الجرائم الواقعة على التجارة الإلكترونية

الدكتور/ حسين بن سعيد الغافري
مستشار قانوني وعضو مجلس إدارة الاتحاد العربي للتحكيم الإلكتروني
hssnrg@yahoo.com

الفهرس

رقم الصفحة

تمهيد وتقسيم

لا يقصد بالتجارة الإلكترونية تلك التجارة التي يكون محلها أجهزة أو مستلزمات إلكترونية، وإنما يقصد بها التجارة التي تتم بين المتعاملين فيها من خلال أجهزة ووسائل إلكترونية كشبكة الإنترنت مثلا. وكثيرة هي التعريفات التي قيلت في التجارة الإلكترونية سواء من قبل المشرع أو الفقه، فنجد مثلا أن المشرع التونسي ومن خلال قانون المبادلات والتجارة الإلكترونية وتحديدا في المادة الثانية منه قد عرّفها بأنها" العمليات التجارية التي تتم عبر المبادلات الإلكترونية " (١). وفي إمارة دبي بدولة الإمارات العربية المتحدة نجد أن المشرّع الإماراتي قد عرّفها بأنها " المعاملات التجارية التي تتم بواسطة المراسلات الإلكترونية" (٢). وفي فرنسا نجد أن اللجنة المشكلة برئاسة وزير الاقتصاد الفرنسي لتعريف التجارة الإلكترونية قد انتهت إلى تعريفها بأنه "مجموعة من المعاملات الرقمية المرتبطة بأنشطة تجارية بين المشروعات ببعضها البعض وبين المشروعات والأفراد وبين المشروعات والإدارة " (٣).

ومن التعريفات التي قال بها الفقه المصري لهذا النوع من التجارة إنها " تنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري وأخر أو بين مشروع تجاري ومستهلك وذلك باستخدام تكنولوجيا المعلومات والاتصالات (٤).

مما سبق يتبين لنا أن لهذه التجارة أنماطا ثلاثة: الأول: تجارة إلكترونية من الشركات إلى الزبائن. الثاني: تجارة إلكترونية من الشركات إلى الشركات. الثالث: تجارة إلكترونية من الشركات إلى الإدارة.

مزاياها: تتميز التجارة الإلكترونية بالعديد من المزايا التي تجعل الإقبال عليها يتزايد وينمو يوما بعد يوم منها على سبيل المثال (٥):

- توفر تسويق أكثر فعالية وتحقيق أرباح أكثر
- تساعد على تخفيض مصاريف الشركات
- تؤدي إلي تواصل فعّال مع الشركاء والعملاء
- توفر الوقت والجهد
- القدرة على تحليل الأسواق والاستجابة لتغير متطلبات المستهلكين
- تساعد على سرعة نشر المعلومات التجارية وتوزيعها
- تساعد على تقديم الخدمات للعملاء على مدار ٢٤ ساعة
- خلق العديد من فرص العمل الحر

أقسامها: تنقسم التجارة الإلكترونية إلى قسمين اثنين هما (٦):

- التسوق الإلكتروني: ويتمثل في تزود العميل أو المستهلك بالمعلومات والبيانات التي يحتاجها لكي يعقد أو يبرم صفقة ما بشكل سليم
- الشراء الإلكتروني: ويتمثل في البنية التكنولوجية اللازمة لتبادل البيانات وإتمام عمليات شراء وبيع السلع والخدمات عبر الإنترنت.

– خصائصها: تتسم التجارة الإلكترونية عبر الإنترنت بخصائص عديدة منها على سبيل المثال أنها تعتمد على الوثـائق الإلكترونية وأنها ترتبط بالأنشطة التجارية ذات المفهوم الواسع الذي لا يقصرها على المعاملات التجارية فحـسب بـل تشمل جميع الأنشطة الاقتصادية كالاستثمارات وعمليات البنوك بالإضافة إلي أنها ذات طبيعة دولية دائما نظرا لعالميـة شبكة الإنترنت (٧). كذلك هي تتميز بالنمو حيث تشير بعض التقديرات الصادرة عـن منظمـة التعـاون الاقتـصادي والتنمية (اوسيد) إلي أن قيمة مبادلات التجارة الإلكترونية في العالم قد تجاوزت ٣٠٠ مليار دولار عام ٢٠٠٠ م و هو يعادل ١٠ أضعاف مقارنة بعام ١٩٩٨ م وقفزت هذه القيمة لتصل عام ٢٠٠٣ إلي ١٣٠٠ مليار دولار، أما في الشرق الأقصى فقد بلغت قيمة المبادلات ٤٠٠ مليون دولار عام ٢٠٠٠ م لتقفز إلي ٣ مليار دولار عام ٢٠٠٣ (٨). ولما كان ذلك كذلك غدت هذه التجارة مرتعا للكثير من الاعتداءات والانتهاكات " مبحث أول "، وبات توفير الحماية الجنائية لهـا أمرا يفرضه الواقع والمستقبل على حد سواء " مبحث ثانيا".

المبحث الأول: ماهية الجرائم الواقعة على التجارة الإلكترونية

تمهيد وتقسيم

بوجه عام تمثل الجريمة اعتداء على مصلحة يرى المشرع أنها جديرة بالحماية التشريعية و بالتالي ينص على حمايتها نظرا لأهميتها ويجرم الاعتداء عليها. والجرائم الواقعة على التجارة الإلكترونية إما أنها جرائم تقع على المضمون كالاعتداء على التوقيع الإلكتروني " فرع أول"، أو أنها تقع على الوسائل الإلكترونية المستخدمة في التجارة الإلكترونية كالاعتداء على حقول الإنترنت وأسماء الدومين " فرع ثاني"، أو السطو على أرقام البيانات الائتمانية " فرع ثالث".

المطلب الأول: الاعتداء على التوقيع الإلكتروني

تمهيد وتقسيم

التوقيع بوجه عام ما هو إلا وسيلة يعبر بها شخص ما عن إرادته في الالتزام بتصرف قانوني معين. ويستعمل مصطلح التوقيع بمعنيين: الأول ينصرف إلى فعل أو عملية التوقيع ذاتها أي واقعة وضع التوقيع على مستند يحتوى على معلومات معينة، والثاني ينصرف إلى العلامة أو الإشارة التي تسمح بتميز شخص الموقع (٩). والقاعدة العامة في التوقيع أنه يجب أن يكون مكتوبا بخط يد الموقع وهذا ما ذهبت إليه محكمة النقض المصرية (١٠). أما في القانون الفرنسي فنجد أن التوقيع يتخذ شكلا واحدا وهو إمضاء الشخص، ويجب أن يكون مكتوبا ولا يجوز أن يأتي في صورة أخرى (١١). والتوقيع أيا كانت وسيلته، يجب حتى يعتد به أن يكون مقروءا إذا كان بالإمضاء ومرئيا، وهو لن يكون كذلك إلا إذا وضع على مستند مادي أيا كانت طبيعته ويترك أثرا واضحا، وأن يكون دائما أي أنه لا يزول مع الزمن (١٢).

وبالتالي فإن للتوقع دورا هاما من ثلاثة جوانب فهو من جهة يحدد شخصية الموقع ومن جهة أخرى يعبر عن إرادته في التزامه بمضمون الوثيقة، وإقراره لها، ومن جهة ثالثة يعد دليل على حضور أطراف التصرف وقت التوقيع أو حضور من يمثلهم قانونا أو اتفاقا (١٣). إلا أنه ومع التقدم التكنولوجي المعاصر في وسائل الاتصال ونقل المعلومات وازدياد التعامل في التجارة الإلكترونية، ظهرت طرق ووسائل حديثة في التعامل لا تتفق تماما مع فكرة التوقيع بالمفهوم التقليدي، فمعظم المعاملات المالية والتجارة أصبحت تتم إلكترونيا، وبالتالي لم تعد الوسيلة التقليدية في إثبات التصرفات القانونية " التوقيع التقليدي" ملائمة للتعاقدات الحديثة التي تتم في الشكل الإلكتروني.

من هنا كان ظهور التوقيع الإلكتروني ليكون بديلا عن التوقيع التقليدي ليتوافق وطبيعة التعاقدات القانونية والعقود التي تتم باستخدام الوسائل والأجهزة الإلكترونية الحديثة. وتعويلا على ما سبق فإننا سوف نتعرف على ماهية هذا النوع المستحدث من التوقيعات وتنظيمه القانوني" فرع أول" وأهم الاعتداءات التي تقع عليه" فرع ثاني".

الفرع الأول: ماهية التوقيع الإلكتروني

ما هو التوقيع الإلكتروني؟ وما هي خصائصه ؟ وما الأهداف المرجوة منه؟ وكيف يتم الحصول عيه؟ كلها أسئلة تدور في ذهن القارئ سوف نحاول الإجابة عنها تبعا.

أولا. تعريف التوقيع الإلكتروني

عرفت المادة ٤/١٣١٦ من التقنيين المدني الفرنسي المعدلة والمضافة بقانون التوقيع الإلكتروني الفرنسي ٢٣/ ٢٠٠٠ م الصادر في ٢٠٠٠/٣/١٣ م التوقيع بصفة عامة بأنه التوقيع الضروري لإتمام التصرف القانوني الذي يميز هوية من وقعه، ويعبر عن رضائه بالالتزامات التي تنشأ عن هذا التصرف وعندما يكون إلكترونيا، فيجب أن يتم باستخدام وسيلة آمنه لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه (١٤).

وقد عرّف القانون الاتحادي الأمريكي التوقيع الإلكتروني بأنه "صوت أو رمز أو معالجة إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو إقرارها من شخص تتوافر لديه نية التوقيع على السجل (١٥)، (١٦). وقد كان قانون التوقيع والسجلات الإلكترونية لولاية نيويورك الصادر سنة ١٩٩٩ ينص على أن "التوقيع الإلكتروني يعني مطابقة إلكترونية تنطوي دون قيد على توقيع رقمي يخص الشخص الذي يستخدمه وحده، وتكون قادرة على التحقيق من هويته وذلك بموجب ضابط وحيد لمن يستخدمه، يرفق أو يتحد في البيانات كوسيلة للتحقق من إسناد التوقيع إلى البيانات الخاصة وسلامة البيانات المرسلة والمعدة من الشخص المستخدم لها كي تكون لها ذات القوة والأثر المقرر لاستخدام التوقيع الموضوع بخط اليد (المادة ١٠٢ (٣) من قانون ولاية نيويورك لسنة ١٩٩٩) (١٧). غير أن الشارع في ولاية نيويورك رأي أن هذا التعريف للتوقيع الإلكتروني لا يفي بمتطلبات التعامل الإلكتروني، فأصدر تشريعا في ٦ أغسطس سنة ٢٠٠٢ عدل بموجبه القانون السابق ووضع تعريفا جديدا للتوقيع الإلكتروني يكفل المرونة للمتعاملين. وبموجب هذا التعديل الجديد فإن "التوقيع الإلكتروني هو صوت أو رمز أو معالجة إلكترونية ملحقة بسجل إلكتروني أو متحدة منطقيا به ويجريها أو يقرها شخص تتوافر لديه نية التوقيع في هذا السجل" (١٨). ويتماثل هذا التعريف مع القانون الاتحادي الأمريكي، كما أنه يكاد يتماثل مع التعريف الذي أورده الشارع الإنجليزي للتوقيع الإلكتروني إذ نص الفصل الأول من لائحة التوقيع الإلكتروني الصادرة في ٨ مارس ٢٠٠٢ على أن التوقيع الإلكتروني يعني بيانات في شكل الكتروني ملحقة أو متحدة منطقيا بغيرها من البيانات الإلكترونية والتي تصلح كوسيلة للتوثيق" (١٩). كما أنه يكاد يتطابق مع التعريف الذي نص عليه الشارع الألماني في المادة الثانية من قانون التوقيع الإلكتروني (٢٠).

ويلاحظ أن اتجاهات التشريعات المقارنة تتجه إلى التوسع في الوسائل التي تصلح لإجراء التوقيع الإلكتروني، وعلة ذلك هي توفير مرونة أكبر للمتعاملين في اختيار الوسيلة التي يرونها تكفل الأمن والثقة في هذا التوقيع (٢١). غير إنه إذا كانت للمتعاملين حرية اختيار الوسيلة الفنية للتوقيع الإلكتروني؛ فإن الجهات العامة قد يفرض عليها القانون استخدام وسيلة معينة دون غيرها في التصرفات التي تدخل فيها مع الغير أو فيما بينها، وعلة ذلك أن هذه الوسيلة قد يتوافر فيها قدر من الحماية للمصلحة العامة أكثر من غيرها. والسلطة التي بيدها تحديد وسيلة التوقيع الإلكتروني في هذه الحالة هي السلطة الإدارية التي عيّنها الشارع لإدارة وحفظ التوقيعات والسجلات الإلكترونية (٢٢).

وقد ميز الشارع الألماني بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم: ويشترك كل منهما في أنه ينطوي على بيان في صورة إلكترونية ملحق ببيان آخر أو مرتبط به منطقيا ويستخدم هذا البيان لتوثيق نسبته لشخص معين. غير أن التوقيع المتقدم في نظر الشارع الألماني ينطوي على ضوابط أشد صرامة من العادي، فهو توقيع يتضمن شفرة مقصورة استخدامها على شخص معين لا يشاركه غيره فيه ويكون قادرا على تحديد هوية مستخدمة وأنه يمكنه أن يحتفظ بشفرة هذا التوقيع تحت إشرافه وحده، وأن يكون بالإمكان اكتشاف أي تغيير في بيانات هذا التوقيع تطرأ لاحقا (٢٣). هذا ولو نظرنا إلى التشريع المصري نجد أن قانون ٢٠٠٤/١٥ م بشأن التوقيع الإلكتروني الصادر في ٢٠٠٤/٤/٢٢ م عرّف التوقيع الإلكتروني بأنه " ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره" (٢٤).

وفي الفقه القانوني نجد أن بعض الفقهاء الفرنسيين يعرّفه بأنه " مجموعة من الإجراءات التقنية التي تسمح بتحديد من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته" (٢٥).

أما في الفقه القانوني المصري: نجد أن بعض الفقهاء المصريين عرّفه بأنه" كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطا ارتباطا وثيقا بالتصرف القانوني، ويسمح بتمييز شخص صاحبها وتحديد هويته، ويتم دون غموض عن رضائه بهذا التصرف القانوني" (٢٦).

ثانيا. عناصر وخصائص التوقيع الإلكتروني (٢٧)

يتميز التوقيع الإلكتروني ببعض العناصر والخصائص على النحو التالي:

- يتكون من عناصر متفردة وسمات ذاتية خاصة بالموقع تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو نبرات صوت أو غيرها.
- يحدد شخص الموّقع ويبين هويته ويميزه عن غيره من الأشخاص.
- يعبر عن رضاء الموّقع والتزامه بالتصرف القانوني الذي يتضمنه المحرر الإلكتروني.
- يوضع على محرر إلكتروني ويتصل به عبر وسيلة إلكترونية.
- يحقق قدرا من الأمان والسرية والثقة في انتسابه للموّقع (صاحب التوقيع)، كونه يستند على منظومة بيانات مؤمنة.

ثالثا. أهداف التوقيع الإلكتروني (٢٨)

يحقق التوقيع الإلكتروني العديد من الأهداف منها:

- تحديد هوية الموّقع: متى ما تم تزاوج مفاتيح التشفير بأن كان أحدهم عام والآخر خاص وارتبط كليهما بموقع معين ومحدد فإن التوقيع الإلكتروني ينسب الرسالة إلى الموقع فهذا التوقيع يتعذر تزويره ، ما لم يفقد الموقع السيطرة على المفتاح الخاص ، بأن يتم إفشاءه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.
- توثيق الرسالة: التوقيع الإلكتروني يهدف إلى تحديد مصدر ومضمون الرسالة الموقعة بصورة أفضل من التوقيع التقليدي على المحررات الورقية. حيث تمكّن المرسل إليه من التأكد من صحة الرسالة والكشف عن أي تغيير يتم بشأنها.

– التروي قبل التوقيع: مع أن توقيع المنشئ على المحرر الإلكتروني يتم بسرعة إلا أن اللغة الحوارية التي يجريها جهاز الحاسب الآلي مع البيانات المطلوب تسجيلها والتأكيد على صحتها تتيح له فرصة التروي والتفكير قبل الإقدام على بث هذه الرسالة عبر شبكة الإنترنت وما يترتب عليها من آثار.

– السهولة والدقة: استخدام التوقيع الإلكتروني يسهل المعاملة التي تتم في الوسط الإلكتروني ويجعل التثبت من صحته بدرجة عالية من الضمان تفوق التوقيع التقليدي الذي يتطلب نماذج توقيع محفوظة لدي جهة التعامل وقد لا يستطيع الموّقع المحافظة على دقة توقيعه مما يعرض إجراء معاملته في يسر وسهولة للخطر.

رابعا. أشكال التوقيع الإلكتروني

يتخذ التوقيع الإلكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشائه، سيما وأن القوانين التي نظمته لم تنص على شكل محدد له، وإنما تركت تحديد شكله والطريقة التي يتم بها للتكنولوجيا، وما قد ينشأ عنها، وأن كانت قد حددت الضوابط العامة التي يجب أن يكون عليها هذا التوقيع. وتتمثل أهم صور التوقيع الإلكتروني في التوقيع الكودي أو السري المرتبط بالبطاقة الذكية الممغنطة، والتوقيع البيومتري، والتوقيع باستخدام القلم الإلكتروني وأخيرا التوقيع الرقمي.

١. التوقيع الكودي أو السري المرتبط بالبطاقة الذكية الممغنطة: يقصد به استخدام مجموعة من الأرقام أو الحروف أو كليهما ، يختارها صاحب التوقيع لتحديد هويته وشخصيته ، ويتم تركيبها أو ترتيبها في شكل كودي معين بحيث لا يعلمها إلا صاحب التوقيع فقط ومن يبلغه بها (٢٩).

وتسمي هذه الطريقة Personal Identification Number (P.I.N) وهي غالبا ما ترتبط بالبطاقات الذكية، البلاستيكية الممغنطة، وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة إلكترونية كبطاقة الفيزا والماستر كارد وأمريكان اكسبريس.

٢. التوقيع باستخدام القلم الإلكتروني " Pen – Op ": يعد هذا النوع من التوقيعات الإلكترونية الأكثر شيوعا، ويتم فيه نقل التوقيع المحرر بخط اليد على المحرر إلى الملف المراد نقل هذا المحرر إليه باستخدام جهاز الماسح الضوئي، وإيصال هذا التوقيع مع المحرر إلى الشخص الآخر باستخدام شبكة الإنترنت.

وتم تطوير هذا النوع من التوقيع باستخدام قلم إلكتروني حسابي يمكنه الكتابة على شاشة الحاسب الآلي، وذلك عن طريق استخدام برنامج خاص بذلك، يقوم بالتقاط التوقيع والتحقق من صحته، وقبوله إذا كان صحيحا، أو رفضه إذا كان غير ذلك. وهذه الطريقة وإن كان كانت تمتاز بالمرونة والسهولة في الاستعمال، إلا أنها قد تؤدي في بعض الأحيان إلى زعزعة الثقة، لأنه باستطاعة الشخص المستقبل الاحتفاظ بهذا التوقيع ووضعه على مستندات أخرى، وبذات الطريقة التي وضع بها هذا التوقيع على المحرر المرسل، كما أنه لا يمكن التأكد من أن الشخص صاحب التوقيع هو من قام بالتوقيع على المحرر لأنه باستطاعة أي شخص أن يضع هذا التوقيع، إذا حصل عليه بأية طريقة، على ما يشاء من المستندات وإرسالها إلى أي جهة (٣٠).

