توجيهات عملية في ضبط وتفتيش انظمة الكمبيوتر والشبكات

ثمة في هذا المقام بعض التوجيهات، لكنها ليست ذات قيمة دون التدخل التشريعي لافراد قواعد تفتيش وضبط خاصة على نحو ما قررته التشريعات الوطنية المقارنة والوثائق الدولية.

١-ان القاعدة الاولى ان التفتيش يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر. واما اجراء التفتيش دون مذكرة قضائية او الحصول على بيانات من جهات ليست محلا للاشتباه لتعلقها بالمشتبه به، فانها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الافراد وتوجب مشروعية الدليل وسلامة مصدره، او تبطل كل اجراء يتم خلافا للقواعد الاصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون ، وهي مسائل - طبعا تختلف احكامها باختلاف النظم القانونية - ينفد من خلالها الجناة عند عدم اجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعلنا متمسكين بضرورة عدم اللجوء الى هذا السلوك - حتى لو اتاح النظام القانوني المعني ذلك مع تحفظنا على مثل هذا الحكم لان المشروعية الاجرائية توجب تحقيق اقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة - ونرى الاصرار على وجوب استصدار مذكرات التفتيش، اما مشكلات التفتيش فان حلها وتجاوزها امر منوط بالقواعد القانونية المتعين سنها اضافة الى التزام جهات التفتيش الحيطة في توفير متطلبات القانون والحيطة في مراعاة بعض المسائل الفنية في هذا الشان - نورد بعضها تاليا - واخيرا أهمية مباشرته ممن تتوفر لديهم الخبرات الفنية الكفيلة بتحقيق التفتيش غرضه.

٢-فاذا كان المحقق يعلم ابتداءا عن وجود الادلة المتصلة بجريمة ما ضمن احد انظمة الكمبيوتر او الشبكات، وكان الجرم ابتداءا من طبيعة الجرائم الالكترونية، فان مذكرة التفتيش يتعين ان تكون واضحة في تحديد النظام محل التفتيش وايراد اوسع وصف يغطي ما يعرفه المحقق سلفا وما يفترض انه يتصل بالمسائل التي يعرفها.

٣-اما ان كان النظام او مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش فيتعين ان تجيء عبارات مذكرة التفتيش عامة ما امكن حتى لا يكون نصها قيدا على نطاق التفتيش والضبط،

فعلى سبيل المثال يمكن ان تتضمن مذكرة التفتيش والضبط ((اجراء التفتيش والضبط لاي من او لكل سجل او معلومات توجد بصورة الكترونية او مادية او خطية موجودة في اي جهاز لتخزين المعطيات سواءا كان نظام كمبيوتر ايا كان وصفه او شبكة معلومات او وسائط تخزين او اجهزة اتصال او اية نظم معالجة وتخزين يمكن ان يوجد فيها الدليل)) لكن عمومية مذكرة التفتيش لا تعني عدم وجوب بيان السبب ومبرر التفتيش، ولا تعني تجاوز الاجراء بذاته للقواعد القانونية المقررة لحماية الافراد، خاصة اؤلئك الذين لا صلة مباشرة لهم بالمشتبه به او بفعله.

٤-ومن حيث الاصل فان التحري والتفتيش في بيئة جرائم الكمبيوتر والانترنت يتوقف على مدى دقة مذكرة التفتيش ونطاقها المكاني، ويتعين ان يحرص المحققون او جهات الضبط المكلفة بالتفتيش من قبل النيابة على ان تغطي مذكراتهم اي مكان توجد فيه هذه البينات الالكترونية في نطاق الاختصاص المكاني وبالنظر الى الشخص او الجهة التي يدور التفتيش بشأنها. وهنا تظهر اهم مشكلة في مسائل التفتيش بالنسبة الى اختراقات الانترنت او الاختراقات الخارجية، اذ قد يتطلب التحري تفتيش انظمة كمبيوتر عائدة لجهات لا صلة لها بالفعل او نتيجته، كتفتيش نظم مزودي خدمات الانترنت، او تفتيش انظمة الخوادم خارج الحدود او الطلب من مالكيها ومديريها تزويد جهة التحقيق ببيانات معينة، ولا يمكن ان يقبل قانونا ان تغطي مذكرات التفتيش مواطن ومواقع واماكن خارج صلاحية نظام العدالة المكانية، ومن هنا نشات الحاجة الى تعاون دولي حقيقي في ميدان انشطة التحري والتحقيق والضبط والتفتيش خارج الحدود.

٥-اما مسالة حاجة انشطة التفتيش للسرعة ومسالة قدرة الجناة على اخفاء الدليل فهي التي استوجبت التفكير بآلية استصدار اوامر الحفظ المستعجلة للجهات التي قد تتوفر لديها البيانات المرتبطة بنشاط المشتبه به (هذا بالنسبة للغير)، ومعلوم انه لا يمكن الزام اية جهة بتقديم اية بيانات بشان الخدمات المقدمة للزبائن او علاقتهم به، لان هذه البيانات في الاصل سرية ولا يجوز افشاؤها الا وفق القانون، فان الحاجة تعدو ماسة للتدخل التشريعي لاتاحة مكنة وايضا آلية الضبط المستعجل للنظم المشتبه بها مع امر كف يد المشتبه به عن استخدام النظام فورا بمجرد البدء باجراءت التفتيش، اضافة الى الحق في ضبط الاجهزة لاجراء التفتيش عليها في مقار التحقيق

باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش، خاصة اذا ما علمنا ان تفتيش جزء صغير جدا من الذاكرة قد يحتاج ساعات، فكيف هو الحال وقد اصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات، اضافة الى ان التفتيش الاولي قد لا يحل مشكلة الملفات المخباة او المحمية او المشفرة. لكن هذه الحلول في نطاق التفتيش تناقض القواعد المقررة قانونا في حقل ضمانات المتهم (اي المتهم المعلوماتي في حالتنا) وضمانات احترام حقوق الانسان والحريات الفردية وفي مقدمتها الخصوصية. فمثل هذه الاجراءت قد تؤدي الى كشف بيانات شخصية او كشف اسرار العمل او الوصول الى ملفات يحرص اصحابها على سريتها او تيح لهم القانون ذلك، وتعدو المسالة اكثر خطورة عندما يمتد التفتيش الى نظم مرتبطة بالنظام موضوع الاشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية او قواعد حماية سرية بيانات العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات او نظم كمبيوترات البنوك او الجهات الصحية او اعمال المحاماة او غيرها.

