الحماية القانونية و التقنية للتجارة الالكترونية

ذ مصطفى الفوركي

باحث بسلك الماستر المقاولة و القانون
بكلية الحقوق سطات جامعة الحسن الاول

MAROCDROIT.COM
تاريخ النشر: 15 دسمبر2011

تمهيد

التجارة الالكترونية هي شكل من اشكال الصفقات التجارية التي يتصل اطرافها بعضها ببعض عبر شبكة المعلومات الدولية سواء على المستوى المحلي او الدولي , ولاتقتصر التجارة الالكترونية على الفرص التجارية فحسب ' وانما تمتد لتشمل نطاقا واسعا من المعلومات التجارية منها التسويق والترويج والتسليم وغيرها .

ويتحدد الاطار القانوني لموضوعنا في قانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية الصادر يوم 6 دجنبر 2007 بظهير شريف رقم 01-07-129 محددا النظام المطبق على المعطيات القانونية التي يتم تبادلها بطريقة الكترونية

فالتجارة الالكترونية في تزايد مستمر مع أنتشار الأنترنت .دراسة حديثة أشارت الى أن حجم التداول الالكتروني بين الشركات كان 109 بليون دولار في عام 2004 ويتوقع أن ينموا الى حجم 2.7 ترليون دولار في عام 2012 , دراسات أخرى أشارت الى أن حجم التجارة الألكترونية يبلغ 15% من أقتصاد دول العالم الأول ,دراسات حديثة متفائلة تتوقع أن تشكل التجارة الألكترونية 30% من الأقتصاد العالمي بحلول 12017. اي كان الحجم التجاري فالدرسات تؤكد أن التجارة الالكترونية بين الشركات تشكل 90% من نشاطاتها عبر الأنترنت.

[1]- موقع http://www.tunisia-sat.com/vb/showthread.php?t=715157

وتظهر اهمية موضوعنا هذا في كون ان من اهم الاسباب وراء عدم ازدهار وتقدم التجارة الالكترونية في بلدنا هوتخوف الناس بصفة عامة والمتعاملين العرضيين – بصفة خاصة – من قرصنة معلوماتهم الشخصية او اموالهم من قبل القراصنة او الهاكرز و حتى من قبل المتعامل معهم الكترونيا لذلك وجب توضيح الحماية التي يتمتع بها هؤلاء سواء التقنية منها او القانونية .

فالى اي حد استطاع المشرع المغربي من خلال قانون 53-05 حماية جميع المتدخلين في التجارة الالكترونية ؟

وهل هذه الحماية كفيلة بدرء جميع الاخطار التي تهدد وجودهم ككيان قانوني ؟

وكيف يمكن حماية التجارة الالكترونية من تطفل المتطفلين و أعمال المخربين ؟

لمعالجة هذه الاشكالات ارتأينا الى تقسيم موضوعنا الى مبحثين الاول متعلق بالحماية القانونية للتجارة الالكترونية اما الثاني فمتعلق بالحماية التقنية للتجارة الالكترونية

كما سنعتمد من حيث المنهج على المنهج المقارن بالاضافة الى المنهج التحليلي

التصميـــــــــــم

✓ المبحث الاول : الحماية القانونية للتجارة الالكترونية

➢ المطلب الاول : الحماية المدنية للتجارة الالكترونية

- الفقرة الأولى : المسؤولية العقدية
- الفقرة الثانية : المسؤولية التقصيرية

➢ المطلب الثاني : الحماية الجنائية للتجارة الالكترونية

- الفقرة الأولى : بعض الجرائم المقترفة من قبل مزود الخدمة المعلوماتية
- الفقرة الثانية : بعض الجرائم المقترفة من قبل الغير

✓ المبحث الثاني : الحماية التقنية للتجارة الالكترونية

➢ المطلب الأول : حماية المواقع الالكترونية

- الفقرة الأولى : اختراق المواقع
- الفقرة الثانية : حماية المواقع من الاختراق

➢ المطلب الثاني : حماية البريد الالكتروني والبطائق البنكية

- الفقرة الأولى : اختراق البريد الالكتروني و طرق حمايته
- الفقرة الثانية : قرصنة االبطائق الالكترونية وسبل حمايتها

المبحث الأول: الحماية القانونية

تنقسم الحماية القانونية التي أولاها المشرع لكل مستعمل لوسائل التجارة الإلكترونية على حماية مدنية و حماية جنائية.

المطلب الأول: الحماية المدنية

لعل أبرز أوجه الحماية التي يمكن أن يستفيد منها كل متعامل بأي وسيلة الكترونية سواء كان هذا الأخير شخا طبيعيا (مستهلك) أو شخصا معنويا في إطار نشاطه التجاري الاقتصادي، أو المدني هي تلك المسؤولية المدنية التي قد تطال كل من أخل بأحد أو بعض الالتزامات الملقاة على عاتقه فهي الالتزامات قد تكون عقدية أي ناشئة عقب إبرام عقد بشكل الكتروني وبالتالي فإن كل مخل لها تكون مسؤولا مسؤولية عقدية كما قد تكون التزامات قانونية ملقاة على جهة معينة بمقتضى القانون وبالتالي فإن الإخلال بها سيعرض الملتزم بها إلى جزاء مدني جزاء مسؤولية التقصيرية.

الفقرة الأولى: المسؤولية العقدية

إن المسؤولية العقدية كما سبقت الإشارة إلى ذلك تنتج عن إخلال في التزامات التعاقدية وبالتالي فلا يمكن الحديث عنها بدون توافر عقد صحيح مبرم بشكل الكتروني حسب ما ينص عليه قانون 05.53 وعليه فهذه العقود يتمثل محلها في شقين لا ثالث لهما إما سلعا أو خدمات.

فالعقد الإلكتروني الذي يعتبر الأداة الفعالة لتحريك التجارة الإلكترونية –إذ لا يمكن التفريق بينهما فهما وجهان لعملة واحدة– لا يتميز عن العقد المبرم بطريقة غير إلكترونية فيما يخص الالتزامات التي يتحملها المتعاقدون إلا فيما يخص طريقة تنفيذ تلك الالتزامات خاصة تلك العقود المنصبة على سلعة أو خدمة مقدمة بطريقة الكترونية أو أن الأداء يتم بوسيلة الكترونية وبالتالي فإن أركان المسؤولية العقدية تبقى هي ذاتها من خطأ وضرر وعلاقة السببية. إلا أن ما يميز المسؤولية العقدية في التجارة الإلكترونية هي طبيعة كل من الخطأ والضرر.

أولا: الخطأ ألعقدي

يعتبر كل طرف من أطراف العلاقة التعاقدية مرتكبا لخطأ عقدي إذا لم يقم بتنفيذ التزامه العقدي أو تأخر في تنفيذه أو تنفيده بشكل معيب باعتبار أن هذا الخطأ يمثل انحرافا في سلوك المدين يؤدي إلى مسائلته.[2]

فقبل التطرق لصور الخطأ في المعاملات الإلكترونية وجب التطرق لطبيعة الالتزام في المجال الإلكتروني، هل هو التزام ببذل عناية أم هو التزام بتحقيق نتيجة؟

إن أغلب الالتزامات في المعاملات الإلكترونية غايتها تحقيق نتيجة لأن المتعاقد يسعى إلى الوصول إلى هدف معين وذلك" إما للاستفادة من خدمة معينة أو من سلعة معينة محلا للإلتزام، وإن عدم تحقيق هذا الهدف ولو بعد بذل العناية الكافية يشكل عدم التنفيذ، ويكون في هذه الحالة

[2]- كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان المسؤولية الجزائية والمدنية، دار الثقافة للنشر والتوزيع طبعة 2008, عمان, الأردن, ، ص37.

