جامعة مولود معمري – تيزي وزو
كلية الحقوق والعلوم السياسية
قسم الحقوق
مدرسة الدكتوراه للعلوم القانونية و السياسية

الآليات القانونية لمكافحة الإرهاب الإلكتروني

مذكرة لنيل شهادة ماجستير في القانون
تخصص : القانون الدولي للأعمال

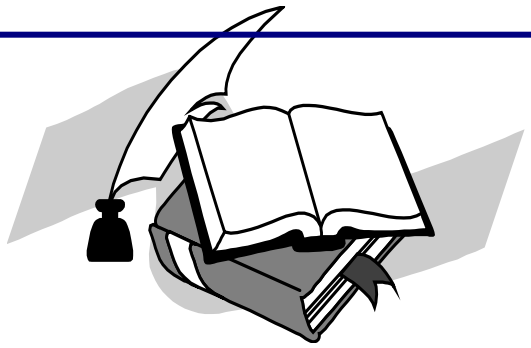
إعداد الطالبة
نجاري بن حاج علي فايزة كريم

إشراف
الأستاذ
أ/د. خلفان كريم

لجنة المناقشة

أ/ د. معاشو عمار، أستاذ، جامعة مولود معمري، تيزي وزو .....رئيسًا؛.
أ/ د. خلفان كريم، أستاذ، جامعة مولود معمري، تيزي وزو ..مشرفا ومقررا؛.
أ/ د. تاجر محمد، أستاذ، جامعة مولود معمري، تيزي وزو .....ممتحنا..

إهداء



إلى عائلتي الكريمة و على رأسهم والدي

أطال الله عمرهما

الى أصدقائي و زملائي

الى كل من ساعدني في إنجاز هذا العمل

من بعيد أو من قريب و أفادني ولو بكلمة

طيبة.

فايزة نجاري بن حاج علي

كلمة شكر و تقدير

أشكر الله سبحانه و تعالى على فضله أن يسّر لي إتمام هذه المذكرة.

اعترافًا بالفضل والجميل أتوجّه بخالص شكري و وامتناني مع كل إحترامي إلى الأستاذ

الدكتور خلفان كريم

الذي تفضّل بالأشراف على هذا العمل وتابعه بالتصويب في جميع مراحل إنجازه

فجزاه الله عني كلّ الخير.

نجاري بن حاج علي

فايزة

قائمة المختصرات باللغة الإنجليزية

EDI: Interchange **E**lectronic **D**ata.

VAN: Valu **A**dded **N**etwork.

ECCP : European **C**ommittee on **C**rime **P**roblems.

WAR : Wgite **A**ryan **R**esistance.

EMP : Electro **M**agistic **P**uls.

OECD : Oranization for **E**conomic **C**ooperation and **D**evlopment.

WOT : Wold **T**rade **O**rganisation.

ICC : International **C**hamber of **C**ommerce.

مقدمة

عاشت البشرية ثورتين غيرتا التاريخ وطبيعة الحياة البشرية هما: الثورة الزراعية والثورة الصناعية، غير أن العالم أصبح اليوم يشهد ثورة جديدة قوامها المعلوماتية، زيادة الإنتاج وسرعة اتخاذ القرارات وهي الثورة التكنولوجية.

يأتي في مقدمة هذه الثورة التكنولوجية 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)، وأمام هذا التحول التكنولوجي، بدأت الطرق التقليدية في مختلف التعاملات خاصة التجارية منها تتلاشى شيئا فشيئا لأنه لم يعد بمقدورها تلبية حاجات المستفيدين، لتتحول الى تعاملات تجارية رقمية وهي إحدى مواضيع الاقتصاد الرقمي وتقنية المعلومات أو صناعة المعلومات في عصر الحوسبة والاتصال.

بتقدم التكنولوجيا، تقدمت الصناعة ووسائل الإتصال بين الدول والشعوب الأمر الذي ساعد على معرفة المستهلكين ورغباتهم بفضل وسائل الإعلام المختلفة وهذا ما دفع الإنسان إلى الرغبة في إقتناء هذه التكنولوجيا الحديثة، قصد الوصول بين البائع والمستهلك وهو السبب الفعلي لوجود التجارة الإلكترونية.

ومع تطور التجارة الإلكترونية كما وكيفا، برزت الحاجة إلى ضرورة إيجاد تنظيم قانوني يحكم هذه التجارة من حيث كيفية التعاقد وحفظ حقوق المتعاقدين وإثباتها، وكذلك الحماية الجنائية لهذه التجارة والمتعاملين بها ،هذه الحاجة بدأت منذ بداية ظهورها من القرن الماضي، حيث كانت التجارة الإلكترونية تعتمد على نظام واسع من التكنولوجيا لتبادل المعلومات إلكترونا يسمى(EDI)[1] ، وذلك لتسهيل عملية الإتصال بين اطراف المبادلة التجارية وإختزال العمليات الورقية، وكذا عدد الأفراد المتعاملين، وكانت طريقة (EDI) تعتمد على شبكة معلومات تسمى(VAN)[2] بمعنى شبكة القيمة المضافة، وعن طريق التخاطب مابين(EDI) وشبكة (VAN)يتم الإتصال المباشر بأجهزة الحاسب الآلي لدى الشركاء عن طريق صندوق بريد إلكتروني.

[1] - http://www.edipourtous.fr/ce-qu-est-l-edi

[2] - http://wwwhttp://definition.actufinance.fr/valeur-actuelle-nette-van-757/.

نمت التجارة الإلكترونية نموا هائلا وسريعا، انعكس على حجم المبادلات التجارية التي تتم من خلالها، وذلك في فترة قصيرة نسبيا، هذا ما جعلها –التجارة الإلكترونية– السمة البارزة كتجارة العصر، بينما أصبحت شبكة الانترنيت مركزا تجاريا يتسع لجميع سكان الأرض، حيث يتم من خلالها تبادل السلع والخدمات وعرض المنتجات للبيع، من خلال ما يعرف بالمتاجر الافتراضية التي احتلت مواقعها صفحات الويب (WEB)[3].

هذا النوع من التجارة وفر الجهد وقلل من المصاريف والنفقات، كما انه أتاح للمستكشف والباحث زيارة المواقع المختلفة على الشبكة العالمية، وتمكنه من تصفح وقراءة ما بها من صفحات والحصول على ما يريد من معلومات أو صور أو مقطوعات غنائية أو طلب السلعة التي يريدها دون أن يبرح مكانه، كما تمكنه من البيع والشراء وإبرام الصفقات التجارية في أي وقت وعلى مدار الساعة.

لكن هذه الثورة التكنولوجية التي كانت السبب في وجود التجارة الإلكترونية، كان لها سلبيات – كغيرها من الثورات الأخرى– في ظهور مجموعة من الأفراد يسيئون استخدام وسائل التكنولوجيا لخدمة العمليات الإرهابية، سواء كان 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 ب"الإرهاب الإلكتروني" بالعاصمة المجرية بودابست، عقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر من العام نفسه[4].

---

[3] - http://www.aidice-web.com/accueil/definition-site-web.php

[4] – 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 أدىإلى عقد اتفاقية دولية في بودابست تحت رئاسة الولايات المتحدة الأمريكيةوالتي أكدت على ضرورة تحديد نوع جديد من الإرهاب يتخطى المفهوم التقليدي وهو الإرهاب الإلكتروني بحكمأن 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 اللجوءإلى التجارة الإلكترونية.

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.

بالعودة إلى اعتبار التجارة الإلكترونية وليدة التطور التكنولوجي وتقنية المعلومات فإنهما ساهما فعلا بانتشار الشبكة المعلوماتية الانترنيت، خاصة مع استخدام الحاسب الآلي وتطبيقاته في مجال الحوكمة الإلكترونية والتجارة الإلكترونية بكل أنشطتها وخدماتها، كما هو الحال في الدول الأوربية وبعض الدول العربية كدولة الإمارات العربية المتحدة، لكن من جهة أخرى التطور التكنولوجي وتقنية المعلومات ساهما أيضا في عولمت 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.

تبرز أهمية دراسة الموضوع من خلال دراسة الأهمية المتنامية التي توليها الدول لخطورة جرائم الإرهاب الإلكتروني في الوقت الراهن على التجارة الإلكترونية باعتباره ظاهرة عالمية، أخذ بالإنتشار والتوسع بشكل خطير يؤثر سلبا على كل التعاملات الإلكترونية، وكذا أهم الطرق الدولية و الداخلية المعتمدة لحماية تجارتها الإلكترونية من الإرهاب الإلكتروني.

على ضوء ما تقدم، فإن إشكالية دراستنا تنحصر في: **البحث في الآليات الدولية والوطنية المكرسة للحد من خطر الإرهاب الإلكتروني الذي يهدد تعاملات التجارة الإلكترونية بطريقة مباشرة و خطيرة؟**

اعتمادا على المنهج التحليلي الذي يتلاءم و دراسة الإشكالية المطروحة، قسمنا الموضوع الى فصلين: نعالج مفهوم كل من التجارة الإلكترونية و الإرهاب الإلكتروني في بعض التعاريف الفقهية و القانونية على الصعيدين الدولي و المحلي و إضهار خصائص كل منهما، ثم تبيان العلاقة الموجودة بينهما من خلال شرح كيفية تأثير الإرهاب الإلكتروني سلبا على التجارة الإلكترونية و الذي أصبح يعتبر أهم معوق لها في**(الفصل الاول)**.

ثم نتناول واقع الجهود الدولية و الوطنية لمكافحة الإرهاب الإلكتروني من خلال التطرق أولا: الى أهم أساليب التعاون الدولي في المجال التقني كإحدى الآليات لمكافحة الإرهاب الإلكتروني، دون ان نغفل على دور بعض المنظمات الدولية التي كرست مجموعة من الجهود لحماية و تفعيل التجارة الإلكترونية الدولية، ثم نأتي الى الجهود الوطنية الشريعية التي جرمت أولا أعمال الإرهاب الإلكتروني ثم حددت مجموعة من العقوبات لها في **(الفصل الثاني)**.

الفصل الأول

علاقة التجارة الإلكترونية بالإرهاب الإلكتروني

تمثل التجارة الإلكترونية واحدا من مواضيع ما يعرف بالاقتصاد الرقمي (**Digital Economy**)، حيث يقوم الاقتصاد الرقمي على حقيقتين: التجارة الالكترونية وتقنية المعلومات؛ فتقنية المعلومات في عصر الحوسبة والاتصال هي السبب الفعلي والحقيقي للتجارة الإلكترونية، باعتبارها تعتمد على مختلف وسائل التقنية لتنفيذ وإدراج النشاط التجاري، هذا ما يجعل العالم يندمج مع بعضه البعض، وكذا تحرر الفرد تدريجيا في تعاملاته التجارية من قيود المكان ليبدو وكأنه موجود في أكثر من مكان في نفس الوقت.

يقابل هذا التحرر التكنولوجي ظهور نوع جديد من الجرائم المسماة ب ـــ"**الجرائم التكنولوجية**"، نتيجة للاستخدام الغير القانوني لوسائل التكنولوجيا (الهاتف، الأنترنيت،الأقمار الصناعية... الخ)، وهي العوامل نفسها التي أدت إلى عولمة هذه الظاهرة لاسيما تلك التي ترتكز أساسا على المجرم الالكتروني المدفوع إلى ارتكاب الأفعال المجرمة في مجال التكنولوجيا من تهديد وترويع، تؤثر سلبا على التطور التكنولوجي خاصة ما كان منها يستخدم في مجال التجارة الإلكترونية، حيث برزت هذه الأخيرة – التجارة الإلكترونية – كأحد أهم الروابط التي قربت العالم وجعلته كتلة واحدة، يسعى إلى تحقيق أهداف الربح في وقت قصير عبر أنحاء العالم، هذا ما سيتم تناوله بمزيد من التفصيل بتحديد ماهية التجارة الإلكترونية والإرهاب الإلكتروني (**المبحث الأول**)، ثم تبيان مخاطر هذا التهديد الجديد أي الإرهاب الإلكتروني على التجارة الإلكترونية (**المبحث الثاني**).

المبحث الأول

ماهية التجارة الإلكترونية والإرهاب الإلكتروني

أدت ثورة المعلومات التي يشهدها العالم في مجال الاتصالات وتكنولوجيا الحاسب الآلي وتنظيم المعلومات، إلى إحداث تغيير مستمر في طبيعة الآليات والعلاقات التي تحكم التعامل بين الأفراد، وتعد شبكة الانترنيت دليلا ملموسا وفعالا وواضحا لهذه الثورة، فانتشارها الهائل جعل منها إحدى أبرز التقنيات الحديثة التي فرضت نفسها على المستوى العالمي وفي مختلف المجالات، منها التعاملات التجارية التي تبنت هذا التطور التكنولوجي لتعمد إلى إنشاء أو خلق ما يسمى بالتجارة الإلكترونية (**المطلب الأول**)، إلا أن هذا التطور في التعاملات التجارية، قوبل بظهور طائفة ترغب في تدمير السوق

الإلكترونية بوسائل وطرق غير قانونية، إذ أساءت استعمال الأسباب التي أدت إلى ظهور التجارة الإلكترونية، وخلق الإرهاب الإلكتروني **(المطلب الثاني)**.

المطلب الأول

مفهوم التجارة الالكترونية

تعتبر التجارة الالكترونية إحدى أهم إنتاجات تواصل تكنولوجيا الاتصالات بالشبكة المعلوماتية العالمية الأنترنيت، وقد ظهرت ملامح هذه التجارة في أول التسعينات عندما استقرت الشبكة العنكبوتية كآلية لممارسة مختلف التعاملات الإلكترونية عبر العالم.

أصبحت التجارة الإلكترونية في فترة وجيزة السمة البارزة لتجارة العصر، بسبب التطور المذهل والسريع للتكنولوجيا والتي قابلها الاستعمال الهائل للأفراد نتيجة الاختزال الرائع والسريع للمكان والوقت، وعليه سيتم تعريف التجارة الإلكترونية **(الفرع الأول)** ثم التطرق إلى تبيان خصائص هذا النوع الجديد من التجارة الرقمية **(الفرع الثاني)**.

الفرع الأول

تعريف التجارة الإلكترونية

يعود ظهور النشاط التجاري الإلكتروني إلى التسعينات من القرن العشرين، كانت تعرف باسم التبادل الإلكتروني، واقتصرت في البداية على تبادل بيانات البيع والشراء بين المؤسسات الكبيرة على الشبكات الإلكترونية الخاصة، أما المصاريف فقد استعملت ما يعرف بنظام تحويل الأموال الإلكترونية بهدف تحسين خدماتها المالية، وفي أواخر القرن العشرين عوضت الانترنيت شيئا فشيئا نظام تبادل المعلومات الإلكتروني المستعمل من طرف المؤسسة[1]، إلى أن وصلت في صورتها الحالية أو إلى ما هي عليه اليوم.

موضوع التجارة الإلكترونية ليس حديث النشأة، ولكنه حديث الساعة بحكم الأهمية التي تكتسبها مجموع المعاملات الاقتصادية في هذا النموذج التجاري المتطور على اقتصاد السوق العالمية، وهو ما دفع كيانات قانونية دولية تتبنى هذه التجارة ضمن أجندة أعمالها بداية بتعريفها، نذكر منها التعاريف الواردة في بعض المنظمات الدولية، تعاريف في بعض الهيئات الإقليمية ثم على الصعيد الداخلي.

أولا – تعريف التجارة الإلكترونية في بعض المنظمات الدولية:

تعتبر المنظمات هيئات دولية ذات سلطة قانونية معتبرة، تؤثر وتتأثر بالتكنولوجيا لدرجة أن بعض الفقهاء في علم السياسة والاقتصاد جعلوا منها المحرك الرئيسي للمجتمع

[1] – رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 1999، ص 16.

الدولي، انطلاقا من هذا يمكن القول فعلا أنها محفز للتطور التكنولوجي، فمعظم هذه المنظمات تخلت تدريجيا عن الأساليب التقليدية في مختلف تصرفاتها، وتبنت التكنولوجيا كبديل لتجعل من العالم قرية صغيرة.

رجوعا إلى كون التجارة الإلكترونية هي أحد محفزات عمل هذه المنظمات الدولية جعلت هذه الأخيرة –المنظمات الدولية– مجموعة من القوانين والأسس للعمل بهذه التجارة وكذا حمايتها من المخاطر التي تهددها كالإرهاب الإلكتروني، والبداية كانت بمحاولة إعطاء تعريف لهذا النوع الجديد من التجارة وتجسيدها دوليا.

أ– منظمة الأمم المتحدة (United Nations):

تعتبر الأمم المتحدة من أهم المنظمات الدولية التي اهتمت بتنظيم التجارة الإلكترونية إذ اعتمدت بتاريخ 16 ديسمبر 1996 قانون الأنسترال النموذجي بشأن التجارة الإلكترونية الذي حدد كل من ماهية النشاط التجاري والوسيلة الإلكترونية التي تستخدم لإبرامه، وتنص مادته الأولى على ما يلي « ***ينطبق هذا القانون على أي نوع من المعلومات، يكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية*** » وفي الوقت نفسه تضمن دليل تشريع هذا القانون أنه ينبغي تفسير هذا المصطلح "أنشطة تجارية" تفسيرا واسعا، حيث يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجاري سواء التعاقدية منها أو غير التعاقدية، وتشمل بذلك: التمثيل أو الوكالة التجارية، الخدمات الإستشارية، الأعمال الهندسية، الرخص، الإستثمار، الأعمال المصرفية، التأمين، الإتفاق أو امتياز الإستغلال وغيرها من أشكال التعاون التجاري.

أما المادة الثانية حددت تعريف مصطلح البيانات الإلكترونية في الفقرة (ب) على أنها « **البيانات الإلكترونية هي المعلومات** ***التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني، أو التلكس أو البرق أو النسخ البرقي*** »[1].

---

[1] – قانون الأنسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996، على الموقع:
http://www.uncitral.org/pdf/arabic/texte/electcom/ml-ecomm-aebook.pdf.
وراجع أيضا: بن غرابي سامية، عقود التجارة الإلكترونية ومنهج تنازع القوانين، مذكرة ماجستير في القانون، فرع قانون التعاون الدولي، جامعة مولود معمري، كلية الحقوق، تيزي وزو، 2009، ص 05.

هذا يعني أن هيئة الأمم المتحدة رغم أنها أول الهيئات التي اهتمت بتنظيم المعاملات التجارية الإلكتروني، إلا أنها لم تعط تعريفا صريحا لها بل تركت المجال مفتوح حتى لا يقتصر فقط على التعاملات التجارية التي تتم عبر شبكة الانترنيت، بل يشمل ذلك جميع المبادلات الإلكترونية باستخدام جميع الوسائل الإلكترونية.

وعليه، يمكن تعريف التجارة الإلكترونية في إطار قانون الأنسترال النموذجي بأنها « ***جميع الأنشطة التجارية التي تتم عبر المبادلات الإلكترونية باستخدام جميع الوسائل الإلكترونية*** ».

ب – منظمة التجارة العالمية (WOT):

قامت المنظمة العالمية للتجارة منذ سنة 1998 بدراسة حول التجارة الإلكترونية بعنوان "التجارة الإلكترونية وقواعد المنظمة العالمية للتجارة (Electronic commerce and the role of WOT) وتوصلت إلى اعتبار التجارة الالكترونية ضمن أنشطة التجارة التي تستوعبها وتطبق عليها قواعد الإتفاقية الدولية الخاصة بالتجارة في الخدمات[1].

حددت المنظمة العالمية للتجارة موقفها الرسمي من التجارة الالكترونية في مؤتمرها المنعقد في شهر أكتوبر عام 1998، عندما أعلن مديرها العام في ذلك الوقت(Renata ROGGIERO) أن المنظمة لا تسعى لوضع قواعد جديدة للتجارة الإلكترونية، وإنما تسعى إلى استخدام التنظيم القانوني القائم والمحدد ضمن اتفاقية الغات الخاصة بالتجارة واتفاقية تريبس، والإتفاق الخاص بخدمات الإتصال.

عرفت المنظمة العالمية للتجارة (WOT) التجارة الإلكترونية بأنها « ***عملية إنتاج وتوزيع للمنتجات من خلال شبكة الإتصال*** »[2]، وهذا التعريف يفيد أن التجارة الإلكترونية تتم من خلال شبكة الإتصال ولا تقتصر على الأنترنيت.

ج – منظمة التعاون الإقتصادي والتنمية (OECD):

كرست منظمة التعاون الاقتصادي والتنمية (OECD) سنة 1998 أعمالها بشكل رئيسي للتجارة الإلكترونية، انطلاقا من قناعة أجزتها بأن تلك التجارة تتطلب حلولا دولية في مرحلة تنظيمها، على أساس الحلول المتباينة لا تتفق مع الطبيعة الكونية لهذا النمط من الأعمال، ولأن هذا التباين يقيم حدودا لا تقبلها التجارة الإلكترونية، فمن أبرز

---

[1] – سعد عبد الله أنور، مبادئ المنظمة العالمية للتجارة (WOT)، الطبعة الثانية، دار وائل للنشر والتوزيع، عمان، 2009، ص 43.

[2] – Emmanel ROUCOUNAS, Facteurs privées et droit international public, Recueil des cours, académie de la haye Volume 299, Martinus NIJHOFF, 2002, p 305.

أنشطة المنظمة في ميدان التجارة هو المؤتمر العالمي للتجارة الإلكترونية الذي عقد في فترة ما بين 7-09 أكتوبر 1998 في مدينة أوتاوا، حيث توصل المؤتمر إلى إقرار آليات عديدة حدد من خلالها مناطق الإهتمام القانونية الرئيسية[1]، أهمها:

- أن تضع الدول في حسبانها بالنسبة لتشريعها المحلي القواعد المتصلة لحماية الخصوصية والحريات الفردية المنصوص عليها في الإرشادات الموجودة بملحق هذه التوصية التي هي جزء لا يتجزأ منها.

2 - يجب على الدول الأعضاء إزالة وتجنب وضع عواقب غير مبررة أمام الإنسياب المتسلسل للبيانات الشخصية، بحجة حماية الخصوصية.

3 - على الدول الأعضاء التعاون في تنفيذ الإرشادات الملحقة بهذه التوصيات.

4 - أن تقوم الدول الأعضاء بالاتفاق بقدر الإمكان على إجراءات معينة للتشاور والتعاون من أجل تطبيقها.

وقد عرفت هذه المنظمة التجارة الإلكترونية في تقرير صدر عنها بأنها « ***جميع أنواع الصفقات التجارية التي تعقد، سواء بين الإدارات أو الأفراد عن طريق المعالجة الإلكترونية للبيانات أيا كانت تلك البيانات، مقروءة أو أصوات أو صور مرئية*** »[2]، وقد بين هذا التقرير أن هذه التجارة سوف تسيطر على كافة الأنشطة التجارية كالإعلانات، وتقديم المعلومات عن السلع والخدمات مجانا، وقد تكون صفقات تجارية كما هو الحال في العقود الإلكترونية.

ثانيا - تعريف التجارة الإلكترونية على المستوى الإقليمي والهيئات المتخصصة:

تبعا للمنظمات الدولية، فإن بعض الهيئات الإقليمية مثل الاتحاد الأوروبي (EU) تبنى التعامل بالتجارة الإلكترونية من أجل اختزال الوقت وزيادة نسبة الربح، وكذلك المعهد الدولي لتوحيد القانون الخاص غرفة التجارة الدولية.

أ - الإتحاد الأوروبي (European Union):

يعتبر دور الإتحاد الأوروبي في صياغة قواعد موحدة للدول الأوربية مميز إذ يظهر ذلك في التشريعات التجارية والإقتصادية، وتميز هذا الدور في أنه أسند إلى دراسات قامت بها جهات متعددة لها خبرة كبيرة في مجال التعاقد الإلكتروني، وبناء عليها أصدر هذا الإتحاد العديد من التوصيات بشأن التجارة الالكترونية.

---

[1] - محمود لطفي، دور المنظمات الدولية في تسيير صندوق النقد الدولي، دار الثقافة للطباعة والنشر، القاهرة، مصر، 2009، ص ص 27 - 29.

[2] - محمود لطفي، المرجع السابق، ص 35.

بدأت مبادرة المفوضية الأوربية بوصف التجارة الإلكترونية بأنها « ***كل الأعمال التجارية التي يتم إنجازها إلكترونيا وتقوم على معالجة ونقل البيانات سواء نصية مسموعة أو مرئية، والمزادات التجارية على الشبكة والمناقصات العامة والتسويق الآلي المباشر للمستهلكين، وكذا التبادل الإلكتروني للسلع والخدمات والنقل الإلكتروني للأموال، وكل المنتوجات كالسلع الإستهلاكية، برامج الكومبيوتر، التعليم عن بعد، والمراكز التجارية الإفتراضية... الخ*** »[1].

وقد نصت المادة الأولى من التوجيه الأوربي رقم(7/97) بشأن حماية المستهلك فيما يتعلق بالعقود المبرمة عن بعد أن « ***أن موضوع هذا التوجه هو التقريب بين القوانين واللوائح والأحكام الإدارية الخاصة بالدول الأعضاء فيما يتعلق بالتعاقد عن بعد بين المستهلكين والموردين*** »[2].

بينما حددت المادة (2/2) المورد أو التاجر بأنه أي شخص طبيعي أو معنوي يبرم عقودا تتعلق بتجارة أو مهنة، وحددت أيضا وسائل الإتصال عن بعد وهي الوسيلة التي يمكن أن يستخدمها دون الوجود المادي للمورد أو المستهلك في مكان واحد عند العقد بينهما.

وإضافة إلى ما سبق أصدر الإتحاد الأوربي توجيه رقم(31/2000) بخصوص جوانب قانونية معينة لخدمات مجتمع المعلومات وخاصة التجارة الإلكترونية في السوق الداخلية، حيث أكد واضعوه على أن الإتحاد يسعى نحو وضع علاقات أوثق بين دول أوربا من أجل التأكد على التقدم الإقتصادي والإجتماعي، إذ عالجت (المادة 90) منه مسألة إبرام العقود إلكترونيا وتنص على أنه « ***يجب على الدول الأعضاء أن تتأكد من أن نظامها القانوني يسمح للعقود بأن تبرم بواسطة الوسائل الإلكترونية، ويجب على الدول الأعضاء أن تتأكد على وجه الخصوص أن القواعد القانونية الواجبة التطبيق في العملية التعاقدية لا تؤدي إلى عوائق أمام إبرام العقود الإلكترونية، ولا تؤدي إلى حرمان تلك العقود من الفعلية القانونية والصلاحية بحجة أنها أبرمت بالوسائل الإلكترونية*** ».

---

1 – Jean-Christophe FINIDORI, Marketing direct sur internet, international Thomson publishing, Paris, 2001, p 55.

22 – Jean-Christophe FINIDORI, Op.Cit., p 61.

ب – غرفة التجارة الدولية (ICC) :

كان لغرفة التجارة الدولية دور هام وفعال في مؤتمر منظمة التعاون الاقتصادي والتنمية (OECD) بشأن التجارة الإلكترونية، حيث قدمت العديد من الإرشادات والنماذج للقوانين والدراسات البحثية التي كان لها الدور الأكبر في تعميق مسائل البحث وصياغة نتائجه وتوصياته بشكل فعال.

بدأت الغرفة منذ 15سبتمبر 2003 بصياغة دليل إرشادي (Manuel)، عبارة عن قواعد اختيارية لمساعدة الشركات على التفاوض إلكترونيا، وأطلقت عليه اسم "**المصطلحات الالكترونية لعام 2004**" والتي أصبحت سارية المفعول في 2006، ويعد هذا الدليل أحد أهم الأدلة الشاملة التي تتيح المساعدة الفعالة في مجال الأنشطة التشريعية والتنظيمية للأزمة التجارة الإلكترونية، وقد تم تعزيز هذا الدليل بكتيبات إرشادية لاحقة أكثر تخصصا ابتداءا من عام 2005، حيث تتسم بالطابع المكمل للدليل الإرشادي، ومنها الدليل الخاص بالأنشطة الإعلامية على الانترنت[1].

الجدير أن غرفة التجارة الدولية لم تعط تعريف كغيرها من الهيئات والمنظمات الدولية، ولكنها كانت السبب في إيجاد تعريف من خلال منظمة التعاون الاقتصادي والتنمية عن طريق مجموع الدراسات والإرشادات لتجسيد وتفعيل دور التجارة الإلكترونية، إذ أن غرفة التجارة الدولية منظمة غير حكومية مقرها باريس تهدف إلى وضع قوانين دولية موحدة في ميدان العمل التجاري، عبر ما يعرف بنشرات الغرفة، وتركز على توحيد القواعد ذات العلاقة بالأنشطة القانونية التي تتم عبر الحدود الوطنية للدول، ولها قطاع آخر من النشاط والعمل يتمثل في القيام بأنشطة فض النزاعات التجارية الدولية عن طريق التحكيم أو محكمة التحكيم التابعة للمنظمة في عضويتها 63 دولة، ويلجأ إليها حوالي 700 شركة من حوالي130 دولة[2] لفض منازعاتهم التحارية.

ثالثا – تعريف التجارة الإلكترونية وفقا للتشريعات الوطنية:

لقد كان للعديد من الدول جهودا مميزة بشأن سن قواعد قانونية للتجارة الإلكترونية وتضمينها لتعريف خاص بها، نذكر منها:

---

[1] – نعمان العياش، التجارة الإلكترونية: أداة للمنافسة في الأسواق العالمية، دار الراتب الجامعية للطباعة والنشر، بيروت لبنان، 2010، ص 96.

[2] – الموقع الرسمي لغرفة التجارة الدولية www.icc.org

أ – تعريف المشرع الأمريكي:

تعتبر الولايات المتحدة الأمريكية من بين الدول التي تشجع على ممارسة التجارة الإلكترونية، فقد تضمن التقنين الأمريكي الموحد (Uniform Commercial Code (UCC) لعام 1978، وقبل ظهور الأنترنت، تعريف للعرف التجاري في الجزء (7/303)

بأنه: « ***أية ممارسة أو طريقة تتبع في مكان ما أو حرفة ما وتطبق عادات أو أعراف معينة*** » بينما الجزء (31/201) الخاص بالتعريفات، أشار إلى ماهية السجلات القانونية حيث نص على أن المقصود بها: « ***المعلومات المكتوبة على أي وسيط ملموس أو مادي أو المخزنة على أي وسيط إلكتروني أو ما شابهه، ويمكن استرجاعها في صورة ملموسة*** »[1].

