

المحاضرة التاسعة

مبادئ حماية الخصوصية المعلوماتية

الحماية الدولية والإقليمية للحق في الخصوصية المعلوماتية (الحماية المعنوية)

• عناصر المحاضرة:

المحور الأول : حقوق الشخص الذي سجلت المعلومات الشخصية المتعلقة به:

أولاً: الحق في الإطلاع.

ثانياً: الحق في التصحيح.

ثالثاً: الحق في المحافظة علي خصوصية المعلومات.

رابعاً: الحق في الإشراف المستقل.

خامساً: الحق في الإخطار العام.

المحور الثاني : الحماية الدولية والإقليمية للحق في الخصوصية المعلوماتية (الحماية المعنوية):

أولاً: المنظمات الدولية ودورها في حماية الخصوصية المعلوماتية.

1. منظمة التعاون الاقتصادي والتنمية.

2. مجلس أوروبا.

3. الاتحاد الأوروبي.

4. الأمم المتحدة.

5. مجموعة الدول السبعة لاحقاً مجموعة الثمانية G8.

6. منظمة التجارة العالمية.

ثانياً: المؤتمرات الدولية والمحلية ودورها في حماية الخصوصية المعلوماتية. (المحاضرة القادمة بمشيئة الله تعالى).

المحور الأول

حقوق الشخص الذي سجلت المعلومات الشخصية المتعلقة به

ثانيا : الحق في التصحيح:

إن المعلومات التي يدلي بها المرء المودنة عنه في الكمبيوتر يجب أن تكون دقيقة ومتكاملة وذات صلة بالموضوع. وبطبيعة الحال فإن من أعدت عنه المعلومات هو خير من يحكم علي صحتها، ويكون له حق طلب تصحيحها ومراجعتها أو محوها، ولذلك يجب سن قوانين تضمن للأفراد ذلك.

ويعتبر الحق في التصحيح هو الهدف النهائي من ممارسة الحق في الإطلاع؛ لأن القصد من الإطلاع الحصول علي مستخرج من المعلومات يستهدف في النهاية تمكين الشخص من المنازعة في صحة ودقة البيانات المسجلة، ومن ثم طلب تصحيحها.

ومن المبادئ الأساسية في مجال قانون المعلوماتية أن الجهة القائمة علي الكمبيوتر تلتزم بمراعاة صحة ودقة المعلومات المسجلة، وأن تقوم بانتظام بتنقيح المعلومات بما يجعلها متفقة مع الحقيقة الواقعة.

وتنص المادة (٣٤) من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي أنه: (يلتزم المسئول عن المعالجة الآلية للمعلومات الشخصية باتخاذ كافة الاحتياطات الهامة، بالنسبة لطبيعة المعطيات ومخاطر المعالجة الإلكترونية للبيانات الشخصية، وذلك للحفاظ علي سلامة المعلومات، وبصفه خاصة تجنب إفسادها، أو إتلافها، أو دخول الغير غير المسموح له للإطلاع عليها إلخ).

وقضى في فرنسا بأن بنوك المعلومات تلتزم بالتحري عن جدية المعلومات التي تتلقاها وتسجلها، وتنعقد مسئوليتها في أحوال سوء التحريات أو الاعتماد علي وثائق مشكوك فيها، أو في حالة سوء عمليات البرمجة ومما يدعم التشدد في مسئوليتها أن تستهدف الربح من بيع المعلومات فيجب أن يكون الحصول علي المعلومات وتسجيلها قد تم بناء علي إجراءات معقولة، وإلا توافر عنصر الخطأ في جانب الجهة القائمة علي الكمبيوتر.

وإذا تحقق للشخص ضرر من جراء هذه المعلومات الخاطئة وغير الدقيقة، فإن له الحق في الحصول علي تعويض طبقا للقواعد العامة في المسئولية المدنية. وسواء تحقق الضرر أم لا، فإنه للشخص الحق في طلب تصحيح البيانات الخاطئة لتفادي حدوث الضرر في المستقبل، ويجوز لقاضي الاستعجال أن يأمر بحظر نشر أو توزيع المعلومات الخاطئة إلي حين إجراء التصحيح.

ولا تكتفي التشريعات المقارنة بالقواعد العامة، وإنما ينص علي تنظيم تفصيلي للحق في التصحيح في مجال المعلومات الشخصية. ويعتبر هذا الموضوع من أهم موضوعات قانون الخصوصية المعلوماتية.

فتذهب التشريعات المقارنة إلى إعطاء الشخص الحق في تصحيح، وتكملة أو إيضاح أو تنقيح أو محو المعلومات الخاصة به إذا كانت تلك المعلومات غير صحيحة، أو ناقصة، أو غامضة، أو تغيرت، وكذلك محو المعلومات التي يكون الحصول عليها أو لاستخدامها أو الاحتفاظ بها غير مشروع قانوناً.

ولقد نصت المادة السادسة علي الشروط التي يجب توافرها في البيانات الشخصية من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م والذي صدر تعديلاً لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي: (أن البيانات الاسمية التي يتم معالجتها إلكترونياً يجب أن تتوفر فيها الشروط التالية : ٤. أن تكون صحيحة وكاملة وضرورية؛ فإنه ينبغي أن يتم اتخاذ التدابير بالمحو أو التصحيح نحو البيانات التي تكون غير صحيحة أو غير كاملة).

والشخص الذي يحق له طلب التصحيح هو نفسه الذي يحق له الاطلاع والحصول علي مستخرج من المعلومات وفي أحوال الاطلاع غير المباشر يحق فقط للأشخاص الذين يخولهم القانون الاطلاع طلب التصحيح لأن الشخص المتعلقة به المعلومات قد لا يطلع عليها إطلاقاً كما هو الحال بالنسبة للمسائل المتعلقة بأمن الدولة، وكذلك أحياناً قد لا يطلع عليها، إذا تراءى للطبيب عدم إطلاع المريض علي البيانات، أما إذا أطلع عليه عليها جاز للمريض إجراء التصحيح .

ومن المسائل الهامة تحديد من الذي يقع علي عاتقه عبء الإثبات: هل هو الشخص طالب التصحيح؛ حيث يلتزم بإثبات عدم صحة البيانات، أم الجهة القائمة علي الكمبيوتر ؛ حيث تلتزم بإثبات صحة البيانات؟

تذهب التشريعات المقارنة إلى الخروج على القواعد العامة في الإثبات، وإلقاء عبء الإثبات علي عاتق الجهة القائمة علي الكمبيوتر، وذلك فيما عدا حالة واحدة وهي المتعلقة بالحصول علي المعلومات من الشخص نفسه صاحب المعلومات والقصد من قلب عبء الإثبات هو حماية الشخص بإعطائه حق التصحيح دفعة واحدة تجلعه أكثر فاعلية.

