# الفصل التاسع

# المعلومات والخصوصية

## مقدمة

يقصد بالخصوصية من الناحية اللغوية، حالة الخصوص، أي خص فلان بالشيء، فهو يخصه خصا (بالفتح) أو خصوصا (بالضم)، وخصوصية ( بالضم على ما يشبع وبالفتح، والفتح أفصح). واختصه أي أفرده به دون غيره، فنقول اختص فلان بالأمر وتخصص له إذا انفرد به.

يرجع استخدام اصطلاح الخصوصية في اللغة الانجليزية إلى القرن الخامس عشر، ليدل على الحالة أو الوضع الذي يكون الفرد فيه كحال السحاب من المجموع فيتوارى عنهم وينأى بنفسه عن أي اهتمام من قبلهم.

يمكن القول إن الخصوصية في نشأتها جاءت إنجليزية الجذور، فتطور مفهومها في بريطانيا خلافا لهذه النشأة المبكرة وبقى حبيس المفهوم المادي للخصوصية، في حين هي أمريكية التطوير في النطاق الفقهي والدستوري، وهي فرنسية الاعتراف كحق عام، فقها وقضاء وتشريعا، تجاوز المفاهيم المادية بحماية المعنويات وبالحماية من كافة مظاهر التدخل.

أما في فرنسا فإن اللغة الفرنسية تنطوي على مرادفات لتعبير الحياة الخاصة . ( Lavie Priuee)

وتبعا لذلك فإن النظام القانوني الفرنسي، ينطوي على اصطلاحات عديدة للدلالة على الخصوصية إضافة لاصطلاح الحياة الخاصة، والحق في السرية

desecnet، والحق في الخلوة، والحق في الألفة dintinite الذي جرى استخدامه تشريعيا في ذات نص المادة (٩) من قانون ١٩٧٠ المعدل للقانون المدني الفرنسي، التي كرست للاعتراف بمبدأ حماية الحياة الخاصة.

**تعريف الخصوصية** :-

بالرغم من الاهتمام الموجه إلى الخصوصية وبشكل خاص في الآونة الأخيرة فإنه لم يتحقق سوى القليل من الاتفاق حول ما تعنيه الخصوصية حيث وجدت هناك عدة تعريفات للخصوصية.

فقد عرفها ( لويس هنكين ) بأنها " الاستقلال الذاتي أو الحرية المعنوية للفرد في ان ينشغل بأفكاره وأعماله أو قراراته الخاصة.

ووفقا لما أورده (فريد هـ. كيث) عرف مصطلح الخصوصية "بأنه السرية، وأنه يعني حق الأشخاص والمؤسسات في التحكم في جمع وتخزين وإصدار أية معلومات عنهم أو تخصهم. ومن ثم تكون لهم حرية منعها عن أي شخص لا يحق له تداولها، أي تحكم الفرد بالمعلومات الخاصة بذاته ".

كما تعني حرص الفرد على الاحتفاظ بجانب من حياته وأفكاره وميوله وأنشطته في مجال الحرمات الشخصية لنفسه أو لمن يختارهم من أعضاء عائلته وأصدقائه، وعدم الإفضاء غير المصرح به.

و هو حق الفرد في الاحتفاظ بمعلومات معينة عن نفسه، دون إفشاء أو كشف إلا بموافقته وحمايتها من الإتاحة غير المصرح بها.

و هي " عبارة عن السيطرة على المعلومات الشخصية عن أحد الأشخاص. وهذا الرأي متفق عليه من خلال القضاة والمحامين والفلاسفة".

عرفها ( باوند روسكو) (P. Rosco) و(بول فرونيد) (P. Fraind) بأنها" تعبير عن شخصية المرء أو صفاته الشخصية، ويركز على حق الفرد في تحديد جوهره ككائن بشري ".

و يعرفها (هناكين لويس) (H.Lewes) بأنها " الاستقلال الذاتي أو الحرية المعنوية لفرد في أن ينشغل بأفكاره أو أعماله أو قراراته الخاصة ".

أما ( ألان ويستن ) ( A. Weston)، ( تشارلز فرايد) (C. Fraidr) فيعرفان الخصوصية على أنها " قدرة المواطنين على تنظيم المعلومات عن أنفسهم، ومن ثم التحكم في علاقاتهم مع غيرهم من البشر ". أو هي مفهوم يتعلق بالعزلة والسرية والاستقلال الذاتي ".

## عناصر الخصوصية :-

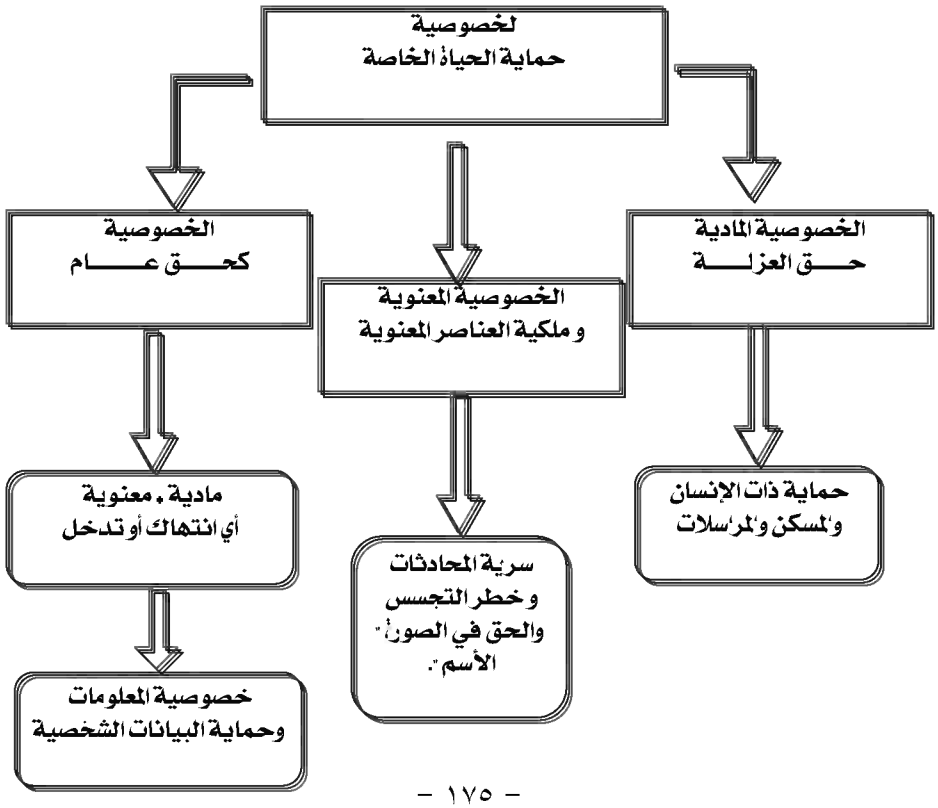
الخصوصية " هي الحق في حماية الشخصية ومنع الاعتداء عليها واستغلال الأفراد وكرامتهم

و سلامتهم. والخصوصية لها ثلاث عناصر.

١- السرية.

٢- العزلة.

٣- التخفي والتستر.



جدول يبين خصوصية حماية البيانات في العصر الرقمي

لقد شهدت نهاية الستينات والسبعينات القرن الماضي انطلاق الدراسات حول مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية وتحديدا التدخل المادي ومسائل الرقابة، ويعزى الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلفين أمريكيين هامين في هذا الحقل، الأول كتاب الخصوصية والحرية Freedom and Privacy لمؤلفه ( ويستن ) – Alan Westin عام ١٩٦٧. والثاني كتاب الاعتداء على الخصوصية Assault on Privacy The لمؤلفه ( مليز ) (Miller). وكلاهما قدما مفهوما وتعريفا لخصوصية المعلومات.

فوفقا لـ ( ويستن )، فإن خصوصية المعلومات تعني " حق الأفراد في تحديد متى وكيف

و إلى أي مدى تصل المعلومات عنهم للآخرين "، في حين أن تعريف مليز أكثر عمقا مع أن ويستن يعتبر منظر الحق في خصوصية المعلومات – إذ عرف خصوصية المعلومات بأنها

" قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم ".

ويؤصل (وستن) فكرة حماية الخصوصية باتجاهه في الأساس إلى اعتبار الخصوصية قلب الحرية فهو يعرف الحياة الخاصة بأنها : (الانسحاب الاختياري للفرد من المجتمع عموما ، جسمانيا أو نفسيا، سواء أراد أن يعيش في عزلة، أوفي مجموعة صغيرة متألقة، أو أن يعيش في حالة تستر أو تحفظ عندما يكون بين مجموعات كبيرة ) ويحدد( ويستن ) الأحوال التي يمكن ان يوجد فيها الفرد في حالة خصوصية، طبقا لهذا التعريف، فيما يلي :

- العزلة Solitude، وفيها ينفصل الفرد عن الجماعة ويتحرر من مراقبة الآخرين له، وهذه الوحدة هي أعلى وأكمل حالات الخصوصية التي يحققها أي فرد من الأفراد.
- السرية Intimacy، وفيها يتصرف الفرد كجزء من وحدة صغيرة لها الحق في

نوع من العزلة المشتركة، مثل علاقة الزوج بزوجته، أو بعائلته، أو بمجموعة من أصدقائه... الخ.

■ التسترAnonymity، وفيها قد يوجد الشخص في مكان عام أو يقوم بعمل عام، ولكنه يرغب في التحرر والتخلص من المراقبة ويريد أن لا يتعرف عليه الآخرون، ويتحقق له ذلك بالفعل، حيث يذوب في خضم المجتمع الذي يوجد فيه ولا يتعرف عليه احد، وسنجد هذا العنصر بالذات من أهم عناصر استخدام شبكات المعلومات حين يتوقع المستخدم قدرا من التخفي لا يرغب ان يكون محل كشف من الآخرين.

■ التحفظ Reserve، وفيها يرغب الفرد في تحديد علاقاته مع الآخرين، ويدرك الآخرون ذلك بكل لباقة وحسن تصرف.

فإذا تجاوزنا فكرة تحديد المعنى وتأصيلها، نجد أن كتاب قواعد الحياة الخاصة والرقابة العامة لمؤلفه ( رول ) J. Rule والمنشور في العام ١٩٧٣ قد استعرض على نحو شامل ومعمق مسائل جمع واستخدام البيانات الشخصية كوسيلة للسيطرة الاجتماعية.

كما شهد عام ١٩٩٤ إعداد دراسات واسعة بشأن المسائل المتصلة بالخصوصية وحقوق الإنسان في ضوء التطورات الحديثة، مثلا دراسة ( ميشيل) Michaelبعنوان ( الخصوصية وحقوق الإنسان. تحت إشراف اليونسكو، حيث قام المؤلف بتقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالميا.

## مفاهيم الخصوصية ( أنواعها ) :

يمكن تقسيم الخصوصية إلى عدد من المفاهيم المنفصلة لكنها ترتبط معا في الوقت ذاته :-

١- خصوصية المعلومات :

وهي التي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية.

٢- الخصوصية الجسدية أو المادية :

و هي التي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات تمس النواحي المادية لأجسادهم كفحص الجينات وفحص المخدرات.

٣- خصوصية الاتصالات :

وهي التي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الالكتروني وغيرها من وسائل الاتصالات.

٤- الخصوصية الإقليمية " نسبة إلى الإقليم المكاني ":

و هي التي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة والتوثيق من بطاقات الهوية.

هناك ثلاثة عناصر تشكل الخصوصية وهي :

- القيود على تجميع المعلومات وأسلوب عمل النظام.
- تحديد حقوق الأفراد في الوصول للنظام.
- المسؤولية الإدارية عن سجلات النظام.

**الخصوصية والسرية** :

إن الحق في الخصوصية، أو كما يعرف في النظام اللاتيني بالحق في الحياة الخاصة، ويعرف بحق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجذور من الوجهة التاريخية، ففي الكتب السماوية ثمة العديد الإشارات للخصوصية تنطوي على اعتراف بحماية الشخص من أن يكون مراقبا، وثمة حماية للخصوصية في الشرائع اليونانية والصينية القديمة. وقد جاء القرآن الكريم صريحا في حماية السرية وفي منع أنشطة التجسس وكذلك في حماية المساكن من الدخول دون أذن.

تمثل السرية القيود على استخدام المعلومات التي تم جمعها من الأفراد، وقد لا يحب نشرها خارج المنظمة، يمكن تصنيف السرية إلى عدة تصنيفات :-

١- سري : وهي الوثائق والمعلومات غير القابلة للنشر العام لخصوصيتها

الموضوعية أو الزمنية، ويمكن تداولها في نطاق القائمين عليها أو المخاطبين بها.

٢- سري شخصي : وهي نفس الوثائق والمعلومات السابقة ولكن ينحصر نطاق تداولها في أشخاص محددين بالاسم يتم حصرهم وإثباتهم في أصل الوثيقة، وفي هذه الحالة يتحدد نطاق المسؤولية في هؤلاء الأفراد على وجه التحديد.

٣- سري جدا : وهي المعلومات التي تتضمنها الوثائق التي تحدد الخطط الحالية والمواقف الجارية والبيانات الهامة.

٤- سري للغاية :وهي تلك الوثائق التي تضمن معلومات عن النوايا والخطط والأهداف المستقبلية ذات المضمون الاستراتيجي، التي يشكل اختراقها تهديدا خطيرا، من الواجب أن يكون تداول ذلك النوع من الوثائق في أضيق نطاق شخصي وزماني، كما يجب أن يكون أطراف هذا التداول على أعلى مستوى من المسؤولية والثقة.

**قيم الخصوصية** :

١- الاستقلال الذاتي: لتطبيق الخصوصية بالنسبة للأفراد والمؤسسات فلابد من درجة معينة من الاستقلال الذاتي الشخصي أو التنظيمي. ويتمثل الاستقلال الشخصي بالنسبة للفرد في ألا تكون أسراره الجوهرية مكشوفة لأي شخص آخر، حيث يوفر الاستقلال الشخصي مساحة لتنمية وتأمل الأفكار والآراء قبل أن تكون علنية، وبالتالي لا يكون هناك خوف من السخرية أو العقاب عند إعلانها.

٢- التحرر من الأدوار العامة: تعتبر الخصوصية ضرورية للأفراد لأنها تتيح لهم الفرصة ليكونوا بعيدين عن المراقبة العامة وليعبروا عما بداخلهم دون الخوف من رد الفعل. وبالنسبة للمؤسسات فهي تحتاج لأن تكون بعيدة عن المراقبة العامة لتسهيل الاتصال والتجريب والمخاطرة الفردية بصورة واضحة وهادئة داخل نطاق التنظيم والإدارة.

٣- التقدير الذاتي وصنع القرار: توفر الخصوصية فرصة لتقدير الذات حيث يحتاج الأفراد أو المؤسسات إلى المكان والوقت الذي يستطيعون فيه تدبر

وتقييم فيض المعلومات التي يتلقونها حتى يستطيعوا التصرف بصورة متسقة وملائمة بقدر الإمكان، واتخاذ القارات المناسبة.

٤- الاتصال المحدود والمصون : أي لا يكون الفرد صريحا تماما في اتصالاته مع الآخرين ويقول كل ما يعرفه، ولكن بإمكانه أن يتصل مع الآخرين ومشاركتهم في المعلومات التي قد تكون ذات قيمة لهم. وكذلك المؤسسات في حاجة إلى اتصالات محدودة.

## مبادئ خصوص المعلومات :-

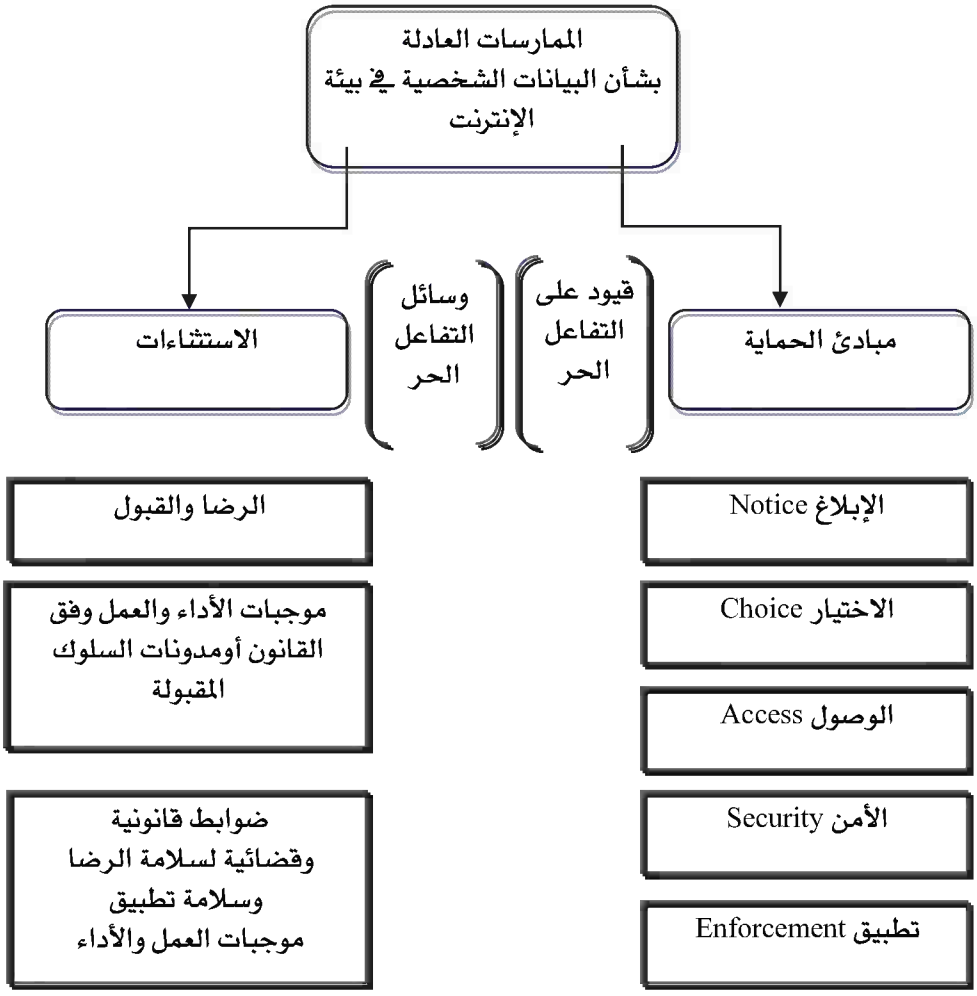
ثمة خمسة مبادئ أساسية تحكم ما يمكن تسميته بالممارسات العادلة والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية في بالبيئة الرقمية، هذه المبادئ هي:-

- الإبلاغ / الإخطار Notice : 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 وإلى أي مدى تجمع هذه البيانات وتستخدم ؟.
- الاختيار Choice : ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بشأن استخدام بياناته فيما يتجاوز غرض جمعها الابتدائي.
- الوصول للبيانات Access : ويوجب هذا المبدأ قدرة المستخدمين للوصول إلى بياناتهم والتثبت من صحتها وتحديثها.
- الأمن Security : ويتعلق هذا المبدأ بمسئوليات جهات جمع البيانات ( المواقع ومزودي الخدمة ) بشأن معايير الأمن المتعين تطبيقها لضمان سرية البيانات وسلامة الاستخدام وحظر الوصول غير المصرح به لهذه البيانات، وتتضمن من ضمن وسائل كلمات السر والتشفير وغيرها من وسائل امن المعلومات.
- تطبيق القانون Enforcement : ويتعلق هذا المبدأ بالآليات المناسبة المتعين اعتمادها لفرض الجزاءات على الجهات غير المتوافقة مع المبادئ المتقدمة وما يتصل بها من الممارسات النزيهة بشأن جمع البيانات الشخصية في البيئة

الرقمية.

شكل "١"

مبادئ الممارسات العادلة في حقل جمع البيانات الشخصية في البيئة الرقمية / الانترنت




## مبادئ حماية الخصوصية :

١- أولوية المسئولية الفردية والعمل غير الحكومي :

ويقصد بها قدرة الأفراد على تحقيق خصوصيتهم المعلومات،الأمر الذي يمثل أهم حماية لخصوصية المعلومات، وهذا يتطلب بالتأكيد وعيا بدلالات خصوصية الأنشطة لفردية خاصة على ( الانترنت ) حيث يجب على الأفراد أن ينمو لديهم الوعي بالخصوصية ويكونوا على دراية بأساليب العمل الخفية مع الحاسب الآلي ومكوناته، إلا أنهم وفي إطار تعاملهم مع المجتمع المتمثل في مؤسساته وقطاعاته المختلفة لا يستطيعون أن يضمنوا خصوصيتهم في المعلومات التي يقدمونها إلي هذه المؤسسات حيث يمكن أن تستعمل في غير الأغراض التي أعطيت من أجلها، وبذلك تكون المسئولية الفردية غير كافية في تحقيق الخصوصية.

٢- دور القانون الوطني :

قد يحتاج المواطنون إلي اللجوء للحماية القانونية عندما تتعرض خصوصيتهم للمعلومات للانتهاك. لذلك فلابد من وجود قانون يوفر هذه الحماية لمن يحتاجها.

ويعد مضمون قوانين الخصوصية موضع خلاف كبير بين الدول، ولكي تقدم هذه القوانين الحماية اللازمة للخصوصية بأن تخدم مصالح مقدمي ومستخدمي المعلومات، فينبغي أن تكون واضحة ودقيقة، ويمكن تحقيق ذلك بقانون واحد شامل للخصوصية تكمله عند الضرورة إجراءات قانونية خاصة.

٣- دور الحكومة :

تستطيع الحكومات أن تلعب أدوارا عديدة في حماية خصوصية المعلومات بصياغة المبادئ الأساسية وسن وتنفيذ القوانين، وإدارة نظم حماية البيانات.

و قد قام الاتحاد الأوربي بتوجيه ينص على وجود سلطات رقابية تشمل مسئولياتها مراقبة تنفيذ قوانين حماية البيانات، وتنفيذ قوانين الخصوصية والعمل كمفوض عن الأفراد الذين يرغبون في الوصول إلي السجلات الخاصة بهم أو الذين يرون أنه قد جرى انتهاك حقوقهم في الخصوصية.

٤- دور المعايير متعددة الجنسيات :

بما أن المعلومات أصبحت اليوم عالمية وتتخطى التكنولوجيات التي تحملها الحدود الوطنية. وفي وجود الشركات متعددة الجنسيات كشبكات الأعمال المصرفية مثل "شيبس وسويفت " وشبكات الخدمات الائتمانية مثل " ماستركارد " وشبكات الأوراق المالية وغيرها التي تتقاسم البيانات فيما بينها في جميع أنحاء

العالم.

**الإطار العام لتشريعات الخصوصية المعلوماتية :**

لقد أصبح الحق في الخصوصية واحدا من أهم حقوق الإنسان في العصر الحديث، وجرى الاعتراف بالخصوصية ضمن ثقافات ونظم غالبية الدول فجرى حمايتها في الإعلان العالمي لحقوق الإنسان وفي العهد الدولي للحقوق المدنية والسياسية.

و أن قوانين الخصوصية تنطوي على ثلاث طوائف رئيسية من القواعد هي :

- نطاق الاعتراف بالحق وقواعد كفالته وحمايته : وهو نطاق اعتراف الدولة به وكفالته

والالتزامات المقررة على الجهات العامة والخاصة في حق حماية البيانات الشخصية واحترام الخصوصية فيما تمارس من أنشطة جمع ومعالجة البيانات الشخصية باستخدام التكنولوجيا.

- القواعد التنظيمية والإجرائية والمعايير : وهي القواعد المتعلقة بآليات جمع البيانات ومعالجتها ونقلها وتحدد المعايير التي يتعين على جهات التكنولوجيا والاتصالات التقيد بها إلى جانب بحثها في جهات رقابة حماية الخصوصية.
- القواعد الموضوعية للحماية المدنية والجنائية : وتشمل نصوص التجريم مع تحديد للأفعال المجرمة وعقوباتها، إضافة لبيان نطاق المسؤولية المدنية، وبيان الجهات محل المساءلة وغير ذلك من القواعد الموضوعية المتعلقة بالحماية القانونية للبيانات الشخصية في كافة مراحل التعامل التكنولوجي معها.

خصائص ومحتوى تشريعات حماية الخصوصية

| مسماها الشائع | قوانين الخصوصية أو قوانين حماية المعطيات |
|---|---|
| ❶ وصفها العام | تشريعات حماية الحياة الخاصة من مخاطر المعالجة الإلكترونية للبيانات الشخصية. |

| مسماها الشائع | قوانين الخصوصية أو قوانين حماية المعطيات |
| --- | --- |
| ❷ مبرر وجودها | هذه التشريعات جاءت كردة فعل للتحديات التي واجهتها الحياة الخاصة بسبب مخاطر المعالجة الآلية للبيانات الشخصية وازدياد أنشطة جمع وتخزين وتبادل ونقل البيانات بالتكنولوجيات الحديثة. |
| ❸ هدفها ونطاقها | سنت هذه القوانين لحماية حق المواطنين في الخصوصية وحماية بياناتهم الخاصة وأسرهم ضمن قواعد إدارية ومدنية وجزائية |
| ❹الحقبة الزمنية لانطلاقها وترتيبها بين موجات تشريعات التكنولوجيا | في عام ١٩٦٨ وعلى اثر عقد مؤتمر الأمم المتحدة (طهران) لحقوق الإنسان ومناقشة موضوع مخاطر تكنولوجيا المعلومات على الحق في الخصوصية ظهرت التشريعات كأول موجة تشريعية وقد انطلقت خلال السبعينات والثمانينات وخضعت لتعديلات متتالية خلال الثمانينات والتسعينات . |
| ❺الفرع القانوني ذو العلاقة | حقوق الإنسان (تحديدا الحق في الحياة الخاصة) القانون الجنائي (المسؤولية الجزائية عن الإخلال بواجبات المعالجة وعن إفشاء البيانات ) القانون الإداري (أنظمة التنظيم الإداري، وقواعد نقل تبادل المعلومات بين الهيئات الحكومية ). |
| ❻محلها ذو العلاقة بالتكنولوجيا | البيانات الشخصية المخزنة والمعالجة والمتبادلة بواسطة الحاسوب وشبكات نقل المعلومات بما فيها وفي مقدمتها الإنترنت. |

| مسماها الشائع | قوانين الخصوصية أو قوانين حماية المعطيات |
| --- | --- |
| ❻محتواها بوجه عام | القواعد القانونية المنظمة لمعالجة البيانات وتخزينها في مراصد المعلومات وتبادلها وتشمل القواعد التي تحظر جمع المعلومات دون سند قانوني وتوجب للغرض المعلن واستخدامها في هذا الغرض وحده، وتتيح الحق في تصحيحها وتعديلها من أصحابها، ولا تجيز إفشائها وتقرر عقوبات على القائمين بالمعالجة والتحكم في هذه البيانات عند الإخلال بواجباتهم وتقييم المسؤولية على التوصل إليها من الأشخاص الخارجين عن المؤسسة المعنية بالجمع والمعالجة والمسؤولية عن إفشائها أو الابتزاز بوساطتها. |

إن الدول المستخدمة التي قطعت شوطا كبيرا في استخدام الحواسيب ومراصد المعلومات فسنت تشريعات للمحافظة على هذه الخصوصية. فقد صدر في الولايات المتحدة الأمريكية عام ١٩٧٤ م قانون حماية الخصوصية المعروف باسم Privacy Actالذي قامت بإعداده لجنة متخصصة وحددت فيه عدة مبادئ لحماية الخصوصية منها :

١) لا يجوز القيام بإعداد شبكات سرية للمعلومات تحتوي على بيانات الأفراد.

٢) من حق الفرد أن يعلم ويعي محتويات أي سجل يحتوي بياناته الشخصية وأين، وكيف يستخدم.

٣) كما أن من حقه أن يمنع استخدام بياناته الشخصية في غير الأغراض التي جمعت من أجلها.

٤) من حقه أن يصحح البيانات أو يعدلها في حالة وقوع خطأ من قبل الآخرين عند تسجيلها أو إعدادها.

٥) و أخيرا فإن من يستخدم البيانات الشخصية يكون مسئولا عن تصحيحها

وأن يعمل على منع استخدامها استخداما غير صحيح.

وصدر أيضا قانون آخر عن خصوصية الاتصالات الإلكترونية عام ١٩٨٦ م والمعروف باسم (Electronic communication Privacy) لحماية البيانات المتداولة عبر شبكات الحاسوب وحدد القانون عقوبة من ينتهك أمن هذه البيانات بعقوبة تصل إلى (١٠) سنوات من السجن وغرامة تصل إلى مائة ألف دولار ويسري ذلك على الأفراد والمؤسسات.

## أثر تكنولوجيا المعلومات على الحياة الخاصة :

لقد أضافت التكنولوجيا الجديدة أبعادا جديدة للخصوصية تتعلق باختزان واسترجاع المعلومات عن الناس بوساطة الحاسوب، وإمكانية الوصول لهذه المعلومات عن طريق شبكات الاتصال. ولعل التطورات المعاصرة في مجال تكنولوجيا المعلومات والخاصة ببروتوكول الاتصال وبوابات شبكات الاتصال (Network gateways) سيؤدي إلى عالمية الوصول إلى جميع الشبكات ومراصد المعلومات الأساسية في العالم.

و كما يذكر ( م. والكر، د. لارج، د. باليستر). P. Lange, D. , walker.M Pallisters فلا أحد يعلم ما البيانات والمعلومات الشخصية المرصودة في سجلات الشرطة أو المخابرات في أي بلد. وعلى الرغم من التأكيدات الرسمية بالاستخدام العادل (Fair Use) لهذه المعلومات، فإن التشريعات في هذه البلدان نفسها غير كافية لضمان سرية هذه المعلومات واستخدامها فقط من قبل السلطات الرسمية وحدها استخداما عادلا.. ولا أحد يعرف طبيعة هذه المعلومات التي تجمع بصفة مستمرة لاستخدامها في حالة تواجد صاحبها ولو بالمصادفة في مكان جريمة أو مكان محظور. كما أن أحدا لا يعلم على وجه الدقة إذا كانت هناك جهات أخرى لها حق الوصول إلى هذه المعلومات الشخصية أم لا.

## مخاطر الخصوصية في بيئة الإنترنت :

فالأفراد عندما يستخدمون مواقع الإنترنت فأنهم يتوقعون قدرا من الخفية في نشاطهم أكثر مما يتوقعون في العالم المادي الواقعي، ففي الأخير يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين، وما لم يكشف الشخص عن بيانات تخصه،

فانه يعتقد إن أحدا لن يعرف من هو أو ماذا يفعل، لكن الإنترنت عبر نظم الخوادم ونظم إدارة الشبكات تصنع قدرا كبيرا من المعلومات عند كل وقفة في فضاء الشبكة.

وهذه البيانات قد يتم اصطيادها ومعرفتها عن موظفي منشاة – مثلا – من قبل صاحب العمل عند استخدامه للشبكة أو لاشتراكاتهم المربوطة عليها، وقد تجمع من قبل المواقع المزارة نفسها وكما قلنا فان جمع شتات معلومات وسلوكيات معينة قد يقدم أوضح صورة عن شخص لم يرد كشف أي من تفاصيل ما تضمنته.

يشكل أمن وسرية المعلومات الشخصية بالذات مشكلة كبرى أمام ثورة الاتصالات الجارفة وأمام شبكة الإنترنت مما يتطلب وجود أجهزة خاصة يمكنها منها فقط استرجاع أو الإطلاع على الملفات السرية التي لا يسمح بالإطلاع عليها إلا من قبل الأشخاص المرخص لهم بذلك حيث يمنحون أرقاما سرية خاصة لهم باسترجاع مثل هذه الملفات، إضافة إلى ترميز الملفات ذاتها.

إن أمن وسرية المعلومات رهن بمدى الحفاظ على عدد من إجراءات الوقاية ومن أهمها الحفاظ على سرية الكلمات السرية. وتعتمد درجة حماية المعلومات على درجة السرية المطلوبة.

**مستويات سرية المعلومات** :-

ومن الممكن حصر مستويات سرية المعلومات كما تراها (هنريت أفرام) H.AVRAM في أربعة أمور إدارية وقانونية مثيرة للاهتمام في نقل المعلومات دوليا وهي:

أولا : المستوى الفردي ( الشخصي ) : وهذا يتعلق بحقوق الأفراد الشخصية بسرية المعلومات المحفوظة في بلد ما وترسل إلى بلد آخر حيث القانون أقل صرامة.

ثانيا : مستوى البيانات : قد تتعرض المعلومات لمخاطر إضافية للاستعمال غير المشروع أو التلف المادي أثناء عملية التراسل عبر الشبكات من بلد إلى آخر.

ثالثا : المستوى الوطني : تتعرض البيانات المنتجة في بلد ما يفتقر إلى الإمكانات الفنية لتعالج في بلد آخر لإحدى الاحتمالات التالية :

١- قد لا تتوافر هذه البيانات للبلد الأصلي المنتج لها.

٢- تسرب المعلومات الحساسة أو السرية إلى خارج البلد المنتج لها بواسطة الطريق الثاني.

٣- افتقار البلد المنتجة للسيطرة على التحكم في البيانات، وعليه تكون عالة إلى حد ما على بلد آخر.

رابعا : مستوى المهارات والخبرات : إن معالجة البيانات خارج بلد المنشأ يمكن أن يؤدي إلى هجرة ذوي المهارات في الموضوع الأمر الذي يؤثر على هذه الدول اقتصاديا.

تمكن تكنولوجيا المعلومات الجديدة خزن واسترجاع وتحليل كميات هائلة من البيانات التي تجمعها من قبل المؤسسات والدوائر والوكالات الحكومية والشركات الخاصة بفضل الحاسوب ويكمن مقارنة المعلومات المخزنة في ملف بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبيا " وهذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية ".

## مخاطر التكنولوجيا الحديثة علي الخصوص :-

وتتزايد مخاطر التكنولوجيا الحديثة على حماية الخصوصية حيث إن استخدام التكنولوجيا العالية في جمع ومعالجة البيانات الشخصية من قبل الدولة أو القطاع الخاص، قد عمق التناقضات الحادة التي برزت منذ القدم بين حق الأفراد في الحياة وموجبات الاطلاع على شئون الأفراد وتتمثل هذه التناقضات بمعالم رئيسية هي :

١) التناقض بين حق الحياة الخاصة وحق الدولة في الإطلاع على شئون الأفراد وليس المراد بهذا الإطلاع على معلومات معينة عن الأفراد لتنظيم الحياة الاجتماعية على نحو أفضل بل استخدام الدولة للمعلومات لأغراض تتناقض مع صونها واحترامها.

٢) التناقض بين حق الفرد في الاحتفاظ بسريته، ومصلحته في كشف حياته ليتمتع بثمار هذا الكشف.

٣) التناقض بين الحق في الحياة الخاصة، والحق في جمع المعلومات لغايات البحث العلمي أو حرية البحث العلمي.

٤) التناقض بين البحث في الحياة الخاصة وبين حرية الصحافة وتبادل المعلومات ( الحرية الإعلامية ).

ولقد برزت هذه التناقضات منذ القدم بين حق الفرد في حماية حياته الخاصة، وبين موجبات الإطلاع على شئون الأفراد بما فيها التي تقع ضمن نطاق حياته الخاصة.

إن استخدام الحواسيب في ميدان جمع المعلومات الشخصية المتصلة بالحياة الشخصية خلف آثار إيجابية عريضة لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية، وغيرها وهذا ما أوجد ما يعرف بمراصد المعلومات التي تعرف بأنها " تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسوب لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة "

ان حجم التخوف من الاستخدام غير المشروع للتكنولوجيا وتحديدا الحاسوب من شأنه تهديد الحق في الحياة الخاصة ويمكن إجمال المعالم الرئيسية لمخاطر الحواسيب ومراصد المعلومات على الحق الخاص بالأتي :

١) إن الكثير من المؤسسات الكبرى والشركات الحكومية والخاصة، تكون مرصد معلومات وهو ما يجعل فرص الوصول إلى البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل ويفتح مجالا أوسع لإساءة استخدامها.

٢) إن شيوع ( النقل الرقمي ) للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات " تبدي المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق غير مشروعة عن بعد على المعلومات".

٣) إن أكثر معالم خطر مراصد المعلومات ما يمكن أن تحويه من بيانات غير دقيقة أو معلومات غير كاملة لم يجر تعديلها بما يكفل إكمالها

وتصويبها.

٤) إن المعلومات الشخصية التي كانت فيما قبل منعزلة متفرقة، والتوصل إليها صعب متعذر، تصبح في مراصد المعلومات مجمعة متوافرة متكاملة سهلة المنال، متاحة أكثر من ذي قبل لاستخدامها في أغراض الرقابة على الأفراد.

٥) إن تكامل عناصر الحوسبة مع الاتصالات والوسائط أتاح وسائل رقابة متطورة سمعية ومرئية ومقروءة إضافة إلى برمجيات التتبع وجمع المعلومات آليا، كما أتاحت الإنترنت - بواسطة هذه العناصر جميعا - القدرة العالية على جمع المعلومات ومعالجتها بوساطة تكنولوجيا الذكاء الاصطناعي التي تتوافر لدى محركات البحث وبرمجيات تحليل الاستخدام والتصرفات على الشبكة، بحيث لا يستغرب أن الشخص الذي يتصل بأحد مواقع المعلومات البحثية بأن يجد أمامه المواقع التي كان يفكر في دخولها.

إن هذه المخاطر أثارت وتثير مسألة الأهمية الاستثنائية للحماية القانونية - إلى جانب الحماية التكنولوجية للبيانات الشخصية وبالتالي أن هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداء من عقد السبعينات تتضمن قواعد إدارية ومدنية وجنائية من أجل حماية الخصوصية وتوصف بأنها التشريعات السرية التي توجب 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 جمعها ومدة استخدامها، وإقرار مبدأ مسؤولية القائمين على وظائف مراصد المعلومات لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية.

**الخصوصية والإنترنت** :

يمكن مناقشة الخصوصية في الإنترنت في النقاط التالية :

١- الإنترنت نظام كوني له مشكلات مرتبطة بعضها البعض وهي تشترك في عنوان واحد وتستخدم الإنترنت للاتصال الإلكتروني ولاسترجاع البيانات والإتاحة بوساطة الحواسيب.

و يتم تنفيذ الاتصال الإلكتروني بوساطة البريد الإلكتروني وهو الذي يرسله شخص معين إلى شخص آخر.. والمرسلون والمستقبلون المباشرون أو المستقبلون الآخرون يمكنهم اختزان الرسائل في بريدهم الإلكتروني.

و يقوم العديد من المستخدمين للإنترنت بتزويد المستخدمين الآخرين بإمكانية الوصول إلى قواعد البيانات الخاصة بهم وعادة تكون المعلومات في قواعد المعلومات ذات طبيعة عامة وليس هناك إجراء عالمي متبع في هذا الخصوص فهناك بعض المؤسسات التي لا تطلب الكشف عن هوية المستفيد من قواعد معلوماتها ولكنها تحدد أو تمنع أي وصول خارجي إلى قوائم بريدها.

٢- المناقشات السابقة لقضية الخصوصية في الإنترنت :

لعل أول ذكر لقضية الخصوصية في مؤتمرات الإنترنت يعود إلى مؤتمر عام ١٩٩٢ في اليابان ،كما تمت مناقشات وتقديم أوراق بحوث أيضا في اجتماعات مؤتمر عام ١٩٩٣ في سان فرنسيسكو.. وكان الاتجاه العام في هذه المناقشات هو أنه لا ينبغي تجاهل قضايا الخصوصية في الإنترنت وخصوصا أن الاهتمام بالخصوصية يتخلف عادة في المناقشة عن التطورات التكنولوجية المتسارعة ولكن المشكلة هنا هي أن الإنترنت ذات طبيعة كونية ولكن المستفيدين منها يخضعون في هذا الخصوص لقوانين بلادهم ولما كان هناك أكثر من ١٥٠ دولة مشتركة في الإنترنت فإن صعوبة تطبيق قواعد تسري على الجميع يعد أمرا عسيرا ولعل بعض هذه الصعوبات تظهر في الاستعراض المختصر التالي لقوانين الخصوصية في بعض الدول ذات الاستخدام الواسع للإنترنت.

يلاحظ أن اجتماعات ومؤتمرات الإنترنت تخصص بعض مناقشاتها لقضية الخصوصية وهذا يعكس اهتمام المنظمين لهذه المؤتمرات بضرورة عدم تجاهل قضية الخصوصية حتى في الاجتماعات المخصصة أساسا لمناقشة التطورات الفنية مع اتساع نشاطات واستخدامات الإنترنت.

إن وضع نظام لحماية الخصوصية في بيئة الإنترنت عليه أن يراعي طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية في نطاق استخدام عمليات الإنترنت. فالإنترنت تخلق سلسلة من التحديات الجديدة في مواجهة خطة حماية المستهلك والطفولة وحماية الخصوصية. وتتمثل هذه التحديات بما يلي:

- الإنترنت تزيد كمية البيانات المجمعة والمنشأة : أي في نطاق مسائل الخصوصية تحديدا فإن المعلومات عن الأفراد وعاداتهم وهواياتهم ومسلكياتهم وآرائهم واتجاهاتهم في التسوق أمست متوافرة في ظل الإنترنت.
- الإنترنت أتاحت عولمة المعلومات والاتصالات : في بيئة تتدفق فيها المعلومات والاتصالات عبر الحدود دون أي اعتبار للجغرافيا والسيادة، والأفراد يعطون معلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوافر فيها مستويات الحماية القانونية للبيانات الشخصية.
- التحدي الناشئ عن فقدان المركزية وآليات السيطرة والتحكم : إن إقرار قانون وطني أو تطوير إستراتيجية وطنية ملائمة لحماية أحد حقوق الإنسان، قد يكون فاعلا، ويرجع ذلك لعنصر السيطرة والسيادة وتوفير الجهة القادرة على الرقابة ومنع الاعتداء أو استمراره التي تتيح أيضا التعويض وملاحقة المخالفين، ولكن كيف يكون الوضع في ظل الإنترنت التي يملكها كل شخص وغير مملوكة لأحد والتي لا تتوافر فيها سلطة مركزية ولا جهة سيادة توفر الحماية أو تتيح الفرصة للحماية القانونية عند حدوث الاعتداء.

## قضية الخصوصية مع البريد الإلكتروني وقواعد البيانات :

البريد الإلكتروني :

تبرز قضية وصول الموظفين إلى رسائل البريد والمعلومات المخزنة في صناديق البريد الإلكتروني نظرا لأن معظم المستخدمين للبريد الإلكتروني هم موظفون في المؤسسات الكبيرة والقضية لها جانبان على الأقل:-

- إن أولئك الذين يستخدمون البريد الإلكتروني في الاتصال لديهم توقع أن اتصالاتهم هذه تغلفها الخصوصية.
- إن استخدامهم البريد الإلكتروني يكون عادة أثناء ساعات العمل وإن الأجهزة نفسها المستخدمة في أجهزة صاحب العمل ومن هنا جاءت المناقشات مؤيدة ومعارضة لحق الخصوصية.

وهناك قضية أخرى للخصوصية تتعلق بالبريد الإلكتروني وهي قضية كلمة

المرور password ودرجة سريتها فإلى جانب الدراسات التي تشير إلى أن العديد من المستفيدين يستخدمون كلمات مرور ليست سرية على الإطلاق إلا أن التكنولوجيا الحالية تجعل معظم كلمات المرور متاحة للذين لديهم الخبرة والرغبة في التعرف عليها.

## قضايا البريد الإلكتروني وقواعد البيانات في إطار القانون الحالي:

يضع الإنتاج الفكري للمعلومات الخصوصية في دائرة الحقوق الإنسانية الأساسية وإذا كانت القوانين الحالية في معظم الدول لا تقدم إجابات شافية للأسئلة المطروحة فيرى البعض أن ذلك أمر طيب لأنه من خلاله تتمكن شبكة الإنترنت من العمل دون معوقات قانونية في مكان معين وفي الوقت نفسه.

هناك فرصة لوضع القيود أو التحفظات للحفاظ على الخصوصية المشروعة لجميع المستخدمين لشبكة الإنترنت ذلك لأن ثقافة الإنترنت كما يقال تتعدى الحدود الوطنية وأصبحت ثقافة كونية ومن الممكن أن تتضمن هذه الثقافة الكونية بعض القيم الإنسانية المتصلة بالخصوصية غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الحاسوب والإنترنت) واستخدام اصطلاح أمن المعلومات وكان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بوساطة وسائل الحوسبة والاتصال، إذ مع شيوع الوسائل التكنولوجية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات – وتحديدا الإنترنت – احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء بين أبحاث المعلومات المختلفة.

## الجهود الدولية والإقليمية والقطرية لحماية الخصوصية المعلوماتية:

إن العديد من المنظمات الدولية طورت أنشطة مختلفة تهدف إلى تنظيم حماية المعلومات الخاصة وتنظيم تدفق انتقال البيانات، وقد أنجز الجزء الأكبر من هذا الجهد في هذا الحقل من قبل هيئة الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي، مجموعة الدول السبع

و منظمة التجارة العالمية.

## التدابير التشريعية لحماية الخصوصية المعلوماتية:

هناك ثلاثة نماذج تشريعية لحماية الخصوصية المعلوماتية، وبالنسبة للدول توفر حماية فاعلة للخصوصية فإنها قد تستخدم نموذجا أو أكثر لضمان حماية الخصوصية وهي :-

١) القوانين الشاملة : في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام والخاص، مع وجود جهة لضمان التواؤم مع القوانين وتطبيقها.

٢) القوانين القطاعية المخصصة : وهي التي تتعلق بقطاع معين، إذ أن بعض الدول تجنبت سن تشريعات عامة لحماية الخصوصية وفضلت إصدار قوانين معينة تحكم قطاعات بعينها كالخصوصية المالية (المصرفية) أو الخصوصية المهنية كما في حقل المحاماة أو غيرها.

٣) التنظيم الذاتي : إن موضوع التنظيم الذاتي للتشريعات هو موقف بشأن موضوعات تكنولوجيا المعلومات عموما. ومنها حقول التجارة الإلكترونية ومعايير الخدمات التكنولوجية وحماية البيانات وأمن المعلومات وغيرها.

## أولا: هيئة الأمم متحدة:

عكفت هيئة الأمم المتحدة على النظر بجدية نحو الآثار المترتبة على استخدام تكنولوجيا المعلومات والاتصالات في حقوق الإنسان وضرورة احترام حياته الخاصة وحريته من خطر التعدي عليها، وعقدت لذلك مؤتمرها الأول في طهران سنة ١٩٦٨.حيث تبنت الجمعية العامة للأمم المتحدة في اجتماعها المنعقد بتاريخ ١٩ ديسمبر ١٩٦٨ توصية مؤتمر طهران الخاصة باستخدام تكنولوجيا المعلومات والاتصالات وأثرها على حقوق الإنسان ودارسة المشاكل المتعلقة بذلك وخاصة فيما يتعلق منها بما يؤثر على حقوق الأفراد، وحدود هذا الاستخدام في المجتمعات الديمقراطية.

وفي العام ١٩٩٠ تبنت الجمعية العامة أيضا المشروع التوجيهي المتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية وأصدرت دليل تنظيم لاستخدام المعالجة الإلية للبيانات الشخصية، والمعروف بدليل الأمم المتحدة بخصوص ملفات البيانات

الشخصية المؤتمتة لعام ١٩٩٠.

وقد قرر الدليل مبدأ عدم التمييز في المعاملة بإجراء حماية إضافية للبيانات الحساسة، كما أقر مبدأ حرية نقل وتدفق البيانات شريطة الحماية المماثلة الملائمة في الدولة المنقول إليها البيانات. وبذلك يتضمن ذات المبادئ المقررة لدي منظمة التعاون الاقتصادي والتنمية، ولدي مجلس أوربا. وهي مبادئ غير ملزمة، ومجرد توصيات للدول الأعضاء لتنظيمها واتخاذ التدابير التشريعية في هذا الحقل حيالها. كما صدر عن السكرتارية العامة للأمم المتحدة عام ١٩٩٧ قرار بشأن تطبيق الدليل على المستويات الوطنية والإقليمية ومستوي نظام الأمم المتحدة.

**ثانيا : منظمة التعاون الاقتصادي والتنمية :**

شهد العام ١٩٧٧ بداية الاهتمام بمسألة حماية الخصوصية وحماية معالجة واستخدام البيانات الشخصية ونقلها وتدفقها عبر الحدود من قبل المنظمة، ومع العام ١٩٧٨ بدأت بوضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات، وقد تم تبنيها والالتزام بها من قبل مجلس المنظمة بتاريخ ٢٣سبتمبر ١٩٨٠.

و يتضمن الدليل ثمانية مبادئ عرفت بمبادئ الخصوصية Privacy Principles وهي:

١- تقييد جمع البيانات الشخصية :-

تعين وفق هذا المبدأ فرض قيود على تجميع البيانات Collection – Limitation بأن تكون عملية جمع البيانات الشخصية محددة ومقيدة ويتعين أن يتم الحصول عليها بطريقة قانونية وشرعية ونزيهة Lauful and Fair Means بعيدا عن الإكراه والخداع، كذلك بمعرفة واطلاع الشخص المعني بالبيانات ( محل أو موضوع البيانات Data Subject ).

٢- نوعية البيانات:-

يتعين أن تكون البيانات الشخصية متعلقة Relevant بالغرض المحدد لاستخدامها وضرورية لهذا الغرض وصحيحة Accurate ومكتملة Complete ويجري تحديثها باستمرار .Kept Up –to-date

٣- تحديد الغرض (Purpose – Specification):-

إن الغرض من جمع البيانات الشخصية يتعين أن يكون محددا في وقت لا يزيد عن وقت جمع البيانات وأن يكون استخدام البيانات محددا في نطاق الغرض المعلن أو الأغراض المتوافقة معه وأن يبقى محددا في كل وقت يتم فيه تغيير الغرض.

٤- حدود أو قيود الاستخدام ( Use- Limitation):-

البيانات الشخصية يتعين أن لا يتم إفشاؤها ولا تكون متاحة للاستخدام لغير الأغراض المحددة للجمع والمعالجة باستثناء الحالات التي يتوافر فيها رضاء صاحب البيانات أو الحالات التي يقررها القانون.

٥- معايير الأمن أو الوقاية الأمنية ((Security Safeguards):-

يتعين حماية البيانات الشخصية بإجراءات ووسائل حماية مناسبة ضد أخطار الوصول أو الدخول غير المصرح به أو الإتلاف أو الاستخدام أو التعديل غير المصرح بهما أو الإفشاء في كافة مراحل الجمع والمعالجة والنقل.

٦- العلانية والانفتاح (Openness):-

يتعين وجود سياسة عامة تتمتع بالوضوح والانتفاع بشأن التطورات والممارسات واستراتيجيات البيانات الشخصية ويتعين أن يمتد الوضوح إلى وجود أنشطة معالجة البيانات الشخصية والأغراض الأساسية للاستخدام والتعريف بجهات المعالجة وأماكن تواجدها.

٧- مشاركة الأفراد / المشاركة الفردية Individual Participation

يتعين أن يحظى الفرد بحق الحصول – من جهة المعالجة أو الغير – على تأكيد فيما إذا كان هناك بيانات شخصية تعود له أم لا لدى هذه الجهة، والحق في التواصل مع هذه الجهة ومع البيانات الموجودة لديها في وقت معقول ولقاء مقابل معقول وبأسلوب ملائم وبشكل يتيح أخطاره بسبب منع ممارسته لأي من الحقوق المتقدمة مع حقه برفض عدم قبول ممارسته لحقوقه المشار إليها وأن ينكر البيانات المتعلقة به وإذا تبين صحة إنكاره فمن حقه ان تشطب هذه البيانات أو تعدل أو تكمل.

٨- المساءلة (Accountability ):-

يتعين أن تكون جهات المعالجة مسئولة عن التواؤم مع المبادئ المتقدمة.

## ثالثا :الاتحاد الأوربي :-

أقرت اتفاقية مجلس أوربا رقم (١٠٨) لسنة ١٩٨١ بشأن حماية الأفراد فيما يتصل بالمعالجة الآلية للبيانات الشخصية وأصبحت نافذة ببداية شهر أكتوبر ١٩٨٥.

و تتكون الاتفاقية من ثلاثة أجزاء رئيسية :-

١- المبادئ الأساسية.

٢- قواعد خاصة بشأن تدفق المعطيات خارج الحدود.

٣- آليات المساعدة المتبادلة والمشورة بين الدول الأطراف في الاتفاقية.

