الحماية التقنية للمعلومات و دورها في تأمين نظام الدفع الالكتروني

Technical Protection of Information and its Role in Securing Electronic Payment System

Protection Technique des Informations et sa Rôle dans la Sécurisation du Système de Paiement Electronique

تاريخ استلام المقال: 2018/11/24	تاريخ المراجعة: 2018/11/25	تاريخ القبول: 2018/12/15

أ/ هداية بوعزة

كلية الحقوق - جامعة وهران2

د/ يوسف فتيحة

كلية الحقوق و العلوم السياسية - جامعة أبو بكر بلقايد تلمسان

hidayetb@ymail.com

ملخص:

إن توفير أمن الصفقات و المدفوعات الجارية بواسطة شبكة الانترنت، ذات الطبيعة الدولية و المفتوحة، هو أمر محفوف بالمخاطر و يعتبر أحد أبرز العوائق أمام نمو التجارة الالكترونية إذ بالرغم مما توفره الآليات التقنية من تقليص للمخاطر، فان الشبكات المفتوحة لا تقدم أي أمان جوهري في هذا المجال ، و بذلك تبقى عمليات الدفع الالكتروني عرضة للاعتداءات من قبل الغير، الذين يصعب إثبات هويتهم . فلتأمين انطلاقة ثابتة لعصر التجارة الالكترونية بتمرير للبيانات المالية و التبادل العلني و الحر للمعلومات ، لابد من امتلاك أنظمة دفع الكترونية تتبع آليات مبسطة و موثوقة في آن واحد و تقدم ضمانات تقنية و قانونية فعالة تتعلق بالأساس بالموثوقية والسرية والثبات. فاستخدام وسائل الدفع الحديثة بشكل معلن و عدم الاهتمام بوسائل المحافظة على سرية هذه الوسائل، يمثل خطورة على الأطراف المتعاملين بها. بناءا على ذلك فان موضوع الحماية من مخاطر الدفع الالكتروني لا يقتصر على الحماية التقليدية الممثلة في الحماية القانونية بتوفير حماية مدنية وجزائية في آن واحد ، بل إن الأمر يتعدى ذلك إلى نوع آخر من الحماية القبلية أو الوقائية يطلق عليه الحماية التقنية.

الكلمات المفتاحية: الانترنت، وسائل الدفع الحديثة،التجارة الالكترونية، الجريمة المعلوماتية، الأمن المعلوماتي.

Abstract:

The security of online transactions and payments, the nature of which is international and open, is risky and one of the major obstacles to the growth of e-commerce. This is why electronic payments are vulnerable to third-party attacks, whose identity is difficult to prove. To ensure a stable and steady start to the era of e-commerce by transmitting financial data and an open and free exchange of information, it is necessary to have electronic payment systems with simple and reliable mechanisms and technical guarantees. legal. The use of modern means of payment and the lack of interest in preserving the confidentiality of these means constitute a danger for the parties concerned. Therefore, the issue of the protection of the risk of electronic payment is not limited to the traditional protection which is represented in the legal protection, providing civil and criminal protection at the same time, but goes beyond another type priority or preventive protection called technical.

Key words: Internet, modern means of payment, e-commerce, computer crime, information security.

Résumé:

La sécurité des transactions et des paiements en ligne, dont la nature est internationale et ouverte, est risquée ,et constitue l'un des principaux obstacles à la croissance du commerce électronique. C'est pourquoi les paiements électroniques sont vulnérables aux attaques de tiers, dont l'identité est difficile à prouver . Pour assurer un début stable et régulier de l'ère du commerce électronique en transmettant des données financières et un échange d'informations ouvert et libre, il est nécessaire de disposer de systèmes de paiement électroniques dotés de mécanismes simples et fiables et de garanties techniques et juridiques. L'utilisation de moyens de paiement modernes et le manque d'intérêt pour préserver la confidentialité de ces moyens constituent un danger pour les parties concernées. Par conséquent, la question de la protection du risque de paiement électronique ne se limite pas à la protection traditionnelle qui est repésentée dans la protection juridique , en assurant la protection civile et pénale en même temp, mais elle va au-delà à un autre type de protection prioritaire ou préventive appelée protection technique.

Mots clés: Internet, moyens de paiement modernes, commerce électronique, criminalité informatique, sécurité de l'information

مقدمة:

أدى انتشار التكنولوجيا الالكترونية الحديثة كالانترنت و الحاسب الآلي إلى ازدهار التجارة الالكترونية ،و التي اعتمدت هذه الوسائل المتطورة إلى حد كبير ، مما أدى إلى ظهور وسائل دفع حديثة في الصورة الالكترونية تتماشى و مبادئ التجارة الالكترونية وتعد الدعامة الأساسية لهذه الأخيرة و أحد متطلباتها. حيث شهد العالم اتساعا في نطاق التجارة الالكترونية وتشعبا في أنواعها و مجالاتها ،كما تعددت في المقابل التشريعات الدولية المنظمة لها و أصبحت صناعة المعلوماتية المجال الخصب لجذب الاستثمارات خصوصا مع تحقيق التزاوج بين المعلوماتية و أدوات الاتصال اللاسلكية.

لقد لعبت المعلوماتية دورا هاما في تغيير محل التجارة الالكترونية و وسائل تحقيقها، حيث تم استبدال الوثائق التقليدية بالوثائق الالكترونية ، و تضاءل دور النقود الورقية ووسائل الدفع التقليدية أمام انتشار وسائل ا لدفع الحديثة و الالكترونية. غير أن تكنولوجيا المعلومات التي تم إقحامها في مجال المعاملات المالية و المصرفية ، تعد سلاحا ذو حدين . فإضافة إلى مزاياها ووظائفها المتعددة، إلا أن استخدامها في بيئة افتراضية هو أمر محفوف بالمخاطر .فآلية الدفع الالكتروني تعد عملية مصرفية دولية متعددة الأطراف ،تتم عبر فضاء مفتوح ، مما يغري ضعاف النفوس بالدخول إلى سوق وسائل الدفع الحديثة لتزويرها أو السطو عليها و إساءة استخدامها في النصب و الاحتيال على التجار و البنوك. لذلك كان لزاما على الدول الاهتمام بموضوع الحماية من مخاطر الدفع الالكتروني ،و البحث عن وسائل تضمن المحافظة على سرية هذه الآليات وحمايتها من قراصنة الانترنت.

فموضوع الحماية من مخاطر الدفع الالكتروني لا يقتصر على الحماية التقليدية الممثلة في الحماية القانونية بتوفير حماية مدنية وجزائية في آن واحد ، بل إن الأمر يتعدى ذلك إلى نوع آخر من الحماية القبلية أو الوقائية يطلق عليه الحماية التقنية ،أي كل ما يتعلق بالأمن المعلوماتي و جميع الوسائل الكفيلة بضمان أمن و سرية المعلومات المتداولة الكترونيا .

سنحاول من خلال هذه الورقة البحثية الإجابة عن إشكالية هامة مفادها ما معنى الحماية التقنية للمعلومات في مجال الدفع الالكتروني ؟ و ما هو الدور الذي تؤديه في سبيل تفعيل آلية الدفع الالكتروني و التعزيز من الثقة في مصداقيتها وتشجيع التعامل بها ؟.

إن الإجابة عن هذا الإشكال تتطلب منا البحث في عدة نقاط .لذلك سنقسم هذه الورقة البحثية إلى مبحثين اثنين، بحيث نتعرض في المبحث الأول إلى مفهوم الحماية التقنية للمعلومات في مجال الدفع الالكتروني ، على أن نخصص المبحث الثاني إلى آليات الحماية التقنية للدفع الالكتروني.

المبحث الأول: مفهوم الحماية التقنية للمعلومات في مجال الدفع الالكتروني

من مشكلات الانترنت العويصة هي تسخير بعض البرامج من قبل قراصنة المعلومات (الهاكرز) للهجوم على الأجهزة و شبكات الكمبيوتر و كذلك التجسس على معلومات مستخدمي الشبكة العنكبوتية. و سنبين فيما يلي المقصود بالحماية التقنية **(المطلب الأول)** كما نبين ما هي أدوات القرصنة التي تهدد الأمن المعلوماتي و التي ينبغي مواجهتها و التصدي لها بواسطة أسلوب الحماية التقنية أو الفنية **(المطلب الثاني)**.

المطلب الأول : المقصود بالحماية التقنية للمعلومات في مجال الدفع الالكتروني

يقصد بالحماية التقنية للمعلومات في مجال الدفع الالكتروني جميع وسائل الحماية و التدابير التقنية التي تستهدف حماية نظام الدفع الالكتروني من أي اعتداء على أنظمة المعلومات الخاصة به ، بحماية المواقع الالكترونية و البرمجيات و مصنفات الحاسب الآلي وكذلك حماية قاعدة البيانات ببنك المعلومات . فاستعمال وسائل الدفع الالكتروني يمكن أن يعترضه عديد من المخاطر خاصة ذات الطابع الأمني ، و هو ما يترك أثرا بالغا في ثقة المتعاملين بهذه الوسائل ، و إغفال معالجة هذه المخاطر من شأنه تهديد مستقبل العمل بوسائل الدفع الحديثة.

و بذلك تعد الحماية التقنية للدفع الالكتروني الوسيلة الأمثل لمواجهة المخاطر الأمنية الناشئة عن استخدام وسائل الدفع الالكتروني.فالدفع الالكتروني يحمل في طياته إشكاليات و مخاطر متعددة خاصة إذا كان هذا الدفع عبر الانترنت ،لذلك كان لزاما على الدول وكذا المؤسسات المصدرة لوسائل الدفع الحديثة إجراء تقييم لهذه المخاطر بصورة كافية و سريعة لمنع تفاقمها و العمل على ابتكار وابتكار تقنيات و آليات تكنولوجية متطورة للعمل على معالجة تلك المخاطر الأمنية. إن العلة من توفير الحماية التقنية للدفع الالكتروني سببها اعتبارات الأمن و حماية خصوصية المعلومات المتداولة عبر شبكة الانترنت لاسيما المتعلقة بنظام الدفع الالكتروني.

تجدر الإشارة في هذا الصدد ، إلى أن مجلس الشيوخ الفرنسي قد أشار إلى ضرورة الحماية التقنية أو الفنية عند تعريفه لمفهوم نظام المعالجة الآلية للمعطيات[1] ، غير أن هذا النص ذكر عنصر الحماية الفنية ولكن من غير إشارة إلى مدى ضرورة وجود أو عدم وجود الحماية الفنية أو التقنية كشرط لازم للتمتع بالحماية الجنائية في هذا المجال.