والتصحيح يدخل في إطار الإجراءات الوقائية التي تستهدف في الدرجة الأولى تفادي حدوث أضرار من جراء وجود معلومات خاطئة، فالتصحيح من إجراءات الحماية الوقائية للفرد الذي جمعت عنه معلومات شخصية. وإذا كانت المعلومات خاطئة، أو غامضة أو ناقصة، فإن الجهة القائمة علي الكمبيوتر تلتزم بإجراء التصحيح المناسب دون حاجة لأن يقدم صاحب الشأن ما يثبت أن له مصلحة في ذلك، ولا يخفى أن للجهة القائمة على الكمبيوتر مصلحة في إجراء التصحيح؛ حتى تكون معلوماتها صحيحة مما يعزز مصداقيتها.

كما يحق طلب محو البيانات التي تم الحصول عليها بطريقة غير مشروعة، مثل تسجيل البيانات المحظور تسجيلها أو التي تم الحصول عليها بوسائل احتيالية.

ويجوز للشخص طلب محو البيانات التي عفا عليها الزمن، أي القديمة التي تعدلت، وله كذلك أن يطلب محو المعلومات التي لا يجوز الاحتفاظ بها، وإذا كانت بعض البيانات غامضة فيحق للشخص أن يطلب إلحاق تفسير بوجهة نظره ويقدم مع المعلومات عند تداولها .

ولهذا تنص المادة ٣٨ من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م، - وتتعلق هذه المادة بحقوق الأشخاص بالنسبة للمعلومات الاسمية الخاصة بهم التي تتم معالجتها إلكترونيا - على أنه : (لكل شخص طبيعي الحق في الاعتراض، لأسباب مشروعة على أن تشكل المعلومات الاسمية الذي تتعلق به محلا للمعالجة فلكل شخص الحق في أن يعترض دون مصاريف عن أي معلومات تتعلق به تستخدم لأغراض العرض أو بصفة خاصة لأغراض تجارية، وذلك من جانب المسئول الحالي للمعالجة أو من جانب المسئول اللاحق. وهذه النصوص لا تنطبق عندما تفي المعالجة بالتزام قانوني، أو عندما يستبعد تطبيق هذه النصوص بنص صريح للتصرف الذي يجيز المعالجة) .

وإذا ثبت أحقية الشخص في التصحيح، فإن التصحيح يجب إبلاغه إلى الغير الذين سبق تزويدهم بالمعلومات الخاطئة أو غير الدقيقة، وعلى الآخرين إجراء التصحيح اللازم في أجهزة الكمبيوتر التابعة لهم. ويترتب علي وجود نص ينظم أحكام التصحيح من شأنه أن يعطي للشخص حماية في الأحوال التي لا تتوافر فيها شروط المسئولية المدنية. وحتى لا تتحكم الآلة وخصوصا الكمبيوتر في العلاقات القانونية المختلفة، وحتى لا يكون الكمبيوتر مصدرا للخلل في التوازن بين العلاقات الأفراد بعضهم ببعض، وبالسلطة القضائية وأجهزة الدولة والإدارة، فإن التشريعات المقارنة تتجه إلى حظر أن يكون القرار الصادر من الجهة القضائية أو جهة الإدارة أو الأفراد في شأن تقدير مسلك الشخص قائما فقط علي أساس المعالجة الإلكترونية لمعلومات تعطي تعريفا لوجه من الشخصية أو لشخصية صاحب الشأن.

ولقد نصت المادة العاشرة من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي هذا الأمر وذلك علي النحو التالي: (لا يمكن أن يصدر أي قرار قضائي يتضمن تقديرا لسلوك الشخص مستندا إلى المعالجة الآلية للبيانات الاسمية بشأن تقدير بعض مظاهر شخصيته.

كذلك لا يمكن أن يصدر قرار ينتج آثار قانونية تجاه الشخص يستند إلى المعالجة الآلية للبيانات، تستهدف تحديد الشخص المعنى أو تقدير بعض مظاهر شخصيته..... إلخ) .

فإدخال البيانات المختلفة عن الشخص ومعالجة هذه البيانات عن طريق الكمبيوتر يؤدي إلى التوصل إلى نتائج معينة حول شخصية صاحب الشأن وكفاءته وقدرته بل واستخلاص مدى خطورته أو

تسجيله كشخص خطر من الناحية الأمنية . وبناء على ما سبق فإنه يحظر الاستناد إلى نتائج تلك المعالجة لاتخاذ قرار قضائي، أو إداري، أو خاص. فلا يجوز لأي جهة أن تكون هذه النتائج هي الأساس الوحيد للقرار.

وعلي هذا يحق للشخص الاعتراض والمنازعة في القرار الصادر علي الأسس المحظورة، **فلااعتراض والتصحيح لا يشمل فقط المعلومات الخاطئة بل تمتد إلي أسس اتخاذ القرار.**

فلا يكون تسبب القرار الإداري، بالترقية أو التخطي بالترقية كافيا إذا كان قد استند إلى تقدير الشخصية المستخلص من معالجة المعلومات عن طريق الكمبيوتر، فيجب أن تتخذ قرارات الترقية بالنظر إلي الملف الفردي للشخص، ولا يجوز للبنك أن يتخذ قراره برفض الائتمان لشخص استنادا إلى نتائج مستخلصة عن طريق اللجوء إلي نظام النقاط الذي سبق وأن بيناه ولا يجوز تحديد مسلك شخص علي أساس معلومات معينة، مثل وضع مواصفات للعميل الممتاز أو السيئ، ثم يتحدد وصف كل عميل تلقائيا بإنزال هذه المواصفات علي الأشخاص، وهكذا لتحديد مدي توافر الخطورة الإجرامية.

لما كان هذا الحق يتقرر للشخص في مواجهة الجهة القائمة علي الكمبيوتر، سواء كان شخصا من أشخاص القانون العام، أم من أشخاص القانون الخاص، يذهب الرأي الراجح في الفقه المقارن إلى أن هذا الحق من الحقوق للصيقة بالشخصية. فلكل شخص الحق في ألا يأخذ الناس عنه فكرة مختلفة عما يكون عليه حقيقة. فإذا كان من شأن المعلومات المختزنة في الكمبيوتر أن تعطي عنه فكرة مخالفة للحقيقة، فيجب أن يكون له الحق في بيان حقيقة شخصيته، فيجب حماية الشخصية ضد كل ما يؤدي إلى تشويهها في مواجهة الناس. فللشخص الحق في أن تكون معالم شخصيته أمام الناس مطابقة للواقع والحقيقة.

فالحماية القانونية للشخص في مواجهة الكمبيوتر تعتبر مجرد امتداد للقواعد العامة في حماية الحقوق للصيقة بالشخصية، فهذه القواعد تستهدف حماية حقوق الشخصية في مواجهة مخاطر الكمبيوتر، فقد أقر القانون حماية الخصوصية وفاعلية تلك الحماية لا تكتمل إلا بتوفير سبل الحماية المناسبة للمخاطر التي تهددها فموضوع الحماية ليس المعلومات المختزنة، وإنما المصالح التي تهددها هذه المعلومات غير الصحيحة.