٣. التوقيع باستخدام الخواص الذاتية " البيومترى" (٣١): يعتمد هذا النوع من التوقيع على طرق التحقق من الشخصية التي تعتمد على الخواص الفيزيائية والطبيعية والسلوكية للأفراد، ومن هذه الطرق:

- البصمة الشخصية Finger Printing
- مسح العين البشرية Iris and Rentina Scanning
- التعرف على الوجه البشري Facial Recognition
- خواص اليد البشرية Hand Geometry
- التوقيع الشخصي Voice Recognition
- التحقق من نبرة الصوت Hand written Signatures

ويتم التحقق من الشخصية إما بأخذ صورة دقيقة جدا للعين البشرية، أو بصمة الأصابع، أو ملامح الوجه البشري، أو الخواص الموجودة باليد البشرية، أو عن طريق نبرة الصوت، أو التوقيع الشخصي، ففي كل حالة يتم تخزين البيانات الخاصة في الحاسب الآلي واسترجاعها متى دعت الحاجة إليها للتأكد من شخصية صاحبها، والسماح له بإتمام العملية المطلوبة، أو الدخول إلى نظام الحاسب الآلي (٣٢).

٤. التوقيع الرقمي: يعد من أشهر أنواع التواقيع الإلكترونية، ويقصد به بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة، والذي يسمح للمرسل إليه إثبات مصدرها، والاستيثاق من سلامة مضمونها، وتأمينها ضد أي تعديل أو تحريف (٣٣). ومن أكثر التوقيعات الرقمية شيوعا وأكثرها انتشارا ذلك النوع القائم على ترميز المفاتيح، ما بين مفتاح عام (٣٤) وآخر خاص (٣٥)، وهذه المفاتيح تعتمد في الأساس على تحويل المحرر المكتوب من نمط الكتابة الرياضية إلى معادلة رياضية، وتحويل التوقيع إلى أرقام، فإضافة التوقيع إلى المحرر عن طريق الأرقام يستطيع الشخص قراءة المحرر والتصرف فيه، ولا يستطيع الغير التصرف فيه إلا عن طريق هذه الأرقام (٣٦). من شأن هذه الطريقة للتوقيع الإلكتروني أن تحقق الثقة والأمان للمحرر، وتضمن تحديد هوية الأطراف بدقة، والعيب الوحيد في هذه الطريقة يتمثل فقط في حالة سرقة هذه الأرقام أو معرفتها من قبل الغير، والتصرف فيها بطريقة غير مشروعة، وخاصة مع ازدياد عمليات الاحتيال والقرصنة وما يواكبها من تطور في المجال التكنولوجي، ومحاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها، وإعادة استخدامها بعد ذلك (٣٧).

ويحتاج التوقيع الإلكتروني الرقمي باستخدام تقنية شفرة المفتاحين العام والخاص إلى سلطة إشهار أو جهة تصديق إلكتروني مرخص لها أو معتمدة، تقوم بالتحقق من هوية الأشخاص المستخدمين لهذا التوقيع الرقمي والتأكد من نسبة المفتاح العام المستخدم إلى صاحبه وإصدار شهادة تصديق إلكتروني (٣٨) تفيد صحة توقيع العملاء بموجبها، وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.

خامسا. كيفية الحصول على التوقيع الإلكتروني

يتم الحصول على هذا التوقيع عن طريق التقدم إلى إحدى الهيئات المتخصصة في إصدار هذه الشهادات ومن أشهرها VeriSign and Digital Signature Trust وذلك مقابل مبلغ معين من المال سنويا و تتم مراجعة الأوراق والمستندات ومطابقة الهوية بواسطة جواز السفر أو رخصة القيادة وتصعب الإجراءات أو تسهل تبعا للغرض من استخدامها حيث يتطلب منك الحضور شخصيا في بعض الحالات وفي بعض الحالات يكفي إرسال الأوراق بالفاكس أو البريد (٣٩).

سادسا. كيفية عمل هذه التكنولوجيا (٤٠):

١. يتم التقدم إلى الهيئة المتخصصة بإصدار الشهادات.

٢. يتم إصدار الشهادة و معها المفتاح العام و الخاص للمستخدم الجديد.

٣. عندما ترسل الرسالة الإلكترونية يقوم الشخص بتشفير الرسالة باستخدام المفتاح العام التابع للمستقبل أو المفتاح الخاص به و في كلتا الحالتين يتم إرفاق توقيع الشخص المرسل الإلكتروني داخل الرسالة.

٤. يقوم البرنامج الخاص بالمستقبل بإرسال نسخة من التوقيع الإلكتروني إلى الهيئة التي أصدرت الشهادة للتأكد من صحة التوقيع.

٥. تقوم أجهزة الكمبيوتر المتخصصة في الهيئة بمراجعة قاعدة البيانات الخاص بها و يتم التعرف على صحة التوقيع و تعاد النتيجة و المعلومات الخاصة بالشهادة إلى الأجهزة الخاصة بالهيئة مرة أخرى.

٦. يتم إرسال المعلومات و النتيجة إلى المستقبل مرة أخرى ليتأكد من صحة و سلامة الرسالة.

٧.يقوم المستقبل بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على أساس رقمه العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، و من ثم يجيب على المرسل باستخدام نفس الطريقة و هكذا تتكرر العملية.

سابعا. الضوابط الفنية للتوقيع

ذكرنا أن التشريعات التي نصت على الأخذ بالتوقيع والسجلات الإلكترونية قد جعلت لها قوة في الإثبات مساوية للمستندات الورقية للتوقيعات بخط اليد، غير أنه لا محل لهذه القوة إلا إذا توافرت ضوابط تكفل ضمان صحة وسلامة هذه المستندات. ولتحقيق هذا الهدف صدرت لوائح إدارية تتضمن الضوابط والإجراءات الواجب اتخاذها بشأن استخدام وتوثيق التوقيع الإلكتروني والانتفاع من السجلات الإلكترونية. ويتوقف نجاح هذه اللوائح على التوفيق بين اعتبارين أساسيين: الأول هو أن يتيح التنظيم التشريعي للتوقيع والسجلات الإلكترونية الحرية والمرونة للأفراد في إجراء تعاقداتهم ومعاملاتهم بأي وسيلة من وسائل التحقق الإلكتروني يرونها ملائمة لهم. ولتحقيق هذا الاعتبار فإن القانون لا يجوز أن يسلبهم حقا أو ميزة مقررة لهم بمقتضى القانون أو التعاقد في حال استخدامهم للتوقيع والسجلات الإلكترونية (٤١). والاعتبار الثاني هو أن التنظيم التشريعي يجب أن يكفل توفير الوسائل المناسبة لصحة وسلامة استخدام المستندات الإلكترونية.

– الضوابط الفنية العامة: هناك عدة ضوابط فنية عامة يجب أن تتوافر في التوقيع الإلكتروني: فيجب أن يكون التوقيع خاصا بالشخص وحده ولا يشاركه فيه غيره، كما يجب ألا يكون قد سبق استخدام هذا التوقيع من قبل حتى ولو من

صاحبه، وعلة ذلك هي كفالة أكبر قدر من السرية على هذا التوقيع. ويجب على الشخص صاحب التوقيع أن يقر كتابة بأن توقيعه الإلكتروني ملزم قانونا ويتساوى مع توقيعه بخط اليد من حيث الأثر القانوني، غير أن هذا الإقرار غير لازم في كل مرة يضع فيها الشخص توقيعه الإلكتروني. ويجوز للهيئة المسئولة عن التوقيع الإلكتروني أن تطلب من صاحب التوقيع أن يقدم شهادة بصحة توقيعه بمناسبة تصرف معين، وفي هذه الحالة فإنه يجب عليه تقديمها، ويخضع التزوير في هذه الشهادة للقواعد العامة في جريمة التزوير (٤٢).

– الضوابط الفنية الخاصة: إلى جوار الضوابط العامة سالفة الذكر، فإنه يجب أن تتوافر ضوابط فنية خاصة بالتوقيع الإلكتروني وهي تختلف من نظام تشريعي إلى آخر بحسب ما توفره من أمن وسلامة المعاملات من ناحية، ومرونة وعدم عرقلة هذه المعاملات من جهة أخرى. وتتصل هذه الضوابط بتشفير المستند، سواء أكان توقيعا أم سجلا إلكترونيا، ويلاحظ أنه لا يكفي لضمان سلامة إتمام المعاملة الإلكترونية أن يتم تشفير الرسالة المنسوبة لشخص معين، وإنما يجب التأكد من نسبة هذه الرسالة لهذا الشخص وأن مضمونها لم يتعرض لتبديل أو تشويه (٤٣).

– الاختيار بين تشفير الرسالة وعدم تشفيرها: هناك صورة مبسطة من الشفرة التي تستخدم في التصرفات التي تتم على الشبكات المفتوحة أي تلك التي يمكن لأي شخص أن يدخل إليها دون قيود، ومثالها شبكة الإنترنت. وفي هذا النظام فإن المرسل يملك أن يختار بين مفتاحين الأول عام والآخر خاص، والمفتاح الأول يستخدم عندما لا يرى المرسل حاجة إلى تشفير رسالته، وأما المفتاح الخاص فهو الذي يسمح للمرسل أن يقوم بإرسال رسائل سرية إلى الطرف الثاني ومن ثم لا يتسنى الإطلاع عليها. وفي حالة ما إذا أراد المرسل أن يبعث برسالة إلكترونية مشفرة فإن عليه أن يستخدم المفتاحين معا، أما إن لم يرد لها هذا القدر من السرية فإنه يكفيه أن يستخدم المفتاح العام. وقد يعهد إلى طرف ثالث مهمة التأكد من صحة المستند والتوقيع المنسوب إلى صاحبه، وهذا الطرف يكون موضع ثقة الطرفين وتتحدد مهمته في أن يجري تحقيقا يقف من خلاله على ما إذا كانت الرسالة المنسوبة إلى الشخص صادرة منه فعلا، ويتحقق ذلك بالربط بين المفتاحين العام والخاص والتأكد من أنهما قد استخدما من شخص معين، وأن يحدد تاريخ وساعة إرسال المستند (٤٤).

– ضوابط المضاهاة الإلكترونية: يتضمن التنظيم الفني للتوقيع الإلكتروني الأخذ بوسائل تقنية لإجراء المضاهاة الإلكترونية للتوقيع الإلكتروني والتي يمكن بمقتضاها الوقوف على صحة هذا التوقيع. وتختلف الطرق الفنية للمضاهاة إلى عدة طرق، تكفل كل واحدة قدرا معينا من الطمأنينة والثقة في المستند وتضمن سلامته، وحمايته من أن يجحد ممن صدر منه (٤٥).

– ومن هذه الوسائل: مطالبة الشخص الذي يريد التعامل مع المستند الإلكتروني بالإدلاء ببيانات شخصية معينة ومضاهاتها بالبيانات المسجلة سلفا عنه، وذلك قبل قيامه بالتوقيع الإلكتروني. وتستخدم هذه الوسيلة في التعاملات الأقل أهمية أو الأقل قيمة (٤٦). وإذا كانت وسائل المضاهاة تختلف وتتعدد فإن استخدام الشفرة السرية تعد أهم هذه الوسائل، غير أن نوع هذه الشفرة وقواعدها الفنية هو أمر يختلف بحسب كل نظام قانوني كما سبق الذكر، ويلحق بالشفرة استخدام التوقيع الرقمي.

– المضاهاة باستخدام شفرة سرية: في هذه الصورة يطالب الشخص بإدخال رقم خاص به أو كلمة سر معينة (٤٧) يتم مطابقتها على رقم أو كلمة سر مخزنة سلفا، ويطلق عليها "السر المشترك" (٤٨) الذي يتقاسم العلم به الشخص ومقدم الخدمة، فإن تطابقتا كان التوقيع تاما. ويصاحب إدخال الشفرة السرية عدة إجراءات تهدف إلى توثيق التوقيع مثل كتابة اسم المتعامل، والغرض من وضع التوقيع في المستند. وعملية التوثيق تجري إذا كان التعامل يجري على الشبكات المفتوحة مثل الإنترنت، والسر المشترك يتم تشفيره باستخدام تقنية معينة يتم إنشاؤها في أغلب المتصفحات الشهيرة على الشبكة ويتم توصيل البيانات المشفرة إلى الجهة الأخيرة التي تكون طرفا في التعامل. وفي التعاملات البسيطة أو التي لا يكون لها قيمة كبيرة، فإنه يكتفي بإدخال الشفرة السرية بعد استيفاء بعض البيانات عن شخص المتعامل. أما في التعاملات التي تقتضي درجة أكبر من الأمن، فإن هيئة أخرى هي التي تقوم بوضع الشفرة السرية بعد إجراء عملية تحقق دقيقة لشخص المتعامل (٤٩).

الفرع الثاني: صور الاعتداء على التوقيع الإلكتروني

تقسيم: من أشهر صور الاعتداء على التوقيع الإلكتروني التزوير أو التقليد، الدخول غير المشروع على أنظمة معلوماتية أو قواعد بيانات خاصة بالتوقيع الإلكتروني. وفيما يلي بيان لما أجمل:

أولا. تزوير وتقليد التوقيع الإلكتروني

الركن المادي لهذه الجريمة يدور حول فعل التزوير أو التقليد الإلكتروني – المعلوماتي. ويقصد بالتزوير المعلوماتى " أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر المعلوماتى أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات غير ورقية شرط أن تكون محفوظة على دعامة – كبرنامج منسوخ على أسطوانة – وشرط أن يكون المحرر المعلوماتى ذا أثر في إثبات حق أو أثر قانوني معين" (٥٠). ومفهوم ما سبق أن التزوير المعلوماتى يرد على وثائق معلوماتية وهي تلك الوثائق التي يتم الحصول عليها بوسائل معلوماتية، أي تكون ناشئة عن جهاز إلكتروني أو كهرومغناطيسي أو طبع ممغنط. وإن كان هناك في الفقه من يري عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية، فالوثيقة المعلوماتية هي وثيقة لم تبرمج بعد (٥١).

كذلك توجد جهات يُرخص لها سواء كانت شخصية أو اعتبارية، باعتماد التوقيعات الإلكترونية، بشهادات مصدق عليها منهم، وهذه الشهادات يترتب عليها آثارا قانونية تتمثل في إنشاء التزامات وإثبات حقوق بالنسبة لطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما. ولذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته.

ومن أشهر الوسائل التي يمكن الاعتماد عليها في تقليد أو تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها، وإعادة استخدامها بعد ذلك. والجريمة السابقة تعد من الجرائم

العمدية، صورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة، حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات، ومع ذلك تتجه إرادته إلى الفعل المجرم ويقبل النتيجة المترتبة عليها.

ثانيا. الدخول غير المشروع على قاعدة بيانات تتعلق بالتوقيع الإلكتروني

لقيام هذه الجريمة لا بد وأن الركن المادي المتمثل في الدخول غير المشروع قد وقع على أنظمة معلوماتية أو قاعدة بيانات (٥٢) تتعلق بالتوقيع الإلكتروني. وتصنف هذه الجريمة من جرائم الخطر حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه. وتعد هذه الصورة من الجرائم العمدية وبالتالي فإنه لا يتصور وقوعها بطريق الخطأ، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة. هذا وسوف نتناول هذه الجريمة وبشيء من التفصيل في الفصل الثالث من هذا الباب.

المطلب الثاني: الاعتداء على حقول الإنترنت

تمهيد وتقسيم

تعد حقول الإنترنت أو كما يطلق عليها شبكة المعلومات العالمية أكثر أقسام الإنترنت تطورا واستخداما، حيث وصل عددها في أواخر عام ٢٠٠٠ م إلى أكثر من ٢٢ مليون حقل (٥٣). وكل موقع أو حقل يتم إنشاؤه لا بد وأن يكون له عنوان خاص به يطلق عليه اسم النطاق أو اسم الحقل أو عنوان الموقع " الدومين"، فهو ضروري حيث يبين موقع الإنترنت لمن يسعى للوصول إليه، تماما مثل اسم الشخص الذي يشير إلى فرد معين أو بشكل أكثر دقة إلى مدى صحة علامة تجارية لمؤسسة أو لشركة، فأسم الشركة يشر إلى هوية شركة معينة (٥٤).

ولأن كان ذلك كذلك فقد أصبحت هذه الحقول وتلك العناوين محلا للكثير من الاعتداءات الغير مشروعة. ودراستنا لهذه الظاهرة سوف تكون من خلال محورين اثنين: الأول نبحث من خلاله ماهية هذه الحقول وأنواعها المختلفة، والثاني نبحث من خلاله الاعتداءات الواقعة عليها. وسوف نخصص لكل محور فرع خاص به.

الفرع الأول: ماهية حقول الإنترنت وأنواعها المختلفة

أولا: ماهية حقول الإنترنت

يطلق عليها أيضا شبكة المعلومات الدولية أو الشبكة العنكبوتية العالمية أو نظام الويب العالمي. تم ابتكارها على يد المهندس الإنجليزي المتخصص في المعلوماتية Tim Berners عندما قام عام ١٩٨٩ م بتصميم برنامجا أطلق عليه اسم World Wide Web يرتكز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت. ومن هنا جاءت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجانا عبر شبكة الإنترنت في عام ١٩٩١ م، وأعتمد في مرحلة أولى عام ١٩٩٣ م من

خلال برنامج التصفح Mosaic ثم لا حقا من قبل شركة Netscape الأمريكية التي عملت على تعميمه ونشره فعليا اعتبارا من ١٩٩٤ م (٥٥).

وتعّرف حقول الإنترنت أو مواقع الإنترنت بأنها "مجموعة مصادر للمعلومات متضمنة في وثائق متمركزة في الحاسبات والشبكات حول العالم" (٥٦). أوهي "مجموعة من الوثائق الموضوعة إلكترونيا في حاسبات مختلفة متصلة بالإنترنت" (٥٧) وتعّرف كذلك بكونها "الارتباط الدولي المتصل بشبكة حواسيب حول العالم " (٥٨). وهناك من يري أنها عبارة عن " نظام معلومات نشط يعمل على الإنترنت له طابع اتصال عالمي متفاعل ومتنامي يخترق الحدود بأسلوب الربط التصويري" (٥٩).

وترتكز حقول الإنترنت على بروتوكول (٦٠) HTTP الذي يسمح بربط المواقع الموصولة بشبكة الإنترنت فيما بينها. وهو لا يعمل إلا بواسطة برامج تصفح خاصة Browsers تسمح بالاتصال بالملقمات وبالمواقع المختلفة الموصولة بالشبكة وذلك بالاعتماد على تقنية الهيبرميديا ، وهذه الأخيرة تعد أداة مثالية للتجول في الإنترنت بفضل تقنيات الربط الفائق بين النصوص والصفحات والعناصر داخل الموقع ذاته ، وحتى بين الموقع والمقلمات المختلفة الموصولة بالشبكة وذلك في إطار أو تصور يشبه بالشجرة يسمى (٦١) Hypertext أو Hyper ling.

ثانيا: ماهية أسماء حقول الإنترنت " الدومين" Domain Name

إزاء الأهمية الكبيرة التي تمثلها حقول الإنترنت أو مواقع الويب العالمية كان من الضروري إيجاد آلية معينة للوصول إليها عبر هذا الفضاء الرحب. وتمثلت هذه الوسيلة في البداية في مجموعة من الأرقام تشير إلى الموقع المقصود. فإذا أراد المستخدم الوصول إلى موقع معين على الشبكة كان عليه أن يحفظ الأرقام التي تشير إلى هذا الموقع. ولكن نظرا لصعوبة حفظ هذه الأرقام لطولها وتعقدها وكثرتها اتجهت الأنظار إلى وسيلة جديدة سهلة تتفادى عيوب الوسيلة السابقة. تمثلت في مجموعة من الحروف بكتابتها نصل إلى الموقع الذي نريده. ويطلق عليها عنوان الموقع أو اسم النطاق (٦٢) Domain Name. ولقد أثار تعريف عنوان الموقع أو اسم النطاق جدلا كبيرا فاختلفت التعريفات التي قيلت بشأنه فهناك من ركز على الطبيعة الفنية للعنوان فعرفه بأنه " مجرد تحويل أو نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحا تتمشي مع اسم المشروع أو المنظمة (٦٣). وهناك من عرّفه بأنه "ترجمة لأرقام تتم عن طريق حروف معينة تسمح بدوران المعلومات عبر شبكة الإنترنت". والحروف المقصودة هنا الحروف اللاتينية (٦٤). في حين أن جانبا من الفقه استند في تعريفه لعنوان الموقع إلى الوظيفة التي يؤديها هذا العنوان فعرفوه بأنه " اسم ينفرد به حائزه عبر الإنترنت مهمته تحديد المواقع والصفحات على شبكة الإنترنت. فهو جزء من (Uniform Resource Locater URL) الذي يتعامل مع الخادم الذي يتتبع طلب الصفحة أو الموقع، ومن حيث الشكل هو عبارة عن سلسلة من الكلمات يفصل بينها نقاط تتولى تعريف عنوان برتوكول الإنترنت" (٦٥).

