

المحاضرة العاشرة

المؤتمرات الدولية والمحلية

والحماية الدستورية والجنائية والإدارية

للحق في الخصوصية المعلوماتية

• عناصر المحاضرة:

المحور الأول : المؤتمرات الدولية والمحلية لحماية الحق في الخصوصية المعلوماتية:

أولاً: المؤتمرات الدولية لحماية الخصوصية المعلوماتية.

1. المؤتمر الدولي لحقوق الإنسان المنعقد في طهران.

2. مؤتمر مونتريال.

3. موقف مؤتمر اليونسكو من أخطار الخصوصية المعلوماتية.

4. المؤتمر الدولي السابع للمركز الدولي للدراسات والبحوث الاجتماعية والجنائية والإصلاحية.

5. المؤتمر الدولي لأمن المعلومات الإلكترونية.

ثانياً : المؤتمرات المحلية لحماية الخصوصية المعلوماتية:

- موقف مؤتمر دول الشمال في استوكهولم من حماية الخصوصية المعلوماتية.

المحور الثاني: الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية:

أولاً: الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية في البيئة الغربية:

1. النماذج الدستورية في حقل حماية الحق في الخصوصية المعلوماتية وذلك على النحو التالي:

2. الأنماط والنماذج القانونية في حقل حماية الخصوصية المعلوماتية :

3. ماهية الأوصاف العامة لتشريعات حماية الخصوصية المعلوماتية :

4. التشريعات القانونية في حقل حماية الحق في الخصوصية المعلوماتية في الدول الغربية:

ثانياً: الحماية التشريعية للحق في الخصوصية المعلوماتية في البيئة العربية:

المحور الثالث : الحماية الإدارية للحق في الخصوصية المعلوماتية :

لقد اختلف القانون المقارن حول إنشاء جهة إدارية متخصصة للإشراف والرقابة علي تطبيق قانون الخصوصية المعلوماتية اختلافاً بيناً:

1. ترك الرقابة للقواعد العامة دون حاجة لجهة خاصة.
2. مفوض نظم المعلومات.
3. جهاز أو لجنة للإشراف والرقابة.

المحور الأول

المؤتمرات الدولية والمحلية لحماية الحق في الخصوصية المعلوماتية

انعقدت عدة مؤتمرات دولية لتداول موضوع الحق في الخصوصية المعلوماتية، وأصدرت عدة توصيات تتعلق بحماية هذا الحق. إلا أننا سوف نركز علي أهم هذه المؤتمرات. وهذه المؤتمرات إما مؤتمرات ذات صبغة دولية، وإما مؤتمرات ذات صبغة إقليمية أو محلية، وذلك علي النحو التالي:

- أولاً: المؤتمرات الدولية لحماية الخصوصية المعلوماتية.
- ثانياً: المؤتمرات المحلية لحماية الخصوصية المعلوماتية.

أولاً: المؤتمرات الدولية لحماية الخصوصية المعلوماتية:

عقدت مجموعة من المؤتمرات علي المستوي الدولي عنيت بدراسة الخصوصية المعلوماتية، ومن أهمها:

1. المؤتمر الدولي لحقوق الإنسان المنعقد في طهران.
2. مؤتمر مونتريال.
3. موقف مؤتمر اليونسكو من أخطار الخصوصية المعلوماتية.
4. المؤتمر الدولي السابع للمركز الدولي للدراسات والبحوث الاجتماعية و الجنائية و الإصلاحية.
5. المؤتمر الدولي لأمن المعلومات الإلكترونية.
6. المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت.
7. المؤتمرات الدولية لمفوضي الخصوصية وحماية البيانات. وذلك على النحو التالي:

1. المؤتمر الدولي لحقوق الإنسان المنعقد في طهران:

قد أُنْعِد هذا المؤتمر في طهران في الفترة الممتدة من ٢٢ نيسان/أبريل إلى ١٣ أيار / مايو ١٩٦٨ م - بمقتضي القرار الصادر من الجمعية العامة رقم (٢٠٨١) الصادر في ديسمبر سنة ١٩٦٥ م ، وذلك كجزء من البرنامج العام الدولي لحقوق الإنسان لسنة ١٩٦٨ م.

أ. قرارات المؤتمر :

هذا وقد اتخذ المؤتمر مجموعة من القرارات الرئيسية تناولت مختلف نواحي حقوق الإنسان، وبعيننا منها القرار الثامن عشر، وهو القرار الذي يهدف إلى حماية حق الإنسان في الخصوصية ولا سيما بعد زيادة الأخطار الناجمة بسبب التقدم العلمي والتكنولوجي.

ونص القرار علي (وأن الحديث عن المكتشفات العلمية وخطوات التقدم التكنولوجي، علي رغم كونه قد فتح آفاقا واسعة للتقدم الاقتصادي، والاجتماعي والثقافي يمكن أن يعرض للخطر حقوق الأفراد وحررياتهم، وبالتالي سيكون من الضروري أن يجعل محل انتباه متواصل).

ب. توصيات المؤتمر:

وقد أوصي المؤتمر بدراسة المشكلات المتصلة بحقوق الإنسان والناشئة عن التطورات العلمية والتكنولوجية، ولا سيما في النواحي التالية:

1. احترام خصوصية الإنسان علي ضوء الإنجازات المحققة في تقنيات التسجيل.
2. حماية الشخص وسلامته البدنية والعقلية في ضوء الإنجازات المتحققة في علم الأحياء و الطب، والكيمياء الحيوية.
3. الاستخدامات المتصلة بالإلكترونيات والتي قد تمس حقوق الشخص، والقيود التي يجب أن تفرض علي استخداماتها.
4. وبصفة عامة ينبغي إقامة التوازن بين التقدم العلمي والتكنولوجي وبين رقي الإنسانية الفكري، والثقافي، والأخلاقي.

ج. مدي القوة الإلزامية لقرارات هذا المؤتمر :

علي الرغم من أن القرارات التي صدرت عن المؤتمر والتوصيات التي تمخضت عنه إلا أن هذه التوصيات ليست لها أي قوة إلزامية تجاه الدول المشاركة في هذا المؤتمر ؛ حيث إن هذه التوصيات ذات قيمة أدبية فقط وبالتالي لا يوجد إلزام علي الدول بتنفيذ هذه التوصيات.

2. مؤتمر مونتريال

انعقد المؤتمر الدولي لحقوق الإنسان في مونتريال بكندا سنة ١٩٦٨ م . وقد تم في هذا المؤتمر بحث الآثار السلبية للتكنولوجيا الحديثة على الخصوصية للأشخاص، وقد وجه عنايته إلى الأخطار التي نشأت بسبب التطورات الحديثة.

• توصيات المؤتمر :

صدرت عن هذا المؤتمر عدة توصيات منها مكافحة الأضرار التي تحدثها الأجهزة الإلكترونية ووسائل الاتصال السمعية والبصرية بحق الإنسان في الخصوصية .

كما أوصي المؤتمر بضرورة اهتمام الهيئات غير الحكومية، والهيئات الحكومية، والمهنة القانونية وقيامها بدور فعال لدرء الخطر عن طريق رفض الاعتراف بالأدلة المتحصلة بالوسائل العلمية والتكنولوجية الحديثة، مثل استعمال الكمبيوتر والإنترنت للتصوير الخفي العالي في الدقة

3. موقف مؤتمر اليونسكو من أخطار الجرائم التي تمس الخصوصية المعلوماتية:

لقد كانت الحاسبات الإلكترونية محور النقاش في هذا المؤتمر، إذ اتفق الرأي على إن استخدام الحاسبات الإلكترونية يهدد الخصوصية إذا أسئ استخدامها لما لها من قدرة فائقة علي تخزين أكبر قدر من البيانات واسترجاعها في أقصر وقت ممكن وتلم بقدر عظيم من المعلومات، وهذه المعلومات تتجمع من مصادر مختلفة وتخزن في مكان واحد. وأن تكنولوجيا الكمبيوتر يمكن أن تستخدم في المستقبل لتزويد الحكومة أو قطاع الأعمال بقدر كبير من المعلومات عن الأفراد ، وبشكل يفوق هو متاح في الوقت الحاضر، مما يهدد الخصوصية للأفراد، ويفرض وجود ضرورة وسائل له للرقابة علي تخزين البيانات وتحدد ما هو الذي يجوز اختزاله منها ، ومن حق تداولها، وكذلك تحديد أغراض التداول، وإقرار حق الأفراد في الوصول إليها، والاطلاع عليها وتصحيحها كلما دعا الأمر إلى ذلك .