ويترتب علي هذا التأصيل في حالة وفاة الشخص فإن الخلف يحق له طلب البيانات والتصحيح استنادا إلي أن من واجبه الحفاظ علي سمعة وصورة السلف والدفاع عن الأسرة.

ثالثا : الحق في المحافظة على خصوصية المعلومات :

من المبادئ الأساسية أن تخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أن الرضاء بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى كافة.

وطبقا لذلك ينبغي اتخاذ كافة الاحتياطات الهامة بغرض الحفاظ على سلامة المعلومات الشخصية، ولاسيما منع الإفساد بهذه المعلومات، أو اطلاع الغير غير المرخص لهم عليها. وقد أوقفت اللجنة القومية للمعلوماتية والحريات في فرنسا إرسال نتائج تحاليل الدم عن طريق التليفون.

ومن الناحية العملية فإن المعلومات تختزن من أجل استعمالها، سواء في النطاق الداخلي أو الخارجي. والحق في المحافظة علي خصوصية المعلومات لا يتوافر في الحالتين من حيث المبدأ، وإن كان يختلف من حيث المدى أو الصورة التي يكون عليها، ومن أهم سبل المحافظة علي الخصوصية اتخاذ الإجراءات اللازمة لمنع تسريبها علي خلاف ما يقتضيه التداول المسموح.

و الواقع أنه لحماية البيانات الشخصية التي تستهدف ضمانه حق السرية لذوي الشأن، ينبغي - لتحقيق هذه الحماية - أن يؤخذ "حظر الدخول للمعلومات الشخصية " بالمفهوم الواسع؛ حتى يمكن الحماية الفعلية للحق في السرية؛ حتى يندرج تحت هذا المفهوم الواسع المعاقبة علي التصرف الذي يقع عند الدخول في الأنظمة المعلوماتية بالطرق العادية ولكن قد يقع تعسف بعد ذلك.

ولا صعوبة في إلزام الجهة القائمة علي الكمبيوتر بالمحافظة على السرية إذا كانت الجهة ملتزمة بعدم إفشاء السر قانونا مثل السر الطبي، فالمعلومات الطبية المخزنة لدي إحدى المستشفيات لا يجوز أن تفشى على خلاف ما يقضي به القانون، وفي الأحوال التي ينشأ فيها نظام المعلومات طبقا للقانون فإن المشرع يلزم القائمين علي المعلومات بالمحافظة علي السرية.

ومثال علي ذلك فقد نصت المادة ٤٤ بند ٣ الفقرة الثانية من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي أنه: (يكون للطبيب وحده الاطلاع على المعلومات الطبية الفردية التي تتضمنها معالجة ضرورية لأغراض الطب الوقائي، وللأبحاث الطبية والتشخيص الطبي ولإدارة العلاج أو لإدارة مرفق الصحة والتي قام بها عضو من مهنة الصحة. ويثبت حضوريا محضر التحقيقات والزيارات التي قام بها تطبيقا لهذه المادة) .

وخلاصة ما سبق تبدو أهمية وجود قواعد خاصة في مجال نظم المعلومات الآلية ومبادئ الخصوصية المعلوماتية تتمثل في أمرين أولهما، عدم نقل أو تداول المعلومات خارج الهدف من إقامة المعلومات، ثانيهما وضع ما يلزم القائمين علي الكمبيوتر بالمحافظة علي الخصوصية المعلوماتية.

وتطبيقا لذلك لقد نصت المادة ٣٥ من القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤ م ، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي أنه: (لا يمكن للمعلومات الاسمية أن تكون محلا لعملية المعالجة الإلكترونية من جانب مستخدم من الباطن يتصرف تحت سلطة المسئول عن المعالجة إلا بناء على تعليمات من مسئول المعاملة. ويعتبر كل شخص يعالج معلومات اسمية إلكترونيا وذلك لحساب المسئول عن المعاملة بمثابة مستخدم من الباطن بمفهوم هذا القانون . وهذا الأخير ينبغي أن يضع ضمانات كافية لضمان تنفيذ تدابير السلامة والسرية المنصوص عليها في المادة ٣٤ هذا القانون، وهذه الضمانات لا تعفي المسئول عن المعاملة).

وطبقا للقواعد العامة في حماية الخصوصية فإن الرضاء بإعطاء المعلومات أو التحري عن الحياة الخاصة لا يفيد بالضرورة الرضاء بنشر هذه المعلومات، كما أن الرضاء بالنشر لا يفيد الرضاء بإعادة النشر، بل لابد من الحصول علي رضاء جديد بإعادة النشر فمن يأتمن الغير علي خصوصيات حياته بإطلاعه علي دقائقها لا يقبل بالضرورة إذاعة ونشر هذه البيانات، ومن يقبل النشر علي طائفة معينة وفي ظروف معينة لا يقبل بالضرورة النشر علي الكافة وفي أي وقت طال أم قصر.

ولهذا ثار التساؤل عن أثر قبول تقديم المعلومات الشخصية لتخزينها في الكمبيوتر علي نشر هذه المعلومات بنقلها إلى الغير الراغب في الحصول عليها ؟

وبموجب القواعد العامة في حماية الخصوصية المعلوماتية، كان يقتضي القول بضرورة الحصول علي موافقة الشخص في كل مرة يطلب فيها الغير الاطلاع علي هذه المعلومات، ولكن يعيب ذلك أنه لا يتلاءم مع طبيعة الكمبيوتر من حيث كم المعلومات المخزنة وعدد الأشخاص الذين ترتبط بهم، والأخذ بهذا الرأي يعوق التقدم المنشود من إقامة نظام للمعلومات، ويحمل الجهات القائمة علي الكمبيوتر نفقات ضخمة. والواقع أن الرضاء بتقديم المعلومات يكون رضاء متبصرا متى صدر بالنظر إلى أمرين:

أولهما: أن هذه المعلومات سوف تخزن وتسجل في الكمبيوتر.
ثانيهما: أن القصد من إقامة نظام المعلومات هو تحقيق غرض معين، وأن هذه المعلومات تدخل في عناصر إقامة النظام أو البرنامج.

ولهذا فإن الرضاء في ظل هذه الظروف يفيد ضمنا الرضاء باستخدام هذه المعلومات ونشرها في الحدود اللازمة لتحقيق غرض البرنامج، ومن ثم فإن الرضاء ينسحب إلي النشر والتداول المتوقع وفقا للغرض من البرنامج، ويجب أن يقتصر نقل المعلومات إلى الغير المرتبط بالغرض من البرنامج. وبناء عليه فإن الجهة القائمة علي الكمبيوتر، تلتزم بعدم تقديم هذه المعلومات أو نشرها إلا للأشخاص المتوقع اطلاعهم عليها، ووفقا للغرض من نظام المعلومات، وهذا الالتزام تفرضه القواعد العامة في حماية

الأشخاص في مواجهة الجرائم السيبرانية، بمعنى أنه التزام قانوني وليس مصدره العلاقة العقدية، وهذا الالتزام بالنظام العام، ومن ثم لا يجوز الاتفاق علي ما يخالفه.

