الفصل التاسع

الأمن المعلوماتي لأنظمة المعلومات

الفصل التاسع
الأمن المعلوماتي لأنظمة المعلومات

مقدمة:

ان التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة ومضطردة في أساليب العمل والميادين كافة، إذ أصبحت عمليه انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسوب من الأمور الروتينية في عصرنا الحالي وإحدى علامات العصر المميزة التي لا يمكن الإستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب خزن وتوفير المعلومات حيث أن انتشار أنظمة المعلومات المحوسبة أدى الى أن تكون عرضة للإختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على إقتناءه و توفير سبل الحماية له.

ان موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقاً بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم والتي أثرت على الإمكانات التقنية المتقدمة المتاحة والرامية الى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وبحسب الإمكانات المتوافرة لحمايتها من أي اختراق أو تخريب، وكان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء امنية للمعلومات تضمن الحفاظ عليها.

أولا: مفهوم الأمن المعلوماتي

تشكل المعلومات لمنظمات البيئة التحتية التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لإستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

ومن أجل فهم الأمن المعلوماتي (Information Security) لا بد من تحديد معناه، حيث عرفه (السالمي) بأنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة الى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال، أما (المشهداني) فقد عرفه بأنه (الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر

الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية، أما (أنور) فقد عرفه بأنه مجموعة من التدابير الوقائية المستخدمة في المجالين الإداري والفني لحماية مصادر البيانات من أجهزة وبرمجيات وبيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي الى فقدان بعض المصادر كلاً أو جزءاً، ومن ثم التأثير على نوع ومستوى الخدمة المقدمة، من كل ما سبق يمكن أن نعرف الأمن المعلوماتي بأنه ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزونة في أجهزة الحاسوب إضافة الى الأجهزة الملحقة وشبكات الاتصالات والتصدي للمحاولات الرامية الى الدخول غير المشروع الى قواعد البيانات المخزونة أو تلك التي ترمي الى نقل أو تغيير أو تخريب الخزين المعلوماتي لهذه القواعد.

ثانياً: مراحل تطور مفهوم الأمن المعلوماتي

إن مفهوم الأمن المعلوماتي مر بمراحل تطويرية عدة أدت الى ظهور ما يسمى بأمنية المعلومات، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج والإيعازات ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة وكان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحواسيب (Computer Security) والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق بالمعالجة للحجوم الكبيرة من البيانات، تغير الإهتمام ليمثل السيطرة على البيانات وحمايتها. وفي السبعينات تم الانتقال الى مفهوم أمن البيانات (Data Security) ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة الى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط لخزن نسخ اضافية من البيانات و البرمجيات بعيدا عن موقع الحاسوب، وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى الى الإنتقال من مفهوم أمن البيانات الى أمن المعلومات، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوافرها ودرجة موثوقيتها، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها، وكانت شركة IBM الأمريكية أول من وضع تعريف لأمن المعلومات، وكانت تركز على حماية

البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات وأشارت الشركة الى أن أمناً تام للبيانات لا يمكن تحقيقه ولكن يمكن تحقيق مستوى مناسب من الأمنية، والسؤال الذي يطرح هنا ماذا سيكون بعد أمن المعلومات؟ البعض يقول أمن المعرفة (knowledge Security) وذلك لإنتشار أنظمة الذكاء الإصطناعي وازدياد معدلات تناقل البيانات بسرعة الضوء أو التفاعل بين المنظومات والشبكات وصغر حجم أجهزة الحاسوب المستخدمة.

ثالثا: الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب

لقد أصبح اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الأخيرة ومع مرور الزمن نجد أن على الرغم من سبل الحماية التي تتبعها المنظمات، الى أن هناك ارتفاعا واضحا في معدل الإختراقات مع تنوع الوسائل المستخدمة في الإختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة، فالبعض منها قد يكون مقصود كسرقة المعلومات أو ادخال الفيروسات وغيرها وهي الأشد ضرراً على نظم المعلومات ويكون مصدرها أحيانا من داخل أو خارج المنظمة، وقد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية ويمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات الى ثلاث فئات:

1. **الأخطاء البشرية** Humane Errors: وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو اثناء ادخالها الى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المنظمات.
2. **الأخطار البيئية** Environmental Hazard: وهذه تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق إضافة الى المشاكل القائمة في تعطل أنظمة التكييف والتبريد وغيرها، وتؤدي هذه الأخطار الى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.
3. **الجرائم المحوسبة** Computer Crime: تمثل هذه تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة وبشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة وهي:

أ. **سوء الاستخدام لجهاز الحاسوب**: وهو الاستخدام المقصود الذي يمكن أن يسبب خسارة للمنظمة أو تخريب لأجهزتنا بشكل منظم.