ويجب العمل علي تقرير الحماية الكافية والضمانات الفعالة لصيانة الحق في الخصوصية من تدخل السلطة العامة في الدولة، والآثار السلبية للتقدم العلمي، الانتهاكات الصادرة من فئة الموظفين الإداريين الحكوميين؛ فهؤلاء يتعدد أوجه انتهاكهم لخصوصيات الناس.

واهتم الاجتماع بحق الأفراد في مناقشة البيانات التي تسجل ملفاتهم، والاطلاع عليها وتحديد وسائل تمكن الطعن عليها.

4. المؤتمر الدولي السابع للمركز الدولي للدراسات والبحوث الاجتماعية و الجنائية و الإصلاحية

عقد هذا المؤتمر في مدينة مدريد بأسبانيا في الفترة من 3 إلى 13 أكتوبر ١٩٨٤ م ، وشاركت فيه وفود ثمان وثلاثين دولة، بالإضافة إلى الأمم المتحدة ومنظمة الشرطة الجنائية الدولية (الإنتربول) ، والمجلس الأوروبي، وبعض المنظمات الدولية المتخصصة. ونظم المركز الدولي للدراسات والبحوث الاجتماعية والجنائية والإسلامية هذا المؤتمر، وكان موضوعه هو " إعداد وتأهيل رجل الشرطة للتحري عن الحقائق القانونية ولحماية حقوق الإنسان ".

• توصيات المؤتمر:

وقد أصدر المؤتمر توصيات عديدة في مجال عمل الشرطة و حقوق الإنسان، شملت توصية تتعلق بحماية الحق في الخصوصية المعلوماتية تنص علي: (يجب أن يكون استخدام الأساليب الفنية الحديثة في مراقبة الأفراد بالوسائل السمعية والبصرية بالقدر الضروري وبالطرق المشروعة لما يترتب عليها من انتهاك الخصوصية) .

5. المؤتمر الدولي لأمن المعلومات الإلكترونية

عقد هذا المؤتمر في العاصمة العمانية مسقط، من ١٨ إلى ٢٠ ديسمبر ٢٠٠٥ . ويبحث المشاركون في هذا المؤتمر عدة محاور، أبرزها مستقبل أمن المعلومات والجيل الجديد من التهديدات الإلكترونية، والعقبات المترتبة عليها، والمخاطر الأمنية المعلوماتية وتهديدها لاقتصاديات وخطط وبرامج التنمية الوطنية، وتأهيل القدرات البشرية ومواجهة المخاطر الإلكترونية، والخسائر المترتبة على الهجمات الإلكترونية والتعاون الدولي للحد من تنامي الجرائم السيبرانية.

ومن توصيات المشاركين في المؤتمر التأكد علي ضرورة تبني سياسة مشتركة تحقق أمنا معلوماتيا، للقضاء علي الآثار السلبية التي تهدد البيانات الشخصية بالفناء، والعمل على وضع تشريع متكامل لحماية البيانات والخصوصية علي الإنترنت لاسيما في ظل الانتشار والاستخدام اللامتناهي للشبكة العنكبوتية في شتي المجالات .

6. المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت

عقدت الجمعية الدولية لمكافحة الإجرام السيبري بفرنسا بالتعاون مع الجمعية المصرية لمكافحة الجرائم المعلوماتية والإنترنت هذا المؤتمر بفندق شيراتون بمدينة القاهرة مصر من ٢ - ٤ يونيو ٢٠٠٨ م .

لقد تناول هذا المؤتمر مناقشة العديد من الموضوعات المرتبطة بالاستخدام غير المشروع لتقنية المعلومات والإنترنت، مثل الحماية المتداولة عبر الإنترنت والتجارة الإلكترونية، ونظم الدفع الإلكتروني، والجريمة الإلكترونية، والدليل الرقمي .

وقد انتهى هذا المؤتمر إلى التوصية بالإسراع بالانضمام إلى اتفاقية مكافحة الجرائم المعلوماتية "بودابست"، وتبادل الخبرات، والتجارب الدولية بين الدول بعضها ببعض؛ لعرض النظم القانونية والتقنية لأمن المعلومات، وحث المشرع على الإسراع في إصدار تشريعات حول الخصوصية وأمن المعلومات، والعقوبات الرادعة لارتكاب مثل هذه الأفعال غير المشروعة، وضرورة تبني مفاهيم حديثة في مجال حكومة تقنية المعلومات باعتبارها آلية لحماية الخصوصية وأمن المعلومات.

7. المؤتمرات الدولية لمفوضي الخصوصية وحماية البيانات :

ومن أهم هذه المؤتمرات في الخصوصية المعلوماتية مايلي :

أ. المؤتمر الدولي السابع والعشرون لمفوضي الخصوصية وحماية البيانات:

عقد هذا المؤتمر في مدينة مونتريو Montreux بسويسرا من ١٤ - ١٦ سبتمبر ٢٠٠٥م، وأوصى المؤتمر بضرورة التقليل من حجم البيانات الشخصية التي يتم جمعها في إطار الاتصالات السياسية، وخصوصا تلك التي تتعلق بالحملات الانتخابية، احتراماً لحقوق الفرد، وأيضاً حقه في حماية بياناته الشخصية وعدم العبث بها. وكما أوصى بعدم معالجة البيانات الاسمية إلا عندما يكون ذلك ضرورياً لتحقيق الأغراض التي جمعت من أجلها، وأن تستخدم لفترة مؤقتة .

ب. المؤتمر الدولي الثامن والعشرون لمفوضي الخصوصية وحماية البيانات:

عقد هذا المؤتمر في مدينة لندن بالمملكة المتحدة من ٢ - ٣ نوفمبر ٢٠٠٦ م. وأكد هذا المؤتمر على خطورة محركات البحث على الحق في الخصوصية المعلوماتية، وعلى أثر ذلك أوصى المؤتمر بضرورة أن يقوم مقدمو محركات البحث بإعلام المستخدمين مسبقاً وبطريقة واضحة وسهلة بكيفية معالجة البيانات الشخصية الخاصة بهم، وبكيفية استخدامها عند استخدام محركات البحث، وعدم السماح لمقدمي محركات البحث بالاحتفاظ بالبيانات بعد انتهاء جلسة البحث دون الموافقة الصريحة والمسبقة من المستخدم .

كما أوصى بضرورة التقليل من البيانات التي يضعها المستخدم في محركات البحث علي اعتبار أن التقليل من كمية تلك البيانات يعد الحل الوحيد والأنسب لحماية الخصوصية في ظل الوضع الحالي لمحركات البحث.

ج. المؤتمر الدولي التاسع والعشرون لمفوضي الخصوصية وحماية البيانات:

انعقد هذا المؤتمر في مدينة منتريال بكندا في الفترة من ٢٥ - ٢٨ سبتمبر ٢٠٠٧م، وتناول هذا المؤتمر مدي مشروعية قيام الحكومات الدول بأخذ البيانات الشخصية المعالجة آليا والخاصة بالمسافرين عبر وسائل النقل وحفظها، وذلك لأغراض مكافحة الإرهاب والمحافظة علي الأمن القومي. وأوصى المؤتمر بضرورة أن تقوم السلطات بإثبات أن استخدام هذه البيانات الشخصية للمسافرين كان ضروريا لمعالجة مشكلة معينة .

