دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

العنوان:	جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات
المصدر:	المجلة العربية للدراسات الأمنية
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	المسند، صالح بن محمد
مؤلفين آخرين:	المهيني، عبدالرحمن بن راشد(م. مؤلف)
المجلد/العدد:	مج 15, ع 29
محكمة:	نعم
التاريخ الميلادي:	2000
الشهر:	محرم - ابريل
الصفحات:	147 - 207
رقم MD:	211739
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	الدول المتقدمة، الجريمة، الجاسب الألي، الإنترنت، أنظمة التشغيل، جرائم الحاسب الآلي، تعليم الطلاب، الحرب النووية، هيئة الدفاع الوطني، قواعد البيانات، الاتصالات الالكترونية
رابط:	http://search.mandumah.com/Record/211739

© 2021 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

جرائم الحاسب الآلي:

الخطر الحقيقي في عصر المعلومات

د. صالح بن محمد المسند(*)

د. عبدالرحمن بن راشد المهيني(**)

الأمور المسلم بها أن الحاسبات الآلية سمة من سمات العصر الحاضر وستستمر على هذا الحال في المستقبل، وعليه لا يمكن لأي إنسان يريد العيش على مستوى الأحداث أن يتجاهل أهميتها أو يعيش بدونها (ايسيسكو، ١٩٨٧ : ٣١).

وكانت بداية إنتاج الحاسبات الشخصية في أواخر السبعينات وأوائل الثمانينيات وكانت إمكانات تلك الأجهزة المنتجة في ذلك الوقت محدودة بشكل عام ولم تنتشر في قطاعات المجتمع بالشكل الذي شهده العالم في عقد التسعينيات الميلادية وحتى اليوم. ففي عام ١٩٥٠م كانت أعداد أجهزة الحاسب لا تصل إلى ١٠٠ جهاز ثم ازدادت إلى أن بلغت حوالي ١٠,٠٠٠ جهاز في عام ١٩٧٠م كما أنه قد بلغ ما أنتج من أجهزة الحاسب الشخصي

(*) كلية العلوم الاجتماعية - قسم المكتبات والمعلومات - جامعة الإمام محمد بن سعود الإسلامية، الرياض.

(**) كلية الشريعة - قسم الاقتصاد - جامعة الإمام محمد بن سعود الإسلامية، الرياض.

حتى نهاية عام ١٩٩١م فقط أكثر من خمسة وثمانين مليون جهاز، وهذا الرقم في تزايد مستمر، حيث تقدر أعداد الحاسبات اليوم إلى أكثر من ٧٠٠ مليون جهاز في العالم (الإنترنت والحاسب، يناير، فبراير، ١٩٩٨م؛ التعزي، ١٤١٤هـ). كما أنه «في عام ١٩٦١م كانت أل ٤ ملايين بيت من ذاكرة الكمبيوتر تكلف حوالي ٢٤ مليون دولار، وفي عام ١٩٩٤م تبلغ تكلفة نفس حجم الذاكرة إلى حوالي ٦٠ دولار أمريكي وفي أوائل هذا العام (١٩٩٨م) فإنه بإمكانك شراؤها بحوالي ٣٠ دولار أمريكي» (الإنترنت والحاسب، يناير، فبراير، ١٩٩٨: ٨).

ومع انتشار الحاسبات الشخصية في المنازل ومواقع العمل، بدأ التفكير في إيجاد وسيلة يمكنها أن تصل بين هذه الأجهزة. وقد كان الغرض في البداية من ربط هذه الأجهزة ببعضها هو المشاركة في استخدام بعض الطرفيات غالية الثمن كطابعات الليزر وأجهزة الرسم واسطوانات التخزين الصلبة، ولكن الأمر أخذ منحىً آخر بعد ذلك. فقد ظهرت أنظمة تشغيل عديدة ذات قدرات عالية في إدارة الشبكات المحلية[1]. كما ظهرت فيما بعد عدة وظائف جديدة للشبكات كاستخدام البريد الإلكتروني وغير ذلك من اختيارات ومميزات جديدة (التعزي، ١٤١٤هـ: ٢، ٣). وكان لكل هذا التطور آثار عظيمة على الفرد والمجتمع.

---

(١) الشبكة المحلية Local Area Network هي شبكة اتصال لنقل البيانات وتستخدم لربط عدد من الحاسبات، والطرفيات، والطابعات، وأجهزة تخزين البيانات الاحتياطية، وذلك ضمن جغرافية محدودة تصل مساحتها إلى عشرة كليومترات مربعة (Rowley, 1996: p 104).

يقول عضيمة في مقال له بعنوان «دور الحاسوب الشخصي في صياغة مجتمع عصر المعلومات:

أصبحت ثورة المعلومات التي تعزى إلى الحاسوب أعمق أثرًا من الثورة الصناعية، حتى إن تأثيرات الحاسوب في تغيير الأسس الاجتماعية والحضارية غدت بادية الوضوح في مجالات حياتنا كافة: في المؤسسات الحكومية والمكاتب وقطاعات النقل والتجارة والزراعة والتصميم الهندسي والثقافة والعلوم وفي حياتنا الشخصية نفسها. ولم يعد بإمكان أحد أن يتراجع عن هذه الثورة لأن في ذلك نزوعًا إلى الوراء، وضربًا من ضروب العبث. وعلينا جميعًا أن نتدارك ما فاتنا من زخمها، وأن نسعى إلى التحكم في عناصرها إذا كنا ننشد أن يكون لنا موضع قدم في مسيرة التطور الحضاري المتسارعة (عضيمة، ١٤١٦هـ: ١٣).

ومن العناصر التي يجب أن تحظى بنصيب وافر من العناية والاهتمام أمن المعلومات وأمن نظم المعلومات. فقد صاحب تنامي الحاسبات الآلية ووجودها في مواقع كثيرة، في العمل والمنزل وغير ذلك ومع تزايد الإقبال على الإنترنت واستعمالها بشكل أكبر في هذا العصر، أن ظهرت أنماط جديدة من الجرائم ونسل جديد من المجرمين ينبغي التعامل معه تعاملاً خاصًا. كما أن التخوف العالمي من التطور التقني في أساليب النسخ والتصوير عن طريق الناسخات والطابعات الملونة وما صاحبه من اتجاه نحو أفول دور المستندات الورقية والاتجاه نحو التعامل الإلكتروني أدى إلى ظهور أنواع أخرى من الجرائم هي جرائم تزوير البطاقات البنكية والائتمانية (بصلة، ١٤١٦هـ).

ولقد حظي موضوع جرائم الحاسب الآلي باهتمام كبير لدى الرأي العام والباحثين على حد سواء على المستوى العالمي وخاصة في الدول المتقدمة صناعيًا ومعلوماتيًا. ففي الولايات المتحدة الأمريكية، أنتجت هولي وود «Hollywood» في صيف عام ١٩٨٣م فلماً بعنوان «ألعاب الحرب «War Games» يحكي قصة طالب في المرحلة الثانوية استخدم حاسبًا شخصيًا للوصول إلى حاسب هيئة الدفاع الوطني وكان على وشك إشعال حرب نووية. وقد حاز هذا الفلم على اهتمام الرأي العام وتحليلات الصحافة. وفي خريف العام نفسه استخدم مجموعة من الطلاب في مدينة ميلواكي في ولاية وسكانسن الأمريكية حاسبات شخصية للدخول إلى نظم حاسبات منتشرة في عدد من الولايات الأمريكية تملكها الحكومة، والقطاع الصناعي، ومؤسسات الخدمات العامة مثل المستشفيات. حتى أنه أذيع أن هؤلاء الطلاب استطاعوا الدخول إلى حاسب أحد المستشفيات أكثر من ٨٠ مرة (Simddy, 1992:142). وفي العام نفسه أيضاً حاول مجموعة من الإرهابيين تفجير حاسب «شركة مان» الألمانية لاحتجاجهم على مساهمة الشركة في تطوير صواريخ حربية. وقد كانت الخسائر المالية كبيرة إلا أن ملفات البيانات الاحتياطية سلمت من الدمار (Sieber, 1986:15). وفي اليابان، تم البلاغ عن ٢٨٨ جريمة متعلقة بأجهزة الصرف الإلكتروني في عام ١٩٨١م وحده (Sieber, 1986:5). وفي كوريا الجنوبية، استطاع شاب بريطاني لا يتجاوز عمره السادسة عشرة التسلل إلى قواعد بيانات تابعة لمركز أبحاث الطاقة النووية الكورية عبر شبكة الإنترنت التي ارتبطت بها شبكات المركز مؤخراً (عبده، ١٩٩٥ : ٦٩). ومن حاسب متواضع بمنزله في لندن، استطاع طالب فاشل واسمه ريتشارد برايس (١٦ عاماً) أن يخترق شبكة معلومات

القوات الجوية الأمريكية وهو في غرفة نومه (الرياض، ١٤١٧ : ٣٤).

أما على مستوى البحث العلمي فقد تم عقد العديد من المؤتمرات والندوات لمناقشة جريمة الحاسب الآلي وأمن الحاسبات خلال العقدين الماضيين. فقد ناقش المؤتمر الوطني للحاسبات الآلية الذي عقد في مدينة الرياض عام ١٤١٢هـ أمن الحاسبات الآلية. كما نظم المركز المعلومات الوطني بوزارة الداخلية حلقة أمن الحاسب والمعلومات في الفترة ٥ ـ ٨ ـ ١١/ ١١/ ١٤١٩هـ، وتمت مناقشة عدد من أوراق البحث التي تناولت الموضوع. ونظمت شركة «IBC» مؤتمراً حول الاتصالات الإلكترونية وشبكات الحاسب الآلي في مدينة دبي في نوفمبر من عام ١٩٩٥؛ حيث تم مناقشة المشكلات الأمنية الناجمة عن تزايد الاعتماد على شبكات الحاسب الآلي في منطقة الخليج العربي (عبده، ١٩٩٥/ يناير: ١٠١). كما تم عقد ست ندوات ومؤتمرات في أمريكا وفرنسا وبريطانيا ونيوزيلاندا وفنلندا خلال شهري سبتمبر وأكتوبر فقط من عام ١٩٩٥م لمناقشة أمن الحاسبات الآلية (عبده، ١٩٩٥/ سبتمبر: ١١٨).

وعلى صعيد الاهتمام بدراسة قضايا أمن الحاسبات الآلية وتطوير أفضل الوسائل للحد من ظاهرة جريمة الحاسب الآلي فقد قامت «وكالة الحاسبات الوطنية National Computerization Agency في كوريا الجنوبية بإقامة مركز أبحاث مهمته وضع إجراءات أمنية وبرامج محكمة كفيلة بضمان حد أدنى من أمن النظم والشبكات (عبده، ١٩٩٥/ يونيو: ٦٩). كما تم إنشاء «المركز الوطني لبيانات جريمة الحاسب الآلي «The National Center of Computer Crime Data» في الولايات المتحدة الأمريكية. كما تم تأسيس «تحالف برامج الأعمال «Business Software Alliance» وهي

هيئة أمريكية هدفها محاربة القرصنة المعلوماتية على المستوى العالمي .

ويعتقد بعض الخبراء والمحللي والمستشارين أمن الحاسبات والمعلومات أنه سوف يكون لجريمة الحاسب الآلي أثر كبير على نظم المعلومات في المنظمات على جميع المستويات وكذلك على جميع أفراد المجتمع . بل ربما يصل تأثيرها على الأشخاص في ذلك المجتمع بذاتهم وخاصة مع وجود الإنترنت وانتشار استخدامها والاستفادة منها بشكل كبير في كل أرجاء المعمورة . فعالم اليوم يتزايد اعتماده على المعلومات وتقنياتها المختلفة . ومع التسليم التام بكل ما يمكن أن تقدمه هذه التقنية من إيجابيات وفوائد عظيمة ومتعددة إلا أنها أيضًا لا تخلو من سلبيات وأوجه قصور قد تكون محل استغلال سيئ من قبل قراصنة الفضاء الذين لديهم المهارات والمعرفة التقنية الضرورية . فالمتسللون «Hackers» يمثلون تهديدًا حقيقيًا في هذا الجانب وهم مسؤولون بدرجة كبيرة عن تعطيل أنظمة المعلومات والإضرار بها . ولكن ليس هؤلاء المجرمون هم الوحيدون الذين ينبغي التنبه لهم وأخذ الحيطة منهم . فالدلائل تشير إلى وجود منظمات إرهابية هدفها مهاجمة البنية التحتية للمعلومات مثل الإنترنت والهاتف والبنوك وغيرها من المواقع الحساسة وذلك لتحقيق أغراضها (Furnell, S.M & Warren, M. J., 1999:28) .

وعندما نمعن النظر في هذه الجرائم وأساليب ارتكابها ، فإن الفرصة متاحة الآن لهؤلاء المجرمين أفرادًا أو منظمات لإضعاف أو تقويض المجتمع دون الحاجة إلى إطلاق رصاصة أو صاروخ واحد . ومن أجل أن ندرك هذه الحقيقة ، فلنا أن نتصوركم من القطاعات الرئيسة في هذا المجتمع الحديث التي تعتمد على التقنية والتي بفقدانها ربما تحل كارثة في المجتمع ، ومن ذلك على سبيل المثال : القطاع الصحي ، وقطاع البنوك والمال ،

والقطاع الصناعي ، وقطاع النقل المواصلات ، والقطاع الحكومي . . . الخ . فأن ضعفت هذه القطاعات أو تقوضت بنيتها التقنية فسوف ينجم عن ذلك تعطل الصناعات ، وتجمد الأموال ، وفقدان العناية الصحية في المستشفيات ، إلى غير ذلك . كما أن كثيرًا من النشاطات التي نشأت وازدهرت بمصاحبة هذه التقنية الحديثة كالتجارة الإلكترونية سوف تكون أول الخاسرين وأول الضحايا إزاء هذه المشكلات المعقدة والجديدة على حياة الناس والمجتمع .