وهذا القيد يستهدف حماية الأشخاص ضد توسع بنوك المعلومات في نشر المعلومات علي أوسع مدى تحقيقا للربح المادي، فاستخدام المعلومات ونشرها خارج الدائرة المتوقعة والمتفقة مع الغرض من البرنامج ينطوي علي مساس بالخصوصية المعلوماتية.

وبطبيعة الحال فإن مسألة تحديد الأشخاص المتوقع اطلاعهم علي المعلومات لا يخلو من المرونة التي يخضع تقديرها للقضاء أو للجهة الإدارية المشرفة علي نظم المعلومات والكمبيوتر، ولكن ينصح بأن يكون التفسير تفسيرا ضيقا.

تذهب التشريعات المقارنة إلى إلقاء الالتزام بالحفاظ علي الخصوصية المعلوماتية علي عاتق الأشخاص الذين يحق لهم النفاذ إلي المعلومات الشخصية محل المعالجة الآلية.

وتوقع عقوبة جنائية علي كل من ينقل إلي الغير المعلومات الشخصية، وكذلك كل من يكشف معلومات تتعلق بالخصوصية أو الاعتبار دون رضا صاحب الشأن.

وتنص المادة ٤٥ بند من القانون الفرنسي رقم 108 سنة 2004م، والذي صدر تعديلا لقانون المعلوماتية والبطاقات والحريات سنة ١٩٧٨م علي أنه: (في حالة الاعتداء الجسيم والمباشر علي الحقوق والحريات **يمكن لرئيس اللجنة أن يطالب بإجراء الاستعجال من القضاء المختص، بأن يأمر إذا كان هناك مقتضي تنفيذ الغرامة التهديدية وكافة إجراءات السلامة الضرورية للحفاظ علي هذه الحقوق والحريات**)، بمعنى أن تطلب من القضاء المختص أن يتخذ كافة التدابير الضرورية مع توقيع الغرامة التهديدية، للحفاظ علي الحقوق والحريات.

ويجوز أن يكون مصدر الالتزام بالسرية العقد الذي يبرم بين بنك المعلومات ومن يحق له الاستفادة من المعلومات وفقا للغرض من البرنامج، فالالتزام بالسرية كما يسري في العلاقة بين الشخص وبنك المعلومات فإنه يجب أن يسري ذلك في العلاقة بين البنك ومن تنقل إليه المعلومات. ولما كان تخزين المعلومات في الكمبيوتر يجعله مستودعا للأسرار أو الخصوصيات المعلوماتية في الأحوال التي يجوز فيها تخزين مثل تلك البيانات، فإن القائم علي الكمبيوتر يلتزم باتخاذ الوسائل والإجراءات اللازمة لعدم تسرب هذه المعلومات لغير من يحق له الاطلاع عليها ولمنع ما يمكن تسميته بسرقة المعلومات والنصب في مجال الكمبيوتر.

فقد أثبتت التجربة في العديد من البلدان أن المعلومات كانت محلا لسرقات شهيرة، ويتم ذلك عادة بالتواطؤ مع العاملين أو المسؤولين عن الكمبيوتر ، وفي نفس الوقت يندر الإعلان عن هذه الجرائم حفاظا علي سمعة الجهة التي بها الكمبيوتر، ومنعا لإشاعة الذعر لدي المتعاملين مع هذه الجهة، كالمصارف علي وجه الخصوص.

ولهذا تنص التشريعات المقارنة علي أن الجهة القائمة علي الكمبيوتر، وبرامجه تلتزم تجاه الأشخاص الذين أدخلت بيانات شخصية متعلقة بهم إلي الحاسب، باتخاذ إجراءات الحيلة المناسبة للحفاظ علي سلامة المعلومات لمنع تشويهها أو إتلافها، أو تحويرها، أو إطلاع الغير عليها .

ونلاحظ أن إجراءات الأمن للمعلومات الشخصية تتكون من شقين أساسيين: أولهما ما يسمى بالشق الفني، ويشمل الإجراءات الفنية المتعلقة بالشفرة الخاصة بمستخدم الكمبيوتر ، والتي تتيح له الدخول إلى الكمبيوتر واستخدامه، وهذا الشق لا يوفر حماية إلا في حدود ٢٠٪، ولهذا كان لابد من الشق الثاني، وهو حسن التنظيم الإداري والفني للجهة القائمة على الكمبيوتر وحسن اختيار الموظفين والعاملين بها ووضع النظم اللازمة لرقابتهم من أجل المحافظة علي سلامة المعلومات.

والقصد من إجراءات الأمن هو الحفاظ علي سرية وخصوصية المعلومات من ناحية والتأكيد علي احترام المبادئ التي يقوم عليها القانون من ناحية أخرى .

نخلص من ذلك أنه يتعين وضع النظم والإجراءات اللازمة لتأمين حماية المعلومات الشخصية والتي تكفل المحافظة عليها الحريات و لاسيما الحق في الخصوصية المعلوماتية.

رابعاً : الحق في الإشراف المستقل:

يتعين على كل دولة إنشاء هيئة رقابية إشرافية مستقلة، تتمتع بسلطة تدقيق أنشطة معالجة البيانات وتتمتع أيضا بسلطة الوصول للبيانات الأساسية، وكذلك سلطة التدخل للأمر بمحو البيانات ووقف المعالجة، ووقف نقل البيانات لأطراف آخرين.

وتختص هذه اللجنة بإصدار الإذن بإنشاء بنوك المعلومات أو تلقي الإخطارات بذلك، والسهر علي تطبيق أحكام القانون، وإبلاغ ذوي الشأن بحقوقهم وواجباتهم، وتحقيق من احترام نظام المعلومات لأحكام القانون وكما يتعين تفويض السلطة الرقابية بالاستماع للشكاوي الصادرة من أصحاب البيانات.

وعلى هذه الهيئة أن تضع تحت تصرف الجمهور قائمة بنظم المعلومات الموجودة موضحة فيها القانون الذي أنشئت وفقا له، واسم النظام والهدف منه، والجهة التي تمارس حق الاطلاع والتصحيح في

مواجهتها، وطوائف المعلومات الاسمية المسجلة، ومن يحق له تلقي هذه المعلومات، وعليها أن تضع تحت علم الجمهور ما تصدره من توصيات وقرارات وآراء، والتي تكون ضرورية لتطبيق القانون وتفسيره.

وخير مثال علي ذلك في فرنسا ، فقد نص القانون الفرنسي علي اللجنة القومية للمعلوماتية والحريات في المادة ١١ من الفصل الثالث - المعني باللجنة القومية للمعلوماتية والحريات من القانون الفرنسي رقم ٨٠١ - والصادر تعديلا لقانون المعلوماتية والبطاقات والحريات تنص على: (أن اللجنة القومية للمعلوماتية والحريات تعد سلطة إدارية مستقلة، وأنها تمارس المهام التالية :)، وسوف نستعرض مهام هذه اللجنة ودورها في حماية الخصوصية في مواجهة المعالجة الإلكترونية للبيانات الشخصية في موضعها.