بعد ظهور الأنترنت ازداد اهتمام الولايات المتحدة الأمريكية بوضع تنظيم قانوني يناسب عالمية استخدامها، حيث أصدرت العديد من التشريعات الفدرالية، من أهمها القانون الفدرالي الموحد لمعاملات معلومات الكمبيوتر لعام 1999، الذي عرف التاجر في المادة (45) من الجزء 102 بأنه الشخص الذي يقوم على سبيل الإحتراف بعمل من الأعمال التالية:

1 – جمع المعلومات.

2 – ممارسة أي مهنة أو حرفة.

3 – تشغيل العاملين وتوظيفهم.

أما بالنسبة للفظ "الإلكتروني" فقد عرفته المادة (26) من الجزء 102 من هذا القانون بأنه « ***كل ما يصل التكنولوجيا بوسيط إلكتروني، له قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية كهرومغناطيسية أو أي قدرات مماثلة*** ».

ومتابعة لاهتمامات الولايات المتحدة الأمريكية بالجوانب القانونية للتجارة الإلكترونية نجد أنها أصدرت عام 2000، القانوني الفدرالي الأمريكي بشأن التوقيعات الإلكترونية في التجارة العالمية والمحلية، حيث حددت المادة (3) من الجزء 106 مصطلح عامل أو وسيط إلكتروني بأنه يعني « ***برامج الكومبيوتر أو أي وسيلة إلكترونية أو أية وسيلة أوتوماتيكية أخرى، تستخدم على نحو مستقل من أجل بدء عمل***

[1] – دوج جيرلاش، الحوكمة الإلكترونية والتجارة الإلكترونية، دار العفيون للترجمة والنشر، سوريا، 2009، ص 109 و110.

معين أو استجابة معينة لمستندات إلكترونية، أو أي أداء لكل أو في جزء منه دون مراجعة أو تدخل من شخص في وقت أداء هذا العمل »[1].

كما تناولت المادة (8) من الجزء 106 تعريف التاجر حيث تنص على أنه أي فرد أو شركة ذات المسؤولية المحدودة أو وكالة حكومية أو مؤسسة عامة أو أي كيان قانوني أو تجاري آخر، وعند استقراء نصوص هذا القانون نجد أن المادة (13) من الجزء (106) تناولت اصطلاح التجارة ضمن مفهوم الأعمال التجارية، ونصت على أن « ***مصطلح صفقة يعني كل الأفعال المتصلة بنشاط تجاري أو أكثر على نحو يشتمل أي فعل مما يلي:***

1 – بيع أو تأجير أو تبادل أو انتقال للمعلومات الشخصية بما في ذلك البضائع والأشياء غير الملموسة، والخدمات وأي خليط من هذه الأشياء.

2 – بيع أو تأجير أو تبادل أو أي تصرف في أية ممتلكات فعلية أو خليط من هذه الأشياء ».

ويلاحظ على هذا التعريف أنه لم يفرق بين المعاملات التعاقدية وغير التعاقدية، وكذلك لم يميز بين المعاملات المدنية والتجارية.

ب – تعريف المشرع الفرنسي:

أوجدت فرنسا منذ سنة 1987 نظام قانوني للتجارة الإلكترونية، إذ في السنة نفسها المذكورة أعلاه صدر قانون حماية المستهلك بشأن الثمن في المادة (14) منه على « ***ثمن كل سلعة أو خدمة معروضة على المستهلك وفق تقنية اتصالات عن بعد يجب أن يكون ظاهرا بشكل واضح بالنسبة للمستهلك بأي وسيلة قبل إنشاء العقد*** »، من أمثلة تلك التقنية الهاتف والفاكس، وهذا النص يوجد حتى قبل ظهور الأنترنت، إلا أنه قابل للتطبيق على العقود التي تتم من خلالها.

وتأكيدا على رغبة المشرع الفرنسي في تنظيم المعاملات الإلكترونية، نجد أنه أدخل عدة تعديلات على القانون المدني، وذلك من خلال القانون رقم(2000/230) الصادر بتاريخ 13 مارس 2000، حيث نصت (المادة 1/1316) على أن « ***الوثيقة التي شكلها الالكتروني تكون مقبولة كدليل بنفس طريقة الوثيقة الورقية، بشرط أن تساهم بالتعرف على هوية مرسلها، وتخزن في ظرف تحافظ على سلامتها*** » أما الفقرة الثالثة من تلك المادة فتنص على أن « ***الوثيقة الالكترونية لها نفس قيمة الوثيقة الكتابية***

---

[1] – دوج جيرلاش، مرجع سابق، ص 115.

»[1]، وتفاعلا مع النهج ذاته بموجب القانون رقم (2004/575) بتاريخ 21 يونيو 2004 تم تعديل المادة رقم (1/1369) من القانون المدني الفرنسي لتصبح كالتالي « ***إن الوسيلة الالكترونية يمكن أن تستخدم من أجل تحديد الظروف التعاقدية أو المعلومات الخاصة بالبضائع والخدمات*** »[2].

إن المشرع الفرنسي لم يضع تعريفا صريحا للتجارة الإلكترونية، إلا أن تقرير وزارة الإقتصاد الفرنسية في يناير 1998 حدده بأنها « ***تشمل مجموع المعاملات الرقمية المرتبطة بأنشطة تجارية بين الشركات بعضها البعض أو بينها وبين الأفراد، أو بينها وبين المؤسسات الإدارية*** »[3]، وبهذا نجد أن التقرير تبنى تعريفا موسع للتجارة الإلكترونية بما فيها الأنشطة البنكية التي تساهم في إبراز المعاملات التجارية عن طريق أنظمة الدفع الإلكتروني.

ج – تعريف المشرع الجزائري:

توجد في الجزائر بعض القوانين التي تمس بشكل أو بآخر مفهوم التجارة الإلكترونية دون أن يرد تعريف صريح في هذا الموضوع، وذلك في المرسوم التنفيذي رقم(98–257) المعدل، الذي يضبط شروط وكيفية إقامة خدمات الأنترنيت واستغلالها[4]، وكذا القانون رقم (04–15) الذي تم بموجب المادة (12) منه من الفصل الثالث من الباب الثاني من الكتاب الثالث، من الأمر رقم 66–156 المتضمن قانون العقوبات، سابع مكررتحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**" ، ويشمل المواد من (394) مكرر إلى (394) مكرر 7[5].

يمكن تعريف التجارة الإلكترونية في إطار القانون التجاري الجزائري الذي عرّف التاجر في المادة الأولى منه على أنه « ***كل شخص طبيعي أو معنوي يباشر عملا تجاريا ويتخذه مهنة معتادة له*** ... » بدلا من تعريف التجارة، جعل في المواد(2، 3، 4) إلى

---

[1] – إبراهيم رفعت جمال، الجوانب القانونية للمعاملات الإلكترونية، دراسة مقارنة بين القانون المصري والفرنسي، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص 19.

[2] – إبراهيم رفعت جمالي، المرجع السابق، ص 25.

[3] – Hubert BITAN, les Contrats d'informatiques, Juris-classeur, Paris, 2002, p 175.

[4] – مرسوم تنفيذي رقم 98–257، مؤرخ في 25 أوت 1998، يضبط شروط وكيفيات إقامة خدمات الانترنيت واستغلالها، ج ر عدد 63، صادر في 1998/08/26.

[5] – قانون رقم 04–15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66–156 مؤرخ في 08 يونيو 1966، والمتضمن قانون العقوبات، ج ر عدد 71، صادر في 2004/11/10.

تعداد الأعمال التجارية[1]، وعليه بالرجوع إلى القانون الجزائري، فالتجارة هي ممارسة الأعمال التجارية على وجه الاعتياد، بالتالي فالتجارة الإلكترونية ليست سوى ممارسة تلك الأعمال على وجه الاعتياد عن طريق الوسائل الإلكترونية، وهي السبب الفعلي لوجود التجارة الإلكترونية.

يمكن من خلال ما تقدم أن نعتمد تعريفا شاملا وهو أن التجارة الإلكترونية هي **كل معاملة تجارية تتم عن بعد باستخدام الوسائط الإلكترونية (Electoronic Data Interchange) (EDI) أو من خلال البريد الإلكتروني (E.mail)، النشرات الإلكترونية والفاكس وباستخدام التحويلات الإلكترونية (Electronic Funds Transfer) EFT وكل الوسائل الإلكترونية المشابهة لها، شأنها تقديم أو تسهيل أعمال تجارية في صبغة افتراضية أو رقمية بين مختلف المتعاملين التجاريين.**

الفرع الثاني

خصائص التجارة الإلكترونية

تكسب التجارة الإلكترونية أهمية يوما بعد يوم، لأنها توسع السوق من نطاق محلي إلى نطاق دولي، توفر الجهد والوقت باستعمالها الحاسب الآلي بدل الإستعانة بالأنشطة الورقية، وكل هذا عبارة عن خصائص التجارة الإلكترونية التي يمكن أن نجملها على النحو التالي:

أولا – غياب وجود مادي للأطراف:

يتم التعاقد المادي دون وجود مجلس عقد بالمعنى القانوني التقليدي له، فعملية العقد تتم عن بعد، دون أن يرى أو يعرف أطراف العقد بعضهما البعض، أو يتفاوضوا وجها لوجه، كما هو الحال في الطريقة التقليدية حتى أنه في بعض الأحيان، يغيب تماما العنصر البشري، ويتم التراسل فقط بين أجهزة الحاسوب لأطراف العقد، كما هو الحال في بعض البرامج التي تضعها الشركات على أجهزتها [2]، ومن ذلك ما تقدمه البنوك من خدمات لزبائنها بناءًا على طلبهم لتسديد فواتير الماء والكهرباء والغاز من حساب العميل مباشرة دون أن يضطر لتسديدها عبر الأنترنيت، أو للذهاب بنفسه لتسديد هذه الفواتير، إذ تربط البنوك حواسيبها بحواسيب شركات الماء، الكهرباء، والهاتف باستخدام برامج

---

[1] – أمر رقم 75–59 مؤرخ في 26 ديسمبر 1975، يتضمن القانون التجاري، معدل ومتمم، ج ر عدد 78، صادر في 1975/09.

[2] – المومني عمر حسن، التوقيع الإلكتروني وقانون التجارة الكترونية، دراسة قانونية وتحليلية مقارنة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2003، ص 32.

معينة، تقوم هذه البرامج بتصدير الفواتير الشهرية أوتوماتيكيا إلى حواسيب البنوك، والتي تقوم بدورها بتحويل قيمة هذه الفواتير من حساب العملاء إلى حساب الشركات[1].

تسمى هذه التقنية (Web Service) خدمة الويب، أو (Application Service) وهي عبارة عن برنامج يظهر على شبكة الأنترنيت بواسطة ملفات وقسيمة تسمى (XML) ويتوجب وجود قوانين للربط بين المستخدم والبرامج الموجودة على جهاز السفير.

وفي هذا النمط يتمكن المستهلك من تسديد فواتير الماء والكهرباء والهاتف للمؤسسات التي تزوده بهذه الخدمات عن طريق الأنترنيت بواسطة بطاقة الإعتماد، أو يقوم المستهلك بإجراء أمر تحويل قيمة الفواتير بواسطة الأنترنيت من حسابه إلى حساب المؤسسات التي توفر هذه الخدمات.

ثانيا – وجود الوسيط الإلكتروني:

يقصد بالوسيط الإلكتروني الوسيلة المستخدمة لإتمام العقد، وتتمثل هذه الوسيلة بجهاز الحاسب الآلي المتصل بالشبكة العالمية الأنترنيت لدى الطرفين المتعاقدين، تجري عملية التعاقد أو التفاوض بين المتعاقدين، وبدونهما لا يمكن الحديث عن تجارة إلكترونية عبر الانترنيت [2]، كما يمتد تعريف الوسيط الإلكتروني إلى وسائل الإتصال الفورية الحديثة، إذ أن المادة (2) من قانون المعاملات الأردني رقم (85) لسنة 2001 عرّف الوسيط الإلكتروني بأنه « ***برنامج الحاسوب أو أي وسيلة إلكترونية أخرى تستعمل من أجل تنفيذ إجراء أو الإستجابة لإجراء، بقصد إنشاء أو إرسال أو تسلم رسالة معلوماتية دون التدخل الشخصي*** »[3]، الملاحظ في هذا التعريف أنه لم يقتصر فقط على جهاز أو برنامج الحاسوب فقط.

والجدير بالذكر أن قانون الأنسترال النموذجي بشأن التجارة الإلكترونية لعام 1996، لم يورد تعريفا للوسيط الإلكتروني، وكذلك الأمر بالنسبة لمشروع قانون المبادلات التجارية والتجارة الإلكترونية الفلسطيني لسنة 2003، ومشروع قانون المعاملات الإلكترونية المصري لسنة 2001.

---

[1] – لما عبد الله صادق سهب، مجلس العقد الإلكتروني، مذكرة ماجستير في القانون، جامعة النجاح، نابلس، فلسطين، 2008، ص 17.

[2] – المومني عمر حسن، مرجع سابق، ص 35.

[3] – قانون المعاملات الإلكترونية الأردني رقم 85 المؤرخ في 31 كانون الأول 2001، الجريدة الرسمية الأردنية، العدد 4524.

وهنا يمكن أن نأخذ مثال كأن يقوم شخص بعرض سيارته أو أي ممتلكات أخرى للبيع ليس بالطرق التقليدية كإشهارها أو في مزاد علني أو في السوق، ولكن باستعمال وسيط إلكتروني كالانترنت، من خلال موقع إلكتروني معين (website)، ليتاح للمتسوقين والمتصفحين لمواقع الأنترنت الحصول على معلومات عن السلعة المعروضة وإمكانية شرائها من المالك مباشرة من الانترنيت.

ثالثا – السرعة في إنجاز الأعمال التجارية الإلكترونية:

تتفادى الأعمال التي تتم بالوسائل الإلكترونية العديد من الأوراق المكتوبة التي تصاحب أوامر البيع والشراء وشحن الصناعة وغيرها، غير أن الأمان في إرسال الرسائل عن طريق الحاسب الآلي ما زالت مشكلة قائمة لم يتم التغلب عليها، لأن بعض الأشخاص تخصصوا في دخول الحواسب وإرسال الرسائل المغلوطة، وتوافرت لديهم التقنية التي تساعدهم على الدخول إلى حسابات البنوك والحكومات[1].

زيادة على ذلك فإن التجارة الإلكترونية أتاحت إمكانية وصول المتعاملين إلى جميع أسواق العالم بأقل النفقات، فإبرام العقود والصفقات من خلال شبكة الأنترنيت، يمكن أن يتم خلال دقائق معدودة، مما يوفر الجهد والوقت والتكاليف، وبوجود التجارة الإلكترونية، أصبح الكثير من المستهلكين يسألون أنفسهم لماذا يضيعوا الكثير من الوقت والجهد، بينما يمكنهم شراء ما يريدون في لحظات أو دقائق دون أن يتحركوا من أماكنهم[2].

رابعا – تتخطى الحدود الجغرافية:

لا تعرف التجارة الإلكترونية حدود جغرافية لدخول الأسواق التجارية الدولية، إذ يمكن تسميتها حتى بالتجارة العابرة للقارات، لكن مقابل هذا نجد مشكل تطبيق القوانين في حالة وجود نزاع، وكذا الهيئة المختصة قضائيا، دون أن ننسى حماية العلامة التجارية المسجلة[3].

---

[1] – الجنبيهي منير وممدوح محمد، الشركات الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص 11.

[2] – حمارشة رياض وليد، عقد البيع الإلكتروني في ظل التجارة الإلكترونية، إبرامه، آثاره، إثباته، مذكرة ماجستير في القانون، جامعة الدول العربية، كلية الحقوق، القاهرة، مصر، 2000، ص 17.

[3] – عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، 1997، ص 83.

وعلى اعتبار عقد التجارة الإلكترونية من عقود الإتصال عن بعد أو ما يسمى عقود المسافة، يترتب على ذلك أن كلا من المتعاقدين لا يستطيع التأكد من هوية أو شخصية الآخر، كما لا يستطيع المشتري معاينة البضاعة المتعاقد عليها بشكل مباشر، وعليه لابد أن يلتزم البائع من تمكين المشتري أو طالب الخدمة من الاطلاع على المعلومات الوافية اتجاه البضاعة أو الخدمة التي يريدها، لأنه لا يستطيع التنقل من أجل المعاينة للتحقيق أو التأكد[1]، كما يمكن للمشتري العدول عن التعاقد بعد قبوله بفترة معينة يحددها القانون.

ولصعوبة التلاقي بين الأطراف في تعاملات التجارة الإلكترونية إذ يصعب التحقق من تاريخ التصرفات والمستندات الإلكترونية والإعداد المسبق لأدلة الإثبات والتحقيق من مكان إبرام التصرفات [2]، إيستوجب وضع قواعد خاصة في عقود التجارة الإلكترونية التي تنبع من طبيعة هذه العقود التي تؤدي بالبداهة إلى اختلاف أحكامها عن العقود المبرمة بين حاضرين [3]، والتي تبرم في غالبيتها بالحضور المادي للطرفين في مجلس واحد يصدر فيه الإيجاب والقبول في المكان نفسه وفي الجلسة نفسها.

يمكن القول أن التجارة الإلكترونية وسعت نطاق السوق إلى نطاق دولي وعالمي، بقليل من التكلفة مختزلة النطاق الزماني والمكاني، حيث أنها توفر لأي متعامل تجاري إيجاد مستهلكين أكثر واستيراد أفضل، بصورة سهلة وسريعة عن طريق وسائل التكنولوجيا، كما أنها تعطي الخيار للمستهلك بأن ينهي المعاملات أو يتسوق على مدار 24 ساعة في اليوم أو في أي يوم من السنة، ومن أي مكان على سطح الأرض، السبب في ذلك قابلية الوصول إلى منتجات وشركات لم تكن متوفرة للمستهلك من قبل[4].

وبالرغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالمية في إيجاد وتفعيل التجارة الإلكترونية، فإنها بالمقابل أوجدت خطرا حقيقيا تمثل بإمكانية جمع المعلومات وتخزينها أو إتلافها أو تزويرها لسهولة الوصول إليها عن طريق قرصنتها دون علم أو معرفة أصحابها، وغيرها من الإنتهاكات والإستعمالات

---

[1] – نضال إسماعيل إبراهيم، أحكام عقود التجارة الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 58.

[2] – مجاهد أسامة أبو الحسن، التعاقد عبر الانترنيت، دار الكتب القانونية، مصر، 2002، ص 42.

[3] – المرجع نفسه، ص 41.

[4] – سهيلة خليل الغازي، معوقات التجارة الرقمية في الدول العربية، دار الوفاء للنشر، القاهرة، مصر، 2003، ص 95.

الغير القانونية كانت ولا تزال المعوق الحقيقي لممارسات التجارة الإلكترونية، تشكل كل هذه المعوقات خطرا يسمى ب "**الإرهاب الإلكتروني**".

المطلب الثاني

ماهية الإرهاب الإلكتروني

نتيجة للتطورات الهائلة في عالم الحاسوب والإتصالات ودخولنا في العصر الرقمي عصر السرعة والإنفجار المعلوماتي، وكذا الإنتشار السريع لشبكة الأنترنيت العالمية، ومع استخدام الحاسب الآلي وتطبيقاته خاصة في مجال التجارة الإلكترونية بكل أنشطتها وخدماتها، غيّر في إدارة شؤون الدول، وبفعل هذه التقنيات الحديثة، فإنّ حدود الدول تكون مستباحة بأقمار التجسس والبث الفضائي.

أيضا بسبب طبيعة شبكة الأنترنيت وانفتاحها غير المحكوم، وعدم ارتباطها بدولة واحدة أو حدود جغرافية معينة، وبسبب صعوبة الرقابة أو المحاسبة على ما ينشر عليها أصبحت التجارة الإلكترونية، مسرحا سهلا للإعتداءات 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 الأنترنيت.

بناءًا على ذلك فقد جرى توظيف التقنيات الرقمية من قبل الأفراد، المنظمات والدول للإضرار بالغير والقيام بأعمال إجرامية سميت بـــ"الإرهاب الإلكتروني"، وهو ما سيتم تحليله بتحديد مفهومه في بعض القوانين الوضعية (**الفرع الأول**)، ثم التطرق إلى خصائصه (**الفرع الثاني**).

الفرع الأول

مفهوم الإرهاب الإلكتروني في بعض القوانين الوضعية

يعتبر الإرهاب الإلكتروني نوع من الإرهاب الحديث الذي وظّف واستثمر تقنيات المعلومات والإتصالات 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:

أولا – 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 والإتصالات، 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[1].

قامت في السنة نفسها (1996) كلية الحرب 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 كلية الحرب، 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.

أما الباحث الأمريكي(POLITT Mark) بوليت مارك، باحث في مكتب معهد أمن المعلومات، بالتعاون مع مكتب التحقيقات الفيدرالية للولايات المتحدة الأمريكية، يعرف الإرهاب الإلكتروني أنه « ***هجوم ذات دوافع سياسية، اقتصادية أو شخصية ضد المعلومات، ونظم الحاسوب وبرامجه، من قبل مجموعة إرهابية أو عملاء سريون*** »[2]، ما يمكن ملاحظته في هذا التعريف أنه لا يختلف عن تعريف الإرهاب التقليدي من حيث الدوافع بل في الأساليب، وهذا ما أكدته مجموعة الإجراءات التي قامت بها الولايات الأمريكية من أجل دراسة هذه الظاهرة، بدلا من إعطائها تعريفا واضحا، حيث تم إنشاء وكالة استخبارات مركزية خاصة بالحروب المعلوماتية.

---

[1] – http://searchsecurity-techtarget.com

[2] – ذياب موسى البداينة، الإرهاب المعلوماتي، مذكرة ماجستير في القانون، كلية التدريب، جامعة نايف للعلوم الأمنية، 2008، ص 13.

قامت المكاتب الفيدرالية باتخاذ إجراءات أمنية في المجال نفسه، حتى تتمكن بالرد السريع والفعال إزاء المتغيرات السريعة لعمليات الإرهاب الإلكتروني[1].

كما أظهرت دراسة أمريكية أن الإرهابيين لديهم شغف استخدام شبكة الانترنيت في عملياتهم الإرهابية، مظهرين بذلك مستوى براعتهم في تحطيم أو التفوق على أي تقنية مستخدمة[2].

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، هي 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[3].

ثانيا – 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 [4]، 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؟

---

[1] – أحمد أنور زهران، التكنولوجيا والحرب المعاصرة، دار الوفاء للنشر، القاهرة، 1987، ص 72.

[2] – 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.

[3] – 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.

[4] – 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.

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*** »[1].

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*** »[2]، 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*** »[3].

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

---

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

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

3 – http://ar.wikipidia.org/wiki.

بتلك العمليات الإرهابية كالترويع، التهديد، إجبار الخصم بالقيام بعمل أو الامتناع عنه أو زعزعة الاستقرار.

إذا اعتبرنا أن الإرهاب إلكتروني يدخل ضمن هذا التعريف، لأنه حتى وإن اختلفت وسائله يظل إرهابا، لما 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؟

ثالثا – 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.

صرحت العديد من الدول العربية اعترافها 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*** »[1].

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*** »[2].

---

[1] – محمد الغامدي، الإرهاب الأخطر هو المشكلة التي تواجهها المملكة خلال الفترة المقبلة على الموقع: http://www.assakina.com/pdf/arabic/text.

[2] – محمد الغامدي، المرجع نفسه.

أما مصر فقد عرفت الإرهاب الإلكتروني بأنه « ***الاستخدام الغير 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*** »[1].

العراق تبنى التعريف التالي « ***الإرهاب المعلوماتي هو كل نشاط أو فعل إجرامي هجومي متعمد أو مقصود، يقوم به فردا أو جماعة أو منظمة، ذو دوافع سياسية استهدف أو يستهدف فردا أو مجموعة أفراد أو منظمات أو دولا أوقع أو يوقع أضرارا بالممتلكات العامة أو الخاصة، بهدف الإخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو إدخال الرعب والخوف والفزع بين الناس، باستخدام الوسائل والموارد المعلوماتية لتحقيق غايات إرهابية*** »[2].

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 الإختلاف 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.

بعد عرضنا لمجموعة من التعاريف في مختلف القوانين الوضعية للإرهاب الإلكتروني نجده بدأ على شكل انتهاكات فردية كسرقة البرامج والكتب والملفات، ثم تطور حتى أصبح ظاهرة عابرة للأوطان من خلال توفير إمكانية وصول سهلة إلى وسيلة اتصال لا يحكمها أي تقنيين أو أي شكل من أشكال المراقبة الحكومية، تسهل قدرة الجماعات الإرهابية إستغلال التدفق السريع للمعلومات، لنشر دعايتهم في مواقع مجانية، كما أنها توفر آلية مناسبة من شأنها جذب متلقي الرسالة الإرهابية بسهولة أكبر، نظرا لأن بعض المواقع التي تستخدمها الجماعات الإرهابية تمكن من تحميل معلومات إرهابية خطيرة عن عملياتهم، قصد نشرها وترهيب الناس.

---

[1] – علي العبيدي، الإرهاب الإلكتروني أحدث صرعة في معارك الصراعات الدولية العابرة على الموقع: http://www.ibb7.com/pdf/arabic/text.

[2] – جعفر حسن جاسم الطائي، الإرهاب المعلوماتي وآليات الحد منه، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، العراق ص ص 484 – 507.

وعليه من خلال التعاريف السابقة، يمكن إستخلاص تعريف الإرهاب الإلكتروني على أنه « ***إرهاب يقوم باستخدامات متعددة لتكنولوجيا المعلومات، لتنظيم وتنفيذ الهجمات ضد الانظمة الحاسوبية لنظم المعلومات أو الهياكل المركزية للاتصالات السلكية، واللاسلكية، لأغراض تخريبية وتدميرية، وذلك تحقيقا أهداف سياسية أو اقتصادية أو اجتماعية، ونشر الرعب والخوف ضد المجتمع الدولي والأفراد، من خلال استخدام جملة من الهجمات الإرهابية*** ».

الفرع الثاني

خصائص الإرهاب الإلكتروني

شهدت السنوات الأخيرة تزايدا ملحوظا في استخدام الإرهابيين لوسائل التكنولوجيا بكل سهولة ويسر، كاستخدامهم للشبكة الدولية الأنترنيت، حيث وصل عدد المواقع الإرهابية لسنة 2013، 9000 موقع وفقا للإتحاد الأوربي، تعمل هذه المواقع كلها في ترويج للأعمال الإرهابية سواء داخل أو خارج إقليم واحد، دون تحمل أعباء التنقل والمواجهة بين المنفذين والمخططين، وبأقصى درجة من ضمان التنفيذ والتأمين، هي حقا عملية إرهابية عن بعد[1].

وبالرجوع 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 اتصالاتهم ببعضهم البعض، مما زاد من اتساع مسرح عملياتهم الإرهابية، والتي أصبح من الصعب حصرها والقضاء عليها لأنها تتمتع بالخصائص التالية:

أولا – التعامل بالبريد الإلكتروني:

أ – تعريف البريد الإلكتروني:

تقوم فكرة البريد الإلكتروني على تبادل الرسائل والملفات والرسوم والصور وغير ذلك بطريقة إلكترونية حيث يتم إرسالها من المرسل إلى المرسل إليه شخص كان أو أكثر، وذلك باستعمال عنوان البريد الالكتروني للمرسل إليه بدلا من عنوان البريد العادي.

ولقد وضع الفقه والتشريع عدة مفاهيم محاولا الوصول من خلالها إلى معنى واضح للبريد الإلكتروني.

---

[1] – محمد مؤنس محي الدين، الإرهاب في القانون الجنائي، مكتبة أنجلو مصرية، مصر 1999، ص 70.

1 – التعريف التشريعي للبريد الإلكتروني:

لقد بذلت جهود دولية لحل المشاكل القانونية الناجمة عن استخدام التقنيات العلمية الحديثة ومنها البريد الإلكتروني، فقد عرفه القانون الأمريكي بشأن خصوصية الإتصالات الإلكترونية بأنه « ***وسيلة اتصال يتم من خلالها نقل المراسلات الخاصة عبر شبكة الخطوط التلفونية الخاصة أو العامة، وغالبا يتم كتابة الرسائل على جهاز الكومبيوتر، ثم يتم إرسالها إلكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه، حيث يتم إرسالها عبر نظام الخطوط الهاتفية إلى كمبيوتر المرسل إليه*** »[1]. وعرفه القانون النموذجي العربي بأنه « ***نظام للتراسل باستخدام شبكات الحسابات*** »[2]. أما في فرنسا فقد عرفه القانون الفرنسي بشأن الثقة في الإقتصاد الرقمي الصادر في 22 جوان 2004 بأنه «***كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صوت أو صور أو أصوات ويتم إرسالها عبر شبكة الإتصال العامة وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها*** »[3].

2 – التعريف الفقهي للبريد الإلكتروني:

يعرف بعض الفقهاء البريد الإلكتروني على أنه « ***مكنة التبادل الإلكتروني غير المتزامن بين أجهزة الحاسب الآلي للرسائل الإلكترونية*** »[4]، أي هو تبادل إلكتروني للرسائل سواء نصية أو صورية بين أجهزة الحاسب الآلي، ولكن ليس في نفس الوقت بل في فترة متفاوتة المدة، كما يعرفه فريق آخر من الفقهاء على أنه « ***طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة الأنترنت*** »[5]، ويعرف أيضا « ***مستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم، شرط أن يتم تأمين هذا الصندوق بعدم الدخول إليه، وذلك من خلال نظام التشفير، أو كلمة المرور***

---

[1] – عبد الهادي فوزي العوضي، مرجع نفسه.

[2] – صدر القانون العربي النموذجي بشأن مكافحة جرائم الكمبيوتر والانترنيت وذلك بالتعاون بين مجلس وزراء الداخلية العرب ومجلس وزراء العرب تحت مراقبة جامعة الدول العربية.

[3] – Manar (C), Aspects juridiques de l'e-mail, Dalloz, 8 Affaires, n° 140, 1999.

وراجع أيضا عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، المكتبة القانونية/ مصر، 2004، ص 06.

[4] – أسامة الكسواني، "تقنية البريد الإلكتروني والقانون"، مجلة القبس الكويتية، العدد 12، الصادرة في 2008/03/31، ص ص 1 – 5.

