المسؤولية الجزائية الناشئة عن انتهاك أمن المعلومات

د.أسامة أحمد محمد النعيمي
مدرس/ كلية الحقوق/ جامعة الموصل
usama200670@yahoo.com

معلومات البحث

تاريخ الاستلام
٢٠١٩/٩/١

تاريخ القبول
٢٠١٩/١٠/١٥

الكلمات المفتاحية
- المسؤولية الجنائية
- أمن المعلومات
- السرية
- التكاملية

مستخلص البحث

لاشك أن المعلومات وتقنياتها تعد من ثمار التطور الحاصل في مجالات الحياة كافة، لاسيما في ظل الثورة العلمية الهائلة التي يشهدها العالم في مجال تكنولوجيا المعلومات، بحيث أصبحت المعلومات في الوقت الحاضر قوة وقيمة ووسيلة لتحقيق الأهداف السياسية والاقتصادية والاجتماعية خصوصا لمن يحسن جمعها وتنسيقها واستخدامها، والى جانب ذلك برزت صور جديدة من الاعتداءات التي تهدد وتعكر امن المعلومات باستخدامها بشكل غير مشروع أو غير قانوني، ومنها تلك التي تؤدي إلى انتهاك العناصر الأساسية التي يستند إليها أمن المعلومات وذلك بانتهاك حرمة المعلومات أو البيانات الشخصية، وكشف المعلومات السرية، وكذلك التلاعب بالمعلومات عن طريق تعديلها أو تغييرها أو إتلافها وهو ما يشكل صور انتهاك امن المعلومات التي اتجهت الدول إلى ترتيب المسؤولية الجزائية عنها، وهذا ما تناولناه في هذا البحث من خلال تقسيمه إلى مبحثين خصصنا الأول لمفهوم امن المعلومات، أما الثاني فبينا فيه صور المسؤولية الجزائية الناشئة عن انتهاك امن المعلومات.

Criminal Liability Arising from the Violation of Information Security

Dr. Usama A. Mohammad Alnuaimy
Lecturer / Faculty of Law / University of Mosul
usama200670@yahoo.com

Article info.

Article History

Received:

1/9/2019

Accepted:

15/10/2019

Keywords
- **Criminal Responsibility**
- **Information Security**
- **Confidentiality**
- **Integrity**

Abstract

There is no doubt that information and its technologies are the fruits of development in all areas of life, especially in light of the tremendous scientific revolution witnessed in the world in the field of information technology, so that information has become at present a force, value and a means to achieve political, economic and social goals, especially for those who are better collected, coordinated and used.In addition, new forms of attacks that threaten and disturb the security of information have emerged illegally or unlawfully, including those that violate the basic elements of information security by violating the inviolability of information or data. This is what we discussed in this paper by dividing it into two subjects devoted to the concept of information security. Second, we show the forms of criminal responsibility arising from the violation of information security.

مقدمة

الحمد لله رب العالمين والصلاة والسلام على سيدنا محمد وعلى اله الطيبين الطاهرين وصحبه اجمعين، فأن الثورة العلمية الهائلة التي يشهدها العالم اليوم في مجال تكنولوجيا المعلومات جعلت المعلومات وسيلة وهدفاً وقيمة عالية في تحقيق الأهداف الاجتماعية والاقتصادية والسياسية , وهذا ما استدعى قيام الحكومات والدول بتوفير السبل الكفيلة لحمايتها والمحافظة على امنها، بحيث اصبح أمن المعلومات وظيفة مهمة واساسية تدار لتقليل المخاطر التي تتعرض لها المعلومات، فضلا عن منع الاستخدام غير المشروع لها او اتلافها او التلاعب بها وبالشكل الذي يؤدي الى الاضرار بالجهات التي تملكها او يعّرِض أمن الدول او المؤسسات او الافراد الى الخطر.

وقد أصبحت مشكلة حماية المعلومات والمحافظة على امنها موضع اهتمام العاملين والباحثين في هذا الميدان، وهو ما يتطلب ضرورة دراسة جميع المجالات التي تحمل في طياتها اجراءات حماية المعلومات، ومنها الاجراءات القانونية التي تتخذ لتحمي أمن المعلومات من حدوث اي انتهاكات غير مشروعة حتى لو حدثت عن طريق الصدفة او بشكل متعمد، وتحديد المسؤولية الجزائية الناشئة عنها والعقوبات المفروضة بحق مرتكبيها.

أولا: تساؤلات البحث

نحاول من خلال البحث ايجاد اجابات لمجموعة من التساؤلات والتي من اهمها:

١- ما المقصود بأمن المعلومات وماهي متطلباته.

٢- ماهي أهم العناصر التي يتوقف عليها تحقيق امن المعلومات.

٣- ماهي صور المسؤولية الجزائية الناشئة عن انتهاك امن المعلومات، وما موقف المشرع العراقي منها.

ثانيا : نطاق البحث

يتحدد نطاق البحث بدراسة المسؤولية الجزائية الناشئة عن انتهاك امن المعلومات وفقا للعناصر الاساسية لأمن المعلومات دون بقية صور الجرائم المعلوماتية، مع بيان موقف المشرع العراقي منها، لاسيما وفق مشروع قانون جرائم المعلوماتية العراقي.

ثالثا : منهجية البحث

سنعتمد في البحث على المنهج الاستقرائي لنصوص القوانين التي رتبت المسؤولية الجزائية عن انتهاك امن المعلومات، فضلا عن المنهج المقارن حيث قارنا بموجبه بين موقف المشرع في هذه القوانين مع موقف المشرع العراقي وبالقدر الذي يحقق الفائدة من هذا البحث.

رابعا : هيكلية البحث

في ضوء ما تقدم ارتأينا تناول موضوع البحث وفق الخطة الاتية :

المبحث الاول : مفهوم أمن المعلومات

المطلب الاول : تعريف أمن المعلومات

المطلب الثاني : اهمية أمن المعلومات ومتطلباته

المطلب الثالث : عناصر أمن المعلومات

المبحث الثاني : صور المسؤولية الجزائية الناشئة عن انتهاك أمن المعلومات

المطلب الاول : المسؤولية الجزائية الناشئة عن انتهاك الخصوصية

المطلب الثاني : المسؤولية الجزائية الناشئة عن انتهاك السرية

المطلب الثالث : المسؤولية الجزائية الناشئة عن انتهاك تكاملية المعلومات وسلام

المبحث الأول

مفهوم أمن المعلومات

للتعريف بأمن المعلومات يقتضي الأمر بيان ذلك في مطالب ثلاث، نتناول في الأول تعريف أمن المعلومات، فيما نخصص الثاني لتوضيح أهمية أمن المعلومات ومتطلباته، أما الثالث فنبين فيه عناصر أمن المعلومات.

المطلب الأول

تعريف أمن المعلومات [١]

إن استخدام مصطلح أمن المعلومات (Information Securing) أو الأمن المعلوماتي وجد استخدامه الشائع مع شيوع استخدام الوسائل التقنية لمعالجه وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات ولاسيما الشبكة العالمية الانترنت، إذ أخذت الأبحاث والدراسات المتعلقة به تأخذ حيزا كبيرا من اهتمام الباحثين في تقنيه المعلومات.

وقد خلت القوانين المتعلقة بمكافحة جرائم تقنية المعلومات وكذلك القوانين الخاصة بالمعلومات الإلكترونية من تعريف محدد يبين المراد بمصطلح أمن المعلومات .

أما على صعيد الفقه، فقد عرف بأنه ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطه الاعتداء عليها، أي هو العلم الذي يهدف إلى بناء استراتيجيات ناجحة من حيث أمن الشبكة وأمن النظم ومعالجه الاستخدام وكيفية واغراض حماية البيانات من حيث السرية والتكاملية والاستمرارية وسلامه المحتوى، فضلا عن أنماط ومستويات الحماية على شبكة الانترنت ومخاطر اختراقها وكيفية الوقاية من هذه المخاطر [٢].

كما عرف ايضا بانه الطرق والوسائل المعتمدة للسيطرة على انواع ومصادر البيانات كافه وحمايتها من السرقة والتشويه والتلف والتزوير والاستخدام غير المرخص وغير القانوني، او هو مجموعه الاجراءات والتدابير الوقائية التي تستخدمها

المؤسسة او المنظمة للمحافظة على المعلومات وسريتها سواء من الاخطار الداخلية او الخارجية كالحفاظ عليها من السرقة والتلاعب والاختراق والاتلاف غير المشروع سواء قبل ادخالها الى الحاسب ام خلال ذلك او بعده من خلال تدقيق المعلومات وحفظها في مكان أمن وتسميه الاشخاص المخولين الذين يحق لهم التعامل مع هذه المعلومات، ومن ثم فان أمن المعلومات يشمل المحافظة عليها عند ادخالها وتخزينها وانتقالها واستخدامها[٣].

ويتبين مما تقدم ان أمن المعلومات كمصطلح يرتبط بمفهوم الأمن المعلوماتي على المستوى الوطني الذي يعني ضرورة احساس افراد المجتمع بعدم وجود اي شكل من اشكال التهديدات لبنى المؤسسات المعلوماتية، وضرورة اتباع الوسائل واتخاذ الاحتياطات كافة للتأهب والعمل الفعلي لمواجهة هذه التهديدات، سواء أكان مصدرها داخليا ام خارجيا.

فضلا عن ذلك فان أمن المعلومات يقتضي حماية جميع انواع المعلومات ومصادر الادوات التي تتعامل معها وتعالجها من التجهيزات الحاسوبية وغير الحاسوبية المتصلة بها باتباع اجراءات وقائية محدده تكفل المحافظة عليها وحمايتها من الاخطار التي قد تتعرض لها والتي تتخذ صورا متعددة كاستغلال المعلومات الشخصية لغير الاغراض التي جمعت من اجلها، او كشف ما يعد منها سريا وما قد ينتج عنه من اطلاع الاشخاص غير المصرح لهم على معلومات ما كان ينبغي لهم الاطلاع عليها، او اتلافها او تعرضها للاستعمال غير المشروع سواء بالتغيير او التعديل[٤].

