~~* جرائم الانترنت من منظور شرعي وقانوني *~~

محمد عبدالله منشاوي

باحث في جرائم الانترنت

مكة المكرمة

1423-11-1هـ

مقدمة- تعريف الإنترنت وبداياته واستخداماته:
"الإنترنت هو جزء من ثورة الاتصالات، ويعرّف البعض الإنترنت بشبكة الشبكات، في حين يعرّفهاالبعض الآخر بأنها شبكة طرق المواصلات السريعة" (أبو الحجاج، 1998م : 18)،كما أن الإنترنت " تعنى لغوياً ((ترابط بين شبكات)) وبعبارة أخرى ((شبكةالشبكات)) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرةفي أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى((بروتوكول تراسل الإنترنت)) (TCP/IP)"(الفنتوخ، 1421هـ:11).

بدأ الإنترنت في 1969/1/2 عندما شكّلتْ وزارة الدفاع الأمريكية، فريقاً منالعلماء، للقيام بمشروع بحثي عن تشبيك الحاسبات، وركّزت التجارب على تجزئة الرسالةالمراد بعثها إلى موقع معين في الشبكة، ومن ثم نقل هذه الأجزاء بأشكال وطرقمستقلة، حتى تصل مجّمعة إلى هدفها، وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقتالحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإنالأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها، عن أي طريق آخر بديل، إلى خطالنهاية، ومن ثم تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم عام (1983م)إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبغرضها الأساسي، وهو خدمة الاستخداماتالعسكرية، في حين سُمِّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية ،أي تبادلالمعلومات، وتوصيل البريد الإلكتروني، ومن ثم ظهر مصطلح ((الإنترنت)) حيث أمكنتبادل المعلومات بين هاتين الشبكتين. وفي عام (1986م) أمكن ربط شبكات خمس مراكزللكمبيوترات العملاقة وأطلق عليها اسم (NSFNET) والتي أصبحت فيما بعد العمود الفقري، وحجر الأساس، لنمو وازدهارالإنترنت في أمريكا، ومن ثم دول العالم الأخرى(الفنتوخ،1421هـ: 21- 24).

منيملك الإنترنت؟

لاأحد في الوقت الراهن يملك الإنترنت، وإن كان يمكن القول في البداية بأنّ الحكومةالأمريكية ،ممثلة في وزارة الدفاع، ثم المؤسسة القومية للعلوم، هي المالك الوحيدللشبكة، 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 القطاعالحكومي، إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية ،ذات الصبغةالتجارية، والتى يمكن الاستفادة من خدماتها مقابل اشتراك (أبو الحجاج، 1998م :18).

وهذه الخصوصية أي عدم وجود مالك محدد أو معروف للانترنت يجعل مهمة رجال الأمن أكثرصعوبة (Thompson,1999).

توسعالشبكة:

فيعام (1985م) كان هناك أقلّ من (2.000) ألفي حاسوب آلي مرتبط بالشبكة، ووصل العددإلى (5.000.000) خمسة مليون حاسوب في عام (1995م) وفي عام (1997م) تجاوز(6.000.000) الستة مليون حاسوب، وتستخدم ما يزيد علي (300.000) ثلاثمائة ألف خادمشبكات (SERVER) ،أي شبكة فرعية، متناثرة في أرجاء العالم،ويمكن القول بأن عدد المستخدمين الجدد يبلغ (2.000.000) إثني مليون شهرياً، أي مايعني انضمام (46) ستة وأربعين مستخدماً جديداً للشبكة في كل دقيقة (السيد،1997م :15).

وفي استطلاع أجرته شبكة (NUA)الأمريكية (NUA, 1998)قدّر عدد مستخدمي الشبكة عالمياً في العام (1998م) بحوالي (134.000.000) مئةوأربعة وثلاثين مليون مستخدم، وتصدرت أمريكا وكندا الصدارة من حيث عدد المستخدمينالذي بلغ (70.000.000) سبعون مليون مستخدم (NUA ,6/1998).

وفي تقرير أجرته ايضاً شبكة (NUA) الأمريكية وصدر بتاريخ 2000/10/26م (NUA, 2000) قدّر أن عدد المستخدمين للشبكة عام (2005م)سيكون حوالي (245.000.000) مئتان وخمسة وأربعون مليون مستخدم، وقدّر أنّ غالبيةهذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ,10/2000).

وقدّرت دراسة أجراها موقع عجيب (Ajeeb.com,25/3/2001) تجاوز عدد المستخدمين العرب الـ(5.000.000) الخمسة ملايين مستخدممع نهاية عام (2001م)، وأن يصل العدد إلى (12.000.000) اثني عشر مليون مستخدم عربيمع نهاية عام (2002م)، كما قدرت الدراسة عدد مستخدمي الإنترنت في المملكة العربيةالسعودية بـ(570.000) خمسائة وسبعون ألف مستخدم.

وأشار الرئيس الأمريكي السابق بيل كلينتون إلى مشروع مستقبلي، لتطوير شبكةالإنترنت، باسم (الإنترنت 2) أو الجيل الثاني من الإنترنت فقال: " لا بُدّمن أنْ نبني الجيل الثاني

لشبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدةومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة من سرعات اليوم، وذلك لتطوير كل منالعلاجات الطبية الحديثة ومصادر الطاقة الجديدة، وأساليب العمل الجماعي" (آفاق الإنترنت، 1997م : 38).
وظهر حديثاً ما يشير في هذه الأيام إلى وجود سباق فضاء من نوع آخر، حيث استطاعتشركة ستارباند (Star band)في تجربه أجرتها في شمال أميركا، من إكمال مشروع انترنت بواسطة أقمار اصطناعية ذياتجاهين، وسرعته تبلغ (500) خمسمائة ك.ب في الثانية، من الإنترنت إلى الحاسبالآلي، وسيبدأ تسويقه إلى المستهلك قريباً (الجزيرة،2000).

خدماتالإنترنت :

يوفرالإنترنت خدمات عديدة من أهمها:

1. **البريد الإلكتروني**: لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص لهعنوان بريدي اليكتروني بصورة سريعة جداً لا تتعدى ثواني.
2. **القوائم البريدية**: تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعاتمن الأشخاص لهم اهتمامات مشتركة.
3. **خدمة المجموعات الإخبارية**: تشبه خدمة القوائم البريدية باختلاف أن كل عضويستطيع التحكم في نوع المقالات التي يريد استلامها.
4. **خدمة الاستعلام الشخصي**: يمكن الاستعلام عن العنوان البريدي لأي شخص أوجهة تستخدم الإنترنت والمسجلين لديها.
5. **خدمة المحادثات الشخصية**: يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.
6. **خدمة الدردشة الجماعية**: تشبه الخدمة السابقة إلا انه ،وفي الغالب، يمكنلأي شخص ان يدخل في المحادثة ،أو يستمع اليها، دون اختيار الآخرين.
7. **خدمة تحويل أو نقل الملفات**: (FTP)لنقل الملفات من حاسب إلى آخر وهي اختصار كلمة (FILE TRANSFERPROTOCOL).
8. **خدمة الأرشيف الإلكتروني**: (ARCHIVE) تُمكّن البحث عن ملفات معينة قد تكون مفقودة في البرامجالمستخدمة في حاسب المستخدم.
9. **خدمة شبكة الاستعلامات الشاملة**:(GOPHER) تفيد في خدمات كثيرة كنقل الملفات والمشاركة في القوائم البريديةحيث يفهرس المعلومات الموجودة علي الشبكة.
10. **خدمة الاستعلامات واسعة النطاق**: (WAIS) تسمي باسم حاسباتها الخادمة وهي أكثر دقةوفاعلية من الأنظمة الاخرى، حيث تبحث داخل الوثائق أو المستندات ذاتها عن الكلماتالدالة التي يحددها المستخدم ثم تقدم النتائج في شكل قائمة بالمواقع التي تحتويالمعلومات المطلوبة.
11. **خدمة الدخول عن بعد**: (TELNET) تسمح باستخدام برامج وتطبيقات في حاسب آلي آخر.
12. **الصفحة الإعلامية العالمية**:(WORLD WIDE WEB) أو الويب(WEB) تجمع معاً كافة الموارد المتعددة التي تحتوي عليها الإنترنتللبحث عن كل ما في الشبكات المختلفة وإحضارها بالنص والصوت والصورة، وتعد الويبنظاماً فرعياً من الإنترنت، لكنها النظام

الأعظم من الأنظمة الأخرى فهي النظامالشامل باستخدام الوسائط المتعددة (يونس، 1421هـ : 34-38).

مستلزماتالاتصال بالشبكة:

يلزمالاتصال بالشبكة العالمية (الإنترنت) توفر عدة أشياء هي :

1.حاسب إلى.
2.جهاز مودم.
3.خط هاتفي.
4.الاشتراك في الخدمة.
5.برامج تصفح الشبكة واشهرها (INTERNET EXPLORER)و (NETSCAPE)

وبعد هذه النبذة عن تاريخ الإنترنت واستخداماته، نعرض فيما يلي مباحث نظرية رئيسةتنطلق منها الدراسة، وهذه المباحث هي:

المبحثالاول: جرائم الحاسب الآلي والإنترنت.

المبحثالثاني: جرائم الإنترنت من منظور شرعي وقانوني.

المبحثالثالث: الأبعاد الفنية للأفعال الجنائية المرتكبة من قبل مستخدمي الإنترنت فيالمجتمع السعودي)تصور إسلامي).

المبحث الأول: جرائمالحاسب الآلي والإنترنت

أُشْتُقّتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمةإجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأَجْرَم فهو مجرم وجريم(ابن منظور، بدون : 604 – 605).

وعَرَّفت الشريعة الإسلامية الجريمة بأنها: " محظورات شرعية زجر الله عنهابحد أو تعزير" (الماوردي، 1417هـ : 19).

وتعرّف جرائم الحاسب الآلي والإنترنت بأنها:" ذلك النوع من الجرائم التيتتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيقفيها ومقاضاة فاعليها "(

مندورة،1410هـ : 21).

كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخداممعرفته بالحاسب الآلي بعمل غير قانوني " (محمد ، 1995م : 73).

وهناك من عرّفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أوموضوع للجريمة" (البداينة، 1420هـ : 102).

وفي كل الأحوال فجريمة الحاسب الآلي " لا تعترف بالحدود بين الدول ولا حتىبين القارات،فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة "(عيد،1419هـ: 252).

وتعد جريمة الإنترنت من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت كأداةلارتكاب الجريمة أو تسهيل ارتكابها (Vacca , 1996).

وأطلق مصطلح جرائم الإنترنت (Internet Crimes) في مؤتمر جرائمالإنترنت المنعقد في استراليا للفترة من 16 – 1998/2/17م (بحر، 1420هـ : 2).

أما التعريف الإجرائي لدراسة الباحث فتُعَرَّفُ جرائم الإنترنت بأنها : جميع الأفعالالمخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية، المرتكبة بواسطةالحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسية والممارسات غيرالأخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقعالمعادية، جرائم القرصنة.

وبالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبياً، إلا أنها لقيتْ اهتماماًمن قبل بعض الباحثين، حيث أُجريتْ العديد من الدراسات المختلفة، لمحاولة فهم هذهالظاهرة، ومن ثم التحكم فيها، ومنها دراسة أجرتها منظمة (BusinessSoftware Alliance)في الشرق الأوسط، حيث أظهرت أنّ هناك تباين بين دول منطقة الشرق الأوسط، في حجمخسائر جرائم الحاسب الآلي، حيث تراوحت ما بين (30.000.000) ثلاثين مليون دولارأمريكي في المملكة العربية السعودية، والإمارات العربية المتحدة، و (1.400.000)مليون وأربعمائة ألف دولار أمريكي في لبنان (البداينة، 1420هـ : 98).

وأظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأنّ (24–42٪) من منظمات القطاع الخاص، والعام، على حد سواء، كانت ضحية لجرائم متعلقةبالحاسب الآلي والإنترنت (البداينة، 1999م : 5).

وقَدّرتْ الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي، مابين ثلاثةوخمسة بلايين دولار سنوياً، كما قَدّرتْ المباحث الفيدرالية (FBI)، في نهاية الثمانيناتالميلادية، أنّ متوسط تكلفة جريمة الحاسب الآلي الواحدة، حوالي ستمئة ألف دولارسنوياً، مقارنة بمبلغ ثلاثة آلاف دولار سنوياً ،متوسط الجريمة الواحدة، من جرائمالسرقة بالإكراه. وبينت دراسة أجراها أحد مكاتب المحاسبة الأمريكية أن (240) مئتينوأربعين شركة أمريكية، تضررت من جرائم الغش باستخدام الكمبيوتر ComputerFraud))، كمابينت دراسة أخرى أُجريتْ في بريطانيا، أنه وحتى أواخر الثمانينات، ارتكب ما يقربمن (262) مائتين واثنين وستين جريمة حاسوبية، وقد كلفت هذه الجرائم حوالي(92.000.000) اثنين وتسعين مليون جنيه إسترليني سنوياً (محمد ، 1995م : 21).

وأظهر مسح أُجري من قبل (the computer security institute) في عام (1999م)، أنّ خسائر(163) مئة وثلاثة وستون شركة أمريكية ،من الجرائم المتعلقة بالحاسب الآلي، بلغتأكثر من (123.000.000) مئة وثلاثة وعشرين مليون دولار أمريكي، في حين أظهر المسحالذي أُجري في عام (2000م) ارتفاع عدد الشركات الأمريكية المتضررة من تلك الجرائم،حيث وصل إلى (273) مئتين وثلاث وسبعين شركة، بلغ مجموع خسائرها أكثر من(256.000.000) مائتين وستة وخمسون مليون دولارRapalus,2000)).

كما بينت إحصائيات الجمعية الأمريكية للأمن الصناعي أن الخسائر التي قد تسببهاجرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى (63.000.000.000) ثلاث وستونبليون دولار أمريكي، وأنّ (25٪) من الشركات الأمريكية تتضرر من جرائم الحاسبالآلي، وقد أصيب (63٪) من الشركات الأمريكية والكندية بفيروسات حاسوبية، ووصلالفقد السنوي بسبب سوء استخدام الحاسب الآلي (555.000.000) خمسمائة وخمسة وخمسونمليون دولار .(Reuvid,1998)

ومن الصعوبة بمكان، تحديد أيّ جرائم الحاسب الآلي المرتكبة هي الأكبر من حيثالخسائر، حيث لا يعلن الكثير عن مثل هذه الجرائم، ولكن من أكبر الجرائم المعلنة هيجريمة لوس انجلوس، حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية (EFI) للإفلاس، وبلغت خسائرها(2.000.000.000) ملياري دولار أمريكي. وهناك أيضاً حادثة انهيار بنك بارينجرالبريطاني في لندن، إثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو، حيثحاول البنك إخفاء الخسائر الضخمة، باستخدام حسابات وهمية، أدخلها في الحساباتالخاصة بالبنك، بمساعدة مختصين في الحاسب الآلي، وقد بلغت إجمالي الخسائر حواليمليار ونصف دولار أمريكي (داود، 1420هـ: 31).