[5] – محمود السيد عبد المعطي خيال، الانترنيت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة ،مصر، 2001، ص 134.

وغيرها من تقنية الحماية الفنية »[1]، كما يعرف أيضا بأنه « ***تلك المستندات التي يتم إرسالها واستلامها بواسطة نظام اتصالات بريدي إلكتروني، يتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه اصطحاب مرفقات خاصة مثل معالجة الكلمات وأية مستندات أخرى يتم إرسالها رفقة رسائل أخرى*** »[2].

من خلال كل هذه التعاريف الفقهية يمكنها أن تعرف البريد الإلكتروني على أنه خط مفتوح على كل أنحاء العالم، يستطيع الفرد من خلاله إبرام التصرفات القانونية وإرسال واستقبال كل ما يريده من رسائل بطريق إلكتروني.

3 – التعريف التقني للبريد الإلكتروني:

نقصد بالتعريف التقني للبريد الإلكتروني التعرف على آلية أو إمكانية عمل البريد الإلكتروني، حيث يتكون من جزئين رئيسيين هما (Header) ونص (Body)، ويحتوي الرأس على معلومات حول المرسل والمتلقي (المرسل إليه)، والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب، ويحتوي النص على الرسالة التي تم تكوينها، وعندما يرسل شخص ما إلى شخص آخر، فإنها تنتقل من كمبيوتر المرسل عبر خط تلفون إلى كمبيوتر الخادم (مزود الخدمة) أو ما يسمى مقلم البريد (Mail Server) والذي يوجد به صندوق بريد المرسل، ومن ثمة تنتقل على نحو مباشر إلى كمبيوتر خادم آخر، يخزن صندوق بريد المرسل إليه، وعندها يستطيع المرسل إليه استرجاع محتويات صندوق بريده الالكتروني عند اتصاله بالخادم الخاص به وفق ما يسمى بالتحميل التحتي[3] (Down Loading)، ويتم ذلك وفق بروتوكول (Pop) أو (IMAP)[4].

---

[1] – عبد الفتاح بيومي حجازي، الحوكمة الإلكترونية ونظامها القانوني، المجلد الأول – النظام القانوني للحوكمة الإلكترونية، دار الفكر جامعي، الإسكندرية ،مصر، 2004، ص 142.

[2] – عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، شبكة المحامين العرب على الموقع: http://www.file://hmht/mhtml

[3] – يقصد بالتحميل التحتي أن يقوم الكمبيوتر بتحميل الشيفرة الثنائية الداخلية الخاصة ببرنامج معين إلى كمبيوتر آخر لمستعمل الجهاز، انظر: سعد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنيت، الطبعة الأولى، دار النهضة العربية، مصر، 1999، ص 228.

[4] – Pop هي اختصار لـــ (Post Office protocol) أي بروتوكول مكتب البريد، وهو يستخدم في الطريقة التي يحصل فيها برنامج البريد الإلكتروني على البريد من الملقم، أما (IMAP) فهو اختصار لـــ(International Massage Acces Protocol) أي بروتوكول وصول الرسائل ويتحكم ببعض الطرق التي يصل بها برنامج البريد الإلكتروني من الملقم، انظر محمد أمين الشوابكة، جرائم الحاسوب والانترنيت: الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع عمان، 2007، ص 33.

وبفضل البريد الالكتروني يتاح للحائزين على عنوان البريد الإلكتروني من الإتصال فيما بينهم بالطريقة ذاتها التي تتم بها المراسلة عن طريق البريد الإعتيادي، سوى أن إرسال الرسائل الإلكترونية تتم من خلال العلبة الإلكترونية العائدة إلى كل من المرسل والمرسل إليه الموصلين بشبكة الانترنيت.

وتتماثل العناوين الإلكترونية فيما بينها في الشكل إذ تتكون من مقطعين يفصل بينهم رمز (@) وتكون على الشكل التالي (...@yahoo)، ويلاحظ من ذلك أن الجزء الأول الذي يقع على يسار الرمز(@) يدل على اسم المستخدم والذي يكون عادة أسمه الحقيقي أو مجرد رمز له، أو اسما مستعارا وهذا الجزء هو الذي يميز مستخدم عن غيره من المستخدمين لدى مقدم خدمة البريد الإلكتروني ويتبعه إشارة (@)، أما الجزء الواقع على يسار الرمز(@)، فيشير دائما إلى مقدم الخدمة.

ويستطيع الشخص بمجرد الحصول على عنوان البريد الإلكتروني في تبادل الرسائل الإلكترونية مع الآخرين في فترات متعددة إضافة إلى ذلك يستطيع الشخص صاحب البريد الالكتروني، القيام بكافة التصرفات القانونية كإبرام العقود والرد على المخاطبات الإدارية وكذلك إتمام بعض الإجراءات القضائية[1].

ب – خصائص البريد الإلكتروني:

يتمتع البريد الإلكتروني بمزايا ينفرد بها في إطار الثورة المعلوماتية، فله خصائص تميزه على نحو واضح وجلي ومن هذه الخصائص أنه وسيلة اتصال غير متزامن، أي ليس هناك تزامن في وجود الأشخاص على طرفي الإتصال، وذلك لأن المتصل عبر الأنترنت ومن خلال البريد الإلكتروني يستطيع الحصول على مراده من الجهة المقابلة متى يشاء دون أن يدخل شخص آخر [2]، لذلك فإن إرسال رسائل عبر البريد الالكتروني لا يحتاج وجود المرسل إليه، ومن ثمة الاضطرار إلى الاتصال به مرة أخرى في حالة عدم وجوده إذ يمكن للمرسل ترك ما أراد إيصاله من نص أو رسم أو صوت أو صورة في جزء من ذاكرة حاسوب المرسل إليه مخصص للبريد الإلكتروني يسمى صندوق البريد الإلكتروني.

---

[1] – إبراهيم المنجي، عقد نقل التكنولوجيا – التنظيم القانوني لعقد نقل التكنولوجيا والتجارة الإلكترونية –، دار منشأة المعارف، الإسكندرية ،مصر، 2002، ص 298.

[2] – وليد منيمة، "إنترنيت تقود العالم إلى ثورة في مجال أداء الأعمال إلكترونيا"، PC. Magazine، عدد رقم 03، جوان 1999 على الموقع .http://www.arabic.pcmag-arabia.com

إضافة إلى ذلك أن خدمة البريد الإلكتروني توفر درجات متعددة من الإتصال تتفاوت في القوة والضعف على قدرتها في نقل المعلومات، وهو أمر ينعكس بدوره على مدى القدرة المتوفرة للمتصل في إيصال تعبيره عن إرادته إلى الطرف الآخر، حيث أن الاتصال يقتصر على إرسال نص يظهر على شاشة حاسوب المرسل إليه بشكل كتابة باستخدام بروتوكول ينقل الرسائل الإلكترونية من جهاز إلى جهاز آخر وهو بروتوكول البريد الإلكتروني[1].

ويرى بعض الباحثين أهل الإختصاص في مجال الإعلام الآلي، إن البريد الالكتروني هو أفضل ما في الانترنت لتمتعه بخصوصيات تجعله أفضل من الهاتف والفاكس، ذلك أن المرسل لن يضطر إلى مراعاة فروق التوقيت والأبعاد الجغرافية، إذ يمكن لشخص مقيم في بريطانيا أن يبعث رسالة إلى صديقه في العراق بمجرد معرفة عنوان بريده الالكتروني وفي أي وقت خلال ثوان ودقائق تصل الرسالة.

مع تطور تكنولوجيا الاتصالات، أصبح البريد الإلكتروني من أكثر الوسائل استخداما أو استعمالا في المجتمع الدولي في تواصلاتهم من خلال تبادل الرسائل والمعلومات عبر مختلف وسائل الاتصال كالهواتف النقالة، شبكة الانترنيت، الفاكس إذ معظم هذه الوسائل موصول بالانترنيت والأقمار الصناعية، وهي من أبرز الخدمات التي تقدمها الشبكة العنكبوتية، لما تمثله من سرعة فائقة ودقيقة في الإتصال وإرسال الرسائل وسهولة الإطلاع عليها في أي مكان بفضل خدمة البريد الالكتروني أو (E-Mail) و التي بدت أسهل الوسائل وأسرعها في تبادل المعلومات، خاصة في مجال التجارة الإلكترونية.

بالمقابل أصبح 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[2].

يعد " توم ميتزقر" (Tom METZGER)، أحد أشهر المتطرفين الأمريكيين مؤسس مجموعة "**المقاومة الأريانية البيضاء** "، أول من أسس مجموعة البريد الإلكتروني سنة 1985 لبث أفكاره التطرفية، ثم استعمل البريد الالكتروني كوسيلة للتعامل مع الشركات التجارية الكبرى، للحصول على المعلومات وتقديمها للشركات المنافسة، أدى إلى إفلاس

---

[1] – دراسة عن البريد الإلكتروني على موقع موسوعة الكمبيوتر والانترنيت العربية http://www.c4aral.com

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

عدة مؤسسات تجارية جراء ذلك، ليس لغرض ما، ولكن لمتعته الشخصية كونه يتحكم بالبريد الإلكتروني بطريقة غير قانونية ولا مشروعة، من هنا بدأت الشركات تعلن عن وجود متعامل الإلكتروني يهدد النظام الاقتصادي الخاص بها، متخفيا وراء البريد الإلكتروني، بحكم أن هذه الشركات كانت قد بدأت تتبنى فكرة التعامل بالبريد الإلكتروني لتوسيع دائرة تجارتها ولكن بالرجوع إلى سنة 1985، كانت معظم الشركات تعاني من نقص في المقاومة الإلكترونية لتعاملاتها التجارية، بحكم أنه لم يتم التصريح والاعتراف بما يسمى بالإرهاب الإلكتروني آنذاك[1].

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[2].

كل هذه الأساليب التي يستخدمها الإرهاب الإلكتروني إن دلت على شيء فهو 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، فمثلا أشهر الفيروسات التي انتشرت عن طريق البريد الإلكتروني هي:

1 – (I love you)

2 – (Mellissa Meet)

3 – (Buble boy)

---

[1] – فايز الشهري، الطرح الفكري على شبكة الأنترنيت، المراحل والرموز، بدون دار أو سنة للنشر، مصر ص 134.

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

وكلها فيروسات ظهرت واحدا تلو الآخر وهذا يدل على ضعف برامج الحماية المضادة للفيروسات.

كذلك تتجلى خطورة الإرهاب الإلكتروني في استعمال البريد الإلكتروني بالدخول إليه من غير صاحبه، مما يؤدي إلى فضح أسراره على نحو يصيبه بضرر وهو في ذلك يشبه مودع البريد الذي يستولي على خطابات القراء ويطلع على الأسرار التي تحويها، ويقوم بإذاعتها على نحو يسبب الضرر والخسارة لذوي الشأن [1]، ونذكر في هذا الشأن قضية تم فيها اختراق البريد الإلكتروني للمشتركين لدى الـــ(Hotmail) وإذاعة أسرار المشتركين حيث كانت شركة مايكروسوفت – مالكة الموقع – قد أهملت في احتياطات الأمن، وذلك بنسيان حذف كلمة المرور إلى الموقع أو إلى برنامج الصيانة الخاص بالموقع والتقطه الإرهابيون المختصون في عمليات الاختراق، واستغلوا هذه الثغرة لإفشاء وشتم وتهديد زبائن الـــ(Hotmail) أصحاب النفوذ، لكن الشركة اعتذرت رسميا لزبائنها عن الاختراق، وقالت على لسان مدير التسويق في الشركة أن أحد المخترقين استطاع أن يكتب شفرة متطورة مكنته من تخطي إجراءات الدخول إلى الموقع[2].

أضف إلى أن بعض رسائل البريد الإلكتروني لا تظهر توقيع صاحبها، ذلك أن 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.

ثانيا – التعطيل والتصرف في نظام الخدمات والمعلومات الإلكترونية:

أ – 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

---

[1] – عبد الفتاح بيومي حجازي، مرجع سابق، ص 192.

[2] – فادي سالم، "اختراق بريد الهوتميل الأكبر في تاريخ الانترنيت"، مجلة انترنيت العالم العربي، أكتوبر 1999، على موقعها في الشبكة: http://www.Jawmag.co.ae

الصفقة، بل يعمل نظام التعطيل المؤقت للخدمة على إضعاف قدرة الأنظمة الحاسوبية على إنجاز وظائفها، وبالتالي إيقاف النظام وتعطيله أو إغلاقه دون حدوث تدمير [1].

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 [2] التي تحمل النبضة الهكرومغناطيسية 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 الذي يلقى النبضة الشديدة 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.

ومن أخطر أنواعها، تلك التي تطلق موجات أو إشعاعات تنتشر بسرعة الضوء تتسبب في إتلاف وتعطيل الرادرات والأجهزة الالكترونية في الطائرات والسفن والقواعد العسكرية وهذا يسهل عمل وتنقل الإرهاب الإلكتروني دون أن يتم رصده.

ويرجع استخدام هذه القنبلة على أمريكا من قبل جماعة إرهابية وبطريقة سريعة، حيث شهدت منطقة معينة في أمريكا سنة 2009 بدمار كامل لكل مولدات الضغط

---

[1] – 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.

[2] – القنابل والصواريخ الالكترونية، سلاح حديث متطور يعتمد على مبدأ تفجير قنبلة خاصة تولد نبضات كهرومغناطيسية شديدة تؤثر في الأجهزة الإلكترونيۃ 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.

العالي، و تلف الأسلاك والأجهزة الإلكترونية في البيوت والمستشفيات والمحلات، وانقطاع في التيار الكهربائي لأكثر من 14 ساعة في المنطقة، وعللت أمريكا أن هناك خلل في المولدات الكهربائية، مع أن التحقيقات في الموضوع من قبل المختصين أكدوا أن ما حدث مطابق للعوارض التي تفعلها القنبلة الكهرومغناطيسية [1]، جعل الولايات المتحدة الأمريكية تتكبد خسائر رهيبة اقتصاديا وهو ما أدى بالرئيس الأمريكي الحالي براك أوباما إلى طلب قرض من طرف صندوق النقد الدولي والبنك العالمي.

ب – 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، التجارة 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، كما أن هناك العديد من الجرائم الإرهابية التي تتم عن طريق المعلومات بطرق انتحال شخصية الغير، وسرقة كلمة المرور(passeword)، 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 الإئتمان والشراء بها، واستخدامها، واستخدام اسم الشخص في أعمال إجرامية[2].

كما يتم التصرف في المعلومات بتزويرها، ويعني ذلك، تغيير حقيقية 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 (Defacing) [3].

وأخيرا يمكن التصرف في المعلومات عن طريق إتلافها وكذا البيانات المسجلة على الحواسب والشبكات المحلية والدولية، ويدخل فيها قواعد البيانات وبرامج التحكم

---

[1] – حكيم غريب، مرجع سابق، ص 817.

[2] – 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.

[3] – حكيم غريب، مرجع سابق، ص 820.

والمتابعة للنظم الكبرى في مختلف المجالات، وتتم عملية الإتلاف باستخدام فيروسات 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.

يوجد حوالي 50 ألف نوع من الفيروسات، وقد تعرضت دول العالم خاصة الولايات المتحدة الأمريكية إلى العديد من هذه الهجمات، والتي أدت إلى إبطاء عمل الحواسب والشبكات، خاصة التجارية منها، حيث تم ضبط عدد كبير من القراصنة، منها جماعة معروفة باسم (**Drink or Die**) والتي نفذت أكثر من 100 هجوم على الشبكات التجارية[1].

ثالثا – تعدد صور الإرهاب الإلكتروني:

لعل أهم خصائص الإرهاب الإلكتروني بغض النظر على أنه ينشط ويستعمل التكنولوجيا، هي تعدد أشكاله وصوره بحكم أنه ينشط في عالم افتراضي غير مرئي، لذا يصعب فعلا رصده أو حصره، وتتمثل أهم صوره أو أشكال الإرهاب الإلكتروني في:

أ – إرهاب إلكتروني ضد الأفراد:

يتمثل الإرهاب الإلكتروني الموجه ضد الأفراد كل التصرفات التي يقوم بها من خلال وسائل التكنولوجيا (الانترنيت، الفاكس، الهاتف... الخ) مهما كان نوعها أو حجمها ضد شخص طبيعي لهتك خصوصيته، بعدما أصبح من الممكن التداول إلى الأحاديث عبر الشبكات، إذ شهدت شبكة الانترنيت عدة حالات للابتزاز المعلوماتي، من قبل أشخاص تمكنوا بوسيلة أو بأخرى من اختراق نظام الأمن للبريد الإلكتروني أو التنصت على حلقات الدردشة عبر الانترنيت[2].

ما يساعد على استخدام الانترنيت – مثلا – كوسيلة للابتزاز أن التواصل عن بعد يتيح فرصا عدة لتقمص الشخصيات لخداع الآخرين عبر الجهة الأخرى من العالم وراء هواتفهم أو حواسبهم، لعدة أسباب كالبوح بأسرارهم الشخصية حتى يمكن استغلالها ضدهم، علاوة على ذلك تتيح التكنولوجيا وسائل مبتكرة للتهديد، الابتزاز، القرصنة أو

---

[1] – http://www.alond.com-pxter-com/ologes 002/102/20 newshem.

[2] – علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار منشأة المعارف، الإسكندرية، مصر، 2006، ص 09.

الاختراق نذكر منها على سبيل المثال لا الحصر، التهديد بالوثائق المزورة التي يتم تزويرها إلكترونيا لدرجة لا يمكن ملاحظة الفرق بين الصورة الأصلية والمزورة، بغض النظر عن التهديدات الأمنية كاختراق حساب بنكي أو السرقة من خلال استخدام أرقام بطاقات الائتمان الخاصة في معاملات التجارة الإلكترونية.

ب – إرهاب إلكتروني ضد المؤسسات:

يعد من أخطر مصادر التهديد الإلكتروني للمؤسسات، من خلال اختراق شبكات اتصالاتها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة، وفي ظل المنافسة التي تشهدها معظم الأسواق الحالية، أصبح التجسس على مختلف أنشطة الشركات من قبل منافسيها مصدر قلق حقيقي، وقد تم اختراق شبكات المعلومات لبعض البنوك السودانية في إطار حملة شنت ضد السودان ضمن ما أسموه بتمويل العمليات الإرهابية[1].

من المظاهر الأخرى لإرهاب المؤسسات إلكترونيا، إسقاط موقع المؤسسة على الانترنيت، وذلك بأن يصوب إليه العديد من الرسائل المولدة تلقائيا التي تظل تنهمر إلى أن تصل إلى حد يعجز فيه الموقع تماما عن ملاحقتها ليسقط، وتسقط بالتالي معه جميع المعاملات التجارية والمالية الإلكترونية التي يوفرها موقع المؤسسة لعملائه وشركائه.

من الوسائل الأخرى التي تتعرض لها المؤسسات، فك شيفرة حماية سرية البيانات التي تتبادلها مع الآخرين خارج المؤسسة من عملاء ووكلاء وما شبه، وقد سبق أن عرف العالم تهديد حيث قام شاب من النرويج نشر برنامج في عدة أسطر يمكن به فك الشفرة الرقمية التي تبث بها الأفلام عبر الشبكة، وهو دليل الإرهاب في سطو المؤسسات وهو التهديد نفسه الذي تواجهه حماية الملكية الفكرية[2].

ج – إرهاب إلكتروني ضد الدول:

صورة الإرهاب الإلكتروني ضد الدول تكمن في الدخول إلى شبكات التحكم في المرافق العامة، مما يتسبب في شلل للبنى التحتية الأساسية، بل واحتمال تدميرها كليا[3].

إنّ الدول أصبحت معرضة لما يسمى الدمار الشامل باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في جيوش الفيروسات التي تخترق حدود الدول وتحطم البنية التحتية

---

[1] – علاء علاء الصراط الغامدي، المرجع السابق، ص 15.

[2] – دعاء علي، الطبيعة القانونية للاستيلاء على الأموال من البنك الآلي، مطبعة أوفيست الزمان، بغداد، العراق، 2000، ص 46.

[3] – هشام محمد رستم، الإرهاب الدولي، دار النهضة العربية، القاهرة، مصر، 2003، ص 106.

المعلوماتية، كما أن تزايد الترابط بين هذه الشبكات زاد تعرض الدول لهذا التهديد على شبكات المعلومات في إدارة معظم شؤونها الداخلية والخارجية، وهو ما عاشته مصر من تشويه لصورتها السياحية[1]، وهذا النوع يمس مباشرة بالمصالح الاقتصادية للدولة.

وعليه فإنّ مهما كان نوع الإرهاب الإلكتروني يظل خطرا يشكّل انتهاكا للحريات الشخصية خاصة بعد أحداث 11 سبتمبر، حيث قامت الولايات المتحدة الأمريكية بمراقبة البريد الإلكتروني وحجب بعض مواقع الانترنيت، إلاّ أن هناك جماعة استغلت هذا الوضع لأغراض غير قانونية، كما أن فكرة الجمع بين الإرهاب والتكنولوجيا أثر على الشركات العاملة في مجال التكنولوجيا والذي دفع بها إلى الخوف من توسيع دائرة أسواقها إلى الاستثمار في الخدمات الأمنية التكنولوجية من جانب، وإلى المنافسة الشديدة من جانب آخر بين الشركات العالمية، ضغطا على نفقاتها في البحث والتطوير.

قضيت الإرهاب الإلكتروني ذات أبعاد اقتصادية هامة، سواء من خلال الخسائر الضخمة التي قد تطول البنوك والصفقات العمومية المالية الدولية وأسواق المال ومحطات الطاقة، أو تأثير ذلك على الاقتصاد الرقمي الجديد الذي أصبح يشكّل جزء كبير من الناتج القومي الإجمالي للدول المتقدمة.

المبحث الثاني

مخاطر الإرهاب الإلكتروني على التجارة الإلكترونية

تستخدم الجماعات الإرهابية الإلكترونية الأجهزة الإلكترونية وشبكة الانترنت وأجهزة الحساب الآلي لمزاولة أنشطتهم الإرهابية بدلا من الأسلحة التقليدية، ويمكن القول أن هذا النوع من الإرهاب أصبح يشكل أكبر المخاطر والتهديدات المستقبلية للجرائم المعلوماتية وذلك بتوظيف مهارات الهاكرز [2] من قبل الجماعات الإرهابية، نحو

---

[1] – دعاء علي، مرجع سابق، ص 19.

[2] – الهاكرز (Hackers) كلمة تصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية، وأطلقت كلمة هاكرز أساسا على مجموعة من المجرمين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة، إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي يعلن عن نفسه، ولكن بعضها استغلها بصورة إجرامية تخريبية لمسح المعلومات، والبعض الآخر استغلها تجاريا لأغراض التجسس والبعض لسرقة الأموال لهذا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها، فوجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز مرتبات عالية مهمتهم محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبيل للوقاية اللازمة التي يتسبب فيها قراصنة الحاسوب، في هذه الحالة بدأت صورة الهاكرز في كسب الكثير من الايجابيات إلا أن المسمى الأساسي واحد، وقد أصبحت كلمة الهاكرز تعرف مبرمجا ذات قدرات خاصة يستخدمها في الصواب كما في الخطأ.

فئات مستهدفة، ما يهمنا هو مخاطر هذه الجماعة على التجارة الإلكترونية (**المطلب الأول)**، ثم التهديدات التي تعرقل سير النشاط التجاري الإلكتروني **(المطلب الثاني)**.

المطلب الأول

المخاطر الأمنية للإرهاب الإلكتروني على التجارة الإلكترونية

تتفاقم يوما بعد يوم ظاهرة الإرهاب الإلكتروني نظرا لاستعماله للتكنولوجيا الحالية بالإضافة للثغرات الأمنية المتعددة في التعاملات التجارية الإلكترونية، سهل كثيرا عمل الإرهاب الإلكتروني باستخدامه الفيروسات مثلا لإتلاف المعلومات والبيانات للمؤسسات الاستراتيجية الدولية، حيث يستهدف الإرهابيون عدة أهداف منها الاقتصادية أو التجارية على المستويين الإقليمي والدولي، وذلك عن طريق قرصنة و/أو تعطيل المعلومات**(الفرع الأول)**، أو عن طريق استغلال الشبكات الاجتماعية الموصولة بالانترنيت **(الفرع الثاني)**، أو بالتجسس على مختلف تعاملات التجارة الإلكترونية **(الفرع الثالث)**.

الفرع الأول

قرصنة و/أو تعطيل نظام المعلومات.

إن الحديث عن خطر قرصنة و/أو تعطيل نظام المعلومات، يأتي بتحديد الثغرات الأمنية للعملاء الاقتصاديين، وكذا أنماط الاعتداءات التقنية من طرف الإرهابيين فالفيروسات وسيلة هجوم شائعة من طرف الجماعات الإرهابية لإتلاف معطيات التعاملات التجارية مثلا، لكن أيضا يمكن أن تقوم هذه الجماعات بالعديد من وسائل الهجوم المختلفة لهذا فإننا نقف على أنماط الإرهاب الإلكتروني وأساليب التقنيات المستعملة، وكذا المخاطر والثغرات ليتضح خطر القرصنة والتعطيل لنظام المعلومات معا.

أولا – خرق الحماية المادية (Breachers of Physical Security):

أ – التفتيش في مخلفات تقنية(Dumpster Diving):

يقصد به قيام الإرهابيين بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة، بحثا عن شيء يساعدهم على اختراق النظام المعلوماتي للمؤسسات التجارية أو المالية كالأوراق المدون عليها كلمة السر، أو مخرجات الكمبيوتر، أو الأقراص

الصلبة المرمية بعد استعمالها أو استبدالها أو غير ذلك من المواد المكتوبة أو الأقراص في الاختراق[1].

ب – الالتقاط السلكي (wiretapping) :

وهو توصيل السلك المادي مع الشبكة أو توصيلات النظام لجهة استراق السمع بطريقة سهلة أو معقدة، تبعا لنوع الشبكة وطرق التوصل المادي.

ثانيا – خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين(Breachers of personnel security):

أ – التخفي بانتحال شخصية موظف:

وهو استخدام الإرهابي لوسائل التعريف العائدة للموظف المخول له هذا الاستخدام كاستغلال الإرهابي لكلمة سر أحد العمال، أو استغلال الصلاحيات المخولة للموظف كاقتناص شخصيته، أو إلغاء صفحة أو الحصول على معلومات[2].

ب – البرمجيات الخبيثة (Malicious code):

يقصد بها الفيروسات كفيروس حصان طروادة (Trojan Horses) أو القنابل المنطقية (Logic bombe)، تقوم هذه البرامج بمهام غير مشروعة كتدمير المواقع الإلكترونية للشركات التجارية، هذه الهجمات القائمة من طرف الإرهابيين خسائر بالملايين، وهذا ما سببه فيروس " **الشيفرة الحمراء**" على سبيل المثال، الذي ألحق أكبر الخسائر في بيئة الكمبيوتر والانترنيت قياسا بغيره من أعمال الإرهاب بالإلكتروني[3].

الفرع الثاني

استغلال الشبكات الاجتماعية المعلوماتية

تتمثل مخاطر الانترنيت بشكل عام في برامج التجسس والفيروسات والمواقع الإباحية ومواقع سرقة الملكية الفكرية، ومواقع الترويج للإرهاب، ومواقع مهاجمة الأديان، ومواقع العنف والانتحار والقمار وإدمان الألعاب، وكذا مواقع التدريج للأفكار العنصرية، دون المخاطر صحية عن كثرة الجلوس أمام الكمبيوتر.

ولكن الخطر الحقيقي ليس ذلك الذي نراه ولكن ما كان متخفيا، وهو ما تؤديه الشبكات الاجتماعية بطريقة يجهل معظمنا مخاطرها نلخصها كالآتي:

---

[1] – حكيم غريب، مرجع سابق ص 853.

[2] – سعاد إكرام عوض، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشأة المعارف الإسكندرية، 2008، ص 146.

[3] – سعاد إكرام عوض، مرجع سابق، ص 147.

أولا – مخاطر الشبكة الاجتماعية الفايسبوك (facebook):

انتشار الشبكة الاجتماعية الفايسبوك، جعل الحياة الاجتماعية لا خصوصية لها، فلقد عمل الفيسبوك على البحث في بيانات المستخدمين ووسائلهم وتعليقاتهم وحتى المحادثات الخاصة بين الأفراد المسجلين في أكبر موقع للتواصل الاجتماعي، حيث يمثلون أكبر مجتمع على الأنتيرنت، بقاعدة بيانات تضم 90 مليون مستخدم.

وعليه فإن معظم الشركات التجارية العالمية والمحلية ليست على معزل من هذه التصرفات في الفايسبوك، حيث يستطيع أي مجرم إلكتروني التجسس على تعاملاتها الاقتصادية وصفقاتها التجارية، وكذا تشويه سمعتها الاقتصادية بنشر معلومات أو صور كأن يقوم شخص وضع اسم مستعار لأحد المدراء أو المؤطرين للشركة أو أحد مستثمريها من أجل تشويه سمعته مما يثير عدة مشاكل لا حصر لها[1]

ونأخذ كمثال ما حصل مع مؤسس شركة (Apple)للأجهزة الذكية،ستيف جوبس (Steve JOBS)، الذي تعرض لهجوم لاذع عن طريق الفيسبوك، من قبل جامعة تتهمه بسرقة برامج الهواتف النقالة الذكية وتطبيقها على منتجاته، في حين أنه يملك براءة اختراع على معظم منتجاته، كما شهد عدة إشهارات مزينة وغير نزيهة على عدة صفحات فيسبوك للإطاحة باختراعاته عام 2010.

ثانيا – مخاطر محرك البحث غوغل (google):

وجدت التنظيمات الإرهابية في وسائل الاتصال ملاذا آمنا لبث أفكارهم، واستخدام عناصر جديدة، كما أعطاها الانترنيت كم هائل من المواقع التي تحتوي على تكتيكات وإرشادات تشرح طرق صنع المتفجرات، كيفية قرصنة المواقع والحصول على كلمات السر وغيرها من الموضوعات، إذ شهد استخدام محرك غوغل " google" سنة 2005 للبحث عن مواقع تضم بموضوعاتها كلمات مثل " الإرهابي (Terrorist) و"دليل (Hands book) نتائج بحث تتجاوز ما يقارب 8000 موقع، وقد رصد باحثون في مجال الإعلام الآلي والقرصنة تجاوزات هذه المواقع إلى ما يؤدي إلى البحث والترويج وخلق ما يسمى بالإرهاب الإلكتروني[2].