و في العام ١٩٩٢ أعدت منظمة الاتحاد الأوربي مسودة خاصة بحماية الأفراد (Commission of the European Communities 1992) كان الهدف منها تنسيق التشريعات في الدول الأوربية التي تتعلق بهذا الموضوع، وحث الدول التي لم تبدأ في سن هذه التشريعات للبدء في إعدادها.

إلى جانب تقديم مشاريع أدلة توجيهية متكاملة حول حماية البيانات كان حصيلتها الأمر التشريعي لعام ١٩٩٥ بشأن حماية الأفراد فيما يتصل بمعالجة البيانات الشخصية وحرية انتقالها، والذي نفذت أحكامه اعتبارا من أكتوبر ١٩٩٨. وقد ألزم الأمر التشريعي المشار إليه كافة الدول الأعضاء في الاتحاد وجوب تضمين أحكامه في تشريعاتها الوطنية بالخصوص.

و كتطور لاحق لهذا التشريع صدر الأمر التشريعي رقم (97/66/EC ) المتعلق بحماية معطيات الاتصالات عام ١٩٩٧ ويتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات. كما صدر في عام ٢٠٠٠ نموذج جديد لدليل تشريعي لمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية.

## ثانيا : على مستوى الدول :

١- السويد :

تعتبر السويد من بين أوائل الدول التي وضعت تشريعات لحماية حقوق الإنسان في معلوماته الشخصية، ففي عام ١٧٧٦ تم إقرار قانون حرية الصحافة الذي يعد أقدم قانون للوصول للمعلومات في العالم، وفي عام ١٩٧٣ م تم وضع أول قانون لتنظيم سجلات الحاسوب وحماية البيانات وبذلك تعتبر أول دولة في العالم تقود موجة التشريع في هذا الحقل.

وفي العام ١٩٧٤ أنشأت مجلسا لفحص بيانات نص قانون إنشائه على ضرورة موافق هذا المجلس على إدراج مجموعة البيانات الشخصية في ملفات الحاسوب. وللمجلس حق الإشراف على هذه المعلومات لضمان تنفيذ هذه القواعد وهو الذي يعمل على تحقيق التوازن العادل بين ما قد ينشأ من صدام بين صيانة خصوصية الفرد، وحاجة المجتمع للمعلومات.

٢- فرنسا :

وفي فرنسا صدر القانون الخاص بالصحافة عام ١٩٨١ وفيه تم إقرار حماية الفرد من الاعتداء على كرامته، ومنحه الحق لإقامة دعوى القذف، إلى جانب الحق في نشر رد على ما ورد في خصوصه.. وفي القانون الذي صدر عام ١٩٧٠ نصت مادته التاسعة على حق كل شخص أن تكون حياته الخاصة مصونة. وفي التعديلات اللاحقة لقانون العقوبات جرى إضافة المواد (٣٦٨- ٣٧٢) والتي جرمت التقاط وتسجيل الأحاديث الخاصة والتقاط الصور الخاصة. والحفاظ أو إفشاء أو استعمال السجلات ونشر المونتاج....الخ.

ووفقا للتجربة الفرنسية فهناك مجموعة قواعد لحماية الأفراد من سلطات الحواسيب وخطر المعلوماتية على ألا تنال حرية الحصول على المعلومات من أي شخص أيا كان نوع المعلومات أو أسلوب جمعها أو معالجتها أو الدعامة المثبتة عليها، وأهمها :

١- تكريس لجنة وطنية للمعلومات والحريات لوضع مواصفات قياسية للمعالجة والاسترجاع ومراقبة احترام ما تضعه من مواصفات في هذا الشأن، مع تخويلها الصلاحية في إبلاغ السلطات العامة بأي انتهاك يحدث

في هذا الصدد.

٢- إلزام كل من يطلب معلومات سرية أو يعالجها بأن يتخذ إزاء الأشخاص المعنية كل الاحتياجات الضرورية ليحفظ سرية المعلومات وأن يحول بوجه خاص دون تحريفها أو إتلافها أو توصيل أغراض غير مرخص لهم بمعرفتها أو الاطلاع عليها.

٣- منح الأفراد الحق في رفع أسمائهم من دليل الهاتف، فتدرج أرقام هواتفهم في قائمة حمراء، أو تخويلهم الحق في الاحتفاظ بأسمائهم في الدليل مع حظر استخدام أرقام هواتفهم من قبل الشركات التجارية التي تعرض بضائعها عليهم في قائمة برتقالية. وفي الأحوال تلزم الشركات التجارية بإخطار من هم على قوائمها بذلك.

٤- جريان العمل على عدم إمداد المتعاملين مع مراصد المعلومات القانونية الطابع بأسماء الخصوم في الأحكام القضائية التي تقدمها إليهم لتفادي شبهة المساس بالحياة الخاصة.

٥- إلزام القائمين على معالجة المعلوماتية للبيانات والمعلومات بإعلام المتعاملين معهم بالوفاء بكل ما ألقاه القانون على عاتقهم من التزامات تضمن حماية الحياة الخاصة لهم في مواجهة الحواسيب.

ويؤكد الأستاذ ( بول سيجارت ) Paul Sieghart على مبدأ حماية المعلومات الخاصة في الحواسيب وهو مبدأ الحد الأدنى من تداول المعلومات. فهذه المبادئ تهدف إلى حماية البرامج الخاصة التي توضع في الحاسوب. إن إتباع هذه القواعد عند تشغيل نظم الحواسيب يعني أن المعلومات المخزونة عن الأفراد والهيئات الأخرى تبقي في مأمن من التطاول عليها من استخدامها في غير الأغراض التي استخدمت من أجلها.

٣- بريطانيا :

لقد ظهر أول تشريع في بريطانيا عام ١٣٦١ يحضر استراق السمع والنظر بقصد الاطلاع على خصوصية الأفراد، كما صدر قانون آخر عام ١٩٦٧ يتعلق بتنظيم الخدمات بوساطة الحاسوب، حيث أوجب التزام موظفي نظم المعالجة بالحفاظ على

سرية المعلومات تحت طائلة المسؤولية عن إفشاء هذه البيانات. كما ظهر قانون حماية خصوصية البيانات عام ١٩٨٤، حيث وضع الأسس القانونية لحماية البيانات الشخصية في ملفات الحواسيب، ومنح المواطنين تأكيدات بأن هذه المعلومات سوف يتم حمايتها من إساءة الاستخدام.وقد اقره البرلمان البريطاني بمسمي قانون حماية البيانات رقم (٢٩) لسنة ١٩٩٨، أوجب فيه تطوير مفهوم الخصوصية كقانون حماية البيانات لعام ١٩٩٨،وقانون حرية الوصول للمعلومات لعام ١٩٩٨ أيضا. ونفذت أحكامه في الأول من مارس ٢٠٠٠. وهو تطوير وتحديث لقانون ١٩٨٤.و ثمة بعض الشكوك حول مدى تحقيق هذا القانون للأهداف التي وضع من أجلها، خاصة أن التكاليف التي يتحملها المواطن للحصول على المعلومات يحددها مالك المعلومات نفسه، وهو الذي يفرضها وقد تكون عالية.

وفي تطوير لاحق، صدر قانون حرية المعلومات Information freedom لعام ٢٠٠٠، نص على حقوق الأفراد في الوصول للمعلومات، وقرر إنشاء مفوض حرية المعلومات تم تعديله فيما بعد باسم مفوض المعلومات يباشر مهامه المقررة في كلا القانونين، إضافة إلى دوره الرقابي والتطبيقي أيضا المقرر لـه في نظام حماية خصوصية بيانات الاتصالات النافذ بتاريخ ١ مارس ٢٠٠٠.

٤- الولايات المتحدة الأمريكية :

منذ عام ١٩٩٦، جرى وضع قانون لحماية حرية الوصول للمعلومات Freedom of Information Act وقد تم تحريره في عام ١٩٧٠، فقانون حرية المعلومات الذي أصدره الكونجرس ١٩٧٣ والذي يهدف إلى حرية الناس في الوصول إلى البيانات الهامة والوعي الدائم بالأخبار والمعلومات الوطنية الهامة، مع ذلك فهو يؤدي إلى انتهاك خصوصية الأفراد وإمكانية إعاقة السرية CONFIDENTIAL Lity، وكما جاء في تقرير ( راند ) Rand Report عام ١٩٧٤ " يتطلب المجتمع الاقتصاد والكفاية ودرجة عالية من المنفعة من الوكالات العامة، وهذا الوضع يتعارض مع مطالب الفرد في السرية والخصوصية والقيود المفروضة على الاستخدام والبث والمشاركة في البيانات والتشريع الأكثر معنوية لحماية خصوصية الأفراد هو قانون الخصوصية الفيدرالي Federal Privacy Act لعام ١٩٧٤. يشترط هذا القانون أنه لا يمكن أن توجد ملفات شخصية سرية، ويجب أن يسمح للأفراد

بمعرفة ما هو مخزن في الملفات عنهم وكيف تستخدم البيانات، ويجب أن يتمكنوا من تصحيحها..ولا يمكن لهذه المنظمات أن تحصل على بيانات إلا لغرض محدد، ويجب أن تبرز حاجتها للحصول عليها.

