العنوان:	أمن المعلومات في المكتبات ومراكز المعلومات
المصدر:	مكتبات نت
الناشر:	ايبس كوم
المؤلف الرئيسي:	صالح، مشيرة أحمد
المجلد/العدد:	مج 8, ع 4
محكمة:	لا
التاريخ الميلادي:	2007
الشهر:	أكتوبر - نوفمبر - ديسمبر
الصفحات:	19 - 28
رقم MD:	41286
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الحاسبات الإلكترونية ، المكتبات، مراكز المعلومات، أمن المعلومات، حماية المعلومات، القرصنة الإلكترونية، البرمجيات، الملكية الفكرية، النشر الإلكتروني، القوانين والتشريعات
رابط:	http://search.mandumah.com/Record/41286

أمن المعلومات في المكتبات ومراكز المعلومات

أ. مشيرة أحمد صالح

مدرس مساعد بقسم المكتبات والمعلومات ـ جامعة عين شمس

شغلت قضية أمن المعلومات في الآونة الأخيرة اهتمام أفراد المجتمع والمتخصصين، والواقع أنه نتيجة لظهور تكنولوجيا الحاسبات الشخصية والخوادم servers والشبكات والأقراص المدمجة والاتصال عبر الإنترنت وتسويق المكتبة عبر صفحة الويب، أصبحت المكتبات ومراكز المعلومات تمتلك أفضل أجهزة الحاسب الآلي Computers وأكبر أجهزة الخادم Servers كما أنه أصبح مطلوباً من المكتبات جمع معلومات شخصية عن المستفيدين من المكتبة، بالإضافة إلى أن النظم الآلية المتكاملة للمكتبات Integrated Library System ومواقع الويب Web Sites تعد مخازن مركزية ضخمة تحتوي على معلومات شخصية عن المستفيد والعمليات البحثية التي قام بها واهتماماته القرائية[1]، وهي لم تختلف في ذلك عن بقية مؤسسات المجتمع .

والواقع أن الحرص على أمن المعلومات ليس بالموضوع الجديد على المكتبات، فقد كانت المكتبات ولازالت تحمى مجموعاتها بأساليب متعددة تتمثل في إجراءات الصيانة، والتجليد، والترميم، وكذلك باستخدام النظم الأمنية التي تكفل حماية مجموعاتها، مثل: التشفير، وأنظمة جدران النار، وبرامج مضادات الفيروسات، والنسخ الاحتياطي[2].

إن أمن المعلومات ليس مجرد أمن الحاسب الآلي. إذ إن أمن الحاسب الآلي computer security يرتبط بتأمين أو أمن النظم المحسبة ضد الاستخدام والوصول غير المرغوب للمعلومات، وأمن المعلومات أيضا يحتوي على قضايا مثل إدارة المعلومات information management وخصوصية المعلومات information privacy، وتكامل وصحة البيانات data integrity. فعلى سبيل المثال، يحتوى أمن المعلومات في المكتبة على الأمن الشخصي personal security والسياسات policies والخطوات التي تتخذ للنسخ الاحتياطي الفعال effective backups، والتكامل المادي للتجهيزات المحسبة the physical integrity of computing facilities[3].

وأمن المعلومات الفعال في المكتبات يجب أن يشتمل على :

1. اختيار وتعيين الموظفين للقيام بمهام أمن المعلومات .
2. تدريب كل الأشخاص (المستفيدين والموظفين) على إجراءات وقضايا أمن المعلومات .
3. السياسات الخاصة التي تعالج مسائل خصوصية أمن المعلومات information privacy، والأمن المادي للأجهزة physical security of equipment، وإجراءات أمن الحاسب الآلي computer security procedures، ومستويات الأمن المادي physical security plans .
4. مقاييس ومعايير تكامل وصحة البيانات data integrity measures .

5. مستويات الوصول إلى البيانات أو الأجهزة، ومراقبة الأشكال المختلفة من الوصول إلى المعلومات[4].

وأمن المعلومات يتكون من ثلاثة عناصر أساسية، وهي :

1. درجة السرية المتعلقة بمعلومات معينة أو وثائق تتطلب حماية Confidentiality: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك .
2. أمن وسلامة واكتمال المعلومات والبيانات Integrity: فالتأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص يؤدي إلى عدم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .
3. إتاحة المعلومات أو إمكانية الحصول عليها Availability: أي التأكد من استمرار عمل نظام المعلومات، وقدرته على التفاعل مع المعلومات وتقديم الخدمة للمستفيد، وأنه لن يتعرض إلى منع استخدامه للمعلومات أو دخوله إليها.