بالرجوع إلى خصائص محرك البحث (GOOGLE) الذي يعتبر أهم محرك بحث في العالم، إذ يحتوي على مليارات المعلومات المعلوماتية التي يتم تحميلها أو تغييرها من

---

[1] – فايز الشهري، مرجع سابق، ص 96.

[2] – B-HOFMAN, THE USE of the internet by Islamic Extremists testemony the house of permanent, may 2006, p102.

ثانية إلى أخرى، وكذا سرعة تقديم الأجوبة أو المعلومة ناهيك عن عدد الصفحات اللامتناهية فيه جعلت منه أهم سبيل وأسرعه في إيجاد الإرهاب الإلكتروني من خلال تفسير الأساليب التي يصبح بها أي شخص مجرم إلكتروني، إضافةً إلى عدم وجود رقابة على ما يتم نشره من أمور غير قانونية وغير شرعية، إذ أن شركة (google)تلقت العديد من الشكاوى التي كان محتواها انتهاك خصوصية الأفراد عن طريق المحرك والحصول على ملفات وصور شخصية من أجهزتهم، بيد أن هذا أحد بنود سياسة عمل شركة google وهو سلاح ذو حدين، لأن الشركة تستعمل ذلك البند لدواعي أمنية ولكن أصحاب النفوس الإرهابية لقو الفجوة للتجسس، للاعتداء ونشر السياسة الإرهابية.

ثالثا – مخاطر خدمة الفيديو (You tube):

هي من أبرز الخدمات المطروحة على شبكة الانترنيت من قبل شركة (google) والتي تقدم المادة الإعلامية إلكترونيا، صوت و/أو صورة، وإمكانية الاحتفاظ بها، كما توفر هذه الخدمة أقدم وأحدث البرامج التلفزيونية للأحداث العالمية، والتي يحتفظ بها الجمهور ويسارعون إلى نشرها عبر ال(You tube).

إلا أن أصحاب النفوس الإجرامية والإرهابيين، استغلوا هذه الخدمة من أجل عرض مختلف جرائم القتل، وكذا مهاراتهم في تحويل رؤوس الأموال من البنوك العالمية لحسابات خاصة دون رصدهم، وتصوير اعترافاتهم بوجوه غير مكشوفة... الخ، وهي المشاهد التي ترفض الفضائيات عرضها إلى المشاهدين[1].

يبدو مما سبق عرضه، أنه بفضل المواقع الاجتماعية المعلوماتية وغرف الدردشة جمعت في وقت واحد محدد، عددا من الأشخاص في أماكن جغرافية متفرقة، للتشاور وتبادل المعطيات والاستراتجيات، ونقل الملفات والمعلومات بسرعة مذهلة، ولكن تبقى غير آمنة لأنها كانت السبب في نشر أفكار الإرهاب الإلكتروني والترويج لجرائمهم الإرهابية لكسب الدعم والإتباع، زعزعة الاستقرار الاقتصادي والسياسي والاجتماعي على الصعيدين الداخلي والخارجي.

الفرع الثالث

تأثير التجسس على التجارة الإلكترونية

مما لا شك فيه أن الاقتصاد يعتبر من العوامل الرئيسية في سيادة الدول وأمنها وتهدف الجماعات الإرهابية من خلال التجسس على المعلومات الصناعية والمالية

---

1 – Raul ATAYLOR, Maestros ormisogvnistis ? Gender and the social construction of haking, y-vonne tweaks, william publiching, 2003, p140.

والتجارية، إلى ضرب موقع القوى الاقتصادية لدولة ما، لمعرفة مواردها وثرواتها ووضعها المالي والنقدي، وبالتالي معرفة ثغرات ومواطن الضعف في هيكلها الاقتصادي، بهدف ضرب المواقع الخاصة بالشركات العمومية الكبرى، وتخريب معلوماتها من خلال زرع الفيروسات، وأما عن طريق الابتزاز فيكون وطلب الفدية مقابل إطلاق سراح المختطفين الرهائن، وهكذا تكون شبكة الانترنيت الوسيلة والأداة لتحقيق أهداف الإرهابيين[1].

ومن جهة أخرى الشبكة العنكبوتية عبارة عن سوق مفتوحة لجميع الدول، تتم من خلالها مجموعة من التعاملات بمبالغ ضخمة تصل إلى مليارات الدولارات، مما جعل الجانب الاقتصادي للانترنيت أكثر خطورة لان الإرهابيين دائما ما يسعوا إليها لسببين: الأول بحاجة إلى الأموال، والثاني هو أن الهجمات الموجودة ضد نظم المعلومات الاقتصادية لها تأثير كبير في الرأي الدولي[2].

من الأمثلة على الهجمات الاقتصادية، العملية التي قامت بها مجموعة من الإرهابيين أطلقوا عليها اسم "**نادي الفوضى**" سنة 1997، حيث قامت هذه الجماعة بإنشاء برامج تحكم اللغة " **أكتف إكس**" مصمم العمل على شبكة الانترنيت، يمكنه أن يخدع برامج **(Quicken)** الذي يقوم بتحميل الأموال من الحسابات المصرفية، بالتالي لاستخدام هذا البرنامج أصبح بإمكان الإرهاب سرقة الأموال من أرصدة مستخدمي البرامج في جميع أنحاء العالم[3].

وهكذا اعتبر الإرهابيون الجدد الانترنيت من أفضل الأسلحة الناعمة في أداء العمل الإرهابي، بدون عنف أو إراقة الدماء، يضربون بها الاقتصاد والمؤسسات الكبرى عن طريق التجسس الإلكتروني الذي سمح لهم بتبادل المعلومات ودفع الخطة والتدريبات بين الجماعات الإرهابية، كما اتخذ الإرهاب أبعاد جديدة، وتحددت تقنياته ومخاطره وتهديداته على الحياة الاجتماعية والاقتصادية والسياسية.

وكما سبق الإشارة التجسس الإلكتروني الذي تقوم به الجماعات الإرهابية، غايته الإخلال بالنظام الدولي بالدرجة الأولى، يكون موجهة نحو برامج ومعلومات وأنظمة الشبكة العنكبوتية التي تتحكم في نظم تشغيل النظام الاقتصادي والتجاري والصناعي مثل الشركات العمومية العامة في خدمات الطاقة والكهرباء، الماء، والاتصالات والمواصلات

---

[1] – حكيم غريب، مرجع سابق ص 840.

[2] – سهيلة خليل الغازي، مرجع سابق، ص 106.

[3] – المرجع نفسه، ص 110.

والملاحة الجوية والبحرية، وكذا نظام المصاريف والبورصات... الخ والرسالة الموجهة من طرف الجماعات الإرهابية «***نستطيع أن نسيطر على مختلف جوانب الحياة***»[1].

ولقد حدد رئيس لجنة حماية البنية التحتية مخاطر وتهديدات تكون لها أثر على الحياة البشرية وهي:

1 – مخاطر على وسائل الاتصال وشبكات المعلومات عن طريق التجسس.

2 – مخاطر على قطاعي الغاز والبترول إثر هجوم يؤدي إلى انقطاع في إمداد مصادر الطاقة .

3 – مخاطر على قطاع النقل كالعبث في شبكات التحكم ما يؤدي إلى إضرابات.

4 – مخاطر على قطاع شبكات المياه حيث تستعمل التكنولوجيا في توزيع المياه وقطعها يؤدي إلى إفساد شبكات صرف المياه وبالتالي انتشار الأمراض.

5 – مخاطر على قطاع خدمات الكهرباء حيث أن قطع هذه الأخيرة يؤدي إلى إحداث تذبذبا في الجهد الكهربائي، بالتالي خسائر مادية عظمى.

6 – مخاطر في قطاع الحكومة عبر استهداف واستخدام الشبكات الحكومية الالكترونية مما يؤدي إلى تعطيل الخدمات وإحداث خلل في سير عمل الحكومة وحياة المواطن.

7 – مخاطر على قطاع خدمات الطوارئ حيث تم القبض على هاكر في ولاية تكساس سنة 2000 وهو يحاول زرع فيروسا لتعطيل خدمة الطوارئ 911.

8 – مخاطر على قطاعي البنوك وشركات المال حيث يتم تزيف في أسعار الأسهم والعملات وهذا يؤدي إلى حدوث خسائر مادية وخلق أزمات اقتصادية كبرى.

يصل بنا القول أنه من السهل أن تشن حربا في الفضاء الإلكتروني على العدو بتحول الإرهاب إلى الحاسب الآلي والانترنيت من خلال قيام الجماعات الإرهابية بالهجوم الإلكتروني والتجسس الإلكتروني، ونشر الفيروسات داخل شبكات البنية التحتية ، التي تدار في العالم عن طريق الانترنيت.

المطلب الثاني

المخاطر التجارية للإرهاب الإلكتروني

أعمال الإرهاب الإلكتروني لا تنحصر فقط في كل ما هو تهديد أمني بل تتعدى ذلك لتصل الى تهديدات تجارية تزعزع نظام الاقتصاد والتجارة الإلكترونية الدوليين،

---

[1] – Aye embar SEDDON, cyber terrorisme, the American Behavioral Scientist-vol 45 hsseve (6) fel 2002 p 43.

هذه الأنشطة تتمثل في الاستخدام اليومي للانترنيت من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المنتشرة عبر موقع الشبكة العنكبوتية، وهو التهديد الفعلي في هذه الحالة للشبكة المعلوماتية في معاملات التجارة الإلكترونية (**الفرع الأول**)، غير أن الإرهاب الإلكتروني لا يتوقف عند هذا الحد بل يواصل أعماله التدميرية باختراق مواقع التجارة الإلكترونية **(الفرع الثاني)**.

تعاملات التجارة الإلكترونية تعتمد على النقود بمفهومها التقليدي وأيضا المال الافتراضي الذي يعتمد على بطاقات الدفع الإلكترونية، غير أن هذه البطاقات في الوهلة الأولى تبدو وسيلة أكثر ائتمانا إلا أنها لم تسلم من الإرهاب الإلكتروني الذي أصبح يستعملها لتمويل أو سرقة أصحابها من خلال إساءة استعمالها **(الفرع الثالث)**.

الفرع الأول

موقع الشبكة المعلوماتية في المعاملات التجارية الإلكترونية

تعمد المؤسسات والشركات وحتى الأفراد إلى مواقع الشبكة العنكبوتية للتعريف بأنفسهم وإتاحة المستخدمين بنشر منتوجاتهم وأعمالهم، فقد وصل عدد مواقع الانترنيت حتى شهر أكتوبر 2010 إلى أكثر من 232 مليون موقع[1].

أمام هذا التزايد المستمر والهائل للمواقع الإلكترونية، تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال الشبكة العنكبوتية بإنشاء مواقع لهم لنشر أفكارهم والدعوة إلى مبادئهم، بل وصل الأمر إلى استفادتهم من هذه المواقع في تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية.

صدر في هذا الصدد دراسة عن معهد السلام الأمريكي للخبير الدولي " جابريال ويمان (Gabriel WEIMAN)، وهو يتعرض بالتحليل الوافي للزيادة المخفية في عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على شبكة الأنتيرنت، مما يعد مؤشرا جد خطير لوجود حوالي 4800 موقع في الوقت الحالي، متخصص في الإشهار، ونشر العمليات الإرهابية، وتزويد العام والخاص بالمعلومات السرية من أجل أحداث الفوضى في المجتمع... الخ، وهذا إن دل على شيء، إما يدل على وجود حرب معلوماتية في ساحة الشبكة العنكبوتية لا نراها، وبالتالي نجهل وجودها أساسا.

إن الإرهاب الجديد أصبح أكثر خطورة لاعتماده على التكنولوجيا التي ساعدته في التحكم الكامل باتصالاتهم، مما زاد اتساع سرعة عملياتهم وبالتالي أصبح من الصعب مكافحة هذا الإرهاب الجديد، غير أنه تبقى وظيفته الرئيسية التجسس على كل التعاملات

---

1 – http://neus-neteraft.com

الاقتصادية، قصد منع التبادلات التجارية عن طريق وسائل التكنولوجيا، تحويل رؤوس الأموال، التجسس على المحادثات عبر الهاتف أو الانترنيت، التطلع على الوثائق الرسمية مهاجمة المراكز الرئيسية الاقتصادية بتخريب الحواسب، أو نظم الاتصال أو قاعدة البيانات كل هذه التصرفات تمس بصفة مباشرة التجارة الإلكترونية [1] هذه الأخيرة جعلت من العالم قرية صغيرة، وفرت الوقت، وخاصة كانت السبب في خلق علاقات اقتصادية بين دول فرقت بينها السياسة والجغرافيا، كما أن التجارة الإلكترونية أحد أهم الأسباب التي تحاول النهضة بالاقتصاد العالمي عكس الإرهاب الإلكتروني الذي يحاول القيام بعكس ذلك تماما.

لا يهم هذه الجماعة الإرهابية كم من الناس قتلوا، بقدر ما يهمهم كم عدد المراكز التي دمرت إلكترونيا، كم من الأموال تم تحويلها إلكترونيا في حسابات أفراد الخلية الإرهابية والتي تعتبر أحيانا مجموعة قليلة من الناس مبعثرة جغرافيا، لتشكل مجتمعا خاصا بها يساعدها على التطور والتواصل المستمر.

ومن هنا يجب التأكيد أن الجماعات الإرهابية في السابق كان سلاحها الرشاش، أما اليوم فجهاز كمبيوتر موصول بالانترنيت وهو الوسيلة الرئيسية في نشر الإرهاب الإلكتروني.

الفرع الثاني

اختراق الإرهاب الإلكتروني لمواقع التجارة الإلكترونية

إن معاملات التجارة تعتمد على الثقة في البيانات المعطاة، سواء كانت بيانات عامة عن الشركة التجارية، أو بيانات شخصية عن العملاء والموردين، لذلك فأهم ما يجب أن تتصف به التجارة الإلكترونية هو حمايتها بالمحافظة على سرية المعلومات والحديث عن التهديدات التي تواجه التجارة الإلكترونية في تزايد مستمر كلما تطورت التكنولوجيا، نذكر أهمها:

أولا – انتهاك نظام الحماية السرية للتجارة الإلكترونية:

يستطيع الإرهاب الإلكتروني التوصل إلى المعلومات المالية والشخصية، واختراق الخصوصية وسرية المعلومات بسهولة، ذلك راجع إلى التطور الهائل للحاسب الآلي وتقوم الجريمة المعلوماتية والسبل المتاحة لارتكابها، خاصة بالرجوع إلى كون مرتكب

[1] – حكيم غريب، المرجع نفسه، ص 860.

الجريمة ليسوا بأشخاص عاديين، إنما خبراء كمبيوتر [1]، وقد يتم الاختراق أيضا عن أشخاص آخرين غير الإرهابيين وهم الأشخاص المتدخلون في خدمة الانترنيت، أي الذين يعملون كوسيط بين الشخص طالب الخدمة، وبين الشبكة، هؤلاء هم[2]:

1- متعهد الوصول: ويقصد به أي شخص معنوي أو مؤسسة أو شركة تقوم بدور فني يتمثل في توصيل الجمهور بشبكة الانترنيت.

2- متعهد الإيواء: هو ذلك الشخص الذي يسمح بالوصول إلى موقع من خلال شبكة الانترنيت.

3- ناقل المعلومات: هو العامل الفني الذي يقوم بالربط بين الشبكات، أي نقل المعلومات في هيئة حزم من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الحواسب المرتبطة بمواقع الانترنيت.

- مورد المعلومات: وهو الشخص الذي يقوم بتحميل الجهاز أو نظام المعلومات التي قام بتأليفها أو جمعها حول موضوع معين، وبالتالي تكون له سيطرة كاملة على المعلومات التي يقوم ببثها عبر الشبكة.

- متعهد الخدمات: وهو ناشر الموقع، وهو المسؤول الأول عن المعلومات التي تعبر الشبكة لأنه هو الوحيد الذي يملك سلطة حقيقة لمراقبة المعلومات.

وهناك عدة طرق يمكن عن طريقها التقاط المعلومات التي تتعلق بالتجارة الإلكترونية:

- التوصيل المباشر على خط هاتفي بوضع مركز تصنت يسهل الاتصالات.

- التدخل غير المشروع في نظام معلوماتي بواسطة طرفية بعيدة تسهل فسخ أو تدمير بعض المعلومات.

- التقاط المعلومات المتواجدة ما بين الحاسب الآلي والنهاية الطرفية.

---

[1] - علاء علاء الصراط الغامدي، مرجع سابق، ص 50. وراجع أيضا بهذا الصدد: دعاء علي، مرجع سابق، ص 200.

[2] - الإشارة إلى هؤلاء الأشخاص ليس القصد به حصر المسؤولين عن مهاجمة مواقع التجارة الإلكترونية، وإنما تبيان أساس المسؤولية عندهم، إذ أن مستخدمي الشبكة والقراصنة، تقوم مسؤوليتهم بمجرد المحاولة غير المشروعة، لدخول الموقع، إنما المستخدمين العاديين تقوم مسؤوليتهم متى دخلوا الموقع دون سداد رسم معين، أو لم يكن مشتركا أو تعد من دخوله المدة المحددة له.

بالرغم من أن الاختراق لمواقع التجارة الإلكترونية من الأخطار الحقيقية التي آلت إلى وجود هذا النوع من التهديد الإلكتروني، إلا أن غياب تعاون دولي لمواجهة هذه الظاهرة يعتبر أيضا معوق للتجارة الإلكترونية ويتمثل في:

- عدم وجود قانون دولي يجرم هذا النوع من الجرائم.
- عدم وجود السلطة القضائية المخصصة لمثل هذه الجرائم.
- عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما في شبكة "يوروبول"[1].
- الاختراق في الشكل والحجم الذي تتخذه تلك الجرائم.
- صعوبة السيطرة على الإرهابيين.
- وجود بعض المواقع على شبكة الانترنيت دون رقابة والتي يمكن من خلالها إرسال أي رسالة دون تحديد اسم المرسل أو العنوان.

ثانيا – إتلاف مواقع التجارة الإلكترونية باستخدام الفيروسات:

الفيروس كما سبق الإشارة إليه هو برنامج للحاسب الآلي، يهدف إلى إحداث أكبر ضرر بنظام الحاسوب، وله القدرة على ربط نفسه بالبرامج الأخرى وإعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيا، ويقوم الانتشار بين برامج الحاسب الآلي وبين مواقع مختلفة في الذاكرة.

من خصائص الفيروس أنه معدي، إذ هو عبارة عن مجموعة من التعليمات والأوامر المتعارضة والممنوعة وغير المشروعة، وتتلخص وسائل عدوى الفيروس في ثلاث طرق كما حددها اتحاد الفيروس للكمبيوتر بولاية كاليفورنيا الأمريكية من خلال نقل الأجهزة، أو من خلال شبكات الاتصال ، وأخيرا من قرص ليس مصابا من مصدر خارجي[2].

رجوعا إلى كون التجارة إلكترونية تعتمد في تصرفاتها نظام الحاسب الآلي المتصل بشبكات المعلومات كأحد الآليات التي يتم من خلالها ممارسة مختلف النشاطات التجارية

---

[1] – الشبكة الأمنية يورب بول هي شبكة نظام ربط أجهزة الحاسب الآلي باستخدام تقنية نظم المعلومات بين دول الاتحاد الأوروبي من اجل تبادل المعلومات والموارد والبيانات أو البرامج التطبيقية أيا كان نوعها بين المستخدمين، بطريقة جد أمنية حيث تتضمن تصميم صناعي لكيفية وضع التدابير الأمنية المضادة للاختراقات وكل أنواع الانتهاكات المعلوماتية، هذه الشبكة المنية تخدم غرض الحفاظ على السمات النوعية للنظام المعلوماتي من بينها السرية والعلانية، على الموقع: الشبكة الأمنية اليوروبول /http://ar.wikipedia.org/uniki

[2] – Frédéric BULOI, Internet et commerce électronique, 2ème édition, éditions Hermès, Paris, 2003,(pp 24 – 25).

الإلكترونية، فإنّ الفيروس المعلوماتي الذي ينشط هو الآخر على نفس مستوى التجارة الكترونية، يتميز بخاصيتين في غاية الخطورة، أولها الانتقال والانتشار والثانية التدمير.

وأما بخصوص انتقال الفيروس وانتشاره، فالفيروس ينتقل من جهاز إلى آخر بسرعة يساعده في ذلك وجود وسائل اتصال حديثة، وأما بخصوص أثر الفيروس في التدمير، فإنّ ذلك الفيروس يرتبط ببرنامج معين يدخلها المستخدم أو تاريخ معين أو ساعة معينة، وبعدها يبدأ الفيروس في التدمير والذي يشمل مسح البيانات المخزنة، ومن أعراض الإصابة بالفيروس بطئ نظام التشغيل، ضيق السعة التخزينية، كما يؤدي إلى تشويش المعلومات وكذا إدخال معلومات غير صحيحة.

هذا التدمير أو الانتقال للفيروسات تتبين خطورتها تبعا لتكوينها وهدفها وهي:

1 – فيروس محدد العدوى: يستهدف نوع محدد من النظم لمهاجمتها ويتميز ببطئ في الانتشار ويصعب اكتشافه.

2 – فيروس عام العدوى: ينتقل إلى أي برنامج أو اي ملف.

3 – فيروس عام الهدف: ويندرج في إطاره غالبية الفيروسات، يتميز بسهولة إعذاره واتساع تدميره.

4 – فيروس محدد الهدف: هو لا يعطل البرنامج، بل يغير الهدف منه، كأن يحدث تلاعب ماليا أو تعديل معين في تطبيق ما، وهو يحتاج إلى مهارة عالية ودراية تامة.

هذه هي خطورة الفيروسات في إتلاف أو تدمير مواقع التجارة الإلكترونية، إذ مستقبل هذه التجارة مرهون بمدى تقدم سبل الحماية الفنية لمواقع التجارة الإلكترونية من الاختراق أو حمايتها من الفيروس ضد الإتلاف أو التدمير.

الفرع الثالث

مشكل بطاقات الدفع الإلكترونية (بطاقات الائتمان)

بموجب بطاقات الدفع يمكن لحاملها سحب المبالغ النقدية من ماكنات سحب النقود الخاصة بالبنوك، أو أن يقدمها كأداة وفاء للسلع والخدمات للشركات والتجار الذين يتعامل معهم، وتستخدم هذه البطاقة من قبل حامليها كوسيلة وفاء لالتزاماتهم بدلا من الدفع الفوري بالنقود، و لابدّ أن يتأكد من توافر عدة شروط في حق العميل وتتمثل في ضمانات شخصية وعينية يقدمها العميل وتصدر البطاقة في حدود ثمن مالي معين لا يجوز تجاوزه، وذلك وفقا لشروط البنك التي تكون معدة سلفا من قبله[1].

[1] – محمد سليمان أحمد، أساسيات الاستثمار الإلكتروني وتحليل الأعراف المالية، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 2005، ص 76.

هذه بطاقات منها ما هو محلي لا يتجاوز استعماله حدود الدولة التي صدر فيها ومنها ما هو عالمي يستخدم في كل دول العالم، وهناك البطاقة الذهبية التي تمنح حاملها سقفا ائتمانيا عاليا، أطراف العملية المصرفية التي تتم عن طريق هذه البطاقات هم بنك العميل حامل البطاقة، وكذلك حامل البطاقة والتاجر وبنك التاجر، أما البطاقة ذاتها تحمل البيانات السالفة الذكر، بالإضافة إلى البيانات الأخرى تتعلق بالصورة المجسمة ثلاثية الأبعاد، وهو ما يطلق عليه اسم الهولوجرام، وتتضمن كذلك شريط التوقيع ورقم التمييز الشخصي.

الاستعمالات غير القانونية لبطاقة الائتمان تكون في:

أولا – إساءة استعمال بطاقة الدفع الإلكتروني من طرف حاملها:

يقصد بحامل البطاقة ذلك الشخص الذي يحصل على البطاقة من البنك بمقتضى اتفاق بينهما، أساليب تلاعب حامل البطاقة أو العميل كثيرة ونذكر منها:

1 – الحصول على بطاقات الائتمان صحيحة بناء على مستندات مزورة بأن ينتحل صفة الغير أو يقدم بيانات غير صحيحة، فلا يتمكن البنك من استرداد قيمتها بعد ذلك لعدم الاستدلال على صاحب البطاقة.

2 – الغش الذي يرتكبه حامل البطاقة بعد انتهاء مدة صلاحيتها، فيجب على العميل إعادة البطاقة عند انتهاء مدتها للبنك لكن قد يفكر باستخدامها رغم انتهاء مدتها.

الحالة الثانية: يقوم صاحب البطاقة باستعمالها رغم إلغائها من قبل البنك.

وإلى جانب الصور السابقة هناك صور أخرى لإساءة الاستعمال قد تقع منها[1]:

– تجاوز حد السحب بالتواطئ مع الموظف أو التاجر.

– التحايل على نقاط البيع العاملة خارج الخط.

– استخدام خدمات نقاط البيع الإلكتروني في إيداع شيكات بدون رصيد بحيث تضاف قيمة الشيك إلى قيمة الحساب الأصلي، ثم يلجأ العميل لتحصيل قيمة هذه الشيكات بواسطة نقطة البيع الإلكترونية قبل تمام المناقصة بالبنوك.

ثانيا – إساءة الاستعمال من قبل الغير:

يقصد بالغير أي شخص غير التاجر الذي يتعامل معه حامل البطاقة أو موظفي البنك المصدر للبطاقة فهؤلاء لهما أحكاما خاصة، وتظهر مشكلة الغير لو فقدت البطاقة أو سرقت، وكذلك في حال ضياع أو سرقة الرقم السري الخاص بها، وبمجرد فقد البطاقة ورقمها السري على العميل إبلاغ البنك المصدر حتى لا يتحمل مسؤولية المبالغ

[1] – محمد سليمان أحمد، المرجع السابق، ص ص 80 – 81.

التي يسحبها الغير من رصيده، فيرى جانب من الفقه الجنائي أن استعمال البطاقة المسروقة من قبل الغير ينطوي على جريمة النصب لأن المتهم انتحل اسما كاذبا، ويرى جانب آخر أن هذا الفعل يشكّل جريمة سرقة مفتاح مصطنع لبطاقة ائتمانية[1].

كما يحدث أن يقوم الغير بتزوير بطاقات الدفع أو السحب عن طريق بطاقات ائتمان مسروقة ومن ثم استبدال ما بها من بيانات.

ثالثا – إساءة الاستعمال من قبل موظفي البنوك:

يتم التلاعب ببطاقات الائتمان من طرف موظفي البنك باتفاق موظف البنك مع العميل حامل البطاقة أو بالاتفاق مع التاجر أو مع الغير، وهذا الاتفاق تنعكس صورته فيما يلي:

- استخراج بطاقة تعليمة البيانات.
- السماح للعميل بتجاوز حد البطاقة في السحب.
- السماح للعميل بتجاوز انتهاء الصلاحية، أو غض الطرف عن قرار سحبها.

وأما اتفاق موظف البنك مع التاجر في صورته غير الشرعية يكون في:

- تجاوز حد السحب في صرف قيمة إشعارات.
- اعتماد إشعارات بيع صدرت إلى بطاقات وهمية أو مزورة أو منتهية الصلاحية أو مسحوبة، وأخيرا قد يتواطئ موظف البنك مع عصابات إجرامية ويمدهم بدون وجه حق بيانات بطاقة الوفاء أو السحب الصحيحة والمتداولة لاستخدامها في التقليد.

رابعا – إساءة الاستعمال من قبل التاجر:

التاجر له دور كبير في إتمام عمليات البيع أو تقديم الخدمة باستخدام بطاقات الدفع الإلكترونية، إذ يقوم التاجر باستخدام البطاقات التي ليس لها أرصدة كافية للصرف، وذلك عن طريق إجراء عمليات بيع عديدة بمبالغ صغيرة، وصرفها من البنك، ثم يتضح عدم وجود أرصدة لأصحاب هذه البطاقات، كما يقوم بعض التجار بقبول البطاقات المزودة من العملاء والتلاعب ببرنامج الماكنة[2].

خامسا – إساءة استعمال بطاقات الائتمان عن طريق شبكة الانترنيت:

نظام الدفع الإلكتروني مبني على أساس عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد فيه حسابه من

---

[1] – Jacque-Robert BROUEN, Gestion des risques bancaires, Dalloz, Paris, 2000, p 79.

[2] – Jacque-Robert BROUEN, Gestion des risques bancaires, op.cit, p 145.

خلال شبكة تسوية إلكترونية للهيئات الدولية الفيزاكارد والماستركارد [1]. ويتم الحصول على السلع والخدمات بمقتضى هذه البطاقة وسداد قيمة هذه السلع بطريقتين هما:

– في حضور العميل بأن يحصل التاجر على بصمة بطاقة العميل مطبوعة إشعار البيع من الماكنة مع أخذ توقيع العميل على الإشعار، وهذه الطريقة تسمى (face to face transaction).

– أو عن طريق تصريح كتابي أو تلفوني بخصم القيمة على حساب بطاقة الدفع الإلكتروني التي تخصه، وهذا يطلق عليه(Ordre Moil thone)، وهنا يدخل استخدام شبكة الانترنيت.

تمكن الإرهاب الإلكتروني من التقاط أرقام بطاقات الدفع الإلكتروني الخاصة ببعض العملاء من الشبكة، واستخدموا أرقامها في الحصول على السلع التي يرغبونها، رغم خصم القيمة من حساب العملاء الشرعيين لهذه البطاقة، يتبع هذا النوع من الإرهاب عدة طرق في ذلك، نذكرها على سبيل المثال:

– **الاختراق غير المشروع لمنظومة الاتصالات العالمية (Illegalaccess):** وهي الخطوط التي تربط الحاسب الآلي للمشتري بالتاجر، بهدف الحصول على الأرقام الخاصة بالبطاقات الائتمانية المملوكة للغير، وذلك عبر موقعهم على شبكة الانترنيت.

– **تقنية تفجير الموقع المستهدف:** يعتمد على منح الآلاف من الرسائل الإلكترونية من جهاز الحاسب الآلي للمجرم، إلى الحواسيب المركزية للبنوك والمؤسسات المالية بهدف التأثير على السعة التخزينية للحاسوب وزيادة الضغط عليه حتى تفجير العامل على الشبكة وتشتيت المعلومات والبيانات المخزنة فيه، ومنه تحصيل البطاقات الائتمانية[2].

