أثر استخدام تكنولوجيا المعلومات على حماية الخصوصية كأداة للتنمية الاقتصادية

د.بدر أسماعيل محمد*

مقدمة:

بالرغم من أن الإنسان كائن إجتماعى — كما يقول الاجتماعيون— لا يتمكن من العيش منفردا منفصلا ومعزولا عن المجتمع، إلا إنه يعيش جانبا مهما من حياته فى نطاق ضيق يسمى (الخصوصية).

ولقد استخدم مصطلح الخصوصية منذ القرن الخامس عشر ليدل على "الحالة أو الوضع الذى يكون فيه الإنسان قد انسحب من مجتمع الآخرين أو التوارى من أن يكون محل اهتمام ". ويعد احترام هذه الخصوصية من أهم مكونات وأساسيات حقوق الإنسان، التى يجب على القانون حق رعايتها وصونها.

وقد تعرض الحق فى الحياة الخاصة فى العصر الحديث إلى أزمة حقيقية وعامة، ترجع بشكل اساسى إلى التطور العلمى والتكنولوجى السريع فى المجالات السمعبصرية وأنظمة الحاسبات. ذلك التطور الذى سمح بالإطلاع على أسرار الحياة الخاصة واختراق وتدمير حاجز السرية وبطرق خفية دون علم صاحبها، وجاء دور تكنولوجيا المعلومات والاتصالات وقمة إبداعاته "الإنترنت" ليكون أداة فائقة ساعدت على معرفة الأسرار الشخصية للأفراد، ويسرت من قدرة الأفراد والمنظمات على تبادل المعلومات ومعالجتها، وساعدت شبكة الإنترنت على وجود طفرات هائلة ومتوازية فى وسائل التطفل والتجسس والاختراق بدون وجه حق، وجعلت هذه الشبكة من شخصية المستخدم لها وأسراره كتابا مفتوحا أمام الراغبين فى اقتحام خصوصيته.إن انتشار تكنولوجيا المعلومات والاتصالات على مستوى الأفراد والمؤسسات الحكومية وغير الحكومية. وتطور أساليب القرصنة والاختراق الإلكترونى. شكلت ضغوطا على سلامة الحرية الشخصية من تلقى رسائل غير مرغوب فيها. تنهال على الفرد عبر المحمول والبريد الإلكترونى إعلانات وبلاغات دون سابق إنذار...الخ.

* د.بدر اسماعيل محمد : مركز المعلومات التخطيطية. معهد التخطيط القومى. القاهرة، جمهورية مصر العربية.

لقد تعدى اختراق تكنولوجيا الاتصالات للحرية الشخصية من الاستخدام المؤسسى للنظم إلى الاستخدام الفردى المنفلت. ولنا فى فوضى (البلوتوث) خير مثال ومعها سوء استخدام كاميرات الهاتف المحمول. مما يدل على أن تكنولوجيا المعلومات والاتصالات أوجدت عالما يتصارع فيه السرعة والتقنية من جهة، مع الحريات الشخصية والقيم الأخلاقية من جهة أخرى. ومع عدم القدرة حتى الآن على وضع مجموعة من الأنظمة والقوانين التى تحكم التفاصيل الدقيقة فى الاستخدام الفردى لهذه التكنولوجيا، كما هو الحال فى الاستخدام المنظم من قبل المؤسسات والشركات.أصبح الوازع الأخلاقى والقيمى واحترام الفرد لحريات الآخرين بمثابة المحدد الأول لحسن أو إساءة استغلال تكنولوجيا الاتصالات المتطورة.

لقد بدأت صيحات التحذير من مخاطر وسلبيات الانترنت على الحياة الخاصة تنطلق من دول عديدة، وحتى من داخل أمريكا – الطرف المهيمن على الشبكة العالمية – وعلى سبيل المثال نشرت مجلةTimes الأمريكية بعددها الصادر فى ٢٥ أغسطس ١٩٩٧ مقالا بقلم Jashua Quittner تحت عنوان " اختراق الخصوصية " تحدث المقال عن انهيار الحريات الشخصية والخصوصيات الإنسانية فى عالم الإنترنت بحيث إن ما يعمله الإنسان اليوم من معاملات وصفقات شراء وبيع ومخاطبات كلها أصبحت معلنة ومعروفة وموثقة عبر قنوات الشبكة، ويمكن التوصل إليها وكشفها.

٢- تكنولوجيا المعلومات والتنمية الاقتصادية[١]

التنمية من الكلمات التى كثيرا ما ترددها الألسن والأقلام، وهى فى الواقع جزء من نتاج الفكر السياسى والاجتماعى والاقتصادى المعاصر ، وأصبحت هذه القضية – التنمية الاقتصادية- من القضايا المهمة التى تفرض نفسها على الساسة والمفكرين فى جميع أنحاء العالم، ولعلها تتضمن مفاهيم كثيرة مثل " مستوى الحياة" و"الرفاهية" و"التقدم التكنولوجى". وتمثل التنمية تلك التحديات التى تواجه دول العالم عند قيامها بعمليات استثمار فى المجالات المختلفة كالزراعة والصناعة والنقل والدفاع وغيرها، وهى تعنى بصورة عامة زيادة الإنتاجية فى كل هذه المجالات. فضلا عن تغيرات هيكلية اقتصادية وهيكلةاجتماعية ونسياسية وثقافية ومن ذلك يتضح أن التنمية عملية مجتمعية شاملة تهدف إلى تحولات فى البناء الاقتصادى والاجتماعى والثقافى والسياسى.

ومن ذلك يمكننا استنتاج الآتى: -

- التنمية عملية مجتمعية واعية ومقصودة على المدى القريب والمتوسط والبعيد.
- التنمية عملية شاملة الاقتصادية والاجتماعية والثقافية والسياسية.
- هدف التنمية تحقيق إشباع الحاجات الأساسية المادية، والتى منها (الغذاء والسكن والصحة والتعليم والعمل وغيرها)، والمعنوية (تحقيق الذات من خلال الإنتاج والمشاركة فى تقرير المصير . وحرية التعبير والتفكير، والشعور بالأمن والكرامة، وغيرها)، وزيادة درجات مثل هذا الإشباع.
- تعتمد التنمية أساسا على المقدرة الذاتية للمجتمع، والمتمثلة فى استغلال مواردها الطبيعية والبشرية المتاحة، واستغلالها بما يضمن استمرارية هذه الموارد وتطويرها.

ولقد أكد كثير من الدراسات أن وسيلة التنمية هى امتلاك القدرة العلمية والتكنولوجية مع الإطار التخطيطى والتنظيمى. كما أن التطور التكنولوجى ركيزة أساسية لأى عملية تنموية، وأهم مصادر هذا التطور هى: -

- مصدر داخلى : ينبع من القدرة على التجديد والابتكار داخل المجتمع الذى تنعكس آثاره على قدرات أفراده فى مجالات العمل المختلفة.
- مصدر خارجى: ويتركز فى نقل التكنولوجيا من بلدان متقدمة فى هذا المجال إلى الدول النامية.

إن المفهوم الديناميكى لعملية التطور التكنولوجى يتمثل فى استحداثات جديدة تحددها احتياجات خطة التنمية نفسها، وفق معطيات الظروف الموضوعية لكل بلد نام على حدة، ووفق مصلحة تطور البلدان النامية بصورة عامة – بغض النظر عن مستواها التكنولوجى — وتهدف فى مجملها إلى تخفيف التبعية الاقتصادية والتكنولوجية، وتحقق الاستقلال الاقتصادى.

ويتلخص دور تقنية المعلومات والاتصالات في التنمية في محورين أساسيين[٣]:

المحور الأول: يتمثل في الدور الذي تلعبه صناعة تقنية المعلومات والاتصالات كأحد أهم مصادر التقدم وزيادة الدخل القومي في معظم الدول المتقدمة. فقطاع المعلومات والاتصالات يعتبر قطاعا اقتصاديا حيويا، يشتمل على عمليات إنتاجية مركبة تتسم بقيمة اقتصادية مضافة مرتفعة وعمالة ذات قدرات فنية عالية، وتتصل بها عمليات تجارية وخدمية واسعة النطاق تشمل شراء المعدات، والبرمجيات، وغيرها، مما يجعل من تقنية المعلومات والاتصالات قطاعا ذا أهمية حيوية في كافة الدول تقريباً، بل وأكثر أهمية في الدول التي تعتمد عملية التنمية فيها اعتماداً مباشراً على القدرة على التواصل كما هو الحال في البلدان العربية وقد

اكتسب هذا القطاع أهمية مضاعفة نتيجة للنمو المطرد للإنترنت وشبكة الويب العالمية، والتطبيقات المجتمعية باستخدام الإنترنت. مثل تطبيقات كل من الحكومة الإلكترونية والتجارة الإلكترونية والتعليم الإلكتروني والخدمات الطبية الخ.

أما المحور الثاني: فيشير إلى الآثار الإيجابية للتقدم في تقنية المعلومات والاتصالات على جميع القطاعات الاقتصادية الأخرى. حيث تساهم تقنية المعلومات والاتصالات في توفير وسائل دعم الأنشطة التي تنتفع من المعلومات الموجهة والموثوق بها بما في ذلك تحسين ظروف المجتمعات المحرومة، والخفض من حدة الفقر؛ فعلى سبيل المثال، تجعل تقنية المعلومات والاتصالات الرعاية الصحية أكثر شمولاً وتتيحها لقطاعات أوسع من خلال العلاج عن بعد، كما تزيد من فاعلية التعليم و توجهه إلى شرائح أكثر عن طريق التعلم عن بعد. ومن الأهمية بمكان إيجاد محتوى باللغة العربية حتى تستفيد منه جميع شرائح المجتمعات العربية، الأمر الذي يستدعي وجود صناعة خاصة بالمحتوى و أيضا النظر في تعريب المستويات المختلفة التي تتكون منها تقنية المعلومات والاتصالات بالإضافة إلى دراسة جدوى استخدام أسماء النطاقات باللغة العربية.[٤]

٣- أمن البيانات [٥]

٣-١ المقصود بأمن البيانات

يقصد بأمن البيانات، من الناحية الأكاديمية، " العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للبيانات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها". ومن الناحية التقنية، "هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية البيانات من الأخطار الداخلية والخارجية"ومن الناحية القانونية، فإن أمن البيانات "هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر البيانات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة"، وهو هدف تشريعات حماية البيانات ونظمها من الأنشطة غير المشروعة وغير القانونية (جرائم الكمبيوتر والإنترنت).

واستخدام اصطلاح أمن البيانات وان كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات والاتصالات[٦]، إلا انه وجد استخدامه الشائع، بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحاسبات والاتصال، إذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات– وتحديدا الإنترنت – أصبحت أبحاث ودراسات أمن البيانات ذات أهمية كبرى لتعظيم استخدام هذه التقنيات والحد من سلبياتها.

٣-٢ عناصر أمن البيانات

يتطلب دراسة وسائل أمن البيانات سواء من الناحية التقنية و/أوالتشريعية، ضمان توفر العناصر التالية للبيانات المطلوب حمايتها:-

- **السرية:** وتعني التأكد من أن لا يسمح بالإطلاع على البيانات من قبل الآخرين.
- **تكامل وسلامة المحتوى:** التأكد من سلامة ودقة البيانات، وعدم إمكانية إجراء عمليات (إضافة/حذف/تعديل) في أية مرحلة من مراحل المعالجة أو التبادل، سواء أثناء التعامل مع البيانات أو عن طريق تدخل غير مشروع.
- **استمرارية توفر المعلومات أو الخدمة:** التأكد من استمرار عمل النظام المعلوماتي، واستمرار تقديم الخدمة للمستفيدين، مع التأكيد على عدم حرمان المستفيدين من التعامل مع النظام وحصولهم على كافة البيانات المتوفرة به.
- **المصارحة وعدم الإنكار** :- ويقصد به ضمان عدم إنكار (مصارحة) المستفيد إذا قام بأي عمليات (إضافة/حذف/تعديل) على البيانات.

٣-٣ خطة حماية البيانات [٧]

إن ضمان توفر عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها. فليس كل المعلومات تتطلب السرية وضمان عدم الإفصاح. لهذا تنطلق خطط أمن المعلومات من الإجابة على التساؤلات التالية:-

- **التساؤل الأول: - ما هي المعلومات المطلوب حمايتها ؟** وإجابة هذا التساؤل تتطلب تصنيف البيانات والمعلومات من حيث أهمية الحماية، إذ تصنف المعلومات بالتدرج من معلومات لا تتطلب الحماية، إلى معلومات تتطلب حماية قصوى.
- **التساؤل الثاني:- ما هي المخاطر التي تتعرض لها هذه المعلومات؟** وتبدأ بحصر المخاطر التى يمكن أن تهدد المعلومات وأمنها، ابتداء من انقطاع التيار الكهربائى، وإساءة الموظفين استخدام كلمات السر، حتى مخاطر اختراق النظام من الخارج بأحد وسائل الاختراق. ثم يتم تصنيف هذه المخاطر حسب مصدرها ووسائل تنفيذها، وأهداف الاختراق، وأثر ذلك على المعلومات ونظام الحماية.

-التساؤل الثالث :- ما هى وسائل الحماية من هذه المخاطر؟ وهى تختلف من منشأة لأخرى حسب أهمية هذه المعلومات والإمكانيات المادية للمنشأة، ولكن الحد الأدنى لوسائل الحماية تتطلب تحديد كلمة سر للدخول إلى الملفات الهامة الموجودة بجهاز الكمبيوتر الشخصي أو حتى للنظام كله، وان يستخدم برنامجا فعالا للحماية من الفيروسات الإلكترونية الضارة، وتراعي إجراءات مقبولة في حماية الدخول إلى شبكة الإنترنت والتأكد من مصدر البريد الإلكتروني مثلا. وإذا كانت بيانات المنشأة ذات أهمية كبيرة يفضل زيادة إجراءات الأمن بأن يضاف للنظام برنامج خاص ، وإذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الإفشاء، تكون تقنيات التشفير مطلوبة بالقدر المناسب. مع مراعاة أن إجراءات الحماية تنطلق من احتياجات الحماية الملائمة، فان زادت عن حدها كان لها اثر سلبي على الأداء، يصبح الموقع أو النظام بطيئا وغير فعال في أداء مهامه الطبيعية، وان نقصت عن الحد المطلوب ازدادت نقاط الضعف وأصبح أكثر عرضة للاختراق الداخلي والخارجي.

- التساؤل الرابع :- ما هى الأساليب الواجب اتباعها عند حدوث الخطر رغم توفر وسائل الحماية؟

وإجابة هذا التساؤل هو ما يعرف بخطط مواجهة الأخطار عند حدوثها، وتتضمن مراحل متتالية:-

١- تبدأ من مرحلة الإجراءات التقنية والإدارية والإعلامية والقانونية اللازمة عند حدوث ذلك، ثم

٢- مرحلة إجراءات التحليل لطبيعة المخاطر التي حدثت وسبب حدوثها، وكيفية الحد منها فى المستقبل.

٣- وأخيرا، إجراءات القضاء على الخطر.

٣-٤ العمليات التشغيلية الرئيسية لأمن المعلومات

بالرغم من تعدد هذه العمليات في بيئة تكنولوجيا المعلومات والاتصالات وتبادل البيانات، إلا أنه يمكن تحديد العمليات الرئيسية على النحو التالى[٨]:-

(١) تصنيف المعلومات:-

وهي عملية أساسية عند بناء أي نظام، أو في بيئة أي نشاط يتعلق بالمعلومات. وتختلف التصنيفات حسب طبيعة عمليات المنشأة، فمثلا قد تصنف المعلومات إلى متاحة وموثقة، وسرية، وسرية للغاية. أو قد تكون معلومات متاح الوصول إليها، وأخرى محظور التوصل إليها، ... وهكذا.

(٢) التوثيق:-

تتطلب عمليات تشغيل المعلومات أساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها. وبشكل رئيسى فإن التوثيق ضروري لنظام التعريف، وتصنيف المعلومات، والأنظمة التطبيقية. وفي إطار أمن المعلومات، فإنه يتطلب أن تكون إستراتيجية أو سياسة الأمن وإجراءاتها موثقة ومكتوبة، بالإضافة إلى خطط التعامل مع المخاطر والحوادث، والجهات المسئولة ومسئولياتها ، وخطط الحماية، وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

(٣) المهام والواجبات الإدارية والشخصية:-

يتطلب نظام أمن المعلومات حسن اختيار الأفراد المؤهلين نظريا وعمليا، على أن يتم التأهيل العملي بالتدريب المتواصل. وبشكل عام، فان المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسية وهى:- تحليل المخاطر، وضع السياسة أو الإستراتيجية ، وضع خطة أمن المعلومات، وضع البناء التقني الأمني (توظيف الأجهزة والمعدات والوسائل)، وأخيرا، تنفيذ الخطط والسياسات.

(٤) وسائل التعريف ونطاق الاستخدام:-

إن الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموما، يمكن تقييده بالعديد من أنظمة التعرف على شخصية المستخدم وتحديد نطاق الاستخدام.

وتتكون عملية التعريف أو الهوية من خطوتين:-

-الأولى وسيلة التعرف على شخص المستخدم.

-والثانية قبول وسيلة التعريف أو التأكد من صحة الهوية المقدمة.

ووسائل التعريف تختلف تبعا للتقنية المستخدمة. وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات ، وبشكل عام، فان هذه الوسائل **تنقسم إلى ثلاثة أنواع:-**

أ يملكه الشخص (مثل البطاقة البلاستيكية او غير ذلك).

ب يعرفه الشخص (متل كلمات السر أو الرمز أو الرقم الشخصي إلى غير ذلك) .

ج- يرتبط بذات الشخص (مثل بصمة الإصبع، أو بصمة العين، والصوت وغيرها).

وأيا كانت وسيلة التعريف التي نتبعها فإنها تخضع لنظام أمن وإرشادات أمنية يتعين مراعاتها. فكلمات السر على سبيل المثال، وهي الأكثر شيوعا من غيرها من النظم، تتطلب أن تخضع لسياسة مدروسة

من حيث طولها ومكوناتها والابتعاد عن تلك الكلمات التي يسهل تخمينها أو تحريها. وكذلك خضوع الاستخدام لقواعد عدم الإطلاع وعدم الإفشاء والحفاظ عليها. و بعد الدخول للنظام، يتم تحديد نطاق الاستخدام ، وهو ما يعرف بالتصريح لاستخدام جزء ما من المعلومات في النظام، وهذه المسألة تتصل بالتحكم فى الدخول أو التحكم فى الوصول إلى المعلومات أو أجزاء النظام .

(٥) سجل الدخول:-

تتخذ سجلات الدخول أهمية استثنائية في حال تعدد المستخدمين، وتحديدا في حالة شبكات الكمبيوتر، وبشكل عام، فان سجلات الدخول تتطلب تحديد المستخدم ووقت الدخول للنظام، ومكانه، والعمليات التى قام بها. وأية معلومات إضافية أخرى تبعا للنشاط ذاته.

(٦) عمليات النسخ الاحتياطية -:-

وهى تتعلق بعمل نسخة إضافية من البيانات المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه، وتخضع لمجموعة من القواعد التى يتعين أن تكون محددة مسبقا، وموثقة ومكتوبة، ويتم الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

(٧) وسائل الأمن الفنية ونظام منع الاختراق:-

تتعدد تقنيات وسائل الأمن المتعين استخدامها في بيئة تكنولوجيا المعلومات والاتصالات، كما تتعدد أغراضها ونطاقات الاستخدام. ومن أهمها فى الوقت الحاضر وسائل التعريف والتوثيق وتحديدا كلمات السر السابق ذكرها بالإضافة إلى الوسائل المساعدة مثل الجدران النارية ، والتشفير. وكذلك نظم التحكم في الدخول و نظام تعقب الاختراق ، وأنظمة وبرامج مقاومة الفيروسات.

(٨) نظام التعامل مع الحوادث :-

تختلف مراحل وخطوات نظام التعامل مع الحوادث من مؤسسة إلى أخرى تبعا لعوامل عديدة تتعلق بطبيعة الأخطار التي أظهرتها عملية تحليل المخاطر، وما أظهرته إستراتيجية الأمن الموجودة في المؤسسة، أو بالنظام ذاته من كونه نظام كمبيوتر مغلق أم مفتوح، أو قواعد بيانات أو شبكات أو مزيج منها، أو نظام خدمة خاص أم خدمات للعامة عبر الشبكة (المحلية أو الدولية). وبوجه عام، فان نظام التعامل مع الحوادث يتم من خلال ستة مراحل (الإعداد المسبق، التحري /التعقب، الملاحظة، الاحتواء والاستئصال، القضاء على الخطر، المتابعة).

٣-٦ ما هى المخاطر والتهديدات ونقاط الضعف؟ [٩]

٣-٦-١ المفاهيم والمصطلحات:-

يوجد العديد من المصطلحات التى يتم استخدامها لتحديد الاختلاف بين أنواع المخاطر مثل:-

التهديد:- ويعني الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصا كالمتجسس أو الهاكرز المخترق، أو شيئا يهدد الأجهزة أو البرامج أو البيانات، أو حادث كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية.

نقاط الضعف أو الثغرات :- وتعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق مثل الأشخاص الغير مدربين لاستخدام النظام وحمايته. والاتصال بالإنترنت إذا لم يكن مشفرا، أو الموقع المكاني للنظام إذا لم يكن مجهزا بوسائل الوقاية والحماية. وبالعموم فان نقاط الضعف تمثل أحد الأسباب المؤدية لحدوث المخاطر أو التهديدات. ويرتبط بهذا الاصطلاح اصطلاح وسائل الوقابة: وتعني الأسلوب المتبع لحماية النظام ككلمات السر، ووسائل الرقابة والجدران النارية وغيرها.

أما المخاطر:- وهى تستخدم بشكل مترادف مع تعبير التهديد، مع إنها حقيقة تتصل بأثر التهديدات عند حدوثها. وتقوم إستراتيجية أمن المعلومات الناجحة على تحليل المخاطر . وتحليل المخاطر هي عملية وليست مجرد خطة محصورة، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف وأخيرا وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف.

أما الحوادث:- فهو اصطلاح متسع يشمل المخاطر ويشمل الأخطاء. وهو بالمعنى المستخدم في دراسات أمن المعلومات التقنية يشير إلى الأفعال المقصودة أو غير المقصودة، ويغطي الاعتداءات والأخطاء الفنية. أما التوصيف الدقيق لهذا المفهوم في الإطار الإداري والقانوني يتمثل فى الحوادث غير المقصودة لأسباب فنية غير مقصودة أو بفعل الطبيعة.

أما الهجمات:- فهو اصطلاح لوصف الاعتداءات مثل هجمات تدمير (إعاقة) الخدمة، أو هجمات إرهابية، أو هجمات البرامج، أو هجمات الموظفين الحاقدة أو الهجمات المزاحية. ويستخدم كمرادف لاصطلاح الاختراقات أو الاختلالات، وهو اصطلاح توصف به مختلف أنماط الاعتداءات التقنية.

أما في إطار المصطلحات القانونية

فإنه يجب تحديد الفرق بين ثلاث مصطلحات وهي:-

الجرائم الإلكترونية: - وتدل على مختلف جرائم الكمبيوتر والإنترنت في الوقت الحاضر.

إرهاب السيبر أو إرهاب العالم الإلكتروني: وهي هجمات تستهدف نظم الكمبيوتر والبيانات لأغراض دينية أو سياسية أو فكرية أو عرقية، وفي حقيقتها هى جزء من الجرائم الإلكترونية باعتبارها جرائم إتلاف للنظم والبيانات، أو جرائم تعطيل للمواقع وعمل الأنظمة. وتتميز عنها بسمات عديدة مثل ممارسة مفهوم الأفعال الإرهابية لكن في بيئة الكمبيوتر والإنترنت من خلال الاستفادة من خبرات الكريكرز – أي مجرمي الكمبيوتر الحاقدين – العالية ، وفي إطار الجريمة المنظمة للجماعات.

حرب المعلومات ، وهو اصطلاح ظهر في بيئة الإنترنت للتعبير عن اعتداءات تعطيل المواقع وتدهور (إعاقة) الخدمة والاستيلاء على البيانات، وهى في الغالب هجمات ذات بعد سياسي، أو هجمات منافسين حاقدين في قطاع الأعمال ، وهو ما يجعلها مترادفة هنا مع أعمال إرهاب السيبر. ولذا وصفت حملات الهاكرز اليوغسلافيين على مواقع الناتو إبان ضربات الناتو بأنها حرب معلومات . ووصفت كذلك هجمات المخترقين الأمريكان على مواقع صينية في إطار حملة أمريكية على الصين، تحت ذريعة حقوق الإنسان والتي تمت بدعم الحكومة الأمريكية، بأنها حرب معلومات ، وأشهر حروب المعلومات القائمة المعركة المستمرة بين الشباب العربى والمسلم ، وتحديدا شباب المقاومة اللبنانية والمدعومين من خبراء اختراق عرب ومسلمين ، وبين جهات تقنية صهيونية في إطار حرب تستهدف إثبات المقدرة في اختراق المواقع وتعطيلها أو الاستيلاء على بيانات من هذه المواقع . وهذا الاصطلاح في حقيقته اصطلاح إعلامي أكثر منه أكاديمي. ويستخدم مرادفا في غالبية التقارير لاصطلاح الهجمات الإرهابية الإلكترونية. ونجده لدى الكثيرين اصطلاح واسع الدلالة لشموله على كل أنماط مخاطر وتهديدات واعتداءات وجرائم البيئة الإلكترونية.

٣-٦-٢ تحديد المخاطر ونقاط الضعف وأنماط الاعتداءات التقنية[١٠]

تختلف آليات تحديد قائمة المخاطر والاعتداءات تبعا لنوع التصنيف وأساسه، وهي معايير تختلف طبقا لتقسيم المخاطر، واختلاف التسميات. ويمكن إجراء عمليات التصنيف على النحو التالى:-

٣-٦-٢-١ تصنيف الهجمات في ضوء مناطق ومحل الحماية:-

تصنف المخاطر والاعتداءات على النحو التالي[١١]:-

أولا:- خرق الحماية المادية

- التفتيش في مخلفات التقنية :- ويقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام، كالأوراق المدون بها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو وسائط التخزين المختلفة، أو غير ذلك من المواد التي تحتوى على أية معلومة تساهم في الاختراق.

- التوصيلة السلكية :- وهى التوصيل السلكي المادي مع الشبكة أو توصيلات النظام بغرض التصنت أو الاستيلاء على البيانات المتبادلة عبر الأسلاك.

- التصنت الموجى :- ويتم ذلك باستخدام تقنيات لتجميع الموجات المنبعثة من النظم المختلفة مثل موجات شاشات الكمبيوتر الضوئية أو الموجات الصوتية من أجهزة الاتصال.

- تدهور (إعاقة) الخدمة:- والمقصود هنا الإضرار المادي بالنظام لمنع تقديم الخدمة. ومن أمثلة ذلك تعطيل مواقع الإنترنت بضخ كم كبير من رسائل البريد الإلكترونى إليها دفعة واحدة.

ثانيا :- خرق الحماية المتعلقة بالأشخاص وشئون الموظفين

- التخفي بانتحال صلاحيات شخص مفوض:- والمقصود هنا الدخول إلى النظام عبر استخدام وسائل التعريف كاستغلال كلمة سر أحد المستخدمين واسم هذا المستخدم، أو عبر استغلال نطاق صلاحيات المستخدم الحقيقي.

- الهندسة الاجتماعية:- ويصنف هذا الأسلوب ضمن الحماية المادية أحيانا. وهى تتم عن طريق اتصال شخص ما بأحد العاملين ويطلب منه كلمة سر النظام تحت زعم انه من قسم الصيانة أو قسم التطوير أو غير ذلك، ولطبيعة الأسلوب الشخصي في الحصول على معلومة الاختراق أو الاعتداء سميت الهندسة الاجتماعية.

- الإزعاج والتحرش :- وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز، أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة وإزعاجا بالغين. وليست حكرا على البريد الإلكتروني بل تستغل مجموعات الحوار والأخبار

والنشرات الإلكترونية في بيئة الإنترنت والويب ، كما أنها ليست حكرا على بيئة الموظفين والمستخدمين، بل هي نمط متواجد في مختلف التفاعلات عبر الشبكة وعبر البريد الإلكتروني، وهى اعتداءات تأتى من خارج إطار المنشأة، ومرتبطة بالأشخاص أكثر من مؤسسات الأعمال.

- قرصنة البرامج وتتم قرصنة البرامج عن طريق نسخها دون تصريح، أو استغلالها على نحو مادي دون تخويل بهذا الاستغلال، أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المبرمج. وتم وضعها من قبل أصحاب هذا التصنيف ضمن قائمة الإخلالات المتصلة بالأشخاص وشئون الموظفين، حيث يقومون بنسخ البرامج لتبادلها مع أصدقائهم وأقربائهم، أو لاستغلالها في بيئات عمل أخرى.

ثالثا:- خرق الحماية المتصلة بالاتصالات والبيانات

وتخص الأنشطة التي تستهدف البيانات والبرامج، وتشمل:-

(١) هجمات البيانات

- **النسخ غير المصرح به للبيانات**:- و تشمل نسخ البيانات والمعلومات والأوامر والبرامج وغيرها.

- **تحليل الاتصالات** :- وهى رقابة حركة النظام بغرض الهجوم عليه. حيث يتم دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد سلوك المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب.

- **القنوات المخفية**:- وهي قيام المقتحم بإخفاء بيانات أو برامج أو معلومات مسروقة كأرقام بطاقات ائتمان في مكان معين داخل النظام. وتتعدد أغراض الإخفاء، فقد تكون تمهيدا لهجوم لاحق، أو تغطية اقتحام سابق، أو مجرد تخزين لبيانات غير مشروعة.

(٢) هجمات البرامج

- المصائد أو الأبواب الخلفية:- الأبواب الخلفية ثغرة أو منفذ في برنامج يتيح للمخترق الوصول من خلاله إلى النظام. فهو ببساطة مدخل مفتوح تماما كالباب الخلفي للمنزل الذي ينفذ منه السارق.

- السرقة أو اختلاس المعلومة أو الاستخدام اللحظي (سرقة أو اختطاف الجلسات):- المقصود أن يستغل المقتحم الفرصة لاستخدم النظام، سواء لانشغال المستخدم الأصلي، أو أن يجلس مكان مستخدم النظام للإطلاع على المعلومات، أو إجراء أية عملية بقصد الاستيلاء على بيانات، أو الحصول على معلومات تستخدم في اختراق أو اعتداء لاحق، أو لتنفيذ نشاط تدميري، أو لكشف بيانات بشكل فوري.

- نقل البيانات عبر الأنفاق :- أنفاق النقل هى طريقة تقنية مشروعة لنقل البيانات عبر الشبكات غير المتوافقة، لكنها تصبح طريقة اعتداء عندما تستخدم لنقل بيانات بطريقة غير مشروعة.

- الهجمات الوقتية : - وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به إلى البرامج أو البيانات. وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام. وتضم في نطاقها العديد من الأساليب التقنية لتنفيذ الهجوم ، منها الأداء الفعلى للنظام ، والهجمات غير المتزامنة المتصلة باستغلال ترتيب تنفيذ العمليات الروتينية .

- البرامج الخبيثة :- (كالفيروسات، وحصان طروادة، والدودة الإلكترونية ، والسلامي ، والقنابل المنطقية). والعامل المشترك بين هذه البرامج أنها تستخدم للتدمير سواء للنظام ككل أو البرامج أو البيانات أو الملفات أو الوظائف، أو تستثمر للقيام بمهام غير مشروعة (مثل الغش والاستيلاء) في النظام. وهى تختلف عن بعضها من حيث تركيبها أحيانا، أو أسلوب الهجوم والحصول على النتائج.

رابعا :- الهجمات والمخاطر المتصلة بعمليات الحماية

ويمكن حصر هذه الأساليب والاعتداءات على النحو التالى :-

- **العبث (الغش) بالبيانات**:- ويستهدف هذا الهجوم أو الاعتداء تغيير البيانات، أو إضافة بيانات وهمية في مراحل الإدخال أو الإخراج.

- **محاكاة بروتوكول الإنترنت** (التخفي باستغلال بروتوكولات النقل):- حيث يقوم المهاجم بتزوير العنوان المرفق مع حزمة البيانات المرسلة بشكل يتقبله النظام ويسمح بمرور حزمة البيانات.

- **اكتشاف كلمات السر** (جمعها والتقاطها):- وهى طريقة لا تعتمد على التخمين، بل يتم استخدام برامج لاكتشاف كلمات السر أثناء تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة. بحيث يقوم هذا البرنامج بجمع أول ١٢٨ بايت أو أكثر – مثلا – من كل اتصال بالشبكة التي يتم مراقبتها ورصد حركة الاتصال عليها، وعندما يطبع المستخدم كلمة السر أو اسم المستخدم، فان البرنامج (المكتشف) يجمع هذه المعلومات وينسخها. كما أن هناك من البرامج التي تجمع بعض المعلومات وتعيد تحليلها وربطها معا لاكتشاف كلمة السر.

- **المسح والنسخ** :- وهو أسلوب تقني لا يعتمد على التخمين البشرى، بل يستخدم برنامج الذى يعتمد على نظرية الاحتمالات للوصول إلى كلمة السر أو رقم هاتف المودم الصحيحة.

- هجمات استغلال المزايا الإضافية :-

وهى تتصل بمنح بعض الموظفين مزايا تتجاوز اختصاصه ورغباته، وفي هذه الحالة من الممكن أن يستغلها فى تدمير مختلف ملفات النظام أو جزء منها. وهذا وحده يعطينا التصور لأهمية إستراتيجية أمن المعلومات في المنشاة فتحديد الامتيازات والصلاحيات قد يمنع في حقيقة الأمر من حدوث دمار شامل أو جزئى ويحد من الاختراقات.

٣-٦-٢-٢ تصنيف المخاطر تبعا لموقع المعلومة من النظام :-

وتصنف على النحو التالى[١٢]:-

- المخاطر التي تتعرض لها المعلومات داخل النظام في مراحل إدخال واسترجاع وتعديل وإلغاء المعلومات.
- المخاطر التي تتعرض لها المعلومات عندالنقل، أي التبادل بين شبكات الكمبيوتر أو وسائط التخزين.
- المخاطر التي تتعرض لها المعلومات خارج النظام في مرحلة التخزين والنسخ.

٣-٦-٢- ٣ تصنيف المخاطر والأساليب التقنية في الاعتداء تبعا لشيوع أساليب الهجوم وتقنياته وأغراض الهجوم وقيمة المعلومات[١٣]:-

وطبقا لهذا التصنيف، تتعدد معايير التقسيم وتختلف المخاطر وأساليب التقنية بل والأشخاص الذين يقومون بالاعتداء تبعا لدرجة شيوع أنواع الاعتداءات وأساليبها، وهو ما قد يتأثر بالوقت الذي تجري فيه المعالجة. ففى عام ٢٠٠٠ كان من بين الهجمات الشرسة هجمات تدهور (إعاقة) الخدمة التي استهدفت مواقع الإنترنت و هجمات الفيروسات العالمية. بينما في الوقت الحاضر ازدادت الاعتداءات التي تستهدف مواقع الأعمال الإلكترونية للحصول على المال عبر ما يعرف باحتيال الإنترنت متعدد الأنواع والأشكال، ونجد أيضا شيوعا لهجمات المضايقة والتحرش والإزعاج وإثارة الأحقاد عبر رسائل البريد الإلكتروني.

وتصنف عادة المخاطر الشائعة إلى مجموعات على النحو التالى:- الأخطاء التقنية ، الغش أو الاحتيال والاستيلاء على البيانات ، أحقاد الموظفين ، الأخطار المادية ، النجمات الحاقدة. التجسس الصناعي والتجسس الحكومي ، البرامج الخبيثة.

وفي أحدث التصنيفات الآن على مواقع الإنترنت المتخصصة، تصنف المخاطر وأنواع الهجوم حسب مناطق الاختراق والثغرات، وفيها يتم تحديد المخاطر تبعا للوصف التقني لمصدر الإقحام أو نقطة الضعف في النظام.

أما من ناحية تحديد الثغرات ونقاط الضعف فتتصف أنواع الهجوم عامة إلى :- الدخول غير المصرح به إلى شبكة النظام ، أو الدخول غير المصرح به لمصادر الشبكة ، بغرض التعديل غير المصرح به للبيانات والبرامج. وكشف حركة المرور على الشبكة أو التخفي للوصول إلى حركة المرور، أو العبث بحركة المرور على الشبكة، أو تعطيل وظائف الشبكة.

٣-٦-٣ تحليل المخاطر القانونية في بيئة المشاريع المعلوماتية [١٤]

هى عملية مستمرة تبدأ من لحظة الشروع والإعداد للمشروع، فتحدد كافة احتياجات المشروع القانونية إضافة إلى تحليل العمليات التقنية والتسويقية والخدمية والأدائية الداخلية والخارجية المتصلة بالمشروع من زاوية العلاقات والمسئوليات القانونية، وتحديد متطلبات الحماية القانونية ومواجهة المسئوليات المتوقعة.

والجدير بالذكر أن مواقع الانترنت العربية ومشروعات الاستثمار المعلوماتي العربية تفتقر لرؤيا وتصور في هذا المجال،وإذا كان خطرا إغفال المخاطر القانونية على مستوى كافة المواقع والمؤسسات، فانه يصبح خطرا مضاعفا في بيئتي التجارة والأعمال الالكترونية، خاصة الأعمال المصرفية اللاسلكية والأعمال المصرفية الالكترونية على شبكة الانترنت . مما يؤثر سلبيا وبشكل كبير على الحق فى الخصوصية على كافة المستويات.

٤- الحق فى الخصوصية[١٥]

٤-١ نشأة الحق في الخصوصية

ترجع نشأة الحق في الخصوصية من الوجهة التاريخية إلى ما ذكر فى الكتب السماوية من إشارات للخصوصية تنطوي على الاعتراف بحماية الشخص من أن يكون مراقبا، وثمة حماية للخصوصية في الشرائع اليونانية والصينية القديمة. وقد جاء القران الكريم[١٦] صريحا في حماية السرية وفي منع أنشطة التجسس وكذلك في حماية المساكن من الدخول دون إذن.

وفي العصر الحديث فان مفهوم الحق في الخصوصية ظهر في عام ١٩٤٨ مع الإعلان العالمي لحقوق الإنسان. حيث نصت المادة ١٢ فيه على أنه "لا يتعرض أحد لتدخل تعسفى فى حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق فى حماية القانون له من مثل هذا التدخل أو تلك الحملات".

والعديد من اتفاقيات حقوق الإنسان العالمية اعترفت بالحق في الخصوصية كالعهد الدولي للحقوق المدنية والسياسية ،واتفاقية الأمم المتحدة للعمال المهاجرين، واتفاقية الأمم المتحدة لحماية الطفولة وغيرها.

أما على المستوى الإقليمي فالعديد من الاتفاقيات اعترفت بالحق في الخصوصية، ونظمت قواعد حمايته كما هو الحال في الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية (روما لعام ١٩٥٠)، حيث قررت فى المادة الثامنة منها "لكل إنسان الحق فى احترام حرمة حياته الخاصة، ومنزله ومراسلاته".

يمنع تدخل السلطة فى ممارسة الإنسان لحقه المذكور عدا الأحوال التى حددها القانون، وفى حالة حماية الأمن القومى للمجتمع الديمقراطى، أو لحماية سلامة الناس، أو للمصلحة الاقتصادية، أو لمنع حالات الفوضى أو ارتكاب الجرائم، أو لحفظ الصحة والأخلاق العامة، أو لحماية ورعاية حقوق وحريات الآخرين.

وهذه الاتفاقية قد تمخض عنها كل من المفوضية الأوروبية لحقوق الإنسان والمحكمة الأوروبية لحقوق الإنسان لمراقبة تطبيقها، وكلتاهما كانت نشطة في تطبيق وحماية الحق في الخصوصية، والحد من نطاق الاستثناءات على أحكام المادة الثامنة وما تقرره من حماية.

وفي هذا الشأن فإن المفوضية الأوروبية لحقوق الإنسان أقرت عام ١٩٧٦ (أن الحق في احترام الحياة الخاصة هو الحق في الخصوصية، والحق في الحياة إلى المدى الذي يتمناه الإنسان، والحق في الحماية من العالمية). ووفقا لرأي اللجنة فان الحق في احترام الحياة الخاصة لا ينتهي إلى هذا الحد بل يمتد إلى الحق في تأسيس وتطوير العلاقات مع الأشخاص الآخرين.

أما المحكمة الأوروبية لحقوق الإنسان، فقد راجعت العديد من قوانين دول الأعضاء في معرض نظرها للدعاوى المقامة إليها وقررت أن العديد من الدول فشلت في تنظيم عمليات التصنت على نحو مس خصوصية الأفراد. وقد راجعت قضايا لبعض الأفراد من اجل حقهم للوصول إلى المعلومات الخاصة بهم، والموجودة في الملفات الحكومية لضمان صحتها وسلامة إجراءات المعالجة. وقد طبقت حكم المادة الثامنة على الجهات الحكومية لتشملها والخاصة معا.

وهناك اتفاقيات إقليمية أخرى، بدأت تنص بوضوح على حماية الخصوصية، كالمادة ١١ من الاتفاقية الأمريكية لحقوق الإنسان التي جاءت مطابقة تقريبا للنص المقرر في الإعلان العالمي لحقوق الإنسان.

وفي عام ١٩٦٥ تبنت الولايات المتحدة الإعلان الأمريكي للحقوق والواجبات الذي يتضمن مجموعة من الحقوق من بينها الحق في الخصوصية، وقد بدأت المحاكم الأمريكية الداخلية والمحكمة الأمريكية لحقوق الإنسان إظهار ومعالجة حق الخصوصية ومسائله فيما تنظر من دعاوى.

تطور الحق في الخصوصية وحماية البيانات في الستينات والسبعينات نتيجة للتأثر بتقنية المعلومات وبسبب القوى الرقابية المحتملة لأنظمة الكمبيوتر التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة. وفي هذا المجال فان أول معالجة تشريعية في ميدان حماية البيانات كان عام ١٩٧٠ في هيس بألمانيا والذي تبعها سن أول قانون وطني (متكامل) في السويد عام ١٩٧٣ ثم الولايات المتحدة عام ١٩٧٤ ثم المانيا على المستوى الفيدرالي عام ١٩٧٧ ثم فرنسا عام ١٩٧٨.

وفي عام ١٩٨١ وضع الاتحاد الأوروبي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا إرشاديا لحماية الخصوصية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الالكترونية للبيانات، وهذه القواعد تصف البيانات والمعلومات الشخصية على أنها بيانات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر.

ويتطلب مفهوم حماية البيانات في المواثيق المتقدمة والقوانين أن تكون البيانات الشخصية :-

١ - قد تم الحصول عليها بطريق مشروع وقانوني.

٢ - تستخدم للغرض الأصلي المعلن والمحدد.

٣ - تتصل بالغرض المقصود من جمعها ولا تتجاوزه ومحصورة بذلك.

٤ - صحيحة وتخضع لعمليات التحديث والتدقيق.

٥ - أن يتوفر حق الوصول إليها.

٦ - حماية وسرية البيانات.

٧ - تمسح بعد انتهاء الغرض من جمعها.

وقد كان للاتفاقية الأوروبية ودليل منظمة التعاون الاقتصادي الأثر المباشر في سن العديد من التشريعات في مختلف دول العالم، وقد وقع ما يقارب ٣٠ دولة على الاتفاقية الأوروبية، وكثير من الدول الآن تخطط للانضمام إليها. كما تم استخدام دليل منظمة التعاون الاقتصادي والتنمية بشكل واسع في وضع التشريعات الوطنية حتى خارج إطار الدول الأعضاء في هذه المنظمة.

٤-٢ تعريف الخصوصية:-

هناك تعريفات متعددة ومتباينة قد تم وضعها للحق في الحياة الخاصة بين النظم القانونية المختلفة. وفي إطار النظام القانوني الواحد. فللفقه تعريفاته وللقضاء تعريفاته[١٧]، وهي تتباين في الإطار الواحد. أما التشريعات، فقد اتجهت إلى عدم تحديد تعريف للحق في الحياة الخاصة تاركة هذا الأمر للفقه والقضاء، واكتفت بوضع نصوص تكفل حماية الحق وتعدد صور الاعتداء عليه.

أما سبب شبه الإجماع على أن تعريف الحق في الخصوصية من الأمور الصعبة، فهو يرجع لاختلاف المفهوم الذي يمثل أساسا لتحديد التعريف إضافة إلى التباين في التعريفات تبعا للنظم القانونية المختلفة.

في كثير من الدول اختلط مفهوم الخصوصية وارتبط بمفهوم حماية البيانات، وهو ما يضع الخصوصية ضمن إطار الحق في حماية البيانات الخاصة، وخارج نطاق هذا المفهوم فإن الخصوصية ظهرت كوسيلة لتحديد الخطوط الفاصلة بين حق الفرد المطلق وبين حق المجتمع بالتعرض لشئونه، لكن هذا التباين لم يمنع من وجود العديد من التعريفات من قبل الفقه القانوني والنظم القضائية.

في عام ١٩٦٧عرف Alan Westin الخصوصية فى مقالته تحت عنوان Privacy and Freedom "بأنها رغبة الأفراد في الاختيار الحر للأسلوب الذى يعبرون فيه عن أنفسهم ورغباتهم وتصرفاتهم للآخرين". ووفقا لتعريفRuth Gavison فان الخصوصية "هي الحق في حماية الشخصية وعدم الاعتداء عليها واستقلال الأفراد وكرامتهم وسلامتهم". ووفقا لهذا التعريف فان للخصوصية " ثلاثة عناصر هى السرية ، والعزلة ، والتخفي ". أما لجنةCALCUTT في بريطانيا فقالت انها لم تتمكن من الوصول الى تعريف كاف ومرضى للخصوصية لكنها تبنت تعريفا قانونيا فى تقريرها حول الخصوصية وهو (حق الأفراد في الحماية ضد التدخل في الحياة الخاصة، وشئونهم وشئون عائلاتهم بوسائل مادية مباشرة أو عن طريق نشر المعلومات عنهم)[١٨]. من هذه التعريفات، يمكن إيجاز الحقائق التالية المتصلة بتحديد ماهية الحق في الحياة الخاصة:-

أولا: من الصعب وضع تعريف جامع للحق في الحياة الخاصة أو الخصوصية صنوا للاصطلاح المستخدم في الفقه الانجلو الأمريكي Privacy ،لان تعريف هذا الحق يرتبط في الحقيقة بمنظومة " التقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع " [١٩].

ثانيا: يستخلص جانب من الفقه عناصر رئيسية للحق في الحياة الخاصة تلتقي عندها – كحد أدنى -- الآراء المتباينة بشان تعريف هذا الحق:-

١- "اقتران الخصوصية بالانسحاب من الوسط أو العالم المحيط، وربطها بفكرة الخلوة أو العزلة " وسندا لذلك تتمثل غاية هذا الحق – كما يحددها P. Kayser – بضمان السلام والسكينة لهذا الجانب المنعزل من الحياة غير المتصل بالأنشطة العامة بجعله بمنأى عن التقصي والإفشاء غير المشروعين".

٢- "الاعتراف للشخص بسلطة الاعتراض على التدخل أو التقصي عن خصوصياته من جهة، وسلطة الاعتراض على وصول معلومات تتعلق بخصوصياته إلى الغير من جهة أخرى" .

٤-٣ أنواع الخصوصية

يمكن تقسيم الخصوصية إلى عدد من الأنواع المنفصلة لكنها ترتبط معا في الوقت ذاته، وهي:-

أ- خصوصية المعلومات: والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات البطاقات الشخصية والمعلومات المالية والسجلات الطبية والسجلات الحكومية والتى تتصل عادة بمفهوم حماية البيانات.

ب-الخصوصية الجسدية أو المادية: والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات ، وفحص المخدرات.

ج- خصوصية الاتصالات: والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد، والبريد الالكتروني وغيرها من الاتصالات.

د- الخصوصية الإقليمية (نسبة إلى الإقليم المكاني): والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة مثل البنوك والمطارات...الخ، والتي تتضمن التفتيش والرقابة الالكترونية والتأكد من بطاقات الهوية.

٥- مخاطر تكنولوجيا المعلومات على الحياة الخاصة

تساعد تقنية المعلومات الجديدة على تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية والشركات الخاصة. ويعود الفضل فى هذا إلى إمكانيات الحاسبات الآلية الهائلة، وإمكانياتها فى إجراء المقارنات بين الملفات الموجودة فى قواعد بيانات مختلفة. كما تيسر نقل هذه الملفات من مكان لآخر داخل/خارج البلد فى ثوان وبأقل تكلفة. مما يكون له

أكبر الأثر على تهديد الخصوصية. وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية. كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الالكترونية، وقواعد البيانات الشخصية، ووسائل رقابة البريد الإلكترونى والاتصالات، ورقابة بيئة العمل وغيرها.

إن استخدام الحاسبات في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد كان له آثار إيجابية عريضة، لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشئون الأفراد الاقتصادية والاجتماعية والعلمية... وغيرها، وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات ، وبنوك المعلومات قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه كبنوك المعلومات الصناعية مثلا، أو قد تكون شاملة لمختلف الشئون والقطاعات، 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.

وإذا كانت الجهود الدولية والاتجاه نحو الحماية التشريعية للحياة الخاصة عموما، وحمايتها من مخاطر استخدام الحاسبات وبنوك المعلومات على نحو خاص، تمثل الأسلوب الأفضل في مواجهة الأثر السلبي للتقنية على الحياة الخاصة، فان هذا الأسلوب قد رافقه اتجاه متشائم لاستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل لاستخدام الحاسبات قد أثار المخاوف من إمكانيات انتهاك الحياة الخاصة. ويرجع السبب لهذه المخاوف أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية، كالوضع الصحي والأنشطة الاجتماعية والمالية والسلوك والآراء السياسية ، يمكن جمعها وتخزينها لفترة غير محددة . كما يمكن استرجاعها فى أى وقت. ومع الزيادة في تدفق المعلومات التي تحدثها الحاسبات، تضعف قدرة الفرد على التحكم في تدفق المعلومات عنه، وعملية إعداد المعلومات ومعالجتها عبر أجهزة الحاسبات واستخلاص النتائج منها يزيد – كما يرى الكثيرون في الغرب [٢٠]– خطر التقنوقراطية (تملك الكمبيوترات) ، لان الاعتماد على الحاسب لتحديد الخيارات في الإنفاق والتخطيط والتعليم والسياسة وغيرهايعرض مفهوم الديمقراطية للخطر لأن الخيارات المتخذة وفقا لمبادئ حسابية تستبعد السيكولوجية الاجتماعية ، وحتى إذا أدرجت هذه الاعتبارات كعامل مساعد في المعلومات التي يغذي بها الحاسب ، فهي لن تكون إلا ذات أهمية ثانوية .

يقولRobert M.Bowie :– "إن التقنوقراطية، قد تصبح على درجة بالغة من القوة بحيث تحجم الحياة الخاصة داخل حدود ضيقة ، ويزداد ارتباط حياة الفرد وأسرته بهذه الأجهزة من خلال مسلحة

اقتصادية أو اجتماعية . وبذلك يصبح الإنسان كالأرقام، يتحكم الحاسب فى حياته الخاصة ويسلب شخصيته . وينوب عنه فى اتخاذ القرارات ". ويمكن القول بأن ما يهدد الجنس البشري ليس حربا نووية، بل جهاز حاسب مستقل "[٢١].

وكما يبدو أن هذه الآراء متشائمة من انتشار استخدام الحاسبات وأثرها على تهديد الخصوصية. وهي وان كانت نظرة تبدو مبالغا فيها، إلا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية وتحديدا الحاسبات في كل ما يهدد الحق في الحياة الخاصة.

ويمكن حصر المخاطر الرئيسية لتكنولوجيا المعلومات على الحق في الحياة الخاصة فيما يلي:-[٢٢]

أولا: "أن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل..الخ، وتستخدم الحاسبات وشبكات الاتصال في تخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو مما يحد من فرص الوصول إلى هذه البيانات. ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها بشكل خاطئ. أو مراقبة الأفراد ومعرفة خصوصياتهم، أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة ".

فعلى سبيل المثال، وفقا لدراسة عام ١٩٩٠ لحكومة الولايات المتحدة، تم جمع ٤ بليون سجل مختلف حول الأمريكيين، بمعدل (١٧) بندا لكل رجل وامرأة وطفل. كما تمتلك مصلحة الضرائب في الولايات المتحدة سجلات ضرائب لحوالي (١٠٠) مليون أمريكي على حاسباتها. وتمتلك الوكالات الفيدرالية – عدا البنتاجون – ثلاث شبكات اتصالات منفصلة تغطي كل الولايات المتحدة الأمريكية لنقل وتبادل البيانات.

ثانيا : أن شيوع (النقل الرقمي) للبيانات خلق مشكلة أمنية وطنية ، إذ سهل عمليات التصنت والتجسس الإلكتروني نتيجة لعدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة عن بعد على المعلومات ". والجدير بالذكر أنه، في الأعوام من ١٩٩٣ وحتى ٢٠٠٠ نشط البيت الأبيض الأمريكي، والهيئات المتخصصة التي أنشأها لهذا الغرض في توجيه جهات تكنولوجيا المعلومات إلى العمل لإيجاد على خلق تقنيات أمان كافية

للحفاظ على سرية الخصوصية، وبالرغم من التقدم الكبير فى هذا الصعيد إلا أن أحدث تقارير الخصوصية تشير إلى انه مازالت حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل عدم تكامل عمليات الحماية(التنظيمية والتقنية والقانونية).

ثالثا: أن أكثر مخاطر بنوك المعلومات على الحياة الخاصة، ما يمكن أن تحويه من بيانات غير دقيقة أو معلومات غير كاملة لم يتم تعديلها بما يكفل تكاملها ودقتها. فعلى سبيل المثال، قام مكتب تقييم التقنية في الولايات المتحدة في عام ١٩٨١ بتكليف الدكتور (لوردن)، وهو عالم في مجال الجريمة، بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات (وكالة الشرطة الفيدرالية) وملفات وكالة شرطة ولاية نيويورك، وقد وجد أن نسبة عالية من البيانات كانت غير كاملة وغير دقيقة ومبهمة، وأن معظم هذه البيانات متعلقة بجنح بسيطة تمت في الماضي القديم. واعترفت أربع من خمس ولايات أمريكية تم الاتصال معها بواسطة مكتب تقييم التقنية أنها لم تتأكد أبدا من دقة البيانات في ملفاتها.

رابعا: "أن المعلومات الشخصية التي كانت فيما قبل منفصلة ويصعب التوصل إليها، أصبحت في بنوك المعلومات مجمعة ومتكاملة ويمكن الوصول إليها بسهولة، ويمكن استخدامها في أغراض الرقابة على الأفراد، وهكذا تتأكد مقولة آرثر ميللر:- أن الحاسب بشراهته التي لا تشبع للمعلومات، وانسمعة التي ذاعت حول عدم وقوعه في الخطأ وذاكرته القوية، قد يصبح المركز العصبي لنظام رقابي يحول المجتمع إلى عالم شفاف تظهر فيه بيوتنا ومعاملاتنا المالية، واجتماعاتنا وحالتنا العقلية والصحية لمستخدمى الحاسب "[٢٣].

خامسا :- إن تكامل عناصر تكنولوجيا المعلومات مع الاتصالات والوسائط المتعددة أتاح وسائل رقابة متطورة سمعية ومرئية ومقروءة ، إضافة إلى برامج الرصد وجمع المعلومات آليا. كما أتاحت الانترنت القدرة العالية لجمع المعلومات ومعالجتها عبر تقنيات الذكاء الاصطناعي التي تتمتع بها شبكات الحاسبات، والتي تتوفر لدى محركات البحث وبرامج تحليل البحث على الشبكة.

وفي بيئة الانترنت، يستخدم العديد من الوسائل التقنية لرصد المعلومات الشخصية للمشتركين. من اشهرها ما يعرف برسائل (كوكيز -) التي تنتقل إلى المستخدم بمجرد دخوله للموقع وتتمكن من تسجيل بياناته، ومع أنها كوسيلة استخدمت لغرض غير جرمي وهو إرسال بريد الكتروني من الشركات التجارية في إطار أنشطتها الدعائية، إلا أن ذلك لا يمنع أنها تكشف عن بيانات قد لا يرغب الشخص الكشف عنها. أما الوسيلة الأخطر فهي ما تعرف بـ (برامج الرصد) وهي وسيلة رصد لجمع اكبر قدر من المعلومات السرية

والخاصة عن طريق ما يعرف بأنظمة جمع المعلومات. وفى هذا الصدد، أساء العديد من جهات الرقابة استخدام البيانات الخاصة حتى في أكثر الدول المتقدمة، وكان الهدف من وراء ذلك غالبا إما سياسيا أو اقتصاديا. لهذا كانت البيانات المستهدفة هي بيانات المعارضة السياسية والصحفيين وناشطي حقوق الإنسان، وهو ما اقتضى تزايد النشاط الدولي في مجال حماية الخصوصية من أنشطة الرقابة الالكترونية.

٦- الجهود الدولية والإقليمية لحماية الخصوصية فى مجال تكنولوجيا المعلومات والاتصالات [٢٥]

قام العديد من المنظمات الدولية بجهود كبيرة لتنظيم حماية المعلومات الخاصة وتنظيم تدفق وانتقال البيانات، مثل منظمة التعاون الاقتصادي والتنمية، ومجلس أوروبا، واتحاد أوروبا، والأمم المتحدة، ومجموعة الدول السبع ومنظمة التجارة العالمية.

٦-١ منظمة التعاون الاقتصادي والتنمية :

تضم منظمة التعاون الاقتصادي والتنمية في عضويتها ٢٩ دولة حتى أواخر عام ٢٠٠٠ وغرضها الرئيسى تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتزامن التطور الاقتصادي مع التنمية الاجتماعية.

بدأت هذه المنظمة عام ١٩٧٨ فى وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات[٢٦]، وقد تم تبني هذه القواعد من قبل مجلس المنظمة. وفي عام ١٩٨٠ تم توصية الأعضاء بتبنى هذه القواعد، وهى غير إلزامية وإنما مجرد إرشادات وتوصيات. وتغطي هذه القواعد الأشخاص الطبيعيين فقط وتطبق على القطاعين العام والخاص ، وتتعلق أيضا بالبيانات المعالجة آليا أو يدويا ، وتتضمن التوجيهات المبادئ الثمانية الرئيسة لحماية الخصوصية أو الحق في حماية البيانات الخاصة ، وهذه المبادئ هي :-

- تحديد حصر عمليات جمع البيانات -
- الاقتصار على طبيعة البيانات الشخصية
- تحديد نوعية البيانات
- تحديد الغرض وحصر الاستخدام بالغرض المحدد
- توفير وسائل حماية وامن المعلومات
- العلانية والحق في المشاركة والمساءلة.

وكان لهذه الوثيقة دور رئيسي في اتجاه الدول الأوروبية إلى إقرار تشريعات وطنية في مجال الخصوصية، ومنذ ذلك التاريخ تتابع هذه المنظمة موضوع الخصوصية وتضعه ضمن أجندتها السنوية و التدابير التشريعية .

٦-٢ مجلس أوروبا:-

وقد كلف عام ١٩٥٠بوضع الاتفاقية الأوروبية لحقوق الإنسان والحريات العامة، حيث أوجبت المادة الثامنة منها حماية الحياة الخاصة (وجوب حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم)، كما قررت المادة العاشرة من هذه الاتفاقية وجوب حماية حق الوصول إلى المعلومات.

في عام ١٩٨١ تبنت لجنة الوزراء - المكلفة بمعالجة موضوع الخصوصية- اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية، وقد وقعت على هذه الاتفاقية ٣١ دولة. وقد أصبحت هذه الاتفاقية نافذة بتاريخ ١٩٨٥/١٠/١.

وعلى خلاف توصيات منظمة التعاون الاقتصادي والتنمية، فان هذه الاتفاقية ملزمة للأعضاء المتعاقدين وينحصر نطاقها في الأشخاص الطبيعين وفي الملفات الإلكترونية، وتطبق على الملفات الإلكترونية في القطاعين العام والخاص، وتحدد هذه الاتفاقية عشر مبادئ تمثل الحد الأدنى لمعايير حماية الخصوصية المتعين على الدول الأعضاء تضمينها في التدابير التشريعية والقوانين التي تضعها، وهذه المبادئ مقاربة جدا لمبادئ منظمة التعاون الاقتصادي والتنمية ولكن مع مزيد من التفصيلات وهي:- (تحقيق العدل الاجتماعي، قيود الجمع، الوقاية، العلنية، تحديد الغرض والمدى، الدقة، مشاركة الأفراد)، واستنادا إلى هذه المبادئ الأساسية للحماية فان قواعد الاتفاقية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة، وتمنع نقل أية معلومات خارج الحدود إلا للدولة التي يتوفر بها أسلوب حماية موازية.

٦-٣ الاتحاد الأوروبي:

بدأ الاتحاد الأوروبي جهوده عام ١٩٧٦ بشأن توحيد القواعد المقررة في قوانين حماية الخصوصية، وفي هذا المجال صدر عن الاتحاد تعليمات عديدة وهي:- تعليمات ٧٦/٤/٨ المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات ، وتعليمات ٧٩/٥/٨ المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات وتعليمات ٨٢/٣/٩ بذات الموضوع . وقد طلب البرلمان الأوروبي من الاتحاد إصدار خطة تدفع الدول الأعضاء إلى توقيع الاتفاقية الأوروبية المتعلقة بالخصوصية، وصدر بتاريخ ٨١/٧/٢٩ توصية للدول الأعضاء بتوقيع اتفاقية مجلس أوروبا المشار إليها أعلاه. ومنذ عام ١٩٨٥ فان حماية الخصوصية بالنسبة للأشخاص الطبيعين والمعنويين (الشركات والمؤسسات) يجري مناقشتها والتعامل معها من قبل المجلس الاستشاري القانوني التابع للجنة الأوروبية، هذا إلى جانب تقديم الاتحاد مشاريع (حزمة) أدلة توجيهية متكاملة حول حماية

البيانات كان حصيلتها دليل عام ١٩٩٥ بشان حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية نقلها [٢٧]، وهو الدليل المقرر من قبل البرلمان الأوروبي ومجلس أوروبا إضافة إلى دليل ١٩٩٧ المتعلق بحماية بيانات الاتصالات[٢٨].

٦-٤ الأمم المتحدة:

تبنت الأمم المتحدة في عام ١٩٨٩ دليلا يتعلق باستخدام الحاسبات في عملية تدفق البيانات الشخصية، وبتاريخ ٩٠/١٢/١٤ تبنت الجمعية العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية[٢٩]. ويتضمن المبادئ المقررة لدى منظمة التعاون الاقتصادي والتنمية ولدى مجلس أوروبا والاتفاقيات المشار إليها أعلاه، وهي مبادئ غير ملزمة ومجرد توصيات للدول الأعضاء لتضمينها التدابير التشريعية في هذا المجال وقد بذل العديد من الجهود لحماية الخصوصية من قبل لجنة حقوق الإنسان في المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة.

٦-٥ مجموعة الدول السبع (لاحقا مجموعة الثمان)

أطلقت مجموعة الدول السبع مجموعة توصيات لحماية الخصوصية ضمن مؤتمرها الذي عقد حول مجتمع المعلومات في عام ١٩٩٥[٣٠].

٦-٦ منظمة التجارة العالمية

ناقشت منظمة التجارة العالمية مسائل الخصوصية فيما يتعلق بحرية انتقال المعلومات تحديدا بالنسبة إلى اتفاقية تحرير الخدمات، وقد أقرت المنظمة بان الخصوصية قيد عادل على عملية انتقال البيانات.

٧- المبادئ الأساسية للممارسات العادلة في نطاق خصوصية (حماية) البيانات الشخصية بالبيئة الرقمية

إن حماية الخصوصية في البيئة الرقمية عملية وليست مجرد إجراء، بمعنى أنها تنطلق من رؤيا محددة المعالم واضحة الأهداف تكون مخرجاتها مجموعة من الوسائل والإجراءات في مجالات التقنية والقانون وإدارة النظم التقنية، وبوصفها عملية تكاملية، فإنها محكومة بإستراتيجية تحدد عناصر الحماية ونطاقها، لهذا فان من الخطأ مجرد الاعتقاد أن استخدام بعض التقنيات التي تحدي البيانات الشخصية قد تحقق حماية الخصوصية، ومن الاعتقادات الخاطئة أيضا أن مجرد التزام جهات جمع البيانات باحترام الخصوصية يحقق الحماية، والخطأ الأكثر خطورة إغفال أهمية الحماية القانونية الشمولية وتكاملها مع الحماية التقنية والخطوات التنظيمية.

وهناك خمسة مبادئ أساسية تحكم ما يمكن تسميته بالممارسات العادلة والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية في بالبيئة الرقمية، وهي[٣١]:-

- **الإبلاغ / الإخطار:** ويراد بهذا المبدأ أن مستخدمي المواقع يتعين إبلاغهم من قبل مزود الخدمة أو الموقع ما إذا كان الموقع أو مقتضيات الخدمة ينطويان على جمع بيانات شخصية والى أي مدى تجمع هذه البيانات وتستخدم.

- **الاختيار:** ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بشان استخدام بياناته فيما يتجاوز غرض جمعها الأساسى.

- **الوصول للبيانات:** ويوجب هذا المبدأ قدرة المستخدمين للوصول إلى بياناتهم والتأكد من صحتها وتحديثها.

- **الأمن:** ويتعلق هذا المبدأ بمسؤوليات جهات جمع البيانات (المواقع ومزودي الخدمة) بشان معايير الأمن المتعين تطبيقها لضمان سرية البيانات وسلامة الاستخدام ومنع الوصول غير المصرح به لهذه البيانات، باستخدام كلمات السر والتشفير وغيرها من وسائل امن المعلومات.

- **تطبيق القانون:** ويتعلق هذا المبدأ بالآليات المناسبة الواجب اعتمادها لفرض الجزاءات على الجهات غير المتوافقة مع المبادئ المتقدمة وما يتصل بها من الممارسات النزيهة بشان جمع البيانات الشخصية في البيئة الرقمية.وفي المقابل فان هذه المبادئ الخمسة ، يتعين أن لا تنتقص من سمات مجتمع الانترنت الديمقراطي، وهي في حقيقتها لا تتعارض مع هذه السمات لان موجبات ديمقراطية الانترنت عدم المساس بحقوق المستخدمين، وأن تكون عمليات الاستخدام في منأى من التشدد. ويعمل بالتوازي مع هذه المبادئ. مبدأ رضا وموافقة المستخدم إلى جانب الاستثناءات المقررة بموجب معايير تقديم الخدمة التي تتيح قدرا من الحرية لجهات جمع البيانات وفقا لنظم مسئولياتها القانونية أو مدونات السلوك التي تحكمها مع ضوابط لضمان صحة وسلامة الرضا وضبط الاستثناءات أو ما يمكن تسميته الممارسات المسموح بها لجهات تقديم الخدمة وإدارة المواقع.

إن التوازن بين مجتمع الإنترنت الديمقراطي وموجبات حماية خصوصية المستخدمين يتحقق عن طريق المعيار المنضبط والمرن في ذات الوقت، معيار يكفل للمستخدم حماية بياناته الشخصية التي يتم جمعها من المواقع .ويتيح للمواقع التعامل بشكل مناسب مع أغراض وسمات الانترنت وأغراض الموقع نفسه دون مغالاة.

٨- عناصر الحماية المتكاملة لخصوصية المعلومات فى البيئة الرقمية

في أكتوبر عام ١٩٩٧ قررت منظمة التعاون الاقتصادي والتنمية فحص ورصد مختلف الحلول التي تساعد على تطبيق مبادئ حماية الخصوصية في بيئة شبكات المعلومات العالمية وذلك في إطار السعي لبناء الثقة بين التجارة الإلكترونية وبيئة التقنية والاتصالات. وقد صدر تقرير خاص عن المنظمة بهذا الخصوص، وهو تقرير (تطبيق دليل للخصوصية في البيئة الإلكترونية مع التركيز على الإنترنت)[٣٢] وتوصل التقرير إلى أن دليل الخصوصية الصادر عن المنظمة عام ١٩٨٠ قابل للتطبيق على التقنيات الجديدة أياً كان وضعها ما دامت تقوم بأنشطة جمع ومعالجة البيانات، ودعا التقرير جهات الأعمال في البيئة الالكترونية إلى:-

- تبني سياسات واستراتيجيات وحلول تقنية لضمان حماية خصوصية الأفراد في نشاطهم عبر الشبكة وتحديداً الإنترنت،
- توسيع أنشطة التوعية والتعليم للمسائل المرتبطة بحماية الخصوصية واستخدام التقنيات الحديثة.
- مناقشة الاتجاهات الجديدة المتصلة بحماية البيانات الشخصية في بيئة الشبكات من خلال القطاعات الحكومية والصناعية وقطاعات الأعمال والمستخدمين وسلطات حماية البيانات.

واستناداً إلى التقرير المشار إليه، عقدت اللجنة الاستشارية للأعمال الصناعية ورشة عمل تحت عنوان "حماية الخصوصية في مجتمع الشبكات العالمية" خلال الفترة من ١٦ — ١٧ فبراير ١٩٩٨، لتحديد آلية تطبيق دليل الخصوصية، الصادر عن المنظمة على الشبكات العالمية، في ضوء الاتجاهات التشريعية للدول الأعضاء في مجال حماية الخصوصية مع التركيز على تشجيع القطاع الخاص لتبني مدونات سلوك وتنظيمات خاصة لحماية البيانات الشخصية في بيئة شبكات المعلومات العالمية. وقد تناولت ورشة الأعمال التالي:-

- تحديد احتياجات القطاع الخاص والمستخدمين والمستهلكين لبناء إستراتيجية التعريف بالخصوصية وصيغة هذه الإستراتيجية ، وتطوير تقنيات حماية الخصوصية.
- تطبيق تشريعات الخصوصية ومدونات السلوك والمعايير المقررة في القطاع الخاص.
- تبني حلول تعاقدية نموذجية من أجل تدفق ونقل البيانات خارج الحدود.

وفي النهاية توصل المشاركون إلى أن:- تعميم استخدام الوسائل التقنية لحماية الخصوصية على الخط مسألة أساسية وجوهرية لتطور الأعمال الالكترونية والتجارة الإلكترونية. وحماية خصوصية الأفراد في بيئة الشبكات. وذلك بالحفاظ على الحقوق من جهة، وضمان عدم الحد من تدفق البيانات خارج الحدود من جهة أخرى.

- تتطلب حماية الخصوصية الوعي والشفافية والفعالية، وتبني الحلول التكنولوجية الملائمة والشاملة.

وأوصت الورشة بإجراء دراسة مسحية للمتوفر من التعليمات والقواعد القانونية بما في ذلك القوانين والتنظيمات الخاصة والعقود والتقنيات من أجل تحديد فعالية تطبيق القواعد المقررة في بيئة الشبكات. وهذه الدراسة يتعين -كما أوصت الورشة- أن تحدد السياسات التقنية والأدوات القانونية اللازمة لضمان حماية فاعلة للخصوصية[٣٣].

ولتحقيق تكاملية حماية البيانات الشخصية في البيئة الرقمية، يتطلب الأمر توفر العناصر التالية:-

١- توفير أدوات حماية متطورة للحد من أو منع عمليات جمع البيانات الشخصية التي تتم دون علم المستخدم، وكذلك تقنيات تتيح للمستخدم التعامل مع البيئة الرقمية بقدر من التخفي ملائم لأغراض الاستخدام. (البعد التقني للحماية)

٢- توفير البناء القانوني الملائم لتنظيم عمليات الحماية، ويشمل ذلك تشريعات حماية البيانات الشمولية والقطاعية. ومدونات السلوك والتنظيم الذاتي لقطاعات الخدمة والإنتاج، ووسائل الحماية التعاقدية كسياسات الخصوصية الملائمة التي تلتزم بها جهات الخدمات التقنية نفسها، أو عقود تبادل المعلومات المناسبة التي تبرم لتغطية نقل البيانات خارج الحدود للدول التي لا تتوفر فيها تشريعات الحماية الملائمة. (البعد القانوني للحماية)

٣- توفير وتعميم استراتيجيات التعامل الإدارية والتنظيمية الملائمة لدى المؤسسات والمستخدمين لتحقيق الحماية المنطلقة من معرفة المخاطر ووسائل تقليلها أو منع حدوثها. (البعد التوعوي للحماية)

٨-١ وسائل وأدوات الحماية التقنية

يمكن للأفراد في تعاملهم مع الإنترنت استخدام وسائل جديدة لحماية خصوصياتهم، فمن البريد المتخفي والمتصفحات التي تسمح بالتجول دون كشف الهوية عبر الإنترنت ، وحتى برامج التشفير التي تحمي البريد الإلكتروني والمراسلة عبر الشبكة؛ وما بينهما من وسائل، يمكن للمستخدم توظيف التقنية ذاتها لتعزيز

الخصوصية. ونجد المجلس الفيدرالي الأمريكي المشرف على البنوك الأمريكية يطلب من البنوك معرفة عملائهم، وهي بالفعل إستراتيجية مصرفية سليمة لخدمة العمل المصرفي، لكنها في الوقت ذاته ساعدت على توظيف تقنيات الرصد والرقابة وجمع البيانات عن العملاء[٣٤].

إن تطبيقات تقنية المعلومات والاتصالات في مجال حماية الخصوصية تعرف على نطاق واسع (بتقنيات تعزيز الخصوصية) [٣٥] ، وتعرف بأنها معايير أنظمة تقنيات الاتصالات والمعلومات المتكاملة التي تحمي الخصوصية عن طريق إزالة أو تقليل البيانات الشخصية، أو عن طريق الحماية من عمليات معالجة البيانات الشخصية غير الضرورية أو غير المرغوب فيها دون التأثير على كفاءة أداء نظام البيانات[٣٦].

وتحث كل الوثائق الدولية والإقليمية وكذا القوانين الوطنية جهات المعالجة على اعتماد وسائل تقنية ملائمة لحماية عمليات معالجة البيانات الشخصية [٣٧]. ولو أخذنا — مثلا – الأمر التشريعي الأوروبي لعام ١٩٩٥ لحماية معالجة البيانات الشخصية وتدفقها عبر الحدود فإننا نجد أن المادة ١٧ منه تطلب من جهات المعالجة أن تطبق معايير تقنية وتنظيمية لحماية البيانات الشخصية وخاصة أثناء تبادلها عبر الشبكات.

٨-١-١ وسائل الأمن التقنية [٣٨]

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والأدوات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها.

والجدير بالذكر أن وسائل الأمن متعددة من حيث الطبيعة والغرض، لكن يمكن بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية إلى المجموعات التالية:-

- **مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وصلاحية الاستخدام ومشروعيته** ، وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه المجموعة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع البرامج التي تزود كلمات سر آنية أو وقتية متغيرة الكترونيا، والمفاتيح المشفرة، بل تضم هذه المجموعة ما يعرف بتحديد الصلاحيات.

- **مجموعة الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة** وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة. وتشمل تحديد حقوق المستخدمين، أو قوائم أشخاص

المستخدمين أنفسهم، أو تحديد مزايا الاستخدام أو غير ذلك من الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة.

- **مجموعة الوسائل التي تهدف إلى تحقيق سرية المعلومات** ، وتشمل تقنيات تشفير البيانات والملفات ، وإجراءات حماية نسخ الحفظ الاحتياطية، والحماية المادية للأجهزة ومكونات الشبكات.

- **مجموعة وسائل إلى الحماية المتكاملة (سلامة المحتوى)** Data and message integrity وهي الوسائل المناط بها ضمان عدم تعديل محتوى البيانات من قبل جهة غير مخولة بذلك، وتشمل تقنيات الترميز والتوقيعات الإلكترونية وبرامج تحري الفيروسات وغيرها.

- **مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص)** - ، وتهدف هذه الوسائل إلى ضمان عدم إنكار المستخدم للتصرفات التى قام بها على البيانات، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط [٣٩]، وترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

- **وسائل مراقبة الاستخدام ورصد سجلات النفاذ أو الأداء (الاستخدام)** ، وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بعمل ما في وقت معين، وتشمل كافة أنواع البرامج والسجلات الإلكترونية التي تحدد الاستخدام.