المطلب الثاني

أهمية أمن المعلومات ومتطلباته

إن أهمية أمن المعلومات تنبع من أهمية المعلومات بحد ذاتها، إذ أن المعلومة في الألفية الثالثة أضحت قوة، وتمثل قيما اقتصاديه مستحدثه مما ينبغي معه احقاق مبدأ الحق في المعلومات؛ وذلك لتحقيق التوازن بين الاستخدام الحر والكامل للمعلومات وبين الحقوق والحريات والمصلحة العامة بحمايه من تتعلق بهم المعلومات من المساس بشرفهم او اعتبارهم او حرمه حياتهم الخاصة او استخدام هذه المعلومات على نحو غير مشروع [٥].

وكذلك تنبع أهميتها من كون المعلومات اصبحت تستخدم من الجميع بلا استثناء، سواء الدول ام المنظمات ام الشركات ام الافراد. كما انها هدف للانتهاك من جانب الجميع بلا استثناء، اذ قد تكون المعلومات الفاصل بين المكسب والخسارة للشركات، وقد تكلف الفرد في ثروته وربما حياته في بعض الاحيان، ومن هنا فان مشكله هذا العصر لم تعد تنحصر في كيفيه الحصول على المعلومات وانما اصبحت المشكلة في خضم الفيض الهائل من المعلومات تتمثل في كيفيه حمايتها من الاخطار التي تهددها،[٦] والمحافظة عليها من خلال منع اي تغيير للمحتوى الخاص بها، سواء اكان ذلك بشكل متعمد ام غير متعمد، اذ بغير ذلك تصبح المعلومة عديمة الجدوى و غير أمنه للاستخدام[٧].

ولتلافي العبث بالمعلومات او تشويهها او اتلافها تضع الدول والمنظمات والشركات الخطط الاستراتيجية المتكاملة للرقابة والحفاظ على أمن المعلومات وسريتها، فضلا عن بناء سلسلة قيمه تتضمن حزمه متكاملة من انشطه التطوير والأمن والرقابة والكشف السريع على المشاكل التي قد تواجه عمل نظم المعلومات[٨]، فأمن المعلومات سواء اكان ماديا لمراكز المعلومات ام معنويا للبرمجيات او الشبكات يتطلب بناء نظام متكامل لأمن المعلومات الذي اصبح وظيفة مهمة واساسية يجب ان تدار لإجراءات منع وتقليل المخاطر التي تتعرض لها المعلومات ولديها مجموعة

من المتطلبات الأساسية لضمان مستوى مناسب من التنفيذ الحالي والمستقبلي لأمن المعلومات، وبالإجمال فان هذه المتطلبات تتمثل في تحقيق:

١- الأمن المادي لمراكز المعلومات

ويقصد به أمن مركز المعلومات وأمن غرفه تشغيل الأجهزة وأمن الأجهزة ووسائط التخزين وأمن الافراد[٩]، اذ ينبغي اعطاء اهميه للمواقع والأبنية التي تحتوي الأجهزة وملحقاتها وتوفير الحماية اللازمة لها من الاخطار التي قد تتعرض لها نتيجة الاخطاء الإنسانية او الحوادث الطبيعية كالسرقة والتخريب الاختراق وقطع الامداد بالتيار الكهربائي والحرائق والفيضانات.

ويجب لذلك اتخاذ الاجراءات الاحترازية لحماية هذه المراكز وتحصينها ضد السرقة والتخريب والحريق والفيضانات ومحاوله ادامة القدرة الكهربائية وانتظامها، وكذلك تحديد اساليب التفتيش واجراءاته للتحقق من هوية الافراد الداخليين والخارجيين من والى مراكز المعلومات لمنع وصول غير المخولين وتلافي التدمير وتجنب الحوادث[١٠].

كما يجب ان تكون هنالك مراقبه مستمرة ذات بعد يتصل بأمن وسلامة المكونات المادية والأجهزة والبرمجيات وحمايتها من كل اشكال التخريب او الحاق الضرر المادي المتعمد بها، فضلا عن ذلك ينبغي اتخاذ الاجراءات الأمنية اللازمة للسيطرة الخارجية على المباني وكشف المتسللين ووضع العراقيل امامهم كإحاطة الأبنية بأسوار مرتفعة او اسلاك شائكة، واستخدام اجهزه مراقبة مثل الكاميرات واجهزة التجسس عن بعد، وكذلك ابقاء حراس متدربين على حمايه الأبنية لحراستها ليلاً ونهاراً[١١].

٢- الأمن المعنوي للبرمجيات

تعد البرمجيات من المكونات غير المادية وعنصرا مهما واساسيا في نجاح استخدام اي نظام معلوماتي، ومن ثم يجب ان يؤخذ أمنها بعين الاعتبار عند تصميم النظام، اذ من الافضل اختيار اجهزة حواسيب ذات انظمة تشغيل لها خصائص أمنية

يمكنها ان تحقق حماية للبرامج من التهديدات التي قد تتعرض لها والتي يكون مصدرها اما داخليا، اي من داخل مركز المعلومات وذلك من قبل الاشخاص العاملين فيها بهدف الوصول الى معلومات مهمة غير مخول لهم الاطلاع عليها ومن ثم استخدامها لتحقيق مصالح معينة او من قبل الاشخاص العاملين في النظام ولهم الحق في الاطلاع على المعلومات وهؤلاء يشكلون تهديدا داخليا ايضا ويمكن من خلالهم تسريب معلومات هامة الى الغير بقصد او بغير قصد.

واما ان يكون مصدرها خارجيا، وهي التي تتم من خارج مركز المعلومات و تكمن خطورتها ليس فقط في عدم معرفه او صعوبة معرفة الشخص او الجهة التي تحاول اختراق النظام، وانما من عدم معرفة مدى اختراقه للنظام ومدى خبرته في التخريب، وما الهدف الذي يسعى الى تحقيقه من وراء ذلك[١٢].

وفي كلتا الحالتين تكون حماية البرمجيات من التهديدات الداخلية او الخارجية بالمحافظة عليها قدر الامكان؛ بعمل نسخ احتياطية للمعلومات والبيانات، واتخاذ الاجراءات لحمايتها من الفايروسات واستعادتها في حاله حدوث عطل او خلل بالنظام، فضلا عن استخدام شيفرات مختلفة ذات معايير عالية ووضع قيود للأمان والسرية التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها، وكذلك منع اي شخص من امكانية الدخول الى النظام والتلاعب به او تدميره من خلال تحديد الصلاحيات في مجال القراءة للملفات او الكتابة فيها[١٣].

٣- الأمن البشري أو الفردي

يلعب الافراد دورا اساسيا ومهما في مجال أمن المعلومات والحواسيب الآلية، فهم من جهة عامل مؤثر في حماية المعلومات والحواسيب، ومن جهة اخرى لهم دور سلبي في مجال تخريب الاجهزة وسرقة المعلومات واتلافها سواء لمصالح ذاتيه ام لمصالح الغير، لذا فان الاهتمام بالأفراد العاملين في مراكز المعلومات يعد من متطلبات أمن المعلومات، وبالتالي يجب تحديد مواصفات محددة للعاملين فيها ووضع

تعليمات واضحة لاختيارهم وتحديد المسؤول عن التعامل مع المعلومات والبيانات في هذه المراكز .

ومن اجل تقليل المخاطر التي يمكن ان يكون الافراد العاملين في مراكز المعلومات مصدرها؛ ينبغي وضع خطط لزيادة الحس الأمني لديهم والقيام بمراجعة دورية للتدقيق في الشخصية والسلوكية من وقت لآخر، وربما تغيير موقع عملهم وعدم احتكار المهام على موظفين محددين، كما يجب تدريبهم وتعريفهم بأهمية المعلومات ومراقبتهم وتغيير طرق الحماية من وقت لأخر، فضلا عن ذلك ينبغي وضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن وبناء ثقافة الأمن لدى العاملين التي تتوزع بين وجوب مراعاه اخلاقيات استخدام التقنية وبين الاجراءات المتطلبة من الكل لدى ملاحظة اي خلل، كما يجب ان يحدد للعاملين ما يتعين عليهم القيام به وما يحظر عليهم القيام به اثناء استخدامهم لوسائل التقنية المختلفة في مراكز المعلومات[١٤].

المطلب الثالث

عناصر أمن المعلومات

ان اغراض ابحاث واستراتيجيات أمن المعلومات – سواء من الناحية التقنية او الأدائية –وكذلك هدف القوانين والأنظمة والتعليمات التي تصدر في هذا الصدد تتمثل في ضمان توافر عناصر اساسية لأي معلومات يراد توفر الحماية اللازمة لها، وهي:

- السرية او الموثوقية
- تكاملية المعلومات وسلامتها
- استمرارية توافر المعلومات او الخدمة
- وهناك اتجاه يضيف لها عنصراً رابعا وهو عدم امكانية انكار التصرف ممن قام به .

اولا : السرية او الموثوقية (Confidentiality)

ان النظام الآمن هو النظام الذي يضمن للمعلومات المخزنة فيه سريتها واتاحتها فقط للأشخاص المخولين بالاطلاع عليها، فضلا عن تامين الطرق المناسبة التي تكفل حمايتها من الاطلاع غير المشروع عليها، سواء اكان ذلك في الاماكن التي يتم فيها خزن هذه المعلومات ام اثناء نقلها عبر شبكة الاتصالات العالمية، لذا يجب اتخاذ كافة التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات السرية او الحساسة، كالمعلومات الشخصية، والموقف المالي لشركة ما قبل اعلانه والمعلومات المتصلة بالأمن القومي والاسرار العسكرية....الخ[١٥].

ويمكن ضمان أمن المعلومات السرية من خلال وسائل متعددة تختلف باختلاف المعلومات فمثلا يمكن استخدام كلمه سر للولوج الى الملفات المهمة او حتى النظام كله بالنسبة للمعلومات الموضوعة على جهاز الحاسب الالي الشخصي، اما اذا كان الحاسب الالي خاص بدائرة او مؤسسة ويضم معلومات مهمة مصنفة على انها سرية، كان لازما زيادة اجراءات الأمن كإضافة نظام جدران نارية تحد من دخول الاشخاص من الخارج وتمنع الاعتداءات المنظمة التي قد يتعرض لها النظام او الموقع الالكتروني[١٦].

ثانيا: تكامليه المعلومات وسلامتها (Integrity)

ويقصد بها حمايه المعلومات وضمان سلامتها تجاه عمليات تدمير المحتوى او العبث به عن طريق الحذف او التعديل او التغيير، فالنظام الامن هو النظام الذي يضمن تكاملية المعلومات المخزنة فيه، وسلامتها من التدمير او التغيير او العبث بها في اي مرحلة من مراحل المعالجة او التبادل، سواء في مرحلة التعامل المباشر مع المعلومات ام عن طريق التدخل غير المشروع، ومن ثم ينبغي اتخاذ التدابير اللازمة لحماية المعلومات من الحذف او التغيير فمثلا من الضروري في مواقع التجارة الإلكترونية ان لا يصل امر الشراء الى الزبون وقد لحقه تغيير او تحريف ما[١٧].

