جامعة بنغازي – كلية الحقوق

قسم القانون الجنائي

رسالة مقدمة استكمالاً للحصول على متطلبات درجة التخصص العالي

(الماجستير) في القانون الجنائي

الحماية الجنائية للخصوصية المعلوماتية

(دراسة تحليلية مقارنة)

إعداد الطالب:

محمد ارحومة محمد القماطي

إشراف:

أ.د موسى مسعود ارحومة

العام الدراسي 2016 – 2017

بِسمِ اللَّهِ الرَّحمٰنِ الرَّحِيمِ

﴿ وَقُل رَّبِّ زِدنِي عِلمًا ﴾

سُورَة طٰـه الآية 114

إهداء

إلى أمي وأبي . . إلى أهلي

إلى أساتذتي

إلى الشموع التي تحترق لتضيء للآخرين

إلى كل من علمني حرفا

أهدي هذا البحث المتواضع راجياً من المولى

عز وجل أن يجد القبول والنجاح

شكر وتقدير

أرى واجباً علي أن أتقدم بالشكر الجزيل لأستاذي ومعلمي

الأستاذ الدكتور : موسى مسعود ارحومة

لما تفضل علىَ به من توجيهات سديدة كان لها الأثر الكبير في

انجاز هذا العمل.

البـــــاحث

مُقَدِّمَة

إن الإنسان اجتماعي بطبعه لا يحبذ العيش وحيداً ، إلا أن هذه الطبيعة في الإنسان ليست مطلقة ، فيحتاج الإنسان لفسحة من الخصوصية يحتفظ بها بنفسه ، وهذا ما يطلق عليه اصطلاحاً " الحياة الخاصة " ، ولا يعتبر هذا المصطلح مصطلحاً حديثاً ، كما أن فكرة توفير الحماية له لم تكن وليدة اللحظة ، فلكل إنسان الحق في حماية حياته الخاصة من أي انتهاك قد تتعرض له .

فعندما نبحث في مجال الخصوصية سنجد النص عليها في الشرائع اليونانية والصينية القديمة وكذلك في الشرائع السماوية ؛ ومن ذلك ما ذُكر في القرآن الكريم من تحريم استراق السمع ﴿يَا أَيُّهَا الَذِينَ آمَنُوا اجْتَنِبُوا كَثِيراً مَّنَ الظَّنَّ إِنَّ بَعْضَ الظَّنِّ إِثْم وَلاَ تَجَسَّسُو ﴾[1] ،أو دخول البيوت بدون إذن﴿ يَا أَيُّهَا الّذِينَ آمنُوا لاَ تْدخُلوا بُيُوتاً غَيْرَ بُيُوتكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ﴾.[2]

ولم تقتصر صور الحماية على ما ذكر ، وإنما تعدت ذلك ، فنجد محاولات عديدة لحماية الحياة الخاصة عن طريق التشريعات الوضعية ، إلا أن الحياة الخاصة لها مفهوم نسبي، فما يدخل في إطار الحياة الخاصة في زمان أو مكان مُعين لا يمكن اعتباره كذلك في زمان أو مكان آخر ، ويمكن حصر أهم العناصر التي تمثل الجوانب الرئيسة لفكرة الخصوصية في :

---

1) الآية 12 من سورة الحجرات.

2) الآية 27 من سورة النور.

- حماية سلامة الفرد وممتلكاته (الحماية المادية) أي الحق في حمايته من الانتهاكات التي تقع على حياته الشخصية.
- حماية قيمة المعنوية(الحماية المعنوية).

ويظهر لنا أن توفير الحماية للحياة الخاصة لا يقتصر على حماية الممتلكات الخاصة بالفرد وإنما تتعدى ذلك لتشمل حماية مجموعة من المعلومات الخاصة بحياة الفرد والتي تتعلق بذاته.

ومع تطور العصر والدخول في ما يُعرف بالعصر الرقمي واستحواذ تقنية المعلومات على حياتنا أصبحنا نُخزن ونسترجع ونُحلل كميات هائلة من البيانات الشخصية عن طريق هذه التقنية والتي يتم تجميعها إما عن طريق الدوائر الحكومية أو عن طريق مؤسسات القطاع الخاص _ من هنا يتضح لنا حجم التهديد الكبير للحياة الخاصة جراء استخدام هذه التقنيات الحديثة _ فوجب أن يُقابل التطور في استخدام مثل هذه التقنيات تطور آخر في مجال الحماية الجنائية للخصوصية المعلوماتية.

ففي العصر الحديث ظهرت الحاجة الماسة لمُعالجة الكثير من المعلومات ، حيث أصبحت المعلومات عصب الحياة لاسيما الاقتصادية والسياسية منها ، وأصبح استخدام الحاسوب من سمات هذا العصر ومن الأساسيات التي من شأنها تحسين التنظيم الإداري ، ولهذا وصفت المرحلة التي نحن فيها بـ(عصر الحاسوب) وبـ(العصر الرقمي) فبناء مجتمع رقمي يتطلب أن تكون هناك مواكبة دائمة وفورية للتكنولوجيا الحديثة التي تظهر في المجال المعلوماتي سواء من قبل المؤسسات الحكومية أو المؤسسات الخاصة .

فقد أصبح استعمال الكمبيوتر أمراً لا يمكن الاستغناء عنه كما أن شبكة الإنترنت وما توفره من سهولة تصفح المعلومات وجمعها جعل منها وسيلة عالمية مهمة جداً في حياتنا اليومية، ولأجل هذا دأبت العديد من المنظمات على عقد عديد المؤتمرات لدراسة هذه المستجدات ووضع الخطط والاستراتجيات لمواجهة ما قد يقع على الخصوصية من انتهاكات نتيجة استعمال التكنولوجيا الحديثة ، وهذا ما حذا بالمجتمع الدولي إلى الاهتمام بهذا الأمر وعقد المؤتمرات وإبرام الاتفاقيات لمواجهة المخاطر التي تشكلها الانتهاكات التي تقع على الخصوصية المعلوماتية .

أما في القوانين والتشريعات الوطنية فقد تم تناول هذه المواضيع بنصوص ضُمنت لقانون العقوبات أو عن طريق قوانين خاصة لمُعالجة هذا الأمر.

إن الاعتداءات التي تقع على الخصوصية من شأنها أن تهز الثقة القائمة عند مستخدمي التكنولوجيا الحديثة والشبكة المعلوماتية ، فكما توفر التكنولوجيا الحديثة طرق سهلة وسريعة لنقل المعلومات وتداولها (الأثر الإيجابي)، من شأنها أيضاً أن تجعل هذه المعلومات عرضه لخطر الاعتداءات التي قد تقع عليها(الأثر السلبي).

وبالتالي فإن مسألة التطور المستمر للإنترنت وما يُشكله هذا التطور من مخاطر على المعلومات والبيانات الخاصة من شأنه أن يُظهر لنا أهمية البحث في هذا الموضوع.

اولاً: أهمية موضوع البحث:

إن دراسة هذا الموضوع تكتسب أهميتها سواء من الناحية الموضوعية أو العملية كونها تمس احد أهم المصالح في المجتمع ألا وهي خصوصية المعلومات والتي أصبحت عرضة للانتهاكات نتيجة للثورة التقنية في مجال الاتصالات ، حيث أن التقنية الحديثة بالرغم من توفيرها تسهيلات تجعل الحياة أيسر إلا أن هذا (الجانب الايجابي) يواجهه جانب آخر (سلبي) وهو ما

تتسبب فيه هذه التقنية من تعريض الحياة الخاصة لانتهاكات في المجال المعلوماتي، ومن هنا كان لزاماً ضرورة دراسة هذه التطورات حتى يتسنى للأفراد استخدام هذه التقنيات بشكل أمن ويحقق الغاية التي تم تطويرها من أجله .

ولعل كم الانتهاكات التي الواقعة على الخصوصية المعلوماتية يجعل البحث في هذا الموضوع من الأهمية بمكان، كما أن التقصير الواضح من قبل العالم العربي في مُعالجة الخصوصية المعلوماتية على وجه العموم والجانب الليبي على وجه الخصوص يجعل من دراسته والبحث فيه أمر بالغ الأهمية وذلك لتسليط الضوء عليه لعله يكون من البحوث التي يستهدي بها الباحثون والمهتمون بهذا المجال.

ثانياً: إشكالية البحث:

إن الطرح القانوني لموضوع انتهاك حرمة الحياة الخاصة في ظل التقنيات الحديثة وعبر شبكة الانترنت يتعدى الإشكاليات التقليدية التي تناولتها العديد من الدراسات الفقهية والأطروحات العلمية القانونية حول حرمة الحياة الخاصة ، والتي ركزت في معظمها على مفهوم الحق في خصوصية الفرد وماهيتها والانتهاكات التقليدية لها ، ولكن قلة من هذه الدراسات سلطت الضوء على انتهاك الحياة الخاصة عبر شبكة الانترنت ومن خلال وسائل الاتصالات والتقنيات الحديثة ، وتتمحور الإشكالية الرئيسة في تحقيق التوازن بين حق الفرد في حماية خصوصيته من أي انتهاك أو تدخل ، في المقابل الاحتفاظ بحق الدولة في التدخل في خصوصية أفرادها عند الضرورة وذلك لحماية أمن واستقرار المجتمع ، وهذه الإشكالية تثير بدورها العديد من التساؤلات المهمة نوجزها في الأتي :

- هل الخصوصية التي عالجها الفقه منذ القرن التاسع عشر تقريباً وكفلتها الدساتير والقوانين الوضعية هي ذات الخصوصية التي نتحدث عنها في العصر المعلوماتي؟ أم أنها ذات محتوى مغاير؟
- هل يمكن عد الخصوصية وحماية البيانات تعبيرين مترادفين للموضوع ذاته ؟ أم أن الحياة الخاصة مفهوم أكثر شمولاً من حماية البيانات؟
- هل القانون وحده كافٍ لحماية خصوصية المعلومات؟ أم لابد من تكاتف الاستراتجيات التنظيمية والوسائل التقنية لحماية المعلومات الخاصة من خطر الانتهاك؟
- هل النصوص الموجودة في القوانين العقابية كافية لحماية الخصوصية من الانتهاكات التي قد تقع عليها عبر الشبكة المعلوماتية والتقنية الحديثة؟

ومن هنا نهدف في هذا البحث إلى الإجابة عن هذه التساؤلات من خلال:

أ. تسليط الضوء على مخاطر التقنيات الحديثة وتأثيرها على الحق في الخصوصية المعلوماتية.

ب. الوقوف على مدى الحماية التي توفرها المنظمات الدولية والإقليمية للخصوصية المعلوماتية.

ج. توضيح الحماية التي وفرها المشرع للخصوصية المعلوماتية في التشريعات الوطنية.

ثالثاً: نطاق البحث:

وقبل الخوص في دراسة الموضوع والبحث فيه رأينا أنه من الواجب علينا رسم نطاق البحث وبيان خطوطه العريضة حيث سيتم تناول الخصوصية المعلوماتية من حيث أهميتها وما تشكله التكنولوجيا الحديثة من مخاطر عليها .

كما سنتولى البحث في آليات الحماية الدولية وذلك من خلال دراسة أهم أعمال المنظمات سواء على المستوى الدولي أو الإقليمي في مجال الخصوصية المعلوماتية، وكذلك المؤتمرات الدولية في هذا المجال، كما ستشمل الدراسة النصوص الموضوعية في التشريعات الوطنية.

رابعاً: منهج البحث :

سيتم تناول هذه الدراسة باستخدام المنهج التحليلي ؛ وذلك بتحليل أعمال المنظمات الدولية ، وما توفره من حماية للخصوصية المعلوماتية، وكذلك أعمال المؤتمرات الدولية ؛ بالإضافة إلى استخدام المنهج المقارن ؛ وذلك بمقارنة النصوص الخاصة بحماية الخصوصية المعلوماتية الواردة في التشريعات الوطنية.

خامساً: خطة البحث:

نبحث في موضوع الحماية الجنائية للخصوصية من خلال خطة بحث تتناول دراسة عموميات في الخصوصية المعلوماتية ، يتم فيها بحث ماهية الخصوصية المعلوماتية ، ونطاقها، والمخاطر التي تتهددها في الفصل الأول ، كما سنُفرد الفصل الثاني لدراسة آليات الحماية التي وفرتها المنظمات الدولية ، والإقليمية للخصوصية المعلوماتية ، كما سنتناول بالبحث آليات الحماية الوطنية للخصوصية المعلوماتية في الفصل الثالث ؛ وذلك كالتالي :

الفصل الأول: عموميات في الخصوصية المعلوماتية.

الفصل الثاني: آليات الحماية الدولية للخصوصية المعلوماتية.

الفصل الثالث: آليات الحماية الوطنية للخصوصية المعلوماتية.

الفصل الأول

عموميات في الخصوصية المعلوماتية

تمهيد

إن الحق في الخصوصية ، أو كما يُعرف في النظام اللاتيني بالحق في الحياة الخاصة، يُعرف بحق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجذور من الوجهة التاريخية.

وللخصوصية وفق تطورها التاريخي ثلاث محطات رئيسة ، الأولى: الاعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم ، وهي ما تعرف بالخصوصية المادية ؛ والثانية : انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص ، وهي ما يُعرف بالخصوصية المعنوية ؛ والثالثة: الخصوصية كحق عام يمتد نطاقه لحماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته أياً كان مظهرها أو طبيعتها ، وفي نطاق المعنى الأخير ولد مفهوم جديد للخصوصية ارتبط بأثر التقنية على الحياة الخاصة، تمثل بخصوصية المعلومات أو حق الأفراد في السيطرة على المعلومات والبيانات الخاصة بهم في مواجهة تحديات العصر الرقمي. [1]

وسنتناول في هذا الفصل ماهية الخصوصية المعلوماتية ثم نشأة خصوصية المعلومات وتطورها، ونطاق هذه الخصوصية، ومخاطرها، وأضرارها، على الحياة الخاصة، في مبحثين:

المبحث الأول: ماهية الخصوصية المعلوماتية.

المبحث الثاني: نطاق الخصوصية المعلوماتية والمخاطر التي تُهددها.

المبحث الأول
ماهية الخصوصية المعلوماتية

1) منى تركي الموسوي ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها ، جامعة بغداد ، مجلة كلية بغداد للعلوم الاقتصادية ، العدد الخاص بمؤتمر الكلية 2013م ، ص4.

تمهيد

للخصوصية أصول عميقة الجذور من الناحية التاريخية ، فلها إشارات في الشرائع اليونانية والصينية القديمة ، وقد جاء ذكرها في القرآن الكريم أكثر صراحة، وذلك بتحريم استراق السمع أو دخول المنازل بغير إذن.

بالنسبة للخصوصية في التشريعات الوضعية ، أو الاتفاقيات الدولية ، فهي أيضاً ليست حديثة النشوء ، ومع تطور العصور أصبحت الخصوصية تتخذ مفهوماً أوسع، فأخذت تتخطى خصوصية الفرد في مسكنه ومقتنياته الخاصة ، لتشمل أبعاداً أشمل وأوسع ، وخاصة بعد دخولنا في ما يُعرف بالعصر الرقمي (Digital Age) ، حيث أصبحت البيانات الشخصية التي يتم جمعها سواء عن طريق الجهات الحكومية أو عن طريق المؤسسات الخاصة تتداول بشتى الطرق ، ومنها شبكة المعلومات الدولية (The Internet) ، ويتم تخزينها وحفظها واسترجاعها ومُعالجتها وإرسالها من جهة لأخرى ، وهذا أصبح يُشكل خطراً على هذه البيانات ، ومن هنا ظهر لدينا نوع جديد من الخصوصية ، ألا وهو الخصوصية المعلوماتية.

ولإضفاء الحماية اللازمة على هذا النوع من الخصوصية يتطلب تحديد ماهية الخصوصية المعلوماتية ، وكيفية نشوئها ، وهنا سنتناول هذا المبحث من خلال مطلبين:

المطلب الأول: تعريف الخصوصية المعلوماتية.

المطلب الثاني: نشأة خصوصية المعلومات وتطورها.

المطلب الأول

تعريف الخصوصية المعلوماتية

1. الخصوصية لغةً:

المقصود من الناحية اللغوية بالخصوصية: حالة الخصوص ، فالخصوصية عكس العموم ونقيضاً لها فيُقال: اختص فلان بالأمر إذا أفرده به وخصه به دون غيره ، فالخاصة خلاف العامة.

والخصوص إذاً الإنفراد ويُقابله العموم ، كما يفيد الحصر وضده الإطلاق ، فنقول أعجبني هذا الصديق خصوصاً ، ويمتزج الإنفراد والتحديد في قولنا على الخصوص أو خصوصاً لاسيما ومن مرادفات الخصوصية في اللغة العربية ، الانزواء ، والانعزال، والعزلة، والتوحد ، والتفرد ، والوحدة ، والانطواء.[1]

وبإضافة لفظة (حق) إلى الخصوصية يمكن أن نتصور معنى هذه الإضافة من الناحية اللغوية بأنها : حق الشخص في أن ينفرد بأمور لنفسه ، أو خاصته ، على ألا تتخذ هذه الأشياء صفة العموم. [2]

2. الخصوصية اصطلاحاً:

يرجع استخدام اصطلاح الخصوصية في اللغة الإنجليزية إلى القرن الخامس عشر، ليدل على الحالة أو الوضع الذي يكون الفرد فيه بحالة انسحاب من المجتمع فيتوارى عنهم وينأى بنفسه عن أي اهتمام من قبلهم ، وهذا الاصطلاح أدرج في اللغة الانجليزية يساير حقيقة أخرى، وهي أن الأفكار الأولى بشأن الخصوصية أو الحالات الأولى كتطبيقات لهذا الحق في إطار مفهوم الخصوصية المادية ظهرت أيضاً في نطاق المجتمع الانجليزي، والنظام القانوني الإنجليزي ، الذي أمسى المثال على النظم القانونية التي لا تعترف بالخصوصية كحق عام، ولا يقبل قضاؤها

---

1) ابن منظور ، لسان العربي ، الجزء الثامن ، الطبعة الأولى ، منشورات مطبعة بولاق ، القاهرة ، ص290.

2) عبداللطيف الهميم ، احترام الحياة الخاصة ، الخصوصية بين الشريعة الإسلامية والقانون المقارن ، دار عمار ، عمان ، الأردن ، الطبعة الأولى ، 2004م .

تطوير الفكرة ما لم يتدخل المشرع ليعترف بهذا الحق ، وهو ما أُنجز أخيراً في عقدي الثمانينات والتسعينات.[1]

أما في الولايات المتحدة الأمريكية فإن الحق في الخصوصية طرح في أجواء التعديل الرابع على الدستور الأمريكي عام 1791م ، هذا التعديل الذي وإن كان يحصر فكرة الخصوصية في حماية منزل وذات الشخص وأوراقه ، أصبح فيما بعد المصدر الدستوري للاعتراف بالخصوصية كحق عام للفرد في مواجهة أي انتهاك لشؤون حياته الخاصة ، ونفس النص الدستوري استخدم أساساً لتطوير مفهوم الخصوصية ، وتوسيع نطاقه في النظام القانوني الأمريكي ، وهو تطوير اضطلع به القضاء – وليس التشريع – متأثراً بالاجتهاد الفقهي. [2]

في المقابل ، وجرياً على مسلك النظام القانوني اللاتيني عموماً في اتجاهه لإقرار المبادئ العامة ، لعب الفقه والقضاء في فرنسا دوراً بارزاً في تكريس مفهوم الحق في الحياة الخاصة وحماية الحياة الخاصة ، كحق عام على نحو سابق من إقرار النظام القانوني الأمريكي له. غير أن ما يتعين ملاحظته أن اللغة الفرنسية تنطوي على مرادفات لتعبير الحياة الخاصة ، وتبعاً لذلك فإن النظام القانوني الفرنسي ، ينطوي على اصطلاحات عديدة للدلالة على الخصوصية ، إضافة لاصطلاح الحياة الخاصة كالحق في السرية والحق في الخلوة ، والاهم الحق في الألفة ، الذي جرى استخدامه تشريعياً في ذات نص المادة 9 من قانون 1970م، المعدل للقانون المدني الفرنسي التي كرست للاعتراف بمبدأ حماية الحياة الخاصة.

وبالانتقال إلى الشريعة الإسلامية، نجد أن هناك اتجاهاً خاصاً في بيان الحق وتحديد أقسام هذا الحق. ولها أيضاً تطبيقات في مفهوم الخصوصية ، وبالرغم من ذلك فإن مصطلح الحق

1) John H. F. Shattuch, Right of Privacy, National Textbook Co, 1977, P2

2) Richard A. Posner, The Uncertain Protection of Privacy by the Supreme court. تاريخ الزيارة 2016/04/10م http://www.law.cornell.edu/constitation/constitution.billofrights.html#amendmentiv

في الخصوصية أو حق الفرد في الانفراد والاختلاء لم يكن وارداً في الشريعة الإسلامية بهذه الصورة.[1]

ويكاد ينعقد الإجماع على صعوبة التوصل إلى تعريف جامع مانع للحق في الحياة الخاصة أو الخصوصية أو السرية الشخصية كما يسميها بعضهم .[2] ولهذا نجد تعريفات متعددة ومتباينة تم وضعها للحق في الحياة الخاصة ، ليس في إطار النظم القانونية المختلفة ، ولكن في إطار النظام القانوني الواحد فللفقه تعريفاته،[3] وللقضاء تعريفاته،[4] وهي تتباين في الإطار الواحد. أما التشريعات فقد اتجهت إلى عدم إيراد تعريف للحق في الحياة الخاصة تاركة هذا الآمر للفقه والقضاء ، واكتفت بوضع نصوص تكفل حماية الحق وتعدد صور الاعتداء عليه.

إن الإجماع على صعوبة وضع تعريف الحق في الخصوصية لا يجد له مبرراً سوى الاختلاف في المفهوم الذي يستند إليه هذا الحق، وتبيانه من وجهة نظر الأنظمة القانونية المختلفة

---

1) حول موقف الشريعة الإسلامية من الخصوصية ، واستعراض مفهوم الحق عموماً وتطبيقات الخصوصية في الشريعة الإسلامية، حسني الجندي ، ضمانات حرمة الحياة الخاصة في الإسلام ، الطبعة الأولى، دار النهضة العربية ، القاهرة، 1993م. ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي ، الطبعة الأولى ، دار النهضة العربية، القاهرة مصر ، 2011م، ص 42 وما بعدها. إبراهيم بن سليمان بن عبد الله الشايع ، حق الخصوصية في الفقه الإسلامي ، رسالة ماجستير مقدمة لجامعة الإمام محمد بن سعود الإسلامية ، السعودية، 2006م .

عادل عبدالعال ابراهيم خراشي ، الحماية الجنائية للحق في الخصوصية ، شركة ناس ، القاهرة مصر ، الطبعة الأولى ، 2015م ، ص 16 وما بعدها.

2) عبد الرؤوف مهدي ، الجوانب الإجرائية لحماية الحق في الحياة الخاصة ، بحث مقدم إلى مؤتمر الحق في الحياة الخاصة بكلية الحقوق ، جامعة الإسكندرية . بتاريخ 4 إلى 6 يونيو 1987 ص3.

3) يعرف أستاذ القانون الدولي (I.F Westin) الحق في الحياة الخاصة أو الحرمة الشخصية بأنه: "حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم على الآخرين؛ الخصوصية منظوراً إليها من علاقة الفرد بالمشاركة الاجتماعية ، هي انسحاب الفرد الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية".

انظر صالح جواد كاظم ، التكنولوجيا الحديثة والسرية الشخصية مباحث في القانون الدولي ، الطبعة الأولى ، دار الشؤون الثقافية العامة ، بغداد 1991م ، ص136. ويعرفه خبراء مكتب العلوم والتقنية المرتبط بالبيت الأبيض الأمريكي: بأنه " حق الفرد في أن يُحدد بنفسه ما يتقاسمه مع الآخرين في أفكاره وعواطفه والحقائق المتعلقة بحياته الشخصية".

انظر سامي الشوا ، الغش المعلوماتي كظاهرة إجرامية مستحدثة ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ، 1993م.

انظر أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، الطبعة الثالثة، دار النهضة ، القاهرة ،1994م، ص13.

4) انظر فيما يلي تعريف القضاء الأمريكي للخصوصية:

فارتباط هذا المفهوم في عديد من الدول بحماية البيانات هذا من شأنه وضع الحق في الخصوصية في خانة حماية البيانات الخاصة وجعل الخصوصية تظهر لتفصل بين حق الفرد المطلق وبين حق المجتمع بالتعرض لشؤونه وكل هذا وذلك لا يمنع من وضع جملة تعريفات من قبل القضاء والفقه.

3. التعريفات الفقهية للخصوصية المعلوماتية:

يمكن القول بان الباحث عن تعريف للخصوصية في الفقه[1] وتحديد نطاقها يجدها تختلف باختلاف الزاوية التي يتناول المسألة منها ، فقد يتم توسيع نطاق الخصوصية ليجعلها تختلط بمفهوم الحرية أو يضيق منها فيشتمل على مادياتها فقط، وقد يتناولها بشكل إيجابي أو سلبي باعتبارها نقيض للحياة العامة.

وهناك اتفاق بأن تعريف الخصوصية تعريفاً جامعاً مانعاً من الصعوبة بمكان،[2] وبالرغم من ذلك سنجد العديد من التعريفات للخصوصية، إلا أن هذه التعريفات في الغالبية تمثل صدى لبعضها.

فقد جاء تعريف الحق في الخصوصية بأنه : "حق من طبيعة مادية يرتبط بالشخصية الإنسانية التي لها عليه سلطة تقديرية كاملة"، وذلك من حيث كون هذه السلطة تتكون من مجموعة من الوقائع والعلاقات التي تساهم في تحديد الشخصية، وتضم كافة العلاقات ذات الطابع الشخصي للإنسان مثل الحياة العاطفية ، والأمومة، والحالة الصحية ، وممارسة الشعائر الدينية، والحالة المدنية ، ومحل الإقامة .. إلى غير ذلك.[3]

---

1) على نحو ما درج به مؤلفات الفقهين الفرنسي والعربي في هذا الشأن ، مع اتساع أو ضيق في تناولها لهذه المسألة ، ولهذا فإن الباحث في الخصوصية بوجه عام ، وفي معناها ونطاقها يجد صعوبة في وضع أو اختيار تعريف يمكن الاتفاق عليه بشأنها أنظر في الفقه المصري:

حسام الدين كامل الأهواني ، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دارسة مقارنة، دار النهضة العربية 1978م، ص480.

ممدوح خليل بحر ، مرجع سابق ، 656.

حسني الجندي ، ضمانات حرية الحياة الخاصة في الإسلام ، مرجع سابق ، ص621.

2) أنظر عادل عامر ، بحث بعنوان مفهوم الحق في الحياة الخاصة للأفراد ، منشور على الموقع التالي: تاريخ الزيارة 2015/1/29م-al- http://www.safsaf.com .

3) لمعلومات أكثر حول هذا الموضوع أنظر الموقع التالي: http://www.Juriscim.net

وهنا يجب التنبيه إلى أن تعريف الخصوصية المعلوماتية يتباين من بيئة إلى أخرى إلا أنه هناك قاسم مشترك في جميع هذه التعريفات؛ ألا وهو كون الخصوصية إحدى حقوق الإنسان في حياته ، ولكن تحديد نطاقه يعتمد على البيئة المتواجد فيها ، فمن وجهة نظر روجر كلارك الاستشاري والخبير في خصوصية البيانات والأعمال الإلكترونية ، فإن الخصوصية هي ((قدرة الأشخاص على المحافظة على مساحتهم الشخصية في مأمن من التدخل من قبل منشآت أو أشخاص آخرين)).[1]

فلدى كل شخص مجموعة من البيانات التي تتعلق به والتي تعتبر مهمة جداً في مجال المعلوماتية ، حيث إن هذه الأخيرة مرتبط استعمالها بالمعلومات الخاصة بكل شخص ولا يمكنها الاستمرار أو مواكبة التقدم إلا باستخدام هذه المعلومات، وضخ وتدفق هذه المعلومات للشبكة مع وجوب حمايتها من أي اعتداء ، وبالتالي يظهر مصطلح الخصوصية المعلوماتية.

فالخصوصية المعلوماتية هي حق الأفراد أو المجموعات أو المؤسسات في أن يحددوا لأنفسهم متى وكيف أو إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين،[2] وبالتالي أصبح التجسس على الأسرار والمعلومات الشخصية للأفراد انتهاكاً للخصوصية، حتى لو حدث ذلك في مكان عام ، حيث إن القانون يحمي الأشخاص وليس الأماكن أو الملكية.

ومن خلال ما سبق نستطيع أن نضع تعريفاً للخصوصية المعلوماتية: " وهو الحق في الحصول على حماية للبيانات الخاصة، مادية كانت أو معنوية ، ومنع ومعاقبة أي اعتداء قد يقع عليها " فالخصوصية لا تقتصر على الحماية المادية للشخص من أي اعتداء مادي مباشر على حياته وإنما تذهب لأبعد من ذلك لتشمل أيضاً الجانب المعنوي، كالأفكار والمشاعر والأحاسيس والقوى العقلية .

1) منى تركي الموسوي ، مرجع سابق ، ص4.

2) سوزان عدنان ، انتهاك حرمة الحياة الخاصة عبر الانترنت ، رسالة دكتوراه مقدمة لكلية الحقوق جامعة دمشق ، منشورة بمجلة دمشق للعلوم الاقتصادية والقانونية ، المجلد 29 ، العدد 3 ، 2013م ، ص433.

المطلب الثاني
نشأة خصوصية المعلومات وتطورها

إن أول حقيقة تاريخية تكرس في هذا المجال هي أن فكرة الخصوصية وارتباطها بتقنية المعلومات هي أول المسائل القانونية التي أُثيرت عموماً من الوجهة التاريخية ، وهي أول مناطق التساؤل عن أثر التقنية على النظام القانوني وما آلت إليه . وقد انطلقت في الستينيات وفي أجواء التطور التكنولوجي الواسع وأجواء الاستخدامات المتزايدة لنظم المعلومات وإنشاء بنوك المعلومات، وعمليات المعالجة الآلية للبيانات، وفي سياق حماية الأفراد من مخاطر التقنية التي تتهدد حياتهم الخاصة فتمس على نحو مباشر خصوصياتهم وأسرارهم، ولهذا ارتبطت ولادة مفهوم خصوصية المعلومات بالخشية من مخاطر التقنية ذاتها.

إن الدراسات القانونية الأكاديمية التي عنيت بالخصوصية وبحقوق الإنسان في ضوء التطورات التقنية لا تجاري التطورات الحاصلة في هذا المجال ، ويمكن القول بأن نهاية الستينيات والسبعينيات شهدت انطلاق مثل هذه الدراسات ، وأن هذه الفترة تحديداً هي التي أثير فيها لأول مرة وبشكل متزايد مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية، وتحديداً التدخل المادي ومسائل الرقابة. [1]

ومما سبق يمكن القول: بأن الخصوصية من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصار لمعالجتها آلياً أو إلكترونياً أو تقييد استخدامها وفق

---

1) يعزى الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلفين أمريكيين هامين في هذا المجال ، الأول كتاب الخصوصية والحرية Privacy and Freedom لمؤلفه ويستن Alan Westin عام 1967م أنظر Westin A.F, Privacy and Freedom, New York, Atheneum 1967ad. والثاني كتاب الاعتداء على الخصوصية The Assault on Privacy لمؤلفه ميلر Miller وكلاهما قدما مفهوماً وتعريفاً لخصوصية المعلومات. Miller A, The Assault on Privacy, Ann Arbor, University of Michigan Press. 1971ad ، وفضلاً عن ذلك كتاب قواعد الحياة الخاصة والرقابة العامة Private Lives and Public Surveillance لمؤلفه Rule والمنشور في العام 1973م قد استعرض على نحو شامل ومعمق مسائل جمع واستخدام البيانات الشخصية كوسيلة للسيطرة الاجتماعية وتضمن تفاصيل حالات تطبيقية ودراسية لعدد من الهيئات والقطاعات كنظام ترخيص السائقين البريطاني UK Driver Licensing System ونظام تقارير ائتمان المستهلكين الأمريكي US Consumer Credit Reporting تضمنت بحث ما تقوم هذه الأنظمة بجمعه من بيانات ووسائل الجمع ، ومن له حق الوصول لها وكيف تستخدم ، وكيف يؤثر هذا الاستخدام على صاحب البيانات أنظر:

Rule J.B, Private Lives and Public Surveillance, Social control in the computer Age, New York Schocken Books, 1974ad.