فمع انفتاح شبكة الانترنت ازدادت المخاطر التي تهدد أمن المعاملات المصرفية الالكترونية ، تبينت أهمية وضرورة معالجة إشكالية أمن المعاملات خاصة من قبل مصدري وسائل الدفع الالكتروني و كذا القائمين على البنوك الالكترونية لما يمكن أن يرتبه المساس بها من خسائر سواء للبنوك أو للعملاء. يرى البعض[2] بأن الإنتاج في مجال التقنية العالية يتجه منذ عشرات السنين إلى زيادة إنتاج وسائل الحماية التقنية أكثر من إنتاج التقنية نفسها ، فمجرمو التقنية تفوقوا على أنفسهم عندما ارتكبوا الاعتداء على أنظمة الحماية ذاتها، و التي صممت لمنع

الاعتداء على أنظمة التقنية العالية بما تشتمل عليه هذه الأنظمة من حواسيب و برامج و شبكات ربط و اتصال . و نشير إلى أنه يقصد بالحماية التقنية للدفع الالكتروني جميع وسائل الحماية و التدابير التقنية التي تستهدف حماية نظام الدفع الالكتروني من أي اعتداء على أنظمة المعلومات الخاصة به ، بحماية المواقع الالكترونية والبرمجيات ومصنفات الحاسب الآلي وكذلك حماية قاعدة البيانات ببنك المعلومات .

كما يقصد بمصطلح الحماية التقنية أو الحماية الفنية للدفع الالكتروني أيضا، ذلك الإجراء الوقائي الذي يتخذه مصدر وسيلة الدفع الالكتروني أو صانعها أثناء وضعه لها للحد من الاعتداءات الخارجية التي قد تقع عليها.[3]حيث تعمل الحماية الفنية التقنية على إيجاد أنظمة أمان لحماية نظم المعلوماتية و تقنية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج .[4]

كما عرفت الحماية التقنية للدفع الالكتروني بأنها : " حماية جميع أنواع المعلومات و مصادر الأدوات التي يتعامل بها و تعالجها من منظمة و غرفة تشغيل أجهزة ، و الأجهزة و وسائط التخزين و الأفراد من السرقة و التزوير و التلف و الضياع و الاختراق "[5].

وتتخذ الحماية التقنية بهذا المفهوم أشكالا و صورا متعددة يمكن تصنيفها إلى عدة فئات ،بحسب الآليات المتبعة والتقنيات المستخدمة ، وكذا الأهداف المرجوة من كل صورة من الحماية. حيث تختلف أهداف هذه التدابير من تدابير **وقائية** إلى تدابير **الكشف** فتدابير **الاحتواء**.فبالنسبة لتدابير الوقاية فإنها تهدف إلى إحباط الهجمات على مكونات النظام قبل تنفيذ أي عملية احتيالية عليه.أما تدابير الكشف عن الهجمات فهي ترمي إلى تنبيه المصدرين أو مشغلي النظام إلى حدوث عمليات احتيالية وتحديد مصدرها.و عن تدابير الاحتواء فهي ترمي إلى الحد من نطاق النصب المرتكب عقب اكتشافه. غير أنه و قبل التعرض إلى الآليات المستخدمة في الحماية التقنية للدفع الالكتروني و ذلك من خلال القسم الثاني لهذه الورقة البحثية.ينبغي تحديد المقصود بالمعلومات كونها مسألة أولية في البحث، على اعتبار أن المعلومات هي المحل الذي يقع عليه الاعتداء في جرائم المعلوماتية ، و هي مسألة تقتضي توضيحا دقيقا و فهما عميقا من أجل إصباغ الحماية عليها على نحو صحيح.

لقد ذهب البعض[6] إلى القول بأنه من الصعب أو من المستحيل وصف المعلومة بدقة و ما يمكن فقط هو إدراك أثرها .في حين يرى البعض الآخر أن المعلومات يقصد بها " مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل و الاتصال أو للتفسير و التأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الالكترونية و هي تتميز بالمرونة بحيث يمكن تغييرها و تجزئتها و جمعها أو نقلها بوسائل و أشكال مختلفة ".[7]

ومن الجانب القانوني تجدر الإشارة إلى وجود بعض المحاولات التشريعية لتحديد المقصود من المعلومة، ومن ذلك ما نص عليه المشرع الفرنسي في القانون 652/82 الصادر في 1982/07/26

الخاص بالاتصالات السمعية و البصرية، حيث يقصد بالمعلومات في مفهوم ذلك القانون " صور الوثائق و البيانات و الرسائل من أي نوع ".كما عرف القرار المتعلق بإثراء المصطلحات المعلوماتية بأنها :" تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة من شأنها أن توصل المعلومة إلى هذا الغير "[8].كما عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الالكترونية لسنة 1999 بأنها :" تشمل البيانات و الكلمات و الصور و الأصوات و الرسائل و برامج الكمبيوتر و البرامج الموضوعة في الأقراص المرنة و قواعد البيانات أو ما شابه ذلك "[9]. و على الصعيد العربي هناك بعض التشريعات التي تطرقت إلى مفهوم المعلومات ، حيث نص القانون الاتحادي لدولة الإمارات العربية المتحدة رقم 1 لسنة 2006 المتعلق بالمعاملات الالكترونية على أن المعلومات هي بيانات و معلومات الكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها .[10]

المطلب الثاني: أدوات القرصنة التي تهدد الأمن المعلوماتي و تستوجب الحماية التقنية

عرفت السنوات الأخيرة تطويرا في الإجراءات المبتكرة لحماية أمن الكمبيوتر ، غير أن كثيرا من نظم الكمبيوتر التي تعتمد عليها أنظمة الدفع الحديثة لا تزال غير مأمونة بشكل مثير للدهشة ؛ حيث يلجأ المخربون و القراصنة إلى استخدام مجموعة متنوعة من الأدوات والتقنيات للتغلب على عائق الأمن. و سنبين فيما يلي أهم أدوات القرصنة[11] التي تهدد أمن المعاملات البنكية الحديثة و المعاملات الالكترونية بواسطة الكمبيوتر وشبكة الانترنت بصفة عامة [12].

الفرع الأول: تقنيات السلامى

يقصد بذلك أن يقوم المخرب بإجراء مجموعة رموز سرية لبرنامج الكمبيوتر مسببا بذلك تغييرات صغيرة جدا من المستبعد أن تكتشف و لكن تأثيرها التراكمي يمكن أن يكون كبيرا .

الفرع الثاني: الباب الخلفي أو باب المصيدة

عند تطوير برنامج ما ، يقوم المبرمجون أحيانا بإدخال كود ليسمح لهم بتخطي إجراءات الأمن المعتادة . و ما إن تكتمل البرمجة قد يظل الكود في البرنامج إما بالصدفة أو بشكل متعمد ، و يعتمد المهاجمون على هذا الكود الزائد في اختراق الأمن .

الفرع الثالث: الحفلة التنكرية

تتم كتابة برنامج كمبيوتر تنشط أو تحفز البرنامج الحقيقي كأن تتم كتابة برنامج لتنشيط شاشة log in والديالوج المتصل بها و عندما يحاول مستخدم الدخول log-in يلتقط الكمبيوتر رقم هوية المستخدم وكلمة السر و يعرض رسالة خطا ، فيحاول المستخدم الدخول من جديد ، و ينجح فعلا في المرة الثانية ولكنه لا يعرف أبدا أن عملية الدخول الأولى كانت خدعة للحصول على ال ID .

الفرع الرابع : جمع القمامة

لا يمحو الكمبيوتر في العادة البيانات التي لم تعد هناك حاجة لها ، و عندما يقوم المستخدم بحذف البيانات لا يتم تدمير المعلومات فعلا ، و لكن يتاح حيز لكي يكتب عليه الكمبيوتر فيما بعد . و جامع القمامة يقوم فيما بعد بسرقة بيانات حساسة ظن المستخدم أنها حذفت بينما هي ما تزال في الكمبيوتر.

الفرع الخامس: الفيروسات و ديدان الانترنت

تستخدم كلمة فيروس في مجال المعلوماتية للدلالة على كل البرامج الخبيثة التي تسبب إتلافا لأنظمة المعالجة الآلية للمعلومات وهي تتسبب في إتلاف المكونات المنطقية للحاسب الآلي ، أو تعطيل أجهزة الكمبيوتر أو الشبكات عن تأدية عملها[13].

تتميز الفيروسات بالسرعة في الانتشار في النظام ؛ كما أن إزالته يمكن أن تكون مكلفة وشاقة . ويتم عادة للاحتياط من الفيروسات استخدام برمجيات من خارج الشركة و ماسحات للفيروسات على كل الملفات التي يتم إنزالها قبل استخدامها. و الفرق بين الفيروسات و ديدان الانترنت أن الفيروس في حاجة إلى أحد البرامج المنتشرة بين المستخدمين لكي يحتضنه [14]، و بالتالي يستطيع الانتشار و التكاثر عن طريقه .و أشهر مثال على ذلك "فيروس ميليسا"[15] و"فيروس الحب" ، حيث أن الأخير كان بحاجة إلى برنامج " مايكروسوفت أوت لوك " كحاضن له ؛ أما الديدان فليست بحاجة إلى أي برنامج يحتضنها ، و مثالها الشهير" دودة موريس"[16].

الفرع السادس : حصان الطروادة[17]

يعتبر حصان الطروادة برنامجا يضعه المخربون مخبأ داخل البرامج العادية لمنشأة ما . و يواصل الكمبيوتر عمله بصورة طبيعية في الوقت الذي يجمع فيه البرنامج المخبأ البيانات و يجري تعديلات سرية في البرامج والملفات و يمحو أو يدمر البيانات أو حتى يسبب إغلاقا كاملا. و يمكن أن تبرمج أحصنة الطروادة لتدمير كل آثار وجودها بعد التنفيذ .[18]و لتحقيق نظرية الاختراق عن طريق ملفات أحصنة الطروادة لابد من توفر برنامج تجسسي يتم إرساله و زراعته من قبل الجاني في جهاز الضحية ، و يعرف بالملف اللاصق و يسمى(الصامت) أحيانا و هو ملف باتش صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (الخادم) و هو حلقة الوصل بينه و بين المخترق (المستفيد).و تتم عملية إرسال برمجيات التجسس بعدة طرق من أشهرها البريد الالكتروني ، حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه أو يقوم بفتحه من باب الفضول ليجده لا يعمل بعد فتحه فيتجاهله ضانا بأنه معطوب و يهمل الموضوع بينما في ذلك الوقت يكون المخترق قد وضع قدمه الأولى بداخل الجهاز ؛ قد يقوم بعض الأشخاص

بحذف الملف مباشرة بعد اكتشافهم بأنه لا يعمل و لكن يكون قد فات الأوان لأن ملف الباتش من هذا النوع يعمل فورا بعد فتحه و إن تم حذفه[19].

في الأخير تجدر الإشارة إلى ضرورة حماية أية قاعدة بيانات أو برامج أو نظم معلوماتية من خطر هجومات القراصنة و الهاكرز لاسيما إذا تعلقت بالدفع الالكتروني أو التجارة الالكترونية على العموم. وفيما يلي عرض لأهم آليات الحماية التقنية المعدة لذلك.

المبحث الثاني : آليات الحماية التقنية للدفع الالكتروني

تكتسي حماية المعلومات الالكترونية[20] الخاصة بنظام الدفع الالكتروني و المتداولة عبر شبكة الانترنت أهمية كبيرة لما يشكله المساس بها من آثار على الذمة المالية لعملاء البنك و على سمعة هذا الأخير وما يمكن أن ينتج من خسائر مادية للبنك نتيجة الإضرار بسمعته[21]. و تجدر الإشارة إلى أن العبث بالمعلومات الالكترونية هو من المخاطر الناتجة عن استخدام الانترنت في المجال البنكي .[22] و توجد مخاطر أخرى منها ما يتخذ شكل انتحال الغير شخصية أحد عملاء البنك عن طريق سرقة كلمات السر الخاصة به ، أو تسجيل بعض الرسائل و إعادة إرسالها ، بالإضافة إلى إمكانية اختراق الموقع و العبث بمحتوياته و الاستخدام غير المرخص به و العديد من المخاطر الأخرى.