ثالثا: استمرارية توافر المعلومات او الخدمة (Availability)

ويعني ان النظام الآمن يؤمن استمرارية وصول مستخدم المعلومات الى المعطيات الخاصة به دون عائق او تأخير وهو ما يتطلب التأكد من استمرار عمل النظام المعلوماتي وقدرته على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية بحيث تكون المعلومات متاحة للمستخدمين بصوره كاملة ويكون بمقدورهم الحصول عليها دون اي تأخير، فضلا عن عدم تعرضهم الى اي منع عند استخدامهم لها او الدخول اليها[١٨] .

ولهذه الخاصية عدد من السمات المتمثلة بالمقاومة، وهي قدرة النظام على الحفاظ على نفسه من العمليات التي تجعله غير متاح امام المستخدمين المخولين باستخدامه، والمقدرة على التوسع لسد الاحتياجات المستقبلية، والمرونة المتمثلة في توفر الامكانيات والادوات التي تمكن من ادارة النظام من دون ان يؤدي ذلك الى توقفه وسهولة استخدامه[١٩]، اذ بغير ذلك تصبح المعلومات غير ذات قيمة اذا كان من يحق له الاطلاع عليها واستخدامها لا يمكنه الوصول اليها او ان الوصول اليها قد يستغرق وقتا طويلا.

رابعا: عدم انكار التصرف المرتبط بالمعلومات (Non-repudiation)

ويقصد به ضمان عدم امكانية قيام الشخص الذي قام بتصرف مرتبط بالمعلومات او مواقعها من انكار انه الذي قام بهذا التصرف، بمعنى ان تتوفر قدرة

اثبات ان تصرف معين قد تم من شخص ما في وقت معين[٢٠]، ومن ذلك ان يتم التأكد بان مرسل المعلومات او البيانات قد حصل على اثبات بوصولها الى المرسل اليه، وبان المستقبل قد حصل بالمقابل على اثبات لشخصية المرسل مما يمنع احتمال انكار اي من الطرفين بانه قد عالج المعلومات واستخدمها.

وتكون الية منع انكار المسؤولية بالتشفير او التوقيع الالكتروني حيث يتم ربط هوية المرسل بالرسالة التي يقوم بأرسالها او التحكم بالوصول و سلامة البيانات وتبادل الصلاحيات او بالشهادة القانونية او من خلال اجراء معين يتضمن وجود طرف ثالث موثوق به، اذ في حاله حصول نزاع بسبب انكار التصرف يكون من الصعب اكتشاف او تتبع التغيرات التي تطرأ على المصادر الإلكترونية بسبب تشعب نظم المعلومات وتعقيداتها[٢١].

ومن الجدير بالذكر ان ضمان توافر العناصر السابقة وان كان ضروريا للحفاظ على أمن المعلومات الا ان درجه اهميه كل عنصر تختلف باختلاف طبيعة المعلومات المراد المحافظة على أمنها، فمثلا يتطلب ايلاء عنصري السرية والتكاملية اقصى درجات الاهتمام بالنسبة للمعلومات المتعلقة بالأمن القومي والاسرار العسكرية، نجد انه فضلاً عن العنصرين المتقدمين يتطلب ايلاء عنصري الاستمرارية وعدم الانكار ذات القدر من الأهمية بالنسبة للخدمات الإلكترونية التي تقدمها المصارف لاسيما تلك التي تتم عن بعد، في حين نجد ان مواقع الانترنت مثلا تتطلب ايلاء عنصر الاستمرارية الاهتمام الاكبر بينما تتطلب مواقع التجارة الإلكترونية الحرص على توافر عناصر الحماية الأربعة بذات القدر من الأهمية، اذ تتطلب ضمان السرية والخصوصية بالنسبة للبيانات الخاصة بالزبائن كأرقام بطاقات الائتمان وتتطلب التكاملية والسلامة بالنسبة للبيانات المتبادلة عبر الرسائل الإلكترونية بين الزبون والموقع، كما تتطلب استمرارية الموقع في تقديم خدماته طوال وقت سريان عملية التصفح والشراء بل في اي وقت يريد الزبون فيه الولوج الي الموقع، فضلا عن تطلب ضمان عدم انكار الزبون ان التصرف الذي اجراه على الموقع كطلب الشراء صدر عنه او انكار الموقع ذاته انه تعاقد مع الزبون[٢٢].

المبحث الثاني

صور المسؤولية الجزائية الناشئة عن انتهاك أمن المعلومات

تعد المعلومات في الوقت الحاضر ركيزة اساسية من ركائز التطور العلمي والمعرفي والانساني، فضلا عن ذلك فإنها اصبحت قوة وقيمة ووسيلة لتحقيق الاهداف الاجتماعية والاقتصادية والسياسية لاسيما لمن يحسن جمعها وتنسيقها واستخدامها، والى جانب ذلك برزت صور جديدة من الاعتداءات التي تهدد وتعكر امن المعلومات باستخدامها بشكل غير مشروع او غير قانوني، ومنها تلك التي تؤدي الى انتهاك العناصر الاساسية التي يستند اليها أمن المعلومات وذلك بانتهاك حرمة المعلومات او البيانات الشخصية، وكشف المعلومات السرية، وكذلك التلاعب بالمعلومات عن طريق تعديلها او تغييرها او اتلافها وهو ما يشكل صور انتهاك امن المعلومات التي اتجهت الدول الى ترتيب المسؤولية الجزائية عنها.

وهذا ما سنتناوله في هذا المبحث من خلال تقسيمه الى ثلاث مطالب نتناول في الاول المسؤولية الجزائية الناشئة عن انتهاك الخصوصية، اما الثاني فنبين فيه المسؤولية الجزائية الناشئة عن انتهاك السرية، فيما نخصص الثالث للمسؤولية الجزائية الناشئة عن انتهاك تكاملية المعلومات وسلامتها.

المطلب الأول

المسؤولية الجزائية الناشئة عن انتهاك الخصوصية

بعد أن كانت المعلومات والبيانات في ظل الطرق التقليدية لا يطلع عليها إلا صاحب الشأن نفسه باتباع إجراءات معينة أصبح بإمكان أي شخص يمتلك قدرا لابأس به من الإمكانيات التقنية أن يصل الى هذه المعلومات أو البيانات مما يؤدي إلى انتهاك خصوصية الشخص الذي تتعلق به هذه المعلومات[٢٣] ، فالتقدم العلمي اصبح يمثل تهديدا خطيرا لخصوصية وأسرار الإنسان نظرا لما تقدمه الاجهزة الحديثة من امكانيات استراق السمع أو نقل محادثات خاصة أو التقاط ونقل صورة لشخص في مكان خاص من دون أن يشعر صاحب الحديث او الصورة بذلك[٢٤].

ويراد بالخصوصية[٢٥]، في إطار أمن المعلومات المحافظة على سرية المعلومات الخاصة وعدم إظهارها لغير الأشخاص المخولين قانونا بالاطلاع عليها[٢٦]، أي حماية ما يتضمنه النظام المعلوماتي من معلومات وبيانات يسعى اصحابها إلى المحافظة عليها من الإتاحة غير المصرح بها، فضلا عن تلك القيود الخاصة بالبيانات الشخصية وضرورة عدم اتاحة أو الوصول إليها بالطرق العامة الشائعة[٢٧].

ونتيجة لازدياد مخاطر استخدام التقنية الحديثة وتهديدها لخصوصية الافراد كتقنيات رقابة كاميرات الفيديو وبطاقات الهوية الإلكترونية ووسائل اعتراض ورقابة البريد والاتصالات.... الخ، وتنامي الشعور بهذه المخاطر بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية، فضلا عن اتساع دائرة الاعتداء على حق الافراد في الحياه الخاصة الذي ظهر في صور عديده تدور جميعها حول عدم شرعية الاطلاع على المعلومات الخاصة، سواء اكان ذلك عن طريق الالتقاط الذهني للمعلومات كقيام الشخص بالاطلاع على المعلومات والبيانات المعالجة اليا التي تظهر على شاشه الحاسب الالي ام عن طريق القيام بالتنصت على المعلومات او التقاطها بواسطة مكبر الصوت او الميكروفونات الصغيرة او مركز تنصت ام عن طريق التقاط ونقل الصور الشخصية دون موافقه اصحابها[٢٨].

فقد اتجه المشرع في العديد من الدول الى سن القوانين الخاصة التي تكفل حماية خصوصية الافراد وما يتعلق بهم من معلومات شخصية وضمنت تلك القوانين

النصوص التي رتبت المسؤولية الجزائية على انتهاك خصوصية المعلومات او البيانات المتعلقة بالأفراد، وقد كان المشرع الفرنسي من اوائل المشرعين الذين ساروا في هذا الاتجاه، اذ اصدر قانون انتهاك الخصوصية المعلوماتية والحرية العامة رقم (١٧) لسنه ١٩٧٨ وعاقب بموجبه بالحبس من ستة اشهر الى ثلاث سنوات والغرامة من الفي فرنك الى مئتي الف فرنك او بإحدى هاتين العقوبتين كل من قام بأجراء المعالجة الإلكترونية للبيانات الشخصية دون ترخيص من اللجنة المختصة بذلك[٢٩].

كما عاقب بالحبس من شهرين الى ستة اشهر والغرامة من الفي فرنك الى عشرين الف فرنك او بإحدى هاتين العقوبتين كل شخص ارتكب عمدا فعلا من شانه الكشف عن البيانات الشخصية بمناسبة تسجيل او نقل او معالجة البيانات الشخصية باي شكل من الاشكال اذا ترتب على كشفها الاعتداء على الشخصية الاعتبارية لصاحب الشأن او حرمة حياته الخاصة دون تصريح بذلك من صاحب الشأن للغير الذي لا توجد له اي صفة في تلقى هذه المعلومات، اما اذا وقع اي فعل من الافعال السابقة نتيجة اهمال او رعونه فتقتصر عقوبة مرتكب الجريمة على الغرامة السابقة دون الحبس[٣٠] .