وهذه العناصر الثلاثة هي التي تؤلف برامج الأمن الفعالة لحماية معلومات المكتبة ومواردها، والإعداد الفني، والمدخلات والمخرجات، والتي تكون متاحة عندما يحتاج إليها المستفيدون المرخص لهم بالاستخدام[5].

أهم صور جرائم الحاسب الآلي والشبكات :

ومن الممكن تقسيم المخاطر أو الجرائم التي تتعرض لها نظم المعلومات إلى مجموعتين أساسيتين :

المجموعة الأولى: جرائم تقع على الحاسب الآلي والإنترنت .

الجرائم التي تقع على الحاسب الآلي والإنترنت هي الجرائم التي يكون فيها الحاسب الآلي وشبكة الإنترنت هدف المجرم، وهي ذاتها محل الاعتداء. ومن هذه الجرائم :

1) جرائم الاختراقات Hacking

الاختراق هو الدخول غير المصرح به إلى أجهزة الحاسب الآلي وشبكات المعلومات، وذلك اعتمادا على برامج الاختراق المتوفرة على شبكة الإنترنت، ويستهدف الاختراق بالدرجة الأولى نظم المعلومات (الحاسب الآلي، والشبكات بصفة عامة وشبكة الإنترنت بصفة خاصة) التي تفتقر إلى الأمن أو تشتمل على الثغرات الأمنية في نظم الحماية الخاصة بها. وتختلف أهداف جرائم الاختراقات ما بين تدمير المواقع على الإنترنت، واختراق المواقع الرسمية والشخصية والتحريف فيها، والاقتحام والدخول عنوة إلى نظام المعلومات للوصول إلى ملفات البيانات لتغيير أو تعديل أو مسح أو تخريب أو سرقة معلومات معينة، أو استخدام النظام في أغراض غير مشروعة، مثل: تخزين البرمجيات التي يحصل عليها الفرد عن طريق القرصنة والدخول إلى شبكات الهواتف بأنواعها لاستغلال الموارد المتاحة فيها، وكسر شفرات البرمجيات التطبيقية المحمية أو الملفات المشفرة، ونشر الفيروسات لإحداث خلل في أداء نظام المعلومات، واختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية[6].

2) الفيروسات Viruses

والفيروس هو " عبارة عن برنامج حاسب آلي مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد، هو إحداث

أكبر ضرر ممكن بنظام الحاسب الآلي، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيا، مما يتيح له القدرة على الانتشار بين برامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في ذاكرة الحاسب الآلي حتى يحقق أهدافه التدميرية[7]."

والفيروسات لا تظهر صدفة، بل يكتبها مبرمجون ذوو مهارات عالية عادة، ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها. وكلما أصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجون من جهودهم لتطوير فيروسات أذكى، للتحايل عليها. والهدف من تطوير الفيروسات، بالنسبة للكثير من مؤلفيها، ليس أكثر من التحدى، والرغبة في إثبات تفوقهم، بينما هو للبعض الآخر تلذذ بإثارة حيرة الآخرين وشكوكهم في الحاسب الآلي، أو إزعاجهم، وحتى إيذائهم، وهذا أمر سيئ جداً، إذ يمكنهم أن يجنوا أموالاً طائلة، إذا وجهوا مواهبهم لمساعدة الشركات. وقد لا يتجاوز تأثير الفيروس بعد انتشاره أداء عمل غير ضار مثل ترك رسائل غير مرغوبة، أو تدمير مساحات تخزين على القرص، وجزء من ذاكرة الحاسب الآلي، كما يشغل جزءا من طاقة المعالج، ومن ثم فهو يؤثر على سرعة وكفاءة الجهاز، ومسح أو تدمير البيانات، وإعادة تهيئة الأقراص الصلبة. والفيروسات تنتشر في المقام الأول عن طريق الأقراص المرنة، أو البرامج المنقولة عبر الشبكات (ومن بينها الإنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attachment) برسالة بريد إلكتروني[8].