ان الحاجة الى التنظيم التشريعي لجوانب الضبط والتفتيش في حقل جرائم الكمبيوتر ومسائل حماية البيانات الشخصية ايضا، تجد موجبها في الحاجة الى توفير معيار مقبول يقيم توازنا بين حقوق وحريات الافراد وحماية خصوصياتهم، وبين موجبات المكافحة وحاجتها الى قواعد استثنائية فرضتها تحديات هذه الجرائم التي تزيد عن تحديات غيرها.

ففي ظل سرعة اتلاف الدليل وطبيعة ما يثبت الجريمة ذاتها من الادلة، وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة، وفي ظل ارتباط مادة الجريمة او وسيلتها بانظمة اطراف اخرى لا صلة لهم بها او بشبكات ونظم معلومات خارج الحدود، فان المكافحة الفاعلة قد تنطوي على اهدار لحقوق وحريات الكثيرين والتفريط بضمانات المتهم وما توجبه قرينة البراءة المقررة له، وهذا التناقض لا مجال لفضه الا باقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها يعدو مقبولا في ضوء اعتبارات مصلحة المجتمع وامنه متى ما توفر بحق هذا المبرر ومتى ما كان المعيار مدركا ان الاستثناء لا يجوز التوسع فيه ويتعين تقييده بالقيد التشريعي

الواضح الذي لا يتيح للسلطات التغول بما منحها القانون من حقوق او بما تفسره هي وفق رؤيتها لما قرره القانون لها من صلاحيات.

وسنقف في محاضرتنا المخصصة للجوانب الاجرائية على مسائل الضبط والتفتيش والاختصاص ولا يتسع المقام لاستعراض هذه المسائل وايراد القواعد الجديدة التي انطوت عليها التدابير التشريعية المقارنة، ونحيل القارئ الكريم بشان قواعد الملاحقة الاجرائية ومشكلاتها العملية الى مؤلفنا – جرائم الكمبيوتر والانترنت السابق الاشارة اليه.

تعريف الانترنت وبداياته واستخداماته

«الإنترنت هو جزء من ثورة الاتصالات، ويعرّف البعض الإنترنت بشبكة الشبكات، في حين يعرّفها البعض الآخر بأنها شبكة طرق المواصلات السريعة» (أبو الحجاج، ١٩٩٨م: ١٨)، كما أن الإنترنت « تعنى لغوياً ((ترابط بين شبكات)) وبعبارة أخرى ((شبكة الشبكات)) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى ((بروتوكول تراسل الإنترنت)) (TCP/IP).

بدأ الإنترنت في ١٩٦٩/١/٢ عندما شكّلتْ وزارة الدفاع الأمريكية، فريقاً من العلماء، للقيام بمشروع بحثي عن تشبيك الحاسبات، وركّزت التجارب على تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة، ومن ثم نقل هذه الأجزاء بأشكال وطرق مستقلة، حتى تصل مجّمعة إلى هدفها، وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإن الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها، عن أي طريق آخر بديل، إلى خط النهاية، ومن ثم تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم عام (١٩٨٣م) إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبغرضها الأساسي، وهو خدمة الاستخدامات العسكرية، في حين سُمِّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية،أي تبادل المعلومات، وتوصيل البريد الإلكتروني، ومن ثم ظهر مصطلح ((الإنترنت)) حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام

(١٩٨٦م) أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وأطلق عليها اسم (NSFNET) والتي أصبحت فيما بعد العمود الفقري، وحجر الأساس، لنمو وازدهار الإنترنت في أمريكا، ومن ثم دول العالم الأخرى.

من يملك الإنترنت؟

لا أحد في الوقت الراهن يملك الإنترنت، وإن كان يمكن القول في البداية بأنّ الحكومة الأمريكية،ممثلة في وزارة الدفاع، ثم المؤسسة القومية للعلوم، هي المالك الوحيد للشبكة، ولكن بعد تطّور الشبكة، ونمّوها، لم يعد يملكها أحد، واختفى مفهوم التملك، ليحل محله ما أصبح يسمي بمجتمع الإنترنت، كما أنّ تمويل الشبكة تحول من القطاع الحكومي، إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية،ذات الصبغة التجارية، والتى يمكن الاستفادة من خدماتها مقابل اشتراك (أبو الحجاج، ١٩٩٨م: ١٨).

وهذه الخصوصية أي عدم وجود مالك محدد أو معروف للانترنت يجعل مهمة رجال الأمن أكثر صعوبة (Thompson، ١٩٩٩).

توسع الشبكة

في عام (١٩٨٥م) كان هناك أقلّ من (٢,٠٠٠) ألفي حاسوب آلي مرتبط بالشبكة، ووصل العدد إلى (٥,٠٠٠,٠٠٠) خمسة مليون حاسوب في عام (١٩٩٥م) وفي عام (١٩٩٧م) تجاوز (٦,٠٠٠,٠٠٠) الستة مليون حاسوب، وتستخدم ما يزيد علي (٣٠٠,٠٠٠) ثلاثمائة ألف خادم شبكات (SERVER)،أي شبكة فرعية، متناثرة في أرجاء العالم، ويمكن القول بأن عدد المستخدمين الجدد يبلغ (٢,٠٠٠,٠٠٠) إثني مليون شهرياً، أي ما يعني انضمام (٤٦) ستة وأربعين مستخدماً جديداً للشبكة في كل دقيقة (السيد،١٩٩٧م: ١٥).

وفي استطلاع أجرته شبكة (NUA) الأمريكية (NUA، ١٩٩٨) قدّر عدد مستخدمي الشبكة عالمياً في العام (١٩٩٨م) بحوالي (١٣٤,٠٠٠,٠٠٠) مئة وأربعة وثلاثين مليون مستخدم،

وتصدرت أمريكا وكندا الصدارة من حيث عدد المستخدمين الذي بلغ (٧٠,٠٠٠,٠٠٠) سبعون مليون مستخدم (NUA ،١٩٩٨/٦).

وفي تقرير أجرته ايضاً شبكة (NUA) الأمريكية وصدر بتاريخ ٢٠٠٠/١٠/٢٦م (NUA، ٢٠٠٠) قدّر أن عدد المستخدمين للشبكة عام (٢٠٠٥م) سيكون حوالي (٢٤٥,٠٠٠,٠٠٠) مئتان وخمسة وأربعون مليون مستخدم، وقدّر أنّ غالبية هذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ،٢٠٠٠/١٠).