وهناك من يرى في هذه الأسماء بدائل للعنوان البريدي المحدد للتعرف على شخص بعينه عبر شبكة المعلومات العالمية (٦٦)، وهناك من ينظر إليها كوسيلة تمكن مستخدمي الإنترنت من الوصول إلى المواقع عبر شبكة الإنترنت فهو عنوان للهيئات والمنظمات والمشروعات والأشخاص يمكن الوصول لها عن طريقه (٦٧)، وهناك من يذهب إلى

أن هذه الأسماء ما هي إلا مجرد عنوان يعهد لصاحبه بحق استخدام المصطلح الذي سجله على شبكة الإنترنت (٦٨). وبهذا الاتجاه الأخير أخذت محكمة استئناف باريس في تعريفها لاسم حقل الإنترنت التجاري حينما عرفته في حكم صادر لها في عام ٢٠٠٠ م بأنه" مجرد عنوان افتراضي يحدد مواقع المشروعات على شبكة الإنترنت" (٦٩).

أما من الناحية القانونية فإن هذه الأسماء عبارة عن "علامة تأخذ مظهر اندماج الأرقام والحروف بحيث يتولى هذا المظهر تحديد مكان الحاسب الآلي أو موقع أو صفحة عبر شبكة الإنترنت، وهو يتكون من ثلاثة مقاطع: المستوى العالي أو العام الذي يتولى تحديد طبيعة الجهة التي يتم الاتصال معها، ومستوى ثان يتناول العلامة التجارية أو الاسم المختار أو اسم فرد ما وغيرها، ومستوى ثالث يتناول تحديد خادم مضيف محدد يتم التعامل معه" (٧٠).

وأيا كان تعريف اسم حقل الإنترنت فثمة حقيقة قائمة لا يختلف عليها اثنان وهي أن لهذا الاسم أهمية فنية واقتصادية كبيرة خاصة بالنسبة للمشروعات على شبكة الإنترنت، فمن الناحية الفنية أو التكنولوجية نجده قد سهل التعامل مع شبكة الإنترنت، فبعد أن كان هذا الاسم أو العنوان رقميا يتكون من مجموعة من الأرقام الكثيرة والمعقدة التي يصعب تخزينها أو حفظها في الذاكرة أصبح سهلا بسيطا يتكون من مجموعة من الحروف يتم ترجمتها تلقائيا إلى أرقام (٧١).

ومن الناحية الاقتصادية نجده يشكل وسيلة فعّالة للإعلان عن المشروعات والشركات والتعريف بها وعرض منتجاتها وخدماتها (٧٢). بالإضافة إلى أنه أصبح له دورٌ كبيرٌ في التعريف بالمنتجات والخدمات التي تقدمها المشروعات أو الشركات. كما وأن له دورا في تميز المشروعات التجارية. فطبقا لقاعدة "الأسبقية في التسجيل" (٧٣) والتي تحكم تسجيل هذه العناوين الإلكترونية، يتميز كل مشروع بأن له موقعا أو عنوانا خاصا به يميزه عن غيره من المشروعات الأخرى.

– أجزاء اسم الحقل: ويتكون اسم الحقل أو عنوان الموقع من ثلاثة أجزاء رئيسية: الأول هو الجزء الثابت دائما ويتمثل في المقطع http://www وهو يشير إلى البروتوكول المستخدم ويحدد أن الموقع يتواجد على شبكة الإنترنت، وهو يثبت لكافة المشروعات والشركات والأشخاص الذين يمتلكون مواقع على الشبكة. أما الجزء الثاني فهو عبارة عن اسم أو رمز أو اختصار للمؤسسة أو الشخص أو الجهة صاحبة الموقع مثل Google، Omantel وغيرها. وأخيرا الجزء الثالث: وهو الجزء الأكثر أهمية ومعرفة من قبل مستخدمي الشبكة ويعرف باسم نطاق المستوى الأعلى Top- Level Domain وهو يتكون من فئتين: الأولى هي نطاق المستوى الأعلى العام (gTLD) للدلالة على هوية أو نشاط أو شكل صاحب الموقع مثل (.com)، (.org) ،(.net) وهي توجه بالدرجة الأولى إلى المستهلكين في كل دول العالم ، والفئة الثانية هي نطاقات المستويات العليا لرموز الدول (ccTLD) وتستخدم للدلالة على اسم القطاع أو المنطقة الجغرافية مثل: om بالنسبة لسلطنة عمان ، eg بالنسبة لجمهورية مصر العربية (٧٤).

الهيئات المانحة لأسماء حقول الإنترنت في شبكة الإنترنت: في البداية كان نظام تسجيل وإدارة عناوين المواقع حكرا على لجنة IANA (٧٥)، إلا أنه ولعجز نظام العنونة الذي كان قائما (٧٦) وعدم قدرته على التحكم في النزاعات

والصعوبات التي نشأت في هذا المجال، وانسجاما مع توجه الحكومة الأمريكية نحو تخصيص نظام منح عناوين المواقع في شبكة الإنترنت DNS (٧٧). دفعا باتجاه إعادة النظر بهيكلية لجنة منح الأرقام في الإنترنت LANA.

من هذا المنطلق تأسست عام ١٩٩٨ م مؤسسة الإنترنت لمنح الأسماء والأرقام والمعروفة باسم "آيكان" (٧٨) ICANN وهي مؤسسة أمريكية خاصة من فئة المؤسسات غير الربحية مقرها مدينة لوس أنجلس بولاية كاليفورنيا، مهمتها الأساسية تقوم على التحكم في الأسماء والأرقام وبالتالي السيطرة على آلية المعاملات والاتصالات عبر شبكة الإنترنت. وفي ذات العام وقعت هذه المؤسسة مذكرة تفاهم مع وزارة التجارة الأمريكية ترمي إلى إيجاد نظام للعضوية والانتساب إلى ICANN يؤمّن تمثيلا واسعا لمستخدمي الإنترنت المنتشرين حول العالم عن طريق ابتكار آليات وقواعد جديدة في منح عناوين المواقع تأخذ في الحسبان البعد الدولي لشبكة الإنترنت. وبموجب هذا النظام الجديد (٧٩)، استمرت لجنة منح الأرقام في الإنترنت IANA في تولي عناوين المواقع بالنسبة إلى القطاعات التي ترمز إلى أسماء الدول "ccTLD" في حين انتقلت صلاحية منح عناوين المواقع المستقلة من مؤسستي INTERNIC و NIC إلى أكثر من خمسين مكتبا متخصصا تعمل تحت إشراف ICANN ويتوزع على سبع مناطق حول العالم (٨٠). وقد أصدرت ICANN منذ تأسيها عدة تقارير تضمنت توزيعا جديدا لأسماء الحقول وآليات جديدة في أصول منحها وكيفية حل المنازعات بشأنها، والتي بوشر في تنفيذها اعتبارا من العام ١٩٩٩ م.

ثالثا: الأنواع المختلفة لحقول الإنترنت

نوع حقل الإنترنت أو موقع الإنترنت يرتبط ارتباطا وثيقا بالاسم المطلق عليه وهذا الأخير يؤخذ بإحدى الصورتين: إما اسم عام أو دولي، أو اسم وطني أو محلى، وهذا معناه أن المواقع قد تكون عامة أو دولية وقد تكون وطنية أو محلية. وفيما يلي بيان لما أجمل:

١. أسماء حقول الإنترنت العامة أو الدولية (٨١): تعرف باسم نطاقات المستويات العليا ويطلق عليها اصطلاحا general Top-Level Domains(gTLD)، وهي تشير إلى أنشطة دولية عامة لا تنتمي إلى دولة بعينها وإنما توجه بالدرجة الأولى إلى المستهلكين في جميع دول العالم. وفي فترة معينة كانت هذه الأسماء تتمثل في عدد معين تغطي سبعة مجالات ثلاثة منها متاح للجميع وأربعة متاحة بشروط محددة لجهات محددة كالتالي (٨٢):

- ثلاثة أسماء دومين متاحة للجميع القيد بها وهي بلا قيد أو شرط:
- com. وهو يشير إلى كل ما يتعلق بالأنشطة التجارية (٨٣)
- net. وهو يتعلق بالشبكات المعلوماتية.
- org. ويتعلق بالمنظمات المختلفة التي لا تسعى التي تحقيق الربح.

- أربعة أسماء دومين مقيد التسجيل بها وهي فئتان:

الأولى: أسماء مقصور التسجيل فيها على الولايات المتحدة الأمريكية وهي:

- gov. ويخص الهيئات المختلفة التي تتكون منها الحكومة الأمريكية.
- mil. وهو خاص بهيئات الدفاع الأمريكية.

الثانية: أسماء مقصور التسجيل بها على من يستوفي شروط معينة وهي:
- edu. خاص بالهيئات والمعاهد التعليمية المانحة لمؤهلات دراسية.
- int. وهو يتعلق بالهيئات والمنظمات الدولية المختصة بعقد الاتفاقيات الدولية.

إلى جانب هذه الأنواع السابقة تقدمت شركة IAHC (٨٤) في فبراير ١٩٩٧ م بمشروع ينص على إنشاء سبعة أسماء أخرى تختلف بحسب الأنشطة وتتمثل هذه الأسماء السبعة في (٨٥):
- firm. يتعلق بالشركات التجارية ومجال الأعمال.
- web. وتخص إلى الأنشطة المتعلقة بالإنترنت.
- nom. تخص الأسماء والألقاب.
- arts. خاص بالفن والثقافة.
- info. وتشير إلى مجال بنوك المعلومات.
- store. يتعلق بخدمات طلبات البضائع.
- rec. خاص بأنشطة التسلية والترفيه.

وعلى الرغم من تقديم هذا المشروع إلا أنه لم يلق النور بسبب اعتراض الإدارة الأمريكية (٨٦).
وخلال عام ٢٠٠٠ م وافقت مؤسسة ICANA على إضافة سبعة أسماء عامة لنطاقات عالية المستوى هي:
- aero. خاصة بالنسبة للنشاط الجوي
- biz. تخص النشاط المهني
- coop. تعلق بالنشاط التعاوني
- name. خاصة بالمواقع ذات الطابع الشخصي
- info. تتعلق بالنشاط الإعلامي وبنوك المعلومات
- museum. تخص المتاحف
- pro. تشير إلى كل ما يتعلق بالنقابات المهنية

وفي وقت لاحق وخلال عام ٢٠٠٥ م وافقت المؤسسة السالفة الذكر على استخدام اسم post. بالنسبة للنشاط البريدي. واسم travel. بالنسبة للنشاط السياحي.

٢. أسماء حقول الإنترنت الوطنية أو المحلية: تعرف باسم نطاقات المستويات العليا لرموز الدول ويطلق عليها اصطلاحا country code Top-Level Domains (ccTLD) ويقصد بها تلك الأسماء التي تنتهي بحرفين يشيران إلى اسم الدولة التي تنتمي إليها هذه العناوين، وهي لا تتقيد بحدود جغرافية فكل دولة موصولة على شبكة الإنترنت لها اسم موقع دولي فمثلا أسماء الحقول العمانية نجدها تنتهي بأول حرفين من كلمة Oman وهو ".om" ، وأسماء الحقول المصرية تنتهي بـ ".eg"، وأسماء الحقول الفرنسية تنتهي بـ ".fr" ، وأسماء الحقول الأمريكية تنتهي بـ ".us" "

وهكذا. وغالبا ما تلجأ المشروعات إلى تسجيل عناوينها الإلكترونية أولا في مجالها الوطني فإذا ما حقق هذا التسجيل فائدة لها، يبحث بعد ذلك عن تسجيل عنوان آخر دولي عام وغالبا ما يكون في المجال com. (٨٧).

الفرع الثاني: الاعتداء على حقول الإنترنت وأسماء الدومين

تمهيد وتقسيم

نظرا لما لحقول الإنترنت وعناوينها من أهمية، باتت محلا للكثير من الاعتداءات الغير مشروعة التي أصبحت تشكل خطرا عليها. ولخطورة هذه الظاهرة فإننا سوف نحاول في الأسطر القادمة تسليط الضوء عليها، سواء بالنسبة للاعتداءات الواقعة على حقول الإنترنت ذاتها، أو تلك الواقعة على أسماء النطاقات". وفيما يلي بيان لما أجمل.

أولا. الاعتداء على حقول الإنترنت

تتعدد أساليب وطرق الاعتداء على المواقع، إلا أنها في مجملها تهدف إلى مهاجمة هذه المواقع وتحقيق نفع معين للمهاجم من وراء ذلك، وفي بعض الأحيان لا يكون هناك نفع للمهاجم سوى تعريض الموقع الضحية للخطر والضرر، ومن أهم الأساليب والطرق:

١. تدمير المواقع: يقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (server-pc) أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو النظام. ومن الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي (٨٨). والجدير بالذكر أن هجومين من هذا النوع تعرض لها موقع Hotmail وذلك في أواخر عام ٢٠٠٠ م، وتسبب في خسائر مالية تجاوزت ملايين الدولارات (٨٩). ولعل من أخطر وسائل تدمير المواقع وأشدها ضررا استخدام ما يعرف بالفيروس المعلوماتى الذي سنعرض له وبشيء من التفصيل لاحقا عند دراسة جرائم إتلاف وتدمير المعطيات (٩٠).

وفي الواقع هناك أسباب تكمن وراء عملية تدمير المواقع منها: ضعف الكلمات السرية المستخدمة، حيث نجد أن بعض مستخدمي شبكة الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسرها أو تخمينها من قبل المخترق.ومن الأسباب أيضا عدم وضع برامج حماية كافية لحماية الموقع من الاختراق والتدمير أو عدم تحديثها بصورة مستمرة. كذلك استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر أو تستخدم برامج وأنظمة غير موثوقة أمنيا ولا يتم تحديثها باستمرار الشيء الذي قد يكون سببا من أسباب تدمير الموقع. ناهيك عن عدم القيام بالتحديث المستمر لنظام التشغيل والذي يساعد في كثير من الأحيان على اكتشاف المزيد من الثغرات الأمنية. ومن الأسباب التي تساعد على تدمير المواقع عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة (٩١).

٢. تشويه المواقع Defacement: ماذا سيكون رد فعلك، إذا دخلت إلى موقع إحدى الشركات التجارية الكبرى، أو أحد مواقع الإنترنت الحكومية، بقصد شراء بعض السلع أو الحصول على بيانات رسمية معينة، وإذ برسالة بذيئة، تطالعك في الصفحة الرئيسية من هذا الموقع؟! إذا كنت مستخدماً عادياً، فستنتقل بسرعة، غالباً، من حالة الصدمة والاندهاش، إلى حالة السخرية من الموقع والجهة التي يمثلها! أما إذا كنت مشرفاً على هذا الموقع، أو مسئولاً عن الشبكة التي تنتمي إليها، فنتوقع أن يؤدي مزيج المشاعر التي ستنتابك، إلى تصبب العرق منك بغزارة.. لأنك ستكون أنت، موضع السخرية! يوجد تشابه كبير، بين ما يحصل في العالم الافتراضي من عمليات تشويه مواقع ويب (Defacement)، وبين ما يحدث على أرض الواقع عندما يتم إنزال علم دولة معينة، من السفينة، ورفع علم القراصنة مكانه، حيث أن عملية التشويه، في أغلب الأحيان، ليست سوى تغيير الصفحة الرئيسية للموقع، بصفحة أخرى، يعلن المخترق فيها انتصاره على نظام مزود ويب، والإجراءات الأمنية للشبكة، ويقصد من ورائها إبراز قدراته التقنية، وإعلان تحدّيه للمشرفين على نظم مزودات ويب، ليثبت لنفسه، أو لغيره، امتلاكه المقدرة التقنية على كسر نظام الحماية في هذه المزودات، الأمر الذي يتطلب معرفة معمقة، لطريقة عمل إنترنت، وبروتوكولات التشبيك، وأنظمة التشغيل المختلفة التي تعمل عليها مزودات ويب. وتتضمن الصفحة الجديدة أحياناً، رسالة يرغب الشخص الذي قام بعملية التشويه إيصالها للعالم. وقد تتضمن هذه الرسالة اعتراضاً منه على حالة سياسية أو اجتماعية، أو صرخة يريد إيصالها، إلى كل من يزور هذا الموقع!

وتقتصر الأضرار التي تتسبب بها عمليات تشويه مواقع ويب، على الإضرار بسمعة الجهة المالكة للموقع، حيث يتم تغيير الصفحة الرئيسية فقط من الموقع، بصفحة HTML من تصميم المخترق، الذي يقتصر هدفه ، كما ذكرنا، على إيصال رسالته إلى العالم عبر الموقع. ولا يلجأ المخترقون، عادةً، في عمليات التشويه إلى تدمير محتويات الموقع، حيث يمكنك في أغلب المواقع التي تتعرض لعمليات التشويه، الوصول إلى جميع صفحاته المكونة للموقع، إذا كنت تعلم عنوان الصفحة كاملاً. ومن الأمثلة على عمليات تشويه المواقع قيام مجموعة قرصنة إسرائيلية في أكتوبر ٢٠٠٠ م باقتحام موقع حزب الله وحذف محتوياته ووضع نجمة داود وعلم إسرائيل عليه (٩٢). كذلك وفي عام ٢٠٠١ م قامت المخابرات الإسرائيلية باقتحام موقع حركة حماس ونشر صورا إباحية عليه (٩٣). وبتاريخ ٢٠٠١/١/٢١ م شنت مجموعة من الهاكرز حملة على مواقع حكومية في كل من الولايات المتحدة الأمريكية والمملكة المتحدة وأستراليا حيث استبدلت الصفحات الخاصة بتلك المواقع الحكومية بشعار المجموعة مع رسالة تفيد بأن هذا الهجوم يعتبر أكبر تشويه لمواقع حكومية وعسكرية في تاريخ البشر، وكان من بين تلك المواقع، موقع الهيئة التشريعية لولاية كاليفورنيا وموقع وزارة الداخلية للأسكا وبعض مواقع السلطات المحلية بالمملكة المتحدة (٩٤). أيضا من أبرز ضحايا هذا الأسلوب موقع قناة الجزيرة الفضائية القطرية الذي تعرض لهجوم القراصنة في بداية عام ٢٠٠٣ م إبان الحرب على العراق حيث قوبل الزائر لموقع القناة بشعار للعلم الأمريكي وعبارة "دعوا الحرية تصدح" (٩٥). وهناك أيضا موقع جريدة مصر العربية الإلكترونية الذي تعرض لأكبر وأعنف هجوم إلكتروني منذ تدشينه أدى إلى تعطيله ليوم كامل، حيث وضعت على الصفحة الرئيسية الخاصة به صورا إباحية وعبارات يهودية (٩٦).