ومما يهدف إليه هذا البحث الوقوف عند هذه القضية المعاصرة ومحاولة التعرف عليها وعلى بعض أبعادها المختلفة وخاصة الأمنية وإبرازها للوجود ومن ثم محاولة طرح بعض الحلول والتوصيات في كيفية التعامل معها على مستوى الأفراد والمنظمات والدول ، وذلك من خلال الدراسة النظرية باستعراض ومراجعة أهم ما كتب فيها من دراسات وأبحاث تناولت هذا الموضوع .

وتحتوي هذه الدراسة على أربعة فصول ويندرج تحت كل فصل عدة مباحث وذلك على النحو التالي :

الفصل الأول : تمهيدي وفيه المباحث التالية :

ـ مشكلة البحث

ـ أهمية البحث

الفصل الثاني : وفيه المباحث التالية :

ـ تعريف الحاسب الآلي ومكوناته وخصائصه أو مميزاته .

ـ تعريف الإنترنت وتاريخ تطورها وخدماتها .

الفصل الثالث : جرائم الحاسب الآلي ، وفيه المباحث التالية :

ـ أنواعها ،

ـ فئات مرتكبيها .

ـ لماذا الاهتمام بجرائم الحاسب الآلي؟

ـ أثر جرائم الحاسب الآلي في المجتمع .

الفصل الرابع : مكافحة جرائم الحاسب الآلي وعلاجها ، وفيه المباحث التالية :

ـ عقوبات جرائم الحاسب الآلي في الشريعة الإسلامية والنظم السعودية .

ـ الجهود المبذولة في سبيل مكافحة هذه الجرائم .

ـ أساليب مكافحة ، منع جرائم الحاسب الآلي :

التوعية

سياسة أمن البيانات والمعلومات

خطة لمواجهة الظروف الطارئة

ـ التوصيات .

مشكلة البحث :

لقد تم إدخال الحاسب الآلية في المملكة العربية السعودية في بداية السبعينيات الميلادية واستشعرت أهميته . ومن العلامات والشواهد الدالة على انتشاره ونمو استخدامه كون المملكة العربية السعودية أكبر سوق تجارية

للحاسب في الشرق الأوسط، حيث بلغت وارداتها في تلك الفترة فقط من الحاسبات ومعدات معالجة البيانات حوالي ٦ , ١ بليون دولار أمريكي. وأن عدد الحاسبات الشخصية المتوفرة في المملكة إلى نهاية عام ١٩٨٩م جعلها في المرتبة الثانية من بين دول العالم النامية مسبوقة فقط بدولة البرازيل (O'Sullvan, Cited in Magzoub & Abdulaaly,1992) . وقد جاء في «النشرة الشهرية» لسفارة المملكة في واشنطن (1994 Saudia Arabia, May) أن مبيعات تقنيات المعلومات في المملكة تمثل ٦٠٪ (ستين بالمائة) من إجمالي المبيعات في منطقة الشرق الأوسط (نقلا عن الحلوة ١٤١٦هـ)، والإحصائيات المنشورة عن إجمالي المبيعات حديثا يجعل المملكة الدولة الثانية في دول الشرق الأوسط بعد مصر حيث يمثل السوق السعودي أكثر من ٤٠٪ من حجم التعاملات في المنطقة، ويقدر حجم المبيعات السنوية في مجال تقنية المعلومات ب ٣ آلاف مليون ريال سعودي.

ومن المتوقع أن يرتفع هذا الرقم مع ازدهار ونمو التجارة عبر الإنترنت (مجلة التدريب والتقنية، ع. ١١ ، ١٤٢٠هـ، البدر، ١٩٩٩م). كما ينبغي الإشارة هنا إلى أنه يقام معرض الرياض للحاسب الآلي سنويًا حيث اختتم معرض هذا العام (المعرض الدولي السابع عشر للكمبيوتر وتقنية المعلومات) قبل فترة وجيزة وعرضت فيه أكثر من ٤٥٠ شركة ومؤسسة معروضاتها. وتشهد مثل هذه المعارض إقبالاً كبيراً، حيث بلغ عدد الزوار لعام ١٩٩٨م أكثر من ٠٠٠ , ٧٧ زائر (مجلة التدريب والتقنية، ع. ١١ ، ١٤٢٠هـ).

ورغم أن دخول المملكة لعالم الإنترنت رسميًا جاء متأخرًا وذلك بعد صدور قرار مجلس الوزراء الموقر ذي الرقم ١٦٣ والمؤرخ في ٢٤/ ١٠/ ١٤١٧هـ والذي أناط بمدينة الملك عبد العزيز للعلوم والتقنية مهمة تنفيذ

إدخال خدمة الإنترنت إلى المملكة والتي بدأت فعلياً في ٢٦/ ٨/ ١٤١٩هـ، حيث تم ربط الجامعات السعودية بالمدينة إضافةً إلى شركات تقديم الخدمة التي تتولى عملية تقديم الخدمة للمستخدمين لها في المملكة، إلا أن عدد المستخدمين المحليين للشبكة العالمية في الستة أشهر الأولى يقدر بنحو (٣٠) ألف مشترك عن طريق مقدمي الخدمة، ويضاف إليه حوالي (٢٠) ألف عشرين ألف مستخدم عن طريق الجهات الحكومية التي تتوفر لها الإنترنت عن طريق المدينة . أما المستخدمون عن طريق السوق السوداء فيقدر عددهم بحوالي (١٠) عشرة آلاف مستفيد ليصبح المجموع حوالي (٦٠) ستين ألف مشترك يمثلون أقل من ٥ , ٠٪ من سكان المملكة (الصرامي، ١٤٢٠هـ).

إن جرائم الحاسب الآلي مع وجود ودعم الإنترنت وانتشارها السريع بهذا الشكل قد تمثل تهديدًا مباشرًا وفوريًا وسريعًا للأمن الوطني والاقتصاد المحلي والعالمي، وانتهاكًا لحقوق الأفراد والشركات على اختلاف أنواعها. وقد وجد المتسللون والمتطفلون ومحترفو الجرائم ضالتهم في الشبكة العالمية لممارسة جرائم مثل التزوير واختلاس الأموال والاستغلال الجنسي للأطفال. فقد أصبحت الأجهزة الحكومية والبنوك والشركات والأفراد فريسة سهلة لقراصنة المعلوماتية الذين يستغلون الثغرات ويوظفون معارفهم التقنية في اقتراف كل أنواع الجرائم ذات العلاقة بالحاسب الآلي. ومن الأمثلة لهذه الجرائم ما حدث من اختراقات لبعض مواقع الإنترنت لجهات سعودية حكومية وقطاع خاص وموقع شركة هندسية سعودية كبيرة في مدينة الرياض «mbce.com.sa» الذي تعرض لهجوم من قبل قراصنة من البرازيل. كما تعرضت مؤخرًا مواقع حساسة في الكويت والإمارات العربية المتحدة

ولبنان مثل موقع مطار الكويت الدولي ومصلحة الكهرباء والمياه في دبي وشركة دجي سيستم في لبنان لاختراقات قراصنة عبر الإنترنت (Jarrah,2000). وكذلك ما حصل للمصرف الأمريكي العملاق «سيتي بنك» الذي كان ضحية اختلاس لمبلغ قدر بعشرة ملايين دولار، وحادثة حجب الدخول إلى الخدمة لعدد من المواقع الشهيرة والمهمة في الإنترنت مثل موقع ياهو «yahoo.com»، وأكبر المواقع المستقلة ومواقع البيع بالتجزئة مثل باي إنك «buy.com» وإبي إنك «ebay.com» وأمازون «amazon.com» وسي إن إن «cnn.com» أيام الاثنين إلى الأربعاء من ٧ـ٩/ ٢/ ٢٠٠٠م مما كبد هذه المواقع خسائر قدرت بالملايين يوميًا (Wolf, J., 2000; DIT net Staff Reporter,2000). ولم تكن هذه هي المرة الأولى التي تهاجم مواقع شهيرة وحساسة بطريقة حجب الدخول إلى الخدمة. ففي الأسبوع الأول من مارس من عام ١٩٩٨م استطاع متسللو الحاسب مهاجمة العشرات من شبكات الحاسب الآلي في الولايات المتحدة الأمريكية من ضمنها جميع مواقع وكالة الفضاء والطيران الأمريكية «NASA»الخمسة عشر إلا موقعًا واحدًا، وكذلك موقع جامعة بيركلي في كاليفورنيا. وقد كان الهجوم مستهدفًا الحاسبات التي تشغّل بنظام نوافذ مياكروسوفت (Stephn, 1998:116).

وقد أحست العديد من الدول بخطورة الوضع وضرورة منع هؤلاء المجرمين الجدد من قرصنة الأنظمة المعلوماتية خصوصًا في المواقع الاستراتيجية. فقد طالبت الحكومة الأمريكية كلينتون بميزانية لعام ٢٠٠١م قدرها بليونا دولار لمواجهة المشكلات الناجمة عن القرصنة الفضائية بزيادة قدرها ١٥٪ عن العام الماضي (Wolf, J.,2000). وأنشأت السلطات

الأمريكية قبل سنة مركزًا لحماية شبكاتها مرتبطًا بجهاز المباحث الفدرالية (أف بي آي)[١] لمراقبة جميع المواقع التي تعتبر استراتيجية في الأراضي الأمريكية، مثل محطات الكهرباء ومصالح المياه والمصارف وأجهزة الطوارئ والدفاع.

ما طبيعة هذه الجرائم؟ وما آثارها الأمنية والاجتماعية والاقتصادية؟ ومن هم الأشخاص الذين يقومون بمثل هذه الأعمال؟ وما الوسائل التي تتبع في ارتكابها؟ وكيف يمكننا مواجهتها؟ كل هذه الأسئلة مثيرة حقًا وتبرز حاجة ماسة إلى أنه لابد من تحقيق الأمن في هذا الجانب، والقيام بالدراسات والأبحاث وسن الأنظمة والقوانين وزيادة التوعية للأفراد والمؤسسات في المجتمع. وستحاول هذه الدراسة الإجابة على هذه الأسئلة وتسليط الضوء على الجوانب التي تحتاج إلى مزيد من الدراسة والبحث الشرعي والقانوني.

أهمية البحث :

تكمن أهمية هذا البحث في النقاط الآتية :

١ ـ نظرًا لكون الحاسب الآلي من التقنيات الحديثة التي تستعين بها المنشآت والمنظمات للرفع من كفاءة وفاعلية أدائها ، فإن التعرف على بعض الجوانب السلبية لهذه التقنية أمر في غاية الأهمية والخطورة لإدارة تلك المنظمات .

---

(١) المباحث الفدرالية الأمريكية FBI مسؤولة عن الأمن الوطني على مستوى الولايات المتحدة الأمريكية.

٢ ـ محاولة هذا البحث في الإسهام في التعرف على بعض أوجه جوانب الجرائم التي ترتكب مع وجود الحاسب الآلي في المنظمات الإدارية والتوعية بها . فهذا البحث يتوقع منه أن يسهم في نشر الوعي لدى تلك المنظمات ولدى قياداتها الإدارية العليا من أجل أخذ الحيطة والحذر .

٣ـ قلة البحوث والدراسات في هذا المجال ليس على مستوى المملكة العربية السعودية فحسب ، بل على مستوى العالم العربي ومنظماته الإدارية المختلفة ، وأجهزته التشريعية والتنفيذية ، ويتضح ذلك من خلال مراجعة ما أتيح لنا مراجعته في المكتبة العربية ، وبالتالي فإن هذا البحث قد يكون خطوة إلى إلقاء المزيد من الضوء على مثل هذا الموضوع ومن ثم تشجيع البحث العلمي في هذا الجانب إثراء المكتبة العربية بمثل هذه النوعية من البحوث .

ولكي تكتمل الصورة وتتضح في ذهن القارئ فسوف نقدم في الفصل التالي نبذة موجزة عن الحاسب الآلي : تعريفه ، مكوناته ، خصائصه ومميزاته . وكذلك عن الإنترنت : تعريفها ، ومراحل تطورها ، وأساليب الاتصال بها ، واستخداماتها ، وخدماتها .

الفصل الثاني: تعريف الحاسب:

لم يبدأ اختراع الحاسب الآلي من فراغ ؛ فلقد كانت هناك محاولات عديدة وسابقة لتسهيل إجراء العمليات الحسابية وتطوير الوسائل لمعالجة البيانات ، ولا يزال هذا التطوير مستمرا إلى وقتنا الحاضر . ولو عدنا لكلمة حاسب آلي أو حاسوب واستخدامها لوجدناها ترجع إلى الفعل يحسب (Compute) ، ومن هنا يمكن ربط الحاسب الآلي وتطوره واستخدامه إلى

زمن قدرة المخلوق البشري على العدو والحساب . ومن هنا أيضا يمكن القول بأن المراحل الأولى لتطور الحاسب الآلي واستخدامه تبدأ من مراحل بدائية وذلك حينما استخدم الإنسان الحصى وأصابع اليدين في العد . بعد ذلك طور الصينيون العداد الصيني Abacus وكان ذلك سنة ٣٠٠٠ ق . م . كما أشار إلى ذلك بيسلر (Bassler) حيث قال بأن هذا العداد يحتمل أن يكون أول أداة عرفت للعد والحساب (Bassler,1976) وأنها استخدمت بشكل واسع ولا تزال تستخدم في العالم (Sanders, 1970; Sanders, 1985; Feingold,1975) إلى أن وصل إلى ما وصل إليه في وقتنا الحاضر .

يمكن تعريف الحاسب بأنه عبارة عن جهاز إلكتروني (مكون من مجموعة آلات تعمل معًا) مصمم لمعالجة وتشغيل البيانات بسرعة ودقة ، حيث يقوم هذا الجهاز بقبول البيانات وتلقيها وتخزينها آليًا ثم يجري عليها بعض العمليات الحسابية (الجمع ، الطرح ، الضرب ، والقسمة) والمنطقية (المقارنة بين شيئين أو أكثر ، الاختيار والتصنيف) ثم يستخلص ويستخرج نتائج هذه العمليات ، كل ذلك وفقًا واتباعًا لتوجيهات مجموعة تفصيلية من أوامر وتعليمات تسمى برامج وهذه البرامج معدة ومخزنة مسبقًا Stored-program . ويقوم الحاسب بأداء مثل هذه العمليات على البيانات الرقمية Numeric والبيانات الأبجدية Alphabetic أو عليهما معًا Alphanumeric . (طلبه وآخرون ، ١٩٩٢ ، الفيومي ١٩٨٩ ، ساندرز ١٩٨٥) .