ب- **الجريمة المحوسبة**. وهي عبارة عن سوء استخدام لأجهزة الحاسوب بشكل غير قانوني يؤدي الى ارتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب.

ج- **الجرائم المتعلقة بالحواسيب** : وهي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة.

ويمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة يقومون باختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول الى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة، وتشير الدراسات التي أجرتها دائرة المحاسبة العامة وشركة Orkand للإستشارات الى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود 1.5 مليون دولار لشركات المصارف المحوسبة في الولايات المتحدة الأمريكية، ومن ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن 70% من جرائم الكمبيوتر المسجلة حدثت من الداخل، أي من قبل من يعملون داخل المنظمات، هذا وأن جرائم الحاسوب تزداد بصورة واضحة مما أصبحت تشكل تحديا خطيرا يواجه الإدارات العليا عموما و إدارة نظم المعلومات على وجه الخصوص.

رابعا :الحماية من الأخطار

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب الآتية:

1- العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات.

2- توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة.

3- وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة وأحيانا خارجها.

4- صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية.

5- التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.

6- التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة امكانية التعلم من التجربة والخبرة المتاحة.

7- تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها.

هذا وتقع مسؤولية وضع خطة الحماية للأنشطة الرئيسة على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يأتي:

- الوقاية من الأخطار غير المتعمدة.

- إعاقة أو صنع الأعمال التخريبية المتعمدة.
- اكتشاف المشاكل بشكل مبكر قدر الإمكان.
- المساعدة في تصحيح الأعطال واسترجاع النظام.

ويمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات ويجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار، ويمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات والبرمجيات والشبكات.

خامسا: العناصر الأساسية لنظام الأمن المعلوماتي

إن النظام الأمني الفاعل يجب أن يشمل جميع العناصر ذات الصلة بنظام المعلومات المحوسبة ويمكن تحديد هذه العناصر بما يلي:

1- **منظومة الأجهزة الإلكترونية وملحقاتها**: إن أجهزة الحواسيب تتطور بشكل بالمقابل هناك تتطور في مجال السبل المستخدمة لإختراقها مما يتطلب تطوير القابليات والمهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب والعبث المقصود في الأجهزة أو غير المقصود.