د. المؤتمر الدولي الثلاثون لمفوضي الخصوصية وحماية البيانات:

انعقد هذا المؤتمر في بفرنسا في الفترة من ١٥ - ١٧ أكتوبر ٢٠٠٨م، وإن الغرض من إقامة هذا المؤتمر، توعية الناس من مخاطر استخدام بعض مواقع الانترنت علي الحياة الخاصة بحيث صار من السهل اختراقها من جراء استخدام بعض المواقع، كما اهتم المؤتمر بكيفية حماية الخصوصية المعلوماتية.

وأوصى هذا المؤتمر بضرورة العمل علي حماية الخصوصية عند استخدام الإنترنت، وذلك من خلال توعية الأفراد وتثقيفهم بكيفية الاستخدام الأمثل لهذه الشبكة، بشكل يقلل من مخاطر استخدامها على حياتهم الخاصة.

هـ. مؤتمر مفوضي الخصوصية وحماية البيانات الأوروبي :

وتناول هذا المؤتمر مخاطر التقدم العلمي والتقني علي الخصوصية، ودعا المؤتمر جميع المشاركين إلى الاستمرار في العمل علي تعزيز حماية الخصوصية والمعلوماتية وفقا لمتطلبات العصر والقوانين المنظمة لحماية البيانات الشخصية المعالجة آليا والتركيز علي أوجه التشابه بين الأنظمة القانونية المختلفة، والبحث عن حلول عالمية لحماية البيانات الاسمية المعالجة إلكترونيا.

و. المؤتمر الدولي الثاني والثلاثون لمفوضي الخصوصية وحماية البيانات:

وأوصى هذا المؤتمر بوجوب الانضمام إلى الاتفاقية الأوروبية لحماية الأفراد من مخاطر المعالجة الآلية للبيانات والبروتوكول الإضافي الملحق بها، وتشجيع المنظمات الدولية والمحلية ومنظمات المجتمع المدني المهتمة بالحياة الخاصة وحماية البيانات لدعم الدعوة إلي مؤتمر حكومي دولي لمناقشة مخاطر التقدم العلمي على البيانات الشخصية المعالجة إلكترونيا.

ر. المؤتمر الدولي الثالث والثلاثون لمفوضي الخصوصية وحماية البيانات :

ومن الموضوعات التي تناولها هذا المؤتمر هي كيفية حماية البيانات الشخصية في زمن الكوارث الطبيعية أو غير الطبيعية.

ثانيا : المؤتمرات المحلية لحماية الخصوصية المعلوماتية:

ومما يعكس أهمية الحق في الخصوصية المعلوماتية علي المستوى المحلي أو الإقليمي تبني هذا الحق مؤتمر دول الشمال في استوكهلم، وذلك علي النحو الآتي:

• موقف مؤتمر دول الشمال في استوكهلم من حماية الخصوصية المعلوماتية :

نبه المؤتمر على ضرورة إعادة النظر في التشريعات الجنائية والمدنية التقليدية لحماية الفرد من التعدي على الخصوصية، بعد أن اتسع نطاق انتهاك الخصوصية نتيجة للتطور العلمي والتكنولوجي، الأمر الذي يستلزم تشريعات ملائمة لما حدث من تطورات علمية وتكنولوجية في وسائل الاتصال والتنصت وغيرها من الوسائل العلمية التي تهدد حرمة الخصوصية، وذلك لتحقيق حماية أكثر فاعلية لهذا الحق .

ولقد جرمت استخدام وسائل التنصت الإلكترونية الدقيقة، والأجهزة الإلكترونية مثل الكمبيوتر والإنترنت، التي تستخدم للحصول على المعلومات أو التسجيلات أو الصور بطريقة غير المشروعة، وفي هذه الحالة تنعدم القيمة القانونية لهم .

وخلاصة القول وبالعوموم يمكننا القول بإيجاز إن مفهوم حماية البيانات أو المعلومات الشخصية في المواثيق المتقدمة تتطلب أن تكون :-

1. قد تم الحصول عليها بطريق مشروع وقانوني.
2. تستخدم للغرض الأصلي المعلن والمحدد، ولا تكشف لغير المصرح لهم بالاطلاع عليها.
3. تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك .
4. صحيحة وتخضع لعمليات التحديث والتصحيح .
5. يتوفر حق الوصول إليها مع حق الإخطار بأنشطة المعالجة، أو النقل وحق التصحيح والتعديل وحتى طلب الإلغاء.
6. تحفظ سرية، وتحمي سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المعالجة.

7. تتلف عند استنفاد الغرض من جمعها.

ورأينا فيما سبق كيف كانت الحماية الدولية للحق في الخصوصية بصفه عامه، وكذلك رأينا الاتفاقيات والمؤتمرات التي نصت على ضرورة حماية الخصوصية المعلوماتية - أيضا - بصفة خاصة ، وعلى الرغم من ذلك ستظل هذه القضية حية ومتجددة تثير الفقهاء والباحثين، وذلك بسبب التطور التكنولوجي للوسائل المستخدمة في الجريمة السيبرانية التي تهدد باستمرار انتهاك الخصوصية عن طريق الكمبيوتر والإنترنت مما أدى لاستخدامهما كوسيلة للمراقبة السمعية والبصرية، ولكن بطرق حديثة سهلة وبسيطة وغير مكلفة عن الطرق التقليدية.

المحور الثاني

الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية

• تمهيد وتقسيم:

تظهر أهمية مشكلة الجرائم السيبرانية التي تنتهك الخصوصية في تحقيق التوازن الضروري بين مصلحة المجتمع عامة، في الاستعانة بالتكنولوجيا الحديثة وما أفرزته الثورة الرقمية، وبين مصلحة الإنسان في حماية الخصوصية المعلوماتية وعدم انتهاك أسراراه . وذلك سوف نستعرض الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية وذلك على النحو التالي:

أولا: الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية في البيئة الغربية:

ثانيا: الحماية التشريعية للحق في الخصوصية المعلوماتية في البيئة العربية:

أولا: الحماية الدستورية والجنائية للحق في الخصوصية المعلوماتية في البيئة الغربية:

لم تسلك الدول الغربية - في الأنظمة القانونية المختلفة - مسلكا موحدا لحماية الحق في الخصوصية المعلوماتية، بل تباينت مواقفها في هذا الشأن .

ويمكننا القول إن كافة دول العالم على وجه التقريب أقرت بشكل أو بآخر الحق في الخصوصية في واحد أو أكثر من مظاهره، وهذا لا يعني توافر حماية كافية، أو شمولية في الحماية لدى كافة الدول، وفي الوقت الذي قد نجد فيه حماية الخصوصية بمفهومها المادي أكثر شيوعا واتساعا، تضيق حماية خصوصية المعلومات وفي ذات الوقت نجدها الشغل الشاغل في الوقت الحاضر للمؤسسات التشريعية ومؤسسات القرار في العديد من دول العالم .

1. النماذج الدستورية في حقل حماية الحق في الخصوصية المعلوماتية وذلك على النحو التالي:

- أسبانيا:

نص دستورها في 9 ديسمبر سنة ١٩٧٨ م والمعدل في ٢٧ أغسطس ١٩٩٢ م:
المادة ١٨:

١. يتم ضمان الحق في الشرف وحرمة الحياة الخاصة والأسرية والحق في السمعة الذاتية.
٢. لا يمكن التعدي على المسكن لا يمكن دخول أي مسكن أو تفتيشه دون الحصول على موافقة صاحبه أو دون أمر قضائي، باستثناء حالة التلبس في الجريمة.
٣. يتم ضمان سرية الاتصالات وبوجه خاص الاتصالات البريدية، والتلغرافية واتصالات الهاتف باستثناء أن يصدر حكم قضائي.
٤. يعين القانون حالات الحد من استخدام تكنولوجيا المعلومات من أجل ضمان الشرف وحرمة الحياة الخاصة والأسرية والممارسة الكاملة لحقوقهم.