وتجدر الإشارة هنا إلى التعليق الوارد علي المادة ٢١ من هذا القانون، والذي ينص على: أن اللجنة القومية للمعلوماتية والحريات تتمتع باعتبارها سلطة إدارية مستقلة بمراقبة احترام نصوص قانون ٦ يناير لعام ١٩٧٨م الخاص بالمعلوماتية والبطاقات والحريات، بسلطة تقدير الشكاوي التي تعرض عليها، وذلك بغض النظر عن القرار الذي يصدر بعد ذلك من جانب السلطات القضائية التي يؤول إليها الأمر إعمالا للمادة 4/21 من هذا القانون، والمادة ٤٠ من قانون الإجراءات الجنائية الفرنسي.

خامسا: الحق في الإخطار العام:

ومقتضي هذا الحق هو أن نظم جمع المعلومات يجب أن يكون الجمهور على علم بها، ومن مقتضاه أيضا أن الشخص لا يستطيع أن يتحقق من الضرر حتى يعلم به، ويعلم من المسئول عنه. وفي المملكة المتحدة يعلم معظم الناس أن مجالس الكهرباء والغاز ومصلحة البريد لديها معلومات عنهم مخزنة إلكترونيا، ولذلك فمن البسير اكتشاف ما الذي تسجله عنهم، وهذا هو أساس مبدأ الإخطار العام، ولا يعتبر هذا المبدأ قد حقق أهدافه ما لم يتمكن الأفراد من معرفة ما يسجل عنهم من معلومات شخصية.

ولقد نص القانون الفرنسي علي هذا الحق في المادة (٣١) من الفصل المعني بالشكليات السابقة علي المعالجة الإلكترونية بالبيانات من القانون الفرنسي رقم 801 لسنة 2004 والصادر تعديلا لقانون المعلوماتية والبطاقات والحريات فنص علي : (البند الأول: تضع اللجنة تحت تصرف العامة قائمة المعلومات المبرمجة والتي تشكل محلا للمعلومات المنصوص عليها في المواد من ٢٣ إلى ٢٧ باستثناء المعاملات المشار إليها في المادة ٢٦ بند ٣. وهذه القائمة تحدد هذه المعلومات :

1. التصرف الذي أنشأ المعالجة الإلكترونية للبيانات الشخصية أو تاريخ بيان هذه المعالجة.
2. تسمية والغرض من المعالجة الإلكترونية للبيانات.
3. الهوية وعنوان المسئول عن المعالجة الإلكترونية للبيانات، أو الممثل لمن لم يقيم على الإقليم القومي أو على إقليم أي دولة عضوا في المجموعة الأوروبية.

4. وظيفة الشخص أو المرفق الذي يمارس خلاله الحق في الدخول إلى المعلومات الشخصية.
 5. طوائف المعلومات الشخصية التي تشكل محلا للمعالجة الإلكترونية، وكذلك المرسل إليهم، والطوائف المكلفة بتلقي الاتصال .
 6. انتقال المعلومات الشخصية - عند الضرورة - والمتجهة لدولة غير عضو في المجموعة الأوروبية
- البند الثاني: وتضع اللجنة تحت تصرف العامة آراءها، أو قراراتها، أو توصياتها .
- البند الثالث: وتنشر اللجنة القومية للمعلوماتية والحريات قائمة الدول التي مكنت لها لجنة المجموعة الأوروبية أنها تكفل مستوى من حماية كاف بالنسبة لنقل أو لطائفة نقل معلومات شخصية).

والخلاصة :

أن تلك المبادئ والحقوق تستهدف تقرير حماية الخصوصية المعلوماتية التي تجمع إلكترونياً، ومجمل تلك المبادئ يعني في المقام الأول أن ما يخزن عن الأفراد من معلومات يجب أن يبقى في مأمن من أيدي العابثين و المتطفلين ، كما يعني ضمان استخدامها فيما خصصت له من أغراض .

وفي رأينا أن تلك المبادئ ما لم تتدعم بتأييد تام من جانب السلطات العامة في الدولة، وتصاغ في شكل قواعد دستورية أو قانونية ملزمة فإنها لن تتعدي مرحلة التوصيات وبالتالي لن تؤتي ثمارها .

المحور الثاني

الحماية الدولية والإقليمية للحق في الخصوصية المعلوماتية

(الحماية المعنية)

• تمهيد وتقسيم:

وفي حقل حماية الخصوصية المعلوماتية، فإن العديد من المنظمات الدولية طورت أنشطة مختلفة تهدف إلى تنظيم حماية المعلومات الخاصة وتنظيم تدفق وانتقال البيانات، وقد أنجز الجزء الأكبر من هذا الجهد في هذا الحقل من قبل منظمة التعاون الاقتصادي والتنمية، ومجلس أوروبا، واتحاد أوروبا، والأمم المتحدة، ومجموعة الدول السبعة ومنظمة التجارة العالمية، وسوف نتناول - أيضا - المؤتمرات الدولية والإقليمية وذلك علي النحو التالي:

أولاً: المنظمات الدولية ودورها في حماية الخصوصية المعلوماتية.

ثانياً: المؤتمرات الدولية والمحلية ودورها في حماية الخصوصية المعلوماتية.

أولاً: المنظمات الدولية ودورها في حماية الخصوصية المعلوماتية:

لقد تضاعف حرص المنظمات الدولية ومنها الأمم المتحدة - على الحفاظ علي حقوق الإنسان بدرجة كبيرة، مما يشير إلى استقرار جذور فرع القانون الدولي المتعلق بحقوق الإنسان. ويرجع هذا التطور المهم في مسيرة حقوق الإنسان ومنها حقه في الخصوصية المعلوماتية إلى عدة أسباب أهمها:

1. تطور الحياة الإنسانية وزيادة التقارب والاحتكاك بين الشعوب بفضل تطور وتقدم سبل المواصلات وتطور الحياة الاقتصادية وزيادة المبادلات التجارية، وزيادة استخدام وسائل التكنولوجيا الحديثة، كل ذلك أدى إلى تعرف الشعوب على أوضاع حقوق الإنسان لدى غيرها، وتعرفها علي مبادئ جديدة في هذا المجال، ومنها الحق في الخصوصية المعلوماتية.

2. شيوع استخدام وسائل التكنولوجيا الحديثة وما لها من آثار سلبية تؤثر علي انتهاك حقوق الإنسان، وخصوصا الخصوصية المعلوماتية.