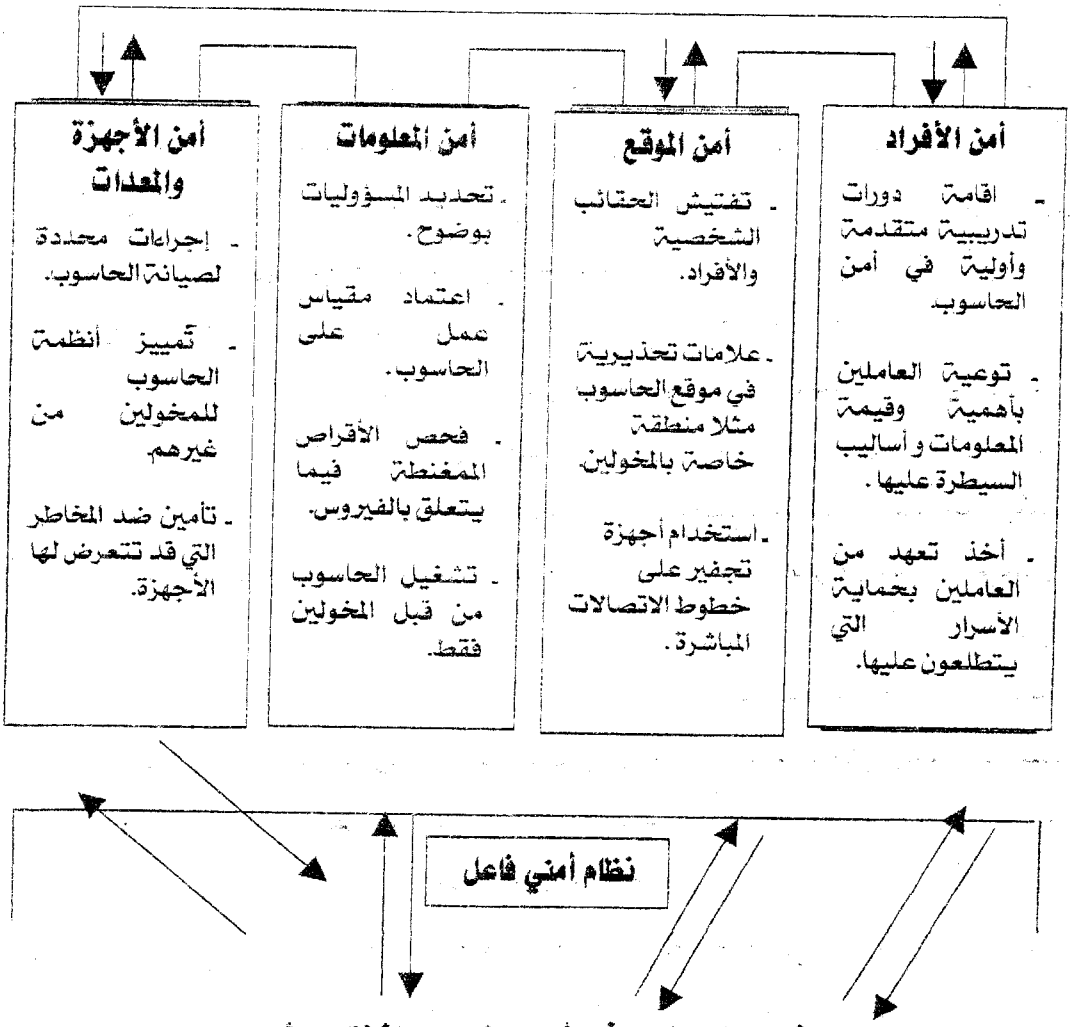
2- **الأفراد العاملين في أقسام المعلومات**: يلعب الفرد دورا أساسيا ومهما في مجال أمن المعلومات والحواسيب وله تأثير فاعل في أداء عمل الحواسيب بجانبيه الإيجابي والسلبي، فهو عامل مؤثر في حماية الحواسيب والمعلومات ولكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة وسرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة الى وضع الخطط لزيادة الحس الأمني والحصانة من التخريب، كما يتطلب الأمر المراجعة الدورية للتدقيق في الشخصية والسلوكية للأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محدودين.

3- **البرمجيات المستخدمة في تشغيل النظام**: تعتبر البرمجيات من المكونات غير المادية وعنصر أساس في نجاح استخدام النظام، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن أن تحقق حماية للبرامج وطرائق حفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الاتصالات، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الإعتبار عند تصميم النظام وكتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول الى النظام وذلك من خلال

أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها، ومحاولة التمييز بين اللذين يحق لهم الإطلاع وحسب كلمات السر الموضوعة، وهناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المجفرة.

4- **شبكة تناقل المعلومات**: تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الإتصالات كما أنها سهلت عملية التراسل بين الحواسيب وتبادل واستخدام الملفات، ولكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كإستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة، لذلك لا بد من وضع إجراءات حماية وضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات وتوفير الأجهزة الخاصة بالفحص، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل الى الشبكة وذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المجفرات وربطها بخطوط الإتصال والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تجفير تناقل المعلومات أو الملفات.

5- **مواقع منظومة الأجهزة الإلكترونية وملحقاتها**: يجب أن تعطى أهمية للمواقع والأبنية التي يحوي أجهزة الحواسيب وملحقاتها، وبحسب طبيعة المنظومات والتطبيقات المستخدمة يتم إتخاذ الإجراءات الإحترازية لحماية الموقع وتحصينه من أي تخريب أو سطو وحمايته من الحريق أو تسرب المياه والفيضانات، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها وتحديد أساليب وإجراءات التفتيش والتحقق من هوية الأفراد الداخلين والخارجين من الموقع وعمل سجل لذلك. ويمكن تمثيل أهم عناصر النظام الأمني الناجح والإجراءات المتعلقة بالنموذج الآتي:



شكل (70) يمثل أهم عناصر النظام الأمني

سادسا : بعض المشاكل المعاصرة التي تواجه أمن أنظمة المعلومات

تواجه أنظمة المعلومات بعض المشكلات الشائعة التي بدأت تغزو أنظمة المعلومات وتساهم في تدميرها أو تخريبها أو سرقة الخزين المعلوماتي المحفوظ في أجهزة الحاسوب ومن أهم هذه المشاكل هي:

1- **الفيروسات** (Virus)

تعتبر من أهم جرائم الحاسوب وأكثرها انتشاراً في الوقت الحاضر، ولم يعد يخفى على أحد ما المقصود بفيروس الحاسوب حتى من العامة ممن لا يستخدموا الحاسوب وذلك بسبب تناقل الصحف لأخبار خسائر الشركات والحكومات والأفراد بسبب تخريب أحدثه فيروس معين، ولم يعد أحد يخلط بين معنى فيروس الحاسوب والفيروس البيولوجي الذي يصيب الإنسان كما كان يحدث سابقا بسبب عدم انتشار ثقافة الحاسوب. ويمكن تعريفه على أنه برنامج حاسوب له أهداف تدميرية يهدف الى إحداث أضرار جسيمه بنظام الحاسوب سواء البرامج أو الأجهزة ويستطيع أن يعدل تركيب البرامج الأخرى حيث يرتبط بها ويعمل على

تخريبها، وهو برنامج مكتوب بإحدى لغات البرمجة من قبل المبرمجين وهو قادر على التوالد والتناسخ ويستطيع الدخول الى البرامج وعلى الأفضلية أكبر من نظم التشغيل تساعده في فحص المكونات المادية مثل الذاكرة الرئيسة أو القرص المرن أو الليزري، وقد ظهرت الفيروسات في نهاية الأربعينات وكان أول من فكر فيها هو اختصاصي الكمبيوتر (جون فون نيومان) حيث نشر مقاله حولها وظهرت بعد ذلك آثار الفيروس في عام 1950 إلا أنها بقيت محدودة الإنتشار حتى عام 1983 عندما تفشت الفيروسات في برنامج UNIX وأثار ذلك ضجة على الساحة العلمية والعملية ثم ظهرت بعض الحوادث الفردية لصغار المبرمجين الذين قاموا بزرع الفيروسات في شبكات الكمبيوتر، فقد قام موريس الذي كان طالبا في جامعة كورنيل بإعداد برنامج مدمر ساهم في تعطيل آلاف من الحواسيب مما كلف الشركات الأمريكية (100) مليون دولار، أما كيفية اكتشاف الفيروس فكان عن طريق مبرمج هندي، حيث قام بعمل برنامج خفي من أجل المحافظة على برنامجه الذي كان أحدث برنامج للطباعة، حيث قام بحمايته من النسخ من خلال دخوله على الملفات التشغيلية وهي في حالة النسخ ثم يقوم بتكبير حجم الملفات ومن ثم تخريبها (أي الملفات المستنسخة) واستمرت مع التطورات الحاصلة في مجال تكنولوجيا الحاسوب والبرمجيات تطور كل من برامج الحماية، مقابل ازدياد حالات ابتكار واعداد برامج فيروسية.

- الإجراءات الوقائية للحماية من الفيروسات

إن التطورات الحاصلة في مجال إعداد برامج الفيروسات جعلت من الصعوبة ايجاد طريقة مضمونة بدرجة كبيرة للوقاية من الفيروسات ولكن هناك بعض الأساليب الفاعلة التي يمكن اتباعها للحماية وهي:

- تركيب برنامج مضاد للفيروسات ملائم لنظام التشغيل المستخدم في جهاز الحاسوب ويفضل أن يكون نسخة أصلية للإستفادة من الدعم الفني للشركات التي يتم شراء البرامج المضادة منها.
- عدم وضع برنامج جديد على جهاز الحاسوب إلا قبل اختباره والتأكد من خلوه من الفيروسات بواسطة برنامج مضاد للفيروسات.
- عدم استقبال أية ملفات من أفراد مجهولي الهوية على الإنترنت.
- عمل نسخ احتياطية من الملفات الهامة وحفظها في مكان آمن.
- التأكد من نظافة أقراص الليزر التي يحمل منها نظام التشغيل الخاص بجهاز الحاسوب.

هذه الأساليب إضافة الى العديد منها التي يمكن اتباعها من شأنها أن تساهم في ضمان حماية أجهزة الحاسوب ولكن يجب أن نضع نصب أعيننا ولا نتصور أن وجود برنامج مضاد

للفيروسات محدث دائما في أجهزة الحاسوب يعني أننا في مأمن من الفايروسات، كما أن أي مشكلة في الأجهزة لا تعني دائما أن هناك فيروسا لذا يجب تحديد سبب المشكلة ومحاولة إيجاد العلاج لها.

