ULUM ISLAMIYYAH | VOL. 22 | DECEMBER 2017 | Pp 89-102
ISSN 1675 – 5936 | E-ISSN 2289 - 4799
www.uijournal.usim.edu.my

Manuscript received date: 13th January 2017
Manuscript acceptance date: 6th November 2017
Manuscript publication date: 1st December 2017

أمن المعلومات في المملكة العربية السعودية

[The Information Security In Kingdom Of Saudi Arabia]

IBRAHIM SULAIMAN AL-HARBI
King Fahd Security College, 11461 Riyadh, Kingdom of Saudi Arabia
E-mail: asdh555@yahoo.com

الملخص

يعد أمن المعلومات في عصرنا الحالي الركيزة الأساسية للأمن الوطني، ومع الحاجة للخدمات الإلكترونية الحديثة، ودخولها في شتى المجالات، وتطورها المتسارع، فإن الفائدة منها لا تكون بالشكل المطلوب –بل قد تنعكس سلبا– ما لم يتوافر مع ذلك حماية لها، وهو ما يسمى بأمن المعلومات. يعد هذا البحث مساهمة في بيان المراد بأمن المعلومات وعلاقته بالأمن الوطني والعناصر الأساسية لأمن المعلومات ومهدداته والوقاية من جرائم أمن المعلومات عن طريق بيان حماية أمن المعلومات في المملكة العربية السعودية. استخدم الباحث الدراسة الوصفية وذلك باتباع المنهج التحليلي من خلال جمع المعلومات المتعلقة بكل موضوع والمواد النظامية ذات العلاقة وتحليلها. وينقسم البحث إلى أربعة فصول: الفصل الأول وهو موضوع البحث، والفصل الثاني وهو مفهوم أمن المعلومات وعلاقته بالأمن الوطني، والفصل الثالث وهو العناصر الأساسية لأمن المعلومات ومهدداته، والفصل الرابع وهو الوقاية من جرائم أمن المعلومات ثم نتائج الدراسة والتوصيات.

الكلمات المفتاحية: أمن المعلومات، المملكة العربية السعودية، الأمن الوطني

ABSTRACT

The information security in our time is the fundamental national security substrate, especially with the need for modern electronic services in various fields, however, the need for a protection of her which is called information security is considered most important topic. This research is contribution as a statement of information security and its relationship to national security, explanation of the basic elements of information security and its threats, analyses the prevention of information security crimes by a statement varieties of information security criminals and then release the protection of information security in the Kingdom of Saudi Arabia. The researcher has used the descriptive study by following the analytical method by collecting information on each topic and related law then analyzed them. The research has divided into four chapters: the first chapter which is the subject of research, and the second chapter is the concept of information security and its relationship to national security, the third chapter which the basic elements of information security and its threats, the fourth chapter is the prevention of information security crimes، then the results of the study and recommendations.

Keywords: information security, Kingdom of Saudi Arabia, national security

مقدمة

يعد الأمن أهم عنصر من عناصر الحياة وقاعدة من قواعد صلاح الدنيا، كما ذكر الماوري بأن قواعد صلاح الدنيا وانتظام عمرانها في ستة أمور (دين متبع، وسلطان قاهر – دولة قوية – وعدل شامل، وأمن عام، وخصب دائم، وأمل فسيح) فجعل "الأمن العام" القاعدة الرابعة من قواعد صلاح الدنيا وانتظام العمران، فالأمن العام تطمئن إليه النفوس، وتنتشر به الهمم، ويسكن فيه البريء، ويأنس به الضعيف، فليس لخائف راحة، ولا لحاذر طمأنينة، وقد قال بعض الحكماء: الأمن أهنأ عيش، والعدل أقوى جيش، لأن الخوف يقبض الناس عن مصالحهم، ويحجزهم عن تصرفهم، ويكفهم عن أسباب المواد التي بها قِوام أوَدِهم، وانتظام جملتهم (Al-Mawardi, 1987).

وتعد المعلومة من أهم ممتلكات الانسان على مر العصور، فالقدماء قاموا بنقش بياناتهم الشخصية ورصدوا معلوماتهم وقيدوها فيما توفر لديهم من إمكانات كان من أشهرها الحجارة، وتطور الأمر إلى تدوينها على الأوراق، وصولاً الى عصرنا الحديث على الورق الذي تعددت أشكاله، ثم الأقراص الإلكترونية الممغنطة.

وقد صاحب ذلك، إضافة للتطور الذي عرفه المجتمع الدولي في مجال تكنولوجيا الاتصالات، تطور كبير في مجال شبكات الاتصال، فأصبحت من أهم وسائل المعاملات على المستوى الدولي، مما أضحى من الصعوبة بمكان أن يستغنى عنها، ولعل من أهم الشبكات الاتصالية التي تأخذ حيزاً كبيراً في الحياة اليومية لمعاملات الافراد والدول على حد سواء شبكة الانترنت (As-Sanbuti, 2001). فهناك الآن الملايين من أجهزة الحاسب الآلي، وملايين الأميال من الأسلاك الضوئية والألياف التي تلتف حول العالم لتصله ببعض في أقل من الثانية. إلا إن تلك النقلة النوعية في حياة البشر لم تخل من السلبية، فبقدر ما فيها من النفع والفائدة لم تكن بمنأى عن الاستعمالات غير الصحيحة بل والمجرمة (Hasbu, 2000). إضافة لما يوجد من فجوة عميقة لدى الكثير من الدول فيما بين هذا التطور التقني والمعلوماتي من جهة، وبين التشريعات المنظمة لهذا الامر.

بناء على ما سبق وغيره؛ ظهر ما يسمي بالجرائم الإلكترونية أو السيبرانية التي أصبحت تتخذ من وسائل التقنيات الحديثة هدفاً ووسيلة فاعلة لارتكاب هذا النوع من الإجرام المعاصر؛ مما ترتب عليه صعوبات قانونية بالغة في تطبيق قواعد القانون الجنائي التقليدي على هذه النوازل القانونية المستحدثة؛ خاصة لما تتميز به هذه الجرائم من سرعة التنفيذ وسهولة إخفاءها والقدرة على محو آثارها وتعدد صورها وصعوبة ضبط الدليل الرقمي.

هذا البحث عن أمن المعلومات، سيكون في أربعة فصول، يخصَّص الأول لبحث مفهوم أمن المعلومات، في حين يخصَّص الفصل الثاني لبحث العلاقة بين أمن المعلومات والأمن الوطني، أما الفصل الثالث فيُفرد لمسألة العناصر الأساسية لنظام أمن المعلومات والفصل الرابع لدراسة مهدداته سواء وسائل تهديد أمن المعلومات أو طرق الوقاية وحماية الأمن السيبراني في المملكة العربية السعودية.

مشكلة الدراسة

تكمن مشكلة الدراسة في التعرف على مفهوم أمن المعلومات والعلاقة بينه والأمن الوطني وبيان العناصر الأساسية لأمن المعلومات ودراسة مهدداته وطرق الوقاية من جرائم المعلومات في المملكة العربية السعودية. أهمية الدراسة: تكمن أهمية الدراسة في حداثة موضوعها وهو أمن المعلومات وتطوره المستمر تبعا لتطور الأجهزة المعلوماتية، فضلا عن خصوصية الجريمة والمجرم في هذا الموضوع وما لذلك من أهمية على الفرد والمجتمع والدولة.

تهدف الدراسة إلى: بيان المراد بلفظة الأمن والمعلومات ومفهوم مصطلح أمن المعلومات؛ بيان العناصر الأساسية لأمن المعلومات؛ استقصاء أهم جرائم الاعتداء على أمن المعلومات ووسائل تهديد أمن المعلومات؛ معرفة آلية حماية أمن المعلومات في المملكة العربية السعودية.

مفهوم أمن المعلومات وعلاقته بالأمن الوطني

الأمن: هو مصدر من أمن يأمن أمناً؛ فهو آمن، بمعنى اطمأن ولم يخف، والأمن يعني الاستقرار والاطمئنان، والأمان والأمانة بمعنى واحد، فالأمن ضد الخوف وفعله أَمِنَ، والأمانة ضد الخيانة وفعله أَمُنَ، والإيمان ضد الكفر وفعله آمَنَ وهو بمعنى التصديق وضده التكذيب (Ibn Manzur, 2000). قال ابن فارس: "الهمزة والميم والنون أصلان متقاربان: أحدهما الأمانة التي هي ضد الخيانة، ومعناها سكون القلب، والآخر التصديق (Ahmad, 1999). وجاء في القرآن والسنة لفظ الأمن بهذا المعنى قال تعالى "الذي أطعمهم من جوع وآمَنَهم من خوف" سورة قريش :4. وقال تعالى: (وَضَرَبَ اللّهُ مَثَلاً قَرْيَةً كَانَتْ آمِنَةً مُّطْمَئِنَّةً يَأْتِيهَا رِزْقُهَا رَغَدًا مِّن كُلِّ مَكَانٍ فَكَفَرَتْ بِأَنْعُمِ اللّهِ فَأَذَاقَهَا اللّهُ لِبَاسَ الْجُوعِ وَالْخَوْفِ بِمَا كَانُواْ يَصْنَعُونَ) سورة النحل:112. وقد أخرج الترمذي في سننه عن سلمة بن عبيد الله بن مُحصِنٍ الخطمي عن أبيه – وكانت له صحبة – قال: قال رسول اللَّه صلى الله عليه وسلم: "مَنْ أصبح منكم آمناً في سربه، معافى في جسده، عنده قوت يومه، فكأنَّما حيزت له الدنيا" وهو من حسنه الألباني برقم1913.