– **أسلوب الخداع:** ويكون بإنشاء مواقع وهمية على شبكة الانترنيت، وكأنه موقع أصلي يقدم الخدمة، ويتحقق الضرر باستقبال الموقع الوهمي لكافة المعاملات المالية والتجارية الخاصة بالتجارة الإلكترونية والتي يقدمها الموقع الأصلي عبر الشبكة ومنها

---

[1] – الفيزاكارد والماستركارد بطاقات ائتمانية تحتوي على رصيد يسمح لصاحبها السحب منها بأي وقت بنسبة فائدة محددة متفق عليها مع العميل، الرصيد الموجود في البطاقة يعرف بأسهم الحد الائتماني وهو محرر حسب الجهة المصدرة للفيزا، بالنسبة للشهرة بين الفيزا والماستر كلاهما تؤديان الغرض نفسه، فقط الماستركارد في أوروبا وبريطانيا والفيزاكارد في أمريكا، على الموقع:
http://www.mbt3th.us/vb/forum127/thread171445.htm

[2] – محمد سليمان أحمد، المرجع السابق، ص90

بيانات بطاقة الدفع الإلكتروني، ومن ثم يتسنى الإطلاع عليها والاستفادة غير المشروعة من المعلومات المتضمنة فيها.

- **تحصيل أرقام بطاقات الائتمان:** تعني تحصيل بطاقات الائتمان الاعتماد على إجراء محاولات رياضية وإحصائية بهدف تحصيل أرقام بطاقات ائتمانية مملوكة للغير، فهذه العملية تؤدي في النهاية لناتج معين هو الرقم السري لبطاقة ائتمان متداولة.

الفصل الثاني

التدابير الدولية والوطنية في مكافحة الإرهاب الإلكتروني

تتعدد الآليات وطرق مكافحة الإرهاب الإلكتروني على المستويات الدولية الإقليمية وكذا الداخلية، بحكم أن هذه الظاهرة تعد سلوك إجرامي مدفوع بأسباب مختلفة سياسية، اقتصادية أو اجتماعية...الخ ضد نظم المعطيات المعلوماتية بأنواعها وبرامج الكمبيوتر والاتصالات، تحقيقا لأغراض إرهابية تنطوي على العنف، التهديد، الاستغلال الذي يستهدف حياة الأشخاص وسلامتهم وإثارة الخوف وتعطيل الأداء الطبيعي لنظم السيطرة والرقابة الالكترونية، وكذا عمل الأجهزة والهيئات الحكومية والمرافق الإستراتيجية في الدولة.

إن الحاجة إلى اتخاذ تدابير دولية لردع ظاهرة الإرهاب الالكتروني كونه ذو طبيعة معنوية وليس مادية كما في الجرائم التقليدية، فعندما يكون الكمبيوتر مثلا هدافا للإرهاب فإن السلوك يستهدف بيانات تمثل قيما مالية أو اعتبارا ماليا، وعندما يكون الكمبيوتر بيئة للجريمة الإرهابية فإن مضمون الفعل غير المشروع هو انتهاك المعلومات وهو التهديد الحقيقي الذي دعا تكاثف الجهود الدولية (**المبحث الأول**)، أما بالرجوع إلى الشرعية الجنائية الإقليمية 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 الإقليمية والوطنية محاولة إما الحد من هذا الإجرام، أو حصره وتفادي ما يسببه من خسائر على جميع الأصعدة (**المبحث الثاني**).

المبحث الأول

الجهود الدولية لمكافحة الإرهاب الإلكتروني

تكاثفت الجهود الدولية لحماية البيئة الإلكترونية بكل تطبيقاتها وعناصرها من خطر الإرهاب الإلكتروني بشتى أنواعه وأشكاله وفي جميع صوره الإجرامية، كالجريمة الالكترونية التي تستهدف المعطيات بأنواعها وتستخدم التكنولوجيا لارتكاب جرائم تمس الأموال والأشخاص وعمل المؤسسات الحكومية، وهذا ما أدى إلى وجود تعاون دولي ينتهج إستراتيجية دولية لحماية التجارة الإلكترونية (**المطلب الأول**)، دون أن نفصل دور المنظمات التي كانت هي أحد أهم العوامل الدولية التي تصدت إلى الإرهاب الالكتروني (**المطلب الثاني**).

المطلب الأول

تحديد منهج دولي لحماية البيئة الإلكترونية

بات مؤكدا أن جرائم الإرهاب الإلكتروني هي جرائم عابرة للحدود أي أنها لا تتم ولا تنتهي في أراضي دولة بعينها، وعليه فالحديث عن ضرورة إيجاد إستراتيجية دولية لمحاربة الإرهاب الالكتروني وتأمين البيئة الإلكترونية، يأتي نظرا لتزايد عدد الهجمات الإرهابية على المستوى الدولي لأسباب عديدة أبرزها التحديات والعوائق لمحاربة هذه الظاهرة خاصة في المجال الأمني، وهو أحد أهم الأسباب في نجاح الإرهابيين في استغلال التكنولوجيا في أنشطتهم، بالإضافة إلى ضعف التشريعات والعقوبات المخصصة لهذا النوع الجديد من الإرهاب.

فبغير وجود منهج دولي لمكافحة هذه الظاهرة، يظل الإرهابي يقوم بعملياته بكل حرية متنقلا من دولة إلى أخرى ضامنا عدم القبض عليه، وهو ما كان أحد أهم الأسباب التي أدت إلى ضرورة إيجاد آليات الأمنية دولية للحد منه **(الفرع الأول)**، ثم لا بد من أن يكون هذا التعاون أمنية مصحوبا بآليات تقنية دولية لحصره بحكم أنه ينشط في عالم إلكتروني افتراضي **(الفرع الثاني)**.

الفرع الأول

الآليات الأمنية الدولية المكرسة للحد من الإرهاب الالكتروني

تعتبر المراكز العسكرية، مصادر الطاقة، مراكز التحكم بالطيران المدني والملاحة البحرية والمؤسسات البنكية والمالية وشبكة المعلومات والاتصالات، أهدافا أساسية للجماعات الإرهابية المعاصرة في ظل التقدم التكنولوجي والتقني الهائل، حيث أن هذه الأخيرة – الاتصالات الالكترونية– شهدت انتشارا واسعا في العالم متخطية كل الحدود الجغرافية، وهو ما أدى إلى فتح المجال أمام الإرهاب الإلكتروني الذي يشمل أخطار ضد جميع الشبكات الإلكترونية للدول، خاصة بالهجوم على المعلومات وبصورة شرعية مقارنة بتلك الوسائل والتقنيات المستخدمة للقيام بهجمات مضادة[1].

أمام هذا التطور في تعميم استعمال وسائل الاتصال والمعلومات، أصبح يدعم التعاون الأمني ضد الإرهاب الالكتروني، وينادي إلى تعزيز تبادل المعلومات والخبرات بين الدول لحماية المنشآت الأساسية، والنهوض بنموذج جديد لمجتمع معرفي يشجع على

---

[1] – Joshua GREEN, the myth of cyber terrorism

على الموقع:

http://www.washing tonmonthly.com/features/2001/green html

تبادل واكتساب المعارف بعيدا عن المخاطر، ففي الأعوام الأخيرة أصبح الفضاء الالكتروني يواجه العديد من الأعمال الإرهابية، مما يؤدي إلى آثار وخيمة على الاقتصاد، وتذبذب وتيرة عمل المنشآت القاعدية، إذ تقدر الخسائر الاقتصادية الناجمة عن الإرهاب الالكتروني، كانتشار الفيروسات الحاسبة بعشرات المليارات الدولارات.

أولا – التعاون الأمني ضد الإرهاب الإلكتروني:

أصبح الأمن الالكتروني ومفاهيم السلم والأمن الوطني والدولي اليوم مرتبطان ببعضهما البعض أكثر من أي وقت مضي، وبات من الضروري وجود تعاون دولي فعال في إطار إيجاد إجراءات وتدابير منسقة وفعالة، من خلال مراجعة التشريعات القانونية واستحداث تعاون يهتم بالجانب القانوني والسياسي والتقني والاقتصادي، لكشف ومتابعة المتورطين من الجماعات الإرهابية والمنظمات المتطرفة عن تلك الهجمات [1] وأصبح ضمان أمن المعلومات في الوقت الراهن يفرض نفسه أكثر من أي وقت مضى أمام المجتمع الدولي، وتحديا عالميا واسعا ومعقدا بسبب القضايا والمسائل التي يجب أن تسوي إلى جانب عدد الأطراف الفعالة.

إن تنظيم الفضاء الإلكتروني يشمل إطارًا قانونيا مفصلا، ويهتم بتسيير الشبكة العنكبوتية من خلال وضع آليات محلية ودولية في القطاع الخاص والمجتمع المدني والتي تعرف جميعها بالأطراف الفعالة في عالم الأنظمة المعلوماتية.

ونظرا لتعقيد الفضاء الالكتروني وتعدد آثاره عند سوء استخدامه من طرف الجماعات المتطرفة، سعت المؤسسات الدولية من أجل تعزيز حماية الأنظمة المعلوماتية والشبكات عن طريق الاتحاد الدولي للاتصالات، الذي عزز قدراته في مجال الأمن الالكتروني، من خلال تقديم المساعدات التقنية والفنية وإقامة مشاريع تعتمد على تكنولوجيات الأمن المتطور، إلى جانب تنظيم دورات حول دعم وتعزيز القدرات في مجال الأمن الالكتروني[2].

---

[1] – March M.POLLITT , cyber terrorism : factor fanncy ? procceding of the 20th national information system, conference, October, 1997,pp285-289.

[2] – الاتحاد الدولي للاتصالات يعمل على دراسة الأنظمة التشريعية للرسائل الالكترونية غير المرغوب فيها، والتي يتم اعتمادها في العالم، ومنشورات حول الأمن والإرهاب الالكتروني، ودراسة التأثيرات المالية لأمن الشبكات، ضمن هذا السياق قد تم انعقاد أربع ملتقيات أولا بأثينا اليونانية سنة 2006/ والثاني بريو دي جانيرو البرازيلية سنة 2007، أما القمة الثالثة فكانت في ديسمبر 2008–2009 بمصر، أين تم التطرق إلى مسائل نظمت الحاجة إلى تعاون دولي من أجل تسيير ناجح في المجال الأمني بالإضافة إلى الجانب التشريعي لإشكالية أمن الانترنت.

وفي هذا الإطار بعث الاتحاد الدولي للاتصالات سنة 2007 البرنامج العالمي للأمن الالكتروني الذي يحمل اسم **برنامج الأمن الالكتروني الشامل (comprehensiv éléctronic security program)** حيث تم تشكيل فريق من الخبراء ذو المستوى العالي مكلف بتقديم اقتراحات وتوجيهات حول استراتيجيات خاصة لفائدة الأمن الدولي والتصدي للإرهاب الالكتروني، من خلال تعزيز قدرة المجتمع الدولي لمنع حدوث الهجمات الالكترونية والحماية والدفاع ضد تلك الهجمات التدميرية للبنى التحتية للدول، وإعطاء الأولوية لتعزيز أمن أنظمة الإعلام الآلي والاتصال، وتحسين المعايير والتدابير الأمنية والإجرائية أمام هذا التهديد الإلكتروني.

تحقيق الأمن الشامل لا يتحقق إلا بدراسة جملة من المؤثرات المستقبلية لتطور وتنامي ظاهرة الإرهاب الالكتروني أهمها:

– إن الإرهاب في المستقبل سوف يتجه نحو رفع عدد العمليات الإرهابية، ولكن الخطورة والآثار تبقى قائمة وكارثية وذات قوة تدميرية أكثر حداثة وعصرنة، مما يعني وجود مجموعة صغيرة من الهجمات تم إنشاءها لجذب انتباه أجهزة الأمن ووسائل الإعلام والجمهور على حد سواء، في وقت هناك جماعة إرهابية ذات كفاءة عالية في استخدام أسلحة الدمار الشامل، تعمل بكل حرية في التخطيط والإعداد لهجمات إلكترونية أكثر خطورة[1].

– عادة الإرهاب الالكتروني غير قابل للتفاوض السياسي بحجة أنهم لن يتوفقوا إلا بتحقيق أهدافهم والتعبير عن غضبهم، ناهيك أنه يصعب بالأساس التفاوض مع هذا النوع الجديد من الإرهاب لأنه غير مرئي عكس الإرهاب التقليدي.

– وجود جماعات إرهابية صغيرة وهي قوة فعالة على نحو متزايد لا يستهان بها، وقد أظهرت هجمات 11 سبتمبر 2001، سهولة الحصول على المعلومات من طرف الإرهابيين والاستفادة من التكنولوجيا التي يمكن استغلال ثغراتها لاختراق الاتصالات والتخطيط وتنفيذ الأعمال الإرهابية، ويظهر مدى قدرة الجماعات الإرهابية القيام بعمليات مستقلة وصعبة للغاية من حيث كشفها أو تعقبها، والاستفادة من شبكة الانترنيت بكل سهولة للحصول على المعلومات.

---

[1] – أحمد جلال عز الدين، مكافحة الإرهاب، مطابع دار السهب، القاهرة، مصر، 1990، ص 96، وراجع في هذا الصدد أيضا أحمد جلال عز الدين، الإرهاب الدولي وفقا لقواعد القانون الدولي، دار النهضة العربية، القاهرة، مصر، 1992.

لقد أصبح الإرهاب الالكتروني في متناول أي شخص مهيئا للقيام بعملية إرهابية بالاعتماد على الشروحات الموجودة على شبكة الانترنيت لصنع القنابل والإرشادات التشغيلية، وسيلجأ الإرهابيون في العقود القادمة إلى العديد من الأساليب والطرق الجديدة لاستهداف نقاط ضعف جديدة بأقل تكلفة، كما فعل الإرهابي ريتشاد ريد سنة 2001 بإخفاء متفجرات في حذائه، وأخفى النيجيري عمر فاروق في ديسمبر 2009 متفجرات في ملابسه الداخلية، كما تم العثور على قنابل في خراطيش الحبر في رحلة إلى اليمن في أكتوبر 2010[1].

هذا التطور في الأساليب والأدوات، يمثل ذروة تطور طويل في الإرهاب، وهو تطور لا يقتصر فقط على مضمون وطبيعة عمل الإرهاب بحد ذاته، ولكنه يمتد أيضا إلى متغيرات البيئة الدولية التي يتحرك فيها، والتي تعتبر العامل الرئيسي وراء التحول في أشكال الإرهاب الدولي، فعلى الرغم من أن وجود الظاهرة الإرهابية يضل واحدا من حيث استخدام التهديد والعنف والقتل والدمار، إلا أن أشكاله وأدواته وتكتيكاته تختلف وتتطور بسرعة الزمن.

إن هجمات 11 سبتمبر 2001 خير دليل على تمثيل هذا الجيل الجديد من الإرهاب نظرا لسرعة العملية وعدد الأضرار الملحقة بالولايات المتحدة الأمريكية والتي تعد أكبر دولة في العالم، والأضرار غير المباشرة بالاقتصاد العالمي تبين خطورة الإرهاب الالكتروني.

وعليه يمكن القول أن التكنولوجيا أتاحت وصول أي شخص إلى مواقع تحتوي على معلومات مفصلة حول مسائل إنتاج القنابل أو كيفية اقتنائها... الخ، في حين كان وقت مضى يصعب الحصول على أبسط معلومة تتعلق بالسلاح والتسلح، فالأكيد أن الحكومة قلصت بشكل كبير الحدود بين الدول كوسيلة دفاعية، يقابلها سهولة نفاذ الإرهابي وحصوله على معلومات حساسة لتدمير تلك الأنظمة، وحسب المختصين والخبراء في مجال الإرهاب فإن العالم سوف يواجه نموا مستمرا في الهجمات الإرهابية في العقد القادم، والهجمات تصبح واسعة النطاق لتشمل مئات الضحايا والقتلى لكنه موت صامت، إذ يمكنه أن يبيد مجتمع بكامله من دون إراقة الدماء، فالإرهابيون اليوم أصبحوا أكثر مهارة تقنيا، مما يمكنهم أن يشغلوا مستوى أعلى من العنف، فمثلا يمكنهم الهجوم على

[1] – حكيم غريب، مرجع سابق، ص 943.

إمدادات المياه بتلويثها بجراثيم قاتلة عن طريق قرصنة المحركات الأوتوماتكية لتصفية المياه وعرقلتها أو تخريبها من أداء المهمة الخاصة بها[1].

الإرهاب المستقبلي يستهدف البنى التحتية لطاقة الأنظمة الالكترونية أو الشبكات المعلوماتية، وعلى هذا الأساس لابد من وضع نظرة مستقبلية لمكافحة الإرهاب الإلكترونية[2]، في ظل التقدم العلمي والتكنولوجي وتداعياته على الأمن والسلم الدوليين وكذا الأخطار المعقدة والتهديدات ذات الطابع العابر للحدود، الذي يتعرض له الفضاء الإلكتروني مسببا خسائر فادحة على الهياكل المعلوماتية والأنظمة الحاسوبية، وعليه يتوجب على المجتمع الدولي إقامة ضمان مسار الأمن الالكتروني ومستقبله على الصعيدين الداخلي والخارجي، من خلال ترقية ثقافة الأمن الالكتروني لهذه الثورة الرقمية والتكنولوجية المعاصرة، التي تعرف يوما بعد يوم اختراعات جديدة ومذهلة لخدمة الجنس البشري.

ثانيا – تبادل المعلومات والخبرات:

التنسيق فيما يخص تبادل المعلومات والخبرات يكون بتفعيل تعاون دولي يتبادل البيانات والمعلومات حول المنظمات الإرهابية، لأن هذه الأخيرة تتضامن فيما بينها باستخدام شبكة الانترنيت لإرسال المعلومات فيها، وعليه فالتعاون الدولي يكون بنشر التعليم والوعي وتكثيف دور الإعلام بالتصدي للإرهاب الإلكتروني.

أ – التعليم ونشر والوعي بمخاطر الإرهاب الإلكتروني:

تكون توعية الفرد والمجتمع من خلال التعليم والقنوات الإعلامية، أو من خلال الشبكات العنكبوتية نفسها بمخاطر الإرهاب الالكتروني، والتركيز على فئة الشباب لأنها الفئة المستهدفة من قبل الجماعات الإرهابية، وأيضا توعيتهم بأنواع الجرائم الإلكترونية كي لا يتعرضوا لعملية زرع الأفكار الإرهابية ومعتقداتهم، وتشكيل قناعات لدى الملايين

---

[1] – Brian Michael JINIKING, The future cource of terrorism, futurist interview, January 2001, in http://www.wfs.org/intjenikins.htm.

[2] – يقول في هذا الصدد إفلين وهايدي أولفر في مقالتهما " المستقبل المتواصل، تنبؤات حديثة ومفرطة في التفاؤل moderne future predectuns and overly وهما يناقشان كتاب "باري بوزان وجيرالد سيجان" الباحثان في مجال optimistic) الدراسات الإستراتيجية المستقبلة « ... الواقع أن المرأ يحتاج إلى شجاعة خاصة فنحن لا نريد أن نزرع الوهم، بل نحاول تحديد من معالم الرؤية عن قرب حاضر، وعن بعد مستقبلي قبل وقوع كارثة، ونحن نحتاج إلى شجاعة أيضا بتحديد معالم الفجوة التكنولوجية العلمية وما يتبعها من أخطار رقمية واقتصادية في 50 سنة القادمة على الأقل... » على الموقع:

http://www.moderne future predections and overly optimistic. Org/I- Hidi/Article.html.

منهم خاصة إذا عرفنا أن من أهم هذه الأسباب للإقبال على الانترنيت عند الشباب [1] هي:

- الملل والفراغ القاتل.
- القلق المدمر.
- السرية في تصفح مواقع الانترنيت.
- المغريات الخطيرة.

وبالنظر إلى مجتمع الانترنيت بحسب بعض الباحثين، نجد أنهم يمثلون المجتمع الإنساني الذي يوجد فيه أطياف وشرائح مختلفة من الناس، وهم الشباب والمراهقون الذين يحبون الاكتشاف والمغامرة، وبينهم من يعاني الفراغ والتفكك الأسري، ما يجعلهم عرضة للاستغلال والتطرف [2]، وعليه كان لابد من حث الشباب على الاستخدام الأمثل للانترنيت والابتعاد عن المواقع المشبوهة والإرهابية التي تؤثر في تربية الشباب، بحكم أن التربية هي تحقيق للاستقرار باعتبار أن الأخلاق أساس التعامل وعنوان الأمم ورمز تطورها وبقائها.

ومن هنا يمكن القول أن مكافحة الإرهاب الإلكتروني تعتمد أولا وقبل كل شيء على مبدأ التعليم وإعداد الشباب اجتماعيا، إذ أن موضوع التعليم والوعي يعد من أهم وأخطر المواضيع التي واجهت ولازالت تواجه المجتمعات الإنسانية، وذلك لم لها من دور مؤثر، بل وفعال في بناء الحضارة الإنسانية [3].

ب – تفعيل دور الإعلام ضد الإرهاب الإلكتروني:

يمكن دور الإعلام في التفاعل بشتى وسائله مع مختلف الأشكال الإرهابية التي تقع في العالم بحيادة وشفافية عالية، لا تؤثر على حقيقة الرأي العام أو تزور الأحداث من أجل التحريض، أو أن تكون سلبية أو تتعارض وسياسة الدولة، كما لا يجب على الإعلام المبالغة في تناول الأحداث الإرهابية أو تضخيمها أكثر من حجمها لأن في ذلك تشجيع للإرهابيين القيام بأعمال بطولية –حسب نظرهم– أخرى ربما أكثر ضررا فقط لخدمة أفكارهم وأهدافهم اللاإنسانية.

---

[1] – رولا الحمصي، إدمان الأنتيرنت عند الشباب وعلاقته بمهارات التواصل الاجتماعي، بحث مقدم في مؤتمر الملتقى الطلابي الإبداعي الثاني عشر جامعة أسيون، مصر، 2000.

[2] – عبد الله عبد العزيز اليونسي، دور المدرسة في مقاومة الإرهاب والعنق والتطرف، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب، مصر، 2003.

[3] – Rosa NEGPALE, Defining cyber terrorism, 2004, Asian scool of cyber law, 04 june, 2006, P30.

على الإعلام بشتى أنواعه (مرئي، سمعي) تكثيف البرامج والنداءات لتوعية الرأي العام ضد خطر الإرهاب، والدعوة إلى التصرف بحكمة ضد هذا التهديد لأن في ذلك نبذ للعنف والتطرف.

وأخيرا مما شك فيه أن نجاح أي إستراتجية دولية لمكافحة الإرهاب الإلكتروني تبنى على أساس تعاون دولي فعال، دون أن يتم انتهاك حقوق الإنسان لأن الكثير من التدخلات الأمنية لنبذ الإرهاب والتطرف يروح ضحاياها عدة أبرياء من مختلف الأعمار وهو ما يشهده مسرح العالم اليوم من انتهاكات لحقوق الإنسان كالتدخل الروسي في سوريا ضد داعش[1].

الفرع الثاني

الآليات التقنية الدولية لحصر الإرهاب الإلكتروني

بعدما تم وضع مجموعة من الآليات الأمنية الهادفة لحماية التجارة الإلكترونية 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.

أولا – حماية المعاملات المالية الإلكترونية:

تتجلى حماية المعاملات المالية الإلكترونية في البطاقة البنكية التي تعتمد كوسيلة للوفاء الإلكتروني، بالإضافة إلى ذلك هناك حافظة النقود الإلكترونية الافتراضية.

أ – وسيط الوفاء الإلكتروني:

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

---

[1] – في دراسة جديدة قام بها عدد من الباحثين في شأن الشرق أوسطي قدمت لمركز البحوث الإستراتجية الأمريكية والتي بحثت آثار التدخل الروسي في الشأن السوري وحيثياته على الشرق الأوسط، أشاروا إلى أن التدخل العسكري الروسي في الحرب المستعمرة في سوريا منذ سنوات يثير جدلا واسعا في الأوساط المحلية والإقليمية والدولية، بعد إعلان الكرملين منح الرئيس فلاديمير بوتن تفويضا بنشر قوات عسكرية في سوريا لمواجهة خطر تنظيم داعش غير أن الملاحظ أن الغارات الروسية لا تفرق بين معتدل ومتطرف، وأنها تستهدف جميع القوى المناهضة للأسد. على المواقع:
www.bbc.com/arabic/interactivity/2015/comments- syria-russia-military.

1 – النظام الافتراضي الأولي (First Virtual):

يقتضي هذا النظام أن يكون للتاجر حساب بنكي في بنك أمريكي 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 (Identifiant)[1].

يقوم العميل بإرسال رقم تعريفه الشخصي للتاج ر، هذا الأخير الذي يسم ح له بالتأكيد من وجود وكفاية حساب العملية لدى الشركة الوسيطة ، وذلك بأن يرسل لها معلومات خاصة بالصفقة ، ورقم التعريف الشخصي للعميل والتاج ر، 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 الأمن 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 ال تأكد من التاجر أن ترسل بطاقة الوفاء إلى العميل[2].

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 إن هذه الطريقة (وسيط الوفاء الإلكتروني) قلل ت من مخاطر الوفاء

---

[1] – ضياء علي أحمد نعمان، "الحماية التقنية للتجارة الالكترونية"، مجلة القانون، العدد الأول، مطبعة وراقة وطنية، مراكش، المغرب 2011، ص 20.

[2] – المرجع نفسه، ص 21.

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 – حافظة النقود الإلكترونية والافتراضية:

ويقصد بهذه التقنية تجميع وحدات للقيمة وذلك في أداة مستقلة عن الحسابات البنكية فظهرت بذلك فكرتي حافظة النقود الإلكترونية (PME) وحافظة النقود الافتراضية (PMV) فبالنسبة للأولى فإنها تشحن مسبقا برصيد مالي ويتم تسجيل هذا الرصيد المالي في بطاقة أما بالنسبة لحافظة النقود الافتراضية ، فإنها تشحن برصيد مالي على القرص الصلب لجهاز الكمبيوتر الخاص الذي يستعمل الشبكة ، وبالتالي فقطع النقود أو النقود الافتراضية تمثل من الناحية الفنية تلك المعاملات المختزلة على ذاكرة جهاز الكمبيوتر ويستطيع بذلك العميل الذي يرغب في التعامل بهذه النقود ، أن يحصل من أحد البنوك أو أحد المؤسسات الوسيطة على رخصة تسمح له باستعمال النقود الإلكترونية بالمقابل الذي يتفق عليه ويكون لديه مفتاح عام وخاص من أجل تأمين معاملاته وتحققه منها[1].

والهدف من هذه التقنية تفادي اختراق البيانات التي يتم تداولها عبر شبكة الإنترنت من طرف الإرهاب الإلكتروني، والتغلب على إمكانية استخدامها الغير المشروع، لأنه بهذه التقنية يصبح لوحدات القيمة الإلكترونية ذات مستقلة ، حيث يمكن نقلها من محفظة إلكترونية إلى أخرى على نحو يؤدي إلى الوفاء من قبل المدين بمجرد قفل هذه الرموز الإلكترونية، ويمكن لمتلقي هذا الوفاء على حافظة إلكترونية أن يقوم بتحويل هذه النقود الإلكترونية إلى نقود رقمية من خلال البنك المصدر لها.

ثانيا – حماية المواقع الخاصة بالإنترنت:

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

أ – 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 أ و استخدامها غير المشروع، ويعرف كذلك التشفير بأنه عملية تحويل المعلومات إلى رموز غير مفهومة تبدو غير ذات معنى بحيث يمنع الأشخاص غير المرخص لهم من الاضطلاع على المعلومة أو فهمها، فعملية التشفير تنطوي على تحويل النصوص العادية

[1] – http://www.bshmokh.com

إلى نصوص مشفرة ومن المعلوم أن الإنترنت تشكل الوسيط الأضخم لنقل المعلومات الحساسة للحركات المالية والتواقيع الإلكترونية بصيغة مشفرة للحفاظ على سلامتها من عبث القراصنة[1].

ويسمح نظام التشفير بت فادي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية الاحتيالية في المعاملات التجارية ، حيث يتم التأكد م ن 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 داخل التجارة الإلكترونية.

والغاية من التشفير هو إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها لكي لا يستطيع أي شخص الاضطلاع 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[2].

التشفير نوعان:

1- نظام التشفير المتماثل أو المتناظر:

وهو أسلوب من أساليب التشفير ، يستخدم فيه مفتاح سري لتشفير رسالة ما وفك تشفيرها ويسمى بالمفتاح المتناظر لأن المفتاح الذي يستخدم لتشفير الرسالة هو نفسه المستخدم لفك تشفيرها، لكن هذه الطريقة تتطلب إحالة المفتاح بين الأطراف بطريقة يجب أن تضمن سلامته وتعطي هذه التقنية حماية أكثر في الشبكة المغلقة.

2- نظام التشفير اللامتماثل واللامتناظر:

يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر ولهذا السبب يسمى بالتشفير بالمفتاح اللامتناظ ر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير وهكذا فللفرق بين التشفير المتناظر والتشفير اللامتناظر بسيط جدا وكلاه ما غاية في الأهمية على مستوى ودرجة الأمن ، حيث أنه في التشفير المتناظر يتم تشفير الرسالة أو التوقيع باستخدام الرقم العام وفي الوقت نفس ه يتم فك الشفرة وإرجاع المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام ، ولكن إن حصل أن شخص آخر يعرف هذا الرقم أو توصل إليه عن طريق الدليل العام فبإمكانه فك الشفرة وقراءة الرسالة أو

---

[1] – هدى حامد قشقوش، الحماية الجنائية لتجارة الالكترونية عبر الانترنيت، دار النهضة العربية، الاسكندرية – مصر دون سنة نشر، ص 61.

[2] – علي كحلول، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الالكترونية بدون دار أو سنة النشر، ص 282.

التوقيع، أما إذا تم تشفير المعلومات بأسلوب التشفير اللامتناظر فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه التشفير[1].

بالنسبة لمستويات التشفير أصبح يستعمل ويستخدم في أكثر من مستوى من أجل تحقيق أعلى درجة من الأمان ، فعلى سبيل المثال أصبحت المعاملات المالية الآن يتم تشفيرها باستخدام نظام تأمين المعاملات الإلكترونية (SET) بالإضافة إلى تشفير مستوى التصفح باستخدام (net escape)ونظام التأمين(SSl).