مكونات الحاسب:

يتكون الحاسب بصفة عامة من العناصر التالية :

أ ـ وحدات الإدخال :Input Devices وهي الوحدات التي تقوم بقراءة

المدخلات مثل : لوحة المفاتيح ، الفأرة ، الأقراص المغناطيسية ، وحدات المسح الضوئية Scanners وغيرها .

ب ـ وحدات التشغيل أو المعالجة المركزية :Central Processing Unit (CPU) وهي الوحدة التي تقوم بتنفيذ العمليات المطلوبة والتي تتكون من الأجزاء الرئيسة التالية :

ـ وحدة الذاكرة الرئيسة التالية والتي تستخدم لتخزين البيانات والبرامج مؤقتا .

ـ وحدة التحكم والتي تقوم بالإشراف على تسلسل تنفيذ العمليات في الحاسب .

ـ وحدة الحساب والمنطق :Arithmetic & Logic Unit (ALU) والتي تقوم بتنفيذ كافة العمليات الحسابية والمنطقية .

ج ـ وحدات الإخراج :Output devices وهي الوحدات التي تعرض نتائج التشغيل مثل : الطابعة والنهاية الطرفية Terminal . (القاضي وآخرون ، ١٩٩٤) .

ولا تستطيع هذه الوحدات العمل بدون توفر الأشياء اللازمة لها والتي يمكن تقسيمها إلى قسمين هما : المعدات Hardware والبرمجيات Software .

وتضم البرمجيات الأجزاء الرئيسة التالية :

١ ـ أنظمة التشغيل Operating Systems والتي تقوم بعملية الإشراف على الوحدات المختلفة وتوجيه أعمالها .

٢ ـ البرمجيات الجاهزة Packages وهي مجموعة من البرامج الجاهزة

يستطيع المستخدم للحاسوب استعمالها لتأدية نمط معين من المعالجة ومن الأمثلة على هذه البرمجيات: برمجيات تحرير ومعالجة النصوص، برمجيات الجداول الإلكترونية، برمجيات الرسم والتصميم وغيرها الكثير.

٣ ـ البرامج التطبيقية: وهي برامج تكتب من قبل مستخدم الحاسب بإحدى لغات البرمجة (بيسك، فورتران، كوبول، باسكال . . . الخ) لحل مسألة معينة» (القاضي وآخرون ١٩٩٤ : ٦ ـ ٧).

والأجهزة والبرامج لا معنى ولا فائدة لأحدهما دون الآخر. فبدون البرامج لا يستطيع الحاسب الآلي إجراء أية عملية ذات فائدة. كذلك بدون الأجهزة، فإن البرامج لا تمثل أكثر من إجراءات لحل المسائل. ولا يستطيع نظام آلي إنجاز أي عمل بدون الأجهزة والبرامج المناسبة لذلك.» (شمروخ، ١٤١٥ : ٢٤).

خصائص ومميزات الحاسب الآلي:

يجمع معظم المؤلفين الذين كتبوا عن الحاسب الآلي بأن سبب الانتشار الواسع له يرجع لما يتميز ويختص به من خصائص ومميزات، من أهمها ما يلي:

ـ السرعة العالية في المعالجة والحصول على النتائج Speed. فالحاسب يستطيع تنفيذ ملايين العمليات في الثانية الواحدة. وكما ذكر شمروخ (١٤١٥) «بأن دقيقة واحدة من وقت الحاسب تساوي أكثر من ٦٧ ساعة من وقت موظف محترف في استخدام الآلة الحاسبة».

ـ الدقة العالية Accuracy. حيث يعطي الحاسب نتائج عالية الدقة، وذلك

لأن الحاسب يعطي نتائج خالية من الخطأ تماما إذا كانت البيانات المدخلة والتي تعتمد على العامل الإنساني صحيحة ويمكن أن يشار هنا إلى المصطلح المعروف Garbage in garbage out (GIGO).

ـ المصداقية أو الموثوقية وإمكانية الاعتماد عليه Reliability. فالحاسب يستطيع العمل المتواصل ولفترات طويلة دون أن يكل أو يمل أو يتعب بعكس الإنسان.

ـ القدرة على التخزين وإمكانيته الكبيرة في ذلك: فيمكننا أن نخزن فيه كميات كبيرة من البيانات والمعلومات والتي يمكننا الرجوع إليها في أي وقت وبسرعة.

ـ إمكانية تنفيذ تعليمات مخزنة. فالحاسب يمكنه تنفيذ الأوامر المخزنة دون تدخل من الإنسان.

ـ سهولة التعامل معه: فالتعامل مع الحاسب عملية سهلة خاصة بعد توفر البرمجيات الجاهزة، وكذلك إمكانية التعامل معه عن طريق المخاطبة. (القاضي وآخرون ١٩٩٤، شمروخ ١٤١٥، الفيومي ١٩٨٩).

ـ انخفاض التكاليف مقارنة بتكاليف التشغيل اليدوي، علاوة على أن هناك العديد من التطبيقات التي لم يكن من الممكن تحقيقها بدون استخدام الحاسب الآلي.

هذا بالإضافة إلى وجود فوائد أخرى منها أنها:

ـ تمد المديرين والعاملين بمرونة كبيرة وذلك بمساعدتهم في عملية اتخاذ القرارات وإمدادهم بالمعلومات في الوقت المطلوب.

ـ تمد العملاء والمستهلكين بإجابات فورية على استفساراتهم.

ـ تمكن المنظمة أو المؤسسة من النظر إلى المستقبل ومواجهة منافسات المؤسسات الأخرى بفعالية.

ـ ثم إن الاستخدام الشخصي للحاسب أدى إلى تحسين الظروف المعيشية والحياة المرفهة وذلك عن طريق المساعدة في حفظ السجلات الشخصية، وتقديم المساعدات التعليمية، وتمكين الأفراد من الوصول إلى بيانات مركزية للاستعلام عن الفنادق ورحلات الطيران المتاحة والحصول على معلومات عن سوق الأوراق المالية، والتسوق عن طريق الحاسب، وتقديم العاب مسلية وغير ذلك كثير. (سترن وسترن ١٩٨٣ ترجمة سرور والحمامي ١٤١٠هـ).

الإنترنـــت :

الإنترنت هي مجموعة من شبكات الحاسب الآلي المتصلة مع بعضها، أو هي شبكة الشبكات. وتصل الإنترنت ملايين الحاسبات في شبكة على مستوى العالم ومعدل زيادة الاستخدام في تزايد مستمر يوميًا. وتوفر الإنترنت اتصالاً دوليًا بواسطة مجموعة ضخمة من الشبكات مبنية على بروتوكولات «TCP/IP» وَ«OSI» وَ «SNA» وَ«NOVELL IPX/SPX». وقد بدأت الإنترنت كشبكة أكاديمية وأصبح استخدامها لجميع الأغراض هو السائد ولم تعد وسيلة اتصال بين الجامعات ومراكز البحث (Rowley, 1998:181).

مراحل تطور الإنترنت :

بدأت الإنترنت كشبكة واحدة كان اسمها أربانت «ARPANET» تم تطويرها عام ١٩٦٩م نتيجة لتجارب الحكومة الأمريكية لإنشاء شبكة تحويل

الحزم. وقد قامت وكالة مشروعات البحوث المتطورة «DARPA» التابعة لوزارة الدفاع الأمريكية بربط الباحثين بمراكز الحاسب الآلي في الولايات المتحدة الأمريكية ليتسنى لهم المشاركة في الموارد المتاحة من الأجهزة والبرامج مثل المساحة التخزينية وقواعد البيانات. ومن خلال هذا المشروع تم ربط عدد من الشبكات التي كانت تحت التجريب والتي تستخدم حزم الراديو والأقمار الصناعية بشبكة أربانت. في البداية سميت هذه الشبكات داربا إنترنت «DARBA INTERNET»، لكنها أصبحت فيما بعد تسمى فقط إنترنت. وقد تمخض عن هذا المشروع أبحاث وتطورات في مجال برامج اتصال الحاسبات مختلفة الأنواع مع بعضها البعض وتبادلها البيانات حيث كان له أعمق الأثر في دعم شبكات الحاسب الآلي التي طورت في ذلك الوقت وحتى وقتنا الحاضر. وأطلق على هذه البرامج ببروتوكولات الإنترنت «INTERNET PROTOCOLS (IP)»[1].

وقد كانت الاستفادة من خدمات الإنترنت في البداية مقصورة على الجيش الأمريكي، والشركات المتعاقدة مع وزارة الدفاع الأمريكية، والجامعات التي تجري بحوثًا لصالح الوزارة نفسها. وأثمر التطور في توفير نظم اتصالات آلية على مستوى أمريكا عن تعزيز الاتصالات بين مراكز البحوث الأكاديمية والجامعات. ويعد إنشاء شبكة مؤسسة العلوم الوطنية

(١) هو تقنية تسمح بنقل المعلومات من شبكة إلى أخرى عند الطلب، ويقوم بارسال حزم البيانات عبر بوابة الإنترنت وتوجيهها إلى أهدافها وكل حزمة IP ترسل بعنوان إلى أحد الحاسبات المتصلة بالإنترنت فهو بمثابة عنوان رسالة قبل وضعها في صندوق البريد.

في أمريكا في عام ١٩٨٨م علامة بارزة في تاريخ الإنترنت. فقد تم ربط الباحثين هناك باثني عشر مركز حاسب ضخماً على مستوى الولايات المتحدة الأمريكية. وقد كانت هذه المراكز أيضًا مرتبطة بشبكات معلومات إقليمية مما أدى إلى ربط هذه الشبكات وسهل تبادل البيانات فيما بينها. وهذه الخطوة أدت إلى ولادة الإنترنت كشبكة تعاونية ليس لها هيئة مركزية تديرها، وحلت شبكة مؤسسة العلوم الوطنية الأمريكية محل شبكة أربانت السابقة الذكر التي تم إيقافها في عام ١٩٩٠م. وفي الوقت الذي تم فيه بناء شبكة مؤسسة العلوم الوطنية نمت شبكة الإنترنت وتطورت واحتلت مكانة بارزة في ربط الشبكات والحاسبات والأفراد والاستفادة من خدماتها المتنامية يومًا بعد يوم (Rowley, 1998:181-182). وأول من فكر في إنشاء هذه الشبكة باحثون في مؤسسة سيرن (CERN). ويرجح أن استعمالها المكثف في المؤسسات العلمية قد تم على يد الباحث البريطاني تم برنارز لي Tim Barners Lee الذي فكر في اختراع طريقة يعجل بها نتائج الأبحاث بينه وبين زملائه بسهولة وسرعة فاخترع عام ١٩٩١ نظامه الخاص بنقل المعلومات مما أدى إلى ظهور ما يسمى ب World Wide Beb (WWW) وذلك داخل المختبر الأوربي للفيزياء العملية في جنيف بسويسرا. (بومعرافي، ١٩٩٧؛ قنديلجي وآخرون، ١٤٢٠؛ جرايمز، ١٩٩٩). ويرتبط بالشبكة العالمية في الوقت الحاضر ملايين المستخدمين في أكثر من ٨٠ دولة، ويبلغ معدل الزيادة حوالي ١٥٪ شهريًا، ويتوقع أن يبلغ عدد المستخدمين في عام ٢٠٠٣م أكثر من سكان آسيا وأفريقيا مجتمعين (الإنترنت والحاسب، يناير/ فبراير، ٢٩٩٨؛ بومعرافي، ٢٩٩٧).

أساليب الاتصال بالإنترنت :

يمكن الاتصال بالإنترنت من خلال عدة أساليب هي :

١ ـ الاتصال الكامل حيث يوجد اتصال دائم بين الحاسب والإنترنت باسم وعنوان مسجلين لدى الشبكة .

٢ ـ الاتصال بإدارة قرص الهاتف وذلك بواسطة اتصال مؤقت بجهاز يتوافر له اتصال دائم بالإنترنت .

٣ ـ الاتصال عبر البوابة وذلك من خلال اتصال بشبكة أو مزود خدمة مثل كمبيوسرف (Rowley, 1998:183) .

استخدامات الإنترنت :

يوجد ثلاثة استخدامات للإنترنت في الوقت الراهن هي :

١ ـ البريد الإلكتروني «E-mail» لتبادل الرسائل والملفات بين المستخدمين .

٢ ـ الأخبار حيث تستخدم الإنترنت بروتوكول نقل الإخبار الذي ينظم طريقة توزيع الأخبار ونقلها والاستعلام عنها .

٣ ـ بروتوكول نقل الملفات «FTP» الذي يمكن المستخدم من الاتصال واسترجاع الملفات المخزنة في مواقع بعيدة ونسخها وتحميلها .

٤ ـ الاتصال بالمواقع من بعد حيث يتمكن مستخدمو الشبكة من الدخول

---

(١) بروتوكول نقل الملفات File Transfer Protool يعرض قائمة بأسماء الملفات الموجودة على حاسب بعيد، ويمكن المستخدم من جلبها أو إرسالها من جهازه إلى جهاز آخر .

إلى أي موقع متاح في أي مكان من العالم (عباس، ١٩٩٩م: ٩٥ ـ ٩٨ ؛ Rowley, 1998:183).

الخدمات والمعلومات المتاحة على الشبكة :

تشمل الخدمات والمعلومات التي يمكن الحصول عليها من المواقع البعيدة :

١ ـ مجموعات النقاش حيث يستطيع المشاركون تبادل المعلومات وإجراء النقاش حول مختلف القضايا العامة والمتخصصة .

٢ ـ قواعد المعلومات الموضوعية التي تطورها المؤسسات الأكاديمية .

٣ ـ المعلومات المجتمعية من خلال المكتبات العامة وبعض مؤسسات المجتمع الأخرى .

٤ ـ مصادر المعلومات الحكومية وذلك بواسطة مواقع للجهات الحكومية .

٥ ـ فهارس المكتبات .

