليس من هجمات الاختراق حيث لا يهدف هذا النشاط إلى تغيير أو تعديل النظام أو تدبيره، كتغيير معطيات صفحة تجارية عن طريق الانترنيت بإنقاص أو إضافة بيانات أو حذفها تماما من الموقع الإلكتروني المعروضة في الصفقة، بل يعمل نظام التعطيل المؤقت للخدمة على إضعاف قدرة الأنظمة الحاسوبية على إنجاز وظائفها، وبالتالي إيقاف النظام وتعطيله أو إغلاقه دون حدوث تدمير.[15]

فالتعطيل المؤقت للخدمة يهدف إلى غلق نظام تشغيل الكمبيوتر، من خلال وقف تدفق المعلومات، ويقدر الباحثون في مجال أمن الحاسب الآلي، بأن هناك ما يقارب 4000 هجوم يحدث على مستوى العالم أسبوعيا، ويمكن أن يكون هذا النشاط محليا عندما يصيب شبكة حسابات محلية، ودوليا عندما يصيب أجهزة الكمبيوتر خارج إقليم دولة واحدة.

يكون التعطيل عادة باستخدام القنابل والصواريخ الإلكترونية[16]، التي تحمل النبضة الكهرومغناطيسية الناتجة عن انفجار طاقة هائلة تضر بالتجهيزات الإلكترونية

الحساسة وخاصة تلك التي تعمل بأنصاف النواقل والدارات المتكاملة، الأمر الذي يجعل معظم التجهيزات الإلكترونية المستخدمة –خاصة تجارية منها- والتجهيزات الحاسوبية تتعرض للتخريب عند تلقي نبضة شديدة من هذا النوع.

تتدرج الآثار المترتبة على نبضة الأمواج الكهرومغناطيسية، بين تخفيض استطاعة أجهزة بث الراديو إضعاف حساسية الأجهزة العامة إلى شلل كامل، وتعطل أنظمة الأشغال (Ignition Systems) في السيارات، وأجهزة الاتصالات والكمبيوترات.

ج- التصرف في المعلومات الإلكترونية

يتم التصرف في المعلومات الإلكترونية بوسائل فنية لحل الشفرات والدخول إلى شبكة المعلومات وسرقة ما بها من معلومات أو بيانات، لأغراض الابتزاز والتهديد، التشهير والإعلام، كشف حقائق للتجارة بها أو استخدامها في مجالات أخرى للإرهاب، ويشمل ذلك السطو على حسابات البنوك الكبرى وتحويل المال إلى جماعات إرهابية، أو سرقة برامج واختراعات وابتكارات المصانع والشركات في إطار التجسس الصناعي و/ أو السياسي، كما أن هناك العديد من الجرائم الإرهابية التي تتم عن طريق المعلومات بطرق انتحال شخصية الغير، وسرقة كلمة المرور(password)، وتتم عن طريق إرسال رسائل إلكترونية، مدعيا المجرم تقديم خدمة، ومن ثمة ينال المتلقي عن طريق كلمة المرور الخاصة به، ولهذا يستطيع أن يدخل على البريد الإلكتروني ويحل محله في الرد على الآخرين والحصول على بطاقات الائتمان والشراء بها، واستخدامها، واستخدام اسم الشخص في أعمال إجرامية.[17]

كما يتم التصرف في المعلومات بتزويرها، ويعني ذلك، تغيير حقيقة العمل الذي تؤديه البرمجيات، كتغيير البنى التحتية لنظام مصرفي، وتزوير الرسائل الإلكترونية المتداولة أو زرع رسائل كاذبة ونشر الشائعات وغيرها، إلا أن الهدف النهائي منها غالبا ما يكون الإضرار بالمعلومات المتداولة والبرامج، بما يحقق غرض الإرباك وتحريف المعلومات وتغيير وجه الموقع [18] (Defacing).

وأخيرا يمكن التصرف في المعلومات عن طريق إتلافها وكذا البيانات المسجلة على الحواسب والشبكات المحلية والدولية، ويدخل فيها قواعد البيانات وبرامج التحكم والمتابعة للنظم الكبرى في مختلف المجالات، وتتم عملية الإتلاف باستخدام الفيروسات وديدان الحواسب التي يمكنها تدمير البيانات ومسح المعلومات في الأوقات المحرجة

كالحروب وتستخدم عادة ضد أهداف عسكرية، ولكن مؤخرا صارت تستخدم ضد كل ما له علاقة بالمال كالبورصة، الصفقات التجارية الدولية وكذا عمل الشركات الاقتصادية العملاقة، يتم ذلك بواسطة هجمات رقمية على الحواسب وشبكة الانترنيت، باستخدام الفيروسات.

المحور الثاني: التدابير التقنية والتشريعية المقررة لمكافحة الإرهاب الإلكتروني

إن الحاجة إلى اتخاذ تدابير دولية لردع ظاهرة الإرهاب الالكتروني كونه ذو طبيعة معنوية وليس مادية كما في الجرائم التقليدية، فعندما يكون الكمبيوتر مثلا هدفا للإرهاب فإن السلوك يستهدف بيانات تمثل قيما مالية، وعندما يكون الكمبيوتر بيئة للجريمة الإرهابية فإن مضمون الفعل غير المشروع هو انتهاك المعلومات وهو التهديد الحقيقي الذي دعا إلى تكثيف وتطوير النظم التقنية.

أما بالرجوع إلى الشرعية الجنائية الدولية والإقليمية اللذان يمنعان المسائلة إذا لم يتوفر النص القانوني إذ لا جريمة ولا عقوبة إلا بنص، وبالرجوع إلى طبيعة الإرهاب الإلكتروني، فإن معظم الدول التي تعي تهديد هذا الأخير، أصبحت تكثف الجهود التشريعية محاولة إما الحد من هذا الإجرام، أو حصره وتفادي ما يسببه من خسائر على جميع الأصعدة

أولا: الحماية التقنية لحصر الإرهاب الإلكتروني

بعدما تم وضع مجموعة من الآليات الأمنية الهادفة للحماية من خطر الإرهاب الإلكتروني، كان لا بد من توفير حماية ذات طبيعة تقنية قادرة على تقديم أمن أكثر للمستخدم، فدرجة الحماية المطلوبة تختلف حسب نوع المعلومة المراد حمايتها، بمعنى أن إجراءات الحماية تنطلق من احتياجات الحماية الملائمة كحماية المعاملات المالية الإلكترونية وحماية المواقع الخاصة بالإنترنت.

أ- حماية المعاملات المالية الإلكترونية عن طرق وسيط الوفاء الإلكتروني

يتم عبر هذا الأسلوب نقل النقود من حساب العميل لحساب الدائن التاجر ذلك بعد إتمام إجراءات الوفاء بين بنكي العميل والتاجر، وقد كان من أبرز أنظمة التحويل بين الحسابات:

1- النظام الافتراضي الأولي (First Virtual)

يقتضي هذا النظام أن يكون للتاجر حساب بنكي في بنك وان يقوم العميل بتقديم المدين طلبا بفتح حساب لديها بعد أن يرسل لها خارج شبكة الإنترنت بالبريد العادي أو الهاتف رقم حسابه البنكي ورقم بطاقته البنكية الخاصة به بعد ذلك تقوم الشركة بتزويد العميل بمعرف[19] (Identifiant).

يقوم العميل بإرسال رقم تعريفه الشخصي للتاجر، هذا الأخير الذي يسمح له بالتأكد من وجود وكفاية حساب العملية لدى الشركة الوسيطة، وذلك بأن يرسل لها معلومات خاصة بالصفقة، ورقم التعريف الشخصي للعميل والتاجر، ثم ترسل هذه الشركة للعميل الذي يتطابق مع المعرف (الهوية) رسالة إلكترونية تطلب منه تأكيد عملية التسوية، فتقوم الشركة الوسيطة بعد حصولها على رضا العميل، بإرسال كامل المعلومات عبر شبكة البنوك التقليدية التي يتم من خلالها تنفيذ عملية تحويل النقود من حساب العميل لحساب الشركة الوسيطة، وليس لهذه الشركة بعد ذلك غير الوفاء بالنقود للتاجر وإخطاره بنجاح عملية الوفاء حتى يتمكن من تنفيذ التزامه تجاه العميل.

2- نظام (kleline)

وعلى خلاف النظام السابق يحتاج العميل المستفيد من نظام (kleline) إلى أن يضيف إلى حسابه الإلكتروني الشخصي برنامج للوفاء الأمني يسمى (Kleline)، وبعد أن يرسل العميل طلب شراء بضاعة معينة إلى التاجر، يرسل هذا الأخير بطاقة وفاء إلكتروني إلى الشركة الوسيطة التي يجب عليها بعد التأكد من التاجر أن ترسل بطاقة الوفاء إلى العميل.[20]

وبعد استلامه لهذه البطاقة على العميل أن يصدر قبوله لها إلكترونيا وبعد رضا العميل تقوم (Kleline) بإتمام عملية الوفاء وتضع تحت تصرف التاجر قسيمة صندوق (Bonde caisse).

الميزة الأساسية (لنظام Kleline) يتمثل في ضمان الأمان لعملية الوفاء عبر برنامج حاسوبي خاص وضمان الوجود الفعلي للتاجر الذي يجب أن يكون مسجلا لدى الشركة.

كما أن هذه الطريقة (وسيط الوفاء الإلكتروني) قللت من مخاطر الوفاء الإلكتروني فتدخل الوسيط بين المتعاقدين يعد أمرا آمنا سواء من جانب المورد أو من جانب عملائه، إذ أنها لا تسمح بتدخل الإرهاب الإلكتروني بهوية مزورة.

ب- حماية المواقع الخاصة بالإنترنت

يتجلى حماية المواقع الخاصة بالإنترنت من خلال نظام التشفير بالإضافة إلى الجدران النارية.