وسنتناول فيما يلي أهم الآليات التقنية المستخدمة للتحقق من هوية العميل في المطلب الأول ، ثم أهم الوسائل المستخدمة في حماية أمن المراسلات و المواقع الالكترونية في المطلب الثاني من هذا المبحث .

المطلب الأول :تقنيات تحديد الشخصية و التحقق منها

سجل مؤخرا عديد من عمليات السطو على المعلومات الالكترونية و البيانات المستخدمة في المعاملات البنكية الالكترونية ، و وسائل الدفع الالكتروني بصفة عامة.الأمر الذي دفع بالبنوك إلى استخدام وسائل تقنية إضافية لحماية العملاء تتمثل في تقنيات تحديد الشخصية و كذا التحقق منها. و يهدف استخدام هذه التقنيات إلى التأكد من مشروعية الاستفادة من الخدمات البنكية الالكترونية و أن المستفيد هو العميل صاحب الحساب البنكي .[23] و تتمثل هذه التقنيات في كل من تقنية هوية المستخدم وكلمة السر(الفرع الأول)، و تقنية كلمة السر التي لا تتكرر(الفرع الثاني).

الفرع الأول :نظام هوية المستخدم و كلمة السر

قبل أن يسحب العميل النقود بالبطاقة وعند دخول العميل لموقع البنك على الانترنت للاستفادة من الخدمات الالكترونية ، فان أول ما يصادفه طلب إدخال هوية المستخدم و كلمة السر حتى يتمكن من الوصول لحسابه. و بالتالي فان إدخالهما يشكل وسيلة للتحقق من الشخصية و دليلا على أن الذي قام بالعملية هو صاحب الحساب ، و إذا كان موقع البنك

يسمح بإجراء العمليات بمجرد الدخول إليه باستخدام الهوية و كلمة السر فإنهما بذلك يشكلان دليلا على اتجاه إرادة العميل إلى الالتزام بمقتضى العملية التي أجراها.

تعد كلمة السر خط الحماية الأول الذي يعتمد عليه نسبة كبيرة من مستخدمي أجهزة الحاسب الآلي ، و لذلك فان أول خطوة يقوم بها القراصنة هي التعامل معها لكي يتمكنوا من الدخول إلى أنظمة الحاسب الآلي وبالتالي يفتح الطريق أمامهم لارتكاب جرائمهم.[24]

يعتبر نظام هوية المستخدم و كلمة السر أحد الوسائل التأمينية[25] التي تمكن البنوك والمؤسسات المصدرة لوسائل الدفع الالكتروني من الكشف عن هوية القراصنة و أماكن دخولهم إلى الشبكة ، بحيث يكون تمنع هذه البرامج اقتحام الشبكة أو نظام المعلومات[26].

و تجدر الإشارة إلى أن بعض البنوك بدأت تصدر بطاقات تجيز السحب و الوفاء في آن واحد و تحمل هذه البطاقات رمزا سريا لا تتم عمليات السحب و الوفاء إلا به . و قد ساهم استخدام الرمز السري كثيرا في التقليل من الاستخدام غير المشروع لبطاقات الاعتماد ، بحيث يمنع سارق البطاقة أو مزورها من استخدامها.[27]

يعد الرمز السري رمزا معلوماتيا تحتويه بطاقة سحب الأموال النقدية لا يعلمه إلا الحامل ، يتيح هذا الرمز للحامل بعد إدخال البطاقة في الصراف الآلي سحب الأموال النقدية ، و لا يستطيع سارق البطاقة أو من يجدها استعمالها إلا إذا استطاع الحصول على هذا الرمز ، ولذلك يتحمل العميل مسؤولية الإهمال في المحافظة على هذا الرمز.

كما أنه و بغية الحد من فرص الاستخدام غير المشروع للبطاقات ، استحدثت بطاقات وفاء ذكية ذات رقم سري خاص و هي تشكل بذلك بطاقة دفع آمنة[28] . حيث يتولد الرقم السري عن طريق دالة خوارزمية فيدخل العميل البطاقة في آلة قراءة مع إدخال الرقم السري الموجود في البطاقة ؛ فإذا كانا متطابقين تتم العملية ، أما إذا كانا غير متطابقين فانه يعطي حامل البطاقة محاولتين أخريين ، فإذا أخطأ رغم ذلك في إدخال الرقم السري الصحيح يعطي ال micro processor أمرا تلقائيا لإعطاب نفسه بنفسه فتصبح البطاقة غير صالحة للاستعمال .[29]

وعليه فان استخدام مثل هذا النظام للولوج للخدمات البنكية يمكن اعتباره بمثابة توقيع الكتروني لأنه لا يمكن إجراء العملية إلا بإدخال كلمة السر و هوية المستخدم و هي بذلك تكون مرتبطة برسالة المعلومات المتضمنة للعملية المجرات ، و باعتبارها خاصة بالعميل وحده فإنها تميز شخصيته و تدل عليها و على إرادته في القيام بالعملية و الالتزام بمضمونها[30].

غير أنه رغم الاحتياطات التي قد يتخذها العميل من أجل عدم كشف كلمة السر الخاصة به فان ابتكارات بعض الأشخاص الذين يحترفون الإجرام عبر الانترنت تجعلهم قادرين على

التوصل لمعرفتها [31]، مما دفع البنوك إلى استخدام وسائل حمائية إضافية مثل كلمة السر التي لا تتكرر.

الفرع الثاني :كلمة السر التي لا تتكرر

سميت هذه الطريقة بكلمة السر التي لا تتكرر لأن كلمة السر المستخرجة من جهاز التوثيق لا تكون صالحة إلا لعملية واحدة و خلال مدة محددة في دقيقة واحدة فقط ، وهي شأنها شأن الكلمة المستخرجة بطريقة خوارزمية القيمة الاختيارية تعتبر بمثابة توقيع الكتروني.

و بالنسبة لطريقة عمل هذا النظام فانه يمكن التمييز بين طريقتين ، تسمى الطريقة الأولى بنظام S/key و تعتمد على اشتراك كل من العميل و البنك للتوصل لكلمة السر التي لا تتكرر ، حيث يتم تزويد كل منها في البداية بنفس جملة المرور و عدد مرات إدخال البيانات لخوارزمية القيمة الاختبارية hash [32]، فيبدأ العميل بإرسال رسالة البداية ، فيرد البنك برقم عشوائي يتم استخدامه في استخراج كلمة السر التي لا تتكرر .[33] حيث أن العميل يستخدم هذه الكلمة مرة واحدة فقط بإرسالها إلى البنك الذي يتأكد من صحتها ، و بعد أن تتم العملية المراد انجازها تصبح هذه الكلمة غير صالحة للاستعمال.

غير أنه و نظرا لتعقد هذا النظام فان البنوك لجأت إلى استخدام طريقة أخرى تعمد فيها إلى تزويد العميل بجهاز توثيق[34] و كلمة السر اللازمة لتشغيل الجهاز. حيث يكون هذا الجهاز متصلا بالبنك في حالة تشغيله، فإذا أراد العميل القيام بأي عملية من العمليات التي تؤثر في ذمته المالية يقوم باستخراج كلمة السر اللازمة لذلك من الجهاز بالضغط على أحد مفاتيحه فتظهر له الكلمة بشكل مقروء على شاشة الجهاز ، ثم يقوم بإدخالها في الخانة المخصصة لذلك على شاشة الكمبيوتر لتتم بذلك العملية المطلوبة.[35]

المطلب الثاني: الوسائل المستخدمة في حماية أمن المراسلات و المواقع الالكترونية

مع التطور المسجل في وسائل ارتكاب الجريمة المعلوماتية وتنوع الوسائل التي قد يلجأ إليها المجرمون أصبحت تقنيات التحقق من الشخصية غير كافية خاصة إذا قام المجرمون باستخدام طرق أخرى للسطو على الحسابات غير تلك القائمة على سرقة كلمات السر[36] .

لذلك سعى العاملون في الميدان الالكتروني إلى ابتكار وسائل حديثة لحماية أمن و سرية المراسلات والمعلومات عن طريق تشفيرها(الفرع الأول) و بحماية المواقع الالكترونية و الشبكات الداخلية من خلال جدران الحماية(الفرع الثاني) .

الفرع الأول : التشفير

التشفير أو التعمية أو الكتابة السرية كلها مفردات تدل على تلك الوسيلة التقنية لحماية أمن المعلومات ضد أعمال قرصنة والاختراق و بث الفيروسات و الاعتداء على المعلومات الاسمية و بيانات وسائل الدفع الالكتروني كبطاقات الائتمان الممغنطة.[37]

و سنتطرق فيما يلي إلى المقصود بتقنية التشفير(أولا) ، آلياتها وأنواعها(ثانيا)و كذا مستوياتها (ثالثا).

أولا :المقصود بتقنية التشفير

التشفير هو فن حماية المعلومات عن طريق تحويلها إلى رموز معينة غير مقروءة لا يمكن حلها إلا من خلال مفتاح سري يقوم بتحويل تلك الرموز إلى نص عادي مقروء[38].

و هو تغيير لمظهر المعلومات بحيث يختفي معناها الحقيقي ، من خلال إخفائها عن كل من ليست له صفة الاطلاع عليها أو العبث بمحتوياتها بتغيير شكلها إلى صورة لا يمكن فهمها إلا بعد إرجاعها إلى صورتها الأصلية ، و ذلك لا يمكن أن يتم إلا باستخدام مفتاح معين لا يملكه إلا صاحب الحق في الاطلاع على المعلومات.[39] كما يقصد بتشفير البيانات كل تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها[40] . و الهدف من إجراء التشفير هو ضمان حفظ الخصوصيات و عدم السماح لأحد بالعبث بها أو الاطلاع عليها و ذلك لكونها سرية أو خاصة جدا .[41]

إذ يقوم التشفير كإجراء بتوفير الثقة و الأمان في المعاملات الالكترونية ، حيث يسمح من خلال أدوات ووسائل و أساليب تحويل المعلومات بهدف إخفاء محتوياتها و الحيلولة دون تعديلها أو استخدامها غير المشروع بحيث يتم التأكد من أن المعلومات بهدف إخفاء محتوياتها و الحيلولة دون تعديلها أو استخدامها غير المشروع بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي ذات البيانات التي قام المرسل بالتوقيع عليها .[42]

تقوم تقنية التشفير على تغيير محتوى الرسالة الالكترونية باستخدام برنامج مخصص يسمى مفتاح التشفير ، حيث يجري تشفير الرسالة قبل إرسالها عن طريق هذا البرنامج الذي يمكن المرسل إليه من استعادة الصورة الأصلية لمحتوى الرسالة عن طريق العملية العكسية للتشفير[43] .