وتعتبر هذه الخسائر بسيطة نسبيا مع الخسائر التي تسببتها جرائم نشر الفيروساتوالتي تضر بالأفراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف أعمال بعضتلك

الشركات نتيجة إتلاف قواعد بياناتها، وقد يصل الضرر في بعض المنشئات التجاريةوالصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلتخسائر فيروس (Code Red) إلى ملياري دولار أمريكي، في حين وصلتالأضرار المادية لفيروس الحب الشهير (8.7) مليون دولار واستمر انتشار الفيروسلخمسة اشهر وظهر منه (55) نوعا. وتتراوح أضرار الفيروسات ما بين عديمة الضرر إلىالبسيط الهين وقد تصل إلى تدمير محتويات كامل الجهاز، وأن كان الأكثر شيوعا هو مايسبب ضرراً محصوراً في إتلاف البيانات التي يحتويها الجهاز .(Ajeebb.com,8/8/2001)

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

وكثيراً ما تكون الجرائم التي ترتكب بواسطة الإنترنت وثيقة الصلة بمواقع أرضية علىالطبيعة كما حدث منذ حوالي سنتين عندما قام البوليس البريطاني بالتعاون مع أمريكاودول أوروبية بمهاجمة مواقع أرضية لمؤسسات تعمل في دعارة الإنترنت.

وإن كانت متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيثأن " هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وأن ماهي أرقام تتغير في السجلات. ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعدوقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التيكشف الستر عنها" (مندورة ، 1410هـ : 22).

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 علىمرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها (موثق في شتا،2001م : 103).

إلا أن أهم خطوة في مكافحة جرائم الإنترنت هي تحديد هذه الجرائم بداية ومن ثمتحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بمايتناسب وطبيعة

هذه الجرائم المستجدة ويأتي بعد ذلك وضع تعليمات مكافحتها والتعاملمعها والعقوبات المقترحة ومن ثم يركز على التعاون الدولي لمكافحة هذه الجرائم .

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

وحددت دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت عشر خدمات أمنيةيمكن تقديمها للجمهور عن طريق شبكة الإنترنت، وأبرزت (15) سلبية أبرزها الإباحيةوالمعاكسات والاحتيال والتجسس والتهديد والابتزاز (البيان،2000م).

كما حددت دراسة الشهري الايجابيات الأمنية لشبكة الإنترنت في تلقي البلاغات، توفيرالسرية للمتعاونين مع الأجهزة الأمنية، طلب مساعدة الجمهور في بعض القضايا، نشرصور المطلوبين للجمهور، نشر المعلومات التي تهم الجمهور، تكوين جماعات أصدقاءالشرطة، توعية الجمهور امنيا، استقبال طلبات التوظيف، نشر اللوائح والأنظمةالجديدة، توفير الخدمة الأمنية خارج أوقات العمل الرسمي، سهولة الوصول إلىالعاملين في الجهاز الأمني ، إجراء استفتاءات محايدة لقياس الرأي العام، وسيط فاعلفي عملية تدريب وتثقيف منسوبي القطاع وأخيرا وسيط مهم للإطلاع على خبرات الدولالمتقدمة ولاتصال مع الخبراء والمختصين في مختلف دول العالم (الشهري، فايز،1422هـ).

وليس الأمر قاصرا على ذلك بل بادرت الدول الأوروبية إلى الاستخدام الفعلي لشبكةالإنترنت في البحث عن المجرمين والقبض عليهم " فقد تمكنت العديد من الدول وفيمقدمتها ألمانيا وبريطانيا وتأتي في المرتبة الثالثة فرنسا من استخدام شبكةالإنترنت في السعي نحو ضبط المجرمين – بل التعرف على كل الحالات المشابهة في كلأنحاء أوروبا والاتصال فورا بالانتربول عبر شبكة الإنترنت" (الشهاوي، 1999م :25)

فئات الجناة في جرائم الحاسب الآلي :

يمكن حصر أنواع الجناة في جرائم الحاسب الآلي في أربعةفئات(محمد،1995م :74-75):

الفئة الأولي : العاملون على أجهزة الحاسب الآلي في منازلهم نظرا لسهولةاتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهمللجهاز.

الفئة الثانية : الموظفون الساخطون على منظماتهم التي يعملون بها فيبعودونإلى مقار

عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتىسرقته.

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

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

خصائص وأنواع جرائم الحاسب الآلي والإنترنت :

من الصعوبة الفصل بين جرائم الحاسب الآلي وجرائمالإنترنت،فلابد للأول لارتكاب الثاني، ويُصنِّف محمد ومندورة (محمد،1995م؛مندورة،1410هـ) تلك الجرائم إلى مجموعات:

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

المجموعة الثانية : تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلييقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبرالبريد الإلكتروني أو بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيلبرامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامجحماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامجالحماية لضمان أقصى درجة من الحماية . ومع أن وجود هذه البرامج في جهاز الحاسبالآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقايةوالتي قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناتهخاصة إذا كان الفيروس حديث وغير معروف من السابق .

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

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

المبحث الثاني: جرائمالإنترنت من منظور شرعي وقانوني

" يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة فيالمجتمعات المغلقة والشرقية، حيث أن تعّرض مثل هذه المجتمعات لقيم وسلوكياتالمجتمعات الأخرى قد تسبب تلوثا ثقافيا يؤدي إلى تفسخ اجتماعي وانهيار في النظامالاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي واللاقانوني للشبكة قديصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم النمو السليمويوقعهم في أزمات نمو، وأزمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصةعند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الإباحية" (البداينة،1999م : 101)

والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين و" مع دخولالكمبيوتر (الحاسب الآلي) الذكي إلى المنازل فان ذلك سيفتح الباب لأنواع متطورةمن الجرائم التي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآليوبشكبة الانترنت، فطالما انك تستطيع مثلا وصل خزانة الأموال في مكتبك بشبكةالانترنت لإعطاء إنذار عند محاولة فتحها فربنا يكون من الممكن فتحها عن بعد بواسطةالكمبيوتر (الحاسب الآلي) ثم الوصول إليها وإفراغها " (داود، 1420هـ : 32).

واستلزم التطور التقني تطور في طرق إثبات الجريمة والتعامل معها، فالجرائم العاديةيسهل – غالباً - تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشفملابسات الجريمة، في حين انه من الصعوبة بمكان تحديد مكان وقوع الحادثة عندالتعامل مع جرائم الانترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلىآخر في ثواني قليلة، كما انه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدوددولية أو جغرافية. ونتيجة لذلك فإن تحديد أين تكون المحاكمة وما هي القوانين التيتخضع لها أمر في غاية الحساسية والتعقيد خاصة وان كل دولة تختلف قوانينها عنالدولة الأخرى، فما يعتبر جريمة في الصين مثلا قد لا يعتبر جريمة في أمريكا والعكسصحيح، بل أن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولةالواحدة كما في الولايات المتحدة الأمريكية (Thompson,1999).

وأدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي،مما اجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمةالمعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكةالإنترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما اثارته منمشكلات قانونية حول تطبيق القانون

الجنائي من حيث الاختصاص القضائي ومكان وزمانارتكاب الجريمة حيث يسهل على المجرم في مثل هذه الجرائم ارتكاب جريمة ما في مكانغير المكان الذي يتواجد فيه أو الذي حدثت فيه نتائج فعله (تمام، 2000م : 1- 3).

وتطوير القوانيين الجنائية وتحديثها امر يستغرق بعض الوقت فـ" هناك تعديلاتكثيرة مطلوب ادخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبارالمعطيات الجديدة التي نشأت عن إستخدام الحاسب الآلي في مجال المعلومات وعن ظهورشبكات المعلومات العالمية" (داود، 1421هـ : 68).

ولاقت جرائم الحاسب الآلي اهتماما عالميا فعقدت المؤتمرات والندوات المختلفة ومنذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (1993م) الذي تناول موضوعجرائم الحاسب الآلي والجرائم الأخرى في مجال تكنلوجيا المعلومات وتوصل الي توصياتاحاطت بجوانب مشكلة جرائم الحاسب الآلي الا انها لم تتعرض لجزئية هامة وهي التعاونالدولي الذي يعتبر ركيزة اساسية عند التعامل مع هذه النوعية من الجرائم (عيد،1419هـ:56 – 259).

وهذا المؤتمريعتبر تحضيرا للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانونالعقوبات الذي عقد في البرازيل عام (1994م) والذي وضع توصيات حول جرائم الحاسبالآلي والانترنت والتحقيق فيها ومراقبتها وضبطها وركز على ضرورة ادخال بعضالتعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وافرازاتها(احمد،2000م : 5 – 10).

والتعاون الدولي مهم عند التعامل مع جرائم الإنترنت، كونه سيطّور اساليب متشابهةلتحقيق قانون جنائي واجرائي لحماية شبكات المعلومات الدولية ،خاصة ان هذه الجرائمهي عابرة للقارات ولا حدود لها، وفي المقابل فان عدم التعاون الدولي سيؤدي إلىزيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين منالإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية (الشنيفي، 1414هـ :113).

وتعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدرقانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسبالآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البياناتالحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها (الشنيفي، 1414هـ :108؛ عيد، 1419هـ : 255)

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمةالحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسةأنواع رئيسة للجرائم المعلوماتية وهي:

جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعببالحسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات الماديةللحاسب. وفي عام (1986م) صدر قانونا تشريعاً يحمل الرقم (1213) عرّف فيه جميعالمصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلباتالدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتهاالخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسبالآلي، وقد خولت وزارة العدل الأمريكية في عام (2000م) خمسة جهات منها مكتبالتحقيقات الفيدرالي (FBI)للتعامل مع جرائم الحاسب الآليوالانترنت(الشنيفي، 1414هـ: 109؛ عبدالمطلب، 2001م: 92 – 94؛ عيد، 1419هـ: 255).

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانونمكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداةالتزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواءبالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى (الشنيفي، 1414هـ : 109؛ عيد،1419هـ : 255)

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيثعدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآليوالانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائمالتدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهاتالتحقيق كما جاء في قانون المنافسة (The Competition Act) مثلا الذي يخول لمأمورالضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعاملمعها وضبطها (احمد، 2000م : 263؛ الشنيفي، 1414هـ : 110؛ عيد، 1419هـ : 255)

وفي عام (1985م) سنّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنتوالتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروعإلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أوالتلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها(الشنيفي، 1414هـ : 110؛ عيد، 1419هـ : 255)

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجداتالإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88) الذي أضاف إلى قانونالعقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (1994م)تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصةبالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك

طلبالتحريات وسماع الأقوال (تمام، 2000م : 91- 92، 115؛ شتا، 2001م : 70)

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآليمتى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حقالتنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانيةالحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معهاوذلك خلال مدة أقصاها ثلاثة أيام (احمد، 2000م : 222، 263)

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انهلا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاءكلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرت عام (1991م)شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل (احمد، 2000م : 222، 276).

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفيةالتعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدمطبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطيالشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ماكان ذلك إلى إدانته أو إدانة احد أقاربه. بل تذهب القوانين الجنائية المعمول بهافي بولندا إلى ابعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أوتفسيره بما يضر المتهم (احمد، 2000م : 276).

هذا وعلى مستوى الدول العربية فانه وحتى تاريخه ،وبحسب علم الباحث، لم تقم أي دولةعربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظامقانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانونالجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضدالأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية، ومن ذلك مثلا اعتبرأن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآليةللمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاءالأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية، وأوكل إلى القضاء الجنائيالنظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية (تمام، 2000م : 91-104، 126).

وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجدنص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرارالمترتبة على جريمة الإنترنت. وقد أوكل إلى شركة البحرين للاتصالات السلكيةواللاسلكية (بتلكو) مهمة تقديم خدمة الإنترنت للراغبين في ذلك، كما أنيط بهامسئولية الحد من إساءة استخدام شبكة الإنترنت من قبل مشتركيها (بحر، 1420هـ : 39،43).

وعلى المستوي المحلي نجد أن المملكة العربية السعودية أيضا لم تسن قوانين خاصةبجرائم الإنترنت ،إلا أن الوضع مختلف هنا، فهي ليست في حاجة لتحديث قوانينهاوتشريعاتها كونها تنطلق من الشريعة الإسلامية الكاملة، فالمشرع واحد لا ثاني لهوالتشريع أزلي لا تجديد له، وهو مع كونه أزلي فانه صالح لكل زمان ومكان كونه صادرمن خالق الكون والعليم بما يَصْلُحُ له ويُصْلِحُهُ " وتركت الشريعةالإسلامية الباب مفتوحا لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة منها لاضرر ولا ضرار وتركت لولي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاةلمصلحة المجتمع ويندرج ذلك تحت باب التعازير" (الشهري، عبدالله، 1422هـ :38)، وهناك قاعدة سد الذرائع أي "دفع الوسائل التي تؤدي إلى المفاسد، والأخذبالوسائل التي تؤدي إلى المصالح" (أبو زهرة، 1976م : 226)

"ومن المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح" (أبو زهرة،1976م : 228)

ونظراً لأن "الظاهرة الإجرامية من الظواهر الاجتماعية التي تتميز بالنسبية،لأنها تختلف باختلاف الثقافات، فما يعد جريمة أو جنحة في مجتمع ما قد يعد مقبولافي مجتمع آخر. فالتشريع والثقافة السائدان في كل مجتمع هما اللذان يحددان الجرائموالفضائل" (السيف، 1417هـ:1).

لذا فان هذا البحث وعند دراسته لجرائم الانترنت في المجتمع السعودي فانه ينطلق منالقوانين الشرعية المعمول بها في المملكة العربية السعودية التي تستمد قوانينها منكتاب الله وسنة نبيه محمد عليه أفضل الصلاة وأزكى التسليم، وليس من القوانينالوضعية 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 امتناععن فعل يقضي به القانون، ولا يعتبر الفعل أو الترك جريمة إلا إذا كان مجرّماً فيالقانون. أما التعريف الشرعي للجريمة فهي إتيان فعل محرم معاقب على فعله أو تركفعل محرم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقابعليه. (عودة، 1401هـ : 66). أو بمعنى آخر هي "فعل ما نهي الله عنه، وعصيان ماأمر الله به" (أبو زهرة، 1976م : 24).

وقد لا يبدوا أن هناك اختلاف كبير بين التعريفين ،وهذا صحيح إلى حد كبير، ولكنيتّضح الاختلاف في التقسيم الذي يأخذ به كل فريق، ففي الشريعة الإسلامية تقّسمالجريمة من حيث جسامة العقوبة إلى حدود، قصاص أو دية، وتعازير، في حين تقّسمالقوانين الوضعية الجريمة من حيث العقوبة إلى جنايات، جنح، ومخالفات (الدمينى،1402هـ، طالب، 1998م : 168). أو بمعنى آخر فان القوانين الوضعية " تقسمالجريمة 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 منحيث المساس بالضرورات

الخمس" (منصور، 1410هـ : 213 – 214).

وبشكل أدق فالاختلاف يقع في التقسيم الثالث أي في قسم التعازير في الشريعة وقسمالمخالفات في القوانين الوضعية، ففي الأولي أشمل واعم حيث انه يدخل في التعازير كلالأفعال سواء المجرمة أو غير المجرمة، أي التي لها عقوبة محددة أو التي لم ينص عليعقوبة محددة لها، فالعقوبة هنا تقديرية للقاضي وتبدأ من الزجر والتوبيخ وتصل إلىحد إيقاع عقوبة القتل تبعا للفعل المرتكب ولنظرة القاضي لذلك الفعل. في حين يحددالقانون الوضعي عقوبات محددة للمخالفات بمعنى انه لا يمكن معاقبة أي فعل ما لم يكنهناك نص محدد له في القانون وإلا لم يعتبر جرما، ومن هنا تختلف النظرة إلى الجريمةفي الشريعة الإسلامية عنها في القوانين الوضعية حيث أنها أشمل وأعم في الشريعةعنها في القوانين الوضعية، الأمر الذي يجعل معه الشريعة الإسلامية متطورة ومتجددةدوما 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 أومنافي لتعاليم الدين الإسلامي ولو كان جديدا فان هناك عقاب له في الشريعة،فـ"الأساس بلاشك في اعتبار الفعل جريمة في نظر الإسلام هو مخالفة أوامرالدين"(أبوزهرة، 1976م: 31)، أما العقوبة المقررة لكل جريمة فمتفاوتة حيث"تتفاوت الجرائم في الإسلام بتفاوت ما فيها من مفاسد" (أبو زهرة، 1976م:185)، فالشريعة حددت إطار عام للأفعال المقبولة وغير المقبولة جديدها وقديمها، كماحددت العقوبة المناسبة لكل جريمة أو فعل غير مقبول، وهنا سر تفوق الشريعةالإسلامية.

ومن هذا فقضية الجريمة والعقوبة ومستجداتها أمر محسوم في المملكة العربية السعوديةويميزها عن غيرها من الدول، فالقانون الجنائي لديها ،والمستمد من الشريعة، يتسم"بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث عالجها الشارع الحكيمفي إطار النظام القانوني الشامل المتكامل الذي يغطي كل جوانب الحياة ويصلح لكلزمان ومكان. فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحمايةالمصالح المعتبرة في الإسلام، وهي الدين والنسل والنفس والمال والعقل، وأي اعتداءعلى مصلحة من تلك المصالح يعتبر جريمة يعاقب فاعلها، ويختلف بالطبع مقدار العقوبةحسب جرامة الفعل الإجرامي" (عجب نور، 1417هـ : 13).

ومع ذلك فالأمر يحتاج إلى وضع أسس تنظيمية فاعلة وشاملة لتحديد الجهة المخولةبداية للتعامل مع جرائم الإنترنت والأفعال غير الأخلاقية والتصرفات السلبية التيتحدث أثناء استخدام شبكة الإنترنت تحقيقاً وضبطاً ووقايةً، وكذلك تحديد كيفيةالتعامل الإداري والإجرائي في هذه القضايا، فلا بد أن يواكب استخدام المملكةالعربية السعودية لتقنية الإنترنت ظهور أنماط جديدة من الإجرام -كغيرها من الدولالتي 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 مرتكبيهاوإعطاء الحق للمتضررين منها. فهذه التنظيمات سوف تُفَعِّلْ قوانين وتشريعاتالمملكة المستمدة من الشريعة الإسلامية لتضع بعض الحواجز والروادع أمام من يرتكبمثل هذه الجرائم من داخل المملكة.

وقد بدأت المملكة بالعمل في هذا الاتجاه حيث أوكلت المهمة مبدئيا إلى مدينة الملكعبدالعزيز للعلوم والتقنية لتقديم هذه الخدمة عبر مزودي خدمة تجاريين، كما شكلتلجنة أمنية دائمة برئاسة وزارة الداخلية وعضوية ممثلين من القطاعات الأمنيةوالدينية والاجتماعية والاقتصادية المختصة للإشراف على أمن خدمة الإنترنت فيالمملكة وتشمل مهمتها تحديد المواقع غير المرغوبة والتي تتنافى مع الدين الحنيفوالأنظمة الوطنية ومتابعة كل ما يستجد منها لحجبها خاصة تلك المواقع الإباحية أوالفكرية أو الأمنية (النشرة التعريفية، 1419هـ).

وفي تقرير صحفي نشر في موقع صحيفة الجزيرة بتاريخ1421/2/2هـ (الجزيرة، 1421هـ)،كشفت مدينة الملك عبدالعزيز للعلوم والتقنية من خلال وحدة الإنترنت المشرفة علىعمل مقدمي خدمة الإنترنت في المملكة عن إجراءات فنية تهدف إلى محاصرة أعمالالمخربين أو المتسللين ومنعهم ومخالفتهم. وأوضحت الوحدة أنها قد ألزمت جميع مقدميخدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللينوإساءة استخدام البريد الإلكتروني وغيرها من المخالفات المتعلقة بالجوانب الأمنيةلاستخدام شبكة الإنترنت في المملكة ومن بين هذه الإجراءات ما يلي:

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

2.منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـE-MailSpamming)) سواءللتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحاباسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.

3.الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي(Proxy) لمدة لا تقل عن (6) أشهر.

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

5.تحديث سجلات منظمة رايب (www.ripe.com) الخاصةبمقدمي الخدمة.

6.ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبةالمخالفات

الأمنية.

كما أشارت صحيفة عكاظ في عددها رقم (12789) وتاريخ1422/6/13هـ (عكاظ،1422هـ)، بأنمجلس الوزراء السعودي يدرس نظاما جديدا للإنترنت يتضمن فرض عقوبات من بينها السجنوغرامات مالية على مخربي شبكة المعلوماتية (المتسللين)، وأن العقوبات على مخربيالإنترنت ستحدد وفقا للضرر الناجم عن عمليات الاختراق والأعمال التخريبية وأنالعقوبة قد تصل إلى السجن سبع سنوات إلى جانب غرامات مالية.

وهذه التنظيمات مفيدة ولا شك إلا أنها ليست كافية، فالمهم هنا وبداية تحديد جهةمتخصصة ومؤهلة للتعامل مع جرائم الإنترنت تحقيقا وضبطا ووقاية، خلاف مدينة الملكعبدالعزيز التي تضطلع بمهام كثيرة ومختلفة عن المهام التي ستوكل للجهة التي ستحددلمثل هذا العمل. وعلى كل حال فيجب أن لا يركن إلى الأنظمة والتعليمات فقط عندالتعامل مع الجرائم والتجاوزات، فالأنظمة ليست وحدها الرادع لأي مخالفات أو سلبياتوخاصة في بيئة دينية محافظة كالمملكة العربية السعودية حيث يلعب الوازع الدينيوالرقابة الذاتية دور مهم في عملية في عملية الردع والحد من أي تجاوزات، فمن المهمأن يؤخذ

" الجانب الديني في الاعتبار عند مناقشة أخلاقيات تدوال المعلومات كنوع منالضوابط الدينية التي تحكم أخلاقيات استخدام وتداول المعلومات، والتي تردع أياتجاه لدى الأفراد نحو ارتكاب جرائم نظم المعلومات (الانترنت)، فالملاحظ انهتوجد معلومات تقدمها جهات كثيرة بالمجان وشبكة الانترنت متخمة بكميات هائلة من هذهالمعلومات الصالح منها والمفسد. وينطبق هذا على جميع أنواع العلوم والفنون من خلالملايين المواقع التي يطلع على محتواها أكثر من ستين إلى مائة مليون متصل بالشبكةيوميا ويتضاعف عددهم بسرعة مخيفة. ومن ثم يجب أن نركز على ضرورة وجود الضوابطالدينية والأخلاقية، فالذي لا وازع ولا ضمير له قد أتيحت له وسيلة سهلة للغاية فيتوصيل أفكاره ونشر مفاسده بالدرجة نفسها المتاحة أمام النافعين للناس، وقوانين الدولتختلف فيما تتبناه من أساليب للتحكم فيما ينشر عبر شبكة الانترنت، والمحرمات تختلفمن مكان لآخر." (داود ، 1420هـ : 217).

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

<!--[supportLineBreakNewLine! if]-->
<!--[endif]-->

المبحث الثالث:

الأبعاد الفنية للأفعال الجنائية المرتكبة

من قبل مستخدمي الإنترنت في المجتمع السعودي (تصور إسلامي)

<!--[supportLineBreakNewLine! if]-->
<!--[endif]-->

الاستعراض السابق كان يتحدث بصفة عامة عن مواكبة القوانين الدولية والعربية والمحليةللجرائم المستحدثة ومنها جرائم الإنترنت، ولكن ما هي المنطلقات الشرعية والقانونيةلإطلاق مصطلح جريمة على الأفعال المرتكبة أثناء استخدام الإنترنت في المجتمعالسعودي. وللإجابة على هذا السؤال يستحسن التطرق بشيء من التفصيل للجرائم والأفعالالتي تطرقت إليها الدراسة وتكيفها شرعياً وقانونياً وهذه الأفعال هي:

أولا : الجرائم الجنسية والممارسات غير الأخلاقية وتشمل:

1.المواقع والقوائم البريدية الإباحية:

يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها،أو إنشائها. وقد" أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكةالإنترنت يشكل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل فيأعداد مستخدمي الإنترنت حول العالم" (الزعاليل، 1420هـ: 76)، وتختلفالمواقع الإباحية عن القوائم البريدية - التي تخصص لتبادل الصور والأفلام الجنسية- في أن المواقع الإباحية غالبا ما يكون الهدف منها الربح المادي حيث يستوجب علىمتصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهريأو سنوي مقابل الاستفادة من خدمات هذه المواقع، وأن كانت بعض هذه المواقع تحاولاستدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يومية على عناوينهمالبريدية، كما أن تصفح الموقع يتطلب في الغالب الاتصال المباشر بشبكة الإنترنت ممايعنى انه قد يتم حجبه من قبل مدينة الملك عبدالعزيز للعلوم والتكنولوجيا فلا يمكنالوصول إليه إلا باستخدام البروكسي.

أما القوائم البريدية فهي أسهل إنشاءً، وغالباً مجانية ويقوم أعضائها من المشتركينبتبادل الصور والأفلام على عناوينهم البريدية وربما تكون القوائم البريدية ابعد عنإمكانية المتابعة

الأمنية حيث يركز نشاطها على الرسائل البريدية والتي تكون منالصعوبة بمكان منعها عن أعضاء أي مجموعة، حتى وأن تم الانتباه إلى تلك القائمةلاحقا وتم حجبها، فان الحجب يكون قاصرا على المشتركين الجدد واللذين لا يتوفرلديهم وسائل تجاوز المرشحات، أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلىموقع القائمة حيث يصل إلى بريدهم ما يردونه دون أن تستطيع وسائل الحجب التدخل.ويشترك في القوائم البريدية ألاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلىجميع المشتركين مما يعنى كم هائل من الرسائل والصور الجنسية التي يتبادلها مشتركيالقائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التيتقدمها حيث " تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلامالخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفانهائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ"(داود،1420هـ : 93)، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الإنترنتالذي لا يعترف بأي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للأطفال فضلا عنالكبار نتيجة تأثيراته المؤذية وغير المرغوبة (موثق في الزغاليل، 1420هـ : 78).ويوجد على الإنترنت ألاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية والتيأصبحت أكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم أخرى تصنف تحتدول محددة ومن المؤسف انه وجدت بعض المواقع الشاذة بمسميات عربية بل وسعوديةوالأدهى والأمَّرْ أن يربط بين بعض القوائم الإباحية والإسلام كموقع أسمى نفسه" السحاقيات المسلمات " وهكذا.

وكشفت إحدى الدراسات أن معدل التدفق على الواقع الإباحية في أوقات العمل التي تبدأمن الساعة التاسعة صباحا إلى الخامسة عصرا تمثل (70٪) من إجمالي نسبة التدفق علىتلك المواقع (بي بي سي، 2001م).

كما كشفت دراسة قام بها الدكتور مشعل القدهي (القدهي،1422هـ) بان هناك إقبال كبيرجدا على المواقع الإباحية حيث تزعم شركة (Playboy) الإباحية بأن (4.7)مليون زائر يزور صفحاتهم على الشبكة أسبوعياً، وبأن بعض الصفحات الإباحية يزورها(280.034) زائر يوميا وأن هناك مائة صفحة مشابهة تستقبل أكثر من (20.000) ألف زائريوميا وأكثر من ألفين صفحة مشابهة تستقبل أكثر من (1400) زائر يوميا، وأن صفحةواحدة من هذه الصفحات استقبلت خلال عامين عدد (43.613.508) مليون زائر، كما وجد أن(83.5٪) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية، وبأنّ أكثر من(20٪) من سكان أمريكا يزورون الصفحات الإباحية حيث تبدأ الزيارة غالبا بفضولوتتطور إلى إدمان، وغالبا لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفحالمواد الإباحية بها أو شراء مواد خليعة منها وقد بلغت مجموعة مشتروات موادالدعارة في الإنترنت في عام (1999م) ما نسبته (8٪) من دخل التجارة الإلكترونيةالبالغ (18) مليار دولار أمريكي في حين بلغت مجموعة الأموال المنفقة للدخول علىالمواقع الإباحية (970) مليون دولار ويتوقع ارتفاع المبلغ ليصل إلى (3)

مليارد ولار في عام (2003م)، وقد أتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهمما بين (12) و (15) عام في حين تمثل الصفحات الإباحية أكثر صفحات الإنترنت بحثاوطلبا.

كما وضحت دراسة أدست (Adsit, 1999)(Adsit) أن المواقع الإباحية أصبحت مشكلة حقيقيةوأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر، ويمكن أن يلمسأثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة،العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذالبدل الاحترام. ويبدوا أن لكثرة المواقع الإباحية على الإنترنت والتي يقدر عددهابحوالي (70.000) ألف موقع دور كبير في إدمان مستخدمي الإنترنت عليها حيث أتضح أننسبة (15٪) من مستخدمي الإنترنت البالغ عددهم(9.600.000) مليون شخص تصفحوا المواقعالإباحية في شهر ابريل عام (1998م).

وقد جرى حصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقععلى شبكة الإنترنت ومنها موقع الياهو (YAHOO) فوجد أنها تصل إلى(171) قائمة، بلغ عدد أعضاء اقل تلك القوائم (3) في حين وصل عدد أكثرها أعضاء إلى(8683) أما موقع قلوب لست (GLOBELIST) فقد احتوى على (6)قوائم إباحيةعربية، في حين وجد عدد (5) قوائم عربية إباحية على موقع توبيكا (TOPICA) وقد قامت مدينة الملكعبدالعزيز للعلوم والتقنية مشكورة بإغلاق تلك المواقع.

فارتياد مثل هذه المواقع ومشاهدة المواد الجنسية بها من المحظورات الشرعية التيحرص الشارع الحكيم على التنبيه عليها وتحريمها، بل أن الشارع الحكيم امرنا بغضالبصر وحرّم النظر إلى الأجنبيات سواء بصورة أو حقيقة وليس فقط تجنب النظر إلىالحرام فقال عز وجل في كتابه الحكيم في سورة النور: (قُلْ لِلْمُؤْمِنِينَيَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَلِكَ أَزْكَى لَهُمْإِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ(30)).

فهناك ولا شك علاقة بين " ارتكاب الأفعال الجنسية المحرمة والنظر إلى الصورالجنسية العارية، فالدين الإسلامي الحنيف حذر من ظاهرة النظر للعراة، لما تحدثه منتصدعات أخلاقية في الفرد والمجتمع" (السيف، 1417هـ : 100).

ويذهب الشارع إلى ابعد من ذلك لعلمه بمخاطر النظر وما يمكن أن يوصل إليه، فحرّمرسول الله صلى الله عليه وسلم أن تصف المرأة لزوجها جمال امرأة أخرى لا تحل لهوكأنه ينظر إليها فقال عليه الصلاة والسلام في الحديث الذي رواه البخاري في صحيحهواحمد في مسنده واللفظ للبخاري: " قَالَ النَّبِيُّ صَلَّى اللَّهم عَلَيْهِوَسَلَّمَ لَا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَاكَأَنَّهُ يَنْظُرُ إِلَيْهَا".

كل هذه الأمور اهتم بها الشارع وحرمها كونها موصلة لجريمة الزنا التي تعد منالكبائر والتي متى ما اجتنب الأفراد هذه الأفعال فلن يقعوا في الزنا. ولعل من حكمةالشارع ومعرفته بالغرائز البشرية التي يساهم الشيطان في تأجيجها ليوقع الإنسانفيما حرم الله، ولعظمة جريمة الزنا فانه لم يحرم الزنا فقط بل حرم الاقتراب منهفقال تعالى في سورة الإسراء: (وَلَا تَقْرَبُوا الزِّنَى إِنَّهُ كَانَ فَاحِشَةًوَسَاءَ سَبِيلًا(32))

يقول القرطبي رحمه الله في تفسير هذه الاية " قال العلماء قوله تعالى"ولاتقربوا الزنى" ابلغ من ان يقول ولا تزنوا فإن معناه فلا تدنوا منالزنا. فاي اقتراب من المحظور هو فعل محظور في حد ذاته، ومن ذلك مشاهدة الموادالجنسة فضلا عن الاشتراك في تلك القوائم الاباحية أو شراء مواد جنسية منها أو ،وهوالاخطر ضررا، انشائها كون الفعل الاخير متعدي ضرره للغير ويدخل فاعله في وعيد اللهعز وجل حين قال في سورة النور: (إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَالْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَاوَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ(19))

وقد اثبتت بعض الدراسات في المجتمع السعودي ان (68.8 ٪) من مجموعة المبحوثين يرونان هناك علاقة بين الانحراف والجرائم المرتبكة وبين مشاهدةاشرطة الفيدوا الجنسية،كما اثبتت احدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمعالسعودي والتي اجريت في الاصلاحيات المركزية بالمملكة ان (53.7 ٪) من مرتكبيالجرائم الجنسية كان لهم اهتمامات بالصور الجنسية وان فئة كبيرة منهم كانوا يميلونإلى مشاهدة الافلام الجنسية الخليعة وقت فراغهم، كما تبين من الدراسة قوة تأثيرمثل هذه الصور في ارتكاب جرائم الاعتداء الجنسي من قبل مجرمي اغتصاب الاناث وهاتكياعراض الذكور بقوة (السيف، 1417هـ : 99).

2.المواقع المتخصصة في القذف وتشويه سمعة الاشخاص:

تعمل هذه المواقع على ابراز سلبيات الشخص المستهدف ونشراسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أوبتلفيق الاخبار عنه. وهناك حادثة مشهورة جرتدأولها بين مستخدمى الإنترنت في بدايةدخول الخدمة للمنطقة حيث قام شخص في دولة خليجية بإنشاء موقع ونشر صور احدىالفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل علي تلك الصور بعد التسللإلى حاسبها الشخصي وحأول ابتزازها جنسيا ورفضت فهددها بنشر تلك الصور على الإنترنتوفعلا قام بتنفيذ تهديده بانشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديدمن المنتديات والقوائم البريدية وادى ذلك إلى انتحار الفتاة حيث فضحها بين ذويهاومعارفها.

كما وقعت حادثة تشهير أخرى من قبل من اسموا نفسهم " الامجاد هكرز " حيثاصدروا بيان نشر على الإنترنت بواسطة البريد الالتكروني ووصل العديد من مشتركيالإنترنت أوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر على التطاول في احدىالمنتديات بالقدح والسب السافر على شيخ الإسلام ابن تيمية والشيخ محمد بنعبدالوهابوغيرهم من رموز الدعوة السلفية وقد استطاع (الأمجاد هكرز) اختراق البريدالإلكتروني الشخصي للمذكور ومن ثم تم نشر صورهوكشف اسراره في موقعهم على الإنترنتحيث خصصوا صفحة خاصة للتشهير به وعنوانها على الشبكة هو :
http://216.169.120.174/hijazi.htm(موقع منتدىالفوائد،1421هـ)

وحوادث التشهير والقذف في شبكة الإنترنت كثيرة فقد وجد ضعفاء النفوس في شبكةالإنترنت، وفي ظل غياب الضوابط النظامية والجهات المسئولة عن متابعة السلبيات التيتحدث اثناء إستخدام الإنترنت، متنفسا لاحقداهم ومرتعا لشهواتهم المريضة دون رادعأو خوف من المحاسبة وقد قيل قديما "من أمن العقوبة أساء الادب".

والقذف مُجَّرم شرعاً، ونظرا لشناعة الجرم ومدى تاثيره السلبي على المجنى عليهوالمجتمع كونه يساعد على اشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعلعقوبته من الحدود والتي لا يملك احد حق التنازل عنه ولا يجوز العفو عنها بعد طلبالمخاصمة امام القضاء،كما جعلها عقوبة ذات شقين الأول عقوبة بدنية بجلده ثمانينجلدة لقوله تعالى في سورة النور(وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْيَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً (4))،والشقالثاني عقوبة معنوية بعدم قبول شهادة الجاني بعد ثبوت جلده لقوله تعالى في ذاتالاية وذات السورة: (وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُالْفَاسِقُونَ (4)) وشدد رسول الله صلى الله عليه وسلم في جريمة القذف حيثاعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفق عليه"اجتنبوا السبع الموبقات، قالوا يارسول الله، وما هن؟ قال الشرك بالله،والسحر، وقتل النفس التي حرم الله الا بالحق، وأكل الربا، واكل مال اليتيم،والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات". ولا تعاقب الشريعة علىالقذف الا اذا كان كذبا واختلاقا فان كان حقيقة واقعية فلا جريمة ولاعقوبة (عودة،1401هـ: 645-646؛ فرحات، 1404هـ : 151-164).

3.استخدام البروكسي للدخول إلى المواقع المحجوبة:

البروكسي هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدميالإنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدي مستخدمي الانترنتللبروكسي هو ما يستخدم لتجأوز المواقع المحجوبة وهو ما نقصده في هذه الدراسة حيثيستخدم البروكسي من قبل مستخدمي الإنترنت في المجتمع السعودي لتجأوز المواقعالمحجوبة من قبل مدينة الملك عبدالعزيز للعلوم والتقنية والتي عادة ما تكون هذهالمواقع المحجوبة اما مواقع

جنسية أو سياسية معادية للدولة، وقد يتم حجب بعضالمواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر احصائيات عن الجرائمأو حتى بعض المواقع العادية ويعود ذلك للالية التي يتم بها عملية ترشيح المواقعوربما لخطأ بشري في حجب موقع غير مطلوب حجبه، ولذلك فقد تجد من يستخدم البروكسيللدخول إلى موقع علمي أو موقع عادي حجب خطأً، وهذا في حكم النادر والشاذ لا حكمله، في حين ان الغالبية العظمى تستخدم البروكسي للدخول إلى المواقع الجنسية أوالمواقع السياسية ولكن بدرجة اقل.

ومن هنا فاستعمال البروكسي للدخول إلى المواقع المجوبة يعتبر امرا مخالفا للنظامالذي اقر حجب تلك المواقع حتى لو افترضنا جدلا ان هناك نسبة بسيطة جدا قد تستخدمالبروكسي للدخول إلى المواقع التي قد تكون حجبت بطريق الخطأ، الا ان هذه النسبةسواء من الافراد أو من المواقع التي تحجب بالخطأ تكاد لاتذكر وهي في حكم الشاذ،اضف إلى ذلك انه يفترض في المواطن والمقيم احترام النظام والتقيد به دون ان يعملبوسيلة أو بأخرى تجاوز هذا النظام لاي مبرر حتى وان شاب النظام خلل اثناء تنفيذه،ففتح مثل هذه الثغرة والسماح للافراد بتجأوز التعليمات التي اقرها النظام لمبرر قديكون واهي أو لخطأ قد يكون واكب تنفيذ امر فيه من الخطورة الشي العظيم حيث سيجرأالافراد على تجاوز النظام لاي مبرر وتعم الفوضي وتسود الجريمة.

هذا من ناحية مخالفة إستخدام البروكسي للنظام، اما من ناحية مخالفة إستخدامالبروكسي للشرع فهو من شقيين :

أ-ان النظام أُقِّر من ولي الامر و مخالفة ولي الامر من المحظورات الشرعية ، مادامت تلك الأنظمة لا تخرج عن تعاليم الشرع، والدليل على ذلك قوله تعإلى في سورةالنساء (َاأَيُّهَا الَّذِينَ آمَنُوا أَطِيعُوا اللَّهَ وَأَطِيعُوا الرَّسُولَ وَأُولِيالْأَمْرِ مِنْكُمْ(59)) وقوله صلى الله عليه وسلم في الحديث الذي روي في المعجمالكبير " يا أيها الناس اتقوا الله واسمعوا وأطيعوا لمن كان عليكم وان عبداحبشيا مجدعا فاسمعوا وأطيعوا ما أقام فيكم كتاب الله" وفي الحديث الذي رواهاحمد في مسنده " قد تركتكم على البيضاء ليلها كنهارها، لا يزيغ عنها بعدي إلاهالك، ومن يعش منكم فسيرى اختلافا كثيرا، فعليكم بما عرفتم من سنتي و سنة الخلفاءالراشدين المهديين، و عليكم بالطاعة و إن عبدا حبشيا عضوا عليها بالنواجذ ، فإناالمؤمن كالجمل الأنف حيثما انقيد انقاد".

ب-اذا كان مشاهدة المواقع الجنسية حرام، فإن إستخدام البروكسي للدخول إلى تلكالمواقع حرام ايضا فما بني على باطل فهو باطل، والفعل اذا كان محرماً فان الوسيلةالموصله اليه تكون محرمة. وتنطبق هنا قاعدة سد الذرائع أي "دفع الوسائل التيتؤدي إلى المفاسد، والاخذ بالوسائل التي تؤدي إلى المصالح" (ابوزهرة، 1976م :226)، كما انه "من المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح"(ابوزهرة، 1976م : 228).

4.إخفاء الشخصية:

توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيتهسواء اثناء إرسال البريد أو اثناء تصفح المواقع. ولا شك ان اغلب من يستخدم هذهالبرامج هدفهم غير نبيل، فيسعون من خلالها إلى إخفاء شخصيتهم خوفا من مسائلةنظامية أو خجلا من تصرف غير لائق يقومون به. ومن الامور المسلمة بها شرعا وعرفا انالافعال الطيبة لا يخجل منها الاشخاص بل يسعون عادة ،الا في حالات معينة، إلىالاعلان عنها والافتخار بها، اما الافعال المشينة فيحرص الغالبية على اخفائها.فاخفاء الشخصية غالبا امر مشين وتهرب من المسئولية التي قد تلحق بالشخص متى ماعرفت شخصيته، ولعل ما يدل على ذلك حديث رسول الله صلى الله عليه وسلم الذي رواهمسلم في صحيحه "البر حسن الخلق، والاثم ما حاك في صدرك وكرهت ان يطلع عليهالناس".

5.إنتحال الشخصية:

وهي تنقسم إلى قسمين:

أ-انتحال شخصية الفرد :

تعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة الا ان التنامي المتزايدلشبكة الإنترنت اعطى المجرمين قدرة اكبر على جمع المعلومات الشخصية المطلوبة عنالضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير منالاعلانات المشبوهة والتي تداعب عادة غريزة الطمع الانساني في محاولة الاستيلاءعلى معلومات اختيارية من الضحية، فهناك مثلا اعلان عن جائزة فخمة يكسبها من يساهمبمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصيةكالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهةالخيرية، وبالرغم من ان مثل هذا الاعلان من الوضوح بمكان انه عملية نصب واحتيالالا انه ليس من المستبعد ان يقع ضحيته الكثير من مستخدمي الإنترنت. ويمكن ان تؤديجريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقتهالائتمانية أو حتى الاساءة إلى سمعة الضحية (داود، 1420هـ: 84-89).

ب-انتحال شخصية المواقع :

مع ان هذا الاسوب يعتبر حديث نسبياً، الا انه اشد خطورة واكثر صعوبة في اكتشافه منانتحال شخصية الافراد، حيث يمكن تنفيذ هذا الاسلوب حتى مع المواقع التي يتمالاتصال بها من خلال نظم الاتصال الامن (Secured Server) حيث يمكن وبسهولةاختراق مثل هذا الحاجز الامني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقعللسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحأول المجرم اختراق موقع لاحدمقدمي الخدمة

المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيهأي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع ان يكثر استخدام اسلوبانتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها (داود، 1420هـ:89-93).

والمحاذير الامنية والمخالفات النظامية والشرعية واضحة في هذه الفقرة سواء ماكانمنها قاصرا على انتحال شخصية الافراد أو المواقع، فقد حفظت الشريعة السماويةوالأنظمة الوضعية الحقوق الشخصية وصانت الملكيات الفردية وجعل التعدي عليها امرامحظورا شرعيا ومعاقب عليه جنائياً.

وفي انتحال شخصية الآخرين تعدي صارخ على حقوقهم وانتهاكا لملكياتهم التي صانهاالشرع لهم، كما انه ترتب على انتحال شخصية الاخرين اضرار متنوعة قد تلحق بهم،وتتفأوت هذه الاضرار بتفأوت نتيجة الفعل والذي قد تقتصر على اضرار معنوية كتشويهسمعة الشخص وقد تصل إلى اضرار مادية كالاستيلاء غير المشروع على ممتلكات ومقتنياتمادية للمجنى عليه.

ومهما كان حجم هذه الاضرار الناتجة عن هذا الفعل غير النظامي فانه لا يمكن الا انيتضرر المجنى عليه من هذا الفعل وخاصة ان الهدف الغالب من وراء انتحال الشخصية لنيكون حميدا أو بحسن نية أو لخدمة شخص اخر خلاف منتحل الشخصية.

وتتفق الشريعة مع القوانيين الوضعية في جعل الانسان مسئولا عن كل فعل ضار بغيره،سواء اعتبر القانون ذلك الفعل جريمة ام لم يعتبره (عودة، 1401هـ :77)،

ولا شك ان انتحال شخصية الافراد أو المواقع مضر باصحابها الاساسيين ولذلك فهيجريمة قانونية ومخالفة شرعية.

ثانيا: جرائم الاختراقات:
يشمل هذه القسم جرائم تدمير المواقع، اختراق المواقع الرسمية أو الشخصية، اختراقالأجهزة الشخصية، اختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه،الاستيلاء على اشتراكات الآخرين وأرقامهم السرية و إرسال الفيروسات والتروجنات.

ولعل جميع هذه الجرائم والافعال مع اختلافها الا انها يجمعها امر واحد وهي كونهاجميعا تبدأ بانتهاك خصوصة الشخص ، وهذا سببا كافيا لتجريمها، فضلا عن الحاق الضررالمادي والمعنوي بالمجنى عليهم.

وتتفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوصية الفرد ويعتبرمجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريدهالالتكروني أو في أي مكان اخر انتهاكاً لخصوصيته الفردية وحقوقه.

ومن المعلوم "ان الفقهاء يقسمون الحقوق إلى حقوق لله وحقوق للافراد إلا أنالكثيرين منهم يرون بحق ان كل ما يمس حق الجماعة الخالص أو حق الافراد الخالصيعتبر حقا لله تعالى أي من حقوق الجماعة ونظامها" (عودة، 1401هـ :206)، ومنهنا يعتبر التعدى على حقوق الافراد وانتهاك خصوصياتهم الشخصية مخالفة شرعية وجريمةنظامية كونه ينظر اليه شرعا تعدياً على حق الله.

وقد أدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهمالفردية سواء عمدا أو مصادفة، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع علىشبكة الإنترنت حتى يقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة باجهزتهم(******s)وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز منيزور تلك المواقع لعدة اسباب لعل منها التعرف على من يكرر الزيارة للموقع أولاسبابأخرى، وتبقى واحدةمن الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينهاعلى القرص الصلب لجهاز الزائر للموقع في أحد الملفاتالتي قامت الموقع الأخربتخزينها من قبلدون أن يشعر صاحب الجهاز بذلك أو حتى الاستئذان منه! وفورا يتماصدار رقم خاص ليميز ذلك الزائر عنغيره من الزوار وتبدأ الكعكة بأداء مهمتهابجمعالمعلومات وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات وهيعادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم ارسالالمعلومات وتجديد النسخةالموجودة لديهم ويقوم المتصفح لديه بعمل المهمة المطلوبة منهمالم يقم صاحب الجهاز بتعديلوضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكاتبنسخ تلك الملفات والاستفادة منها بطريقة أو بأخرى. كما قد يحصل اصحاب المواقع علىمعلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة اقل ترددا عندما يفشىمعلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعاملمعه انسان اخر (موقع مجلة الأمن الإلكترونية، 1421هـ ؛ داود،1420هـ: 50-52).

هذا وان كانت هناك وسائل لحماية الخصوصية اثناء تصفح الإنترنت، الا انه " منالصعب جدا السيطرة على مايحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي)وعلى ذلك فان حماية الخصوصية يجب ان تبدأ من البداية بتحديد نوعية البيانات التيلاينبغي ان تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلكالمعلومات"(داود،1420هـ:53).

يتضح من كل ما تقدم ان هذه الافعال غير شرعية أو حتى اخلاقية ولا تتمشى مع تعاليمديننا الحنيف الذي حرّص على احترام الحقوق الشخصية وحفظ الملكية الفردية وراعخصوصية الافراد والجماعات، بل اعتبر التعدي على الحقوق الشخصية تعدي على

حقوقالله، مما يعنى انها افعال اجرامية وتصرفات لا اخلاقية يعاقب عليها الشرع بعقوباتتختلف بحسب نوع الفعل المرتكب وبحسب الضرر الواقع على المجنى عليه، وقد يدخل الفعلوعقوبته تحت جرائم الحدود أو القصاص أو التعازير وليس المجال هنا مجال تفصيل لهذهالانواع بقدر ما هو مجال تحديد وايضاح ان هذه الافعال مجرّمة وان هناك عقوبة شرعيةبحق من يرتكب هذه الافعال.

وقد اجْمَلْتُ ايضاح التكييف الشرعي والنظامي لهذه الافعال كونها متشابهة ومتداخلةإلى حد كبير، الا انه ونظرا لخطورتها وشيوعها فيلزم الامر النتطرق وبشيئ منالتفصيل إلى شرح فني لهذه الافعال واضرارها لعله يضيف بعدا اخر يساهم وبوضوح اكثرفي التَعَّرُفْ على كونها مجرَّمة، وهذه الافعال هي:

1.الاقتحام أو التسلل :

يشمل هذا البند جرائم الاختراقات سواء للمواقع الرسمية أو الشخصية أو إختراقالأجهزة الشخصية، إختراق البريد الإلكتروني أو الاستيلاء عليه، الاستيلاء علىاشتراكات الآخرين وأرقامهم السرية. وهي افعال اصبحت تنشر يوميا في الصحف والاخبارفكثيراً ما " تتدأول الصحف والدوريات العلمية الان أنباء كثيرة عن الاختراقاتالأمنية المتعددة في اماكن كثيرة من العالم ليس اخرها اختراق اجهزة الحاسب (الآلي) في البنتاجون (وزارة الدفاع الأمريكية) " (داود، 1420هـ: 99).

ولكي يتم الاختراق فان المتسللون إلى اجهزة الاخرين يستخدممون ما يعرف بحصانطروادة وهو برنامج صغير يتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس علىأعمال الشخص التي يقوم بها على حاسوبه الشخصي فهو في أبسط صورة يقوم بتسجيل كلطرقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السريةأو حساباته المالية أو محادثاته الخاصة على الإنترنت أو رقم بطاقة الائتمان الخاصةبه أو حتى كلمات المرور التي يستخدمها لدخول الإنترنت والتي قد يتم إستخدامها بعدذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية.

و" يعتبر الهجوم على المواقع المختلفة في شبكة الإنترنت (اقتحام المواقع)من الجرائم الشائعة في العالم، وقد تعرضت لهذا النوع من الجرائم في الولاياتالمتحدة مثلا كل من وزارة العدل والمخابرات المركزية والقوات الجوية، كما تعرض لهحزب العمال البريطاني" (داود، 1420هـ: 83).

وقد قام قراصنة اسرائيلين باقتحام صفحة الإنترنت الاعلامية الخاصة ببنك فلسطينالمحدود ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى الغاء الصفحة ومحوهاكليا، كما تعرضت العديد من الشركات الخاصة في مناطق الحكم الذاتي للهجوم والعبثومنها شركة اقتحم المتسللون اجهزتها ووضعوا صورة زوجة مدير الشركة وهي عارية

بعدتجريدها من الملابس بواسطة الحاسب الآلي (ابوشامة، 1420هـ: 37).

وفي عام (1997م) قدّرَتْ وكالة المباحث الفدرالية الأمريكية (FBI) تعرض(43٪) من الشركاتالتي تستخدم خدمة الإنترنت لمحولة تسلل تتراوح مابين (1-5) مرات خلال سنة واحدة (Wilson,2000)، ولا يقتصر التسلل علىالمحترفين فقط بل انه قد يكون من الهواة ايضا حيث يدفعهم إلى ذلك الفراغ ومحاولةاشغال الوقت، كما حدث مع مراهقة في الخامسة عشر من عمرها قامت بمحاولة التسلل إلىالصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة وذلك بسببانها لم تكن تحب مشاهدة التلفزيون لذلك فكرت ان تكون متسللة (Hacker)(Koerner,1999).

وهو ايضا ما اتضح لوكالة المباحث الفدرالية (FBI) اثناء حرب الخليجالأولى عندما اجروا تحقيقا حول تسلل اشخاص إلى الصفحة العنكبوتية الخاصة باحدىالقواعد العسكرية الأمريكية، وكانت الشكوك قد اتجهت بداية إلى ارهابين دوليين الاان الحقيقة تجلت بعد ذلك في ان المتسللين هما مراهقان كانا يعبثان بجهاز الحاسبالآلي في منزلهما (Wilson,2000).

وفي عام (1997م) قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطارماشيتيوشش (Massachusetts) مما ادى إلى تعطيل نظام الملاحة الجويةوأنظمة أخرى حيوية لمدة ستة ساعات، وبالرغم من فداحة الضرر الذي تسبب فيه الا انعقوبته اقتصرت على وضعه تحت الرقابة لمدة سنتين مع الزامه باداء خدمة للمجتمع لمدة(250) يوما (Wilson,2000)، وبهذا فان القانون الامريكي يلعب دورا غيرمباشر في تشجيع المراهقين على اعمال التسلل حيث نادرا ما يعاقب المتسللين دون سنالثامنة عشر، كما يساهم أولياء امور المراهقين في ذلك ايضا حيث يعتبرون ابنائهماذكياء اذا مارسوا انشطة حاسوبية تتعلق بالتسلل إلى اجهزة الاخرين (Koerner,1999).

وأوضحت دراسة اجريت عام (1979م) على عدد (581) طالب جامعي امريكي ان (50٪) منهم قداشترك في اعمال غير نظامية اثناء استخدام الإنترنت خلال ذلك العام، وأن (47) طالباأو مانسبته (7.3٪) سبق وقبض عليه في جرائم تتعلق بالحاسب الآلي، وأن (75) طالبا أومانسبته (13.3٪) قبض على اصدقائهم في جرائم تتعلق بالحاسب الآلي (Fream,1997 & Skinner).

فالعقوبات الحالية لاتساعد على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسبالآلي، ففي خلال عام واحد تضاغفت تلك الجرائم على مستوى الولايات المتحدةالأمريكية، ففي عام (1999م) تحرت وكالة المباحث الفدرالية (FBI) عن (800) حالة

تتعلقبالتسلل(Hacking) وهو ضعف عدد الحوادث التي قامت بالتحريعنها في العام السابق أي عام (1998م)، أما الهجوم على شبكات الحاسب الآلي علىالإنترنت فقد تضاعف (300٪) في ذلك العام ايضا (Koerner,1999).

وللحد من تزايد عمليات التسلل(Hacking) ونظرا لان المتسللين عادة يطورون تقنياتهمبصفة مستمرة ويملكون مهارات متقدمة، فقد اضطر مسئولوا أمن الحاسبات الآلية وشبكاتالإنترنت وكذلك رجال الامن على الاستعانة بخبرات بعض محترفين التسلل ليستطيعواتطوير نظم الحماية ضد المتسللين (Hackers)، وعلى سبيل المثال يرسل مسئولي امنالحاسبات اسئلة تتعلق باحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أوما تعرف باسم (hacker internet chat room) ولطلب نصائح تقنية حولأحدث سبل الحماية (Staff, 2000, February 17).

بل ان وكالة المباحث الفدرالية (FBI) استعانت ايضا بخبراء في التسلل (Hackers) لتدريب منسوبي الوكالةعلى طرق التسلل (Hacking) لتنمية خبراتهم وقدراتهم في هذا المجالوليستطيعوا مواكبة خبرات وقدرات المتخصصين من المتسللين (Hackers)، ومنهم أحد أشهرالمتسللين (Hackers) ويدعى (BrianMartin)والمشهور باسم (Jericho) وهو متهم حاليا بالتسلل والعبث بمجتوياتالصفحة الرئيسية لصحيفة (New Youk Times) على شبكة الإنترنت (Staff,2000 April 2).

واكدت وحدة الخدمات السرية الأمريكية (The US Secret Service) ان الجرائم المنظمةتتجه نحو استغلال التسلل (Hacking) للحصول على المعلومات اللازمة لتنفيذمخططاتها الإجرامية (Thomas,2000).

وفي خبر نشرته صحيفة لوس انجلوس تايمز أوضحوا ان متسللين قاموا باقتحام نظامالحاسب الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنياالأمريكية (موقع ارابيا،2001/6/10م).

2.الاغراق بالرسائل :

يلجأ بعض الاشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني لشخص ما بقصدالاضرار به حيث يؤدى ذلك إلى تعطل الشبكة وعدم امكانية استقبال أي رسائل فضلا عنامكانية انقطاع الخدمة وخاصة اذا كانت الجهة المضررة من ذلك هي مقدمة خدمةالإنترنت مثلا حيث يتم ملء منافذ الاتصال (Communication-Ports) وكذلك قوائم الانتظار (Queues) مما ينتج عنه انقطاعالخدمة وبالتالي تكبد خسائر مادية

ومعنوية غير محدودة، ولذلك لجأت بعض الشركات إلىتطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق اعداد كبيرة منها(داود،1420هـ:93).

واذا كان هذا هو حال الشركات الكبيرة فلنا ان نتصور حال الشخص العادي اذا تعرضبريده لمحاولة الاغراق بالرسائل حيث لن يصمد بريده طويلا امام هذا السيل المنهمرمن الرسائل عديمة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرةالحجم، خاصة اذا علمنا ان مزود الخدمة عادة يعطي مساحة محددة للبريد لا تتجاوزعشرة ميقا كحد اعلى.

3.الفيروسات الحاسب الآلية :

الفيروسات الحاسب الآلييه هي احدى انواع البرامج الحاسب الآلية الا أن الأوامرالمكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكنعند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالةالبريدية المرسل معها الفيروس اصابة الجهاز به ومن ثم قيام الفيروس بمسح محتوياتالجهاز أو العبث بالملفات الموجودة به.

وقد عرفها احد خبراء الفيروسات (Fred Cohen) بانها نوع من البرامجالتي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعنيببساطة أن الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي اخر بحيث يتكاثر باعدادكبيرة (Highley,1999).

ويمكن تقسيم الفيروسات إلى خمسة انواع :

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس Brain)) و(Newzeland)

الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).