للمتعاقد الآخر أن يثبت فقط وجود الالتزام لكي يكون الملتزم مجبرا ببيان أنه حقق النتيجة التي التزم بها وإقامة مسؤوليته التعاقدية، ما عدا إذا أثبت تدخل السبب الأجنبي المتمثل إما في القوة القاهرة أو الحدث الفجائي أو خطأ الدائن (الطرف الأخر) أو خطأ الغير.[3]

غير أن بعض الفقه[4] يرى بأن هناك من العقود المعلوماتي ة التي يكون فيها الالتزام مجرد بدل عناية، إلا أننا نستدل بقرار لمحكمة استئناف باريس عقب قضية أحيلت عليها تدور حول عدم تمكن مهندس معلوماتي من تصميم برنامج للحاسوب حيث اعتبرت أن الالتزام في هذه الحالة يبقى التزاما بتحقيق نتيجة, لأن مصمم البرنامج إذا لم يكن واثقا من نتيجة عمله فعليه ألا يلتزم بالقيام به، ومن ثم فإن إرادة الطرفين عند التعاقد هي التي تحدد طبيعة الالتزام.[5]

هذا عن طبيعة الالتزام أما فيما يخص صور الخطأ، فإن هذا الأخير يتخذ صورتان:

أ. **الإخلال بالتزام السليم أو أداء الخدمة**

يمتاز تسليم محل المعاملات التجارية بنوع من الخصوصي ة وفقا لطبيعة الخدمة أو السلعة. فبرنامج الحاسوب مثلا تسلم من خلال تحميلها على دعامات "الأقراص المغنطة أو مفتاح الفلاش ديسك" أو على شبكة الانترنت مباشرة في دفعة واحدة أو عبر مراحل.

---

[3]- محمد الكشبور،، نظام التعاقد ونظريانا القوة القاهرة والظروف الطارئة مطبعة النجاح الجديدة، الدار البيضاء, الطبعة الأولى، ص1993.

4 c. a Paris 15 sep 1995 GP, 1995 2P 329 led gabadoux

[5]- محمد حسين المنصور, المسؤولية الالكترونية , دار الجامعة الجديدة للنشر , الاسكندرية, الطبعة الاولى . 2003 ص58.

والتسليم لا يقتصر على الشيء وحده وإنما يشمل كذلك ملحقاته التي توضح كيفية عمل الأنظمة المعلوماتية ومعداتها وتحضيراتها المادية وأساليب الصيانة, وهي في الغالب بيانات تسجل على أقراص أو يتم تحميلها عبر الإنترنت.[6]

ولعل ميعاد التسليم يكتسي أهمية كبرى في العقود المعلوماتية إذا كان محددا, لأن ضرر التأخير يشكل أهم صور المسؤولية العقدية، أما إذا لم يكن كذلك فيفترض وقوعه فور إبرام العقد ما لم تقض طبيعة الشيء محل المعاملة بمواعيد أخرى، أو إذا كان العمل ذهنيا يتطلب فترة زمنية ملائمة لانجازه.[7]

ب. **عدم مطابقة السلعة أو الخدمة للمواصفات**

إن المورد في المجال المعلوماتي ملزم بمعرفة احتياجات زبونه وإعلامه بالضرورات التقنية للنظام والأجهزة المعلوماتية التي يقدمها إليه ومدى قدرتها عل تحقيق الغاية التي يسعى إليها.

فالتسليم في المجال المعلوماتي يتسم بنوع من الخصوصية حيث قد يقوم المزود بإرسال السلعة أو الخدمة المطلوبة نوعا لكنها غير المطلوبة من حيث الإصدار مثلا، ذلك أن البرامج المعلوماتية سريعة التحديث أو أنها هي المطلوبة نوعا و إصدارا إلا أنها غير ملائمة لحاسوب المستفيد لذلك وجب على المزود إعلام الطرف الآخر بكل البيانات التي قد تساعده على تلبية حاجاته من وراء

---

[6]- محمد حسن منصور، م س، ص89.

[7]- العربي جنان، م س، ص59.

التعاقد,لكي يكون التسليم مطابقا لتلك الاحتياجات. وللوصول إلى هذه الغاية فإن الزبون والمورد مطالبان معا بإقامة حوار بينهما يمهد لتنفيذ العقد على الوجه الأكمل.[8]

* الضرر العقدي

إن الضرر العقدي المباشر الذي يطال طرف العلاقة التعاقدية المبرمة بشكل الكتروني ينقسم إلى قسمين ضرر متوقع وضرر غير متوقع، فالمدين لا يسأل إلا أن الضرر المباشر المتوقع أما الضرر غير المتوقع فلا يثير مسؤولية.

ونظراً الارتباط الضرر بالتعويض عن المسؤولية العقدية وكون الضرر يختلف حسب طبيعة المعاملة الإلكترونية، فإن هذا الأخير يكون مفترضا بمجرد تحقق الخطأ إلا في حالة الغش المعلوماتي.

* علاقة السببية:

إن علاقة السببية في المجال الإلكتروني لا تختلف عن علاقة السببية المقررة في القواعد العام وهي ذلك الرابط بين الخطأ والضرر أي بصفة أخرى أن يكون الضرر هو نتيجة خطأ مرتكب وبالتالي فإذا ما ألحق ضرر بأحد أطراف العلاقة التعاقدية بطريقة الكترونية دون أن يخل الطرف الأخر بأي التزام من التزاماته فلا وجود لمسؤولية عقدية كأن يقوم مقدم الخدمة بإرسال البرنامج الإلكتروني محل البيع للمستفيد غير أن حاسوب هذا الأخير قام بمحوها بطريقة أوتوماتيكية عن

---

[8]- A. Bensoussan, J francois foronerio les arrêts tendons de l'informatique hermès science la version octobre 2003, p 96-97.

طريق مضاد الفيروسات أو بأي طريقة تقنية أخرى ففي هذه الحالة لا وجود لمسؤولية مقدم الخدمة متى أثبت توصل المستفيد بمحل البيع أو الخدمة.

ثانيا: المسؤولية التقصيرية

إن أساس المسؤولية التقصيري هو الإخلال بالتزام قانوني لا عقدي وقد يتساءل الكثير في ما مدى إمكانية تطبيق المسؤولية التقصيرية في التجارة الإلكترونية حيث إن هذه الأخيرة لا يمكن أن تنشق عن العقد المبرم بشكل إلكتروني.

فكثيرة هي الحالات المسؤولية التقصيرية إذ أن المشرع أنشأ مجموعة من الجهات من بينها الجهة المكلفة بالمصادقة الإلكترونية -المكلفة بتفعيل التجارة الإلكترونية- إلا أنه في نظريات يبقى أهم ما يثير المسؤولية التقصيرية هو ذلك النزاع الذي يثار بين أسماء النطاق والعلامات التجارية.

ولعل أهم ما دفع التشريعات على اختلافها على سن قواعد قانونية موجبة للمسؤولية التقصيرية هو أنه في السنوات الأولى لإتاحة شبكة الإنترنت للاستخدامات التجارية، فإن العديد من الشركات الكبيرة كانت لا تزال غير مقتنعة بأن هذه الشبكة ذات أهمية في نماذج أعمالها، وكذا فإن الكثير من المالكين للعلامات التجارية لم يكونوا على درجة كافية من الإدراك على ضرورة تسجيل علاماتهم التجارية كأسماء نطاق.

وقد سمح هذا الاتجاه الأخير لقراصنة الإنترنت بالاستفادة من هذه الفرصة, والقيام بتسجيل الكثير من العلامات التجارية أوالإشارات أو العلامات المشابهة كأسماء نطاق لا تقل أهمية عن العلامات التجارية التي يملكونها ويتمتعون بحق استغلالها. وقد أصبح أسماء النطاق عنصراً مكملا

للعلامات التجارية، لأنها تتفق مع المعايير النموذجية للعلامات التجارية في أغلب الأحيان[9] بل أكثر من ذلك فإن هناك رقابة معينة أقرتها مجموعة من المواقع الإلكترونية ونذكر على سبيل المثال, موقع "ياهو" Yahoo في المحاكم الفرنسي، حيث إن يبيع المخلفات التذكارية النازية غير الشرعي في العديد من أفراد أوربا، ومن ضمنها فرنسا ولكن ليس في الولايات المتحدة الأمريكية.

وتتلخص الوقائع عندما أقامت منظمة فرنسية دعوى ضد موقع ياهو في فرنسا للسماح لمزادات المخلفات التذكارية النازية على موقعه الأمريكي مع العلم أن مثل هذه المزادات لم تحدث على موقع ياهو الفرنسي، و قد طلبت محكمة النقض الفرنسية من موقع ياهوأن يمنع المستهلكين من الوصو ل إلى المزادات على الموقع الأمريكي. وتنفيذا لهذا القرار فقد أرسل موقع ياهو التحذيرات للفرنسين على موقعه الأمريكي لكي ينذرهم بعدم الدخول في هذه المزادات، ولكنه اعترض على القرار بأنه يستحيل من الناحية التقنية ضمان تنفيذ مثل هذا المنع.