كيف تحدث عمليات تشويه موقع ويب؟

يتّبع المخترقون أساليب عدة، في عمليات تشويه صفحات ويب. وتختلف هذه الأساليب من موقع إلى آخر، بناءً على نوع نظام التشغيل، ومزود ويب الذي يعتمد عليه الموقع. ونوضح هنا، أكثر هذه الأساليب انتشاراً (٩٧):

أ. الدخول بهوية مخفية (anonymous)، عبر منفذ بروتوكول FTP: تمكن هذه الطريقة، في بعض الحالات، المخترق من الحصول على ملف كلمة الدخول المشفرة، الخاصة بأحد المشرفين على الشبكة، أومن يملكون حق تعديل محتويات الموقع، والعمل على فك تشفيرها، حيث يتم إرسال كلمة السر مشفرة في مختلف المزودات. لكن هذه الشيفرة، تظهر في بعض المزودات، ضمن ملف كلمة السر، ويظلل البعض الآخر من المزودات، هذه الكلمة بعد تشفيرها (أي يظهر حرف x مكان كل رمز من الكلمة المشفرة). وتصعب في الحالة الأخيرة على المخترقين، عملية كسر الشيفرة. ويلجأ المخترقون، بعد الحصول على ملف كلمة السر، إلى استخدام برامج خاصة لتخمين كلمات السر (٩٨). حيث تعمل على تجربة جميع الاحتمالات الممكنة لكلمة السر، من حروف وأرقام ورموز، وكلما كانت كلمة السر طويلة بحيث تحوى عدداً كبيراً من الرموز كان التوصل إليها يستغرق وقتا أطول يصل إلى سنوات بناءً على عدد الرموز المستخدمة، والنظام المستخدم في عمليات التخمين. وننصح باستخدام كلمة سر طويلة نسبياً، وتغييرها خلال فترات متقاربة، للتقليل من احتمال توصل أحد المخترقين إليها. فمن شأن حصول المخترق على كلمة السر الخاصة لأحد المشرفين، السماح له بالدخول إلى مزود ويب، وتغيير الصفحة الرئيسية.

ب. استغلال الثغرات الأمنية في مزودات ويب، وأنظمة التشغيل: لا يخلو أي نظام تشغيل، أو مزود ويب، من ثغرات أمنية تعرض مستخدميه لخطر الاختراق، ويعمل المطورون بشكل مستمر، على سد هذه الثغرات، كلما اكتشفت. ويستغل الهكرة هذه الثغرات الأمنية في عمليات الاختراق، إلى أن تجد الشركة المصممة للنظام، الحل المناسب لها. وتبقى بعض الثغرات متاحة لفترة طويلة حتى يتم اكتشافها، وذلك لأن أغلب الثغرات التي يكتشفها الهكرة، لا يعلنون عنها بسرعة، ليتمكنوا من استغلالها فترة أطول! لأجل ذلك ينبغي على جميع مدراء ومشرفي الشبكات، متابعة مواقع الشركات المصممة لنظم التشغيل، ومزودات ويب، ليتسنى لهم الإطلاع على آخر ما تم التوصل إليه من ثغرات أمنية، وجلب برامج الترقيع (patches) لها، حيث تحرص هذه الشركات على تقديم مثل هذه البرامج بأسرع وقت ممكن.

ج. استخدام بروتوكول Telnet: تسمح كثير من الثغرات الأمنية في الأنظمة المختلفة، سواء كانت يونكس،أو ويندوز، أو غيرها، باستخدام تطبيقات تعتمد على بروتوكول Telnet، الذي يسمح بالوصول إلى أجهزة الكمبيوتر عن بعد، وتنفيذ الأوامر إليها. ويمكن استخدام هذا البروتوكول للدخول إلى مزودات ويب، وتغيير الصفحات فيها.

٣. حجب الخدمة Denial of service (DoS): "الوصول إلى هذا الموقع، غير ممكن!" قد تعني الرسالة السابقة أن الموقع الذي تحاول أن تزوره، تعرض لهجمات حجب الخدمة، خاصة إذا كان واحداً من المواقع الكبرى، التي يعني ظهور مثل هذه الرسالة في موقعها، خسارة عشرات الآلاف من الدولارات! وتتم هذه العملية عن طريق توجيه جهة معينة، حزم بيانات شبكية بصورة كثيفة جداً، إلى هذه المزودات، بهدف إيقافها عن العمل. ويعتبر القيام بمثل هذه

الهجمات سهلاً للغاية، حيث يوجد عدد كبير من البرامج التي يمكن استخدامها لتوجيه الطلبات والحزم الشبكية إلى هدف محدد، كموقع إنترنت، أو عنوان IP.

اعتمدت أولى هجمات حجب الخدمة، التي ظهرت في العالم، على توجيه طلبات كثيفة باستخدام بروتوكول رسائل التحكم بإنترنت (٩٩) ICMP (الذي يسمح بتبادل رسائل التحكم، والتعامل مع رسائل الخطأ، بين مزودات ويب. وتحدث هذه الهجمات اليوم، باستخدام منافذ بروتوكولات TCP، وUDP، بالإضافة إلى ICMP، في تسليط سيل من الرزم الشبكية إلى مزودات معينة، عبر أوامر، مثل Ping. ومن أشهر الهجمات، تلك التي تستخدم نوع الهجوم المعروف باسم WinNuke، والتي تسلط سيلاً من الحزم الشبكية عبر المنفذ ١٣٩ من نظام NetBIOS، الذي يسمح ربما بتحاور التطبيقات الموجودة على الأجهزة المرتبطة بالشبكة. وتوجد بالإضافة إلى ما سبق، عشرات الطرق التي يمكن إتباعها لدفع الحزم أو الطلبات الشبكية، إلى مزودات معينة، لإيقافها عن العمل، سواء كانت مزودات ويب، أو مزودات بريد إلكتروني، أو أي مزود يمكنه أن يستقبل الحزم الشبكية. وتعرف أنواع هذه الهجمات، بأسماء غريبة، منها: SYN، وSmurf، و Floods، وLand، وPing Bomb، وPing O'Death، وFraggle، بالإضافة إلى Winnuke، المذكور سابقاً. وبالإضافة إلى سهولة القيام بمثل هذه الهجمات، نجد أن توقعها،أو صدها صعب جداً! لكن ما دوافع هذه الهجمات؟!

توجد عدة أهداف، قد تدفع جهة معينة، أو شخصاً معيناً، إلى القيام بمثل هذه الهجمات، أهمها:
أ- التسلل إلى النظام: قد يكون الهدف من توجيه الهجمات الرغبة في التسلل إلى النظام وقت انهياره وحجبه عن الخدمة، أو وقت إعادة إقلاعه. وتوجد عدة طرق لذلك، على مختلف الأنظمة، وهي أحد الأسباب الأكثر منطقية لمثل هذه الهجمات.

ب- أسباب سياسية: قد توجه جهة معينة، مثل هذه الهجمات، إلى موقع حكومي يتبع دولة تعاديها، أو موقع شركة تنتمي إلى هذه الدولة. مثلما حصل عندما تمكن هاكر أمريكي من تعطيل موقعين إسلاميين يملكهما أحد مواطني المملكة العربية السعودية هما jehad.net وjehadonline.org بزعم أنهما يؤيدان تنظيم القاعدة، وذلك بعدما استطاع الوصول إلى البريد الإلكتروني الخاص بمالك الموقعين والحصول منه على بعض المعلومات الخاصة بهذين الموقعين منها اسم المستخدم وكلمة المرور وباستخدام هذه المعلومات تمكن من حجب الخدمة عن هذين الموقعين (١٠٠) ومن الأمثلة أيضا ما قام به شخص أمريكي من أصل يهودي عندما أسس موقع الهاجانة (١٠١) بهدف ملاحقة المواقع الإسلامية التي تتحدث عن الجهاد أو التي تنقل أخبار الجهاد وتدميرها (١٠٢). هذا ويتوقع أن تزداد في المستقبل، الهجمات ذات الأهداف السياسية، مع ازدياد انتشار إنترنت!

ج- أسباب اقتصادية: قد توجه شركة صغيرة مثل هذه الهجمات، إلى شركة كبيرة تسيطر على السوق، في نوع من المنافسة التجارية غير الشريفة!

د- الانتقام: يحدث كثيراً، أن تسرّح شركة أحد الموظفين المسئولين عن إدارة الشبكة. وقد يلجأ بعض هؤلاء، إذا ما شعروا بالظلم، إلى الانتقام من الشركة!

هـ- الطبيعة التخريبية: يلجأ بعض الأشخاص إلى مثل هذه الهجمات، لإشباع رغبات تخريبية تتملكهم! مثلما حصل عام ٢٠٠١ م عندما تمكن طالب أمريكي يدعي دينيس موران (١٨ سنة) من التسلل إلى موقع شرطة لوس أنجلس الخاص بمكافحة المخدرات على شبكة الإنترنت ومحاولة إيقافه وتخريبية (١٠٣)، وفي ذات العام هوجم موقع البيت الأبيض على شبكة الإنترنت على يد مجموعة من الهاكرز وتسبب هذا الهجوم في قفل الموقع وتعطله عن العمل (١٠٤). ومن المواقع التي تعرضت للتعطيل وحجب الخدمة في منتصف شهر يوليو ٢٠٠٣ م على يد بعض القراصنة موقع وكالة الأنباء الإماراتية "وام" (١٠٥).

وتعتبر هجمات حجب الخدمة الموزعة Distributed Denial of Service (DDoS)، من أحدث أنواع هجمات حجب الخدمة العادية التي تعتمد على استخدام برامج معينة في الهجوم. ومن المواقع التي هوجمت بهذا النوع من هجمات حجب الخدمة: ZDNet وYahoo!، وeBay، وAmazon، وCNN، وغيرها. وتعتمد هذه الهجمات على تجنيد أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت، بدون علم مالكيها، وتوجيهها إلى بث الرزم الشبكية إلى مزود معين، بهدف إيقافه عن العمل، نتيجة ضغط البيانات المستقبلة. وتقوم فكرته على وضع برنامج خبيث خاص، من نوع "حصان طروادة" (Trojan Horse)، في كل جهاز حاسب آلي متصل بالإنترنت يمكن الوصول إليه، عن طريق إرسال البرنامج بواسطة البريد الإلكتروني، مثلاً، و تفعيله على هذه الأجهزة، لتعمل كأجهزة بث للرزم الشبكية، عند تلقيها الأمر بذلك من برنامج محدد يقبع على جهاز أحد المخترقين. ومن أشهر البرامج المستخدمة في إجراء هذه الهجمات: TRINOO، وTribeFloodNet، وTFN2K، وStacheldraht. ويعتبر هذا النوع من هجمات حجب الخدمة، أكثر الأنواع خطورة، حيث يمكن أن يشكل خطراً على شبكة الإنترنت كلها، وليس على بعض المواقع فقط . مما قد يهدد الشبكة بالكامل (١٠٦).

٤. المحاكة والاختلاس والتضليل: البحث عن المعلومة في موقع ما هو بالتأكيد بحث عن المضمون الذي يعد الدم الطازج للموقع الذي يخشى امتصاصه دون وجه حق. فالمعطيات الموجودة عليه من صور ونصوص ورسومات وعناصر صوتية وغيرها يمكن بسهولة نسخها وإعادة عرضها على موقع أخر دون إذن أو إشارة إلى الموقع الأصلي أو التضليل بالإيحاء بأن ذلك المضمون المعروض خاص بالموقع العارض. فكثير ما تثور القضايا بصدد أوجه التشابه بين المواقع فيما يتعلق بالشكل والمضمون وأسلوب عرض الخدمات (١٠٧).

٥. محاكة المواقع: غالبا ما يستخدم هذا الأسلوب في السطو على أرقام البطاقات الائتمانية وأرقام الحسابات والأعمال التجارية، وفكرته تقوم على تقليد أحد المواقع الحقيقية التي غالبا ما تكون مواقع تجارية بكافة تفاصيلها من تخطيط وألوان ووظيفة. وهو ما يتم عن طريق تسجيل اسم نطاق يكون وثيق الصلة بمواقع سليمة قانونا وربما يختلف في حرف واحد، بعدها يقوم موقع الويب غير القانوني بنسخ بعض محتويات الموقع القانوني وينشئ بعض الوظائف

بغرض تقليد الإحساس بالروابط المحتواة في الموقع، والخطوة الثالثة تكمن في تقديم منتج عام بسعر مدهش لحث الناس على إرسال معلوماتهم الائتمانية (١٠٨).

٦. انتحال شخصية الموقع: يتم بهجوم يشنه الهاكرز على الموقع والسيطرة عليه ومن ثم يقوم بتحويله لموقع آخر. أو يحاول الهاكرز اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرامج الخاصة به هناك. مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة أسم الموقع المشهور (١٠٩).

ثانيا. الاعتداء على أسماء حقول الإنترنت " الدومين" Domain Name

عندما سطا "جون ويليامز راسين " على موقع " الجزيرة نت aljazeera.net " التابع لقناة الجزيرة الفضائية أثناء الحرب على العراق ، لم يستخدم لغات برمجة معقدة أو برامج معينة لاعتراض البيانات .. كل ما كان عليه أن يعمله هو الحصول على بطاقة هوية هاتفية وتزوير توقيع وإرسال طلب بالفاكس بالتوقيع المزور إلى شركة " نيتورك سولوشن " وهي أكبر شركة لحجز أسماء الحقول على شبكة الإنترنت تابعة لمؤسسة " فيري سين Verisign " التي تمنح شهادات الضمان الأمني للمواقع وخاصة تلك التي تتعامل في التجارة الإلكترونية، يطلب فيه إعادة تخصيص بيانات المستخدم يتم فيه تغير بيانات التحكم باسم الحقل القديم ببيانات حديثة. وهكذا وبكل بساطة قامت شركة " نيتورك سولوشن " بإعادة تخصيص الموقع إلى جون البالغ من العمر ٢٦ عاما ويقطن في ولاية كاليفورنيا الأمريكية، حيث اضطرت القناة للدخول في دوامة إدارية وفنية حتى تستعيد موقعها مرة أخرى (١١٠).

وتجربة قناة الجزيرة تلك ليست جديدة في هذا الشأن، فعمليات سرقة أسماء الحقول كانت تجري على قدم وساق منذ عدة سنوات سابقة، حيث احترف بعض الأشخاص عديمي الضمير ممارسة السطو الإلكتروني بهدف انتزاع الأموال من المالك الشرعي للاسم، أو تظليل المستهلك أو إحداث اللبس لديه. ولقد وقعت عدة شركات كبيرة كانت أو صغيرة ضحية عمليات نصب عديدة، فمثلا في عام ١٩٩٥ م كان عنوان موقع الويب mcdonlads.com المملوك لشركة Mc Donald's العالمية الشهيرة المتخصصة بتقديم الوجبات السريعة مسجلا باسم صحفي يعمل بمجلة Wired الأمريكية، ولقد تمكنت هذه الشركة وبعد مساومات مالية كبيرة من استرجاع هذا العنوان الخاص بها . وفي عام ٢٠٠٠ م تمت سرقة اسم الحقل الخاص بشركة GTE وهي من كبرى شركات الاتصال في الولايات المتحدة، وفي نفس الفترة خاضت شركة " ليسلي هاربولد" حربا لمدة عام كامل من أجل استعادة اسم الحقل الخاص بها وهو hoopla.com (١١١).

وإذا اكتشفت أن العلامة التجارية أو علامة الخدمة لشركتك أو اسم الموقع الخاص بك قد تعرض للسطو الإلكتروني (١١٢) فما عليك سوى إتباع إجراءات بسيطة موجودة على شبكة الإنترنت حيث يتخذ خبير مستقل قرار يبت بإمكانية رد اسم الحقل إليك، عندها يكون أمناء التسجيل ملزمين بإتباع ذلك القرار. و جاءت هذه الإجراءات بالسياسة الإدارية الموحدة لتسوية المنازعات UDRB في الأصل بناء على اقتراح من الويبو كنتيجة لمشروعي الويبو الأول والثاني بشأن الإنترنت والتي تم اعتمادهما من قبل هيئة الإنترنت المعنية بالأسماء والأرقام "الايكان" (١١٣).

فضلا عن أن أسماء الحقول – الدومين– بوصفها علامة لتميز السلع والخدمات عبر شبكة الإنترنت لا تقع حصراً، إلا أنها تتمتع بالحماية القانونية المقررة طبقا لمبدأ أسبقية التسجيل (١١٤)، بمعنى أنه في حالة التزاحم بين عدة شركات

أو أشخاص لهم ذات الاسم بالنسبة لأحد السلع والخدمات، فإن الحماية القانونية المقررة تكون لمن بادر وسبق غيره في التسجيل. بالإضافة إلى ذلك فإنه يوصى دائما بتفادي اختيار أسماء الحقول التي تتألف من بعض الكلمات الأخرى المثيرة للجدل كالمصطلحات الجغرافية وأسماء المشاهير وأسماء الأدوية وأسماء المنظمات الدولية والأسماء التجارية التي قد تتداخل مع حقوق الغير أو أنظمة الحماية الدولية.

المطلب الثالث: جرائم السطو على أرقام البطاقات الائتمانية

بطاقة الائتمان (١١٥) Credit card تعد إحدى الخدمات المصرفية التي استحدثها الفن المصرفي في الولايات المتحدة الأمريكية منذ قرابة ثلاث وخمسين سنة. وأول بداية حقيقية لبطاقات الائتمان بالمفهوم الحديث ترجع للأمريكيين (فرنك بكن مارا ورالف سيندر) في عام ١٩٥٠ م. وتقوم هذه البطاقات أساسا على فكرة الائتمان لافتراضها وجود فاصل زمني بين تقديم مانح الائتمان لوسائل الوفاء لعملية الشراء وبين استرداد تلك الوسائل. وبعد التطور الكبير التكنولوجي في مجال الاتصالات وظهور التجارة الإلكترونية وانتشارها الكبير واعتماد الكثير من الناس في شراء حاجاتهم على شبكة الإنترنت أمتد نشاط هذه البطاقات إلى شبكة الإنترنت الذي شكّل عملية متسارعة لكونه يعد إحدى الطرق السهلة لشراء كل شيء تقريبا، فالتسوق عبر شبكة الإنترنت أصبح يتم في أي مكان على الأرض وفي أي وقت دون حاجة إلى مغادرة المنزل أو المكتب، فكل ما يحتاجه الشخص هو اتصال بالإنترنت وبطاقة ائتمان سارية المفعول.

لا أن استعمال هذه البطاقات على الشبكة يثير مشاكل كبيرة على عكس الدفع العادي الذي يتم مباشرة بين البائع والمشترى في دقائق معدودة، فالتعامل بهذه البطاقات في ساحة الإنترنت يكون عبر فضاء مفتوحا، لأن من يقوم بالدفع ببطاقته هو في حقيقة الواقع يتعامل مع مئات الآلاف ممن يحاولون اصطياد بيانات هذه البطاقة وأرقامها ليقوموا باستعمالها في مشترياتهم، وانعدام عملية التوقيع على النموذج الورقي لبطاقة الدفع يثير أيضا مشاكل أخرى لأن مطابقة التوقيع على النموذج الأرضي لبطاقة الدفع يكون دافعا لكشف سارقها في حين أن التعامل الإنترنتى لهذه البطاقة لا يكشف هوية مستعملها وتوقيعه. فشخص موجود في الخليج مثلا يستطيع سرقة بيانات بطاقة شخص آخر موجود في جنوب أمريكا عندما يقوم هذا الأخير باستعمالها في الشراء عبر إحدى المواقع المنتشرة على شبكة الإنترنت، وبالتالي يمكن أن يستعملها الشخص الأول في عمليات شراء من مواقع أخرى موجودة على الشبكة وفي أي وقت ومن أي مكان. من هنا كان ظهور أحد أهم وأخطر صور الأنشطة الإجرامية المستحدثة التي تقع على البطاقات الائتمانية ألا وهو السطو على الأرقام والمعلومات الخاصة بتلك البطاقات واستخدامها فيما بعد استخداما غير مشروع من قبل الغير.ففي اليابان ألقت الشرطة القبض على رجلين قاما بسرقة ١٦ مليون ين من حساب عميل احد البنوك بعد تمكنهما من سرقة بيانات بطاقته الائتمانية خلال ترددهما على مقاهي الإنترنت (١١٦)، وفي الولايات المتحدة الأمريكية وجه مكتب التحقيقات الفيدرالية الإتهام إلى ثلاثة أشخاص لحصولهم على بيانات بطاقات ائتمانية من خلال أجهزة الحاسب الآلي، واستغلالها في سرقة نحو ثلاثة ملايين دولار من حسابات مصرفية لأكثر من ثلاثين ألف شخص، وتعد هذه الوقائع حسبما جاء على لسان ممثل الادعاء العام في ولاية نيويورك أكبر قضية سرقة بالحاسب الآلي في تاريخ الولايات المتحدة الأمريكية (١١٧).