الثالث: الفيروسات المتعددة الانواع كفيروس (Spanish-Telecom) وفيروس (Flip)

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أوالوندوز
الخامس: يعرف بحصان طرواده وهذا النوع يصنفه البعض كنوع مستقل بحدذاته ،الا انه ادرج في تقسيمنا هنا كاحد انواع الفيروسات، وينسب هذا النوع إلىالحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاءسلمي الا أن اثره التدميري خطير. وتعمل الفيروسات على اخفاء نفسها عن البرامجالمضادة للفيروسات باستخدام طرق تشفير لتغيير اشكالها لذلك وجب تحديث برامج الخاصةبمكافحة الفيروسات بصفة دائمة (عيد،1419هـ : 63-66).

وهناك فريق من الخبراء يضع تقسيما مختلفا للفيروسات على أساس المكان

المستهدفبالاصابة داخل جهاز الكمبيوتر ويرون أن هناك ثلاثة أنواع رئيسية من الفيروسات وهيفيروسات قطاع الاقلاع (Boot Sector) وفيروسات الملفات (FileInjectors)وفيروسات الماكرو (Macro Virus). كما أن هناك من يقوم بتقسيم الفيروساتإلى فيروسات الاصابة المباشرة (Direct action) وهي التي تقوم بتنفيذمهمتها التخريبية فور تنشيطها أو المقيمة (staying) وهي التي تظل كامنة فيذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفةتندرج تحت هذا التقسيم، وهناك أيضا الفيروسات المتغيرة (Polymorphs) التي تقوم بتغيير شكلهاباستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات (الجزيرة ،2000).

ومن الجرائم المتعلقة بارسال فيروسات حاسوبية قيام شخص امريكي يدعى (RobertMorris)بارسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (1988م) عبر الإنترنت وقد كررالفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفايروس وادى ذلك إلى تعطيل مايقارب من (6200) حاسب إلى مرتبط بالإنترنت، وقدرت الاضرار التي لحقت بتلك الأجهزةبمئات الملايين من الدولارات. ولو قدر لمصمم الفيروس تصميمه ليكون اشد ضررا لكانقد لحقت اضرار أخرى لا يمكن حصرها بتلك الاجهزة، وقد حكم على المذكور بالسجن ثلاثةسنوات بالرغم من دفاع المذكور بانه لم يكن يقصد احداث مثل تلك الاضرار(Morningstar,1998).

كيف يتم اقتحام الجهاز :

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

1. يرسل عن طريق البريد الإلكترونيكملف ملحق حيث يقوم الشخص بإستقبالهوتشغيله وقد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى.

2. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثةانتجة اسرائيل.

3.عند تحميل برنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.

4.طريقة أخرى لتحميله تتلخص في مجرد كتابة كوده على الجهاز نفسه في دقائققليلة.

5.في حالة اتصال الجهازبشبكة داخلية أو شبكة إنترانت.

6.يمكن نقل الملف أيضا بواسطة برنامج (FTP)أو (Telnet) الخاصة بنقل الملفات.

7.كما يمكن الاصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكروزالموجود في برامج معالجة النصوص (Nanoart,2000).

وبصفة عامة فإن برامج القرصنه تعتمد كليا على بروتوكول الـ ((TCP/IP وهناك ادوات (ActiveX) مصممه وجاهزة لخدمةالتعامل بهذا البروتوكول ومن اشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجةالداعمة للتعامل مع هذه الادوات. ويحتاج الامر إلى برنامجين، خادم في جهاز الضحيةوعميل في جهاز المتسلل حيث يقوم الخادم بفتح منفذ في الجهاز الضحية ويكون هذا المنفذمعروف من قبل العميل اصلا في حين يكون برنامج الخادم في حالة انتظار لحظة محاولةدخول المخترق لجهاز الضحية حيث يتعرف برنامج الخادم (server) على اشارات البرنامجالمخترق ويتم الاتصال ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق حيثيتمكن من العبث بها أو الاستيلاء على ما يريد منها .

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز وهناك وهناك مايقارب الـ(65000) منفذ تقريبا في كل جهاز يميز كل منفذ عن الآخر برقم خاص ولكلمنها غرض محدد، فمثلا المنفذ (8080) يخصص احيانا لمزود الخدمة، وهذه المنافذ غيرمادية مثل منفذ الطابعة، وتعتبر جزء من الذاكرةلها عنوان معين يتعرف عليها الجهازبأنهامنطقة إرسال واستقبال البيانات، وكل ما يقوم به المتسلل هو فتح احد هذهالمنافذ للوصول لجهاز الضحية وهوما يسمى بطريقة الزبون/الخادم (Client\Server)) حيث يتم ارسال ملفلجهاز الضحية يفتح المنافذ فيصبح جهاز الضحية (server) وجهاز المتسلل (Client) ومن ثم يقوم المتسللبالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج ((NetBus أو NetSphere)) ولعل الخطورة الاضافيةتكمن في انه عند دخول المتسلل إلى جهاز الضحية فانه لن يكون الشخص الوحيد الذييستطيع الدخول لذلك الجهاز حيث يصبح ذلك الجهاز مركزا عاما يمكن لأي شخص الدخولعليه بمجرد عمل مسح للمنافذ (Portscanning) عن طريق احد البرامجالمتخصصة في ذلك.

خطورة برامج حصان طروادة:

بداية تصميم هذه البرامج كانلأهداف نبيلة كمعرفة ما يقوم به الأبناء أو الموظفونعلى جهاز الحاسب في غياب الوالدين أو المدراء وذلك من خلال ما يكتبونه على لوحةالمفاتيح، الا انه سرعان ما اسيئ استخدامه. وتعد هذه البرامج من أخطرالبرامجالمستخدمه من قبل المتسللين كونه يتيحللدخيل الحصول على كلمات المرور (passwords) وبالتالي الهيمنهعلىالحاسب الآلي بالكامل. كما أن المتسلل لن يتممعرفته أو ملاحظته كونه يستخدمالطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة ايضا في

أنمعظم برامجحصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات إضافة إلى أن الطبيعةالساكنة لحصان طروادة يجعلها اخطر من الفيروسات فهي لا تقوم بتقديمنفسها للضحيةمثلما يـقـوم الفيروس الذي دائما ما يمكن ملاحظته من خلالالإزعاج أو الأضرار التييقوم بها للمستخدم وبالتالي فإنه لا يمكن الشعور بهذه الاحصنة أثناء أدائهالمهمتها التجسسية وبالتالي فإن فرص إكتشافها والقبض عليها تكادتكون معدومه (Nanoart,2000).

أهم المنافذ المستخدمة لاختراق الجهاز:

إذن فأهم مورد لهذه الاحصنة هي المنافذ (Ports) التي تقوم بفتحها فيجهاز الضحية ومن ثم التسلل منها إلى الجهاز والعبث بمحتوياته. فما هي هذه المنافذ؟

سنحاول هنا التطرق بشكل اجمالي إلى أهم المنافذ التي يمكن استخدامها من قبلالمتسللين والبرامج المستخدمة في النفاذ من هذه المنافذ :

راجع هذا الموقع(http://www.nanoart.f2s.com/hack/ports3.htm)

ثالثا: الجرائم المالية

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمةالمنظمة، المخدرات، غسيل الاموال، ولعل جرائم هذا القسم أوضح من ناحية معرفة كونهامُجَّرَمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمىوالتي يعرف الجميع انها مخالفة للنظام وللشرع كونهم من الجرائم التي اشتهرمحاربتها جنائيا. ونظرا للاختلاف البسيط في تصنيف كل جريمة من جرائم هذا القسمفسيتم توضيح التكييف الشرعي والقانوني لكل جريمة بشكل مفصل.

1.جرائم السطو على أرقام البطاقات الائتمانية:

بدأ مفهموم التجارة الإلكترونية ينتشر في السبعينات الميلادية وذلك لسهولة الاتصالبين الطرفين ولامكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في ارسالالبيانات

وتخفيض تكلفة التشغيل والأهم هو ايجاد اسواق اكثر اتساعا. ونتيجة لذلكفقد تحول العديد من شركات الاعمال إلى استخدام الإنترنت والاستفادة من مزاياالتجارة الإلكترونية، كما نحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقةليصبح خطرا متوافقا مع التجارة الإلكترونية.

فالاستيلاء على بطاقات الائتمان عبر الإنترنت امر ليس بالصعوبة بمكان اطلاقا،فـ" لصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الالوف من ارقامالبطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات للاخرين" (داود، 1420هـ: 73)، وقد وقعت بالفعل عدة حوادث ومن ذلك حادثة شخص المانيقام بالدخول غير المشروع إلى احد مزود الخدمات واستولى على ارقام بطاقات ائتمانيةالخاصة بالمشتركين ومن ثم هدد مزود الخدمة بافشاء ارقام تلك البطاقات ما لم يستلمفدية وقد تمكنت الشرطة الالمانية من القبض عليه. كما قام شخصان في عام (1994م)بانشاء موقع على الإنترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها الكترونيا،ولم تكن الطلبات لتصل اطلاقا حيث كان الموقع وهمي قصد منه النصب والاحتيال وقد قبضعلى مؤسسيه لاحقا (موثق في عبدالمطلب، 2001م : 85)

واثبت شبكة (MSNBC) عمليا سهولة الحصول على ارقام بطاقاتالائتمان من الإنترنت، حيث قامت بعرض قوائم تحتوي على اكثر من (2500) رقم بطاقةائتمان حصلت عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بياناتمتوفرة تجاريا، ولم يكن يصعب على اي متطفل استخدام ذات الوسيلة البدائية للاستيلاءعلى ارقام تلك البطاقات واستخدامها في عمليات شراء يدفع قيمتها اصحابها الحقيقين.ويقترح بعض الخبراء باستخدام بطاقة ائتمان خاصة بالإنترنت يكون حدها الائتمانيمعقول بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الامر الذيبدأت بعض البنوك الدولية والمحلية في تطبيقه اخيرا (عبدالمطلب،2001م : 86 – 90).

ويتعدى الامر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في بداية ثورةنقدية تعرف باسم النقود الإلكترونية (Electronic Cach) أو (CyberCash)والتي يتنبأ لها ان تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان)وأن يزداد الاعتماد عليها والثقة بها، كما ان هناك الاسهم والسندات الإلكترونيةالمعمول بها في دول الاتحاد الأوروبي والتي اقر الكونجرس الامريكي التعامل بها فيعام 1990م، وبالتالي فان التعامل معها من خلال الإنترنت سيواجه مخاطر امنية ولاشك.

ولذلك لجأت بعض الشركات والبنوك إلى العمل سويا لتجأوز هذه المخاطر كالاتفاق الذيوقع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC) وهي من اكبر المؤسساتالمصرفية في هونج كونج وشركة كومباك للحاسب الآلي وذلك لتطوير أول نظام الي آمنللتجارة الالتكرونية والذي يمنح التجار خدمة نظام دفع امن لتمرير عمليات الشراءعبر الإنترنت (داود، 1420هـ : 123 – 124).

وجرائم السطو على أرقام البطاقات الائتمانية مُجَّرمة شرعا وقانونا حيث تصنف ضمنجرائم السرقات، "فالشارع الاسلامي يرغب في المحافظة على اموال الناس وصيانتهامن كل اعتداء غير مشروع بحيث يهدد الامن والاستقرار" (فرحات،1404هـ:29).

والسرقة من الكبائر المحرمة التي نصت الايات القرآنية والاحاديث النبوية علىتحريمها ووضعت عقوبة رادعة لمرتكبها. قال تعالى في سورة المائدة (َالسَّارِقُوَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِنْاللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ (38))

بل لعن رسول الله السارق نظراً لشناعة فعله وعظيم جرمه، ففي الحديث الذي رواهالبخاري في صحيحه عن أبي هريرة رضي الله عنه عن النبي صلى الله عليه وسلم قال:" لعن الله السارق، يسرق البيضة فتقطع يده، ويسرق الحبل فتقطع يده".

كما نفى الحبيب المصطفى عليه الصلاة والسلام صفة الايمان عن السارق فروى البخاريفي صحيحه عن ابن عباس رضي الله عنهما، عن النبي صلى الله عليه وسلم قال: " لايزني الزاني حين يزني وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن".

2.القمار عبر الإنترنت:

كثيرا ما تتداخل عملية غسيل الاموال مع اندية القمار المنتشرة، الامر الذي جعلمواقع الكازيهونات الافتراضية على الإنترنت محل اشتباه ومراقبة من قبل السلطاتالأمريكية. وبالرغم من ان سوق القمار في امريكا يعتبر الاسرع نموا على الاطلاق الان المشكلة القانونية التي تواجه اصحاب مواقع القمار الافتراضية على الإنترنت انهاغير مصرح لها حتى الان في امريكا بعكس نوادي القمار الحقيقية كالمنتشرة في لاسفيجاس وغيرها، ولذلك يلجأ بعض اصحاب تلك المواقع الافتراضية على الإنترنت إلىانشائها وادارتها من اماكن مجاورة لامريكا وخاصة في جزيرة انتيجوا على الكاريبي.

ويوجد على الإنترنت اكثر من الف موقع للقمار يسمح لمرتاديه من مستخدمى الإنترنتممارسة جميع انواع القمار التي توفرها المواقع الحقيقية، ومن المتوقع ان ينفقالامريكيون ما يزيد عن (600) مليار دولار سنويا في اندية القمار وسيكون نصيبمواقع الإنترنت منها حوالي مليار دولار.

وقد حاول المشرعون الامريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت ويسمحبملاحقة اللذين يستخدمون المقامرة السلكية أو اللذين يروجون لها سواء كانت

هذهالمواقع في امريكا أو خارجها (عبدالمطلب، 2001م : 78 – 82).

فإذا كان هذا هو حال القمار ونظرة القوانيين الوضعية له، فما هو نظرة الشرع له وهليوجد في تعاليم الدين الاسلامي ما يُجِّرم لعب القمار ويجعله من الافعال المحرمةشرعا والمعاقب عليه قانونا؟

ينظر الاسلام إلى القمار كمحظور شرعي منهي عن فعله وماعقب على ارتكابه، وقد وردتادلة متعددة في كتاب الله وفي كتب الاحاديث، اما دليل تحريم القمار من القرآن فهوقوله تعالى في سورة المائدة (يَاأَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُوَالْمَيْسِرُ وَالْأَنصَابُ وَالْأَزْلَامُ رِجْسٌ مِنْ عَمَلِ الشَّيْطَانِفَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ (90))

ولم يكتفي الشرع بالنهي عن هذا الفعل بل وضح لاتباعه ان هذا العمل انما هو مناعمال الشيطان التي يسعى من خلالها إلى ايقاع العدأوة والبغضاء بين الناس ووضح انفي اجتاب هذا الفعل فلاح وصلاح وفوز في الدنيا والاخرة ، قال تعالى في سورةالمائدة: (إِنَّمَا يُرِيدُ الشَّيْطَانُ أَنْ يُوقِعَ بَيْنَكُمْ الْعَدَاوةَوَالْبَغْضَاءَ فِي الْخَمْرِ وَالْمَيْسِرِ وَيَصُدَّكُمْ عَنْ ذِكْرِ اللَّهِوَعَنْ الصَّلَاةِ فَهَلْ أَنْتُمْ مُنتَهُونَ (91))

واتفق المفسرون على ان الميسر هو القمار فورد توضيح كلمة الميسر في تفسير الجلالينبانها القمار، اما ابن كثير فقد أورد في تفسيره لهذه الاية، حديثاً رواه احمد فيمسنده عن ابي هريرة رضي الله عنه ان امير المؤمنين عمر بن الخطاب رضي الله عنهفسَّر الميسر هنا بالقمار، كما ورد تفسير كلمة الميسر ايضا في فتح القدير بانهاقمار العرب بالازلام، وكذلك اكد تفسير البغوي بان المراد بالميسر هو القمار، اماالبيضأوي فقد وضح ان الميسر سمي به القمار لانه اخذ مال الغير بيسر.