و فيما يلى، نوضح بإيجاز أكثر وسائل وأدوات الأمن شيوعا في بيئة تكنولوجيا المعلومات:- [٤٠]

(أ) برامج كشف ومقاومة الفيروسات

بالرغم من أن تقنيات مضادات الفيروسات تعد الأكثر انتشارا وتعد من بين وسائل الأمن المعروفة للعموم، إلا أن حجم تطبيق هذه التقنيات واستراتيجيات وخطة التعامل معها تكشف عن ثغرات كبيرة، وعن أخطاء في فهم دور هذه المضادات. وهناك بعض القواعد الأساسية لتحقيق فعالية هذه الوسائل والتي تعتمد في الواقع على الموازنة ما بين ضرورات هذه التقنيات لحماية النظام، وما قد يؤثره الاستخدام الخاطئ لها على الأداء وفعالية النظام.

(ب) الجدران النارية والشبكات الافتراضية الخاصة

تطورت الجدران النارية بشكل كبير، حيث إنها كانت تقوم عند نشأتها بتصفية (فلترة) حركة البيانات اعتمادا على قوانين ومعاملات بسيطة. أما برامج الجدران النارية الحديثة، ورغم أنها لا تزال تقوم بعملية

التصفية، فإنها تقوم بإنشاء الشبكات الافتراضية الخاصة ، ورقابة محتوى البيانات، والوقاية من الفيروسات، وحتى إدارة نوعية الخدمة. وهذه الخدمات جميعها تعتمد على ميزة أساسية وهي أن الجدران النارية تقع على طرف الشبكة، وتضمينها قدرات متعددة مثل: التحقق من هوية المستخدمين،الشبكات الافتراضية الخاصة، مراقبة المحتوى ، البحث عن الفيروسات.

(ج) التشفير

تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمن المعلومات، والسبب في ذلك أن حماية التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة(السرية والتكاملية وتوفير المعلومات). ومن حيث المفهوم، فان التشفير يمر بمرحلتين رئيستين، الأولى تشفير النص وتحويله إلى رموز غير مفهومة أو مقروءة، والثانية، فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء.

وهذه المسالة تقوم بها برامج التشفير التي تختلف أنواعها ووظائفها. أما من حيث طرق التشفير، فهناك التشفير الترميزي. والتشفير المعتمد على مفاتيح التشفير،التي قد تكون مفاتيح عامة أو خاصة أو مزيجا منها.

٨-١-٢ إستراتيجية أمن المعلومات وكيف يتم بناؤها [١١]

٨-١-٢-١ المفاهيم والمحددات الأولية

(أ) إستراتيجية أمن المعلومات

إن إستراتيجية أمن المعلومات، أو سياسة أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص عند التعامل مع التقنية داخل المنشأة، وتتصل بإجراءات الدخول إلى المعلومات والعمل على تنظيمها وإدارتها.

(ب) أهداف إستراتيجية أمن المعلومات

تهدف إستراتيجية أمن المعلومات إلى تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم لحماية نظام الكمبيوتر والشبكات، وكذلك حماية المعلومات بكافة أشكالها وفي مراحلها المختلفة من إدخال ومعالجة وتخزين ونقل واسترجاع، وتحديد التقنية المناسبة لتنفيذ الواجبات المحددة للمتعاملين مع المعلومات وتنظيمها، وتحديد المسئوليات عند حدوث الخطر، وتحديد الإجراءات الواجب اتباعها لتجاوز المخاطر والتهديدات ، وتحديد الجهات المنوط القيام بذلك

(ج) فريق عمل إعداد إستراتيجية أمن المعلومات

يتطلب إعداد إستراتيجية أمن معلومات أن تتضافر جهود مختلف المستويات الوظيفية في المنشأة الواحدة، ولكنها بوجه عام تشمل مسئولي أمن الموقع ومديري الشبكات وموظفي وحدة الكمبيوتر ومديري الوحدات المختلفة في المنشأة كوحدة الأعمال والتسويق والبحث وغيرها، وتشمل أيضا فريق الاستجابة للحوادث والأعطال وممثلي مجموعات المستخدمين والإدارة العليا إلى جانب الإدارة القانونية.

(د) أسباب نجاح إستراتيجية أمن المعلومات

من حيث فعالية الاستخدام:- لكي توصف إستراتيجية أمن المعلومات بأنها ناجحة يتعين أن تعمم على كافة القطاعات، وان تكون مقبولة من الجهات التى تقوم بتنفيذها، إلى جانب توفر دليل التوجيه والإرشاد لضمان استمرار التنفيذ. والتنفيذ يعنى الاستخدام الفعلي لأدوات الحماية من جهة، والتطبيق الفعلي لقواعد العمل والتعامل مع البيانات ونظمها من جهة أخرى. ولذلك يجب أن تتصف الإستراتيجية بالدقة والوضوح لمنفذيها لضمان نجاحها.

أما من حيث المحتوى :- يجب أن تحتوى الإستراتيجية على سياسة واضحة بشأن اقتناء وشراء الأجهزة التقنية وأدواتها ، والبرامج ، والحلول المتصلة بالعمل ، والحلول المتعلقة بإدارة النظام . كما يجب أن توضح الإستراتيجية درجة أهمية المعلومات وقيمتها ووصفها من حيث السرية، كما تبين الاستثناءات التي تعتمدها على حق الخصوصية لموظفي المنشأة مع مبررات هذه الاستثناءات، مثل رقابة الوصول إلى ملفات المستخدمين بالمنشأة. ومن حيث الدخول إلى الشبكات والمعلومات فلا بد من وجود إستراتيجية واضحة تحدد حقوق وامتيازات كل شخص في المنشأة للوصول إلى الملفات أو مواقع معينة في النظام إضافة إلى سياسة بشأن التعامل مع الاتصالات الخارجية، والبيانات ، وأجهزة ووسائل الاتصال المستخدمة، وإضافة البرامج الجديدة، واستراتيجيات المراسلة مع الآخرين.

وتضم إستراتيجية المعلومات أيضا سياسة المنشأة بشأن اشتراكات الغير في شبكتها أو نظمها، وكذلك سياسة التعامل مع المخاطر والأخطاء، بحيث تحدد ماهية المخاطر وإجراءات الإبلاغ عنها والتعامل معها، والجهات المسئولة عن التعامل مع هذه المخاطر.

٨-١-٢-٢ أسس إستراتيجية أمن المعلومات [٢]

يتعين أن ينطلق أمن المعلومات من تحديد المخاطر، وأغراض الحماية، ومواطن الحماية، وأنماط الحماية اللازمة. وإجراءات الوقاية من المخاطر.

(أ) أغراض حماية البيانات الرئيسية.

(١) السرية: التأكد من أن المعلومات لا يتم الإطلاع عليها من قبل أشخاص غير مخولين بذلك.

(٢) التكاملية وسلامة المحتوى: التأكد من أن محتوى المعلومات صحيح لم يتم تعديله أو العبث به. وبشكل خاص لن يتم تدمير المحتوى أو تغيره عن طريق تدخل غير مشروع.

(٣) استمرارية توفر المعلومات أو الخدمة:- التأكد من استمرار تقديم الخدمة للمستفيدين، مع التأكيد على عدم حرمان المستفيدين من التعامل مع النظام وحصولهم على كافة البيانات المتوفرة به.

(ب) مناطق أمن المعلومات

(١) أمن الاتصالات: ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر

(٢) أمن الكمبيوتر: ويراد به حماية المعلومات داخل النظام بكل أنواعها وأنماطها كحماية نظام التشغيل، و حماية برامج التطبيقات، وحماية برامج إدارة البيانات، وحماية قواعد البيانات بأنواعها المختلفة.

ولا يتحقق أمن المعلومات دون توفير الحماية المتكاملة لهذين القطاعين عبر معايير أمنية تكفل توفير هذه الحماية. ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة.

(ج) أنماط ومستويات أمن المعلومات

(١) الحماية المادية: وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من الوسائل التي تمنع الوصول إلى أجهزة المنشأة الهامة.

(٢) الحماية الشخصية: وهي تتعلق بالموظفين العاملين على النظام التقني من حيث توفير وسائل التعريف الخاصة بكل منهم، وتدريبهم بشكل مستمر لضمان تأهيل المتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات.

(٣) الحماية الإدارية: ويراد بها السيطرة على إدارة نظم المعلومات وقواعدها، مثل التحكم فى البرامج الخارجية عن المنشأة، و التحقيق فى اخلالات الأمن، وعمليات الإشراف والمتابعة لأنشطة الرقابة، بالإضافة إلى القيام بأنشطة التحكم فى الاشتراكات الخارجية.

(٤) الحماية الإعلامية– المعرفية : كالسيطرة على إعادة إنتاج المعلومات، وعلى عملية مسح المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها.

(د) المخاطر

هناك مخاطر يمكن أن تواجه نظام المعلومات بما في ذلك أنظمة التجارة الإلكترونية، وابرز هذه المخاطر هى:

(١) اختراق الأنظمة: ويتحقق الاختراق بشكل تقليدي من خلال أنشطة التخفي، ويراد به تظاهر الشخص المخترق بأنه شخص أخر مصرح له بالدخول. أو من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية، أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مختلفة، كالتنقيب في قمامة المنشأة للحصول على كلمات السر أو معلومات عن النظام أو عن طريق الهندسة الاجتماعية.

(٢) الاعتداء على حق التفويض: ويتم من خلال قيام الشخص المخول له استخدام النظام القيام ببعض الأعمال دون أن يحصل على تفويض بذلك. وهذا الخطر يعد من الأخطار الداخلية في مجال إساءة استخدام النظام من قبل موظفي المنشأة ، وهو قد يكون أيضا من الأخطار الخارجية ، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به، أو استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع ومن ثم القيام بأنشطة غير مشروعة .

(٣) زراعة نقاط الضعف: عادة ينتج هذا الخطر عن اقتحام من قبل شخص غير مصرح له بذلك أو من خلال مستخدم مشروع تجاوز حدود التفويض الممنوح له. ومن أشهر هذه الأمثلة مخاطر حصان طروادة، وهو عبارة عن برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن أن يستخدم في الخفاء للقيام بنشاط غير مشروع، كأن يستخدم برنامج معالجة كلمات ظاهريا لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام أو نقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتوياته.

(٤) مراقبة الاتصالات: حيث يتم من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها الحصول على معلومات سرية عن المجنى عليه – دون اختراق كمبيوتر الخاص به– تساعد مستقبلا على اختراق النظام.

(٥) اعتراض الاتصالات: تتم عملية اعتراض الاتصالات عن طريق قيام الجانى بعمل نظام وسيط يسمح من خلاله بمرور بيانات المجنى عليه أثناء عمليات نقل البيانات – دون اختراق كمبيوتر – ، ثم إجراء التعديلات اللازمة على هذه البيانات لخدمة عملية الاعتداء لاحقا.

(٦) تدهور (إعاقة) الخدمة: ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة. وابرز أنماط تدهور (إعاقة) الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة –تفوق القدرة التخزينية– إلى موقع الخدمة.

(٧) عدم الإقرار بالقيام بالتصرف: وهو إنكار الشخص لقيامه بعمل أو تصرف معين مثل إنكاره بإرسال طلب الشراء عبر الإنترنت.

والجدير بالذكر، أن عملية تحليل المخاطر هي في حقيقتها نظام متكامل للتحليل وسلامة التصرف تبدأ من الإعداد الجيد القائم على فهم وإدراك وتحديد عناصر النظام والعمليات والمخاطر . ومن ثم تحديد معايير التهديد ونطاق الحماية المطلوب منها، ووسائل الحماية . لتنتهي ببيان معيار الخسارة المقبولة التي يتصور تحققها بغض النظر عن مستوى الحماية ومستوى الاستعداد للمواجهة.

(هـ) الوقاية من مخاطر الاعتداء على المعلومات

في ميدان حماية الاتصالات وحماية الكمبيوتر يعبر عن إجراءات الوقاية بخدمات الأمن، ولا يقصد بها الخدمات بالمعنى المعروف، وإنما أطلق هذا التعبير جراء وجود شركات متخصصة بأمن المعلومات تقدم هذه الخدمات، وبالعموم فان هناك خمسة أنواع أساسية لخدمات الأمن تستهدف حماية خمسة عناصر رئيسة في ميدان المعلومات وهي :

(١) خدمات (وسائل) حماية التعريف هذه الخدمات تهدف إلى التأكد من الهوية وتحديدا عندما يقوم شخص ما بالتعريف عن نفسه، فان هذه الخدمات تهدف إلى التأكد من ذلك. ولهذا فان التعريف يحدد الوسائل التي تحمي من أنشطة التخفي والتنكر، ومن هنا فان هناك نوعين من خدمات التعريف الأول تعريف الشخصية وأشهر وسائلها كلمة السر، وثانيها التعريف بأصل المعلومات كالتأكد من أصل الرسالة .

(٢) خدمات (وسائل) التحكم فى الدخول: وهذه الخدمات تستخدم للحماية من الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات. ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن (الاستخدام، والإفشاء، والتعديل، والإتلاف) الغير مصرح بها، وإصدار المعلومات والأوامر غير المصرح بها، ولهذا فان خدمات التحكم فى الدخول تعد الوسائل الأولية لتحقيق التفويض والتأكد منه .

(٣) خدمات (وسائل) السرية: هذه الخدمات تحمي المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها. والسرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها على سبيل المثال، أو من خلال وسائل أخرى كمنع التعرف على حجمها أو مقدارها أو الجهة المرسلة إليها.

(٤) خدمات (وسائل) حماية تكامل وسلامة المحتوى: هذه الخدمات تهدف إلى حماية مخاطر تغيير البيانات خلال عمليات إدخالها أو معالجتها أو نقلها. وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو إعادة تسجيل جزء منها أو غير ذلك، وتهدف هذه الوسائل أيضا إلى الحماية من أنشطة تدمير البيانات بشكل كامل أو إلغائها دون تخويل.

(٥) خدمات (وسائل) عدم الإنكار: وهذه الخدمات تهدف إلى منع الجهة التي قامت بالتصرف من إنكار فعل ما قد قامت به، مثل نقل البيانات.

التوصيات

- يجب إنشاء مجلس قومي لمكافحة الجريمة الإلكترونية- خاصة وأنها في ازدياد مستمر- مما يتطلب جهاز أمن وادعاء وقضاء الكتروني، وأيضاً قوانين الكترونية للحد من تلك الجريمة وضبطها. ويتطلب تحقيق الجهاز لأهدافه وجود مجموعة من العاملين ذوى مهارات الكترونية متقدمة.
- يجب على المؤسسات التشريعية بالدول العربية في ظل عصر المعلومات، إدراك الحاجة إلى سن حزمة متكاملة من التشريعات لمعالجة كافة مشاكل عصر المعلومات وآثاره على النظام القانوني، حيث أصبح شعار الحد الأدنى من التنظيم القانوني للتجارة الالكترونية -بالنسبة للبيئة العربية- ليس مقبولا لغياب القواعد الأساسية التي تغطي مختلف جوانب قانون الكمبيوتر والإنترنت.
- يجب الاعتراف بقانونية الوثائق والرسائل الإلكترونية والتوقيعات والعقود الإلكترونية وقبولها كدليل في المنازعات القضائية، وإلا سيؤدى ذلك إلى إعاقة تطور التجارة الإلكترونية في زمن انتشار استخدام الانترنت.

– تطوير تشريعات التجارة والشركات لمواكبة المستجدات في السداد النقدي ونقل الأموال بالطرق الالكترونية، وأوراق الدفع، والمشاريع الاستثمارية، والاندماج، واتفاقيات التجارة الدولية، ونقل التكنولوجيا، وإجازة الأنشطة المصرفية الالكترونية وغيرها.

– يجب على المصارف العربية تبنى استراتيجيات عمل واضحة، تغطى الأبعاد الاستثمارية والتقنية والقانونية لاستخدامات الهواتف المحمولة والوسائل اللاسلكية في العمل المصرفي.

– يجب حماية مستخدم الانترنت من العديد من أنشطة الغش والمساس بمصالحه، وذلك بوضع نصوص تشريعية تنظم سوق وخدمات التقنية، وتضمن معايير الجودة، ومعايير موثوقية النظم، وخصوصية وامن المعلومات المخزنة فيها، وقواعد السلوك المهني في مجال خدمات الانترنت.

– يجب تحديد مسئولية مقدمي خدمةِ شبكة الانترنتِ، ومسئولية الجهات القائمة بخدمة التسليم المادي، ومسئولية جهات الإعلان، ومسئولية جهات التوثيق وإصدار الشهادات.

– ضرورة وجود نظام قانوني فعال لمواجهة مخاطر أمن المعلومات في بيئة الأعمال الإلكترونية ومواجهة مخاطر الاعتداء على خصوصية سرية بيانات الأفراد والمؤسسات. بحيث تجرم الدخول غير المصرح به إلى نظم المعلومات، وأنشطة الغش المعلوماتي والتجسس ، وتدمير البيانات. حفاظا على الخصوصية وتحقيقا للمبادئ الدولية المقررة لحماية البيانات الخاصة. واعتبار قضية حماية الخصوصية أداة للتنمية الاقتصادية لا عائقا لها وذلك عبر خلق ثقة متبادلة بين الشركات والعملاء.

– ضرورة توعية الشباب بصفة خاصة حول كيفية حماية خصوصيتهم عبر مجموعة من الآليات: قراءة وثيقة الخصوصية التي توضع بالمواقع الإلكترونية، تحديد نوع المعلومات التي يمكن نشرها وكيف يمكن مسحها إن اقتضى الحال.

المراجع والهوامش

١– البلوتوث، هى تقنية وصل رخيصة تمكنا من وصل أجهزة المحمول(هواتف ، الحواسب، والطابعات) بشبكة لا سلكية لمسافات قريبة تسمى منطقة الشبكة الشخصية . ظهرت هذه التقنية إلى الوجود فى النصف الثانى من عام ١٩٩١. ويرجع أصل هذه التسمية إلى ملك القراصنة الدانماركى المنقولة من الإنجليزية الذى عاش فى العقد الأخير من القرن العاشر. حكم هذا الملك الدانمارك والنرويج ووحدهما (من هنا أتت روح التسمية بتوحيد الأجهزة عبر تقنية البلوتوث)، وهى تعتبر أهم تقنيات المستقبل القادرة على ربط معدتنا الشخصية المحمولة بكل حرية وبدون قيود وربطها بشبكة الإنترنت.

٢– أحمد بدر وآخرون، السياسة المعلوماتية وإستراتيجية التنمية: دراسات شاملة لمصر والوطن العربى وبعض البلاد الأوربية والأمريكية والأسيوية والأفريقية ، دار الغريب للطباعة والنشر والتوزيع ، القاهرة.

٣- يعقوب فهد العبيد، التنمية التكنولوجية : مفهومها ومتطلباتها، الدار الدولية للنشر والتوزيع، القاهرة، ١٩٨٩.

٤- إعلان القاهرة: الوثيقة العربية نحو مجتمع معلومات عربي خطة العمل المشترك القاهرة في ١٨ يونيو ٢٠٠٣، ص٦

٥- عايض المرى، ما المقصود بأمن المعلومات وما هي عناصره، http://www.facebook.com/topic.php?uid=30922409577&topic=8015

٦- تعرف منظمة اليونسكو -من بين أشمل تعريفاتها- تكنولوجيا المعلومات بأنها "الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات وفي تطبيقاتها ، والمتعلقة بالحواسيب وتفاعلها مع الإنسان والآلات ، وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية" .

٧- عايض المرى، المرجع السابق

٨- عايض المرى، المرجع السابق

٩- إبراهيم حسن الملا، موقف القانون من أثر المعلومات والنظم الإحصائية وأثرها على الحياة العامة والخاصة، المؤتمر الدولى "أثر المعلومات والنظم الإحصائية المتكاملة على التنمية الاجتماعية والاقتصادية"، رأس الخيمة، الإمارات، ٨-١٠ نوفمبر ،٢٠٠٨.

١٠- http://www.arablaw.org/Download/Privacy_DataProtection.doc

١١- فؤاد جمال، جرائم الحاسبات والانترنت (الجرائم المعلوماتية).، http://www.tashreaat.com/view_studies2.asp?id=591&std_id=90،

١٢- فؤاد جمال، المرجع سابق.

١٣- فؤاد جمال، المرجع سابق.

١٤- http://www.arablaw.org/Download/Privacy_DataProtection.doc

١٥- يونس عرب ، موسوعة القانون وتقنية المعلومات ،الكتاب الثاني — دليل امن المعلومات والخصوصية — ج١ / جرائم الكمبيوتر والانترنت ، ج ٢ الخصوصية وحماية البيانات في العصر الرقمي، اتحاد المصارف العربية ،٢٠٠٢ .

١٦- سورة النور ، الآية ٢٧ ، (يأيها الذين أمنوا لا تدخلوا بيوتاً غير بيوتكم حتى تستأنسوا وتسلموا على أهلها)، سورة الحجرات ، الآية ١٢، (ولا تجسسوا ولا يغتب بعضكم بعضا).

١٧- صالح جواد كاظم، مباحث في القانون الدولي: التكنولوجيا الحديثة والسرية الشخصية، الطبعة الأولى، دار الشئون الثقافية العامة، بغداد، ١٩٩١. ص ١٣٦ . (وفى هذا الصدد يعرف أستاذ القانون الدولي) الحق في الحياة الخاصة أو الحرمة الشخصية بأنه : — " حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم إلى الآخرين ، والخصوصية : منظورا إليها من علاقة الفرد بالمشاركة الاجتماعية ، هي انسحاب الفرد الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية ". ويعرفه خبراء

مكتب العلوم والتقنية المرتبط بالبيت الأبيض الأمريكي بأنه: -" حق الفرد في أن يحدد بنفسه ما يتقاسمه مع الآخرين في أفكاره وعواطفه والحقائق المتعلقة بحياته الشخصية. كما عرفه مؤتمر رجال القانون المنعقد في استوكهولم في مايو ١٩٦٧ بأنه: - " الحق في أن يكون الفرد حرا في أن يترك ليعيش كما يريد مع أدنى حد للتدخل الخارجي.

١٨- The 2000 Privacy Report, The Electronic Privacy information centre, 2000. http://www.pricacyinternational.org.

١٩- يونس عرب ، مرجع سابق. وفي هذا الصدد يقول د. هشام رستم :- " أن هناك تباينات عدة حول تصور ماهية هذا الحق ، وتحديدا العناصر المكونة لمضمونه ، وهذه التباينات تفرضها في تقديرنا طبيعة هذا الحق وظروف نشأته وتطوره ، فضلا عن تأثره بجميع الأطر المجتمعية والثقافية بما في ذلك الدين والنظام السياسي والفلسفة ، والتغيرات التي تطرأ دوما على المجتمعات الإنسانية "

٢٠- الأمم المتحدة، أعمال الأمم المتحدة فى ميدان حقوق الإنسان، المجلد الأول، منشورات هيئة الأمم المتحدة، نيويورك، ١٩٩٠.

٢١- منيرة بنت فهد الحمدان، جواهر بنت عبد العزيز آل سعود، الجرائم الإلكترونية ومكافحتها، ٢٠٠٥، ص.٤.

٢٢- عبد الرحمن عبد العزيز الشنيفى، أمن المعلومات وجرائم الحاسب الآلى، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٧.

23- Ulrich Sieber, Computer-related Crime,1994.

24- Ulrich Sieber, the previous research.

٢٥- إبراهيم حسن الملا، مرجع سابق.

26- http://www.oecd.org

27- European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 :-
http://www2.echo.lu/legal/en/dataport/directive/directive.html

28- Ulrich Sieber, previous research .

29- http://www.datenschutz-berlin.de/gesetze/internat/aen:htm , http://www.un.org

30- www.g7.utoronto.ca

٣١- يونس عرب، استراتيجيات وتقنيات الحماية من أنشطة الاعتداء على خصوصية المعلومات، مرجع سابق.

32- Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet, DSTI/ICCP/REG (97)6/FINAL).

٣٣- يونس عرب، استراتيجيات وتقنيات الحماية من أنشطة الاعتداء على خصوصية المعلومات، مرجع سابق.

34- Inventory of Instrument and Mechanisms Contributing To The Implementation of the OECD Privacy Guidelines on Global Networks, Working Party on Information Security and Privacy, 19 May 1999.

35- Center for Democracy & Technology, Privacy Not Price: Keeping People Off The Internet, CDT's Analysis of Recent Privacy Surveys http://www.cdt.org/privacy/survey/findings/surveyframe.html.

36- Herbert Burkert, Privacy-Enhancing Technologies: Typology, Critique, Vision, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 125,142 (Philip E. Agre & Marc Rotenberg, eds. MIT Press 1997).

37- Privacy Enhancing Technologies - the Path to Anonymity, TNO/FEL (the Dutch national research centre) and the Information and Privacy Commission of Ontario, Canada, August 1995

٣٨- إبراهيم حسن الملا، مرجع سابق.

٣٩- وسائل الحد الأدنى لحماية الخصوصية على الخط، http://www.cdt.org/privacy/guide/start/privacy.html

٤٠- يونس عرب، الخصوصية وحماية البيانات، عمان ، الأردن، ٢٠٠٢.

٤١- عبد المجيد ميلاد، نشر الطمأنينة و بناء الثقة في العصر الرقمي: إستراتيجية أمن المعلومات، جريدة الصباح، ٣/١٦/ ٢٠٠٦.

٤٢- أمان الخالد، بناء إستراتيجية لأمن المعلومات وليس مجرد شراء أدوات الحماية، جريدة الرياض اليومية، العدد ١٤٦٤٧، ٣١ يوليو٢٠٠٨م.