كذلك عاقب المشرع الفرنسي كل شخص حاز بيانات شخصية لغرض تصنيفها او نقلها او تسجيلها او معالجتها تحت اي شكل من الاشكال وانحرف عن الغاية او الغرض من المعالجة الإلكترونية لهذه البيانات وفرض عقوبة الحبس من سنة الى خمس سنوات والغرامة من عشرين الف فرنك الى مئتي الف فرنك على من ارتكب هذه الجريمة[٣١].

وفي ذات الاتجاه سار المشرع المصري اذا اصدر قانون تنظيم الاتصالات رقم (١٠) لسنة ٢٠٠٣ وضمنه النص المتعلق بحماية الخصوصية المعلوماتية لمستخدمي شبكات الاتصال، اذ عاقب بالحبس مده لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن خمسة الاف جنيه ولا تزيد عن خمسين الف جنيه او بإحدى هاتين العقوبتين كل من قام اثناء تأدية وظيفته في مجال الاتصالات او بسببها بإذاعة او نشر او تسجيل لمضمون رساله اتصالات او لجزء منها دون ان يكون له سند قانوني

في ذلك او قام بإفشاء اي معلومات خاصة بمستخدمي شبكات الاتصالات او عما يجرونه او يتلقونه من اتصالات وذلك دون وجه حق[٣٢].

وكذلك فعل المشرع الاماراتي في القانون الاتحادي الخاص بشان مكافحة جرائم تقنية المعلومات رقم (٥) لسنه ٢٠١٢، اذ عاقب بالحبس مده لا تقل عن ستة اشهر والغرامة التي لا تقل عن مئة وخمسين الف درهم ولا تتجاوز سبعمائة وخمسين الف درهم او بإحدى العقوبتين كل من دخل الى موقع الكتروني او نظام معلومات الكتروني او شبكة معلومات او وسيلة تقنية معلومات بدون وجه حق او البقاء فيه بصورة غير مشروعة وترتب على ذلك الغاء او حذف او تدمير او افشاء او اتلاف او تغيير او نسخ او نشر او اعاده نشر اي بيانات او معلومات، وشدد هذه العقوبة وجعلها الحبس مده لا تقل عن سنة واحدة والغرامة التي لا تقل عن مئتي وخمسين الف درهم ولا تتجاوز مليون درهم او بإحدى هاتين العقوبتين اذا كانت البيانات والمعلومات محل الجريمة شخصيه[٣٣].

كما عاقب بالحبس مده لا تقل عن ستة اشهر والغرامة التي لا تقل عن مئة وخمسين الف درهم ولا تتجاوز خمسمائة الف درهم او بإحدى هاتين العقوبتين كل من استخدم شبكة او نظام معلومات الكتروني او احدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الاحوال المصرح بها قانونا بإحدى الطرق الآتية :

١- استراق السمع او اعتراض او تسجيل او نقل او بث او افشاء محادثات او اتصالات او مواد ضوئية او مرئية.

٢- التقاط صور الغير او اعداد صور الكترونية او نقلها او كشفها او نسخها او الاحتفاظ بها.

٣- نشر اخبار او صور الكترونية او فوتوغرافية او مشاهد او تعليقات او بيانات او معلومات ولو كانت صحيحة وحقيقية.

فيما عاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مئتي وخمسين الف درهم ولا تتجاوز خمسمائة الف درهم او بإحدى هاتين العقوبتين كل من يستخدم نظام معلومات الكتروني او احدى وسائل تقنية المعلومات لأجراء اي

تعديل او معالجة على تسجيل او صورة او مشهد بقصد التشهير او الإساءة الى شخص اخر او الاعتداء على خصوصيته او انتهاكها[٣٤].

اما بالنسبة لموقف المشرع العراقي فنجد انه لم يفرد قانونا خاصا لضمان حماية المعلومات او البيانات الخاصة من الانتهاك، وبالتالي فان الحماية المتحققة لها تقتصر على النصوص الواردة في قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل، والذي بمقتضاه رتب المشرع المسؤولية الجزائية على كل من نشر بإحدى طرق العلانية اخبارا او صورا او تعليقات تتصل بأسرار الحياة الخاصة او العائلية للأفراد ولو كانت صحيحة اذا كان من شأن نشرها الإساءة اليهم، او قام بالاطلاع على رسالة او برقية مكالمة تليفونية فأفشاها لغير من وجهت اليه وكان من شان ذلك الحاق الضرر بالغير[٣٥]، وعاقب مرتكب الجريمة بالحبس مده لا تزيد عن سنه وبغرامة لا تزيد عن مائة دينار[٣٦]، او بإحدى هاتين العقوبتين.

ومع ذلك نجد ان المشرع العراقي قد ضمن مشروع قانون جرائم المعلوماتية[٣٧]، النصوص التي تكفل حماية المعلومات او البيانات الخاصة من الانتهاك، اذ عاقب بالحبس وبغرامة لا تقل عن عشرة ملايين دينار ولا تزيد عن خمسة عشر مليون دينار كل من تجاوز عمدا نطاق التصريح المخول له او اعترض اية معلومات خلال عمليات تبادلها او قام بالتنصت او مراقبة البيانات والمعلومات المخزنة او المتبادلة في نظم المعلومات .

وشدد العقوبة وجعلها الحبس مده لا تقل عن اربع سنوات والغرامة التي لا تقل عن خمسة عشر مليون دينار ولا تزيد عن خمسة وعشرين مليون دينار اذا نشأ عن احد الافعال السابقة حذف أو تدمير أو تغيير أو تعييب أو تعطيل أو اعادة نشر بيانات او معلومات تعود للغير بغير وجه حق[٣٨].

كما عاقب بالحبس مده لا تقل عن ثلاث سنوات وبغرامه لا تقل عن خمسة ملايين دينار ولا تزيد عن عشرة ملايين دينار كل من باع او نقل او تداول البيانات الشخصية المقدمة اليه من الافراد لأي سبب من الاسباب دون اذن منهم لتحقيق منفعة ماديه له او لغيره[٣٩].

وشدد من المسؤولية وجعل عقوبة الجريمة السجن مدة لا تزيد عن سبع سنوات والغرامة التي لا تقل عن خمسة ملايين دينار و لا تزيد على عشرة ملايين دينار اذا كان مرتكب احد الافعال السابقة موظفاً او مكلفاً بخدمة عامة اثناء تأدية وظيفته او بسببه[٤٠].

وفي هذا الصدد نرى ان المشرع العراقي فعل حسنا باتجاهه الى اصدار قانون خاص بالجرائم المعلوماتية وذلك لمواكبة التطور الهائل الذي احدثته ثورة تقنية المعلومات على الصعيد العالمي والثقافي والاجتماعي والاقتصادي، وكذلك مواجهة مرتكبي الجرائم التي ترتكب باستخدام نظم او شبكات المعلوماتية او وسائل تقنية المعلومات التي لم تعد النصوص الجزائية التقليدية كافية لمواجهتها.

كما اننا وبقدر تعلق الامر بالنصوص التي رتبت المسؤولية الجزائية عن انتهاك الخصوصية المعلوماتية نقترح على المشرع العراقي تعديل نص المادتين (١٥ و ١٩/ اولا / ج) من مشروع قانون جرائم المعلوماتية وبالشكل الآتي :

- ❖ اضافه عباره (او بإحدى هاتين العقوبتين) الى نص المادتين، وذلك تطبيقا لمبدأ التفريد العقابي الذي يعد من المبادئ الأساسية التي يقوم عليها القانون الجنائي الحديث والذي يتيح للقاضي اختيار العقوبة التي تتلائم مع جسامة الجريمة وخطورة الجاني واللذان هما معياران لاختيار العقوبة كرد فعل للجريمة.
- ❖تعديل نص الفقرة (اولا / ج) من المادة (١٩) من المشروع وذلك بالنص على صور الاعتداءات المحققة لانتهاك الخصوصية المعلوماتية، اسوة بما ذهب اليه المشرع الاماراتي الاتحادي في المادة (٢١) من القانون الخاص بشأن مكافحة جرائم تقنية المعلومات رقم (٥) لسنه ٢٠١٢ واعتماد هذه المادة كأساس لتحديد صور انتهاك الخصوصية او الحياه الخاصة للأفراد، وعدم قصر ذلك على افعال البيع والنقل والتداول للبيانات الشخصية التي حددها المشرع لتحقق انتهاك الخصوصية.

فضلا عن ذلك نقترح حذف عبارة (لتحقيق منفعة ماديه له او لغيره) من نص الفقرة اعلاه حيث ان تطلب هذا القصد قد يؤدي الى افلات العديد من مرتكبي الجريمة من العقوبة وذلك على الرغم من تحقق انتهاك الخصوصية، اذ كل ما يتطلب لتحقق انتهاك الخصوصية ان يقع اي فعل من افعال الانتهاكات دون وجه حق او مسوغ قانوني.

المطلب الثاني

المسؤولية الجزائية الناشئة عن انتهاك السرية

ترتبط السرية بالخصوصية الا انهما يختلفان في المعنى، فالأولى تدل على ان هناك موضوعاً معيناً لا يجوز نشره او بثه للأخرين، اما الثانية فتدل على القيود الخاصة بالبيانات الشخصية وضرورة عدم اتاحتها او الوصول اليها بالطرق الشائعة العامة[٤١]، ويرى جانب من الفقه[٤٢]، أن السرية تتطلب التكتم، اما الخصوصية فلا تتطلب السرية فقد تتواجد الخصوصية مع عدم توافر السرية، اذ جوهر السر هو التكتم بعكس الخصوصية التي لا تتطلبه.

وبمعنى اخر فان السرية وموثوقية المعلومات تعني بان المعلومات لا تكشف ولا يطلع عليها اشخاص غير مخولين بالكشف او الاطلاع عليها[٤٣]، وتستمد المعلومات سريتها اما من طبيعتها كاكتشاف في احد المجالات التي تتصف بالسرية واما لرغبة صاحبها في ذلك واما للسببين معا، وفي كل الاحوال فان السرية التي تتمتع بها المعلومات هي التي تحدد نطاق استعمالها في دائرة محددة بحيث يستفيد اصحابها من خاصية ثانية للمعلومات وهي الاستئثار بها والتي تعد امرا ضروريا، اذ انه في مختلف السلوكيات التي تنطوي على اعتداء على الاموال فان الفاعل فيها يعتدي على حق خاص بالغير يرجع الى سلطة هذا الشخص على المعلومات الذي يمنحه الحق في التصرف فيها على سبيل الاستئثار، فيكون الاستئثار لمؤلف المعلومة[٤٤].