وقدّرت دراسة أجراها موقع عجيب (Ajeeb.com،٢٠٠١/٣/٢٥) تجاوز عدد المستخدمين العرب الـ(٥,٠٠٠,٠٠٠) الخمسة ملايين مستخدم مع نهاية عام (٢٠٠١م)، وأن يصل العدد إلى (١٢,٠٠٠,٠٠٠) اثني عشر مليون مستخدم عربي مع نهاية عام (٢٠٠٢م)، كما قدرت الدراسة عدد مستخدمي الإنترنت في المملكة العربية السعودية بـ(٥٧٠,٠٠٠) خمسائة وسبعون ألف مستخدم.

وأشار الرئيس الأمريكي السابق بيل كلينتون إلى مشروع مستقبلي، لتطوير شبكة الإنترنت، باسم (الإنترنت ٢) أو الجيل الثاني من الإنترنت فقال: " لا بُدّ من أنْ نبني الجيل الثاني لشبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة ومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة من سرعات اليوم، وذلك لتطوير كل من العلاجات الطبية الحديثة ومصادر الطاقة الجديدة، وأساليب العمل الجماعي" (آفاق الإنترنت، ١٩٩٧م: ٣٨).

وظهر حديثاً ما يشير في هذه الأيام إلى وجود سباق فضاء من نوع آخر، حيث استطاعت شركة ستاربلند (Star band) في تجربه أجرتها في شمال أميركا، من إكمال مشروع انترنت بواسطة أقمار اصطناعية ذي اتجاهين، وسرعته تبلغ (٥٠٠) خمسمائة ك.ب في الثانية، من الإنترنت إلى الحاسب الآلي، وسيبدأ تسويقه إلى المستهلك قريباً (الجزيرة،٢٠٠٠).

خدمات الإنترنت

يوفر الإنترنت خدمات عديدة من أهمها:

١- البريد الإلكتروني: لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي اليكتروني بصورة سريعة جداً لا تتعدى ثواني.

٢- القوائم البريدية: تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.

٣- خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.

٤- خدمة الاستعلام الشخصي: يمكن الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الإنترنت والمسجلين لديها.

٥- خدمة المحادثات الشخصية: يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.

٦- خدمة الدردشة الجماعية: تشبه الخدمة السابقة إلا انه،وفي الغالب، يمكن لأي شخص ان يدخل في المحادثة،أو يستمع اليها، دون اختيار الآخرين.

٧- خدمة تحويل أو نقل الملفات: (FTP)لنقل الملفات من حاسب إلى آخر وهي اختصار كلمة (FILE TRANSFER PROTOCOL).

٨- خدمة الأرشيف الإلكتروني: (ARCHIVE) تُمكّن البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم.

٩- خدمة شبكة الاستعلامات الشاملة: (GOPHER) تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريدية حيث يفهرس المعلومات الموجودة علي الشبكة.

١٠- خدمة الاستعلامات واسعة النطاق: (WAIS) تسمي باسم حاسباتها الخادمة وهي أكثر دقة وفاعلية من الأنظمة الاخرى، حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلمات الدالة التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتوي المعلومات المطلوبة.

١١- خدمة الدخول عن بعد: (TELNET) تسمح باستخدام برامج وتطبيقات في حاسب آلي آخر.

١٢- الصفحة الإعلامية العالمية:(WORLD WIDE WEB) أو الويب (WEB) تجمع معاً كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما في الشبكات المختلفة وإحضارها بالنص والصوت والصورة، وتعد الويب نظاماً فرعياً من الإنترنت، لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة (يونس، ١٤٢١هـ: ٣٤-٣٨).

مستلزمات الاتصال بالشبكة:

يلزم الاتصال بالشبكة العالمية (الإنترنت) توفر عدة أشياء هي:

١. حاسب إلى.

٢. جهاز مودم.

٣. خط هاتفي.

٤. الاشتراك في الخدمة.

٥. برامج تصفح الشبكة واشهرها (INTERNET EXPLORER)و (NETSCAPE)

تعريف جرائم الحاسب الالى والانترنت

اُشْتُقّتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأَجْرَم فهو مجرم

(ابن منظور، بدون: ٦٠٤ - ٦٠٥).

وعَرَّفت الشريعة الإسلامية الجريمة بأنها: " محظورات شرعية زجر الله عنها بحد أو تعزر.

وتعرّف جرائم الحاسب الآلي والإنترنت بأنها: " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً

بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني ".

وهناك من عرّفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة".

وفي كل الأحوال فجريمة الحاسب الآلي " لا تعترف بالحدود بين الدول ولا حتى بين القارات،فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة.

وتعد جريمة الإنترنت من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها (Vacca ، ١٩٩٦).

وأطلق مصطلح جرائم الإنترنت (Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في استراليا للفترة من ١٦ - ١٩٩٨/٢/١٧م (بحر، ١٤٢٠هـ: ٢).

أما التعريف الإجرائي لدراسة الباحث فتُعَرَّفُ جرائم الإنترنت بأنها: جميع الأفعال المخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية، المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسية والممارسات غير الأخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة.

وبالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبياً، إلا أنها لقيتْ اهتماماً من قبل بعض الباحثين، حيث أُجريتْ العديد من الدراسات المختلفة، لمحاولة فهم هذه الظاهرة، ومن ثم التحكم فيها، ومنها دراسة أجرتها منظمة (Business Software Alliance) في الشرق الأوسط، حيث أظهرت أنّ هناك تباين بين دول منطقة الشرق الأوسط، في حجم خسائر جرائم الحاسب الآلي، حيث تراوحت ما بين (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دولار أمريكي في المملكة العربية السعودية، والإمارات العربية المتحدة، و (١,٤٠٠,٠٠٠) مليون وأربعمائة ألف دولار أمريكي في لبنان.

وأظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأنّ (٢٤- ٤٢؟)

من منظمات القطاع الخاص، والعام، على حد سواء، كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت.

وقَدّرتْ الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي، مابين ثلاثة وخمسة بلايين دولار سنوياً، كما قَدّرتْ المباحث الفيدرالية (FBI)، في نهاية الثمانينات الميلادية، أنّ متوسط تكلفة جريمة الحاسب الآلي الواحدة، حوالي ستمائة ألف دولار سنوياً، مقارنة بمبلغ ثلاثة آلاف دولار سنوياً،متوسط الجريمة الواحدة، من جرائم السرقة بالإكراه. وبينت دراسة أجراها أحد مكاتب المحاسبة الأمريكية أن (٢٤٠) مائتين وأربعين شركة أمريكية، تضررت من جرائم الغش باستخدام الكمبيوتر Computer Fraud))، كما بينت دراسة أخرى أُجريتْ في بريطانيا، أنه وحتى أواخر الثمانينات، ارتكب ما يقرب من (٢٦٢) مائتين واثنين وستين جريمة حاسوبية، وقد كلفت هذه الجرائم حوالي (٩٢,٠٠٠,٠٠٠) اثنين وتسعين مليون جنيه إسترليني سنوياً (محمد، ١٩٩٥م: ٢١).