- البرازيل:

يقر الدستور البرازيلي بأن الخصوصية حق أساسي من حقوق الإنسان الأساسية، حتى أن الدولة لا يسمح لها بانتهاك البيانات الشخصية، العلاقات الحميمة، الحياة الخاصة، الشرف والسمعة (المادة 5، البند اكس). وفي الحالات القصوى يمكن لأمر قضائي إجازة بعض الكشف، ولكن حتى بعض المعلومات مثل المراسلات تبقى ذات حرمة مطلقة ولا يمكن حتى لأمر قضائي بالسماح للكشف عنها.

- البرتغال:

نص دستورها في ٢ أبريل سنة ١٩٧٦ م:

في المادة ٣٥: (استخدام الحاسب الآلي):

1. لكل المواطنين الحق في معرفة المعلومات التي تتعلق بهم، وما تتضمنه بنوك المعلومات من بيانات خاصة بهم والاستخدامات المعدة لها، ويكون لهم طلب تصحيحها أو تحديثها.
2. يحدد القانون مفهوم البيانات الشخصية، بما يتوافق مع الشروط والأحكام التي تنطبق على كيفية معالجتها إلكترونياً ونقلها واستخدامها وضمان حمايتها ولا سيما عن طريق هيئة إدارية مستقلة.
3. لا يجوز استخدام الحاسبات الإلكترونية في معالجة البيانات التي تتعلق بالاتجاهات السياسية، أو الانتماءات النقابية، أو المعتقدات الدينية، أو العرقية للحياة الخاصة إلا بموافقة صريحة، أو لغرض معالجة البيانات الإحصائية التي لا يمكن تحديدها بشكل فردي.

4. يحظر على طرف ثالث الوصول إلى البيانات الشخصية، إلا في حالات استثنائية ينص عليها القانون.
5. كما منع المشرع الدستوري في هذه الفقرة الخامسة إعطاء المواطن رقما قوميا .
6. حرية الوصول والاستخدام إلى شبكات الكمبيوتر مكفولة، ويحدد القانون القواعد التي علي حد سواء تنطبق علي تدفق المعلومات عبر الحدود والوسائل المناسبة لحماية البيانات الشخصية .
7. تتمتع البيانات الشخصية المسجلة يدويا بنفس الحماية الواردة في الفقرات السابقة من هذه المادة.

- الدنمارك:

المادة ٧٢ من دستور ١٩٥٣ والمتعلقة بخصوصية المكان والاتصالات .

- سويسرا:

نص الدستور الفيدرالي الجديد (١ / ١ / ٢٠٠٠) في المادة (13 / 2) منه، لكل شخص لديه الحق في الحماية ضد إساءة استخدام البيانات الشخصية .

2. الأنماط والنماذج القانونية في حقل حماية الخصوصية المعلوماتية :

وقد شهدت الستينيات انطلاق الاهتمام بحماية الخصوصية من مخاطر التكنولوجيات الحديثة، لينطلق معه مفهوم حماية المعلومات الخاصة من مخاطر التقنية، ومنذ مطلع السبعينيات بدأت دول العالم تتبنى قوانين حماية الخصوصية المعلوماتية، إما عن طريق القوانين الشمولية التي تعترف بالحق وتقر المبادئ الأساسية وتقدم الإطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات، أو حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة (المعلومات الشخصية)، أو عن طريق حزمة قوانين قطاعية تتعلق بالبيانات في قطاعات معينة، كالبيانات الصحية، أو المالية، أو بيانات الأحوال المدنية أو غيرها إلى جانب مدونات سلوك تحكم قطاعات معينة كقطاعات الصناعة أو الخدمات التقنية فيما يعرف بوسيلة التنظيم القانوني الذاتي للقطاعات أو السوق .

وبناء علي ما سبق هناك ثلاثة أنماط تشريعية لتدابير حماية الخصوصية المعلوماتية، وهذه التدابير تعتمد في تطبيقاتها على ما إذا كان منطلق النظام القانوني مجرد الاعتراف بالخصوصية معتمدا على عدم إباحة كل ما يدخل في نطاق الحق، أو باستخدام وسيلة مواجهة الأنشطة التي تمثل اعتداء على الخصوصية وفي كثير من الدول يستخدم الاتجاهان معا، وبالنسبة للدول التي توفر حماية فاعلة للخصوصية فإنها قد تستخدم نموذجا أو أكثر لضمان حماية الخصوصية وهذه النماذج هي : .

أ. القوانين الشاملة Comprehensive Laws:

في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع، وإدارة ومعالجة البيانات الشخصية في القطاعين العام والخاص، مع وجود جهة لضمان التوافق مع القانون وتطبيقه، وهذا هو النموذج الشائع في الدول التي تتبنى قوانين حماية المعلوماتية كما هو حال دول الاتحاد الأوروبي، وهي الدول المتعين عليها التوافق مع دليل حماية البيانات الإرشادي الصادر عن الاتحاد الأوروبي. وقد تم وضع العديد من مثل هذه القوانين في دول خارج الاتحاد الأوروبي - أيضا - كما هو الحال في كندا، وأستراليا.

- الغرض من تبني تشريعات شاملة لحماية الخصوصية المعلوماتية :

هناك أسباب رئيسية ثلاثة للتوجه نحو اعتماد نموذج التشريع الشامل للخصوصية وحماية المعلوماتية والدول بشكل عام بنت هذه القوانين لسبب أو أكثر من بين هذه الأسباب الثلاثة:

أ. تجاوز ومعالجة الانتهاكات السابقة، فالكثير من الدول وتحديدا في وسط أوروبا وأمريكا الجنوبية وجنوب أفريقيا تبنت مثل هذه القوانين؛ لمعالجة الاعتداءات التي مارسها السلطات السابقة على الحق في الخصوصية المعلوماتية ضمن واقع غياب احترام حقوق الإنسان عموما .

ب. تشجيع التجارة الإلكترونية وتنظيمها، فالكثير من الدول، وخاصة في آسيا، وضعت مثل هذه القوانين بغرض تشجيع التجارة الإلكترونية منطلقا من أن المستهلكين لن يقدموا على التجارة الإلكترونية في ظل خشيتهم على بياناتهم الخاصة، وقد سنت تشريعات الخصوصية المعلوماتية كجزء من حزمة تشريعات تهدف إلى تسهيل التجارة الإلكترونية من خلال مجموعة قواعد موحدة.

ت. **التأكد من أن القوانين تتلاءم مع المعايير الأوروبية**، فغالبية الدول في وسط وشرق أوروبا تبنت قوانين الخصوصية المعلوماتية مستندة إلى اتفاقية مجلس أوروبا، ودليل حماية البيانات المقرر من قبل الاتحاد الأوروبي، إذ إن غالبية هذه الدول ترغب بالانضمام للاتحاد الأوروبي في المستقبل، وتعلم أن ذلك يتطلب الانسجام مع ما يقرره الاتحاد والبرلمان الأوروبيين من قوانين وكذلك فإن عددا من الدول خارج أوروبا تبنت مثل هذه القوانين؛ لأن المعايير الأوروبية تمنع تبادل البيانات خارج الحدود مع دول لا تحمي الخصوصية المعلوماتية، أو لرغبة بعض الدول التي لها مصالح مباشرة مع الدول الأوروبية للانسجام مع الأنظمة القانونية الأوروبية، كما هو الحال بالنسبة لكندا وأستراليا .

ب. القوانين القطاعية المخصصة : Sectoral Laws :

وهي التي تتعلق بقطاع معين، إذ أن بعض الدول، كما هو الحال في الولايات المتحدة الأمريكية، تجنبت سن تشريع عام لحماية الخصوصية المعلوماتية، وفضلت إصدار قوانين معينة تحكم قطاعات بعينها، كما هو الحال بسجلات تأجير الفيديو ، والخصوصية المالية، وحماية خصوصية الأطفال علي الخط العام وغيرها، وفي مثل هذه الحالة فإن إنفاذ القواعد القانونية يتحقق من خلال آليات مختلفة، وليس كما هو الحال بالنسبة للقانون الشامل الذي ينشئ جهة رقابة عامة.

ويؤخذ على هذا النموذج أنه يتطلب أن تسن تشريعات جديدة كلما نشأت تقنيات جديدة، ولهذا فإن الحماية تظل متخلفة عن تقنيات الاعتداء، إضافة إلى مشكلة عدم وجود الجهة الحكومية المشرفة.