ويتخذ انتهاك السرية صور بعض السلوكيات التي تنطوي على اعتداء على سرية المعلومات والتي تتمثل في الاطلاع المجرد على المعلومات او الاطلاع بقصد الافشاء او التهديد او الابتزاز او الاحتفاظ بنسخه منها، ويستوي في هذا الصدد ان تكون هذه المعلومات مخزنة في الحاسب الالي العائد للشخص سواء اكان منفردا ام متصلا بشبكه اتصالات محلية او عالمية ام كانت لدى جهات اخرى يرتبط معها

الشخص بعلاقة ما كعيادة طبيب او مكتب محاماة يتولى شؤونه القانونية او ان تكون لدى جهات حكومية او وزارة او مؤسسة او دائرة [٤٥].

وعليه يمكن من خلال مكان وجود المعلومات تحديد اوجه الخطورة التي تتعلق بسريتها وردها الى امرين هما :

١- الاطلاع المباشر على المعلومات السرية من قبل الشخص الذي يشرف عليها من حيث تصنيفها وتبويبها وتخزينها، سواء اكان هو القائم بالفعل ام مشتركا مع غيره ام مساهما بذلك بطريقه مباشره بإهماله تدابير الحفظ والحماية واجراءاتها .

٢- الاطلاع غير المباشر على المعلومات السرية وذلك باستخدام تقنية الاتصالات المعلوماتية الحديثة المعتمدة على اجهزه الاتصال عن بعد[٤٦].

وللمحافظة على سرية المعلومات وموثوقيتها فقد اتجه المشرع في العديد من الدول الى ترتيب المسؤولية الجزائية بحق من يقوم بانتهاك سرية المعلومات الإلكترونية، سواء اكان ذلك ضمن القوانين الخاصة بالمعاملات الإلكترونية ام تلك المتعلقة بمكافحة جرائم المعلوماتية، وفي هذا الخصوص ذهب المشرع المصري الي اقرار المسؤولية الجزائية على كل من قام اثناء تأديته لأعمال وظيفته في مجال الاتصالات او بسببها بإذاعة او نشر او تسجيل لمضمون رسالة اتصالات او لجزء منها او قام بإفشاء او نشر او اذاعة معلومات خاصة عن مستخدمي شبكه الاتصال او عما يجرونه او يتلقونه من اتصالات دون ان يكون له سند قانوني في ذلك، وعاقب على ذلك بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن خمسة الاف جنيه ولا تتجاوز خمسون الف جنيه او بإحدى هاتين العقوبتين[٤٧].

كما رتب المسؤولية الجزائية على كل من قام بإفشاء او نشر او اذاعة اي معلومة حصل عليها بحكم وظيفته او بسببها عن منشأة عاملة في مجال الاتصالات متى كان من شان ذلك ان يؤدي الى قيام المنافسة غير المشروعة بين المنشآت العاملة في هذا المجال، وعاقب مرتكب الجريمة بالحبس وبغرامه لا تقل عن عشرين الف جنيه ولا تتجاوز مئة الف جنيه او بإحدى هاتين العقوبتين[٤٨] .

وكذلك فعل المشرع الاماراتي الاتحادي اذ تدرج بالعقوبة المفروضة على انتهاك سريه المعلومات[٤٩]، وذلك بحسب طبيعة المعلومات السرية وخطورة النتائج المترتبة على الاطلاع عليها او افشائها، اذ عاقب بالسجن المؤقت والغرامة التي لا تقل عن مئتي وخمسين الف درهم ولا تتجاوز خمسمائة الف درهم او بإحدى هاتين العقوبتين كل من دخل موقعاً او نظاماً او شبكة معلوماتية بقصد الحصول على بيانات حكومية او معلومات سرية تتعلق بمنشأة مالية او تجارية او اقتصادية دون وجه حق، وشدد من العقوبة وجعلها السجن مده لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تتجاوز مليوني درهم اذا ترتب على الدخول إلغاء تلك المعلومات او البيانات او حذفها او اتلافها او تدميرها او افشائها أو تغييرها أو نسخها او نشرها او اعادة نشرها[٥٠].

فيما عاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين الف درهم ولا تتجاوز خمسمائة الف درهم او بإحدى هاتين العقوبتين كل من التقط او اعترض عمدا اي اتصال يتم عن طريق شبكة معلوماتية دون تصريح بذلك، فاذا قام بإفشاء هذه المعلومات فانه يعاقب بالحبس مده لا تقل عن سنة واحده[٥١].

بينما عاقب بالحبس مده لا تقل عن ستة اشهر والغرامة التي لا تقل عن خمسمائة الف درهم، ولا تتجاوز مليون درهم او بإحدى هاتين العقوبتين كل من يستخدم دون تصريح شبكة معلوماتية او موقعاً الكترونياً او وسيلة تقنية معلوماتية لكشف معلومات سرية حصل عليها اثناء تأديته لوظيفته او بسببها[٥٢].

اما بالنسبة لموقف المشرع العراقي فان المسؤولية الجزائية المترتبة على انتهاك سرية المعلومات لا تزال تحكمها النصوص الواردة في قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل، اذ فرض المشرع على الاشخاص الذين يطلعون على اسرار الغير بحكم وظيفتهم او مهنتهم المحافظة على تلك السرية وعدم افشائها الا في الأحوال المصرح بها وبخلاف ذلك يعاقب كل من قام بإفشائها بالحبس مدة لا

تزيد عن سنتين وبغرامة لا تزيد على مائتي دينار[٥٣] او بإحدى هاتين العقوبتين [٥٤].

والملاحظ ان النص المتقدم لا يستوعب جميع صور الانتهاكات السرية للمعلومات المعالجة آليا والتي تقع عن طريق استخدام التقنيات الحديثة متمثلة بجهاز الحاسب الالي او الشبكة المعلوماتية او أية وسيلة تقنية معلوماتية اخرى، ومع ذلك نجد انه قد عالج هذا الموضوع ضمن نصوص مشروع قانون جرائم المعلوماتية، اذ عاقب بالحبس مده لا تقل عن ثلاث سنوات او بغرامة لا تقل عن خمسة ملايين دينار ولا تزيد عن عشرة ملايين دينار او بكلتا هاتين العقوبتين كل من علم بحكم عمله ببيانات التوقيع الالكتروني او الوسائل الإلكترونية او المعلومات فأفشاها بقصد الاضرار بالغير او تحقيق منفعة مالية له او لغيره [٥٥].

كما عاقب بالحبس مده لا تقل عن ثلاث سنوات وبغرامة لا تقل عن خمسة ملايين دينار ولا تزيد على عشرة ملايين دينار كل من حصل بطريقة غير مشروعة على معلومات فأفشاها او اعلنها عمدا من خلال استخدام الحاسب الالي وشبكة المعلومات بقصد الاضرار بالغير، او قام بإفشاء اي نوع من انواع معلومات المشتركين او اسرارهم لأي جهة دون مسوغات صادرة عن جهة رسميه مختصة [٥٦]، واذا كان من قام باي فعل من هذه الافعال موظفاً اثناء تأديته لوظيفته او بسببها فان العقوبة تكون السجن لمدة لا تزيد عن سبع سنوات وبغرامة لا تقل عن خمسة ملايين دينار ولا تزيد على عشرة ملايين دينار[٥٧].

وبهذا الصدد نكرر على المشرع العراقي اقتراحنا السابق الخاص بإضافة عبارة (او بإحدى هاتين العقوبتين) الى نص المادة (١٩/ اولا) من مشروع قانون الجرائم المعلوماتية، كما نقترح عليه تجريم الافعال المتعلقة بإفشاء المعلومات السرية بنص مستقل عن النص الخاص بتجريم الافعال المتعلقة بانتهاك الخصوصية.

المطلب الثالث

المسؤولية الجزائية الناشئة عن انتهاك تكاملية المعلومات وسلامتها

من المعلوم ان صناعة المعلومات اصبحت في الوقت الحاضر المجال الاهم لجذب الاستثمارات، لاسيما في ظل التزاوج الحاصل بين المعلوماتية والاتصالات، فهي تعد مالا لأنها ذات قيمة اقتصادية حيث تمثل مصدراً حقيقياً لتحقيق العائدات المالية لمالكيها، ومن ثم فان قيمة المعلومات واهميتها ترتبط ببقائها صالحة للاستعمال في الغرض الذي خصصت له، ولا يتم ذلك الا بالمحافظة عليها وحمايتها من اي اعتداء يؤدي الى افنائها او على الاقل احداث تغييرات شاملة عليها بحيث تصبح غير صالحة للاستعمال في الاغراض المخصصة لها، او بعبارة اخرى لحمايتها من اي اعتداء يترتب عليه انتهاك تكاملية المعلومات او سلامتها.

ويتخذ انتهاك تكاملية المعلومات وسلامتها او ما يعرف في نطاق نظم المعلوماتية بالأتلاف المعلوماتي[٥٨] ، صورة التعديل غير المشروع للمعلومات الذي يعد واحدا من اكثر صور اتلاف المعلومات شيوعا وانتشارا، ويقصد به اجراء نوع من التغيير غير المشروع على المعلومات المحفوظة داخل النظام واستبدالها بمعطيات ومعلومات جديدة باستخدام احدى وظائف الحاسب الالي[٥٩].

كما يتخذ صورة تدمير المعلومات الذي يعد من اخطر صور الاتلاف التي ترد على المعلومات، اذ انها لا تقتصر على مجرد اجراء بعض التعديلات على المعلومات وانما تدميرها بمحوها او الغائها كليا او جزئيا او تعطيلها على نحو يصيب نظام المعالجة الالية للمعلومات والبيانات بالشلل المؤقت اي توقيفه عن القيام بوظيفته لفترة محددة [٦٠].

فضلا عن ذلك فقد يتخذ صورة الادخال غير المشروع للمعلومات ويقصد به اضافة معطيات جديدة للمعلومات لم تكن موجودة من قبل، وهو ما يترتب عليه فضلا

عن التعديل الذي يطرأ على ذاكرة الحاسب الالي تعديلاً للمعلومات ذاتها او تدميرها كما في حاله ادخال برامج خبيثة الى نظام الحاسب الالي[٦١].

