الفصل العاشر

تأمين التجارة الالكترونية

تشفير البيانات بعد الاعتداءات على مواقع التجارة الالكترونية[1] طبق المتعاملون نظام التشفير للمحافظة على المواقع التي يتعاملون بها وفي الوقت الحالي أصبح أغلب المتعاملين على الإنترنت يقومون بتشفير أي معلومات تخصهم. ويهدف التشفير لمنع أي متطفل على هذه المواقع من التقاط المعلومات بحيث يعمل المتعاملان على تحويل المعلومات إلى إشارات ورموز وبيانات بحيث لو أطلع عليها أي شخص لما فهم منها شيء. وكان التشفير في البداية عمليه سهله ومبسطه مما جعل المتخصصين المهرة يستطيعون حلها والدخول لهذه التعاملات لذلك أصبح الآن هناك أسلوبين متطورين[2] للتشفير:

أولاً: وتستخدم هذه الطريقة بأن يكون هناك مفتاح واحد يتم الاتفاق عليه لفك رموز الشفرة ثم بعد ذلك يتم إرسال الرسائل وتبادلها وعادة يكون هذا الأسلوب معقداً.

ثانيًا: ويستخدم هنا مفتاحين أحدهما عام والآخر خاص، وعادة يكون المفتاح العام هو لمواقع التجارة الالكترونية وهذا معلوم لأغلب الذين يتعاملون بالشراء عن طريق الإنترنت، أما الخاص فهو يكون للمتعامل مع هذا الموقع بالتحديد بحيث يدخل بمفتاحه للموقع ويتم التعامل بين الطرفين.

برنامج (الخصوصية الفائقة) وهو برنامج تشفير يستخدم أسلوب المفتاح العلني وهو يوزع مجانًا على مواقع شبكة الإنترنت ولأي شخص استخدامه ومتاح لمن يريد معرفة آلية التشفير.

ويعتبر التوقيع على شيء معين المحدد الأساسي لهوية الموقع والدليل الثابت على الموافقة لأنه يتم بخط يده، ولم تتراجع أهميته بالرغم من التعامل بالوسائل الحديثة لعقد الصفقات التجارية ولذلك نجد قانون المعاملات الالكترونية الأردني قد تطرق في المادة الأولى منه إلى تعريف التوقيع حيث جاء فيها "التوقيع الالكتروني": البيانات إلى تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجه بشكل الكتروني أي وسيله أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها وتميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه.

(1) د. عبد الفتاح حجازي ـ الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ـ المرجع السابق.
(2) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

ومن خلال ذلك نجد أن الهدف من التوقيع هو التأكد من أن الشخص الذي يتعامل عبر الإنترنت ليس متدخل أو متلاعب، وكذلك لرفع مستوى الأمن والخصوصية والمحافظة على سرية المعلومات والرسائل والمفاوضات قبل التعاقد. والتوقيع إما أن يكون بشكل أرقام محدده إذا ما انهي بها مستخدم الكمبيوتر رسالته فإنها تكون بمثابة التوقيع أو أن تكون مجموعه من الأحرف أو أي رمز يختاره الشخص أو إشارة معينه وقد يكون التوقيع عن طريق استخدام القلم الالكتروني وهو قلم يتم الكتابة به على شاشة الكمبيوتر ويقوم الأخير بالتقاط التوقيع والتحقق من صحته. ونجد الآن هناك وسائل أحدث من اتخاذ رموز أو أحرف. . . إلخ للتوقيع الالكتروني، حيث أصبح بالإمكان اتخاذ البصمة الشخصية، أو مسح العين البشرية أو خواص اليد البشرية أو التحقق من نبرة الصوت أو صورة الوجه الفسيولوجية وذلك من خلال أجهزه دقيقه وكاميرات أصبحت تضاف إلى أجهزة الكمبيوتر بحيث عند بداية المفاوضات يتم طلب البائع من المشتري أخذ صوره أو نبرة الصوت ويتم تخزينها مشفره داخل الحاسب وعند أي مفاوضات أو إتمام للبيع يتم التأكد من مطابقة بين البيانات التي تؤخذ حاليًا وما سبق أخذه[٣].

استخدام الجدران النارية وتعتبر هذه برامج وأجهزه تفصل شبكة المعلومات والأنظمة الداخلية للمستخدم عن الشبكة الواسعة للإنترنت. والمقصود بذلك أنه توجد شبكه محمية لا يتم ربطها بأي نظام يمكن الوصول إليه من خارج المنظمة، ويشبه علماء الكمبيوتر هذه الجدران بأنها مصفاة (فلتر) لا تسمح إلا بمرور الاتصالات المرغوب فيها وتمنع عداها، مع الأخذ بعين الاعتبار عدم إعاقة هذه المصفاة لعمليات وأنشطة المستفيد. ويعتبر جهاز (المودم) الطريقة المثلي لتطبيق هذا الأسلوب الذي اتجه الآن الكثيرون لتركيبه على حواسيبهم.

وهناك عدة أنواع لجدران الحماية:

أولاً: الموجه الحاجب: وهذا ينظر إلى مقدمات الرسائل فقط وليس للمحتوى وما سمح الجدار بمروره من خلال عنوانه فإنه يدخل للجهاز وغير ذلك لا يسمح بمروره[٤].

ثانيًا: الوسيط: وهذا جدار يقوم بفحص الطلبات الواردة للنظام ولا يتلقي إلا الطلبات السليمة، ومثال ذلك أن هناك شركه تريد إنشاء قائمه بأسعار يطلع عليها العملاء مباشرة بحيث يمكن لأي شخص من خارج الشركة إن يرى المنتجات التي تقدمها الشركة وأسعارها

(3) د. أسامه أبو الحسن مجاهد ـ التعاقد عبر الانترنت ـ دار الكتب القانونية ـ ٢٠٠٢ المرجع السابق.
(4) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

مع عدم التلاعب بهذه الأسعار أو تغيرها أو أن يصل العملاء إلى الأسعار فقط دون الوصول للملفات الحساسة المخزنة على الشبكة الداخلية.

ثالثًا: الحارس: وهذا البرنامج على درجه من التعقيد ـ حيث يتقبل البيانات ويتفحصها ويفسرها وبناء على ذلك يسمح بمرورها أو لا يسمح أو يعطي الإمكانات المتاحة للمرور حسب التعليمات الموجودة مسبقًا في هذا البرنامج المعطاة من المسؤول عن هذا الموقع[٥].

بطاقات الائتمان فكما هناك حماية أوجدها العرف الالكتروني للمفاوضات والتوقيع والبيانات والمعلومات كان لا بد من إيجاد طرق حماية للمقابل المادي لهذه البضائع. وتسليم المقابل المادي بهذه الطرق الحديثة يثير الكثير من المشاكل فهو لا يتم بشكل مباشر بين البائع والمشتري وإنما يتم عن طريق البطاقات الالكترونية وهذه البطاقات هي عبارة عن مستطيل صغير من البلاستيك تحمل معلومات أساسيه عن حاملها، ويتم صرف هذه البطاقات من البنوك وعند التعاقد عبر الإنترنت[٦] يقوم المشتري بإعطاء البائع رقم البطاقة ونوعها وتاريخ انتهاء صلاحيتها بالإضافة لعنوانه البريدي لتصل بعد ذلك بفترة محدده السلعة المطلوبة والتي تم الاتفاق عليها من خلال شبكات البنوك العالمية وشركات الوساطة المالية لتتم عمليات التقلص بين الحسابات وقيد الفوائد والعمولات. وخير مثال على التلاعب ببطاقات الائتمان إن هناك لص يدعي (تيم كورادو) بريطاني الجنسية قام باقتحام عشرات المواقع في شبكة الإنترنت واستولى على بيانات وأرقام ما يزيد على (١٢٤) بطاقة ائتمان تخص عملاء هذه المواقع وبعد استخدام بعض الأموال الموجودة فيها قام بنشر هذه المعلومات على الشبكة بشكل عام.

وحتى الآن لم تستطيع الشرطة إيجاد دليل واحد على تصرفه هذا، وكلما حاولت إخضاعه لمحاكمه استطاع الخروج منها بريئًا، ولوقوع مثل هذه التعديات قام العملاء بتشفير أرقام البطاقات في محاولة منهم لإيجاد طريقه تمنع التعدي على البطاقات[٧]. حماية التجارة الالكترونية من خلال القوانين الوضعية فكما هناك طرق لحماية المواقع ذاتها من خلال المتعاملين تدخلت التشريعات كذلك بوضع نصوص قانونيه لحماية التجارة الالكترونية.

(5) د. رأفت رضوان "عالم التجارة الالكترونية" بحث المنظمة الإفريقية للتنمية المرجع السابق.
(6) خالد الطويل ـ الجريمة الالكترونية عبر الإنترنت ـ المرجع السابق.
(7) د. شريف محمد غانم " محفظة النقود الالكترونية " المرجع السابق.

١. الجدار الناري والتشفير وطرق أمن المعلومات الالكترونية:

أ. مزايا وعيوب الجدار الناري[٨]:

١ـ منع دخول المستعملين غير المصرح لهم بالدخول إلى الشبكة.
٢ـ حماية استعمال الخدمات المهمة عند دخول الشبكة ومغادرتها.
٣ـ حماية عامة من جميع الجهات.
٤ـ توفير الحماية اللازمة للشبكة والمعلومات.
٥ـ توفير خدمات التشفير في تكنولوجيا الجدار الناري.
٦ـ الجدار الناري يتوافق مع جميع الشبكات المفتوحة مثل.
٧ـ تخزين العمليات والمعلومات التي تمر عن طريقه.
٨ـ متابعة المستخدمين للشبكة ومن يحاول العبث بها.