أما معناه الاصطلاحي لا يختلف عن المعنى اللغوي وهو عدم الخوف. إلا أنه نظرا لشمولية هذا اللفظ (الأمن) وتعدد فروعه ولتنوع النظرة واختلاف التصور لدى العلماء والباحثين فقد تعددت تعاريفه لدى العلماء؛ فهناك من عرفه باعتبار نتيجته وما يؤول إليه فقال الأمن هو:" عدم توقع مكروه في الزمن الآتي" (Al-Jurjani, 1988) أو هو "إحساس بالطمأنينة يشعر به الفرد، سواء بسبب غياب الأخطار التي تهدد وجوده، أو نتيجة لامتلاكه الوسائل الكفيلة بمواجهة تلك الأخطار حال ظهورها" (Zuhrah, 1991) وهناك من عرفه باعتبار وصفه فقال الأمن هو: "تلك الحالة من الاستقرار التي يجب أن تشمل المنطقة بعيدا عن أي تهديد سواء من الداخل أو الخارج" (Al-Baz, 1978) وهناك من عرفه باعتبار وسائل تحقيقه فقال الأمن هو: "الإجراءات التي تتخذها الدولة في حدود طاقاتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة المتغيرات الدولية" (Huwaidi, 1975) ومع هذا التعدد لتلك التعاريف إلا أنه يلاحظ أن هناك العديد من التعريفات تحدثت عن الأمن باعتبار الفعل المؤدي إليه وهذا من الناحية اللغوية لا يستقيم لأن لفظة (الأمن) ليست فعلا وإنما هي مصدر.

والمعلومات جمع معلومة وهي مشتقة من مادة "علم" ولها العديد من المعاني والمشتقات ومنها العلم والمعرفة والدراية والإدراك والوعي. (Ibn Manzur, 2000). نظرا لشمولية هذه

الكلمة لمعاني عديده يصعب حصرها فإنه لا يوجد تعريف جامع مانع لهذه الكلمة وإنما هي تدور حول معناها اللغوي ثم يتم تخصيصها بالعلم مجال البحث لذا نجد العديد من التعريفات التي يغلب عليها التأثر بما لدى صاحب التعريف من خلفية علمية في التخصص تكون منطلقا له في تعريفه وهذا ينطبق أيضا على ترجمة الكلمة وهي باللغة الإنجليزية على سبيل المثال تعني (information) نجد أن لها أكثر من أربعمائة تعريف وفي النتيجة تم التوصل إلى أن لابد من ذكر الفن أو العلم المراد تعريفه للوصول للمعنى الصحيح (Zhang Yuexiao, 1988). التالي فتعريف هذه الكلمة بشكل دقيق يتطلب ربطها بالموضوع العلمي أو الاجتماعي المصطلح عليه عند أهل فن معين فمثلا في الحاسب الآلي نجد أن المعلومات تعرف بأنها البيانات المترابطة والواضحة بعد معالجتها بالحاسب الآلي لتعبر عن معاني مفيدة (Al-Qasim, 2005). وفي مجال المكتبات تعرف المعلومات بأنها الحقائق الثابتة التي يتم جمعها والحصول عليها من اشخاص او وثائق او سجلات (Al-Asaf, 2000) وفي مجال بحثنا (أمن المعلومات) تعرف المعلومات بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنشطة الالكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة" (Salamah, 2002). وهذا ما يقودنا لتعريف هذه الكلمة تحت مصطلح أمن المعلومات.

ويقصد بأمن المعلومات كمصطلح ذلك النوع من الاهتمام الأمني المتعلق بالمعلومات ذات الصلة بالحاسوب أو بالشبكة الإلكترونية (الإنترنت) ولذا يسمى بأمن الحاسوب (الكمبيوتر) أحيانا كما يسمى أيضا بأمن الإنترنت أو الأمن السيبراني وهي مأخوذة من كلمة سايبر (syber) بمعنى أمن الإنترنت. وعرف أمن المعلومات بعدة تعاريف منها أنه "مجموعة الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها" (As-Sharman, 2000). ومنها أنه "ضمان الحفظ وعدم الاتلاف، أو التغيير، أو التعديل بالحذف والإضافة للمعلومات المخزنة، او المنقولة عبر الشبكة" (Abu Maghaid, 2004).

وعرفه الاتحاد الدولي للاتصالات كما جاء في توصيته ITU-T X.1205الفقرة رقم 5.2.3 في التقرير النهائي للاتحاد الدولي للاتصالات تحت عنوان تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن

السيبراني، المسألة 221/1 بأنه "مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة والمستعملين" وبالاطلاع على تعريفات مصطلح أمن المعلومات نلحظ أنها تتحدث عن بعض جوانبه دون أن تستوعب كل ما يدخل في هذا المصطلح الواسع من مفردات لا زالت تتوسع بتقدم التكنولوجيا الحديثة وتطور الجريمة في الوقت الحاضر. فأمن المعلومات وإن كان يطلق على وسائل تحقيقه إلا أنه بشكل عام هو عدم إساءة استعمال المعلومات عن طريق وسائل التكنولوجيا الرقمية الحديثة. فيشمل ذلك الاستخدام غير المصرح لتلك الأجهزة وما تحويه من معلومات أو سوء استعمالها.

ويعد الأمن من أهم متطلبات الحياة، فلا يمكن للإنسان أن يقوم بمتطلبات الحياة بدون الأمن، وهو مما يعين على عمارة الأرض، وقد خلق الله الخلق لعبادته كما قال تعالى (وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ) سورة الذاريات:56. ولا يتأتى القيام بالعبادة على الوجه المطلوب إلا إذا توفر الأمن، والمراد بالأمن الأمن بمعناه الشامل، فلا يتوفر الأمن بمجرد ضمان الحياة بل يشمل الأمن في المعتقد والفكر والحياة وجميع جوانب الحياة المختلفة، والأمن بمعناه المطلق الذي يستلزم عدم الخوف المطلق لا يمكن أن يتحقق في هذه الحياة وإنما في دار النعيم، كما قال تعالى (ادْخُلُوهَا بِسَلَامٍ آمِنِينَ) سورة الحجر: 46. ففي الجنة لا خوف ولا فزع، وقد جاء في السنة النبوية ما يؤكد أهمية الأمن لحياة الإنسان. قال صلى الله عليه وسلم (من أصبح منكم آمنا في سربه، معافى في جسده، عنده قوت يومه، فكأنما حيزت له الدنيا) رواه الترمذي: 2643. وقد وضعت الشريعة الإسلامية الحدود والقصاص والتعازير لتوفير العيش في مجتمع آمن، وكفلت خصوصية الفرد في حياته، فله ولمسكنه حرمه ولا يجوز التجسس عليه كما قال تعالى (يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ) سورة النور:27. وقال تعالى (يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ) سورة الحجرات: 12. وذلك تأكيدا على أهمية الأمن للشخص في نفسه وحياته الخاصة.

ووضعت الشريعة الإسلامية الضرورات الخمس: العقل، الدين، النفس، النسل، والمال موضع الاهتمام، فلا يجوز المساس بها بل يجب حفظها، فمهما تطورت وسائل التقنية؛ فإن الشريعة الإسلامية لها فضل السبق في تجريم ما يسمى بالجرائم المعلوماتية التي تستهدف أحد الضروريات الخمس المصونة في الشريعة الإسلامية،

العلاقة بين أمن المعلومات والأمن الوطني

أخذ المجتمع الدولي على عاتقه تنفيذ العديد من الخطط والبرامج التي تسعى إلى تشييد بنية معلوماتية قومية شاملة على كل المستويات، لاسيما وأن المعلومات المتاحة داخل البنية المعلوماتية تعد ركيزة من ركائز الأمن الوطني كالمعلومات العسكرية والأمنية وعندئذ يتعين تأمينها وشمولها بالحماية. ومن ذلك يتضح أن التطور الذي حدث في مجال تكنولوجيا المعلومات قد أدى إلى إعطاء الأموال المعنوية قيمة اقتصادية قد تفوق قيمة الأموال المادية. وهذا التطور هو الذي أدى بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال أو طبيعة الشيء الذي يرد عليه الحق المالي، ليصل من خلاله إلى إسباغ صفة المال على الشيء المعنوي ولجأ إلى معيار القيمة الاقتصادية وذلك على أساس أن القانون إذا لم يسبغ صفة المال على الأشياء ذات القيمة الاقتصادية يعد قانوناً منفصلاً عن الواقع (Latif, 2006) وبالتالي يمكن إسباغ صفة المال على برامج وبيانات ومعلومات الحاسب الآلي على أساس مالها من قيمة اقتصادية، وجعل الحماية الجنائية لهذه البرامج والمعلومات أمراً حتمياً ومسلماً به (As-Shazili, 2003). ولذلك لابد من القاء الضوء على مدى الارتباط بين أمن المعلومات والأمن الوطني، وذلك على النحو التالي:

الارتباط بين أمن المعلومات والأمن الوطني

يثير موضوع أمن المعلومات العديد من القضايا القانونية الهامة والتي تؤثر على الحياة العامة والخاصة. فأمن المعلومات يؤثر على حقوق الملكية الفكرية، والسرية والخصوصية، وحماية البيانات، والحق في حرمة الحياة الخاصة. كما أن أمن المعلومات والتكنولوجيا الحديثة قد استحدثت العديد من الجرائم مثل الجريمة المعلوماتية، والإرهاب الالكتروني، والاحتيال المالي، والسرقة، والقرصنة، والعديد من الجرائم الاخرى التي ترتكب داخل البيئة الإلكترونية (Sultan, 2012). والمعلومات تصلح أن تكون محلاً للجريمة، فهي المجال الذي يرد عليه السلوك أو الفعل او النشاط الاجرامي في الجريمة المعلوماتية والذي يختلف عنه في الجريمة التقليدية بأنواعها المختلفة، سواء كانت واقعة على النفس، أو المال، والتي نظمتها جميع التشريعات التقليدية في الدول المختلفة من خلال قوانين العقوبات.

نظرًا لما يتعرض له بعض الأفراد والجهات الحكومية والخاصة في المملكة من خطورة التعامل في مجال أمن المعلومات وانعكاس ذلك على الجانب الاقتصادي والمعرفي وما أصبحت تمثله الجرائم المعلوماتية ومخاطر الانترنت وشبكات التواصل الاجتماعي على أفراد المجتمع والأسرة من هاجس مؤرق، إما بسبب عدم تصور البعض لمدى الخطورة، أو عدم الإلمام بكيفية حماية أجهزتنا وشبكاتنا، أو ارتكابنا أخطاء عفوية بإتاحة بياناتنا الشخصية على صفحات التواصل الاجتماعي، ولأن هذه التقنيات أصبحت ضرورة ملحّة من ضروريات حياتنا اليومية. فإن أمن المعلومات ترتبط مباشرة بالأمن الوطني، ولذلك تسعى الدول جاهدة في سبيل حفاظها على أمنها الوطني للاهتمام بأمن المعلومات، فنجد المركز الوطني للأمن الإلكتروني بوزارة الداخلية في المملكة العربية السعودية ومركز سلطان بن عبد العزيز للعلوم والتقنية "سايتك" أطلقوا أول مشروع وطني للتوعية بأمن المعلومات السعودي والذي يهدف إلى الحد من المخاطر الإلكترونية، مستهدفين بذلك توعية القطاع الحكومي والقطاع الخاص وجميع أفراد المجتمع.

حيث يتضمن المشروع ملتقى لعدد من الخبراء والمهتمين وعدد من المحاضرات وورش العمل ومعارض تفاعلية مبتكرة مصاحب موجه للأسر لتوعيتهم عن مخاطر الانترنت –وتوعيتهم بأفضل الممارسات المتبعة لأمن المعلومات– بطرق تفاعلية حديثة بالتعاون مع الجهات الحكومية والخاصة – البرنامج الوطني لأمن المعلومات، 2006. إضافة لما سيأتي بيانه من جهود في الوقاية من الجرائم المعلوماتية.

بناء على ما سبق فتحقيق تقدم ملموس في قضية أمن المعلومات عالميا أو عربيا لن يتم إلا بتغيير المنهج القائم حاليا والذي يتعامل مع القضية باعتبارها قضية "تقنية بحتة" تقع مسؤوليتها على الفنيين والمختصين في علوم الحاسب وتأمين الشبكات، والانتقال للأخذ بالمنهج الذي يعتبر أمن المعلومات ركيزة أساسية من ركائز الأمن الوطني الشامل، ومن ثم يتعين رفعها من مستوى التعامل "الفني والتقني"، إلى مستوى التعامل السياسي والاستراتيجي، وألا تترك للتعامل العفوي غير الخاضع لاستراتيجية أو سياسة وطنية عامة ترشد مساره (Amir, 2006).

العناصر الأساسية لأمن المعلومات ومهدداته

العناصر الأساسية لأمن المعلومات

إن الاستخدام المكثف لوسائل التقنيات الحديثة نتج عنه أن أصبحت عملية التنقل عبر الشبكات المعلوماتية سواء المحلية او الدولية من الأمور اليومية المعتادة في عصرنا الحالي وذلك لتأثيرها الواضح في تلبية احتياجات المستخدمين والرواد

للوازم حياتهم؛ الامر الذي أدى لتطور مفهوم أمن المعلومات. ولا شك أن هناك ارتباط وثيق بين الأمن المعلوماتي وأمن الحاسوب حيث أن المعلوماتي نتيجة منطقية لأمن الحاسوب وفي ظل تنامي ظاهرة اختراق الأمن الالكتروني وانتشار الإجرام الإلكتروني كان لا بد من اتخاذ العديد من الوسائل الدفاعية والوقائية والفنية للوقاية من الهجمات الواقعة على المعلومات والبيانات الالكترونية. لقد أصبحت مشكلة حماية البيانات أو

المعلومات والحفاظ عليها من السرقة أو التلاعب او الاختراق غير المشروع موضع اهتمام العاملين والباحثين وهذا يتطلب دراسة جميع المجالات الفنية والمادية والبشرية والقانونية التي تحمل في طياتها إجراءات حماية المعلومات والحد من محاولات الانتهاك او الإتلاف (Lamin, 2016).

عناصر أمن المعلومات

تتطلب المحافظة على أمن المعلومات توافر ثلاثة عناصر هي سرية المعلومات، وسلامتها وتوافرها وذلك على النحو التالي:

سرية المعلومات

تعني ضمان حفظ المعلومات المخزنة او المنقولة عبر الشبكة وعدم الاطلاع عليها او استخدامها الا بإذن. وتهدف سرية المعلومات الى التأكد من عدم إطلاع غير المصرح لهم عليها، فضلاً عن تحديد حدود وصلاحية الاستخدام سواء كان كلي او جزئي، مع تحديد من له صلاحية التعديل أو الإدخال أو الحذف او الإضافة أو القراءة فقط من بين المصرح لهم بوجه عام.

سلامة المعلومات

تعنى ضمان عدم تغيير المعلومات المخزنة أو المنقولة، حيث يتكون عنصر سلامة المعلومات من شقين: الاول سلامة المعلومة، والثاني سلامة المصدر، فالمفهوم الصحيح لسلامة المعلومة هو عدم تغييرها بشكل غير ملائم سواء بقصد أو بدون قصد، وأنها أدخلت بشكل صحيح يعكس الظروف الحقيقية للمعلومة، أما سلامة المصدر فيقصد بها الحصول على المعلومة من مصدرها الأصلي، وتشير سلامة المعلومات بصفة عامة الى الإجراءات التي تضمن حفظ المعلومات خلال مراحل إدخالها أو نقلها بين الأجهزة والشبكات للمحافظة على سريتها وسلامتها.

توافر المعلومات

يعني ضمان بقاء المعلومات وعدم حذفها أو تدميرها، وأهم الاخطار التي تهدد أمن المعلومات:

i. رفض (منع) الخدمة: يعني الأعمال التي تعطل خدمات نظم الحاسب وشبكاته بصورة لا تمكن المصرح لهم من

ii. استخدام الحاسب الآلي والاستفادة منها والوصول الى المعلومات.

iii. فقدان القدرة على معالجة البيانات نتيجة الكوارث الطبيعية، أو الافعال العمدية (Al-Quhtani, 2008).

مهددات أمن المعلومات

تزداد التهديدات الإلكترونية يوماً بعد يوم، خصوصاً بعد أن أصبح الإنترنت جزءاً أساسياً من حياتنا اليومية. فالآثار العنيفة للإرهاب الإلكتروني لم نرها ولم نسمع دوي انفجارها بعد، ولكن مؤشرات الخطر تتصارع وترتفع الى القمة. وتقتضي دراسة مهددات الأمن السيبراني في هذا المبحث استعراضنا لما يلي:

جرائم الاعتداء على أمن المعلومات

تقع جرائم الإخلال بأمن المعلومات من خلال العاملين بالوظائف المتعلقة بالمعلومات الإلكترونية، إما بالقيام بها أو نتيجة تساهلهم، أي تكون متعمدة أو غير متعمدة، فعدم إتباع السياسات الأمنية الموضوعة لهم تعد إخلالاً بأمن المعلومات، إفشاء كلمات المرور أو عدم تطبيق متطلبة السياسة الأمنية بشأنها، أو سرقة وسائط الحفظ الخارجية نتيجة تساهل العاملين وتفريطهم، أو نسخ البيانات والبرامج، أو تشغيل الأجهزة عن طريق القرص المرن للدخول غير المرخص على الأقراص الثابتة والحصول على البيانات، أو عدم متابعة إجراءات الصيانة حتى لا تتم زراعة برامج اختراق بواسطة موظفي الصيانة والتشغيل أو الحصول على البيانات السرية خلال أعمال صيانة الأجهزة، أو الاستخدام غير القانوني لأجهزة الغير حين تراها غير مؤمنة (Al-Musnad, 2002).

تحدث المشكلة الأمنية على المعلومات الإلكترونية من خلال عدد من الطرق، منها عندما يتم اختراق المواقع من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة. حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئة حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول الى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم

وقد يتم الهجوم على الأنظمة الإلكترونية بواسطة:

i. هجوم التنصت على الرسائل: بحيث يقوم المهاجم بمراقبة الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال.

ii. هجوم الإيقاف: هذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة او البيانات من الوصول الى المستقبل وهو ما يسمي ايضاً برفض الخدمة.

iii. هجوم يعدل في محتوى الرسالة: وهنا يتدخل المهاجم بين المرسل والمستقبل وعندما تصل اليه الرسالة يقوم بتغيير محتواها ومن ثم ارسالها الى المستقبل الذي لا يكون على علم بتغيير الرسالة.

iv. الهجوم المزور او المفبرك: وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة. (Abu Saad, 2005)

ومن خلال ما عرضناه سابقاً يتضح أن الهجمات الإلكترونية التي تنال من الأمن الإلكتروني تشمل أربعة مواطن أساسية، وهي الأجهزة أو البرامج أو البيانات أو الاتصالات.

وسائل تهديد أمن المعلومات

إن جريمة الاعتداء على الأمن السيبراني أو الإلكتروني من الممكن أن ترتكب بأي وسيلة من وسائل الاعتداء أو الهجوم التقليدية المختلفة سواء بالحرق أو التكسير أو التفجير... الخ. وهذا النوع من الاعتداء يحدث اثراً محدوداً من الضرر، إلا إن هناك وسائل فنية حديثة يقوم بها بعض الجناة في ارتكاب هذه الجريمة والتي يتحقق معها تدميراً واسعاً خلافاً للوسائل التقليدية الأخرى، وهي كالآتي:

الاختراق: تعود سهولة اختراق أنظمة الحاسب الآلي من قبل المخترقين والوصول إلى ما تحويه من برامج وبيانات ومعلومات، إلى عدد من العوامل منها (Al-Abidi, 2012):

i. عدم اهتمام الشركات المصنعة لبرامج الحاسب الآلي بشكل كاف بتوفير الأمن والحماية لتلك البرامج والحاسبات وتركيزها بشكل كبير على رفع القدرة الوظيفية وتحسين مستوى أداء تلك البرامج والحاسبات، حتى لا تتكبد تكلفة إضافية، ومن ثم زيادة أسعار تلك البرامج والحاسبات.

ii. الزيادة الكبيرة في أعداد الحاسبات الآلية واستخدام شبكة الانترنت بما يفوق القدرة على توفير الحماية لها من جريدة الشرق الأوسط،2010/7/81م.

الفيروسات: تُعد الفيروسات من الوسائل بالغة الخطورة على الحاسب الآلي وتُعرّف بأنها "برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يُماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان" (Afifi, 1999). ذلك أن للفيروس قدرة كبيرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى للتمويه كالدخول إلى ملفات مخفية أو خاصة بالذاكرة وبعد فترة معينة أو مباشرة يشغل نفسه ويبدأ بنشاطه التدميري (Hasan, 2008). وهناك أنواع عديدة من الفيروسات منها (من حيث درجة خطورتها من الأقل إلى الأكثر خطورة) فيروس محاكاة الأخطاء، فيروس الإبطاء، الفيروسات النائمة، التطورية، القاتلة (Umar, 1989)، فيروس السرطان، فيروس الجنس وفيروس القردة (As-Shawa, 1984) فيروس حصان طروادة (Qasyqusy, 1992)، وفضلاً عن هذه الفيروسات هناك أنواع أخرى ظهرت بمناسبات معينة منها فيروس مايكل انجلو الذي أُطلق بمناسبة ميلاد هذا الرسام الايطالي وفيروس ناسا وفيروس الكريسماس (Mansur, 2006).

أسلوب تفجير الموقع المستهدف

ويعتمد هذا الاسلوب على ضخ مئات الآلاف من الرسائل الالكترونية من جهاز الحاسب الآلي الخاص بالجاني إلى الجهاز المستهدف بهدف التأثير على ما يسمى بالسعة التخزينية، بحيث يشكل هذا الكم الهائل من الرسائل ضغطاً يؤدي في النهاية إلى تفجير الموقع على شبكة الإنترنت، وتشتيت المعلومات والبيانات المخزنة فيه، فيتمكن الجاني من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على بيانات بطاقات الإئتمان المملوكة للغير. وهذه الطريقة توجه إلى الحواسيب المركزية للبنوك والمؤسسات المالية والفنادق والمطاعم ووكالات السفر، وذلك بهدف الحصول على أكبر قدر ممكن من أرقام البطاقات الائتمانية (Abd Al-Baqi, 2002).

برامج الدودة

هي برامج من شأنها استغلال أي فجوات في نظم التشغيل من أجل الانتقال من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات الرابطة بينها وتتكاثر أثناء انتقالها كالبكتيريا بإنتاج نسخ منها (Ibabanah, 2005) حتى تقوم بتغطية شبكة بأكملها ومن ثم تكون لها الإمكانية لتعطيل أو إيقاف نظام الحاسب الآلي بصورة كاملة.

القنابل المنطقية والزمنية

من الممكن تعريف القنابل المنطقية بأنها برنامج أو جزء من برنامج ينفذ في لحظة معينة أو في كل فترة زمنية منتظمة يتم وضعه على شبكة معلوماتية بهدف معرفة ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع. أما القنابل الزمنية فهي برامج تثير حدثاً في لحظة زمنية محددة بالساعة واليوم والسنة يتم إدخالها في برنامج وتنفذ في جزء من ثانية أو في ثوان أو دقائق وقد يتم ضبطها لتنفجر بعد عام. تستخدم القنابل المنطقية أو الزمنية على نطاق واسع لأنها تحقق أهدافا يطمح لها الفاعل (الجاني) ومن هذه الأهداف أو الميزات أنه يمكن القيام بتوقيت عملية الإتلاف بوقت معين وأن الأثر يكون جسيما كما أن من شأن التوقيت جعل اقتفاء أثر الفاعل أمراً متعذراً أو مستحيلا (Abas, 2010).

أسلوب الخداع

ويتحقق هذا الأسلوب بإنشاء مواقع وهمية على شبكة الإنترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة بحيث يظهر بأنه الموقع الأصلي المقدم لتلك الخدمة. ولإنشاء هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي من خلال شبكة الإنترنت، ومن ثم يستخدم هذه البيانات في إنشاء الموقع الوهمي مع تعديل البيانات السابقة على الموقع الأصلي بالشبكة، بحيث لا يكون هناك غير موقع واحد بنفس العنوان (Abas, 1998).

الوقاية من جرائم أمن المعلومات في المملكة العربية السعودية

استفحلت الجريمة الالكترونية وانتشرت في كل دول العالم واستغل مرتكبو الجرائم الإلكترونية التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات في تنفيذ جرائمهم ذات الطبيعة الخاصة التي يصعب إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية (Abd Ar-Rahman, 2005). ودراسة الوقاية من جرائم الأمن السيبراني في هذا المبحث من خلال المطالب التالية:

أصناف مجرمي نظم المعلومات

رغم صعوبة تحديد شخصية محترفي أنظمة المعلومات، إلا إنه يمكن تحديد كيفية الاختراق وزمانه، وكلمة السر التي استخدمت في الاختراق، وذلك من خلال مراجعة ملفات الدخول للنظام والملفات التأمينية الخاصة به، على نحو يسمح بجمع أكبر قدر من الأدلة التي تشير للجاني (Al-Jahni, 2016) وتتم غالباً محاولات اختراق النظم المعلوماتية بشكل عشوائي بمعنى أن المخترق لا يحدد شخصاً بعينه لاختراق جهازه تحديداً، إلا إنه من الممكن للمخترق أن يحدد جهازاً مملوكاً لشخص معين ويقوم باختراقه (Fadhl, 2007).

ويمكن تصنيف مجرمي نظم المعلومات على حسب أهدافهم إلى أصناف عدة، منها: شخص يعمل بمفرده أو يكون ضمن منظومة بغض النظر عن هذه المنظومة فقد تكون تجارية أو سياسية أو عسكرية، ويكون خطيراً عندما يعمل داخل الجهة المستهدفة، وتكمن خطورة هذا الشخص في قدرته على معرفة معلومات حساسة وخطيرة كونه يعمل داخل تلك الجهة، لذلك فإن حرب التجسس بين الدول التي تعتمد على عناصر يعملون داخل الجهة الأخرى تعد من أخطر أنواع التجسس حيث تفرض الدول أشد الأحكام صرامة على من يمارس ذلك، والتي تصل إلى حد الإعدام في كثير من الدول (Az-Zahrani, 2003).

ولا يقتصر هذا الصنف على الممارسات بين الدول بل قد يكون ذلك الشخص يعمل داخل شركة حيث يقوم بسرقة معلومات تجارية سرية من تلك الشركة وذلك لغرض إفشاءها أو بيعها لمؤسسات منافسة أو التلاعب بالسجلات المالية لتحقيق أهداف عامة أو خاصة، والصنف الثاني الذين يسعون لسرقة معلومات حساسة من جهات تجارية أو حكومية وذلك لغرض بيعها على جهات أخرى تهمها تلك المعلومات والصنف الثالث لا يهدفون إلا للمغامرة وإظهار القدرات أمام الأقران، أو حب الاستطلاع، فلا توجد عادةً عند هؤلاء أطماع مالية، والصنف الرابع تلك الجهات المتنافسة التي يسعى بعضها للوصول إلى معلومات حساسة لدى الطرف الآخر، وذلك سعياً للوصول إلى موقف أفضل من الجهة المنافسة، والصنف الخامس حكومات بعض الدول، التي تسعى من خلال حروب جاسوسية إلى الحصول على معلومات استراتيجية وعسكرية عن الدول الأخرى، ولعل من أشهر تلك الحروب الجاسوسية تاريخياً تلك التي كانت بين الولايات المتحدة و الاتحاد السوفييتي خلال الحرب الباردة (Al-Hajiri, 2004).

حماية أمن المعلومات في المملكة العربية السعودية

يشير واقع تقنية المعلومات في المملكة العربية السعودية الى التطور المتسارع في تقنية المعلومات نتيجة كفاءة البنية التحتية وقدرتها المتعاظمة على استيعاب متطلبات تطبيق مشاريع التعاملات الإلكترونية، فضلاً عن الاستخدامات المتنامية للشبكات الداخلية والخارجية، وزيادة أعداد مستخدمي الإنترنت في التواصل في الداخل والخارج، واستخدام تقنيات الاتصال التي ساهمت بدورها في زيادة الإقبال عليها بصورة غير مسبوقة. وهناك دراسة صدرت أخيراً، كشفت أن الضعف الحاصل في التعامل مع الحسابات الإلكترونية فتح آفاقا جديدة لتزايد الجرائم الإلكترونية التي تعالج من قبل المختصين بالأمن العام ممثلا في إدارة مكافحة الجرائم المعلوماتية، وحددت الدراسة ثلاثة عناصر تبرهن ضعف التعامل الإلكتروني، إما بالإهمال أو التفريط أو الثقة المبالغ فيها تجاه الآخرين. وشهدت الآونة الأخيرة العديد من الجرائم الإلكترونية في تعاملات البنوك، حين سرق عدد من المراهقين ما يقارب مليوني ريال عن طريق بطاقة الألعاب الترفيهية للأطفال بإدخالها عبر صرافات إحدى البنوك المحلية (As-Shairi, 2014).

وقد أثر استخدام التقنيات الحديثة ومنها الحاسب الآلي في المنشآت السعودية على طبيعة العمل ومهام ودور الموظف في إنجاز عمله، فأصبح بإمكانه طباعة وتعديل الوثائق وحفظها بسهولة وسرعة، وقد أدى تطور أجهزة الاتصال الحديثة كالهاتف، والفاكس والإنترنت، والاتصال الفيديوي، بشكل كبير على عملية تبادل المعلومات بين الجهات المتباعدة داخل المملكة وخارجها، ومن ثم حتم إيجاد آليات لحفظ المعلومات التي يتم تبادلها، وتقنيات للحفاظ على أمن وسرية المعلومات. كما ساهم استخدام منتجات التقنية الحديثة في تنظيم وتوفير المعلومات للعاملين في المنشآت السعودية وأصحاب العمل، مما استدعى إنشاء مراكز للمعلومات لحفظ قواعد البيانات الخاصة بكل منشأة لضمان المحافظة على سرية وخصوصية المعلومات وأمنها من وزارة الاتصالات وتقنية المعلومات،2007م.

وأفادت التوقعات بأن الجرائم الإلكترونية قد تتسبب بخسارة دول مجلس التعاون الخليجي بين 2.07 مليار و2.68 مليار

درهم، أي ما يعادل بين 550 مليون و735 مليون دولار أميركي سنويا. ومن المتوقع أن ترتفع هذه الأرقام نظراً لتزايد استخدام الإنترنت على نطاق واسع للتواصل وعقد المعاملات والصفقات التجارية من قبل كل من الأفراد والمؤسسات على حد سواء من جريدة الرياض،2010/1/1م. وضمن إحصائية حول جرائم الانترنت وجد أن النتائج هي (Abd Ar-Rahman, 2014):

i. (13.7%) من مجموع المشاركين في الدراسة الميدانية قاموا بتدمير المواقع.
ii. (3.9%) منهم دمرت مواقعهم.
iii. (5.6%) اخترقوا مواقع حكومية.
iv. (5.3%) اخترقوا مواقع تجارية.
v. (8.9%) اخترقوا مواقع شخصية.
vi. (13.2%) اخترقوا مواقع محلية.
vii. (5%) اخترقوا مواقع خليجية.
viii. (2.9%) اخترقوا مواقع عربية غير خليجية.
ix. (3.1%) اخترقوا مواقع آسيوية غير عربية.
x. (0.3%) اخترقوا مواقع أفريقية غير عربية.
xi. (1.8%) اخترقوا مواقع أوروبية.
xii. (0.5%) اخترقوا مواقع أمريكية جنوبية.
xiii. (7.8%) اخترقوا مواقع في الولايات المتحدة الأمريكية وكندا.
xiv. (65.4%) لا يذكرون المواقع التي اخترقوها.
xv. (4.7%) تعرضت مواقعهم للاختراق.

وأن انتشار الجرائم الالكترونية وذيوع صيتها بما ترتب على ذلك من مهددات للأمن المعلوماتي ومخاطر أصبحت تحيق بأمن المعلومات حتى ارتقت الى مستوى التهديد الأمني الذي دعا حكومة المملكة العربية السعودية الى متابعة هذا الموضوع والبحث فيه وإصدار الأنظمة المكافحة له ومنها نظام مكافحة الجرائم الالكترونية للحد من هذه الجرائم ومواجهتها حماية لمصالح الفرد والمجتمع.

تعاقب غالبية التشريعات المقارنة الحديثة على الدخول غير المصرح لنظام الكمبيوتر (Ramadan, 2004) غير أن موقف التشريعات الحديثة تتباين في تجريم الدخول غير المصرح به. من هذه التشريعات ما يقيد تجريم الدخول بقيد يتعلق بالركن المعنوي، فيستلزم توافر قصد خاص لدى المتهم كما فعل النظام السعودي وإن كان في تعريف الدخول غير المشروع في المادة الأولى من النظام لم يشترط الركن المعنوي إلا أنه بعد ذلك نص عليه في المواد التالية وهو قصد التأثير في البيانات أو التأثير في نظام الكمبيوتر نفسه أو قصد الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني للعقاب على هذا الدخول أو قصد التهديد أو الابتزاز.

وقد صدر في المملكة العربية السعودية نظام لمكافحة الجرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الانترنت وإنشاء مواقع الإنترنت الإرهابية. ويهدف النظام إلى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني (Hijazi, 2002). فعالج المشرع السعودي الاعتداء على البيانات والمعلومات من خلال نصوص نظام مكافحة جرائم المعلوماتية ونظام التعاملات الإلكترونية في المملكة العربية السعودية، حيث نص نظام مكافحة جرائم المعلوماتية السعودي في المادة الثانية على أنه "يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

i. المساعدة على تحقيق الأمن المعلوماتي.
ii. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
iii. حماية المصلحة العامة، والأخلاق، والآداب العامة.
iv. حماية الاقتصاد الوطني.

وقد عرفت المادة الأولى المقصود بالنظام المعلوماتي بأنه "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية". كما عرفت المقصود بالشبكة بأنها "ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول

على البيانات وتبادلها مثل الشبكات الخاصة والعامة والشبكة العالمية للإنترنت". وكذلك عرفت الفقرة رقم (7) من المادة الاولى من ذات النظام الدخول غير المشروع بأنه دخول شخص بطريق متعمد الى حاسب آلي، أو موقع الكتروني أو نظام معلوماتي، او شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول اليها ... بيد أنه، من المتصور أيضاً في بعض الحالات، أن يتم الاعتداء على الأمن الالكتروني بأفعال سلبية أو امتناع أعقبته نتيجة ايجابية ناشئة عن هذا الامتناع.

ومن المفيد هنا التأكيد على أن الأمن المعلوماتي هو أحد تحديات الحكومات الإلكترونية إضافة ل**ثلاثة** تحديات هي:

i. التحدي التقني الناجم عن الفجوة الرقمية وتباعد الهوة

والافتقار للبنية التحتية المعلوماتية.

ii. التحديات الإدارية التي يتمثل أهمها بغياب إدارة التغيير التي تستتبع إعادة مقاومة تصميم العملية الإدارية برمتها التي قد تواجه بعقبات منها تصلب الثقافة التنظيمية والتغيير وغيرها.

iii. التحدي المعرفي المرتبط بالجمهور الإلكتروني وهذا بالتأكيد ناجم عن تأخر المؤسسات التعليمية في الدول النامية عن استخدام التقنيات المعلوماتية (الأمية المعلوماتية) إضافة الى احتكار الدول المتقدمة لهذه التقنيات وأسباب اخرى عديدة.

لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية، 2012م ونص المشرع في الفقرة الثالثة من المادة الثالثة على أنه "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه." وقد حددت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية عدداً من صور السلوك غير المشروعة والتي يتحقق من خلالها الاعتداء على الامن المعلوماتي، وهي كالآتي:

i. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه.

ii. الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.

iii. الدخول غير المشروع إلى موقع الكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

iv. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

v. التشهير بالآخرين وإلحاق الضرر بهم، عبر وسائل تقنية المعلومات المختلفة.

وكذلك ما نصت عليه المادة الرابعة "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

i. الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة

ii. الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

وقد جرم ذات النظام العبث بالنظام في شكل إيقاف عمله أو تعطيله أو تدميره أو مسح البرامج وذلك بنصه في المادة الخامسة على أنه "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

i. الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها.

ii. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

iii. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

ولم يشترط النظام السعودي أن يكون النظام محميا بكلمة السر، بل إن الدخول غير المشروع معاقب عليه حتى ولو لم يعتن صاحبه بوضع كلمة المرور عليه ليحميه من تطفل الآخرين.

ويعد من صور الدخول غير المشروع المعاقب عليه قانوناً ذلك الذي يكون بغرض الحصول على بيانات تمس الأمن أو الاقتصاد الوطني وهذا ما نصت عليه المادة السابعة "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية هي الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن – طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".

وجعل نظام مكافحة جرائم المعلوماتية عقوبة المصادرة وعقوبة الإغلاق عقوبتين تكميليتين يجوز الحكم بهما، وهذا ما نصت عليه المادة الثالثة عشرة أنه: "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه".

وفيما يتعلق بالجرائم المرتكبة عن طريق النظام المعلوماتي فهي متعددة وجرمتها الأنظمة في المملكة العربية السعودية ومن ذلك: نظام عقوبات نشر الوثائق والمعلومات السرية الصادر بالمرسوم الملكي رقم م/35 وتاريخ 1432/5/8هـ، لتجريم نشر الوثائق والمعلومات السرية وإفشاؤها ويقصد بالوثائق السرية: الأوعية بجميع أنواعها التي تحتوي على معلومات سرية يؤدي إفشاؤها إلى الإضرار بالأمن الوطني للدولة أو مصالحها أو سياستها أو حقوقها سواء أنتجتها اجهزتها المختلفة أو استقبلتها. ويقصد بالمعلومات السرية: ما يحصل عليه الموظف –أو يعرفه بحكم وظيفته– من معلومات يؤدي إفشاؤها إلى الإضرار بالأمن الوطني للدولة أو مصالحها أو سياستها أو حقوقها.

وكذلك أصدر المنظم في المملكة العربية السعودية ضوابط تطبيق التعاملات الالكترونية الحكومية، الصادر بقرار مجلس الوزراء رقم (40) وتاريخ 1427/2/27هـ، والتي نصت في المادة الحادية والعشرين منها على أنه "تقوم كل جهة حكومية بحماية معلوماتها وبياناتها وأنظمتها المعلوماتية وفق المعايير ذات العلاقة، وحسب معايير استرشادية يعدها برنامج التعاملات الالكترونية الحكومية لهذا الغرض، كما أكدت هذه الضوابط على جميع الجهات الحكومية بأن تتفادى الازدواجية والتكرار في قواعد المعلومات والبيانات وأن يقوم برنامج التعاملات الالكترونية الحكومية بالتنسيق مع الجهات الحكومية الأخرى من أجل تكامل المعلومات والبيانات، بحيث تكون هناك جهة واحدة مسؤولة عن حفظ المعلومات والبيانات وتعدد مصادرها، وبما لا يخل بوجود نسخة احتياطية لكل قاعدة معلومات وبيانات.

وسائل الوقاية الفنية

استخدام وسائل التحقق من الشخصية

استخدام كلمة مرور مكونة من عدة حروف وأرقام خاصة يصعب التنبؤ بها، بهدف حماية الجهاز من عملية الاختراق أو الاستخدام إلا بعد كتابتها بشكل صحيح. إدخال بطاقة ممغنطة مخصص لها مكان في الحاسب الآلي (Al-Hamid, 2007). وتستخدم البطاقات الممغنطة لفتح الخدمة للمصرح لهم فقط. وتمكن هذه البطاقة من يحملها من الدخول للمنظمة أو غرفة الحاسب أو حتى النظام، ولذلك يجب الحفاظ عليها، لأنها تمكن أي فرد من محاولة اختراق النظام في حالة العثور عليها (Al-Hamdan, 2015).

فالمجرم المعلوماتي يتصف في الغالب بمهارات تقنية مقارنة بنظيره المجرم العادي، وهذا يمكّنه من التخطيط لجريمته قبل أن يقدم على ارتكابها محاولاً بذل الجهد في ألاّ يُكتشف أمره متوسّلاً بأساليب وتدابير الحماية الفنية التي من شأنها إعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل، كما في استخدام كلمات المرور password، وترميز البيانات وتشفيرها للحيلولة دون الاطلاع على محتواها أو ضبطها (As-Saghir, 2001).

جدران الحماية

يعد ضرورة لا غنى عنها تزويد الأجهزة ببرامج حماية كافية لتأمين الدعم الفني المستمر وحماية الموقع من الاختراق أو التدمير ومحاولة التحديث المستمر لها ودعم وسائل مكافحة الاختراق لاسيما وأن هذه البرامج تقوم بإرسال التنبيهات في حالة وجود اختراق للأجهزة او الموقع. جدران الحماية هي: أجهزة وبرامج تعزل الشبكة المحلية عن الشبكات الاخرى بصفة جزئية أو كلية، فهي عبارة عن أجهزة حاسب آلي تقع بين الشبكة المحلية والشبكة العالمية كبوابة لحماية معلومات الشبكة المحلية والتحكم في الدخول اليها (As-Shadi, 2000).

وكذلك فإن عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها. وحذرت شركة مايكروسوفت

من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجة، ودعت المستخدمين إلى تركيب برنامج ترقيعي لحل المشكلة من جريدة الرياض، 20/ 1423/88هـ. يتوقف اختيار نوع جدار الحماية على حاجة المنظمة ومجال عملها، حيث توجد عدة أنواع من جدران الحماية لكل منها مميزات وإمكانيات مختلفة عن الأخرى، ومن أهم هذه الأنواع الموجه الحاجب، والوسيط، والحارس.

التشفير

عرف التشفير بتعاريف متعددة كلها تدور حول معنى واحد هو أنه تدبير احترازي يصار إليه لمواجهة الجرائم المرتكبة باستخدام

التقنيات العلمية الحديثة والتدخلات غير المشروعة من الغير بقصد ضمان عدم تسرب المعلومات والبيانات المخزونة الكترونياً إلى الغير حيث يقوم الترميز أو التشفير بالحيلولة دون الدخول غير المشروع للغير في الاتصالات والمبادلات التي تتم بين طرفي العقد لأنه يكون أمام نص مشفر عبارة عن رموز غير مفهومه وهذا يؤدي بالنتيجة إلى حمايته (Abd Al-Majid, 2007). ويستخدم مفاتيح تشفير encryption النصوص المرسلة وفك الشفرة من قبل صاحبها والمسموح له بتسلمها، وتستند هذه المفاتيح إلى صيغ رياضية معقدة في شكل خوارزميات وتعتمد قوة وفعالية التشفير على نوعية الخوارزميات، ومازالت تلك العملية تتم بواسطة مفتاح سري يعتمد لتشفير النصوص وفي نفس الوقت لفك تشفيرها وترجمتها إلى وضعها الأصلي باستخدام نفس المفتاح السري، وهو ما يعرف بالتشفير المتناظر symmetric، ثم جاء ما يعرف بالتشفير اللامتناظر asymmetric حلا لمشكلة التوزيع الغير آمن للمفاتيح في عملية التشفير المتناظر معوضاً عن استخدام مفتاح واحد باستخدام مفتاحين اثنين مرتبطين بعلاقة رياضية عند بنائهما، وهما مفتاحان الأول: المفتاح العام؛ والثاني: المفتاح الخاص(Abd Ar-Razak, 2007).

إجراءات إدارية

وتشمل تطوير خطط واستراتيجيات لتأمين الحاسب الإلكتروني أو الشبكة المحلية وتقليص احتمالات المخاطرة، على أن تتضمن تلك الخطط الإجراءات الفنية الواجب اتخاذها، وأساليب التعامل مع الأزمات والاستعاضة في حالة الطوارئ، ومراقبة التعامل، وإجراءات السرية ونشر الوعي بجرائم الحاسب الآلي وأساليب مواجهتها، والتزويد المستمر بأحدث أساليب الحماية، واستخدام وسائل التخزين الخارجية للملفات والبيانات مع وجود إدارة نظم معلومات مزودة بكادر بشري مؤهل.

العامل البشري هام جداً حتى في الشبكات، وكلما كان العنصر البشري مدرباً ومؤهلاً بالشكل العلمي والقدر الكافي كان ذلك أحد أسباب حماية شبكات المعلومات، فهناك بعض الأخطاء التي تنتج عن سوء استخدام الأفراد لشبكات المعلومات تلحق الضرر البالغ على أمن وسلامة البيانات داخل الشبكة، وسواء كان هذا الإهمال وسوء الاستخدام متعمداً أو غير متعمد فإنه في النهاية يؤدي إلى النتيجة نفسها، بحيث يمكن أن يكون نافذة إلى إحداث ثقوب في جدر الحماية الخاصة بالشبكات.

النتائــج

توصل البحث لعدد من النتائج أهمها:

i. أن مصطلحي الأمن والمعلومات مصطلحان عامان يندرج تحت كل منهما العديد من المعاني والتي لا تخرج عن المعنى اللغوي لكل منهما، إلا أنهما كمصطلحين يراد بهما ذلك النوع من الاستقرار وعدم الخوف والحماية للمعلومة الواردة من أو إلى أجهزة الحاسب أو الاتصال المختلفة والتي تنتقل غالبا عن طريق شبكة المعلومات الإلكترونية (الإنترنت)

ii. أن أمن المعلومات ركيزة أساسية من ركائز الأمن الوطني، لا يتم الأمن الوطني إلا به.

iii. يتطلب أمن المعلومات توفر عناصره الثلاثة وهي: سرية المعلومات وسلامتها وتوافرها.

iv. لا حصر للجرائم المعلوماتية فيشمل كل اعتداء يتم متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، وقد أحسن المنظم السعودي حين عرف الجريمة المعلوماتية في الفقرة الثامنة من المادة الأولى من نظام مكافحة جرائم المعلوماتية بأنها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام."

v. يتعدد مجرمي أمن المعلومات إلا أنه يغلب عليهم المعرفة التقنية والفنية في الحاسب، ويضاف لذلك أنه قد يكون لديه معلومات سرية لا يمكن لغيره الحصول عليها.

vi. حداثة الأنظمة والتقنين لحماية أمن المعلومات، رغم سرعة تطور الجريمة المعلوماتية.

vii. لا يمكن تطبيق الحكومة الإلكترونية وغيرها من الأنظمة الإلكترونية الحديثة دون وجود الأمن المعلوماتي.

viii. عرف نظام مكافحة الجرائم المعلوماتية الدخول غير المشروع بأنه "دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها" وهذا تعريف شامل إلا أنه لم يجرم ذلك الدخول ما لم يقترن بقصد التهديد والابتزاز أو قصد تغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه كما ورد في المادة الثالثة، أو قصد إلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها كما ورد في المادة الرابعة، أو قصد الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني كما ورد في المادة السابعة

ix. تنامي ظاهرة الاعتداء على أمن المعلومات، ترتب عليه جملة من التحديات سواء تقليل أداء الأنظمة الحاسوبية أو تخريبها بالكامل، أو تعطيل تقديم الخدمات الإلكترونية أو التقليدية أو إفشاء المعلومات السرية، وأحسن المنظم السعودي حين جرّم الإخلال بسير النظام المعلوماتي أو قيام الجاني بمسح أو إتلاف أو تعديل البيانات المعلوماتية.

التوصيات

i. استحداث إدارة للشؤون المعلوماتية في جميع الجهات الحكومية لمواجهة التهديدات الداخلية أو الخارجية سواء بضبطها أو بالوقاية منها والتوصية إذا لزم الأمر بتعديل الأنظمة وإبرام الاتفاقيات لمواكبة مستجدات الأمن المعلوماتي.

ii. تطوير الاتفاقيات الأمنية على المستويات المختلفة سواءً لمنع الاعتداء أو لضبط المجرمين أو لتبادل تسلم المجرمين أو المعلومات وتبادل الخبرات في هذا المجال.

iii. تعريف المجتمع بجهات استقبال البلاغات وضبط الجريمة المعلوماتية وتسهيل الوصول إليها للإبلاغ عن أي خروقات أو ثغرات لهذا النوع من الجرائم.

iv. استخدام تقنية تشفير المواقع حيث يتم إرسال البيانات إلى جهة الإدارة ثم استقبالها من قبل الجهة المختصة من خلال مفتاحها الخاص. والدخول إلى المواقع الاستراتيجية باستخدام الهوية الالكترونية أو البصمات.

v. حفظ المعلومات وتخزينها بصورة مشفرة ومبهمة وعلى وجه الخصوص المعلومات المهمة التي لها علاقة بالأمن القومي. واستخدام كلمات مرور معقدة وتغييرها تلقائيا بمرور وقت معين حيث يتم مراعاة الأمن والسرية.

vi. إعادة النظر في مقررات الكليات الحقوقية القانونية والأمنية بحيث يخصص مقرر مستقل للجرائم المعلوماتية ووسائل مكافحتها.

vii. تطوير جهات الضبط الجنائي للجريمة المعلوماتية للسيطرة على الجرائم المعلوماتية ومجرميها من خلال المعرفة المتميزة لوسائل التقنية الحديثة والمستجدات العلمية ذات الصلة.

viii. تجريم الدخول غير المشروع للنظام المعلوماتي والأجهزة الإلكترونية، وهذا يفرضه واجب احترام خصوصية الغير وعدم التدخل في شؤونه، فضلا عن أن ذلك يفرضه تعريف النظام للدخول غير المشروع في مادته الأولى.

REFERENCES (المراجع)

Abas, Ali Husni. (1998). *Makhatir Bataqat Ad-Dafa' Al-Elektroni Ibar Shabkah Al-Internet : Masyakil wa Al-Hulul.* Waraqah Amal Muqadimah li An-Nadwah As-Suwar Al-Mustahdisah li Jaraim Bataqat Al-Dafa' Al-Elektroni. Al-Qaherah, Misr : Markaz Buhus As-Syurtah.

Abd Al-Majid, Asmat. (2007). Asar Al-Ilmi fi Al-Aqad. *Majalah Al-Qada'*. Adad As-Sani, Sanah Al-Khamisah wa Al-Khamsun. Baghdad, Iraq. N.p.

Abd Ar-Rahman, Muhamad Jalal. (2005). *Al-Jaraim Al-Elektroniah fi Al-Fiqih Al-Islami wa Al-Qanun : Dirasah Muqaranah*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: MAktabah Al-Qanun wa Al-Iqtisad.

Al-Abidi, Usamah bin Ghanim. (2012). *Jarimah Ad-Dukhul Ghair Al-Masyru' ila An-Nizam Al-Ma'lumati : Dirasah Qanuniah Muqaranah fi Dau'i Al-Qawanin*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Ma'had Al-Idarah Al-Amah.

Abu Bikhutwah, Ahmad Syauqi Umar. (1999*). Sharah Al-Ahkam li Qanun Al-Uqubat*. Al-Qaherah, Misr: Dar An-Nadwah Al-Arabiyyah.

Abu Hasan, Ahmad bin Faris. (1999). *Mu^{c}jam Maqayis Al-Lughah*. Tahqiq : Abd As-Salam Muhamad Harun. Beirut, Lubnan : Dar Al-Jayl.

Abu Maghaid, Yahha bin Muhamad. (2004). *Al-Hukumah Al-Elektroniyah: Saurah Ala Al-Amal Al-Idari At-Taqlidi*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Maktabah Al-Obeikan.

Al-Abudi, Abas. (2009). *Tahdiyat Al-Isbat bi As-Sanadat Al-Elektroniah wa Mutatallibat An-Nizam Al-Qanuni li Tajawazuha*. Babel, Iraq : Maktab Al-Wiam li Al-Hisabat wa At-Taba'ah wa An-Nasyar.

Afifi, Kamel Afifi. (1999). *Jaraim Al-Kombiuter wa Dawur As-Syurtah wa Al-Qada'.* Misr: Jamiah Al-Iskandariah.

Ammar, Majid Ammar. (1989). *Al-Mas'uliah Al-Qanuniah An-Nasyiah 'an Istikhdam Virus Baramij Al-Kombiuter wa Wasail Himayatiha.* Al-Qaherah, Misr: Dar An-Nahdah.

As-Asaf, Saleh bin Muhamad. (2000). *Al-Madkhal ila Al-Bahs fi Al-Ulum As-Sulukiah*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Maktabah Al-Obeikan.

Basil, Yusof. (2000). *Al-Iktoraf Al-Qanuni bil Mustanadat wa A-Tawaiqi' Al-Elektroniyah fi At-Tasyri'at Al-Muqaranah*. Bahs manyur fi majalah dirasat qanuniah. Baghdad, Iraq : Bayt Al-Hikmah.

Fadhl, Sulaiman Ahmad. (2007). *Al-Muwajahah At-Tasyri'iyah Al-Amaniah li Al-Jaraim An-Nasyiah 'an Istikhdam Syabkah Al-Ma'lumat Ad-Dauliah : Al-*

Internet. Al-Qaherah, Misr : Dar An-Nahdah Al-Arabiyah.

Farid, Hisham Muhamad. (2000). *Qanun Al-Uqubat wa Makhatir Taqniah Al-Ma'lumat*. Asyut, Misr: Maktabah Al-At Al-Hadisah.

Gloria, Evans. (2005). *Al-Hukumah Al-Elektroniyah*. Al-Qaherah, Misr : Dar Al-Faruq lil Nasyar wa At-Tauzi'.

Al-Hamdan, Abd Rahman bin Abd Al-Aziz & Al-Qasim, (n.d). Muhamad bin Abdullah. *Asasiyat Aman Al-Ma'lumat.* Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Matabi' Al-Humaidi.

Al-Hamid, Muhamad Dabas & Nino, Marco Ibrahim. (2007). *Himayah Anzimah Al-Maklumat*. Amman: Dar Al-Hamid lil An-Nasyar wa At-Tauzi'.

Hasbu, Umar Ahmad. (2000). *Himayah Al-Huriyat fi Muwajahah Nizam Al-Ma'lumat*. Al-Qaherah, Misr : Dar An-Nahdah Al-Arabiyah.

Hijazi, Abd Al-Fattah Bayumi. (2015). *Ad-Dalil Al-Jina'I wa At-Tazwir fi JAraim Al-Kombiuter wa Al-Internet: Dirasah Muta'amiqah fi Jaraim Al-Hasib Al-Ali wa Al-Internet*. Al-Qaherah, Misr : Dar Al-Kutub Al-Qanuniah.

Ibabinah, Mahmud Ahmad. (2005). *Jaraim Al-Hasib Al-Ali wa Ab'aduha li Dauliah*. Amman : Dar As-Saqafah li An-Nasyar wa At-Tauzi'.

Ibn Manzur, Muhamad bin Mukram. (2000). *Lisan Al-Arab*. Beirut, Lubnan : Dar Sadir.

Mansur, Muhamad Husin. (2006). *Al-Mas'uliah Al-Elektroniah*. Al-Iskandariah, Misr : Mansya'ah Al-Ma'arif.

Al-Mawardi, Abu Al-Hasan Ali bin Muhamad. (1987). *Adab Ad-Dunya wa Ad-Din*. Beirut, Lubnan : Dar Al-Kutub Al-Ilmiah.

Al-Mutalaqah, Muhamad Fawaz. (2006). *Al-Wajiz fi Uqud At-Tijarah Al-Elektroniah*. Amman : Dar As-Saqafah li An-Nasyar wa At-Tauzi'.

N.a. (2007). *Nizam At-Ta'amulat Al-Elektroniah.* N.p. N.p.

N.a. (2007). Nizam Mukafahah Al-Jaraim Al-Ma'lumatiah. N.p. N.p.

Al-Qasim, Muhamad bin Abdullah, (2005). *Siasat Aman Al-Ma'lumat*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Markaz Al-Buhus wa Ad-Dirasat bi Kuliah Al-Malik Fahd Al-Amaniah.

Qasyqusy, Huda Hamid. (1992). *Jaraim Al-Hasib Al-Elektroni fi At-Tasyri' Al-Muqaran*. Al-Qaherah, Misr : Dar An-Nahdah Al-Arabiah.

Qasyqusy, Huda Hamid. (2000). *Al-Himayah Al-Jina'iyah li At-Tijarah Al-Elektroniah 'Ibar Al-Internet.* Al-Qaherah, Misr : Dar An-Nahdah Al-Arabiah.

Al-Quhtani, Mansur bin Said. (2008). *Muhaddadat Al-Aman Al-Ma'lumati wa Subul Muwajahatuha : Dirasah Masahiyah 'ala Mansubi.* Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Markaz Al-Hasib Al-Ali bi Al-Quat Al-Bahriah Al-Malakiyah As-Saudiah.

Ramadan, Madhat Ramadan. (2004). *Al-Himayah Al-Jinaiyah li Mauqi' Al-Internet Wa Muhtawiyatuhu*. Waraqah Amal li An-Nadwah At-Tijarah Al-Elektroniyah Al-Mun'aqidah fi Al-Ma'had Al-'Ali li Al-Ulum Al-Qanuniah wa Al-Qada'iyah. Dubai, Al-Imarat Al-Arabiyah Al-Muttahidah.

As-Sanbuti, Ata Muhamad. (2001). *Mauqif As-Syariah Al-Islamiyah min Al-Ijram Ad-Dauli : Jaraim Al-Hasib Al-Ali wa Al-Internet*. Muktamarn Al-Wiqayah min Al0Jarimah fi Asr Al-Aulamah, Kuliah As-Suariah wa Al-Qanun, Jamiah Al-Imarat Al-Arabiyyah Al-Muttahidah.

As-Shady, Tareq Abdullah. (2000). *Aliah Al-Bina' Al-Amani li Nizam Al-Ma'lumat*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Dar Al-Watan li At-Tiba'ah wa An-Nasyar.

As-Sharman, Ziyad Muhamad. (2014). *Muqadimah fi Nizam Al-Ma'lumat Al-Idariah*. Amman, Al-Urdun : Dar As-Safa' li An-Nasyar wa At-Tauzi'.

As-Shawa, Muhamad Sami. (1996). *Saurah Al-Ma'lumat wa An'akasatuha 'ala Qanun Al-Uqubat*. Al-Qaherah, Misr: Dar An-Nahdah Al-Arabiyah.

Az-Zahrani, Sulaiman Mahja'. (2003). *Wasail At-Tahqiq fi Jaaim Nizam Al-Ma'lumat*. Riyadh, Mamlakah Al-Arabiyah As-Saudiyah: Jamiah Al-Malik Saud.