والقانون الأكثر حداثة هو قانون حماية خصوصية الفيديو Video Privacy Protection Act لعام ١٩٩٨ م، الذي يمنع إفشاء سجلات استئجار أشرطة الفيديو للأفراد الذين يقومون بذلك إلا بقرار من المحكمة، ويريد مدعمو الخصوصية تطبيق نفس القواعد على الملفات الطبية، وملفات التأمين.

والخطوة الأخرى في هذا الاتجاه هي قانون حماية الخصوصية، واتفاق الحاسوب Computer Matching and Privacy Protection Act العربية ١٩٩٨ م، والذي يمنع الحكومة من مقارنة سجلات معينة في محاولة إيجاد اتفاق. وقد جرى تعديله لمرات عديدة، ويسمح القانون بالوصول إلى سجلات الحكومة الفدرالية من قبل من يطلب ذلك، باستثناء ملفات البيت الأبيض والمحاكم، ويرد على هذا الحق عدد من الاستثناءات، وقد اعترضت " جماعة قيادة حماية النظم " المؤسسة سنة ١٩٨٦ بشدة وبعنف على قصر إتاحة المعلومات والوصول إليها على المعلومات الحكومية بزعم تحقيق الأمن الوطني. وفي سبيل حماية ما سمى بالمعلومات الحساسة ولكن غير السرية اقترحت الجماعة مجموعة من القيود تفرض على تداول تلك المعلومات.

ومن ضمن أهم تعديلات هذا القانون، التعديل الذي تم بموجب قانون حرية المعلومات الإلكترونية لعام ١٩٩٦المعدل لقانون حرية المعلومات Electronic 1996 Freedom of Information Act Amendments of.. وقد أتاح هذا التعديل الوصول إلى الملفات الحكومية ذات الطبيعة الإلكترونية، أي المخزنة في نظم المعلومات بأشكال إلكترونية.

٥- سنغافورة :

في ظل توجه سنغافورة لتحقيق موضع لها في العصر الرقمي، جرى تشكيل المجلس الوطني الاستشاري للإنترنت National Internet Advisory Board وقد أطلق في سبتمبر ١٩٩٨ مدونة سلوك ( قواعد تنظيم ذاتي للقطاع الصناعي ) عرفت باسم (كود التجارة الإلكترونية لحماية المعلومات الشخصية واتصالات المستهلكين في بيئة تجارة الإنترنت "E-Commerce Code for the Protection of

Personal Information and Communications of Consumers of Internet Commerce" وقد أكدت مدونة السلوك هذه على احترام سرية البيانات الشخصية وحمايتها، كما تضمنت قيودا على جمع ومعالجة ونقل البيانات الشخصية.

٦- تشيلـــي :

تعتبر تشيلي أول دولة من دول أمريكا اللاتينية تضع تشريعا لحماية البيانات الشخصية. فقد أصدر المشرع بتاريخ ١٩٩٨/٨/٣٠ قانون حماية الحياة الخاصة رقم (١٩٦٢٨) لسنة ١٩٩٩ " Law for the Protection of Private Life" وأصبح نافذا بتاريخ ١٩٩٩/١٠/٢٨. ويتضمن القانون ٢٤ مادة تغطي معالجة واستخدام البيانات الشخصية في القطاعين العام والخاص وحق الأفراد في الوصول إلى بياناتهم وتصحيحها وحقهم في السيطرة عليها عبر الأوامر القضائية.

٧- المجـــر Hungary :

تقضي المادة (٥٩) من الدستور المجري ( لعام ١٩٤٩ وفق التعديل المقرر عامي ١٩٨٩ و١٩٩٨) بحق الأفراد في حماية بياناتهم الشخصية إضافة إلى إقرار هذه المادة حماية مظاهر الخصوصية المادية ( حرمة المسكن والمراسلات)، وسندا لهذا النص قررت المحكمة المجرية العليا Supreme Court في عام ١٩٩١ ان وضع قانون يتيح استخدام رقم تعريف واحد لأغراض متعددة ينطوي على اعتداء على حق الأفراد في الخصوصية.أما على صعيد القوانين، فان المجر من بين الدول التي وضعت قانونا واحدا يحكم حرية المعلومات وبنفس الوقت يحكم حماية البيانات الشخصية.. ويطبق القانون على السجلات الإلكترونية واليدوية، في القطاعين العام والخاص وعلى الأشخاص الطبيعيين فقط.

٨- الصيـــن China:-

تقضـي المادة ٤٠ من الدستور الصيني لعام ١٩٩٣ ( دستور ١٩٨٢ المعدل عام ١٩٩٣ ) بان حرية وخصوصية مراسلات الأفراد مكفولة بموجب القانون ولا يجوز المساس بخصوصية المراسلات إلا في حدود الأمن والسلامة العامة وفي إطار أغراض التحقيق الجنائي.

ان المادة (٧) من نظام حماية وإدارة معلومات الحاسوب وأمن الإنترنت

والشبكات لعام١٩٩٧ Computer Information Network and Internet Security Protection and Management Regulations تقرر حماية الحق في خصوصية الشبكات، وتحظر على أي جهة استخدام الإنترنت للمساس بخصوصية المستخدمين للشبكات.

٩- جنوب أفريقيا South Africa :-

يقرر القسم (١٤) من دستور جنوب أفريقيا لعام ١٩٩٦حق الأفراد في الخصوصية ويمنع العديد من مظاهر الاعتداء على الخصوصية بالمعني المادي (الشخص وممتلكاته). أما القسم ٣٢ فيقرر حق الأفراد في المعلومات والوصول إليها.

وفي فبراير ٢٠٠٠ صدر قانون الوصول إلى المعلومات The Access to Information Act رقم (٢) لسنة ٢٠٠٠، وتغطي أحكامه القطاعين العام والخاص، وتكفل وصول الكافة إلى البيانات والحق في تصحيحها، كما تفرض قيودا وقواعد بشأن كشف وإفشاء البيانات.

١٠-الوطن العربي :-

رغم مبادرات تكنولوجيا المعلومات واستراتيجيات تعميمها والتوجه نحو تطبيقاتها في الوطن العربي، ورغم خطط العمل الإدارية والتكنولوجية والقانونية، وما أنجز في حقل التجارة الإلكترونية من إقرار عدد من القوانين لعدد من الدول العربية كما في ( الأردن وتونس ودبي ) ووضع مشاريع في بقيتها لهذا الغرض كما في ( مصر والبحرين ولبنان )، إلا انه ليس ثمة قانون واحد عام لحماية البيانات الشخصية في الوطن العربي باستثناء تونس – جزئيا – حيث تضمن قانون المعاملات والتجارة الإلكترونية الموضوع فيها بعض النصوص الخاصة بحماية البيانات الشخصية المتعلقة بأنشطة التجارة الإلكترونية. كما انه ليس ثمة قانون واحد عام لحرية الوصول للمعلومات وما يسود ليس أكثر من نصوص متناثرة في بعض التشريعات كقوانين الإحصاءات والأحوال المدنية والوثائق والأسرار الحكومية وتشريعات المصارف وبعض تشريعات المهن التي تقرر الأسرار المهنية كقوانين تنظيم مهنة المحاماة أو التشريعات الصحية، وبعض قوانين الأراضي، وأنظمة إنشاء مراصد المعلومات – المحدودة في الوطن العربي – وبعض نصوص قوانين العقوبات.

وفي الجماهيرية قرر المشرع الليبي الحماية القانونية للحق في الحياة الخاصة وحمايتها من التدخل في شئونها. حيث نص صراحة على حق الإنسان في حرمة حياته الخاصة في القانون المدني الليبي المادة (٥٠)، وكذلك نصت المادة (٤٣٦) من قانون العقوبات على حرمة المسكن وجرائم الاعتداء على سرية المراسلات، وجرائم الاعتداء على حرية الأشخاص وانتهاك كرامتهم وسمعتهم...الخ.

كما أرست الوثيقة الخضراء الكبرى لحقوق الإنسان في عصر الجماهير مبدأ حرمة الحياة الخاصة حيث نصت في البند السابع على " ان أبناء المجتمع الجماهيري أحرار في تصرفاتهم الخاصة وعلاقتهم الشخصية، ولا يحق لأحد التدخل فيها، إلا إذا اشتكى أحد أطراف العلاقة، أو إذا كان التصرف، أو كانت العلاقة ضارة بالمجتمع أو مفسدة لها، أو منا فيه لقيمه ".

ووفقا للقانون رقم (٢٠) لسنة ١٩٩١ بشأن تعزيز الحرية، نصت المادة السادسة عشر على أن للحياة الخاصة حرمة، ويحضر التدخل فيها إلا إذا شكلت مساسا بالنظام والآداب العامة أو ضررا بالآخرين، أو إذا اشتكى أحد أطرافها.