ث. التنظيم الذاتي Self - Regulation :

ابتداء لابد من الإشارة إلى أن موضوع التنظيم الذاتي موقوف بشأن موضوعات تقنيات المعلومات عموما وهو النقيض لما يعرف بالتدخل التشريعي لتنظيم موضوعات تقنية المعلومات، ولكل اتجاه مؤيدوه ومعارضوه، إيجابياته وسلبياته، وبالعموم يمكننا القول إن النموذج الأمريكي للتعامل مع تقنية المعلومات دعا إلى مزيد من تبني فكرة التنظيم الذاتي في حقول التجارة الإلكترونية، ومعايير الخدمات التقنية، وحماية البيانات، وأمن المعلومات وغيرها، مع أنه ليس كذلك في حقل الملكية الفكرية مثلا.

أما الاتحاد الأوروبي، فإنه يتجه نحو التنظيم الحكومي أكثر، لهذا نجد أن منظماته قد اتجهت دائما إلى توجيه الدول الاعضاء إلى إصدار تشريعات تتلاءم مع القواعد المقررة في الأدلة الإرشادية والتوجيهية الصادرة عن منظماته، كمجلس أوروبا واللجنة الأوروبية والاتحاد الأوروبي، بل إتجه إلى التنظيم التشريعي الشامل عبر قوانين البرلمان الأوروبي .

بين هذين الرأيين **ثمة منطقة رمادية** تؤمن بترك كثير من المسائل للتنظيم الذاتي للسوق وجهات الصناعة والإنتاج، لكنها في الوقت ذاته تتدخل لتنظيم مسائل أخرى، وطبعا كل ذلك وفق الظروف الخاصة بالدولة، وتبعا للموضوع محل التنظيم والاستراتيجية الوطنية بشأنه، فإذا كانت أمريكا مثلا تترك مسألة المعايير والمواصفات التقنية للتنظيم الذاتي للسوق، فإن هذا الأمر مبرر لما يتوافر من قواعد واسعة في حقل منع التنافس غير المشروع، وحقل منع الاحتكار وحماية المستهلك وقواعد منع الغش، في أن دولا نامية، أو حتى متقدمة لا يتوافر لها مثل هذا الإطار ، لا يكون قرارها بترك تنظيم المعايير للسوق، بل يتعين التدخل من اجل حماية المستهلك وضمان سلامة الخدمات التقنية الموجهة إليه.

3. ماهية الأوصاف العامة لتشريعات حماية الخصوصية المعلوماتية :

مسماها الشائع	قوانين الخصوصية Privacy أو قوانين حماية المعطيات Data Protection laws أو قانون الحريات أو قوانين الخصوصية المعلوماتية أو قانون الخصوصية وحماية البيانات، أو قوانين حماية البيانات الشخصية.
وصفها العام	تشريعات حماية الخصوصية من مخاطر المعالجة الإلكترونية للبيانات الشخصية.
مبرر وجودها	هذه التشريعات جاءت كرد فعل للتحديات التي واجهتها الخصوصية بسبب مخاطر المعالجة الآلية للبيانات الشخصية وازدياد أنشطة جمع (Collecting)، وتخزين (Storing)، وتبادل ونقل البيانات (Transmitting data) بالتقنيات الحديثة .
هدفها ونطاقها	سنت هذه القوانين لحماية حق المواطنين في الخصوصية المعلوماتية، وحماية بياناتهم الخاصة، وأسرارهم ضمن قواعد إدارية، ومدنية، وجنائية.
الحقبة الزمنية لانطلاقها	في عام ١٩٦٨م وعلى أثر عقد مؤتمر الأمم المتحدة (طهران) لحقوق الإنسان ومناقشة موضوع مخاطر تكنولوجيا المعلومات على الحق في الخصوصية ظهرت هذه التشريعات كأول موجة تشريعية وقد إنطلقت خلال السبعينيات والثمانينيات. وخضعت لتعديلات متتالية خلال الثمانينيات والتسعينيات.
الفرع القانوني ذو العلاقة	تدخل الجرائم الخصوصية المعلوماتية - بصفة عامة - في نطاق دراسات القانون الجنائي الداخلي (الوطني)، والتي تقع في صميم القسم الخاص لقانون العقوبات، وكذلك أدي تكون المجتمع الإلكتروني إلى تزايد انتهاك الحقوق الأساسية والحريات الفردية للأفراد التي كفلتها القوانين الدستورية، وخصوصا الحق في الخصوصية؛ مما يدل على ارتباط الموضوع بالقانون الدستوري، وحيث إنها من الجرائم التي تتخطى حدود الدولة الواحدة فهي تدخل أيضا في نطاق دراسات القانون الجنائي الدولي. وتدخل كذلك في عداد الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي وتدرجي له صفة الاستمرارية لتحقيق مكاسب طائلة. وبصفة عامة، فإن الجرائم الخصوصية المعلوماتية تتداخل مع جميع فروع القانون العام والخاص، غير أن ما جاءت به يبرز في مواجهة القانون الجنائي الداخلي والدولي الذي يهتم بمعالجة كل النواحي الأساسية التي يلزم مراعاتها لحسن سير الحياة الاجتماعية.
محلها ذو علاقته بالتكنولوجيا	بيانات الشخصية المخزنة والمعالجة والمتبادلة بواسطة الكمبيوتر وشبكات نقل المعلومات (بما فيها وفي مقدمتها الإنترنت).
السمات العامة لها	إن السمات العامة لقوانين الخصوصية المعلوماتية تنطوي على ثلاث طوائف رئيسية من القواعد : 1. الطائفة المتعلقة بإقرار المبادئ الرئيسية للحق في الخصوصية المعلوماتية، ونطاق اعتراف الدولة به، وكفله، والالتزامات المقررة على الجهات العامة والخاصة في حقل حماية المعلومات الشخصية، واحترام الخصوصية فيما

تمارسه من أنشطة جمع، ومعالجة البيانات الشخصية باستخدام التقنية. 2. القواعد التنظيمية والإجرائية والمعايير، وهي تلك القواعد المتعلقة بآليات جمع البيانات، ومعالجتها، ونقلها وتحدد المعايير التي يتعين على جهات التقنية والاتصالات التقيد بها إلى جانب بحثها في جهات رقابة حماية الخصوصية، وتنظيم تشكيلها، وعملها، وبيان دورها وتحديد مهامها وصلاحياتها، يضاف إليها أيضا القواعد الإجرائية الخاصة التي تطبق بالنسبة للحماية المدنية أو الجزائية المقررة في نطاق القواعد الموضوعية للحماية. 3. 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 قواعد موضوعية تتعلق بالحماية القانونية للبيانات الشخصية في كافة مراحل التعامل التقني معها .	
--	--

4. التشريعات القانونية في حقل حماية الحق في الخصوصية المعلوماتية في الدول الغربية :
ومن الدول من وضعت تشريعات خاصة لحماية الخصوصية المعلوماتية، وذلك على النحو التالي:

- أستراليا:

صدر في أستراليا قانون الخصوصية عام ١٩٨٨م. ولقد نص هذا القانون علي مجموعة من المبادئ التي تعرف باسم (IPPS) لحماية الخصوصية المعلوماتية.

- ألمانيا:

أصدر المشرع الألماني في ٧ أكتوبر سنة ١٩٧٠م أول تشريع لحماية الفرد ضد النتائج المحتملة لاستخدام الهيئات العامة لأجهزة الكمبيوتر، كبنوك للمعلومات، وإن كان نطاق الحماية التي فرضها المشرع محدودا، إلا إنه كان الأساس الأول لحماية الفرد في مواجهة استخدام الحاسبات الإلكترونية في القطاع العام ووضع نظام المراقبة، كما قرر مبدأ التوازن في المعلومات بين البرلمان والحكومة وأعطى للأحزاب والنواب البرلمانيين الحق في الوصول مباشرة إلى بنوك المعلومات؛ لتحقيق الرقابة البرلمانية عليها.