وبالتالي فإن ما يمكن استنتاجه هو أن القواعد القانونية المطبقة في ميدان التجارة الإلكترونية ذهب هي التي يجب أن تماشى مع الوسائل التقنية المتوفرة حيث هناك من الأمور التي يعجز الإنسان ردعها.

ولعل أهم أسباب نشوء نزاع بين العلامات التجارية وأسماء النطاق أو "الدومين" هو أن هيئة حلول الشبكة المتخدة (NSI) لتسهيل أسماء النطاق تعتبر غير مسؤولة عن التحقق من أن اسم النطاق يتعارض مع علامة تجارية, والمشاكل غالبا ما تظهر في مكتب تسجيل اسم النطاق لأن هيئة

[9]- محمد اسماعيل أحمد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية منشورات الحلي الحقوقية بيروت الطبعة الأولى سنة 2009، ص423.

NSI تمتنع عن التحقيق في سجل مكتب العلامة التجارية وبرادة الاحترام (PTO) لتقرير فيما إذا كان اسم النطاق المقترح يتعارض مع علامة تجارية موجودة بل إنما تقوم بترك مهمة البحث في سجل **pto** إلى مقدم طلب التسجيل لاسم النطاق بيد أنه تستطيع هيئة NSI أن تستفيد بسهولة من سجل PTO للقيام بالبحث عن العلامة التجارية حينما يتقدم أحد الأشخاص بطلب تسجيل اسم نطاق ولكنها لا تفعل ذلك.[10]

فبالنسبة لتجربة الولايات المتحدة الأمريكية في هذا الصدد باعتبارها من أوائل التشريعات العالمية المنظمة للمجال الإلكتروني والأكثر إلماما بما تتوفر عيله من إمكانيات لوجستيكية وتقنية تكفل لها ذلك، دعت منظمة حقوق اسم النطاق لمعرضة سياسة هيئة NSI باعتبارها غير عادلة، ولذلك فإن الكونكرس الأمريكي وافق على إنشاء هيئة ICANN لتبني سياسة التحقيق في النزاعات الخاصة بالعلامات التجارية، حيث إجا اقترح مقدم طلب التسجيل اسم نطاق يتعارض مع علامة تجارية، فإن المسجلين يحدروا مقدم بأن هناك علامة تجارية مطابقة لدلك الإسم المقترح كاسم نطاق, وعندئذ يكون لمقدم الخدمة إما أن يعدل عن الطلب أو يستمر في إجراءات التسجيل متحملا بذلك المخاطر التي يمكن أن تنجم عن هذا التسجيل المتمتلة في غرامات كبيرة نتيجة التعدي على علامة تجارية موجودة.

وبالتالي فإن هذا النظام يمكن ن يتصدى للسطو الإلكتروني على العلامات التجارية إلا أنه في المقابل يترك لحرية التسجيل إما العدول أو الاستمرار في تسجيل اسم النطاق وهو ما يمثل حماية

[10]- محمد اسماعلي أحمد اسماعيل، م س، ص447.

بعدية أي بعد التطاول والإضرار بالعلامة التجارية عن طريق جبر الضرر بواسطة التعويض عن طريق تطبيق قانون حماية التحففيف للعلامات التجارية(FTDA)، غير أن العقوبات المعمول بها وفق هذا القانون تبقى قاصرة على منع الاعتداء عل العلامات التجارية المشهورة بالسطو الإلكتروني عليها وتسجيلها كأسماء نطاق على شبكة الإنترنت هذا من جهة أما من جهة أخرى فالشروط الصعبة التي يتطلباه القضاء الأمريكي لتطبيق قانون FTDA أدى إلى ترك العلامة التجارية بدون حماية قانونية وقضائية كافية وفعالة .لذلك فقد قرر الكونجر س الأمريكي إصدار قانون حماية المستهلك من القرصنة الإلكترونية في 29 نونبر 1999 المعدل لقانون العلامة التجارية وكان الهدف من اختيار القواعد القانونية التي يتضمنها بعناعة ودقة متناهية، وذلك ليمتد تطبيقها على الحالات التي يتبين فيها أن المسؤول قد سجل، أو مرر أو استخدم اسم نطاق بشكل سيء, وبقصد بسوء نية لتحقيق الربح من أصحاب النية الحسنة لمالكي العلامة التجارية المعتدى عليها.

ولعل أهم التدابير التي جاء بها قانون (ACPA)والموجبة للمسؤولية التقصيرية هي منع قرصنة الإنترنت حيث عندما تتعرض العلامة التجارية للسطو الإلكتروني من قبل قراصنة الإنترنت، فإن مالك هذه العلامة يستطيع اتخاذ بعض الإجراءات وفقا لهذا القانون وذلك على النحو التالي:

إن أي شخص سيكون مسؤولا بموجب دعوى مدنية من قبل مالك العلامة تجارية إذا توافرت مجموعة من الشروط:

- لديه سوء نية للربح من تلك العلامة

- استخدام صاحب النطاق لاسم مماثل أو مشابه لعلامة متميزة أو علامة مشهورة أو كلمة أو اسم محمي بالاستناد إلى قوانين الولايات المتحدة

وبالتالي فإن كل مسجل لاسم نطاق عن حس نية يستثنى من المسؤولية.

أما فيما يخص الأضرار والتعويضات فإنها تتحد بموجب قانون العلامة التجارية وتعديلاته بمقتضى قانون ACPA حيث يعطي للمدعي إمكانية الاختيار في أي وقت كان قبل صدور الحكم النهائي في القضية من المحكمة المختصة أن يطلب التعويض عن الأضرار الحقيقية والأرباح المتوقعة، بدلا من الحكم بالتعويض عن الأضرار القانونية بنما لا يقل عن 1000 دولار أمريكي وليس أكثر من 100000 دولار أمريكي لكل اسم نطاق وذلك وفقا لاعتبارات التي تقدرها المحكمة.

وتجدر الإشارة إلى قانون الولايات المتحدة على غرار القانون الفرنسي قام بحماية كل متعامل عن طريق الوسائل الإلكترونية من تلك الرسائل الإلكترونية المشوشة على مستوى البريد الإلكتروني التي لا تتميز بأية منفعة قد يستفيد منها المرسل إليه بالعكس من ذلك، أي أنها لا تقوم ألا بتعكير صفو المرسل إليه.

فقبل دراسة الحماية الجنائية التي أولاها المشرع لبعض المراكز القانوني المعتدلة في التجارة الإلكترونية وجب علينا التطرق إلى أنه ليس هناك حد فاصل بين كل من المسؤولية التقصيرية والمساءلة الجنائية, ذلك أن الفرق بينهما راجع تكييف المشرع لطبيعة الخطأ مع المراعاة لجسامة الضرر, إلا أنه نظرا للخصوصية التي يعرفها هدا الأخير في مجال التجارة الإلكترونية فقد يرتب فعل ما خطأ ضررا يسيرا موجبا للمسؤولية التقصيرية، ونظرا للسرعة التي يعرفها كل من عالم

المعلوميات و مجال التجارة فقد يتحول هدا الضرر اليسير إلى ضرر جسيم, بالاقترا ن بتبصر القضاء بنية محدث الفعل التي قد تكون عمدية، وبالتالي فإذا ما تحقق هدين العنصرين الا و هما النية العمدية في إحداث الفعل الضار,و الإضرار بالغير ضررا جسيما عن طريق الوسائل الإلكترونية ألا وتحولت المسؤولية التقصيرية إلى مساءلة جنائية لمرتكب الفعل الإجرامي.

المطلب الثاني: الحماية الجنائية للتجارة الإلكترونية

إن من أهم وظائف النظام القانوني أن يحدد الأموال والمصالح التي يجب عليه حمايتها وذلك بوضع قواعد قانونية جنائية تجرم السلوك الذي يهدر المصالح أو يتهديدها بكل خطر محتمل، فالجناة يزدادون مهارة كلما تم تطوير برامج الحماية بخلق وسائل تدميرية، إما عن طريق القرصنة للمعلومات والبرامج، واستعمال وسائل احتيالية واختلاس البيانات وتزويرها [11]، لذلك كان من الطبيعي أن يجرم المشرع، أية أفعال يرى أنها تمثل اعتداءا على أموال وبيانات التجارة الإلكترونية عن طريق تضمين قوانين التجارة الإلكترونية نصوصا هدفها مكافحة ظاهرة الجريمة المعلوماتية في نطاق التجارة الإلكترونية. [12]

الفقرة الأولى: بعض الجرائم المقترفة من قبل مزود الخدمة المعلوماتية

[11]- ادريس النوازلي: حماية عقود التجارة الإلكترونية في القانون المغربي، المطبعة والوراقة الوطنية مراكش، الطبعة الأولى 2010، ص113.