2ـ قرصنة المعلومات

قد يسمع الكثير عن ما يسمى بالهاكرز أو مخترقي الأجهزة Hackers ونتساءل كيف يتم ذلك وهل الأمر بسيط الى هذا الحد أم يحتاج لدراسة وجهد، في الحقيقة أنه مع انتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز حاسوب ومن دون عناء فور انزال إحدى برامج القرصنة. والمقصود بالقرصنة هو سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية إما بالحصول على كلمة السر أو بواسطة التقاط موجات الكهرومغناطيسية بحاسبة خاصة ويمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة. أما عن الهدف من عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحيانا بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال أو يكون الهدف الكشف عن أسرار صناعية (تصاميم منتجات) بهدف إعادة تصنيعها دون إجازة قانونية أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية. والأمثلة على حالات القرصنة عديدة فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة وكندا مستخدمة الحاسوب ومن ثم القيام بإنتاج سلع على ضوء ذلك وتصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية ونفس الشيء قامت به شركة متسوبيشي لبناء السفن والصناعات التقليدية حيث استخدمت سماسرة للقيام بعملية التجسس الصناعي.

ـ المخاطر التي تهدد خصوصية المعلومات في العصر الرقمي

تمكن تقنية المعلومات الجديدة خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، ويعود الفضل في هذا الى مقدرة الحوسبة الرخيصة، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزونة في ملف مؤتمت بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبيا، إن هذا بوضوح يكشف الى أي مدى يمكن أن يكون تهديد الخصوصية.

وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات الفيديو) وبطاقات الهوية الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها.

ان استخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثارا ايجابية عريضة، لا يستطيع أحد انكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية وغيرها وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات (Bank Data). وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص، كمراكز وبنوك معلومات الشركات المالية والبنوك وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي.

و إذا كانت الجهود الدولية والاتجاه نحو الحماية التشريعية للحياة الخاصة عموما، وحمايتها من مخاطر استخدام الحواسيب وبنوك المعلومات على نحو خاص، تمثل المسلك الصائب في مواجهة الأثر السلبي للتقنية على الحياة الخاصة فإن هذا المسلك قد رافقه اتجاه متشائم لإستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل لإستخدام الحواسيب قد أثار المخاوف من إمكانات انتهاك الحياة الخاصة، وممكن إثارة هذه المخاوف، أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية كالوضع الصحي والأنشطة الإجتماعية والمالية والسلوك والآراء السياسية وغيرها، يمكن جمعها وخزنها لفترة غير محددة، كما يمكن الرجوع اليها جميعا بمنتهى السرعة والسهولة. ومع الزيادة في تدفق المعلومات التي تحدثها الحواسيب، تضعف قدرة الفرد على التحكم في تدفق المعلومات عنه. ان هذه النظرة كما يظهر لنا، نظرة متشائمة من شيوع استخدام الحواسيب أثرها على تهديد الخصوصية، وهي وان كانت نظرة تبدو مبالغا فيها، الا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية، وتحديدا الحواسيب، في كل ما من شأنه تهديد الحق في الحياة الخاصة، ويمكننا فيما يلي اجمال المعالم الرئيسة لمخاطر الحواسيب وبنوك المعلومات على الحق في الحياة الخاصة بما يأتي:

1- ان الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الإجتماعية أو العمل ..الخ، و تستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول الى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة ..

على سبيل المثال فإن حكومة الولايات المتحدة وفق دراسات 1990 جمعت (4) بليون سجل مختلف حول الأمريكيين، بمعدل (17) بند لكل رجل وامرأة وطفل، ومصلحة الضريبة (IRS) في الولايات المتحدة تمتلك سجلات الضرائب لحوالي (100) مليون أمريكي على حواسيبها، وتملك الوكالة الفدرالية – عدا البنتاجون – ثلاث شبكات اتصالات منفصلة تغطي كل الولايات المتحدة الأمريكية لنقل وتبادل البيانات.

2- ان شيوع (النقل الرقمي) للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، وامكانية استخدام الشبكات في الحصول بصورة غير مشروعة، عن بعد على المعلومات. في الأعوام من 1993 وحتى 2000 نشط البيت الأبيض الأمريكي والهيئات المتخصصة التي أنشأها لهذا الغرض في توجيه جهات التقنية الى العمل الجاد على خلق تقنيات أمان كافية للحفاظ على السرية الخصوصية، وبالرغم من التقدم الكبير على هذا الصعيد الا أن أحدث تقارير الخصوصية تشير الى أنه ما تزال حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للإعتداء في ظل عدم تكامل حلقات الحماية (التنظيمية والتقنية والقانونية).