وازاء هذه الاشكالية فقد اتجه المشرع في العديد من الدول التي ترتيب المسؤولية الجزائية عن اتلاف المعلومات وبالشكل الذي يعرض تكامليتها وسلامتها الى الانتهاك، فقد عاقب المشرع الفرنسي في قانون العقوبات الفرنسي لسنة ١٩٩٤ على الدخول او البقاء بطريق الغش داخل كل او جزء من نظام المعالجة الآلية للمعلومات بالحبس لمدة سنة وغرامة مقدارها مئة الف فرنك، وشدد على الجاني إذا ما نشأ عن هذا الدخول محو او تعديل في المعطيات المخزنة في النظام او إتلاف تشغيل هذا النظام وجعل العقوبة الحبس لمدة سنتين وغرامة مقدارها مئتي الف فرنك [٦٢]،

كما عاقب على تعطيل أو افساد نظام التشغيل بالحبس لمدة ثلاث سنوات والغرامة التي مقدارها ثلاثمائة الف فرنك[٦٣]، وكذلك عاقب بالعقوبة ذاتها على إتلاف المعلومات عن طريق إدخال البيانات بصورة غير مشروعة في نظام المعالجة الآلية أو محوها أو التعديل عليها[٦٤].

وفي ذات الاتجاه سار المشرع الإماراتي الاتحادي في القانون الخاص بشأن مكافحة جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢، إذا عاقب بالحبس والغرامة التي لا تقل عن مئة الف درهم ولا تزيد على ثلاثمائة الف درهم أو بإحدى هاتين العقوبتين على الدخول إلى موقع أو نظام إلكتروني أو شبكة معلوماتية بدون تصريح او بتجاوز حدود التصريح أو البقاء فيه بصورة غير مشروعة[٦٥]، كما شدد على الجاني وجعل العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مئة وخمسين الف درهم ولا تتجاوز سبعمائة وخمسون الف درهم أو بإحدى هاتين العقوبتين اذا ترتب على الدخول أو البقاء إلغاء أو حذف أو تدمير البيانات أو المعلومات[٦٦].

كم عاقب بالحبس والغرامة التي لا تقل عن مئة الف درهم ولا تتجاوز ثلاثمائة الف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى الشبكة المعلوماتية او موقع او نظام معلومات إلكترونية[٦٧].

فيما عاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تتجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين على إدخال برنامج إلكتروني بصورة عمدية إلى الشبكة المعلوماتية، او إلى نظام معلوماتي أو إحدى وسائل تقنية المعلومات وترتب على ذلك إيقافها عن العمل أو تعطيلها أو تدميرها او مسح او حذف او إتلاف البرنامج او النظام او الموقع الإلكتروني أو البيانات أو المعلومات، فإذا لم تتحقق النتيجة تكون العقوبة السجن والغرامة التي لا تتجاوز خمسمائة الف درهم او احدى هاتين العقوبتين.

فيما جعل العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا كان القصد من الفعل اغراق البريد الالكتروني بالرسائل وايقافه عن العمل او تعطيله او اتلاف محتوياته[٦٨].

اما المشرع العراقي فقد رتب المسؤولية الجزائية بموجب قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل على كل من عطل عمداً وسيلة من وسائل الاتصال السلكية او اللاسلكية المخصصة للمنفعة العامة او قطع او اتلف شيئاً من اسلاكها او اجهزتها، وعاقب على ذلك بالسجن مدة لا تزيد على سبع سنوات او بالحبس[٦٩]، وهو بهذا قد كفل حماية منشآت الاتصالات ومنها الشبكة المعلوماتية من الاعتداء بإتلافها أو إلحاق الضرر بها دون المعلومات المعالجة الياً.

كما أنه قد ضمن مشروع قانون جرائم المعلوماتية النصوص التي رتبت المسؤولية الجزائية على إتلاف المعلومات وبما يضمن عدم انتهاك تكامليتها او سلامتها إذا عاقب بالسجن المؤبد و بالغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار كل من استخدم عمداً أجهزة الحاسوب وشبكة المعلومات بقصد اتلاف أو تعييب او اعاقة أجهزة أو أنظمة او برامج او شبكة المعلومات العائدة للجهات الأمنية او العسكرية او الاستخباراتية إذا كان من شان ذلك المساس بأمن الدولة الداخلي او الخارجي او تعريضهما للخطر[٧٠].

وجعل العقوبة السجن المؤبد أو المؤقت والغرامة التي لا تقل عن خمسة وعشرين مليون دينار ولا تزيد على خمسين مليون دينار إذا كان الاستخدام بقصد إتلاف أو تعطيل أو تعييب أو إعاقة أو الأضرار بأنظمة أو أجهزة الحاسوب او شبكة المعلومات التابعة لدوائر الدولة أو المساس بنظامها او البنى التحتية لها(٧١).

وكذلك عاقب بالحبس مدة لا تزيد على ثلاث سنوات او الغرامة التي لا تقل عن عشرة ملايين دينار ولا تزيد على خمسة عشر مليون دينار كل من اتلف او عيب او عطل سندا أو بطاقة إلكترونية مثبتة لدين أو تصرف أو أية حقوق مالية أو معنوية أو أي محرر إلكتروني يستخدم لإثبات الحقوق(٧٢).

فيما عاقب بالحبس مدة لا تقل عن ثلاث سنوات والغرامة التي لا تقل عن خمسة عشر مليون دينار ولا تزيد على خمسة وعشرين مليون دينار أو بإحدى هاتين العقوبتين كل من عطل أجهزة الحاسوب وبرامجه وشبكات المعلومات المخصصة للمنفعة العامة أو تلفها أو اعاق عملها(٧٣).

واخيراً عاقب بالحبس مدةً لا تزيد على ثلاثة اشهر او الغرامة التي لا تقل مليونين دينار ولا تزيد على خمسة ملايين دينار كل شخص عهدت اليه مهمة تشغيل او الاشراف على جهاز الحاسوب فتسبب عمداً في اتلاف او تعطيل او اعاقة او تعييب اجهزة الحاسوب او انظمته او برامجه او شبكاته وما في حكمها(٧٤).

ومما تقدم يمكن القول بأن المشرع العراقي في مشروع قانون جرائم المعلوماتية قد عاقب على مختلف صور الانتهاك التي يمكن أن تلحق بتكاملية المعلومات وسلامتها، وحدد لذلك صوراً أربع هي الإتلاف والتعييب والتعطيل والإعاقة، وان تحقق هذه النتائج أو أحدها بالفعل يكفي للقول بتحقق المسؤولية الجزائية عنها ، كما أنه لم يحدد وسائل معينة يتم بها الانتهاك، مما يعني أن النصوص تتسع لتشمل استخدم الجاني لكافة الطرق الفنية والتقنية لأتلاف المعلومات بما في ذلك استخدام البرامج الخبيثة كالفيروسات وبرامج الدودة والقنابل المعلوماتية. ..الخ، فضلا عن ذلك فأن العقاب عليها لم يرتبط بالدخول غير المصرح به إلى الحاسب الآلي او الى اي نظام

معلوماتي، ومع ذلك فإننا نقترح على المشرع العراقي وأسوةً بما ذهب إليه المشرع الإماراتي الاتحادي في المادة (١٠) من قانون مكافحة جرائم تقنية المعلومات رقم ٥ لسنة ٢٠١٢، ايراد نص خاص يتم من خلاله تجريم أفعال الانتهاك لسلامة المعلومات وتكامليتها التي تتم عن طريق استخدام الجاني للبرامج الخبيثة ، وكذلك تلك التي يكون القصد منها إغراق موقع على الشبكة المعلوماتية او نظام معلوماتي بالرسائل الإلكترونية التي تؤدي الى إيقافه عن العمل أو تعطيله او إتلاف محتوياته وذلك لسهولة ارتكاب هذه الأفعال وانتشارها على نطاق واسع، فضلا عن جسامة الأضرار التي تترتب عليها.

الخاتمة

بعد أن انتهينا من بحثنا الموسوم المسؤولية الجزائية الناشئة عن انتهاك أمن المعلومات فأننا قد خرجنا بمجموعة من الاستنتاجات والتوصيات ندرجها كالآتي:-

أولا : الاستنتاجات

١- إن أمن المعلومات كمصطلح يرتبط بمفهوم الأمن المعلوماتي الذي يعني ضرورة إحساس أفراد المجتمع بعدم وجود إي شكل من أشكال التهديدات لبنى المؤسسات المعلوماتية، وضرورة اتخاذ الاحتياطات كافة للتأهب والعمل الفعلي لمواجهة هذه التهديدات، سواء أكان مصدرها داخليا أم خارجيا.

٢- إن أمن المعلومات يقتضي حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها من التجهيزات الحاسوبية وغير الحاسوبية المتصلة بها بإتباع إجراءات وقائية محددة تكفل المحافظة عليها وحمايتها من الأخطار التي قد تتعرض لها، سواء أكان ذلك من حيث الأمن المادي لمراكز المعلومات أم من حيث امن البرمجيات أم من حيث الأفراد العاملين في مراكز المعلومات.

٣- يحتل الحفاظ على امن المعلومات بعناصره الرئيسية المذكورة في البحث أهمية كبيرة في الواقع العملي نتيجة لازدياد اعتماد الدول والمؤسسات الرسمية وغير الرسمية والأفراد في تعاملاتهم على المعلومات الالكترونية.

ثانيا : التوصيات

١- استحداث أقسام أو وحدات إدارية مستقلة في دوائر الدولة ومؤسساتها المختلفة تتولى مهمة اتخاذ الإجراءات اللازمة لحماية المعلومات الالكترونية والمحافظة على أمنها، ورفدها بالكوادر المدربة والمتخصصة في هذا المجال.

٢- عقد الندوات وورش العمل في دوائر الدولة ومؤسساتها المختلفة لتعريف الموظفين والعاملين فيها بضرورة المحافظة على امن المعلومات وسلامة الحواسيب

وملحقاتها، ومدى أهمية المعلومات وجسامة الأضرار التي تترتب على الاعتداءات غير المشروعة عليها أو انتهاك أمنها.

٣- نقترح على المشرع العراقي في حال إصدار قانون جرائم المعلوماتية ما يأتي :

أ- تعديل نص المادتين (١٥ و ١٩/ ٣) من مشروع قانون جرائم المعلوماتية وذلك بإضافة عبارة (أو بإحدى هاتين العقوبتين) إلى نص المادتين، تطبيقا لمبدأ التفريد العقابي الذي يعد من المبادئ الأساسية التي يقوم عليها القانون الجنائي الحديث والذي يتيح للقاضي اختيار العقوبة التي تتلائم مع جسامة الجريمة وخطورة الجاني واللذان هما معياران لاختيار العقوبة كرد فعل للجريمة.