وفي كتب الحديث ورد ذكر القمار ايضا فقد ورد في مصنف ابن أبي شيبة عن وكيع قالحدثنا حماد بن نجيح قال: رأيت ابن سيرين مر على غلمان يوم العيد المربد و هميتقامرون بالجوز، فقال: يا غلمان! لا تقامروا فإن القمار من الميسر، كما أورد فيمصنفه ايضا عن ابن سيرين قال: كل شيء فيه قمار فهو من الميسر، وفيه ايضاً عن عبدالله بن عمرو قال: من لعب بالنرد قماراً كان كآكل لحم الخنزير، ومن لعب بها من غيرقمار كان كالمدهن بودك الخنزير. كما أخبر عبد الرزاق في مصنفه عن معمر عن ليث عنمجاهد قال: الميسر القمار كله، حتى الجوز الذي يلعب به الصبيان.

3.تزوير البيانات:

تعتبر من اكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظمالمعلومات من شكل من اشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى

قاعدةالبيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادةغير المشروعة من ذلك. وقد وقعت حادثة في ولاية كاليفورنيا الأمريكية حيث عمدتمدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السياراتالمسجلة في الحاسب الآلي بحث تصبح باسم احد لصوص السيارات والذي يعمد إلى سرقةالسيارة وبيعها وعندما يتقدم مالك السيارة للابلاغ يتضح عدم وجود سجلات للسيارة باسمهوبعد بيع السيارة تقوم تلك الفتاة باعادة تسجيل السيارة باسم مالكها وكانت تتقاضيمقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى ان قبض عليها، وفي حادثةالخرى قام مشرف تشغيل الحاسب باحد البنوك الأمريكية بعملية تزوير حسابات اصدقائهفي البنك بحيث تزيد ارصدتهم ومن ثم يتم سحب تلك المبالغ من قبل اصدقائه وقد نجح فيذلك وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك الا ان طمع اصدقاءهاجبره على الاستمرار إلى ان قبض عليه (داود، 1420هـ :45- 47).
ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرصارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهلالدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمةاهدافهم الإجرامية. وجرائم التزوير ليست بالجرائم الحديثة، ولذا فانه لاتخلوا الأنظمةمن قوانيين واضحة لمكافحتها والتعامل معها جنائيا وقضائيا و" تكفي التشريعاتالحالية لتجريمها وتحديد العقوبة عليها" (داود ، 1421هـ : 67).

وعالجت أنظمة المملكة العربية السعودية جرائم التزوير بشكل مفصل حيث صدر المرسومالملكي رقم (114) وتاريخ 1380/11/26هـ بالمصادقة على نظام مكافحة التزوير، ومن ثمتم التعديل على هذا النظام ليواكب المستجدات وذلك بالمرسوم الملكي رقم (53) وتاريخ1382/11/5هـ،كما صدر نظام جزائي خاص بتزوير وتقليد النقود وذلك بالمرسوم الملكيرقم (12) وتاريخ1379/7/20هـ(موقع السوق الخليجي، 1423هـ).

4.الجرائم المنظمة*:
يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصاباتمن اشهر المؤسسات الإجرامية المنظمة والتي بادرت بالاخذ بوسائل التقنية الحديثةسواء في تنظيم أو تنفيذ اعمالها، ومن ذلك انشاء مواقع خاصة بها على شبكة الإنترنتلمساعدتها في ادارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع اعمال وغسيلالاموال، كما تستخدم تلك المواقع في انشاء مواقع افتراضية تساعد المنظمة في تجاوزقوانين بلد محدد بحيث تعمل في بلد اخر يسمح بتلك الانشطة.
ويوجد على الشبكة (210) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (24)موقعا يحتوى على كلمة مافيا، كما وجد (4) مواقع للمافيا اليهودية. وقد خصص بعضهذه المواقع للاعضاء فقط ولم يسمح لغيرهم بتصفح تلك المواقع في حين سمحت بعضالمواقع للعامة بتصفح الموقع وقامت مواقع أخرى بوضع استمارة تسجيل لمن يرغب

فيالانضمام إلى العصابة من الاعضاء الجدد (الجنيدي(أ)، 1999م : 36).
والجريمة المنظمة ليست وليدة التقدم التقني وإن كانت استفادت كثيرا منه فـ"الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنلوجيا والعولمة أصبحت غير محددةلا بقيود الزمان ولا بقيود المكان وأن ما أصبح إنتشارها على نطاق واسع وكبيروأصبحت لاتحدها الحدود الجغرافية"(اليوسف، 1420هـ ، ص : 201)، كما أستغلتعصابات الجريمة المنظمة " الامكانيات المتاحة في وسائل الإنترنت في تخطيطوتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة" (حبوش،1420هـ: 253).

وهناك من يرى ان الجريمة المنظمة والارهاب هما وجهان لعملة واحدة، فأوجه التشابهبينهما كبير حيث يسعى كلاهما إلى إفشاء الرعب والخوف، كما انهما يتفقان في اسلوبالعمل والتنظيم وقد يكون اعضاء المنظمات الارهابية هم اساساً من محترفي الجرائمالمنظمة حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صلةوتعاون وثيق بينهما (عزالدين، 1414هـ : 23- 35).

وحظيت مكافحة الجريمة المنظمة باهتمام دولي بدأ بمؤتمر الامم المتحدة السابع عام(1985م) لمنع الجريمة حيث اعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيالالتعامل مع الجريمة المنظمة والقضاء عليها.

وتبع ذلك الاجتماع الاقاليمي التحضيري عام (1988م) الذي أقر فيه المبادئ التوجيهيةلمنع الجريمة المنظمة ومكافحتها، ثم المؤتمر الثامن لمنع الجريمة بفنزويلا عام(1990م)، فالمؤتمر الوزاري العالمي المعنى بالجريمة المنظمة عبر الوطنية في نابوليبايطاليا عام (1994م) والذي عبّر عن ارادة المجتمع الدولي بتعزيز التعاون الدوليواعطاء أولوية عليا لمكافحة الجريمة المنظمة.

كما وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الارهابوالتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة، وفي عام (1996م)وافق المجلس في دورته الثالثة عشر على مدونة سلوك طوعية لمكافحة الارهاب، ووافق فيعام (1997م) وفي الدورة الرابعة عشر على استراتيجية عربية لمكافحة الارهاب وفي عام(1998م) تم اقرار الاتفاقية العربية لمكافحة الارهاب من قبل مجلس وزراء الداخليةوالعدل العرب (عيد، 1419هـ :77-194).

5. تجارة المخدرات عبر الإنترنت:
كثيرا ما يحذّر أولياء الامور ابنائهم من رفقاء السوء خشية من تأثيرهم السلبيعليهم وخاصة في تعريفهم على المخدرات فالصاحب ساحب كما يقول المثل وهذا صحيح ولاغبار عليه ولكن وفي عصر الإنترنت اضيف إلى أولياء الامور مخأوف جديدة لا تقتصر علىرفقاء السوء فقط بل يمكن ان يضاف اليها مواقع السوء - ان صح التعبير- ومن تلكالمواقع طبعا

المواقع المنتشرة في الإنترنت والتي لاتتعلق بالترويج للمخدراتوتشويق النشئ لاستخدانها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافةاصنافها وأن واعها وبأبسط الوسائل المتاحة.
والامر هنا لايحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلىاي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخأوف أحد الخبراء التربوينفي بتسبيرج بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثالوثالمراهقة والمخدرات وانترنت.
ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تسأهم المنتديات وغرف الدردشة فيذلك ايضا. وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعهاالا ان هذه المواقع لم تدق جرس الانذار بعد ولم يهتم باثارها السلبية وخاصة علىالنشئ كما فعلته المواقع الاباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة.

وقد اعترف الناطق الرسمي للتحالف المناهض للمخدرات بانهم خسروا الجولة الأولي فيساحة الإنترنت حيث لم يطلق موقعهم الخاص على الشبكة http://www.cadca.org الا منذ عامين فقط.

وبالإضافة إلى هذا الموقع توجد مواقع أخرى تحارب المخدرات وتساعد المدمنين علىتجاوز محنتهم ومن ذلك الموقع الخاص بجماعة (Join-Together) وعنوانهم على النت هو http://192.12.191.21 إلا أن هذه المواقعقليلة العدد والفائدة مقارنة بكثرة وقوة المواقع المضادة (الجنيدي(ب)، 1999م :39-40).
واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات وعقدت المؤتمرات والاتفاقياتالدولية المختلفة ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (1961م)، اتفاقيةالمؤثرات العقلية عام (1971م)، واتفاقية الامم المتحدة لمكافحة الاتجار غيرالمشروع في المخدرات والمؤثرات العقلية عام (1988م).
وعلى المستوى العربي تم عام (1996م) اقرار الاتفاقية العربية لمكافحة الاتجار غيرالمشروع في المخدرات والمؤثرات العقلية، كما تم عام (1986م) اقرار القانون العربيالنموذجي الموحد للمخدرات.

اما على المستوى المحلي فقد صدر نظام مكافحة الاتجار بالمواد المخدرة في المملكةالعربية السعودية بقرار مجلس الوزراء رقم (11) عام (1374هـ) والحق به قرار هيئةكبار العلماء رقم (138) وتاريخ 1407/6/20هـ الخاص باعدام مهربي المخدرات أو منيقبض عليه في قضية ترويج للمرة الثانية، والموافق عليه بالامر السامي رقم(4/ب/966) وتاريخ 1407/7/10هـ (عيد، 1422هـ :94-110)

6. غسيل الاموال :

مصطلح حديث نسبيا ولم يكن معروفا لرجال الشرطة فضلا عن العامة وقد بدأ استخدامالمصطلح في امريكا نسبة إلى مؤسسات الغسيل التي تملكها المافيا، وكان أول استعمالقانوني لها في عام (1931م) إثر محاكمة لاحد زعماء المافيا تمت في امريكا واشتملتمصادرة اموال قيل انها متأتية من الاتجار غير المشروع بالمخدرات.

واختلف الكثير في تعريف غسيل الاموال وقد يكون التعريف الاشمل هو " أي عمليةمن شأنها اخفاء المصدر غير المشروع الذي اكتسبت منه الاموال"(عيد، 1422هـ:124). ومن البديهي ان ياخذ المجرمون باحدث ما توصلت اليه التقنية لخدمة أنشطتهمالإجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التي استفادت من عصر التقنية فلجأتإلى الإنترنت لتوسعة وتسريع اعمالها في غسيل اموالها غير المشروعة، ويجد المتصفحللانترنت مواقع متعددة تتحدث عن غسيل اموال ومنها الموقع http://www.laundryman.u.net.com: كما يجد ولا شك ايضاالمواقع التي تستخدم كساتر لعمليات غسيل الاموال ومنها المواقع الافتراضية لنواديالقمار والتي قام مكتب المباحث الفدرالية(FBI) الامريكي بمراقبة بعضهذه المواقع واتضح انها تتواجد في كاراكاو، جزر الانتيل، جزيرة أنتيجوا وجمهوريةالدومينكان وقد اسفرت التحريات التي استمرت خمسة اشهر عن اعتقالات واتهامات للعديدمن مدراء تلك المواقع.

ومن المميزات التي يعطيها الإنترنت لعملية غسيل الاموال السرعة، اغفال التوقيع وأنعدام الحواجز الحدودية بين الدول، كما تسأهم البطاقات الذكية، والتي تشبه في عملهابطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الاموال بواسطة المودمأو الإنترنت مع ضمان تشفير وتأمين العملية.

كل هذا جعل عمليات غسيل الاموال عبر الإنترنت تتم بسرعة اكبر وبدون ترك اي اثار فيالغالب. ويقدر المتخصصون المبالغ التي يتم تنظيفها سنويا بحوالي (400) ملياردولار (عبدالمطلب،2001م : 68 - 72).
وإلى عهد قريب لم تكن جرائم غسيل اموال تشكل جرما بذاتها إلى ان تضخمت الاموالالمتحصلة من الجرائم وخاصة من تجارة المخدرات فاصدرت بعض الدول قوانين خاصة تسمحبتعقب وتجميد ومصادرة عائدات الجرائم الخطرة، فأصدرت الولايات المتحد الأمريكيةعام (1970م) قانون المنظمات القائمة على الابتزاز والنساء، وقانون منع ومكافحةجرائم اساءة إستخدام العقاقير المخدرة، كما اصدرت مصر عام (1971م) القانون رقم(34) والخاص بتنظيم فرض الحراسة على الاموال المكتسبة بطرق غير مشروعة، كما اقرالقانون العربي النموذجي الموحد للمخدرات الصادر عن مجلس وزراء الداخلية العرب عام(1986م) مكافحة جرائم غسيل الاموال وخاصة في مادته التاسعة والاربعون والتي سمحتللمحكمة المختصة بحجز الاموال المتحصلة من تجارة المخدرات والتحقق من مصادر تلكالاموال. كما اصدرت بريطانيا وايرلندا عام (1986م) قانون يسمح بمصادرة عائداتالجريمة. واصدرت استراليا عام (1987م) قانونا يسمح بمصادرة اموال الشخص المدان فيجرائم اتحادية.

ولم تتخلف المملكة العربية السعودية عن ركب محاربة جرائم غسيل الاموال فقد كانتالمملكة من ضمن دول العالم الـ(106) اللذين وقعوا عام (1988م) على اتفاقية الاممالمتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية والتي كانتأول خطوة دولية مهمة لتعريف غسيل الاموال وتحديد الافعال الواجب تجريمها (عيد،1419هـ : 263-319)

رابعا: المواقع المعادية:

يكثر انتشار الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت ومن هذهالمواقع ما يكون موجها ضد سياسة دولة ما، أو ضد عقيدة أو مذهب معين أو حتى ضد شخصما. وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد أو الشخصالمستهدف.