1 - نظام التشفير كوسيلة لحماية سرية المعلومات

التشفير هو إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات ووسائل تحويل المعلومات، بهدف إخفاء محتواها والحيلولة دون تعديلها أو استخدامها غير المشروع، ويعرف كذلك التشفير بأنه عملية تحويل المعلومات إلى رموز غير مفهومة بحيث يمنع الأشخاص غير المرخص لهم من الاضطلاع على المعلومة أو فهمها، فعملية التشفير تنطوي على تحويل النصوص العادية إلى نصوص مشفرة ومن المعلوم أن الانترنيت تشكل الوسيط الأضخم لنقل المعلومات الحساسة للحركات المالية والتواقيع الإلكترونية بصيغة مشفرة للحفاظ على سلامتها من عبث القراصنة.[21]

ويسمح نظام التشفير بتفادي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية الاحتيالية في المعاملات التجارية، حيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، فالتشفير يساعد على حفظ سرية المعلومات والتوقيع الإلكتروني، الذي يتطلب الحفاظ على الأرقام والرموز لحمايته ضمن الاقتصاد الرقمي.

والغاية من التشفير هو إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها لكي لا يستطيع أي شخص الاطلاع على هذه البيانات غير المتعاقدين أو من يصرح له قانونا بذلك، كما يهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات ومن ثم منع وصولها مشوهة للطرف الآخر في المعاملات التجارية على نحو يعرقلها.[22]

2 - نظام المعاملات الإلكترونية الآمنة (set)

وهو أهم برتوكول متعلق بالنواحي التأمينية وهدفه الأساسي هو تأمين عملية الوفاء والمعاملات المالية التي تتم أثناء المعاملة التجارية.

ويتميز هذا النظام عن الأنظمة التأمينية الأخرى بعدة مميزات كونه[23]:

- يضمن أن طلب الشراء المرسل هو نفسه الطلب الذي يستقبله صاحب المشروع أو التاجر عن طريق بصمة ورقية معينة تكون مميزة لهذا الطلب.
- يضمن سرية طلب الشراء عن طريق تشفير المعلومات التي يشملها الطلب وكذلك البيانات الخاصة بعمليات الوفاء.
- يضمن للتاجر أو صاحب المشروع أن حامل البطاقة البنكية هو الشخص نفسه، عن طريق الشهادة التي يحملها والصادرة عن البنك الضامن أو شركة الائتمان الضامنة له والتي تؤكد لصاحب المشروع أو التاجر أن هذا الشخص الراغب في الشراء هو نفسه صاحب رقم الحساب المذكور، كما أنه يعطي للتاجر ضمان بأن حساب المشتري يسمح بشراء هذه السلعة أو الخدمة المراد شرائها دون معرفة البائع برقم البطاقة البنكية الخاصة بالمشتري.

ثانيا: الجهود التشريعية في مكافحة الإرهاب الإلكتروني

رجوعا إلى كون التكنولوجيا ساحة حرب الإرهاب الإلكتروني الذي لا يقف عند حدود جغرافية معينة بل يتعداها دون أن يعترضه حاجز، كان لابدّ على التشريعات بناء منظومة قانونية قوية تتلائم مع أساليب ووسائل مكافحة الإرهاب الإلكتروني أو بتعديلها حتى تصبح أكثر فعالية، لأن التصدي التقني لهذا التهديد لا يكفي بل لابدّ من وجود تشريعات صارمة.

أ- الإطار التشريعي في الولايات المتحدة الأمريكية

تعد التجربة الأمريكية في مكافحة الإرهاب الأقدم وربما الأهم، إذ أنها كانت وعلى مرّ الزمن تحاول تحديد وحصر مفهوم هذه الظاهرة والآليات الفعالة لمكافحته، والجدير بالذكر أن أمريكا قد أصدرت مجموعة من القوانين قبل التاريخ – 11 سبتمبر 2001 – للتحكم في المنظومة الإلكترونية التي ينشط من خلالها الإرهاب الإلكتروني، ففي عام 1984 صدر قانون جرائم الحاسب الآلي الفيدرالي، بناءً على جهود الكونغرس بهذا الخصوص وأطلق على هذا القانون اسم قانون الاحتيال وإساءة استخدام الحاسب الآلي(The computer frond and abuse act)، وتم تعديله مرتين عام 1986 وعام 1994.[24]

بموجب هذا القانون يعتبر الوصول إلى المعلومات الحكومية المصنفة بدون رخصة، من عداد الجنايات، والوصول إلى القيود المالية أو بيانات الائتمان في المؤسسات المالية أو الوصول إلى الحسابات الآلية الحكومية من عداد الجنح، فالمادة (1030) من هذا القانون الذي تناول في الفقرة الأولى جريمة الاحتيال والنشاطات المرتبطة بالاتصال مع الحاسب الآلي، تقضي بمعاقبة كل من يتوصل عن علم وبدون تصريح إلى نظام الحاسب أو استغل فرصة للوصول إليه على نحو غير مصرح به لتحقيق أغراض لا يمتد إليها التصريح الممنوح له إذا تمكن بهذا الأسلوب من استخدام أو تعديل أو تدمير أو كشف المعلومات المخزنة داخله عن علم بذلك، أو منع نظام الحاسب الآلي من القيام بوظائفه المتعددة.