وأظهر مسح أُجري من قبل (the computer security institute) في عام (١٩٩٩م)، أنّ خسائر (١٦٣) مئة وثلاثة وستون شركة أمريكية،من الجرائم المتعلقة بالحاسب الآلي، بلغت أكثر من (١٢٣,٠٠٠,٠٠٠) مئة وثلاثة وعشرين مليون دولار أمريكي، في حين أظهر المسح الذي أُجري في عام (٢٠٠٠م) ارتفاع عدد الشركات الأمريكية المتضررة من تلك الجرائم، حيث وصل إلى (٢٧٣) مائتين وثلاث وسبعين شركة، بلغ مجموع خسائرها أكثر من (٢٥٦,٠٠٠,٠٠٠) مائتين وستة وخمسون مليون دولارRapalus،٢٠٠٠)).

كما بينت إحصائيات الجمعية الأمريكية للأمن الصناعي أن الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى (٦٣,٠٠٠,٠٠٠,٠٠٠) ثلاث وستون بليون دولار أمريكي، وأنّ (٢٥؟) من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي، وقد أصيب (٦٣؟) من الشركات الأمريكية والكندية بفيروسات حاسوبية، ووصل الفقد السنوي بسبب سوء استخدام الحاسب الآلي (٥٥٥,٠٠٠,٠٠٠) خمسمائة وخمسة وخمسون مليون دولار. (Reuvid،١٩٩٨)

ومن الصعوبة بمكان، تحديد أيّ جرائم الحاسب الآلي المرتكبة هي الأكبر من حيث الخسائر، حيث لا يعلن الكثير عن مثل هذه الجرائم، ولكن من أكبر الجرائم المعلنة هي جريمة لوس انجلوس، حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية (EFI) للإفلاس، وبلغت خسائرها (٢,٠٠٠,٠٠٠,٠٠٠) ملياري دولار أمريكي. وهناك أيضاً حادثة انهيار بنك بار بنجر البريطاني في لندن، إثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو، حيث حاول البنك إخفاء الخسائر الضخمة، باستخدام حسابات وهمية، أدخلها في الحسابات الخاصة بالبنك، بمساعدة مختصين في الحاسب الآلي، وقد بلغت إجمالي الخسائر حوالي مليار ونصف دولار أمريكي (داود، ١٤٢٠هـ: ٣١).

وتعتبر هذه الخسائر بسيطة نسبيا مع الخسائر التي تسببتها جرائم نشر الفيروسات والتي تضر بالأفراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف أعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وقد يصل الضرر في بعض المنشئات التجارية والصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلت خسائر فيروس (Code Red) إلى ملياري دولار أمريكي، في حين وصلت الأضرار المادية لفيروس الحب الشهير (٨,٧) مليون دولار واستمر انتشار الفيروس لخمسة اشهر وظهر منه (٥٥) نوعا. وتتراوح أضرار الفيروسات ما بين عديمة الضرر إلى البسيط الهين وقد تصل إلى تدمير محتويات كامل الجهاز، وأن كان الأكثر شيوعا هو ما يسبب ضرراً محصوراً في إتلاف البيانات التي يحتويها الجهاز.(Ajeebb.com،٢٠٠١/٨/٨)

وجرائم الإنترنت كثيرة ومتنوعة ويصعب حصرها ولكنها بصفة عامة تشمل الجرائم الجنسية كإنشاء المواقع الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسيا، وجرائم ترويج المخدرات أو زراعتها، وتعليم الإجرام أو إرهاب كصنع المتفجرات، إضافة إلى جرائم الفيروسات واقتحام المواقع.

وكثيراً ما تكون الجرائم التي ترتكب بواسطة الإنترنت وثيقة الصلة بمواقع أرضية على الطبيعة كما حدث منذ حوالي سنتين عندما قام البوليس البريطاني بالتعاون مع أمريكا ودول أوروبية

بمهاجمة مواقع أرضية لمؤسسات تعمل في دعارة الإنترنت.

وإن كانت متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن " هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وأن ما هي أرقام تتغير في السجلات. ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها".

اسباب صعوبة جرائم الحاسب الالى

وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أمور هي:

أولا: أنها كجريمة لا تترك اثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ثالثا: أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها.

إلا أن أهم خطوة في مكافحة جرائم الإنترنت هي تحديد هذه الجرائم بداية ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بما يتناسب وطبيعة هذه الجرائم المستجدة ويأتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم.

والإنترنت ليس قاصرا على السلبيات الأمنية فقط حيث يمكن أن يكون مفيدا جدا في النواحي الأمنية كأن يستخدم الإنترنت في إيصال التعاميم والتعليمات بسرعة وكذلك في إمكانية الاستفادة من قواعد البيانات المختلفة والموجودة لدى القطاعات الأخرى وتبادل المعلومات مع الجهات المعنية، ويفيد أيضا في مخاطبة الإنتربول ومحاصرة المجرمين بسرعة.

وحددت دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت عشر خدمات أمنية يمكن تقديمها للجمهور عن طريق شبكة الإنترنت، وأبرزت سلبية أبرزها الإباحية والمعاكسات والاحتيال والتجسس والتهديد والابتزاز (البيان،٢٠٠٠م).

كما حددت دراسة الشهري الايجابيات الأمنية لشبكة الإنترنت في تلقي البلاغات، توفير السرية للمتعاونين مع الأجهزة الأمنية، طلب مساعدة الجمهور في بعض القضايا، نشر صور المطلوبين للجمهور، نشر المعلومات التي تهم الجمهور، تكوين جماعات أصدقاء الشرطة، توعية الجمهور امنيا، استقبال طلبات التوظيف، نشر اللوائح والأنظمة الجديدة، توفير الخدمة الأمنية خارج أوقات العمل الرسمي، سهولة الوصول إلى العاملين في الجهاز الأمني، إجراء استفتاءات محايدة لقياس الرأي العام، وسيط فاعل في عملية تدريب وتثقيف منسوبي القطاع وأخيرا وسيط مهم للإطلاع على خبرات الدول المتقدمة ولاتصال مع الخبراء والمختصين في مختلف دول العالم (الشهري، فايز، ١٤٢٢هـ).