ويقدر مكافي MCAFEE، وهو من أهم بائعي البرمجيات المضادة للفيروسات، أن حوالي 70٪ من مجموع الفيروسات تكون منقولة عن طريق الإنترنت، مع ملاحظة أن هذه الفيروسات تتغير باستمرار، فتقترب بعض الفيروسات من بعضها وتتشابه وتظهر أنواع جديدة[9]. ومن أخطر وأشهر الفيروسات في تاريخ شبكات الحاسب الآلي [10]:

1. فيروس الشفرة الحمراء Code Red ضرب شبكة الإنترنت في عام 2001 وأحدث الكثير من الخسائر.
2. فيروس جرثومة الحب Love bug أسرع الفيروسات انتشارا عبر التاريخ، وكان مكتوبا بلغة (VB script) واستغل برنامج البريد الإلكتروني (Outlook) للانتشار. وقدرت خسائره بمبلغ 10 بلايين دولار .
3. فيروس مليسا ثاني أسرع الفيروسات انتشارا عبر التاريخ واستخدم في انتشاره البريد الإلكتروني، وقد أصاب أكثر من 1.2 مليون جهاز حاسب آلي خلال ساعات قليلة .

وهناك برامج أخرى مصممة لإلحاق الأذى بالحاسبات، ويطلق عليها أيضا مصطلح فيروس على الرغم من أنها لا تستطيع نسخ نفسها، ومنها ما يأتي :

أ. حصان طروادة Trojan Horse

نسبة للأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس[11]. وتعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو مظهرها بريئاً، وعندما يشغل المستخدم واحداً من هذه البرامج، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وتختلف أحصنة طروادة عن الفيروسات العادية، في أنها لا تعيد إنتاج نفسها[12].

وحصان طروادة هو برنامج غير مرخص unauthorized متضمن في برنامج شرعي legitimate، ويقوم البرنامج غير المرخص

بجملة من الأنشطة غير المشروعة التي لا يريدها المستخدم، مثل: سرقة كلمة المرور، واستنساخ الملفات أو إلغائها دون علم المستخدم، والتجسس ومتابعة كل ما يتم عمله من إجراءات، وتقوم أحيانا بنوع آخر من الأذى على الأجهزة المصابة، مثل تشفير البيانات، أو التعريض والتشهير بنظام المعلومات من خلال كشف أسراره[13].

ولا يمكن لحصان طروادة أن ينسخ نفسه والالتصاق بالبرامج الأخرى، ولكنه يؤدى عملا معينا تم تصميمه من أجله، فهو يقوم بأداء أعمالٍ عادية توحي للمستخدم بأنه يقوم بعمل معين في حين أنه في واقع الأمر يؤدى عملا آخر تخريبياً في الغالب[14].

والإصابة بهذا النوع من الفيروسات لا يتم إلا عن طريق استلام ملف يحوى هذه الآفة، ويتم إعداده بواسطة مبرمج متخصص، وليس هناك احتمال لنشوء حصان طروادة نتيجة لعملية طباعة عشوائية يقوم بها المستخدم على الحاسب الآلي حتى لو استمرت هذه العملية بضعة أيام[15].

وتكمن خطورة حصان طروادة في صعوبة تحديد مستوى الاختراق الذي حققه في النظام، الأمر الذي يورث إدارة النظام قلقا مستمرا حتى بعد اكتشافه، لصعوبة تحديد حجم الاختراق، والمدى الذي ستمتد عليه تأثيراته.

ب. القنابل المنطقية Logic Bombs والقنابل الموقوتة Time Bombs

القنابل المنطقية هي من أنواع أحصنة طروادة، وتعمل عند حدوث شرط منطقي محدد، مثل: وصول الموظفين لعدد معين، أو رفع اسم أحد الموظفين من كشف الرواتب، أو كتابة كلمة معينة[16].

أما القنابل الموقوتة فهي أيضا من أنواع حصان طروادة، وتقوم بتنفيذ مجموعة من التعليمات في وقت وتاريخ محددين، مثل إظهار رسائل معينة على الشاشة (فيمكن برمجة قنبلة مثلاً، لمسح كافة الملفات ذات الامتداد .DOC من على القرص الصلب، عشية رأس السنة الميلادية، أو لعرض رسالة على الشاشة، في اليوم المصادف لعيد ميلاد شخصية مشهورة)، أو مسح نظام المعلومات نفسه. وليس التوقيت فقط هو المقياس الوحيد لبدء القنابل الموقوتة، فهذه القنابل قد تبدأ بالعمل عند تشغيل برنامج معين لعدد محدد من المرات[17].