٦ ـ قواعد المعلومات التي تنشئوها جهات خاصة بهدف الربح .

٧ ـ لوحات الإعلانات .

٨ ـ العمليات التجارية والتسوق .

٩ ـ خدمات توصيل الوثائق (Rowley, 1998:183-184) .

الفصل الثالث: جرائم الحاسب الآلي :

يؤمن كثير من الناس بميزات الحاسب الآلي ومنهم من يغض الطرف عن كثير من سلبيات استخدامه حيث يعتقدون أن مخرجات الحاسب يتوافر فيها دائمًا الدقة والمصداقية ولا يرقى إليها الشك، وهذه النظرة خاطئة تحتاج

إلى إعادة نظر . ويتوارد إلى الذهن أسئلة تطرح نفسها بقوة في هذا الوقت بالذات، منها : هل نحن في العالم العربي وفي المملكة بوجه خاص نعيش في معزل عن جرائم الحاسب الآلي التي تحدث في العالم من حولنا أم نحن محصنون ضدها؟ . هل حدوثها عندنا أقل منه عند غيرنا؟ . أم هل نحن نعيشها واقعًا ولكن لا نعرف عنها شيئا الأمر الذي قلل وعينا واهتمامنا بها؟ . وإذا أردنا أن نجيب عن هذه التساؤلات، فيكفينا أن نجيب عن بعض الأسئلة التالية :

ـ ألم يتعرض حاسب أحدنا في يوم من الأيام إلى فيروس ما؟

ـ ألم يضطر أحدنا يومًا إلى أخذ جهازه الخاص إلى محلات الصيانة لإصلاحها؟ ثم هل تم الكشف على الجهاز بعد الإصلاح للتأكد من أن قطعه الأصلية موجودة أم بدلت من قبل بعض العاملين في هذه المحلات؟

ـ ألم تُسرق أجهزة الحاسب الآلي أو ملحقاته من مكتب أحدنا، أو مكتب صديق لنا، أو سمعنا عن سرقة هذه المعدات من المنظمة التي نعمل فيها؟

ـ ألم نر بعض الموظفين يستخدمون أجهزة الحاسب الآلي أو ملحقاتها في ما ليس له علاقة بالعمل؟

ـ ألم يتوقف أو يتأخر العمل في منظمة أحدنا بسبب موظف كان يعمل لديك في قسم الحاسب واستغنيت عن خدماته ، وبعد سفره لم يستطع الآخرون فتح الملفات أو قواعد البيانات التي أنشأها، وأخذ الأرقام السرية لفتحها معه؟

ـ ألم تتعرض بطاقة أحدنا الائتمانية إلى السرقة أو الاستعمال من قبل آخرين وتم تحميلها مبالغ إضافية لأغراض لم نقم بشرائها نحن؟

ـ ألم يتعرض حساب أحدنا في البنك إلى خصم مبالغ بسيطة (قد تكون هللات فقط) منه بدون علمنا، وبدون أن تشد انتباهنا للمطالبة باستردادها؟

ـ ألم يعترض أحدنا مجرماً عند استخدامه لمكائن الصرف الآلية ويطلب منه النقود التي سحبها من حسابه، أو أن يسحب له المزيد، أو سمعنا بقصص عن مجرمين فعلوا ذلك لآخرين عند استخدامهم لتلك الأجهزة؟

لا شك أن الإجابة عن هذه الأسئلة كلها أو بعض منها بنعم، وبناء على ذلك فكل هذه الأسئلة وغيرها مما يشابهها كثير هو ما ينعت في أدبيات علم المعلومات بجرائم الحاسب الآلي.

لماذا الاهتمام بجريمة الحاسب الآلي؟

لقد تغلغل الحاسب الآلي في كل مناشط الحياة في دول العالم النامي والمتقدم. وقد بلغ أكثر من ٨٠٪ من المعاملات المالية اليومية التي تتم في أمريكا من خلال تحويلات النقد الإلكترونية. كما أن العديد من البنوك، والمصارف، والأجهزة الحكومية، والشركات والمؤسسات الخاصة في معظم دول العالم وفي المملكة تعتمد على نظم الحاسبات الآلية بشكل أساسي. ولابد من الإشارة هنا إلى أن العديد من هذه النظم معرضة للهجمات الإجرامية والاختراقات.

ومما يزيد الأمر صعوبة أنه يصعب اكتشاف جرائم موظفي المنشأة عموماً وجرائم الحاسب الآلي على وجه الخصوص ومقاضاتهم لأنه لا يوجد في أغلب الأحوال شاهد للقضية ولا دلائل يمكن استخدامها للتوصل إلى الجاني (Sessions , 1991:13). كما أن كثيرً ا من المنشآت تتكتم على ما

يحدث لنظمها من اختراقات حيث تشير الإحصاءات إلى أن ١١٪ فقط من جرائم الحاسب يتم الإبلاغ عنها .

وبناءً على ما تقدم فإن من الأسباب التي أدت إلى الاهتمام بجريمة الحاسب الآلي أن نسبة كبيرة من المنظمات والمؤسسات الموجودة في عالم اليوم أصبحت تعتمد على نظم المعلومات بتزايد مطرد مما قد يعرض وظائفها للتعطل الكامل أو الجزئي في حال وقوع خلل في تلك الأنظمة . وقد ذكرت النتائج التي توصلت إليها إحدى الشركات الأمريكية الاستشارية «برايس واتر هاوس» أنه إذا فقدت بعض الشركات نظام المعلومات لديها لمدة تزيد عن ثلاثة أيام متتالية ، فإن نسبة احتمال إفلاسها تصل إلى ٦٠ ٪ ، بمعنى أنه كلما زادت مدة فقدان ذلك النظام المعلوماتي زادت الخسائر المترتبة على ذلك ، وإذا استمر فقدان الشركة لنظام المعلومات الخاص بها لمدة شهر فإن نسبة خروجها من السوق وإفلاسها تقفز إلى ٩٠٪ . (التعزي ، ١٤١٤هـ : ٢) .

كما يمكن أن يضاف سبب آخر للاهتمام بدراسة جريمة الحاسب ألا وهو انتشار شبكات الاتصالات التي تربط نظم حاسبات آلية يحوي بعضها معلومات على درجة كبيرة من الخطورة والسرية . وتشير التقديرات إلى أن ٦٠٪ من الحاسبات المصغرة في أمريكا (بلغ عدد ما بيع في أمريكا في عام ١٩٨٨ وحده ٤,٧ مليون جهاز) ربطت في شبكات (Nablett, 1993:7) . فما بالك بما بيع بعد هذا التاريخ وكذلك بعدد أجهزة الحاسب المربوطة في شبكات في الوقت الحاضر ! ! .

واتجهت كثير من الشركات الكبيرة والصغيرة على حد سواء وخصوصًا في الدول المتقدمة إلى إنشاء مواقع لها على شبكة الإنترنت بغرض الدعاية والإعلان عن الشركة ومنتجاتها وخدماتها ، والشركة إذ تقوم بذلك تعرض نفسها أمام ملايين البشر متعدية بذلك حواجز الحدود الإقليمية وتفتح أبواب معارضها للزائرين طوال الأربع والعشرين ساعة وفي كل أيام الأسبوع . ويوفر استخدام الإنترنت في المعاملات التجارية والنقدية إضافة إلى سعة الانتشار خفض العمالة والتكلفة حيث تصل تكلفة إنجاز العمليات التجارية عبر الإنترنت في بعض الأحيان إلى ٥٪ فقط من تكلفة إنجازها بالطرق التقليدية . إلا أنه يقابل ذلك جهل وعدم دراية من مستخدمي هذه التقنية بالأدوات المتاحة لحماية المعلومات عبر الإنترنت وكيفية عمل هذه التقنيات وما مدى صلاحيتها .

وتتزايد مخاطر جريمة الحاسب الآلي في دول العالم النامي خصوصًا في الدولة التي دخلت مجال تقنيات المعلومات بقوة كما هو الحال في المملكة العربية السعودية حيث بلغ عدد أجهزة الحاسبات الشخصية التي تم تسويقها في عام ١٩٩٤م حوالي ٧٤ ألف جهاز . ويتوقع أن تكون الزيادة في عدد الأجهزة بنسبة لا تقل عن ١٥٪ سنوياً للسنوات القادمة (الشرق الأوسط ، ١٩٩٥/ نوفمبر) . وتنتشر أجهزة الحاسب الآلي في القطاعات الحكومية وشركات ومؤسسات القطاع الخاص بل حتى في المنازل والمدارس . ونظرًا لحداثة دخول الإنترنت في المملكة لا توجد دراسات تكشف مدى ونوعية استخدامها في هذه القطاعات . إلا أنه يتوقع أن تكون الشركات والمؤسسات قد بدأت بتفعيل استغلال تطبيقات الإنترنت والاستفادة من الخدمات المتاحة من خلالها .

أثر جريمة الحاسب الآلي في المجتمع:

لا أحد يشك في خطورة جرائم الحاسب الآلي بمختلف أشكالها على الفرد والمجتمع . ومن هذه الآثار الخسائر ، والإصابات ، وانتهاكات حقوق الإنسان لقطاعات كبيرة من السكان ، وزعزعة الاستقرار الاجتماعي ، وتهديد سيادة الدول . حيث أصبح بإمكان المجموعات الإرهابية المدربة تدريباً جيداً التغلغل في المجتمع وتهديد أمن المطارات ، والمصانع الكيميائية ، ومحطات الطاقة النووية ، والصواريخ . . . وغيرها التي تسير بالحاسب الآلي ولا تطبق فيها إجراءات أمنية كافية . وقد حدثت هجمات على أنظمة حاسبات آلية من قبل جماعات إرهابية في كل من فرنسا وإيطاليا .

كما أن الاعتماد على النظم الإلكترونية في تزايد مستمر في القطاع المالي حيث يستخدم في تحويلات النقد وربط أسواق المال بشبكات اتصال ضخمة تعمل على مدار الساعة . فيمكن أن تسبب أي معلومات مغلوطة أو أي خلل كبير في الاتصال في مشكلات كبيرة وربما تذبذب خطير في أسواق المال . وربما تعد نتائج مثل هذه الأفعال وسهولة ارتكابها دافعاً قوياً للجريمة المنظمة التي تملك المال والخبرات والتنظيم الذي يمكنها من تنفيذ ذلك (Caelli, Lonley, & shain, 1989:322) . وقد أفاد استطلاع أجري في أواخر عام ١٩٩٤م في الولايات المتحدة الأمريكية لآراء مسئولي أمن الحاسبات الآلية أن هذه الجرائم تتزايد يوماً بعد يوم (عبده ، ١٩٩٥ ، مارس : ٩٩) .

كما أشار مسح شمل ١٠٠٠ مؤسسة أمريكية إلى أن الخسائر المؤكدة الناجمة عن جريمة الحاسب الآلي في أمريكا قدرت عام ١٩٨٥م ما بين ١٤٥ و ٧٥٠ مليون دولار . وتشير التقديرات إلى أن جرائم الحاسب الآلي التي

ترتكب في محيط العمل فقط تكلف القطاع التجاري الأمريكي حوالي ثلاثة مليارات دولار سنوياً (Coutoure , 1989:19) وقُدرت الخسائر الناجمة عن الجرائم ذات العلاقة بالحاسب الآلي التي تمنى بها الشركات الأمريكية أكثر من ٥ مليارات دولار سنوياً (Sessions , 1991 : p13) . وتحتل اليابان المرتبة الأولى في العالم في قرصنة البرامج حيث تقدر خسائر الشركات اليابانية المنتجة للبرامج حوالي ١,٣١ بليون دولار خلال عام ١٩٩٤م (عبده، ١٩٩٥ يونيو : ٦٩).

وبالإضافة إلى الكوارث المالية التي يمكن أن تسببها جرائم الحاسب الآلي للمؤسسات التجارية الصغيرة والأفراد، يمكن أن تهدد هذه الجرائم حياة فئات من المجتمع كما حدث في أحد المستشفيات الأمريكية؛ حيث قام أحد المجرمين بالدخول إلى حاسب المستشفى وعبث بملفاته وكانت النتيجة وفاة أحد المرضى. كما أن المحادثات الإلكترونية عبر شبكة الإنترنت أصبحت وسيلة تهدد سلامة المجتمع ونظامه الأخلاقي. فقد تسببت تلك المحادثات في ارتكاب أفعال شائنة وجرائم أخلاقية ضد الأطفال على أيدي أشخاص عديمي الأخلاق والضمير. فقد تم في ولاية فلوريدا في الولايات المتحدة الأمريكية مؤخرًا اعتقال رجل يبلغ من العمر أربعين عامًا بتهمة انتهاك عرض فتاة من ولاية مريلاند تبلغ من العمر ١٥ عامًا التقى بها عبر الإنترنت. كما أدين رجل من ماريلاند يبلغ من العمر ٢٣ عامًا لاتهامه باغتصاب طفلة صغيرة لا يتجاوز عمرها ١٢ عامًا التقى بها عبر نظام الإنترنت أيضًا.

وهذه النوعية من الجرائم قد تحصل على جميع مستويات الدول المتقدم منها والنامي كما أنها قد تحصل لجميع الأفراد سواء منهم الخبير في الحاسب

أو المبتدئ إذا لم تتبع الطرق الصحيحة للحذر منها والتحرز لوقوعها، فالجرائم التي تحصل في دول العالم على اختلافها تمت الإشارة إليها في ثنايا هذا الموضوع، أما ما قد يحصل للأفراد وخاصة الخبراء منهم فكثيرة ومنها ما حصل لخبير الحاسب الأمريكي شيمومورا «Shimomura» حيث تم تحويل البريد القادم إليه على الإنترنت إلى موقع آخر عن طريق أحد اللصوص. وتعرف هذه الطريقة بالاختطاف عن طريق إرسال E-Mail باسم الخبير.