[12]- عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، دار الفكر الجامعي، الإسكندرية الطبعة الأولى 2003، ص255.

لعل أهم الجرائم التي يقترفها مزود الخدمة هي تلك المتعلقة بإفشاء الأسرار (أولا) نظرا لموقع القوة التي يكتسبها من خلال علاقته التعاقدية وتلك المتعلقة بعدم مراعاة المواصفات من قبل مزود الخدمة (ثانيا) نظر لما لها من خصوصية في التشريع المغربي

أولا: جريمة إفشاء الأسرار:

إن لكل معلومة إلكترونية قيمة اقتصادية وتجارية تختلف حسب القيمة الاقتصادية التي يمتلكها المتعامل، هذه الأخيرة قد تفقد قيمتها عن طريق إفشاء وفضح سريتها.

يتمثل هدف المشرع المغربي في حماية المصالح والحفاظ على الحقوق فإن القانون الجنائي يهدف إلى الإصلاح والتأهيل.

حيث بالرجوع إلى القواعد العامة المتمثلة في القانون الجنائي نجد أن المادة 447 تحمل المسؤولية الجنائية لكل مدير أو مساعد أو عامل في مصنع إذا أفشى أو حاول إفشاء أسرار المصنع الذي يعمل به على سواء أكان ذلك الإفشاء إلى أجنبي أو إلى مغربي مقيم بالمغرب. أما فيما يخص قانون رقم 05-53 فإنه يعاقب بالحسب من شهر إلى ستة أشهر كل من أفشى المعلومات المعهود إليه في إطار ممارسة نشاطاته أو وظيفته على نشرها أو ساهم في ذلك، وذلك حسب المادة 30 منه.

ففي هذه الجريمة ليس هناك أي اختراق للبيانات الشخصية التي تمت معالجتها لكن هناك شخصا ذي صفة في تدوين ونقل ومعالجة البيانات قام بترسيبها وإفشائها للغير.

وقد ذكر القانون التجارة الإلكترونية التونسي ضمن هؤلاء الأشخاص مزودي خدمات المصادقة الإلكترونية وأعوانهم الذين يساعدون في أداء مهما خدمات التصديق الإلكتروني وذلك من خلال المادة 52.[13]

ويشترط في البيانات والمعلومات التي يتم إفشاؤها أن تتعلق بالشخص صاحب المعامل ة الإلكترونية.

وإفشاء هذه المعلومات أو الأسرار يعني إذاعتها أو نقلها وإطلاع الغير عليها, وإعلانها لكثير من الناس وخروجها من حيز الكتمان أو السرية بعد أن كان العلم بها قاصرا على أصحابها أو اللدين ائتمنوا عليها بحكم وظيفتهم, وهو ما حرص المشرع على منعه.

ويستوي في المعلومات التي يتم إفشائها أن تكون مكتوبة في أوراق أو مسجلة على دعامة إلكترونية على قرص مدمج أو تكون مخزنة ضمن برنامج معلوماتي في جهاز حاسب آلي.

ولكي تطبق العقوبات التي أقرها المشرع يستلزم أمن يقدم الجاني على ارتكاب الجريمة مع علمه بأنه يخالف نص قانوني وتتجه إرادته إلى الفعل المجرم و يقبل النتائج المترتبة عليه.[14]

---

[13]- تنص المادة 52 من قانون التجارة الإلكترونية التونسي على أنه "يعاقب طبقا لأحكام الفصل من المحلية الجنائية مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفضون أو يبحثون ويشاركون في إفشاء المعلومات التي عمدت إليهم في إطارها في نشاطاتهم باستثناء ثلاثي رخص صاحب الشهادة كتابيا أو إلكترونيا في نشرها أو الإعلان بما في الحالات المنصوص عليها في التشريع التجاري العمل به."

ثانيا: جريمة عدم مراعاة المواصفات من قبل مزود الخدمة

لقد وضع المشرع المغربي من خلال قانون 53.05 مجموعة من الشروط التي يجب أن يتوفر في كل شخص يسعى لاكتساب صفة مقدم خدمات المصادقة الإلكترونية أو أن يحترمها وذلك من خلال المادة 21 منه، وهذه قد أوردها المشرع على سبيل الحصر على سبيل المثال وهي شروط الزامية. ولعل أهم هذه الشروط هو كون أن مقدم خدمات المصادقة الإلكترونية لا يمكن أن يكون إلا في شكل شركة يوجد مقرها الاجتماعي بتراب المملكة, فهذا الشرط الأخير ما هو إلى شرط شكلي حيث بتخلفه عنه لا يمكن الحديث عن مقدم لخدمة المصادقة الإلكترونية ,أما عند تحققه آنذاك تقوم السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية من التحقق من باقي الشروط الموضوعية التي تنقسم بدورها إلى شروط تقنية وقانونية.

أما في حالة ما إذا اكتسب مقدم الخذمة هده الصفة و لم يحترم كل أو بعض الشروط المنصوص عليها في المادة 21 فقد أورد المشرع جزاءا يتمثل في غرامة مالية ما بين 10.000 و100.000 درهم ويعاقب عليها كذلك بالحبس من ثلاثة أشهر إلى سنة وذلك من خلال المدة29[15] من قانون 05.53 أما فيما يخص القانون التونسي فقد نصت المادة 45 من قانون

---

[14]- عبد الفتاح بيومي حجازي م ،س ص283.

[15]- تنص المادة 29 من قانون 05.53 على ما يلي: "يعاقب بغرامة من 10.000 إلى 100.000 درهم وبالحبس من 3 إلى سنة كل من قدم خدمات للمصادقة الإلكترونية المؤمنة دون أن يكون معتمدا وفق الشروط المنصوص عليها في المادة 21 أعلاه واصل نشاطه رغم اعتماد أو إصدار أو سلم أ دبر شهادات إلكترونية مؤمنة خلافا لأحكام المادة 20 أعله".

التجارة الإلكترونية على أنه "علاوة على العقوبات المبينة بالفصل-المادة 44- من هدا القانون يعاقب كل مزود خدمات المصادقة الإلكترونية الذي لم يراع مقتضيات كراس الشروط المنصوص عليه بالمادة 12 من هذا القانون بخطية تتراوح بين 1000 و10.000 دينار تونسي".

وبالرجوع لأحكام المادة 12 من قانون التجارة الإلكترونية التونسي نجد أنها لم تدرج أي شرط –على عكس قانون 05-53 من خلال المادة 21- يلتزم مقدم خدمة المصادقة الإلكترونية أن يكون في شكل شركة, بل يمكن أن يكون شخصا طبيعيا كما يمكن أن يكون شخصا معنويا.

وبالتالي فإن مخالف للشروط الواردة في المادة 12 يتعرض للجزاء المتراوحح بين 1000 و10.000 دينار بالإضافة إلى تلك المنصوص عليها في المادة 44 المتمثلة في وقف نشاط مزود الخدمة وسحب الترخيص الخاص و الممنوح له من قبل الوكالة الوطنية لمصادقة الإلكترونية.

وعلى ذلك فالركن المادي لهذه الجريمة يخلص في عدم مراعاة مزود خدمة المصادقة الإلكترونية للشروط والمقتضيات المنصوص عليها، ومؤذي ذلك أن السلوك الإجرامي لمزود الخدمة في هده الجريمة, يتوافر بمجرد عدم القيام بعمل من الأعمال المفروض عليه القيام بها [16]، أي أن الخطأ المنبني على أساسه الجرم هو خطأ سلبي أي هو ما كان على مزود الخدمة القيام به و لم يفعل.

وبالتالي فإذا توافر السلوك الإجرامي لمزود الخدمة قامت الجريمة في ركنها المادي، و لم يبين المشرع ما إذا كان تطبيق الجزاء يستلزم القصد الجنائي في مرتكبيها .

[16]- عبد الفتاح بيومي حجازي، م س، ص257.

فبقي أن نشير إلى أن المشرع لم يضاعف العفوية في حالة تكرار الفعل الذي يمثل الجريمة (العودة).