أما الفقرة الثانية من المادة نفسها فقد فرضت عقوبة الغرامة المالية التي لا تتجاوز خمسة ألاف دولار أو على ضعف القيمة التي حصل عليها الجاني أو الخسارة التي سببها بجريمته، أو الحبس لمدة لا تزيد على سنة أو بكلتي هاتين العقوبتين[25].

المادة 223 في الفقرة الأولى قررت العقوبة السابقة على كل من يقوم بعمله وبواسطة وسيلة من وسائل الاتصال بخلق أو تشجيع أو صناعة أو بث أو طلب أو اختراع أو صورة أو أي اتصال يكون فاضحا(Obxene) أو غير أخلاقي (Indecent)وعلما أن المتلقي لم يبلغ 18 سنة.[26]

في عام 1998 تم وضع مشروع القانون الأمريكي لجرائم، الكومبيوتر والانترنت من قبل فريق بحثي أكاديمي والمسمى (Model stat computer crimes) وتم تقسيم الجرائم بموجبه على النحو التالي:

1. الجرائم التي تستهدف الأشخاص.
2. جرائم الاحتيال والسرقة (Froud and theft crimes).
3. جرائم التزوير.
4. جرائم الانترنت ضد الحكومة(Crimes against the gouverment)

ب- الإطار التشريعي في فرنسا

إنّ التجربة الفرنسية في مجال مكافحة جرائم الانترنيت ليس أقل نضجا من التجربة الأمريكية، بل إن فرنسا من أوائل الدول التي تعاملت مع ظاهرة جرائم

الكمبيوتر والانترنيت تعاملا واقعيا، بحيث استجابت مبكرة لما تطلبه هذه الظاهرة الإرهابية من تدابير تشريعية[27] ففي عام 1988 صدر قانون العقوبات الفرنسي حيث تم تجريم الدخول إلى نظام المعالجة الآلية للمعلومات أو البقاء فيها بطريق غير مشروع، وعاقب على ذلك بالحبس مدة تتراوح بين شهرين وعام، وبغرامة من 300 إلى 5000 فرنك أو بإحدى هاتين العقوبتين.[28]

بعدها صدر قانون 1170 لسنة 1990 والذي اشتملت مادته 28 لبيان معنى التشفير وضمان سرية المعلومات والاستيلاء على المعلومات بطريق اختراق التشفير، حيث عرفت التشفير بقولها «كل التسهيلات أو الخدمات التي تهدف إلى النقل أو التحويل وذلك عن طريق ترتيب سرية المعلومات أو الإرشادات الواضحة إلى معلومات أو إشارات مفهومة لأطراف ثالثة، من خلال أجهزة أو برامج تصوره لهذا الغرض وهو الدفاع الوطني والحفاظ على المصالح الداخلية والخارجية وأمن الدولة ».

بعدها صدر المرسوم رقم 92-1358 سنة 1992 والمتعلق بالبلاغات والالتماسات للحصول على إذن الترميز المتعلق بالوسائل والتسهيلات، حيث تحدد مواد هذا المرسوم تفاصيل تقديم وتصدير خدمات أي نوع من أنواع المرافق المشفرة أو بموجبه أيضا لا تعتبر وسيلة من وسائل الترميز إذا كانت الوسيلة تتعلق بأجهزة أو برمجيات خاصة لحماية البرامج من النسخ غير المشروع استخدامها والتي تستفيد من وسائل أو أجهزة سرية، شريطة ألا يسمح التقييد بشكل مباشر أو غير مباشر من خلال البرنامج المعني.

وأخيرا صدر قانون العقوبات الفرنسي الجديد لعام 1994 والذي عالج بدوره تنظيم المعالجة الآلية للبيانات في المادة 323 بفقراتها الأربع، فالفقرة الأولى ذهبت إلى تجريم الوصول أو البقاء بطريقة مخادعة في كل جزء من نظام المعالجة الآلية للمعطيات، وعاقبت بالحبس لمدة عام وبغرامة مالية مئة ألف فرنك، وإذا نتج عن حذف أو تعطيل أو تعديل المعطيات الموجودة في النظام أو تحريض لمجريات النظام، فإنّ العقوبة تكون الحبس لمدة عامين وبغرامة مالية مقدارها مائتي ألف فرنك.

أما الفقرة الثانية فقد حرمت إعاقة النظام وتزوير المعطيات والمعالجة الآلية، وعاقبت بالحبس لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك، والفقرة الثالثة فجرمت فعل كل من يدخل بطريقة مخادعة إلى المعطيات داخل نظام المعالجة الآلي، أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، ويعاقب بالحبس مدة ثلاث سنوات، وغرامة مالية ثلاثمائة ألف فرنك، أما الفقرة الرابعة فقد تضمنت

موضوع الاشتراك والمساهمة في هذه الأفكار، إذ يعاقب الشريك بالعقوبة ذاتها الفاعل الأصلي، وما يسجل بشأن القانون الفرنسي الجديد (قانون العقوبات) أنه جاء خاليا من الإشارة للجرائم المالية والجرائم التي تهدد الشخصية الفردية والجرائم غير الأخلاقية، كما أنه جاء خاليا من تجريم المقامرة عبر الانترنيت والاتجار بالبشر، وجرائم الاختراقات والصناعة ونشر الفيروسات.