أسباب انتشار الجرائم ذات العلاقة بالحاسب الآلي:

إن من أهم أسباب انتشار جرائم الحاسب الآلي صعوبة اكتشاف هذه الجريمة ومقاضاة المتهم لأنه لا يوجد في أغلب الأحوال شاهد للقضية ولا دلائل يمكن استخدامها للتوصل إلى الجاني (Sessions , 1991:13). وقد يستهان في هذه الجرائم أو يركن إلى السكوت عنها حيث أن كثيرًا من المنشآت التي تخترق نظم معلوماتها لا تلاحق مرتكبي هذه الجرائم قضائيًا مفضلة استقالتهم من أعمالهم ـ إن كانوا من داخل المنشأة ـ دون إثارة ضجة لئلا تشوه سمعة المنشأة. ويحاول كثير من مديري نظم المعلومات الإدارية التكتم على ما يحدث من جرائم ذات علاقة بالحاسب الآلي وعدم رفعها إلى المستويات الإدارية العليا في المنشأة، وتحاول المستويات العليا أيضًا أن تخفيها عن مجلس الإدارة، كما أن مجالس الإدارة يتجاهلونها إذا وصلت إليهم ولا يوصلوها إلى المساهمين (Stevens, 1987:75-76) مما أدى إلى إفلات كثير من القراصنة من العدالة وتشجيعهم على ارتكاب جرائم أخرى.

ومما يزيد الأمر صعوبة التطور التقني السريع الذي يساعد القراصنة

على كسر الحواجز واختراق النظم باستخدام تقنيات وبرامج أكثر تطورًا لم تؤخذ في الحسبان عند وضع إجراءات الحماية. وقد سهل انتشار شبكة الإنترنت في الآونة الأخيرة على مستوى عالمي اختراق نظم المعلومات المرتبطة بالشبكة من قبل قراصنة المعلومات الذين يقبعون في أماكن بعيدة لم تكن تشكل خطرًا في السابق لانعدام الوسيلة. ولاحظ سكوت شارني المسؤول عن مكافحة الجريمة على الإنترنت في وزارة العدل الأمريكية أن: «الكمبيوتر الموصول بشبكة الإنترنت أصبح سلاحًا لاقتراف هذه الجرائم في عالم بلا حدود». وأضاف أن: «شبكة الإنترنت تسهل الجريمة أيضًا على غرار دعارة الأطفال». واعترف دوغلاس بيريت أحد المسؤولين في مركز الحماية من جرائم الحاسب الآلي التابع للشرطة الفدرالية الأمريكية بأنه: «لا يمكننا أن نتوقع كل شيء لأن تحديد الخطر أمر بالغ الصعوبة» (الرياض، ١٤١٠هـ).

كما أن غياب الأنظمة والقوانين الرادعة نظرًا لجدة هذه الجرائم على المجتمع أدت إلى انتشارها واستفحال خطرها مما ينجم عن عدم إلحاق العقوبات المناسبة بمن يقبض عليه من القراصنة. ويمكن أن يضاف إلى هذه الأسباب أيضًا ضعف الوعي بهذه الجرائم وأساليب ارتكابها وكيفية الحماية من أخطارها.

الجريمة التقليدية وجرائم الحاسب الآلي:

تعد جريمة الحاسب الآلي من الجرائم الرئيسية في العصر الحاضر، وذلك من حيث تداخلها مع جرائم أخرى كالنصب والسرقة والتزييف والتزوير، ولكنها مع ذلك تمثل شكلاً من الجرائم ذات هوية خاصة؛ الأمر

الذي يستلزم معه سن القوانين والتشريعات لتجابه وتواكب التنامي المتوقع لهذه الجريمة. ونرى أن جرائم الحاسب الآلي هي جرائم ذات خصوصية تستوجب أساليب ورؤية وبحث وتحر وملاحقة ومنظمات وأشخاص وتدريب من نوع خاص ومختلف.

وبمعنى آخر إن هناك أهمية لتطوير أو تطويع أو إيجاد نصوص في القانون الجنائي لتجريم من يرتكب مثل هذه الأعمال بشكل مباشر. وكذلك تطوير أو إيجاد المؤسسات والأشخاص المدربين الذين يقومون بعملية الرقابة والملاحقة والمكافحة لمثل هذه النوعية من الجرائم.

تعريف جريمة الحاسب الآلي:

تستخدم عدة مصطلحات في أدبيات الموضوع لوصف ظاهرة جريمة الحاسب الآلي تبعًا لتنوع الجرائم واختلاف أشكالها وأساليب ارتكابها. وفيما يلي تعريف لهذه المصطلحات :

جريمة الحاسب الآلي:"Computer crimes" إساءة استخدام الحاسب الآلي بطريقة غير مشروعة حيث يستخدم في ارتكاب الجريمة. أو حسب تعريف وزارة العدل الأمريكية، أي جريمة وظف مرتكبها معرفته بتقنية الحاسب الآلي.

الجريمة ذات العلاقة بالحاسب الآلي :"Computer related crimes" مصطلح واسع يشمل أي تصرف غير مشروع يتطلب ارتكابه معرفة بتقنيات الحاسب الآلي.

إساءة استخدام الحاسب الآلي «computer abuse» : أي تصرف متعمد يجمع بين الحاسب الآلي، ومرتكب واحد أو أكثر جنوا أو كان بإمكانهم

أن يجنوا ثمار فعلهم، وضحية أو عدة ضحايا عانوا أو كان محتملاً أن يعانوا أو يفقدوا شيئاً نتيجة ذلك الفعل.

التحايل باستخدام الحاسب الآلي «computer fraud» : أي سلوك تحايلي مرتبط بالحاسب الآلي بقصد استغلال فرص بطريقة غير مشروعة (Caelli, Lonley, & shain, 1989:320).

أنواع جريمة الحاسب الآلي وفئات مرتكبيها:

جرائم الحاسب الآلي ليست فئة واحدة أو نوعًا واحدًا، إلا أنه يمكن تصنيفهما في فئتين عريضتين تندرج تحتهما كل جرائم الحاسب الآلي المعروفة حتى الآن:

١ ـ الحاسب الآلي كأداة للجريمة: عندما يستخدم المجرم الحاسب الآلي كأداة فإن الجريمة التي ترتكب هي جريمة تقليدية كالسرقة ولكن ارتكبت باستخدام أسلوب غير تقليدي. فالمجرم في هذه الحالات يستخدم الحاسب الآلي كأداة مثله مثل استخدام القلم في التزوير أو استخدام القنابل الإرهابية. ومعظم الجرائم ذات العلاقة بالحاسب الآلي التي تحقق فيها المباحث الفيدرالية الأمريكية تقع ضمن فئة استخدام الحاسب الآلي كأداة للجريمة.

٢ ـ الحاسب الآلي هدف للجريمة: يحدث هذا النوع من الجرائم داخل المؤسسة بواسطة موظف من موظفيها أو بواسطة مجرم من خارجها. ويستخدم في التهديد الخارجي شبكات الاتصالات السلكية واللاسلكية من أجل الوصول غير القانوني لنظام الحاسب الآلي (Sessions, 1991: 13-14 ,Carter, 1995:21-23).

ويمكن تصنيف جرائم الحاسب إلى فئات حسبما اعتبرته قوانين بعض الولايات الأمريكية داخلاً ضمن جرائم الحاسب :

١ ـ الوصول غير المرخص لنظام الحاسب[١] : يشير الوصول غير المرخص لنظام الحاسب الآلي في هذا السياق إلى التفاعل مع النظام، أو استرجاع معلومات منه، أو تخزين بيانات فيه، أو استخدام وسائل الاتصالات للاتصال بنظام آخر .

٢ ـ سرقة خدمات الحاسب الآلي : تحدث سرقة خدمات الحاسب عندما يستخدم فرد دون إذن مسبق نظاماً يخص فرداً أو جهة أخرى كاستخدام موظف في مؤسسة حاسب تلك المؤسسة لأداء أعمال تخص مؤسسة أخرى أو تخصه هو .

٣ ـ العبث بعمليات الحاسب الآلي : يشمل هذا النوع من جرائم الحاسب أي نشاط لا يستند إلى تفويض يهدف إلى التلاعب بعمليات الحاسب، أو إيقافها، أو منع مستفيدين مفوضين من خدمات الحاسب الآلي كزرع

---

(١) الوصول غير المرخص unauthorized access of computer systems . كثرت في الآونة الأخيرة إصابة بعض الأجهزة المرتبطة بشبكة الإنترنت ببرامج ما يسمى بـ: «برامج الباب الخلفي BACK DOOR » . ومن أشهر تلك البرامج برنامج نت بص NET BUS والذي يصيب أجهزة الحاسب التي تستخدم أنظمة WINDOWS 95/98 وبرنامج باك أورفيس BACK ORIFICE والذي يصيب أنظمة WINDOWS 95/98 . وعندما يصاب جهاز مرتبط بشبكة الإنترنت بأحد هذه البرامج يستطيع أي مستخدم لشبكة الإنترنت ـ يقوم بتحميل برنامج العميل CLIENT لذلك البرنامج أن يخترق الجهاز المصاب ويتحكم فيه عن بعد . فيستطيع أن يقرأ جميع المعلومات التي على الجهاز بما في ذلك ملفات النظام والتي تضم كلمات السر PASSWORDS .

قنبلة زمنية موقوتة تؤدي إلى إيقاف عمليات النظام في حال توفر شروط محددة .

٤ ـ إساءة استخدام المعلومات المخزنة بالحاسب الآلي : ويحدث هذا النوع من جرائم الحاسب في حالة الكشف غير المفوض للمعلومات المخزنة ، أو استخدامها ، أو تغييرها ، أو إتلافها .

٥ ـ التحايل الحاسبي «computer fraud» يعني هذا النوع التحايل باستخدام الحاسب الآلي كاستخدام الحاسب في مطالبة شركة التأمين والحصول على فائدة من جراء ذلك .

٦ ـ سرقة أجهزة الحاسب الآلي وملحقاتها أو تدميرها «computer theft» (Simddy, 1992:145-147) .

٧ ـ حجب الخدمة عن مواقع الإنترنت «denial of service» ، وذلك باستغلال حاسبات طرف ثالث لإرسال كمية هائلة من البيانات إلى المواقع المستهدفة بحيث يستحيل على المستخدمين الآخرين الدخول إلى تلك المواقع كما حصل للحادثة المشار إليها سابقاً لموقع ياهو «yahoo.com» ، وأكبر المواقع المستقلة ومواقع البيع بالتجزئة مثل باي إنك «buy.com» وإبي إنك «ebay.com» وأمازون «amazon.com» وسي إن إن «cnn.com» أيام الاثنين إلى الأربعاء من ٧ـ٩/ ٢/ ٢٠٠٠م (Wolf,2000) .

٨ ـ نشر معلومات (نص أو صورة أو صوت) على الإنترنت كفرية أو مخلة بالدين أو منتهكة لحقوق الأفراد والجماعات التي ضمنها الإسلام .

٩ ـ التطفل على مواقع الإنترنت . وتتعرض مواقع الإنترنت لأربعة أنواع من المتطفلين وهم :

أ ـ متطفل يريد أن يرى مكنون موقعك لمجرد الرؤية وإشباع رغبة الفضول فقط .

ب ـ متطفل يريد أن يرى مكنون موقعك ويغير معلوماته أو يلغيها أو حتى يبيعها للآخرين .

ج ـ متطفل يريد أن يستخدم موقعك كأداة هجوم على موقع آخر أكثر أهمية وأماناً من موقعك مما يحملك عواقب تدمير ذلك الموقع في حال تدميره .

د ـ متطفل يريد أن يستخدم موقعك لنشر المعلومات التي يعاقب عليها القانون كبيانات الشركات السرية أو حتى صفحات العري وتجارة الجنس بشكل عام (المجاهد، ١٤١٩هـ) .

أما من حيث فئات مرتكبي تلك الجرائم فكما أشار سشن «Sessions» مدير الشرطة الفيدرالية الأمريكية إلى أنه من خلال التحقيقات في جرائم الحاسب الآلي يمكن تصنيف مرتكبي جرائم الحاسب في ثلاث مجموعات :

تتألف المجموعة الأولى وهي الأكبر من أفراد يخترقون نظم الحاسبات الآلية فقط لممارسة الهواية ومعرفة مدى مقدرتهم على إنجاز ذلك وليس بهدف السرقة أو تدمير البيانات .

وتخترق المجموعة الثانية الحاسبات الآلية بهدف تدمير البيانات، أو تعطيل النظام، أو تغييره، أو إيقافه . وتعد أفعال هذه المجموعة من نوع الإزعاج الماكر لأنها لا تهدف إلى تحقيق ربح مادي .

وتهدف المجموعة الثالثة إلى تحقيق ربح مادي . ولهذه المجموعة تهديد خطير للقطاع التجاري والأمن الوطني لأنها تتألف من أفراد ذوي كفاءة

عالية يوظفون مهارات متخصصة لسرقة المعلومات، أو التلاعب بالبيانات، أو التسبب في خسائر تلحق بخدمات نظم الحاسب الآلي (Sessions, 1991).

الجريمة عن طريق الموظفين العاملين أو الموظفين المفصولين واردة جدًا. وتشير التقديرات إلى أن ٨٠٪ من جرائم الحاسب ترتكب من قبل موظفي الجهة نفسها (Romney,1995). ومن الوقائع التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها ١٥٠ ألف دولار لأنه أدخل فيروسًا[١] في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع ١٦٠ سجلاً من سجلات العملاء، وذلك انتقامًا من الشركة لأنها قامت بفصله من العمل (أبو العلاء، ١٩٩٠ : ١٤)

أساليب ارتكاب جريمة الحاسب:

فيما يلي عدد من الأساليب الشائعة في ارتكاب جريمة الحاسب الآلي :

١ ـ القنبلة الموقوتة[٢]: وهي تعليمات غير مرخصة موضوعة في برنامج

(١) الفيروس هو برنامج تعليمي يوضع داخله برنامج يقصد منه الأذى. وقد يكون نوع من أنواع التخريب يثير الفوضى ويدمر البرامج أو يصيب النظام بالشلل. ويوجد حوالي ١٨٠٠٠ فيروس حاسوبي معروف. وقد ارتفعت نسبة الفيروسات الجديدة التي تكتشف على مستوى العالم من ٢٠٠ فيروس في كل شهر إلى ٥٠٠ فيروس في الفترة الأخيرة.