3 – 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[2]:

– 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.

4 – نظام التأمين (SSL):

وتكمن مهمة البرتوكول في تشفير جميع الاتصالات في برامج التصفح أو النوافذ على شبكة المعلومات (Bowser) وأحد المواقع أو مقر المعلومات على خادم الشبكة

---

[1] – العربي بوجمعة جنان، التبادل الإلكتروني للمعطيات القانونية، مطبعة ووراقة – مراكش المغرب 2006، ص 46.

[2] – 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.

(Server)، وبالتالي فهو يقلل من فرصة وقوع المعلومات أثناء عملية انتقالها في أيدي أي شخص غير مرغوب فيه، إلى أن تصل إلى المستقبل النهائي فهو يعطي للعملاء الثقة والطمأنينة بأن المعلومات والبيانات الخاصة بهم بما فيها إتمام البطا قات البنكية لن تكون متاحة سوى للتاجر أو المنشأ أو المؤسسة المراد التعامل معها للتأمين البطاقة البنكية.

ب – الجدران النارية كوسيلة لحماية المحتوى:

يعتبر الجدار الناري وسيلة تستعمل لحماية الشبكات الخاصة من الدخول وتمنع الوصول الغير مشروع لها، حيث تحمي وحدات التحكم والإرسال في الإنترنت.

وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة ، التي تعمل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو لمجموعة من المضيفين ليرى ويسمع كل منهم الآخر ، ويوفر الهيكل الإذاعي المتكامل على الإنترنت عن طريق برنامج (Mphone) المتوافر لكل الناس،إلا أن هذا البرنامج يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الإنترنت، لكن بوجود الجدران الناري يعدم تماما التطفل[1].

وتتجلى مزايا هذه الجدران النارية في:

– توفير الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها.

– تسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عن د خروجها أو دخولها الإنترنت.

– تسجيل كافة المعلومات عن حركة مرور المعلومات.

المطلب الثاني

دور المنظمات الدولية في مكافحة الإرهاب الإلكترونية

يعتبر الإرهاب الالكتروني أحد أهم الأسباب التي أدت إلى خلق تعاون دولي يتجاوز كل النزاعات والخلافات الجغرافية والسياسية، واستحداث أساليب جديدة من أجل حماية البيئة الإلكترونية، هذه التدابير شملت المنظمات الدولية التي كانت هي أيضا من بين الدعاة لوجود إستراتجية ملزمة لتنظيم النشاط الاقتصادي الإلكتروني بكل تطبيقاته وعناصره، وتركيب نظام وقائي ضد جميع أشكال الإرهاب الإلكتروني وأساليبه، وفي

[1] – ضياء علي أحمد نعمان، مرجع سابق، ص 39.

إطار جميع صوره الإجرامية التي يتضمنها مفهوم الإرهاب الإلكتروني كالجريمة الإلكترونية[1].

ولعل أهم هذه المنظمات الدولية التي تمارس نشاط دولي نجد الأمم المتحدة التي لم تفوت فرصة التحدث عن الإرهاب الإلكتروني وتبيان مخاطره **(الفرع الأول)**، ثم منظمة التعاون الاقتصادي والتنمية التي وإن كان نشاطها اقتصادي، إلا أنها خصصت في مدونة عملها ما يتعلق بالتعامل بتقنية المعلومات الذي يدخل ضمن التجارة الالكترونية **(الفرع الثاني)** وأخيرا مجموعة الثمانية ودورها في مكافحة الإرهاب الإلكتروني **(الفرع الثالث)**.

الفرع الأول

دور الأمم المتحدة

تعرف منظمة الأمم المتحدة باجتهاداتها التي قامت ولا تزال تقوم بها في سبيل مكافحة الإرهاب التقليدي، وكذا تدخلاتها المتعددة على المستوى الدولي من أجل حماية حقوق الإنسان، وقد أدرجت في برنامج عملها في إطار مكافحة الإرهاب، الإرهاب الالكتروني.

بذلت الهيئة الأممية جهودا في سبيل العمل على مكافحة جرائم الإرهاب الإلكتروني وذلك لما تسببه هذه والجرائم من خسائر اقتصادية، ومشاكل سياسية واجتماعية جد خطيرة وإن التصدي لهذا التهديد ومكافحته يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[2].

---

[1] – الجريمة الإلكترونية وهي كل عمل أو امتناع يأتي به الإنسان بواسطة نظام المعلوماتي معين ينتج عنه اعتداء على حق أو مصلحة أو أية بيانات معلوماتية يحميها القانون، إما أضرار المكونات المنطقية للحسب الآلي ذاته أو بنظام شيكات المعلومات المتصلة به إذا كانت الواقعة تمس حدود أكثر من دولة بالنسبة للوسيلة المستخدمة في هذه الجرائم الإلكترونية هي برامج المعلوماتية أو نظم الحاسوب، محل الجريمة المعلوماتية هو الاعتداء على بعض الحقوق أو المصالح القانونية وهي الغش المعلوماتي، التزوير المعلوماتي، الإنتاج غير المشروع للمواد الإباحية الطفولية، الاعتداء على الملكية الفكرية وحقوق النشر، كشف سرية البيانات، الدخول الغير المصرح به، الإتلاف غير المشروع للنظم المعلوماتية، أو البرامج أو البيانات.

[2] – عواطف عثمان محمد عبد الحليم، جرائم المعلوماتية، مجلة العدل، العدد 24، دون سنة أو بلد النشر، ص 69.

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب وأشار القرار إلى أن الإجراء الدولي لمواجهة الجرائم الإلكترونية بين الدول الأعضاء يتمثل في[1]:

1 – تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة، على نحو ملائم وإدخال التعديلات إذا دعت الضرورة.

2 – مصادرة العائد والأصول من الأنشطة غير المشروعة.

3 – اتخاذ تدابير أمن والرقابة مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

4 – رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذه الجرائم ومحاكمة مرتكبيها.

5 – التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمن مناهج مدرسية.

6 – حماية مصالح الدولة وحقوق ضحايا جرائم الانترنيت.

تزايد الجرائم المرتكبة من طرف الإرهاب الإلكتروني وما تخلفه من خسائر ومخاطر أدى بمنظمة الأمم المتحدة إلى عقد اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إرهابية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة الإرهاب الإلكتروني، بالإضافة إلى الدور الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية[2]

كذلك عقدت منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12–19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء بنوع من التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب الإرهابيين والسلطات المختصة في مكافحة الجريمة، لما في ذلك الجرائم الحاسوبية، إذ احتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا عن خطورتها والتحديات التي تطرحها.

---

[1] – غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، رسالة دكتوراه في القانون، الجامعة الإسلامية، كلية الحقوق، بدون سنة النشر، لبنان، ص 186.

[2] – اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) الصادرة عن هيئة الأمم المتحدة، الكلية العامة 81، ديسمبر 2000.

ودعت لجنة منع الجريمة والعدالة الجنائية التي عقدت اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية من أجل دراسة شاملة للجريمة السيبرانية بالتطرق إلى المواضيع التالية[1]:

1 – جمع المعلومات والإحصائيات المتعلقة بالإرهاب الإلكتروني وتحدياته.

2 – مدى فعالية التشريعات للظاهرة الإرهابية الإلكترونية.

3 – إجراءات التحقيق.

4 – التعاون الدولي.

5 – الأدلة الإلكترونية.

6 – مسؤولية متعهدي خدمات الانترنيت.

7 – التصدي للجريمة خارج دائرة التدابير القانونية.

8 – المساعدة التقنية الدولية.

9 – دور القطاع الخاص في الحد من الجريمة.

وعملت منظمة الأمم المتحدة في إطار استمرار تلك الجهود المبذولة لمكافحة الإرهاب الإلكتروني، من خلال محاربة جرائم الكمبيوتر والانترنيت، وهذا من خلال ثلاث اتجاهات رئيسية وهي:

حماية البيانات الشخصية:

وهو حماية الخصوصية المعلوماتية وكل البيانات الشخصية من مخاطر التلف التزوير، القرصنة، الاستعمال، الحذف، التشويه، وهذا يعتبر أيضا حماية لحقوق الإنسان.

حماية الملكية الفكرية للمنصفات الرقمية:

وهو حماية البرمجيات وقواعد البيانات والدوائر المتكاملة وعناصر مواقع الانترنيت في الوقت الحاضر.

حماية استخدام الكمبيوتر والانترنيت:

حماية استخدام الكمبيوتر والانترنيت من الأنشطة التي تستهدف المعلومات ونظامها وأداء الكمبيوترات ووظائفها وأداء الشبكات وهي نفسها جرائم الكمبيوتر والانترنيت، لهذا عملت الأمم المتحدة في ميدان تطوير التشريعات الجنائية، وبحث الظواهر الجديدة في ميدان الانترنيت.

---

[1] – كان اجتماع لجنة منع الجريمة والعدالة الذي يعمل تحت لواء منظمة الأمم المتحدة بفيينا في الفترة 17–21 جانفي 2011، تحديد فريق من الخبراء المهنيين بالجريمة السيبرانية وهو أحد المشاريع المطروحة للنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية وتدابير التصدي لها.

ولكن تبقى العقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي الإلكتروني، أما المعوق الثاني هو تنوع واختلاف النظم القانونية الإجرامية على المستوى الدولي والإقليمي، إلا أن منظمة الأمم المتحدة كغيرها من المنظمات الدولية تولي هذا الموضوع، اهتماما خاصا وهو الأمر الذي أحرز مجموعة من المعايير الدولية، إلا أن المجتمع الدولي لازال في حاجة إلى اتفاقية دولية ملزمة في مجال مكافحة الإرهاب الإلكتروني.

الفرع الثاني

دور منظمة التعاون الاقتصادي والتنمية (OECD) [1]

عملت منظمة التعاون الاقتصادي والتنمية ابتداء من سنة 1978 على وضع أدلة وقواعد إرشادية تتصل بتقنية المعلومات كان أولها الدليل المتعلق بحماية الخصوصية وقواعد تنقل البيانات[2]، وقد تم تبني هذه القواعد من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها في ميدان حماية المعلومات ومكافحة جرائم الكمبيوتر والانترنيت، فقد بادرت المنظمة بعقد اجتماع في باريس عام 1983 لتكريس جدول بحث للجرائم المرتبطة بتقنية المعلومات.

وفي عام 1985 صدر عن المنظمة تقرير بعنوان " **الجريمة المرتبطة بالحاسوب وتحليل السياسة الجنائية القانونية**" حيث تضمن التقرير قائمة الحد الأدنى للأفعال سواء استخدام الكمبيوتر التي يجب على الدول أن تجرمها، وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال، تغيير برامج الكمبيوتر أو المعلومات المخزنة فيه، سرقة الأسرار المودعة في قواعد الكمبيوتر[3].

وبتاريخ 26 نوفمبر، وقعت المنظمة توصيات إرشادية بخصوص أمن نظم المعلومات[4]، ومن مجمل أعمال منظمة التعاون الاقتصادي والتنمية (OECD) حول

---

[1] – منظمة التعاون الاقتصادي والتنمية (OECD)، تظم مجموعة من الدول هي أستراليا، النمسا، بلجيكا، كندا، جمهورية التشيك، الدنمرك، فنلندا، فرنسا، ألمانيا، اليونان، إسلندا، إيرلندا، السويد، سويسرا، لكسمبورغ، المكسيك، هولندا، نيوزلندا، النرويج، بولندا، البرتغال، اسبانيا، السويد، تركيا، بريطانيا، وأخيرا الولايات المتحدة الأمريكية تعمل هذه الدول متحدة في إطار المنظمة على التنمية الاقتصاد العالمي وكذا التنمية الاجتماعية.

[2] – OECD, Gidlines on the protection of privacy and transborder flous of personal data.

[3] – www.oecd org.

[4] – Rocommendation of council concering guidelines for the security.

جرائم الكمبيوتر والانترنيت تولد اتفاق على ضرورة أن يحظى قانون العقوبات في كل دولة الأفعال التالية:

1 – التلاعب في البيانات المعالجة آليا بما في ذلك محتواها.

2 – التجسس الإلكتروني، ويندرج تحته الحصول أو الاستعمال غير المشروع للمعطيات.

3 – التخريب الإلكتروني، الاستخدام الغير المشروع أو سرقة المعلومات.

4 – قرصنة البرامج.

5 – الدخول غير المشروع على البيانات أو نقلها.

وأما عن جدول أعمال المنظمة الحالي بخصوص مكافحة جرائم الإرهاب الإلكتروني فإن المنظمة معتمدة على عشرات الدراسات التحليلية المجرات في السنوات الأخيرة حول مدى تطبيق الدول الأعضاء لتوجيهاتها في هذا المجال، وحول تدابير التشريعات الوطنية التي اعتمدتها هذه الدول، ولمواكبة الحالات المستجدة والتحديات الجديدة، تعقد سنويا عددا من الملتقيات وورش عمل معمقة للقطاعات ذات علاقة، ترتكز فيها على معايير الأمن ومستوياته، إضافة إلى معايير تنفيذ وتطبيق القانون.

الفرع الثالث

دور مجموعة الثمانية (G8)

تتضمن أنشطة مجموعة الثمانية، أو مجموعة الدول الصناعية الثمانية، مؤتمرات على مدار السنة ومراكز بحث سياسية، مخرجتها تتجمع في القمة السنوية التي يحفزها زعماء الدول الأعضاء، أما بالنسبة للاتحاد الأوروبي، فيتم تمثيله في هذه القمم[1].

تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات والأبحاث الميدانية في مختلف المجالات التي تهم المنظمة، وهي ليست تشريعا للدول الأعضاء، ولكنها تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك ببلورة خططا عملية

[1] – مجموعة الثمانية G8، تظم الدول، الصناعية الكبرى في العالم، أعضاؤها هم الولايات المتحدة الأمريكية، اليابان، ألمانيا، روسيا، إيطاليا، المملكة المتحدة، فرنسا وكندا، يمثل مجموع اقتصاد هذه الدول الثمانية 65% من اقتصاد العالم وأغلبية القوة العسكرية تمثل من 7 إلى 8 مراكز الأكثر أنفاقا على التسلح وتقريبا كل الأسلحة النووية عالميا، كل سنة الدول الأعضاء في مجموعة الثمانية تتناوب على رئاسة المجموعة، تضع الدولة الحائزة على الرئاسة الأجندة السنوية للعمل وتستضيف القمة لتلك السنة.

كحصيلة لتوجيهات قادة هذه الدول، ومكافحة كل من شأنه التأثير أو تهديد أمن واستقرار الدول الأعضاء[1].

أطلقت المجموعة توصيات لحماية الخصوصية ضمن مؤتمرها الذي عقد حول مجتمع المعلومات سنة 1995، أما في إطار جرائم الكمبيوتر والانترنيت، فإن المجموعة عبر لجان الخبراء المشكلة لهذا الموضوع، ساهمت في الوضع الكثير من الخطط العملية في حقل أنشطة المكافحة، هذا فعلا ما تحقق في العديد من الموضوعات، منها مسائل أمن المعلومات.

كما كان للمجموعة الثمانية دور فعال وكبير في محاولاتها الرامية إلى إيجاد حلول دولية باتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية، وفي عام 2001، ناقشت مجموعة الثمانية الأدوات الإجرامية لمكافحة الجريمة الإلكترونية في ورشة عمل بطوكيو، ركزت على إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات، أو ما كان حفظ البيانات يعد بديلا، وتجري الأنشطة في هذا المجال ضمن إطار أوسع وهو وجود المنظمة في حقل المكافحة العالمية للجرائم بوجه عام.

وحول الأجندة الحالية للمنظمة، فإن جرائم الكمبيوتر والانترنيت تحتل البند الأول من بين بنود مكافحة الجرائم، وتخضع الأنشطة للتقييم وإصدار الخطط والتوجيهات، إضافة إلى أن أحد بنود أجندة عمل هذه المنظمة على مسائل الإرهاب الإلكتروني، والتعاون بينها لوقف أنشطة الاعتداء على المواقع والشبكات[2]

لكن هذا لا ينفي أن المنظمة قامت بمجموعة من الأعمال في إطار تشجيع التعاون بين الدول الأعضاء، وتطبيق سياسة حول مكافحة الإرهاب الإلكتروني، حيث قامت بـــ:

– سنة 1997 بواشنطن اعتماد مبادئ لمكافحة جرائم الحاسب الآلي في أي مكان بالعالم.

– في ماي 2002، اجتمع وزراء دول مجموعة الثمانية بكندا، لإصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدودية، من أجل مكافحة الأعمال الإرهابية في جميع صوره.

– في 11 ماي 2004، أصدرت مجموعة الثمانية، بيان مشتركا صدر بعنوان **موصلة تعزيز القوانين المحلية** ، الذي وصى جميع الدول أن تواصل تحسين القوانين

---

[1] – غازي عبد الرحمان هيان الرشيد، مرجع سابق، ص 21.

[2] – مجموعة الثمانيةG8 نشأتها ومؤتمراتها السنوية، أجندة عملها على الموقع www.g8 utoriontо.com.

التي تجرم إساءة استخدام الشبكات الإلكترونية، والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالانترنيت.

ويظل دور هذه المنظمات (الأمم المتحدة، المنظمة التعاون الاقتصادي والتنمية (OECD) وكذا مجموعة الثمانية (G8) فعال ومستمر، رغم اعترافها بتطور الإرهاب الإلكتروني، وكذلك اعترافها بالمشكلات والصعوبات العملية والإجرامية التي تظهر عند ارتكاب الإرهابيين جرائمهم باستخدام التكنولوجيا، وهو السبب نفسه الذي يجعل هذه المنظمات تشجع التعاون بين أجهزة الدول الأعضاء وعلى نحو فعال في مكافحة الإرهاب الإلكتروني، وذلك عن طريق المكاتب المركزية الوطنية للخلايا المخصصة لمكافحة هذا التهديد الجديد الموجود في أقاليم دول المنظمات الثلاث، بتبادلها المعلومات والخبرات وكل البيانات اللازمة من أجل ضبط المجرمين.

ويجدر الإشارة خاصة أن أحد أهم الأهداف التي كانت السبب في وجود هذه المنظمات بالرجوع إلى تاريخ نشأتها هو تحقيق الأمن والسلم والاستقرار الدولي.

المبحث الثاني

الجهود الإقليمية والوطنية في مكافحة الإرهاب الإلكتروني

استعمال الإرهاب للتكنولوجيا جعل منه إرهابا أكثر تعقيدا وأكثر تكلفة، مقارنة بالإرهاب التقليدي، نظرا لمجموع الخسائر التي يحققها خاصة تلك التي تمس الاقتصاد والسوق وحركة رؤوس الأموال التي تبنت التجارة الإلكترونية كآلية جديدة لتسيير النشاط المالي على المستوى العالمي.

وبالرجوع إلى عدد الجرائم المرتكبة من قبل هذا النوع الجديد من الإرهاب، كان لابد من وجود حلول على المستويين، الإقليمي باعتبار الدول هي محور المجتمع الدولي وأساس التعامل المشترك، قامت بتوحيد المجهودات فيما بينها لحصر هذا التهديد على المستوى الإقليمي(**المطلب الأول**)، وعلى المستوى الوطني أو الداخلي الذي يمثل تجربة شخصية لكل دولة تعترف بالإرهاب الإلكتروني كتهديد أولا داخلي يمس بمصالحها ويهدد استقرارها وأمنها الداخليين، وتعترف به كنوع جديد وشكل من أشكال الإرهاب الجديد الذي يعتبر امتداد للإرهاب التقليدي ولكنه أكثر ضررا لأن الإرهاب التقليدي خسائره غالبا ما تكون بشرية، أما الإلكتروني فيمس كل المجالات البشرية، الاقتصادية، والاجتماعية، وإن كان الإرهاب التقليدي نستطيع حصره، فالإلكتروني هو موت صامت لا نشعر به إلا من خلال نتائج أعماله التخريبية (**المطلب الثاني**).

المطلب الأول

الجهود الإقليمية لمكافحة الإرهاب الإلكتروني

رغم الجهود الدولية لمكافحة الإرهاب الإلكتروني التي سبق التطرق إليها، تظل غير فعالة إذ اعتبرناها الآلية الوحيدة لمكافحة هذا التهديد، وعليه كان لابد من تكثيف دائرة المجهودات من دولية إلى إقليمية لحصر وإحاطة أكبر بالظاهرة الإجرامية.

أكيد أنه كلما صغرت دائرة التصدي للظاهرة على المستوى الدولي تكون احتجاز للإرهاب الإلكتروني من حيث دائرة نشاطه فتكثيف الآليات الدفاعية والوقائية من دولية إلى إقليمية، يزيد فرصة القضاء عليه أو على الأقل ضبطه وحصره، دون أن ننسى زيادة فهم تحركات وتكتيكات هذا الاعتداء الإلكتروني، بالتالي جعل آليات إجرائية وتشريعية فعالة ورادعة له، وهو هدف الاتحاد الأوروبي (**الفرع الأول**)، وكذا المجهودات العربية التي تحاول أيضا مواكبة التكنولوجيا بفرض آليات إجرائية لمكافحة الإرهاب الإلكتروني (**الفرع الثاني**).

الفرع الأول

دور الاتحاد الأوروبي في مواجهة الإرهاب الإلكتروني

عمل الاتحاد الأوروبي على مواجهة الإرهاب الإلكتروني، وكانت البداية بحماية الحياة الشخصية من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، حين برزت مجهودات الاتحاد بوضع معاهدة حماية الأشخاص من مخاطر المعالجة الآلية للبيانات، ووضعت الاتفاقية للتوقيع في يناير 1981.

بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر 1985، يعتبر هذا الجهد نتيجة اهتمام لجنة الوزراء في المجلس بمسألة الخصوصية السرية منذ عام 1968، والتي انطوت على توجيهات بصدد وجوب توفير قواعد تكمل حماية البيانات الشخصية من مخاطر المعالجة الآلية[1].

حرص المجلس الأوروبي على التصدي للاستخدام غير المشروع للحسابات وشبكات المعلومات، وذلك من خلال العديد من الجهود التي بذلت في هذا الشأن بداية من مطلع السبعينات من القرن الماضي.

---

[1] – وقعت على هذه الاتفاقية كل من النمسا، بلجيكا، الدنمارك، فرنسا، اليونان، إسلندا، إيطاليا، لكسمبورغ، النرويج، البرتغال، السويد، تركيا، المملكة المتحدة، وقد صادقت عليها كل من فرنسا، ألمانيا، النرويج، إسبانيا، السويد.

كان العمل في البداية ينصب على حماية البيانات الشخصية حتى لا تؤدي الرغبة في زيادة فعالية عمل الحسابات الآلية لخدمة المجتمع في تهديد حق الأفراد في الخصوصية.

في عام 1981، تم التوقيع على الاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا، وقد تضمنت تلك الاتفاقية عدة مبادئ تمثلت في الحد الأدنى من الاحتياطات التي يجب أن تتضمنها التشريعات الداخلية للدول أطراف المعاهدة لحماية الأفراد من إساءة استعمال البيانات المعالجة إلكترونيا، وضرورة الحصول على البيانات الشخصية من مصادر مشروعة، وأن تكون البيانات صحيحة أو متفقة مع الغرض الذي وضعت لأجله، وأن تكون المعلومات حديثة، وأن تراعي القواعد الشكلية اللازم اتباعها للحيلولة دون إساءة استخدام البيانات الشخصية[1]

والواقع أن هذه المبادئ لا تختلف عن تلك الصادرة عن منظمة التعاون الاقتصادي والتنمية عام 1980 في شكل توصيات، وإن كان الاختلاف يمكن في عنصر الإلزام الذي تتميز به اتفاقية المجلس الأوروبي باعتبارها اتفاقية قانونية تلزم الدول الأطراف فيها.

وقد أكدت الاتفاقية على اتخاذ التدابير التشريعية والتنظيمية ، وضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على أهمية التعاون المحلي والإقليمي والدولي ووجوب إقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الأساسية والسيادة.

ولأن الاتفاقية جاءت حصيلة جهود دولية وإقليمية، فقد أكدت على أهمية ما أنجز من جهود في حقل جرائم الكمبيوتر من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي ومجموعة الدول الصناعية، وبالنتيجة فإن مقدمة مشروع الاتفاقية ركزت على ثلاث عناصر أساسية هي[2].

---

[1] – محمد حسام، الحماية القانونية لبرامج الحاسب الإلكتروني، الطبعة الثانية، دار الثقافة للطباعة والنشر، القاهرة – مصر، 2000، ص 161.

[2] – تتلخص، أهداف الاتفاقية المتعلقة لحماية الحياة الشخصية من مخاطر المعالجة الآلية الالكترونية لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية، كما أنها تؤكد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والانترنيت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية، مع ضرورة تفعيل خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة المعلومات وأنظمة الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الإجرائي بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستويين الوطني والدولي، وهذا إن دل على شيء أنما يدل على وجود اعتراف مبدئي بالإرهاب الإلكتروني والذي يقوم بمجموع الأعمال التي كانت السبب في وجود هذه الاتفاقية التي تحاول

1 – أهمية التدابير التشريعية الموضوعة لمواجهة جرائم الكمبيوتر.

2 – أهمية التعاون الدولي والإقليمي في حقل مكافحة الجرائم الإلكترونية والانطلاق مما أنجز من جهود دولية وإقليمية في هذا المجال.

3 – أهمية التدابير التشريعية الإجرائية الملائمة مع طبيعة الكمبيوتر.

يتمثل الإطار الموضوعي للاتفاقية فيما جاءت به المادة الأولى منها، إذ عرفت معطيات الكمبيوتر تعريفا واسعا يشمل الحقائق والمعلومات والمفاهيم بأي شكل مناسب لعمليات المعالجة في نظام الكمبيوتر، وتشمل مجموعة الأوامر والتعليمات المناسبة لجعل النظام قادرا على أداء العمليات أو يلاحظ أن الجزء الأخير من التعريف هو تعريف البرامج بأنواعها المختلفة، مما يعني أن البرامج سواء التطبيقية أو التشغيلية موجودة ضمن تعريف المعطيات والبرامج، ثم عرفت المادة الأولى في فقرتها الثالثة مزوري الخدمة بـــ « ***يشمل كل شخص عام أو خاص يزود المستخدمين بالخدمات التي تتيح للكمبيوترات الاتصال معا ويعالج المعطيات المخزنة للهدف المتقدم نيابة عن مزور الخدمة*** »[1].

حسب التعريف المقدم يمكن القول أن المعلومات التي يحوزها أو يمتلكها مزور الخدمة وتكون ضرورية لمعرفة وتمييز العنوان المادي للمشترك أو المستخدم أو الحساب ملتقي الخدمة الاتصالية من مزود الخدمات، وتشمل أي معلومات تتعلق بالشبكة أو الأجهزة أو الأفراد أو الحسابات أو بيانات التعريف أو الخدمات أو الرسوم أو المكان الحقيقي للأجهزة إذا كانت مختلفة عن موقع تزويدها بيانات المرور حسب تعريفها المقدم.

أما في المادة (07) من الاتفاقية فإنها تحدد الجرائم المرتبطة بالكمبيوتر وكذا التزوير المرتبط بالكمبيوتر، وتليها المادة (08) التي تعالج مشكل الاحتيال المرتبط بالكمبيوتر.

المادة(09) تتحدث عن الجرائم المرتبطة بالمحتوى، وتشمل صورة واحدة من هذه الجرائم، هي جرائم دعارة الأطفال.

حماية الخصوصية في حيازة المعلومات والاستفادة من عناصر الملكية الفكرية لها بالاستعمال الغير المشروع أو باحتكارها.

[1] – فتيحة محمد قواريري، "المواجهة الجنائية لقرصنة المصنفات الالكترونية(peer to peer)، مجلة الحقوق الكويت، العدد الأول، مارس 2010، ص ص 45–51.

المادة(10) تتعلق بحق المؤلف والحقوق المجاورة وتشمل الجرائم الجنائية التي تعد اعتداء على المصنفات المحمية بحق المؤلف والحقوق المجاورة.

أما كل من المواد(11-12-13) فقد جرمت مجموعة من المساهمات الإجرامية والمساعدة على التحريض، وحددت مسؤولية كل من الشخص المعنوي والطبيعي وأخيرا معايير العقاب، ويجدر الإشارة أن الخلاف لا يزال قائما إلى يومنا هذا حول تعداد وتقييم جرائم الكمبيوتر، لذا وجدت الاتفاقية أنه من المناسب أن نضع نصوص تجريمية ضمن النصوص والمواد القانونية التي تفسر وتحدد مفهوم الجرائم المعلوماتية دون أن تخصص لها أبواب منفردة.

استنادا في المواد المشار إليها فإن الاتفاقية تلزم الدول الأعضاء سواء الأوروبية أو غير الأوروبية المنظمة إليها باتخاذ التدابير التشريعية والإجرامية الملائمة لتجريم تسعة جرائم في ميدان الجرائم التكنولوجية نتناولها تبعًا:

جريمة الدخول غير القانوني المتعمد:

نعني به الدخول المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق أو إذن، سواء كان بنية انتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر، أو لأي فئة غير مشروعة.

الملاحظ هنا هو استعمال الاتفاقية لصيغة الدخول الغير القانوني المتعمد في حين نجد أن معظم التشريعات تستعمل صيغة الدخول الغير المصرح به، وذلك لسبب بسيط كون مجموع الجرائم التي عددتها الاتفاقية حاولت استخدام أكبر قدر ممكن من المصطلحات القانونية حتى لا يحصل لبس في تطبيقها لأن الدول الأطراف لا تعتمد نفس اللغة في تسمية المصطلحات.

جريمة الاعتراض غير القانونية المتعمد:

جريمة الاعتراض غير القانوني المتعمد ودون حق بواسطة وسائل تكنولوجية لبيانات المرسلة غير العامة إلى أو من نظام الكمبيوتر، وكذلك اعتراض الإشاعاعات الكهرومغناطسية المنبعثة من نظام الكمبيوتر تحمل مثل هذه المعطيات، وهو ما نصت عليه المادة (03) من الاتفاقية.