وبعد هذه اللمحة الموجزة عن البطاقات الائتمانية يثور التساؤل عن أهم الطرق وأشهرها المستخدمة في عملية السطو على أرقام هذه البطاقات ؟

أولا: الطرق والأساليب:

تعتمد آلية الشراء عبر شبكة الإنترنت باستخدام البطاقات الائتمانية على تزويد التاجر برقم البطاقة الخاصة بالعميل والعنوان الذي يرغب باستلام السلعة من خلاله ومعلومات أخرى، ليصله طلبه خلال الفترة الزمنية التي تم الاتفاق عليها، في الوقت الذي تتولى فيها شبكات البنوك العالمية والشركات إجراء عمليات التقاص بين الحسابات وقيد الفوائد والعمولات وفقا للاتفاقيات والبروتوكولات بهذا الشأن (١١٨). إلا أن هذه الميزة الإيجابية لعملية الشراء باستخدام شبكة الإنترنت قابلها استغلال غير مشروع لمواطن الضعف التي كشف عنها التطبيق العملي لهذا النظام، حيث أصبحت الأرقام والبيانات الخاصة بتلك البطاقات المنقولة عبر شبكة الإنترنت عرضة للالتقاط غير المشروع من قبل الغير، وبالتالي الاعتداء على الذمة المالية لصاحب البطاقة أو البنك المصدر لهذه البطاقة، ففي عام ٢٠٠٠ م ألقت الأجهزة الأمنية بإحدى الدول القبض على أحد الطلاب بتهمة قرصنة أرقام إحدى البطاقات الائتمانية الخاصة بأستاذ جامعي في تلك الدولة عبر شبكة الإنترنت واستخدامها بصورة غير مشروعة في عمليات شراء وتسوق عبر شبكة الإنترنت وذلك بالتعاون مع أحد الأجانب من محترفي عمليات القرصنة على الشبكة (١١٩). وفي شمال شرق الولايات المتحدة الأمريكية أغلقت شركة ستزن بنك المصرفية ٨٨٠٠ حسابا مصرفيا من بطاقات ماستر كارد لاقتحامها من قبل بعض المخترقين (١٢٠).

وتوجد عدة طرق وأساليب يتمكن قراصنة الحاسب الآلي والإنترنت خلالها من الحصول على أرقام وبيانات البطاقات الائتمانية، وبالتالي استعمالها بصورة غير مشروعة، أشهرها (١٢١):

١. الاختراق الغير مشروع لمنظومة خطوط الاتصالات العالمية (١٢٢) Illegal access: يعد هذا الأسلوب من أخطر الأساليب التي تهدد عملية التسوق عبر شبكة الإنترنت، حيث يقوم المقتحم بتسخير كل خبراته وبرامجه لمحاولة اقتحام وفك رموز الشفرات وتجاوز جدر الحماية للملفات المتضمنة للمعلومات الشخصية للعملاء والمخزنة في الكمبيوتر الرئيسي عبر الشبكة العنكبوتية، والدافع الأساسي من اللجوء إليه يتمثل في الرغبة الكامنة في نفوس محترفي الإجرام التقني في قهر نظم التقنية والتفوق على الحماية وتعقيدها.

٢. الاستدراج أو الصيد Phishing: أخذت هذه التسمية من كلمة Fishing والتي تعني صيد السمك (١٢٣)، ويعتبر من أحدث الأساليب المستخدمة في جرائم الهاكرز عالميا ونسبة نجاحه ٥%. ويقوم هذا الأسلوب على نسخ موقع من مصدر موثوق به من مصرف على سبيل المثال، ثم يقوم المحتالين بإرسال وصلة إلى موقع إلكتروني آخر مخادع يطلبون فيه بعض المعلومات المهمة كالاسم ورقم الحساب المصرفي والرقم القومي واسم المستخدم وكلمة المرور من المستهلكين، ويقوم المستهلكون بالرد مقدمين تلك المعلومات، ليتم استخدامها بعد ذلك من قبل أولئك المحتالون في فتح حسابات مصرفية أو شراء سلع غالية الثمن كالمجوهرات والمواد الإلكترونية (١٢٤).

ومن أشهر الأمثلة على استخدام هذا الأسلوب في الحصول على أرقام وبيانات البطاقات الائتمانية المنقولة على شبكة الإنترنت، ما حصل عام ١٩٩٤ م عندما قام شخصان بإنشاء موقع على شبكة الإنترنت مخصص لشراء حاجات معينة يتم إرسالها فور تسديد قيمتها إلكترونيا، إلا أن الطلبات في حقيقة الواقع كانت لا تصل إلى الزبائن لأن الموقع ببساطة ما هو إلا موقع وهمي هدفه النصب والاحتيال (١٢٥). وفي أكتوبر ٢٠٠٣ م حكم على امرأة أمريكية الجنسية بسبب قيامها بإرسال رسائل مكثفة إلى مشتركي شركة AOL موهمة إياهم بأنها من قبل إدارة أمن الشركة وأن هناك مشكلة ما حصلت لهذه الشركة في سحب مبالغ مالية من بطاقات الائتمان للمرة الأخيرة التي قام بها الزبائن بالشراء، لذا يجب عليهم أن يملوا نموذج معين يحتوى على بيانات ومعلومات خاصة بالاسم ورقم بطاقة الائتمان وتاريخ انتهائها ورقمها السري. ولقد انطلت الحيلة على أكثر من شخص حتى أوقعها حظها العاثر مع أحد عملاء F.B.I المتخصص في جرائم الحاسب الآلي والإنترنت. وفي واقعة مماثلة رصد خبراء شبكة الإنترنت بمركز الأهرام للإدارة والحاسبات الإلكترونية بجمهورية مصر العربية "أماك" سيلا من الرسائل الإلكترونية الموجهة إلى مستخدمي الشبكة العنكبوتية بمصر تحمل أسماء العديد من البنوك الأجنبية، واسم البنك داخل الرسالة يتغير بطريقة عشوائية بين مجموعة من أسماء البنوك العالمية الكبرى، وتقول الرسالة " أنه نظرا للتحديث في نظم تطبيقات الحاسب الآلي بالبنك فنحن نطلب منك أن تزور الموقع التالي لكي تدخل بياناتك وهى رقم حسابك، اسمك، عنوانك، وإلا فإن نظم البنك سوف ترفض التعامل معك". وبفحص الرسالة من قبل خبراء أماك تبين أن العنوان المكتوب على الرسالة هو بالفعل عنوان حقيقي للبنك الذي يظهر شعاره مع الرسالة إلا أنه عند الوقوف بالفارة على هذا العنوان يظهر عنوان رقمي آخر، وأضاف الخبراء أنه عند تتبع هذا العنوان الرقمي أتضح أنه يوجد في إحدى الدول الأجنبية، وانتهي الخبراء إلى أن مصمم هذه الرسالة ما هو إلا محتال إلكتروني يهدف إلى الحصول على بعض المعلومات والبيانات المهمة واستخدامها بعد ذلك بصورة غير شرعية في إجراء عمليات مصرفية أو شراء سلع عبر شبكة الإنترنت (١٢٦).

٣. تقنية تفجير الموقع المستهدف: عادة يوجه هذا الأسلوب إلى الحاسبات الآلية المركزية (خادم الإنترنت) للبنوك والمؤسسات المالية والمطاعم والفنادق ووكالات السفر وذلك بهدف الحصول على أكبر قدر ممكن من أرقام البطاقات الائتمانية. ويقوم على ضخ مئات الآلف من الرسائل الإلكترونية من جهاز الحاسب الآلي الخاص بالمجرم إلى الجهاز المستهدف، بهدف التأثير على ما يعرف بالسعة التخزينية، بحيث يشكل هذا الكم الهائل من الرسائل ضغطا كبيرا على تلك الأجهزة، مما يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتت المعلومات والبيانات المخزنة فيه، لتنتقل بعد ذلك إلى الجهاز الخاص بالمجرم، أو تمكن هذا الأخير من حرية التجوال في الموقع المستهدف بسهولة ويسر وبالتالي الحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة ببطاقات الائتمان المملوكة للغير.

٤. أسلوب الخداع: يقوم على إنشاء مواقع وهمية (١٢٧) على شبكة الإنترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية التي توجد على الشبكة ويظهر وكأنه هو الموقع الأصلي التي يقدم الخدمة.ويكمن الخطر في استقبال الموقع الوهمي لجميع المعاملات المالية والبنكية والتجارية والتي يقدمها الموقع الأصلي عبر شبكة الإنترنت لأغراض التجارة الإلكترونية، وبالطبع أغلب هذه المعاملات تعتمد على البطاقات الائتمانية، مما يعني الحصول على المعلومات الخاصة بتلك البطاقات، هذه من جهة ومن جهة أخرى يتم في هذا الموقع الوهمي استقبال كافة الرسائل الإلكترونية

الخاصة بالموقع الأصلي والإطلاع عليها والاستفادة غير المشروعة من المعلومات الموجودة بها على نحو يضر بأصحاب المواقع الأصلية.ويزعزع الثقة بالتجارة الإلكترونية.

٥. تخليق أرقام البطاقات الائتمانية: يعرف هذا الأسلوب لدى مجرمي البطاقات بـ "Card Math" وهو يعتمد بالدرجة الأولى على إجراء معادلات رياضية وإحصائية بهدف تحصيل أو تخليق أرقام بطاقات ائتمانية مملوكة للغير. وهي كل ما يلزم للشراء عبر شبكة الإنترنت (١٢٨). ومن الأمثلة على استخدام هذا الأسلوب ما حصل بجمهورية مصر العربية حيث تمكنت الإدارة العامة لمباحث الأموال العامة من ضبط طالب جامعي بمدينة الإسكندرية بتهمة الاستيلاء على مبالغ طائلة من حسابات بعض البطاقات الائتمانية الخاصة بعملاء أحد البنوك بالجيزة عبر شبكة الإنترنت واستخدامها في عمليات الشراء والتسوق، بعدما تمكن من الحصول على أرقام تلك البطاقات باستخدام بعض المعادلات الحسابية الدقيقة (١٢٩). وعادة ما يقوم مجرموا البطاقات بنشر هذه المعادلات وبيان الكيفية التي يمكن من خلال إتباعها خطوة بخطوة الحصول على أرقام البطاقات الائتمانية المملوكة للغير عبر مواقعهم المنتشر على شبكة الإنترنت (١٣٠).

وللحد من ذلك قام العلماء باختراع بطاقة ائتمان جديدة لا تعمل إلا من خلال كلمة سر بصوت صاحبها، تعد أولى المحاولات من قبل العلماء بهدف مكافحة سرقة أرقام البطاقات الائتمانية خاصة تلك التي يتم تداولها عبر شبكة الإنترنت. ولمزيد من الأمان وحتى لا يعمد المجرم إلى تسجيل تلك البصمة ليستخدمها فيما بعد فإنها تتغير بعد كل مرة تستخدم فيها البطاقة بتتابع معين لا يعلمه إلا الحاسب الآلي (١٣١). ومن الوسائل التي ابتدعتها بعض الشركات لخداع القراصنة حتى تكون عملية الشراء عبر شبكة الإنترنت آمنه، تلك التي ابتدعها ستي بنك والمعروفة باسم الحساب المؤقت، حيث يسمح لعملائه بفتح حساب مؤقت للشراء عبر شبكة الإنترنت يمكن الحصول عليه بالتلفون أو البريد، يستخدم لمرة واحدة فقط ثم يلغى بعد ذلك، أو لأكثر من مرة بحيث يصل إلى سقف ائتماني محدد، وهو مرتبط بالحساب الأساسي للعميل (١٣٢).

٦. إن أحدث الطرق وأخطرها قيام الهاكر بالتنصت على سيل البيانات الإلكترونية بوقوفه في مكان متوسط بين عملاء معنيين والشركة المخاطبة لهم حيث يقوم بعد الاستيلاء على خط الاتصال المؤمن بينهم يقوم بدور الوسيط بين المتحادثيين من غير علم أي من الطرفين، وبذلك تصل إليه جميع المعلومات الحساسة ليستغلها كيفما يشاء. هذه باختصار أشهر الأساليب المستخدمة في قرصنة أرقام وبيانات البطاقات الائتمانية (١٣٣)، لتستخدم في النهاية في الإثراء غير المشروع على حساب تلك البطاقات (١٣٤).

ثانيا: أركان جريمة الاستيلاء على أرقام بطاقات الائتمان

لتحقق هذه الجريمة فإنه يشترط توافر ركنان مادي يتمثل في سلوك ونتيجة ورابطة سببية وركن معنوي وذلك على النحو التالي:

١. الركن المادي: يتكون الركن المادي في هذه الجريمة من ثلاثة عناصر: سلوك إجرامي يتمثل في النشاط المادي الصادر من الجاني سواء باختراق خطوط الاتصال العالمية أو بإنشاء المواقع الوهمية أو عن طريق التجسس وغيرها من الأساليب التي تتطور يوما بعد يوم، والجاني هنا ليس بحاجة إلى استعمال العنف لانتزاع الرقم أو المعلومة. ونتيجة

تتحقق بحصول الجاني على هذه الأرقام. ورابطة سببية بين النشاط الإجرامي والنتيجة. ويذهب بعض الفقهـــاء (١٣٥) إلى ضرورة وجود نشاط مادي بعد الاستيلاء على المال المعلوماتى كبيعه أو استعماله.

٢. الركن المعنوي: هذه الجريمة من الجرائم العمدية، التي تقوم على توافر القصد الجنائي، والقصد المطلوب هنا هـــو القصد العام بعنصرية العلم والإرادة، فالجاني وهو يقوم بعملية السطو على أرقام البطاقات الائتمانية لا بـــد وأن يكـــون عالما بأن هذه المعطيات مملوكة للغير ولا يجوز الاستيلاء عليها ومع ذلك يسعى وبإرادته إلى الاستحواذ عليها بقـــصد تملكها أو استعمالها فيما بعد بصورة غير مشروعة.

المبحث الثاني: الموقف التشريعي من هذه الجرائم

تمهيد وتقسيم

نظرا لما للاعتداء الواقع على التجارة الإلكترونية من أثر سيء على الاقتصاد العالمي، بات توفير الحماية الجنائية لها أمرا يفرضه الواقع والمستقبل على حدا سواء. لذا نجد غالبية الدول في المجتمع الدولي سارعت إلى الاهتمام بهذه التجارة المستحدثة، وفرض حمايتها الجنائية عليها. فكان للتشريعات الغربية موقف وللتشريعات العربية موقف.

أولا. الموقف في التشريعات الغربية

لقد تضمنت الكثير من التشريعات الغربية نصوصا خاصة تتعلق بالاستعمال التعسفي وغير المشروع للتواقيع الإلكترونية والبطاقات الائتمانية. والأمثلة التالية توضح ذلك:

١. الوضع في التشريع الأمريكي:

بالنسبة للتواقيع الإلكترونية فإن الولايات المتحدة الأمريكية تعد من أولى الدول التي أصدرت تشريعات تعترف بالتوقيع الإلكتروني وتمنحه حجية كاملة في الإثبات شأنه في ذلك شأن التوقيع التقليدي. وتوفير الحماية الجنائية له.

فقد أصدر الشارع الأمريكي في ٣٠ يونيه سنة ٢٠٠٠ قانونا اتحاديا "للتوقيع الإلكتروني العالمي والتجارة الوطنية" (١٣٦) أجاز بموجبه قبول واستخدام التوقيع والسجلات الإلكترونية في التعاملات التجارية الدولية وبين الولايات (١٣٧). وقد أبقى هذا القانون الاتحادي على كافة التشريعات الصادرة من الولايات للتوقيع والسجلات الإلكترونية، غير أنه في حال عدم صدور مثل هذه التشريعات فإن القانون الاتحادي للتوقيع الإلكتروني هو الذي يطبق. وهو ما يعني أن الغطاء التشريعي للمستندات الإلكترونية يمتد إلى كافة الولايات الأمريكية، حتى ولو لم تصدر قانونا خاصة به (١٣٨). وقد سبق القانون الاتحادي للتوقيع الإلكتروني جهودا تشريعية لإقرار التوقيع والسجلات الإلكترونية ومساواتها بالمستندات الكتابية، ومن هذه الجهود: القواعد الاتحادية للتوقيع والسجلات الإلكترونية الصادرة في ٢٠ مارس سنة ١٩٩٧ والتي وضعت لتطبيقها في مجال شركات الأجهزة والقانون الاتحادي للغذاء والدواء ومستحضرات التجميل (١٣٩) وقانون الخدمة الصحية العامة (١٤٠)، (١٤١).

وتعود الجهود التشريعية للتوقيع والسجلات الإلكترونية إلى ما طالب به ممثلو الصناعات الصيدلانية في سنة ١٩٩١ عن رغبتهم في استخدام البدائل الإلكترونية مثل تلك المحررة بخط اليد. وكان تبرير ذلك ما تحققه هذه الوسائل وخاصة في مجال حفظ السجلات من أهمية كبيرة لشركات التصنيع الصيدلاني. وقد أثمرت هذه الدعوة عن تشكيل مجموعة عمل تتحدد مهمتها في تنمية سياسة قبول التوقيع الإلكتروني من الهيئات. وقد وضعت مجموعة العمل تقريرا في يوليو سنة ١٩٩٢ اقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني؛ غير أنها في ٣١ أغسطس ١٩٩٤ أصدرت تقريرا وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية. كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في ٢٠ مارس سنة ١٩٩٧ لتطبق على شركات الأجهزة (١٤٢). كما صدر نموذج لقانون

المعاملات الإلكترونية الموحد (١٤٣)، وهو نموذج اختياري، وذلك بهدف توحيد القواعد التي تتصل بالمعاملات التجارية الإلكترونية بين تشريعات الولايات.

وإلى جانب هذه التشريع فإن هناك بعض التشريعات التي يكفل الحماية الجنائية للبيانات المخزنة إلكترونيا تضمنتها تشريعات اتحادية منها ما ينص عليه الفصل ١١٩ من القسم الأول من تقنين الولايات المتحدة سالف الذكر والذي يحمل عنوان "اعتراض وسائل الاتصالات السلكية والإلكترونية والشفهية" (١٤٤). أما على مستوى الولايات فقد أصدرت الكثير من الولايات الأمريكية تشريعات تتضمن وضع تنظيم للسجلات والتوقيع الإلكتروني. ويعد أول تشريع يصدر في هذا الموضوع هو "قانون المعاملات الإلكترونية الموحد (UETA) "Uniform Electronic Transaction Act" الذي أصدرته ولاية كاليفورنيا في ١٦ سبتمبر سنة ١٩٩٩ والذي دخل إلى حيز النفاذ في أول يناير سنة ٢٠٠٠ (١٤٥). وقانون المعاملات الإلكترونية الموحد (١٤٦) الذي أصدرته ولاية نورث كارولينا والذي دخل حيز النفاذ في الأول أكتوبر سنة ٢٠٠٠ (١٤٧). وهناك التشريع الذي أصدرته ولاية نيويورك في ٢٨ سبتمبر سنة ١٩٩٩ الخاص بالسجلات والتوقيع الإلكتروني (١٤٨)، وذلك بهدف تنظيم وتشجيع التعامل بالسجلات الإلكترونية وقبول التوقيع الإلكتروني في التعاملات التجارية (١٤٩). وقد كلف الشارع في ولاية نيويورك مكتب تقنيات الولاية (١٥٠) بوضع تقرير يتضمن وضع تنظيم ودليل عمل لأفضل السبل لإنشاء واستخدام وتخزين والمحافظة على التوقيع والسجلات الإلكترونية (المادة الثالثة من الفصل الرابع من هذا القانون). كذلك أصدرت ولاية كونتيكتكت قانونا للمعاملات الإلكترونية في فبراير سنة ٢٠٠٢ م ودخل حيز النفاذ في الأول من أكتوبر في ذات السنة (١٥١). كما أصدرت ولاية بنسلفانيا قانونا مماثلا في ١٦ ديسمبر سنة ١٩٩٩(١٥٢).