القانون فقط . وفي أمريكا وأوروبا جرى تطوير هذه الفكرة ضمن حزمة شاملة من مبادئ السلوك والممارسات المقبولة ، أهمها تأكيد الاستخدام العادل والمنصف للبيانات الشخصية والتدخل بالحدود الدنيا وتقييد وتضييق أغراض استخدام البيانات وحصر الاستخدام في غرض الجمع.

وقد كان للتطورات التقنية ، وتحديداً إنشاء بنوك المعلومات وإجراء عمليات المعالجة والتحليل بواسطة نظم المعلومات الأثر في خلق مفهوم خصوصية المعلومات بالمحتوى الأسبق في ظل هذه الدراسات الأكاديمية ، وقامت الدول الغربية بسن تشريعات حماية البيانات انطلاقاً من مطلع التسعينات، وترافق ذلك مع دراسات مقارنة بين القوانين الوطنية.[1]

وقد شهدت التسعينيات من القرن الماضي دراسات عديدة في مجال الحق في الخصوصية، ويرجع ذلك للتطورات الحاصلة في مجال التقنية الحديثة وانعكاسها على الخصوصية.[2]

والحق في الوصول للمعلومات مقرر في عدد من الدول مُنذ القدم ، ففي السويد أُقر هذا الحق بموجب قانون حرية الصحافة لعام 1776م الذي يعد أقدم قانون للوصول للمعلومات في العالم ، ومن جديد تعود السويد لتكون أول دولة تضع قانوناً لتنظيم سجلات الكمبيوتر وحماية البيانات؛ وتقود موجة التشريع في هذا المجال من خلال قانون عام 1973م بشأن حماية البيانات.[3]

---

1) Law and Technology Sources of Literature on Data Protection and Human Rights, Adam Warren.
مقال منشور على الموقع التالي تاريخ الزيارة 2015/02/01م
http://www2.warwick.ac.uk/fac/soc/law/elg/gilt/2001_Warren/

2) انظر على سبيل المثال الدراسة أعدها البروفسور Michael بعنوان الخصوصية وحقوق الإنسان ، Privacy and Human Rights ، وتحت إشراف اليونسكو قام المؤلف بتقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالمياً والمفيد في مؤلف Michael أنه استعرض الصعوبات والتباينات الثقافية في استخدام اصطلاح الخصوصية واختلاف المفهوم القانوني للخصوصية أوضح هذا المؤلف ثلاث مواقف (موقف مؤتمر دول الشمال الأوروبي ، موقف النظام القانوني المدني – اللاتيني ، وموقف نظام القانون العام الأنجلو أمريكي) فعرض في نطاق المفهوم الأول ، موقف لقاء الخبراء القانونيين في ستوكهولم عام 1967م الذي نتج عنه إعلان غير ملزم حول معنى الحق في الخصوصية تضمن المبادئ التي قام عليها فيما بعد أول تشريع شمولي لحماية البيانات وهو القانون السويدي لعام 1973م.
James Michael . Privacy and Human Rights (An International survey of privacy laws and practice) UNESCO 1994ad. Publishing on http://www.gilc.org تاريخ الزيارة 2015/02/01م

3) انظر حول هذا الموضوع : دويب حسين صابر، النظام القانوني لحرية الحصول على المعلومات ، دار النهضة العربية ، القاهرة، مصر، 2014م ، ص119 – 127.
وبالموقع التالي : http://www.loc.gov/law/help/online-privacy-law/sweden.php

أما الفهم القائم في نطاق القانون المدني ، فإنه مختلف ، وذلك لقيامه على إقرار المبدأ العام ، وهذا ملحوظ بالأساس من خلال الموقف الأوروبي الذي يظهر أفضل ما يظهر من اتفاقية حقوق الإنسان الأوروبية ، وهو الفهم الذي تقارب معهُ الموقف الأمريكي – رغم انتمائه لطائفة القانون العام ، وعندما جرى توسيع القواعد والمبادئ الدستورية العامة لحماية طائفة من الحقوق كالحق في الخصوصية من أنشطة الرقابة الحكومية متى ما توفر للفرد اعتقاد وتوقع مقبول بخصوصيته.

وإذا كان القانون المدني – اللاتيني – يقوم في تعامله مع الخصوصية ومفهومها على أساس أن القانون العام يطبق مبادئ الحماية وفق الحالات الفردية ، ففي بريطانيا مثلاً والتي تمثل بوضوح هذا النظام ، فإن المكنات التي اعترف بها القضاء – بعيداً عن تدخل المشرع – والحقوق التي أقرت كانت تتعلق بحقوق خاصة في حالات انتهاكات واعتداءات خاصة ، وكأن إقرار الحق يعتمد على مكنات قانونية متباينة ، كقانون السرية أو نصوص القذف والتشهير وغيرها وهذا ما يفسر عدم ورود هذا المفهوم نفسه في قانون حماية الخصوصية صراحة ، وان كانا ينظمان مبادئ حماية البيانات الخاصة والتعامل معها ، مع أن مجموعة القوانين الجديدة من عام 1998م في بريطانيا ، أوجبت تطوير مفهوم الخصوصية كقانون حماية البيانات لعام 1998م ، وقانون حقوق الإنسان لعام 1998م ، وقانون حرية الوصول للمعلومات لعام 1998م أيضاً ، وبالرغم من اعتراف المادة (8) من قانون حقوق الإنسان بالحق في الخصوصية ، فإن هذا التطوير لم يصل إلى إقرار المبدأ ونطاقه ومقتضياته بالقدر المقرر في بقية التشريعات الأوروبية، وفيما اعتمدت عليه هذه القوانين من الأدلة والقرارات الصادرة عن الاتحاد الأوروبي.[1]

في عام 1981م وضع مجلس أوروبا اتفاقية حماية الأفراد من مخاطر المُعالجة الآلية للبيانات الشخصية ، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلاً إرشادياً لحماية

1) انظر في هذا الخصوص عائض المري ، بحث بعنوان الخصوصية وحماية البيانات منشور بالموقع التالي:
http://www.dralmarri.com/show.asp?field=res_a&id=199 تاريخ الزيارة 2015/02/01م.
انظر بحث بعنوان دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي منشور بالموقع التالي:
http://www.startimes.com/f.aspx?t=7280689 تاريخ الزيارة 2015/02/08م.

الخصوصية ونقل البيانات الخاصة ، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الالكترونية للبيانات ، وهذه القواعد تصف البيانات والمعلومات الشخصية[1] على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع Collection والتخزين Storage والمعالجة Processing والنشر Dissemination ، ثم وفي خطوة متطورة على المستوى التشريعي الإقليمي؛ بل وذات أثر عالمي أصدر الاتحاد الأوروبي الأمر التشريعي الخاص بحماية البيانات ونقلها عبر الحدود لعام 1995م ، الذي مثل مرحلة جديدة في إعادة تنظيم خصوصية المعلومات أدت إلى إعادة وضع العديد من دول أوروبا تشريعات جديدة أو تطوير تشريعاتها القائمة في هذا المجال ؛ بل أثر فيما تضمنته من معايير في مجال نقل البيانات خارج الحدود لدرجة جعلت العديد من دول العالم خارج نطاق أوروبا تسعى إلى التواؤم مع ما قرره هذا القانون،[2] ويمكن إيجاز مفهوم حماية البيانات في المواثيق المتقدمة بمراعاة أن تكون البيانات الشخصية:-

1. قد تم الحصول عليها بطريق مشروع وقانوني.
2. تستخدم للغرض الأصلي المعلن والمحدد ولا تكشف لغير المصرح لهم بالإطلاع.
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 وتحمي سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المُعالجة.
7. تتلف عند استنفاذ الغرض من جمعها.

ومن خلال ما سبق نقف على أن خصوصية المعلومات : هي حماية البيانات ، لكن الخصوصية ليست هي حماية البيانات ، فالأخيرة شيء من الخصوصية وتتعلق بمواجهة

---

1) يعتبر بياناً شخصياً أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة ، للمزيد حول مفهوم البيانات الشخصية وصورها انظر : سامح عبدالواحد التهامي ، الحماية القانونية للبيانات الشخصية ، بحث منشور بمجلة الحقوق جامعة الكويت ، مجلس النشر العلمي ، العدد 3 السنة 35 ، 2011م ، ص384 وما بعدها .

2) انظر في ذلك حسين بن سعيد الغافري ، الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الالكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2 إلى 4 يونيو 2008 منشور على الموقع التالي:

http://www.arab-afli.org/old/indx.php?page=43&link=928&sub=938type=conference&id=517 تاريخ الزيارة 2015/02/22م.

الاعتداءات على البيانات الشخصية وتنظيم الحق في البيانات الشخصية وسيطرة صاحبها عليها، في حين أن الخصوصية على إطلاقها ، تنطوي على خصوصية البيانات وخصوصية الاتصالات في مواجهة أنشطة الرقابة والتجسس ، وخصوصية المكان وحرمته في مواجهة أنشطة الاعتداء المادية ، وهي مسائل حرمة المسكن وحرمة الشخص من التفتيش غير القانوني، وأيضاً خصوصية المراسلات ومن ضمنها مراسلات مادية وأخرى إلكترونية ، وغير ذلك من أوجه الحماية ذات الطبيعة أو المحتوى المادي أو المعنوي ولا يعني ذلك تقسيم الحق في الخصوصية ، فهو بوصفه الحق الذي تحمي فيه حياة الفرد الخاصة من كل اعتداء ، أو انتهاك ، أو تدخل مادي ، أو معنوي ، ولهذا فهو يشمل هذه المظاهر وغيرها دون أن ينتقص ذلك من كونه حقاً موحداً ومستقلاً ، فالخصوصية بالعموم تنطوي على حماية مظاهر مادية ومعنوية ومعلوماتية ولا تقف عند حماية البيانات الشخصية، وبالتالي من المهم أن ندرك أن الترادف بوجه عام قائم ما بين اصطلاح خصوصية المعلومات وحماية البيانات ، وليس بين الخصوصية وبين حماية البيانات، أما شيوع استخدام اصطلاح الخصوصية مستقلاً ومنفرداً دون إلحاقه بالبيانات في البيئة الالكترونية للدلالة على حماية البيانات واستخدامه كذلك في الدراسات الأكاديمية وفي الدراسات التقنية وأبحاث وتقرير قطاعات الأعمال ، فهو أمر يرجع إلى أن تعبير الخصوصية صار أكثر شيوعاً خاصة في ظل تزايد مخاطر المُعالجة الآلية للبيانات ، كما أن استخدام اصطلاح الخصوصية في بيئة مواقع الانترنت ومسائل عقود التقنية أو خدمات التقنية عموما يشير إلى حماية الخصوصية المعلوماتية أو حماية البيانات.

المبحث الثاني
نطاق الخصوصية المعلوماتية
والمخاطر التي تهددها

تمهيد

لدراسة أي موضوع والبحث فيه يجب رسم الإطار الذي يُحدد نطاق هذه الدراسة حتى يسهل تناوله ورسم خطوطه العريضة ، ومن هذا المنطلق نتمكن من الإجابة عن عدة تساؤلات منها ما هو الحق المراد حمايته ؟ وما هي المخاطر التي تُهدد هذا الحق؟

غير إن صعوبة وضع تعريف للخصوصية يجعل المهمة صعبة لتحديد نطاق خصوصية المعلومات ، وهذا يستتبع بالتأكيد صعوبة تحديد ما يعترضها من مخاطر.

ولكن بالبحث سنجد أن هُناك مُحاولات كثيرة من الفقه والقضاء وكذلك من المنظمات وفي الاتفاقيات الدولية لوضع تعريف للخصوصية وكذلك الخصوصية المعلوماتية ، وفي ضوء كل ذلك سيتم تحديد نطاق خصوصية المعلومات ، وبيان المخاطر التي تُهدد هذه الخصوصية.

ولذلك سيتم تناول هذا المبحث في مطلبين:

المطلب الأول: نطاق الخصوصية المعلوماتية.

المطلب الثاني: المخاطر التي تُهدد الخصوصية المعلوماتية.

المطلب الأول
نطاق الخصوصية المعلوماتية

يستخلص جانب من الفقه[1] عناصر رئيسة للحق في الحياة الخاصة تلتقي عندها – كحد أدنى – الآراء المتباينة بشأن تعريف هذا الحق ، أولها " اقتران الخصوصية بالانسحاب من الوسط أو العالم المحيط ، وربطها من ثم بفكرة الخلوة أو العزلة " ، ووفقاً لذلك تتمثل غاية هذا الحق – كما يحدده بعض الفقه – بضمان السلام والسكينة لهذا الجانب المنعزل من الحياة غير المتصل بالأنشطة العامة بجعله بمنأى عن التقصي والإفشاء غير المشروعين، وثانيهما الاعتراف للشخص بسلطة الاعتراض على التدخل في خصوصياته من جهة، وسلطة الاعتراض على وصول معلومات تتعلق بخصوصياته إلى الغير من جهة آخرى ".[2]

لقد أصبحت تكنولوجيا الاتصالات ، مثل الانترنت والهواتف الذكية النقالة والأجهزة العاملة بالاتصال اللاسلكي بالانترنت ، جزءاً من الحياة اليومية . وبإدخال تحسينات جذرية على إمكانية الوصول إلى المعلومات والاتصال الفوري ، عززت الابتكارات في مجال تكنولوجيا الاتصالات حرية التعبير ويسرت النقاش.

حيث تُعد الشبكة العنكبوتية (الإنترنت) وسيلة الاتصال الأولى بالعالم في هذا العصر. وبسبب انتشارها وتنوع خدماتها وانخفاض تكلفة الوصول إليها نسبياً ، أصبح العالم مجتمعاً افتراضياً ، ويمكن أفراده من التفاعل مع بعضهم ومشاركة معارفهم (Knowledge Sharing).

وفي العصر الرقمي، عززت تكنولوجيا الاتصالات أيضاً قدرات الحكومات والمؤسسات والأفراد على القيام بأعمال المراقبة واعتراض الاتصالات وجمع البيانات، كما زاد التقدم التكنولوجي من فعالية القيام بعمل المراقبة حيث أنها لم تعد محدودة من حيث النطاق والمدة ، ومما ساعد

---

1) يقول هشام رستم : أن للخصوصية وجهين متميزين ، مادي ، وقوامه عدم إقحام النفس في خصوصيات الآخرين والتدخل في شؤونهم الخاصة ، والخصوصية منظوراً إليها من هذه الوجهة مادية Physical Privacy حسب الوصف الذي يطلقه عليها بعضهم.
والثاني إعلامي: ومقتضاه ألا تكون الشؤون الخاصة بالفرد محلاً للحق في الإعلام بالنسبة للغير ، وهو ما يستتبع عدم استخدام الآخرين معلومات تتعلق بحياة الفرد الخاصة ؛ والخصوصية من هذا الوجه –كما يسميها بعضهم– إعلامية Informational Privacy.
انظر هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، الطبعة الأولى ، مكتبة الآلات الحدية ، أسيوط ، مصر ، 1992م، ص 176–178.

2) المرجع السابق ، ص 178.

على ذلك انخفاض تكاليف التكنولوجيا وتخزين البيانات ، وتملك الدول حالياً من القدرات أكثر من أي وقت مضى للقيام بعمل مراقبة متزامنة واقتحامية ومحددة الهدف وواسعة النطاق. [1]

إن مفهوم خصوصية المعلومات يعني حق الإنسان في التحكم بوصول الآخرين وإطلاعهم على معلوماته الشخصية حتى وإن كانت هذه المعلومات لدى جهات أخرى مُخولة بحفظها أو حفظ بعضها : (مثل السجل الطبي للمريض لدى المستشفى) ، وتشمل البيانات الشخصية للمستخدم كل المعلومات المتعلقة بجوانب حياته الخاصة كاسمه، وعمره، ومكانه وسجلاته الطبية والمالية، وغيرها مما يتعلق بشخصه.

ومما يدخل في نطاق الخصوصية للإنسان مراعاة الشركات والمؤسسات لخصوصية معلومات موظفيها وعملائها ، فهذه المؤسسات مسؤولة قانونياً عن حماية المعلومات الشخصية التي تحفظها من المتطفلين أو غير المخولين ، ويجب اقتصار استخدامها على الخدمات التي يتم الاتفاق مع العميل على تقديمها له.

وكذلك المعلومات التي يتم جمعها من قبل الجهات الحكومية ، حيث يقع على هذه الأخيرة مسؤولية حماية هذه المعلومات ، فالخطورة تتمثل فيما قد يقع على هذه المعلومات من تزوير في المحررات الرسمية باستخدام جهاز الحاسب الآلي في تغيير إقرار أولى الشأن، حيث أنه ومن خلال التطور التكنولوجي الذي دأبت على استخدامه الكثير من المرافق الحيوية والمتمثل في استخدام جهاز الحاسب الآلي لتنظيم التعاملات في هذه الجهة أو تلك ، يُمكن الموظف المختص بالقسم المعلوماتي من التلاعب بالمعلومات والبيانات لمصلحته أو لمصلحة غيره ، الأمر الذي يمكن معه تحقيق التزوير المعلوماتي. [2]

كما إن خصوصية المعلومات تشمل أيضاً المعلومات التي يتم تبادلها عن طريق الهواتف المحمولة من برامج ومعلومات ورسائل ، فيجب أن يتم توفير حماية لمثل هذه المعلومات من أي

---

1) انظر في ذلك محمد حلمي محمد رمضان ، الحماية الجنائية للمحادثات الهاتفية، رسالة ماجستير مقدمة لكلية الحقوق ، جامعة الإسكندرية ، 2008م. انظر هشام فريد رستم ، مرجع سابق، ص 176-178.

2) لمعلومات أكثر حول هذا الموضوع راجع على محمد قاسم الطلي ، جريمة التزوير في المحررات الرسمية في القانون اليمني، رسالة ماحستير مقدمة لكلية الحقوق جامعة عدن ، اليمن ، 2006م ، ص 49-61.

انتهاك أو تعدّ على خصوصية المعلومات الخاصة بهم، [1] فإن معرفة سبل حماية خصوصية معلوماتك أثناء استخدامك للانترنت ووسائل الاتصالات والتقنية الحديثة يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع والذي يلحق الضرر بك معنوياً أو مادياً.

ففي الآونة الأخيرة ظهرت العديد من الانتهاكات لهذا الحق تتمثل في إساءة استعمال البيانات والمعلومات المتعلقة بالأفراد ؛ فالمعلومات التي يتم تجميعها وتخزينها لابد وأن يكون لها هدف واضح ومُحدد سلفا، ولابد من التزام الجهة القائمة على النظام المعلوماتي بالهدف الذي من أجله قامت بتجميع ومُعالجة المعلومات.

غير أن الواقع عكس ذلك تماماً حيث تشهد يومياً خروقات من خلال تجاوز شركات الاتصالات للهدف الذي تم من أجله تجميع المعلومات ومُعالجتها عن العملاء، حيث يُعاني الكثير من المواطنين من رسائل الدعاية القصيرة التي تصل إلى الهواتف المتنقلة دون الحصول على إذن خطى مسبق من العميل يسمح فيه باستقبال هذه الرسائل ، ويظهر ذلك أيضاً من خلال رسائل البريد الالكتروني الدعائية التي تصل إلى الأفراد دون علم منهم كيف ومتى تم الحصول على المعلومات المتعلقة بعنوان بريدهم الالكتروني. [2]

علاوة على ذلك فالهدف من جمع المعلومات عن الأفراد يجب أن يكون مرتبطاً بمهمة ووظيفة الجهة القائمة على التخزين ، وهذا الأمر تنبهت له المحكمة الدستورية في ألمانيا حيث جاء في أحد قراراتها " أنه لا حرية رأي أو حرية اجتماع ولا حرية مؤسسات يمكن أن تمارس كاملة ما دام الفرد غير متيقن في ظل أي ظروف ولأجل أي هدف جمعت عنه المعلومات الفردية وعولجت آلياً في الحاسوب".[3]

---

1) لمعلومات أكثر حول هذا الموضوع راجع محمد رشاد إبراهيم مفتاح ، الحماية الجنائية للحق في حرمة الاتصالات ، رسالة دكتوراه مقدمة لكلية الحقوق ، جامعة الإسكندرية ، 2009م. انظر هشام فريد رستم ، مرجع سابق، ص 176-178.

2) ومن الخروقات التي تحصل من الشركات التي تجمع البيانات الشخصية للأفراد ما تقوم به شركات البطاقات الائتمانية ، التي تراقب السلع المشتراة بالبطاقة، ويتم بعد ذلك استغلال المعلومات التي جمعت عنك والمعلومات التي قمت بإعطائها عند الاشتراك في خدمة البطاقة الائتمانية كرقم هاتفك وبريدك الالكتروني لإرسال مجموعة من الدعايات المتعلقة بميولك الشرائية ، وهذا كله يشكل تعدٍ صارخ للخصوصية .

3) راجع مقال منشور على صفحة المركز الوطني لحقوق الإنسان، بعنوان قانون جرائم أنظمة المعلومات والحق في الحياة الخاصة، منشور على الموقع التالي :http://www.nchr.org تاريخ الزيارة 2015/01/31م.

كما أن السماح بجمع البيانات أو المعلومات عن الأشخاص مع عدم معرفة أوجه استخدامها في المستقبل يمثل أحد الأخطار التي تهدد الحياة الخاصة للأفراد ، ويظهر هذا الخطر جليا من خلال بنوك المعلومات التي تنشئها شركات التأمين والأموال والبنوك وغيرها من المؤسسات التي تقوم بجمع معلومات تتعلق بحياة عملائها الشخصية أو الصحية أو عن حجم معاملاتهم ومنافسيهم ، وغير ذلك من معلومات قد يتم استغلالها بطريقة غير مشروعة في المستقبل.[1]

1) انظر بحث بعنوان مفهوم الحق في الحياة الخاصة للأفراد منشور على الموقع التالي :
http://www.mudwen.com/index.php?ajax=prewiew&id=4847 تاريخ الزيارة 2015/2/18م

المطلب الثاني
المخاطر التي تهدد الخصوصية المعلوماتية

كتب الفقيه الفرنسي Mellor في عام 1971م، إن الكمبيوتر بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها ، وما يتصف به من دقة واستمرار ما يخزن فيه يقلب حياتنا رأساً على عقب ، يخضع فيها الأفراد لنظام رقابة صارم ، ويتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا ومُعاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد.[1]

ومع تزايد إقبال الناس للاستفادة من ايجابيات استخدام الانترنت ، ظهر الشعور بمخاطره وتهديداته أيضاً ، وتنامي هذا الشعور مع زيادة حالات الاعتداء على البيانات الشخصية للمستخدمين واستخدامها بشكل غير قانوني.[2]

إن الخطر تعاظم باستخدام وسائل الكشف والمعالجة التقنية ، وكان لزاماً أن تظهر وسائل تقنية أيضاً لمواجهة هذا الخطر ، لكن الحماية عبر الوسائل التقنية تأتي لاحقة على المخاطر

---

1) راجع حول هذا الموضوع في الموقع التالي:
http://www.usdoj.gov/criminal/cybercrime/cybercrime/johnson2html

2) وتبدأ عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية أو يهدد أمنها ابتداءً من قطع مصدر الكهرباء عن الكمبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد أو أكثر من وسائل الاختراق عبر نقاط الضعف مروراً بإساءة الموظفين. للتوضيح أكثر انظر عائض المري ، بحث بعنوان أمن المعلومات وماهيتها وعناصرها وإستراتجيتها ، منشور على الموقع التالي: http://www.draalmarri.com/show.asp?field=res_a&id=205 تاريخ الزيارة 2015/04/22م.

ويحدث الاعتداء على الحق في الخصوصية عادة من عدة وجوه:

1. نشر وإعلان مفردات الحياة الخاصة للشخص في وسائل الإعلام والاتصالات والمختلفة دون موافقة الصريحة أو الضمنية ، ذلك أن حق الفرد في الخصوصية في مجال المعلومات يعني حق الفرد في أن يُقرر بنفسه متى ، وكيف وإلى آي مدى يمكن أن تصل المعلومات الخاصة به إلى الآخرين ، والرضاء بالمعلومة أو التحري عن الحياة الخاصة لا يعني بالضرورة الموافقة على نشرها.
2. يحمي القانون الخصوصية وما يتعلق بها من معلومات مثل الصداقات والحالة الصحية والعاطفية والأسرية، ويخرج عن نطاقها المعلومات المتعلقة بالحياة العامة للشخص ، ولا تثور صعوبة بالنسبة للأفراد العاديين ، ولكن تدق التفرقة ما بين الأعمال المتعلقة بالحياة الخاصة والمتعلقة بالحياة العامة حيث يكون الحد الفاصل بينهما من الصعب التحكم فيه بالنسبة للأشخاص الذين يشغلون مناصب أو أعمال عامة مثل رجال السياسة والاقتصاد أو العلوم والفنون.
3. وتزداد حدة المسألة بالنسبة لحماية الخصوصية في مجال الانترنت والمعالجة الآلية للبيانات حيث تبدو مخاطر انتهاك حرمة الحياة الخاصة للأفراد من خلال تبادل وتخزين المعلومات فيما بين مراكز وبنوك المعلومات ، وكذلك عدم قدرة شبكة المعلومات على توفير الأمان المطلق والسرية الكاملة لتلك المعلومات كما يمكن استخدام الشبكة نفسها في الحصول على المعلومات بصورة غير مشروعة.

وللتوضيح أكثر انظر محمد حسين منصور، المسئولية الالكترونية ، دار الجامعة الجديدة للنشر، الإسكندرية، ص 365، وما بعدها.

والاختراقات التقنية ، لهذا تظل المخاطر أسبق في الحصول ، وتظل الحماية في موضوع متأخر عنها.

الفرع الأول: تأثير تقنية المعلومات على الحياة الخاصة

تمكن تقنية المعلومات من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزنة في ملف معين ، بالمعلومات في قاعدة بيانات أخرى ، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة ، وهذا يكشف بوضوح حجم التهديدات الواقعة على الخصوصية.

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

إن استخدام نظم المعلومات في ميدان جمع ومُعالجة البيانات الشخصية المتصلة بالحياة الخاصة للفرد خلف أثاراً إيجابية عريضة ، لا يستطيع أحد إنكارها، خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية وغيرها ، وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات ، والتي تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه، كبنوك المعلومات القانونية مثلاً ، أو قد تكون شاملة لمختلف الشؤون والقطاعات ، وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص ، كمراكز وبنوك معلومات الشركات المالية والمصارف وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي.[1]

وبفعل الكفاءة العالية لوسائل التقنية والإمكانيات غير المحدودة في مجال تحليل واسترجاع المعلومات ، فقد اتجهت دول العالم بمختلف هيئاتها ومؤسساتها إلى إنشاء قواعد البيانات لتنظيم

---

1) ويطلق عليها في اللغة الإنجليزية Data Banks .

انظر أسامة عبدالله قايد ، مرجع سابق ، ص 48. محمد حسام محمود لطفي ، بنوك المعلومات وحقوق المؤلف، القاهرة 1996م، ص3 وما بعدها.

عملها،[1] واتسع على نحو كبير استخدام نظم المعلومات لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية ، ومع إحساس المجتمعات لإيجابيات استخدام نظم المعلومات في هذا المضمار ظهر بشكل متسارع أيضاً الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية.

فهذا الانتشار في استعمال التقنية يصاحبه أيضا التخوف من الانتهاكات التي قد تقع على المعلومات التي يتم جمعها بواسطتها ، فالجرائم المرتبطة باستخدام التقنيات الحديثة عديدة ومتنوعة ، وبشكل عام يمكن أن تصنف جرائم التقنية الحديثة والحاسب الآلي إلى صنفين :-

- جرائم ذات الجانب الاقتصادي : وذلك كالاحتيال المعلوماتي ، أو التجسس في نطاق الأعمال بهدف توظيف هذه المعلومات والبيانات ضد المجني عليه ، وقرصنة برامج الحاسب الآلي ، وإتلاف المعلومات سواء كانت البيانات نفسها أم الوسائط التي تحمل هذه البيانات وسرقة الخدمات والاستعمال الغير مصرح به لنظام الحاسب الآلي.
- الجرائم المتصلة بانتهاك حرمة الحياة الخاصة : وذلك باللجوء إلى أساليب غير مشروعة للحصول على بيانات صحيحة عن الأفراد بطريق غير مشروع ، أو إفشاء بيانات شخصية ، وهي التي تمس الأمور الجوهرية في حياة الأفراد. [2]

إن الشعور بخطورة هذه التقنية نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة، مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراعاتها حماية الحق في الحياة الخاصة ، وبالضرورة إيجاد التوازن بين حاجات المجتمع لجمع وتخزين ومُعالجة البيانات الشخصية ، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع للتقنيات.[3]

---

1) راجع حول انتشار استخدام التقنيات الحديثة وبالمقابل تأثيرها على الخصوصية ، حسين بن سعيد الغافري ، مرجع سابق.

2) راشد بن حمد البلوشي ، الدليل في الجريمة المعلوماتية ، بحث منشور في مجلة الحقوق، كلية الحقوق، جامعة الإسكندرية، مصر، العدد الأول ، 2008م ، ص10.

3) انظر أعمال الأمم المتحدة في ميدان حقوق الإنسان ، المجلد الأول ، منشورات هيئة الأمم المتحدة ، نيويورك 1990م.
ومن ضمن الأعمال كذلك تبني الاتحاد الأفريقي اتفاقية بشأن الأمن السيبراني وحماية البيانات، انظر مقال منشور حول هذا الموضوع على الموقع التالي :http://www.moehaner.net تاريخ الزيارة 2016/09/20م ، كذلك برنامج اليونسكو في هذا المجال بعنوان (الوصول إلى المعلومات وحماية الحريات الأساسية- هذا حقك) منشور على موقع المنظمة :http://www.unesco.org تاريخ الزيارة 2016/09/20م.

الفرع الثاني: التهديدات التي تواجه الخصوصية في ظل العصر الرقمي

تعبيراً عن تلك المخاطر يقول كل من " Jerry Berman و Mulligan Deirdre" أن تتصور أنك تسير في أحد مخازن الأسواق بين مخازن عديدة لا تعرف أياً منها ، فتوضع على ظهرك إشارة تبين كل محل زرته وما الذي قمت به وما اشتريته ، إن هذا شئ شبيه لما يمكن أن يحصل في بيئة الانترنت.

وكما ذكرنا سابقاً بأن الكفاءة العالية لوسائل التقنية الحديثة يسرت العمل في مجالات عديدة ، الأمر الذي دفع بدول العالم للاستعانة بها سواء في مجالات القطاع العام أو استخدامها من قبل القطاع الخاص ، وعلى الرغم من المميزات التي تحظى بها هذه الوسائل إلا أنها غير آمنة بالمطلق، فقد تتعرض هذه الوسائل إلى العديد من الاعتداءات ، [1] وهذا ما ثبت بالفعل من خلال الانتهاكات التي تحصل بشكل شبه يومي وتكبد مستخدمي هذه التقنية خسائر فادحة، حيث تقول دراسة أشرفت عليها شركة (ماك في) لحماية برامج الانترنت : أن هذه الانتهاكات تكلف الاقتصاد العالمي خسائر تقدر ما بين 375 و575 مليار دولار سنوياً؛[2] وبالتالي فإن التهديدات التي تواجه الخصوصية تتمثل في ما يلي:

1. الانترنت يجمع كميات هائلة من المعلومات:

هناك ارتفاع متزايد تشهده شبكة الانترنت في جمع البيانات المتوفرة في العالم الحقيقي.[3] وذلك لسهولة الوصول إليها ، وكذلك المقدرة على تبويبها وتصنيفها بسرعة وبشكل ملائم ، الأمر

---

1) والاعتداءات الناتجة عن استخدام وسائل التقنية الحديثة متنوعة ولا تقع على الخصوصية فقط فهذه المخاطر عديدة منها :

أ- مخاطر على الأمن القومي (التجسس الالكتروني ، الحرب الالكترونية).

ب- القرصنة عبر الانترنت.

ج- الجرائم المنظمة والمافيا عبر الانترنت.

د- غسل الأموال عبر الانترنت.

هـ- تجارة المخدرات عبر الانترنت.

راجع في ذلك: محمد احمد ابو سن ، الجرائم الالكترونية وأدلة إثباتها بين الواقع الماثل والمثال المأمول ، ورقة عمل مقدمة للمؤتمر الثالث لرؤساء المحاكم العليا ، الخرطوم ، السودان ، من 23 إلى 25 سبتمبر 2012م ، ص2 إلى 4.

2) انظر تقرير مفصل حول قرصنة الانترنت بعنوان ، القرصنة الالكترونية سلاح العصر الرقمي ، على الموقع التالي: http://www.algzeera.net/knowledgegate/2gnewscover تاريخ الزيارة 2016/02/13م.