3. شعور الضمير الجماعي بعدم كفاية نظم القانون الداخلي لحماية حقوق الإنسان، وخصوصا الحق في الخصوصية المعلوماتية وإن السبيل لضمان هذا الاحترام هو حمايتها عن طريق نظم القانون الدولي العام، وما يترتب من التزامات على الأعضاء في المجتمع الدولي، وما يملكه من وسائل لضمان احترام الخصوصية المعلوماتية. وسوف نتناول أهم هذه المنظمات الدولية ودورها وذلك علي النحو التالي:

1. منظمة التعاون الاقتصادي والتنمية.
2. مجلس أوروبا.
3. الاتحاد الأوروبي.
4. الأمم المتحدة.
5. مجموعة الدول السبعة لاحقا مجموعة الثمانية G8.
6. منظمة التجارة العالمية.

1. منظمة التعاون الاقتصادي والتنمية:

ابتداء من عام ١٩٧٨م بدأت هذه المنظمة وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات، وقد تم تبني هذه القواعد من قبل مجلس المنظمة في عام ١٩٨٠م ، مع التوصية للأعضاء بالالتزام بها، ولا تعد هذه القواعد إلزامية، وإنما مجرد إرشادات وتوصيات، وتغطي هذه القواعد الأشخاص الطبيعيين فقط، وتطبق على القطاعين العام والخاص، وتتعلق أيضا بالبيانات المعالجة آليا أو غير

المعالجة آليا، وتتضمن التوجيهات المبادئ الثمانية الرئيسية لحماية الخصوصية المعلوماتية أو الحق في حماية البيانات الخاصة، وهذه المبادئ هي:

1. تحديد حصر عمليات جمع البيانات (Collection-limitation).
 2. الاقتصار على طبيعة البيانات الشخصية وتحديدتها (Data quality).
 3. تحديد الغرض (Purpose-specification) الذي يتم تجميع البيانات من أجله .
 4. حصر الاستخدام بالغرض المحدد (Use-limitation) ، بمعنى ألا تستخدم البيانات إلا في الغرض المحدد للجهة الطالبة للبيانات، ولا يتم الخروج علي ذلك إلا بموافقة الشخص.
 5. توفير وسائل حماية وأمن المعلومات (Security-Safeguards).
 6. . العلانية (Openness)، ومقتضي ذلك أن يكون ما يتعلق بالحياة الشخصية من سياسة عامة للتطوير والتخطيط والتطبيق معلنة للكافة لمعرفتها .
 7. الحق في المشاركة (Individual Participation)، بمعنى أن يكون للأشخاص الحق في المشاركة عن طريق الحق في الوصول والتعرف علي البيانات الخاصة بهم، وحقوقهم في الرد عليها، والتعديل فيها.
 8. المساءلة (Accountability) ، ويعني هذا المبدأ مساءلة الشخص المنوط به التعامل مع البيانات الشخصية عن مدى كفالتهم للقواعد والمبادئ السابقة في التعامل مع تلك البيانات.
- وهذه المبادئ تصف البيانات والمعلومات الشخصية على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع (Collection)، والتخزين (Storage) والمعالجة (Processing) والنشر (Dissemination).

ومثل هذا الدليل – الوثيقة - لعب دورا رئيسا وكان الأكثر تأثيرا في اتجاه الدول الأوروبية إلى اقرار تشريعات وطنية في حقل الخصوصية، ومنذ ذلك التاريخ تتابع هذه المنظمة موضوع الخصوصية المعلوماتية وتضعه ضمن أجندتها السنوية وتتابع تطورات التدابير التشريعية في هذا الحقل .

2. مجلس أوروبا (Council of Europe)

• تمهيد وتقسيم :

كان للمجلس الأوروبي دور لا ينكر في حماية خصوصية للأفراد، والبيانات الشخصية من إساءة استخدامها بواسطة المعالجة الإلكترونية لها، وتمثل ذلك في التوصيات التي وضعها البرلمان الأوروبي في ٨ مايو سنة ١٩٧٩م، وفي ٢٣ سبتمبر سنة ١٩٨٠م، وأقر المجلس الأوروبي التوصية الخاصة بحماية تدفق ونقل المعلومات ذات الصبغة الشخصية بين الدول الأعضاء. وفي ١٨ يناير سنة ١٩٨١م ، وقعت اتفاقية

تحت مظلة المجلس الأوروبي تتعلق بحماية الأفراد في نطاق المعالجة الإلكترونية للبيانات الشخصية في 10 / 1985م.

وقد بذل مجلس أوروبا جهودا إضافية في هذا الحقل من خلال لجنة الخبراء العاملة في حقل حماية البيانات الشخصية، وقد أصدرت هذه اللجنة سلسلة من الأدلة التوجيهية المعتمدة على الاتفاقية المذكورة، وهي ليست أكثر من توصيات موجهة إلى حكومات الدول الأعضاء، وتتعلق توصيات اللجنة بحماية قواعد المعلومات الطبية، وقواعد المعلومات الخاصة المتعلقة بالأنشطة الطبية، والإحصاءات وقواعد المعلومات الخاصة لأغراض التسويق وقواعد المعلومات الخاصة لأغراض الضمان الاجتماعي، وكذلك لأغراض البوليس، والبيانات الجنائية، وقواعد المعلومات الخاصة بأغراض التوظيف، وكذلك خدمات الاتصال، وقد عمل جزء من اللجنة المذكورة على موضوع البيانات المتعلقة بالقطاع المصرفي.

ومن أهم المبادئ التوجيهية التي اعتمدها المجلس الأوروبي هي " المبادئ التوجيهية للتعاون بين السلطات القضائية وبين مزودي خدمة الإنترنت لمكافحة جرائم السيبرانية" . وسوف نتناول أهم هذه المبادئ والتي تتناول موضوع الخصوصية المعلوماتية وأيضا (اتفاقية حماية الأفراد في نطاق المعالجة الإلكترونية للبيانات الشخصية) من خلال التقسيم التالي:

أولا : اتفاقية حماية الأفراد في نطاق المعالجة الإلكترونية للبيانات الشخصية.

ثانيا : المبادئ التوجيهية للتعاون بين السلطات القضائية وبين مزودي خدمة الإنترنت لمكافحة جرائم المعلوماتية. وذلك على النحو التالي:

أولا: اتفاقية حماية الأفراد في نطاق المعالجة الإلكترونية للبيانات الشخصية

(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)

تم عقد هذه الاتفاقية في ٢٨ يناير سنة ١٩٨١ في إطار مجلس أوروبا علي خلاف توصيات منظمة التعاون الاقتصادي والتنمية، فإن هذه الاتفاقية ملزمة للأعضاء المتعاقدين، وينحصر نطاقها بالأشخاص الطبيعيين، وتقرر هذه الاتفاقية عشرة مبادئ تمثل الحد الأدنى لمعايير حماية الخصوصية المعلوماتية 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، وقيود الجمع والوقاية والعلنية، وتوقيت الغرض، وتحديد مدى الدقة ومشاركة الأفراد) ، واستنادا إلى هذه المبادئ الأساسية للحماية، فإن قواعد الاتفاقية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة، وتمنع نقل أية معلومات خارج الحدود إلا للدولة التي تتوفر لها حماية موازية مع استثناءات لهذه القاعدة.