يتم التشفير وفقا للضوابط و القواعد المتمثلة في[44] :

أ- إباحة تشفير البيانات و المعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الالكترونية.

ب- احترام سرية البيانات المشفرة و اعتراف بحق أصحابها في الخصوصية بتجريم الاعتداء عليها.

ت- استخدام التشفير كوسيلة معتد بها قانونا في شأن تحرير البيانات و المعلومات بواسطة الجهات المختصة.

تجدر الإشارة إلى أنه ونظرا لأن التشفير يسمح بتلافي بعض المخاطر المتوقعة من استخدام الطرق الالكترونية في التجارة الالكترونية ، فقد اهتمت به المواثيق الدولية و منها الاتحاد

الأوروبي في توجيهه رقم 1993/1999 الصادر في 13 ديسمبر 1999 بشأن إطار أوروبي للتوقيع الالكتروني،حيث عرف هذا التوجيه الشخص الذي يتولى عملية التشفير بأنه :" كل شخص طبيعي أو اعتباري يقدم شهادات الصحة و التوثيق و الخدمات الأخرى المتعلقة بالتوقيع الالكتروني ".كما ألزم التوجيه مقدم هذه الخدمة بالقيود الواردة في التوجيه رقم 46/95 الصادر في 24 أكتوبر 1995 في شأن حماية البيانات الشخصية، و التزامه بعدم جمع هذه البيانات سوى من الشخص المعني أو برضاء صريح منه ، و أن تتعلق هذه البيانات بالشهادة المطلوبة [45].كما أن عديدا من التشريعات أوجبت الاعتماد على التشفير كتقنية لحماية التوقيع الالكتروني و جميع المعاملات التجارية الالكترونية،حيث أوجب القانون الفرنسي الصادر في 26 جوان 1996 استخدام التشفير أو الترميز من أجل حماية التجارة الالكترونية و حماية سريتها[46]. فقد أعطى هذا القانون المشروعات الصغيرة الحق في تشفير رسائلها ومعلوماتها، بعد أن كان قاصرا على المجالات العسكرية الدبلوماسية و الحكومية[47] .كما اعتمد قانون التجارة الالكترونية الأمريكي و الصادر في 30 يونيو 2000 التشفير كوسيلة للتعامل في التجارة الالكترونية ، خاصة تشفير التوقيع الالكتروني .[48]كما وقعت مسودة إعلان مشترك للتجارة الالكترونية بين دول مجلس التعاون الخليجي و الولايات المتحدة الأمريكية ، و تضمنت النص على التوقيع الالكتروني و تقنيات التشفير للحفاظ على السرية والخصوصية و أمن المعلومات و التجارة الالكترونية. كما نصت على ضرورة احترام سرية البيانات المشفرة والاعتراف بحق أصحابها في الخصوصية.[49]

كما سار مشروع قانون التجارة الالكتروني المصري على قبول مبدإ تشفير البيانات وفقا للقواعد والضوابط الخاصة بتشفير المحررات و البيانات الالكترونية . وقد عرفه بأنه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها. وقد أحال ذلك المشروع على اللائحة التنفيذية وضع القواعد والإجراءات المنظمة لاستيراد أو تصنيع أجهزة و برامج خاصة بتشفير المحررات من خلال ترخيص مسبق من الوزارة المختصة ، و بإنشاء مكتب للتشفير يمثل جهة إيداع لمفاتيح الشفرة و حماية البيانات المشفرة و قصر فضها على صدور أمر قضائي بذلك[50].أما اللائحة التنفيذية للقانون المصري رقم 15 لسنة2004 فقد عرفت التشفير بأنه منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة و تحويل البيانات و المعلومات المقروءة الكترونيا بحيث تمنع استخلاص هذه البيانات و المعلومات إلا عن طريق استخدام مفتاح أو مفاتيح تلك الشفرة[51].

أما المشرع التونسي فقد اعترف بالتشفير و عرفه من خلال الفصل 5/2 بأنه استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم

من قبل الغير أواستعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها[52]. كما قضى المشرع التونسي بتجريم الاعتداء على البيانات المشفرة [53].

على الرغم من الفائدة التي يحققها نظام التشفير فانه يتميز بنوع من الخطورة بحيث أنه يجعل من مهمة الشرطة مستحيلة أحيانا ، فقد يمنعها من اكتشاف الجرائم التي تتضمنها الحاسبات الآلية ، مما يجعل إقامة الدليل على ارتكاب الجريمة مستحيلا[54]. لذلك اتجهت العديد من دول العالم إلى حظر عمليات التشفير المعقدة أو وضعها تحت السيطرة الحكومية أو القضائية ، لضمان مراقبة العمليات المشبوهة التي تتم عبر تلك الشبكة[55].

و نظرا لخطورة تقنية التشفير أصدرت بعض الدول مثل هولندا ،مشروع قانون يخضع عملية التشفير للحصول على ترخيص مع الالتزام بإيداع مفاتيح الشفرات لدى مكتب متخصص ملتزم بالسرية ، و الذي يجب عليه أن يقدم هذه المفاتيح لرجال البحث الجنائي الذين حصلوا على أمر بالضبط و التفتيش من سلطات التحقيق ، و إن كان احتمال إفشاء مثل هذه المفاتيح قد يضعف من وسائل الحماية ضد الجرائم المعلوماتية.[56] وتجدر الإشارة إلى أن المشرع الفرنسي لوعيه أن استخدام التشفير في نقل المعلومات قد يسهل الأنشطة الإجرامية ، تدخل و ضبط هذه العملية بنصوص قانونية [57].

و يرى البعض[58] أنه من عيوب نظام التشفير أنه كثيرا ما ينجح الحدس و المنطق في أسلوب فك الشفرات ، كما يمكن للعمليات التكرارية التي يطلق عليها اسم التنفيذ المتكرر في علم إعداد البرامج أن يتم من خلالها فك تلك الشفرات الخاصة بالرسائل بدون أن يقوم ذكاء الإنسان بتعقب النتائج أثناء عملية فك الشفرة .و يمكن كذلك برمجة جهاز الحاسب الآلي بحيث يقوم باستخدام الرسالة المشفرة باستمرار و بكل الطرق الممكنة و يتم التوقف عند العثور على معنى الكلمة المشفرة .[59]

ثانيا : أنواع التشفير

تختلف أنواع و أشكال برامج التشفير، وتعتمد على مفهوم أن كل معلومة مشفرة تحتاج إلى ثلاثة عناصر مجتمعة لإعادتها إلى أصلها ؛ و بناءا على ذلك ظهرت ثلاثة مصطلحات هي المفتاح العام[60] ، المفتاح الخاص [61]و رقم الأساس،حيث أن أي معلومة مشفرة يمكن الاطلاع عليها بوجود هذه المفاتيح الثلاثة معا، فبهذه الطريقة لا يستطيع أحد فك الشفرات و قراءة المعلومات المحمية دون اكتمال الحلقة التي لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام و المفتاح الخاص.[62]

وسنتناول فيما يلي أهم أنظمة التشفير المتعددة :

1-التشفير باستخدام المفتاح المتماثل :[63]

يقوم هذا النظام على استخدام مفتاح متماثل للتشفير و حله ، حيث يقوم المنشئ بعد كتابة الرسالة وتشفيرها بتزويد المرسل إليه بذات المفتاح المتماثل ، ليتسنى له بعد تلقي الرسالة المشفرة حلها و استعادة محتوى الرسالة في صورتها الأصلية .[64]

2- نظام التشفير بالمفتاح العام أو ما يعرف بنظام التشفير غير المتماثل[65] :

يقوم هذا النظام على استخدام مفتاحين ؛ مفتاح عام وآخر خاص . و المفتاح العام متاح لكل شخص ، ويقتصر استخدامه على التشفير فقط . أما المفتاح الخاص فيكون شخصيا غير معروف إلا بالنسبة للمرسل إليه ، و يقتصر استخدامه على حل شفرة الرسائل المشفرة بالمفتاح العام [66].وعليه يتم تشفير المعلومات طبقا لهذا النظام بالرقم العام ، لكن لا يمكن فك الشفرة إلا بالمفتاح الخاص لصاحب المفتاح العام.[67]

3-المزج بين نظامي المفتاح المتماثل و المفتاح العام :

يعتبر هذا النظام مختلطا[68] ، حيث تتم عملية التشفير وفقا له على النحو التالي :

يقوم المنشئ بعد كتابة الرسالة بتشفيرها بالمفتاح المتماثل و تشفير المفتاح المتماثل بالمفتاح العام وإرسالها بعد ذلك للمستقبل الذي سيقوم بحل شفرة المفتاح العام عن طريق مفتاحه الخاص ، ليحصل بذلك على المفتاح المتماثل المستخدم في تشفير الرسالة المستلمة ، ليقوم بعدها بحل شفرة الرسالة باستخدام المفتاح المتماثل.

4-نظام التشفير باستخدام المفتاح العام المزدوج :

يستخدم هذا النظام في تشفير التوقيع الالكتروني ، حيث يتم تشفيره بالمفتاح الخاص للمرسل و القيام بعدها بتشفير كامل للرسالة مفتاح المرسل إليه العام و إرسالها لوجهتها ، باستلام المرسل إليه للرسالة المشفرة يقوم باستخدام مفتاحه الخاص لتسترجع بذلك الرسالة صيغتها الأصلية.[69]ولحل شفرة التوقيع يجري استخدام مفتاح المرسل العام ، لنكون أمام درجتين من التشفير[70] :الدرجة الأولى للتوقيع الخاص بالمنشئ مرسل الرسالة ، و الذي يتم تشفيره بمفتاحه الخاص ، و لحل هذه الشفرة لابد من استخدام مفتاحه العام ، و بذلك يتم التيقن من شخص الموقع.الدرجة الثانية من التشفير هي متن الرسالة ، و التي يتم تشفيرها بمفتاح المرسل إليه العام ، و لحل هذه الشفرة يقوم المرسل إليه باستخدام مفتاحه الخاص ، حيث يضمن بذلك سلامة المحرر من أية تعديلات أجنبية.

ثالثا : مستويات التشفير

يتم تشفير البيانات على عدة مستويات[71] :

1- مستوى الاتصال أو النقل Transmission Level بتشفير كل ما يمر عبر وصلات الاتصالات عند نقطة الإرسال ثم حلها عند نقطة الاستقبال مثل نظم الشبكات الخاصة المؤمنة.

2- مستوى التصفح Session Level بتشفير البيانات المتداولة بين برنامج المتصفح الموقع مثل نظام طبقة المقابس الآمنة(SSL) Secure Socket Layer ، ونظام تأمين بروتوكول الاتصال Secure Hyper text Transport Protocol(SHTTP).

3- مستوى التطبيق Application Layer باستخدام التشفير الجزئي مثل نظام تأمين المعاملات الالكترونية(SET) Secure Electronic Transaction ، و نظام محفظة النقد سايبر كاش Cyber Cash Wallet .

4- مستوى الملفات بتشفير الملفات و الرسائل مثل نظام نورتل انترنست Nortel Entrust و نظام الخصوصية Pertly Good Privacy (PGP).