الفقرة الثانية: بعض الجرائم المقترفة من قبل الأغيار

كثيرة هي الجرائم التي يرتكبها الغير وقصدنا به كل شخص غير المكلف بالمصادقة الإلكترونية للتجارة الإلكترونية, فكثيرة هي الوسائل التي يستعملها القراصنة للاستفادة من معطيات ومعلومات ليس لهم حق الاطلاع عليها بل التصريح بمعطيات خاطئة أو سلم وثائق مزورة إلى مقدم خدمات المصادقة الإلكترونية للوصول إلى هدف معين.

أولا: جريمة التصريح بمعطيات خاطئة

تنص المادة 31 من قانون 05.53 على أنه "بصرف النظر عن المقتضيات الجنائية الأكثر صراحة, يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000 إلى 500.000 درهم كل من أدلى عمدا بتصاريح كاذبة أو سلم وثائق مزورة إلى مقدم خدمات المصادقة الإلكترونية".

يتضح من خلال نص المادة أن المشرع قد وضع ثلاثة شروط لتطبيق مضمون نص هذه المادة وهي أن يقوم الشخص ب:

-الإدلاء بتصاريح كاذبة أو تسليم وثائق مزورة

-أن يكون هذا الإدلاء عمديا

-أن تقدم هده التصريحات أو الوثائق المزورة لصالح مقدم خدمات المصادقة الإلكترونية

أما فيما يخص قانون التجارة الإلكتروني التونسي فقد نصت المادة 48 على تجريم التصريح عمدا بمعطيات خاطئة.

ففيما يتوافق عليه كل من المشرع المغربي والتونسي في أنه يستوي أن تكون التصاريح أو الوثائق المسلمة يدوية أو معالجة بالحاسوب, كما أنهما يتفقان في كون أن يكون الإدلاء بالتصاريح الكادبة عمديا, و بالتالي فإنه متى تحققت واقعة الإدلاء بالمعلومات الخاطئة أو الكاذبة فقد توافر الركائز المادي, أما الركن المعنوي فهو متمثل في العمد أي توفر سوء نية مقدم تلك المعلومات.

غير أن ما يختلف في شأنه كل من المشرعين المغربي والتونسي هو أن المشرع المغربي قد حصر تقديم هذه التصاريح الكاذبة أو الوثائق المزورة إلى مقدم خدمات المصادقة الإلكترونية فقط في حين أن المشرع التونسي قد وسع من مجال إعمال المادة 48 من قانون التجارة الإلكترونية حيث نص في ذات المادة" يعاقب كل من صرح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الإلكترونية ولكافة الأطراف التي طلب منها أن تنفق بإمضائه. وبالتالي فإنه تطبق أحكام المادة 48 سواء أتم الإدلاء بالمعطيات الكاذبة لمقدم خدمة التصديق الإلكتروني أو إلى أطراف التعاقد وهما البائع والمشتري أو المستهلك والمنتج.

ثانيا: جريمة الاعتداء على البيانات المشفرة

إن تشفير البيانات يعني تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارا ت لحماية هذه البيانات من إطلاع الغير عليها ومن تعديلها أو تغييرها.[17]

إن تشفير البيانات بوضعها طريقة فنية من طرق حماية هذه البيانات قد تكون عرضة لاعتداء عليها بذات الطريقة، أي أنه يتم اختراق البيانات رغم تشفريها، وذلك عن طريق فض الشفرة أو تسربيها من قبل من له حق الاحتفاظ بها.

غير أن أهم ما يكن ملاحظته من خلال استقراء المواد المنظمة لخدمة التشفير (المواد 12-13-14-32-33-34) هو أن المشرع نظم عملية التشفير حماية لأمن الدولة لا حماية للتجارة الإلكترونية والمتعاملين بها على عكس المشرع التونسي الذي نص في المادة 48 من قانون التجارة الإلكترونية على أنه "يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية، والتي تتعلق بإمضاء غيره بالحبس لمدة تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1000 و10.00 دينار أو بإحدى هاتين العقوبتين" فكان من الطبيعي أن يعاقب المشرع التونسي على جريمة فض مفاتيح التشفير الإلكتروني, وذلك لأنه اهتم وبكل دقة وعالج تفصيلات هذه التجارة الإلكترونية سواء من حيث انعقاد العقد وحقوق الطرفين أو سرية العمليات التجارية وتنفيذها وسرية بياناتها وعملياتها, وذلك من خلال إعتماء التوقيع الإلكتروني وتشفير بيانات هذه التجارة.

[17]- عبد الفتاح بيومي حجازي، م س، ص267.

والركن المادي لهذه الجريمة يتمثل في فض مفاتيح التشفير التي تتعلق بالتوقيع الإلكتروني, ذلك أن فضها يعني كشف البرامج الخاصة بتشفير التوقيع الإلكتروني وذلك بنقل التوقيع من صورة مكتوبة إلى صورة رقمية.[18]

وهذه الجريمة من جرائم السلوك المجرد، أي يكفي أن يكون الجاني قد فض مفاتيح الشفرة المتعلقة بالتوقيع الإلكتروني، دون انتظار حصول الضرر بالمجنى عليه, دلك أن هده الجريمة من جرائم الضرر التي تتطلب حصول نتيجة معينة.

أما من ناحية الركن المعنوي، فهذه الجريمة من الجرائم العمدية التي تتطلب لقيامها القصد الجنائي.

فقبل ختم موضعنا المتواضع هذا سنتطرق لإشكالية إثبات الجرائم المرتكبة عن طريق الوسائل الإلكترونية بصفةعامة والتجارة الإلكترونية بصفة خاصة. فنظرا للوسائل التي يتم من خلالها إبرام التصرفات القانونية في مجال هذه الأخيرة التي تتسم بالتقنية ذلك أنهاتتم على دعائم إلكترونية لا ورقية فإن مسألة الإثبات تعتبر غاية في الصعوبة خاصة إذا تعلق الأمر بشخص غير متمك ن من الناحية التقنية، ذلك أن العقود المبرمة بشكل إلكتروني تبرم في برهة زمنية لا تترك للمتعاقد أية فرصة لكي يحتفظ بدليل ينفعه إذا ثار نزاع بشأن تلك المعامل ة، فحتى ولو قام المتعاقد بالاحتفا ظ بنسخة من البيانات التي قد ترسل إليه من قبل الطرف الآخر في العلاقة التعاقدية فإن ذلك قد يتعارض مع المبدئ القانوني الناص على أنه "لا بسوغ لأي شخص أن يصنع دليلا لنفسه".

---

[18]- عبد الفتاح بيومي حجازي، م س، ص267.

وبالتالي فنحن أمام مانع مادي أو تقني يجعل إمكانية إثبات المعاملات الإلكترونية عامة والجريمة التي اقترفها المتعاقد الآخر أو الغير بصفة خاصة أهرا شبه مستحيل.

فالمانع المادي هو الذي يمنع بطبيعته الحصول على مستند –سواء أركان على ورقة او على دعامة إلكترونية وقت حسب الالتزام.

المبحث الثاني :

الحماية التقنية للتجارة الالكترونية

بعد الانتهاء من التحدث حول الحماية القانونية للتجارة الالكترونية، سنتحدث في هذا المبحث حول الحماية التقنية للتجارة الالكترونية وسنأخذ على سبيل المثال لا الحصر حماية المواقع الالكترونية والبريد الالكتروني، وفي الأخير بطاقة الائتمان.

المطلب الأول : اختراق المواقع الالكترونية وسبل حمايتها

سنتحدث في هذا المطلب حول سبل اختراق المواقع وطرق حمايتها

- **الفقرة الأولى : اختراق المواقع الالكترونية**

أ- الإختـــراق

الاختراق بشكل عام هو القدرة على الوصول إلى هدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين دون رغبة منهم، مما يحدث أضرارا مادية (إتلاف البيانات والتلاعب بها) ومعنوية (التلاعب بالصور الشخصية والابتزاز عن طريقها). وهناك مجموعة من الدوافع وراء هذا الإختراق.

– دوافع عسكرية : هذا هو ما يصطلح عليه حرب الأنترنت، حيث يقوم مجموعة من الأشخاص في محاولة اختراق مجموعة من المواقع المنتمية إلى البلدان المعادية قصد التجسس حول أسرارها العسكرية ومخططاتها.