وليس الأمر قاصرا على ذلك بل بادرت الدول الأوروبية إلى الاستخدام الفعلي لشبكة الإنترنت في البحث عن المجرمين والقبض عليهم " فقد تمكنت العديد من الدول وفي مقدمتها ألمانيا وبريطانيا وتأتي في المرتبة الثالثة فرنسا من استخدام شبكة الإنترنت في السعي نحو ضبط المجرمين – بل التعرف على كل الحالات المشابهة في كل أنحاء أوروبا والاتصال فورا بالانتربول عبر شبكة الإنترنت".

فئات الجناة في جرائم الحاسب الآلي:

يمكن حصر أنواع الجناة في جرائم الحاسب الآلي في أربعة فئات(محمد،١٩٩٥م:٧٤- ٧٥):

الفئة الأولي: العاملون على أجهزة الحاسب الآلي في منازلهم نظرا لسهولة اتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

الفئة الثانية: الموظفون الساخطون على منظماتهم التي يعملون بها فيبعودون إلى مقار عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتى سرقته.

الفئة الثالثة: فئة المتسللين (Hackers) ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين اللذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز، وتقع اغلب جرائم الإنترنت حاليا تحت هذه الفئة بقسميها.

الفئة الرابعة:العاملون في الجريمة المنظمة كعصابات سرقة السيارات حيث يحددون بواسطة الشبكة أسعار قطع الغيار ومن ثم يبيعون قطع الغيار المسروقة في الولايات الأعلى سعرا.

هل حقا ثمة جرائم كمبيوتر وإنترنت ؟؟

متى تتحول الوقائع والاحداث الغربية الى ظاهرة في خصوص ما ؟؟

انها تمسي ظاهرة حقيقية متى ما ازدادت الأحداث ضمن نسق معين، ومتى ما تشكلت سمات للحدث الحاصل في نطاقها، وللأثر المترتب على الحدث.

وهكذا، ثمة ظاهرة حقيقية بشان جرائم الكمبيوتر والانترنت، فما هي ملامحها، وما هو حجمها، وماذا عن نطاق الخسائر الناجم عنها ؟؟

لدى الحديث عن واقع ونطاق ظاهرة جرائم الكمبيوتر والإنترنت يتعين ابتداء ان ندرك انه ليس ثمة دراسات إحصائية شاملة وليس ثمة اكثر من تقديرات تتباين دقتها تبعا لقدرة الجهات القائمة على إنجاز مثل هذه الدراسات ومدى موضوعيتها، وفي هذا النطاق فان هناك فرقا حقيقيا بين دراسات الجهات غير الربحية وبين المؤسسات التجارية التي غالبا ما تكون دراساتها موجهة لغرض ما فتجيء النتائج معبرة عن هذا التوجه. ومن هذه الزاوية فان ما يعتمده هذا الدليل كامثلة على الدراسات المسحية يركز بشكل رئيس على دراسات الجهات الحكومية او غير الربحية ما امكن.

ومن المهم أيضا ادراك حقيقة ثانية، ان الارقام المتوفرة من الدراسات الموضوعية، لا تعكس باي صورة واقع الظاهرة بل تقدم صورة عن حقائقها العامة، وفي حالة جرائم الكمبيوتر والإنترنت، فان حجم الظاهرة ونطاق الجريمة وحجم المخاسر سيكون بالضرورة اكثر مما تقدمه هذه الدراسات من نتائج، مصدر ذلك حقيقة أخرى باتت معلومة للكافة وتستند الى اساس موضوعي

وحقيقة منطقية، وهي ان غالبية المؤسسات تسعى الى كتم خسائرها بل ربما تعمد الى اخفاء كل حقيقة تتصل بتعرضها لاية جريمة من جرائم الكمبيوتر والإنترنت حماية لثقة زبائنها بها وتمسكا امام الآخرين بفعالية نظام الأمن لديها. وهذا ما يعبر عنه في الدراسات البحثية بالرقم الاسود.

خلاصة احدث الدراسات المسحية حتى إعداد هذا الدليل

اعلن معهد أمن المعلومات Computer Security Institute نتائج تقرير عام ٢٠٠١ وهو التقرير السادس حول جرائم الكمبيوتر ودراسة أمن المعلومات المسحية٢٠٠١ CSI/FBI Computer Crime and Security Survey (٢٥)، وهذه الدراسة يتم إجراؤها سنويا من قبل المعهد بتعاون مع مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية، بغرض رفع مستوى الوعي لمسائل أمن المعلومات وتحديد واقعها.

وقد اجريت هذه الدراسة الشاملة بمشاركة ٥٣٨ مؤسسة أمريكية تضم وكالات حكومية و بنوك ومؤسسات مالية ومؤسسات صحية وجامعات، واظهرت بوجه عام تنامي خطر جرائم الكمبيوتر وارتفاع حجم الخسائر الناجمة عنها بالرغم من زيادة الوعي بإلحاق المعلومات، فقد تبين ان ٨٥٪ من المشاركين في الدراسة وتحديدا المؤسسات الحكومية الكبرى تحرت اختراقات كمبيوتر خلال السنة السابقة، وان ٦٤٪ لحقت بهم خسائر مادية جراء هذه الاعتداءات وان ٣٥٪ تمكن من حساب مقدار خسائره المادية التي بلغت تقريبا ٣٧٨ مليون دولار في حين كانت الخسائر لعام ٢٠٠٠ بحدود ٢٦٥ مليون دولار وان معدل الخسارة السنوية لاعوام الثلاثة السابقة لعام ٢٠٠٠ بلغت ١٢٠ مليون دولار، وان اخطر مصادر الخسارة المالية تمثل بسرقة المعلومات المتعلقة بالاموال والممتلكات (حوالي ١٥١ مليون) والاحتيال المالي (حوالي ٩٣ مليون). واظهرت الدراسة أيضا ان ٧٠٪ من الاعتداءات حصلت من نقطة الاتصال الخارجي عبر الإنترنت مقابل ٣٠٪ حصلت من نقطة تتعلق بداخل النظام نفسه، في حين كانت نسبة الاختراق عبر اتصال الإنترنت ٥٩٪ في عام ٢٠٠٠.

ان ٣٦٪ من المشاركين بالدراسة قد ابلغوا جهات القانون حول هذه الاختراقات بزيادة بنسبة ١١٪ عن عام ٢٠٠٠، حيث كانت نسبة المبلغين ٢٥٪ عام ٢٠٠٠ في حين كانت ١٦٪ عام ١٩٩٦.