ج. الديدان Worms

لا تحتاج الدودة إلى برنامج آخر تلتصق به للقيام بدورها كما هو الحال بالنسبة للفيروس، فهى عبارة عن برنامج قائم بذاته ويوجد بشكل مستقل عن أي برنامج آخر، ولديها القدرة على نسخ نفسها والانتقال من ملف إلى آخر، ومن جهاز إلى آخر متصل بالشبكة. وهذه الديدان لا تكون مدمرة، ولكن لديها ميول عدوانية، مثل استهلاك الذاكرة أو المعالج أو الأقراص أو سائر موارد الحاسب مما يؤدى إلى زيادة عبء على تحميل الشبكة، ومن ثم توقف النظام[18].

ط. الكوكيز cookies

الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب عندما يتم زياراتها لأول مرة على القرص الصلب الخاص بجهاز الحاسب الآلي المستخدم، وتحتوي هذه الملفات النصية (الكوكيز) على معلومات عن الشخص أثناء تصفحه لمواقع الويب المزارة، مثل عنوان IP الخاص به، ونوع المتصفح الذي يستخدمه، ونظام التشغيل مما يعد انتهاكاً لخصوصية المستخدم، كما تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة، أو عند زيارة الشخص للموقع مرة أخرى[19]. ومع أنها وسيلة اتبعت ابتداء لغرض غير جرمي وهو إرسال بريد إلكتروني من الشركات التجارية في إطار

أنشطتها الدعائية، إلا أن ذلك لا يمنع أنها تمثل كشفا عن بيانات قد لا يرغب الشخص في الكشف عنها. فشركة مثل دبل كليك Double click استخدمت ما حصلت عليه من رسائل الكوكيز لتحديد أهداف وجهة خطط الإعلان على الخط. إن ملفات الكوكيز، وبعيدا عن فوائدها، مثلت وسيلة مهمة لملاحقة واقتفاء أثر المستخدمين وجمع المعلومات عنهم وتحليلها لغايات الإعلان ولغايات الدراسات التسويقية على الخط. ولم تكن هذه المعلومات بعيدة عن الاستغلال في أغراض غير مشروعة أو على الأقل لا علم لصاحبها بها ولم تتح له خيارات هذه الاستخدام أو رفضه[20].

ويستطيع متصفح الإنترنت internet browser تخزين ملفات الكوكيز تلقائياً ومع ذلك يمكنك أن تختار رفض تخزين بعض ملفات الكوكيز أو أن يطلب موافقتك قبل أن يحفظ أي كوكيز على القرص الصلب، من خلال تعديل الأفضليات في المتصفح. ومع ذلك إذا رفض المتصفح تخزين ملفات الكوكيز قد لا تتوفر بعض مزايا الموقع لك، وقد لا تعرض بعض صفحات الموقع بشكل ملائم. ويهدف الكوكيز إلى جمع بعض المعلومات عن المستخدم وكيفية استخدامه لجهاز الحاسب الآلي، فعلى سبيل المثال يستطيع الكوكيز تسجيل قائمة بمواقع الويب المزارة من خلال الحاسب الآلي، ويمكن استخدام الكوكيز في الإعلان المباشر للزبائن المحتملين، ومعرفة كلمة السر الخاصة بالمستخدم في حالة المواقع التي تتطلب إدخال كلمة مرور لتسمح للمستخدم بزيارة الموقع، أيضا يمكن استخدام الكوكيز في تجميع معلومات شخصية عن المستخدمين من خلال سجلات استخدام الإنترنت records of internet use، وإعداد نسخة أخرى من البيانات العامة والخاصة الموجودة في قاعدة البيانات عن الأشخاص. وهذه المعلومات مثل: الاسم، العنوان، رقم التليفون، المرتب، التأمين الصحي، عادات الأكل إلى أخر ذلك[21].