أما فيما يتعلق بحماية البطاقات الائتمانية فإنه يوجد في الولايات المتحدة الأمريكية منذ عام ١٩٨٤ م نصٌ خاصٌ تناول الاستعمال غير المشروع لبطاقات الائتمان (١٥٣) يجرم الاستعمال التعسفي للأدوات التي تسمح بالدخول إلى حساب بنكي ويمكن من خلاله الحصول على أموال أو أشياء أو خدمات أو أي شيء آخر له قيمه، أو يمكن استعماله من أجل إجراء تحويل للأموال. وتشمل الأدوات البطاقات المسروقة أو المفقودة أو تلك التي انتهت مدة صلاحيتها أو تم إلغاؤها. بالإضافة إلى تجريمه الاتجار في البطاقات غير المصرح باستعمالها، وكذلك تقليد وتزوير البطاقات الائتمانية. وفي عام ١٩٩٤ م عدل هذا النص بإضافة جريمة أخرى إليه تتمثل في حيازة الأجهزه التي تساعد على تقليد وتزوير البطاقات الائتمانية متى ارتبط ذلك بنية غير مشروعة (١٥٤).

وفيما يتعلق بالنشر غير المشروع لأرقام البطاقات الائتمانية والبيانات والمعلومات الخاصة بها عبر شبكة الإنترنت، فقد جرّمها القانون الفيدرالي للاحتيال عبر وسائل الاتصال، الذي جرّم النقل غير المصرح به للمعلومات أو الإشارات أو العلامات أو الصور أو التسجيلات الصوتية عبر أي من وسائل الاتصالات (١٥٥). وإزاء انتشار هذه الظاهرة في العديد من الولايات الأمريكية، تقدم السناتور الديمقراطي رياني فينشتين عضو مجلس الشيوخ عن ولاية كاليفورنيا بمشروع قانون إلى المجلس يطالب فيه شركات إصدار البطاقات الائتمانية في مختلف أنحاء البلاد بإخطار عملائها عن أي اختراق لسجلاتها المخزنة أو ملفاتها المشفرة. وتناول المشروع أيضا فكرة استحداث مكتب خاص بجرائم سرقة الهوية يتبع المفوضية الفيدرالية للتجارة في الولايات المتحدة الأمريكية، كما دعا المشروع إلى ضرورة التحقق من

هوية أي طرف ثالث يريد الدخول على معلومات شخصية خاصة بمواطنين أمريكيين، وتطـوير آليـة معينـة تمكـن المختصين من التعرف على هذا الطرف وتعقبه (١٥٦). وفي ولاية ماسوشو ستس يجري حاليا بحث ومناقشة قـانون يسمح للمستهلك بتجميد حسابه الائتماني، ومنع أي طرف ثالث من الإطلاع على السجلات الخاصة بالمعـاملات التـي تجري من خلال هذا الحساب، حيث تظل هذه السجلات محصورة بين المستهلك وبين الجهة التي يتعامل معها بواسطة بطاقته الائتمانية فقط. كما يمنع هذا القانون من فتح حساب جديد باسم الشخص الذي طلب تجميد حسابه (١٥٧).

٢. الوضع في التشريع الفرنسي:

بتاريخ ١٣ /٢٠٠٠/٣ م أصدرت فرنسا قانونا خاصا بالتوقيع الإلكتروني رقم ٢٣٠ لسنة ٢٠٠٠ م في صورة تعـديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متوافقة مع تقنيات المعلوماتية، وكثرة استخدام التوقيع الإلكتروني في المعاملات الإلكترونية. وقد أدرج هذا التعديل في نص المادة ١٣١٦ من القانون المدني الفرنـسي فـي ست فقرات. ولقد كرس هذا القانون مبدأين أساسين: الأول ينصرف إلى عدم التميز بين الكتابة المعدة للإثبـات بـسبب الدعامة التي تتم عليها و الوسيط الذي تتم من خلاله، والثاني ينصرف إلى المساواة الوظيفية بين المحـرر الإلكترونـي والتوقيع الإلكتروني وبين المحرر العرفي والتوقيع التقليدي (١٥٨).

وبصدور قانون العقوبات الفرنسي الجديد عام ١٩٩٢ م، والمطبق بدءًا من أول مارس ١٩٩٤ م جُرّم التزوير فـي المحررات الرسمية أو العرفية، والذي يقع بأي طريقة، على خلاف قانون العقوبات الفرنسي القديم، بموجب نص خاص هو نص المادة ٤٤١ التي حلت محل المواد ١٤٥-١٥٢ وأصبح ذلك النص بعموميتـه يغطـي التزويـر المعلومـاتى والتزوير بالطرق التقليدية (١٥٩)، حيث نصت الفقرة الأولي من المادة ٤٤١ على أنه " يعد تزويرا كل تغيير تدليـسي للحقيقة، يكون من شأنه أن يحدث ضررا، ويقع بأي وسيلة كانت ، سواء وقع في محرر أو سند معبرا عن الـرأي أيـا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين . ويعاقب على التزوير واستعمال المحرر المزور بالسجن ثلاث سنوات وبالغرامة التي لا تتجاوز ٣٠٠,٠٠٠ يورو".

والواضح من النص السابق أن المشرع الفرنسي أقلع عن الإشارة لتحديد طريقة معينة للتزوير حيث ذكر عبـارة " أي وسيلة" "Par quelques moyen" والعلة في ذلك تكمن في رغبته في أن يكون النص السابق نصا عاما يـستغرق التزوير بكل وسائله العادية مادي أو معنوي، بطريق التقليد أو الاصطناع أو تغير إقرار أولى الشأن وفي الوقت نفـسه يشمل صور التزوير المعلوماتى (١٦٠). بالإضافة إلى النص السابق والذي وفر المشرع الفرنسي من خلالـه الحمايـة الجنائية للمستندات الإلكترونية من التزوير، نجده في جانب آخر يوفر حماية جنائية للمواقع الإلكترونية ومحتوياتها حيث جرم العديد من الأفعال كالدخول غير المشروع على مواقع الإنترنت، وإعاقة تشغيل نظام المعالجة الآلية للمعلومـات، وتدمير البيانات والمعطيات الإلكترونية (١٦١).

وفي جانب آخر نجده يقرر حماية جنائية خاصة لبطاقات الائتمان بموجب القانون رقـم ١٣٨٣-٩١ المـؤرخ فـي ١٩٩١/١٢/٣٠ م في المادة ١١ منه والتي عدلت المادة ٦٧ من المرسوم بقانون الصادر في ١٩٣٥/١٠/٣٠ م لتضيف مادتين هما ١/٦٧ و ٢/٦٧ وذلك بعد المادة ٦٧ من المرسوم بقانون آنف الذكر. حيث جرّمت المادة ١/٦٧ ثلاث جرائم

تتعلق بالبطاقات الائتمانية هي: الأولى تقليد أو تزوير بطاقة وفاء أو سحب، والثانية استعمال أو محاولة استعمال لبطاقة وفاء أو سحب مقلدة أو مزورة مع العلم بذلك، والثالثة قبول الدفع عن طريق الوفاء ببطاقة مقلدة أو مزورة وهو على علم بذلك. في حين أن المادة ٢/٦٧ نصت على وجوب مصادرة وتدمير البطاقات المقلدة ومصادرة الأدوات التي استخدمت أو المعدة للاستخدام في التزوير أو التقليد إلا إذا استخدمت بدون علم مالكها (١٦٢).

ثانيا. الموقف في التشريعات العربية

نظرا لما تمثله التجارة الإلكترونية من أهمية كبرى في عصر عرف بعصر المعلومات والاتصالات سارعت الكثير من الدول العربية إلى توفير الحماية الجنائية لهذه التجارة من الاعتداءات التي قد تتعرض لها، وفيما يلي بيان لبعض الأمثلة:

١. الوضع في التشريع المصري:

بصدور قانون تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ٢٠٠٤/١٥ م وفر المشرع المصري بعض الحماية للتجارة الإلكترونية من خلال تجريمه لبعض الانتهاكات التي يتعرض لها التوقيع الإلكتروني، حيث نصت المادة ٢٣ من القانون على " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة الآلف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كلا من:

ب. أتلف أو عيّب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيا من ذلك بطريق الاصطناع أو التعديل أو التحويل أو بأي طريق آخر.

ك. توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو أعترضه أو عطله عن أداء وظيفته.

ويلاحظ من صياغة النص السابق أن المشرع المصري يجرم نوعين من الانتهاكات الواقعة ضد التواقيع والمستندات الإلكترونية، الأول وهو الإتلاف والتزوير في المجال المعلوماتى، والثاني هو الحصول وبدون وجه حق على المستندات والتواقيع الإلكترونية. وكلتا الحالتين اعتبرهما المشرع وحسنا فعل من جرائم الخطر التي لا يتوقف تجريم السلوك فيها على تحقق نتيجة معين. أيضا من الملاحظ أن طرق التزوير الواردة في الفقرة (ب) من المادة سالفة الذكر جاءت على سبيل المثال وليس الحصر بدليل أن المشرع وفي نهاية هذه الفقرة أورد عبارة " بأي طريق آخر". والجرائم السابقة وبصريح النص القانوني هي من الجرائم العمدية التي لا يتصور ارتكابها بطريق الخطأ، والقصد الجنائي فيها هو العام بعنصريه العلم والإرادة.

أما فيما يتعلق بالاعتداء على المواقع الإلكترونية وأسماءها فإننا نلاحظ خلو القانون السالف الذكر وكذلك المدونة العقابية المصرية من أي نص يجرم ذلك. لذلك نرى أنه من الضرورة بمكان شمولها بالحماية اللازمة مثلها مثل المستندات والتواقيع الإلكترونية. وبالنسبة لجريمة السطو على أرقام البطاقات الائتمانية وهي إحدى الجرائم التي تهدد

التجارة الإلكترونية فإننا نلاحظ أن النصوص المستحدثة الواردة في قانون الجزاء العماني (١٦٣) أو قانون مكافحة جرائم تقنية المعلومات الإماراتي ٢٠٠٦/٢ م (١٦٤) أو قانون العقوبات القطري ٢٠٠٤/١١ م (١٦٥) والتي تنطبق تماما على شبكة الإنترنت، لا يوجد لها نظير في التشريع المصري، حيث لم يرد في التشريع المصري ما يخص هذه الجريمة وبالتالي فلا مناص هنا من الرجوع إلى النصوص التقليدية الواردة في قانون العقوبات كنصوص تجريم السرقة أو النصب أو الاختلاس. إزاء ذلك كان على المشرع المصري في ظل هذه الطفرة المعلوماتية وحتى يكون بمنأى عن القياس الذي يتعارض مع مبدأ المشروعية وليتجنب مشقة تطويع النصوص القانونية التقليدية. أن يلحق بالركب ويستحدث نصوصاً تجرم السطو على أرقام البطاقات الائتمانية.

٢. الموقف في التشريع العماني:

ثمة نقاش فقهي عام يدور لمعرفة ما إذا كانت النصوص التقليدية لجريمة التزوير بالمفهوم الكلاسيكي صالحة للتطبيق في المجال المعلوماتى (١٦٦)، وإزاء ذلك ولسد الفراغ التشريعي وللخروج من دائرة هذا الخلاف والنقاش ولينأ عن اللجوء إلى القياس الذي يتعارض مع مبدأ الشرعية، أوجد المشرع العماني حلا تشريعيا لذلك، حيث جرّم التزوير المعلوماتى بنص مستحدث خاص به، فالبند الخامس من المادة ٢٧٦ مكرر نص على "" يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب إحدى الأفعال التالية:..... ٥- تزوير بيانات أو وثائق مبرمجة أيا كان شكلها "".

والواضح من النص السابق أن المشرع العماني في تجريمه لهذا السلوك الإجرامي لم يحدد الجهة التي يتبع لها معالجة البيانات و لم يضع شروطا تتعلق بطبيعة البيانات و المعلومات محل التزوير بدليل أنه أورد عبارة "" أيا كان شكلها "" في نهاية النص، كما أنه لم يشترط تبعيتها لجهة معينة، وإنما جاء النص عاما ليشمل كافة أنواع المعلومات والبيانات بما فيها التواقيع الإلكترونية سواء أكانت تابعة لجهة حكومية أو خاصة هذا من ناحية. ومن ناحية أخرى لم يحدد وسائل معينة تتم بها عملية التزوير المعلوماتى، مما يعني أن النص يتسع ليشمل كافة الطرق الفنية والتقنية المستخدمة في تزوير المستندات والمعلومات.

ومن ناحية ثالثة نجد أن الجريمة تقوم بمجرد القيام بالسلوك الإجرامي، حيث أن المشرع العماني وحسن فعل لم يشترط تحقق نتيجة معينة كأثر لعملية التزوير كما وأن العقاب على التزوير هنا لم يرتبط بحدوث الدخول غير المصرح به إلى نظام الحاسب الآلي. وهذه الجريمة وكما هو واضح من سياق النص السابق تعد من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي. والقصد المقصود هنا هو العام بعنصرية العلم والإرادة – علم الجاني بأنه يقوم بتزوير أحد البيانات أو المستندات الإلكترونية، وأن تتجه إرادته إلى ذلك – وليس الخاص كبعض التشريعات مثل القانون القطري (١٦٧) الذي اشترط أن تتجه إرادة المجني إلى الإضرار بالغير.

ومن حيث العقوبة نجد أن المشرع قرر لهذه الجريمة نوعين من العقوبة سالبة للحرية وهي الحبس بحد أدني ثلاثة أشهر وحد أقصي سنتين، ومالية تتمثل في الغرامة بحد أدني مائة ريال وحد أقصي خمسمائة ريال، والأصل العام هو أن يتم الحكم بالعقوبتين معا والاستثناء هو الحكم بإحداهن. وتضاعف العقوبة في حالة أن الجاني كان من مستخدمي

الحاسب الآلي. بالإضافة إلى النص السبق الوارد في قانون الجزاء العماني، توجد بعض النصوص في مشروع قانون المعاملات والتجارة الإلكترونية العماني وهى: المادة ٧٨ التي تعاقب بالحبس حتى سنتين والغرامة ٥٠٠٠ ريال عماني كل من يقوم بإجراء تعديلاً غير مشروع في محتويات الحاسب الآلي يترتب عليه إضعاف فعاليته أو يمنع أو يعوق الدخول إلى البرنامج أو البيانات الموجودة به أو يضعف فعالية البرنامج أو الاعتماد على البيانات.

وهناك المادة ٧٩ التي تعاقب كل من يخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة انترنت ويترتب على فعله تعطيل الأنظمة أو إتلاف البرامج ومحتوياتها أو سرقة المعلومات أو استخدامها في أغراض غير مشروعة أو إدخال معلومات وهمية وغير صحيحة بالحبس حتى خمس سنوات أو غرامة تصل إلى ٦٠٠٠ ريال عماني، وفي حالة العود يعاقب بالعقوبتين معاً.

أما بالنسبة للانتهاكات التي تتعرض لها المواقع الإلكترونية وأسماءها فإنه وكما هو الحال في التشريعين القطري والمصري لا يوجد نص يجرّمها على عكس ما ذهب إليه المشرع الإماراتي في المادة ١٤ من قانون ٢٠٠٦/٢ م ، لذا كان الأحرى بالمشرع العماني تجريمها ليوفر أقصي حماية ممكنة للتجارة الإلكترونية.

وبخصوص الاعتداء الواقع على بطاقات الدفع الإلكتروني بما فيها البطاقات الائتمانية وما له من أثر سلبي على العمليات المصرفية وعلى الاقتصاد الوطني وزعزعة الثقة بهما، فإننا نجد أن الشارع العماني قد سارع إلى فرض حمايته الجنائية لهذه البطاقات من أي إساءة في استخدامها أو أي اعتداء يقع عليها وعلى المعلومات والبيانات الخاصة بها سواء كان من قبل الغير أو من قبل الحامل الشرعي للبطاقة، وسواء كان الاعتداء بالطرق التقليدية أو بالطرق المستحدثة. وذلك من خلال استحداثه لمجموعة من النصوص في مدونته العقابية (١٦٨). فالمادة المادة (٢٧٦) مكرراً (٣) تنص على أن " يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تجاوز ألف ريال كل من:

١- قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب

٢- استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك

٣- قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك.

وتنص المادة (٢٧٦) مكرراً (٤) على انه " يعاقب بالسجن مدة لا تزيد على ٣ سنوات وبغرامة لا تجاوز خمسمائة ريال كل من:

١- استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له

٢- استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك

٣- استعمل بطاقة الغير بدون علمه

ويؤخذ على المشرع هنا تقيده باصطلاحات مقيدة في حين كان يمكنه أن يكون أكثر اتساعا حين يجرم صور الاعتداء المذكورة على كل أنواع البطاقات منعا للدفع بان البطاقة محل الاعتداء ليست بطاقة وفاء (١٦٩). بالإضافة إلى النصوص السابقة نجد أن القانون العماني يجرّم عملية الاستيلاء على أرقام وبيانات ومعلومات البطاقات الائتمانية

بنصوص أخرى مستحدثة وإن لم ينص على ذلك صراحة: فمن جهة أولى نجده في المادة ٢٧٦ مكرر – إحدى النصوص المستحدثة – ينص على معاقبة كل من يتعمد استخدام الحاسب الآلي في ارتكاب أفعال معينة حددها على سبيل الحصر ذكر منها " الالتقاط غير المشروع للمعلومات أو البيانات، والتجسس والتصنت عليها وانتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وجمع المعلومات عنهم والبيانات وإعادة استخدامها بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال. والنص السابق ينطبق دون أدنى شك على الفعل الإجرامي مدار الحديث، فهو يتم عن طريق الالتقاط غير المشروع للمعلومات والبيانات المتعلقة بالبطاقات الائتمانية أو عن طريق التجسس والتصنت عليها باستخدام بعض التقنيات الفنية التي أصبحت تتم بشكل كبير عبر شبكة الإنترنت، أضف إلى ذلك أن هذا الفعل في حد ذاته يشكل اعتداءا صريحا على خصوصيات الغير وعلى حقهم في الاحتفاظ بأسرارهم الخاصة بالبطاقات الائتمانية التي تعد من أهم الأسرار الخاصة التي لا يجوز الإطلاع عليها بأي وجه دون إذن صاحبها. أضف إلى ذلك أنه في أغلب الأحيان يتم إعادة استخدام تلك المعطيات المتحصل عليها بطريقة غير مشروعة مرة أخرى في التسوق عبر شبكة الإنترنت أو من أجل ابتزاز أصحابها أو المؤسسات المالية التي أصدرتها (١٧٠).

ومن جهة ثانية نجد أن المادة ٢٧٦ مكررا (١) – نص مستحدث– من ذات القانون نصت على معاقبة كل من يستولي أو يحصل بطريقة غير مشروعة على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات بالسجن مدة لا تقل عن ستة أشهر ولا تزيد عن سنتين وبغرامة لا تقل عن مائة ريال ولا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين. وإذا رجعنا إلى جريمة السطو على المعلومات والأرقام الخاصة بالبطاقات الائتمانية لوجدناها في الأساس عبارة عن عملية استيلاء وحصول على معلومات وبيانات مملوكة للغير تتم بطريقة غير مشروعة . بالإضافة إلى أن تلك المعطيات يتم الاستيلاء عليها إما وهي منقولة أثناء عملية التسوق عبر شبكة الإنترنت أو عن طريق التجسس والاختراق فيما لو كانت مخزنة في جهاز الحاسب الآلي الخاص بالضحية سواء أكان الضحية فردا عاديا أو مؤسسة مالية.