اما حول مصدر وطبيعة الاعتداءات فان ٤٠٪ من الاعتداءات تمت من خارج المؤسسات مقابل ٢٥٪ في عام ٢٠٠٠، وان ٣٨٪ من الاعتداءات تعلقت بهجمات انكار الخدمة مقابل ٢٧٪ عام ٢٠٠٠ وان نسبة الموظفين الذين ارتكبوا أفعال إساءة استخدام اشتراك الإنترنت لمنافع شخصية بلغت ٩١٪، تتوزع بين الاستخدام الخاطئ للبريد الإلكتروني وتنزيل مواد اباحية من الشبكة، في حين كانت هذه النسبة ٧٩٪ في عام ٢٠٠٠، وان ٩٤٪ من المشاركين تعرضوا لهجمات الفيروسات مقابل ٨٥٪ عام ٢٠٠٠.

وفيما يتعلق بالتجارة الإلكترونية، فان ٩٧٪ من المشاركين لديهم مواقع على الإنترنت، وان ٤٧٪ منهم يتعامل بالتجارة الإلكترونية، وان ٢٣٪ قد تعرضوا لدخول غير المصرح به او إساءة الاستخدام وان ٢٧٪ لا يعرفون فيما اذا كانت مواقعهم قد تعرضت لمثل هذه الاعتداءات، وان ٢١٪ من الجهات المشاركة التي تعرضت الاعتداءات أبلغت عن ٢-٥ حوادث وان ٥٨٪ ابلغ عن عشرة حوادث فاكثر، وان ٩٠٪ من الاعتداءات كانت اعتداءا حاقدة مقابل ٦٤٪ عام ٢٠٠٠، وان ٧٨٪ من الاعتداءات تتعلق بانكار الخدمة مقابل ٦٠٪ عام ٢٠٠٠ وان ١٣٪ ابلغوا عن سرقة معلومات مقابل ٨٪ عام ٢٠٠٠ وان ٨٪ ابلغوا عن احتيال مالي مقابل ٣٪ عام ٢٠٠٠.

خصائص وأنواع جرائم الحاسب الآلي والإنترنت:

من الصعوبة الفصل بين جرائم الحاسب الآلي وجرائم الإنترنت،فلابد للأول لارتكاب الثاني،

وتصنف تلك الجرائم إلى مجموعات:

المجموعة الأولي: تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة، وما يميز هذا النوع من الجرائم انه من الصعوبة بمكان اكتشافه مالم يكن هناك تشابهه في بعض أسماء أصحاب هذه البطاقات.

المجموعة الثانية: تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو

بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية. ومع أن وجود هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقاية والتي قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديث وغير معروف من السابق.

المجموعة الثالثة: تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة (وإن كان اليانصيب غير مشروع أصلاً).

المجموعة الرابعة: تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل.

جرائم الإنترنت من منظور شرعي وقانوني

" يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات المغلقة والشرقية، حيث أن تعّرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي واللاقانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قيمة لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الإباحية".

والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين و" مع دخول الكمبيوتر (الحاسب الآلي) الذكي إلى المنازل فان ذلك سيفتح الباب لأنواع متطورة من الجرائم التي تستغل إمكانية

برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشكبة الانترنت، فطالما انك تستطيع مثلا وصل خزانة الأموال في مكتبك بشبكة الانترنت لإعطاء إنذار عند محاولة فتحها فربنا يكون من الممكن فتحها عن بعد بواسطة الكمبيوتر (الحاسب الآلي) ثم الوصول إليها وإفراغها ".

واستلزم التطور التقني تطور في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل – غالباً – تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين انه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الانترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما انه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود دولية أو جغرافية. ونتيجة لذلك فإن تحديد أين تكون المحاكمة وما هي القوانين التي تخضع لها أمر في غاية الحساسية والتعقيد خاصة وان كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلا قد لا يعتبر جريمة في أمريكا والعكس صحيح، بل أن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما في الولايات المتحدة الأمريكية (Thompson، ١٩٩٩).

وأدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، مما اجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكة الإنترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما اثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الاختصاص القضائي ومكان وزمان ارتكاب الجريمة حيث يسهل على المجرم في مثل هذه الجرائم ارتكاب جريمة ما في مكان غير المكان الذي يتواجد فيه أو الذي حدثت فيه نتائج فعله (تمام، ٢٠٠٠م: ١- ٣).

وتطوير القوانين الجنائية وتحديثها امر يستغرق بعض الوقت فـ" هناك تعديلات كثيرة مطلوب ادخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن إستخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية".

ولاقت جرائم الحاسب الآلي اهتماما عالميا فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (١٩٩٣م) الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنولوجيا المعلومات وتوصل الي توصيات احاطت بجوانب مشكلة جرائم الحاسب الآلي الا انها لم تتعرض لجزئية هامة وهي التعاون الدولي الذي يعتبر ركيزة اساسية عند التعامل مع هذه النوعية من الجرائم.

وهذا المؤتمر يعتبر تحضيرا للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام (١٩٩٤م) والذي وضع توصيات حول جرائم الحاسب الآلي والانترنت والتحقيق فيها ومراقبتها وضبطها وركز على ضرورة ادخال بعض التعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وإفرازاتها.

والتعاون الدولي مهم عند التعامل مع جرائم الإنترنت، كونه سيطّور اساليب متشابهة لتحقيق قانون جنائي واجرائي لحماية شبكات المعلومات الدولية،خاصة ان هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فان عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية.

وتعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (١٩٧٦م - ١٩٨٥م)، وفي عام (١٩٨٥م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي:

جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (١٩٨٦م) صدر قانونا تشريعاً يحمل الرقم (١٢١٣) عرّف فيه جميع المصطلحات الضرورية

لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام (٢٠٠٠م) خمسة جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع جرائم الحاسب الآلي والانترنت.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (The Competition Act) مثلا الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها وفي عام (١٩٨٥م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها.

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (١٩٨٨م) القانون رقم (١٩-٨٨) الذي أضاف إلى قانون العقوبات الجنائي

جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (١٩٩٤م) تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال (تمام، ٢٠٠٠م: ٩١- ٩٢، ١١٥؛ شتا، ٢٠٠١م: ٧٠)

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرت عام (١٩٩١م) شرعية التصنت على شبكات الحاسب الآلي للبحث عن دليل.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما كان ذلك إلى إدانته أو إدانة احد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى ابعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم.

هذا وعلى مستوى الدول العربية فانه وحتى تاريخه،وبحسب علم الباحث، لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة

لأركان الجريمة المعلوماتية، ومن ذلك مثلا اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية

.وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجد نص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت. وقد أوكل إلى شركة البحرين للاتصالات السلكية واللاسلكية (بتلكو) مهمة تقديم خدمة الإنترنت للراغبين في ذلك، كما أنيط بها مسئولية الحد من إساءة استخدام شبكة الإنترنت من قبل مشتركيها.