(٢) القنبلة الموقوتة time bomb . ويحدث أن يستقبل مستخدمي الإنترنت في الوقت الراهن رسائل بريدية ملغومة بفيروسات مدمرة من مجهولين وتنشط بمجرد فتح تلك الرسالة.

بهدف إجراء عمليات غير مشروعة في وقت محدد مسبقاً أو حين تحقق شروط معينة.

٢ ـ أسلوب تقريب الأرقام: ويستخدم هذا الأسلوب لاستغلال المؤسسات المالية التي تدفع الفائدة.

٣ ـ أسلوب السجق (سلامي): ويستخدم هذا الأسلوب في سرقة المال بمقدار بسيط على مدى فترات طويلة.

٤ ـ أسلوب الباب السحري: وهو تعليمات تعطي للحاسب لتسمح للمستفيد بتجاوز قيود التحكم المعتادة في النظام. وهذه العمليات تعطي للحاسب أثناء تطوير الأنظمة وتحذف في الغالب قبل وضع النظام في مرحلة التشغيل النهائي.

٥ ـ البرامج المعدة لأغراض محددة: استخدام برامج النظام الخاصة مثل «سوبر زاب Super Zap» ـ الذي تم تطويره في «IBM» لاستخدامه في حالة الطوارئ ـ لتجاوز قيود التحكم العادية وتنفيذ عمليات غير مشروعة.

٦ ـ قرصنة البرامج: وتعني النسخ غير المفوض للبرامج.

٧ ـ غش البيانات: ويشمل حذف البيانات، أو تغييرها، أو إضافتها قبل أو بعد أو في أثناء إدخالها في النظام.

٨ ـ تسريب البيانات: وتعني النسخ غير المفوض للبيانات.

٩ ـ التنصت على الاتصالات السلكية واللاسلكية.

١٠ ـ التزوير: ويحدث عندما يستخدم شخص غير مفوض رقم هوية وكلمة السر الخاصة بمستفيد مفوض.

١١ ـ الهواية .

١٢ـ الخداع الإلكتروني : ويحدث هذا النوع عندما يتصل مخادع آلياً بمستفيد مفوّض ويوهمه بأنه له حق الاستفادة من النظام (Romney, 1995: 30-31) .

الفصل الرابع: عقوبات جرائم الحاسب الآلي في النظم السعودية من مظور إسلامي:

ليس القصد في هذا الفصل إقرار رأي الشريعة الإسلامية في مثل هذه القضايا ولكننا أردنا إثارة بعض الأسئلة التي تحتاج لدراسة وبحث من قبل المتخصصين في الشريعة الإسلامية الغراء . وقضية الجريمة والعقاب في الشريعة تتسم «بوضع متميز بين سائر التقنينات الجنائية المقارنة ، حيث عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل الذي يغطي كل جوانب الحياة ويصلح لكل زمان ومكان . فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحماية المصالح المعتبرة في الإسلام ، وهي الدين والنسل والنفس والمال والعقل ، وأي اعتداء على مصلحة من تلك المصالح يعتبر جريمة يعاقب فاعلها ، ويختلف بالطبع مقدار العقاب حسب جرامة الفعل الإجرامي« (نور ، ١٤١٧هـ: ١٣) . «ويقسم الفقهاء المسلمون الجرائم إلى فئتين : تسمى الأولى منهما بالجرائم ذات العقوبات المقدرة ، وتضم جرائم الحدود والقصاص والدية ، بينما يطلقون على الفئة الثانية ، الجرائم ذات العقوبات غير المقدرة ، وهي جرائم التعزير التي تشمل كل ما يخرج عن نطاق الجرائم ذات العقوبات المقدرة من معاص تستوجب العقاب» .

ومن الأسئلة والقضايا التي تثار هنا وقد تعد جريمة ويستحق مرتكبها العقاب ما يلي :

هل يجوز في الشريعة نسخ البرامج أم أن هناك حماية لحقوق المنتج؟ ما مدى شرعية نسخ حزم البرامج الجاهزة، هل هو جائز أم لا؟ وهل يختلف الحكم باختلاف الغرض من النسخ؟ فيجوز مثلا إذا كان الغرض الاستفادة الشخصية ويكون محرماً إذا كان الغرض منه التجارة؟ . (رفعت، ١٤١٣ : ١٨).

ولقد ناقش علماء الشريعة هذه القضية (حماية حقوق منتجي برامج الحاسب من قراصنة النسخ) وصدر فيها فتاوى شرعية وقرارات رسمية تدعم هذا الحق وتحميه .

ولئن كان رأي كثير من العلماء على أنه لا يجوز نسخ البرامج، إلا إن هناك من العلماء من يخالف هذا الرأي . ولقد استعرض الدكتور رفعت في مقالة له بعنوان «حقوق الإنتاج الذهني ومن مفرداته : حقوق تأليف الكتب وتصميم حزم البرامج» في مجلة عصر الحاسب، العدد الأول : 1413هـ، هذه المسألة وذكر رأي الشيخ عبد الرزاق عفيفي حينما استفتي فيها فقال : «يجوز نسخ حزم البرامج الخاصة بالحاسبات بصفة عامة وبصرف النظر عن الغرض من النسخ فيجوز النسخ حتى لو كان الغرض منه الاتجار» . (رفعت، ١٤١٣هـ: ١٩) . ثم ينقل رفعت عن الشيخ عفيفي العلة في ذلك بأنها «هي أن ادعاء حقوق النشر لمصمم البرامج في حالة حزم البرامج الجاهزة، هذا الادعاء ليس له أصل ولا يجوز المنع من النشر (المرجع السابق : ١٩).

أما عدد كبير من العلماء فيرون عدم جواز نسخ هذه البرامج ومن أولئك الدكتور محمد الحبيب بن الخوجه، حيث قال:

بأن الكتاب فكرة وتصور وإنتاج عند المؤلف يتحول إلى صناعة طباعة وإخراج عند الناشر ثم بضاعة يتولى تصريفها والمتاجرة فيها الناشر وحده أو بواسطة الموزع.

وقياساً على هذا فنستطيع القول بأن حزم البرامج الجاهزة في مجال الحاسبات هي عبارة عن فكرة وتصور وتصميم عند مصمم البرامج تتحول إلى صناعة وإخراج وإنتاج على الأقراص المرنة أو الشرائط المغناطيسية أو غيرها من الوسائط عند شركة الحاسبات المتخصصة في إنتاج البرامج وأخيراً تتحول حزم البرامج إلى بضاعة تتولى نفس الشركة المنتجة توزيعها أو توكلها إلى وكلاء وموزعين معتمدين لدى الشركة المنتجة لهذه البرامج (المرجع السابق: ١٩).

وقال «بوجوب إعطاء الناشر حق المؤلف وأن امتناعه من ذلك إثم لما فيه من السحت ومن أكل أموال الناس بالباطل وذهب أيضاً إلى أنه لا يرفع الإثم عن الموزع إذا علم أن الكتاب الذي يقوم بتوزيعه لم يعط مؤلفه حقه وأن الناشر قد امتنع من أداء ما عليه، واستمراره على توزيعه وقيامه به فيه إثم لكونه من باب التعاون على الظلم والإثم والعدوان» (المرجع السابق: ٢٠). كما أنه قد صدرت من اللجنة الدائمة للبحوث العلمية والإفتاء فتوى برقم (١٨٤٥٣) وتاريخ ٢/ ١/ ١٤١٧هـ إجابة لأحد الأشخاص الذين يسألون عن حكم نسخ برامج الحاسب للعمل عليها دون أن شراء النسخ الأصلية مع علمه وقراءته للعبارات التحذيرية المكتوبة عليها والتي تحذر من نسخها وبأن حقوقها محفوظة. فأجابت اللجنة بعد دراسة الاستفتاء

بأنه «لا يجوز نسخ البرامج التي يمنع أصحابها نسخها إلا بإذنهم لقوله ﷺ : المسلمون على شروطهم. ولقوله ﷺ: لا يحل مال امريء مسلم إلا بطيبة من نفسه. وقوله ﷺ: من سبق إلى مباح فهو أحق به. سواء كان صاحب هذا البرنامج مسلماً أو كافراً غير حربي لأن حق الكافر غير الحربي محترم كحق المسلم». (الأمانة العامة لهيئة كبار العلماء، فتوى ١٨٤٥٣).

ولقد صدر في المملكة العربية السعودية نظام حماية حقوق المؤلف بالمرسوم الملكي برقم م/ ١١ في ١٩/ ٥/ ١٤١٠هـ حيث توضح المادة الثالثة منه، الأنواع المشمولة بالحماية وورد في البند عاشراً: برامج الحاسب الآلي. وأوكل إلى وزارة الإعلام متابعة تنفيذ هذا القرار، حيث تم إنشاء إدارة متخصصة لهذا الغرض باسم «إدارة حقوق المؤلفين». ومما تجدر الإشارة إليه أن عقوبة نسخ البرامج في السعودية تصل إلى إغلاق المحل المخالف ١٥ يوماً وتغريمه ٠٠٠ ,١٠ ريال مع مضاعفة هذه العقوبة في حالة تكرار المخالفة» (الإنترنت والحاسب، ١٩٩٧م: ١١). وتطبيقاً لهذا النظام فقد صادرت وزارة الإعلام هذه الأيام أكثر من ٣٠ ألف نسخة برامج كمبيوتر «منسوخة» وغير مرخصة في منطقة واحدة فقط من مناطق المملكة وهي المنطقة الشرقية (الرياض، ١٤٢٠ هـ). كما أن لجنة النظر في المخالفات أصدرت كثيراً من العقوبات على عدد من المحلات التي قامت ببيع برامج مقلدة أو منسوخة في عام ١٤١٨هـ وبلغ مجموع قيمة تلك الغرامات والتعويضات الصادرة عليها بموجب النظام حوالي مليون ريال، كما بلغت في عام ١٤١٩هـ أكثر من مليون ونصف المليون ريال (الثقافية، ١٤٢٠).

ولئن كانت هذه إحدى القضايا التي صدرت فيها فتاوى واتخذت فيها قرارات وطبقت فيها أحكام إلا إن هناك بعض القضايا الكثيرة والمعاصرة

التي لم يصدر فيها شيء ولم تناقش مناقشة مستفيضة من قبل العلماء ولم تصدر فيها فتاوى على حد علم الباحثين ومن ضمن تلك القضايا السرقة التي تتم بواسطة الحاسب وهل يطبق عليها حد السرقة في الشريعة الإسلامية أم لا؟ بمعنى هل العقوبة التي تتخذ ضد مرتكب جريمة السرقة من الحاسب أو عن طريق الحاسب من العقوبات المقدرة أم غير المقدرة؟ وهل تنطبق على مرتكبها شروط إقامة حد السرقة؟ وذلك كأن تكون السرقة من حرز أم لا؟ وأن تبلغ القيمة المسروقة النصاب؟ أو غير ذلك. ثم هل حد القطع كاف أم لا بد أن يكون لها عقوبة أكبر من ذلك؟

ومن الأسئلة والقضايا التي ينبغي دراستها وإصدار الأحكام فيها كذلك: حكم من تهجم على الإسلام من خلال هذه الأداة باستخدام الإنترنت فاستهزأ بالله وكتابه ورسوله والمسلمين. حيث نجد أن هناك مواقع على الإنترنت تسيء لله وكتابه ورسوله وما جاء به من أحكام وتشريعات وأخلاق فاضلة. فعلى سبيل المثال نشر أحد المواقع حديثا سوراً محرفة للقرآن الكريم حيث وجد موقعا يتضمن نصوصاً لأربع سور مزيفة ومكتوبة بلغة عربية ركيكة وتحمل أسماء: الإيمان، المسلمون، التجسد، و الوصايا. كما أنه توجد مواقع أخرى نشر فيها معلومات مغلوطة وتسيء للإسلام (لطفي، ١٤١٩هـ: ١٠ ـ ١١).

كذلك يوجد فيها صور جنسية إباحية فاضحة تعين على نشر الرذيلة وتوقع الناس في مهاوي الردى، فما حكم تصفح مثل هذه المواقع ودخولها؟

وكذلك التقول على الآخرين وسبهم وشتمهم والافتراء عليهم ونشر أخبار وأقوال كاذبة عنهم وعن أعمالهم وصور مزيفة لهم باستخدام القص

واللزق بسهولة، ناهيك عن نشر الرذيلة عنهم واتهامهم بالباطل والخوض في أعراضهم.

وكذلك ما الحكم فيمن ارتكب جريمة الحاسب بتزييفه للنقود الورقية والوثائق وغيرها حيث أصبحت المحاكاة والتقليد للعملة والوثائق أسهل عما كانت عليه في السابق. ففي تقرير أذاعته قناة ABC News في ٢٥/ ١٢/ ١٤١٩هـ ذكرت فيه أن الصغار وطلاب المدارس بدأوا يرتكبون مثل هذه الجرائم بكثرة، وأن أحد الطلاب وعمره لا يتجاوز السابعة عشر أعطاه زميله قرصا جاهزاً للحاسب لطباعة ورقة نقدية من فئة الخمس دولار.

وكذلك ما حكم الشريعة في المتطفلين/ المتسللين من المهرة من المخترقين الذين يتعمدون التخفي بمحاولة تفادي برامج الحماية الموجودة في حاسب الضحية أو مسح آثار جريمتهم لتحقيق أهدافهم، فما الحكم فيهم إذا تم التعرف عليهم؟.

كل هذه القضايا وغيرها مما يستجد تحتاج إلى بحث ودراسة من قبل المتخصصين قبل أن يحكم فيها الإنسان. وهناك بعض القضايا المتعلقة بجريمة الحاسب معروضة في محاكم المملكة ولكن لم يصدر فيها حكم حتى الآن.