بالإضافة إلى النص السابق الوارد في قانون الجزاء العماني، يوجد نص خاص بهذه الجريمة في مشروع قانون المعاملات والتجارة الإلكترونية العماني وهو نص المادة ٧٩ التي تعاقب كل من يخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة انترنت ويترتب على فعله تعطيل الأنظمة أو إتلاف البرامج ومحتوياتها أو سرقة المعلومات أو استخدامها في أغراض غير مشروعة أو إدخال معلومات وهمية وغير صحيحة بالحبس حتى خمس سنوات أو غرامة تصل إلى ٦٠٠٠ ريال عماني وفي حالة العود يعاقب بالعقوبتين معاً.

المراجع

(١) صدر هذا القانون في ٢٠٠٠/٨/٩ م منشور في الرائد الرسمي للجمهورية التونسية ٢٠٠٠/٨/١١ م.

(٢) المادة الثانية من قانون المعاملات والتجارة الإلكترونية رقم (٢) لسنة ٢٠٠٢ بإمارة دبي.

(٣) الدكتور/ عبد الفتاح بيومي حجازي: مقدمة في التجارة الإلكترونية العربية "ج ١"، دار الفكر الجامعي، الإسكندرية ٢٠٠٢ ص ١٨.

(٤) الدكتور/ أسامة مجاهد: خصوصية التعاقد بطريق الإنترنت، بحث مقدم لمؤتمر القانون و الكمبيوتر و الإنترنت، جامعة الإمارات ٢٠٠٠ م ص ٣٦.

(٥) نظر في ذلك: الدكتور. محمد أبو العلا عقيدة: الحماية الجنائية للتجارة الإلكترونية، بحث مقدم إلى مؤتمر مكافحة جرائم تقنية المعلومات (التشريع والتطبيق)، جامعة الشارقة، كلية الشريعة والقانون ٢٦-٣٠ نوفمبر ٢٠٠٦ م & بهاء شاهين: العولمة و التجارة الإلكترونية، الفاروق الحديثة للطباعة والنشر، القاهرة ٢٠٠٠ م ص ٦٢-٦٣ & مراد شلباية؛ وائل أبو مغلي؛ ماهر جابر، المرجع السابق ٣٢-٣٣ & التجارة الإلكترونية، موضوع منشور على الإنترنت من خلال موقع (www.c4arab.com).

(٦) بهاء شاهين: المرجع السابق ص ٦٢-٦٣.

(٧) الدكتور/ حمدي عبد العظيم، الجهود الدولية لمكافحة غسل الأموال- ورقة عمل قدمت للندوة التي نظمها مركز الخليج للدراسات الإستراتيجية بالقاهرة بتاريخ ٢٠٠٠/١٠/٣٠ م والتي كانت بعنوان غسل الأموال وقائمة الجنات الضريبية، ص ٥٢.

(٨) محمد بن أحمد بن سنجور البلوشي: مزايا شبكة الإنترنت و سلبيات، مقال منشور على مجلة البحرية اليوم العدد ٣٨ ديسمبر ٢٠٠٢ م ص ٣٠.

(٩) الدكتور/ محمد المرسي زهرة: الدليل الكتابي وحجية مخرجات الكمبيوتر في الإثبات في المواد المدنية والتجارية: بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة المنعقد في الفترة من ١-٣/ ٥/٢٠٠٠ م ص ١١٤.

(١٠) مجموعة أحكام النفض في ١٩٧٨/١/١٣ م السنة ٢٩ ص ٣٥٧.

(١١) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة ٢٠٠٥ م ص ٢٣٥.

(١٢) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٣٥.

(١٣) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٣٥.

(١٤)

La loi no 2000-2230 du 13 mars 2000, J.O.14 mars 2000.P.3986.J.C.P.2000,III , 20259.

(١٥)

"an electronic sound, symbol, or process" that is attached to or logically associated with" a contract or other record, and that is "executed or adopted by a person with the intent to sign the record. "E-Sign Law 106(5). Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 11.

(١٦) التوقيع الإلكتروني لولاية كانسس يعني صوتا أو رمزا أو معالجة إلكترونية مرفقة بسجل أو متحـــدة بـــه ويـــتم إجرائها أو إقرارها من شخص مصحوبة بنية التوقيع على السجل.
An act concerning the Connecticut uniform electronic transactions, op-cit.

(١٧)

"Electronic signature" shall mean an electronic identifier, including with out limitation a digital signature, which is unique to the person using it, capable of verification, under the sole control of the person using it, attached to or associated with data in such a manner that authenticates the attachment of the signature to particular data and the integrity of the data transmitted, and intended by the party using it to have the same force and effect as the use of a signature affixed by hand". ESRA 102 (3). Report to the Governor and Legislature, p. 7 note 3.

(١٨)

Electronic signature shall mean an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."Laws of 2002, Chapter 314, 2
Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 7 note 4.

(١٩)

"Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". Statutory Instrument 2002 No. 318, The Electronic Signatures Regulations 2002, op-cit.

(٢٠)

Draft of a Law on the Framework Conditions, 2 (2), P. 4.

(٢١)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p.7.

(٢٢) أنظر مثال على ذلك قانون التوقيع والسجلات الإلكترونية لولاية نيويورك الذي يعهد لمكتب تقنيات الولاية بالحق في إختيار وسيلة التوقيع الإلكتروني بالنسبة للأجهزة الحكومية.
Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 7-8.

(٢٣)

Draft of a Law on the Framework Conditions, 2 (2), p.4.

(٢٤) أنظر الجريدة الرسمية: العدد ١٧ تابع (د) الصادر في ٢٠٠٤/٤/٢٢ م.

(٢٥)

DAVIO (E), internet face au droit ,cohiers du C.R.I.D 12 é d . story – scientica, 1997 , P. 80.

(٢٦) الدكتور/ ثروت عبد الحميد: التوقيع الإلكتروني "ط ٢"، مكتبة الجلاء، المنصورة ٢٠٠٢-٢٠٠٣ ص ٥٠.

(٢٧) الدكتور/ ممدوح محمد على مبروك: مدي حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربيـــة، القـــاهرة ٢٠٠٥ ص ٨.

(٢٨) الدكتور/ عبد الحميد عثمان: مسئولية مزود الخدمة المعلوماتية في القانون البحريني ورقة عمل مقدمة لورشة العمل " المعاملات الرقمية " والتي نظمتها المنظمة العربية للتنمية الإدارية بمدينة شرم الشيخ بجمهورية مصر العربية في الفترة من ٥-٢/٩ ٢٠٠٦ م.

(٢٩) إبراهيم الدسوقي أبو الليل: الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت ٢٠٠٣ م ص ١٥٨.

(٣٠) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٣٩.

(٣١) الدكتور/ ممدوح محمد علي مبروك: المرجع السابق ص ١٢& محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٣٩.

(٣٢) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٣٩.

(٣٣) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٤٠.

(٣٤) المفتاح العام عبارة عن أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني، وللتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي. أنظر الدكتور/ ممدوح محمد على مبروك، المرجع السابق ص ١٧.

(٣٥) المفتاح الخاص عبارة أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية، ويتم الاحتفاظ بها في بطاقة ذكية مؤمنة . أنظر الدكتور. ممدوح محمد على مبروك: المرجع السابق ص ١٨.

(٣٦) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٤١.

(٣٧) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق ص ٢٤١.

(٣٨) تعتبر شهادة التصديق الإلكتروني ضمانا لعدم إنكار أحد الطرفين توقيع الوثيقة المرسلة إلكترونية، ودلالة واضحة على أن الموقع يملك المفتاح الخاص، وبالتالي فهو الذي قام بالتوقيع.

(٣٩) التوقيع الإلكتروني خطوة إلى الأمام Electronic Signature: مقال منشور على شبكة الإنترنت بتاريخ ١٥/٦/٢٠٠٦ م.

http://www.egovs.com/egovs_webo2/news.php?main=7&detailsid=22.

(٤٠) التوقيع الإلكتروني خطوة إلى الأمام Electronic Signature: مرجع سابق.

(٤١)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 9.

(٤٢)

Gibbs and Mazan, op-cit.

(٤٣)

ABA Section Creates First Digital Signature Guidelines To Aid In Security Of The Internet, 1996
http:/www.abanet.org/media/home.html

(٤٤)

ABA Section Creates First Digital Signature Guidelines op-cit

(٤٥)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 9. 12-13.

(٤٦)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 13.

(٤٧)

"Personal Identification Number (PIN) or password".

(٤٨)

"Shared Secret".

(٤٩)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 14.

(٥٠) الدكتور/ عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة ٢٠٠٢ م ص ١٧٠.

(٥١) الدكتور/ عبد الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية ص ٣٠٦.

(٥٢) يقصد بالنظام المعلوماتى: البيانات أو المعلومات التي تم معالجتها بعد إتباع طرق وإجراءات إلكترونية معينه، فصارات برنامجا تطبيقيا تم تحميله على جهاز الحاسب الآلي من أجل تشغيله والحصول على نتائج معينة خاصة بالتوقيع الإلكتروني كذلك. في حين يقصد بقاعدة البيانات: البيانات المخزنة عن موضوع ما، داخل الحاسب الآلي، أو على قرص منفصل، من ذلك البيانات المتعلقة باسم صاحب التوقيع، ومهنته وكافة بياناته الشخصية وكافة المعلومات المتعلقة بذلك التوقيع والتي يفترض سريتها أنظر: الدكتور. عبد الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها الجنائية، المرجع السابق ص ٢٩٦-٢٩٧.

(٥٣) الدكتور/ عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني " حكمها في الإسلام وطرق مكافحتها"، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب – جدة ٢٠٠٤ م ص ١٢.

(٥٤) الدكتور:عمر محمد أبو بكر بن يونس: الأيكان، دراسة تم عرضها في محاضرة في ندوة تأثير محركات البحث عن إدارة الإنترنت – الإسكندرية ٣١ يوليو-٤ أغسطس ٢٠٠٥ م، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية. ص ٢٢.

(٥٥)

Le Monde Edition Proche – Orient , 26 November 1999, Supplement le Monde Interactif , Sabir cyber , P V.

(٥٦) الدكتور/عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت ، المرجع السابق، ص ٤٧.

(٥٧)

American Net working , inc vs. , access America / Connect Atlanta , inc . 96 . civ . 6823 (lls) August 13 1997.p 1.

(٥٨)

Katyal) Navin – The Un authorized dissemination of celebrity image on the internet , p 2 –) Tulan Journal of technology & intellectual property , vol . 2 Issue 1 Spring 2000 Available on line in aug 2000. www.law.tulane.edu/journals/jtip/v211/index.html.

(٥٩)

see Lind Harrading – The automated lawyer : The impact of computers on the legal profession computer and the law Hawardl .Meyer December 2 ,1996 available on line in Feb 2001 at http://wings.buffalo.edu/law/complaw.

(٦٠) بروتوكول نقل الربط الفائق Hypertext Transfer Protocol وهو بروتوكول يربط مواقع الويب الموصولة بشبكة الإنترنت فيما بينها ويسمح بالاتصال بها والتجول في عمقها باستخدام نظام الوصلات الفائقة . أنظر الدكتور طوني . ميشال عيسي: المرجع السابق ٥١٠.

(٦١) الدكتور: طوني ميشال عيسي – المرجع السابق ص ٦٠.

(٦٢) بدأت تدخل فكرة Domain Name في منتصف الثمانيات. وكان أول عنوان إلكتروني يتم تسجيله عن symbplics.com أنظر في ذلك:

Real – life Corpoate Domain Name Challenges, Issues and strategic Solution Available at: www.verisign.com

(٦٣)

Richard Milchir (M), Marques et Noms de domaine de quelques problemes actuels .lamy droit commercial.no 135 . juillet .2000.Bulletin d'actualite.p2

(٦٤) كتابة أسماء النطاقات بالحروف اللاتينية يشكل عائقا كبيرا أمام المستخدمين من غير المتحدثين باللغة الإنجليزية خاصة الدول العربية. إذ يجد الكثيرون صعوبة في التعامل مع هذه اللغة المهيمنة حاليا على شبكة الإنترنت. وهنا تبرز أهمية إيجاد الحلول والتقنيات اللازمة التي تمكننا كعرب من الاستفادة القصوى من الإنترنت، ومن ذلك تعريب الإنترنت وزيادة المحتوى العربي فيها، ويشمل ذلك تعريب أسماء المواقع حتى يتمكن المستخدم العربي من الوصول إلى المعلومة باستخدام أسماء نطاقات عربية. من هذا المنطلق قامت مجموعة عمل أسماء عناوين نطاقات الإنترنت بدول الخليج المنبثقة من لجنة تقنية المعلومات التابعة للأمانة العامة لمجلس التعاون لدول الخليج العربية في اجتماعها المنعقد بتاريخ ٢٠٠٤/٣/٧ م بتأسيس فريق عمل خليجي لتنفيذ مشروع تجريبي لدعم استخدام اللغة العربية في أسماء النطاقات على شبكة الإنترنت، ويضم هذا الفريق ممثلين من مراكز تسجيل أسماء النطاقات في دول الخليج العربية وهي: المركز السعودي لمعلومات الشبكة، مركز الإمارات لمعلومات الشبكة، وزارة المواصلات البحرينية، شركة اتصالات قطر، وزارة المواصلات الكويتية، الشركة العمانية للاتصالات. وقد تم الانتهاء من تجهيز الخدمات الرئيسية لأسماء النطاقات العربية في كل من المملكة العربية السعودية، دولة الإمارات العربية المتحدة، دولة قطر، وتم تسجيل عدة نطاقات باللغة العربية لغرض التجريب منها: (موقع. السعودية، موقع. امارات ، موقع. قطر).

(٦٥) الدكتور/ عمر محمد أبو بكر بن يونس: الايكان، المرجع السابق ص ٢٢.

(٦٦) حول هذا التعريف أنظر: الدكتور. محمد حسام محمود لطفي: المشكلات القانونية في مجال المعلوماتية " خواطر وتأملات"، بحث مقدم إلى مؤتمر تحديات حماية الملكية الفكرية من منظور عربي ودولي والذي عقد في القاهرة في الفترة من ٢١-٢٣/٣/ ١٩٩٧ م وذلك برعاية الجمعية المصرية لحماية الملكية الصناعية والجمعية الدولية لحماية الملكية الصناعية ص ٩٤.

(٦٧)

Larrffeu (J.), Protection d'une marque renommee contre le cyberpritage, Expertises,Aout et September 1999,p.260.

(٦٨)

Bucki(c.) , le conflit enter marque et nom de domaine , 2000, Revue du droit de la propriete intellecuelle,2000, Fase 112, p.9.

(٦٩) الدكتور/ شريف محمد غنام: حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني – دار النهضة العربية القاهرة – ص ١٤.

(٧٠) الدكتور/ عمر محمد أبو بكر بن يونس: الايكان، المرجع السابق ص ٢٢.

(٧١) الدكتور: شريف محمد غنام – المرجع السابق ص ١٦.

(٧٢) وفقا لبعض الإحصاءات التي تبين استخدام الإنترنت في العالم العربي، أن هناك نسبة ٦٤% من إجمالي الشركات المشتركة في خدمة الإنترنت تستخدم الشبكة كوسيلة للإعلان عنها. ويتمثل الاستخدام الرئيسي لمواقع هذه الشركات عبر الشبكة في عرض البيانات الرئيسية عنها مثل عنوان الشركة وطبيعة نشاطها وأرقام هواتفها وفاكساتها وبريدها العادي والإلكتروني. لمزيد من الإيضاح حيال هذا الموضوع أنظر: مهندس: رأفت رضوان – اتجاهات مجتمع الأعمال العربي نحو التجارة الإلكترونية – بدون ناشر– ١٩٩٩ م ص ٢٤٥.

(٧٣) تقضي هذه القاعدة بأنه لا يجوز لأكثر من مشروع أن يكون له نفس العنوان الإلكتروني ومن ثم يكون لكل مشروع عنوان إلكتروني واحد يميزه عن غيره من المشروعات.

(٧٤) للاستزادة حول هذا الموضوع راجع:

– الدكتور : شريف محمد غنام – المرجع السابق ص ١١–١٢

– الدكتور طوني ميشال عيسي – المرجع السابق ص ٦٤

– ناتالي بورين؛ ايمانويل جيز : أسماء مواقع الإنترنت ، مكتبة صادر ناشرون ، لبنان ٢٠٠٤ م ص ٦–٩

– الدكتور/ يونس عرب: الملكية الفكرية للمصنفات الرقمية، بحث منشور على شبكة الإنترنت في www.arablaw.org ص ٦

– (www.intenic.net/feqs/domain-names.html (26/4/2005.

(٧٥) تسمي هذه اللجنة بلجنة منح الأرقام على شبكة الإنترنت Internet Assigned Number Authority. ومهمتها إدارة نظام منح عناوين الأرقام في شبكة الإنترنت، ولقد إنبثق عن هذه اللجنة ثلاث هيئات مهمتها إدارة ومسك سجلات عناوين المواقع عبر العالم وهي: RIPE NCC بالنسبة لأوربا و APNIC بالنسبة لآسيا والباسفيك بما في ذلك الصين وكوريا وأستراليا و INTERNICE بالنسبة للولايات المتحدة الأمريكية والدول الأخرى غير المشمولة في الهيئتين السابقتين. حول هذه اللجان أنظر: الدكتور طوني ميشال عيسي – المرجع السابق ص ٦٦.

(٧٦) يقوم هذا النظام على تقسيم الكرة الأرضية إلى قطاعات أو مناطق هرمية لا مركزية يطلق عليها المساحات أو المجالات الفضائية المرسومة لغرض منح الأسماء، وتسمي اصطلاحا بعناوين المستوى الأول الأعلى Top level Domains، ويسمح لأفراد ولهيئات أو مكاتب منتشرة في هذه المناطق بتولي مهمة إدارة عناوين مواقع الإنترنت الخاصة بكل قطاع أو منطقه وغالبا ما يكون هذا التقسيم هو ذاته المعتمد للدول. لمزيد من الإيضاح حيال هذا النظام والقواعد التي يعتمد عليها يرجع إلى الدكتور. طوني ميشال عيسى: المرجع السابق ص ٧١–٧٣.

(٧٧) الاسم الكامل له Domain Name system وهو نظام يسمح بحفظ كل عنوان بروتوكول إنترنت في هيئة نطاق اسم، ومهمته مساعدة مستخدمي الإنترنت على الوصول إلى ما يبحثون عنه في رحاب الإنترنت حيث يتولى ترجمة الاسم الذي نكتبه باستخدام الحروف إلى العنوان الرقمي المقابل له وبالتالي الاتصال بالموقع المطلوب الذي نرغب في زيارته. كما يساعد هذا النظام على تشغيل البريد الإلكتروني بالشكل الصحيح بحيث تصل الرسائل إلى المرسل له المقصود: حول هذا النظام أنظر:

www.icann.org/tr/arabic.html.

(٧٨) الاسم الكامل لها: Internet Corporation for Assigned Name and Number ولقد انبثق عنها مجموعة من اللجان الاستشارية أبرزها اللجنة الاستشارية الحكومية Governmental Advisary Committee (GAC) وهي لجنة مراقبة خاصة مؤلفة من ممثلين عن حكومات الدول الموصولة بشبكة الإنترنت ، تتولى مهمة الإشراف على حسن إدارة عمليات التسجيل من قبل ICANN ومن قبل مكاتب التسجيل التابعة لها وتقدم الآراء في حال حصول تعارض بين قرارات ICANN وبين مضمون الاتفاقيات الدولية أو النصوص التشريعية الداخلية للدول الأعضاء في هذه اللجنة . لمزيد من المعلومات حول هذه اللجنة أنظر:

www.icann.org/governmental.com.html.