غير أن استخدام مستوى واحد من التشفير يحقق درجة أمان لكن المألوف هو استخدام أكثر من نوع واحد للتشفير لضمان درجة تامين و سرية أعلى فعلى سبيل المثال أصبحت المعاملات المالية تشفر باستخدام نظام تأمين المعاملات الالكترونيةSET بالإضافة إلى تشفير لمستوى التصفح باستخدام تأمين المقابس(SSL)Secure Socket Layer.

ونتولى فيما يلي شرح بروتوكولي[72] أو نظامي SET وSSL .

1-بروتوكول الصفقة الالكترونية الآمنةSET :

الصفقة الالكترونية الآمنة Secure Electronic Transaction هي بروتوكول أمن مصمم بالاشتراك بين ماستر كارد و فيزا بمساعدة ميكروسوفت وNestcap وIBM وGTE وSAIC شركات أخرى ، والغرض من الصفقة الالكترونية الآمنة هو توفير الأمن لمدفوعات البطاقة عند عبورها الانترنت من مواقع التجار و البنوك .[73]

تستخدم مواصفات SET بيانات خفية أساسية عامة و شهادات رقمية لضمان صلاحية كل من المستهلكين والتجار. كما يقدم بروتوكول السرية و تكامل البيانات و توثيق المستخدم و التاجر و عدم نسخ بيانات المستهلك.

تتم عملية السداد وفقا لبروتوكل SET بإتباع الآلية التالية[74] :

1-يقوم المتسوق بالشراء من التاجر الذي يتبع مواصفات SET و باستخدام محفظة الكترونية مركبة على برواز و يبعث المستخدم معلومات مالية مشفرة من المحفظة مع شهادته الرقمية .

2-يقوم سيرفر الويب للتاجر بتحويل صفقة المشفرة إلى مركز معالجة بطاقة السداد و الذي يفك شفرة الصفقة و يتم تنفيذها .

3-يقوم مركز معالجة بطاقة السداد بتحديد مسار الصفقة و توجيهها إلى المؤسسة المالية التي أصدرت بطاقة سداد المستهلك للموافقة.

4-يتلقى التاجر إعلانا من بنك المستهلك بالموافقة على الصفقة ، بعدئذ يحمل حساب بطاقة سداد المستهلك بقيمة الصفقة.

5-يقوم التاجر بعمل قسائم البضاعة و يضيف قيمة الصفقة إلى مجموعة صفقات بطاقة السداد التي حولت أخيرا إلى بنك التاجر لإيداعها.

2- بروتوكول تأمين المقابس أو البيانات SSL[75] :

يطلق على هذا البروتوكول[76] تسمية بروتوكول طبقة الفتحات الآمنة أيضا.

و هو عبارة عن برنامج به بروتوكول تشفير متخصص لنقل البيانات و المعلومات المشفرة بين جهازين عبر شبكة الانترنت بطريقة آمنة بحيث لا يمكن قراءتها لغير المرسل إليه.[77] وتختلف عن بقية طرق التشفير في عدم طلب اتخاذ أية خطوات لتشفير المعلومات المراد حمايتها من مرسل البيانات ، فكل ما يفعله المستخدم هو التأكد من استخدام هذا البروتوكول .[78]

فتقنية تأمين البيانات ما هي إلا أحد أنواع التكنولوجيات المستخدمة في تشفير مجموعة المعلومات التي تنتقل عبر الانترنت بحيث تقتصر إمكانية إعادة المحتوى على المرسل و المستقبل فقط[79]. يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم المشتري بجهاز خادم خاص لموقع الشراء إذا كان الخادم مزودا بهذه التقنية ، و يقوم البرنامج بتشفير أي معلومة صادرة من المتصفح وصولا إلى جهاز خادم الموقع باستخدام بروتوكول تحكم النقل و بروتوكول الانترنت TCP/IP[80].يهدف بروتوكول تأمين طبقة المقابس إلى تأمين نقل المعلومات ، و البيانات بين العميل و الوحدات التجارية ، و بصفة خاصة تأمين بيانات بطاقات الدفع البنكية ، و قد تم تطوير هذا البروتوكول بواسطة إحدى الشركات التي تعمل في مجال تقديم برامج التصفح عبر مواقع الويب المنتشرة على الانترنت ، وهي شركة NESTCAPE .[81]

يضمن نظام (SSL) مستوى كاف للإرسال الآمن ، مثلا المراسلات الخاصة برقم بطاقة الدفع على الخط ؛ ولا يجب تأمين المعلومات فقط حين إرسالها على الخط ، و إنما ضمان هذه الحماية طول مدة صلاحية المعلومة.[82] ورغم أن بروتوكول SSL Secure Socket Layers يحول بيانات السداد والمعلومات الحساسة الأخرى بأمان بين التجار والعملاء إلا أن SSL لا يتحقق من أن المستهلك هو صاحب السداد الذي يمتلك بطاقة السداد[83].

الفرع الثاني : حماية المواقع الالكترونية و الشبكات الداخلية من خلال جدران الحماية

في إطار تسهيل تبادل المعلومات و البيانات بين جميع الفروع للبنك ، يقوم هذا الأخير بربط فروعه المتعددة بشبكة واحدة بقصد تسهيل تبادل المعلومات و البيانات بين جميع الفروع ، و تسمى هذه الشبكة بالشبكة الداخلية الخاصة .و يمكن أن يقوم البنك بإنشاء شبكة خاصة افتراضية و هي عبارة عن قناة اتصال مشفرة تقام من خلال شبكة غير آمنة مثل الانترنت ، و تكون هذه الشبكة الافتراضية في العادة رابطة بين شركتين أو موقعين لتشفير جميع الرسائل المتبادلة بينها.[84]

وإذا ما أراد البنك الدخول إلى شبكة الانترنت ، فعليه ربط شبكته الخاصة بالانترنت ، غير أن ذلك من شأنه أن يجعل موقع البنك عرضة للمقتحمين ، الأمر الذي جعل البنوك تلجأ إلى استخدام أنظمة خاصة لحماية الشبكة الداخلية من تلك المخاطر عن طريق إقامة حاجز يفصل بين الشبكة الداخلية و شبكة الانترنت[85] . وقد اصطلح على تسمية هذا الحاجز بجدار الحماية أو الجدار الناري[86] .

يقصد بجدار الحماية مجموعة الأنظمة التي توفر وسيلة أمنية بين الانترنت و شبكة المؤسسة الداخلية والخروج منها للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول للشبكة بدون صفة . حيث تمنع جدران الحماية من دخول الأخطار القادمة من شبكة الانترنت إلى الشبكة الداخلية الخاصة بالمؤسسة البنكية .[87]و يتمثل الجدار الناري في برنامج يمكن أن يكون على هيئة جهاز متكامل أو برنامج يتم تحميله إلى الحاسب الآلي بمواصفات جيدة ، وظيفته حماية شبكة الحاسب الآلي الداخلية و شبكة الانترنت ، ووظيفته الرئيسية مراقبة كل البيانات الداخلية و الخارجية من الشبكة والتأكد من مطابقتها لشروط المستخدم التي يحددها البرنامج من قبل.[88]

تستخدم جدران الحماية بالخصوص في تركيز الإجراءات الأمنية عند نقطة واحدة لأن ذلك أفضل من توزيعها، فرض السياسة الأمنية التي يريدها البنك على عملائه ،تسجيل وقائع استخدام الموقع بدقة عند مرورها بجدار الحماية و الحد من درجة تعرض الشبكة الداخلية للأخطار القادمة من الانترنت.[89]غير أن هذه الجدران لا تحمي من أخطار الاتصالات التي لا تمر عبرها كتلك التي قد تتم عن طريق مودم مركب في أحد أجهزة الشبكة الداخلية وكذا من الأخطار الحديثة التي لم يضع الجدار الحماية منها، لذلك فان تحيينه ضروري كلما ظهرت أخطار جديدة . كما أنها لا تحمي من الأخطار القادمة من الشبكة الداخلية نفسها ، فالجرائم كما يمكن أن يرتكبها أشخاص من خارج الشبكة يمكن أن ترتكب من داخلها مثل موظفي البنك نفسه أو أحد المكلفين بصيانة برامج و نظم البنك و آخرين ممن يملكون الكفاءة التقنية للتلاعب بالبيانات من داخل الشبكة.[90]

و يمكن القول بأن وظيفة الجدار الناري تنحصر في أنه يقوم بعملية مسح للمعلومات التي تصل من شبكة الانترنت و يقوم بتحليلها ، و عندما يجد أي شك في المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة فانه يقوم بمنع هذه المحاولة و طردها خارج الشبكة ، أما إذا كانت المعلومات عادية و آمنة فان الجهاز يسمح لها بالمرور و الدخول على أجهزة الحاسبات الآلية [91]. تجدر الإشارة إلى أن جدران الحماية متنوعة[92]، فقد يكون الجدار الناري برنامجا[93] أو جهازا . غير أنه ومهما اختلفت أشكالها و مع تعدد الشركات الصناعية فان جميعها تعمل بنفس الفكرة أو التقنية فهي تشكل نظام أمن لحماية شبكة المنظمات ضد

المقتحمين و المخربين يمنع الأجهزة المستخدمة للشبكة من الاتصال مباشرة مع حواسب خارج الشبكة .كما أن هذه الجدران تتساوى تقريبا في قدراتها في حماية الشبكة و يكمن الاختلاف فيما بينها في طريقة تركيبها و تشغيل برمجيتها.

الخاتمة:

في ختام هذه الورقة البحثية ، يجدر بنا القول أن الحماية التقنية للمعلومات بشكل عام و في مجال التعامل البنكي الالكتروني ليس بالأمر السهل ، لكنه أمر ضروري لابد من تجسيده على الميدان ،لان اختراق سرية تلك المعلومات سيؤدي بالإضرار بمصالح البنوك و كذا الأفراد المتعاملين بمثل هذا النظام الالكتروني للدفع .كما أن السماح للقراصنة و المجرمين بانتهاك تلك السرية سيؤدي لا محالة إلى زعزعة الثقة في المعاملات الالكترونية و إلى العزوف عن التعامل بأسلوب الدفع الالكتروني مما سيؤثر على نمو الاقتصاد الوطني للدول .فلابد من تظافر الجهود على كل الأصعدة لمكافحة هذا النوع من الإجرام الحديث ولابد من العمل على توفير الإمكانيات المادية و البشرية اللازمة لذلك و العمل على تكوين مستخدمي البنوك في مجال تقنية الاتصالات الحديثة و توعية المستهلكين و تحسيسهم .

في ختام هذه الورقة البحثية تجدر الإشارة إلى بعض النتائج المتوصل إليها و المتمثلة في أن :

- العبث بالمعلومات الالكترونية هو من أهم المخاطر الناتجة عن استخدام الانترنت في المجال البنكي.

- سجل مؤخرا عديد من عمليات السطو على المعلومات الالكترونية و البيانات المستخدمة في المعاملات البنكية الالكترونية.لذلك فالمعلومات لم تعد في مأمن .

- بدأ اهتمام المشرع الجزائري مؤخرا بموضوع الخصوصية و أمن و سرية المعلومات المتداولة الكترونيا ، و الدليل على ذلك إصداره لقانون التوقيع و التصديق الالكترونيين. و كذلك تنظيمه للتجارة الالكترونية بقانون خاص.