أما عيوبه:

١ـ أنه لا يتعامل مع تنفيذ البرامج الداخلية التي تهاجم النظام.
٢ـ لا يقدم حماية للنقل الإذاعي والتليفزيوني.

ب. التشفير:

كذلك يمكن المحافظة على سرية المعلومات وحمايتها بواسطة (التشفير)، وفكرة هذا النظام هي: أن رسالة ترسل من خلال قناة **Channel** غير آمنة، وهدف العدو هو أن يحصل على المعلومات السرية من خلالها، أو تغيير محتوى الرسالة، وإرسال رسالة أخرى متلاعب بها إلى المستقبل، وقد يستحوذ العدو عن كل شيء، ويمنع وصول الرسالة إلى المستقبل. وفي كل الأحوال لا بد من حماية الرسالة، وضمان وصولها بالشكل المطلوب إلى المستقبل.

وتستخدم طرق التشفير لتحويل الرسالة الأصلية **Plaintest** إلى رسالة مشفرة **C: pretext** بواسطة المرسل، وأكثر طرق التشفير هي تلك التي تعتمد على المفاتيح العامة **Public- key**، وأشهرها استخدامًا **RSA**، اختصار لمخترعيها ريفيست **Rivest**، وشامير **Shamir**، وأديمان **Adleman** وهذه الطريقة تقوم عن مجموعة من الأفكار الرياضية، وما تزال أكثر الطرق فعالية في مجال تشفير الرسائل والمعلومات.

(8) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

تقنيات أخرى:

وهناك تقنيات عديدة أخرى ابتكرها مصممو برامج الحاسبات الالكترونية لحماية الشبكات الخاصة وجعلها آمنة[٩]، وقدمت هذه التقنيات أنواعًا عديدة للأمن وأهمها:

١ـ **أمن الدخول**: وهو يسمح للمستعملين بالربط بالشبكة باستعمال كلمات السر الصحيحة فقط.

٢ـ **أمن نظام الملف**: وهو نظام أمني يعطي قدرة على التحكم في الوصول لنظام الملف وبمقتضاه يمكن حماية البيانات من المتطفلين. ويعطي المستعملين الملتزمين دلائل الوصول إلى الملفات التي يحتاجونها بينما تحفظ هذه الملفات آمنة[١٠].

٣ـ **أمن الحاسب الخادم**: وبمقتضاه يمكن التحكم في الوصول للحاسب الخادم ذاته.

٤ـ **أمن طبع الشبكة**: وبمقتضاه يتم التحكم في الوصول لطابعات الشبكة.

إلى غير ذلك من نظم الأمن الذي لا يتسع المقام لذكرها.

الحماية القانونية لأمن المعلومات في الإنترنت:

٤. أهم صور الاعتداء الجنائي على المعلومات في الإنترنت:

يمكن أن نجمل أهم صور الاعتداء الجنائي[١١] على المعلومات في الإنترنت فيما يلي:

١ـ جرائم النصب والاحتيال عبر الإنترنت عن طريق الدخول على البنوك والمصارف المالية أو إساءة استخدام بطاقة ائتمان الغير.

٢ـ جرائم سياسية عن طريق التجسس على الدول عبر الإنترنت، ومحاولة اختراق أنظمتها العسكرية.

٣ـ جرائم التدمير والعبث بأنظمة الحواسيب، وذلك عن طريق الدخول على الشبكة وتدمير برامج الحاسب، أو تدمير المعلومات، أو نشر مواقع تخريبية وفيروسات.

٤ـ جرائم سرقة حقوق الملكية الفكرية عن طريق نسخ البرامج الأصلية وتسويقها أو استخدامها دون إذن مسبق، مما يعرض الشركات المنتجة لهذه البرامج للكثير من الخسائر المالية.

---

(9) د. عبد الفتاح بيومي حجازي – النظام القانوني لحماية التجارة الالكترونية – الكتاب الأول – دار الفكر الجامعي – الاسكندريه –٢٠٠٢.

(10) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

(11) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

٥ـ الجرائم المتعلقة بإعادة إنتاج المعلومات المسجلة عبر الإنترنت بصورة غير مشروعة، أو تقليدها.

٦ـ سرقة المعلومات بحسبها مجرد معلومات معنوية.