في حين نص القانون الجديد على الجرائم التي تقع مباشرة على الشبكة العنكبوتية وهي الجرائم المتعلقة بأنظمة المعالجة الآلية للبيانات وسرية وسلامة توافر البيانات والمعلومات المعالجة آليا، وبهذا الخصوص جرم المشرع الأفعال التالية:

- الدخول غير المشروع أو الوصول الاحتيالي إلى نظام آلي لمعالجة البيانات (المادة 323) من قانون العقوبات الفرنسي الجديد.
- التحريض والتمجيد للإرهاب وما تنص عليه المادة (24) من الجرائم الواقعة على أمن الدولة من القانون الفرنسي.
- الدفاع عن ارتكاب جرائم ضد الإنسانية (المادة 24).

ج- الإطار التشريعي في الجزائر

الجزائر معروفة بتجربتها في مكافحة الإرهاب، إذ أشاد بها المجتمع الدولي بمجموع الإجراءات التشريعية المتخذة في هذا المجال في الجزائر، وتبعا لنفس السياسة الأمنية، تحاول الجزائر مواكبة التطور التكنولوجي بتحصين الترسانة القانونية بمجموعة من الإجراءات في مكافحة الإرهاب الجديد أي الإرهاب الإلكتروني.

رجوعا إلى كون الجزائر تحاول تبني فكرة الاقتصاد الرقمي في تعاملاتها التجارية المستقبلية، وبما أن الإرهاب الإلكتروني ينشط على مستوى المال الإلكتروني من حيث الوسائل، تدارك المشرع الجزائري الفراغ القانوني في مجال الإرهاب الإلكتروني عموما والإرهاب عبر الانترنيت خصوصا بموجب القانون رقم 04-15[29]، المعدل لقانون العقوبات.

نجد المادة(394 مكرر) تجرم كل دخول غير مصرح به عن طريق الغش على المنظومة المعلوماتية، سواء مسّ ذلك الدخول أو البقاء في كامل المنظومة أو جزء منها، أما المادة(394 مكرر 1)، تجرم كل عملية إتلاف وتدمير للمعطيات، وتليها المادة (394 مكرر 2) تجرم كل

عملية استيلاء على المعطيات، كما نصت مواد القسم السابع مكرر من قانون العقوبات، وخاصة المادة(394 مكرر 2) فقرة ثانية على تجريم أفعال الحيازة الإفشاء والنشر التي ترد على المعطيات الآلية، بأهداف المنافسة غير المشروعة، الجوسسة الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة، إضافة إلى ما نصت عليه المادة (394 مكرر 6) بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محل لجريمة من الجرائم المنصوص عليها في القسم السابع من قانون العقوبات.[30]

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة (394 مكرر 6) والمتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة، وإغلاق المواقع والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنيت الذي ترتكب فيه الجرائم بشرط علم مالكه.

أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي:

- حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب النظام.
- إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام.

ولقد دفع القصور الذي عرفه القانون رقم 04-15 والمعدل لقانون العقوبات الذي نص على حماية جزئية نسبية لأنظمة المعلومات، من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى إصدار لقانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

جمع هذا القانون بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصادرها والتعرف على مرتكبيها.[31]

يتضمن القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على 06 فصول أهمها:

- الفصل الثاني الذي جسد أحكام خاصة بمراقبة الاتصالات الإلكترونية، وقد راعى في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، إذ نص القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو بمقتضيات التحريات والتحقيق، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[32]

- أما الفصل الخامس فقد أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة.[33]

يعد القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مجالا شاملا في ميدان مكافحة الإرهاب الإلكتروني، إذ جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب على شبكة الانترنيت، وجهاز الحاسوب الآلي.

وفي هذا السياق من الضروري أن تجتهد الدول العربية في وضع قوانين وطنية لمكافحة الإرهاب الإلكتروني، وأن تسارع في إصدارها نظراً للتزايد الخطير لهذه الظاهرة، وما تحمله من تهديدات وآثار تدميرية على الأفراد والمجتمعات وحقوق الإنسان.

الخاتمة

يتشعب موضوع الإرهاب الإلكتروني في ظل الأمن الدولي والاقتصاد الرقمي، لأن التطور التكنولوجي والتقدم العلمي الذي عرفه العالم المعاصر قد أنعكس على النشاط الإرهابي، إذ باتت المنظمات الإرهابية أكثر تنظيما وأوسع انتشارا، بفضل شبكة الأنترنيت والاتصالات المتقدمة.