– دوافع تجارية : بينت دراسات حديثة أن المواقع الالكترونية لكبريات الشركات العالمية يجرى عليها أكثر من 50 محاولة اختراق يوميا.

– دوافع فردية : بدأت أولها بين طلاب جامعات الولايات المتحدة الأمريكية كنوع من التباهي بالنجاح في اختراق الأجهزة أو المواقع الشخصية لأصدقائهم.

ب– أساليب الاختراق

هناك أساليب قديمة يتبعها الأشخاص المبتدئون، وأساليب حديثة للاختراق يتبعها الخبراء.

1) الأساليب القديمة :

– التلاعب بالرمز السري للمدير : وهذه الطريقة تتم عن طريق إعطاء المدير نفسه لشخص ما رمزه السري بحسن نية، فيقوم هذا الشخص بالتلاعب في الموقع وقد يتم أخذ الرمز السري كذلك بجلوس مدير الموقع أثناء قيامه بالدخول إلى لوحة التحكم، فيقوم الشخص بحفظ الرمز السري، ويقوم أخيرا بالدخول والتحكم في الموقع والتعديل عليه.

- برنامج Key logger : هذا البرنامج غني عن التعريف، مهمته التقاط كل ما يلمس في لوحة المفاتيح، فأي كتابة كتبت في الحاسوب يقوم هذا البرنامج بتسجيلها في ملف نصي، وهناك من أنواع هذا البرنامج الذي يسجل حتى الصور.

ومن الناحية التطبيقية، يقوم الشخص بإرسال صورة أو ملف آخر مرفقا بخادم هذا البرنامج، فبمجرد أن يتوصل مدير الموقع بهذا الملف أو الصورة، يصبح أي رمز سري يكتبه يرسل إلى الشخص الأول، ومن هنا يستطيع أن يتلاعب بالموقع ويعدل فيه ما يريد.

2) الأساليب الحديثة :

هذه الأساليب الحديثة والتي لا تكون في متناول المبتدئين، وسنتحدث هنا عن عنصرين على سبيل المثال وهما الشيل الروسي، والبحث عن الثغرات واستثمارها.

- الشيل الروسي : أولا سنقوم بتعريف الشيل، فهذا الأخير هو عبارة عن سكريبت مكتوب بلغة php shell، ويعمل الشيل كوسيط بينك وبين النظام الذي هو Linux حيث يستقبل الأوامر منك ويرسلها إلى السيرفر المخترق وتعرض نتائج الأوامر على الشيل، فيستخدم الشيل للسيطرة على الموقع والتنقل بين ملفاته السرية وفتحها وتحريرها، ولأجل تشغيل هذا الشيل يجب رفعه على الموقع المراد اختراقه، ومن هنا نجد سؤالا يثير نفسه : أين سأجد هذا الشيل ؟ وكيف أقوم برفعه ؟

للإجابة على هذا السؤال لابد من اتباع خطوات كثيرة للحصول على الشيل ومن تم رفعه وأخيرا التحكم في الموقع.

لإيجاد الشيل يجب البحث في مواقع الهاكرز والقراصنة، فهو يكون غالبا في صيغة C99.PHP وهذا مثال عن الشيل الروسي الذي له مجموعة من الإصدارات، وهذا الإصدار هو الأحسن والأنجع فحال التوفر عليه نقوم برفعه إلى الموقع المراد اختراقه في صيغة صورة فيتحول الملف إلى C99.php.jpg أو في صيغة ملف C99.php.doc أو في صيغة مقطع موسيقي C99.php.mp3 ، وعند نهاية الرفع نقوم باستعراض الملف المرفوع ونأخذ على سبيل المثال www.site.com/C99.php.mp3 فينفتح ملف الشيل، ونكون أمام الصفحة الرئيسية للشيل المرفوع، فنقوم بتطبيق أوامر اللينوكس لأجل التحكم في الموقع وإيجاد كلمة سر المدير.

– البحث عن الثغرات واستثمارها : هذه المرحلة صعبة نوعا ما لأنها تحتاج إلى ذكاء كبير من طرف الشخص المخترق الذي يريد اختراق الموقع بحيث يقوم بعمل Scan (مسح) على الموقع لإيجاد الثغرات التي من خلالها يمكن الدخول إلى الموقع وقرصنته والإطلاع على ملفاته السرية.

(الثغرات هي أخطاء برمجية في برامج معينة مثل سير فرا ت المواقع أو أي برامج أخرى لأنها من صنع البشر، لذا يجب أن تحتوي على أخطاء أو ثغرات).

وكمثال على هذه الثغرات نجد ثغرات المتصفح، والتي يتم استغلالها عن طريق المتصفح مثل ثغرات CGI، فإذا كان الموقع هو Google.com فنكتب الثغرة هكذا في المتصفح www.google.com/cgi-bin/password.txt، هذه الثغرة تعرض أسماء المستخدمين وكلمات السر الخاصة بهم.

أما الثغرات الأخرى التي لابد الإطلاع عليها من عمل Scan (مسح) لأجل الوقوف على الثغرات، فهناك مجموعة من المواقع التي تقدم هذه الخدمات من بينها موقع

www.milworm.com

3) تدمير المواقع :

هذه الطريقة تقوم عبر إرسال مجموعة من الملفات إلى الموقع بصفة متواترة حتى يسقط الموقع، ومفاد هذه الطريقة هي أن يقوم مجموعة من الأشخاص (أكثر من خمسة) بإرسال مجموعة من الملفات إلى المواقع المراد تدميره، فيكتظ الموقع بالبيانات المرسلة، فيحدث فيه الضغط ثم بعد مدة لا يمكنه العمل، وكمثال تطبيقي لهذه العملية نقوم بفتح Démarrer ثم Exécuter ثم بعد ذلك نكتب cmd وتظهر شاشة سوداء وفيها نكتب :

Ping -T-a-L-F google.com

فإذا قام بهذه العملية مجموعة من الأشخاص، فإن الموقع سيسقط لا محالة خصوصا المواقع ذات الاستضافة المجانية وكذا المواقع ذات مساحة تبادل الملفات الصغيرة، فهذه العملية تستهدف خصوصا الTrafic وهي المساحة المخصصة لتبادل الملفات وهي مستقلة عن المساحة الحقيقية للموقع وتجدد شهريا، فهذا الضغط الذي يحدث للموقع يتسبب في نفاذ المساحة المخصصة مما يؤدي إلى تعطيل الموقع.

- **الفقرة الثانية : حماية الموقع من الاختراق**

لحماية المواقع من الاختراق، هناك مجموعة من الأساليب الوقائية، لكن في دراستنا هذه سنعتمد على مثالين أو طريقتين، وهما استعمال برامج مؤمنة، والتصرف في الملفات بعد عملية التثبيت.

أ- استعمال برامج مؤمنة :

لا يخفى على أحد وخصوصا للشخص الذي يريد إنشاء الموقع الالكتروني مجموعة من البرامج التي يمكن له أن يستعملها، فمثلا إن أراد شخص أن ينشئ مدونة Blog فإنه يقوم بالاستعانة ببرنامج Word presse، أما إذا أراد الشخص إنشاء موقع إخباري فهناك مجموعة من البرامج المتخصصة لذلك وأحسنها Xoops و Joomla، لكن بيت القصيد في هذا المحور هو اقتناء البرنامج وشراءه لأنه وكما هو معلوم فكل البرامج المجانية تكون مليئة بالثغرات وغير محمية كفاية، لأن صانعها ينشئها كنسخة تجريبية فقط في انتظار أن يقوم الشخص بشراء النسخة الأصلية والتي تكون درجة حمايتها كبيرة، لذلك يجب القيام بتحديثها دوريا واستمرارا، ففي أي وقت أصدر الموقع الرئيسي تحديثا فيجب القيام بتثبيته، لأن هذه الأخيرة تكون غالبا لسد الثغرات أو لإضافة أشياء جديدة للموقع، هذا من جهة، ومن جهة أخرى سد ثغرات برنامج الموقع، وهنا يكمن دور المبرمج الذي يقوم بتثبيت البرنامج للموقع الالكتروني عن طريق زيادة حماية الموقع بالجدار الناري وكذلك بكتابة مجموعة من الرموز التي تضاف إلى سكريبت الموقع والتي يكون من شأنها سد مجموعة من الفراغات والتي من خلالها يمكن أن يدخل المتطفل.