وعلى المستوي المحلي نجد أن المملكة العربية السعودية أيضا لم تسن قوانين خاصة بجرائم الإنترنت،إلا أن الوضع مختلف هنا، فهي ليست في حاجة لتحديث قوانينها وتشريعاتها كونها تنطلق من الشريعة الإسلامية الكاملة، فالمشرع واحد لا ثاني له والتشريع أزلي لا تجديد له، وهو مع كونه أزلي فانه صالح لكل زمان ومكان كونه صادر من خالق الكون والعليم بما يَصْلُحُ له ويُصْلِحُهُ « وتركت الشريعة الإسلامية الباب مفتوحا لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة منها لا ضرر ولا ضرار وتركت لولي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاة لمصلحة المجتمع ويندرج ذلك تحت باب التعازير» وهناك قاعدة سد الذرائع أي «دفع الوسائل التي تؤدي إلى المفاسد، والأخذ بالوسائل التي تؤدي إلى المصالح» (أبو زهرة، ١٩٧٦م: ٢٢٦)

«ومن المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح» (أبو زهرة، ١٩٧٦م : ٢٢٨)

ونظراً لأن «الظاهرة الإجرامية من الظواهر الاجتماعية التي تتميز بالنسبية، لأنها تختلف باختلاف الثقافات، فما يعد جريمة أو جنحة في مجتمع ما قد يعد مقبولا في مجتمع آخر. فالتشريع والثقافة السائدان في كل مجتمع هما اللذان يحددان الجرائم والفضائل» (السيف، ١٤١٧هـ:١).

لذا فان هذا البحث وعند دراسته لجرائم الانترنت في المجتمع السعودي فانه ينطلق من القوانين

الشرعية المعمول بها في المملكة العربية السعودية التي تستمد قوانينها من كتاب الله وسنة نبيه محمد عليه أفضل الصلاة وأزكى التسليم، وليس من القوانين الوضعية التي قد تتفق في تعريف الجريمة إلا أنها تختلف حتما في تقسيمها للجريمة.

فالجريمة في القوانين الوضعية تعّرف بأنها كل فعل يعاقب عليه القانون، أو امتناع عن فعل يقضي به القانون، ولا يعتبر الفعل أو الترك جريمة إلا إذا كان مجرّماً في القانون. أما التعريف الشرعي للجريمة فهي إتيان فعل محرم معاقب على فعله أو ترك فعل محرم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه.

. أو بمعنى آخر هي «فعل ما نهي الله عنه، وعصيان ما أمر الله به» (أبو زهرة، ١٩٧٦م: ٢٤).

وقد لا يبدوا أن هناك اختلاف كبير بين التعريفين،وهذا صحيح إلى حد كبير، ولكن يتّضح الاختلاف في التقسيم الذي يأخذ به كل فريق، ففي الشريعة الإسلامية تقّسم الجريمة من حيث جسامة العقوبة إلى حدود، قصاص أو دية، وتعازير، في حين تقّسم القوانين الوضعية الجريمة من حيث العقوبة إلى جنايات، جنح، ومخالفات

أو بمعنى آخر فان القوانين الوضعية « تقسم الجريمة أساسا على مقدار العقوبة، وبذلك كأن تحديد الجريمة يعتبر فرعا من العقوبة، في حين أن التشريع الإسلامي يجعل الأساس في العقوبة هو جسامة الجريمة وخطرها من حيث المساس بالضرورات الخمس» (منصور، ١٤١٠هـ: ٢١٣ – ٢١٤).

وبشكل أدق فالاختلاف يقع في التقسيم الثالث أي في قسم التعازير في الشريعة وقسم المخالفات في القوانين الوضعية، ففي الأولي أشمل واعم حيث انه يدخل في التعازير كل الأفعال سواء المجرمة أو غير المجرمة، أي التي لها عقوبة محددة أو التي لم ينص علي عقوبة محددة لها، فالعقوبة هنا تقديرية للقاضي وتبدأ من الزجر والتوبيخ وتصل إلى حد إيقاع عقوبة القتل تبعا للفعل المرتكب ولنظرة القاضي لذلك الفعل. في حين يحدد القانون الوضعي عقوبات محددة للمخالفات بمعنى انه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لم يعتبر جرما، ومن

هنا تختلف النظرة إلى الجريمة في الشريعة الإسلامية عنها في القوانين الوضعية حيث أنها أشمل وأعم في الشريعة عنها في القوانين الوضعية، الأمر الذي يجعل معه الشريعة الإسلامية متطورة ومتجددة دوما فهناك عقوبة لكل فعل شاذ أو غير مقبول وان لم ينص على تجريمه قانونيا.

ولا يعنى هذا أن كل الأفعال مجرّمة في الشريعة بل المقصود هو أن أي فعل شاذ أو منافٍ لتعاليم الدين الإسلامي ولو كان جديدا فان هناك عقاب له في الشريعة، ف«الأساس بلاشك في اعتبار الفعل جريمة في نظر الإسلام هو مخالفة أوامر الدين

، أما العقوبة المقررة لكل جريمة فمتفاوتة حيث «تتفاوت الجرائم في الإسلام بتفاوت ما فيها من مفاسد» (أبو زهرة، ١٩٧٦م: ١٨٥)، فالشريعة حددت إطار عام للأفعال المقبولة وغير المقبولة جديدها وقديمها، كما حددت العقوبة المناسبة لكل جريمة أو فعل غير مقبول، وهنا سر تفوق الشريعة الإسلامية.

ومن هذا فقضية الجريمة والعقوبة ومستجدات ها أمر محسوم في المملكة العربية السعودية ويميزها عن غيرها من الدول، فالقانون الجنائي لديها،والمستمد من الشريعة، يتسم «بوضع متميز بين سائر التقنيات 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 العقوبة حسب جرامة الفعل الإجرامي».

ومع ذلك فالأمر يحتاج إلى وضع أسس تنظيمية فاعلة وشاملة لتحديد الجهة المخولة بداية للتعامل مع جرائم الإنترنت والأفعال غير الأخلاقية والتصرفات السلبية التي تحدث أثناء استخدام شبكة الإنترنت تحقيقاً وضبطاً ووقايةً، وكذلك تحديد كيفية التعامل الإداري والإجرائي في هذه القضايا، فلا بد أن يواكب استخدام المملكة العربية السعودية لتقنية الإنترنت ظهور أنماط جديدة من الإجرام -كغيرها من الدول التي أخذت بالتقنية الحديثة- فهذه الأنماط ليست قاصرة على

دولة دون أخرى.