الإرهاب الإلكتروني ينشط دون أن يلجأ للعنف المادي أو الجسدي، إنه إرهاب تقني ومخطط له يستند على أسس منهجية، مرتكبوه أشخاص أذكياء مؤهلون علميا وتقنيا، فهم يهدفون إلى نشر الفوضى في البنوك والتحولات المالية العالمية، جمع الأموال

والاستيلاء عليها، إلحاق الضرر بالبنى التحتية وتدميرها، الإضرار بوسائل الاتصال وتقنية المعلومات، وكل هذه التصرفات تعتبر ابتزاز للسلطات العامة والمنضمات الدولية وكذا المنشآت العامة والخاصة، قصد زعزعة نظام التجارة الإلكترونية الذي يمس الاقتصاد الدولي.

يعتبر اعتماد الدول على أجهزة الكمبيوتر وشبكة الانترنيت، عاملا فعالا في فتح المجال أمام الإرهابيين لتحقيق أهدافهم الإجرامية وتدمير منتجات الفكر الإنساني بصورة غير مشروعة بترهيب وإكراه الآخرين، أو بسرقة هويتهم أو التعدي على أملاكهم الافتراضية كالبريد الإلكتروني أو شريحة الهاتف النقال، أو عن طريق التجسس الإلكتروني واختراق أمن المواقع الافتراضية لسرقة المعلومات، تغييرها أو تزويرها.

كل هذه التصرفات تدل على أن الإرهاب الإلكتروني هو إرهاب جديد لا يعتمد على استخدام الأسلحة والمتفجرات، وإنما يستغل التكنولوجيا لدوافع سياسية، اقتصادية واجتماعية ضد أنظمة الكمبيوتر والبيانات، والتحكم في كل ماله علاقة بالتجارة الإلكترونية.

غير أن هذا الخطر القاتل عملت الجهود الدولية على محاربته من خلال محاولة إيجاد اتفاقية دولية شاملة لمكافحة الإرهاب الإلكتروني، و كذا التعاون في مجال نقل التكنولوجيا السليمة ليس كسلطة تجارية تباع لغرض الربح، بل كوسيلة لتوفير الأمن على مستوى العالم بأسره.

والأكيد أن مكافحة الإرهاب الالكتروني لا تكتمل إذا لم يتم تبني آليات داخلية او وطنية قانونية بتحديد أركان جريمة الإرهاب الإلكتروني و تقديمها كقضية متكاملة أمام المحاكم، أما الجانب التقني فيكون باتخاذ مجموعة من التدابير في تشفير البيانات المهمة الموجودة على الأنترنيت، وكذا جهاز الكمبيوتر المربوط بالشبكة العنكبوتية، دون أن نهمل التركيز على تنمية الوعي بالثقافة المعلوماتية وأمنها، والإلمام بالخطر القادم الذي تخلفه أخطاء الثورة الرقمية.

كل هذه الآليات المتخذة تدل على أن العالم دولا وشعوبا أصبح أمام تحد كبير، يتطلب تنسيقا إلكترونيا عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلا على تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذه المشكلة وخاصة مع تعدد أشكال جرائم هذا الإرهاب الإلكتروني الذي يرتبط بالتطورات التي تحدث في مجتمع المعلومات.

لكن هذا التعاون الدولي والداخلي في مكافحة الإرهاب الإلكتروني وحماية التجارة الإلكترونية يظل نسبيا في غياب مفهوم جامع ومانع له، لأن بداية العلاج تكون بتشخيص المرض، فكيف لنا إذن بتحديد آليات وقائية فعالة إذا كنا لا نستطيع تحديد تعريفا للإرهاب الإلكتروني؟ ولا نستطيع حصر الأسباب التي تؤدي إليه؟ وكذا عدم فهم أشكاله المتباينة والمتعددة؟ ذلك أن التجارب الدولية التي تخوضها الدول وعلى رأسها الولايات المتحدة الأمريكية في محاربة هذا النوع الجديد من الإرهاب، خلقت أخطارا جسيمة على النظام الدولي، و حولت استغلال التكنولوجيا من حق في الدفاع إلى انتهاك للحريات الدولية والفردية بالتجسس على التعاملات والمراسلات والاتصالات الدولية، وهو ما جعل الخلط بين الإرهاب الإلكتروني والحق في استعمال التكنولوجيا لأسباب أمنية وسلمية، وأعطى دوافع وحجج إضافية لمجموعات إرهابية متطرفة في استعمال التكنولوجيا لأغراض معادية للسلم والأمن الدوليين.