ب- تعديل نص الفقرة (أولا / ج) من المادة (١٩) من المشروع وذلك بالنص على جميع صور الاعتداءات المحققة لانتهاك الخصوصية المعلوماتية، وعدم قصر ذلك على أفعال البيع والنقل والتداول للبيانات الشخصية التي حددها المشرع لتحقق انتهاك الخصوصية.

ج- حذف عبارة (لتحقيق منفعة مادية له أو لغيره) من نص الفقرة (اولا / ج) من المادة (١٩) حيث إن تطلب هذا القصد قد يؤدي إلى إفلات العديد من مرتكبي الجريمة من العقوبة وذلك على الرغم من تحقق انتهاك الخصوصية.

د- إيراد نص خاص ضمن القانون يتضمن تجريم أفعال الانتهاك لسلامة المعلومات وتكامليتها التي تتم عن طريق استخدام الجاني للبرامج الخبيثة ، وكذلك تلك التي يكون القصد منها إغراق موقع على الشبكة المعلوماتية أو أي نظام معلوماتي بالرسائل الإلكترونية التي تؤدي إلى إيقافه عن العمل أو تعطيله أو إتلاف محتوياته وذلك لسهولة ارتكاب هذه الأفعال وانتشارها على نطاق واسع، فضلا عن جسامة الأضرار التي تترتب عليها.

ولتحقيق ما ورد في الفقرتين (ب، د) أعلاه يمكن الاستئناس بما ورد في المادتين (١٠، ٢١) من القانون الإماراتي الاتحادي الخاص بشأن مكافحة

جرائم تقنية المعلومات رقم (٥) لسنه ٢٠١٢، كون المشرع الإماراتي قد قطع شوطا كبيرا في هذا الصدد.

الهوامش والمصادر

١ - يراد بالمعلومات في هذا الصدد المعلومات الإلكترونية، وهي كل حقيقة أو فكرة معقولة ذات معنى ولها قيمه مالية سواء كانت بشكل بيانات او نصوص او صور او رموز يمكن نقلها إلى الغير بشكل الكتروني، وهي على خلاف البيانات التي تعرف بأنها المعطيات المجردة التي يتم تجميعها و تصنيفها وتوصيف محتواها و اختزانها داخل الحاسب الآلي أو أي وسيلة اتصال حديثة بحيث ينتج عنها بعد تحليلها المعلومات، ومن هنا يتبين الفرق بين الاثنين إذ ان المعلومات هي المعنى المستخلص من البيانات بعد معالجتها. للتفصيل ينظر : د. السيد عبد المقصود دبيان - نظم المعلومات المحاسبية وتكنولوجيا المعلومات - الدار الجامعية - الإسكندرية - ٢٠٠٤ - ص ص ١٤-١٥ ؛ ندى محمود ذنون - المسؤولية المدنية لمورد المعلومات الإلكترونية - بحث منشور ضمن وقائع المؤتمر السنوي الثالث الذي إقامة كلية الحقوق - جامعة الموصل تحت عنوان ((التشريعات القانونية والنظم المعلوماتية / الوقائع والطموح)) للفترة من ٢٠-٢١ / نيسان / ٢٠١٠ - ص ٣٤٠-٣٤١.

٢- ينظر : د. هالة كمال أحمد - استطلاع رأي النخبة حول جرائم المعلوماتية في المجتمعات الافتراضية - بحث منشور ضمن وقائع المؤتمر السادس الذي أقامته جمعية المكتبات والمعلومات السعودية تحت عنوان ((الأمن المعلوماتي)) للفترة من٦-٧ / نيسان / ٢٠١٠ - مكتبة الملك فهد الوطنية - الرياض - ٢٠١٠ - ص ٤٢٣.

٣- ينظر : فائز جمعة النجار - نظم المعلومات الإدارية من منظور أداري - بلا مكان طبع - عمان - الأردن - ٢٠١٠ - ص ٢٦١.

٤- من الجدير بالذكر أن امن المعلومات في بنوك المعلومات يقصد به المحافظة على المعلومات من التلف والفقدان والتغيير والاطلاع عليها من الأشخاص غير المصرح لهم بذلك نظرا لأهميتها بالنسبة للجهات التي تملكها أو المستفيدة منها، ويتمثل ذلك في المحافظة على المكونات المادية (Hardware) والبرمجيات والمعلومات (Software) وحمايتها من الأخطار المذكورة أعلاه. ينظر : د. زكي حسين الوردي، د. مجبل لازم المالكي - المعلومات والمجتمع - بلا مكان طبع - بغداد - ٢٠٠٢ - ص ٦٥.

٥- ينظر : د. محمد امين أحمد الشوابكة - جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) - ط١ - دار الثقافة للنشر والتوزيع - عمان - الأردن -٢٠٠٤ - ص ١٤.

٦- هناك العديد من المخاطر التي تهدد نظم المعلومات بما في ذلك أنظمة التجارة الإلكترونية و ابرزها : أ- اختراق الأنظمة : ويتحقق ذلك بدخول شخص غير مخول إلى نظام الحاسب الآلي والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات و سرقة المعلومات السرية أو تدمير الملفات أو البرمجيات او النظام او لمجرد الاستخدام غير المشروع. ب- الاعتداء على حق التخويل من خلال قيام الشخص المخول له باستخدام النظام في غرض معين باستخدامه في غير هذا الغرض دون أن يحصل على التخويل بذلك، وهذا النوع من الأخطار قد يكون داخليا كإساءة استخدام النظام من قبل موظف المنشأة او خارجياً كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر او استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع ومن ثم القيام بأنشطة غير مشروعة. ج- زراعة نقاط الضعف وينتج هذا الخطر عن طريق اقتحام النظام من قبل شخص غير مصرح له بذلك او من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له في لزراعة مدخل ما يحقق له فيما بعد اختراق النظام، ومن أشهر الأمثلة على ذلك زراعة برنامج حصان طروادة، وهو عبارة عن برنامج يؤدي غرضاً مشروعا في الظاهر الا أنه يستخدم في الخفاء للقيام بنشاط غير مشروع. د- مراقبة الاتصالات : وعن طريقه يتمكن الشخص من الحصول على معلومات تسهل له مستقبلا اختراق النظام وذلك من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها بدون أي اختراق للحاسب الآلي .هـ- اعتراض الاتصالات ويتم من خلال اعتراض المعطيات المنقولة خلال عملية النقل وإجراء التعديلات عليها بالشكل الذي يحقق غرض الاعتداء. للتفصيل ينظر : المحامي يونس عرب – امن المعلومات وأهميتها و عناصرها و استراتيجياتها – ص ص ٢٢-٢٣ – دراسة منشورة على الموقع www.abhatoo.net.ma تاريخ الزيارة ٣٠ / ٤ / ٢٠١٩.

٧- ينظر : د. عدنان أبو عرفة وآخرون – مقدمة في تقنية المعلومات – دار جرير للنشر – عمان – الأردن – ٢٠١٠ – ص٤٠١.

٨- من الجدير بالذكر أن بناء استراتيجيات أمن المعلومات لأغراض تقليل المخاطر والتهديدات التي يمكن أن تتعرض لها الحواسيب الآلية والشبكات وبالعموم نظم المعلومات وقواعدها تعتمد على : ١ – تحديد درجة الأمن المطلوبة في مختلف المستويات التي سيتعامل معها النظام ٢ – تحديد نوع المعلومات و تصنيفها وأهميتها. ٣ – تحديد الجهات المعنية باختراق أمنية المعلومات من أشخاص أو شركات أو تقدير كفاءتهم ٤- تقدير حجم الخسائر التي يمكن أن تنتج عن الكوارث التي قد تصيب نظام المعلومات. -5 تحديد الأشخاص المسؤولين عن متابعة تطبيق نظام أمن المعلومات والسيطرة والمعالجة لأي خلل قد يحدث.

ويتم على أساسها الاهتمام بتنفيذ مجموعة من الإجراءات الأمنية منها :١ – إجراءات السيطرة الحائلة دون الوصول إلى البرمجيات

.٢– إجراءات كشف المتطفلين ومنع دخولهم إلى شبكات. ٣– تهيئة المعدات والبرمجيات المضادة للفايروسات ٤– خزن نسخة إضافية من المعلومات في مواقع أخرى ٥– التغير المستمر لكلمات السر والتشفير ٦– وضع الخطط استرجاع سريعة في حالة الكوارث والطوارئ. للتفصيل ينظر : سعد غالب ياسين – أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات – ط١ – دار المناهج – عمان – الأردن – ٢٠٠٦ – ص ٢٣١ ؛ نهاد عبد اللطيف عبدالكريم، د. خلود هادي الربيعي – امن و سرية المعلومات وأثرها على الأداء التنافسي – بحث منشور في مجلة دراسات محاسبية ومالية – المجلد الثامن – العدد٢٣ – الفصل الثاني– المعهد العالي للدراسات المحاسبية والمالية – جامعة بغداد – ٢٠١٣ – ص ٢٩٧ ؛ د. محمد دباس الحميد، د. ماركو ابراهيم نينو – حماية أنظمة المعلومات – ط١ – دار الحامد للنشر والتوزيع – عمان – الأردن – ٢٠٠٧ – ص ٣٣ .

٩– ينظر : د. محمد دباس الحميد، د. ماركو ابراهيم نينو – المصدر السابق – ص٤٢.

١٠– ينظر : سعد غالب ياسين – مصدر سابق – ص ٢٣١.

١١– ينظر : أحمد بن علي عبد الله – رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية – رسالة ماجستير – جامعة نايف العربية للعلوم الامنية – الرياض – ٢٠٠٥ – ص ٣٢.

١٢ – ينظر : د. محمد دباس الحميد، د. ماركو إبراهيم نينو– مصدر سابق – ص ٣٨.

١٣– ينظر : د. محمد دباس الحميد، د. ماركو إبراهيم نينو – المصدر السابق – ص ٤٠.

١٤– ينظر : سعد غالب ياسين – مصدر سابق – ص ٢٣٣.

١٥– ينظر : نهاد عبداللطيف عبدالكريم، د. خلود هادي الربيعي – مصدر سابق – ص ٢٩٦ ؛ احمد بن علي عبدالله – مصدر سابق– ص ٤١.