3) قرصنة البرامج والشبكات Software and Network Piracy

قرصنة البرامج software piracy هي نسخ برامج الحاسب الآلي التي تتمتع بحق النشر أو التأليف دون تفويض أو ترخيص. وهناك أساليب عديدة لنسخ هذه البرامج، منها: نسخ برنامج من قرص مرن لقرص آخر، أو تحميل البرنامج على جهاز الكمبيوتر من على شبكة الإنترنت وعمل نسخة منه[22].

أما قرصنة الشبكة network piracy فهي توزيع المواد التي تتمتع بحق النشر والتأليف في صورة تسجيلات رقمية عبر شبكة الإنترنت دون الحصول على ترخيص بذلك[23].

4) الانتهاكات التي تتعرض لها نظم المعلومات من خلال الأشخاص :

أ. الموظفون

يعد الموظفون من العناصر الأساسية التي قد تؤدي إلى تهديد أمن المعلومات بالمكتبة وإلحاق الضرر بها، سواء بشكل مقصود نتيجة لدافع معين (الرغبة في الإساءة للمكتبة، الكراهية، الملل، الطمع، أو الرغبة في التحدي)، أو بشكل غير مقصود، فبعض الموظفين قد لا يكونون على المستوى الفني المطلوب، ومن ثم فقد يتسببون في تدمير البيانات في النظام دون قصد[24].

وقد يرتكب الموظفون أخطاءً فاحشة وساذجة، وتؤدي في الوقت نفسه إلى كوارث معلوماتية، ومن تلك الأخطاء[25]:

1. تعليق كلمات المرور: فكثيرا ما يقوم المستخدمون بتدمير كل إجراءات أمن المعلومات بلصق كلمات المرور على مقدمة

شاشة الحاسب، أو على سطح المكتب، حيث يمكنهم رؤيتها بسهولة، هم وكل من حولهم، ثقة منهم فيهم أو لأي سبب آخر، وقد أثبتت دراسة حديثة أن 20٪ من موظفي تكنولوجيا أمن المعلومات يفعلون ذلك .

2. ترك الجهاز مفتوحا: والابتعاد عنه للحظات أو لمدة من الوقت، وهو ما يسهل مهمة السارق في حصوله على كلمة المرور، وبخاصة إذا كان خبيرا بما يفعل أو عليما بما يريد .

3. فتح مرفقات البريد الإلكتروني: فالبعض لا يكلف نفسه عناء التفكير فيما ورد إليه من رسائل .

4. اختيار كلمة مرور سيئة: وهذا ما يخيف خبراء أمن المعلومات؛ إذ يمكن للمقربين التكهن بهذه الكلمة التي ترتبط باسم الابن، أو فريق الكرة، وكلما طالت الكلمة وتعقدت كان التكهن بها أصعب أو مستحيلا، ولاختيار كلمة المرور قواعد يحسن أن تقوم المؤسسات باتباعها .

5. الثرثرة: كأن يجلس الشخص ويقول: لقد غيرت كلمة المرور إلى كذا، أو أضفت كذا، أو حذفت كذا، ولا يدري أنه قد يكون هناك من يتلقف هذه المعلومة ويسهم مباشرة أو بطريقه غير مباشرة في مخاطر جمة .

6. تجاهل سياسة أمن المعلومات: فمهما كانت هذه السياسة جيدة، فإن إهمالها يتساوى مع عدم وجودها، فهناك من العاملين من لا يقتنع بهذه القواعد، ويرى أن لديه الأسباب الوجيهة لإهمالها، فمثلا قد يعطل بعضهم برامج الكشف عن الفيروسات، لأنها تبطئ من سرعة الجهاز .

7. الفشل في مراقبة الموظفين: لأنهم أعلم بأوجه الضرر أكثر من غيرهم .

8. البطء في مواكبة المستجدات: فالجريمة بشكل عام، وجرائم المعلومات بشكل خاص في تطور مستمر، وهي في أغلب الأحيان تسبق وسائل الأمن والحماية، لذا ينبغي تحديث وسائل وسياسات أمن المعلومات بشكل دائم .