لكن السؤال الذي يطرح نفسه تلقائيا هو :إذا اعتبرنا أن كل هذه الآليات القانونية كالمعاهدات الدولية المكرسة لمكافحة الجريمة المعلوماتية، تعديل التشريعات الداخلية، وكذا التدابير التقنية، موجهة بشكل شخصي لكل دولة تحاول مكافحة الإرهاب الإلكتروني في سبيل حماية البنى التحتية الخاصة بها، هل فعلا هي أساليب ردعية ناجعة؟ أم مجرد محاولة للحد منه بحكم أنه ينشط على مستوى التكنولوجيا وفي عالم افتراضي لا يتقيد بحدود و لا يعرف تراجعا؟

الهوامش

1. في 11 سبتمبر 2001 تلقت الولايات المتحدة الأمريكية، هجوم من خلال قيام مجموعة ممن يوصفون بالإرهابيين باختطاف أربعة طائرات مدنية بركابها، ثم القيام بضرب مبنى مركز التجارة العالمي والبنتاغون، هذا أدى إلى عقد اتفاقية دولية في بودابست تحت رئاسة الولايات المتحدة الأمريكية والتي أكدت على ضرورة تحديد نوع جديد من الإرهاب يتخطى المفهوم التقليدي وهو الإرهاب الإلكتروني بحكم أن الهجمات كانت باستعمال وسائل تكنولوجية تختلف عن السلاح التقليدي، وأيضا استهداف مبنى المركز التجاري يعلن عن حرب اقتصادية، لهذا كان لابد من تطوير التعاملات التجارية بطريقة أكثر حداثة وغير ملموسة، وهو ما شجع كثيرا وحفز الدول اللجوء إلى التجارة الإلكترونية.

2. http://searchsecurity-techtarget.com

3. أحمد أنور زهران، التكنولوجيا والحرب المعاصرة، دار الوفاء للنشر، القاهرة، 1987، ص 72.

4. لابد من الإشارة إلى أن المجرم الإلكتروني يتمتع بذكاء يفوق المجرم العادي، لأن استعمال الوسائل التكنولوجية لصالحه أو من أجل تحطيمها يتطلب مهارة عقلية معتبرة وكذا إرادة محققة لأن ما يقوم به غير مشروع.

5. نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة ماجستير في القانون، فرع قانون التعاون الدولي، جامعة مولود معمري، كلية الحقوق، تيزي وزو، 2009، ص 19.

6. ECCP لجنة أوروبية أنشأت سنة 1996 لحل مشاكل الإجرام في أوروبا، حيث يمارس المجلس الأوروبي نشاطه في مكافحة الجريمة المنظمة بكل أنواعها، وكذا وضع تقويمات بخصوص التشريعات والممارسات ضد الفساد والجريمة المنظمة.

7. Pitter BELLEY, Hached attacked, Abused digital crime exposed, London, Regan Page, 2002, p 107.

8. Steven FURNELL, Cyber crime vandalizing the information society, London, Addison, cuesely, 2002, p 253.

9. http://ar.wikipidia.org/wiki.

10. محمد الغامدي، الإرهاب الأخطر هو المشكلة التي تواجهها المملكة خلال الفترة المقبلة على الموقع:

http://www.assakina.com/pdf/arabic/text.

11. محمد الغامدي، المرجع نفسه.

12. علي العبيدي، الإرهاب الإلكتروني أحدث صرعة في معارك الصراعات الدولية العابرة على الموقع:

http://www.ibb7.com/pdf/arabic/text.

13. Phylles B-GERSTENFELD, others, Hate on line : Acontent Analyses of Extremist internet. Sitirs, vole 3, n° 01, 2003, pp 29- 44.

14. Alexander YONAH SWETMAN, cyber terrorisme et la guerre de l'information : menaces et réponses, transnationales Publisher, In- us, 2001, p19.

15. حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الالكتروني، رسالة دكتوراه العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، جامعة الجزائر 03، كلية العلوم السياسية والعلاقات الدولية الجزائر 2014، ص 815.

16. القنابل والصواريخ الالكترونية، سلاح حديث متطور يعتمد على مبدأ تفجير قنبلة خاصة تولد نبضات كهرومغناطيسية شديدة تؤثر في الأجهزة الإلكترونية وتعطلها مدة طويلة، كتعطيل الكمبيوترات، أبراج الجوال، مزودات الانترنيت الاتصالات الأرضية...الخ، أي شيء يخص الالكترونات والتقنيات، طبعا هذا النوع من الأسلحة لا يتسبب في خسائر مادية، كانت الولايات المتحدة الأمريكية وروسيا، قد شرعتا بتحري أمور حصلت عليها من اختبارات تفجير قنابل إلكترونية فوق وتحت الأرض، وقد تبين لهما أن النبضة الكهرومغناطسية الشديدة ورمزها (ENIP)التي تتولد لحظة الانفجار خطرة جدا على التجهيزات الالكترونية ويتبعها

مفعول تأبين (Effect lonization) يحد من استخدام الاتصالات مدة قد تصل إلى 72 ساعة.

17. عبد الله بن محمد صالح الشهيري، المعوقات الإدارية في التعامل مع جرائم الحساب الآلي، مذكرة ماجستير في القانون، جامعة الملك مسعود، كلية العلوم الإدارية، 2001، ص 31.

18. حكيم غريب، مرجع سابق، ص 820.

19. ضياء علي أحمد نعمان، «الحماية التقنية للتجارة الالكترونية»، مجلة القانون، العدد الأول، مطبعة وراقة وطنية، مراكش، المغرب 2011، ص 20.

20. المرجع نفسه، ص 21.