١٦– ينظر : المحامي يونس عرب – مصدر سابق – ص ص ٢–٣.

١٧– تقرير الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات النيابية العامة العربية حول (أمن المعلومات) المنعقد في الفترة ٥–٧ /٢٠١٢/٣ – بيروت – لبنان – ص٦ – منشور على الموقع الإلكتروني www.carjj.org تاريخ الزيارة ٣٠/٤/ ٢٠١٩.

١٨– ينظر : د. خالد ممدوح ابراهيم – الجرائم المعلوماتية – ط١– دار الفكر الجامعي – الاسكندرية – ٢٠٠٩ – ص ٦٦.

١٩- تقرير الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالبيانات العامة مصدر سابق – ص ٧.

٢٠- ينظر : جمال محمد عبدالله – نظم المعلومات الادارية – ط١ – دار المعتز للطباعة والنشر – عمان الأردن – ٢٠٠٥ – ص ٢٠٠.

٢١- ينظر : أحمد بن علي عبد الله – مصدر سابق – ص ص ٤٣-٤٤.

٢٢- ينظر : المحامي يونس عرب – مصدر سابق – ص ٣.

٢٣- ينظر : د. فتوح الشاذلي، أ. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون – ط٢ – منشورات الحلبي الحقوقية – بيروت – لبنان -٢٠٠٧ – ص٢٧١.

٢٤- ينظر : إبراهيم كمال إبراهيم محمد – الضوابط الشرعية والقانونية لحماية حقوق الإنسان في اتصالات الشخصية – دار الكتب القانونية – مصر – ٢٠١٠- ص ١٥٩.

٢٥- أن تحديد المقصود بالخصوصية او كما يطلق عليه (الحق في الخصوصية) لا يزال محل خلاف في الفقه بسبب نسبية ومرونة هذا المصطلح كون تحديده يتأثر بالقيم السائدة في كل مجتمع وطبيعة النظام السياسي والاجتماعي والثقافي فيه، فضلا عن اختلاف مدلوله باختلاف فروع القانون المختلفة ومع ذلك فهو ينصرف إلى عدد من المفاهيم المرتبطة والمتداخلة معا في الوقت ذاته وتشمل: ١خصوصية المعلومات Information privacy ٢- الخصوصية الجسدية أو المادية Bodily privacy ٣- خصوصية الاتصالات Tele communication privacy٤- خصوصية المكان place privacy للتفصيل ينظر : سحر حيال غانم – الحماية القانونية لأنظمة المعلومات ضمن أ طار الحق في الخصوصية – بحث منشور ضمن وقائع المؤتمر السنوي الثالث الذي إقامته كلية الحقوق – جامعة الموصل تحت عنوان ((التشريعات القانونية و النظم المعلوماتية / الوقائع والافاق)) للفترة من ٢٠-٢١ / نيسان / ٢٠١٠ – ص ص ٥٣٤ – ٥٣٥، فداء زياد حسين العبيدي – الحماية الجنائية لحق الخصوصية في الجنايات الوراثية / دراسة مقارنة – رسالة ماجستير – كلية الحقوق – جامعة الموصل – ٢٠١٧ – ص ص ٥١-٥٢.

٢٦- ينظر : د. علاء حسن الحمامي، د. سعد عبدالعزيز العاني – تكنولوجيا امنية المعلومات و أنظمة الحماية – ط١ – بلا مكان طبع – عمان – الأردن – ٢٠٠٧ – ص٢١.

٢٧- ينظر : د. زكي حسين الوردي، د. مجيد لازم المالكي – مصدر سابق – ص ٥٢.

٢٨- ينظر : د. محمد دباس الحميد، د. ماركو إبراهيم نينو – مصدر سابق – ص ٧٩ ؛ محمود أحمد عبابنة – جرائم الحاسوب و أبعادها الدولية – دار الثقافة للنشر والتوزيع – عمان – الأردن – ٢٠٠٥ – ص ٧٣.

٢٩ – يراجع : المادة (٤١) من قانون انتهاك الخصوصية المعلوماتية والحرية العامة الفرنسي.

٣٠- يراجع : المادتين (٤٢،٤٣) من قانون انتهاك الخصوصية المعلوماتية والحرية العامة الفرنسي.

٣١- يراجع : المادة (٤٤) من قانون انتهاك الخصوصية المعلوماتية والحرية العامة الفرنسي.

٣٢- يراجع : نص المادة (٧٣) من قانون تنظيم الاتصالات المصري .

٣٣- يراجع : نص المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٣٤- يراجع : نص المادة (٢١) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٣٥- يراجع : نص المادة (٤٣٨) من قانون العقوبات العراقي.

٣٦- عدل مبلغ الغرامة في جرائم الجنح واصبح مبلغ لا يقل عن (٢٠٠,٠٠١) مئتي الف وواحد دينار ولا يزيد عن (١,٠٠٠,٠٠٠) مليون دينار بموجب قانون تعديل الغرامات الوارد في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل والقوانين الخاصة الاخرى رقم ٦ لسنة ٢٠٠٨ والذي نشر في الوقائع العراقية بالعدد ٤١٤٩ في ٤/٥/ ٢٠١٠.

٣٧- تمت القراءة الأولى لمشروع قانون جرائم المعلوماتية في مجلس النواب العراقي في جلسة يوم السبت الموافق ١٢ / ١ / ٢٠١٩، وثم نشر مسودة القانون في الموقع الإلكتروني www.alsumaria.tv.

٣٨- يرجع : نص المادة (١٥/ اولا وثانيا) من مشروع قانون جرائم المعلوماتية العراقي.

٣٩- يراجع : نص المادة (١٩/اولاً/ج) من مشروع قانون جرائم المعلوماتية العراقي .

٤٠- يراجع : نص المادة (١٩ / ثانياً) من مشروع قانون جرائم المعلوماتية العراقي.

٤١- ينظر : زكي حسين الوردي و د. مجبل لازم المالكي – مصدر سابق – ص ٧٢.

٤٢- ينظر : د. أسامة فايد – المسؤولية الجنائية الطبيب عن إفشاء سر مهنته – دار النهضة العربية – القاهرة – ١٩٨٦ – ص ٣، نقلا عن د. فتوح الشاذلي و عفيفي كامل عفيفي– مصدرسابق – ص ٣٠١.

٤٣- ينظر : د. محمد دباس الحميد، د. ماركو براهيم نينو – مصدر سابق – ص ٩٧.

٤٤- ينظر : نائلة عادل محمد فريد قورة – جرائم الحاسب الآلي الاقتصادية – منشورات الحلبي الحقوقية – بيروت – لبنان –٢٠٠٥، ص ١١٤.

٤٥- ينظر : د. علي احمد عبد الزعبي – حق الخصوصية في القانون الجنائي – ط١ – المؤسسة الحديثة للكتاب – بيروت – لبنان – ٢٠٠٦ – ص ١٨٩.

٤٦- ينظر : د. جميل عبد الباقي الصغير – الجوانب الإجرائية الجرائم المتعلقة بالأنترنت – دار النهضة العربية – القاهرة – ٢٠٠١ – ص ١١.

٤٧- يراجع : المادة (٧٣) من قانون تنظيم الاتصالات المصري.

٤٨- يراجع : المادة (٧٥) من قانون تنظيم الاتصالات المصري.

٤٩- يقصد بالسرية وفقا للمشرع الإماراتي، أي معلومات غير مصرح للغير بالاطلاع عليها او إفشائها إلا بإذن مسبق ممن يملك هذا الأذن. يراجع : المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم ٥ لسنة ٢٠١٢ الخاصة بالمصطلحات.

٥٠- يراجع : المادة (٤) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

٥١- يراجع : المادة (١٥) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

٥٢- يراجع : المادة (٢٢) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

٥٣- يراجع : هامش رقم (٤) من الصفحة (١٥) من البحث بخصوص عقوبة الغرامة.

٥٤- يراجع : المادة (٤٣٧) من قانون العقوبات العراقي.

٥٥- يراجع : المادة (١٣/اولا/ ج) من مشروع قانون جرائم المعلوماتية العراقي.

٥٦- يراجع : المادة (١٩/اولا / أ، ب) من مشروع قانون جرائم المعلوماتية العراقي.

٥٧- يراجع : المادة (١٩ / ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.

٥٨ – يقصد بالأتلاف المعلوماتي التعدي على البرامج والمعلومات المخزنة والمتبادلة عن طريق الشبكة المعلوماتية بمحوها أو تعديلها أو تغيير نتائجها أو تشويشها على نحو يجعلها غير صالحة للاستعمال. ينظر : د. خالد ممدوح إبراهيم – فن التحقق الجنائي في الجرائم الإلكترونية – ط١ – دار الفكر الجامعي – الإسكندرية – ٢٠١٠ – ص٤٢١.

٥٩- ينظر : د. حسين بن سعيد الغافري – السياسة الجنائية في مواجهة جرائم الإنترنت / دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠٩ – ص٤٢١.

٦٠- ينظر : د.حسين بن سعيد الغافري – المصدر السابق – ص ٤٢١.

٦١- ينظر : د.خالد ممدوح إبراهيم– فن التحقيق في الجرائم الالكترونية – مصدر سابق – ص٤١٩–٤٢٠.

٦٢ – يراجع : المادة (١/٣٢٣) من قانون العقوبات الفرنسي.

٦٣ – يراجع : المادة (٢/٣٢٣) من قانون العقوبات الفرنسي.

٦٤ – يراجع : المادة (٣/٣٢٣) من قانون العقوبات الفرنسي.

٦٥ – يراجع : المادة (١/٢) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٦٦– يراجع : المادة (٢/٢) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٦٧ – يراجع : المادة (٨) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٦٨ – يراجع : المادة (١٠) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

٦٩ – يراجع : المادة (٣٦١) من قانون العقوبات العراقي.

٧٠– يراجع : المادة (٣/ اولا /ج) من مشروع قانون جرائم المعلوماتية العراقي.

٧١ – يراجع : المادة (٦/ ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.

٧٢ – يراجع : المادة (١٤/ اولا/ أ) من مشروع قانون جرائم المعلوماتية العراقي.

٧٣– يراجع : المادة (١٤/ ثانيا) من مشروع قانون جرائم المعلوماتية العراقي.

٧٤ – يراجع : المادة (١٤/ثالثا/ أ) من مشروع قانون جرائم المعلوماتية العراقي.