- لا يمكن الاكتفاء بالحماية المدنية أو الجزائية للمعلومات المتداولة الكترونيا ، إنما ينبغي الاهتمام بنوع آخر من الحماية تتميز بالطابع التقني ، و هي حماية قبلية وقائية تهدف إلى منع التعدي على المعلومات الالكترونية و حمايتها ضد أية محاولة للعبث فيها.

الهوامش:

[1]- ذكر مجلس الشيوخ الفرنسي في اقتراحه لتعريف نظام المعالجة الآلية للمعطيات بأن هذا النظام هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، و التي تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الربط ، والتي تربط بينها مجموعة من العلاقات و التي عن طريقها تتحقق نتيجة معينة و هي حماية معالجة المعطيات ، على أن يكون هذا المركب خاضعا لنظام الحماية الفنية .انظر علي عبد القادر قهوجي،الحماية الجنائية لبرامج الكمبيوتر ،المكتبة القانونية،القاهرة ،1999 ،ص 120.

[2]- عبد الفتاح بيومي حجازي ،النظام القانوني لحماية التجارة الالكترونية ، الكتاب الأول ، ص 133 .
- خثير مسعود ،الحماية الجنائية لبرامج الكمبيوتر – أساليب و ثغرات – دار الهدى ، الجزائر ، 2010 ، ص 111
[3].

[4]- طارق إبراهيم الدسوقي عطيه ، الموسوعة الأمنية الأمن المعلوماتي ، دار الجامعة الجديدة ، الإسكندرية ،2015 ، ص 549.
- محمد دباس الحميد و ماركو إبراهيم نينو، حماية أنظمة المعلومات ، دار الحامد للنشر و التوزيع عمان ،
[5]الأردن ، 2007 ،ص 34 .

[6]-أحمد أنور بدر ، الاتصال العلمي ، دار الثقافة العلمية ، القاهرة ، دون سنة نشر ، ص 17 .

[7]- نائلة عادل محمد فريد ، المرجع السابق ، ص 97 .

[8]- القرار الصادر في 22 ديسمبر 1981 ، متعلق بإثراء المصطلحات المعلوماتية في فرنسا .

[9]- الفقرة العاشرة من المادة الثانية من قانون المعاملات التجارية الالكترونية الأمريكي لسنة 1999 .

[10]- المادة الأولى من القانون الاتحادي رقم 1 لسنة 2006 المتعلق بالمعاملات التجارية الالكترونية .

[11]- كلمة قرصنة تعني في أصلها و معناها الدقيق كل عمل عنف غير مرخص به يرتكب بقصد النهب من قبل سفينة خاصة ضد سفينة أخرى في أعالي البحار، و منذ أوائل القرن الثامن عشر صار وصفا يطلق على نهب المصنفات المنشورة للغير و نسخها دون ترخيص بقصد الاتجار.و من هذا المنطلق شاع استخدام تعبير قرصنة البرامج لوصف عملية النسخ غير المشروع لبرامج الغير .و يقصد بقرصنة البرامج كل أخذ غير مصرح به أو استيلاء أو إعادة إنتاج أو استخدام لبرنامج معلوماتي في الوظيفة المعد لأدائها طالما كان البرنامج معترفا به كمادة ذات قيمة .أما بالنسبة للقرصنة المعلوماتية فيقصد بها نسخ البرامج بصورة غير شرعية أو الحصول على المعلومات المختزنة إما بصورة مباشرة عن طريق الحصول على كلمة السر سواء بالحيلة أو بإجراء تجارب مع الكلمات التي تستخدم لهذا الغرض ، و إما بصورة غير مباشرة عن طريق التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسب ثم ترجمتها . محمد السعيد راشدي ، الإنترنت و الجوانب القانونية لنظم المعلومات ، دار النهضة العربية ، القاهرة ، 2004 ، ص 31-32

[12]- طارق عبد العال حماد ، التجارة الالكترونية :الأبعاد التكنولوجية و المالية و التسويقية و القانونية ، الدار الجامعية ، ط2 ، الإسكندرية ،2007 ، ص 101-102. [12]

[13] -David Davies, Computer Virus-the major computer abuse treat of 1988,p2.

[14]- تقوم هذه البرامج بجمع المعلومات التي يريدها الهاكرز ثم ترسلها إليه ، حتى و لو كانت هناك جدران نارية لحماية الأجهزة من الاختراق ، وذلك لقدرة هذا النوع على استغلال نقاط ضعف في معظم برامج حماية الجدار الناري التي تتحكم في خروج و تصوير المعلومات من الجهاز أو الشبكة المحلية بواسطة Http and Ftp، و أشهر الأمثلة على هذه الأنواع Caligula , Marker and groow، حيث تساعد هذه البرامج قراصنة الكمبيوتر على التحكم الكامل في أي جهاز تصل إليه ، و من أمثلة ذلك برنامج يسمى Back orifio program and net Bus program.كما توجد برامج قادرة على التحكم عن بعد و تستطيع تسخير هذه الأجهزة لتنفيذ الهجوم المنسق و تعطيل عمل المواقع المشهورة .عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 213 .

[15]- وصفت هذه الحادثة في العديد من الدول باطلاع فيروس شرير عبر شبكة المعلومات الدولية (الانترنت) عرف باسم "ميليسا" ، حيث تم التمكن من اعتقال مبرمج حاسب آلي من ولاية نيوجرسي في شهر نيسان عام 1999 ، و اتهم باختراق اتصالات عامة و التآمر لسرقة خدمات الحاسب الآلي ، و تصل العقوبات الموجهة لميليسا إلى

السجن لمدة 40عاما و الغرامة التي تقدر بحوالي 500 ألف دولار ، و قد صدر في هذه القضية مذكرات اعتقال و تفتيش بلغ عددها 19 مذكرة .غانم مرضي الشمري ، الجرائم المعلوماتية ، الدار العلمية الدولية ، عمان ، الأردن ، ط1، 2016 ،

[16]- تعد حادثة موريس أحد أول الهجمات الكبيرة و الخطرة في بيئة الشبكات ، ففي تشرين الثاني من عام 1988 تمكن طالب يبلغ من العمر 23 عاما ويدعى من إطلاق فيروس عرف باسم دودة موريس عبر الانترنت أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الانترنت من ضمنها أجهزة العديد من المؤسسات و الدوائر الحكومية ؛ و قد قدرت الخسائر لإعادة تصليح الأنظمة و تشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة . و قد حكم على موريس بالسجن لمدة 3سنوات و عشرة آلاف غرامة.سامي علي حامد عياد ، الجريمة المعلوماتية و إجرام الانترنت ، دار الفكر الجامعي ،الإسكندرية ، ص 97.

[17]- توجد برامج حديثة من حصان الطروادة تعد الأخطر على الإطلاق ، حيث أنها تستفيد من مزايا البرامج السابقة ، بالدمج بين الخصائص المختلفة لها ، حيث يكون لها خاصية التكاثر مثل الفيروسات مع عدم حاجتها لبرنامج محتضن تماما مثل الديدان ، ولديها القدرة على التعامل مع الملفات الصادرة أوالواردة.فهي برامج جديدة تتمتع بالقدرة على تخطي و خداع جدران النار ، و بالتالي جمع كلمات عبور و أسماء مستخدمين وأرقام بطاقات الائتمان ، وكذلك تدمير بعض الملفات و تعديل مهامها . عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 213.

[18]- طارق عبد العال حماد ، المرجع السابق ، ص 160.

[19]- هناك طرق أخرى لزرع أحصنة طروادة عبر البريد الالكتروني كانتقاله عبر المحادثة و كذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها .كذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص عند زرع ملف الباتش في جهاز الضحية (الخادم) فانه يقوم مباشرة بالاتجاه إلى ملف تسجيل النظام لأنه يؤدي ثلاثة أمور رئيسية في كل مرة يتم فيها تشغيل الجهاز تتمثل في فتح بوابة أو منفذ ليتم من خلالها الاتصال ،تحديث نفسه و جمع المعلومات المحدثة بجهاز الضحية استعدادا لإرسالها للمخترق فيما بعد و تحديث بيانات المخترق في الطرف الآخر.و تكون المهمة الرئيسية لملف الباتش فور زرعه مباشرة فتح منفذ اتصال داخل الجهاز المصاب تمكن برامج المستفيد (برامج الاختراقات) من النفاذ ؛ كما أنه يقوم بعملية التجسس بتسجيل كل ما يحدث بجهاز الضحية أو انه يقوم بعمل أشياء أخرى حسب ما يطلبه المستفيد كتحريك الماوس أو فتح باب محرك و كل ذلك يتم عن بعد ، فيتم الاتصال بين الجهازين عبر بوابات أو منافذ اتصال قد يظن البعض بأنها منافذ مادية في إمكانه رؤيتها كمنافذ الطابعة و الفأرة ، و لكنها في الواقع جزء من الذاكرة له عنوان معين يتعرف عليه الجهاز بأنه منطقة اتصال يتم عبره إرسال و استقبال البيانات و يمكن استخدام عدد كبير من المنافذ للاتصال و عددها يزيد عن 65000 يميز كل منفذ عن الآخر رقمه .و بعد أن يكون المخترق قد تمكن من وضع قدمه الأولى بداخل جهاز الضحية بعد زرع ملف الباتش به و رغم خطورة وجود هذا الملف بجهاز الضحية فانه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك فهو مجرد خادم ينفذ ما يصدر له من أوامر و لكن دونه لا يتمكن المخترق من السيطرة على جهاز الضحية عن بعد ، و حتى يتم له ذلك فان على المخترق بناء حلقة وصل متينة بينه و بين الخادم عن طريق برامج خاصة تعرف ببرامج الاختراق.و تبقى من جانب آخر أحصنة الطروادة عديمة الفائدة إن لم يتمكن المخترق من التعامل معها و هي تفقد ميزتها الخطرة حالما يتم اكتشافها .سعيدي سليمة و من معها ، المرجع السابق ، ص 77.

[20]- يقصد بأمن المعلومات حماية أصول و موارد و مكتسبات أي نظام معلوماتي ما بطرق مشروعة ، وهو أيضا أداة تتحكم في تنظيم البيانات والعلاقات والاتصالات و ذلك دون أن يؤثر على قدرة مستخدمي هذا النظام على الأداء أو يعوق عملهم من حيث الكفاءة أو التوقيت. طارق إبراهيم الدسوقي عطيه ، المرجع السابق ، ص 489.
- محمود محمد أبو فروة ،، الخدمات البنكية الالكترونية عبر الانترنت ، دار الثقافة ،عمان ،الأردن ، 2009 ،
[21]ص 76.

[22]- حسن طاهر داوود ، أمن شبكات المعلومات ، معهد الإدارة العامة ، السعودية ، 2004 ، ص 101-103.

[23]- تقتضي عملية التعاقد مع البنوك لأجل الاستفادة من الخدمات البنكية الالكترونية لهذه الأخيرة أن يطلب البنك من عميله اختيار الهوية التي سيتعامل بها مع البنك على الانترنت userlentification ، و كلمة مرور سرية secret pass word لا يعرفها إلا العميل ، أو أن يقوم البنك بتزويد عميله بالهوية و كلمة المرور بإرسالها على بريده الالكتروني.محمود محمد أبو فروة ، المرجع السابق ، ص 85.