وفي ٢٧ يناير سنة ١٩٧٧م أصدر المشرع قانونا لحماية البيانات الشخصية ضد إساءة استخدامها عند معالجتها إلكترونيا. ثم بعد ذلك وضع المشرع عام ١٩٨٦م قانون حماية البيانات القانون المعدل لقانون ١٩٧٧م متزامنا مع إقرار قانون يصرح باستخدام بطاقات التعريف التي يتم قراءتها بواسطة الحاسوب، ويفرض على كل الألمان الغربيين أن يحملوا بطاقات (ID) الجديدة، مما يسمح للسلطات تخزين البيانات عن حركة الناس على حواسيب مركزية وهو ما لقي معارضة صلبة من الكثيرين، بما فيهم موظفو حماية البيانات في الحكومات الإقليمية؛ لمحاربة استخدام هذه البطاقات لمساسها بالحقوق الشخصية . وعدل هذا القانون جذريا بتاريخ 20 / 12 / 1990 ، كما جرى تعديله في العام 1994م.

ثم صدر مشروع قانون حماية البيانات عام ٢٠٠٠م المتوافق مع القانون الأوروبي لعام ١٩٩٥م.

- الدانمرك:

أصدر المشرع القوانين التالية لحماية البيانات الشخصية :

1. قانون المعالجة الإلكترونية عن طريق البنوك العامة رقم ٢٩٣ في ٨ يونيو سنة ١٩٧٨م.
2. قانون تسجيل السلطات العامة في 8 / 6 / 1978 م والمعدل -أيضا- بتاريخ 1 / 4 / 1978م.
3. قانون معالجة البيانات الشخصية لعام ٢٠٠٠م .

- السويد:

أصدر المشرع عدة تشريعات خاصة بحماية البيانات الشخصية وتنظيم المعالجة الإلكترونية :

1. فأصدر أول قانون حماية المعطيات The Data Protection وهو رقم ٢٨٩ في ١١ مايو سنة ١٩٧٣م وأجرى تعديلا في أول يولييه سنة ١٩٧٩م، والمعدل في الأعوام 1979م و 1982م و 1986م و 1990م، و 1992م.
2. قانون البيانات الشخصية The Personal Data لعام ١٩٩٨م حل محل القانون المشار إليه في 1 أعلاه .

- النرويج:

نص المشرع على حماية البيانات الشخصية وذلك بإصدار :

1. القانون رقم ٤٨ في ٩ يونيو سنة ١٩٧٨م ، والمعدل بالقانون رقم ٥٥ تاريخ 12 / 6 / 1987م، والقانون ٦٦ تاريخ 20 / 7 / 1991م، والقانون ٧٨ تاريخ 11 / 6 / 1993م .
 2. قانون تسجيل البيانات الشخصية لعام 2000م.
- وتنص المادة الأولى من هذا القانون علي أن الغرض من هذا القانون هو حماية الناس من انتهاك سلامتهم الشخصية من خلال معالجة البيانات الشخصية.

- النمسا:

بالرغم من أن المشرع الدستوري نص على حماية البيانات بصفة عامة، إلا إن المشرع أصدر :

1. في ١٨ أكتوبر سنة ١٩٧٨م قانونا لحماية المعطيات، والمعدل بالقوانين رقم ٣١٤ لسنة ١٩٨١م، والقانون رقم ٢٢٨ لسنة ١٩٨٢م، والقانون رقم ٣٧٠ لسنة ١٩٨٦م والقانون رقم ٦٠٥ لسنة ١٩٨٧م ، والقانون رقم ٢٣٣ لسنة ١٩٨٨م، والقانون رقم ٦٠٩ لسنة ١٩٨٩م ، والقانون رقم ٩١ لسنة ١٩٩٣م، والقانون رقم ٧٩ لسنة ١٩٩٤م، والقانون رقم ٦٣٢ لسنة 1994م.
2. قانون حماية البيانات لعام ٢٠٠٠م.

- الولايات المتحدة الأمريكية:

وضع المشرع الأمريكي القوانين التالية :

1. قانون شرف شفافية البلاغ المؤرخ في ١٩٧٠م:

الذي يشمل حقوق المستهلك من حيث المحافظة علي خصوصية المعلومات حول المستهلك والذي يتضمن أحقية المستهلك في معرفة من يطلع علي حقائق استهلاكه ومن ثم يلزم موافقته المسبقة علي ذلك.

2. قانون الخصوصية لعام ١٩٧٤م (The Privacy) :

الذي استلزم ضرورة تحري الدقة حين الحصول على معلومات، على أن يكون مصدرها دائما أصليا وليس نقليا.

3. قانون سياسة كابل الاتصالات لعام ١٩٨٤م:

هذا القانون يلزم شركات الإرسال المرئي بتوزيع بيان سنوي على المشتركين يراعي فيه خصوصية المعلومات عنهم، كما إنه يحظر على شركات الإرسال المرئي بالتجميع، والكشف عن المعلومات الشخصية للمشاركين. ولقد تضمن هذا القانون عقوبات عن الأضرار التي تتسبب في العدوان علي الخصوصية وفقا له كما تضمن - أيضا - تحميل الجاني بنفقات الدعوي العمومية.

4. قانون خصوصية الاتصالات الالكترونية لسنة ١٩٨٦:

والهدف من هذا القانون هو السعي إلى مد الاختصاص القضائي الفيدرالي إلى نطاق الاتصالات الإلكترونية، وذلك من ناحية تجريم المراقبة غير المصرح بها للاتصالات الإلكترونية المخزنة أو المتبادلة. حيث حظر القانون المذكور مراقبة وبث مضمون الاتصالات الإلكترونية المخزنة. ومن ناحية أخرى يحظر هذا القانون الدخول غير المصرح به إلى المرسلات والبيانات التي لها صلة بذاكرة الحاسوب.

5. قانون حماية خصوصية الضمان الاجتماعي على الخط لعام 1997م:

6. قانون حماية البيانات الشخصية لعام ١٩٩٧م:

- بريطانيا:

بالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية، ومتأخرة بالتأكيد عن الاستجابة الأمريكية، إلا أن السنوات الأخيرة وحتى الآن تشهد تميزا في التجربة البريطانية، سواء من حيث محتوى التنظيم، أو الحلول التشريعية المقررة، وليس في نطاق أمن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات وفي مختلف الفروع الأخرى لقانون تقنية المعلومات .

وبناء على ما سبق لقد صدرت قوانين ذات صلة منها: قانون حماية البيانات لسنة ١٩٩٨ م، وقانون حرية المعلومات لسنة ٢٠٠٠ م، ولائحة المعلومات البيئية لسنة ٢٠٠٤ م ؛ وقانون الخصوصية والاتصالات الإلكترونية لعام ٢٠٠٣ م .

- سويسرا :

وإذا وقفنا على حماية المعلومات الشخصية في قانون العقوبات في سويسرا، فإنه تجدر الإشارة إلى أنه في بداية الأمر لم يكن هناك قانون فيدرالي في هذا الشأن، فإن حماية المعلومات الشخصية لم تكلفها إلا الحالات التي تقع فيها جريمة خاصة، أي عند توافر الأركان المنشئة لجريمة خاصة، بعبارة أخرى إن جمع، وإذاعة المعلومات الشخصية يمكن أن تقع في إطار النصوص العقابية الخاصة بالجرح في مجال السرية والجرح ضد الذمة المالية، وكذلك في إطار النصوص العقابية الخاصة بالتجسس الاقتصادي أو العسكري.

فإذاعة هذه المعلومات يمكن أن تشكل مخالفة لسرية الوظيفة (المادة 320 من قانون العقوبات السويسري). وعند الضرورة يمكن يقع جمع، أو إذاعة المعلومات في إطار النصوص التي تتعلق بمجال السرية أو المجال الخاص (المادة ١٧٩).