جريمة التدخل المعتمد في المعطيات بتدميرها:

التدخل المتعمد في المعطيات بتدميرها أو حذفها أو تشويهها أو إفسادها أو تغييرها أو تعطيلها أو كبتها، وقد ذهبت لجنة الخبراء إلى أن تعديل البيانات يشمل خلطها (الغش) فيتعلق الأمر بإجراء منع وصولها إلى العنوان المرسلة إليه كحذف جزء منها على نحو

يتيح وصولها إلى الموضوع الفيزيائي المطلوب، أو تصبح بلا فائدة أو منع الغير من الوصول إليها، والبعض الآخر من الخبراء ذهبوا إلى وجوب اشتراط حصول الضرر جراء التدخل في البيانات كعنصر من عناصر التجريم، إلا أن النص لم يشر إلى هذا العنصر، فجرم كل تدخل في المعطيات على أن يكون مقصودًا وهو ما تؤكده المادة (04) من الاتفاقية.

جريمة التدخل المتعمد في الأنظمة:

التدخل المتعمد في الأنظمة وذلك بارتكاب الأفعال المشار إليها في المادة(04) المتعلقة بالتدخل في المعطيات لتعطيل أداء وعمل الأنظمة بالتدمير والحذف والتعديل والتعطيل مضاف إليها وسيلة البث والإرسال طبقا لأحكام المادة (05).

جريمة إساءة استخدام الأجهزة

تشمل هذه الجريمة طائفتين من الأفعال: الأولى المنصوص عليها في الفقرة الأولى من المادة السادسة، وتشمل بيع أو شراء أو استخدام أو استيراد أو توزيع إنتاج باستخدام الأجهزة والأدوات وبرامج الكمبيوتر بهدف ارتكاب أي فعل جرمي من الأفعال المنصوص عليها في المواد (4 – 5)المشار إليها أعلاه، وكذلك كلمات السر ورموز الدخول أو أية معطيات مشابهة بحيث تتيح اختراق نظام الكمبيوتر، أو الدخول إليه أو إلى أي جزء منه بنية ارتكاب أي فعل منصوص عليه في المواد (5 – 6).

أما الطائفة الثانية من الجرائم وفقا للفقرة الثانية من المادة (06) حيازة وتملك أي عنصر ورد ذكره في الفقرة الأولى أعلاه بنية ارتكاب أي من الأفعال المشار إليها في المواد (6 – 5) من الاتفاقية.

جريمة التزوير المتعمد باستخدام الكمبيوتر:

يتم ذلك بإدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية لتكون مقبولة قانونا، وكأنها بيانات أصلية بغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة، وهنا تقوم المسؤولية الجنائية للفاعل.

جريمة الاحتيال المتعمد باستخدام الكمبيوتر:

الاحتيال المتعمد باستخدام الكمبيوتر بدون حق وعلى نحو يسبب الخسارة للغير على ممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم بيانات الكمبيوتر، أو من خلال التدخل بعمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة اقتصادية لنفسه أو لغيره.

الجرائم المرتبطة بدعارة الأطفال:

هي كل عرض أو توزيع أو نقل أو غير ذلك من الأفعال التي من شأنها أن توفر أو تتيح توفير المواد الإباحية المتعلقة بالأطفال، بغرض التوزيع عبر نظام الكمبيوتر لتوفير إنتاج مواد الدعارة باستخدام الأطفال.

وبما أن مفهوم المواد الإباحية المتعلقة بالأطفال وما تشمله، لم يتم تحديدها في الاتفاقية بشكل واضح، ترك ذلك للنظم القانونية حسب قواعد النظام والآداب العامة، دون أن ننسى أن المقصود بالقاصر يحدد تبعا للقانون الداخلي للدول الأعضاء، على أن يتضمن في جميع الأحوال الأفراد دون 18 سنة.

الجرائم المرتبطة بحق المؤلف:

أوجبت الاتفاقية في (المادة 10) بفقرتيها؛ الأولى بحق المؤلف والثانية بالحقوق المجاورة، وجوب اتخاذ الدول المنظمة تدابير تشريعية تجرم الإخلال أو الاعتداء على حق المؤلف أو الحقوق المجاورة، وفقا لما تحدده القوانين الوطنية للدول الأعضاء.

وعليه فإنّ اتفاقية حماية البيانات الشخصية من مخاطر المعالجة الآلية تقر ضمنيا بالإرهاب الإلكتروني، لأن مجموع الجرائم المشار إليها هي جرائم إرهابية بحكم أنه لا يُعتد بحسن النية في مثل هذه الأعمال غير المشروعة، كما أن ارتكابها لا يكون أبدا لأهداف إنسانية بل سواءً للتهديد، الترويع، الاستغلال، التحطيم أو لدواعٍ مالية وهي الأهداف التي يسعى إليها الإرهاب الإلكتروني، كما أن مجموع التدابير المتخذة بهذا الشأن كانت ناجحة نوعا ما، ولكن ليس بالكثير وهو ما أدى بالاتحاد الأوروبي للاجتماع مرة ثانية بعد مرور مدة من المصادقة على هذه الاتفاقية، ليأتي باتفاقية أخرى تساير التطور التكنولوجي مع صرامة أكثر من حيث الإجراءات وهي اتفاقية بودابست.

تعتبر اتفاقية بودابست وليدة التقرير الذي أعده مجلس أوروبا، وتم اعتماده في 02 أكتوبر 2000 بستراسبورغ، حظى هذا التقرير بقبول دول مجموعة الثمانية (G8) في الاجتماع الذي انعقد في برلين في 24 أكتوبر 2000، إذ أكدت هذه الاتفاقية على الجهود المبذولة من طرف المجلس الأوروبي في مكافحة الجرائم الإلكترونية [1]، والسعي في تحقيق وحدة التدابير التشريعية بين الدول الأوروبية، والتأكيد على أهمية التعاون الدولي والإقليمي في مجال مكافحة الإرهاب الإلكتروني.

---

[1] – واضعو اتفاقية بودابست حول الجرائم المعلوماتية كان هدفهم تبيان الاستعمال السلبي للتكنولوجيا وأنها السبب الحقيقي لظهور جرائم معلوماتية ومجرمين أكثر خطورة مما اعتاد عليه المجتمع الدولي كمفهوم تقليدي للإرهاب والجريمة.

وضعت اتفاقية بودابست من قبل المجلس الأوروبي بالتعاون مع كندا، اليابان، جنوب إفريقيا والولايات الأمريكية بغرض التصدي لمكافحة الإرهاب الإلكتروني والجريمة المعلوماتية، وعرضت للتصديق من طرف وزراء الخارجية للدول الأعضاء، وتعتبر أول معاهدة دولية لمكافحة الجريمة الإلكترونية، فأكدت على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة، مع التركيز على أهمية التعاون الإقليمي والدولي.

تنص هذه الاتفاقية على تعريف وتحديد العقوبات على جرائم الانترنيت في إطار قوانينهم المحلية، وباستقراء هذه الاتفاقية نجد في ديباجتها الكثير من الجرائم المرتكبة عبر الانترنيت، منها المتعلقة بالبيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية[1].

قام الأمين العام المساعد السابق في مجلس أوروبا "**هانس كريستيان كروغو(Hans Christian CROGO)** الذي أشرف على صياغة نص الاتفاقية أن « ***هذه الاتفاقية جاءت في الوقت المناسب لمكافحة الإرهاب عبر الانترنيت، بعد الهجمات التي ضربت الولايات المتحدة الأمريكية في 11 سبتمبر 2001*** » وأشار مدير الشؤون القانونية في المجلس "**غي دوفيل (Gui-DEAUVILLE)** إلى أن:

« ***المجال الحساس في أي اتفاقية تتعلق بالمكافحة ضد الجرائم المعلوماتية والإلكترونية بصفة عامة يكمن في العثور على وسائل التقاط المعطيات المعلوماتية العابرة للحدود*** » والذي لم يتوصل إلى تسوية بشأنه.

أكدت الاتفاقية في مقدمتها على الحاجة لاتخاذ تدابير تشريعية لمكافحة الجرائم المعلوماتية ومخاطرها على الدول، خصوصا في ظل الانترنيت وفي ظل توسع أنظمة الحاسوب المفتوحة ونقل وتدقيق المعلومات، كما أكدت المقدمة على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها، وتوفير قواعد الملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة، مع التركيز على أهمية التعاون الدولي والمحلي والإقليمي مع وجوب إقامة توازن بين متطلبات تنفيذ الاتفاقية، وبين وجوب احترام الحقوق الأساسية والسيادة.

---

[1] – واقد يوسف، النظام القانوني للدفع الإلكتروني، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص 185.

ولأن هذه الاتفاقية جاءت حصيلة جهود دولية وإقليمية، فقد أكدت المقدمة أيضا على أهمية ما أنجز من جهود في حقل الجرائم المعلوماتية من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية (OECD)، ومجموعة الثمانية (G8)، إذ أن مقدمة المشروع أكدت على ثلاثة عناصر أساسية هي:

- أهمية التدابير التشريعية الموضوعية (نصوص التجريم).
- أهمية التدابير التشريعية الإجرائية (النصوص الإجرائية).
- أهمية تدابير التعاون الدولي والإقليمي في مكافحة جرائم المعلوماتية[1].

اتفاقية بودابست تنطلق من اتفاقية مجلس أوروبا لعام 1981، بشأن الحماية من مخاطر المعالجة الآلية للبيانات الشخصية المذكورة سابقا، ومن اتفاقية الأمم المتحدة لعام 1989 بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام 1999 بشأن عمل الأطفال كما تعتمد الاتفاقية على ما تم إقراره من أدلة إرشادية وتوصيات تشريعية منذ عام 1985 بشأن القرصنة والحقوق المجاورة، وتوجيهات عام 1995 المتعلقة بمشكلة القانون الإجرائي المتصلة بتقنية المعلومات، وقد عرّفت هذه الاتفاقية بعض المفاهيم منها نظام الكمبيوتر وبياناته والخدمات في الفصل الأول، أما الفصل الثاني فتم تقسيمه إلى أربع مجموعات:

- المجموعة الأولى: وتتضمن الجرائم التي تستهدف عناصر أمن المعلومات وهي الدخول غير القانوني والاعتراض غير القانوني، والتدخل في المعطيات وإساءة استخدام الأجهزة والتدخل في نظم الحاسوب.
- المجموعة الثانية: وتشمل الجرائم المرتبطة بالكمبيوتر وهي التزوير والاحتيال.
- المجموعة الثالثة: تضمنت الجرائم المرتبطة بالمحتوى وتحوي صورة واحدة وهي جرائم دعارة الأطفال، وتشمل تجريم أي نشاط متعلق بهذا الموضوع.
- المجموعة الرابعة: تضمنت المساهمة الجنائية والعقوبة والشروع ومسؤولية الأشخاص المعنوية ومعايير العقاب.

وبصورة عامة، فإنّ الاتفاقية تلزم دول الأعضاء فيها وأية دولة توقع عليها أو تنضم إليها من خارج المجموعة الأوروبية باتخاذ التدابير التشريعية والإجراءات الملائمة لتجريم هذه الجرائم التي حوتها الاتفاقية[2].

---

[1] – محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 65.

[2] – عبد الله عبد الكريم خالد، جرائم الكمبيوتر والانترنيت على الموقع: www.palip.org

وعليه فإنّ هذه الاتفاقية الأصل فيها تجريم أفعال الإرهاب الإلكتروني الذي ينشط ضمن مجموع الجرائم المصرح بها في الاتفاقية، بل وأكثر من ذلك، إنّ مجموع التدابير الوقائية والعقابية المقررة كلها إجراءات تعمل على حصر أسباب وجود الإرهاب الإلكتروني إن لم نقل تعمل على ردعه.

الفرع الثاني

الجهود العربية في مواجهة الإرهاب الإلكتروني

لا يمكن عدم الإقرار بالتعاون العربي الإقليمي والذي يعتبر الركيزة الأساسية في مواجهة هذا النوع من الإرهاب الجديد، لعل أبرز ما يمكن ذكره هو اعتماد مجلس وزراء العدل العرب للتعاون الجنائي العربي الموحد كقانون نموذجي بموجب القرار رقم 339 لسنة 1996، وهو خطوة جد هامة على الصعيد العربي في مجال محاربة القرصنة وجرائم معطيات الحاسوب، فقد عاقبت (المادة 464) الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة وتغيير المعلومات داخل النظام، وتزوير الوثائق المعالجة آليا وسرقة المعلومات[1].

كما أن المذكرة الإيضاحية لهذا القانون وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص، نجد أن هذا القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص عن طريق الانترنيت، وذلك في (المواد 441 – 446)، كما أشارت (المواد 461 – 463) إلى وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الاسمية وكيفية الإطلاع عليها.

أما (المادة 464) فقد نصت على عقاب من يقوم بفعل الدخول بطريق الغش الكامل أو جزء، أو نظام المعالجة الآلية للمعلومات وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة، وتغيير المعلومات داخل نظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات، تعد هذه المحاولة بالرغم من تواضعها من ابرز ما تم على صعيد تعزيز التعاون على المستوى العربي من الناحية التشريعية، لكن ليست هذه المحاولة الوحيدة أيضا في تكثيف الجهود في مواجهة الجرم الإلكتروني.

---

[1] – حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنيت، دراسة مقارنة، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين شمس، مصر، 2009، ص 120.

الجدير بالذكر أن هناك محاولات جادة لإصدار اتفاقية خاصة بالتعاون الإقليمي العربي في مجال مكافحة الإرهاب الإلكتروني، علاوة على صدور الدليل الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها [1]، بيد أنّ المشروع لم يرَ النور بعد.

كذلك فإن الجمعية المصرية للقانون الجنائي لها اتجاه موحد في هذا المجال، وتمثل ذلك في مؤتمرها السادس المنعقد في القاهرة من 25 – 28 أكتوبر 1993، حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات التي أكد فيها المؤتمرون على عالمية جرائم الحاسب الآلي ووجوب تكاثف الجهود لمكافحتها، لأنها تمثل وجها سلبيا للتقدم الحضاري، ووجوب تعديل نصوص قانون العقوبات التقليدية، أو إضافة نصوص جديدة، لأن النصوص الحالية لا يحيط معظمها بالنشطة المراد تجريمها.

وقد خرج المؤتمر بتوصيات خاصة بصور السلوك الإجرامي في مجال الجرائم الإلكترونية، التي تمثل في واقعها أنماطا أو طوائف جرائم الإرهاب الإلكتروني، وتوصيات بالتعاون الدولي في مجال أنظمة المعلومات، وتنفيذ ما تقره من قواعد ووجب تحقيق التعاون الدولي في مجال مكافحة جرائم الكمبيوتر، وذلك في مجال الإنابة القضائية وتسليم المجرمين، وتنفيذ الأحكام [2]، كما أوصى المؤتمر بوجوب تدريب الضبطية القضائية والنيابية العامة والقضاة، على طرق وكيفية استخدام أجهزة المعلومات وطرق الاستدلال والتحقيق وجمع الأدلة في الجرائم المتعلقة بها.

وفي بيروت انعقد مؤتمر في قانون الملكية الفكرية في الفترة ما بين 25 – 1997/03/26، تمثلت توصيات المؤتمر بضرورة إنشاء محاكم متخصصة للبحث في الالتزامات المتعلقة بالحماية الإلكترونية، وتشجيع التعاون بين الدول العربية، ثم عقد المؤتمر الدولي الثاني للملكية الفكرية في مارس 1998 وطالبت الجهات العربية المشاركة بضرورة إضافة توجيه حول تسهيل نقل التكنولوجيا من الدول الصناعية إلى المنطقة العربية لحماية الاختراعات ومكافحة القرصنة، وتسهيل نقل اختراعات العلماء العرب إلى أوطانهم[3].

---

[1] – صدر طبقا للقرار رقم 417–2004/21 والذي اعتمدته جامعة الدول العربية عبر مجلس وزراء العدل العرب، وهو ما يسمى أيضا بقانون الإمارات العربي الاسترشادي لمكافحة الإرهاب الإلكتروني وجرائم تقنية المعلومات، وما حكمها نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة.

[2] – توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة، مصر من 25 – 28 أكتوبر 1993.

[3] – المؤتمر العربي للملكية الفكرية، مجلة حماية الملكية الفكرية، العدد 62، الربيع الثاني 1998، بيروت، ص 110.

غير أن الملاحظ في هذه الجهود على المستوى العربي هو اعتمادها على التشريعات والأنظمة الخاصة في موضوع جرائم الانترنيت، وكذلك بوضع أطر عامة حول ضوابط استخدام وأمن الانترنيت عن طريق تحديد بعض النشاطات الإجرامية التي يمكن أن توظف الشبكة والحسابات عموما فيها، كما تشمل هذه الجهود العديد من تعليمات أمن المنشآت الحاسوبية، والأجهزة والبرامج، وبعض القواعد العامة المنظمة لارتباط المنشآت الحكومية بالشبكة العنكبوتية[1].

يقابل هذه المجهودات العربية مجموعة من الصعوبات كغيرها من الجهود المبذولة على المستوى الدولي أو الإقليمي، تتمثل أولا في صعوبة اكتشاف وقوع الجريمة، لأن الكثير من الحالات يتم الفعل الإجرامي فيها دون أن يعلم المجني عليه بحدوث اعتداء عليه بالإضافة إلى أنّ الإرهابيين يستخدمون أسماء مستعارة أو يدخلون عبر مقاهي الانترنيت وهنا تكمن الصعوبة في معرفة الجاني أو تحديده.

ثانيا من ناحية المسؤولية فتقوم مشكلة تحديد الأشخاص المسؤولين جنائيا عن جرائم هذه الشبكة بتعدد الأطراف المتعاملين معها، أمّا لو نظرنا لعناصر الأدلة والإثبات فإننا وفي هذا النوع المستحدث من الإرهاب نجد أنفسنا أمام عقبة تتمثل في صعوبة الوصول والسيطرة والمحافظة على تلك الأدلة.

المطلب الثاني

الجهود الوطنية 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 الداخلية بناء منظومة قانونية قوية تتلائم مع أساليب ووسائل مكافحة الإرهاب الإلكتروني أو بتعديلها حتى تصبح أكثر فعالية، لأن التصدي الأمني والتقني لهذا التهديد لا يكفي بل لابدّ من وجود تشريعات وطنية صارمة.

سيتم تناول التجربة الأمريكية وتشريعاتها في مواجهة هذا الخطر الإرهابي (**الفرع الأول**)، ثم التجربة الفرنسية (**الفرع الثاني**)، ثم يتم اختتام المطلب بالتحدث عن التشريعات الوطنية الجزائرية لمواجهة الإرهاب الإلكتروني (**الفرع الثالث**).

---

[1] – فايز عبد الله الشهيري، التحريات الأمنية المصاحبة لوسائل الاتصال الجديدة، مركز الدراسات للنشر والتوزيع، الرياض، 2005، ص 28.

الفرع الأول

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، غير أن ناقوس الخطر ومفهوم الإرهاب تغير عند الولايات المتحدة منذ أحداث 11 سبتمبر 2001 وعلى الساحة الدولية أيضا، هي القفزة النوعية التي اعتبرها الخبراء في مجال مكافحة الإرهاب الحرب العالمية الثالثة، بحكم أنه تهديد في قمة التطور، يقتل ويدمر مستغلا التكنولوجيا باعتماده على عنصر المفاجأة [1]، والجدير بالذكر أن أمريكا قد أصدرت مجموعة من القوانين قبل هذا التاريخ – أي 11 سبتمبر 2001 – لتحكمي 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[2]، وبموجب هذا القانون يعتبر الوصول إلى المعلومات الحكومية المصنفة بدون رخصة، من عدد الجنايات، والوصول إلى القيود المالية أو بيانات الائتمان في المؤسسات المالية أو الوصول إلى الحسابات الآلية الحكومية من عداد الجنح، فالمادة (1030) منه جريمة الاحتيال والنشاطات المرتبطة بالاتصال مع الحاسب الآلي، مثل الفقرة الأولى من هذه المادة تقتضي بمعاقبة كل من يتوصل عن علم أو بدون 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.

---

[1] – رشيد صبحي جاسم محمد، الإرهاب الجديد في نظر الولايات المتحدة الأمريكية، بحث في أصول الظاهرة وأبعادها السياسية، دار الطليعة، بيروت، 2007، ص ص 89 – 90.

[2] – www.usdoj.gov.criminal/cybercrimie/policy-html

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 تتزايد على سنة أو بكلتي هاتين العقوبتين[1].

المادة 223 مع 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[2].

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:

2 – الجرائم التي تستهدف الأشخاص:

وتضم مجموعتين من الجرائم، الأولى الجرائم الغير الجنسية التي تستهدف الأشخاص وتشمل القتل بالكمبيوتر والتسبب بالوفاة عن طريق الإهمال المرتبط بالكمبيوتر والتحريض على الانتحار، والتحريض للقتل عبر الانترنت والتحرش، والمضايقة عبر وسائل الاتصال المؤتمنة، والأحداث المتعمدة للضرر العاطفي أو التسبب بضرر عاطفي عبر وسائل التقنية، والملاحقة عبر وسائل التقنية وأنشطة الاطلاع على البيانات الشخصية أو قنابل البريد الالكتروني أو أنشطة ضخ البريد الالكتروني غير المرغوب فيه، أو بث المعلومات المضللة أو الزائفة أو الانتهاك الشخصي لحركة الكمبيوتر، أو ما يسمى بالدخول غير المصرح به.

أما المجموعة الثانية تشمل الجرائم الجنسية (sexual crimes) وتشمل تحريض القاصرين على أنشطة جنسية غير مشروعة، وإفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية، استضافة المواد الفاحشة، وتصوير أو إظهار القاصرين ضمن أنشطة جنسية عبر الانترنت، لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة.

---

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

[2] – رمضان مدحت، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة–مصر، 2000، ص ص 23 – 24.

جرائم الأموال عدا السرقة:

وتشمل أنشطة اقتحام أو دخول أو توصل غير مصرح به مع نظام الكمبيوتر أو الشبكة، وإيذاء الكمبيوتر واغتصاب الملكية، وخلق البرمجيات الخبيثة والضارة ونقلها عبر الانترنت، وأنشطة إنكار الخدمة وتعطيل أو اعتراض عمل النظم أو الخدمات، وإفشاء كلمة السر الخاصة بالغير، والحيازة غير المشروعة للمعلومات ونقل المعلومات الخاطئة.

جرائم الاحتيال والسرقة (Froud and theft crimes):

وتشمل جرائم الاحتيال، التلاعب بالمعطيات والنظم واستخدام الكمبيوتر للحصول على المعلومات أو استخدام البطاقات المالية دون ترخيص، والاختلاس بالكمبيوتر عبر الانترنت أو بواسطته، وسرقة المعلومات، وقرصنة البرامج، وسرقة خدمات الكمبيوتر، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات.

جرائم التزوير:

وتشمل تزوير البريد الإلكتروني (E-mail Frogery) وتزوير الوثائق والسجلات وتزوير الهوية.

جرائم الانترنت ضد الحكومة(Crimes against the gouverment):

وتشمل جرائم تعطيل الأعمال الحكومية، وتنفيذ القانون، والحصول على المعلومات السرية، والعبث بالأدلة القضائية أو التأثير فيها، وبث بيانات من مصادر مجهولة، وتهديد السلامة العامة والإرهاب الالكتروني، والأنشطة الثأرية الالكترونية أو أنشطة تطبيق القانون بالذات[1].

كما أصدر الكونغرس الأمريكي سنة 2003 قانون مكافحة البريد الالكتروني غير المرغوب فيه (Anti spam law act of 2003) الذي دون القسم (1037) من الفصل 18 من قانون الولايات المتحدة الأمريكية، ويحضر هذا القانون إرسال الرسائل غير المرغوب فيها، ويهدف القانون إلى القضاء على عادة الحصول على عناوين البريد الالكتروني من موقع الانترنت.

إن مراجعة تشريعات الإرهاب الالكتروني والانترنت النافذة في مختلف الولايات المتحدة الأمريكية، يشير إلى أهمية التوجه نحو وضع تشريع شامل وموحد لمكافحة هذه

---

[1] – يونس عرب، جرائم الكمبيوتر والانترنيت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي للدراسات والبحوث الجنائية، أبو ظبي أيام 10 – 2002/02/12، ص 11.

الظاهرة بسبب وجود اختلاف حقيقي في مستويات الحماية، وتحديد أنماط هذه الجرائم، بل بسبب الاختلاف الاصطلاحات المستعملة وأثر ذلك على توفير الحماية، إضافة إلى تباين العقوبات المقررة لهذه الجرائم.

ويرجع التباين والاختلاف بين تشريعات الولايات المتحدة الأمريكية في هذا الحقل إلى عوامل عديدة، أولها التطور السريع الذي شهدته ظاهرة الإرهاب الالكتروني، برغم حداثة الظاهرة وهو ما أدى إلى تباين درجة الاستجابة من ولاية إلى أخرى، خاصة في ظل عدم الاتفاق في أنماط الجرائم ومحدداتها، بل وعلى المفاهيم والاصطلاحات المتصلة بها والعناصر المتضمنة فيها، وأكثر من ذلك الخلط والتشتت الحاصل بشأن الكثير من المفاهيم المتصلة بهذه الظاهرة.

وستظل تشريعات الإرهاب الإلكتروني في الولايات المتحدة الأمريكية قائمة، أولا بسبب عدم قدرة حصر هذه الظاهرة لأنها في تغير مستمر ذات صلة مع التكنولوجيا، ثانيا بسبب وجود مشكل في تنازع القوانين بين مختلف ولايات أمريكا، وثالثا مشكل صلاحيات جهات التحقيق الوطنية خارج الحدود، وتنظيم أنشطة الملاحقة ضمن قانون دولي متوازن وفعال.

الفرع الثاني

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[1] ففي عام 1998 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[2].

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***

---

[1] – J.FRAYSSINET, Internet et protection des données personnelles, expertises des systèmes d'information, Avril 1997, p 99.

[2] – محمد حماد مرهج، جرائم الحاسوب، الطبعة الأولى، إدارة المناهج للنشر والتوزيع، عمان، 2006، ص 179.

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 يبث 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).

الشيء الملاحظ في التجربة الفرنسية في مكافحة الإرهاب الإلكتروني هو الاستجابة المبكرة لهذه الظاهرة في حدود متطلبات الواقع، ولأن فهم الظاهرة أساسا وأخذ التدابير على ضوء هذا الفهم المعمق هو أهم ضمانات النجاح، فإنّ إدراك الدول الأوروبية لظاهرة الإرهاب الإلكتروني متوقف على مستوى انسجام التدابير التشريعية وخطط المكافحة[1] وشكّلت الهيئات التشريعية والتنفيذية الأداة الفعالية لتحقيق هذا الانسجام، والأهم من ذلك ما أسسته جهود التعاون بين دول أوروبا في حقل المكافحة.

الفرع الثالث

الإطار التشريعي في الجزائر

معروفة الجزائر بتجربتها في مكافحة الإرهاب، إذ أشاد بها المجتمع الدولي بمجموع الإجراءات التشريعية المتخذة في هذا المجال، 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 التجارة الإلكترونية في تعاملاتها الاقتصادية المستقبلية، وبما أن الإرهاب الإلكتروني ينشط على نفس مستوى التجارة الإلكترونية من حيث الوسائل، تدارك المشرع الجزائري الفراغ القانوني في مجال الإرهاب الإلكتروني عموما والإرهاب عبر الانترنيت خصوصا بموجب القانون رقم 04-15[2]، 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

---

[1] – R. GASSIN, La protection pénal d'une nouvelle universalité de fait en droit français : Les systèmes de traitement automatisé de données, p 65.

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

(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[1].

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[2].

---

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

[2] – 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.

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[1]،

- 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[2].

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 للتزايد الخطير لهذه الظاهرة، وما تحمله من تهديدات وآثار تدميرية على الأفراد والمجتمعات وحقوق الإنسان.

---

[1] - المادة 04 من القانون رقم 09-04، مرجع سابق.

[2] - المادة 13 و14 من القانون نفسه.

خاتمة

يتشعب موضوع الإرهاب الإلكتروني في ظل التجارة الإلكترونية، لأن التطور التكنولوجي و التقدم العلمي الذي عرفه العالم المعاصر قد إنعكس على النشاط الإرهابي، إذ باتت المنظمات الإرهابية أكثر تنظيما و أوسع إنتشارا، بفضل شبكة الأنترنيت و الإتصالات المتقدمة، الإرهاب الإلكتروني ينشط دون أن يلجأ للعنف المادي او الجسدي، إنه إرهاب علمي و مخطط له يستند على أسس منهجية، مرتكبوه أشخاص أذكياء مؤهلون علميا و عقليا، فهم يهدفون الى نشر الفوضى في البنوك و التحولات المالية العالمية، جمع الأموال و الإستيلاء عليها، إلحاق الضرر بالبنى التحتية و تدميرها، الإضرار بوسائل الإتصال و تقنية المعلومات، و كل هذه التصرفات تعتبر إبتزاز للسلطات العامة و المنضمات الدولية و كذا المنشآت العامة و الخاصة، قصد زعزعة نظام التجارة الإلكترونية الذي يمس الإقتصاد الدولي.

يعتبر إعتماد الدول على أجهزة الكمبيوتر و شبكة الانترنيت، عاملا فعالا في فتح المجال أمام الإرهابيين لتحقيق أهدافهم الإجرامية و تدمير منتجات الفكر الإنساني بصورة غير مشروعة بترهيب و إكراه الآخرين، أو بسرقة هويتهم أو التعدي على أملاكهم الإفتراضية كالبريد الإلكتروني أو شريحة الهاتف النقال، أو عن طريق التجسس الإلكتروني و اختراق أمن المواقع الإفتراضية لسرقة المعلومات، تغييرها أو تزويرها.

كل هذه التصرفات تدل على أن الإرهاب الإلكتروني هو إرهاب جديد لا يعتمد على استخدام الأسلحة و المتفجرات، و إنما يستغل التكنولوجيا لدوافع سياسية، إقتصادية و اجتماعية ضد أنضمة الكمبيوتر و البيانات، والتحكم في كل ماله عالقة بالتجارة الإلكترونية.

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

أما على المستوى الإقليمي فكان بدعم العمليات الثنائية و الجماعية في مكافحة الإرهاب الإلكتروني بحث الدول على بدئ تطبيق التشريعات الضرورية التي تقضي من مقدمي خدمات الأنترنيت و الشبكة العنكبوتية، أن يقدموا المعلومات الضرورية عن

استعمال الإرهابيين لشبكة الأنترنيت الى أجهزة الأمن لتطبيق القوانين المحلية بغرض قمع الإرهاب الإلكتروني.