[24] - Russel De Borah, computer security basics,O.Reiily & associates ,1991,p48.

[25]- يقصد بالوسائل التأمينية لأنظمة الدفع الالكتروني إلزام الشركات المنتجة للبرامج بوضع عراقيل فنية تقنية للحيلولة دون دخول المتلصصين أو القراصنة إلى تلك البرامج و ما تحويه بنوك المعلومات و قواعد البيانات و البريد الالكتروني من أسرار تجارية و صناعية أو مراسلات خاصة.طارق إبراهيم الدسوقي ، المرجع السابق ، ص 549.

[26]- نفس المرجع، ص 549.

-نضال سليم برهم ، أحكام عقود التجارة الالكترونية ،دار الثقافة ، عمان ،الأردن ، ط1 ،اص2 ،2009، ص
[27]161.

[28]- تعد بطاقة الدفع الذكية بطاقة بلاستيكية تحتوي على رقيقة ذكية تسمى Micro processor puce و التي تمثل كمبيوترا مصغرا يمكن طبع برمجته لتلبية بعض الوظائف ، و تتم برمجة البطاقة الذكية من قبل شركات مختلفة ، حيث تعمل على إدخال بعض المعلومات في الذاكرة مثل اسم صاحب البطاقة وعمله و معلومات أخرى.

[29]- نفس المرجع ، ص 160.

[30]- محمود محمد أبو فروة ، المرجع السابق ، ص 87.

[31]-من أكثر أساليب السطو على كلمات السر استخداما هو ما يعرف بأسلوب الاقتحام العشوائي أو التخمين العشوائي ، حيث يقوم المقتحم بتجربة كل القيم الممكنة أو يقوم باستخدام كلمات القاموس مثلا .و قد ظهرت على شبكة الانترنت مجموعة من البرامج تقوم بهذه المهمة بسرعة فائقة مثل برنامج LOphetcrack و يقوم هذا البرنامج بالتخمين العشوائي لمعرفة كلمة السر و يمكن من خلال عدة ساعات من المحاولة معرفة كلمة السر ويمكن كذلك أن يقوم المجرم بانتحال شخصية البنك أو أحد موظفيه طالبا من العميل إعادة إرسال اسم المستخدم و كلمة السر حيث توجد العديد من البرامج على الانترنت تسمح بتزوير مصدر الرسالة.حسن طاهر داوود ، المرجع السابق ، ص 143.

[32]- تتمثل في مجموعة من العمليات الحسابية يتم من خلالها توليد مجموعة من الحروف ذات طول معين مستنتجة رياضيا من مجموعة من الحروف أطول بكثير والتي تمثل الرسالة المراد تشفيرها ، كما تستخدم هذه العملية كذلك لاكتشاف تزوير البيانات ، حيث أن أي تغيير و لو كان بسيطا في الرسالة الأصلية يؤدي إلى تغيير كبير في القيمة الاختبارية .

[33]- حسن طاهر داوود ، المرجع السابق ، ص 139.

[34]- يعتبر جهاز التوثيق جهازا ذا شاشة و مجموعة مفاتيح يكون متصلا مع البنك و مملوكا له و يقوم باستخراج كلمات أو أرقام بشكل عشوائي عند الضغط على احد مفاتيحه و هذه الأرقام تظهر عند البنك الذي يتأكد من صحتها.

[35]- محمود محمد أبو فروة ، المرجع السابق ، ص 89.

-محمد عبد الصمد ، الجريمة المعلوماتية و الاحتساب عليها ، مؤتمر القانون و الكمبيوتر و الانترنت ، المجلد [36]الثالث ، ص 875.

[37]- جميل عبد الباقي الصغير ، الجوانب الاجرائية المتعلقة بجرائم الانترنت ، المرجع السابق ، ص 15.

[38]- عصام عبد الفتاح مطر ، التجارة الالكترونية في التشريعات العربية و الأجنبية ، دار الجامعة الجديدة ، الإسكندرية ،2009،ص 62.

[39]-عادل محمد شريف و من معه ، المرجع السابق ، ص 398.

- عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية ، دار الفكر الجامعي ، الإسكندرية ، [40]2002 ، ص 311.

[41]-عصام عبد الفتاح مطر ، المرجع السابق ، ص 62.

- مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية ، القاهرة ، 2001 ، [42]ص 31.

[43]- محمد إبراهيم أبو الهيجاء ، المرجع السابق ، ص 133.

- هدى حامد قشقوش ، الحماية الجنائية للتوقيع الالكتروني ، مؤتمر الأعمال المصرفية الالكترونية بين [44]الشريعة و القانون ، ص 590.

[45]- مدحت عبد الحليم رمضان ، المرجع السابق ، ص 33.

[46]- نص المشرع الفرنسي على التشفير بموجب القانون الصادر في 1990 ، ثم وضع القرار رقم 98-101 الصادر في 24 /02/ 1998 المحدد للضوابط المتعلقة بالتشفير. Feral Schuhl,cyberdroit ,le droit à l'épreuve de l'internet,Dalloz,Paris,1999,p167

[47]- مدحت عبد الحليم رمضان ، المرجع السابق ، ص 32.

[48]- عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية ،الكتاب الأول ،المرجع السابق، ص 205.

[49]- هدى حامد قشقوش ، المرجع السابق ، ص 60.

[50]- نصت اللائحة التنفيذية لقانون التوقيع الالكتروني المصري على تقنية التشفير و المعايير و الضوابط الخاصة بهذه التقنية في المادة الثالثة من اللائحة ، كما نصت على استخدام المفتاحين العام و الخاص و المعروفة باسم تقنية شفرة المفتاح العام بوصفها منظومة تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحا شفرة منفردين أحدهما عام متاح الكترونيا للكافة ينشأ بواسطة عملية حسابية خاصة ، و تستخدم في التحقق من شخصية الموقع على المحرر الالكتروني و التأكد من صحة و سلامة المحرر الالكتروني الأصلي و الآخر مفتاح شفرة خاص بصاحبها ينشأ أيضا بواسطة عملية حسابية خاصة ، و تستخدم في وضع التوقيع الالكتروني على المحررات الالكترونية و يحفظها الشخص بنفسه و بدرجة عالية من السرية و يتم الاحتفاظ بها على بطاقة ذكية مؤمنة و يأتي دور جهات التصديق الالكتروني في مطالعة الأرقام العامة و الخاصة و التأكد من صحتها

بوصفها شريكا في كل التعاملات و بما يسمح في توفير الثقة لتلك المعاملات الالكترونية بأساليب و وسائل بهدف إخفاء محتوياتها واستخدامها بطريقة غير مشروعة .خالد مصطفى فهمي ، المرجع السابق ، ص 103 .

[51]-المادة 2 من اللائحة التنفيذية للقانون المصري رقم 15 لسنة 2004 بشأن تنظيم التوقيع الالكتروني و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[52]-الفصل الثاني من القانون التونسي رقم 83 لسنة 2000 الخاص بالمبادلات و التجارة الالكترونية .

[53]- الفصل 48 من القانون التونسي رقم 83 المؤرخ في 9 أوت 2000الخاص بالمبادلات و التجارة الالكترونية .

[54]- من القضايا التي منع استخدام التشفير من إقامة الدليل على ارتكاب الجريمة ما حدث في قضية السيد، حيث نشرت رسائل عنصرية و مضادة للهودية تحمل اسم و تم اكتشافها على أحد المواقع بعنوان و الذي تم إيواءه في أمريكا .إلا أن المحكمة لم تستطع إقامة الدليل على أن هذا المتهم هو صاحب الرسالة المجرمة .و أضافت المحكمة أن وجود اسم المتهم في نهاية المقال لا يعني أنه قد صدر عنه على أساس أن هذا الاسم لا يمكن لأي شخص أن يكتبه إمعانا في التمويه ، الأمر الذي يقتضي إلزام متعهد الوصول بتحديد شخصية المشترك و عدم توصيل الأسماء المجهولة بالانترنت. BERTHOU(Renaud),internet et le respect des principes essentiels du droit du for, disponible à l'adresse http//www.juriscom.net/universite/mémoire.12/presentation.htm.p86.

[55]- طعن أحد الأساتذة بجامعة Westernبعدم دستورية القانون الذي يحظر تصدير برامج التشفير و التكنولوجيا المتعلقة بها. إلا أن المحكمة رفضت دعواه على أساس أن التشفير ليس عقبة أمام ممارسة حرية التشفير التي نص عليها الدستور.

[56]- طارق إبراهيم الدسوقي عطية ، المرجع السابق ، ص 560 .

[57] -loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications.J.O du 27 juillet 1996.

- أيمن عبد الحفيظ ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية ، مطابع الشرطة ، 2005 ، ص 149.

[58]

[59]- قام مكتب التحقيقات الفدراليFBI باعتقال المحاضر الروسي الذي ألقى محاضرة في مؤتمرDEF CON الخاص بالمخترقين الذي يعقد سنويا بمدينة بالولايات المتحدة الأمريكية(لاس فيجاس).و كانت هذه المحاضرة في المؤتمر الذي عقد في شهر يوليو 2001 ، حيث ألقى محاضرة عن طريقة مبتكرة لفك تشفير هيئة الكتب الالكترونيةE.BOOK التي تنتجها شركة Adobe .و عقب إلقائه المحاضرة قامت قوات منFBI باعتقاله تلبية لشكوى تقدمت بها شركة ضد شركة Elcom Soft التي يعمل البرنامج بها ، و هي شركة روسية تعمل في مجال إعداد برامج لكشف كلمات السر و فك الشفرات .و قد سعت شركة Adobeإلى إيقاف موقع الشبكة على الانترنت و منعها من بيع برنامج فك التشفير الخاص بهيئة E.BOOK و هو ما نجحت في تحقيقه في شهر أغسطس 2001 . فادي سالم ،المخترقون و خبراء أمن المعلومات وجها لوجه ، مجلة النسخة العربية ،العدد العاشر ، أكتوبر 2001 ، ص 123 .

[60]- المفتاح العام هو رقم يتم تداوله بين بقية المستخدمين لتشفير أي معلومات أو رسالة الكترونية مخصصة للشخص و يعتبر رقمه العام أساس التشفير.

[61]- المفتاح الخاص هو النصف الآخر المكمل للمفتاح العام للوصول إلى رقم الأساس و إعادة المعلومات المشفرة لوضعها الطبيعي قبل التشفير ، ويميز هذا المفتاح كل شخص عن غيره ، و يكون بمثابة هوية الكترونية تمكن

صاحبها من فك أي معلومة مشفرة مرسلة إليه على أساس رقمه العام، لذلك يجب عليه الاحتفاظ بالمفتاح الخاص سرا.

[62]- عبد الحميد بسيوني ، التجارة الالكترونية ، دار الكتب العلمية ، القاهرة ، 2008 ، ص 155 .