ولكن ذلك كان قبل صدور القانون المؤرخ في 19 / 6 / 1992 م بشأن حماية البيانات والذي دخل النفاذ في 1 / 7 / 1993 م، حيث تضمن في المادة الأولى منه تحديدا لهذا النطاق في كونه يغطي بالحماية الشخصية والحقوق الأساسية لأشخاص محل معالجة البيانات .

ولقد توسع المشرع السويسري في تفسير مصطلح المعالجة (Traitement) في المادة الثالثة منه، بحيث تشمل كل عملية تتعلق بالبيانات الشخصية بأي وسيلة كانت والإجراءات المستخدمة، وبصفة خاصة حين تجميعها (Collect)، وحفظها (Conservation)، والكشف عنها (Exploitation)، وتعديلها (Modification)، والاتصال بها (Communication)، ووضعها في أرشيف (Archivage)، وتدميرها (La destruction de données).

- فرنسا :

كانت نداءات الفقه بضرورة وضع تنظيم تشريعي لحماية الخصوصية المعلوماتية، وقصور التشريع الجنائي بنصوصه التقليدية عن توفير الحماية اللازمة لهذه الحياة وحرية الأفراد في مواجهة هذه الأخطار، كل ذلك كان وراء إصدار المشرع الفرنسي للقانون رقم ١٧-٧٨- في ٦ يناير سنة ١٩٧٨ م الخاص بالمعلوماتية، والبطاقات، والحرية.

(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

وحماية الحق في الخصوصية المعلوماتية قد عولج بطريقة مفصلة في فرنسا، وخاصة بعد صدور قانون ٦ يناير (١٩٧٨م) - الخاص بالمعلوماتية والبطاقات والحريات - فقد نص على احترام شكلية خاصة للمعالجة الآلية للبيانات الشخصية، كما أنه نظم كيفية جمع، وتسجيل واستعمال والمحافظة على هذه المعلومات الشخصية، وكذلك بين من لهم الحق في الدخول لهذه الأجهزة وكيفية الرقابة لحماية هذه المعلومات عن طريق الأشخاص المعنية.

ونجد أن المواد من ٤١ إلى ٤٤ من هذا القانون تعاقب جنائيا على مخالفة هذا التنظيم . وقد نقل قانون العقوبات الفرنسي الجديد هذه النصوص وذلك في المواد ١٦ / ٢٦٦ إلى ٢٤ / ٢٦٦.

ثم بعد ذلك صدر القانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م والخاص بالمعالجة الإلكترونية للبيانات الاسمية تعديلا لقانون المعلوماتية و البطاقات و الحريات الصادر في ٦ يناير سنة ١٩٧٨م. ونص على عدة جرائم لحماية البيانات الشخصية، لتعلقها بالحياة الخاصة للأفراد. استنادا إلى مبدأ أساسي استهل به المشرع نصوص القانون، وهو أن المعالجة الإلكترونية للبيانات ألا تحمل تعديا على حصانة الفرد، ولا حقوق الإنسان، ولا حياته الخاصة أو حرياته الفردية والعامه.

وانطلاقا من مبدأ أساسي مقرر في "السياسة الجنائية" مضمونه أن الحقوق والمصالح الهامة اجتماعيا يجب أن تحمي بأقوى صور الحماية القانونية وأكثرها فاعلية وردعا ، وهي الحماية الجنائية.

وتجدر الإشارة علي أن المادة ٥٠ من الفصل الثامن - الخاص بالنصوص العقابية - من قانون الفرنسي رقم ١٠٨ لسنة ٢٠٠٤م نصت على أن : (يعاقب على مخالفة نصوص هذا القانون بالمواد من 16 / 226 إلى 24 / 226 من قانون العقوبات الفرنسي). أي أن نصوص هذه المواد من قانون العقوبات الفرنسي تعاقب على مخالفة نصوص القانون الخاص بالمعالجة المعلوماتية الشخصية. وذلك من خلال نصها علي الجرائم التالية:

1. جريمة المعالجة الالكترونية للبيانات الشخصية دون مراعاة الشكليات القانونية المطلوبة.
2. جريمة عدم اتخاذ الاحتياطات أو التدابير الوقائية للحفاظ علي المعلومات الشخصية.
3. جريمة جمع أو حفظ البيانات الشخصية بطريق العنف أو الاحتيال أو بطريق غير مشروع.
4. جريمة حفظ البيانات الشخصية خارج الوقت المصرح به وفقا للطلب أو الإعلان السابق.
5. جريمة عدم تبصير ذوي الشأن في مجال البحث الطبي.
6. جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية.

7. جريمة الإفشاء غير المشروع للبيانات الشخصية.
8. حماية المراسلات التي تتم بطريق وسائل الاتصالات.

- كندا:

نص المشرع في الباب الرابع مواد (٤٩-٦٢) من القانون الصادر في ٢٤ أبريل سنة ١٩٧٧م، والخاص بحقوق الإنسان على حماية البيانات الشخصية للفرد.

ونلاحظ مما سبق أن التجربة الأوروبية في حقل أمن المعلومات والخصوصية هي التجربة الأكثر نضجا في العالم ، فعلى المستوى الوطني كانت الدول الأوروبية من أوائل الدول التي تعاملت مع الظاهرة تعاملًا واقعيًا عبر دراسات متعمقة للواقع، ولطبيعة المشكلات، وللحلول والتدابير الأفضل ، فلم تكن تجربة متسرعة، لكنها لم تكن أيضًا بطيئة من حيث الاستجابات، بل على العكس كانت استجابات مبكرة في حدود متطلبات الواقع ، ولأن فهم الظاهرة أساسًا وأخذ التدابير على ضوء هذا الفهم المتعمق هو أهم ضمانات النجاح .

ثانياً : الحماية التشريعية للحق في الخصوصية المعلوماتية في البيئة العربية:

بالنسبة لموقف التشريعات العربية المقارنة من حماية حق في الخصوصية المعلوماتية، سوف نذكر على سبيل المثال:

- دولة الإمارات العربية المتحدة :

يشكل القانون الاتحادي لحماية البيانات الشخصية رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية إطارًا متكاملًا لضمان سرية المعلومات، وحماية خصوصية أفراد المجتمع عبر توفير الحوكمة السليمة لإدارة البيانات وحمايتها. يحدد القانون الأطر العامة للتعامل مع البيانات الشخصية للأفراد، وكيفية جمعها ومعالجتها وتخزينها، ووسائل ضمان حمايتها، وحقوق وواجبات كافة الأطراف المعنية.

و بدأ العمل بقانون مكافحة الشائعات والجرائم الإلكترونية، المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في 2 يناير 2022. يهدف القانون إلى توفير إطار عمل قانوني شامل لتعزيز حماية المجتمع من الجرائم الإلكترونية المرتكبة من خلال شبكات وتقنيات الإنترنت. كما يسعى إلى حماية المواقع الإلكترونية وقواعد البيانات الحكومية في دولة الإمارات، ومكافحة انتشار الشائعات والأخبار المزيفة، الاحتيال الإلكتروني، والحفاظ على الخصوصية والحقوق الشخصية.

- المملكة العربية السعودية:

تم تطوير وتبني نظام مكافحة جرائم المعلوماتية في السعودية الصادر في 27 / 3 / 2007 م ، الذي ينص على عقوبات صارمة لمن يخرق الخصوصية السيبرانية. وتوجد بعض القوانين السعودية الأخرى تشمل ضوابط الحوسبة السحابية واستضافة البيانات والمعلومات. ويسعى المشرعون لتفعيل هذه القوانين وتطبيقها بدقة لحماية الأفراد والمؤسسات من الاختراق والتلاعب بالبيانات الشخصية والمتخصصة. ويتواصل المجتمع السعودي والحكومة بجهود مشتركة تكريساً لمبدأ الخصوصية والأمن السيبراني في المملكة.