• الهدف من الاتفاقية :

جاءت المادة الأولى بشأن الهدف من الاتفاقية على هذا النحو:

"إن الهدف من هذه الاتفاقية هو ضمان احترام لكل شخص طبيعي أيا كانت جنسيته، أو إقامته حقوقه وحرياته الأساسية، ولاسيما حقه في الحياة الخاصة بالنسبة للمعالجة الإلكترونية للمعلومات الشخصية التي تتعلق به".

والمادة الثانية تناولت هذه المادة التعريفات لتوضيح غرض هذه الاتفاقية وذلك على النحو التالي:
أ) المعلومات ذات الطابع الشخصي: كل معلومة تتعلق بشخص طبيعي معلوم الهوية يمكن معرفته "بالشخص المعني".

ب ويقصد بالبطاقة المبرمجة : كل مجموع معلومات تشكل محلا لمعالجة مبرمجة.

ج) يقصد "بالمعالجة المبرمجة : العمليات التي تجري كلية أو بصفة جزئية بمساعدة وسائل: تسجيل البيانات أو المعلومات وتطبيق عمليات على هذه البيانات، أو تعديلها، أو محوها أو نشرها.

د) صاحب البطاقة : يقصد به الشخص الطبيعي، أو المعنوي، أو السلطة العامة، أو المرفق، أو أي منظمة أخرى تكون مختصة وفقا للقانون الوطني لتقرير الغاية من البطاقة المبرمجة وطوائف المعلومات الشخصية التي ينبغي تسجيلها، والعمليات موضوع التطبيق عليها.

• نطاق تطبيق هذه الاتفاقية :

تتعلق المادة الثالثة من هذه الاتفاقية بنطاق التطبيق وذلك على النحو التالي :

وفقا لهذه المادة: يتعهد الأطراف بتطبيق هذه الاتفاقيات على البطاقات والمعالجات المبرمجة للمعلومات الشخصية في القطاعات العامة والخاصة. ويجوز لكل دولة وقت التوقيع أو الإيداع لأداة تصديقها أو قبولها، أو انضمامها، أو في أي وقت لاحق أن تعلن ببيان موجه إلى السكرتير العام لمجلس أوروبا.

• توصيات الاتفاقية :

وقد نظمت هذه الاتفاقية عدة توصيات خاصة بحماية البيانات الشخصية ضد إساءة استخدامها أثناء المعالجة الإلكترونية ولمواجهة أخطار بنوك المعلومات وكي تلتزم بها جميع الدول الأعضاء عند وضع تشريعاتها، وتخلص في الآتي:

1. أن تكون البيانات المسجلة صحيحة ودقيقة، ويجب أن يتم الحصول عليها بطريقة مشروعة.
2. أن تكون مدة حفظ هذه البيانات محددة.
3. عدم اطلاع الغير على البيانات الشخصية أو استعمالها في غير الغرض المخصص لها.
4. إقرار حق الشخص في الإطلاع على البيانات الخاصة به، أو تصحيحها، أو تعديلها، أو محوها إذا كانت باطلة أو حصل عليها عن طريق غير مشروع.

5. اتخاذ الاحتياطات اللازمة ضد كل تعسف أو إساءة لاستخدام هذه البيانات، ويجب أن تزود هذه الأجهزة بأجهزة أمان تمنع الوصول إلى هذه المعلومات.
6. تحديد الأشخاص الذين يكون لهم حق الوصول إلى هذه المعلومات وإلزامهم بالكتمان وسر المهنة.

ثانيا: المبادئ التوجيهية للتعاون بين السلطات القضائية وبين مزودي خدمة الإنترنت لمكافحة جرائم السيبرانية

وهذه المبادئ هي ثمار لجولات عديدة من النقاشات بين الممثلين من الصناعة المعلوماتية وبين جهات تطبيق القانون والذين اجتمعوا خلال الفترة بين أكتوبر ٢٠٠٧م وفبراير ٢٠٠٨م برعاية مشروع المجلس الأوروبي حول الجريمة السيبرانية.

وحظيت هذه المبادئ التوجيهية بمزيد من النقاش واعتمدها المؤتمر العالمي "التعاون لمكافحة الجرائم السيبرانية (المجلس الأوروبي . ستراسبورغ ، فرنسا) في ١ - ٢ أبريل ٢٠٠٨ م .

وهذه المبادئ التوجيهية لا تعتبر أداة ملزمة يمكن تعميمها واستخدامها لمساعدة جهات إنفاذ القانون ومقدمي الخدمات في أي بلد في مختلف أنحاء العالم لتنظيم التعاون فيما بينهم لمكافحة الجريمة الحاسوبية، مع احترام أدوار ومسؤوليات كلا منهم فضلا عن حقوق مستخدمي الانترنت.

• ومن أهم هذه المبادئ فيما يتعلق بالخصوصية المعلوماتية ما يلي :

مقدمة، والتي وردت بها المبدأ الثامن: إن الغرض من هذه المبادئ التوجيهية هو مساعدة السلطات القضائية، ومزودي خدمات الإنترنت تنظيم تفاعلهم مع بعضهم البعض فيما يتعلق بقضايا جرائم السيبرانية وهي قائمة على أفضل الممارسات القائمة، على أن تكون قابلة للتطبيق في كل دولة في جميع أنحاء المعمورة، طبقا للتشريعات المحلية مع احترام حرية التعبير والخصوصية، وحماية البيانات الشخصية، وأية حقوق أساسية للمواطنين .

• التدابير التي ينبغي اتخاذها من قبل سلطات إنفاذ القانون، ومن أهمها مايلي :

الثاني والثلاثون

سرية البيانات - ينبغي لجهات إنفاذ القانون ضمان سرية البيانات الواردة.

الخامس والثلاثون

يجب تشجيع جهات إنفاذ القانون على ضمان متابعة أوامر حفظ البيانات وغيرها من التدابير المؤقتة في الوقت المناسب عن طريق أوامر الكشف عن البيانات، أو إبلاغ مزود الخدمة في الوقت المناسب بعدم ضرورة الاحتفاظ بالبيانات.

• التدابير التي ينبغي اتخاذها من قبل مقدمي الخدمات :

الحادي والأربعون: التعاون للتقليل من استخدام الخدمات لأغراض غير مشروعة مع مراعاة حقوق والحريات المطبقة مثل حرية التعبير والخصوصية، والقوانين الوطنية أو الدولية الأخرى، فضلاً عن اتفاقات المستخدم، وينبغي تشجيع مقدمي الخدمات على أن تتعاونوا مع سلطات إنفاذ القانون للمساعدة في تقليل مدى استخدام الخدمات للنشاط الإجرامي حسب تعريفها في القانون.