3) ويقابل هذا المصطلح مصطلح العالم الافتراضي الذي يكثر استخدامه في مجال شبكة المعلومات الدولية (الانترنت) والاتصالات والتقنية الحديثة.

الذي يرجع لما يوفره الحاسب الآلي من تقنيات عالية، وبالتالي أصبحت المعلومات يتم تبادلها بشكل سهل عن طريق برامج التصفح والتبادل والنقل ، وهذا ما جعل الانترنت وسيلة رائجة عند غالبية الناس وأصبح الاعتماد عليها أكثر في الحصول على المعلومات وتتبع مصدرها بالمقارنة مع الوسائل التقليدية الأخرى ؛ لأن الانترنت مصدر غني بالمعلومات حول كل شئ، وفي نطاق مسائل الخصوصية تحديداً، فإن المعلومات عن الأفراد وعاداتهم وهواياتهم وسلوكياتهم وآرائهم واتجاهاتهم صارت متاحة ويمكننا الوصول إليها بسهولة ويسر، وهذا قد يضع هذه المعلومات في خطر الاستعمال السيئ لها.

2. التحديات القانونية في مواجهة عولمة الشبكة العنكبوتية للمعلومات والاتصالات:

يشكل الكم الهائل من البيانات التي يجري تداولها عبر الانترنت أحد مصادر الصعوبات التي تعوق التحقيق في الجرائم التي تقع عليها أو بواسطتها، [1] فالانترنت خلاف الواقع لا يحتوي على حدود وهذا من شأنه أن يجعل المعلومات تنساب بسهولة من كافة أرجاء العالم بلا قيود غير مبالية بالتقسيمات الجغرافية الموجودة في أرض الواقع، وهذا من شأنه أن يفتح الباب في مواجهة أخطار سوء الاستخدام التي قد تتعرض لها البيانات التي يتم تناقلها عبر شبكة المعلومات ، ويظهر هذا جلياً في الدول التي لا تتوفر فيها الحماية القانونية الملائمة للبيانات الشخصية ، فإن وضع نصوص في القوانين الوطنية لغرض التحكم في نقل البيانات لا تؤدي الغاية المرجوة، ألا وهي حماية البيانات من الاستخدام السيئ لها، فهذا يتطلب بالإضافة لحمايتها عن طريق القوانين الوطنية وجود اتفاقيات تضمن حماية نقل البيانات وتوفر تنسيقاً بين هذه الدول لتكفل حمايتها .

فالجرائم المرتكبة عن طريق وسائل التقنية الحديثة المربوطة بالشبكة المعلوماتية تتميز بصعوبة كشفها والتحقيق فيها ، فالوصول إلى الدليل الرقمي تعترضه عقبات من ضمنها كون الجناة متمرسين في هذا المجال، فهم يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف

1) صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية ، جامعة مولود معمري، تيزي وزو ، الجزائر ، 2013م ص129 .

أمرهم ، يضاف إلى ذلك كله تضاؤل خبرة أجهزة العدالة الجنائية من مأموري الضبط وسلطة التحقيق والمحاكمة ؛ إذ يفتقر هؤلاء إلى التأهيل الكافي في هذا الميدان. [1]

وتعد المخاطر أوسع مع وجود دول لا تقيد عمليات المعالجة بأي قيد ولا تتوفر عندها قيود على جمع ومُعالجة البيانات ، وهنا تظهر إمكانية استغلال بيئة الانترنت وقيام المؤسسات بتهريب أعمالها وذلك للإفلات من القيود القانونية ، تماماً كما في حالات البحث عن أماكن لا تُفرض فيها الضرائب، أو تتيح تبادل الأموال دون رقابة . [2]

فمن الناحية العملية يواجه المحققون تحديات كبيرة في فحص جميع البيانات فذلك أمر مكلف ويستغرق في العادة وقتاً طويلاً ، وفي واقع الأمر أن المسألة تزداد تعقيداً حينما يكون محل البحث هو الشبكة المعلوماتية (الانترنت) بخصوص الجرائم عبر الوطنية ، إذ يصبح ضبط الدليل والبحث عنه أمراً في غاية الصعوبة إن لم يكن مستحيلاً أحياناً على اعتبار أن التفتيش والضبط في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدول وفي نطاق دولة أخرى. [3]

وهذا يمثل تحدياً عالمياً وليس مجرد تحدي وطني ، ولعل هذا التحدي هو الأساس الذي يدفع نحو إبرام اتفاقيات ثنائية وعالمية في مجال حماية البيانات الشخصية عبر الحدود وهو نفس الأساس الذي أوجب إيجاد الأدوات العقدية التي تفرض على الجهة متلقية البيانات أو الوسيط في تلقيها لإرسالها لطرف ثالث ، وكل هذه التزامات قانونية معينة تدور في مجموعها حول هدف حماية الخصوصية ومنع إساءة استخدام بيانات الأفراد الخاصة إلى جانب منع الأنشطة الاحتيالية والمساس بالمستهلك في بيئة الانترنت.[4]

---

1) لمعلومات أكثر حول هذا الموضوع راجع موسى مسعود ارحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، تحت تنظيم أكاديمية الدراسات العليا طرابلس، ليبيا ، في الفترة من 28 إلى 29 أكتوبر 2009م ، هلال بن محمد بن حارب البوسعيدي ، الحماية القانونية والفنية لقواعد المعلومات المحوسبة ، رسالة ماجستير ، معهد البحوث والدراسات العربية القاهرة ، دار النهضة العربية ، القاهرة ، مصر ، 2009 ، ص 239-263.

2) انظر مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية ، القاهرة ، 2001م ، ص 21.

3) موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق،ص4-5.

طارق الجملي ، الدليل الرقمي في مجال الإثبات الجنائي ، بحث منشور في مجلة الحقوق ، كلية الحقوق ، جامعة البحرين، البحرين، المجلد 12 ، العدد الأول ، ص 59-66.

نوفل على عبدالله الصفو ، بحث بعنوان: جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، المجلة المصرية للدراسات القانونية والاقتصادية ، مصر ، العدد الثالث ، يناير 2015م ، ص20.

4) انظر مدحت عبدالحليم رمضان ، مرجع سابق ، ص 21 وما بعدها.

3. فقد المركزية والتحديات المترتبة عليها:

إن الانترنت وسيلة عالمية من مميزاتها سهولة انتقال البيانات وعدم ملكية احد لهذه الوسيلة في النقل وهذا من شأنه بالتأكيد أن يُفقد مركزية التحكم في هذه الوسيلة وبالتالي لا تتوفر جهة سيادية معينة توفر الحماية في حالة وقوع الاعتداء ومحاولة إيجاد الحل في وضع تشريع وطني أو وضع خطط إستراتجية ملائمة لحماية حقوق الأفراد أمر مهم ومؤثر وذلك لغرض فرض السيادة على هذه التقنية وإيجاد عنصر السيطرة عليها وبالتالي ملاحقة المخالفين وكذلك التعويض عن مخالفاتهم. [1]

بالرغم من حقيقة أن الصراع يحتدم على السيطرة على الانترنت ، من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع ، والتنافس للسيطرة على سوق استضافة المواقع عبر المواقع الالكترونية ، والتوجه أحياناً للسيطرة على المعلومات وطرق تبادلها عبر التحكم بالحلول التقنية واحتكارها لتكون وسيلة التحكم بمصائر المستخدمين وإدارة السيطرة الفعلية بالرغم من كل ذلك ، ومع ما يرافقه من نشاط مضاد لمنع الاحتكار المعلوماتي ، فإن الانترنت تتصف باللامركزية وغياب السلطة التحكمية وليس دعوات إنشاء حكومة الانترنت أو بوليس الانترنت أو معايير الاستخدام الموحد أو سياسات التنظيم الذاتي للالتزامات إلا وسائل افتراضية شأنها شأن البيئة التي نشأت فيها ، ومن هنا يكون لبعض مسائل التعاون الدولي أهمية بالغة ، أبرزها الاتفاق في مجال الاختصاص القضائي والقانوني الواجب التطبيق في بيئة منازعات الانترنت.[2]

حيث يُعد الانترنت أكبر آلة لجمع ومُعالجة ونقل للبيانات الشخصية ، كما أن تطوير نظم المعلومات الرقمية وتكنولوجيا الشبكات ، وبشكل خاص الانترنت أتاح نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلى العالم الافتراضي – البيئة

---

2)إن فقد المركزية من أهم التحديات التي تواجه سلطات التحقيق أثناء قيامهم بملاحقة المخالفين ، فيصعب على هذه السلطات معرفة مكان وقوع الجريمة ، كما يصعب عليهم تحديد المسئول جنائياً ، وهذا ما يجعل التهرب من إجراءات الدعوى الجنائية أمراً ميسوراً، لمعلومات أكثر انظر : غنام محمد غنام ، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم بإستعمال شبكة الإنترنت ، دار الفكر والقانون ، المنصورة ، مصر ، الطبعة الأولى ، 2016م ، ص227-238.

2) راجع في ذلك Ulrich Sieber, legal Aspects of Computer –Related Crime in The Information Society-Com Crime Study Prepared For The European commission version 1.0 Of 1st January 1998ad.

الالكترونية – ويوماً بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف أنشطة الحياة، وفي نفس الوقت فإن التطور الثقافي في توظيف التقنية رافقه توجه واسع بشأن حماية خصوصية الأفراد ، ففي العالم الرقمي وعالم شبكات المعلومات العالمية يترك المستخدم آثاراً ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة والأمور التي بحث عنها ، والمواد التي قام بتنزيلها ، والرسائل التي أرسلها، والخدمات والبضائع التي قام بطلبها وشرائها، إنها سجلات تتضمن تفاصيل دقيقة عن شخصية وحياة وهوايات وميول المستخدم على الشبكة وهي سجلات مُبرمجة ذات محتوى شخصي يتصل بالفرد والأشخاص ومشترياتهم.[1]

والتصفح والتجول عبر الانترنت يترك لدى المواقع التي تم زيارتها كمية واسعة من المعلومات على الرغم من أن جزءاً من هذه المعلومات لازم لإتاحة الربط بالانترنت والتصفح، وبمجرد الدخول إلى صفحة الموقع فإن معلومات معينة تتوفر عن المستخدم ، وهو ما يعرف بمعلومات رأس الصفحة (Header Information) وهي التي يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الانترنت ، وهذه المعلومات تتضمن:

1. عنوان بروتوكول الانترنت الخاص بالمستخدم (IP) ومن خلاله يمكن تحديد اسم النطاق وتبعاً له تحديد اسم الشركة أو الجهة التي قامت بتسجيل الدخول عن طريق نظام أسماء المنظمات وتحديد موقعها.
2. المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادي المستخدمة من قبله.
3. وقت وتاريخ زيارة الموقع.
4. مواقع الانترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل زيارة.
5. وقد تتضمن أيضاً معلومات محرك البحث الذي استخدمه المستخدم للوصول إلى الصفحة وتبعاً لنوع المتصفح يظهر عنوان البريد الالكتروني للمستخدم.

1) Jerry Berman & Deirdre Mulligan, privacy in the Digital Age :Work in Progress, Nova law Review, The internet and law, Volume 23, November 2 winter 1999, x. P. 6 .

6. وأيضاً تبعاً لتشغيل المستخدم أوامر خاصة حول إدارة التعامل مع الشبكة تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وبيان المعلومات التي أرسلت واستقبلت.[1]

والعديد إن لم يكن كافة المواقع وتحديداً مواقع النشاط التجاري والتجارة الإلكترونية على الانترنت ، تتطلب من المستخدم تقديم وتعبئة نموذج يتضمن معلومات مختلفة ، سواء أكان في معرض الاشتراك بخدامات معينة أو التسجيل أو الانضمام لمجموعات النقاش أو حتى لإجراء تعليق أو إرسال رسالة ، وتتضمن هذه المعلومات اسم المستخدم وعنوانه للعمل والمنزل وأرقام الهاتف والفاكس وعنوان البريد الالكتروني ومعلومات حول السن والجنس والحالة الاجتماعية ومكان الإقامة والدخل الشهري أو السنوي وأحياناً اهتمامات الشخص ، وأما مواقع البيع والشراء على الانترنت والمواقع التي يتم فيها إجراء عمليات دفع فإنها تتطلب رقم بطاقة الاعتماد ونوعها وتاريخ انتهائها.[2]

بالرغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالمية فإنها أيضاً أوجدت خطراً حقيقياً تمثل بإمكانية جمع المعلومات وتخزينها والاتصال بها والوصول إليها ، وجعلها متاحة وقابلة للاستخدام من قبل مختلف قطاعات الأعمال والأجهزة الخلوية – الهاتف النقال – بدون علم أو معرفة صاحب المعلومات.

---

1) لمعلومات أكثر حول هذا الموضوع راجع الموقع التالي:
http://www.arablaw.org/download/privacy&itsecurity_article تاريخ الزيارة 2015/12/25م.

2) انظر في شروط وحماية الخصوصية على مواقع الانترنت على سبيل المثال:
http://www.microsoft.com/windows/messenger/ar/privacypolicy/asp
http://wwwgoogle.com/intl/ar/privacy.html
http://www.etisalat.co.ae/html_arabic/custom_info/privacy.htm

الفصل الثاني

آليات الحماية الدولية للخصوصية المعلوماتية

تمهيد

إن الاستعمال المتزايد لتكنولوجيا المعلومات وتدخلها في شتىّ جوانب الحياة – لاسيما الحياة الخاصة – يستوجب التدخل لتنظيم تدفق المعلومات والبيانات الخاصة وحمايتها من الانتهاكات التي قد تقع عليها ، وهذا ما جعل المنظمات الدولية والإقليمية تتحرك لتعقد المؤتمرات وتنشئ اللجان لمنع الانتهاكات ولاظفاء نوع من الحماية عليها .

ولعل أهم هذه المنظمات منظمة الأمم المتحدة التي صدر عنها العديد من المبادرات ومنها مبادرة الأمم المتحدة بإنشاء اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين وعقدها العديد من المؤتمرات أهمها مؤتمر هافانا بكوبا عام 1990م.

وفي الواقع لم تكن المنظمات الدولية فقط هي من اهتمت بتقديم كل ما من شأنه توفير الحماية للخصوصية المعلوماتية ، فقد قامت المنظمات الإقليمية وعلى رأسها الاتحاد الأوروبي بإصدار التوصيات ووضع البرامج التي تكافح الاستعمال السيئ لشبكات المعلومات ، وذلك لغرض حماية الخصوصية المعلوماتية والحد من الانتهاكات التي قد تقع عليه ، ولهذا سيتم دراسة هذا الفصل وفقاً للتقسيم التالي:-

المبحث الأول: الجهود الدولية لحماية الخصوصية المعلوماتية.

المبحث الثاني: الجهود الإقليمية لحماية الخصوصية المعلوماتية.

المبحث الأول
الجهود الدولية لحماية الخصوصية المعلومـــــــاتية

تمهيد

لقد شكلت المنظمات – سواء كانت العامة أو المتخصصة – الإطار القانوني الملائم لتوحيد الجهود الدولية في مجال حماية الخصوصية المعلوماتية من الانتهاكات التي تقع عليها، وقد أوجبت هذه الانتهاكات وما تشكله من مخاطر ضرورة تكثيف الجهود من قبل المجتمع الدولي لمواجهة هذه التحديات، فقامت العديد من المنظمات الدولية بالعمل على إيجاد الحلول لحماية البيانات والمعلومات الخاصة.

وهذا الاهتمام بحماية الخصوصية من قبل جميع المنظمات الدولية أو الإقليمية ، التي أعدت بشأنه الاتفاقيات والمؤتمرات، كان من شأنه أن يساعد في استقرار جذور فرع آخر من فروع القانون الدولي المتعلق بحقوق الإنسان وهو القانون الدولي الإنساني. [1]

ولعل أهم البرامج في هذا المجال هو برنامج الأمم المتحدة والمنظمات التابعة لها، كذلك المنظمة العالمية للملكية الفكرية (Wipo) ومنظمة التعاون الاقتصادي والتنمية التي بدأت من عام 1978م بوضع قواعد إرشادية بشأن حماية الخصوصية ونقل البيانات.[2]

وترتيباً على ما تقدم فإن الدراسة في هذا المبحث ستوزع على مطلبين:

المطلب الأول: جهود الأمم المتحدة والوكالات التابعة لها .

المطلب الثاني: جهود منظمة التجارة العالمية ومنظمة التعاون الاقتصادي والتنمية.

المطلب الأول

1) احمد أبو الوفا ، الوسيط في القانون الدولي العام ، دار النهضة العربية ، القاهرة ، مصر ،الطبعة السادسة، 2016م ، ص582.

2) لمعلومات أكثر حول هذا الموضوع راجع الموقع التالي :
http://www.fcdrs.com/h-articales.php?act=view_articales&aid=100

جهود الأمم المتحدة والوكالات التابعة لها

لعبت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة دوراً مهماً في الحفاظ على الأمن والاستقرار ، وخاصة في مجال مواجهة الجريمة المعلوماتية [1] عبر إقرار العديد من الاتفاقيات وعقد المؤتمرات أهمها مؤتمر منع الجريمة ومُعاملة المجرمين كما أنشأت وكالاتها المتخصصة لهذا الغرض كمنظمة الأمم المتحدة للتربية والعلم والثقافة (UNESCO)،[2] وكذلك المنظمة العالمية للملكية الفكرية (WIPO). [3]

فإن مفهوم الحق في الخصوصية ظهر في الإعلان العالمي لحقوق الإنسان في عام 1948م[4] والذي كفل حماية الأماكن والاتصالات.[5] كما أن العديد من اتفاقيات حقوق الإنسان

---

1) إن الواقع الحالي يتميز بتدخل وسائل التقنية الحديثة في شتى مجالات الحياة ، الأمر الذي صاحبه ظهور نوع جديد من الجرائم "الجرائم المعلوماتية"، ولهذا النوع من الجرائم تعريفات عديدة من الناحية الفقهية حيث إنه في الأصل لا يقوم المشرع بوضع التعريفات، وإنما يكتفي بتجريم الفعل وتحديد أركانه ، إلا أن القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات قد عرفها بأنها " كل فعل مؤثم يتم ارتكابه عبر أي وسيط إليكتروني" ، أما الفقه فقد وضع لهذه الجريمة العديد من التعريفات منها " الاستخدام غير المشروع للحاسبات " ، للإطلاع أكثر حول التعريف بالجريمة المعلوماتية أنظر: عبدالفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، منشأة المعارف، الإسكندرية مصر، الطبعة الأولى، 2009م ، ص 14 وما بعدها .

أنظر أيضاً : عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشأة المعارف، الإسكندرية مصر ، د ط ، د ت ، ص 464-467.

فتحي محمد أنور عزت ، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دار النهضة العربية ، القاهرة مصر ، ص277 وما بعدها .

2) The United Nation Educational Scientific and Cultural Organization

3) world intellectual property organization

4) نصت المادة 12 من الإعلان العالمي على أنه ((لا يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه ولكل شخص الحق في حماية القانون من قبل هذا التدخل أو تلك الحملات)).

5)راجع في ذلك المواقع التالية:

http://www.un.org/ar/documents/udhr/ http://www.unhchr.ch/html/menu3/b/a_ccpr.html تاريخ الزيارة 2015/08/20م.

العالمية اعترفت بالحق في الخصوصية كالعهد الدولي للحقوق المدنية والسياسية (ICCPR)[1] واتفاقية الأمم المتحدة للعمال المهاجرين واتفاقية الأمم المتحدة للطفولة وغيرها.

وهنا يظهر لنا جلياً دور المنظمات الدولية في توفير الحماية للخصوصية عامة وخصوصية المعلومات خاصة.

الفرع الأول: دور الأمم المتحدة.

لم يكن للحق في الخصوصية تلك الأهمية إلا بعد تبني الأمم المتحدة له كحق أساسي، فقد تولد عن اجتماع لجنة حقوق الإنسان التابعة للأمم المتحدة إصدار قائمة دولية للحقوق والحريات الأساسية للإنسان سميت (بالإعلان العالمي لحقوق الإنسان) فكان الحق في الخصوصية أحد الحقوق التي تضمنها هذا الإعلان،[2] والدليل على ذلك أن هذا الحق لم يذكر في أي دستور من دساتير الدول المتحضرة إلا مؤخراً.

وتجدر الإشارة إلى أن الأمم المتحدة حاولت بقوة إضفاء عنصر الإلزام للإعلان ، وذلك بعد أن اقترح ممثلو العديد من الدول الاعتراف له بالقيمة القانونية ، إلا أن أغلب الدول اتجهت إلى اعتباره ذو قيمة أدبية فقط وغير ملزم لها من الناحية القانونية، [3] ولأجل حماية هذه الحقوق من أي انتهاك قد يقع عليها أنشأت الأمم المتحدة لجاناً لرسم الخطط ووضع السياسة في مجال منع الجريمة.

---

1) International Covenant on Civil and Political Rights

2) محمد أنس جعفر،احمد محمد رفعت ، حقوق الإنسان ، مركز جامعة القاهرة للتعليم المفتوح ، 1991م ، ص61 .

3) راجع في هذا الموضوع المقارنة بين الإعلان العالمي لحقوق الإنسان والاتفاقية الأوروبية لحقوق الإنسان ، عبدالعزيز محمد سرحان ، الاتفاقية الأوروبية لحماية حقوق الإنسان ، دار النهضة العربية ، د ت ، ص27 .

وفي هذا النطاق تُعقد مؤتمرات دورية كل 5 سنوات، [1] وذلك لتبادل الخبرات بين المتخصصين في هذا المجال ومن مختلف البلدان لتدعيم التعاون الدولي لمكافحة الجريمة، ولعل أهم هذه المؤتمرات في هذا السياق " المؤتمر السابع لمنع الجريمة ومُعاملة المجرمين"، الذي انعقد في مدينة ميلانو بإيطاليا في سنة 1985م (منع الجريمة من أجل الحرية والعدالة والسلم والتنمية)[2]، حيث أوصى هذا المؤتمر بضرورة تطبيق التطورات التي تحدث في مجال التكنولوجيا والتي من شأنها إفراز أنواع جديدة من الجرائم.

ومن هذا المنطلق يجب اتخاذ كل ما من شأنه أن يحول دون وقوعها وبالتالي وضع التدابير التي تكافح إساءة استعمال هذه التكنولوجيا، فكان لحماية الخصوصية نصيب من هذا المؤتمر وما يمكن أن يقع عليها من انتهاكات ، وذلك بالاطلاع على البيانات الشخصية المخزنة، كما أشار المؤتمر إلى ضرورة تشجيع التشريعات التي تُجرم الأفعال الإجرامية التي ترتكب عن طريق الحاسوب من ذلك انتهاك الخصوصية المعلوماتية.

ولم تقف جهود الأمم المتحدة عند هذا الحد بل واصلت جهودها عبر عقد عدة مؤتمرات أهمها المؤتمر التاسع لمنع الجريمة ومُعاملة المجرمين والذي عُقد في القاهرة عام 1995م، وكان من أهم توصياته العمل من أجل حماية حياة الإنسان الخاصة وملكيته الفكرية في مواجهة مخاطر

---

1) إن المؤتمرات التي تعقدها المنظمات بخصوص مكافحة الاعتداء على الحق في الخصوصية عديدة ولعل أهم هذه المؤتمرات (المؤتمر الدولي لحقوق الإنسان الذي عقد في طهران عام 1968م ، مؤتمر حقوق الإنسان المنعقد بمونتريال كندا عام 1968، المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في ري ودي جانيرو بالبرازيل) لمعلومات أكثر حول هذا المؤتمرات وغيرها انظر: محمد رشاد القطعاني ، الحماية الجنائية للحق في حرمة الاتصالات الشخصية ، دار الفتح ، الإسكندرية ، مصر، الطبعة الثانية ، 2014م ، ص47–56 .

2) اللجنة الاستشارية لخبراء منع الجريمة تجتمع كل 5 سنوات وقد عقدت عديد المؤتمرات ، ابتدءاً من:
جنيف ، سويسرا 1955م / لندن ، بريطانيا 1960م / استوكهولم ، السويد 1965م / كيوتو ، اليابان 1970م / جينيف ، سويسرا 1975م / كركاس ، فنيزويلا 1980م / ميلانو ، إيطاليا 1985م / هافانا ، كوبا 1990م / القاهرة ، مصر 1995م / فيينا ، النمسا 2000م / بانكوك ، تايلاند 2005م / سلفادور ، البرازيل 2010م / الدوحة ، قطر 2015م. انظر الموقع التالي:
http://www.aljazeera.net/encyclopedia/events/2015/4/21 تاريخ الزيارة 2016/02/13م.

التكنولوجيا، والعمل كذلك على التنسيق وتعزيز التعامل بين أعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد من المخاطر التي قد تواجهها.

الفرع الثاني: دور منظمة اليونسكو في حماية الخصوصية المعلوماتية.

من أهداف الأمم المتحدة تنمية العلاقات الودية ودعمها بين الدول وحفظ السلام وتحقيق التعاون الأمني في مواجهة الجرائم ذات البعد الدولي ، ومن هذه الجرائم ((الجرائم المعلوماتية)) وذلك عن طريق المصادقة على العديد من الاتفاقيات الدولية ذات الصلة بالموضوع ، أهمها (الاتفاقية العالمية لحق المؤلف) فقد انبثقت هذه الاتفاقية عن منظمة اليونسكو بتاريخ 6 سبتمبر 1952م إذ نصت على أنها اتفاق خاص ضمن إطار اتفاقية (برن) لحماية المصنفات الأدبية والفنية ، والتي تهدف لتسهيل انتشار نتاج العقل البشري وتعزيز التفاهم الدولي.[1]

ولعل ما يجب التنبه لهُ في هذه الاتفاقية أنه يؤخذ عليها عدم البيان بشكل مُحدد ما هي المصنفات محل الحماية بل أعطت لها أمثلة وأوكلت الأمر في تحديدها للمبادرات التي تصدر عن التشريعات المحلية للدول المصادقة عليها وهذا ما نصت عليه نص المادة الثانية من الاتفاقية، [2] فالأمر مختلف تماماً في بقية المعاهدات والتي تنص صراحة على المصنفات محل الحماية من خلال بنود طويلة،[3] وهنا يظهر لنا أن حماية الخصوصية المعلوماتية لم يكن هو بيت القصيد في هذه الاتفاقية.

---

1) محمد الأزهر ، حقوق المؤلف في القانون المغربي ، دراسة مقارنة في الملكية الأدبية الفنية، دار النشر المغربية، 1994م، ص 61-62.

2) نصت المادة الثانية من الاتفاقية على تحديد المصنفات التي تتمتع بالحماية ، فقامت بتعريف المصنفات الأدبية والفنية (م1/2) بأنه "كل إنتاج في المجال الأدبي والعلمي والفني أياً كانت طريقته أو شكل التعبير عنه .." وجاء هذا التعريف بأمثلة عديدة لهذه المصنفات تاركاً التشريع الوطني في كل دولة من دول الاتحاد أن تقصر الحماية على المصنفات التي تتخذ شكلاً مادياً معيناً (م2/2).

3) ومنها اتفاقية (تريبس) للتدابير المتعلقة بأثر التجارة على حقوق الملكية الفكرية لعام 1994م، والاتفاقية العربية لحقوق المؤلف لعام 1981م والتي حددت المصنفات في المادة الأولى والثانية .

وإن كان يمكن تطويع بعض نصوصها لخدمة هذا الغرض ، ويمكن أن يرجع السر في ذلك إلى أن الاعتداءات على الخصوصية المعلوماتية في ذلك الوقت لم تكن بالصورة التي هي عليها الآن في العصر الرقمي حيث ظهر فيها الإعلان الصريح عن موضوع الحماية للبرامج وذلك ضمن نصوص الاتفاقية التي تُعنى بالجوانب المتصلة بالملكية الفكرية ، ولكن ما يؤخذ على هذه الاتفاقية أيضاً هو توسيعها محل الحماية ليشمل برامج الكمبيوتر ، وهذا أمر خطير لما لهذه الأخيرة من وضع خاص يستوجب حماية خاصة.

الفرع الثالث: دور منظمة الويبو (Wipo) [1] في حماية خصوصية المعلومات

الويبو (Wipo) أو المنظمة العالمية للملكية الفكرية تعتبر المنتدى العالمي للخدمات والسياسة العامة والتعاون والمعلومات.

وهي وكالة من وكالات الأمم المتحدة ، ويبلغ عدد أعضائها 188 دولة عضو، ومهمتها حماية الملكية الفكرية ووضعها في موضع ريادي لتشجيع الابتكار والإبداع ، وتم تأسيسها بموجب اتفاقية (Wipo) لعام 1967م،[2] ولعل الحديث عن منظمة الويبو ودورها في حماية الخصوصية المعلوماتية يجعلنا نسلط الضوء على أهداف المنظمة.

أولاً- أهداف المنظمة:

ولتوضيح دور المنظمة في مواجهة الجرائم الالكترونية والاعتداء على الخصوصية لا ضير من إيضاح أهداف المنظمة:

---

1) world intellectual property organization

2) لمزيد من المعلومات حول دور منظمة الويبو في حماية الخصوصية المعلوماتية وبرامج الحاسب الآلي راجع : عبدالرحمن جميل محمود حسين ، الحماية القانونية لبرامج الحاسب الآلي ، رسالة ماجستير مقدمة لكلية الدراسات العليا جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2008م ، ص 86-90، وكذلك موقع المنظمة :http://www.wipo.int

- إيجاد قواعد دولية متوازنة للملكية الفكرية.
- حماية الملكية الفكرية عبر الحدود وتسوية المنازعات وذلك لتشجيع الإبداع والابتكار.
- الربط بين أنظمة الملكية الفكرية وتبادل المعارف.
- مساعدة البلدان النامية باعتبارها إحدى منظمات الأمم المتحدة وتكوين الكفاءات لتمكين جميع البلدان لاستخدام الملكية الفكرية لأغراض التنمية الاقتصادية والاجتماعية والفكرية.[1]

ولهذه المنظمة أهمية كبرى في مجال الاقتصاد الدولي ، فقد اهتمت هذه المنظمة اهتماماً كبيراً ببرامج الكمبيوتر من أوائل إنشاءها ، وقامت أيضاً بدعم تنفيذ الاتفاقيات التي لها علاقة بها وذلك لغرض حماية الملكية الفكرية في جميع أنحاء العالم ، وهو ما يستتبع بالضرورة الحديث عن دور المنظمة في حماية الخصوصية المعلوماتية.

ثانياً- دور المنظمة في حماية الخصوصية المعلوماتية:

لقد عملت المنظمة على تبني نصوص تشريعية لحماية برامج الحاسب الآلي حيث قامت بتعريفه واعتبرته " مجموعة تعليمات يمكنها إذا ما وضعت على ركيزة يستوعبها الجهاز ، أن تحقق نتيجة ما بواسطة هذه الآلة القادرة على التعامل مع المعلومات "، كما قامت بإعداد نصوص نموذجية من خلال جمع عدد من الخبراء من شتى أنحاء العالم من أجل مساعدة الدول على استكمال تشريعاتها في مجال حماية البرامج أو مجرد توضيحها.[2]

---

1)http://www.wipo.int : موقع المنظمة مرجع سابق.

2) محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر ، القاهرة ، الطبعة الأولى ، 1987م ، ص 161.

فالتطورات التي حدثت في مجال المعلوماتية سهلت من عملية تبادل البيانات، فقد يتواجد مستخدم الحاسب الآلي في بلد ويقوم بنقل المعلومات لشخص آخر في بلد آخر، الأمر الذي يجعلها عرضة لانتهاك خصوصيتها ، ولذلك شرعت المنظمة في وضع نصوص أو تبني تشريعات مستقلة مثل تشريعات حق المؤلف وتشريعات تتضمن حماية أسرار التجارة وتحضر المنافسة غير المشروعة ، في حال عجز هذه التشريعات لوحدها بالصورة التي هي عليها على أن تبسط الحماية.

ولعل السبب وراء ذلك في ما يمثلهُ هذا التوحيد في القضاء على ما ينتج عن نقل المعلومات من مشاكل ولتحقيق هذا الغرض قامت بوضع نصوص لحماية البرامج وضحت فيها المصنفات محل الحماية ، وقد شملت هذه المصنفات " البرنامج ، وصف البرنامج، المستندات الملحقة به " إلا أنه يُعاب على هذه الصياغة تضييقها لمحل الحماية ووجوب استبدالها بنص أشمل لا يقتصر على هذه المصنفات فقط.

وبما أن هذه النصوص قد وضعت سنة 1978م ولما لهذه الانتهاكات من صفة مُتجددة، وما يشهده واقع الحياة من تجدد استوجب الوضع ضرورة تشريع نصوص اتفاقية دولية جديدة لمواجهة الاعتداءات المتزايدة التي تطال المجال المعلوماتي.

المطلب الثاني
جهود منظمـــة التجـــارة العالميـــة
ومنظمة التعاون الاقتصادي والتنمية

إن الجرائم الالكترونية باتت تشكل تحدياً كبيراً فلا يكاد يمر علينا وقت إلا ويحدث فيه انتهاك على شخص ما وفي مكان ما عن طريق الوسائل المعلوماتية الحديثة ، حيث يشهد العالم جريمة كل (3) دقائق عبر شبكة الانترنت ، كما أن معدلات القرصنة الالكترونية سجلت عام 2008م أعلى زيادة في نحو أربعة أعوام سببت خسائر تجاوزت 48 مليار دولار في العام المذكور وفقاً لدراسة أعدتها جمعية مُنتجي برامج الكمبيوتر التجارية.[1]

وهذا ما دفع المجتمع الدولي إلى تكثيف الجهود لمكافحة هذا التهديد الذي لا يُسبب خسائر اقتصادية فقط، وإنما يُهدد الجميع في خصوصية بياناتهم ومعلوماتهم الشخصية ، فأخذت المنظمات على عاتقها عقد المؤتمرات وسن الاتفاقيات لمواجهة هذا النوع من الجرائم وهذا ما كان من منظمة التجارة العالمية ومنظمة التعاون الاقتصادي والتنمية .

الفرع الأول: دور منظمة التجارة العالمية.

لطالما كانت منظمة التجارة فاعلة في مجال مُكافحة أي شكل من أشكال انتهاك حُرمة البرامج وخصوصيتها من النسخ والتقليد التي تتعرض لها وذلك من خلال عقدها لاتفاقية تريبس

1) راجع في ذلك مقال منشور بعنوان أبو غزالة: العالم يشهد جريمة الكترونية كل ثلاث دقائق ، 25/مارس/2009م، على الموقع التالي: http://www.agip.com تاريخ الزيارة 2015/10/05م.

(TRIPS)،[1] فلهذا أوجبت المنظمة حماية البرامج من القرصنة التي قد تتعرض لها وفي ذلك تتفق مع المنظمة العالمية للملكية الفكرية.[2]

فقد نصت الاتفاقية في المادة (9) على علاقتها مع معاهدة برن ، وكذلك نصت في المادة (10) منها على الحماية التي تتمتع بها برامج الحاسب الآلي وتجميع البيانات سواء كانت مقروءة آلياً ، أو بأي شكل آخر ، كما نصت في المادة (11) على حقوق التأجير فيما يتعلق ببرامج الحاسب الآلي وجاء نص المادة (12) لمدة الحماية الممنوحة للأعمال السابقة.[3]

ولكن ما يُؤخذ على هذه الاتفاقية أنها لم تتناول مدى التزام الدول بالنصوص الواردة في الاتفاقية ، ولم تُعالج مسألة تعارض نصوص الاتفاقية مع نصوص التشريعات الوطنية للدول الأعضاء وكل هذا يؤدي إلى مشاكل عند وضع النص موضع التطبيق ، فهذا من شأنه أن يُخلف نوعاً من الفراغ التشريعي الأمر الذي قد يُستغل من قبل القراصنة للإفلات من العقاب.

كما أنه من العيوب التي لم تُعالجها الاتفاقية مسألة الفيروسات[4] بالرغم من خطورة هذا الأمر وبالرغم من أن أغلب الاعتداءات التي تحصل تكون بهذه الصورة ، الأمر الذي يستوجب توفير قدر من الحماية ضد هذا النوع من الانتهاكات، مما يقتضي النص صراحة على تجريم مثل هذه الأفعال ، والنص على صور مثل هذه الاعتداءات ، وما يكفل ذلك هو وضع تشريع لغرض الحماية من هذه الاعتداءات.

---

1) إن المصادقة على اتفاقية تريبس هو شرط إلزامي من شروط عضوية منظمة التجارة العالمية ، فأي دولة تسعى للحصول على سهولة الوصول إلى العديد من الأسواق العالمية المفتوحة من قبل منظمة التجارة العالمية يجب أن تسن قوانين الملكية الفكرية الصارمة من قبل تريبس.

2) لمعلومات أكثر حول برامج المنظمة في مجال التجارة وموضوعات الملكية الفكرية راجع موقع المنظمة التالي: http://www.wtoarab.org. تاريخ الزيارة 2015/10/25م.

3) جابر فهمي عمران ، منظمة التجارة العالمية ، دار الجامعة الجديدة ، الإسكندرية ، مصر ، 2016م ، ص 532-534.

4) ويمكن تعريف الفيروس بأنه " برنامج يلج إلى جهاز الحاسب الآلي ويقوم بتدمير البرامج و المعلومات المسجلة فيه إما بإتلافها أو حذفها أو تدوينها " أنظر : محمود احمد طه ، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت ، دار الفكر والقانون ، المنصورة مصر ، 2016م ، ص47- 48..

إلا أنه على الرغم من كل الانتقادات التي وجهت لها تعتبر هذه المجهودات التي بذلت من المنظمة مبادرة جيدة ضد الاعتداءات التي قد تقع على برامج الكمبيوتر وخصوصيتها.

الفرع الثاني: دور منظمة التعاون الاقتصادي والتنمية.

منظمة التعاون الاقتصادي والتنمية كانت أول منظمة تثير مسألة الحماية الدولية للخصوصية المعلوماتية في عام 1980م،[1] وسعت المنظمة لتدعيم الثقة بالتجارة الالكترونية وبيئة التقنية والاتصالات ، وذلك من خلال إيجاد الطرق التي تسهل تطبيق مبادئ حماية الخصوصية في بيئة الانترنت والتقنية الحديثة ، وقد عملت المنظمة عمل حثيث في هذا المجال فصدر عنها (دليل لحماية الخصوصية في مجال الانترنت لعام 1980م)، [2] وهذا الدليل نص على ضرورة قيام الدول والجهات التي تعتمد على التقنيات الحديثة على رسم الخطط والاستراتجيات وتبني خطط وسياسات تقنية لضمان حماية الخصوصية في المجال المعلوماتي (الانترنت) ، كما طالب التقرير بضرورة قيام الجهات المعنية بحملات توعية واسعة بخصوص المسائل المتعلقة بحماية الخصوصية واستخدام التقنيات الحديثة، كما دعا أيضاً الجهات الصناعية ، وجهات الأعمال والمستخدمين الحكوميين ، وسلطات حماية البيانات لمناقشة المستجدات المتصلة بحماية البيانات الشخصية في بيئة الشبكات.

---

1) Implementing The OECD " privacy Guidelines" In Electronic Environment : Focus The Internet, 27 may 1998ad P6 , Published on http//www.oecd.org تاريخ الزيارة 2015/12/25م

2) يعرف هذا الدليل باسم (قواعد OECD الإرشادية بشأن حماية الخصوصية ونقل وتدفق البيانات الشخصية) ، وهي قواعد إرشادية لا تتمتع أحكامها بالصيغة الإلزامية ، وتقتصر على الأشخاص الطبيعيين وتسري على كلا القطاعين الحكومي والخاص، لمعلومات أكثر انظر: محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت والجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع، عمان، الأردن ، 2011م ص75- 77.

وبتاريخ 16–17 فبراير 1998م تم عقد ورشة عمل تحت عنوان حماية الخصوصية في مجتمع الشبكات العالمية والتي قامت بها اللجنة الاستشارية للأعمال الصناعية (BIAC) [1] بناءاً على التقرير المشار عليه سابقاً، [2] وذلك لوضع آليات تضع الدليل الصادر من منظمة التعاون الاقتصادي والتنمية موضع التطبيق في ظل التشريعات الوطنية للأعضاء في المنظمة ، وهذا من أجل حماية الخصوصية المعلوماتية وتحفيز القطاعات الخاصة ووضع نظام لحماية البيانات الشخصية في مجال الشبكات المعلوماتية.

وقد كانت لهذه الورشة مجموعة من المحاور الرئيسية وهي:

- التعريف باحتياجات القطاع الخاص والمستخدمين والمستهلكين وذلك لوضع إستراتجية الغرض منها التعريف بالخصوصية.
- تطوير تقنيات حماية الخصوصية.
- تطبيق التشريعات المتعلقة بالخصوصية ووضع معايير في هذا الشأن للقطاع الخاص.
- تبني حلول تعاقدية نموذجية من أجل تدفق ونقل البيانات خارج الحدود. [3]

وبعد البحث في هذه المحاور الأربعة توصلت هذه الورشة إلى ضرورة تشجيع انتشار الوسائل التقنية لحماية الخصوصية ، وذلك لتحقيق النمو المطلوب والأساسي في مجال التقنية الالكترونية والتجارة الالكترونية ، كما تم التأكيد على ضرورة توفير الحماية اللازمة للخصوصية في بيئة الشبكات الأمر الذي له فضل المحافظة على الحقوق من جهة وضمان منع اعتراض تدفق

1) Business and Industry Advisory Committee .

2) Workshop on "privacy protection in global networked society" published on: http//www.oecd.org تاريخ الزيارة 2015/12/25م

3) المرجع السابق.

المعلومات والبيانات خارج الحدود من جهة أخرى، والتي لا تتأتى بدون الشفافية والفاعلية في أنٍ واحد ، وكذلك تبني الحلول التكنولوجية الملائمة.

كما أوصت بإجراء دراسات مسحية للقواعد والتعليمات القانونية والقوانين والعقود والتقنيات وذلك لغرض بيان مدى فعالية تطبيق القواعد المقررة في بيئة الشبكات ، كما أوصت الورشة بأنه يتعين تحديد السياسات التقنية والأدوات القانونية اللازمة لضمان حماية فعالة للخصوصية.

المبحث الثاني

الجهـــود الإقليميـــة لحمـــاية الخصوصية المعلوماتية

تمهيد

لم تتوقف الجهود لمكافحة الاعتداءات التي قد تقع على الخصوصية المعلوماتية على مجهودات المنظمات الدولية فقط ، فكانت للمنظمات الإقليمية دوراً فعالاً ، وكل هذا يرجع إلى خطورة هذه الاعتداءات وما تلحقه من ضرر ، فهذه الجرائم من شأنها أن تضرب أهم عناصر أمن المعلومات وهي "السرية، سلامة المحتوى ،و توفر المعلومات".

ومن هنا برزت على المستوى الإقليمي عدة جهود لمكافحة الجرائم المعلوماتية والاعتداء على الخصوصية ، ولعل أهمها مجهودات المجلس الأوروبي والذي يسعى لتوحيد جهود دول الاتحاد لمواجهة هذه الاعتداءات ، وكذلك مجهودات من قبل منظمات إقليمية أخرى مثل جامعة الدول العربية ، وعليه سيتم تناول هذا المبحث من خلال تقسيمه إلى مطلبين:

المطلب الأول: حماية الخصوصية المعلوماتية في إطار الاتحاد الأوروبي.

المطلب الثاني: حماية الخصوصية المعلوماتية في إطار الدول العربية.

المطلب الأول
حماية الخصوصية المعلوماتية
في إطار الاتحاد الأوروبي

برزت مجهودات المجلس الأوروبي والسوق الأوروبية المشتركة [1] بوضع مُعاهدة مجلس أوروبا، والخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات للتوقيع في يناير 1981م. وقد بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر 1985م، وكان كل ذلك الجهد نتيجة اهتمام لجنة الوزراء في المجلس بمسألة الخصوصية مُنذ عام 1968م، والتي انطوت على توجيهات بصدد وجوب توفير قواعد تكمل حماية البيانات الشخصية من مخاطر المُعالجة الآلية. [2]

وبذل المجلس الأوروبي جهوداً عديدة في مواجهة الاستخدامات الغير مشروعة للحاسب الآلي وشبكات المعلومات ، حيث بدأ الاهتمام بالمشاكل التي تنشأ عن الانتهاكات في المجال المعلوماتي في سبعينيات القرن الماضي ، وقد اتجه بدايةً إلى حماية البيانات الشخصية حتى لا يؤدي الاستعمال المتزايد للحاسب الآلي في الخدمات إلى تهديد حق الأفراد في الخصوصية، وفي عام 1981م تم التوقيع على الاتفاقية الخاصة لحماية الأفراد من إساءة استخدام البيانات المُعالجة إلكترونياً وضرورة الحصول على البيانات الشخصية بوسائل مشروعة ، وأن يكون الغرض الذي تم جمع البيانات من أجله مشروعاً، وتكون المعلومات صحيحة ومتفقة مع الغرض من جمعها.

---

1) للدول الأوروبية دور فعال في حماية الحياة الخاصة من الانتهاكات التي قد تقع عليها من جراء المعالجة الآلية للبيانات ، فقد كان لأوروبا فضل السبق في إنشاء تنظيم إقليمي لحماية حقوق الإنسان ، وذلك بإقرار الدول الأوروبية للاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية بتاريخ 4 نوفمبر 1950م ، والتي تعد خطوة إيجابية صادرة عن المجتمع الدولي لحماية حقوق الإنسان، انظر : ابراهيم علي بدوي الشيخ ، الميثاق العربي لحقوق الإنسان دراسة في خلفيته ومضمونه وآثره على الأمن القومي العربي والنظم السياسية في الوطن العربي ، دار النهضة العربية ، القاهرة ، مصر ، 2004م ، ص 30 ، وانظر أيضاً : محمد رشاد القطعاني ، مرجع سابق ، ص 40–45

2) محروس نصار غايب، الجريمة المعلوماتية ، مجلة التقني ، العراق ،العدد 24 السنة التاسعة، 2011م، ص 119. يونس عرب، الخصوصية وحماية البيانات في العصر الرقمي، بحث منشور على الموقع التالي: http://www.omanlegal.net تاريخ الزيارة 2016/04/06م

والملاحظ أن كل ما تم بيانه في خصوص المبادئ لا يختلف عما صدر عن مجلس التعاون الاقتصادي والتنمية لعام 1980م في شكل توصيات وإن كان الفارق يكمن في ما تتمتع به اتفاقية المجلس الأوروبي من إلزامية باعتبارها اتفاقية مُلزمة للأطراف، حيث ركزت الاتفاقية على ضرورة التعاون المحلي والإقليمي في ملاحقة مُرتكبي هذه الجرائم، وإيجاد التدابير اللازمة والقواعد الملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع احترام الحق الأساسي في السيادة.

الفرع الأول: حماية الخصوصية المعلوماتية في اتفاقية المجلس الأوروبي عام 1981م[1].

جاءت نصوص اتفاقية المجلس الأوروبي لعام 1981م (الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات) بناءً على مجهودات إقليمية ، حيث تم تضمين الاتفاقية الإشادة بالجهود التي تم إنجازها من قبل المنظمات الدولية، كالأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية ، كما أن هُناك عناصر أساسية تم التركيز عليها في الاتفاقية وهي:

- ضرورة وضع نصوص تكافح جرائم الكمبيوتر "نصوص موضوعية للتجريم".
- ضرورة تشريع نصوص إجرائية لتطبيق النصوص الموضوعية.
- مواصلة العمل لمكافحة الجرائم المعلوماتية والتعاون الدولي والإقليمي في هذا المجال.[2]

---

1) تم التوقيع على هذه الاتفاقية من خمس عشرة دولة بتاريخ 28 يناير 1981م ونظراً إلى الأثر الكبير الذي أحدثته هذه الاتفاقية في كفالة حماية البيانات الشخصية المعالجة آلياً فقد صدرت العديد من التوصيات لتوسيع نطاقها بحيث تشمل حماية البيانات الطبية الشخصية المستعملة للبحوث العلمية والإحصائية والقانونية ، أنظر : محمود إبراهيم غازي ، الحماية الجنائية للخصوصية والتجارة الإلكترونية ، مكتبة الوفاء القانونية ، الإسكندرية ، مصر ، الطبعة الأولى ، 2014م ، ص 198– 200

2) لمعلومات أكثر حول هذه الاتفاقية انظر الموقع الخاص بالمجلس الأوروبي : http://www.coe.int تاريخ الزيارة 2014/10/28م.

كما أن لهذه الاتفاقية أهدافاً ، حيث تُشدد على ضرورة التعامل في مجال مُكافحة الجرائم المعلوماتية على الصعيدين الإقليمي والدولي ، وتحث على وضع نصوص تشريعية بين الدول الأوروبية والدول الغير أوروبية المنضمة للاتفاقية ، وتفعيل الوسائل والبرامج التي تهدف إلى الحفاظ على سرية المعلومات وخصوصيتها ، وتكافح الاستعمال السيئ لشبكات المعلومات وكذلك وضع النصوص الموضوعية في ميدان مكافحة جرائم الكمبيوتر على المستوى المحلي والدولي ، وإدخال التعديلات على قانون الإجراءات بما يتناسب مع الطبيعة الخاصة لهذه الجرائم ، فالمادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان تنص على أن "كل شخص له الحق في حرمة حياته الخاصة وحياة عائلته ، ومنزله وعلاقاته الأسرية، ومراسلاته".[1]

حيث ركزت الاتفاقية على ضرورة رسم خطة إجرائية للتحقيق والتحري والمحاكمة، كما نصت على ضرورة إيجاد التوازن بين ما تم الاتفاق عليه في اتفاقية مجلس أوروبا لحماية حقوق الإنسان وحريته لعام 1950م، والعهد الدولي للحقوق المدنية والسياسية لعام 1966م وغيرها من الاتفاقيات في ميدان حقوق الإنسان، وتحديد الحقوق المتصلة بالرأي وحرية الوصول للمعلومات، وبين الحق في الخصوصية والاستفادة من عناصر الملكية الفكرية. [2]

أي أن ما تهدف إليه الاتفاقية هو مُكافحة الجرائم المعلوماتية والانتهاكات التي قد تمس الخصوصية دون أي تأثير على حقوق الأفراد في الوصول إلى المعلومات أو أن تتأثر من الاحتكار والاستغلال غير المشروع للمعرفة ، وجاء في المادة الأولى من الاتفاقية بيان الهدف منها

---

1) Art8/1 "Everyone has the right to respect for private and family life, his home and correspondence".

انظر نصوص الاتفاقية الأوروبية لحقوق الإنسان على الموقع التالي
http://www.gypsy-triveller.org/resources/challenging-racism/promoting-inclusion/human-rights-act/
تاريخ الزيارة 2014/10/30م

2) مرجع سابق الموقع الخاص بالمجلس الأوروبي : http://www.coe.int تاريخ الزيارة 2014/10/28م.

وهو " حماية الأفراد وحماية حياتهم الخاصة فيما يتعلق بالمعالجة الآلية للمعلومات بغض النظر عن أصولهم وجنسياتهم" ، أما المادة الثانية فقد أوضحت معاني المصطلحات المستعملة في الاتفاقية.[1]

وقد جاءت هذه الاتفاقية من سبعة فصول تضمنت التوصيات العامة ، الأسس المبدئية لحماية المعلومة ، انتقال المعلومة خارج حدود البلد ، التعاون المتبادل بين الدول ، اللجنة الاستشارية ، التعديلات الجائز اقتراحها من الأعضاء ، البنود الختامية .

وكانت مسودة الاتفاقية – قبل الصيغة النهائية – قد ميزت بين نوعين من البيانات: بيانات المرور وبيانات المشتركين أو الاشتراك ، وتم نقل تعريف بيانات المشتركين إلى المادة (18) المتعلقة بأوامر إنتاج المعطيات وبالنسبة لبيانات المرور فإنها تشمل الرموز الكودية للشبكات والأجهزة وكذلك الأرقام والحسابات أو أية بيانات تعريف متشابهة تُرسل منهم أو إليهم عن طريق نقطة اتصالية ، بما في ذلك تاريخ وحجم ووقت وأمر الاتصال وأية معلومات تُحدد الموقع المادي (المكان) الذي يتم فيه ، أو آلية نقل البيانات بأي نمط من أنماط الاتصالات الخلوية.

وأما بيانات الاشتراك المُعالجة في المادة (18) فإنها تعني المعلومات التي يحوزها ، أو يمتلكها مُزود الخدمة وتكون ضرورية لمعرفة وتمييز العنوان المادي للمشترك أو المستخدم، أو حساب متلقي الخدمة الاتصالية من مُزود الخدمات ، وتشمل أية معلومات تتعلق بالشبكة، أو الأجهزة أو الأفراد أو الحسابات أو بيانات التعريف أو الخدمات أو الرسوم أو المكان الحقيقي للأجهزة إذا كانت مُختلفة عن موقع تزويد بيانات المرور.

1) محروس نصار غايب ، الجريمة المعلوماتية ، مجلة التقني ، العراق ، العدد 24 السنة التاسعة، 2011م ، ص119.

حيث نصت المواد (7 ، 8) من الاتفاقية على الجرائم المرتبطة بالكمبيوتر وتشمل التزوير المرتبط بالكمبيوتر، والاحتيال المرتبط بالكمبيوتر.

ونصت في المادة (9) على الجرائم المرتبطة بالمحتوى ، وهناك صورة واحدة من هذه الجرائم جرائم دعارة الأطفال ، ونصت في المادة (11 ، 12، 13) على مسئولية الأشخاص المعنوية ومعايير الشروع والمساعدة والتحريض ، كما تلزم الاتفاقية الدول الأعضاء فيها سواء من الدول الأوروبية أو من غيرها " غير دول الاتحاد الأوروبي " باتخاذ ما يلزم تجريم (9) جرائم من الجرائم المعلوماتية.

1. جريمة الدخول غير القانوني المتعمد ، ووردت في غالبية التشريعات الوطنية بتعبير الدخول الغير مُصرح به.
2. جريمة الاعتراض غير القانوني المتعمد.
3. جريمة التدخل المتعمد في المعطيات بتدميرها.
4. جريمة التدخل المتعمد في الأنظمة.
5. جريمة إساءة استخدام الأجهزة ، حيث إن لهذه الجريمة اسماً مغايراً في مسودات الاتفاقية السابقة " الأدوات الغير قانونية " .
6. جريمة التزوير باستخدام الكمبيوتر.
7. جريمة الاحتيال باستخدام الكمبيوتر.
8. الجرائم المرتبطة بدعارة الأطفال.
9. الجرائم المرتبطة بحق المؤلف.

الفرع الثاني: حماية الخصوصية المعلوماتية في اتفاقية بودابست سنة 2001م.[1]

يلعب المجلس الأوروبي دوراً بارزاً وهاماً في مجال حماية الخصوصية المعلوماتية وذلك من خلال العديد من الاتفاقيات والتوجيهات ، فقد تم تكثيف الجهود من أجل مكافحة الانتهاكات التي تطال الخصوصية المعلوماتية ، ومن ضمن هذه الجهود وأبرزها اتفاقية بودابست لسنة 2001م، والتي جاءت نتاجاً لعديد من المحاولات والمبادرات التي قام بها المجلس الأوروبي لمكافحة الجرائم المعلوماتية. [2]

وقبل الوقوف على مضمون هذه الاتفاقية، وأهدافها. يقتضي الأمر تتبع الإرهاصات الأولية التي سبقت ميلادها ؛ فالمجلس الأوروبي قد أقدم على عدة مُبادرات مهدت إلى عقد الاتفاقية المذكورة في نهاية المطاف ، ومن أهم هذه المبادرات في الاتجاه المذكور كانت الدراسة التي أعدها المجلس الأوروبي عام 1989م مضمناً إياها جملة من التوصيات تدعو إلى تفعيل دور القانون لمواجهة الأفعال غير المشروعة التي تُرتكب عبر الحاسوب ، [3] وفي العام 1995م، تلتها دراسة أخرى تتعلق بالإجراءات الجنائية في مجال جرائم الانترنت ، وتأسيساً على ذلك انتهى المجلس إلى تشكيل لجنة لهذا الغرض سُميت بلجنة خبراء الجريمة عبر العالم الافتراضي، والتي أوكلت لها مهمة إعداد اتفاقية دولية لتسهيل التعاون الدولي في مجال الإجراءات الجنائية في الجرائم الناشئة عن استخدام الحاسوب والانترنت ، كما تمت دعوة بعض الدول من خارج المجلس الأوروبي

1) هذه الاتفاقية في أصلها أوروبية، إلا إنها مفتوحة لانضمام دول أخرى (ليست أوروبية) إليها، فهي ذات نزعة دولية، فقد أكدت هذه الاتفاقية على أهمية التعاون الدولي لمكافحة جرائم الحاسب الآلي والإنترنت، أسامة بن غانم العبيدي، الجهود الدولية لمكافحة الجرائم المعلوماتية، بحث منشور بمجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، العدد4 السنة 39، 2015م، ص145.

2) صغير يوسف ، مرجع سابق ، ص100.

3) عبد الإله النوايسة، جرائم تكنولوجيا المعلومات، دار وائل للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2017م ، ص46.

للمساهمة في الإعداد لهذه الاتفاقية بصفة مراقب، والدول التي وجهت إليها الدعوة هي الولايات المتحدة واليابان وكندا وجنوب أفريقيا.[1]

وفيما يتعلق بالاختصاص المكاني بشأن آي جريمة من الجرائم المنصوص عليها في هذه الاتفاقية ، فإن الدول الأطراف المعنية يمكنها حل ذلك بالتشاور فيما بينها متى كان ذلك مناسباً، بغية تحديد الاختصاص القضائي الأكثر ملائمة ؛ في حين خصصت الاتفاقية المذكورة فصلاً مستقلاً للتعاون الدولي في مواجهة جرائم المعلوماتية.[2] وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010م.[3]

وقد تضمنت هذه الاتفاقية الأقسام التالية:

القسم الأول: تحديد المصطلحات.

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني.

القسم الثالث: التعاون الدولي.

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.[4]

فالقسم الأول تم تخصيصه للمصطلحات التي تضمنتها الاتفاقية وتفسيرها ، أما القسم الثاني فاشتمل على ما يجب إتباعه من إجراءات في نطاق التشريعات الوطنية من قبل الدول

---

1) موسى مسعود ارحومة ، السياسة الجنائية في مواجهة الانترنت ، بحث مُقدم إلى مؤتمر الدولي لجامعة الطفيلة التقنية ، الأردن، 2007م، ص 20-21.

2) خالد الشرقاوي السموني، مكافحة جرائم الكمبيوتر على ضوء التشريعين الوطني والدولي ، بحث مقدم لجامعة محمد الخامس، المغرب ، ص5.

3) حول هذه الاتفاقية وغيرها من الاتفاقيات التي تُعنى بحقوق الإنسان عامة والحق في الخصوصية خاصة راجع الموقع التالي: http://www.coe.int/ar_jo/web/compass/legal-protection-of-human-rights تاريخ الزيارة 2014/10/28م.

4) خالد الشرقاوي السموني ، المرجع السابق ، ص 5.

المصدقة على الاتفاقية فيما يتعلق بالجزاءات والإجراءات ، والقسم الثالث نص على الجانب المتعلق بالتعاون بين الدول المصدقة على الاتفاقية، لمكافحة جرائم المعلومات ولحماية الخصوصية ، بينما القسم الرابع بين ما هي الشروط اللازمة للانضمام للاتفاقية.

وقد حددت مجموعة من الجرائم المعلوماتية متمثلة في الدخول غير المشروع أو غير المصرح به إلى شبكة المعلومات أو لأنظمة الحاسب الآلي ، والتلاعب بالبيانات وتدميرها والاحتيال ، والتزوير ، ودعارة الأطفال ، وإقامة المواقع الإباحية ، وانتهاك حقوق الملكية والحقوق المجاورة.[1] ووضعت قواعد في حالة تنازع الاختصاص بين أكثر من دولة طرف في الاتفاقية.

إن أهم ما يميز هذه الاتفاقية أنها تضع إطاراً لتقسيم القواعد الموضوعية بشأن جرائم الكمبيوتر والانترنت ، فاعتمدت في تقسيمها إلى وضع مجموعة أقسام للجريمة تقوم على دور الكمبيوتر بالجريمة ، القسم الأول الجرائم التي تستهدف سرية وسلامة وتوفر المعلومات، وهنا الهدف في الاعتداء هو الكمبيوتر. أما القسم الثاني فهي الجرائم المرتبطة بالكمبيوتر، وهنا يكون الكمبيوتر هو الوسيلة في الجريمة. أما القسم الثالث الجرائم المرتبطة بالمحتوى، وهنا يكون الكمبيوتر هو الحاضنة التي تتم فيها الجريمة . أما القسم الرابع الجرائم المتعلقة بجرائم الملكية الفكرية، وهنا دورها هو أن تتم الحماية المقرر لهذه المصنفات ، أما فيما يتعلق بالجرائم التي تقع على الخصوصية ، فإن الاتفاقية لم تقم بالتمييز بين نوعية البيانات، والمعلومات التي يتم الاعتداء عليها ما إذا كانت شخصية ، أو اقتصادية ، أو مالية ، ولعل سبب ذلك يرجع للرغبة في فرض الحماية على جميع البيانات بغض النظر عن نوعيتها.

---

1) موسى مسعود ارحومة ، السياسة الجنائية في مواجهة الانترنت ، مرجع سابق ، ص23.
عمر محمد بن يونس ، الاتفاقية الأوروبية حول الجريمة الافتراضية ، مؤسسة أدم للنشر والتوزيع ، مالطا ، الطبعة الثانية ، 2005م ، ص 65 – 98.

وبالرغم مما تمثله هذه الاتفاقية في المجال القانوني، حيث تعتبر من أهم الاتفاقيات المبرمة في مكافحة الجرائم المعلوماتية، إلا إنها لم تتناول حماية الخصوصية المعلوماتية بالشكل المطلوب، ليشعر مستخدم الشبكة المعلوماتية والتكنولوجيا الحديثة بالقدر الكافي من الحماية .

المطلب الثاني
حماية الخصوصية المعلوماتية
في إطار الدول العربية

باتت تكنولوجيا المعلومات تُستخدم في شتى مناحي الحياة باختلاف مجالاتها، كما أشرنا سابقاً ، ولإن هذه التكنولوجيا لا تتقيد بالعوائق الجغرافية الموجودة في العالم الواقعي فقد أخذت في الانتشار في العالم وأصبح استخدامها في أغلب أقطار العالم أمراً ضرورياً ومنها الوطن العربي.

حيث تلقى هذه التكنولوجيا استعمالاً واسعاً سواء على مستوى الدول بهيئاتها ومؤسساتها، أو على المستوى الشخصي للأفراد ، فلا يكاد يوجد فرد في الوطن العربي اليوم لا يستخدم الهواتف المحمولة، والبريد الإلكتروني، أو صفحات التواصل الاجتماعي، علاوة عن محركات البحث عن المعلومات.

ونتيجة لهذا التوسع في استخدامها أصبح من الضروري إيجاد كل ما من شأنه أن يكفل الاستعمال الآمن لهذه التكنولوجيا دون التعرض لأي انتهاكات، ونخص بالقول هنا حماية الخصوصية في مجال تقنية المعلومات.

وعلى الرغم من قلة المبادرات في هذا المجال على الصعيد العربي، إلا أنه تظل هناك أعمال مهمة، منها ما كان ضمن إطار جامعة الدول العربية، ومنها ما كان خارج أعمال الجامعة.

الفرع الأول: آليات حماية الخصوصية المعلوماتية في إطار جامعة الدول العربية:

أعتمد مجلس الدول العربية في دورته المنعقدة في 1966م قراراً يقضي بتشكيل لجنة خاصة مهمتها التحضير والتجهيز لما سوف تقدمه الجامعة العربية في موضوع حقوق الإنسان

، نتيجة لهذا المجهود أعتمد المجلس ذاته قراراً آخر بإنشاء لجنة إقليمية عربية دائمة لحقوق الإنسان عام 1967م، مهمة هذه اللجنة تتمثل في أعداد مشروع ميثاق عربي لحقوق الإنسان. [1]

وبعد أكثر من محاولة لصياغة الميثاق العربي لحقوق الإنسان وتدخل من كل الخبراء العرب الأعضاء في هيئات الأمم المتحدة في مجال حقوق الإنسان، أقر المجلس في مايو 2004م الميثاق العربي لحقوق الإنسان في صيغته النهائية، وتكون من ديباجة وثلاثة وخمسون مادة.

خصصت المادة 21 من هذا الميثاق لحماية الخصوصية والتي تكونت من فقرتين نصت فيها على:

1. لا يجوز تعريض أي شخص على نحو تعسفي، أو غير قانوني للتدخل في خصوصيات أو شؤون أسرته أو بيئته أو مراسلاته أو لتشهير يمس به.
2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس . [2]

ومن ضمن جهود الجامعة أنه تم في بغداد 1981م إبرام الاتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر وزراء الشؤون الثقافية ، حيث تم في هذا العام المصادقة عليها من الدول المشاركة ، وجاء في ديباجة الاتفاقية رغبة الدول في حماية حقوق المؤلفين على المصنفات الأدبية والفنية بطريقة فعالة ومُوحدة ، حيث كان ذلك متماشياً مع ما أوصت به المادة 21 من ميثاق الوحدة الثقافية العربية الصادر عام 1964م التي أهابت بالدول العربية بوضع نطاق عربي موحد لحماية حقوق المؤلف يلائم الدول العربية ، ويُضاف إلى الاتفاقية الدولية النافذة، كاتفاقية (بيرن) لحماية المصنفات الأدبية والاتفاقية العالمية لحقوق المؤلف.

---

1) إبراهيم علي بدوي الشيخ ، مرجع سابق ص49–52 .

2) انظر حول الميثاق العربي لحقوق الإنسان الموقع التالي:

http://www. Lasportal.org/ar/legalnetwork/pages/arabcharter.aspex. تاريخ الزيارة 2014/10/28م

كذلك وقد أبرمت نفس المنظمة (المنظمة العربية للتربية والثقافة والفنون) الاتفاقية العربية لتيسير انتقال الإنتاج الثقافي العربي لعام 1989م ، وتعتبر هاتان الاتفاقيتان مثالاً واضحاً على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال حماية خصوصية المعلومات والحفاظ على حقوق المؤلف ، وإن كان هذا يُعد جهداً متواضعاً نظراً لما يُمثله حماية حق المؤلف باعتباره اتجاهاً واحداً من اتجاهات جرائم الحاسب الآلي.

وأيضاً من الخطوات الهامة التي تمت على الصعيد العربي هو اعتماد مجلس وزراء العدل العرب بتاريخ 1996م ، للقانون الجنائي العربي الموحد بموجب القرار رقم 339، وذلك كخطوة في مواجهة القرصنة والجرائم المعلوماتية ، حيث عاقب في نص المادة (164) على الدخول بطريق الغش إلى كامل أو جزء من نظام المُعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة، وتغيير المعلومات داخل النظام وتزوير الوثائق المُعالجة آلياً وسرقة المعلومات. [1]

وبالاطلاع على الباب السابع الخاص بالجرائم ضد الأشخاص من هذا القانون، نجد أنه يحتوي على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، وذلك في المواد (461 إلى 464) ، حيث نصت المادة (461 و 463) على تجريم جمع المعلومات الاسمية ومعالجتها آلياً ، أو استعمالها بالمخالفة لأحكام القانون ، أو المساس بسلامة وسرية معلومات الأشخاص، [2] وتُعد هذه المُحاولة بالرغم من تواضعها من المحاولات البارزة التي تمت لغرض تعزيز التعاون على المستوى العربي من الناحية التشريعية.

---

1) صغير يوسف ، مرجع سابق ، ص101.

2) محمد كامل محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية ، دار الفكر والقانون ، المنصورة ، مصر ، الطبعة الأولى ، 2015م ، ص 199.

ولغرض تعزيز التعاون بين الدول العربية لمكافحة الجرائم المعلوماتية ، فقد تم أيضاً إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بتاريخ 21 ديسمبر2010م ، حيث تم التوقيع عليها من قبل سبع عشرة دولة عربية،[1]وذلك بهدف تبني سياسة جنائية مشتركة مِن أجل حماية أمن المجتمع العربي أفراده ومصالحهم ضد تهديدات جرائم تقنية المعلومات. [2]

وتضمنت هذه الاتفاقية 43 مادة ، جرمت في الفصل الثاني مجموعة من الأفعال التي من شأنها المساس بالخصوصية وذلك في المواد من (6 إلى 18) منها (الدخول غير المشروع، والاعتراض غير المشروع ، الاعتداء على سلامة البيانات ، إساءة استخدام وسائل تقنية المعلومات ، الاعتداء على حرمة الحياة الخاصة ، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة) ، أما المادة (20) تم تخصيصها للمسؤولية الجنائية للأشخاص الطبيعية والمعنوية ، وتم تخصيص الفصل الثالث من الاتفاقية للأحكام الإجرائية وذلك بالمواد (22 إلى 29) بينما تم تخصيص الفصل الرابع للتعاون القانوني والقضائي بالمواد (30 إلى 42).

والملاحظ في هذه الاتفاقية مدى تأثرها باتفاقية بودابست حيث جاء إبرام هذه الاتفاقية بعد مطالبات من قبل المختصين بإصدار اتفاقية متخصصة بمكافحة الجرائم المعلوماتية على المستوى العربي ، وقد شملت هذه الاتفاقية كافة المسائل اللازمة لمكافحة الجرائم المعلوماتية، إلا إنه يؤخذ عليها كونها تستخدم مصطلحات فضفاضة ، كما تفتقد الاتفاقية لمراعاة مبادئ الشفافية في صياغة موادها .

والجدير بالملاحظة هنا : أن الجهود على المستوى العربي تعتمد على سد النقص الموجود في التشريعات العربية الخاصة بحماية الخصوصية المعلوماتية والجرائم المرتكبة عليها عن

1) من الدول العربية التي صادقت على الاتفاقية الأردن ، مصر ، العراق ، في حين ليبيا لم تصادق عليها.
2) المرجع السابق ص 201-202.

طريق الإنترنت ، وذلك بوضع قواعد للاستخدام الآمن للانترنت ، وكذلك النص على بعض النشاطات الإجرامية التي ترتكب بواسطة الإنترنت.

إلا أن هذا يبررهُ البعض في كون أن وضعنا في الدول العربية يختلف عن الدول الغربية المتقدمة التي تعتمد على التكنولوجيا في شتى مناحي الحياة.

الفرع الثاني: مؤتمرات عربية لحماية خصوصية المعلومات:

إن للجمعية المصرية للقانون الجنائي مجهوداً محموداً في هذا الموضوع، وتمثل ذلك في مؤتمرها السادس المُنعقد في القاهرة من 28/25 أكتوبر في العام 1993م، حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، التي أكد فيها المؤتمرون على عالمية جرائم الحاسب الآلي، ووجوب تكاثف الجهود لمكافحتها، لأنها تمثل وجهاً سلبياً للتقدم الحضاري وضرورة ضمان حماية خصوصية المعلومات، وذلك بتعديل قوانين العقوبات التقليدية، وإضافة نصوص جديدة، وذلك لأن النصوص الحالية لا يُحيط معظمها بالأنشطة المراد تجريمها.

وقد خرج المؤتمر بتوصيات خاصة بصور السلوك الإجرامي في مجال جرائم الكمبيوتر، تمثل في واقعها أنماطاً، أو طوائف من الجرائم الحاسب الآلي، كما أوصى المؤتمر بضرورة التعاون الدولي في مجال أنظمة المعلومات، وتنفيذ ما تقره من قواعد ووجوب تحقيق التعاون الدولي في مجال مُكافحة جرائم الكمبيوتر، ذلك فيما يتعلق بالإنابة القضائية وتسليم المجرمين وتنفيذ الأحكام.

كما أوصى المؤتمر بوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات، وطرق الاستدلال، والتحقيق، وجمع الأدلة في الجرائم المتعلقة به.

وإلى جانب هذه الجهود، هناك جهود أخرى تتضح معالمها في ما تم بذله في ميدان حماية الملكية الفكرية، كالمؤتمر العربي الدولي الأول للملكية الفكرية المُنعقد في عمان في عام 1995م في شهر سبتمبر، [1] وقد تم عقد المؤتمر العربي الدولي الثاني بتاريخ 1998م حيث طالبت الجهات العربية المشاركة بضرورة إضافة توجيه حول تسهيل نقل التكنولوجيا من الدول الصناعية إلى المنطقة العربية، لحماية خصوصية المعلومات، والاختراعات، ومكافحة القرصنة، وتسهيل نقل اختراعات العلماء العرب من أوطانهم.

1) لمعلومات أكثر حول المؤتمر انظر الموقع التالي: http://www.hip.jopuls.org.jo تاريخ الزيارة 2015/10/25م.

الفصل الثالث

آليات الحماية الوطنية للخصوصية المعلوماتية

تمهيد:

لم تقتصر حماية الخصوصية المعلوماتية على ما تم الاتفاق عليه في المؤتمرات الدولية وأعمال وجهود المنظمات الدولية ، أو الإقليمية فقط ، حيث نصت العديد من التشريعات الوطنية على نصوص تضمن فيها الخصوصية عامة ، والخصوصية المعلوماتية خاصة، وذلك سواء عن طريق نصوص ضمنتها لدساتيرها،[1] أو في قانون العقوبات، أو عن طريق قوانين خاصة.

وكل هذا الاهتمام يرجع لما لحماية الحياة الخاصة من أهمية ، ويرجع أيضاً للاستعمال المتزايد لتقنية المعلومات ، وتداخلها في شتىّ نواحي الحياة اليومية ، فأخذت الدول تسن القوانين وتضع التدابير التي من شأنها أن تكفل الحماية ضد أي انتهاك قد يقع على خصوصية المعلومات... [2]

ولأن الاهتمام بحماية الخصوصية في المجال المعلوماتي أصبح سمة غالبية التشريعات في دول العالم ؛ لهذا وجب علينا تسليط الضوء على بعض التشريعات المهمة، ومن ضمن هذه التشريعات التشريع الفرنسي ، والأمريكي ، وسيتم تناولها لانتماء كل واحد منهما لنظام قانوني

---

1) فقد نصت العديد من الدول على حماية الخصوصية المعلوماتية في دساتيرها ومنها الدستور الأسباني لعام 1978م ، حيث نص في المادة الثامنة منه على " أن القانون هو الذي يحدد البيانات التي تخضع للمعالجة الالكترونية لضمان الكرامة والحصانة الشخصية والأسرية للمواطنين في ممارستهم لحقوقهم " ، وكذلك الدستور البرتغالي لعام 1982م في المادة 35 وأيضاً المادة الأولى من الدستور النمساوي أقرت حماية دستورية للمعطيات الشخصية .

لمعلومات أكثر حول هذا الموضوع راجع : أمنار إبراهيم ، الحماية الجنائية للمعطيات ذات الطابع الشخصي على ضوء القانون المغربي والقانون المقارن ، رسالة ماجستير منشورة في مجلة القانون والأعمال، 2008م ، منشور على الموقع المجلة:

تاريخ الزيارة 2016/09/20م http://www.droitententtreprise.org

2) إن مراقبة المحادثات الهاتفية وتسجيلها والتقاط الصور بالرغم من مساعدتها في كشف الحقيقة ، وتسهيلها في إثبات الكثير من الجرائم الغامضة التي يتعذر إثباتها بالوسائل التقليدية، إلا إنها تشكل من جانب آخر تمثل انتهاكاً لحرمة الحياة الخاصة للأفراد واعتداء على سرية اتصالاتهم التي كفلتها المواثيق الدولية وكرستها الدساتير المعاصرة في كثير من الدول ، ومع ذلك فقد تفاوتت التشريعات فيما بينها بشأن مدى القيام بهذه الإجراءات في حدود معينة متى كانت مصلحة العدالة تقضى بذلك ، انظر: فتحي محمد أنور عزت ، مرجع سابق ، ص160 إلى 161 .

مختلف ، حيث يُمثل القانون الفرنسي "النظام اللاتيني" بينما يُمثل القانون الأمريكي "النظام الأنجلو سكسوني".

كما أن من المهم في هذه الدراسة بيان مدى الحماية التي وفرتها التشريعات العربية، ولما كانت هذه الأخيرة كثيرة ولا يسعنا دراستها بالكامل ، فقد اخترنا كل من التشريع البحريني والتشريع الإماراتي "إمارة دبي" ويُعزى اختيارنا لهذين التشريعين لمواكبتهما لأحدث التطورات في مجال تكنولوجيا المعلومات ، كما وجب علينا أيضاً دراسة الحماية التي يوفرها المشرع الليبي في هذا المجال.

وعليه سيتم تناول هذا الفصل من خلال تقسيمه إلى مبحثين:

المبحث الأول: حماية الخصوصية المعلوماتية في التشريعين الفرنسي والأمريكي.

المبحث الثاني: حماية الخصوصية المعلوماتية في بعض التشريعات العربية والتشريع الليبي.

المبحث الأول
حماية الخصوصية المعلوماتية
في التشريعين الفرنسي والأمريكي

تمهيد:

إن الاستعمال المتنامي للشبكات المعلوماتية – كما سبق وأن بينا– والاعتماد عليها في العديد من الدول وما تتعرض له هذه الشبكات من انتهاكات تشكل اعتداء على الخصوصية ، أمر جعل الدول تُسرع في رسم الخطط ووضع الأطر لحماية هذه التكنولوجيا المفيدة من الخطر الذي يُهددها ، وذلك بالاعتداء على خصوصية المعلومات والبيانات التي يتم تجميعها لأداء وظيفتها.

ولعل أهم الدول التي تناولت هذا الموضوع ورصدت له الوقت والجهد هي فرنسا، سواء كان من خلال القانون الجنائي الفرنسي ، أو من خلال قوانين خاصة أخري ، ولم تكن الولايات الأمريكية أقل اهتماماً في هذا المجال ، ولهذا سيتم تناول هذا المبحث من خلال تقسيمه إلى مطلبين:

المطلب الأول: حماية الخصوصية المعلوماتية في القانون الفرنسي.

المطلب الثاني: حماية الخصوصية المعلوماتية في القانون الأمريكي.

المطلب الأول
حماية الخصوصية المعلوماتية
في القانون الفرنسي

لطالما كانت فرنسا من الدول الرائدة في مواكبة المستجدات ، وذلك بالمعالجة القانونية ورسم الأطر وتوفير الحماية ضد أي انتهاكات قد تقع على المصالح العامة أو الخاصة، ولم تتغير عن العادة في مجال حماية الخصوصية المعلوماتية.

والملاحظ أن نطاق الحماية الجنائية للمعلوماتية في فرنسا تمتد إلى ثلاث محاور رئيسية وهي: (حماية الأشخاص ، حماية المضمون ، وحماية وسائل الاتصال). فلا يجوز وفقاً للقانون الفرنسي الاعتداء على حرية الحياة الخاصة ، أو التعريض بالغير ، فقد كفل قانون العقوبات الفرنسي ذلك ، وكذلك القواعد العامة للعقود التي تم تنظيمها من خلال القانون رقم (78–17) الصادر في 6 يناير 1978م بشأن أمن معالجة البيانات. [1]

وسيتم تناول هذا الموضوع سواء في القواعد الإجرائية العامة لحماية البيانات الاسمية في قانون 1978م ، و من خلال القانون الجنائي القديم والقانون الجنائي الحديث.

الفرع الأول: القواعد الإجرائية العامة لحماية البيانات الاسمية في قانون 1978م[2]:

اشترط المشرع في قانون المعالجة الرقمية والحرية لسنة 1978م ضرورة الحصول على تصريح مسبق ، إذا كان من يقوم بجمع المعلومات من أشخاص القانون العام ، أو من أشخاص القانون الخاص الذين يعملون لمصلحة الدولة.

---

1) عبدالفتاح بيومي حجازي ، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة ، مصر ،2011م ، ص82 إلى 89.

2) Lio n 78-17 du 6 janvier 1978 relative a l'Informatique, aux fichiers et aux Libertes published on:http://www.legifrance.gouv.fr

وإذا أراد القائمون على موقع من مواقع الانترنت التعامل مع البيانات الشخصية فيتعين عليهم قبل البدء في هذا الأمر إخطار اللجنة القومية للمعلوماتية والحريات،[1] كما اشترط وجوب إخطار اللجنة عند مُعالجة أية بيانات اسمية شخصية من قبل أشخاص القانون الخاص ، وذلك لأن نشر مثل هذه المعلومات على مواقع الانترنت يجعلها عرضة للانتهاك ووقوع الأفعال غير المشروعة عليها ، مثل الالتقاط غير المسموح به والتزييف والاستيلاء عليها والتلاعب بها، ولذلك تشترط اللجنة إخطار الأشخاص بمخاطر وضع بياناتهم الشخصية على المواقع ، وتعطي لهم الحق في الاعتراض على البيانات المنشورة عنهم ، ولهم حق الاطلاع عليها والتصحيح والاعتراض ومحو البيانات لأسباب مشروعة.[2]

يتعين على الجهة التي تستخدم برامج Cookies إخطار اللجنة ، وذلك لأنه يمكن عن طريق هذه البرامج أن يتمكن النظام من معرفة معلومات عن المستخدم الذي يدخل إلى الموقع ، والعلم بالمواقع التي تصفحها قبل ذلك ، وبالتالي معرفة ميوله ورغباته ، ويمكن مُعالجة هذه البيانات ووضعها على قاعدة بيانات لاستخدامها ؛ ولذلك مثل هذا العمل يخضع لأحكام هذا القانون.

والملاحظ أن القضاء قد أسهم كثيراً في تحديد مفهوم البيانات الاسمية التي يوفر لها هذا القانون الحماية ، فقد اعتبر أن من البيانات التي يشملها هذا القانون بالحماية رقم التليفون، ولكنه لم يعتبر اسم الشخص ، وعنوانه ضمن البيانات الاسمية ، كما قرر أن البيانات التي تتعلق

---

1) والجدير بالملاحظة أن اللجنة القومية للمعلوماتية والحريات حتى عام 2011م ، لا تملك السلطة في توقيع أي جزاءات على المخالفين للنصوص الواردة في قانون البيانات الاسمية لعام 1978م ، فهي لا تملك سوى توجيه إنذار للجهات المخالفة، كما لا تملك مثلاً توجيه أوامر لإلزام المخالفين باحترام أحكام القانون ، وكل ما تملكه اللجنة هو إبلاغ النيابة العامة إذا ما تبين لها أن المخالفة الواقعة تمثل جريمة جنائية من الجرائم المعاقب عليها قانوناً ، ونتيجة لذلك تم تعديل المادة 49 من القانون لمنح اللجنة سلطات جزائية ، لمعلومات أكثر أنظر : شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، دار الفكر والقانون، المنصورة ، مصر ، الطبعة الأولى . 2015م، ص132- 146.

2) أيمن عبدالله فكري ، جرائم النظم والمعلومات ، دار الجامعة الجديدة ، الإسكندرية ، مصر، 2007م ، ص680.

بالمعلومات الخاصة بجنسية سكان عقار وأفكارهم الفلسفية هي من البيانات الاسمية التي يحميها القانون.[1]

ورغبة من اللجنة القومية للمعلوماتية ، والحريات في تيسير الإجراءات ، قامت بوضع توجيهات عامة ، بحيث يكون كافياً الأخطار المُبسط للجنة ، إذا تعلق الأمر ببيانات لا تتسم بالخطورة ، أما إذا تعلق الأمر ببيانات على قدر من الحساسية (كالتي تتعلق بالعرق والآراء السياسية والفلسفية والدينية ، أو المتعلقة بالانتماءات النقابية أو بأخلاق الشخص)، فيتعين الحصول على موافقة صريحة من صاحب الشأن، وذلك وفقاً لما نصت عليه المادة 31 والتي تم تضمينها بالمادة 226–19 من قانون العقوبات ، وقد تم إدانة أحد الأشخاص وفقاً لهذا القانون لقيامه بوضع صورة عارية لصديقته على موقعه على الانترنت.[2]

كما اعتبرت اللجنة أن الاستبيان الاختياري الذي يقوم به الشخص عند الدخول للموقع، أو لاستمرار العمل فيه ، والذي يتطلب بعض البيانات من الشخص الذي يريد الدخول إلى الموقع الالكتروني للجهة من قبيل المعالجة للبيانات الاسمية، وكذلك عمليات تتبع الأثر الذي يقوم بها مورد الخدمة والتي يتمكن من خلالها من التعرف على المواقع التي زارها المستخدم، ووقت وتاريخ الزيارة ، وتصفح تلك المواقع ، ويقوم بتخزين هذه البيانات والتي يتمكن من خلالها من تحديد شخصية العميل ، فقد طبقت اللجنة على تلك المسائل الإجراءات الواجب إتباعها وفقاً لقانون 1978م ، وألزمت اللجنة تلك الجهات بإخطار العملاء بقيام الجهة باستخدام برامج Cookies حتى يتسنى لهم الاعتراض على ذلك.

1) أيمن عبدالله فكري ، مرجع سابق ، ص680.

2) مدحت عبدالحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص 88.

الفرع الثاني: الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي الجديد[1]:

في الواقع أن المشرع الفرنسي بشأن حماية الحياة الخاصة في قانون العقوبات الجديد لم يعدل في موقفه السابق بقانون العقوبات القديم ، بل اتجه إلى تعديل صياغة النصوص، وقد كفل المشرع الفرنسي الحماية للحياة الخاصة بالمواد 226–1 ، 226–2 ، 226–8، ويقابل هذه المواد في قانون العقوبات القديم المواد 368 ، 369 ، 370 ، وتتعلق المادة الأولى بتجريم التقاط أو تسجيل أو نقل الكلام الصادر بصورة خاصة ، أو سرية بدون موافقة المجني عليه، وكذلك تجريمه لالتقاط أو تسجيل أو نقل صورة شخص من مكان خاص دون رضاً منه، وتتعلق المادة الثانية بجريمة حفظ أو إعلان أو استعمال تسجيل أو مستند تم الحصول عليه بأحد الأفعال المشار إليها بالمادة 226–1 ، أما المادة الأخيرة فتتعلق بعمل مونتاج لصوت أو صورة لشخص بدون رضاه ، والملاحظ هنا أنه فيما يتعلق بالجريمة الأولى وهي جريمة التقاط أو تسجيل أو نقل لكلام صادر بصورة خاصة وسرية دون موافقة المجني عليه ، والمنصوص عليها بالمادة 226–1، قد ساوى المشرع فيما إذا كان الفعل قد تم من شخص عادي ، أو من شخص من أشخاص القانون العام ، وهذا ما كان عليه الحال في القانون الفرنسي القديم فلم يتم تعديل النص بالرغم من أن هذا المسلك غير عادل لما فيه من مساواة في العقاب ، حيث كان من المفترض تشديد العقوبة على الفعل في حالة ارتكابها من أحد أشخاص القانون العام ، وذلك لما لهم من صلاحية الإطلاع والوصول لمثل هذه المعلومات.

1) انظر في عرض هذه النصوص لدى : علاء عبدالباسط خلاف ، الحماية الجنائية لوسائل الاتصال الحديثة ، دار النهضة العربية، 2002م ،ص137– 140، وكذلك بالموقع التالي:http://www.legifrance.gouv.fr تاريخ الزيارة 2015/03/06م.

وقد استبعد المشرع الفرنسي في هذا القانون اصطلاح التنصت المنصوص عليه بالمادة 368–1 ع القديم ، وحل محلها اصطلاح التقاط ، كما جاء النص الجديد بدون أن يشترط كون فعل الالتقاط أو التسجيل أو النقل قد وقع في مكان خاص ، وبناء على ذلك فإن ما يصدر عن الشخص وكانت له طبيعته الخاصة أو السرية يشمله النص بالحماية سواء أكان في مكان خاص أو عام.

وفيما يتعلق بالتقاط أو تسجيل أو نقل الصورة فقد حافظ المشرع الفرنسي على ذات الصياغة القديمة بالمادة 368 عقوبات قديم ، ولم يُحدد المقصود بالأماكن الخاصة ، وقد رأى بعض من الفقه الفرنسي أنه لا توجد مشكلة بالنسبة للمكان الخاص بطبيعته ، ولكن الأمر يكون دقيقاً بالنسبة للمكان العام والذي تتوافر فيه أحياناً عوامل أخرى تجعل بالإمكان اعتباره من الأماكن الخاصة ، ويرى هذا الجانب من الفقه أن يوجد معيار مادي يمكن تطبيقه في هذا الجانب لتحديد طبيعة الأماكن العامة دون الأخذ في الاعتبار بطبيعة الصورة التي التقطت أو سجلت فيه أو نقلت منه ، كما يوجد معيار شخصي يأخذ في الاعتبار بطبيعة الصورة دون النظر للمكان الذي تم التقاطها فيه أو نقلت منه.

ويعد المكان خاصاً إذا كان لا يمكن للشخص الدخول إليه إلا من خلال موافقة صاحبه أو حائزه ، ويكون المكان عاماً بإمكان أي شخص دخوله ، ويعد من قبيل ذلك الطرق العامة والأماكن العامة كالشواطئ ، والأماكن العامة بالتخصيص، كالمقاهي و المطاعم والمحلات ودور

العرض،[1] والجدير بالملاحظة انه قد يكون المكان الذي تم التقاط التسجيل أو الصورة فيه عاماً ، إلا أنه ليس كل ما يدور في المكان العام يعد عاماً.[2]

وكما أشرنا سابقاً أن المشرع الفرنسي لم يغير موقفه من حماية الخصوصية في القانون الجديد بل اتجه إلى تعديل صياغة بعض النصوص، وتعد المصطلحات التي استخدمها المشرع الفرنسي في قانون العقوبات القديم من المرونة والاتساع لتشمل صور الاعتداء على الحياة الخاصة باستخدام الحاسب أو الانترنت.[3]

كما يجدر تسليط الضوء على الجرائم التي نص عليها المشرع في القانون 1978م وتعديلاته؛[4] المتعلق بالمعلومات والحريات ، والتي أكد عليها القانون الجنائي الفرنسي الجديد بعد أن أجرى عليها بعض التعديلات وأزال عنها الغموض المتعلق بها ، وقد أراد المشرع الفرنسي أن يؤكد على حماية حقوق وحريات المواطنين في مواجهة مخاطر وتطورات تكنولوجيا المعلومات.[5]

ولم يحاول المشرع الفرنسي عند قيامه بصياغة القانون الجنائي الجديد أن يقوم بتغيير روح قانون 1978م أو أن يقوم بتقليص سلطات اللجنة القومية للمعلوماتية والحريات ، وقد تضمن التشريع الجنائي الفرنسي الجديد المواد 41-44 من قانون 1978م في الفصل الخاص بحماية الشخصية ، وتناول الجرائم المتعلقة بالبيانات الاسمية والأحكام الخاصة بالعقاب في المواد 226-16 إلى 226-31 من قانون العقوبات الحديث مع إجرائه لبعض التعديلات في

---

1) مدحت عبدالحليم رمضان ، جرائم الاعتداء على الأشخاص والانترنت ، دار النهضة العربية ،القاهرة ، مصر ، ص104.

2) احمد فتحي سرور ، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، ع54 س26 ، يونيو 1984، ص76.

3) مدحت عبدالحليم رمضان ، جرائم الاعتداء على الأشخاص والانترنت ، مرجع سابق، ص 109.

4) للاطلاع على قانون المعالجة الآلية للمعطيات ، ملفات المعطيات والحريات الفردية رقم 17-7 تاريخ 1978/1/1م وتعديلاته.
The Art on Data Processing. Details and individual liberties. No 17-78/1978ad.
انظر الموقع التالي : http://www.cnil.fr , http://www.arablaw.org/download/Privacy&DataProtecction
تاريخ الزيارة 2015/04/12م.

5) أيمن عبدالله فكري ، مرجع سابق ، ص 685.

هذه النصوص ،[1] والأفعال التي تناولها قانون العقوبات الفرنسي الجديد والمتعلق بحماية البيانات الشخصية هي:

1. عدم اتخاذ الإجراءات الأولية لمُعالجة البيانات م 226–16.
2. عدم اتخاذ الاحتياطات اللازمة لحماية البيانات م 226–17.
3. المُعالجة غير المشروعة للبيانات م 226–18.
4. تسجيل وحفظ بيانات شخصية لأشخاص مصنفين م 226–19.
5. حفظ بيانات شخصية خارج الوقت المسموح به وفقاً للطلب أو الإعلان م 226–20.
6. تغيير الغرض المُحدد لجمع البيانات الاسمية م 226–21.
7. إفشاء البيانات الاسمية بما يضر بصاحب الشأن م 226–22.
8. حماية المراسلات التي تتم بطرق وسائل الاتصالات م 226–15.

وقد سلك المشرع في هذا القانون طريقاً حاول فيها توفير حماية أكثر للخصوصية المعلوماتية ، ويظهر ذلك من عدة نصوص ، ومن ذلك ما نصت عليه المادة 226–16–1–A من ذات القانون ، حيث نصت على أنه عندما يتعلق الأمر بمعالجة البيانات بخلاف الجهات المحددة بالمادة 15 يتعين إخطار اللجنة القومية للمعلوماتية والحريات قبيل إجراء مُعالجة البيانات ، ويجب أن يحتوي ما يفيد أن إخطار المُعالجة تتفق ومتطلبات القانون.

كما نصت في المادة 226–16 و 226–17 على أن يعاقب بالحبس لمدة 5 سنوات وبغرامة 300,000 يورو من يجري أو أمر بإجراء مُعالجة إلكترونية للبيانات الاسمية دون اتخاذ

1) مدحت عبدالحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص 89–91.

الاحتياطات الملائمة لحماية هذه البيانات وخصوصاً الحيلولة دون تشويهها أو إتلافها أو اطلاع الغير غير المصرح له بذلك.

وأيضاً نص المادة 226–18 حيث تتناول هذه المادة في الفقرة الأولى جريمة معالجة البيانات بصورة غير مشروعة من ناحية ، وجريمة مُعالجة البيانات المتعلقة بشخص طبيعي إذا اعترض. وكانت هناك مبررات مشروعة لهذا الاعتراض.

ويرى جانب من الفقه الفرنسي أن عبارة مبررات مشروعة التي استخدمها المشرع مطاطة وغير محددة ، ومع ذلك فقد أراد المشرع بهذا القيد أن يؤكد على حماية حرمة الحياة الخاصة المقررة بالمادة التاسعة من القانون المدني الفرنسي.

المطلب الثاني
حماية الخصوصية المعلوماتية
في القانون الأمريكي

إن الولايات المتحدة الأمريكية تتميز بأسبقية سن التشريعات المتعلقة بكافة مسائل تقنية المعلومات وقطاعات الحوسبة والاتصالات والانترنت، سواء تلك التي ترتبط بالكمبيوتر أو الانترنت بطريقة مباشرة أو غير مباشرة،[1] أما على الصعيد الدستور لم يرد النص صراحة في الدستور الأمريكي على حماية الخصوصية المعلوماتية، وإنما يوجد حقوق أساسية منصوص عليها بصفة عامة ، فتهدف حماية الخصوصية في الدستور الأمريكي إلى حماية الحقوق الواردة في الدستور بصفة عامة من الإجراءات الحكومية فقط ، فهي تأخذ الطابع السلبي فتلزم الحكومة بالامتناع عن اتخاذ أي إجراء ضد الحقوق الدستورية.

ويُعد دور المحكمة الدستورية العليا ضرورياً وحيوياً في مجال تفسير وإيضاح ما يتعلق بالخصوصية وحمايته[2] إلا أنه ونتيجة لعدم وضوح الرؤية لمفهوم الخصوصية في الدستور الأمريكي فإن نظرة المحكمة الدستورية للحماية الدستورية للخصوصية الفردية اتسمت بالاضطراب وعدم الوضوح،[3] ومن الجدير بالملاحظة أنه وحتى الأعوام الأخيرة

---

1) يونس عرب ، الاتجاهات التشريعية للجرائم الالكترونية ، ورقة مقدمة لورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية ، عمان ، الأردن ، من 2 إلى 4 ابريل 2006م ، ص5.

2) ولعل أهم مظاهر الحق في الخصوصية في الولايات الأمريكية ما قضت به محاكمها من توافر الاعتداء على الخصوصية في حالة تركيب المؤجر لأجهزة تسجيل في غرف المستأجرين وكذلك اعتبارها تفتيش حقيبة المرأة بدون سبب مقنع هو انتهاك لخصوصيتها انظر في هذه الأحكام على شبكة الانترنت:http://www.internationalprivacy.org تاريخ الزيارة 2016/02/29م. كذلك قضية (أولمستيد ضد الولايات المتحدة) والتي تتعلق بحماية الرسائل عبر أسلاك التليفون من التفتيش والضبط غير المعقولين، وقد صدر الحكم لصالح المدعي، وذكرت المحكمة في أسباب الحكم أنه ينبغي تفسير التعديلات الدستورية بما يتفق وحماية خصوصية الأفراد من تطفل الأجهزة الحكومية، وهو تطفل غير مبرر، محمود إبراهيم غازي، مرجع سابق، ص259.

3) فريده كيت ، الخصوصية في عصر المعلومات ، ترجمة محمد محمود شهاب ، مركز الأهرام للترجمة والنشر ، الطبعة الأولى، 1999 ، ص 68-70.

من القرن الماضي ظلت المحكمة الفيدرالية العليا الأمريكية تؤكد على أحقية الفرد في الخصوصية.[1]

وإذا كان المشرع الدستوري لم يشر صراحة في صلب الدستور إلى حماية الحق في الخصوصية ، إلا أن ذلك لم يمنع المشرع من تقرير حماية لأوجه خاصة لهذا الحق، من حيث الحد من سلطان التدخل الحكومي في الشئون الخاصة للأفراد، وحق المواطنين في التعبير والمشاركة ، وتقييد عمليات القبض والتفتيش ، وحقهم في حرية اتخاذ القرارات الهامة، وتقييد الكشف عن المعلومات.

وانقسم الفقه الأمريكي فيما يتعلق بإمكانية المواءمة ما بين الدستور الأمريكي وتكنولوجيا المعلومات إلى مؤيد للاكتفاء بالدستور الأمريكي القائم مع الحاجة إلى التوسع في تفسير هذه النصوص بما في ذلك التشريعات الأدنى لكي يتم إحداث المواءمة المطلوبة.

ويستند أنصار هذا الاتجاه إلى حكم قديم للقضاء الأمريكي في 1967م عندما اعترفت المحكمة العليا الأمريكية بحماية الحقوق المعنية ، والتي تندرج ضمن نطاق الحق في الخصوصية باعتبارها من الحقوق الدستورية وفقاً للتعديل الرابع للدستور ، كما هو الشأن أيضاً في الحق في خصوصية الحديث المتبادل عبر الهاتف.[2]

---

1) لمعلومات أكثر حول اعتراف المحكمة العليا الفدرالية الأمريكية بالحق في الخصوصية أنظر موقع جريدة فرجينيا للقانون والتقنية على شبكة الانترنت: http://www.vjolt.net تاريخ الزيارة 2016/03/07م.

أنظر أيضاً : أيمن عبدالحفيظ ، إستراتجية مكافحة جرائم استخدام الحاسب الآلي ، د ن ، د ط ، د ت ، ص 227-228.

2) Katz C.U.S, 389 U.S. Supp 347, 1967ad.
http://www.supreme.justia.com/cases/federal/us/389/347/case.html

واتجاه آخر لا يكتفي بتعديل التشريعات القائمة ، وإنما يطالب بإجراء تعديلات دستورية في إطار حماية الحق في الخصوصية ، الأمر الذي يكفل المواءمة بين النصوص الدستورية والتطورات الحاصلة في مجال الخصوصية لاسيما تأثرها بتكنولوجيا المعلومات.

ونتناول فيما يلي كيفية حماية الخصوصية المعلوماتية في كل من التشريع الفيدرالي وتشريعات الولايات الأمريكية :

الفرع الأول: حماية الخصوصية في التشريع الفيدرالي الأمريكي:

يشتمل قانون شرف شفافية البلاغ الصادر 1970م على حقوق للمستهلك من حيث المحافظة على خصوصية المعلومات ، فيتضمن حق المستهلك في معرفة من يتم اطلاعه على تلك المعلومات الشخصية في نطاق المعلومات المالية ويجب الحصول على موافقته قبل القيام بذلك.[1]

وكذلك قانون الخصوصية الصادر 1974م والذي تم وضعه على أعقاب فضيحة "وترجيت" والذي استلزم ضرورة تحري الدقة عند الحصول على المعلومات ، وأن يكون مصدرها أصلياً وليس نقلياً.[2]

كما صدر في 1974م القانون المتعلق بالسجلات الدراسية ، والذي يحظر فيه هذا القانون على المؤسسات التعليمية كشف سجلات الطلاب لجهة دون موافقة كتابية، ويتعين عليها أن تدون بالسجلات هوية الجهة التي تطلب ، أو تحصل على حق الوصول للسجلات المدرسية للطلاب.[3]

---

1) The fair credit reporting Act of 1970, 15 U.S code sec. 1681 & seq.
انظر في هذا القانون وتعديلاته تفصيلاً لدى فريده كيت ، مرجع سابق ، ص 102-105.

2) 5 US Cod sec. 552a.

3) فريده كيت ، مرجع سابق ، ص 108-109.

وقانون سياسة كابل للاتصالات الصادر 1984م ، والذي يلزم شركات الإرسال المرئي بتوزيع بيان سنوي على المشتركين يراعي فيه خصوصية المعلومات عنهم ، كما أنه يحظر على شركات الإرسال المرئي تجميع والكشف عن المعلومات الشخصية للمشتركين، كما تضمن القانون عقوبات عن الأضرار التي تسبب في العدوان على الخصوصية.[1]

وصدر أيضاً في عام 1984م عن الكونجرس الأمريكي قانون أطلق عليه (قانون الاحتيال وإساءة استخدام الحاسب الآلي) وبموجب هذا القانون يعتبر الوصول إلى المعلومات الحكومية المصنفة بدون رخصة من عداد الجنايات ، كما تم اعتبار الوصول إلى القيود المالية أو بيانات الائتمان في المؤسسات المالية أو الوصول إلى الحاسبات الآلية الحكومية من عداد الجنح ، وقد تم تعديل هذا القانون بعد صدوره مرتين الأولى في عام 1986م والثانية في عام 1994م. [2]

وكذلك قانون الاتصالات الالكترونية الصادر 1986م؛[3] والذي يُعد امتداداً لقانون الاتصالات السلكية الفيدرالي الصادر 1934م ، والذي تم تطويره بمقتضى قانون الشوارع الآمنة والتحكم في الجرائم المرتكبة في العربات العمومية ،[4] ويطلق على هذا القانون الأخير مصطلح Title III إشارة إلى قيامه بإضافة فصل جديد إلى القانون يتعلق بحظر الحصول غير المشروع على أدلة من خلال القيام بتسجيل مضمون المحادثات الهاتفية ورصد تحويل المعلومات بما في ذلك البريد الإلكتروني ، وهو ما يشمل كل أنواع المراقبة الإلكترونية.[5] وقد كان الهدف من هذا

أيمن عبدالحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، د ن ، د ط ، 2005م ، ص 229.

1) The cable communication policy act of 1984ad (47 US code sec 551).

انظر حول هذا التشريع الموقع التالي:http://www.law.cornell.edu/uscode/text/47/551

2) محروس نصار غايب ، مرجع سابق ، ص113.

3) The electronic communications privacy act US code(ECPA) (18US Code – sec 2702).

4) The omnibus crime control and safe streets act of 1968 (18 US Code sea 2510 – 2521).

5) المرجع السابق.

القانون هو مد نطاق الاختصاص القضائي الفيدرالي إلى نطاق الاتصالات الإلكترونية، وذلك من ناحية تجريم المراقبة غير المصرح بها للاتصالات الإلكترونية، ويشمل ذلك نسخ أو الاطلاع على رسائل البريد الالكتروني والاتصالات الإلكترونية، والاتصالات الإلكترونية المخزنة ، كما يحظر القانون الدخول غير المصرح به إلى المراسلات والبيانات التي لها صلة بذاكرة الحاسب ، أي المخزنة في النظام المعلوماتي.

وقبل عام 1996م لم تكن توجد حماية تشريعية للمعلومات الخاصة بمعاملات الاتصالات السلكية واللاسلكية ، مثل أرقام الهواتف أو وقت ومكان الاتصال ومدته، ولم يكن قانون الاتصالات يطبق على المعلومات الخاصة بالمعاملات ، ولذلك لم يكن مقدمو الخدمات يواجهون قيوداً قانونية على جمع أو تخزين أو كشف المعلومات الخاصة بمعاملات الأشخاص الذين يستخدمون خدماتها المعلوماتية، وقد كان القانون يسمح باستخدام سجل مكتوب أو جهاز اكتشاف وتتبع لتسجيل المعلومات الخاصة بالمحادثات أو بمراسلات الأشخاص ، غير أنه وفي الأول من فبراير 1996م فقد أقر الكونجرس الأمريكي قانون الاتصالات السلكية واللاسلكية لعام 1996م الذي يتضمن أحكاماً توفر الحماية للخصوصية أي معلومات الشبكة الخاصة بالعملاء ، ويعرف هذا القانون المعلومات بأنها " المعلومات المتعلقة بالكم ، والشكل ، والنوع، والغرض ، ومقدار الاستخدام لخدمة الاتصالات السلكية واللاسلكية يشترط فيها أي عملية لنقل الاتصالات سلكية أو لاسلكية ، والمتاحة للناقل بواسطة العميل فقط بمقتضى علاقة الناقل بالعميل"، وبموجب هذا القانون يجوز لمقدمي الخدمات استخدام أو الكشف أو السماح بالوصول إلى معلومات الشبكة الخاصة بالعملاء التي يمكن معرفتها بصورة فردية عند الضرورة فقط لتقديم الخدمة.[1]

1) فريده كيت ، مرجع السابق ، ص 106 ؛ أيمن عبدالحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، مرجع السابق، ص 228.

وصدر قانون لحماية خصوصية الأطفال عبر الانترنت الصادر 1998م ، ويحظر هذا القانون على معدي المواقع عبر الانترنت نشر معلومات شخصية مصدرها الأطفال الذين لا تتجاوز أعمارهم ثلاثة عشر عاماً ، حيث يلتزم معدو المواقع وفقاً لهذا القانون بالحصول على إذن مسبق من أولياء الأمور لأجل نشر معلومات عبر الانترنت يكون مصدرها أطفال أقل من ثلاثة عشر عاماً ، كذلك ألزم هذا القانون أصحاب المواقع باتخاذ كافة الإجراءات التقنية والقانونية للمحافظة على المعلومات المتحصل عليها من هؤلاء الأطفال بمناسبة تعاملهم مع هذه المواقع وعدم الكشف عنها لطرف أخر.[1]

الفرع الثاني: حماية الخصوصية المعلوماتية في إطار تشريعات الولايات الأمريكية

بالنسبة للولايات المتحدة الأمريكية ، فقد أقرت ثمان ولايات منها على الأقل ضمانات دستورية صريحة للخصوصية الشخصية ، كما تضمن العديد من قوانين الولايات النص على قوانين تحمي الحق في الخصوصية ، إلا أن هذه الحماية غالباً ما تتسم بالغموض ، بالإضافة إلى أنها عندما تتعارض مع القانون الاتحادي فإن السيادة تكون للقانون الاتحادي وهو الأمر الذي يحد من أثرها في حماية الخصوصية. [2]

وينص قانون ولاية "أريزونا" على عدم إزعاج أي شخص في شؤونه الخاصة، أو التعدي على حرمة بيته بدون سلطة القانون.[3]

---

1) وقد دخل هذا القانون حيز التنفيذ في 2000/4/21م انظر القانون:
The children's online privacy protection act (COPPA) available at: تاريخ الزيارة 2015/04/12م.
http://www.fle.gov/goc/coppal.htm : http://www.bii-compliance.com/coppa.html

2) أيمن عبدالحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، مرجع سابق ، ص 203-204.

3) Arizona const, art 2 & 8. Available at the official website of Arizona http://www.azleg.gov

في عام 1980م عدلت ولاية "فلوريدا" دستورها لينص على " كل شخص طبيعي له الحق في أن يترك لشأنه ، وأن يكون متحرراً من تطفل الحكومة في حياته الخاصة فيما عدا ما ينص عليه بغير ذلك".[1]

وفي قانون ولاية "ألاسكا" لعام 1972م ينص على "حق الناس في الخصوصية حق مسلم به ولا يجوز انتهاكه".[2]

كما أضافت ولاية "كاليفورنيا" الخصوصية إلى الحقوق التي لا يجوز التصرف فيها والتي تصان بموجب قانونها.[3]

ينص قانون ولاية "إلينوي" على أن "من حق الناس أن يكونوا آمنين من التعديات على خصوصيتهم".[4]

وعدلت ولاية "هاواي" قانونها في عام 1978م لتضيف إليه "إن حق الناس في الخصوصية حق معترف به ، ولا يجوز التعدي عليه دون وجود مصلحة اضطرارية للدولة".[5]

وتجرم بعض تشريعات الولايات الأمريكية مجرد استراق النظر ، ويعرف مرتكب هذا الفعل بأنه الشخص الذي يحوم حول المنازل الخاصة ويختلس من نوافذها إلى سكانها على نحو يسبب لهم الذعر والضيق.

---

1) Florida const, art 1 & 23 1968ad. Available at the official website of Florida http://www.leg.state.fl.US

2) Alaska const, art 1& 22 1965ad. Available at the official website of Alaska http://www.itgov.alaska.gov

3) California const, art 1 & 1, 1990ad. Available at the official website of California http://www.leginfo.ca.gov

4) Illinois const, art 1 & 6, 1970ad. Available at the official website of \Illinois http://www.ilga.gov

5) Hawaii const, art 1 & 6. Available at the official website of Hawaii http://www.portalehawali.gov

وينص القانون الجنائي لولاية كاليفورنيا في القسم 64 على أن " يعتبر متشرداً كل شخص عمد ليلاً أثناء تجواله أو تسكعه أو تمضية الوقت على النظر خلسة من باب نافذة مسكن أو مبنى مؤجر مسكون ، دون أن يكون له شأن مع المالك أو شاغل المكان "، يعتبر تشريع ولاية "نيوجرسي" كل شخص يعتدي على الملكية الخاصة أو الحرية الشخصية لآخر، بطريقة الغش ، أو بواسطة اختلاس النظر من نوافذ أو فتحات الأماكن المؤجرة للسكن، وذلك لغرض غير قانوني ، منتهكاً للنظام.

إلا إن غالبية الولايات سنت نصوصاً تشريعية صريحة في تجريم أنشطة إساءة استخدام الحاسوب ، فنصت قوانين كل من (أريزونا ، كاليفورنيا ، كولارادو ، فلوريدا، جورجيا ، الينوى ، ميتشجان ، ميسوري ، مونتانا ، نيومكسيكو ، رود ايلاند ، تينسي، أوتاوا، كونتيكت)، على تجريم إتلاف القيم المعلوماتية غير المالية ، أو غش الحاسوب ، والاستخدام غير المصرح به للحاسوب ، وسرقة وقت أو خدمات الحاسوب ، أو إعاقة استخدامه، والتوصيل غير المصرح به لتعديل ، أو إنشاء ، أو استخدام البيانات المخزنة في نظام الحاسوب.[1]

وهنا يظهر لنا أن سياسة المشرع الولائي الأمريكي تأخذ أبعاداً متفاوتة فيما بينها، فبينما ينص بعضهم على الحماية الدستورية للخصوصية ، نجد بعضهم الآخر يضعها في نطاق الحماية القانونية ، ولهذا فقد تشكلت مجموعات عمل لوضع مفاهيم ومبادئ للخصوصية في القانون الأمريكي كان من أبرزها ما صدر من مبادئ عامة لجميع المشاركين في المجال المعلوماتي والتي صدرت في يونيو 1995م فمنها ما يتعلق بجميع المشاركين في المجال المعلوماتي ، وأخرى لمستخدمي المعلومات الشخصية، وأخرى للأفراد الذين يقدمون المعلومات الشخصية.

1) يونس عرب ، مرجع سابق ، ص5.

بالنسبة للفئة الأولى تتسم بثلاثة مبادئ وهي:

1. مبدأ خصوصية المعلومات ، ويعني الحصول على المعلومات الشخصية ، وكشفها، واستخدامها بطرق تحترم خصوصية الفرد.
2. مبدأ سلامة المعلومات ينبغي عدم تغيير ، أو إتلاف المعلومات الشخصية بصورة غير ملائمة.
3. مبدأ جودة المعلومات ، ينبغي أن تكون المعلومات الشخصية دقيقة ، وفي الوقت الملائم، ومناسبة للغرض التي تقدم وتستخدم من أجله.

أما بالنسبة لمبادئ الفئة الثانية وهي الخاصة بمستخدمي المعلومات ، فقد حددت مجموعة العمل خمسة مبادئ وهي:

1. مبادئ الامتلاك فينبغي لمستخدمي المعلومات تقييم التأثير على الخصوصية لتقرير ما إذا كان يتم امتلاك أو كشف أو استخدام المعلومات الشخصية ، وكذلك الحصول على المعلومات ، أو الاحتفاظ بها في صورة معقولة تدعم الأنشطة التجارية أو المستهدفة.
2. مبدأ الأخطار ، والذي يلزم مستخدمي المعلومات الذين يقومون بجمع المعلومات الشخصية بصورة مباشرة عن الفرد تقديم معلومات كافية ، ومناسبة لماذا يقومون بجمع المعلومات وما هو الهدف أو الغرض من جمعها ؟ وما هي الخطوات والإجراءات التي ستتخذ لحماية سريتها وسلامتها ودقتها ؟ ونتائج تقديم أو حجب المعلومات ، وأي حقوق أخرى لصاحب المعلومات.
3. مبدأ الحماية ، فينبغي على مستخدمي المعلومات استخدام ضوابط فنية وإدارية مناسبة لحماية سرية وسلامة المعلومات الشخصية.

4. مبدأ العدالة ، والذي يجب فيه على مستخدمي المعلومات الشخصية عدم استخدام المعلومات الشخصية بطرق لا تتفق مع فهم الفرد للكيفية التي ستستخدم بها ، ما لم يكن هناك مصلحة عامة اضطرارية لمثل هذا الاستخدام.
5. مبدأ التوعية ، والذي يجب فيه على مستخدمي المعلومات القيام بتوعية العملاء والجمهور بكيفية المحافظة على خصوصية المعلومات.

والمجموعة الأخيرة من المبادئ تتعلق بالأفراد الذين يقدمون المعلومات وتتضمن ثلاثة مبادئ هي:

1. مبدأ الوعي ، والذي ينبغي فيه على الأفراد أن يحصلوا على معلومات كافية ومناسبة عن السبب الذي يتم من أجله جمع المعلومات ، وما الغرض الذي ستستخدم فيه المعلومات، وما هي الخطوات التي ستتخذ لحماية المعلومات من حيث السرية والسلامة والنوعية ؟ نتائج تقديم أو حجب المعلومات ، وأي حقوق أخرى؟
2. مبدأ التمكين ، فيكون الأفراد من خلال تطبيق هذا المبدأ على علم بكيفية حماية خصوصيتهم بأن تتوافر لديهم وسيلة للحصول على معلوماتهم الشخصية ، وسيلة لتصحيح معلوماتهم الشخصية غير الدقيقة ، أو غير الصحيحة ، الفرصة لاستخدام ضوابط فنية مناسبة ، مثل التشفير لحماية سرية الاتصالات والمعاملات.
3. مبدأ العدالة فيكون لدى الأفراد وسيلة يتم اللجوء إليها لحماية معلوماتهم الشخصية في حالة الاستخدام غير المشروع أو الإفشاء غير القانوني.[1]

1) فريده كيت ، مرجع سابق ، ص 112– وما بعدها راجع ايضاً الموقع التالي: http://www.iitf.nist.gov تاريخ الزيارة 2016/09/02م .

ويتضح لنا من خلال ما سبق أن التشريعات الأمريكية توفر حماية على قدر عالٍ جداً للخصوصية المعلوماتية ، وإن كانت تختلف عن ما هو وارد في التشريع الفرنسي ، وذلك لأن القانون الأمريكي يعتمد على تفسير القضاء لنصوص الدستور ، إلا أنه يتفق التشريع الأمريكي والفرنسي في كون كلاهما يواكبان التطورات الحاصلة في مجال التقنية، ويوفران الحماية اللازمة للخصوصية المعلوماتية.

وبمراجعة التشريعات على مستوى الولايات الأمريكية تجد تفاوتاً في مدى الحماية التي توفرها هذه التشريعات للخصوصية عامة والخصوصية المعلوماتية خاصة ، وهذا يرجع سببه لما تتمتع به الجرائم الالكترونية ، والجرائم التي تقع على الخصوصية المعلوماتية من صفة الحداثة ، بالإضافة إلى تطورها ، الأمر الذي يجعل هناك تفاوتاً في مدي تجاوب المشرع في بعض الولايات بالمقارنة بالولايات الأخرى. [1]

1) فكل ولاية من الولايات الأمريكية الحرية في إصدار تشريعات داخلية لتنظيم كل الأمور داخل الولاية فقد تجد فعل في ولاية معاقباً عليه بعقوبة في ولاية ما ومعاقبة عليه بعقوبة مختلفة في ولاية أخرى إلا انه ما يجدر الإشارة إليه إن لنصوص التشريع الفيدرالي الغلبة في التطبيق دائماً في حالة تعارضها مع نصوص تشريعية ولائية.

المبحث الثاني
حماية الخصوصية المعلوماتية
في بعض التشريعات العربية والتشريع الليبي

تمهيد:

إن الدول العربية شأنها شأن غيرها من دول العالم أصبحت تعتمد اعتماداً كبيراً على التكنولوجيا الحديثة وشبكة المعلومات ، وهذا ما استتبع ضرورة قيام الدول العربية باتخاذ الإجراءات والتدابير التي من شأنها توفير الاستخدام الأمن لهذه التكنولوجيا ومواجهة أي انتهاك قد يقع عليها ، ولهذا قامت العديد من الدول إما بإصدار تشريعات خاصة لحماية الخصوصية المعلوماتية أو بالنص على هذه الحماية في قانون العقوبات.

وحتى نوضح ما مدى الحماية للخصوصية المعلوماتية في الدول العربية ، سنسلط الضوء على عدد من الدول ، وفي هذا المجال هناك دول عربية كانت رائدة في مجال حماية الخصوصية المعلوماتية في المنطقة ، ومنها المملكة البحرينية والإمارات العربية المتحدة وتحديداً إمارة دبي.

ولهذا سوف نتناول في هذا المبحث الحماية الجنائية للخصوصية المعلوماتية في بعض التشريعات العربية ، والتشريع الليبي وذلك بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: حماية الخصوصية المعلوماتية في بعض التشريعات العربية.

المطلب الثاني: حماية الخصوصية المعلوماتية في التشريع الليبي.

المطلب الأول

حماية الخصوصية المعلوماتية
في بعض التشريعات العربية

أظهرت الدراسة البحثية أن نحو خمسين دولة من دول العالم قد أقرت تشريعات شاملة في حقل البيانات ، وأن حوالي عشرين دولة تبذل جهوداً تشريعية في هذا الوقت لوضع قوانين في ذات الحقل ، أو تعديل قواعدها القانونية القائمة لتحقيق حماية البيانات ، وتحديداً البيانات الشخصية والأسرار من مخاطر المعالجة الآلية للبيانات.[1]

غير أنه لا تتضمن تشريعات اغلب الدول العربية حتى اليوم إلا بعض النصوص المباشرة في قوانين الأحوال المدنية ، والوثائق والأسرار الحكومية ، وبعض تشريعات المهن ، كقوانين تنظيم مهنة المحاماة ، أو التشريعات الصحية، وبعض نصوص قوانين العقوبات.

وليس الأمر بأفضل على الصعيد الدستوري رغم إقرار أو تعديل عدد من الدساتير العربية في عقد التسعينات،[2] حيث انحصر حد الخصوصية فيما يتجاوز مظاهرها المادية لدى بعض الدول بإقرار المبدأ العام دون التعرض للبيانات الشخصية،[3] وفي هذا الصدد فإن هناك دولاً عربية أقرت حماية الحياة الخاصة للإنسان ، أو خصوصيات الإنسان كمبدأ عام، ومنها الدستور الموريتاني حَيْثُ ينص على أن " .... تضمن الدولة شرف المواطن وحياته الخاصة وحرمة

---

1) انظر عائض المري ، الخصوصية وحماية البيانات ، مرجع سابق .

2) فقد تم إقرار الدستور اللبناني في عام 1984م، وكذلك الدستور الموريتاني في عام 1991م ، وتم تعديل الدستور التونسي في عام 1988م .

3) حيث تم النص في الدساتير العربية فقط على حماية المسكن والمراسلات ومنها الدستور اللبناني لعام 1984م وجاء النص عليها في المادة (14) ، الدستور الأردني لعام 1952م مادة (10 – 18) ، الدستور التونسي لعام 1959م المعدل عام 1988م الفصل التاسع ، دستور دولة الكويت لعام 1962م في المادة (38 – 39) ، الدستور السوري لعام 1973م في المادة (31 – 32) ، دستور دولة البحرين لعام 1973م في المادة (25 –26). أنظر تلك النصوص الدستورية بالموقع التالي:
http://www.arablaw.org تاريخ الزيارة 2015/04/20م

شخصه ومسكنه ومراسلاته "،[1] وينص الدستور الجزائري على أنه " لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ، ويحميها القانون وسرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".[2]

وقد ظهر هذا الحق لأول مرة في الدستور المصري عام 2012م ، حيث نصت المادة (47) على "الحصول على المعلومات والبيانات والإحصاءات ، والإفصاح عنها ، وتداولها حق تكفله الدولة لكل مواطن؛ بما لا يمس حرمة الحياة الخاصة ، وحقوق الآخرين، ولا يتعارض مع الأمن القومي".[3]

إلا أنهُ يُؤخذ على هذا النص ما يشوبه من غموض فيما يتعلق بالأمن القومي، حيث يُعطي هذا المصطلح فرصة لتبرير حجب جميع المعلومات ، أما في دستور 2014م فقد تم إلغاء الشروط المُقيدة لحق الحصول على المعلومات "المساس بالحريات الخاصة، وحقوق الآخرين، والتعارض مع الأمن القومي" من نص المادة (68) التي أحالت كل هذه الأمور للقانون.

يبدو واضحاً أن الدساتير العربية جاءت خالية من أي حماية للبيانات الشخصية للأفراد – باستثناء الدساتير سالفة الذكر – حيث لا يوجد أي دستور عربي ينص على حماية البيانات الشخصية صراحة ، أو يُقيد إجراءات جمع البيانات وتخزينها واستخدامها من قبل السلطات العامة بالخضوع للقانون ، أو للأغراض المستخدمة في النظم القانونية العربية.

الفرع الأول: حماية الخصوصية المعلوماتية في التشريع البحريني

1) الدستور الموريتاني لعام 1991م ، المادة 13.

2) الدستور الجزائري ، المادة 39.

3) الدستور المصري لعام 2012م المعدل عام 2014م ، وانظر سائر تلك القوانين العربية بالموقع التالي
http://www.arablaw.org/Download/Privacy_ArabWorld_Article.doc تاريخ الزيارة 2015/04/20م

اهتم المشرع البحريني بحماية الحياة الخاصة وكفلها بالنص عليها في الدستور، حيث تنص المادة (25) من الدستور البحريني المعدل في عام 2002م على (للمساكن حرمة، فلا يجوز دخولها أو تفتيشها بغير إذن أهلها إلا استثناء في حالات الضرورة القصوى ..) ، كما نص في المادة (26) على (حرية المراسلة البريدية، والبرقية والهاتفية، والإلكترونية مصونة ، وسريتها مكفولة ، فلا يجوز مراقبة المراسلات ، أو إفشاء سريتها ، إلا في الضرورات ...) ، ونلاحظ من النصوص السابقة مدى الاهتمام بحماية الحياة الخاصة لدى المشرع البحريني ، والحال كذلك في القوانين العقابية.

أولاً: حماية الخصوصية المعلوماتية في قانون العقوبات البحريني

يحرص المشرع البحريني على حماية الحياة الخاصة من الاعتداءات التي تهددها نتيجة التقدم العلمي وتكنولوجيا المعلومات ، ومن صور هذه الحماية ما تم النص عليه من خلال نص المادة (370) من قانون العقوبات ، (يعاقب بالحبس مدة لا تزيد على ستة أشهر وبالغرامة التي لا تجاوز خمسين ديناراً ، أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة ، أو العائلية للأفراد، ولو كانت صحيحة ، إذا كان من شأن نشرها الإساءة إليهم) ، والملاحظ هنا أن العقاب على فعل النشر والإذاعة بالوسائل العلانية ، وهذا قد لا يشمل وسائل التكنولوجيا الحديثة حيث يتم إساءة استخدام هذه المعلومات ، أو الصور ، أو الإطلاع عليها ، عن طريق وسائل التقنية الحديثة.

كما نص المشرع في المادة (371) على (يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة التي لا تجاوز مائة دينار من كان بحكم مهنته أو حرفته أو وضعه أو فنه مستودع سر فأفشاه في غير الأحوال المصرح بها قانوناً ، أو استعمله لمنفعته الخاصة أو لمنفعة شخص أخر ،

وذلك ما لم يأذن صاحب الشأن في السر بإفشائه أو استعماله ، وتكون العقوبة السجن مدة لا تزيد على خمس سنين ، إذا كان الجاني موظفاً عاماً ...) ، وهنا المشرع البحريني لم يحدد وسيلة الإفشاء ، أو طريقة الاستعمال ، وبالتالي فهو يشمل كل صور الإفشاء ، سواء العادي أو الإلكتروني.

كما جاء نص المادة (372) من قانون العقوبات البحريني كالأتي: (يعاقب بالغرامة التي لا تجاوز عشرين دينار من فض رسالة أو برقية بغير رضا من أرسلت إليه ، أو استرق السمع في مكالمة تليفونية ، ويعاقب بالحبس مدة لا تزيد على ستة أشهر ، أو بالغرامة التي لا تجاوز خمسين ديناراً ، إذا أفشى الرسالة ، أو البرقية ، أو المكالمة لغير من وجهت إليه ودون إذنه ، متى كان من شأن ذلك إلحاق ضرر بالغير) ، والملاحظ هنا أن الحماية قاصرة على المراسلات البريدية العادية ، وبالتالي لا يمكن تطبيقها على المراسلات الإلكترونية التي تتم بوسائل التقنية الحديثة.

ثانياً: قانون التجارة الالكترونية البحريني وحماية الخصوصية المعلوماتية[1].

عرف المشرع البحريني المعلومات بأنها: البيانات، والنصوص، والصور، والأشكال، والأصوات، والرموز، وبرامج الحاسب، والبرمجيات قواعد البيانات، والكلام، وما شابه ذلك.

ونظام المعلومات بأنه: نظام الكتروني لإنشاء، أو إرسال، أو بث، أو تسلم، أو حفظ، أو عرض، أو تقديم المعلومات. [1]

1) قانون التجارة الالكترونية البحريني سبتمبر 2002م ؛ انظر محمد حسام محمود لطفي ، الإطار القانوني للمعاملات الالكترونية ، دار النهضة العربية ، القاهرة مصر ، 2002 ، ص 200 وما بعدها . وانظر أيضاً هذا القانون بالموقع التالي: http://www.arablaw.org/dawnload/EC_Bahrain.doc تاريخ الزيارة 2015/04/20م:

والتوقيع الإلكتروني: بأنه معلومات في شكل الكتروني يكون وجوده في سجل الكتروني، أو مثبتة، أو مرتبطاً به منطقياً ، ويمكن للموقع استعمالها لإثبات هويته.

ونص المشرع في المادة (24) من القانون على عقوبات لمرتكبي الأفعال التالية:

1. مع عدم الإخلال بأية عقوبة أشد ، ينص عليها أي قانون أخر، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار، أو بإحدى هاتين العقوبتين، كل من ارتكب عمداً فعلاً من الأفعال الآتية:

أ. نسخ، أو حيازة، أو إعادة تكوين أداة إنشاء توقيع الكتروني لشخص آخر، أو الدخول على أداة إنشاء هذا التوقيع دون تفويض بذلك من هذا الشخص، وبسوء نية.

ب. تحريف، أو تغيير، أو استعمال شهادة ، أو إفشاء أداة إنشاء توقيع الكتروني لشخص آخر دون تفويض منه بذلك ، أو بما يجاوز حدود هذا التفويض .

ج. إنشاء، أو نشر، أو تحريف أو استعمال شهادة، أو توقيع الكتروني لغرض احتيالي أو لأي غرض غير مشروع.

د. انتحال هوية شخص آخر، أو الإدعاء زوراً بأنه مفوض من قبله في طلب الحصول على شهادة، أو قبولها ، أو طلب تعليق العمل بها، أو إلغائها.

---

1) والجدير بالملاحظة أن المشرع البحريني قد عرف المعلومات بنفس الصياغة الواردة في قانون المعاملات الإلكترونية وحماية الخصوصية الأردني رقم (58) لعام 2001م وهذا يؤكد أن المشرع البحريني عند صياغة قانون التجارة الالكترونية قد وضع قانون المعاملات الالكترونية الأردني من ضمن مراجعه ، وللإطلاع على هذا القانون انظر الموقع التالي:
http://www.arablaw.org/dawnload/EC_Jordan_Ar.doc تاريخ الزيارة 2015/04/20م.

وهذه الفقرات تجرم أي فعل من شأنه المساس بصحة وسلامة التوقيع الالكتروني، بما في ذلك المعلومات والبيانات الشخصية الخاصة بالأفراد التي يتعلق بها التوقيع الالكتروني، والتي يتم إصدارها للشخص بناءً عليها.

ونص المشرع على مسؤولية الشخص الاعتباري وموظفيه، فيسأل الشخص الاعتباري جنائياً ويعاقب بالغرامة التي لا تجاوز مائتي ألف دينار ، إذا ارتكبت أياً من الجرائم المنصوص عليها في هذا القانون باسمه، ولحسابه، أو باستعماله إحدى وسائله ، وكان ذلك نتيجة تصرف، أو إهمال جسيم، أو موافقة، أو تستر من أي عضو مجلس إدارة أو مدير، أو أي مسؤول آخر – في ذلك الشخص الاعتباري – أو ممن يتصرف بهذه الصفة.

ويعد مرتكباً للجريمة كل من أسند إليه من هؤلاء الأشخاص الطبيعيين ارتكاب أي من الأفعال المذكورة، ويُعاقب بالعقوبة المقررة لها طبقاً لأحكام هذا القانون.[1]

وهنا نرى أن المشرع البحريني قد أصاب عندما أفرد للجرائم التي تقع في المجال المعلوماتي قانوناً خاصاً – وإن كانت هذه النصوص خاصة بالتجارة الالكترونية فقط– وهذا على خلاف ما يراه البعض من أن قوانين العقوبات القائمة تكفي لمواجهة الجرائم المعلوماتية ، فهذه الأخيرة من الصعب تطبيقها مع هذا النوع من الجرائم، ويرجع ذلك لعدة أسباب، منها ما يتعلق بإمكانية تعارضها مع مبدأ الشرعية ، وعدم التوسع في تفسير النصوص الجنائية ، ومنها ما يتعلق بطبيعة الجرائم الالكترونية غير المادية .

وعلى الرغم مما يوفره هذا القانون والقوانين الموازية له في الدول العربية،[1] إلا أن الحماية تظل قاصرة على البيانات التي يتم تداولها في مجال التجارة الإلكترونية.

---

1) مادة 25.

الفرع الثاني:حماية الخصوصية المعلوماتية في التشريع الإماراتي.

لم يكن المشرع الإماراتي اقل اهتماما من نظيره البحريني ، فقد أولى الجرائم المرتكبة ضد الخصوصية اهتماما كبيراً ، لا سيما ما يقع منها بالوسائل التقنية الحديثة ، حيث عالجها بإصدار قوانين خاصة لمكافحتها ، من هذه القوانين القانون رقم (2) لعام 2006م بشأن مكافحة الجرائم المعلوماتية ، وكذلك قانون إمارة دبي رقم (2) لعام 2002م بشأن المعاملات التجارية الإلكترونية.

أولاً: حماية الخصوصية في قانون رقم (2) لعام 2006م بشأن مكافحة جرائم تقنية المعلومات.

قد نص المشرع في هذا القانون علي مجموعة من الجرائم المعلوماتية، منها ما يتعلق بالانتهاكات الواقعة على الخصوصية المعلوماتية من هذه الجرائم (التعدي على البيانات الشخصية، وإلغاء بيانات، أو معلومات، أو حذفها، أو تدميرها، أو إفشائها، أو إتلافها، أو تغييرها، أو إعادة نشرها) ، فقد نص المشرع في هذا القانون على 29 مادة، أفرد المادة الأولى للتعريفات ، بينما نص في المادة (2) على الدخول إلى الموقع، أو النظام، وما يترتب على هذا الفعل من إلغاء، أو حذف، أو تدمير، أو إفشاء وغيرها .

كما نص المشرع في المادة رقم (3) على عقوبة ارتكاب الأفعال الواردة في البند (2) من المادة (2) من قبل أحد الموظفين، أو المخولين بالإطلاع عليها ، ولم يكتف المشرع في هذا القانون بالنص على تجريم الأفعال السابقة، بل ذهب إلى أبعد من ذلك، بأن عاقب من خلال المادة (5) كل من أعاق، أو عطل الوصول إلى الخدمة، أو مصادر البيانات،

---

1) قانون المعاملات الالكترونية التونسي (83) لعام 2000م المعدل عام 2001م ، قانون المعاملات الالكترونية العُماني (96) لعام 2008م ، قانون المعاملات الالكترونية المصري رقم (15) لعام 2004م ، قانون المعاملات الالكترونية السوداني لعام 2007م، قانون المعاملات الالكترونية للسلطة الوطنية الفلسطينية لعام 2010م ، قانون المعاملات والتجارة الالكترونية القطري لعام 2010م. http://www.arablaw.org تاريخ الزيارة 2015/04/20م.

أو المعلومات ، كما شملت الحماية المعلومات الطبية من خلال المادة رقم (7) (يعاقب بالسجن المؤقت، أو الحبس كل من عدل، أو اتلف الفحوصات الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير ذلك، أو مكنه منه باستعمال الشبكة المعلوماتية، أو بإحدى هاتين العقوبتين)، وكذلك البيانات المصرفية من بطاقات ائتمانية وغيرها من خلال المادة رقم (11)، كما أفرد نص المادة رقم (8) للمعاقبة على أفعال التنصت، أو التقاط ما هو مرسل عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات (كل من تنصت أو ألتقط أو أعترض عمداً دون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين).

وبالرغم من قيام المشرع في هذا القانون بتجريم العديد من الأفعال التي من شأنها أن تضر بالمعلوماتية وتكنولوجيا الاتصالات ، إلا إن هذا لوحده لا يوفر الحماية الكافية للخصوصية المعلوماتية بالصورة التي سبق عرضها لدى التشريع الفرنسي، أو الأمريكي. **ثانياً: قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية**[1].

ورد بقانون إمارة دبي بالمادة الثانية تعريف لبعض المصطلحات المستخدمة في هذا القانون وذلك لتحديد مفهومها القانوني نظراً لحداثتها وهي:

المعلومات الالكترونية بأنها: معلومات ذات خصائص الكترونية في شكل نصوص، أو رموز، أو أصوات، أو رسوم، أو صور، أو برامج حاسب آلي، أو غيرها من قواعد البيانات.

1) قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية. http://www.arablaw.org/downlod/EC_UAE.doc تاريخ الزيارة 2015/04/20م.

النظام المعلوماتي الالكتروني بأنه: نظام الكتروني لإنشاء أو استخراج أو إرسال، أو استلام، أو تخزين، أو عرض، أو مُعالجة المعلومات، أو الرسائل الكترونياً.

والتوقيع الالكتروني بأنه: توقيع مكون من حروف، أو أرقام، أو رموز، أو صوت، أو نظام مُعالجة ذي شكل الكتروني وملحق، أو مرتبط منطقياً برسالة الكترونية وممهور بنية توثيق، أو اعتماد تلك الرسالة، والتوقيع الالكتروني المحمي هو التوقيع الالكتروني المستوفى لشروط المادة (20) من هذا القانون، والتي تنص على أن:

1. يعامل التوقيع على أنه توقيع الكتروني محمي إذا كان من الممكن التحقق منه من خلال تطبيق إجراءات توثيق مُحكمة ، منصوص عليها في هذا القانون، أو معقولة تجارياً ومتفق عليها بين الطرفين، من أن التوقيع الالكتروني كان في الوقت الذي تم فيه:
   أ. ينفرد به الشخص الذي استخدمه.
   ب. ومن الممكن أن يثبت هوية ذلك الشخص.
   ج. وأن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه، أو وسيلة استعماله وقت التوقيع.
   د. ويرتبط بالرسالة الالكترونية ذات الصلة به، أو بطريقة توفر تأكيداً يعول عليه حول سلامة التوقيع ، بحيث إذا تم تغيير السجل الالكتروني فإن التوقيع الالكتروني يصبح غير محمي.

وعرف الموقع بأنه " الشخص الطبيعي، أو المعنوي الحائز لأداة توقيع إلكتروني خاصة به، ويقوم بالتوقيع، أو يتم التوقيع بالنيابة عنه على الرسالة الالكترونية باستخدام هذه الأداة ".

نص في الفصل السابع على توقيع العقوبات على ارتكاب الأفعال التالية:

1. لا يجوز لأي شخص أن ينشر شهادة تشير إلى مزود خدمات التصديق مدرج اسمه في الشهادة ، إذا كان الشخص يعرف أن:

أ. مزود خدمات التصديق المدرج اسمه في الشهادة لم يصدر الشهادة.

ب. الموقع المدرج اسمه في الشهادة لم يقبل الشهادة.

ج. الشهادة قد ألغيت أو أوقفت ، إلا إذا كان ذلك النشر بغرض التحقق من توقيع الكتروني، أو رقمي تم استعماله قبل الإيقاف، أو الإلغاء.

2. يعاقب كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات، أو مستندات، أو مراسلات الكترونية ، وأفشى متعمداً أياً من هذه المعلومات ، بالحبس وبغرامة لا تجاوز 100,000 درهم ، أو بإحدى هاتين العقوبتين. وتكون العقوبة الغرامة التي لا تجاوز 100,000 درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات.[1]

يستثني من أحكام الفقرة السابقة من هذه المادة حالات التصريح التي تتم لأغراض تنفيذ أوامر هذا القانون ، أو أية إجراءات جزائية حول جرم ارتكب بالمخالفة لأي قانون، أو لأغراض الأوامر الصادرة عن أية سلطة قضائية.

3. مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب كل من ارتكب فعلاً يشكل جريمة بموجب التشريعات النافذة ، باستخدام وسيلة الكترونية بالحبس لمدة لا تزيد على ستة أشهر ، وبغرامة لا تتجاوز 10,000 درهم ، أو بإحدى هاتين العقوبتين، ويُعاقب

1) قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية (مادة28).

بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذه المادة.[1]

وهذا النص هو نص عام يحيل في تكييف الفعل ووصفه بأنه جريمة على قانون العقوبات ، وتطبق العقوبة الأشد على الفاعل سواء أكانت تلك التي وردت في قانون العقوبات، أو الواردة في هذا القانون، وهنا يساوي بينها وبين الأفعال النظيرة لها المجرمة في قانون العقوبات إلا أنها ارتكبت في هذه الحالة بوسائل معلوماتية، ويترتب على ذلك صعوبة تطبيق النص، نظراً للتغيير الذي يحدث في بعض أركان الجريمة وخاصة في محلها ونشاطها المادي.

وبهذه الصورة يكون المشرع قد حافظ على مبدأ الشرعية ، ولم يغال في التجريم بما يؤدي إلى تداخل النصوص، أو إلى تجريم أفعال لا تجرم في الأحوال العادية، إلا أنه أوجد ازدواجية في العقاب، وكان من الأفضل أن يحيل المشرع إلى النص الجنائي في العقاب، حتى تكون هناك مساواة في المعاملة العقابية للفعل الواحد إلا إذا كان المشرع يريد أن يجعل من استخدام الوسيلة الالكترونية ظرفاً مشدداً للعقاب.

4. يعاقب المشرع على الفعل غير المشروع وفقاً لهذا القانون إذا ارتكب من أي شخص اعتباري، بالمخالفة لأحكام هذا القانون، أو اللوائح الصادرة بموجبه وثبت أن ذلك جاء نتيجة لتصرف، أو إهمال، أو موافقة، أو تستر أي عضو مجلس إدارة، أو مدير، أو أي موظف أخر في ذلك الشخص الاعتباري، أو أي شخص يبدو أنه يتصرف بهذه

1) مادة 2.

الصفة، فإن ذلك الشخص والشخص الاعتباري يدانان بهذه الصفة فإن ذلك الشخص والشخص الاعتباري يدانان بهذه المخالفة، ويعاقبان تبعاً لذلك.[1]

ومن خلال عرض هذه النصوص يتضح لنا أنه بالرغم من حداثة هذه النصوص ومجاراتها للتطورات الحديثة في مجال التجارة الإلكترونية ، إلا أن ما توفره هذه النصوص من حماية للخصوصية المعلوماتية يظل قاصراً على التجارة الالكترونية ، وهذا لا يعد كافياً لتوفير الحماية لخصوصية المعلومات في ظل التطورات التكنولوجية في مجال الاتصالات، والتقنية الحديثة ودخولها في مناحي الحياة المختلفة.

وبالرغم من المبادرات في مجال حماية خصوصية المعلومات وإيجاد الاستراتجيات اللازمة لتطبيقها في الوطن العربي، وما أُنجز في مجال حقل التجارة الإلكترونية في كل من (البحرين ، إمارة دبي ، الأردن ، تونس ، مصر) إلا أنه إلى الآن لا يوجد قانون واحد لحماية البيانات الشخصية، كما لا يوجد قانون يحمي حرية الوصول للمعلومات في هذه الدول.

وهذا الوضع يجعل القاضي في وضع حرج عند مواجهة واقعة متعلقة بانتهاكات بواسطة التقنية الحديثة ، فهو لا يستطيع دائماً تطبيق قانون المعاملات الالكترونية ، وذلك لان هذا الأخير لا يطبق إلا بخصوص الانتهاكات التي تحصل في مجال التجارة الالكترونية، كما أن تطبيقه للنصوص التقليدية في قانون العقوبات يفتح المجال للقياس.

وهذا الأمر محظور في المسائل الجنائية ، وبالتالي تظهر لنا الحاجة الملحة لسن تشريعات خاصة بالجرائم الالكترونية، وجرائم الانترنت وتجريم ما يقع منها على الخصوصية.

---

1) مادة 33 من القانون السابق.

المطلب الثاني
حماية الخصوصية المعلوماتية
في التشريع الليبي

لقد حرم المشرع الليبي المساس بالخصوصية، إذ نص على ذلك في دستور المملكة لعام 1951م حيث حظر التدخل في الحياة الخاصة ما لم يتم المساس بالنظام العام، والآداب أو في حالة تشكيلها خطراً على الآخرين وذلك من خلال المادة (16) " للحياة الخاصة حرمة ويحظر التدخل فيها ، إلا إذا شكلت مساساً بالنظام والآداب العامة ، أو ضرراً بالآخرين ، أو إذا اشتكى أحد أطرافها " .

وباستعراض التشريعات الصادرة في ليبيا نجد أن قانون أمن الدولة رقم (64) لعام 1957م نص على بعض الجرائم التي تشتمل على انتهاك خصوصية المعلومات، من ذلك جريمة إرسال التقارير لحساب جهة أجنبية، والتي أفرد لها عقاباً سواء ارتكبت من قبل شخص طبيعي أو معنوي.

ولم يتوقف النص علي حرمة الحياة الخاصة في التشريعات الليبية على ما هو وارد في الدستور في عهد المملكة الليبية ، فقد صدر قانون رقم (20) لعام 1991م بشأن تعزيز الحرية (وثيقة دستورية)،[1] ونص في المادة 15 منه على " سرية المراسلات مكفولة فلا يجوز مراقبتها إلا في أحوال ضيقة يقتضيها أمن المجتمع، وبعد الحصول على إذن بذلك من جهة قضائية" ، وفي المادة 16 نص على " للحياة الخاصة حرمة ويحظر التدخل فيها ..." ، وهذه الوثيقة الغيت بموجب الإعلان الدستوري الصادر في 3 أغسطس 2011م ونص في المادة (11) على حرمة

1) انظر نصوص هذا القانون على الموقع الرسمي لوزارة العدل الليبية http://www.aladel.gov.ly .

الممتلكات الخاصة وعدم جواز دخولها أو تفتيشها إلا بإذن ، كما نص في المادة (12) على حرمة الحياة الخاصة للمواطنين ، ولعل ما يهمنا هو نص المادة (13) والتي جاء فيها " للمراسلات والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمتها وسريتها وهما مكفولتان ولا يجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي ولمدة محددة وفقاً لأحكام القانون".

وكما هو معروف فإن الحماية الجنائية للخصوصية المعلوماتية لا تتوفر إلا عن طريق نص المشرع على تجريم الأفعال التي من شأنها انتهاك هذه الخصوصية، وكذلك تحديد العقوبات الرادعة لها ، وبالاطلاع علي جُملة التشريعات في ليبيا لا نجد قانوناً يُعنى بحماية خصوصية المعلومات، كما أسلفنا في استعراضنا لبعض التشريعات العربية، [1] حيث نجد بعض القوانين الخاصة التي تحمي الخصوصية في المجالات التي صدرت هذه القوانين من أجل تنظيمها، ومن ذلك ما نصت عليه المادة (13) من قانون المسؤولية الطبية بأنه " لا يجوز إفشاء أسرار المريض التي يطلع عليها بسبب مزاولة المهنة إلا للجهات القضائية، وفقاً للقانون"[2] ، فقد تقضي طبيعة عمل الطبيب معرفة أسرار مريضه الخاصة، وما يتعلق بطبيعة المرض، وأسبابه، ومدى خطورته، ولهذا فإن كلاً من الأطباء والجراحين والصيادلة والقوابل إذا كان مودعاً إليه سر خاص – بمقتضى وظيفته – وكان مؤتمناً عن هذا السر فلا يفشيه إلا في الحالات التي يلزمه القانون بالبلاغ،[3] وقد يكون أول تشريع فيه إشارة واضحة لحماية خصوصية المعلومات هو القانون رقم 4 لعام 1990م بشأن النظام الوطني للمعلومات والتوثيق ، حيث أن الغرض من تشريع هذا القانون هو وضع نظام لتوثيق المعلومات، وإنشاء مرجع معلوماتي

1) هناك مبادرات لإصدار المسودة الأولى لقانون المعاملات الالكترونية الليبي مع منظمة الإسكو التابعة للأمم المتحدة وذلك بتاريخ 2014/03/24م انظر في ذلك الموقع التالي:http://www.ltnet.ly تاريخ الزيارة 2015/07/18م.

2)الجريدة الرسمية ، العدد 28 ، 1986م، القانون رقم 17 لعام 1986م بشأن المسؤولية الطبية .

3) السيد عبد الوهاب عرفة، الوجيز في مسئولية الطبيب والصيدلي، دار المطبوعات الجامعية، الإسكندرية مصر، 2005م، ص77.

وإحصائي يكون في خدمة الأجهزة العاملة في الدولة ، وجاء في هذا القانون عدد من النصوص الغرض منها حماية البيانات، ومنها نص المادة الثامنة التي تجرم إساءة استعمال أو حيازة البيانات ، أو التقصير في التزام تسجيلها ، أو الإخلال بالحفاظ على سريتها ، أو إتلافها أو تغييرها.

وتجدر الإشارة هنا أن الحماية التي يوفرها القانون رقم (4) لسنة 1990م بشأن النظام الوطني للمعلومات والتوثيق، هي حماية قاصرة على المعلومات المخزنة في هذا النظام الوطني، ولا تنطبق على غيره من البيانات سواء المخزنة في المؤسسات العامة أو الخاصة.[1]

إلا أن قانون الاتصالات رقم (22) الصادر عام 2010م بمناسبة تنظيم العمل في قطاع الاتصالات وردت فيه نصوص عديدة بشأن حماية خصوصية المعلومات من الانتهاكات التي قد تقع عليها.

ومن خلال العرض السابق للقوانين سالفة الذكر نجد شُحاً في النصوص القديمة والحديثة التي من شأنها حماية الخصوصية عامة، وخصوصية المعلومات خاصة، ولا يفوتنا في هذا الاطلاع على مدى الحماية التي أفردها المشرع للخصوصية من خلال نصوص قانون العقوبات.

1) رحاب عميش ، تحديات الجريمة المعلوماتية ، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون ، طرابلس، ليبيا ، في الفترة من 28 إلى29 أكتوبر 2009م، ص9.

الفرع الأول: حماية الخصوصية في قانون العقوبات:

إن قانون العقوبات يهدف إلى حماية مصالح المجتمع المختلفة سواء كانت مادية أو معنوية ، فمثلاً المصالح الاقتصادية والصناعية والتجارية يحميها الباب الثامن من الكتاب الثاني من قانون العقوبات الليبي المواد(من 358 إلى 367) ، والمصالح الدينية يحميها الباب الرابع من الكتاب الثالث المواد (من 289 إلى 295) ، أما فيما يتعلق بحريات الأفراد فقد تم حمايتها من خلال الباب الرابع من الكتاب الثالث المواد (من 425 إلى 437)،[1] وبالرجوع إلى الباب الرابع الخاص بالحريات نجد أن المشرع لم يتناول مسألة حماية الخصوصية فيما عدا نص المادة (436) و المادة (437) الخاصة بحماية حرمة المسكن، حيث أن المشرع لم يتطرق لحماية خصوصية المعلومات في هذا الباب ، إلا أنه ومن خلال البحث نجد أن المشرع قد نص في الكتاب الثاني الباب الثاني الفصل الأول ، وهو الفصل الخاص بالجرائم التي ترتكب ضد الإدارة، الجرائم التي يرتكبها الموظفون العموميون على المادة (236) الخاصة بإفشاء أسرار الوظيفة ، والمادة (244) الخاصة بالإطلاع على المراسلات وإتلافها، وبالتالي نجد أن المشرع الليبي لم يتطرق إلى خصوصية المعلومات إلا من خلال المادتين (236 و244)، وهذا يوضح أن المشرع الليبي لم يعطي القدر الكافي من الأهمية لحماية خصوصية المعلومات ، وذلك لأن الانتهاكات التي قد تقع على الخصوصية عامة وخصوصية المعلومات خاصة لا تنحصر على الصور الواردة في نصيي المادتين سالفتي الذكر.

1) ادوارد غالي الذهبي، شرح قانون العقوبات الليبي القسم الخاص، منشورات الجامعة الليبية ، الطبعة الأولى، 1971م، ص 11.

حيث نصت المادة (236) من قانون العقوبات على "يُعاقب بالحبس مدة لا تقل عن 6 أشهر كل موظف عمومي يُخل بواجبات وظيفته أو يُسئ استعمالها بأن يفشي معلومات رسمية يُلزم بقاؤها سرية أو يسهل بأي طريقة كانت الوصول إلى الإفشاء بها ...".[1]

إن إفشاء السر هو في حد ذاته من الأفعال الشائنة التي لا تحتاج إلى نية الإضرار كي تعززها ، والقانون لا يُعاقب على إفشاء السر الصارخ فحسب، بل على كل إفشاء ولو كانت تعوزه مُجرد الكياسة،[2] فهنا قد أصاب المشرع عندما عاقب على مجرد إفشاء السر دون العبرة بالباعث ، وذلك لأن رغبة الشارع هي الحفاظ على الصالح العام لا حماية صاحب السر فقط، ولا يحول دون وقوع العقوبة إلا أن يكون الإفشاء في الأحوال الاستثنائية فقط.

وقد نصت المادة (244) الخاصة بالاطلاع على المراسلات، أو إتلافها، أو إفشائها على " يُعاقب بالحبس مدة لا تقل عن ستة أشهر أو بغرامه لا تزيد عن 50 جنيهاً كل موظف عمومي تابع لمصلحة البريد والتلفون والبرق أخفى، أو أوقف، أو أخر رسالة، أو أطلع عليها، أو أفشى للغير ما حوت".[3]

وهذا النص سالف الذكر منذ صدور قانون العقوبات لم يطرأ عليه آي تعديل بشكل جوهري، وفي هذه المادة يُراد من المراسلات والمكاتيب والمُحادثات التليفونية والبرقيات وما إلى ذلك من وسائل الإرسال ، كما أن هذه الأفعال المذكورة إذا تم ارتكابها من قبل أشخاص آخرين– غير الموظفين العموميين التابعين لمصلحة البريد والتليفون والبرق – تكون العقوبات الحبس مدة لا تزيد عن ستة أشهر أو الغرامة التي لا تجاوز 20 جنيهاً وذلك بناءً على شكوى الطرف المتضرر،

1) مجموعة التشريعات الجنائية ، الجزء الأول ، العقوبات ، إدارة القانون ، 1995م ، المادة 236 ، ص67.

2) محمد مصطفى الهوني ، وسعد العسبلي ، الشامل في التعليقات على قانون العقوبات ،الجزء الأول، منشورات المؤتمر المهني العام للقضاة والنيابة العامة وإدارة القضايا ، ص 295.

3) مجموعة التشريعات الجنائية ، مرجع سابق، المادة 244 ، ص70.

فالغرض من المادة هو المحافظة علي سلامة المراسلات وضمان إيصالها إلى أربابها ولذا فهي تعاقب على فتح الخطابات، أو إفشاء التلغرافات، كما تعاقب على إخفائها [1]، سواء كان الفعل تم من موظفي البريد والتليفون والبرق، أو من الغير.

وباستعراض التشريعات الصادرة في ليبيا نجد أن قانون أمن الدولة رقم (64) لسنة 1957 نص على بعض الجرائم التي تشتمل على انتهاك خصوصية المعلومات، من ذلك جريمة إرسال التقارير لحساب جهة أجنبية والتي أفرد لها عقاباً سواء ارتكبت من قبل شخص طبيعي، أو معنوي.[2]

وأخيراً يجدر الإشارة إلي أن نصوص قانون العقوبات، وغيره من القوانين الخاصة بتنظيم بعض المهن كمهنة الطب، أو المحاماة، أو التي صدرت لتجريم الأفعال الماسة بأمن الدولة مثلاً، غير كافية للتصدي للأفعال الماسة بالخصوصية ومن ذلك خصوصية المعلومات.

كما أن محاولة تطبيق قواعد قانون العقوبات على الانتهاكات التي تقع على الخصوصية المعلوماتية، وجرائم التقنية الحديثة، من شأنها أن تجعل القاضي مجبراً على القياس في بعض الحالات، وذلك لتطبيق النصوص العقابية على بعض الجرائم التي تحصل باستعمال هذه التقنية مثل (الاحتيال عن طريق الانترنت ، أو سرقة المعلومات عن طريق الانترنت) ، وهذا يشكل مخالفة لمبدأ شرعية الجرائم والعقوبات.[3]

---

1) محمد مصطفى الهوني ، وسعد العسبلي ، مرجع سابق، ص301.

2) محمود سليمان موسى، المسئولية الجنائية للشخص المعنوي في القانونين الليبي والأجنبي، دار الجماهيرية للنشر والتوزيع، الطبعة الأولى، 1985م، ص 350 – 351.

3) ومبدأ الشرعية يعني أنه لا جريمة ولا عقوبة إلا بنص قانوني ، أي أنه حتى يعتبر الفعل غير مشروع يجب أن يكون هناك نص يحدد الشروط التي يتطلبها القانون كي يعتبر هذا الفعل غير مشروع ويحدد العقوبة المقررة له ، ويطلق على هذا النص نص التجريم وهنا يشمل قانون العقوبات والقوانين المكملة له والقوانين العقابية والخالصة ، وبالتالي هنا القاضي لا يستطيع أن يعتبر فعلاً معينا جريمة إلا إذا وجد نصاً يجرم هذا الفعل ، ونظراً لأهمية هذا المبدأ لا يوجد قانون عقوبات في الوقت الراهن يخلو من هذا المبدأ ، كما أن جميع المؤلفات

الفرع الثاني: حماية خصوصية المعلومات في القانون رقم (22) لسنة 2010 بشأن الاتصالات.

لعل القانون رقم (22) لسنة 1378 و.ر (2010 مسيحي) بشأن الاتصالات من أهم القوانين التي توفر الحماية لخصوصية المعلومات في ليبيا ، فهذا القانون احتوى على 41 مادة، كانت قد صدرت بمناسبة تنظيم العمل في قطاع الاتصالات، إلا انهُ كان يتضمن نصوصاً من شأنها حماية الخصوصية في هذا المجال.

فقد نص المشرع في المادة (14) من القانون على مراقبة المشغلين ومزودي الخدمات، وألزم الجهات المختصة بالتحقق من التزام مزودي الخدمات والمشغلين بما هو وارد في التراخيص، وأحكام التشريعات ذات العلاقة فيما يتعلق بالكشف على مواقع الشبكات والتأكد من حسن إدارة، المشغل أو المزود، وكذلك التأكد من سلامة الأنظمة المتبعة لإصدار قوائم الحساب ودقتها.

كما جاءت المادة (15) لتنص على سرية الاتصالات، وتحث الجهات التي تقدم الخدمات أن تتخذ ما من شأنه ضمان سرية اتصالات المستفيدين ، كما نص على أنه لا يجوز اعتراض، أو مراقبة، أو تغيير، أو تعديل اتصالات المستفيدين من الخدمة، إلا أن المشرع نص على استثناءات فيما يتعلق بهذا النص وهي كالآتي:

أ. يجوز للمستفيد أن يطلب من الجهة التي تقدم الخدمات مراقبة المكالمات المتعلقة بهاتفه.

ب. يجوز للجهة القضائية المختصة قانوناً إصدار تعليماتها إلى الجهة التي تقدم الخدمات باعتراض أو مراقبة المكالمات الواردة إلى هاتف الفرد أو الصادر منه وعليها التقيد بتلك

الفقهية تشير إليه وتتناوله بالشرح والتفصيل انظر في ذلك :عبدالعزيز عامر ، شرح الأحكام العامة للجريمة في القانون الجنائي الليبي ، جامعة قاريونس ، بنغازي ، الطبعة الثانية ، 1987 ، ص 115، احمد فتحي سرور ، الوسيط في قانون العقوبات ، دار النهضة العربية ، القاهرة ، مصر ، 1996، ص29 –30 ، محمد رمضان بارة ، شرح القانون الجنائي الليبي الأحكام العامة الجريمة والجزاء ،الجزء الأول، مطابع عصر الجماهير، الطبعة الثالثة ، 2000م ، ص24 إلى 35، موسى مسعود ارحومة ، الأحكام العامة لقانون العقوبات النظرية العامة للجريمة ، الجزء الأول ، منشورات جامعة قاريونس، الطبعة الأولى ، 2009م ، ص35.

التعليمات أو التوجيهات ، وعلى الجهة التي تقدم الخدمات تزويد هذه الجهات القضائية بالمعلومات المستمدة من مراقبتها لهاتف الفرد ، بما في ذلك أرقام الهواتف التي يتم الاتصال بها وتواريخ حدوثها.

ج. للجهة المختصة اتخاذ أي إجراء لحماية الأشخاص من المكالمات المضايقة أو المكالمات العدائية، أو غير القانونية ، وإحالة الأمر إلى الجهات المختصة لاتخاذ الإجراءات اللازمة. [1]

وجاءت المادة رقم (16) باسم حماية المعلومات الشخصية وفيها ينص المشرع " تكون الجهة التي تقدم الخدمات مسئولة عن المعلومات المتعلقة بالمستفيد التي تكون بحوزتها أو بحوزة وكلائها، ويجب عليها حماية معلومات اتصالات المستفيدين بوسائل الحماية الأمنية، ومراعاة الخصوصية ، ولا يجوز لها جمع، أو استعمال، أو حفظ، أو إفشاء معلومات أو اتصالات المستفيد لأي غرض كان إلا في الحدود المسموح بها قانوناً، أو بموافقته الشخصية وفي الأغراض التي تمت من أجلها".[2] وكما هو واضح من النص أن الجهة المختصة يكون لها حق حفظ أو إظهار معلومات العميل في نطاق يرسمه لها القانون، أو بالموافقة الشخصية للعميل، أو لأغراض تم جمع البيانات والمعلومات من أجلها.

حيث يقابل نص هذه المادة في القانون البحريني رقم (28) لعام 2002م بشأن المعاملات الالكترونية نص المادة (24) ، وكذلك نص المادة (31) من قانون إمارة دبي رقم (2) لعام 2002م بشأن المعاملات والتجارة الالكترونية، إلا أن ما يميز هذه المادة أنها تختلف عن سابقتها بأنها غير مقتصرة في التطبيق على المعاملات التجارية فقط.

---

1) قانون رقم (22) لعام 2010م بشأن الاتصالات ، اللجنة الشعبية العامة للعدل ، موسوعة التشريعات الليبية ، الإصدار الأول.
2) قانون رقم (22) لعام 2010م بشأن الاتصالات ، مرجع السابق.

وهنا نلاحظ أن الحماية التي وفرها المشرع الليبي من خلال هذا النص لا تقل عن الحماية المتوفرة في الدول المتقدمة ، ومن هذه الدول ما سبق الإشارة له في السابق كالقانون الفرنسي، والقانون الأمريكي ، وإن كان هذان الأخيران يملكان الأفضلية لتوافر العوامل التي من شأنها وضع هذه النصوص موضع التنفيذ وذلك لتوفر التكنولوجيا الحديثة والكوادر المدربة.

كما ورد في قانون الاتصالات رقم (22) لسنة 2010م نص المادة (26) الخاص بإفشاء الأسرار، والتي تنص على أنه " يُعاقب بالحبس مدة لا تزيد على ثلاثة أشهر وبغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة ألاف دينار كل من أذاع، أو نشر، أو أشاع دون حق مضمون رسالة، أو اتصالاً أو جزءاً منه أطلع عليه بحكم عمله، أو أساء استعمال معلومات تتعلق بالمستفيدين".[1]

والمشرع نص في هذا القانون أيضاً على إساءة استخدام شبكة المعلومات الدولية (الانترنت) وجاء ذلك في نص المادة (35) على إنه " .. كل من أساء استخدام شبكة المعلومات الدولية في نشر معلومات، أو بيانات تمس الأمن السياسي، أو الاقتصادي أو الاجتماعي، أو الموروث الثقافي للمجتمع العربي الليبي، أو استخدام الفيروسات، أو أي طرق أخرى لإيذاء الغير"[2] ، هنا عبارة أي طرق لإيذاء الغير جاءت لردع أي تصرف من شأنه المساس بالغير، بما في ذلك المساس بخصوصياتهم على شبكة المعلومات الدولية، وأكدت المادة (36) على هذا المفهوم وذلك بالنص على أنه " مع عدم الإخلال بأحكام المادة (35) من هذا القانون ، يعاقب بغرامة لا تقل عن مائة دينار، ولا تزيد على خمسمائة دينار كل من أساء استخدام

1) المرجع السابق.

2) قانون رقم (22) لعام 2010م بشأن الاتصالات ، مرجع سابق.

وسائل الاتصال للإضرار بالغير"،[1]كما أن المشرع لم يغفل النص على عقوبة الشخص الاعتباري في هذا القانون، وكان ذلك من خلال نص المادة (34) والتي تنص على " يعاقب الممثل القانوني للشخص الاعتباري بنفس العقوبات المقررة للجرائم في هذا القانون إذا ثبت علمه بها، ويسأل الشخص المعنوي عن الوفاء بما يحكم به من عقوبات مالية وتعويضات مع حقه في الرجوع على من تسبب في ذلك".

وهنا يظهر لنا أن المشرع الليبي لا يجاري تطورات، ومستجدات العصر، وما تشكله هذه المستجدات من تأثير على حياة الفرد، لاسيما في مجال الخصوصية المعلوماتية ، إلا أنه – وكما يُقال – أن تأتي متأخراً خير من ألا تأتي أبداً ، فنجد في قانون الاتصالات رقم (22) لسنة 2010م بادرة خير في هذا المجال (حماية الخصوصية المعلوماتية) وإن كان هذا الجهد غير كافٍ لوحده ؛ فيجب أن يتخذ المشرع الليبي كل ما يلزم سواء بسن تشريعات خاصة ووضع الإجراءات اللازمة لحماية الخصوصية المعلوماتية ، وذلك لما لهذه الأخيرة من أهمية نتيجة الاستعمال المتزايد لوسائل الاتصال الحديثة وتداخلها في حياتنا اليومية.

1) المرجع السابق.

الخـــاتمة

لقد تناولنا في هذا البحث من خلال تقسيمه إلى فصل تمهيدي وفصلين مستقلين، ماهية الخصوصية المعلوماتية، وذلك من خلال بيان تعريفها فقهاً، و اصطلاحاً، ونشأتها وتطورها، وكذلك بيان نطاقها، والمخاطر التي تهددها ، ثم عرضنا في الفصل الأول الحماية التي تتمتع بها الخصوصية المعلوماتية على النطاق الدولي ، من خلال بيان جهود المنظمات الدولية والإقليمية في حماية الخصوصية بشكل عام، والخصوصية المعلوماتية بشكل خاص ، أما في الفصل الثاني فقد تم تخصيصه لدراسة مدى الحماية الموفرة للخصوصية المعلوماتية على النطاق الداخلي، من خلال دراسة تشريعات دول أجنبية كالتشريع الفرنسي، والأمريكي، وأخيراً عرضنا للحماية المتوفرة في بعض القوانين العربية (البحريني – الإماراتي) بالإضافة للقانون الليبي.

نخلص مما سبق إلى أن الثورة التكنولوجية، وتقنية الاتصالات الحديثة ، وما سببته من تغيير في الموازين القانونية، والاجتماعية، والاقتصادية ، جعلت لزاماً علينا أن نواجه هذه الظاهرة بالتحليل والدراسة لفهم عناصرها، ومدى تأثيرها في الحياة الإنسانية ؛ ليتسنى لنا التعامل معها والسيطرة عليها.

كما استخلصنا أيضاً ، مدى تأثير تكنولوجيا المعلومات على الخصوصية، الأمر الذي أدى إلى تغيير في مفهوم الخصوصية الذي توصلت إليه التشريعات الأوروبية منذ القرن التاسع عشر ، فظهر نوع آخر من الخصوصية ألا وهو الخصوصية المعلوماتية ، بالتالي كان من الواجب عدم تبسيط ذلك بمحاولة إدراج حماية هذا النوع من الخصوصية ضمن الأسس والمبادئ

القانونية التقليدية في الدساتير والقوانين العقابية ، بل من الواجب البحث عما يلائم طبيعتها من مبادئ قانونية، وما يفي بحاجتها من حماية بعد وضع المعادلة الصحيحة التي تنطبق عليها من حيث الموازنة بين الاحتفاظ بحق الدولة في حفظ الأمن والاستقرار، ومصالح الأفراد المتمثلة في المحافظة على خصوصياتهم.

كما لا يعني ذلك الاكتفاء بسن القوانين لحماية الخصوصية المعلوماتية فقط ؛ بل يجب الاستمرارية في العمل لحماية هذا الحق، من خلال وضع الخطط ورسم الإستراتجيات التي تكفل ذلك ، وهذا يرجع لما تتسم به الاعتداءات الواقعة على الخصوصية المعلوماتية من صفة التجدد.

ومن خلال دراستنا لهذا الموضوع فقد خلصنا لعدة توصيات نلخصها في الأتي :

1. عقد المؤتمرات المحلية والإقليمية لتناول سُبل حماية الخصوصية المعلوماتية وكذلك لمناقشة تأثير التكنولوجيا على الخصوصية وأبعادها.
2. ضمان أن يكون نقل البيانات، وجمعها واستخدامها محكوماً باتفاقيات تكفل حمايتها.
3. ضرورة التعاون الدولي في مكافحة الاعتداءات على الخصوصية، وذلك بتأهيل مأموري الضبط القضائي في التعامل مع هذا النوع من الجرائم أسوة بدول الاتحاد الأوروبي، حيث تم إنشاء قسم متخصص بمكافحة الجرائم التي تقع عن طريق شبكة المعلومات الدولية ، وكذلك تفعيل المعاهدات الدولية المبرمة في هذا المجال ، ومبدأ المساعدة القانونية والقضائية.
4. سن تشريعات خاصة بحماية الخصوصية، لاسيما الخصوصية المعلوماتية، وكذلك النص صراحة على تجريم كل الأفعال التي من شأنها انتهاك الخصوصية في المجال المعلوماتي

، وتحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس عبر شبكة المعلومات العالمية وأجهزة الحاسوب.

5. نحث مشرعنا على الاستفادة من التجربة الفرنسية من خلال قانون حماية البيانات الاسمية في وضع قانون يعطي الحق للأفراد في الاطلاع على بياناتهم ، وكذلك الحق في تعديلها، أو إلغائها، أو حذفها في حالة عدم صحتها.
6. إيجاد السبل التي يمكن من خلالها مراقبة الشبكة المعلوماتية، ووسائل الاتصالات لحماية أمن الدولة ، بشرط ألا يشكل ذلك اعتداء على الحق في الخصوصية.
7. توعية المواطنين بمخاطر التعامل مع شبكات المعلومات ، وما قد يقع عليهم من انتهاكات نتيجة التعامل مع المواقع المشبوهة أو السيئة.
8. تنظيم استخدام شبكة المعلومات من قبل القصر وعدم حصر الاهتمام بهم في هذا المجال على كونهم ضحايا فقط، وسن قوانين خاصة باستخدام القصر لها، كما فعل المشرع الأمريكي.

ثبت المراجـــع

القران الكريم

أ-الكتب العامة

1. ابن منظور ، لسان العربي ، الجزء الثامن ، الطبعة الأولى ، منشورات مطبعة بولاق ، القاهرة ، ص290.
2. إبراهيم علي بدوي الشيخ ، الميثاق العربي لحقوق الإنسان دراسة في خلفيته ومضمونه وآثره على الأمن القومي العربي والنظم السياسية في الوطن العربي ، دار النهضة العربية ، 2004م.
3. احمد ابوالوفا ، الوسيط في القانون الدولي العام ، دار النهضة العربية ، القاهرة ، مصر ،الطبعة السادسة، 2016م.
4. احمد فتحي سرور ، الوسيط في قانون العقوبات ، دار النهضة العربية ، القاهرة ، مصر ، 1996.
5. ادوارد غالي الذهبي ، شرح قانون العقوبات الليبي القسم الخاص ، منشورات الجامعة الليبية ، الطبعة الأولى ، 1971.
6. السيد عبد الوهاب عرفه ، الوجيز في مسئولية الطبيب والصيدلي ، دار المطبوعات الجامعية ، الإسكندرية، 2005م.
7. جابر فهمي عمران ، منظمة التجارة العالمية ، دار الجامعة الجديدة ، الإسكندرية ، مصر ، 2016م.

8. عبدالعزيز عامر ، شرح الأحكام العامة للجريمة في القانون الجنائي الليبي ، الطبعة الثانية، جامعة قاريونس ، بنغازي ، 1987م

9. عبدالعزيز محمد سرحان ، الاتفاقية الأوروبية لحماية حقوق الإنسان ، دار النهضة العربية.

10. محمد الأزهر ، حقوق المؤلف في القانون المغربي ، دراسة مقارنة في الملكية الأدبية الفنية ، دار النشر المغربية ، 1994م.

11. محمد أنس جعفر،احمد محمد رفعت ، حقوق الإنسان ، مركز جامعة القاهرة للتعليم المفتوح ، 1991م.

12. محمد رمضان بارة ، شرح القانون الجنائي الليبي الأحكام العامة الجريمة والجزاء ،الجزء الأول، مطابع عصر الجماهير، الطبعة الثالثة ، 2000م.

13. محمد مصطفى الهوني ، وسعد العسبلي ، الشامل في التعليقات على قانون العقوبات، الجزء الأول ، منشورات المؤتمر المهني العام للقضاء والنيابة العامة وإدارة القضاء.

14. محمود سليمان موسى ، المسئولية الجنائية للشخص المعنوي في القانونين الليبي والأجنبي ، الطبعة الأولى، دار الجماهيرية للنشر والتوزيع ، 1985م.

15. موسى مسعود ارحومة ، الأحكام العامة لقانون العقوبات النظرية العامة للجريمة ، الجزء الأول ، منشورات جامعة قاريونس، الطبعة الأولى ، 2009م .

ب-الكتب المتخصصة

1. أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، الطبعة الثالثة ، دار النهضة ، القاهرة ،1994م.
2. أيمن عبدالحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، د.ن ، د.ط ، 2005م.
3. أيمن عبدالحفيظ ، إستراتجية مكافحة جرائم استخدام الحاسب الآلي ، د ن ، د ط ، د ت.
4. أيمن عبدالله فكري ، جرائم النظم والمعلومات ، دار الجامعة الجديدة ، الإسكندرية ، 2007م.
5. حسام الدين كامل الأهواني ، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دارسة مقارنة، دار النهضة العربية 1978م.
6. حسن الجندي ، ضمانات حرمة الحياة الخاصة في الإسلام ، الطبعة الأولى، دار النهضة العربية ، القاهرة، 1993م.
7. دويب حسين صابر، النظام القانوني لحرية الحصول على المعلومات ، دار النهضة العربية ، القاهرة ، مصر، 2014م.
8. شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، دار الفكر والقانون ، المنصورة ، مصر ، الطبعة الأولى . 2015م.
9. صالح جواد كاظم ، التكنولوجيا الحديثة والسرية الشخصية مباحث في القانون الدولي، الطبعة الأولى ، دار الشؤون الثقافية العامة ، بغداد 1991م.
10. عادل عبدالعال ابراهيم خراشي ، الحماية الجنائية للحق في الخصوصية ، شركة ناس ، القاهرة مصر ، الطبعة الأولى ، 2015م.

11.عبدالإله النوايسة ، جرائم تكنولوجيا المعلومات ، دار وائل للنشر والتوزيع ، عمان ، الأردن ، الطبعة الآولى ، 2017م.

12.عبدالفتاح بيومي حجازي ، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية ، القاهرة ، مصر ،2011م.

13.: عبدالفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، منشأة المعارف ، الإسكندرية مصر ، الطبعة الأولى ، 2009م .

14.عبداللطيف الهميم ، في دراسة عميقة ومتزنة .. احترام الحياة الخاصة بين الشريعة الإسلامية والقانون ، دار عمار ، عمان ، الأردن ، الطبعة الأولى ، 2004م.

15. عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، منشأة المعارف ، الإسكندرية مصر ، د ط ، د ت .

16.علاء عبدالباسط خلاف ، الحماية الجنائية لوسائل الاتصال الحديثة ، دار النهضة العربية، 2002م.

17.عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، المنصورة مصر ، الطبعة الثانية ، 1995.

18.عمر محمد بن يونس ، الاتفاقية الأوروبية حول الجريمة الافتراضية ، مؤسسة أدم للنشر والتوزيع ، مالطا ، الطبعة الثانية ، 2005م .

19.غنام محمد غنام ، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت ، دار الفكر والقانون ، المنصورة ، مصر ، الطبعة الأولى ، 2016م.

20.: فتحي محمد أنور عزت ، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي ، دار النهضة العربية ، القاهرة ، مصر ، الطبعة الثانية ، 2010م.

21.فريده كيت ، الخصوصية في عصر المعلومات ، ترجمة محمد محمود شهاب ، الطبعة الأولى، 1999 ، مركز الأهرام للترجمة والنشر.

22.محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت والجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2011م.

23. محمد حسين منصور ، المسئولية الالكترونية ، دار الجامعة الجديدة للنشر ، الإسكندرية.

24. محمد حسام محمود لطفي ، الحجية القانونية لبرامج الحاسب الآلي ، دارالثقافة العربية، القاهرة ، الطبعة الأولى ، 1987م.

25.محمد حسام محمود لطفي ، بنوك المعلومات وحقوق المؤلف ، دار النهضة العربية ، القاهرة 1996م.

26. محمد حسام محمود لطفي ، الإطار القانوني للمعاملات الالكترونية ، دار النهضة العربية ، القاهرة ، 2002م.

27.محمد رشاد القطعاني ، الحماية الجنائية للحق في حرمة الاتصالات الشخصية ، دار الفتح ، الإسكندرية ، مصر، الطبعة الثانية ، 2014م.

28.محمد كامل محمود الدسوقي ، الحماية الجنائية لسرية المعلومات الإلكترونية ، دار الفكر والقانون ، المنصورة ، مصر ، الطبعة الأولى ، 2015م.

29.محمود ابراهيم غازي ، الحماية الجنائية للخصوصية والتجارة الإلكترونية ، مكتبة الوفاء القانونية ،الإسكندرية ، مصر، الطبعة الأولى ، 2014م .

30.محمود احمد طه ، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت ، دار الفكر والقانون ، المنصورة مصر ، 2016م.

31.مدحت رمضان ، جرائم الاعتداء على الأشخاص والانترنت ، دار النهضة العربية ، القاهرة.

32. مدحت عبدالحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية، القاهرة ، 2001م.

33.ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع، عمان الأردن ، 1996م.

34.هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، الطبعة الأولى ، مكتبة الآلات الحدية ، أسيوط ، مصر ، 1992م.

35.هلال بن محمد بن حارب البوسعيدي ، الحماية القانونية والفنية لقواعد المعلومات المحوسبة ، دار النهضة العربية ، القاهرة ، مصر ، 2009 .

الرسائل والأطروحات العلمية

1. إبراهيم بن سليمان بن عبدالله الشايع ، حق الخصوصية في الفقه الإسلامي ، رسالة ماجستير مقدمة لجامعة الإمام محمد بن سعود الإسلامية ، 1427 هـ .

2. عبدالرحمن جميل محمود حسين ، الحماية القانونية لبرامج الحاسب الآلي ، رسالة ماجستير مقدمة لكلية الدراسات العليا جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2008م.

3. على محمد قاسم الطلي ، جريمة التزوير في المحررات الرسمية في القانون اليمني ، رسالة ماجستير مقدمة لكلية الحقوق جامعة عدن ، اليمن ، 2006م .

4. صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، الجزائر ، 2013م ص129 .
5. محمد حلمي محمد رمضان ، الحماية الجنائية للمحادثات الهاتفية، رسالة ماجستير مقدمة لكلية الحقوق ، جامعة الإسكندرية ، 2008م.
6. محمد رشاد إبراهيم مفتاح ، الحماية الجنائية للحق في حرمة الاتصالات ، رسالة دكتوراه مقدمة لكلية الحقوق ، جامعة الإسكندرية ، 2009م.

الأبحاث والمقالات العلمية

1. احمد فتحي سرور ، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، ع54 س26 ، يونيو 1984م.
2. أسامة بن غانم العبيدي ، الجهود الدولية لمكافحة الجرائم المعلوماتية ، بحث منشور بمجلة الحقوق ، جامعة الكويت ، مجلس النشر العلمي ، العدد4 السنة 39 ، 2015م،
3. خالد الشرقاوي السموني ، مكافحة جرائم الكمبيوتر على ضوء التشريعين الوطني والدولي ، بحث مقدم لجامعة محمد الخامس ، المغرب.
4. راشد بن حمد البلوشي ، الدليل في الجريمة المعلوماتية ، بحث منشور في مجلة الحقوق، كلية الحقوق جامعة الإسكندرية ، مصر ، العدد الأول ، 2008م
5. سامح عبدالواحد التهامي ، الحماية القانونية للبيانات الشخصية ، بحث منشور بمجلة الحقوق جامعة الكويت ، مجلس النشر العلمي ، العدد 3 السنة 35 ، 2011م.
6. سوزان عدنان ، انتهاك حرمة الحياة الخاصة عبر الانترنت ، رسالة دكتوراه مقدمة لكلية الحقوق جامعة دمشق ، منشورة بمجلة دمشق للعلوم الاقتصادية والقانونية، المجلد 29 ، العدد 3 ، 2013م.

7. طارق الجملي ، الدليل الرقمي في مجال الإثبات الجنائي ، بحث منشور في مجلة الحقوق ، كلية الحقوق ، جامعة البحرين ، البحرين ، المجلد 12 ، العدد الأول.
8. منى تركي الموسوي ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، جامعة بغداد ، مجلة كلية بغداد للعلوم الاقتصادية ، العدد الخاص بمؤتمر الكلية 2013م.
9. محروس نصار غايب ، الجريمة المعلوماتية ، مجلة التقني ، العراق ، العدد 24 السنة التاسعة، 2011م.
10. نوفل على عبدالله الصفو ، بحث بعنوان: جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات ، المجلة المصرية للدراسات القانونية والاقتصادية ، مصر ، العدد الثالث ، يناير 2015م.

الوثائق

1. أعمال الأمم المتحدة في ميدان حقوق الإنسان ، المجلد الأول ، منشورات هيئة الأمم المتحدة ، نيويورك 1990م.

التشريعات

1. دستور المملكة الليبية لعام 1951م .
2. مجموعة التشريعات الجنائية ، الجزء الأول ، النصوص العقابية ، إدارة القانون، 1995م .
3. الجريدة الرسمية ، العدد 28 ، 1986م قانون المسؤولية الطبية الليبي رقم (17) لسنة 1986.
4. قانون رقم (4) لعام 1990م بشأن النظام الوطني للمعلومات والتوثيق.
5. قانون رقم (20) لعام 1991م بشأن تعزيز الحرية (وثيقة دستورية).
6. قانون الاتصالات الليبي رقم (22) لعام 2010م.
7. قانون المعالجة الآلية للمعطيات ، ملفات المعطيات والحريات الفردية رقم 17-7 تاريخ 1978/1/1م.
8. الدستور الجزائري.
9. الدستور المصري لعام 2012م المعدل عام 2014م.
10. الدستور الموريتاني لعام 1991م .
11. قانون العقوبات البحريني
12. قانون التجارة الالكترونية البحريني سبتمبر 2002م.
13. قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم (2) لعام 2002.
14. قانون مكافحة جرائم تقنية المعلومات الإمارتي رقم (2) لعام 2006م.

15.قانون المعاملات الالكترونية التونسي (83) لعام 2000م المعدل عام 2001م.

16.قانون المعاملات الالكترونية المصري رقم (15) لعام 2004م.

17. قانون المعاملات الالكترونية السوداني لعام 2007م.

18. قانون المعاملات الالكترونية العُماني (96) لعام 2008م.

19. قانون المعاملات الالكترونية للسلطة الوطنية الفلسيطنية لعام 2010م.

20. قانون المعاملات والتجارة الالكترونية القطري لعام 2010م.

المؤتمرات العلمية

1. حسين بن سعيد الغافري ، الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الالكترونية ، ورقة عمل مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الانترنت ، القاهرة ، 2– 4 يونيو 2008م.

2. سامي الشوا ، الغش المعلوماتي كظاهرة إجرامية مستحدثة ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 1993م.

3. رحاب عميش ، تحديات الجريمة المعلوماتية ، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون ، طرابلس ، ليبيا ، في الفترة من 28 إلى29 أكتوبر 2009م.

4. عبدالرؤوف مهدي ، الجوانب الإجرائية لحماية الحق في الحياة الخاصة ، بحث مقدم إلى مؤتمر الحق في الحياة الخاصة بكلية الحقوق ، جامعة الإسكندرية . بتاريخ 4 إلى 6 يونيو 1987.

5. محمد حمد أبوسن ، الجرائم الالكترونية وأدلة إثباتها بين الواقع الماثل والمثال المأمول ، ورقة عمل مقدمة للمؤتمر الثالث لرؤساء المحاكم العليا ، الخرطوم ، السودان ، 23 إلى 25 سبتمبر 2012م.
6. موسى مسعود ارحومة ، السياسة الجنائية في مواجهة الانترنت ، بحث مُقدم إلى المؤتمر الدولي لجامعة الطفيلة التقنية ، الأردن ، 2007م.
7. موسى مسعود ارحومة ، بحث بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، تحت تنظيم أكاديمية الدراسات العليا طرابلس ، ليبيا ، في الفترة من 28 إلى 29 أكتوبر 2009م.
8. يونس عرب ، الاتجاهات التشريعية للجرائم الالكترونية ، ورقة مقدمة لورشة عمل تطوير التشريعات في مجال جرائم مكافحة الجرائم الالكترونية ، عمان ، الأردن ، من 2 إلى 4 ابريل 2006م.

مراجع باللغة الأجنبية

Specialized books:

1. Rule J.B, Private Lives and Public Surveillance, Social control in the computer Age, New York Schocken Books, 1974ad.
2. John H. F. Shattuch, Right of Privacy, National Textbook Co, 1977ad.
3. Miller A, The Assault on Privacy, Ann Arbor, University of Michigan Press 1971ad
4. Westin A.F, Privacy and Freedom, New York, Athenaeum press 1967ad.

Articles:

1. Jerry Berman & Deirdre Mulligan, privacy in the Digital Age :Work in Progress, Nova law Review, The internet and law, Volume 23, November 2 winter 1999.

Legislation:

1. The electronic communications privacy act US code(ECPA) (18US Code – sec 2702).
2. The omnibus crime control and safe streets act of 1968 (18 US Code sea 2510 – 2521).

Research:

1. Ulrich Sieber, legal Aspects of Computer –Related Crime in The Information Society-Com Crime Study Prepared For The European commission version 1.0 Of 1st January 1998ad.
2. Michael I. Privacy Human Rights an International Comparative Study with Special Reference to Developments in Information Technology, Dartmouth Publishing Company , 1994ad.

شبكة المعلومات الدولية

1. أمنار ابراهيم ، الحماية الجنائية للمعطيات ذات الطابع الشخصي على ضوء القانون المغربي والقانون المقارن ، رسالة ماجستير منشورة في مجلة القانون والأعمال، 2008م ، منشور على الموقع المجلة: http://www.droitententtreprise.org
2. حسين بن سعيد الغافري ، الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الالكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2 إلى 4 يونيو 2008 منشور على الموقع التالي:

http://www.arab-afli.org

3. عادل عامر ، بحث بعنوان مفهوم الحق في الحياة الخاصة للأفراد ، منشور على الموقع التالي: http://www.al-safsaf.com .

4. عائض المري ، أمن المعلومات وماهيتها وعناصرها وإستراتجيتها ، بحث منشور علة الموقع التالي:http://www.draalmarri.com

5. عائض المري ، بحث بعنوان الخصوصية وحماية البيانات منشور بالموقع التالي: http://www.dralmarri.com تاريخ الزيارة 2015/02/04م.

6. يونس عرب ، الخصوصية وحماية البيانات في العصر الرقمي ، بحث منشور على الموقع التالي http://www.omanlegal.net .

7. انظر بحث بعنوان دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي منشور بالموقع التالي: http://www.startimes.com

8. بحث بعنوان مفهوم الحق في الحياة الخاصة للأفراد منشور على الموقع التالي: http://www.mudwen.com

9. الاتحاد الأفريقي اتفاقية بشأن الأمن السيبراني وحماية البيانات، مقال منشور حول هذا الموضوع على الموقع التالي:http://www.moehaner.net

10. تقرير مفصل حول قرصنة الانترنت بعنوان ، القرصنة الالكترونية سلاح العصر الرقمي، على الموقع التالي: http://www.algazeera.net

11. شروط حماية الخصوصية على مواقع الانترنت: http://www.microsoft.com http://www.etisalat.co.ae http://wwwgoogle.com

12. مقال بعنوان أبو غزالة: العالم يشهد جريمة الكترونية كل ثلاث دقائق ، 25/مارس/2009م منشور على الموقع التالي:http://www.agip.com .

13. معلومات حول برامج المنظمة العالمية للتجارة في مجال التجارة وموضوعات الملكية الفكرية راجع موقع المنظمة التالي: http://www.wtoarab.org

14. نصوص الاتفاقية الأوروبية لحقوق الإنسان على الموقع التالي:

http://www.gypsy-triveller.org

15. لمعلومات حول الاتفاقية الأوروبية لعام1981م بشأن (حماية الأشخاص من مخاطر المُعالجة الآلية للبيانات) والاتفاقية الأوروبية لعام 2001م (اتفاقية بودابست) وغيرها من الاتفاقيات التي تُعنى بحقوق الإنسان عامة والحق في الخصوصية خاصة راجع الموقع التالي: http://www.coe.int

16. الميثاق العربي لحقوق الإنسان على الموقع التالي: http://www. Lasportal.org

17. حول المؤتمر العربي الدولي الأول للملكية الفكرية المنعقد في عمان 1995م: http://www.hip.jopuls.org

18. نصوص قانون العقوبات الفرنسي الجديد على الموقع التالي:

http://www.legifrance.gouv.fr

19. حول اعتراف المحكمة العليا الفدرالية الأمريكية بالحق في الخصوصية على موقع جريدة فرجينيا للقانون والتقنية على شبكة الانترنت: http://www.vjolt.net .

20. مقال منشور على صفحة المركز الوطني لحقوق الإنسان ، بعنوان قانون جرائم أنظمة المعلومات والحق في الحياة الخاصة ، منشور على الموقع التالي: http://www.nchr.org

21. موقع متخصص لمختلف التشريعات العربية: دساتير (موريتانيا ، المملكة الليبية ، الجزائر، مصر) قانون التجارة الالكترونية البحريني سبتمبر 2002م، قانون المعاملات الإلكترونية وحماية الخصوصية الأردني رقم (58) لعام 2001م، قانون المعالجة الآلية للمعطيات ،

ملفات المعطيات والحريات الفردية رقم 17-7 تاريخ 1978/1/1م.

http://www.arablaw.org

22. المبادرات لإصدار المسودة الأولى لقانون المعاملات الالكترونية الليبي مع منظمة الإسكو التابعة للأمم المتحدة وذلك بتاريخ 2014/03/24م انظر في ذلك الموقع التالي:http://www.ltnet.ly

23. http://www.kenanaonline.com تاريخ الزيارة 2015/05/14م.

24. حكم للمحكمة العليا الفيدرالية الأمريكية (Katz C.U.S, 389 U.S. Supp 347, 1967ad) منشور على الموقع التالي: http://www.supreme.justia.com

انظر كذلك على هذا الموقع تعريف القضاء الأمريكي للخصوصية. Right to Privacy not Guaranteed by Constitution http://www.Theonion.com

25. : حول اقرار السويد لقانون حرية الصحافة انظر الموقع التالي:

http://www.loc.govllaw/law/help/onllne-privacy-law/Sweden.php

26. موقع منظمة التجارة العالمية التالي: http://www.wtoarab.org.

27. أحكام بخصوص الخصوصية المعلوماتية من القضاء الأمريكي على شبكة الانترنت: http://www.internationalprivacy.org .

28. Arizona const. Available at the official website of Arizona http://www.azleg.gov

29. Florida const, 1968ad. Available at the official website of Florida http://www.leg.state.fl.US

30. Alaska const, 1965ad. Available at the official website of Alaska http://www.itgov.alaska.gov

31. California const, 1990ad. Available at the official website of California http://www.leginfo.ca.gov

32. Illinois const, 1970ad. Available at the official website of \Illinois http://www.ilga.gov

33. Hawaii const. Available at the official website of Hawaii http://www.portalehawali.gov

34. Implementing The OECD "privacy Guidelines" In Electronic Environment: Focus The Internet, 27 may 1998 a.d P6, Published on http//www.oecd.org

35. The definition of privacy by the US supreme court Right to privacy not guaranteed by constitution. available at http://www.Juriscim.net

36. The Art on Data Processing. Details and individual liberties. No 17 . 78/1978ad. Available at http://www.cnil.fr

37. The children's online privacy protection act (COPPA) available at: http://www.fle.gov : http://www.bii-compliance.com

38. James Michael . Privacy and Human Rights (An International survey of privacy laws and practice) UNESCO 1994ad A study published on http://www.gilc.org

39. Law and Technology Sources of Literature on Data Protection and Human Rights, Adam Warren. An article published on http://www2.warwick.ac.uk

40. Richard A. Posner, The Uncertain Protection of Privacy by the Supreme court. Available at http://www.law.cornell.edu

The cable communication policy act of 1984ad (47 US code sec

41. Law and Technology Sources of Literature on Data Protection and Human Rights, Adam Warren. An article published on http://www2.warwick.ac.uk

42. http://www.usdoj.gov

43. http://www.fcdrs.com

44. http://www.unhchr.ch

45. http://www.un.org .

46. http://www.unesco.org .

47. الموقع الرسمي لوزارة العدل الليبية http://www.aladel.gov.ly

المُحتَوَيَاتْ

المواضيع	الصفحة
الآية القرآنية	أ
الإهداء	ب
شكر وتقدير.....	ت
المقدمة	1
فصل تمهيدي:	7
المبحث الأول: ماهية الخصوصية المعلوماتية	9
المطلب الأول: تعريف الخصوصية المعلوماتية	10
المطلب الثاني: نشأة خصوصية المعلومات وتطورها	15
المبحث الثاني: نطاق الخصوصية المعلوماتية والمخاطر التي تُهددها	20
المطلب الأول: نطاق الخصوصية المعلوماتية	21
المطلب الثاني: المخاطر التي تُهدد الخصوصية المعلوماتية	25
الفصل الأول: آليات الحماية الدولية للخصوصية المعلوماتية.....	35
المبحث الأول: الجهود الدولية لحماية الخصوصية المعلوماتية	37
المطلب الأول: جهود الأمم المتحدة والوكالات التابعة لها	38
المطلب الثاني: جهود منظمة التجارة العالمية ومنظمة التعاون الاقتصادي والتنمية.....	45
المبحث الثاني: الجهود الإقليمية لحماية الخصوصية المعلوماتية	50
المطلب الأول: حماية الخصوصية المعلوماتية في إطار الاتحاد الأوروبي	51
المطلب الثاني: حماية الخصوصية المعلوماتية في إطار الدول العربية	60
الفصل الثاني: آليات الحماية الوطنية للخصوصية المعلوماتية	67
المبحث الأول: حماية الخصوصية المعلوماتية في التشريعين الفرنسي والأمريكي	70
المطلب الأول: حماية الخصوصية المعلوماتية في القانون الفرنسي	71
المطلب الثاني: حماية الخصوصية المعلوماتية في القانون الأمريكي	79
المبحث الثاني: حماية الخصوصية المعلوماتية في بعض التشريعات العربية والتشريع الليبي	90
المطلب الأول: حماية الخصوصية المعلوماتية في بعض التشريعات العربية	91
المطلب الثاني: حماية الخصوصية المعلوماتية في التشريع الليبي	104
الخاتمة	114
ثبت المراجع	117