تم إصدار قانون "حماية البيانات الشخصية" في 16 سبتمبر 2021، بعد موافقة مجلس الوزراء في المملكة العربية السعودية، وتم نشره في 24 سبتمبر 2022 والذي يحتوي على عدة شروط لمعالجة البيانات الشخصية بالإضافة إلى سلسلة من الحقوق التي سيتمتع بها "أصحاب البيانات الشخصية" كما يشتمل هذا النظام على اطار مفصل حول معايير معالجة البيانات، والتزامات الهيئات المعنية عند معالجة البيانات الشخصية، بالإضافة الى العقوبات المترتبة على الشركات أو الكيانات العامة العاملة داخل المملكة العربية السعودية في حال عدم الإمتثال.

وقد صرح بأنه يُعمل بالنظام بعد 180 يوماً من تاريخ نشره في الجريدة الرسمية (المادة 43 من النظام)، أي في 23 مارس 2022.

وتُشرف الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) على تنفيذ نظام حماية البيانات الشخصية خلال أول عامين. وبعد ذلك، يتولى "مكتب إدارة البيانات الوطنية" الإشراف على تنفيذه.

- تونس:

بادرت تونس إلى وضع تنظيم في مجال المعالجة الآلية للبيانات الشخصية بعد شعورها بخطورة الاستخدامات الجديدة لتكنولوجيا المعلومات وتطورها وتأثيرها على مختلف المجالات بما فيها تأثيرها على حقوق وحريات الأفراد، فأصدرت القانون السادس عدد 63 لسنة 2004 المتعلق " بحماية المعطيات الشخصية في الفصل الأول منه على "لكل شخص الحق في حماية المعطيات" ، وهي المضمونة بالدستور.."، ومن خلال هذا القانون انشأ سلطة إدارية مستقلة وهي " الهيئة الوطنية لحماية المعطيات الشخصية "، التي من مهامها تحديد الضرورية والتدابير الملزمة لحماية المعطيات الشخصية....

وأصدر في ذات الإتجاه الأمر عدد 3003 لسنة 2007 لتحديد وضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية السابق ذكرها، كما قام المشرع التونسي في نفس السنة ومن خلال الأمر عدد 3004 لسنة 2007 ذكر شروط وإجراءات التصريح والترخيص لمعالجة البيانات الشخصية، حتى توضح

الرؤية لكل شخص معني تكون بيناته الشخصية موضوع المعالجة، أو كل شخص طبيعي أو معنوي مسؤول على عملية المعالجة.

ثم صدر المرسوم عدد 54 لسنة 2022 مؤرخ في 13 سبتمبر 2022 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال، وذكر فيه عقوبات علي الاعتداء على سلامة أنظمة المعلومات والبيانات وسريتها في القسم الأول.

- مصر:

ونص قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م علي عقوبات رادعه كل من ارتكب فعلاً من الأفعال الآتية:

1. الاعتداء على أي من المبادئ أو القيم الأسرية في المجتمع المصري.
2. انتهاك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته.
3. نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.
4. كل من تعتمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

وصدر قانون حماية البيانات الشخصية رقم 151 لسنة 2020 وهدفه ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً، ووضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين، ومكافحة انتهاك خصوصيتهم، وذلك من خلال تطبيق إطار معياري يتواءم مع التشريعات الدولية لحماية البيانات الشخصية للأفراد، وحياتهم، واحترام خصوصيتهم، وصياغة التزامات على كل من المتحكم في البيانات، ومعالج البيانات باعتبارهما من العناصر الفاعلة في مجالات التعامل في البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التبادل أو التخزين أو التحليل أو المعالجة بأي صورة من الصور.

المحور الثالث

الحماية الإدارية للحق في الخصوصية المعلوماتية

لقد اختلف القانون المقارن حول إنشاء جهة إدارية متخصصة للإشراف والرقابة علي تطبيق قانون الخصوصية المعلوماتية اختلافاً بينا:

1. ترك الرقابة للقواعد العامة دون حاجة لجهة خاصة:

فيذهب القانون الإنجليزي في شأن الخصوصية والصادر في سنة ١٩٧٤م إلى ترك ذلك للقواعد العامة، فيختص القضاء العادي بدعوى التعويض الناشئة عن مخالفة القانون.

ولكن يؤخذ علي هذا الاتجاه أن القضاء لا يتدخل إلا لاحقاً، أي بعد قيام النزاع واستحكامه والتوفيق بين تطور المعلوماتية وحماية الخصوصية يستلزم وجود جهة ترعى عدم مخالفة القانون أي الحرص علي الحماية الوقائية.

وفي إطار هذه الفكرة يذهب المشرع الأمريكي إلى عدم الحاجة لوجود جهة إدارية مستقلة للسهر علي تطبيق القانون؛ فذلك الأمر يدخل في اختصاص جهة الإدارة، في ترقب مدى التزام بنوك المعلومات بأحكام القانون، ويحال المخالف إلى القضاء. ولجهة الإدارة أن تلجأ إلى اللوائح أو التشريعات الفرعية لتطبيق القانون، وتفصيل أحكامه، وتوفير الحماية اللازمة للمعلومات الشخصية.

وتتجه غالبية التشريعات المقارنة إلى أن تعهد بمهمة الإشراف والسهر على تطبيق القانون إلى جهة خاصة، وهناك عدة صور في هذا الصدد.

2. مفوض نظم المعلومات:

أخذت ولاية هيس في ألمانيا الغربية بفكرة تعيين مفوض لنظم المعلومات؛ حيث يختص بحماية المواطنين في هذا المجال، ويختص المفوض برقابة عمليات بنوك المعلومات الشخصية. ولكل شخص يشعر بأن أحد نظم المعلومات يمس حياته الخاصة أن يتقدم بشكوى إلى المفوض. ويقوم المفوض ببحث الشكوى مع البنك، وغالبا ما يتوصل إلى حل المشكلة وديا بين الطرفين، وتحصر البنوك على الحل الودي تفاديا للدعوى القضائية.

ولهذا النظام مزايا ولكنه لا يخلو من العيوب وذلك علي الوجه الآتي:

فهو يتميز ببساطته وضآلة ما يحمله للخزانة من أعباء مالية، وتعتمد فعاليته علي شخصية من يتولي هذا المنصب الذي يكون عادة محلا للاحترام والثقة، مما يساعد علي قيامه بمهمته ويدعم من قيامة ما يصدره من توصيات وتعليمات.

ولكن يعيبه، أن المفوض لا يملك التدخل إلا بناء علي شكوى من صاحب الشأن، فلا يحق له القيام بالتحري عن مدى احترام القانون، كما أن المفوض لا تتوفر له - غالبا - الخبرة الفنية اللازمة للتحقق من قواعد السلامة والحماية.

3. جهاز أو لجنة للإشراف والرقابة:

ومن أنجح السبل التي ظهرت في القانون المقارن، هو أن يعهد إلى لجنة أو جهاز مستقل باختصاص الإشراف والرقابة علي تطبيق القانون. وأبرز هذه الأمثلة اللجنة القومية للمعلوماتية والحريات في فرنسا، والتي أنشئت بموجب الفصل الثاني من قانون ١٩٧٨م، ولقد عهد إلى اللجنة القومية للمعلوماتية والحريات منذ تعديل ٢٠٠٤م بسلطة ردع الجرائم المخالفة لهذا التعديل، والذي جاء بمقتضي القانون رقم ٨٠١ - ٢٠٠٤م.

ويعد أول ردع قضت به هذه اللجنة في عام ٢٠٠٦م، أي أول حكم صدر عن هذه اللجنة بخصوص مخالفة هذا القانون يرتد إلي ٢٨ يونيو ٢٠٠٦م.

وتجدر الإشارة إلى أن اللجنة لم تصدر في العديد من الحالات آراء إلا بعد التفاوض مع الإدارة على تعديلات لمشاريعها محل المناقشة. وهذه اللجنة تعد إدارة تراقب إدارة. وقد اعتبر المشرع الفرنسي هذه اللجنة بمثابة الشرطي بالنسبة لرجال المعلوماتية الذين يتعاملون مع المعلومات الشخصية باعتبارها احدي السلطات المكلفة بحماية الحرية الفردية.

• المراجع :

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

تم بحمد الله الإنتهاء من شرح المحاضرة العاشرة

مع تمنياتي بالتوفيق د. أسماء رويحي