3. الاتحاد الأوروبي (European Union)

بدأ الاتحاد الأوروبي جهوده بشأن توحيد القواعد المقررة في قوانين حماية الخصوصية ابتداء من عام ١٩٧٦م، وفي هذا الحقل صدر عن الاتحاد تعليمات عديدة وهي:

1. تعليمات صادرة في ٢٨ / ٤ / ١٩٧٦م والمتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات.
2. وتعليمات صادرة في ٥ / ٨ / ١٩٧٩م والمتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات.
3. وتعليمات صادرة في 9 / 3 / 1982 بذات الموضوع .

وقد طلب البرلمان الأوروبي من الاتحاد اتباع إصدار خطة تدفع الدول الأعضاء إلى توقيع الاتفاقية الأوروبية المتعلقة بالخصوصية، وقد أصدر بتاريخ 29 / 7 / 1981 توصية للدول الأعضاء بتوقيع اتفاقية مجلس أوروبا المشار إليها أعلاه، ومنذ عام ١٩٨٥م فإن حماية الخصوصية بالنسبة للأشخاص الطبيعيين والمعنويين يجري مناقشتها والتعامل معها من قبل المجلس الاستشاري القانوني التابع للجنة الأوروبية.

وفي عامي ١٩٩٥م و ١٩٩٧م، سن الاتحاد الأوروبي دليلين إرشاديين أجل تحقيق الانسجام والتناسق بين قواعد حماية الخصوصية في دول الاتحاد الأوروبي، ولتوفير مستوى معين بالنسبة لحماية المواطنين الأوروبيين، والسماح بالتدفق الحر للبيانات الشخصية داخل نطاق الاتحاد الأوروبي.

وقد قرر هذان الدليلان مستوى معين لحماية الخصوصية لا يقف فقط عند حد حماية البيانات وفق مفاهيم القوانين القائمة حالياً ولكن يتجاوزها إلى تأسيس مزيد من الحقوق وتوسيع نطاق الحق ذاته.

وفي تموز ٢٠٠٠م أصدرت المفوضية الأوروبية نموذجاً جديداً لدليل معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية، وقد قدم هذا الدليل كجزء من حزمة واسعة تهدف إلى تقوية المنافسة في سوق الاتصالات الإلكترونية ويتعين أن يحل محل دليل الاتصالات لعام ١٩٩٧م.

وبتاريخ ٢٠ نيسان ٢٠٠٠ تقدمت اللجنة الأوروبية لمشكلات الجريمة (CDBC)، ولجنة الخبراء في حقل جرائم التقنية ساير كرايم بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقاً في بودابست ٢٠٠١ م، وكانت الاتفاقية جاهزة علي التوقيع في ٢٣ نوفمبر ٢٠٠١م في بودابست بمناسبة المؤتمر الدولي عن جرائم الكمبيوتر، ودخلت حيز التنفيذ في ١ يوليو عام ٢٠٠٤م، وتعرف باتفاقية بودابست ٢٠٠١م (اتفاقية الجرائم الإلكترونية - اتفاقية ساير كرايم - اتفاقية الإجرام الكوني)، ويمكن لأية دولة في العالم الانضمام للاتفاقية إذا رغبت ذلك، وباعتبارها وثيقة قيمة استخدمتها الكثير من البلدان.

وأما ما يتعلق بجرائم الخصوصية أو بشكل أدق الجرائم التي تستهدف البيانات الشخصية في مراحل الجمع والمعالجة والاستخدام، والنقل، فإن الإطار العام للنصوص الموضوعية لم يميز نوعية المعطيات، عما إذا كانت بيانات تتصل بالشخص أو بمصالح اقتصادية، أو مالية، أو مسائل أمنية، أو غير ذلك، ولعل مرد هذا الاتجاه السعي لتعميم حماية المعطيات بكافة أنواعها، إضافة إلى أن مسائل حماية البيانات الاسمية - كما أسلفنا - تحظى بتنظيم تشريعي قائم بل وأكثر تميزاً عن التنظيم التشريعي لجرائم الكمبيوتر؛ إذ يغطي هذا الموضوع بالاتفاقية الأوروبية لحماية البيانات الشخصية، وبقائمة طويلة من التشريعات الوطنية والأدلة الإرشادية في نطاق أوروبا الموحدة.

4. الأمم المتحدة (United Nation)

في عام ١٩٨٩م تبنت الأمم المتحدة دليلاً يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية، وبتاريخ ١٤ / ١٢ / ١٩٩٠م تبنت الهيئة العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية، ويتضمن هذا الدليل ذات 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 الحقل، وقد بذلت العديد من الجهود لحماية الخصوصية من قبل لجنة حقوق الإنسان في المجلس الاقتصادي والاجتماعي في الأمم المتحدة، ومن قبل الجمعية العامة للأمم المتحدة. وأهم قرارات الجمعية العامة للأمم المتحدة بشأن الخصوصية المعلوماتية هي:

1. قرار الجمعية العامة للأمم المتحدة بشأن حقوق الإنسان والتطور العلمي والتكنولوجي رقم 2450 لسنة 1986.

2. قرار الجمعية العامة رقم 3304 لعام 1975م.

3. قرار الجمعية العامة رقم 45 / 95 لعام 1990م.

5. مجموعة الدول السبع لاحقا مجموعة الثمانية (G8)

تعتبر مجموعة دول الثماني G8 مهمة بمسألة التعاون الدولي في مكافحة جرائم الإنترنت. ولقد أطلقت مجموعة الدول السبع مجموعة توصيات لحماية الخصوصية ضمن مؤتمرها الذي عقد حول مجتمع المعلومات في عام ١٩٩٥م.

وخلال اجتماع عقد يومي التاسع والعاشر من ديسمبر ١٩٩٧م، اعتمد وزراء العدل والشئون الداخلية لدول مجموعة الثمانية المبادئ التي تشكل الأساس لشبكة نقاط اتصال وطنية. وبجانب هذه المبادئ، تم وضع خطة عمل لإنشاء شبكة متابعة لتقديم تقارير بشأن مدى التزام الدول الأعضاء في الشبكة، وقد أنشئت الشبكة على غرار نموذج الإنترنت في الفترة ما بين عامي 1998 و 2000م ، وتتواصل الجهود من أجل زيادة عدد الدول المشاركة.

وقد نشأت فكرة إنشاء شبكة مجموعة الثمانية في الأساس، لمواجهة الحاجة الملحة للتعامل على مستوى عال من المهارة، مع مختلف الجرائم المتعلقة بالتكنولوجيا فائقة التطور. وثمة تأكيد على أهمية الحفاظ على الأدلة الموجودة في الوسائط التي تكون فيها المعلومة عرضة للضياع أو التلف بشكل سريع. والفرصة متاحة أمام الدول غير الأعضاء في شبكة المعلومات التابعة لمجموعة الثمانية للانضمام إليها.

سادسا : منظمة التجارة العالمية:

(World Trade Organization- WTO)

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

• المراجع :

د. أسماء رويحي، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراة، جامعة القاهرة، سنة 2013.

تم بحمد الله الإنتهاء من شرح المحاضرة التاسعة

مع تمنياتي بالتوفيق د. أسماء رويحي