فلا بد إذن من وضع تنظيم إداري واضح للحد من سلبيات هذه الأفعال ومحاسبة مرتكبيها وإعطاء الحق للمتضررين منها. فهذه التنظيمات سوف تُفَعِّلْ قوانين وتشريعات المملكة المستمدة من الشريعة الإسلامية لتضع بعض الحواجز والروادع أمام من يرتكب مثل هذه الجرائم من داخل المملكة.

وقد بدأت المملكة بالعمل في هذا الاتجاه حيث أوكلت المهمة مبدئيا إلى مدينة الملك عبدالعزيز للعلوم والتقنية لتقديم هذه الخدمة عبر مزودي خدمة تجاريين، كما شكلت لجنة أمنية دائمة برئاسة وزارة الداخلية وعضوية ممثلين من القطاعات الأمنية والدينية والاجتماعية والاقتصادية المختصة للإشراف على أمن خدمة الإنترنت في المملكة وتشمل مهمتها تحديد المواقع غير المرغوبة والتي تتنافى مع الدين الحنيف والأنظمة الوطنية ومتابعة كل ما يستجد منها لحجبها خاصة تلك المواقع الإباحية أو الفكرية أو الأمنية (النشرة التعريفية، ١٤١٩هـ).

وفي تقرير صحفي نشر في موقع صحيفة الجزيرة بتاريخ ١٤٢١/٢/٢هـ (الجزيرة، ١٤٢١هـ)، كشفت مدينة الملك عبدالعزيز للعلوم والتقنية من خلال وحدة الإنترنت المشرفة على عمل مقدمي خدمة الإنترنت في المملكة عن إجراءات فنية تهدف إلى محاصرة أعمال المخربين أو المتسللين ومنعهم ومخالفتهم. وأوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين وإساءة استخدام البريد الإلكتروني وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الإنترنت في المملكة ومن بين هذه الإجراءات ما يلي:

١. منع انتحال أرقام الإنترنت أو ما يعرف بـIp-spoofing)) والتي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة.

٢. منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـE-Mail Spamming)) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا باسم البريد

المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.

٣. الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (٦) أشهر.

٤. الحصول على خدمة الوقت ((NTP عن طريق وحدة البروكسي ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

٥. تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.

٦. ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

كما أشارت صحيفة عكاظ في عددها رقم (١٢٧٨٩) وتاريخ١٣/٦/١٤٢٢هـ (عكاظ،١٤٢٢هـ)، بأن مجلس الوزراء السعودي يدرس نظاما جديدا للإنترنت يتضمن فرض عقوبات من بينها السجن وغرامات مالية على مخربي شبكة المعلوماتية (المتسللين)، وأن العقوبات على مخربي الإنترنت ستحدد وفقا للضرر الناجم عن عمليات الاختراق والأعمال التخريبية وأن العقوبة قد تصل إلى السجن سبع سنوات إلى جانب غرامات مالية.

وهذه التنظيمات مفيدة ولا شك إلا أنها ليست كافية، فالمهم هنا وبداية تحديد جهة متخصصة ومؤهلة للتعامل مع جرائم الإنترنت تحقيقا وضبطا ووقاية، خلاف مدينة الملك عبدالعزيز التي تضطلع بمهام كثيرة ومختلفة عن المهام التي ستوكل للجهة التي ستحدد لمثل هذا العمل. وعلى كل حال فيجب أن لا يركن إلى الأنظمة والتعليمات فقط عند التعامل مع الجرائم والتجاوزات، فالأنظمة ليست وحدها الرادع لأي مخالفات أو سلبيات وخاصة في بيئة دينية محافظة كالمملكة العربية السعودية حيث يلعب الوازع الديني والرقابة الذاتية دور مهم في عملية الردع والحد من أي تجاوزات، فمن المهم أن يؤخذ

" الجانب الديني في الاعتبار عند مناقشة أخلاقيات تداول المعلومات كنوع من الضوابط الدينية

التي تحكم أخلاقيات استخدام وتداول المعلومات، والتي تردع أي اتجاه لدى الأفراد نحو ارتكاب جرائم نظم المعلومات (الانترنت)، فالملاحظ انه توجد معلومات تقدمها جهات كثيرة بالمجان وشبكة الانترنت متخمة بكميات هائلة من هذه المعلومات الصالح منها والمفسد. وينطبق هذا على جميع أنواع العلوم والفنون من خلال ملايين المواقع التي يطلع على محتواها أكثر من ستين إلى مائة مليون متصل بالشبكة يوميا ويتضاعف عددهم بسرعة مخيفة. ومن ثم يجب أن نركز على ضرورة وجود الضوابط الدينية والأخلاقية، فالذي لا وازع ولا ضمير له قد أتيحت له وسيلة سهلة للغاية في توصيل أفكاره ونشر مفاسده بالدرجة نفسها المتاحة أمام النافعين للناس، وقوانين الدول تختلف فيما تتبناه من أساليب للتحكم فيما ينشر عبر شبكة الانترنت، والمحرمات تختلف من مكان لآخر." (داود، ١٤٢٠هـ : ٢١٧).

ولعلنا لا نغفل العادات والتقاليد المستوحاة من شريعتنا الإسلامية وتقاليدنا العربية الأصيلة والتي تزرع بداخل المواطن الوازع الديني الرادع عن ارتكاب المخالفات والنواهي، ومع كل هذه الضوابط فالنفس أمارة بالسوء والشيطان يجري من ابن ادم مجرى الدم، فيجب أن يكون هناك ضوابط عقابية تحد من يضعف رادعه الإيماني ليجد الرادع السلطاني له بالمرصاد فان الله ليردع بالسلطان ما لا يردع بالقرآن.

الأبعاد الفنية للأفعال الجنائية المرتكبة

من قبل مستخدمي الإنترنت في المجتمع السعودي (تصور إسلامي)

الاستعراض السابق كان يتحدث بصفة عامة عن مواكبة القوانين الدولية والعربية والمحلية للجرائم المستحدثة ومنها جرائم الإنترنت، ولكن ما هي المنطلقات الشرعية والقانونية لإطلاق مصطلح جريمة على الأفعال المرتكبة أثناء استخدام الإنترنت في المجتمع السعودي. وللإجابة على هذا السؤال يستحسن التطرق بشيء من التفصيل للجرائم والأفعال التي تطرقت إليها الدراسة وتكيفها شرعياً وقانونياً