ووفقا للدراسات الخاصة بمجال العمل فإن معظم المشكلات الأخلاقية ethical problems متعلقة بالأشخاص المتخصصين في المهنة ؛ إذ إن المهنيين professional يؤدون دوراً مفتاحياً في أي مهنة. كما أن الغالبية العظمى من هذه المشكلات تكون بين الأطباء doctors والمحامين lawyers. ولذلك فإن العديد من المهن خاصة التي تتطلب مهارة واحترافاً من الأشخاص المشتغلين بالمهنة تمتلك تشريعات خاصة بها professional codes وهذه التشريعات تقوم بضبط وتعديل سلوكيات وأنشطة أهل المهنة الواحدة. لأن أهداف وإخلاص العاملين في المهنة الواحدة لا تكون واحدة تجاه المستفيدين أو العملاء. فعلى سبيل المثال، تنص التشريعات في مجال الطب على أنه من الضروري حصول الطبيب على موافقة كتابية من المريض قبل أن يجري العملية الجراحية. أما في مجال المكتبات والمعلومات، فإن العلاقة ما بين أمين المكتبة والمستفيدين تكون عبارة عن عقد أو اتفاقية أو دفاع عن الثقة، وهذا العقد لا يعتمد فقط على مساعدة المستفيد في الوصول إلى المعلومات التي يحتاج إليها واتخاذ القرار، فإنه يمتد أيضا إلى المحافظة على المعلومات الشخصية للمستفيدين وحماية خصوصيتهم وعدم الكشف عن أي معلومات عنهم إلا بعد الحصول على موافقتهم[26].

ب. المستفيدون

لابد من تدريب المستفيدين ومستخدمي النظام بشكل كاف فقد يتعمد بعض المستفيدين إلحاق الضرر بالنظام، وذلك بعمل الفيروسات، أو إلحاق الضرر بالأجهزة، وقد يكون الدافع لذلك هو تحدي الإجراءات الأمنية المتشددة التي تتبع ضدهم، ومن ثم لابد من توعية المستفيدين بالأسباب التي تدعو إلى استخدام كلمات المرور، والخروج من النظام log off بطريقة سليمة، وضرورة عمل مسح للأقراص المرنة في حالة جلبها معهم للتأكد من خلوها من الفيروسات[27].

المجموعة الثانية: جرائم تقع بواسطة الحاسب الآلي والإنترنت

إن الجرائم التي تقع بواسطة الحاسب الآلي والإنترنت، أو بمعني آخر الجرائم التي وسيلتها الحاسب الآلي والإنترنت، هي تلك الأفعال التي تتخذ من شبكة الإنترنت وسيلة لارتكابها، من أجل سلب قيمة مادية أو أدبية أو اجتماعية تتجاوز حدود جهاز الحاسب الآلي وشبكة الإنترنت ومنها :

1) المواد الإباحية Pornography

المواد الإباحية هي عبارة عن صور وكتابات وأي مواد أخرى ذات طابع جنسي وتكون في متناول الجميع على شبكة الإنترنت، وتعد صناعة ونشر الإباحية جريمة في العديد من الدول إلا أننا نجد أن مصطلح المواد الإباحية Pornography يتمتع بالحماية القانونية من خلال التعديل الأول للدستور الأمريكي the First Amendment الذي يتغاضى أحيانا عن إباحية الكبار بدعوى الحق في حماية الخصوصية Right of Privacy وحق الفرد في بث أفكاره ونشرها والتعبير عنها بحرية، أما مصطلح الدعارة Obscenity فهو لا يتمتع بحماية التعديل الأول للدستور الأمريكي the First Amendment خاصة عندما يتعلق الأمر بإغراء أو إكراه الأطفال على المشاركة في أي نشاطات جنسية غير قانونية، واستغلال الأطفال لأغراض الدعارة أو في العروض أو في المواد الإباحية[28].

2) جرائم الابتزاز والقذف وتشويه السمعة Defamation

تهدف جرائم القذف وتشويه السمعة إلى إبراز سلبيات المستهدف ونشر أسراره التي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، خاصة أن غالبية مستخدمي شبكة الإنترنت لا يكونون على قدر كبير من الحذر والحرص أثناء وجودهم على الشبكة، أو بالافتراء عليه بأخبار غير صحيحة بهدف الإساءة إلى أو تشويه سمعة الشخص[29]. ومن أمثلة هذه الجرائم القضية رقم 6692 إداري شبرا الخيمة، حيث قدمت النيابة العامة المتهم للمحاكمة بالتهم الآتية، أولا: قذف المجني عليها علانية من خلال البريد الإلكتروني بعبارات خادشة لشرفها وهي عبارات تضمنتها وحوتها إحدى عشرة رسالة أرسلها إليها المتهم باستخدام الإنترنت. ثانيا: تعمد المتهم مضايقة المجني عليها، حيث تضررت المجني عليها من قيام المتهم بإرسال رسائل إليها بطريق البريد الإلكتروني عبر شبكة الإنترنت على عنوان البريد الإلكتروني الخاص بعملها تضمنت عبارات سب وقذف وتشهير بها وإرسال صور فاضحة مخلة بالآداب العامة وخادشة للحياء،