ب- التصرف في الملفات :

كما هو معلوم أن كل الملفات توجد في مساحة استضافة الموقع، والولوج إلى هذه المساحة تقوم عبر برامج ال ftp[19]، وهذا الأخير هو file transfère Protocol أي بروتوكول إرسال واستقبال البيانات، وهناك مجموعة من البرامج الرائدة في هذا المجال ومن أبرزها ftp expert و fillezella. فهذه البرامج تسهل عملية الدخول إلى الموقع والتعديل فيه وحذف وإضافة البيانات، لكن المشكل المطروح هنا هو مشكل التصاريح، فعندما نقوم بإضافة **ملف على الموقع** عن طريق ftp نختار التصريح المراد إعطائه فتنقسم التصاريح إلى ثلاثة أنواع من التصاريح وهي القراءة، الكتابة، التنفيذ lire, écrire, exécuter فإذا ما أعطي الملف تصريح القراءة والكتابة والتنفيذ فإن بإمكان أي شخص التعديل عليه واختراق الموقع بأكمله عن طريق هذه الثغرة، لذلك يجب إعطاء الملفات تراخيص القراءة فقط والتأكد من هذه العملية لأنها مهمة جدا في إبقاء الموقع ثابتا ومحميا في وجه الهاكرز. ومن جهة ثانية، فعندما يقوم الشخص بتثبيت البرنامج المختار على موقعه يقوم باتباع مجموعة من الخطوات الموجودة في ملف ال Install (التثبيت)، وعند الانتهاء وكوسيلة للحماية يجب حذف ملفاته كلها لأنها لو تركت، سيقوم الشخص بالدخول إليها وإعادة تثبيت الموقع من جديد وبذلك يضيع العمل ويخترق الموقع.

ولكي لا ننسى ليس فقط ملف التثبيت بل هناك ملفات أخرى يجب تغيير اسمها فقط دون حذفها لأنها تكون هدفا للهاكرز والقراصنة ومخبأ للبيانات الأساسية للموقع وتحتوي على بيانات

[19] - ضياء علي أحمد نعمان , الغش المعلوماتي الظاهرة و التطبيقات , سلسلة الدراسات القانونية في المجال المعلوماتي العدد1 المطبعة والوراقة الوطنية مراكش الطبعة الاولى 2011 صفحة 112

المدير العامة وهذه الملفات هي admincp و administrator، لذلك يجب تغيير أسماءها إلى أسماء أخرى لكي يصعب على المخترق إيجادها.

المطلب الثاني : حماية البريد الالكتروني وبطائق الائتمان

من خلال هذا المطلب سنعالج سبل اختراق البريد الالكتروني وتدميره وكذلك طرق حمايتها في فقرة أولى، أما في الفقرة الثانية فسنتحدث حول سرقة بطائق الائتمان والتصرف فيها وسبل حمايتها.

- **الفقرة الأولى : اختراق البريد الالكتروني وحمايته**

أ- اختـــراق البريد الالكتروني

هناك طرق عديدة لاختراق البريد الالكتروني بحيث يقسمها الخبراء إلى طريقتين، أولها هي الاستيلاء على كلمة المرور، والثانية هي تفجير الإميل.

1) الموقع المزور :

هناك طريقة كثيرة لأجل القيام بالاستيلاء على كلمة السر لكن يظل أحدثها وأنجعها هي طريقة الموقع المزور، ومفاد هذه الطريقة هي أن يقوم المخترق بصنع صفحة كاذبة ومشابهة للصفحة الرئيسية لموقع البريد الالكتروني، فبمجرد أن يقوم الشخص بالدخول إليها ووضع اسمه وكلمته السرية، يقوم ذلك الموقع الكاذب بإرسالها إلى المخترق والذي بدوره يدخل عن طريقها لأجل الإطلاع على الرسائل والعبث بها وإرسال رسائل من بريد المُخْتَرَق وتحقيق أغراضه الشخصية، وكمثال حي على هذا، قام مجموعة من الأشخاص بعمل صفحة مشابهة لصفحة موقع ياهو yahoo.com وفي اسم الموقع تمت إضافة رقم صفر مكان حرف o ليصبح الموقع كالآتي yah0oo.com فتم إرسال هذا الرابط لمجموعة من الأشخاص قصد الدخول إليها وبالتالي تم اختراق بريدهم الالكتروني.

2) استعمال برنامج من برامج الاختراق مثل Sub7أو Prorat

هذا البرنامج يعتمد على ذكاء المخترق في دمج خادم هذا البرنامج مع ملف آخر فيقوم بإرساله إلى الشخص المراد اختراق بريده، فبمجرد أن يدخل الشخص إلى هذا الأخير بتركيبه للإسم والرقم السري، فترسل لبريد المخترِق فيقوم هذا الأخير بإتلاف الرسائل وتغيير كلمة السر فيصبح ذلك البريد من ملكه إذا لم يستطع استرداده.

أما الطريقة الثانية فهي تفجير الإميل، وهذه الأخيرة بدورها يمكن أن تقسم إلى طريقتين، الأولى هي عن طريق إرسال آلاف الرسائل إلى البريد الالكتروني أو إرسال رسائل محملة بملفات كثيرة.

3) إغراق البريد بالرسائل

مفاد هذه الطريقة هي إرسال مجموعة من الرسائل إلى البريد من طرف مجموعة من الأشخاص، فيتم إغراق البريد مما يؤدي إلى ضغط على السيرفر الذي يؤدي بدوره إلى توقيف البريد وبالتالي تلف الرسائل والبيانات.

4) إرسال رسائل محملة بملفات ضخمة :

وتقوم هذه الطريقة عن طريق إرسال مجموعة من الرسائل وكل واحدة منها تكون محملة بملفات ضخمة الحجم مما يؤدي إلى تضخم البريد، وبالتالي تآكل المساحة المخصصة له، مما يؤدي بموقع الخدمة إلى مسح ذلك البريد لأنه يشكل ضغطا على السيرفر وبالتالي يضطر إلى إيقافه لتفادي الضغط على السيرفر.

ب- حماية البريد الالكتروني :

إن البريد الالكتروني هو أثمن ما يملكه الشخص في شبكة الانترنت لأنها طريقة يمكن أن يتواصل عبرها مع الشركات والمواقع التجارية وبالتالي يكون مخبأ لبياناته وإرسالياته، لذلك فإن القراصنة سيسعون إلى اختراقه وهذا ما سيدفع مالك البريد الالكتروني إلى القيام بمجموعة من التدابير الحمائية لأجل حماية البريد من الاختراق.

1) فحص الرسائل قبل الدخول إليها :

معظم الشركات العالمية المانحة لخدمة البريد الالكتروني تكون قد ثبتت برنامج الحماية داخل البريد الالكتروني مثل Kaspersky أو Nod32 مما يمنح الشخص حماية عن طريق فحص

الرسائل من أن تكون محملة بملفات ملوثة بفيروسات تكون من شأنها تدمير البريد أو العثور على كلمته السرية، وهذه الطريقة هي التي يلجأ إليها معظم القراصنة من إرسال فيروسات إلى الضحايا لأجل اختراق البريد الالكتروني.

2) الامتناع عن الضغط على الروابط المشبوهة :

قد تصلنا مجموعة من الرسائل إلى بريدنا الالكتروني وداخل هذه الرسالة نجد مجموعة من الأيقونات التي يطلبون منا أن نضغط عليها، وأثناء الضغط نتفاجأ بصفحة مزورة تطلب منا إعادة كتابة الإسم والرقم السري وهنا سيتم اختراق البريد لا محالة، لذلك يجب على الشخص وحماية لبريده الابتعاد عن الضغط عن الإعلانات الكاذبة ومسحها وكل ما ليس متعلقا به.

بعد أن تعرفنا على مختلف طرق اختراق البريد الالكتروني أصبح الآن بمقدورنا معرفة طرق الحماية وفهمها فيما يلي أهم الإرشادات :

- اختيار كلمة مرور قوية ومعقدة (أرقام وحروف كبيرة وصغيرة ورموز)
- تغيير كلمة المرور بانتظام
- استخدام مكافح فيروسات جيد ومحدث
- المحافظة على تحديث نظام التشغيل (Windows update)
- عدم استخدام البريد الالكتروني في حاسب مشترك
- الحذر الشديد عند التعامل مع رسائل يرسلها أشخاص غرباء أو أشخاص غير موثقين فيهم

• الفقرة الثانية : قرصنة بطائق الائتمان وطرق حمايتها

أ- قرصنة بطائق الائتمان :

هناك من الطرق الالكترونية اللامحدودة لأجل قرصنة البطائق الالكترونية، لكن في عملنا هذا سنقتصر على محاكات المواقع أولا، ثم اختراق الموقع الأصلي الذي تم الشراء منه ثانيا و إساءة استخدام البطاقة البنكية ثالثا .