أكيد ان 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 بالتخاذ مجموعة من التدابير في تشفير البيانات المهمة الموجودة على الأنترنيت، و كذا جهاز الكمبيوتر المربوط بالشبكة العنكبوتية، دون أن نهمل التركيز على تنمية الوعي بالثقافة المعلوماتية و أمنها، و الإلمام بالخطر القادم الذي تخلفه أخطاء الثورة الرقمية.

كل هذه الآليات المتخذة تدل على أن العالم دولا وشعوب 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، فهو يزداد خطورةً وفتكاً كلما زاد التقدم في المجال المعلوماتي، فالاكتشاف والتطور والبناء حتماً يقابله التجسس والتخلف والهدم، فالدمار الذي قد يُلحقه الهجوم الإرهابي بأنظمة المعلومات التي تتحكم في كل مرافق الحياة في هذه المجتمعات التي تعتمد على الكمبيوتر والإنترنت اعتماداً مطلقاً قد يعطل حياة مجتمع بأكملها، والخسائر التي قد تنجم عن مثل هذا الهجوم هي أكبر بكثير مما قد يتصوره العقل إذا لم يدرس ويخطط لوقوعه.

لكن هذا التعاون الدولي و الداخلي في مكافحة الإرهاب الإلكتروني و حماية التجارة الإلكترونية يظل نسبيا في غياب مفهوم جامع و مانع له، لأن بداية العلاج تكون بتشخيص المرض، فكيف لنا إذن بتحديد آليات وقائية فعالة إذا كنا لانستطيع تحديد تعريف للإرهاب الإلكتروني، ولا نستطيع حصر الاسباب التي تؤدي إليه، وكذا عدم فهم أشكاله المتباينة و المتعددة، ذلك أن التجارب الدولية التي تخوضها وعلى رأسها الولايات المتحدة الامريكية في محاربة هذا النوع الجديد من الإرهاب، خلقت أخطارا جسيمة على النظام الدولي،

و حولت إستغلال التكنولوجيا من حق في الدفاع الى انتهاك على الحريات الدولية و الفردية بالتجسس على التعاملات و المراسلات و الإتصالات الدولية، وهو ما جعل الخلط بين الإرهاب و حق الشرعية في استعمال التكنولوجيا لأسباب أمنية و سلمية، و أعطى

دوافع و حجج إضافية لمجموعات إرهابية متطرفة في استعمال التكنولوجيا لأغراض معادية للسلم و الأمن الدوليين.

لذا لابد من دراسة هذا الأمر دراسة مبكرة والأخذ بالاعتبار أسوأ المخاطر المحتملة التي تترتب عليه، وكذلك ضرورة التعاون بين الدول في إنشاء مراكز وطنية تهتم بقضايا الإرهاب الإلكتروني والجرائم الإلكترونية التي اكتسحت عالم الإنترنت والتقنية، ودراستها من النواحي التشريعية والقانونية وبيان أثرها السياسي والاقتصادي والاجتماعي، وكذلك توفير أشخاص ذوي خبرة في مجال التقنية للتصدي لمثل هذه الهجمات في أي وقت أو مكان، وذلك حتى نحدّ من هذه الخطر وننعم بمجتمع ومنشآت ومؤسسات محمية من هذه الاعتداءات.

لكن السؤال الذي يطرح نفسه تلقائيا هو :إذا اعتبرنا أن كل هذه الآليات القانونية كالمعاهدات الدولية المكرسة لمكافحة الجريمة المعلوماتية، تعديل التشريعات الداخلية بما يخدم التعاملات الإلكترونية، و كذا التدابير التقنية المتعارف عليها كالتوقيع الرقمي و ذلك من خلال خدمات التصديق الموثوق بها على هذه التوقيعات، من أجل توفير الأمن في التعامل، و الإهتمام بمفاتيح الشيفرة لحماية سرية البيانات المخزنة و الإتصالات التي تجعلها غير ممكنة القراءة بدون إدخال مفتاح فك الشيفرة، و كذا إستعمال برامج معالجة البيانات و حمايتها من الفيروسات بصفة دورية و مستمرة، موجهة بشكل شخصي لكل دولة تحاول مكافحة الإرهاب الإلكتروني في سبيل حماية تجارتها الإلكترونية، هل فعلا هي أساليب ردعية ناجعة؟ ام مجرد محاولة للحد منه بحكم أنه ينشط على مستوى التكنولوجيا للتواصل و التخطيط و الدعاية و نشر الفيروسات في حين أن هذه الأخيرة– التكنولوجيا – في تطور مستمر و متواصل من خلال شبكة الأنترنيت، شبكات الهاتف المحمول و الاقمار الصناعية...الخ و كلها من الثوابت المركزية في تشكيل أنماط الحياة المعاصرة من حسن الى أحسن في عالم إفتراضي لا يتقيد بحدود و لايعرف تراجعا؟ أو بصورة أكثر دقة نطرح السؤال الموالي: هل يمثل الإرهاب الإلكتروني مفهوم جديد لحرب تكنولوجية أم يظل فقط أحد صور الإرهاب الدولي؟ .

قائمة المراجع

أولا – باللغة العربية:

أ – الكتب:

1. **إبراهيم المنجي** ، عقد نقل التكنولوجيا – التنظيم القانوني لعقد نقل التكنولوجيا والتجارة الإلكترونية –، دار منشأة المعارف، الإسكندرية ، مصر، 2002.
2. **إبراهيم رفعت جمال** ، الجوانب القانونية للمعاملات الإلكترونية، دراسة مقارنة بين القانون المصري والفرنسي، دار الفكر الجامعي، الإسكندرية، مصر 2005.
3. **أحمد جلال عز الدين** ، مكافحة الإرهاب، مطابع دار السهب، القاهرة، مصر، 1990.
4. _____، الإرهاب الدولي وفقا لقواعد القانون الدولي، دار النهضة العربية، القاهرة، مصر، 1992.
5. **أسامة أبو الحسن**، التعاقد عبر الانترنيت، دار الكتب القانونية، مصر، 2002.
6. **أنور زهران** ، التكنولوجيا والحرب المعاصرة، دار الوفاء للنشر، القاهرة، مصر،1987.
7. **الجنبيهي منير وممدوح محمد** ، الشركات الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2005.
8. **دعاء علي**، الطبيعة القانونية للإستيلاء على الأموال من البنك الآلي، مطبعة أوفيست الزمان، بغداد، العراق، 2000.
9. **دوج جيرلاش** ، الحوكمة الإلكترونية والتجارة الإلكترونية، دار العفيون للترجمة والنشر سوريا، 2009.
10. **رأفت رضوان**، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، مصر 1999.
11. **رمضان مدحت** ، جرائم الاعتداء على الأشخاص والأنترنت، دار النهضة العربية القاهرة، مصر، 2000.

12. **رشيد صبحي جاسم محمد** ، الإرهاب الجديد في نظر الولايات المتحدة الأمريكية، بحث في أصول الظاهرة وأبعادها السياسية، دار الطليعة، بيروت، 2007.

13. **سعاد إكرام عوض** ، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشأة المعارف الإسكندرية، مصر، 2008.

14. **سعد عبد اللطيف حسن** ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنيت الطبعة الأولى، دار النهضة العربية، مصر، 1999.

15. **سعد عبد الله أنور** ، مبادئ المنظمة العالمية للتجارة (WOT)، الطبعة الثانية، دار وائل للنشر والتوزيع، عمان، الأردن، 2009.

16. **سهيلة خليل الغازي** ، معوقات التجارة الرقمية في الدول العربية، دار الوفاء للنشر القاهرة، مصر، 2003.

17. **عباس العبودي** ، التعاقد عن طريق وسائل الإتصال الفوري وحجيتها في الإثبات المدني (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الاردن 1997.

18. **عبد الفتاح بيومي حجازي** ، الحوكمة الإلكترونية ونظامها القانوني، المجلد الأول – النظام القانوني للحوكمة الإلكترونية –، دار الفكر جامعي، الإسكندرية مصر، 2004.

19. **عبد الهادي فوزي العوضي** ، الجوانب القانونية للبريد الإلكتروني، المكتبة القانونية مصر، 2004.

20. **العربي بوجمعة جنان** ، التبادل الإلكتروني للمعطيات القانونية، مطبعة وورقة مراكش المغرب، 2006.

21. **علاء الصراط الغامدي** ، الحرب النفسية للإرهاب الجديد، دار منشأة المعارف الإسكندرية، مصر، 2006.

22. **علي كحلول**، الجوانب القانونية لقنوات الإتصال الحديثة والتجارة الإلكترونية، بدون دار، بلد وسنة النشر.

23. **فايز الشهري**، الطرح الفكري على شبكة الأنترنيت، المراحل والرموز، بدون دار النشر مصر، بدون سنة النشر.
24. _____، التحريات الامنية المصاحبة لوسائل الإتصال الجديدة، مركز الدراسات للنشرر و التوزيع، الرياض، 2005.
25. **محمد أمين الشوابكة**، جرائم الحاسوب والانترنيت: الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007.
26. **محمد حسام** ، الحماية القانونية لبرامج الحاسب الإلكتروني، الطبعة الثانية، دار الثقافة للطباعة والنشر، القاهرة، مصر، 2000.
27. **محمد حماد مرهج**، جرائم الحاسوب، الطبعة الأولى، إدارة المناهج للنشر والتوزيع عمان، الأردن، 2006.
28. **محمد سليمان أحمد** ، أساسيات الإستثمار الإلكتروني وتحليل الأعراف المالية، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 2005.
29. **محمد مؤنس محي الدين**، الإرهاب في القانون الجنائي، مكتبة أنجلو مصرية، مصر 1999.
30. **محمود أحمد**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن 2004.
31. **محمود لطفي**، دور المنظمات الدولية في تسيير صندوق النقد الدولي، دار الثقافة للطباعة والنشر، القاهرة، مصر، 2009.
32. **المومني عمر حسن** ، التوقيع الإلكتروني وقانون التجارة الكترونية، دراسة قانونية وتحليلية مقارنة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، 2003.
33. **نضال إسماعيل إبراهيم** ، أحكام عقود التجارة الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.
34. **نعمان العياش**، التجارة الإلكترونية: أداة للمنافسة في الأسواق العالمية، دار الراتب الجامعية للطباعة والنشر، بيروت، لبنان.

35. **هدى حامد قشقوش** ، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنيت، دار النهضة العربية، الإسكندرية، مصر، دون سنة نشر.
36. **هشام محمد رستم**، الإرهاب الدولي، دار النهضة العربية، القاهرة، مصر، 2003.

ب – الرسائل والمذكرات الجامعية:

– الرسائل الجامعية:

1. **حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الانترنيت، دراسة مقارنة، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين شمس، مصر، 2009.
2. **حكيم غريب** ، مكافحة الأشكال الجديدة للإرهاب الدولي، رسالة دكتوراه في العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، جامعة الجزائر 03، كلية العلوم السياسية والعلاقات الدولية، الجزائر، 2014.
3. **غازي عبد الرحمن هيان الرشيد** ، الحماية القانونية من الجرائم المعلوماتية، رسالة دكتوراه في القانون، الجامعة الإسلامية، كلية الحقوق، بدون سنة النشر،لبنان.

– المذكرات الجامعية:

1. **بن غرابي سامية** ، عقود التجارة الإلكترونية ومنهج تنازع القوانين، مذكرة ماجستير في القانون، فرع قانون التعاون الدولي، جامعة مولود معمري، كلية الحقوق،تيزي وزو، 2009.
2. **حمارشة رياض وليد**، عقد البيع الإلكتروني في ظل التجارة الإلكترونية: إبرامه آثاره إثباته، مذكرة ماجستير في القانون ، كلية الحقوق ، جامعة الدول العربية، القاهرة، مصر، 2000.
3. **ذياب موسى البداينة** ، الإرهاب المعلوماتي، مذكرة ماجستير في القانون، كلية التدريب،جامعة نايف للعلوم الأمنية، السعودية، 2008.

a. **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.

4. **لما عبد الله صادق سهب** ، مجلس العقد الإلكتروني، مذكرة ماجستير في القانون،جامعة النجاح، نابلس، فلسطين، 2008.

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

6. **واقد يوسف**، النظام القانوني للدفع الإلكتروني، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.

جـــ – المقالات:

1. **أسامة الكسواني**، "تقنية البريد الإلكتروني والقانون"، مجلة القبس الكويتية، العدد 12 الصادرة في 2008/03/31، (ص ص 1 – 5).

2. **جعفر حسن جاسم الطائي** ، "الإرهاب المعلوماتي وآليات الحد منه"، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، العراق، (ص ص 484 – 507).

3. **رولا الحمصي**، إدمان الأنتيرنت عند الشباب وعلاقته بمهارات التواصل الاجتماعي، بحث مقدم في مؤتمر الملتقى الطلابي الإبداعي الثاني عشر جامعة أسيون، مصر، 2000.

4. **ضياء علي أحمد نعمان** ، "الحماية التقنية للتجارة الالكترونية"، مجلة القانون، العدد الأول، مطبعة ووراقة وطنية، مراكش، المغرب، 2011.

5. **عبد الله عبد العزيز اليونسي**، دور المدرسة في مقاومة الإرهاب والعنق والتطرف، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب، مصر، 2003.

6. **عبد الله عبد الكريم خالد** ، جرائم الكمبيوتر والانترنيت على الموقع: www.palip.org

7. **عبد الهادي فوزي العوضي** ، الجوانب القانونية للبريد الإلكتروني، شبكة المحامين العرب على الموقع: http://www.file://hmht/mhtml

8. **علي العبيدي** ، الإرهاب الإلكتروني أحدث صرعة في معارك الصراعات الدولية العابرة على الموقع:http://www.ibb7.com/pdf/arabic/text

9. **عواطف عثمان محمد عبد الحليم**، "الجرائم المعلوماتية"، مجلة العدل، العدد 24، دون سنة أو بلد النشر.

10. **فادي سالم** ، "اختراق بريد الهوتميل الأكبر في تاريخ الانترنيت"، مجلة انترنيت العالم العربي، أكتوبر 1999، على موقعها في الشبكة: http://www.Jawmag.co.ae

11. **فتيحة محمد قواريري** ، "المواجهة الجنائية لقرصنة المصنفات الالكترونية peer to peer"، مجلة الحقوق الكويت، العدد الأول، مارس 2010، (ص ص 45-51).

12. **محمد الغامدي** ، الإرهاب الأخطر هو المشكلة التي تواجهها المملكة خلال الفترة المقبلة على الموقع:.http://www.assakina.com/pdf/arabic/text

13. **وليد منيمة**، "إنترنيت تقود العالم إلى ثورة في مجال أداء الأعمال إلكترونيا"، PC Magazine، عدد رقم 03، جوان 1999 على الموقع: http://www.arabic.pcmag-arabia.com

14. يونس عرب، جرائم الكمبيوتر والانترنيت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي للدراسات والبحوث الجنائية، أبو ظبي أيام 10 – 2002/02/12.

15. المؤتمر العربي للملكية الفكرية، مجلة حماية الملكية الفكرية، العدد 62، الربيع الثاني 1998، بيروت.

16. دراسة عن البريد الإلكتروني على موقع موسوعة الكمبيوتر والانترنيت العربية: http://www.c4aral.com

د – النصوص القانونية:

-النصوص القانونية الوطنية:

-أمر رقم 75-59 مؤرخ في 26 ديسمبر 1975، يتضمن القانون التجاري، معدل ومتمم،جريدة رسمية عدد 78، صادر في 1975/09.

-قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 مؤرخ في 08 يونيو 1966، والمتضمن قانون العقوبات، ج ر عدد 71، صادر في 2004/11/10.

-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، جريدة رسمية، عدد 47، صادر في 2009/02/16.

-مرسوم تنفيذي رقم 98-257، مؤرخ في 25 أوت 1998، يضبط شروط وكيفيات إقامة خدمات الانترنيت واستغلالها، جريدة رسمية عدد 63، صادر في 1998/08/26

-الوثائق:

-قانون المعاملات الإلكترونية الأردني رقم 85 المؤرخ في 31 كانون الأول 2001 جريدة رسمية الأردنية، العدد 4524.

هـ – الاجتهاد القضائي:

قانون الأنسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996، على الموقع:
http://www.uncitral.org/pdf/arabic/texte/electcom/ml-ecomm-aebook.pdf

- توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة، مصر من 25 – 28 أكتوبر 1993.

و – الاتفاقيات الدولية:

– اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) الصادرة عن هيئة الأمم المتحدة، الكلية العامة 81، ديسمبر 2000.

ز – المواقع الإلكترونية:

1. تعريف نظام(EDI) على الموقع:
http://www.edipourtous.fr/ce-qu-est-l-edi

2. تعريف نظام (VAN) على الموقع :
http://wwwhttp://definition.actufinance.fr/valeur-actuelle-nette-van-757/.

3. الموقع الرسمي لغرفة التجارة الدولية: www.icc.org

4. تعريف الإرهاب الإلكتروني في الولايات المتحدة الأمريكية على الموقع:
http://searchsecurity-techtarget.com

5. أمثلة عن مجموعة هجمات إلكترونية على الشبكات التجارية للولايات المتحدة الأمريكية على الموقع: newshem http://www.alond.com-pxter-com/ologes 002/102/20

6.عدد المواقع الإلكترونية على شبكة الانترنيت على الموقع: http://neus-neteraft.com

7. الشبكة الأمنية اليوروبول على الموقع: http://ar.wikipedia.org/uniki/

8. تعريف الفيزاكارد والماستركارد بطاقات دفع ائتمانية على الموقع:
http://www.mbt3th.us/vb/forum127/thread171445.htm

9. tonmonthly.com/features/2001/green html

10. مقالة إفلين وهايدي " المستقبل المتواصل، تنبؤات حديثة ومفرطة في التفاؤل" على الموقع:
http://www.moderne future predections and overly optimistic. Org/I-

Hidi/Article.html.

11.التدخل الروسي في الشأن السوري وحيثياته على الشرق الأوسط على الموقع:
www.bbc.com/arabic/interactivity/2015/comments-syria-russia-military.

12. حافظة النقود الإلكترونية والافتراضية على الموقع: http://www.bshmokh.com

13.الدليل المتعلق بحماية الخصوصية وقواعد تنقل البيانات على الموقع:
OECD, Gidlines on the protection of privacy and transborder flous of personal data.

14. الجريمة المرتبطة بالحاسوب وتحليل السياسة الجنائية القانونية على الموقع:
www.oecd. Org

15. توصيات إرشادية بخصوص أمن نظم المعلومات على الموقع:
Rocommendation of council concering guidelines for the security.

16. مجموعة الثمانيةG8 نشأتها ومؤتمراتها السنوية، أجندة عملها على الموقع:
www.g8 utorionto.com

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

18. قانون الاحتيال وإساءة استخدام الحاسب الآلي على الموقع:
.www.usdoj.gov.criminal/cybercrimie/policy-html

ثانيا – باللغة الأجنبية:

A – Ouvrages :

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

2. **ROUCOUNAS Emmanel**, Facteurs privées et droit international public, Recueil des cours, l'académie de la Haye Volume 299, Martinus NIJHOFF, 2002.
3. **BITAN Hubert**, Les Contrats d'informatiques, Juris-classeur, Paris, 2002.

4. **FRAYSSINET.J**, Internet et protection des données personnelles, expertises des systèmes d'information, Avril 1997.

5. **BROUEN Jacque-Robert**, Gestion des risques bancaires, Dalloz, Paris, 2000.

6.**FINIDORI Jean-Christophe**, Marketing direct sur internet, international Thomson publishing, Paris, 2001.

GASSIN.R, La protection pénal d'une nouvelle universalité de fait en 7. droit français : Les systèmes de traitement automatisé de données, Paris 2003.

SEDDON Aye Embar, cyber terrorisme, the American Behavioral . 8 Scientist-vol 45 hsseve (6) fel 2002.

HOFMAN.B, THE USE of the internet by Islamic Extremists 9. testemony the house of permanent, may 2006.

BELLEY Pitter, Hached attacked, Abused digital crime exposed, 10. London, Regan Page, 2002.

11. **ATAYLOR Raul**, Maestros ormisogvnistis ? Gender and the social construction of haking, y-vonne tweaks, william publiching, 2003.

12. **NEGPALE Rosa**, Defining cyber terrorism, 2004, Asian scool of cyber law, 04 june, 2006.

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

B – Articles :

1. **BULOI Frédéric**, Internet et commerce électronique, 2ème édition, éditions Hermès, Paris, 2003, pp 24 – 25.
2. **Manar (C)**, Aspects juridiques de l'e-mail, Dalloz, 8 Affaires, n° 140, 1999.

3. **M.POLLITT March**, Cyber terrorism : factor fanncy ? procceding of the 20th national information system, conference, October, 1997, (pp 285-289).

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

5. **JINIKING Michael**, The future cource of terrorism, futurist interview, January 2001, in http://www.wfs.org/intjenikins.htm

6. **W. BRENNER.Susan**, State cyber crime ligistation in the united states of America, Availabel in : www.richmond.edu

فهرس

مقدمة.....	04
الفصل الأول	
علاقة التجارة الإلكترونية بالإرهاب الإلكتروني	08
المبحث الأوّل: ماهية التجارة الإلكترونية والإرهاب الإلكتروني.....	09
المطلب الأوّل: مفهوم التجارة الالكترونية.....	09
الفرع الأول: تعريف التجارة الإلكترونية.....	09
أولا: تعريف التجارة الإلكترونية في بعض المنظمات الدولية.....	10
أ: منظمة الأمم المتحدة (United Nation).....	10
ب: منظمة التجارة العالمية (WOT).....	11
ج: منظمة التعاون الاقتصادي والتنمية(OECD).....	12
ثانيا: تعريف التجارة الإلكترونية على المستوى الإقليمي والهيئات المتخصصة.	13
أ:الإتحاد الأوروبي (European Union).....	13
ب:غرفة التجارة الدولية (ICC)	14
ثالثا: تعريف التجارة الإلكترونية وفقا للتشريعات الوطنية.....	15
أ: تعريف المشرع الأمريكي.....	15
ب: تعريف المشرع فرنسي.....	17
ج: تعريف المشرع الجزائري.....	18
الفرع الثاني: خصائص التجارة الإلكترونية.....	19
أولا: غياب وجود مادي للأطراف.....	20
ثانيا: وجود الوسيط الإلكتروني.....	20
ثالثا: السرعة في إنجاز الأعمال التجارية الإلكترونية.....	21

رابعا: تتخطى الحدود الجغرافية.....	21
المطلب الثاني: ماهية الإرهاب الإلكتروني.....	23
الفرع الأول: مفهوم الإرهاب الإلكتروني في بعض القوانين الوضعية.....	24
أولا: الولايات المتحدة الأمريكية.....	24
ثانيا:الاتحاد الأوروبي.....	26
ثالثا: تعريف الدول العربية للإرهاب الإلكتروني.....	28
الفرع الثاني: خصائص الإرهاب الإلكتروني.....	30
أولا: التعامل بالبريد الإلكتروني.....	31
أ: تعريف البريد الإلكتروني.....	31
1 – التعريف التشريعي للبريد الإلكتروني.....	31
2 – التعريف الفقهي للبريد الإلكتروني.....	32
3 – التعريف التقني للبريد الإلكتروني.....	32
ب: خصائص البريد الإلكتروني.....	34
ثانيا: التعطيل والتصرف في نظام الخدمات والمعلومات الإلكترونية.....	37
أ: تعطيل الخدمات الإلكترونية.....	37
ب: التصرف في المعلومات الإلكترونية.....	39
ثالثا: تعدد صور الإرهاب الإلكتروني.....	40
أ: إرهاب إلكتروني ضد الأفراد.....	40
ب: إرهاب إلكتروني ضد المؤسسات.....	41
ج: إرهاب إلكتروني ضد الدول.....	42
المبحث الثاني: مخاطر الإرهاب الإلكتروني على التجارة الإلكترونية.....	43
المطلب الأوّل: المخاطر الأمنية للإرهاب الإلكتروني على التجارة الإلكترونية..	43
الفرع الأوّل: قرصنة و/أو تعطيل نظام المعلومات.....	44
أولا: خرق الحماية المادية (Breachers of Physical Security).....	44
أ: التفتيش في مخلفات تقنية(Dumpster Diving).....	44

ب: الالتقاط السلكي (wiretapping).....	44
ثانيا: خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين(Breaches of personnel security).....	44
أ: التخفي بانتحال شخصية موظف.....	45
ب: البرمجيات الخبيثة (code Malicious).....	45
الفرع الثاني: استغلال الشبكات الاجتماعية المعلوماتية.....	45
أولا: مخاطر الشبكة الاجتماعية الفايسبوك (facebook).....	45
ثانيا: مخاطر محرك البحث غوغل (google).....	46
ثالثا: مخاطر خدمة الفيديو (You tube).....	47
الفرع الثالث: تأثير التجسس على التجارة الإلكترونية.....	48
المطلب الثاني: المخاطر التجارية للإرهاب الإلكتروني.....	50
الفرع الأوّل: موقع الشبكة المعلوماتية في المعاملات التجارية الإلكترونية.....	50
الفرع الثاني: اختراق الإرهاب الإلكتروني لمواقع التجارة الإلكترونية.....	52
أولا: انتهاك نظام الحماية السرية للتجارة الإلكترونية.....	52
ثانيا: إتلاف مواقع التجارة الإلكترونية باستخدام الفيروسات.....	54
الفرع الثالث: مشكل بطاقات الدفع الإلكترونية (بطاقات الائتمان).....	55
أولا: إساءة استعمال بطاقة الدفع الإلكتروني من طرف حاملها.....	56
ثانيا: إساءة الاستعمال من قبل الغير.....	56
ثالثا: إساءة الاستعمال من قبل موظفي البنوك.....	57
رابعا: إساءة الاستعمال من قبل التاجر.....	57
خامسا: إساءة استعمال بطاقات الائتمان عن طريق شبكة الانترنيت.....	58
الفصل الثاني	
التدابير الدولية الإقليمية والوطنية في مكافحة الإرهاب الإلكتروني	59

المبحث الأوّل: الجهود الدولية لمكافحة الإرهاب الإلكتروني.....	60
المطلب الأوّل: تحديد منهج دولي لحماية البيئة الإلكترونية.....	60
الفرع الأول: الآليات الأمنية الدولية المكرسة للحد من الإرهاب الالكتروني....	61
أولا: التعاون الأمني ضد الإرهاب الإلكتروني.....	61
ثانيا: تبادل المعلومات والخبرات.....	65
أ: التعليم ونشر والوعي بمخاطر الإرهاب الإلكتروني.....	65
ب: تفعيل دور الإعلام ضد الإرهاب الإلكتروني.....	66
الفرع الثاني: الآليات التقنية الدولية لحصر الإرهاب الإلكتروني.....	67
أولا: حماية المعاملات المالية الإلكترونية.....	67
أ: وسيط الوفاء الإلكتروني.....	68
ب: حافظة النقود الإلكترونية والافتراضية.....	69
ثانيا: حماية المواقع الخاصة بالإنترنت.....	70
أ: نظام التشفير كوسيلة لحماية سرية المعلومات.....	70
ب: الجدران النارية كوسيلة لحماية المحتوى.....	72
المطلب الثاني: دور المنظمات الدولية في مكافحة الإرهاب الإلكترونية.....	73
الفرع الأوّل: دور الأمم المتحدة.....	74
الفرع الثاني: دور منظمة التعاون الاقتصادي والتنمية (OECD).....	77
الفرع الثالث: دور مجموعة الثمانية (G8).....	78
المبحث الثاني: الجهود الإقليمية والوطنية في مكافحة الإرهاب الإلكتروني.....	81
المطلب الأوّل: الجهود الإقليمية لمكافحة الإرهاب الإلكتروني.....	81
الفرع الأول: دور الاتحاد الأوروبي في مواجهة الإرهاب الإلكتروني.....	82
الفرع الثاني: الجهود العربية في مواجهة الإرهاب الإلكتروني.....	90
المطلب الثاني: الجهود الوطنية في مكافحة الإرهاب الإلكتروني.....	93
الفرع الأول: إطار التشريعي في الولايات المتحدة الأمريكية.....	93
الفرع الثاني: الإطار التشريعي في فرنسا.....	97
الفرع الثالث: الإطار التشريعي في الجزائر.....	99

خاتمة.....	103
قائمة المراجع.....	106
فهرس.....	117

الملخص

في عصر العولمة و الإنتشار الجوهري لوسائل التقنية الحديثة، بات الحديث عن الإرهاب و جرائم التقنية الحديثة هام جدا،حيث انه يهدد الإستقرار و الأمن الدوليين، و من الواضح ان الجريمة الإلكترونية و الإرهاب باستخدام التقنية الحديثة لم تتضح خطورتهما الا مع ظهور الأنترنيت بإمكانياتها الهائلة، حيث أسهمت في عولمة الكثير من المظاهر الإجرامية، كان من أبرز صورها الإرهاب الإلكتروني.

يختلف الإرهاب الإلكتروني عن الإرهاب العادي كونه يستخدم سلبا التكنولوجيا للتهديد،لتحقيق مكاسب مادية و/او معنوية،و التأثير على الخصوم.

لذلك كان لابد من إيجاد آليات و تدابير قانونية يمكن بها مجابهة هذه الظاهرة ذات الأبعاد غير المتناهية،التدميرية و الخطيرة

Résumé

En pleine époque de mondialisation et de la propagation essentielle des moyens de la technologie moderne, la discussion sur le terrorisme et les crimes liés à la technologie moderne, est devenue très importante, car, ils menacent la stabilité et la sécurité mondiales.

Il est très clair que le crime électronique et le terrorisme via la nouvelle technologie n’est aussi dangereux qu’avec l’apparition de l’internet en ses énormes capacités. Cependant, celle-ci a participé dans la mondialisation de plusieurs aspects criminels, parmi ses principales figures : le terrorisme électronique.

Le terrorisme électronique est différent de celui ordinaire, car, il utilise négativement la technologie aux fin de menacer, d’obtenir des ou morales, voire même influencer sur les ennemis./fins matérielles et

Pour ce, il faux retrouver des mécanismes et des mesures juridiques pour faire face à ce phénomène aux perspectives infinies, désastreuses et dangereuses.