21. هدى حامد قشقوش، الحماية الجنائية لتجارة الالكترونية عبر الانترنيت، دار النهضة العربية، الاسكندرية - مصر دون سنة نشر، ص 61.

22. علي كحلول، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الالكترونية بدون دار أو سنة النشر، ص 282.

23. تم تطوير نظام المعلومات الإلكترونية Set بالتعاون بين أكبر شركات البطاقات البنكية وهما شركة(Master card et Visa card)، وذلك نص في تأمين المعاملات المالية عبر شبكة الانترنيت باستخدام البطاقة البنكية، يمثل عملائهما معا أكثر من 8000 مليون، كما انضمت(American axpress) لهذا التحالف ليصبح بذلك أكبر تحالف موجود لتأمين المعاملات الإلكترونية.

24. www.usdoj.gov.criminal/cybercrimie/policy-html

25. Susan. W. BRENNER, state cyber crime ligistation in the united states of America, Availabel: www.richmond.edu.

26. رمضان مدحت، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة-مصر، 2000، ص ص 23 - 24.

27. J.FRAYSSINET, Internet et protection des données personnelles, expertises des systèmes d'information, Avril 1997, p 99.

28. محمد حماد مرهج، جرائم الحاسوب، الطبعة الأولى، إدارة المناهج للنشر والتوزيع، عمان، 2006، ص 179.

29. قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن قانون العقوبات، جريدة رسمية، عدد 17، صادر في 2004/11/10.

30. انظر المواد 394 مكرر 2 ومكرر 6، من القانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات، مرجع سابق.

31. قانون رقم 09-04 مؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، عدد 47، صادر في 2009/02/16.

32. المادة 04 من القانون رقم 09-04، مرجع سابق.

33. المادة 13 و14 من القانون نفسه.

قائمة المراجع

- http://searchsecurity-techtarget.com

- أحمد أنور زهران، التكنولوجيا والحرب المعاصرة، دار الوفاء للنشر، القاهرة، 1987.

- نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة ماجستير في القانون، فرع قانون التعاون الدولي، جامعة مولود معمري، كلية الحقوق، تيزي وزو، 2009.

- ECCP لجنة أوروبية أنشأت سنة 1996 لحل مشاكل الإجرام في أوروبا، حيث يمارس المجلس الأوروبي نشاطه في مكافحة الجريمة المنظمة بكل أنواعها، وكذا وضع تقويمات بخصوص التشريعات والممارسات ضد الفساد والجريمة المنظمة

- Pitter BELLEY, Hached attacked, Abused digital crime exposed, London, Regan Page, 2002.

- Steven FURNELL, Cyber crime vandalizing the information society, London, Addison, cuesely, 2002.

- http://ar.wikipidia.org/wiki

- محمد الغامدي، الإرهاب الأخطر هو المشكلة التي تواجهها المملكة خلال الفترة المقبلة على الموقع:

- http://www.assakina.com/pdf/arabic/text.

- علي العبيدي، الإرهاب الإلكتروني أحدث صرعة في معارك الصراعات الدولية العابرة على الموقع:

- http://www.ibb7.com/pdf/arabic/text.

- Phylles B-GERSTENFELD, others, Hate on line : Acontent Analyses of Extremist internet. Sitirs, vole 3, n° 01, 2003.

- Alexander YONAH SWETMAN, cyber terrorisme et la guerre de l'information : menaces et réponses, transnationales Publisher, In- us, 2001.

- حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الالكتروني، رسالة دكتوراه العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، جامعة الجزائر 03، كلية العلوم السياسية

والعلاقات الدولية الجزائر 2014.

- عبد الله بن محمد صالح الشهيري، المعوقات الإدارية في التعامل مع جرائم الحساب الآلي، مذكرة ماجستير في القانون، جامعة الملك مسعود، كلية العلوم الإدارية، 2001.
- http://neus-neteraft.com
- ضياء علي أحمد نعمان، «الحماية التقنية للتجارة الالكترونية»، مجلة القانون، العدد الأول، مطبعة وراقة وطنية، مراكش، المغرب 2011.
- هدى حامد قشقوش، الحماية الجنائية لتجارة الالكترونية عبر الانترنيت، دار النهضة العربية، الاسكندرية - مصر دون سنة نشر.
- علي كحلول، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الالكترونية بدون دار أو سنة النشر.
- www.usdoj.gov.criminal/cybercrimie/policy-html
- Susan. W. BRENNER, state cyber crime ligistation in the united states of America, Availabel: www.richmond.edu
- رمضان مدحت، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة-مصر، 2000.
- J.FRAYSSINET, Internet et protection des données personnelles, expertises des systèmes d'information, Avril 1997.
- محمد حماد مرهج، جرائم الحاسوب، الطبعة الأولى، إدارة المناهج للنشر والتوزيع، عمان، 2006.
- قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن قانون العقوبات، جريدة رسمية، عدد 17، صادر في 2004/11/10.
- قانون رقم 09-04 مؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، عدد 47، صادر في 2009/02/16.