قسم بعض الباحثين في مجال المعلومات قرصنة الفضاء الالكتروني إلى نوعين رئيسين:

الأول: وهم ما يطلق عليهم الهاكرز **Hackers**، وجلهم يستهدف بالأساس إلحاق الأذى بالمحتويات التي تضمنتها الذاكرات والدوائر الالكترونية في شبكات الحواسيب[١٢]، سواء الخاصة بالمؤسسات والشركات أو الأفراد، لمجرد إثبات أنهم قادرون على هذا، لذلك فهم ينظرون إلى أنفسهم على أنهم أبطال أذكياء، بينما يعتبرهم الآخرون مخربين خبثاء.

الثاني: وهم لصوص ومافيا السرقات الالكترونية عبر الإنترنت، وهدفهم الرئيس هو سرقة أموال أو بيانات أو أسرار، تضمنها شبكات حواسيب بعينها، وذلك باستخدام تقنيات خاصة بالاختراقات المعلوماتية **Computer Breaches**.

وتتسم هذه النوعية من الجرائم الالكترونية بسهولة ارتكابها، ما لم تكن ثمة احتياطات وتقنيات مضادة قوية تقف سداً منيعًا أمامها، وأيضًا بسهولة إخفاء معالمها.

ومن أشهر طرق الاختراق التي يستخدمها القراصنة واللصوص:

٧ـ طريقة بث الفيروسات، وهي الطريقة المفضلة لدى القراصنة بوجه خاص، قد اشتهرت بعض الفيروسات في هذه الطريقة منها: فيروس (حصان طروادة)، وفيروس (الحب)، وفيروس (المصيدة)[١٣]، وفيروس (السميدا)، وغير ذلك من الفيروسات.

٨ـ طريقة سرقة الشرائح: وهي من أكثر الطرق تداولاً بين لصوص الإنترنت.

٩ـ طريقة القنبلة الموقوتة: وتتمثل هذه الطريقة في برنامج تخزيني صغير، يلج إلى ذاكرة الحاسب، ويظل كامنًا فيها، إلى أن ينشط في وقت معين.

١٠ـ الطريقة المنطقية: وهي شبيهة بالطريقة السابقة، ووجه الاختلاف يتمثل في أن النشاط التخريبي في حالة القنبلة المنطقية يبدأ عند حدوث حالة تشغيل برامج بعينها، وليس عند وقت بعينه كما في القنبلة الموقوتة.

---

(12) م. حسن داود ـ جرائم نظم المعلومات ـ الرياض ٢٠٠٠.

(13) انظر مؤلفنا الجريمة الالكترونية باب الفيروسات ص ٤٢ ـ الناشر دار العلوم ـ القاهرة ٢٠٠٧.

د. أمن المعلومات وحقوق الملكية الفكرية:

يجهل كثير من الناس مبادئ قانون حق التأليف والملكية الفكرية للمعلومات، فعند استخدامك لشبكة معلومات أو أي نظام معلومات آلي بواسطة الحاسب، فقد تكون مستخدمًا لأعمال محفوظة حق التأليف، ضمن قانون الملكية الفكرية، إلى جانب[١٤].

قانون حق التأليف الذي يحمي أعمال التأليف الأصلية الموثقة، وتشتمل هذه الأعمال على الأعمال، وعلى المؤلفات المطبوعة، كالكتب والقصص والروايات والأبحاث المنشورة وغير المنشورة، والبرامج الإذاعية والتلفازية، أو الأعمال الفنية والرسومات والموسيقا والتسجيلات الصوتية، وقواعد البيانات وبرمجيات الحاسب[١٥]. كما أن حقوق التأليف تحمي المؤلفين والمنتجين والناشرين والموزعين، من الانتحال أو الطبع أو التوزيع غير المرخص.

والحقيقة أن حماية حقوق الملكية الفكرية، وحقوق التأليف من محيط المعلومات الالكترونية، أمر في غاية التعقيد والصعوبة، وتكمن الصعوبة هنا خاصة عندما يتم تخزين المعلومات الالكترونية[١٦]. وقد ظهرت العديد من المشكلات مع بنوك معلومات آلية، حيث تمت أعمال قرصنة تمثلت بنسخ عدد منها بشكل كامل، أو أجزاء كبيرة منها بواسطة أجهزة الحاسب ذكية عالية السرعة والسمعة.

وهكذا يبدو أن قانون الملكية الفكرية سهل الاختراق. إذ من الممكن نقل الأعمال الفكرية من دولة إلى أخرى واستنساخها واستعمالها في أماكن لا يطبق فيها قوانين حماية حقوق التأليف أو الملكية الفكرية، وعليه تنطوي المشكلة القانونية لهذه الحقوق على أكثر من تطبيق القانون على المستوى الوطني بل تمتد إلى حل الخلافات على المستوى الدولي.

فإن الجدار الناري[١٧] هو تطبيق برمجي يقوم بمراقبة جميع البيانات والمعطيات التي تصل إلى الخادم، عن طريق الفضاء السيبراني، بهدف حماية البيانات والمعطيات الأصلية المخزنة على خادم الويب، أو أي خادم آخر متصل بالإنترنت فهو إذن بمثابة الحراسة الأمنية المشددة على

---

(14) أمن المعلومات الالكترونية وحقوق الملكية الفكرية عبدا لرازق مصطفى يونس. ـ مجلة المكتبات والمعلومات العربية (س٢٠، ٢٤، ذو الحجة ١٤٢٠هـ/ أبريل ٢٠٠٠م).

(15) م. حسن داود ـ جرائم نظم المعلومات ـ الرياض ٢٠٠٠.

(16) أد. محمد شريف توفيق ـ ورقة عمل بعنوان (تشخيص أهم المشاكل الناجمة عن التجارة الالكترونية على المستوى القومي وسبل حلها.

(17) د. جابر العرا يشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.

بوابة المؤسسة أو الشركة التي تتفحص بشكل دقيق كل من بداخل، وكشف أي محاولة عبثية وإجرامية، تستهدف التخريب ومن حيث آلية تصميمها، فإن ثمة ثلاثة أساليب للجدارن النارية، وهي:

١ـ فرز مظاريف البيانات والمعطيات المرسلة، حيث إن المعلومات التي تنقل في صورة مظروف الكتروني عبر الفضاء السيبراني لشبكة الإنترنت؛ لا يسمح لها بالدخول إلا بعد فرزها وفحصها بشكل دقيق، ووفق شروط محددة سبق تزويد البرنامج المكون للجدار الناري بها.

٢ـ فرز المظاريف مع تغيير عناوين المظاريف القادمة من الشبكة الداخلية (الصادرة)، ويسمى هذا الأسلوب تقنية الوكيل أو التوسط **Proxying**، وهو أكثر تعقيداً وممانعة من سابقه، وفيه لا يرى من الشبكة الداخلية سوى الجدار الناري، الذي يقوم هو وحده بمهمة استلام المظاريف القادمة (الواردة)، وإجراء عمليات فرز وغربلة دقيقة لها، ومن ثم لفظها واستبعادها إذا كانت عبثية، أو تمريرها وتوجيهها إلى الداخل إذا كانت صحيحة. ومن سمات هذا الأسلوب: احتفاظ الجدار الناري بجدول متابعة يربط بين عناوين المظاريف الصادرة والواردة، بما يوفر مزيداً من الأمان والحماية.

٣ـ أسلوب المراقبة حيث يقوم الجدار الناري في هذه الحالة بمهمة (مراقبة حقول معينة، من المظروف الالكتروني، ومقارنتها بالحقول المناظرة لها، من المظاريف الأخرى، التي تدور في ذات السياق[١٨] ويقصد بالسياق هنا: (مجموعة المظاريف الالكترونية المتبادلة عبر الفضاء السيبراني لشبكة الإنترنت، بين جهازين؛ لتنفيذ عملية ما)، ويجرى لفظ واستبعاد المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده؛ لأن هذا يعد دليلاً دامغًا على أنها زرعت في السياق، وليست جزءاً منه، فتعامل معاملة البرامج المسيئة كالفيروسات ونحوها.

وعلى وجه العموم؛ فإن ثمة أسسًا ومعايير يعتد بها عند فرز المظاريف وغربلتها، ومعرفة صالحها من فسادها ويمكن استخدام واحدة منها أو أكثر، ومن أبرز هذه الأسس والمعايير:

١ـ العنوان الرقمي.

٢ـ اسم النطاق.

(18) د. هدى حامد قشقوش ـ الحماية الجنائية للتجارة الالكترونية عبر الإنترنت ـ المرجع السابق.

٣ـ البروتوكول المستخدم للتخاطب، حيث إن هناك بروتوكولاً يستخدم في نقل البريد الالكتروني، يدعى بروتوكول **SMTP**، بينما هناك بروتوكول يستخدم فقط للدخول على جهاز عن بعد، وتنفيذ أوامر بعينها، وبروتوكول **FTP** الذي يستخدم في نقل الملفات، وخاصة تلك التي تتسم بكبر الحجم. بدلاً من إرسالها كمرفقات **Attachments** في البريد الالكتروني وبروتوكول **HTTP** الذي يعنى بتبادل المعلومات والمعطيات بين برنامج المتصفح ومزود الخدمة في الموقع الذي يريد المتصفح الولوج إليه، وبروتوكول **SNMP** وهو يستخدم في إدارة الشبكات وجمع المعلومات عن بعد.

وبحسب إحصائيات عام ٢٠٠٣م فإن حجم سوق أنظمة الجدران النارية في العالم، قد تجاوز الـ(١,٣) مليار دولار، وأن هذا الحجم في تنام مستمر، ويتوقع أن يصل عام ٢٠٠٩م إلى نحو ١٨,٦ مليار، في حين بلغ حجم سوق أنظمة كشف الاختراق ـ وهي وسيلة أخرى من وسائل صد هجوم القراصنة ولصوص الفضاء السيبراني ـ نحو (٦٠٠) مليون، ويتوقع أن يصل بحلول عام ٢٠٠٩م إلى نحو مليارين من الدولارات.

هل حققت الجدران النارية الحماية المرجوة؟

على الرغم من أن الجدران النارية هي وسيلة الحماية المفضلة، لدى جل المؤسسات والشركات والأفراد الذين يعولون على الإنترنت في إتمام الصفقات وتبادل المعلومات والبيانات.. إلا أن جدران النار ليست بهذه الفولاذية من الممانعة والغربلة التي يطمح إليها الجميع حيث إن ما يبتكر على الجانب الآخر من تقنيات يستخدمها القراصنة واللصوص، يجعل ثمة أبوابًا خلفية للجدران النارية، يمكن لهؤلاء العابثين الولوج منها.. فالمواجهة إذن ستظل مفتوحة، والمستفيد الأكبر هم صناع التقانة ومطوروها، الذين يسوقون بضاعتهم الرائجة حول العالم، ويحصدون البلايين من الدولارات، بينما الخاسر الأكبر هم الذين لا يطورون حوائطهم النارية. وموانع اختراق الشبكات الالكترونية التي يتربص بها قراصنة الفضاء السيبراني ولصوصه.

هـ. أمن المعلومات:

أمن المعلومات من زاوية أكاديمية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها، ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية، وسلامة محتوى، وتوفير المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلالها.

إن الأهداف الأساسية لحماية المعلومات هي:

١ـ منع تسرب أو سرقة أو تشويه أو تزوير المعلومات.

٢ـ تأمين أمن الأفراد والمجتمع والدولة.

٣ـ منع الأعمال غير الشرعية لتدمير أو تشويه أو تطويق المعلومات.

٤ـ حماية الحقوق الدستورية للمواطنين للمحافظة على الأسرار الشخصية وسرية المعلومات الشخصية للأفراد.

٥ـ المحافظة على الأسرار الحكومية، والعسكرية، والتجارية، وسرية الوثائق التي لا يجوز البوح بها.

حماية المعلومات من الموظفين، وقد نشرت مجلة **National Law Journal** الأمريكية مقالاً تضمن عدة إجراءات لحماية أمن المعلومات للشركات والمؤسسات تشمل:

١ـ تقييد الوصول إلى هذه المعلومات، وقصره على من يتطلب عملهم الاطلاع عليها، ويجب أن يشمل هذا الإجراء الملفات اليدوية وملفات الكمبيوتر.

٢ـ إبلاغ الموظفين كتابة، أو في محادثة موثقة، وتدريبهم على التعامل مع المعلومات المقيدة بطريقة صحيحة. وينبغي أن ترسل الإدارة مذكرات دورية لتعزيز هذه الإجراءات والتذكير بها.

٣ـ استخدام اتفاقيات السرية من خلال العمل مع مستشار الشركة القانوني لصياغة اتفاقيات تحمي معلومات المؤسسة.

٤ـ مراقبة وصول الموظفين للمعلومات، إذ يجب توزيع بيان سياسة يوضح أن الشركة ستقوم بعمليات تفتيش على نظم الكمبيوتر، للتأكد من أن المواد السرية تستخدم لأغراض العمل فقط. ويجب فحص برامج الكمبيوتر التي يمكن أن تسجل متى ولأي مدة تم الوصول إلى وثيقة ما وبواسطة من؟ وعلى الموظفين تقديم إقرار مكتوب بأنهم مدركون لهذه السياسة. المعوقات التي تمنع توقيع العقاب على مرتكبي جرائم الكمبيوتر.

٥ـ قلة التشريعات التي تواجه جرائم الكمبيوتر بحيث نجد أفعالا إجرامية لا ينطبق عليها أي نص في قانون العقوبات.

٦ـ جرائم الكمبيوتر ذات بعد دولي فيمكن أن يرتكب الجريمة شخص في خارج القطر المعني، ونظراً لوجود ذلك البعد الدولي، يثور التساؤل حول إمكانية توقيع العقاب على المجرم في الخارج[١٩].

(19) د. هشام رستم شرح قانون العقوبات ـ القسم العام كلية للحقوق جامعة أسيوط ٢٠٠٥.

و. تعريف الأمن:

الأمن في اللغة نقيض الخوف، وقد جاء في قوله تعالى: (وآمنهم من خوف) والأمن في الإسلام لا يقتصر على النواحي المادية وإنما يتجاوزها فيشمل الأمن على الدين والنفس والعقل والعرض والمال[٢٠].

وقد اتسع مفهوم الأمن في هذا الوقت ليشمل الأمن الثقافي، والأمن الغذائي، والأمن الاقتصادي، والأمن الاجتماعي، والأمن العسكري، والأمن الصحي، والأمن الصناعي، والأمن البيئي، والأمن السياحي، والأمن المهني، والأمن الإقليمي، والأمن الدولي، وغير ذلك من المجالات التي يدخل فيها الأمن.

وللمعلومات أهمية كبيرة في كل مجالات الحياة منذ أقدم العصور، ويحدثنا التاريخ أن (القادة العظام كانوا يقهرون الدول، ويفتحون والمدن، ويدحرون الجيوش من دون معارك، بمساعدة المعلومات الهادفة، والإبطال المعنوي ـ النفسي لإرادة العدو في المقاومة).

إن متوسط حجم الأضرار جراء جريمة حاسوبية واحدة تتعلق بدخول غير قانوني على شبكة المعلومات للمؤسسات الأمريكية سوف يبلغ ٤٥٠ ألف دولار أمريكي، كما أن الخسائر السنوية لبعض الشركات تزيد عن ٥ مليارات دولار.

تعريف التشفير Cryptography:

التشفير عبارة عن دراسة التقنيات الرياضية المتعلقة بعدد من مظاهر أمان المعلومات، تكامل البيانات **Data Integrity**، إثبات شخصية الكينونة **Entity Authentication**، وإثبات شخصية مصدر البيانات **Data Origin Authenticotion**. إن التشفير ليس عبارة عن وسيلة لزيادة أمان المعلومات فقط، وإنما عبارة عن مجموعة من التقنيات.

أما نظام التشفير[٢١] هي إخفاء المعلومات الموثقة بطريقة معينة، بحيث يكون معناها غير مفهوم للشخص غير المخول، وإن أي شخص يعترض عبارة معينة (أي يحصل عليها) مرسلة من المشفر إلى مستقبل العبارة يسمى المعترض. إن هدف التشفير هو الزيادة إلى الحد الأقصى لعدم الترتيب لغرض إخفاء المعلومات، لذلك فإن تقليص عدد الاختيارات الممكنة يمكن أن يعرف التشفير أيضًا على أنه علم الكتابة السرية.

(20) د. جابر العرايشي الجدار الناري والتشفير وغيرها من أنظمة أمن المعلومات المرجع السابق.
(21) د. فتحي خليفة علي خليفة التجارة الخارجية كلية التجارة جامعة أسيوط ٢٠٠٥.

أهداف أنظمة التشفير:

إن الهدف الأساسي للتشفير والحفاظ على النص الواضح (أو المفتاح، أو كلاهما) بصورة سرية بعيداً عن الأعداء على افتراض أنهم يملكون كامل القدرة للوصول إلى الاتصالات بين المرسل والمستقبل. إذن الهدف من عملية التشفير هو ضمان الخصوصية وذلك بالاحتفاظ بالمعلومات بصيغة مخفية على أي شخص آخر والذي هو غير الشخص المقصود حتى أولئك الذين يملكون صلاحية الوصول إلى بيانات أخرى مشفرة[٢٢]، أو يقال أن الشفرة قابلة للكسر، إذا كان بالإمكان تحديد النص الواضح أو المفتاح من النص المشفر، أو تحديد المفتاح من زوج المعلومات في النص الواضح والنص المشفر.

يجب ملاحظة أن المفاتيح التشفيرية والنصوص الواضحة التي تملك انتظامات متوقعة تنتج نصوصاً مشفرة يمكن تحليلها لكشف إما النص الواضح أو المفتاح. إن علم التشفير يسعى لتوفير اتصالات أمينة، وعليه أن يقاوم علم تحليل الشفرة. يطلق على أي نظام أنه معرض للخطر، إذا كان بالإمكان استرجاع العبارة الأصلية، أو النص الواضح من النص المشفر بدون معرفة المفتاح المستخدم في خوارزمية التشفير.

علم فتح الشفرة يحتاج إلى تخصص عال في الرياضيات، مثل نظرية الاحتمالية، ونظرية الأعداد، والإحصاء والجبر. إذ يجب على محلل الشفرة أن يكون متمكنًا جداً في كل هذه الحقول، وأن لديه القابلية لاستيعابها كما يجب أن يستفيد من المعلومات الثانوية حول النظام، مثل: طبيعة خوارزمياته، ولغة الاتصال، ومحتوى وسياق العبارات والصفات الإحصائية للغة النص الواضح.

ز. الأمن المعلوماتي:

يعرف الأمن المعلوماتي بأنه: مجموعة الإجراءات المتخذة لحماية الوسط المعلوماتي للمجتمع، أو للدولة، أو للمؤسسة، أو الشركة الخاصة التي تؤمن مقاومة وضع وتلافي عواقب التأثير المعلوماتي ـ النفسي والمعلوماتي ـ الفني للطرف المعني.

الأمن المعلوماتي للأشخاص يتميز بحماية الحالة النفسية والوعي من التأثيرات المعلوماتية الخطرة: التحكم عن بعد بسلوك الأشخاص التضليل بالمعلومات، التحريض على الانتحار، التخلي عن المعتقدات الدينية.

(22) انظر مؤلفنا الجريمة الالكترونية الناشر دار العلوم القاهرة٢٠٠٧.

تنقسم التأثيرات المعلوماتية الخطرة إلى نوعين :

١ـ تأثيرات تهدف إلى ضياع المعلومات القيمة .

٢ـ تأثيرات تقوم على إدخال معلومات سلبية أو كاذبة وبالنسبة للنوع الأول فإن ضياع المعلومات، وعلى الأخص المعلومات ذات الطابع السري .

من شأنه أن يخفض فاعلية النشاط الذاتي، أو يزيد من النشاط العدو، أو الطرف المنافس .

أما إدخال معلومات سلبية أو كاذبة، إلى المنظومة المعلوماتية، فقد يؤدي إلى اتخاذ قرارات خاطئة، وإجبارنا على العمل خلافًا للموقف المتشكل (بشكل يلحق الضرر بنا)، وقد يؤدي إلى انقسام المجتمع .

المعلومات: هي أخبار (معلومات) عن الأشخاص، والشركات، والمنظمات، والأشياء، والوقائع، والظواهر، والأحداث، والعمليات، بصرف النظر عن شكل تقديمها، وهذه المعلومات قد تكون عن شكل بياني، أو نص، أو أرقام، أو على شكل رياضي أو الكتروني، أو غيره .

يرى بعض خبراء أمن المعلومات أن الكفاءة الأمنية، أو أمن النظم الآلية للمعلومات، تعتمد بدرجة عالية تتجاوز الـ٨٠٪ على الأفراد المتعاملين مع تلك الأنظمة، وبصفة خاصة على مدى التزامهم الأخلاقي، ولما كان الالتزام الأخلاقي من الموضوعات الفلسفية، والنظرية المعقدة التي يصعب التحكم فيها، يصبح الحل الواقعي هو تقليص الاعتماد على الأفراد، والاتجاه نحو الكفاءة الإدارية .

بعد التمعن في مفهوم التجارة الالكترونية وأهميتها وطرق حمايتها والتطور والتقدم السريع الذي يضفي على هذه التجارة فإننا نجدها عملت على :

١ـ تعمل التجارة الالكترونية على تيسير توزيع الخدمات العامة مثل الصحة والتعليم والرياضة بأسعار منخفضة وكفاءة عالية .

٢ـ رفع مستوى الجودة على المستوى العالمي وذلك نتيجة لزيادة المنافسة من جهة وانخفاض الأسعار من جهة أخرى وقلة التكلفة بالنسبة للمشترى بدل تبادل المراسلات الورقية وكذلك السرعة حيث يمكن عقد الصفقات خلال فترات بسيطة تتراوح من ساعة الى٢٤ ساعة[٢٣] .

(23) رأفت رضوان عالم التجارة الالكترونية المنظمة العربية للتنمية الإدارية المرجع السابق .

٣ـ وجود التجارة المتخصصة فنجد مثلا هناك مواقع متخصصة بالكتب القانونية فقط وأخرى بالكتب الادبيه دون غيرها وهكذا .

٤ـ القضاء على الطرق التقليدية في العمليات التجارية حيث يستطيع الشخص الآن التسوق والتجول في اكبر سوق عالميه[٢٤] (الانترنت) واختيار الأفضل والمقارنة بين الأسعار والشراء دون ترك المنزل أو البيت .

٥ـ يجب أن نشير هنا إلى تطور الجانب الآخر لتطور التجارة الالكترونية وهو تطور طرق الاعتداء عليها خاصة مع فقدان الآثار الخاصة بهذه الجرائم .

٦ـ وكذلك تعذر جمع الأدلة والإثباتات لمعاقبة مرتكبي جرائم التجارة الالكترونية .

٧ـ صعوبة معرفة الأماكن التي يتم الإبلاغ فيها عن هذه الجرائم وكيفية اتخاذهم للإجراءات والقبض على المعتدين .

٨ـ ولا بد من الاشاره إلى انه بالرغم من تطور هذا النوع من التجارة في الدول الأوروبية إلا انه ما زالت في بداياتها في الدول العربية وخاصة الأردن والتشريعات تعتبر حديثه وليست بتلك الدقة المطلوبة .

(24) ا. د عبدا لهادي سويفي التجارة الخارجية ـ كلية التجارة ـ جامعة أسيوط٢٠٠٦ .