مكافحة جريمة الحاسب الآلي:

لا يوجد حل جذري يُنصح به للوقاية من جرائم الحاسب الآلي بأشكالها كافة. فكما رأينا، فإن جرائم الحاسب الآلي تتنوع أشكالها وتتعدد أساليب ارتكابها وتستجد أساليب جديدة بتطور التقنية. إلا أنه يجب وضع استراتيجية أمنية شاملة لنظم المعلومات تحدد عناصرها مسؤوليات

وامتيازات الدخول إلى النظام، ومسؤوليات وامتيازات الدخول إلى التطبيقات، ومتابعة ومراجعة استخدامات النظام، ومتابعة ومراجعة استخدام التطبيقات، ومتابعة ومراجعة استخدام البيانات، وكيفية التعامل مع النفاذ غير المصرح به، والإجراءات الأمنية الفورية اللازمة في حال حصول أي طارئ (العقيل، ١٤١٩هـ). كما يجب وضع خطة طوارئ مفصلة واختبارها ومراجعتها بصفة دورية (القاضي، ١٤١٩هـ). ويوجد إجراءات احترازية يمكن اتباعها لتعزيز أمن النظم والبيانات. وقد نصح لويس وآخرون بتطبيق عشر خطوات يؤمل أن تمكن من مواجهة بعض المخاطر المحتملة:

١ ـ كلما كان ذلك ممكناً، احفظ أجهزة الحاسبات الآلية في منطقة يمكن إغلاقها في حالة عدم توجد أحد فيها، ويمكن إحكام غلق بابها في حالة عدم الاستخدام.

٢ ـ إذا كان لابد من وضع أجهزة الحاسبات الآلية في مكان مفتوح، ركّب أجهزة تثبت الحاسبات الآلية بالمقاعد والطاولات أو أجهزة تصدر أصوات تنبيه عند أية محاولة للعبث فيها.

٣ ـ سجّل قائمة بالأرقام المتسلسلة واحفظها في مكان آمن. ففي حالة حدوث سرقات فإن الأرقام المتسلسلة تسهّل استعادة ما يمكن العثور عليه من الأجهزة المفقودة. فبدون توافر وسيلة للتعرف على الأجهزة فإن ما يمكن العثور عليه لا يمكن استعادته.

٤ ـ ينصح دوماً بنقش علامة مميزة في الأجهزة للمساعدة في التعرف عليها واستعادتها في حالة فقدها.

٥ ـ أمّن على الأجهزة ضد الفقد أو العبث.

٦ ـ تبنّ استراتيجية صيانة تشمل جميع الأجهزة. وإما أن توقع عقد صيانة أو تقوم بصيانة قطع الغيار وأجهزة الحاسبات الآلية لتتمكن من استبدال أي جهاز في حالة وقع الخلل. فاستراتيجية الصيانة تكفل استمرارية التشغيل وتجنّب نفقات غير متوقعة.

٧ ـ ينبغي عمل نسخ احتياطية لجميع ملفات البيانات. فهذا الإجراء يعزز من أمن البيانات أكثر من أي طريقة أخرى. وكما أشرنا سابقاً، فإنه يسهل استبدال الأجهزة المعطوبة بأجهزة أخرى؛ إلا أنه لا يمكن استعادة البيانات ما لم يكن محتفظاً بنسخ احتياطية منها.

فقرص صلب واحد يستوعب مئات الملايين من محارف البيانات وخلل واحد في أحد الأجهزة كفيل بأن يحولها إلى عديمة الفائدة. ويحتوي كل حاسب شخصي على برامج ضمن نظام التشغيل تمكّن من إجراء النسخ الاحتياطي إما بصورة شاملة أو على مراحل.

٨ ـ احتفظ بنسخ احتياطية من البيانات، والبرامج، والنماذج في مكان آخر من خارج مقر العمل. ففي حالة حدوث كارثة كالحريق أو الفيضان فإن النسخ الاحتياطية المحفوظة في المكان نفسه ستتعرض للتدمير أيضاً. هذا بالإضافة إلى أن النماذج خصيصاً تحتاج في الغالب إلى وقت طويل نسبياً لتجهيزها. فإذا احتفظ بنسخ أرشيفية في مكان آخر، فإنه يمكن تشغيل النظام باستخدام أجهزة أخرى.

٩ ـ قيّد استخدام أجهزة الحاسبات الشخصية بالأشخاص المصرح لهم. ولا يمكن التحقيق من مستخدمي الحاسبات الآلية إلا بتقييد استخدامها. وفي الغالب، فإن كل ما يحتاج هو توفير إجراءات أمنية على الأجهزة. أطفئ الحاسب و/ أو أقفله بالمفتاح في حالة عدم الاستخدام. وإذا كان

الحاسب الشخصي موضوع في مكان عام، استخدم كلمة السر لتقييد الاستخدام. واستخدام أدلة مستقلة لكل فرد إذا كان أشخاص متعددون يشاركون في استخدام الحاسب الشخصي. ففي هذه الحالة، فلن يعبث المستخدمون المتعددون في ملفات بيانات تخص الآخرين.

١٠ ـ أخيراً، نفّذ اختبارات تقويم للبرامج وتحقق من النتائج. وعبارة «GIGO» أو «Garbage In, Garbage Out» عبارة قديمة تستخدم لوصف برامج الحاسبات الآلية. أما الآن وللأسف، فإن المصطلح يعني «Garbage In, Gosbale Out» بعد أن أصبح الناس أكثر اعتماداً على الحاسب الآلي. فلا ينبغي الثقة بالمخرجات لمجرد كونها منتجة بواسطة الحاسب الآلي ما لم يتحقق من دقة البرامج باستخدام بيانات اختبار (Luis, et al, 1994: 139_140).

ويقترح «رومني Romney» عدة خطوات ينبغي اتباعها لتقليل احتمال مشاركة الموظفين في أعمال محظورة لها علاقة بالحاسب الآلي:

١ ـ وضع معايير دقيقة للتوظيف وإنهاء عمل الموظف. وينبغي أن تشمل معايير التوظيف المقابلة الشخصية، والبحث الجنائي عن خلفية المتقدم للعمل، واستكمال بيانات استمارة التوظيف، والتوصيات. كما يجب عند فصل الموظف إنهاء ارتباطاته بالأعمال الحساسة فوراً وحظر امتيازات استخدامه للنظام.

٢ ـ امتصاص سخط الموظفين، وبما أن العديد من مرتكبي جريمة الحاسب هم من الموظفين الساخطين كوسيلة للأخذ بالثأر، فإن على الجهة أن تحاول حل مشكلاتهم أو إزاحتهم من الأعمال الحساسة.

٣ ـ تدريب الموظفين. ينبغي تدريب الموظفين على الإجراءات الأمنية التي

تطبق في الجهة . فينبغي تثقيف الموظفين في موضوعات مثل أسباب ارتكاب الأفراد الجرائم وكيفية منعها . كما ينبغي التأكيد على أخلاقيات العمل ونتائج خرق هذه الأخلاقيات (ص ٣١ ـ ٣٢) .

ورغم أن الإنترنت يمكن أن تفتح أبواب عالم جديد للمنشأة يمكن الاستفادة منه في الإعلان تسويق المنتجات وإيصال الخدمات ، إلا أنه سوف تشرع الأبواب أيضًا للمتسللين ولصوص التقنية الحديثة . وبدون وجود قياسات أو أساليب للحماية والأمن مثل جدر الحماية[١] والتشفير[٢] في هذا المكان ، فإنه من الممكن أن يقع التسلل أو اختراق النظم ، أو تسرق المعلومات والرسائل السرية وطلبات الشراء ، وأرقام البطاقات الائتمانية أو المعلومات الخاصة عن طريق البريد الإليكتروني[٣] من قبل المتطفلين . ويشير «مكور MCCURE» إلى بعض التوصيات والخطوات والإجراءات الأساسية التي يمكن أن تتخذ من أجل بناء دفاعات صلبة وقوية في وجه مثل هذه الاختراقات :

(١) جدار الحماية FIREWAL هو «بمثابة نظام حماية أمنية للإنترنت عن طريق بناء بوابة أو حاجز عازل بين الشبكات الداخلية العائدة لهيئات خاصة وشبكة الإنترنت ، حيث يتم التحكم باستخدام هذا الجدار في عملية الخروج من والدخول إلى الشبكة المحلية مما يضفي على الشبكة المحلية نوعاً من الحماية . (الفنتوخ ، ١٤١٩هـ : ١٩٥) .

(٢) التشفير ENCRYPTION هو برنامج حاسوبي يخلط أو يمزج الرسالة مع بعضها (SCRAMBLES) بحيث لا يستطيع قراءتها أو فتحها إلا الشخص المتلقي لها الذي يراد له ذلك عن طريق فك رموزها (DECODE) .

(٣) البريد الإلكتروني E-MAIL أحد الخدمات التي تتيحها شبكة الإنترانت أو الإنترنت وتسمح لمستخدمها بإرسال واستقبال الرسائل والملفات بطريقة الكترونية .

١ ـ أحم المعلومات المخزنة في الحاسبات الآلية من العابثين وخاصة المعلومات الخاصة حساب المدفوعات ، سجلات وملفات الموظفين أو بيانات أسعار البيع . . . الخ .

٢ ـ أحم التعاملات «العمليات» السرية مثل طلبات الشراء ، أرقام البطاقات الائتمانية ، أو المعلومات الشخصية من خلال البريد الإلكتروني وغير ذلك والتي يمكن أن تحمى عن طريق التشفير .

٣ ـ تحقق من البطاقات الشخصية Verifying Ids (Mccure, 1996) .

التوصيات:

أصبح لزامًا على الجهات الأمنية والتشريعية والقضاء أن تتطور وتطوّع أساليبها ووسائلها كي تتمكن من التعامل والتعايش مع عصر الثورة المعلوماتية . وفي ظل التقدم العلمي والتقني الذي فتح آفاقًا جديدة وجلب معه مشكلات ومخاطر جديدة إن لم نستطع التعامل معها بكفاءة عالية واقتدار وأن نطور أنفسنا ومؤسساتنا وأنظمتنا ، فإن أمننا سيكون مهددًا وحياتنا في خطر . ولابد إذن من وضع برامج عملية وأساليب وطرق فعّالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمعات على مستوى العالم . وقد تمخضت هذه الدراسة عن عدد من التوصيات اللازمة للتصدي لهذه الجرائم والمخالفات ، وهي :

١ ـ تعزيز التعاون الدولي والإقليمي والمحلي في قضايا وجرائم الحاسب الآلي بغرض تبادل المعلومات عن طريق إنشاء مكاتب دولية وإقليمية وإنشاء أقسام متخصصة وخاصة تابعة لوزارات الداخلية وبالتعاون مع غيرها من الوزارات المختلفة داخل البلد وخارجه لمكافحة هذا النوع من

الجرائم والتعامل معها، وتدريب العاملين والمتخصصين وتهيئتهم على أساليب البحث والتحري والضبط والملاحقة لمثل هذا النوع من القضايا. وليكن ذلك على مستوى وزراء الداخلية العرب مثلاً.

٢ ـ إنشاء قاعدة بيانات تتضمن معلومات كافية عن مثل هذه القضايا سواء في الداخل والخارج للاستفادة منها في التعرف على ما يدور في هذا الجانب وأساليب محاربته، وتتضمن هذه القاعدة وصفًا للحادثة ومكانها وتاريخها وصفات المتهمين فيها وكيف تم اكتشافها وكيف تمت ملاحقتهم ومتابعتهم وغير ذلك من المعلومات المفيدة الأخرى.

٣ ـ تأسيس موقع في الإنترنت لتقديم المعلومات والمشورة في كيفية التعامل مع جرائم الحاسب الآلي.

٤ ـ العمل على إنشاء لجنة تنسيق تضم العديد من الوزارات المعنية مثل وزارة العدل وزارة الداخلية وزارة التجارة وبعض الجامعات ومراكز البحوث الموجودة والمهتمة، وذلك للبحث في وضع الإجراءات الكفيلة للحد من هذه الجرائم وسبل معالجتها ومكافحتها والتوعية بها، وتبادل الخبرات مع الجهات الأخرى في هذا الخصوص.

٥ ـ نظر هيئة كبار العلماء ومجلس الشورى في المملكة العربية السعودية ومجمع الفقه الإسلامي في هذه القضايا الجديدة التي لم يتم النظر فيها مسبقًا وإصدار الفتاوى والأحكام الشرعية والسياسات المتعلقة بمختلف الجرائم والمخالفات ذات العلاقة بالحاسب الآلي والإنترنت.

٦ ـ إدراج هذه الجرائم ضمن مناهج الكليات والأقسام الشرعية في الجامعات وحث الباحثين من أعضاء هيئة التدريس وطلاب الدراسات العليا على طرق موضوعات تتعلق بالجوانب الشرعية والقانونية لجرائم الحاسب الآلي.

٧ ـ تضمين مناهج مقررات الحاسب الآلي في التعليم العام بوزارة المعارف والرئاسة العامة لتعليم البنات والجامعات والكليات المعنية بالحاسب وتدريسه موضوعات تتعلق بأخلاقيات التعامل مع الحاسب الآلي والإنترنت، وتسليط الضوء على أمن المعلومات واحترام حقوق الآخرين في ضوء ما ورد في الكتاب والسنة.

٨ ـ تدريب طلاب الكليات الأمنية وإنشاء برامج لتوعية منسوبي الجهات الأمنية المعنية لفهم طبيعة هذا النوع من الجرائم وتدريبهم على كيفية مواجهتها.

مواقع مهمة في الإنترنت :

فيما يلي عدد من المواقع المهمة التي يمكن الحصول على معلومات عن أمن الحاسب والمعلومات، والجرائم ذات العلاقة، والفيروسات وطرق الوقاية منها.

1. http://www.cert.org./tech_tips/denial_of_service.html

يحتوي هذا الموقع على معلومات شاملة عن الاختراقات التي هدفت إلى منع ضحايا مستهدفين من الوصول المباشر لخدمات الإنترنت.

2. http://www.discovery.com/area/technology/hackers/glossry.html

يوجد في هذا الموقع شرح لعدد من المصطلحات المستخدمة من قبل قراصنة المعلومات.

3. http://www.inscure.org/

في هذا الموقع معلومات فنية عن أمن المعلومات وأدواته.

4. http://www.fbi.gov/programs/ipcis/index

موقع فريق المباحث الفدرالية الأمريكية المكلف بالتحقيق في الاختراقات غير المرخصة لشبكات الحاسب الآلي الرئيسة في الولايات المتحدة الامريكية، والتحقيق في الاستقبال غير المشروع لإشارات الأقمار الصناعية أو سرقتها، والتحقيق في انتهاكات قانون التأليف والبرامج ذات العلاقة.