(٧٩) هذا النظام الجديد في منح أسماء النطاقات الناشئ عن لجنة ICANN وإن كان مختلفا كثيرا عن النظام السابق الناشئ عن لجنة IANN، إلا أنه أبقى على الكثير من المبادئ والقواعد التي كانت سارية في النظام القادم، حيث أبقى على التقسيم ذاته المعتمد لقطاعات الدول، وعلى مبدأ الثنائية بين عناوين المستوى الأول وبين عناوين المستوى الثاني، كما أبقي على القطاعات العمومية المستقلة.

(٨٠) هذه المناطق هي أمريكا الشمالية وأمريكا الجنوبية وأوربا الغربية وأوربا الوسطي والشرقية ودول البلطيق والشرق الأوسط وأخيرا آسيا. أنظر الدكتور طوني ميشال عيسي – المرجع السابق ص ٧٠

(٨١) أثارت اللجنة الدولية المكونة لدراسة منازعات العناوين الإلكترونية والمعروفة باسم International Ad Hoc (IAHC) تحفظا على مصطلح "الدولية أو العامة" التي توصف بها هذه العناوين، وذلك في تقريرها الصادر في ١٩٩٧/٢/٤ م. حيث أنها ترى بأن المشروعات والشركات الوطنية في أية دولة بمكنتها تسجيل هذه العناوين دون أن يكون لها نشاط دولي حقيقي أو أن يكون لها فروع دولية. هذا التقرير متاح على العناوين التالي:

www.iahc.org/docs/draft-iahc-recommend-fr.htm

(٨٢) أنظر في ذلك:

– الدكتور/ محمد حسام محمود لطفي: النزاع بين أسماء الحقول على الإنترنت والعلامات التجارية، بحث مقدم إلى ندوة الويبو الوطنية عن آخر التطورات في مجال الملكية الفكرية المنعقدة في مسقط في الفترة ٢٠-٢١/١٠/٢٠٠٢ م برعاية المنظمة العالمية للملكية الفكرية الويبو بالتعاون مع وزارة التجارة والصناعة بسلطنة عمان ص ٤-٥

– الدكتور/ شريف محمد غنام، المرجع السابق ص ٢١-٢٣

(٨٣) يعتبر هذا الاسم هو الأشهر بالنسبة لمستخدمي الإنترنت، حيث تشير إحصائية تم نشرها عبر شبكة الإنترنت عن عدد العناوين التجارية التي تم تسجيلها حتى الأول من شهر يونيو ١٩٩٩، أنه من بين حوالي ٨ ملايين اسم تم تسجيلها توجد أربعة ملاين وتسعمائة وسبعة وستون ألف وستمائة وثمانية وثمانين اسم اتخذ النهاية .com أنظر الدكتور شريف محمد غنام – المرجع السابق ص ٢٣.

(٨٤) الاسم الكامل لهذا الشركة (International Ad Hoc Committee (IAHC وهي شركة أمريكية تم إنشائها عام ١٩٩٠ م هي تنظم وتضبط العناوين التجارية.

(٨٥) في هذه العناوين أنظر:

- الدكتور/ محمد حسام محمود لطفي: المشكلات القانونية في مجال المعلوماتية، مرجع سابق ص ٩٦
- الدكتور/ شريف محمد غنام، المرجع السابق ص ٢٤
- ناتالي بورين ؛ ايمانويل جير، المرجع السابق ص ٦-٧

(٨٦) الدكتور/ شريف محمد غنام، المرجع السابق ص ٢٩.

(٨٧) اعتراض الإدارة الأمريكية لم يكن على هذه الأسماء في حد ذاتها وإنما انصب على المادة الرابعة من المشروع والتي نصت على تعيين ٢٨ هيئة أو جهة موزعة على سبع مناطق جغرافية في كل أنحاء العالم يناط إليها مهمة منح هذه الأسماء. ويرجع الاعتراض الإدارة الأمريكية على هذه المادة في كونها تنهي الاحتكار الذي كانت تمارسه الشركة الأمريكية INTERNIC في منح هذه الأسماء، حيث أن إنشاء ٢٨ هيئة مستقلة تمنح هذه الأسماء يقلل من أهمية اللجوء إلى هذه الشركة الأمريكية.

(٨٨) الدكتور/ عبد الرحمن بن عبد الله السند: وسائل الإرهاب الإلكتروني " حكمها في الإسلام وطرق مكافحتها" ، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب ، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية ٢٠٠٤ م ص ١٦-١٧.

(٨٩)

www.khayma.com/tanweer/textes/hacar.htm.

(٩٠) أنظر ما يلي ص ٣١٢.

(٩١) الدكتور: عبد الرحمن بن عبد الله السند – المرجع السابق ص ١٧-١٨.

(٩٢)

www.alarbiya.net/Articlep.aspx?p=4390 at 10/11/2005.

(٩٣)

http://web.fares.net/w/.ee7ebae at 07/09/2001.

(٩٤) هشام سليمان – حملة على مواقع الإنترنت الحكومية بالعالم – مقال منشور على موقع إسلام أون لاين على شبكة الإنترنت بتاريخ ٢٠٠١/١/٢٣ م.

www.islamonline.netLarabic/news/2001-01-24/article5.shtml.

(٩٥) جريدة الإتحاد الإماراتية العدد ١٠١٣٤ المؤرخة في ٢٠٠٣/٤/٤ م.

(٩٦) www.egypty.com/top4/misr-alarabia.asp at 05/10/2005.

(٩٧) اختراق المواقع وطرق الوقاية – دراسة منشورة على شبكة الإنترنت بتاريخ ٢٠٠٥/٩/٦ على شبكة الإنترنت من خلال موقع: www.websy.net/learn/hackers/course44.htm.

(٩٨) من أكثر هذه البرامج انتشاراً: Cracker Jack، وJohn The Ripper، وJack The Ripper، و Brute Force Cracker.

(٩٩) الاسم الكامل لهذا البرتوكول:(Internet Control Message Protocol).

(١٠٠) www.arabact.com/vb/showthread.php?t=280 at 31/8/2005.

(١٠١) يقصد بهذا المصطلح الدفاع ويعود إلى عام ١٩٢١ م عندما تشكلت منظمة عسكرية صهيونية استطانية في القدس بغرض اقتحام الأراضي الفلسطينية. أنظر موضوع الهاجانة حرب صهيونية على مواقع الإنترنت الإسلام، مقال منشور على شبكة الإنترنت بتاريخ ٢٠٠٥/١٠/٥ م على موقع طريق الإسلام على شبكة الإنترنت
www.islamway.com/?iw_s=Article&iw_a=view&article-id=1095

(١٠٢)
www.islamway.com/?iw_s=Article&iw_a=view&article-id=1095

(١٠٣)
http://web.fares.net/w/.ee7ebae at 07/09/2001

(١٠٤)
http://web.fares.net/w/.ee7ebae at 07/09/2001

(١٠٥)
www.ac4mit.org/_uae.asp?fileName=20030724020509 at 07/07/2003

(١٠٦) للاستزادة حول هذا الموضوع يرجع إلى:
- خلاصة ورشة عمل أجرتها منظمةCERT للتعامل مع هجمات حجب الخدمة منشورة على موقع:
www.cert.org/erports/dsit_workshop.pdf
- دراسة لاستراتيجية الوقاية من هجمات حجب الخدمة الموزعة، تقدمها شركة CISCO منشورة على موقع:
www.cisco.com/warp/public/707/22.html

(١٠٧) الدكتور/ محمد حسين منصور: المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية ٢٠٠٣ ص ٢٥٩

(١٠٨) الدكتور: محمد نور شحاته: التجارة الإلكترونية، بحث منشور على شبكة الإنترنت:www.eastlaws.com

(١٠٩) المستشار/ محمد محمد الألفي: أنماط جرائم الإنترنت، بحث منشور على شبكة الإنترنت من خلال موقع:
www.eastlaws.com

(١١٠) أحمد الخالد – سرقة أسماء النطاقات إلى أين – مقال منشور على شبكة الإنترنت من خلال موقع:
www.bab.com/articles/full_article.cfm?id=8498

(١١١) الدكتور: طوني ميشال عيسي: المرجع السابق ص ٧٧ & أحمد الخالد: المقال السابق

(١١٢) يمكن الحصول على معلومات إضافية عن السطو الإلكتروني والجزاءات من خلال مركز الويبو للتحكيم والوساطة، تسوية المنازعات بشأن أسماء الحقول
http://arbiter.wipo.int/domains/index.html

(١١٣) لمزيد من المعلومات يمكن الرجوع إلى موقع مركز الويبو للتحكيم والوساطة على شبكة الإنترنت:
http://arbiter.wipo.int/domains

(١١٤) يقصد بمبدأ الأسبقية في التسجيل أنه يجوز لكل شخص أن يحصل على اسم للحقل متى ما قدم طلبه قبل غيره من المشروعات أو الأشخاص العادية. فالعبرة في الحصول على هذا الاسم هي بسبق طلب التسجيل عن غيره من الطلبات. فإذا توافرت هذه الأسبقية كان من حق مقدم الطلب أن يحصل على هذا الاسم دون اعتراض من أحد. ولا يشترط للحصول على اسم الحقل شرط آخر سوى أن يكون الاسم لا يزال متاحا لم يسبق تسجيله من جانب مشروع أو شخص آخر. وبالتالي متى ما قدم المشروع أو الشخص طلبه إلى الشركات المتخصصة بالتسجيل، فلا تجرى هذه الشركات أي فحص لهذا الطلب، وإنما تمنحه هذا الاسم متى ثبت لها عدم سبق تسجيله، فهي تحرص دائما على النص في مشارطات تسجيل أسما الحقول على أن تعفي نفسها من إجراء أي بحث عن وجود حقوق للغير سابقة لعملية التسجيل. ويتعلق هذا المبدأ بمسائل فنية ترتبط بشبكة الإنترنت حيث يتم منح الاسم مرة واحدة لمن يقدم طلبه أولا،

مثلما يحدث في حالة التقدم للحصول على رقم للهاتف . وقد نصت على هذا المبدأ شروط تسجيل الأسماء المختلفة. لمزيد من التفاصيل حول هذا الموضوع أنظر الدكتور شريف محمد غنام- المرجع السابق ص ٧٦-٨٠

(١١٥) لمزيد من الإيضاح حول نشأة وتطور البطاقات الائتمانية أنظر:

-Drury .Ac .Ferrier , CW Credit card , London, Butter Wrth 1984 p14-29

-Jauffret .Alfred : droit commercial,20 edition par Jacques meste ,libraire generale de droit et de Juris prudence, Paris 1991 , N882 , p 572

(١١٦)

www.albayan.co.ae/albayan/2003/06/07/mnw/15.htm

(١١٧)

www.gulfpark.com/showarticale.php?cat=news&article-id=252

(١١٨) عماد علي الخليل: التكيف القانوني لإساءة استخدام أرقام البطاقات الائتمانية عبر شبكة الإنترنت ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بذات الجامعة في الفترة الممتدة من ١-٢٠٠٠/٥/٣ م المجلد الثاني ص ٩٠٩.

(١١٩)

www.albayan.co.ae/albayan/05/12/2000/mnw/12.htm

(١٢٠)

www.rawna/articles/full-articl.cfm?id=8183

(١٢١) أنظر في ذلك:

- الدكتور: عبد الفتاح بيومي حجازي – النظام القانوني لحماية الحكومة الإلكترونية – الكتاب الأول – دار الفكر الجامعي – الإسكندرية ص ٣٠٣-٣٠٦

- عماد علي خليل – المرجع السابق ص ٩٠٩

- بهاء شاهين – العولمة والتجارة الإلكترونية ص ١٤٣

(١٢٢) يقصد بخطوط الاتصالات العالمية: الخطوط التي تربط جهاز الحاسب الآلي الخاص بالمشترى بذلك الخاص بالتاجر.

(١٢٣)

www.alriyadh.com.sa/contents/13-5-2004/Riyadhnet/cov_1275.php

(١٢٤)

www.himag.com/articles/art4.cfm?topicid=4&id=938

(١٢٥) محمد عبد الله المنشاوي – جرائم الإنترنت في المجتمع السعودي – رسالة سابقة ص ٦٧.

(١٢٦) محمد محمد الألفي: أنماط جرائم الإنترنت، بحث منشور على موقع شبكة المعلومات العربية القانونية على شبكة الإنترنت: www.esatlaws.com

(١٢٧) لإنشاء هذه المواقع الوهمية يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي من خلال شبكة الإنترنت، ومن ثم إنشاء الموقع الوهمي مع تعديل البيانات السابقة التي تم الحصول عليها بطرق غير مشروعة. وذلك في الموقع الأصلي حتى لا يظهر وجود ازدواج في الموقع ويبدو الموقع الأصلي وكأنه الموقع الجديد. أنظر الدكتور/

جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية القاهرة ١٩٩٩ ص ٣٧.

(١٢٨) الرائد: علي حسن عباس: مخاطر استخدام بطاقات الدفع الإلكتروني عبر شبكة الإنترنت (المشاكل والحلـــول)، ورقة عمل مقدمة إلى ندوة " الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني" التي نظمها مركز بحـــوث الـــشرطة بأكاديمية الشرطة، القاهرة ١٤/١٢/١٩٩٨ ص ١٧.

(١٢٩) جريدة الأهرام المصرية – العدد ٤٢٠٠٦٩ – ١/٢/٢٠٠٢ م.

(١٣٠) ومن الأمثلة على هذه المواقع:

www.drak-secrts.com
www.hackers.secrts/credit/credit3txt

(١٣١)

www.akbarelyom.org.eg/akhbarelyom/issues/5118/1500.html

(١٣٢)

www.al-jazirah.com.sa/digimag/20062004/wr25.htm

(١٣٣) الإنتاج في ميدان التقنية العالية أصبح يتجه منذ عشرات السنين إلى زيادة إنتاج وسائل حماية التقنية أكثـــر مـــن إنتاج التقنية ذاتها ومن أهمها:

- استخدام البصمة الإلكترونية للرسالة Message Digest
- التشفير Encryption باستخدام برتوكولات خاصة مثل بروتوكولات التحويلات الإلكترونية الآمنة "Set"
- طرق التعرف الشخصي Authentication
- استخدام مرشحات المعلومات Hardware Filters

(١٣٤) عماد علي الخليل: المرجع السابق ص ٥.

(١٣٥)

Mme Lucas de leyssac- une information seule est ells susceptible de vol/Dalloz, 1985.ch.p43

(١٣٦)

"(Electronic Signatures in Global and National Commerce Act E-Sign Law)"

وقد دخل هذا القانون حيز النفاذ اعتبارا من الأول من أكتوبر سنة ٢٠٠٢.

.E-Sign Act Raises the Speed Limit on the Information Superhighway

.http://www.findlaw.com/computerstechnologylaw_1_75_1. Html"

(١٣٧)

New Law Makes E-Signatures Valid, Contracts created online are now as legal as those on paper, (2002); Report to the Governor and Legislature on New York Stat's Electronic

.Signatures and Records Act, P.11

(١٣٨)

.New Law Makes E-Signatures Valid, op-cit

(١٣٩)

."Federal Food, Drug and Cosmetic Act"

(١٤٠)

."Public Health Act"

(١٤١)

GIBBS (Jeffery N.) and MAZAN (Kate Duffy): Electronic signatures, Understanding FDA's Electronic Records and Signatures Regulation, Medical Device & Diagnostic Industry Magazine, may 1999
http:// www.devicelink.com/phpAds New/adclick
php?source=http://www.devicelink.com/mddi/archive/99/05/009.html

(١٤٢)

Gibbs and Mazan, op-cit

(١٤٣)

"Uniform Electronic Transactions Act (UETA)"

(١٤٤)

"Wire and Electronic Communications Interception and Interception of Oral Communications."
UNITED STATES CODE ANNOTATED TITLE 18. CRIMES AND CRIMINAL PROCEDURE PARTI-CRIMES،
Chapter 119-wire and electronic communications interception and interception of oral communications. http://www.usdoj.gov/wiretap 2510_2. Htm.

(١٤٥)

REID (THELEN) & LLp (Priest): California Is First State In Nation To Adopt Electronic Contracting Law 2002.
http://articles.corporate.findlaw.com//computerstechnologylaw_1_72. Html.

(١٤٦)

"Uniform Electronic Transactions Act (UETA)"

(١٤٧)

Cummings, op-cit

(١٤٨)

Electronic Signatures and Records Act (ESRA)

(١٤٩)

Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, P. 2

(١٥٠)

State Office for Technology's (OFT)

(١٥١)

AN ACT CONCERNING THE CONNECTICUT UNIFORM ELECTRONIC .TRANSACTIONS ACT, Raises Bill No. 561 February Session, 2002

(١٥٢)

Saul, Ewing, and Remick: Governor Ridgs Signs Pennsylvania Electronic Transactions Act http://corporate.findlaw.com/governmentlaw_3_8. Html

(١٥٣) المادة ١٠٢٩(أ) من التقنيين الأمريكي

(١٥٤)

Vergucht (Pascal) : la Repression des Delits Informatiques dans une perspective Internationale These , Universite de Montpellier 1 , 1996 , p 103 ,104,159

(١٥٥) الدكتورة/ نائلة عادل محمد فريد قورة: المرجع السابق ٦٢٢

(١٥٦)

www.al-jazirah.com.sa/digimag/25092005/wr18.htm

(١٥٧)

www.al-jazirah.com.sa/digimag/25092005/wr18.htm

(١٥٨) الدكتور/ ممدوح محمد على مبروك: المرجع السابق ص ١٢٨.

(١٥٩) لدكتور/ أشرف توفيق شمس الدين: الحماية الجنائية للمستند الإلكتروني" دارسة مقارنة "، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، والتي نظمته أكاديمية شرطة دبي بدولة الإمارات العربية المتحدة في الفترة من ٢٦-٢٠٠٣/٤/٢٨، ص ٣٥.

(١٦٠) الدكتور: عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق ص ٢٢٨.

(١٦١) لمزيد من الإيضاح ارجع إلى: الدكتور. محمد أبو العلا عقيدة: الحماية الجنائية للتجارة الإلكترونية، مرجع سابق ص ٩-١١.

(١٦٢) أنظر:

- الدكتورة: نائلة عادل محمد فريد قورة – المرجع السابق ٦٢٦

- سامح محمد عبد الحكم: الحماية الجنائية لبطاقات الائتمان، دار النهضة العربية، القاهرة ٢٠٠٣ م ص ١٣١

(١٦٣) المواد (٢٧٦ مكرر -٢٧٦ مكرر ٤) المضافة إلى قانون الجزاء العماني بموجب المرسوم السلطاني ٢٠٠١/٧٢ م.

(١٦٤) أنظر المواد ١٤,١١,٤ منه.

(١٦٥) أنظر ٣٨١-٣٨٦ منه.

(١٦٦) حول هذا الموضوع أنظر: الدكتور عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير: مرجع سابق ص ١٨١

(١٦٧) المادة ٣٨٠ من قانون العقوبات القطري ٢٠٠٤/١١ م والتي نصت على أنه"يعاقب بالحبس مدة لا تجاوز خمس سنوات، كل شخص ارتكب تزويراً في المستندات المعالجة آلياً، أياً كان شكلها، ترتب عليه الإضرار بالغير، أو استعمل هذه المستندات المزروة مع علمه بذلك....."".

(١٦٨) المواد (٢٧٦ مكرر -٢٧٦ مكرر ٤) المضافة إلى قانون الجزاء العماني بموجب المرسوم السلطاني ٢٠٠١/٧٢ م.

(١٦٩) أنظر في ذلك: الدكتور. يونس عرب: المرجع السابق ص ٢٩.

(١٧٠) مثلما حصل عندما تعرضت شركتا كريدت كاردز كوم، سي دي بوتبوس لعملية إبتزاز من قبل مواطنـــو روس حصلوا عن طريق القرصنة على بيانات ومعلومات تخص آلاف البطاقات الائتمانية في مقابـــل عـــدم نـــشرها. إلا أن الشركتين رفضتا الخضوع لمطالبهم مما حداء بهم إلى نشر تلك البيانات والمعلومات على شبكة الإنترنت.
http://news.bbc.co.uk/hi/arabic/news/newsid_1210000/1210366.stm