1) محاكات المواقع :

هذه التقنية تقوم عبر إنشاء موقع مزيف شبيه بالموقع الأصلي ويقوم الشخص بتخفيض أثمنة البضائع لأجل إغراء الناس، فبمجرد أن يتقدم المشتري لأجل شراء تلك البضائع، فيقوم بإدخال معلومات بطاقته الالكترونية، في تلك اللحظة لا يجد مرحلة تنفيذ العقد، بل فقط صفحة بيضاء أو صفحة أخرى.

ومفاد هذه العملية أن تلك المعلومات قد تم إرسالها إلى القرصان، فيقوم بدوره بالتصرف فيها وشراء حاجاته الشخصية ببطاقة غيره، وهذه العملية تعتبر من أخطر العمليات الموجودة في شبكة الأنترنت وأوسعها، ففي سنة 2009 قام مجموعة من الأشخاص بعمل صفحة على الأنترنت شبيهة بموقع Ebay برابط مزور هو Ebbay.com فقاموا بتعديل أثمنة البضائع وجعلها بخسة مما شجع آلاف المشترين على القيام بعملية الشراء مما خلف خسائر تقدر ب 40 مليون دولار

أمريكي نتيجة قيام القراصنة بإعادة التصرف في البيانات المدخلة للموقع المزيف، وبالتالي إنجاز عمليات شراء واسعة وكذلك تحويل المبالغ إلى موطنهم مما قادهم للثراء السريع.

2) اختراق الموقع الأصلي الذي تم الشراء منه :

إذا كنا في الطرق السابقة قد رأينا أن الشخص مالك البطاقة هو من يقوم بتسهيل عملية الاختراق عن طريق عدم تبصره وفطنته ؛ ففي هذه الحالة فإننا أمام عملية خارج يد مالك البطاقة ومفادها أن يقوم مجموعة من الأشخاص بعملية الشراء من موقع معروف، وبعد مدة يتم اختراق هذا الموقع من طرف القراصنة مما ينتج عنه استيلاء العديد من قواعد بيانات الموقع، ومن بين البيانات معلومات البطائق البنكية التي تكون مخزنة في قاعدة البيانات، مما يؤدي إلى التصرف في المبالغ المالية والتلاعب فيها وبالتالي خسارة مجموعة من الناس التي قامت بالشراء العادي من الموقع المخترق.

(3)إساءة استخدام البطاقة الالكترونية من طرف حاملها

من المشاكل التي تواجه حامل البطاقة الالكترونية سرقتها أو فقدانها، ويزيد من صعوبة المشكلة، ما لوحظ في العمل من أن العملاء يخشون نسيان الرقم السري (PIN)، فيكتبونه على

البطاقة أو في المفكرة الشخصية ومن ثم عندما تسرق البطاقة أو المفكرة يسهل على السارق معرفة الرقم السري.

وللتقليل من مخاطر ضياع البطاقة أو سرقتها، فإنه ينص في عقد انضمام الحامل للبطاقة الالكترونية على التزامه بالمحافظة عليها وإخبار البنك أو الجهة المصدر للبطاقة بفقدها أو سرقتها وذلك لتجنب استعمال الغير لها.

وقد تشترط بعض الجهات المصدرة للبطاقة أن يتم الإعلان بشكل كتابي عن الضياع أو السرقة وإثبات ذلك بمحضر رسمي وإلا عد الحامل مُخلاً بالتزامه.

وعندما لا تحدد الجهة المصدرة للبطاقة طريقة معينة للإخبار، يكون الحامل الحق في اختيار الأسلوب المناسب للإخبار حتى وإن كان عن طريق الهاتف ولكن يجب إثبات الإخبار عندئذ،لأن المسؤولية بعد الاخطار تنتقل من عاتق الحامل إلى عاتق الجهة مصدرة البطاقة[20].

ب- حماية البطائق الالكترونية من القرصنة :

قبل أن تقوم بوضع رقم الحساب أو البطاقة الالكترونية الخاصة بك في أي موقع، تريد الشراء منه أو أثناء تسجيلك الدخول لحساب Paypal الخاص بك، وهذا الأخير هو موقع تجاري يسمح للمستخدم بتحويل المال عبر الأنترنت والبريد الالكتروني لعناوين مختلفة، كما يمكن

[20] - ضياء علي أحمد نعمان , الغش المعلوماتي الظاهرة و التطبيقات , سلسلة الدراسات القانونية في المجال المعلوماتي العدد1 المطبعة والوراقة الوطنية مراكش الطبعة الاولى 2011 صفحة 251

للمستخدم إرسال المال المرسل إليه إلى الآخرين أو تحويله لحساب المصرف، وتعد هذه الخدمة بديلة عن الطرق الورقية التقليدية كالشيكات والحوالات المالية.

فلذلك يجب التأكد أن هذه الصفحة حقيقية، وليست مزورة ومخصصة لسرقة البطاقات الالكترونية وأرقام الحسابات البنكية، ويمكن التأكد من ذلك من خلال شريط العنوان الخاص بالموقع حيث يجب أن يكون حرف S موجود بعد Http ليصبح بالشكل التالي : https، وحرف S اختصار لكلمة Secure بالانجليزية وتعني " آمـــن"، ونفس الشيء ينطبق لحماية البريد الالكتروني عن طريق حرف S قبل إرسال الإسم والرمز السري للموقع.

خاتمة

وختاما ففي ظل الوضع الراهن للتجارة الالكترونية في البلدان العربية عموما وفي بلادنا المغرب خصوصا المتمثل في قلة عدد الاشخاص الذين يستعملون هذه الوسيلة لابرام مختلف معاملاتهم التجارية وذلك راجع للأسباب التي سبق ذكرها من قبل أستاذنا الفاضل "ضياء علي أحمد نعمان " في الحصة الأولى المتمثلة في ضعف البنية التحتية و تفشي الأمية في المجتمع المغربي . ولعل ابرز هذه الأسباب عدم احساس المستهلك بصفة عامة و المتعاقد الكترونيا بصفة خاصة بحماية تكفل جميع حقوقه و أمواله سواء عن طريق القرصنة او عن طريق الاختراق .

لذلك نلتمس من المشرع ان يصب عامل اهتمامه ليولي حماية قانونية تكفل حماية المتدخلين في التجارة الالكترونية

لائحة المراجع

المراجع العامة

محمد الكشبور , نضام التعاقد ونضريتا القوة القاهرة والضروف الطارئة , مطبعة النجاح الجديدة الدار البيضاء , الطبعة الاولى ,1993

المراجع الخاصة

ادريس النوازلي , حماية عقود التجارة الالكترونية في القانون المغربي , المطبعة الوراقة الوطنية , مراكش, الطبعة الاولى 2010,

العربي جنان , التعاقد الالكتروني في القانون المغربي دراسة مقارنة المطبعة الوراقة الوطنية ,مراكش2008

كميت طالب البغدادي , الاستخدام غير المشروع لبطاقة الائتمان المسؤولية الجزائية والمدنية , دار الثقافة للنشر والتوزيع, الطبعة الاولى 2008,

محمد اسماعيل احمد اسماعيل , اساليب الحماية القانونية لمعاملات التجارة الالكترونية , منشورات الحلبي الحقوقية ,بيروت , الطبعة الاولى , سنة 2009

محمد حسين المنصور ,المسؤولية الالكترونية , دار الجامعة الجديدة للنشر , الاسكندرية ,الطبعة الاولى . 2003

عبد الفتاح بيومي حجازي , مقدمة في التجارة الالكترونية العربية , دار الفكر الجامعي , الاسكندرية , الطبعة الاولى , 2003,

ضياء علي أحمد نعمان , الغش المعلوماتي الضاهرة و التطبيق , سلسلة الدراسات القانونية في المجال المعلوماتي العدد 1 المطبعة والوراقة الوطنية مراكش الطبعة الاولى 2011

المراجع الالكترونية

موقع البوابة التونسية – تم الولوج في 2001/06/01 على الساعة 16:00

http://www.tunisia-sat.com/vb/showthread.php?t=715157