وأن تلك الرسائل علم بها كافة زملائها بالعمل مما سبب لها أضرارا معنوية كبيرة، وأنه بضبطه وضبط الجهاز المستخدم أقر بارتكابه للواقعة بقصد التشهير بها[30].

أما عمليات الابتزاز فهي قد ترتكب من جانب موظفي المؤسسة أو المكتبة الحاليين أو السابقين أو المؤقتين، كما قد ترتكب من جانب المستفيدين أو الموظفين كذلك؛ إذ تشجع حالات عدم الرضا الوظيفي بعض الموظفين على ارتكاب هذا النوع من الجرائم خاصة عند قيام المؤسسة أو المكتبة بفصل بعضهم خلال إجراءات تخفيض العمالة مثلا[31].

ومن أمثلة هذه الجرائم قيام موظف بقسم المعلومات بهيئة المصل واللقاح بإنشاء موقعين عبر الإنترنت مستخدما البريد الإلكتروني لهما وهما يحملان الاسم التجاري للهيئة على شبكة الإنترنت وأرسل إلى الشركات العالمية والمتعاملين مع الهيئة ووكلائها في مصر والخارج رسائل تتضمن سبا وقذفا وتشهير بالشركة وتخوفا من منتجاتها وخاصة الأنسولين والمستحضرات الأخرى، وتم القبض عليه ولقد اعترف بارتكابه الواقعة بسبب تأخير صرف المكافأة 15 يوما، وسوء معاملة المسئولين له[32].

3) انتهاك الخصوصية

الخصوصية الفردية هي حق الفرد في حجب معلوماته الشخصية عن الآخرين. ويعد التطفل على مكتب شخص آخر أو منزله أو جهاز الحاسب الشخصي الخاص به والاطلاع فقط على ما به من بيانات أو حتى أفكاره يعد انتهاكا لهذه الخصوصية[33].

ولا يقتصر الأمر على المعلومات الموجودة في الحاسب الآلي الخاص بالفرد بل يمتد إلى المعلومات الشخصية الموجودة على الإنترنت، فأنت عند اتصالك بأي موقع على الإنترنت فإما أن يترك هذا الموقع على جهازك بعض الملفات الصغيرة (Cookies) أو يحصل منك، سواء برغبتك أو دون أن تدرى على الكثير من المعلومات المسجلة في حاسبك الشخصي[34]. فبمجرد الدخول إلى صفحة الموقع فإن معلومات معينة تتوفر عن المستخدم وهي ما يعرف بمعلومات رأس الصفحة (Header Information) وهي التي يزودها الحاسب الآلي المستخدم للحاسب الآلي الخادم الذي يستضيف مواقع الإنترنت، وهذه المعلومات قد تتضمن: عنوان بروتوكول الإنترنت للمستخدم (IP) ومن خلاله يمكن تحديد اسم النطاق وتبعا له تحديد اسم الشركة أو الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها والمعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل المستخدم، ووقت وتاريخ زيارة الموقع ومواقع الإنترنت وعنوان الصفحات السابقة التي زارها المستخدم من قبل دخوله الصفحة في كل زيارة. وقد تتضمن أيضا معلومات محرك البحث الذي استخدمه المستخدم للوصول إلي الصفحة. وتبعا لنوع المتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم[35].

المراجع :

1. Fifarek, Aimee. Technology and privacy in the academic library .- Online Information Review .- v.26 , n.6 (2002) .- p.366 .

2. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- الاتجاهات الحديثة في المكتبات والمعلومات – مج9، ع18 (يوليو 2002) .- ص249 .