5. http://www.antionline.com/

مركز معلومات عن أمن الإنترنت ويشتمل على معلومات عن المواقع التي تم اختراقها، وتقارير حول أمن الإنترنت، وقائمة بالقراصنة المطلوبين من قبل المباحث الفدرالية الأمريكية.

6. http://securityfocus.com/

يحتوي هذا الموقع على معلومات عن أمن الحاسب الآلي مثل أدوات مجانية، ونماذج، ومكتبة.

7. http://www.pzcommunications.com/decss.html

يقدم هذا الموقع معلومات ومصادر عن (DeCSS) البرنامج المستخدم لتشفير (CSS) الصيغة المستخدمة لتشفير البيانات بهدف منع قراءة الملفات من قبل غير المصرحين.

8. http://csrc.ncs1.nist..gov/virus/

يوفر هذا الموقع مراجعات لبرامج الحماية من الفيروسات ومعلومات متنوعة من المعهد القومي للمقاييس والتقنية الأمريكي.

9. Http://www.indyweb.net/~cvhd

يوفر هذا الموقع معلومات أساسية ومجموعة من الارتباطات لمواقع أخرى خاصة بالفيروسات.

10. http//www.stiller.com

يزود هذا الموقع بمعلومات مطولة ولكن سهلة عن الفيروسات .

المراجـــــع

أولاً: المراجع العربية :

أبو العلاء، حسين. (١٤١٠). جرائم الكمبيوتر. الشرطة: مجلة الدراسات والثقافة الشرطية. العدد: ٢٣٥، السنة العشرون، ذو الحجة ١٢ ـ ١٦.

الأمانة العامة لهيئة كبار العلماء. فتوى اللجنة الدائمة للبحوث العلمية والإفتاء رقم (١٨٤٥٣) وتاريخ ٢/ ١/ ١٤١٧هـ. (غير منشورة).

الإنترنت والحاسب. (١٩٩٧). عدد ١، أكتوبر ١١.

الإنترنت والحاسب. (١٩٩٨). يناير/ فبراير ٨.

التدريب والتقنية. (١٤٢٠). معرض الكمبيوتر السعودي ٢٠٠٠م. عدد ١١، ذو القعدة ٥٤ ـ ٥٥.

التعزي، عبد الله علي (١٤١٤هـ). أمن شبكات الحواسيب الشخصية المحلية. القافلة، شوال ٢ ـ ٤.

الحلوة، خالد (١٤١٦هـ). نمو قطاع الاتصالات والمعلومات في المملكة. المبتعث. عدد: ١٦٥، ٣٣ـ٣٦.

الشرق الأوسط. (١٩٩٥). سوق الكمبيوتر السعودية تنمو بمعدل ١٥٪ سنوياً. عدد: ٦١٨٩.

الصرامي، ناصر. (١٤٢٠هـ). جريدة الرياض. ع. ١١٣٠٤.

الضبيعان، سعد. نظام حماية حقوق المؤلف في المملكة العربية السعودية: دراسة تحليلية مقارنة. ١٤١١هـ، ط. ١، مركز البحوث: جامعة الملك سعود، الرياض.

العريني، عبدالرحمن بن سليمان (١٤١٩هـ) خواطر حاسوبية. جريدة الرياض، ٢٣/ ٤/ ١٤١٩هـ، العدد: ١١٠٠٩، السنة: ٣٥.

العقيل، سامي بن إبراهيم (١٤١٩هـ) سياسات أمن المعلومات: اقتراحات تنظيمية وتطويرية. حلقة أمن الحاسبات والمعلومات، مركز المعلومات الوطنية، وزارة الداخلية ٥ـ٨/ ١١/ ١٤١٩هـ، الرياض.

الفنتوخ، عبد القادر عبد الله. (١٤١٩). الإنترنت للمستخدم العربي. ط. ١ مكتبة العبيكان: الرياض.

الفيومي، محمد أحمد. (١٩٨٩). أساسيات نظم الكمبيوتر والبرمجة بلغة باسكال. مكتبة الفلاح، الكويت.

القاضي، إبراهيم عبدالرحمن (١٤١٩هـ) أمن المعلومات: نظرة عامة. حلقة أمن الحاسبات المعلومات، مركز المعلومات الوطنية، وزارة الداخلية ٥ـ٨/ ١١/ ١٤١٩هـ، الرياض.

القاضي، زياد عبد الكريم، محمد حسني لله خليل جابر. (١٩٩٤). أساسيات الكمبيوتر.

المجاهد، (١٤١٩هـ) أمن المعلومات والمواقع على الإنترنت. سعودي شوبر، السنة الأولى ـ العدد الأول ـ رجب ١٤١٩هـ. ص ٣١.

ايسيسكو (١٩٨٧) تطبيقات الحاسوب التربوية: وقائع الندوة التي نظمتها الإيسيسكو بالتعاون مع كلية علوم التربية بالرباط، ٥ـ٩ يناير ١٩٨٧، مطبعة النجاح، الدار البيضاء، المغرب.

بصله، رياض فتح الله. (١٤١٦). جرائم بطاقة الائتمان: دراسة معرفية تحليلية لمكوناتها وأساليب تزييفها وطرق التعرف عليها. ط. ١. دار الشروق، القاهرة.

بومعرافي، بهجة مكي. (١٩٩٧). تكنولوجيا المعلومات والاتصالات في المكتبات الحديثة: ظهورها ومجالات استخدامها. دار الفرقان: الأردن.

جرايمز، جالين. (١٩٩٩). علم نفسك الإنترنت: خطوات مختصرة لنتائج سريعة؛ مكتبة جرير، الرياض: مكتبة جرير

جريدة الرياض (١٤٢٠هـ) « الإنترنت « تصبح مجالا خصبا لكل أنواع الجرائم في أمريكا. عدد: ١١٢٩٦ ، ٣٩.

جريدة الرياض. ١٦، جمادى الآخرة، العدد: ١١٤١٦، السنة ٣٦.

جريدة الرياض. (١٤١٩هـ). التسوق عبر الإنترنت أو السوق العالمي الجديد كيف يتم ويتكون؟ عدد: ١١٢٤٧ , ٣٨.

رفعت، طلعت. (١٤١٣). حقوق الإنتاج الذهني ومن مفرداته: حقوق تأليف الكتب وتصميم حزم البرامج. عصر الحاسب، العدد الأول، جمادى الأولى: ١٨ـ٢٠.

سترن، روبرت ونانسي سترن. (١٩٨٣). الحاسبات الآلية وتشغيل المعلومات. تعريب وترجمة: سرور علي سرور، عاصم الحمامي. (١٤١٠). دار المريخ، الرياض.

شمروخ، عبد الحافظ ربحي. (١٤١٥). المعلوماتية: مقدمة في الحاسب الآلي وتطبيقاته. ط. ١، الرياض: المملكة العربية السعودية.

طلبه، محمد فهمي، وآخرون. (١٩٩٢). الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة كمبيوتر، الجزء الأول، المكتب المصري الحديث، القاهرة.

عباس، بشار (١٩٩٩م) دور الإنترنت والنشر الإلكتروني في تطوير خدمات المكتبات الحديثة. الوطنية للمعلومات. عدد: ٤١، ٩٣ـ١٠٤.

عبد اللطيف، لطفي. (١٤١٩هـ). جريمة على الإنترنت. المستقبل الإسلامي، عدد: ٨٤، ربيع الثاني: ١٠ـ١١.

عبده، نديم. (١٩٩٥). أمن الكمبيوتر. الكمبيوتر والاتصالات والالكترونيات. مج. ١٢، عدد: ٧، سبتمبر: ١١٨ـ١١٩.

عبده، نديم. (١٩٩٥). أمن الكمبيوتر. الكمبيوتر والاتصالات والالكترونيات. مج. ١٢، عدد: ٧، يناير: ١٠١.

عبده، نديم. (١٩٥). أمن الكمبيوتر. الكمبيوتر والاتصالات والالكترونيات. مج. ١٢، عدد: ٧، يونيو: ٦٩.

عضيمة، عدنان. (١٤١٦). دور الحاسوب الشخصي في صياغة عصر المعلومات. الفيصل، عدد: ٢٢٨، جمادى الآخرة، ١٣ـ١٨.

قنديلجي، عامر؛ ربحي عليان و إيمان السامرائي. (١٤٢٠). مصادر المعلومات: من عصر المخطوطات إلى عصر الإنترنت. دار الفكر: الأردن.

نور، أسامة محمد عجب. (١٤١٧). جريمة الرشوة في النظام السعودي. معهد الإدارة العامة، الرياض.

ثانياً: المراجع الأجنبية :

Ball, M. (1987, Dec. 14). To Catch A Thief: Lesson in Systems Security.

Bassler, R. (1976). The Computer Industrys Origins, Present and Future. In Bassler, & N. Enger, (Eds.), Computer Systems and Public Administrators (pp. 26-44). Alexandria, VA: College Readings.

Bloom Becker, J. B. (1994). Viewpoint: My Three Computer Criminological Sins. Communication of the ACM, 37(11), 15-16. Computer World, 73-77.

Caelli, W.: Longley, D. & Shain, M. (1989). Information Security for Managers. London: Macmillan Publishers Ltd.

Carter, D. (1995, July). Computer Crime Categories: How Techno-criminals Operate. FBI Law Enforcement Bulletin, 21-26.

Chrysler, E. (1987, Nov.). Impact of Computer Crime on EPP Audits. Journal of Systems Management, 33-40.

Cook, W. J. (1989, Dec.) Thefts of Computer Software. FBI Law Enforcement Bulletin, 1-4.

Coutoure, L. Lt. (1989, Sept.). The Computer

criminal: An Investigative Assessment. FBI Law Enforcement Bulletin, 18-22.

DITnet Staff Reporter (2000). Hackers Put Down Yahoo for Three Hours. Available: http://www.ditnet.com.ae/itnews/newsfeb 2000/newsfeb17.html [2000, Feb. 10].

Doost, R. K. (1990, May). Accounting Irregularities and Computer Fraud. The National Public Accountant, 36-39.

Feingold, C. (1975). Introduction to Data Processing, (2nd Edtor). Dubuque, IA: W. C. Brown.

Forcht, K. A.; Thomas, D. & Wigginton, K. (1989). Computer Crime: Assessing the Lawyers Perspective. Journal of Business Ethics, 8, 243-251.

Furnell, S.M & Warren, M. J. (1999) Computer Hacking and cyber Terrorism: the Real Threat in the New Millenium? Computers & Security, 18. 28-34.

Hoffer, J. A. & Straub , D. W. (1989, Summer). The 9 to 5 Underground: Are Policing Computer Crimes? Sloan Management Review,

Jarrah, Fawaz (2000). Hackers Intensify Attacks on Middle East Sites. Available: http://www.ditnet.com.ae/itnews/newsfeb2000/newsfeb20.html [2000, Feb. 10].

Loch, D.; Carr, H. & Warkentin, M. (1992, June). Threats to Information Systems: Todays Reality, Yesterdays Understanding. MIS Quarterly, 173-186.

Luis, E. S.; Tyaka, L.A. & Fennelly, L. J. (1994). Office and Office Building Security. (2nd. Ed.). Boston: Butterworth-Heinemann.

Magzoub, M. & Alabdulaaly, A. (1992). The role of research in the advancement of computer technology in Saudi Arabia. Proceedings of the 13th National Computer Conference on Information Technology Transfer (73-94). Riyadh, Saudi Arabia: Techno Printing Press.

Marley, S. (1995, June 12). High Technology Thiefs Lead To High Priced Losses. Business Insurance, 16-17.

MCCURE, JENNY C. CYBERCIME MARCH 96

Moore, R. H., Jr. (1994, Sept.-Oct.). Wiseguys: Smarter Criminals and Smarter Crime In the 21st Century. The futurist, 33-37.

Noblett, M. G. (1993, June). The Computer High-Tech Instrument of Crime. FBI Law Enforcement Bulletin, 7-9.

Parker, D. B. (1989, June). Computer Crimes, Viruses and other Crimoids. Executive Speeches, 15-19.

Powell, D. (1990). Network Abuse: Who's The Enemy? Network Management, 9: 27-34.

Prasad, J. N.; Kathawala, Y.; Bocker, H. J. & Sprague, D. (1991, July/August). The Global Problem of Computer Crimes and the Need for Security. IM, 24-28.

Romney, M. (1995, May). Computer Fraud - What Can Be Done About It? The CPA Journals, 30-33.

Rowley, J. (1996). The Basics of Information Systems. London : Library Association Publishing.

Rowley, J. (1998). The Electronic Library. London: Library Association Publishing.

Sanders, D. (1970). Computers and Management. New York: McGraw-Hill.

Sanders, D. (1985). Computers Today (2nd Edtion). New York: McGraw-Hill.

Session, W.S. (1991, Feb.) Computer Crimes: An Escalating Crime Trend. FBI Law Enforcement Bulletin, 12-15.

Sherizen, S. (1989,February). What's Your Excuse for Inadequate Computer Security? Bank Systems & Equipment, 62-64.

Sieber, Ulrich. The International Handbook on Computer Crime: Computer related economic crime and the infringement

Simddy, L.O. (1992). Computer Low in Encyclopedia of Library and Information Science. V 49ed. Allen Kent. New York: Marcel Doucker.

Sobol, M. Computer Crime Trends: A Brief Guide for Bank. Bank Administration, 52.

Stephn H. (1998). Cyber Wars and other Threats. computer and security, 17, pp.115-118.

Stevens, L. (1987, December). Security Systems : Getting Management to shell out Computer World, 14. pp: 75-76.

Wildey, R.A. (1989, June). Computer Abuse ABD Fraud: Can It Be Controled ? Agency Sales Magazine, 34-38.

Wolf, J. (2000). U. S. Turns Up No Clues in Web Blitz Inquiry. Available: http:\\www.dailynews.yahoo.com/htx/nm/2000210/ts/tech_hackers_19.html [2000, Feb, 10].