[63]- تعرف هذه الطريقة أيضا بالنظام السيمتري للتشفير ، ويقصد بها أن مصدر الرسالة و المرسل إليه يستعملان مفتاح تشفير واحد لفك رموز الرسالة التي لم ترسل بعد، حيث يرسل المفتاح أولا بطريقة آمنة ثم ترسل بعد ذلك ، وهذه التقنية تستخدم مجموعة من الأرقام العديدة و المعقدة التي تجعل من المستحيل تزويرها.عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية ، المرجع السابق ، ص 211 .

[64]- محمد إبراهيم أبو الهيجاء ، المرجع السابق ، ص 134 .

[65]- يطلق على هذه الطريقة أيضا تسمية طريقة الهندسة العكسية ، و يستخدم فيها مفتاحان أحدهما عام و الآخر خاص ، و كلاهما له علامات رياضية معقدة لا يعرفها إلا صاحب المفتاح ذاته ، و المفتاح الخاص لا يعرفه سوى صاحبه و لا يمكن للآخر معرفته ، أما المفتاح العام فقد يكون معلوما لبعض الجهات لكن يبقى مع ذلك سرا بالنسبة للجمهور. هدى حامد قشقوش ، المرجع السابق ، ص 76 .

[66]- تتم عملية التشفير و حلها وفقا للآلية التالية :بعد أن يفرغ المنشئ من إعداد رسالته يقوم بتشفيرها بالمفتاح العام و إرسالها في النهاية إلى وجهتها ليقوم المرسل إليه بعد استلامه للرسالة المشفرة بقراءتها بعد حل شفرتها باستخدام المفتاح الخاص .محمد إبراهيم أبو الهيجاء ، المرجع السابق ، ص 135.

[67]- عبد الحميد بسيوني ، المرجع السابق ، ص 156 .

[68]- يتجاوز استخدام هذا النظام سلبيات الأنظمة السابقة ، حيث سيتم التغلب على مشكلة إرسال المفتاح المتماثل عبر قنوات آمنة لحل شفرة الرسالة من ناحية ، و اقتصار الوقت في تشفير رسالة البيانات باستخدام المفتاح العام و حلها من ناحية ثانية .

[69]- إن نظام التشفير العام المزدوج للتوقيع الالكتروني لا يبقي أدنى شك في شخصية الموقع ، فهو يفوق قدرة التوقيع العرفي المحتمل تزويره.محمد رأفت رضوان ، المرجع السابق ، ص 80 .

[70]- محمد إبراهيم أبو الهيجاء ، المرجع السابق ، ص 138 .

[71]- عبد الحميد بسيوني ، المرجع السابق ، ص 159 .

[72]- في البداية كانت الحكومة الأمريكية هي المالك لشبكة الانترنت ، ثم انتقلت الملكية إلى المؤسسة القومية للعلوم(مؤسسة أمريكية) ، إلا أنه في وقتنا الحاضر لا يمكن القول أن هناك مالكا لشبكة الانترنت إنما هناك ما يسمى بمجتمع الانترنت ، و ليس هذا فقط و إنما التمويل ، فبعد أن كان التمويل حكوميا أصبح التمويل يأتي من القطاع الخاص ، و من هنا أصبح هناك العديد من الشبكات الإقليمية ذات الغرض التجاري التي تعرض الاستفادة من خدماتها بمقابل مالي ، و قد نجم عن الوضع المتفرد للانترنت عدد من العناصر أهمها استخدام مجموعة من البروتوكولات الاتصالية القياسية لتبادل المعلومات.عايد رجا الخلايلة ، المسؤولية التقصيرية الالكترونية ، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب و الانترنت ،دار الثقافة ، عمان ، الأردن ،2009 ، ص 62 .

[73]- طارق عبد العال حماد ، المرجع السابق ، ص 135 .

[74]- إن قبول معيار SET كان بطيئا ، حيث تلقى استقبالا فاترا في الولايات المتحدة الأمريكية ،فحتى الآن ، لم تجتذب عددا كبيرا من التجار والمستهلكين ووفقا لما ذكره النائب الأول للتجارة الالكترونية لدى ماستر كارد فان 80 في المائة من أنشطة SET في الدول الآسيوية و الأوروبية، وجزء من المشكلة التي تواجه قبول SETهو ما يبدو أنها ليست سهلة التطبيق ، و أنها وسيلة ليست رخيصة مثل ما توقعت معظم البنوك والتجار، و قد كان رد

الفعل المثالي لكثير من البنوك إزاء هو رد فعل بنك باركليز البريطاني ، حيث ذكر مدير تكنولوجيا المعلومات لذلك البنك بأن نظام SET ليس ملائما وغير مجرب و غير مختبر وببساطة لسنا بحاجة إليه. طارق عبد العال حماد ، المرجع السابق ، ص 135.

[75] -Secure Socket Layer .

[76]- يقصد بمصطلح بروتوكول في مجال الانترنت اتفاق يحكم الإجراءات المستخدمة لتبادل المعلومات بين كيانين متعاونين (نهايتين طرفيتين أو جهازين من أجهزة الكمبيوتر أو أكثر)يشمل الاتفاق على كيفية إرسال الرسائل و كيفية العودة إلى الوضع السوي من أخطاء الإرسال ؛ و بصورة عامة فان البروتوكول يتضمن شكل الرسالة الالكترونية و تسمى القواعد الخاصة بها و القواعد التشفيرية الخاصة بالرسائل المرسلة بتتابع صحيح. عايد رجا الخلايلة ، المرجع السابق ، ص 63.

[77]- عبد الحميد بسيوني ، المرجع السابق ، ص 159.

[78]- يستخدم مع تكنولوجيا التشفير نظام الشهادات الموثقة الذي ينفذه طرف ثالث لتأكيد أن العميل الحقيقي هو الذي يتعامل مع الموقع و بذلك يتم من خلال الجمع بين هاتين الوسيلتين ضمان سرية المعاملات التجارية و عقد صفقات آمنة فحينما تقوم إحدى الشركات بإنشاء موقع لها باستخدام جهاز خدمة أمن يتفق الحاسوبان على رموز حسابية شفرية و مفاتيح تشفير خاصة تستخدم تقنية تأمين البيانات في تفكيكها و إعادة جمعها و يزود كل مستخدم أو عميل بمفتاحين للتشفير. عبد العال حماد ، المرجع السابق ، ص 176.

[79]- نضال سليم برهم ، المرجع السابق ، ص 176.

[80]- عبد الحميد بسيوني ، المرجع السابق ، ص 159.

[81]-لزهر بن سعيد النظام القانوني لعقود التجارة الالكترونية ، دار هومه ،الجزائر، 2012 ، ص 167.

[82] - Solange Ghernaouti-Hélie , sécurité internet , stratégie et technologie, édition dunod,Paris,p129.

[83]- ذكرت منظمتا فيزا و ماستر كارد علنا أن الهدف من عرض بروتوكول SET هو إيجاد طريقة مفردة للمستهلكين و التجار لاستعمالها في إجراء صفقات بطاقة السداد على الانترنت .طارق عبد العال حماد ، المرجع السابق، ص 134.

[84]- حسن طاهر داوود ، المرجع السابق ، ص 385.

[85]- محمود محمد أبو فروة ، المرجع السابق ، ص 93.

[86]- تقوم جدران الحماية بدور حارس البوابة بين الانترنت و الانترنت ، و أكثر هذه البرامج شيوعا مرشحات الرزم Packet filters و جدران الحماية المستخدمة على مستوى التطبيق Application level firewalls، حيث يقوم مرشح الرزم ، وهو يعمل بصورة نمطية على جهاز يسمى السير Router فحص عنوان المصدرSource و عنوان الوجهةDestination لكل رزمة من البيانات سواء كانت داخلة إلى شبكة الشركة أم خارجة منها ، و يمكن للمرشح منع رزم آتية من عناوين معينة من الدخول إلى الشبكة ، و أن يمنع رزما أخرى من الخروج منها ، أما جدار الحماية المستخدم على مستوى التطبيق ، فانه يقوم بفحص مضمون البيانات المتداولة بالانترنت إضافة إلى العناوين ، لذلك فهو أبطأ من مرشح الرزم ، و لكنه يسمح للجهة صاحبة شبكة الحاسب بتنفيذ خطة أمنية أكثر تفصيلا.طارق إبراهيم الدسوقي ، المرجع السابق ، ص 550.

[87]- إسماعيل عبد النبي شاهين ، أمن المعلومات في الانترنت بين الشريعة و القانون ، مؤتمر القانون ،الكمبيوتر و الانترنت ، المجلد الثالث ، ص 976.

[88]- طارق إبراهيم الدسوقي عطيه ، المرجع السابق ، ص 556.

[89]- محمود محمد أبو فروة ، المرجع السابق ، ص 94.

[90]- حسن طاهر داوود ، المرجع السابق ، ص 263.

[91]- أيمن عبد الحفيظ ، المرجع السابق ، ص 158.

[92]- توجد برامج عديدة لجدران النار من ذلك برنامج شبكة D.A.N، و الذي يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار Fire Walls، و مزودات بروكسي Proxy Servers التي تحتفظ بصفحات الشبكة على القرص الصلب و مرشحات عناوين arl filters،حيث تشبه برامج جدران النار حرس الحدود على الساحل ، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيادة الشبكة المحمية دخولا أو خروجا دون أن يكون مصرحا له بذلك.و تشبه مزودات بروكسي الشاحنات العسكرية الخاصة بالتموين ، التي تجلب البضائع ، و هي في هذه الحالة صفحات الشبكة الخارجية ، حيث يعاد توزيعها داخليا ، و تساعد عملية التوزيع الداخلي على خفض حركة المرور عبر بوابة الدخول إلى الشبكة المحلية ، لأنها تلغي الحاجة إلى استدعاء البيانات مرة ثانية من مواقعها على شبكة انترنت ، إذ سبق استدعاءها و حفظها على القرص الصلب في الشبكة المحلية ، و تستخدم كذلك مزودات بروكسي لمنع دخول البيانات الوافدة من الانترنت إلى الحاسب الآلي بالشبكة المحلية بصفة جزئية أو كلية.أما مرشحات U.R.L فهي عبارة عن فلتر يمنع مستخدمي الشبكة من الدخول إلى مواقع معينة على شبكة الانترنت ، و بالتالي تعطي صاحب الشبكة أو مالكها الحق في التحكم في مستخدمي الشبكة أن يدخلوا أولا إلى مواقع معينة غير مرغوب فيها على الشبكة .

[93]- يعتبر برنامج zone alarm من أشهر برامج الجدران النارية نظرا لكفاءته غير المحدودة في ضبط و رصد كافة محاولات الاختراق على الأجهزة و قيامه بإعطاء إشارة عند حدوث أي اعتداء ، كما أن هذا البرنامج يمكنه القيام بتفقد مرفقات البريد الالكتروني و التي أصبحت أحد مصادر الفيروسات ، بحيث يقوم باحتجازها أو طردها أو مسحها.و يلاحظ كذلك أن هذا البرنامج قبل قيامه يحذف أي من البرامج يتيح للمستخدم فرصة تفحص الملفات ثم يقرر تشغيلها أم لا. D.Brent Chapman ,Elizabeth,buiLding internet fire wall,reillu associates,september,1995,p88