3. Gregory, B. Newby .Information security for libraries .-p.1 .- available at: http://www.petascale.org/papers/library-security.pdf

4. Ibid .- p. 2 .

5. Peltier, Thomas R. "Implementing an information security awareness program". Information Systems Security.- v.14, n.2(May/Jun2005).- p.38

6. Thompson , D. .Computer crime the improvement of investigative skills .- National pp. 6- 11.

7. نادية أمين محمد علي. الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات. في: المؤتمر الدولي حول أمن المعلومات "نحو تعامل رقمي آمن" 18-12/20/ 2005. مسقط- سلطنة عمان: المنظمة العربية للتنمية الإدارية جامعة الدول العربية، بلدية مسقط سلطنة عمان، 2005 .- ص205 .

8. Boss, R.W. Security technologies for libraries: policy concerns and a survey of available products.- library technology reports.- v.35,n.3 (1999).- p.337

9. Ibid.- p.337 .

10. حسن طاهر داود. أمن شبكات المعلومات .- معهد الإدارة العامة: الرياض، 2004 .- ص 170 .

11. حيث ترك الجيش الإغريقي حصاناً خشبياً ضخماً، كهدية لسكان طروادة، وكان يختبئ ضمنه مجموعة من الجنود الأشداء، بعد أن تظاهروا بإنهاء الحصار الطويل، وعندما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجند منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق .

12. حسن مظفر الرزو. الأمن المعلوماتي العربي: معالجة أولية .- مرجع سابق .- ص90 .

13. نفس المرجع السابق والصفحة .

14. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- مرجع سابق .- ص 260 .

15. حسن مظفر الرزو. الأمن المعلوماتي العربي: معالجة أولية .- مرجع سابق .- ص 90 .

16. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- مرجع سابق .- ص 260 .

17. أشرف الغنيمي ؛ إعداد ومراجعة خالد العامري .- نظم الحماية من قراصنة الكمبيوتر .- ط1 .- دار الفاروق للنشر والتوزيع، 1998 .- ص 48 .

18. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- مرجع سابق .- ص 260 .

19. Computer intrusions and attacks .- The Electronic Library .- v.17 , n2 (April 1999) .- pp. 116- 117.

20. سيف عبد الله الجابري. أمن المعلومات والخصوصية الفردية. في المؤتمر الدولي حول أمن المعلومات "نحو تعامل رقمي آمن" 18-2005/12/20 .- مسقط- سلطنة عمان: المنظمة العربية للتنمية الإدارية جامعة الدول العربية، بلدية مسقط سلطنة عمان، 2005 .- ص 248.

21. Computer intrusions and attacks .- The Electronic Library .- v.17 , n2 (April 1999) .- pp. 116- 117

22. شريف درويش اللبان. تكنولوجيا الاتصال: المخاطر والتحديات والتأثيرات الاجتماعية .- ط1 .- القاهرة: الدار المصرية اللبنانية، 2000 .- ص 205 .

23. المرجع السابق .- ص 206 .

24. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- مرجع سابق .- ص 264 .

25. علي بن ضبيان الرشيدي. العدوان على البيئة المعلوماتية خطورته ومواجهته .- مجلة كلية الملك خالد العسكرية .- ع81 (مايو2005) .- متاح في:
http://www.kkmaq.gov.sa/Detail.asp?InNewsItemID=164260

26. Hannabuss, Stuart. Teaching library and information ethics .- Library Management .- v.17 , n.2 (1996) .- pp.27 28 .

27. فاتن سعيد بامفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة .- مرجع سابق .- ص 264 .

28. Nelson, Norman. Legal and liability issues related to internet access .- Library Administration & Management .- v.15 , n.1 .- pp.14- 15 .

29. Eisenschitz, Tamara. Internet law and information policy .- Aslib Proceedings .- v.50 , n.9 (October 1998) .- pp. 268- 269 .

30. محمد محمد الألفي. جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت .
http://www.eapiic.org/PortalArabic/Portals/0/Studies/MElalfy3.pdf

31. حسن طاهر داود. جرائم نظم المعلومات .- مرجع سابق .- ص 49 .

32. محمد محمد الألفي. أهم صور جرائم الإنترنت .- مرجع سابق .

33. حسن طاهر داود. جرائم نظم المعلومات .- مرجع سابق .- ص 50 .

34. حسن طاهر داود. جرائم نظم المعلومات .- مرجع سابق .- ص ص 50- 51 .

35. سيف عبد الله الجابري. أمن المعلومات والخصوصية الفردية .- مرجع سابق .- ص 247 .