إن بدء مشكلات الكمبيوتر في الستينات تراقق مع الحديث – في العديد من الدول الغربية – عن مخاطر جمع وتخزين وتبادل ونقل البيانات الشخصية ومخاطر تكنولوجيا المعلومات في ميدان المساس بالخصوصية والحريات العامة، وانتشر الحديث عن الخطر الكبير الذي يهدد الحرية الشخصية بسبب المقدرة المتقدمة لنظم المعالجة الإلكترونية على كشف والوصول الى المعلومات المتعلقة بالأفراد واستغلالها في غير الأغراض التي تجمع من أجلها. وخلال الثمانينات تغير الواقع التكنولوجي فيما يتعلق بالجهات التي تملك وتسيطر على نظم الكمبيوتر وكان ذلك بسبب اطلاق الحواسيب الشخصية وانتشارها، وأصبح من الواضح أن حماية الخصوصية يتعين أن تمتد الى الكمبيوترات الخاصة وان يتم احداث توازن ما بين الحق في الخصوصية أو الحق في الحياة الخاصة وبين الحق في الوصول الى المعلومات، هذا التغير في الواقع التكنولوجي عكس نفسه على حقل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنية والجزائية وبدأت تكثر الأحاديث بشأن دعاوى الاستخدام غير المشروع للمعلومات وللوثائق الشخصية، وظهرت أحداث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها على سبيل المثال الحادثة التي حصلت في جنوب افريقيا حيث أمكن للمعتدين الوصول الى الأشرطة التي خزنت عليها المعلومات الخاصة بمصابي أمراض الإيدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية الى جهات عديدة. ومن

الحوادث الشهيرة الأخرى حادثة حصلت عام 1989 عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية بأن سرب اليها شريطا يحتوي على أرصدة عدد من الزبائن، وقد تكرر مثل هذا الحادث في المانيا أيضا. وقد أظهرت القضايا التي حصلت ما بين عامي 96-97 في الحقل المصرفي أن الوصول الى البيانات الشخصية ارتبط في الغالب بأنشطة الابتزاز التي غالبا ما تتعلق بالتحايل على الضريبة من قبل زبائن البنوك. وفي عام 1986 اتهمت شركة IBM بأن نظام الأمن الذي تنتجه المسمى RACF يستخدم للرقابة على الموظفين داخل المنشآت، وفي عام 1994 أيضا وفي المانيا أثير جدل واسع حول حق دائرة التأمينات الصحية بنقل البيانات الى شركات خارجية، وشبيه بهذا الجدل ما يدور الآن بشأن مدى أحقية شركات تزويد الانترنت والتلفونات الكشف عن معلومات الزبائن لجهات أخرى.

إن هذه المخاطر أثارت وتثير مسألة الأهمية الاستثنائية للحماية القانونية – الى جانب الحماية التقنية– للبيانات الشخصية، ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، انه وقبل اختراع الكمبيوتر فإن حماية هؤلاء الأشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الأسرار التقليدية (كحماية الملفات الطبية أو الأسرار المهنية بين المحامي والموكل) وعلى الرغم من ذلك فإن هذه النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطي إلا جانبا من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول الى ومقارنة واختيار وسيلة نقل المعلومات في بيئة الوسائل التقنية الجديدة هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداء من السبعينات من القرن العشرين تتضمن قواعد ادارية ومدنية وجنائية من أجل حماية الخصوصية وتوصف بأنها تشريعات السرية وليست فقط مجرد تشريعات تحمي من أفعال مادية تطال الشرف والحياة الخاصة. كما أن هذه المخاطر، وما يتفرع عنها من مخاطر أخرى كتلك الناتجة عن معالجة البيانات في شبكات الحواسيب المربوطة ببعضها البعض والتي تتيح تبادل المعلومات بين المراكز المتباعدة والمختلفة من حيث أغراض تخزين البيانات بها نقول أن هذه المخاطر كانت محل اهتمام دولي واقليمي ووطني أفرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها، واتخاذ تدابير أمنية لمعالجتها وخزنها ونقلها، وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح وطلب إلغاء البيانات، ووجوب تحديد الغرض من حجمها ومدة استخدامها، وإقرار مبدأ مسؤولية القائمين على وظائف بنوك المعلومات لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية.