

حق الخصوصية في مواجهة الاعتداءات الإلكترونية (دراسة مقارنة)

The right to privacy in the face of cyber attacks (comparative study)

تاريخ قبول المقال للنشر: 2017/08/24

تاريخ إرسال المقال : 2017/07/02

الدهبي خدوجة / طالبة دكتوراه جامعة أحمد دراية - أدرار

الملخص :

مع التقدم العلمي والتكنولوجي المعاصر برزت أساليب إجرامية بتقنيات حديثة أثرت بشكل كبير على مسألة حماية الحقوق والحريات عبر العالم الرقمي، وزاد الاهتمام بالحقوق في حرمة الحياة الخاصة في ظل التطور المستمر لتكنولوجيا المعلومات، حيث مكنت تلك التكنولوجيا من انتهاك خصوصية الأفراد والإطلاع على أسرارهم واستغلالها بشكل غير قانوني، مما ألزم التدخل التشريعي على المستوى الدولي والداخلي للحد من هذه الاعتداءات.

الكلمات المفتاحية : العالم الرقمي ، الحق في الخصوصية ، الجريمة المعلوماتية ، البيانات الشخصية ، التجسس الإلكتروني.

Abstract:

With contemporary scientific and technological progress, criminal methods have emerged in modern technologies that have greatly influenced the protection of rights and freedoms throughout the digital world. The interest in the right to privacy has increased in the light of the continuous development of information technology. This technology has enabled the violation of individuals' privacy, Legal, which necessitated legislative intervention at the international and internal levels to curb such attacks.

key words : Digital World, The right to privacy, Information crime, Personal data, Electronic Spy.

مقدمة :

يعيش العالم اليوم عصر ثورة المعلومات، بما تعنيه من يسر وسرعة في انتقال المعلومة وأداء المعاملات الإلكترونية، وما نتج عنه بروز مظاهر العالم المعلوماتي، بحيث أضحى من لوازم الحياة الضرورية على المستوى العام والخاص، ومما لا شك فيه أن كل تطور تقني له انعكاساته على المستوى القانوني، فكل المفردات الحديثة للتكنولوجيا أضحت تثير مسألة توافق إيجابياتها مع ما تخلفه من آثار سلبية على بعض المصالح والحقوق التي تحتاج إلى الحماية الجنائية لها سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها والدور الذي تؤديه في مختلف مجالات الحياة.

وفي ظل التطور الدائم والمستمر لتكنولوجيا المعلومات ظهرت مشكلة تأثيرها في حياة الغير من خلال توسع استخدام شبكة الانترنت في أغراض مختلفة ودخول جميع فئات المجتمع إلى قائمة المستخدمين، ونقل معه النشاطات الاجتماعية والثقافية والاقتصادية والسياسية من عالم واقعي ملموس إلى بيئة افتراضية تفتقد إلى المرئية، فلقد أثبتت الدراسات تضاعف مستخدمي الانترنت من 360 مليون نسمة عام 2000 إلى ما يقارب 2.7 مليار نسمة في عام 2013 وتوسع تفاعل الأشخاص مع الشبكة وأضحى أكثر تأثيراً في حياتهم اليومية من خلال انتقال الحياة اليومية للأفراد من مجالها الحقيقي إلى فضاءات رقمية كمواقع التواصل الاجتماعي والبريد الإلكتروني وبرز ظاهرة التسوق الإلكتروني وغيرها من المجالات التي أضحت ضرورة لا اختياراً يستغنى عنه، وأصبحت تشكل نقطة تماس مع خصوصية الأفراد بشكل مباشر، مما فتح المجال أمام ظهور نوع جديد من الإجرام المعلوماتي ينصب في أحد أبرز صوره في انتهاك تلك الخصوصية واستباحة حق السرية والهدوء للحياة الخاصة للأفراد.¹

وترجع مسألة ظهور الاعتداء على الحق في الخصوصية في العالم الرقمي من خلال مساهمة التكنولوجيا في جمع البيانات الشخصية وتنظيمها ودمجها بسهولة وسرعة غير مسبوقين، كذا أن كثرة نقل وتداول البيانات في إطار الباب الواسع للمعاملات الإلكترونية قد شكلت في مجموعها تهديداً لحدود الحق في الحياة الخاصة، الأمر الذي لزم معه تسييج قنوات التعامل الإلكتروني من خلال ضمان آليات وسبل قانونية تحيط الحياة الخاصة وتحول دون عرضة الخصوصية للكشف والتشهير والاستغلال من قبل الآخرين. وهذا ما يدفعنا للتساؤل عن ماهية الاعتداءات الإلكترونية ضد الحق في الخصوصية في العالم الرقمي وجملة الآليات التشريعية المتخذة داخليا ودوليا لحماية هذا الحق؟

المبحث الأول : الإطار المفاهيمي لحق الخصوصية في العالم الرقمي

مع تزايد التقنيات الحديثة زادت المخاطر على حق الانسان في خصوصيته ، فأصبح الفرد مقيدا في تعاملاته من خلال رصد البيانات الشخصية كتقنيات المراقبة والتجسس والمساس بالمعطيات الخاصة للأفراد وهي جميعها تمثل تهديدا مباشرا على الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات، لا سيما اذا استغلت تلك المعلومات والبيانات لغايات خارجة عن إرادة وعلم أصحابها.

المطلب الأول : تعريف الحق في الخصوصية

ينعقد شبه إجماع بين الفقه والتشريع على عدم إيجاد تعريف جامع مانع للحق في الخصوصية وهذا يترجم من خلال التعدد التعريفي لهذا المفهوم في إطار النظام القانوني الواحد، ولعل هذه الصعوبة في توحيد المفهوم يرجع الى طبيعة الحق التي تكتسب صفة المرونة وعدم التحديد والضبط في إطار محدد وتختلف باختلاف المجتمعات الانسانية والحقب الزمنية عبر العصور.

أولا : الحق في الخصوصية في وجهه التقليدي

وبهذا فقد ذهب العديد من الفقه لإيجاد تعريف الحق في الخصوصية كل وفق توجهاته ومنطلقاته الفكرية على اعتبار أن المكونات المنطقية للخصوصية تتسم باضطرادها المستمر في كل حقبة زمنية فعلى سبيل المثال قد بدأت بلورة مفهوم الخصوصية سابقا في إطار المراسلات التقليدية الورقية ومن ثم بدأت الفكرة تتطور إلى حين وصولها إلى الحياة في العالم الرقمي وهنا يتشكل الفرق في جوهر مفهوم الخصوصية.

فوفقا للفقيه « EDWARD BLOUSTEIN » أن الخصوصية هي الحق في حماية الحياة الشخصية للأفراد وضمان عدم الاعتداء عليها واستقلالها²

أما وفقا للفقيه « GAVISON Ruth » فلقد بني مفهوم الحق في الخصوصية وفقا ل3 عناصر السرية والعزلة والتخفي بحيث اعتبر أنه الحق في الحماية ضد التدخل في الحياة الخاصة وشؤون عائلتهم بوسائل مادية مباشرة او عن طريق نشر المعلومات»

كما يرجع الفقيه هشام محمد فريد رستم قيام مفهوم الحق في الخصوصية بتوافر وجهين أحدهما مادي وقوامه عدم إقحام الشخص في خصوصيات الآخرين ، والثاني إعلامي مقتضاه ألا تكون الشؤون الخاصة بالفرد محلا للحق في الإعلام بالنسبة للآخرين مما يستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير.³

ثانيا : حق الخصوصية في العالم الرقمي

وهنا يسند أغلب الفقه والتشريعات فكرة الحق في الخصوصية إلى النطاق الحديث الذي تتناول فيه، والتي يتشكل مفهومها في حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين، وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها آليا، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم.⁴

وبهذا دل التعريف إلى مفهوم الاستحداث في التعاملات بين الأفراد من خلال معالجة المعلومات الخاصة بهم إلكترونيا وضمان تلك الخصوصية التي تنبع من حصر فكرة الاطلاع على البيانات الشخصية وعدم التطاول عليها من قبل الآخر.

ولقد اتجه غالبية الفقه إلى ربط ولادة مفهوم الحق في الخصوصية المعلوماتية بمخاطر تقنية المعلومات المحيطة بمسألة حماية بنوك المعلومات وعمليات المعالجة الآلية للبيانات الشخصية وبهذا فقد عرفها الفقيه الأمريكي «ويستن» «Alan Westin» في كتابه المعنون «الخصوصية والحرية» فوفقا له فإن خصوصية المعلومات تعني حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين.

في حين جاء تعريف الفقيه ميلر في كتابه «الاعتداء على الخصوصية» أكثر عمقا إذ عرفها بأنها قدرة الأفراد على التحكم في سرية المعلومات المتعلقة بهم.⁵

وبهذا فقد نجد أن الحق في خصوصية المعلومات الشخصية يتوقف على فكرة الاعتداء عليها إلكترونيا من قبل الآخر، واستخدامها وفقا لأغراض خارجة عن القانون بدون علم أو إرادة صاحبها.

وبالارتكاز على منحي الخصوصية في وجهها المستحدث نجد التعريف الصادر عن مركز دراسات البيانات المجتمعية والذي أرجع الحق في الخصوصية إلى إمكانية الفرد بالتصرف بشكل قانوني دونما وجود عائق يحول هذا التصرف⁶، وبهذا فإن المعنى العميق لمفهوم الخصوصية يتجلى في تبني تلك الرخصة في حرية التصرف وضمان عم التدخل أو التطفل من الغير تحت أي ظرف وهنا نستشف تلك الإضافة التي جاء بها هذا التعريف من خلال تسييج الخصوصية ضد أي خروق تصدر من الأفراد أو حتى من الدولة في إطار ما يعرف بالمراقبة الإلكترونية.⁷

ثالثا : المفهوم التشريعي للحق في الخصوصية

بداية إن مفهوم الخصوصية قد بني في مختلف التشريعات المقارنة تحت إطار ضمان الحد الأدنى في حق الفرد بعدم التدخل أو المساس بالحياة الشخصية أو الأسرية أو خرق لسرية المعاملات او الحقائق التي تحيط بحياته، وأما الدستور الجزائري قد قرر هذا الحق من خلال نص المادة 39 التي تنص على: « لا يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحميها

القانون».

سرية المراسلات والاتصالات بكل أشكالها مضمونة»

أما عن نص المادة 39 فلقد كان النص واضحاً مباشراً في تكريس الحماية لحق الخصوصية أما عن نص المادة 40 فقد كانت الإشارة ضمنية تكفل خصوصية الأفراد بعدم خرق حقهم في أن يكونوا آمنين على أنفسهم ضد أي تعسف في التفتيش أو الاحتجاز أو اقتحام المساكن غير مبني على أسس قانونية وهو مظهر من مظاهر الحماية للحياة الخاصة.

وهو نفس الموقف الذي تبناه المشرع الإماراتي من خلال الباب الثالث في المواد 25-44 من الدستور الاتحادي.

المطلب الثاني: مبررات ونطاق حماية حق الخصوصية في المجال الإلكتروني

الفرع الأول: مبررات حماية الحق في الخصوصية

مع تزايد التقنيات الحديثة زادت المخاطر على الحق في الحياة الخاصة وأضحى الفرد مقيداً في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة الوسائل المعلوماتية كتقنيات المراقبة أو التجسس والمساس بالمعطيات الخاصة بالأفراد وهي جميعها تمثل تهديداً مباشراً على الحياة الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات لا سيما إذا استغلت لغايات خارجة عن إرادة صاحبها ودون علمها. وعلى هذا الأساس نجد ان مبررات حماية الحق في الخصوصية في المجال الرقمي وهي على الآتي:

1- اتساع شبكة الانترنت

إن الواقع يثبت أن أهم التقنيات التي تتحكم في مجموع التعاملات الإلكترونية تعتمد على شبكة الانترنت وهذه الأخيرة ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل شتى الاتصالات التي تترك أثراً حتى دون علم مستخدم الشبكة، فتدقق المعلومات والاتصالات عبر الحدود دون أي اعتبار لحدود جغرافية أو سياسية، بحيث يعمل الأفراد على تبادل المعطيات الخاصة بهم لجهات مختلفة وفي قنوات عديدة داخلية وخارجية، وربما جهات ليس لها محل معنون وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها الحماية القانونية للبيانات الشخصية.⁸

2- الطبيعة الخاصة لقنوات التعامل الإلكتروني

هذه الطبيعة الافتراضية التي تفتقد إلى المادية تجعل من الشخص وهو بصدد استخدام شبكة الانترنت يتوقع قدراً من الخفية في نشاطاته أكثر مما هو عليه الحال في العالم الواقعي، بينما الواقع يثبت عكس ذلك على اعتبار أن التعاملات الإلكترونية تترك آثاراً ودلالات على

شكل سجلات رقمية حول الموقع المزار والأمر التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها ، مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها.⁹

3- فقدان المركزية وآليات السيطرة في قنوات التعامل الإلكتروني

يكتسب حق الخصوصية في إطار العالم الرقمي نوعاً من التميز إذ أن إقرار قانون فاعل يكرس من وجود استراتيجية ملائمة لحماية حق الأفراد بعيداً عن العالم الرقمي قد يكون نوعاً من السهولة بحيث يمكن للدولة وضع رقابة على الاعتداءات المختلفة، إلا أن الأمر لن يكون بذات السهولة إذا ما تعلق الأمر بحماية حق الخصوصية المعلوماتية لأن لها ارتباطاً مباشراً بعالم افتراضي شاسع يرتبط بشبكة الانترنت اللامتناهية الحدود، وهنا يحدث الصراع على السيطرة على الانترنت من خلال الصعوبة في التحكم في مركزية أسماء النطاقات وعناوين المواقع وغيرها، وهو ما يوسع من دائرة اختراق حق الأفراد ويصعب من الحماية ضد أي انتهاكات لخصوصياتهم.¹⁰

الفرع الثاني: نطاق حماية حق الخصوصية في المجال الإلكتروني

يتحدد نطاق الحق في الخصوصية في مجال التعاملات الإلكترونية بين حدين متناقضين يتمثل أولاهما في حق الأفراد في الحياة الخاصة وثانيهما موجبات الاطلاع على شؤون الأفراد وما تفرضه الضرورة على الدول والحكومات في توفير حد أدنى من خط الأمان وكبح للجريمة المرتكبة عبر الانترنت، ويتضح هذا النطاق وفق المعالم التالية:

- إيجاد تناسق بين الحق في الخصوصية وحق الدولة في الإطلاع على هذه الخصوصية في إطار تنظيم الحياة الاجتماعية على نحو أفضل، وهذا لا يتعارض في مفهومه مع التعرض للحياة الخاصة للأفراد بأي حال ، إلا في حالة استخدام البيانات الشخصية لأغراض تتنافى مع صونها واحترامها.¹¹
- إيجاد تناسق بين حق الفرد في عدم الكشف عن أي معطيات أو بيانات تتعلق بخصوصيته مع المصلحة في الكشف عن هذه الخصوصية لجني فوائد عملية، إذ أنه يتبين عدم وجود تعارض بين الحق في السرية والكشف الإرادي عن هذه الخصوصية، إلا أن الفكرة تخص مسألة تفادي أي احتمال لاستغلال تلك المعلومات المكشوف عنها إرادياً ليتم استغلالها في أغراض تهدد حرمة الفرد وانتهاك لحرمة حياته الشخصية.¹²
- رسم خط توازي بين استخدام فكرة بنوك المعلومات¹³ كآلية لجمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد والتي خلقت آثاراً إيجابية عريضة في مجال تنظيم تعاملات الافراد إلكترونياً ، فبفعل الكفاءة العالية لوسائل التقنية الحديثة والإمكانات

غير المحدودة في مجال تحليل واسترجاع المعلومات إلكترونيا ، اتجهت أغلبية دول العالم بمختلف هيئاتها إلى إنشاء قواعد بيانات تساهم في هذه العملية⁴¹، إلا أنه ظهر بشكل سريع الشعور بخطورة تقنية المعلومات وتهديدها للخصوصية. ويمكن المخاوف يبرز في أن الوضع الحديث لتقنية المعلومات أضحى يمس بجوانب حياة الافراد الشخصية بتخزينها لتلطق المعلومات وجمعها لفترة غير محددة والرجوع إليها بكل سهولة، مع خطر تدفق تلك البيانات التي تنتج عن المعاملات الالكترونية ويجعلها عرضة للمقرصنة والتملك والاستغلال مما يخلق حالة قلب لإيجابية تلك التقنية الحديثة إلى خطير يهدد استقرار الحياة الخاصة وسريتها.¹⁵

المبحث الثاني : الاعتداء الإلكتروني على الحق في الخصوصية

وآليات الحماية المكرسة دوليا وداخليا

لما شقت التكنولوجيا طريقها إلى حياة الأفراد، أضحت الإعتداءات المرتكبة إلكترونيا تتسم بالحدائثة والتطور ، بحيث أدى الاعتماد على الحواسيب وشبكة الانترنت ودورها في جمع البيانات الشخصية ومعالجتها إلى تهديد خصوصية الأفراد ووقوع الحياة الخاصة فريسة للجريمة المعلوماتية ومن ثم أضحت حياة الأفراد شبه عارية أمام تكنولوجيا المعلومات ، هذا ما نعى الشعور بمخاطر تقنية المعلومات وحرك الجهود الداخلية والدولية الإقليمية والوطنية لإيجاد مبادئ وقواعد من شأنها مراعاة الحماية لحق الخصوصية في العالم الرقمي.

المطلب الأول : الاعتداء على الخصوصية في العالم الرقمي

يمكن تأصيل المخاطر الإلكترونية التي تمس حق الخصوصية في صورتين أولاهما: انتهاك سرية البيانات الشخصية وثانيها الاعتداء على سلامة البيانات المتداولة في مختلف التعاملات.

الفرع الأول : الجرائم الواقعة على سرية البيانات الشخصية

تتعدد صور الاعتداء على سرية البيانات الشخصية ابتداء من المعالجة غير المشروعة للبيانات أو عملية الإفشاء غير المشروع لتلك البيانات أو تعرض المحادثات الشخصية للأفراد للتجسس عبر شبكة الانترنت وكذا عمليات اختراق البريد الإلكتروني .

أولا : المعالجة غير القانونية للبيانات الشخصية

تعد البيانات الشخصية هي قوام الحق في الخصوصية فهي تعد تمثل في مجموعها المعطيات والمعلومات الخاصة بالفرد والتي تكتسب صفة السرية، وعملية المعالجة غير المشروعة لجملة البيانات هي أبرز صور انتهاك لتلك السرية من خلال مخالفة القائمين على عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخليا¹⁶ كعدم منح الترخيص

من الجهات المختصة أو إلغائه أو انتهاء مدته وهذا يشكل في جوهره اعتداء على حق الدولة في الرقابة على تداول ونقل البيانات الممنوحة للأشخاص المعنوية المصرح لها بذلك قانوناً. وبهذا ينشأ مخاطرة تحول دون مهمة القائمين على تلك الرقابة في التكفل عدم الاعتداء على الحياة الخاصة، ومن ثم تغييب دور الدولة في ضبط مجال الرقابة على البيانات وحمايتها من شتى أنواع الجريمة الإلكترونية.¹⁷

كذا أن فكرة المعالجة غير المشروعة للبيانات الشخصية تقوم على مسألة الاعتداء على حق الأفراد في الاستئثار بمعالجة البيانات الشخصية، الأمر الذي يعد ضرورياً في التفرقة بين البيانات القابلة لمعالجتها من قبل الغير وتلك غير القابلة لذلك.¹⁸

ثانياً : الإفشاء غير المشروع للبيانات الشخصية

إن مسألة الإفشاء غير المشروع للبيانات الشخصية كأحد صور انتهاك لحق الخصوصية قد تأخذ مظهرها في بعض المهن التي تعتمد على سرية البيانات كمهنة المحاماة والطبيب أو عمال البنوك، بحيث يفترض احتفاظ صاحب المهنة بسرية البيانات الشخصية للزبون أو العميل بحكم التعامل القائم بينهما.

وتعد أكثر البيانات عرضة للإفشاء غير المشروع هي الخاصة بتعاملات البنوك الإلكترونية وهذا ما ثبت من خلال قضية بنك (جزل تشافت) السويسري التي حاول خلالها عملاء فرنسيين تابعين لإدارة خدمات الرقابة على التعاملات التجارية والمالية فك شفرة بيانات شخصية لمواطنين فرنسيين تحمل حسابات لدى البنك، وذلك للاستعانة بها في أعمال البحث والتقصي التي تجرى بشأن التهريب الضريبي.¹⁹

الفرع الثاني : التجسس الإلكتروني

لقد أثبتت التجربة الواقعية أن خطورة استخدام شبكة الانترنت تكمن أساساً في ضعف الوسائل المستخدمة في حماية انتقال البيانات عبر الشبكة، ضف إلى ذلك صعوبة الوصول إلى الأشخاص القائمين بالاعتداء وبهذا فقد ظهر التجسس الإلكتروني كأخطر صور الاعتداءات التي تحدث في إطار التعاملات الإلكترونية وهذا لارتباطه بشكل مباشر باغتصاب سرية المحادثات الشخصية و جل المراسلات والتعاملات التي تتم عبر شبكة الانترنت في كل المستويات .

ولقد عرف التجسس الإلكتروني في مجال المحادثات الشخصية بأنه : « عملية التنصت أو التقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الانترنت»، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات وذلك باستخدام أي وسيلة من الوسائل التقنية.²⁰

وما يجدر الإشارة إليه أن التجسس الإلكتروني الذي يصدر في سياق خارج عن القانون والممارس من طرف سلطات الدولة يعد من الأساليب المحرمة دولياً وداخلياً لانتهاك حق الأفراد، وهذا في حالة ثبوت حصول فعل التجسس بدون إذن مسبق من المحكمة وهذا يدخل في إطار التعسف في استعمال حق الدولة في المساس بحقوق الأفراد تحت مظلة الأمن القومي أو العام.

ضف أن خطورة التجسس الإلكتروني أضحيت تأخذ صورة أوسع مما كانت عليه سابقاً خاصة في ظل العولمة والتقنيات الحديثة، بحيث لم تعد تقتصر على السلطات أو دوائر المخابرات بل قد أصبحت وسائل التجسس متاحة إلى الأفراد العاديين خاصة في الدول المتقدمة على عكس الدول العربية التي ما زالت حركة تسويق أجهزة التجسس من الأمور المستعصبة والتي لا يمكن تداولها بشكل حر ويسير.²¹

ولقد اختلفت الوسائل المتبعة في إطار التجسس الإلكتروني وهذا تبعاً لاختلاف ثقافة مستخدمي هذه الوسائل ومن أبرزها اتباع تقنية اعتراض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها، فيتم التخل من قبل أحد الأشخاص الخارج عن الاتصالات الشبكية المقامة عبر الانترنت كتبادل النصوص أو الأحاديث الصوتية فيتم التقاط البيانات أو الصور أو التنصت على الأحاديث الصوتية واعتراض المحادثات المقامة بالصوت والصورة عن طريق الكاميرات أثناء الاتصال.²²

الفرع الثالث: اختراق الحاسبات الآلية والبريد الإلكتروني

ذهب البعض من الفقه على تعريف جريمة الاختراق بأنها «عملية دخول غير مصرح بها إلى حاسب الآخر عن طريق استخدام برامج متطورة تحت تقنية وخبرة عاليتين»²³

كما ربط البعض الآخر فكرة الاختراق بالمعالجة غير المشروعة للبيانات فعرفه بأنه الولوج غير المصرح به قانوناً إلى نظام معالجة البيانات باستخدام الحاسوب.²⁴

وهذا نجد أن عمليات الاختراق لا تقل خطورة عن النماذج السابقة على اعتبار أن الحاسب الشخصي أصبح يمثل أهم الوسائل المتاحة للاتصالات الحديثة بين الأفراد وأضحى يعتمد عليه كلياً كآلية للمراسلات والمعاملات التي تصدر في إطار التعاملات الإلكترونية وبهذا فإن فكرة اختراق الحاسب الشخصي تقوم على أساس الاعتداء على خصوصية وسرية المعاملات وتسخيرها واستغلالها في شتى الأغراض غير المشروعة التي تلحق بالفرد عدة خسائر على المستوى المادي والمعنوي، وهذا ما عبر عنه في السنوات الأخيرة من خلال ما يعرف بالاختراق الأسود أو «مخترقي القبعة السوداء» وهي مجموعة من المجرمين الإلكترونيين الذين اعتمدوا أسلوب اختراق الحاسبات الشخصية للأفراد بالدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة وتعديل وتحريف وإتلاف البيانات بغرض الاستفادة المادية أو إحداث الضرر المعنوي للضحية، وقد تخل هذه التصرفات في غالب الأحيان في إطار العداءات الشخصية أو السياسية

أو الدينية أو القيام بتلك الأفعال لحساب جهات منافسة أو معادية.²⁵

ثانيا : جريمة اختراق البريد الإلكتروني

يعتبر البريد الإلكتروني من أحد الوسائل الحديثة في إطار المعاملات الإلكترونية التي تقدمها شبكة الانترنت فهي تدخل في إطار تسهيل الاتصال الإلكتروني عن طريق تبادل الرسائل الفوري، وبهذا يعد اختراق البريد الإلكتروني من أهم المخاطر التي تواجه حق الخصوصية وتعرض الفرد إلى انتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات وبهذا فإن المقرر وفق القواعد العامة تكريس ضمانات لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة سواء كانت تقليدية أو حديثة.²⁶

المطلب الثاني : آليات حماية الحق الخصوصية في العالم الرقمي

لقد أضحت التكنولوجيا الحديثة سلاحا ذو حدين خاصة في مجال الحق الخصوصية ، فبقدر التطور الهائل الذي مس حياة الأفراد وأسبغ عليه يسر ومرونة في التعامل والاتصال عبر شبكة الانترنت إلا أن هذا الأمر قد حمل في ثناياه مخاطر عديدة مست بخصوصيات الأفراد مما استدعى بذل الكثير من الجهود سواء على مستوى التشريعات الداخلية أو على المستوى الدولي لإرساء آليات الحماية ضد انتهاك حق الخصوصية ، وهنا يثار التساؤل حول معالم الحماية التي رسمتها القواعد الدولية في ظل الاتفاقيات والمؤتمرات الدولية الرامية لحماية هذا الحق ، أو الجهود الداخلية للدول في مسارت تفعيل القواعد العامة العقابية بما يتماشى وحماية حق الخصوصية في المجال الإلكتروني أو استحداث تشريعات خاصة تغطي هذه الحماية.

الفرع الأول : حق الخصوصية في ظل الحماية الدولية

مما لا شك فيه أن الحماية الدولية لحقوق الإنسان قد أخذت أهمية واسعة نظرا للدور الذي تقوم المواثيق والمؤتمرات الدولية في ترسيخ تلك الحقوق ودعمها على المستوى الإقليمي في ظل النظام القانوني للدول.

أولا : حماية حق الخصوصية في ظل المؤتمرات الدولية والإقليمية

لقد تبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الأفراد المنعقد في طهران عام 1986، بحيث خرج بجملة من التوصيات التي تبرز خطر الحاسبات الإلكترونية على الحياة الخاصة وضرورة إيجاد آليات على المستوى الإقليمي أو الدولي لمحاربة أجهزة التجسس.²⁷

وأما على مستوى الإقليم العربي فلقد انعقد العديد من المؤتمرات الدولية التي عنيت بمكافحة الجرائم المعلوماتية ومنها انتهاك حق الخصوصية ومن أبرزها:

1- المؤتمر الدولي لأمن المعلومات الإلكترونية المنعقد بمسقط سنة 2005

ركز المؤتمر على بحث ودراسة أهم التهديدات الإلكترونية والمخاطر التي تمس باقتصاديات الدول وتحد من التنمية ، وعمل على الخروج بتوصيات خاصة بالتأكيد على التعاون الدولي لمكافحة الجريمة ووضع سياسات مشتركة للقضاء على الآثار السلبية لتكنولوجيا المعلومات التي تهدد الحياة الخاصة.²⁸

2- المؤتمر الدولي الأول لمكافحة جرائم تقنية المعلومات المنعقد بالشارقة بالإمارات العربية المتحدة سنة 2006

يعتبر هذا المؤتمر شاملا من حيث دراسة وبحث إشكالية الجرائم المعلوماتية من حيث المفهوم والمكافحة على المستوى الوقائي والعلاجي وفتح النقاش لدراسة التوجهات المستحدثة في هذا المجال والسعي لتبادل الخبرات في مجال مكافحة جرائم تقنية المعلومات.²⁹

ثانيا : حماية حق الخصوصية في ظل الاتفاقيات الدولية

تعتبر الاتفاقيات الدولية ذات دور مهم في مسألة التنسيق بين التشريعات المختلفة للدول والجدير ببيان أبرز صور التعاون الدولي في مجال حماية حق الخصوصية في المجال الرقمي من الاعتداءات الإلكترونية.

1- الاتفاقية الأوروبية لحماية الافراد في مجال المعالجة الآلية للبيانات الشخصية

جاءت الاتفاقية الأوروبية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية رقم 108 المنعقدة في 28 يناير 1981 في ظل الانفتاح الواسع للانترنت الذي أتاح التبادل الواسع لمختلف أنماط المعلومات وخلق بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو بيئة الأعمال الإلكترونية، وبحيث أن التقارير الصادرة عن هيئات حماية الخصوصية قد أثبتت عدم أمان العمليات الإلكترونية الصادرة عن الأفراد وخاصة في إطار تجميع وتحليل المعلومات الشخصية كحزمة واحدة للوصول إلى حقائق عن الشخص تساهم في تنفيذ الاعتداء على حق الخصوصية، فلقد كفلت الاتفاقية ضمان حقوق الفرد بغض النظر عن الجنسية أو الإقامة واحترامها في مواجهة الاستخدام الآلي للمعلومات ذات الطابع الشخصي.³⁰

2- اتفاقية بودابست لسنة 2001 المتعلقة بالإجرام المعلوماتي

تعد هذه الاتفاقية أول اتفاقية ذات طابع دول يتبناها المجلس الأوروبي في هذا المجال ، بحيث ضمت العديد من الدول الأوروبية وغير الأوروبية ، وقد دخلت حيز التنفيذ في سنة 2004.

أقرت الاتفاقية في المذكرة التفسيرية لها بالدور الذي تسعى من خلاله مكافحة الجرائم

الناشئة عن الأثر السلبي لتكنولوجيا المعلومات ، لتخصص في الباب الثاني من الاتفاقية بعض النماذج البارزة للاعتداء على حق الخصوصية في العالم الرقمي³¹، تجسدت في الباب الثاني المعنون « الإجراءات الواجب اتخاذها على المستوى الإقليمي» وعلى سبيل المثال ما جاء في فحوى المادة 2 التي نظمت مسألة الولوج غير القانوني لأجهزة الحاسوب بدون وجه حق، ونصت على الشروط الواجب توافرها لقيام هذه الجريمة باعتبارها تنطوي على تهديد لسرية وسلامة النظم والبيانات المعلوماتية للأفراد، كما أقرت ضرورة تكريس التشريعات الداخلية لمجموعة من القواعد في النظم العقابية الخاصة بها بغية وضع إجراءات أمنية فعالة ضد تلك الانتهاكات.³²

وكذا جاءت الاتفاقية في نص المادة على النص على جريمة الاعتراض القانوني غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونياً بين الحواسيب عبر شبكة الانترنت، واختصت المادة الرابعة بالنص على ضرورة توحيد أطراف الاتفاقية للجهود بغية تبني الإجراءات التشريعية التي تجرم الاعتداء على سلامة البيانات من أجل ضمان سلامة المنظومة البيانية للاتصالات الإلكترونية.³³

3- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

تبنت جامعة الدول العربية أول اتفاقية عربية لمكافحة جرائم تقنية المعلومات في 21 يناير 2010، وجاءت الاتفاقية في إطار تعزيز التعاون ودعم الدول العربية لبعضها البعض في مجال مكافحة تقنية المعلومات بحيث سارت الاتفاقية على نهج الاتفاقية العالمية بودابست من خلال إقرارها في الفصل الأول بالهدف من الاتفاقية المتمثل في تعزيز التعاون والدعم بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات ، لدرء أخطار هذه الجرائم وحفاظاً على أمن الدول العربية في هذا المجال.

ولقد أقرت الاتفاقية على التزام الأطراف بتجريم شتى أساليب الاعتداء على حقوق الافراد في المجال الإلكتروني المنصوص عليها الفصل الثاني منها والمعنون «بالتجريم» والذي ركزت فيه على تجريم الدخول غير المشروع وكذا الاعتراض غير القانوني للبيانات الشخصية والاعتداء على سلامتها، لتأتي في نص المادة 14 منها وتنص بشكل مباشر على تجريم الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.³⁴

حق الخصوصية في ظل الحماية الداخلية للتشريعات المقارنة

بعد الحراك التشريعي الدولي الساعي إلى ترسيخ المبادئ الأساسية لمكافحة جرائم تقنية المعلومات بشكل عام ومحاربة الانتهاكات الماسة بحق الخصوصية في المجال المعلوماتي بشكل خاص ، جاء دور التشريعات الداخلية للدول لتأخذ على عاتقها تأسيس قواعد حمائية ضد الاعتداءات الماسة بهذا الحق.

وإن كان من الواضح بعد استقراء العديد من النصوص التشريعية العقابية في مجال مكافحة الاعتداء على الحق في الحياة الخاصة نجد أن طائفة من التشريعات قد عملت على تبني نصوص خاصة لتكفل حماية هذا الحق بعيدا عن النصوص العقابية في القواعد العامة، أما البعض الآخر فقد اكتفى بتعديل التشريع العقابي بما يتوافق ومحاربة جرائم تقنية المعلومات المرتكبة عبر شبكة الانترنت بشكل عام وحق الخصوصية بشكل خاص.

الفرع الثاني: حق الخصوصية في العالم الرقمي في ظل التشريعات الغربية

عمل التشريع الفرنسي على التصدي لجرائم انتهاك الخصوصية في المجال المعلوماتي بعد إصدار جملة من التشريعات التي تبناها في مجال نظم المعالجة الآلية للمعلومات والتي مرت على مرحلتين:

الأول: بموجب القانون رقم 17-78 الصادر في 06/10/1978 الخاص بحماية البيانات الاسمية للمواطنين في مواجهة نظم المعالجة الآلية للمعلومات .

والثاني: القانون رقم 19-88 الصادر في 05/01/88 بشأن جرائم الغش المعلوماتي ولقد حرص المشرع في كلا القانونين على النص على الحلول المناسبة لمواجهة الجرائم الناشئة عن الحاسبات الإلكترونية وخطورتها على الحياة الخاصة والحريات العامة والفردية.³⁵

وحرص المشرع الفرنسي على مواصلة مكافحة الاعتداءات الواقعة على حق الخصوصية في إطار التشريعات العقابية بحيث كرس جملة من المواد بموجب قانون العقوبات الجديد رقم 92-684 الصادر في 22/07/1992 والذي دخل حيز التنفيذ ابتداء من 01/03/1994 وتضمن القانون أحكاما جديدة لمواجهة ظاهرة الإجرام المعلوماتي تحت عنوان: الاعتداء على نظم المعالجة الآلية للمعلومات.³⁶

ولقد جرم المشرع أفعال المساس بالحق في حرمة الحياة الخاصة تحت عنوان الاعتداء على الحياة الشخصية فنجدته خطى خطوة سباقية في مجال حماية الحياة الخاصة من خلال توفير آليات الحماية الوقائية التي تهدف منع الاعتداء على الحق بالإضافة إلى الحماية العلاجية وعلى رأسها حماية الضحايا وفقا لدعاوى التعويض.³⁷

أما على المستوى التشريعات الأنجلوسكسونية فلقد حذت حذو التشريعات اللاتينية في مجال مكافحة الاعتداء على الحق في الخصوصية، بحيث أصدر المشرع الإنجليزي قانون حماية البيانات منذ 1984 الذي حث على تأمين الحصول على البيانات الشخصية المخزنة لأغراض المعالجة بأسلوب صحيح ولتحقيق أغراض مشروعة، وكذا المشرع الأمريكي سعى إلى تكريس هذه الحماية وفق جملة من الإصدارات التشريعية على رأسها قانون الخصوصية سنة 1974 بحيث قرر من خلاله الكثير من الضمانات في مواجهة المخاطر التي تتعرض لها بنوك

المعلومات ، وكذا نجد القضاء الأمريكي قد تأثر بجملة التعديلات الدستورية فأعطى للمحاكم مساحة واسعة لتفسير نصوص الدستور في نطاق حماية الحقوق والحريات وبالأخص الحق في الخصوصية.³⁸

الفرع الثالث : حماية الحق في الخصوصية في إطار التشريعات العربية

سعت تشريعات الدول العربية كغيرها من التشريعات الدولية نحو إصدار قوانين خاصة بحماية الحق في الخصوصية لتحقيق الانسجام مع توجهات المنظمات والاتفاقيات الدولية، إلا أنه يؤخذ عليها أنها تسير بخطوات متواضعة وبطيئة في مجال التصدي لاختراق وسرقة البيانات الشخصية وعمليات التجسس على الحياة الخاصة للأفراد واستخدام المعلومات الشخصية لأغراض غير مشروعة وغيرها من الاعتداءات الإلكترونية على الحياة الخاصة في العالم الرقمي ، ولا ربما يرجع ذلك لضعف الإرادة التشريعية في مواكبة المستجدات في مجال التشريع الإلكتروني ، وفي هذا الإطار سنتطرق لموقف التشريع الجزائري وبعض التشريعات العربية المقارنة.

أولاً: موقف المشرع الجزائري من حماية حق الخصوصية

من الاعتداءات الإلكترونية

عمل المشرع الجزائري كغيره من التشريعات المقارنة على الاعتراف بحق الخصوصية بشكل عام كمبدأ دستوري من خلال نص المادة 39 بنص صريح «لا يجوز انتهاك حرمة المواطن الخاصة وحرمة شرفه ويحميها القانون.سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة»

وقد كرس مبدأ الحماية الجنائية بموجب نص المادة 303 من قانون العقوبات التي نصت على من يعاقب بالحبس من 6 أشهر إلى 3 سنوات كل من تعمد المساس بحرمة الحياة الخاصة بأي تقنية كانت وذلك:

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه ويعتبر هذا النص قد حمل في طياته الحماية المرنة التي تمتد إلى أي طبيعة لحق الخصوصية أو الحديث وهذا باستخدام عبارة أي "تقنية كانت"

وعلى الرغم من النص غير المباشر على حق الخصوصية إلكترونياً نجد المشرع لم يتجه إلى إصدار قانون بالحماية للخصوصية في المجال الإلكتروني، إلا أن المشرع اكتفى بمواكبة محاربة جريمة المساس بالحق في الخصوصية في العالم الرقمي بموجب القانون رقم 04-15 المتضمن

تعديل قانون العقوبات في القسم المعنون: « المساس بأنظمة المعالجة الآلية للمعطيات » من خلال نص المادة 39 يعاقب بالحبس من 3 أشهر إلى سنة أو بغرامة من 50 الف إلى 100 الف كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك» .

وكذا جرم عمليات تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو إفشاء أو استعمالها لأي غرض كل المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم.

ولقد وفر المشرع الحماية الجنائية لحق الخصوصية بموجب المادة 4 من القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال³⁹، وهذا بضمان عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الإلكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

ثالثاً: موقف التشريعات العربية المقارنة من حماية

حق الخصوصية من الاعتداءات الإلكترونية

لقد عملت العديد من التشريعات العربية على التصدي لجريمة الاعتداء على حق الخصوصية بحيث اكتفت غالبية التشريعات محاولة تطويع النصوص العقابية التقليدية على الأنماط المستحدثة من الجرائم المعلوماتية وعلى رأسها انتهاك حق الخصوصية، إلا أنه بالمقابل سعت بعض التشريعات الأخرى على خطو خطوات واسعة في مجال مكافحة الجريمة الواقعة على هذا الحق بإصدار تشريعات خاصة بحماية البيانات المعالجة آلياً أو تخصيص قوانين لمحاربة جرائم تقنية المعلومات وإعطاء مساحة لمسألة الحماية الجنائية ضد الاعتداءات على الحق في الخصوصية في المجال الرقمي ، فلقد أصدر المشرع السعودي قانون مكافحة الجرائم المعلوماتية لسنة 2007 وتضمن القانون جملة من المواد تتعلق بحماية البيانات الشخصية المعالجة آلياً.⁴⁰

كذا أصدر المشرع الإماراتي المرسوم رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بحيث جرم هذا الأخير في بعض مواد الأفعال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آلياً ومثاله المادة 21 بحيث عاقبت مستخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً إما عن طريق الاعتراض أو التسجيل أو نشر صور أو بيانات شخصية.

كما أصدر المشرع البحريني القانون رقم 60 لسنة 2014 في شأن جرائم تقنية المعلومات وتضمن القانون تجريم عدة صور للاعتداء على حق الخصوصية وخاصة في إطار اساءة استخدام البيانات الشخصية للأفراد بقصد التشهير والابتزاز.⁴¹

الخاتمة:

إن المواجهة الفعالة لكافة صور الجرائم المعلوماتية خاصة الواقعة منها على الحياة الخاصة، تتطلب استنفار كافة الجهود على كافة المستويات وهذا من خلال سعي الأجهزة الوطنية والدولية تكريس مفهوم الاستخدام الآمن لتكنولوجيا المعلومات، وتوفير الإمكانيات المادية والبشرية التي تسوغها من امتلاك مهارات ومقومات المواجهة للتطور المتسارع للإجرام المعلوماتي.

كذا أن الإشكالية الحقيقية التي ينبثق عنها مسألة الحماية الجزائية للحق في الخصوصية هو التحدي الأكبر الذي يواجهه هذا الحق في التشريع الداخلي خاصة بعد تأسيس قاعدة حماية عريضة على مستوى المواثيق والاتفاقيات الدولية وهو ما يضع التشريع الجزائري محل رهان مع التحديات المستحدثة لمخاطر التكنولوجيا وعلى رأسها الحق في الخصوصية.

كما أن الحق في الخصوصية في العالم الرقمي يكتسب ميزة عنه في شكله التقليدي مما يلزم التنسيق بين أشكال الحماية التشريعية والتقنية والتنظيمية. وبهذا نخرج بالجملة التالية من التوصيات:

- تعميق دور الشراكة المؤسسية والمجتمعية من خلال اضطلاع المؤسسات ومنظمات المجتمع المدني بدورها المحوري في عقد الندوات والمؤتمرات بغية التوصل لحلول جذرية تعتمد على وسائل متطورة لمواجهة الجريمة الماسة بالحق في الحياة الخاصة إلكترونياً.

- ضرورة إصدار تشريع جنائي معلوماتي ينظم كافة الاعتداءات والجرائم الواقعة على مستوى العالم الرقمي واستخدامات شبكة الانترنت.

- ضرورة الدعوة إلى اعتماد قواعد وحلول تنظيمية مشتركة إقليمياً أو عربياً للمسائل والإشكالات المطروحة عن جرائم الاعتداء على حق الخصوصية عبر الانترنت وبذل جهود التعاون وتبادل الخبرات للاستفادة من التجارب الواقعية للدول في هذا المجال.

الهوامش :

- 1 كريم عاطف ، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، ورقة بحث صادرة في إطار سلسلة أوراق الحق في المعرفة الصادرة عن مركز دعم تقنية المعلومات، القاهرة، 2013، ص 3
- 2 عبد الله عبد الكريم ، جرائم المعلوماتية والانترنت (الجرائم الالكترونية) ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ، ص (36).
- 3 محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة مصر، سنة 1992، ص 176
- 4 حسام الدين الأهواي، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دراسة مقارنة، دار النهضة العربية، ط2، 2002، ص 132
- 5 محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، ط1، الاسكندرية، سنة 2014، ص 272.
- 6 السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2002، ص 61.
- 7 عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الالكترونية، دار الكتب القانونية، مصر، 2007، ص 33
- 8 جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، مصر، سنة 2000، ص 40
- 9 عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت (الاحكام الموضوعية والجوانب الاجرائية)، دار النهضة العربية مصر، سنة 2004، ص 398
- 10 أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، سنة 2000، ص 359
- 11 هشام محمد فريد رستم، المرجع السابق، ص 180.
- 12 منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، سنة 2013، ص 19.
- 13 تعرف بنوك المعلومات بأنها قاعدة بيانات تم إنشاؤها ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية، وذلك لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في اغراض متعددة ، وقد تكون بنوك المعلومات مقصورة على بيانات تتصل بقطاع معين، وقد تكون معدة للاستخدام على المستوى الوطني كمرآكز وبنوك المعلومات الوطنية او تستخدم في مجال قطاع الاعمال انظر د.حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر، 1987، ص 60.
- 14 اسامة قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والامريكي وفقا لآخر التعديلات التشريعية، دار النهضة العربية، مصر، سنة 2008، ص 48
- 15 Pierre TRUCHE; Jean –paul Faugère et Patrice FLICHHY : Administration électronique et protection des données personnelles livre Blanc, rapport au ministre de la fonction public et de la réforme de l'Etat, Paris, la documentation française, 2002, P 77
- 16 محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، سنة 2016، ط1، ص 92
- 17 Jean-jacques Hyst : la fraude informatique vue par le nouveau code pénale, exertes des systèmes de binformation ,Février.1992.N 147.
- 18 يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخليوي، اتحاد المصارف العربية ، عمان، الأردن، سنة 2002، ص 519.
- 19 هشام محمد فريد رستم، المرجع السابق، ص 195.

- 20 يأتي هذا التعريف وفقا لما ورد في نص المادة 3 من اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة الاجرام المعلوماتي .
- 21 نديم عبده، أمن الكمبيوتر(الفيروسات والقرصنة بالمعلوماتية وانعكاساتها على الأمن القومي)، دار الفكر للأبحاث والدراسات، بيروت، ط1، 1991، ص 86.
- 22 محمد عزت عبد العظيم، المرجع السابق، ص 101.
- 23 عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية) ، دار النهضة العربية، مصر، سنة 2004، ص331.
- 24 خالد ممدوح إبراهيم ، الجرائم المعلوماتية، دارالفكر الجامعي، مصر، سنة 2004، ص 242.
- 25 محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، مصر، سنة1994، ص56.
- 26 عمر محمد أبو بكر يونس، المرجع السابق، ص 339
- 27 يونس خالد عرب ، جرائم الحاسوب (دراسة مقارنة) ، رسالة ماجيستر، جامعة الاردن، 1994، ص125.
- 28 ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1983، ص 90
- 29 محمود ابراهيم غازي، المرجع السابق، ص 204
- 30 Daniel Kaplan, Informatique, libertés, identités, Fyp Edition, 1^{er} avril.2010,P10.
- 31 خالد ممدوح إبراهيم، المرجع السابق، ص 276
- 32 محمد عزت عبد العظيم، المرجع السابق، ص 161.
- 33 هلالى عبد اللاه احمد، جرائم المعلوماتية العابرة للحدود(أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية ، مصر، ط1، سنة 2007، ص 22.
- 34 محمود إبراهيم غازي ، المرجع السابق، ص 235
- 35 احمد فتحي سرور، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 54، 1984، ص 30
- 36 أسامة قايد، المرجع السابق، ص 86.
- 37 عمر ابو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيا، أطروحة دكتوراه، جامعة القاهرة، 2009، ص 163.
- 38 جميل عبد الباقي الصغير، المرجع السابق، ص 117
- 39 القانون 04-09 المؤرخ 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج رعدد 47 المؤرخة في 2009/08/16.
- 40 عمر ابو الفتوح عبد العظيم، المرجع السابق، ص 179.
- 41 محمد عزت عبد العظيم، المرجع السابق، ص 220