ففي المواقع السياسية المعادية يتم غالبا تلفيق الاخبار والمعلومات ولو زوراوبهتانا أو حتى الاستناد إلى جزيئ بسيط جدا من الحقيقة ومن ثم نسج الاخبار الملفقةحولها، وغالبا ما يعمد اصحاب تلك المواقع إلى انشاء قاعدة بيانات بعناوين اشخاصيحصلون عليها من الشركات التي تبيع قواعد البيانات تلك أو بطرق أخرى ومن ثم يضيفونتلك العناوين قسرا إلى قائمتهم البريدية ويبدأو في اغراق تلك العناوين بمنشوراتهم،وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولايصالاصواتهم إلى اكبر قدر ممكن.

اما المواقع المعادية للعقيدة فمنها ما يكون موجهاً من قبل اعداء حاقدين من اتباعالديانات الأخرى كالمواقع التي تنشئها الجاليات اليهودية أو النصرانية تحت مسمياتاسلامية بقصد بث معلومات خاطئة عن الاسلام والقرآن، أو بهدف الدعاية للاديانالأخرى ونشر الشبهه والافتراءت حول الاسلام ومن أمثلة هذه المواقع:

موقع http://www.answering-islam.org/

وموقع http://www.aboutislam.com/

وموقع http://www.thequran.com/

اما القسم الثاني من المواقع المعادية للعقيدة فهي المواقع التي يكون افرادها منذات العقيدة واحدة ولكن يختلفون في المذاهب.

وهناك مواقع معادية لاشخاص أو جهات وهي قد تكون شبيهة وإلى حد كبير

بالمواقعالمخصصة للقذف التي سبق التحدث عنها سابقا في القسم الخاص بالجرائم الجنسية، حيثتهدف اساسا لتشويه سمعة الشخص أو الجهة ولذلك فسيكتفى بما سبق التطرق اليه في هذاالمجال وسيركز على الحديث عن المواقع السياسية والدينية والتي لم يتم التطرق لها.

والمواقع المعادية بانواعها مخالفة نظامية وجريمة جنائية وتفصيل ذلك كالاتي:

أ.المواقع السياسية المعادية: قد ينظر البعض إلى إنشاء هذه المواقع كظاهرة حضاريةتتمشي مع الديموقراطية والحرية الشخصية، وهذا غير صحيح فللديموقراطية والحريةالشخصية حدود يجب ان لاتتجاوزها والا اصبحت سوء ادب وبغي. وهناك ولا شك طرقواساليب يمكن معها التعبير عن الاراء الشخصية وضّحتها الشريعة الاسلامية قبلالديمقراطية الوضعية، وحددتها عاداتاتنا وتقاليدنا المنبثقة من قيمنا العربيةالاصيلة في حين غفلت عنها قيم الدول الغربية وابسط هذه القواعد ان يكون النصحبالرفق واللين وبالكلمة الطيبة وليس بالشتم والقذف، قال تعالى في سورة النحل (ادْعُ إِلى سَبِيلِ رَبِّكَ بِالْحِكْمَةِ وَالْمَوْعِظَةِ الْحَسَنَةِوَجَادِلْهُمْ بِالَّتِي هِيَ أَحْسَنُ إِنَّ رَبَّكَ هُوَ أَعْلَمُ بِمَنْ ضَلَّعَنْ سَبِيلِهِ وَهُوَ أَعْلَمُ بِالْمُهْتَدِينَ (125)) وقال تعالى في سورة العمران (فَبِمَا رَحْمَةٍ مِنْ اللَّهِ لِنْتَ لَهُمْ وَلَوْ كُنْتَ فَظًّاغَلِيظَ الْقَلْبِ لَانْفَضُّوا مِنْ حَوْلِكَ فَاعْفُ عَنْهُمْ وَاسْتَغْفِرْلَهُمْ وَشَأَورْهُمْ فِي الْأَمْرِ فَإِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى اللَّهِإِنَّ اللَّهَ يُحِبُّ الْمُتَوَكِّلِينَ (159))، كما ان من الآداب ان يكون النقدأو النصيحة في السر لا في العلن وفي هذا يقول الامام الشافعي: تعمدني بنصحك فيانفراد وجنبني النصيحة في الجماعة

فإن النصح بين الناس نوع من التوبيخ لاارضى استماعه

وان خالفتني وعصيت قولي فلا تجزع إذا لم تعط طاعة

وهذه الاداب هي ابسط الاداب الواجب اتباعها مع العامة فما بالك مع ولي الامر الذيقرن الله طاعته بطاعة الله ورسوله - مالم يأمر ولي الامر بأمر مخالف لله – ولذلكفليس في إنشاء المواقع السياسية المعادية أي حرية رأي أو ديمقراطية بل هي سوء ادبان لم يكن بغي يعاقب عليه الشرع بالقتل فـ" جريمة البغي موجهة إلى نظام الحكموالقائمين بأمره، وقد تشددت فيها الشريعة؛ لإن التساهل فيها يؤدي إلى الفتنوالاضطرابات وعدم الاستقرار وهذا يؤدي بدوره إلى تأخر الجماعة وانحلالها. ولا شكان عقوبة القتل أقدر العقوبات على صرف الناس عن هذه الجريمة التي يدفع اليها الطمعوحب الاستيلاء" (عودة، 1401هـ :663).

والدليل على ان البغي محرم شرعا ومعاقب عليه بالقتل قوله تعالى في سورة الحجرات

(وَإِنْ طَائِفَتَانِ مِنْ الْمُؤْمِنِينَ اقْتَتَلُوا فَأَصْلِحُوا بَيْنَهُمَافَإِنْ بَغَتْ إِحْدَاهُمَا عَلَى الْأُخرى فَقَاتِلُوا الَّتِي تَبْغِي حَتَّىتَفِيءَ إلى أَمْرِ اللَّهِ فَإِنْ فَاءَتْ فَأَصْلِحُوا بَيْنَهُمَا بِالْعَدْلِوَأَقْسِطُوا إِنَّ اللَّهَ يُحِبُّ الْمُقْسِطِينَ(9))، وفي الحديث الشريف الذيرواه مسلم "إنه ستكون هنّات وهنّات، فمن أراد أن يفرق أمر هذه الأمة، وهيجميع، فاضربوه بالسيف، كائناً من كان" كما ورد عن رسول الله صلى الله عليهوسلم حديثا رواه مسلم وابي داود واللفظ لابي دواد: عن عبد الله بن عمرو أن النبيصلى الله عليه و سلم قال"من بايع إماماً فأعطاه صفقة يده وثمرة قلبه فليطعمهما استطاع، فإن جاء آخر ينازعه فاضربوا رقبة الآخر قلت: أنت سمعت هذا من رسول اللهصلى الله عليه وسلم؟ قال: سمعته أذناي ووعاه قلبي، قلت: هذا ابن عمك معأوية يأمرناأن نفعل ونفعل، قال: أطعه في طاعة الله واعصه في معصية الله"

وقد كانت القوانيين الوضعية وإلى عهد قريب تعتبر الجريمة السياسية أشد خطرا منالجريمة العادية، بل كانت تعامل المجرم السياسي معاملة تتنافى مع ابسط قواعدالعدالة حيث تشدد عليه العقوبة وتصادر امواله وتعاقب اهله بجريمته (عودة، 1401هـ :107).

ب.المواقع الدينية المعادية: الدين الاسلامي هو خاتم الاديان السماوية وبه أكمل رسولهصلى الله عليه وسلم تعاليم الدين قال تعالى في سورة المائدة (الْيَوْمَأَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتْمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمُالْإِسْلَامَ دِينًا فَمَنْ اضْطُرَّ فِي مَخْمَصَةٍ غَيْرَ مُتَجَانِفٍ لِإِثْمٍفَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ(3))، ولذلك فلا يقبل أي دين غير الاسلام قالتعالى في سورة ال عمران (وَمَنْ يَبْتَغِ غَيْرَ الْإِسْلَامِ دِينًا فَلَنْيُقْبَلَ مِنْهُ وَهُوَ فِي الْآخِرَةِ مِنْ الْخَاسِرِينَ(85))، ليس ذلك فحسب بلعاقب من بدل دينه بعد اسلامه ففي الحديث الذي رواه البخاري قال النبي صلى اللهعليه وسلم: "من بدل دينه فاقتلوه"

ج.المواقع المعادية للاشخاص أو الجهات: لعل التشابه الكبير بين هذه المواقعوالمواقع المخصصة للقذف والتي سبق الحديث عنها في الجرائم الجنسية، ما يغنى عنالتكرار فما ينطبق على تلك المواقع من تجريم قانوني وشرعي ينطبق على هذه المواقعايضاً.

خامساً: جرائم القرصنة:

يقصد بجرائم القرصنة هنا الاستخدام أو/و النسخ غير المشروع لنظم التشغيلأو/ولبرامج الحاسب الآلي المختلفة.

وقدتطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنةواتسعت واصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامجالمقرصنة مجانا أو بمقابل مادي رمزي.

وادت قرصنة البرامج إلى خسائر مادية باهضة جدا وصلت في العام (1988م) إلى

(11)مليار دولار امريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعةالبرامج إلى الاتحاد وأن شاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلكمنظمة اتحاد برمجيات الاعمال(Busines Software Alliance) أو ما تعرف اختصاراب(BSA)، والتي اجرت دراسة تبين منها ان القرصنة على الإنترنت ستطغى علىانواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرحالحلول المختلفة لتفادي القرصنة على الإنترنت ومنها تهديد بعض الشركات بفحص القرصالصلب لمتصفحي مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامجمقرصنة الا ان تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حمايةالخصوصية لمستخدمي الإنترنت.

كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لابلاغهم عن اي مواقع مخصصةللبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكوي ضدهم ومقاضاتهم ان امكن أو اقفالتلك المواقع على اقل تقدير.

والقرصنة عربيا لا تختلف كثيرا عن القرصنة عالميا ان لم تسبقها بخطوات خاصة في ظلعدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين ان وجدت (الجنيدي، نوفمبر 1999م : 28-35).

وقوانيين حماية الملكية تعتبر من الأنظمة الحديثة في الدول العربية حيث بدأتالفكرة من الدول الرأسمالية ومن ثم بدأت الدول الأخرى تطبيقها وادراجها فيانظمتها، وقد اهتمت دول الخليج بحماية الملكية الفكرية ايضا فقامت امانة مجلسالتعاون الخليجي وفي الاجتماع الثاني للوزراء المسئولين عن الثقافة المنعقدبالرياض في 1987/9/15م بوضع لائحة استرشادية للنظام الموحد لحماية حقوق المؤلف فيدول المجلس (موقع مجلس التعاون لدول الخليج العربية، 1423هـ).

ولم يكن هذا هو اخر المشوار بل البداية حيث توالت دول الخليج في اصدار قوانيينالحماية الفكرية، ففي سلطنة عمان مثلاً صدر قانون الملكية الفكرية بالمرسومالسلطاني رقم (97/65) وتاريخ 1418/5/3هـ وفي الكويت صدر القانون رقم (64) لعام(1999م) بشأن حقوق الملكية الفكرية.

امّا المملكة العربية السعودية فكانت سبّاقة إلى اصدار تنظيمات خاصة لمحاربةالقرصنة فصدر قرار مجلس الوزراء رقم (56) و تاريخ 1409/4/14هـ بالموافقة على نظامبراءات الاحتراع، ثم صدر قرار مجلس الوزراء رقم (30) و تاريخ 1410/2/25هـبالموافقة على نظام حماية حقوق المؤلف (موقع محامو المملكة، 1423هـ).

ووافق مجلس الوزراء الموقر في جلسته بتاريخ 1420/6/17هـ على تشكيل اللجنة

الدائمةلحقوق الملكية الفكرية من ممثلين عن وزارات التجارة، الإعلام، الداخلية، الخارجية،العدل، الصناعة والكهرباء، البترول والثروة المعدنية، المالية والاقتصاد الوطني(مصلحة الجمارك)، ديوان المظالم، ومدينة الملك عبدالعزيز للعلوم والتقنية، ويكونمقرها ورئاستها بوزارة التجارة، وحددت مهام اللجنة بمتابعة ودراسة ما يستجد منأمور في مجال حقوق الملكية الفكرية، وإعداد التوصيات اللازمة بما يتناسب معمتطلبات الاتفاقيات الدولية ذات العلاقة، وفي مقدمتها إتفاقية الجوانب المتصلةبالتجارة من حقوق الملكية الفكرية (موقع وزارة التجارة، 1423هـ).

سادساً: جرائم اختراقات أخرى لم تتطرق اليها الدراسة:

لقد ركزت الدراسة على الافعال الجنائية التي ترتكب من قبل مستخدمي الإنترنت فيالمجتمع السعودي والتي حصرها الباحث من خلال الدراسة الاستطلاعية لمزودي خدمةالإنترنت في المملكة، لكن ينبغى لفت النظر إلى أن هناك جرائم أخرى لم يتبين ممارستهامن قبل الافراد في المجتمع السعودي ولذلك لم تدرج ضمن عناصر الدراسة لبحثها، وانكان هذا لايعنى الجزم بعدم وجودها، أو على اقل تقدير عدم امكانية حدوثها فيالمجتمع السعودي، ولذا لم تدرج في الدراسة كون الدراسة تركز على الجرائم الاكثرشيوعا في المجتمع السعودي.

الا انه ونظرا لاهمية هذه الجرائم على المستوى الامني وجب اخذ الاحتياطات اللازمةللتوقي منها واخذها في الحسبان عند وضع الضوابط النظامية للتعامل مع جرائمالإنترنت وللفت نظر الباحثين في هذا المجال، ولذا وجب التطرق اليها هنا بالشرحوالايضاح وهذه الجرائم:

1.التجسس الإلكتروني:*
" في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحةبأقمار التجسس والبث الفضائي" (البداينة، 1988م)، والعالم العربي والاسلاميكان ولا يزال مستهدف امنيا وثقافيا وفكريا وعقديا لاسباب لاتخفى على احد.

وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخداماالإنترنت وانتشاره عربيا وعالميا.

ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة فيحماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولايمكن حتما الاعتماد علىوسائل الحماية التي تنتجها الشركات الاجنبية فهي ليست في مأمن ولا يمكن الاطمئنانلها تماما.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقيالأنظمة

أو ما يعرفون اصطلاحا (hackers) فمخاطر هؤلاء محدودة وتقتصر غالبا علىالعبث أو اتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة فيموقع امن، اما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزةالاستخباراتية للحصول على اسرار ومعلومات الدولة ومن ثم افشائها لدول أخرى تكونعادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية للدولة.

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف اخيرا عن مفتاح وكالة الامنالقومي الأمريكية (NSA) والتي قامت بزاعته في نظام التشغيل الشهيروندوز، وربما يكون هذا هو احد الاسباب الرئيسية التي دعت الحكومة الالمانيةباعلانها في الأونة الاخيرة عن استبدالها لنظام التشغيل وندوز بأنظمة أخرى.

كما كشف اخيرا النقاب عن شبكة دولية ضخمة للتجسس الالتكروني تعمل تحت اشراف وكالةالامن القومية الأمريكية بالتعاون مع اجهزة الاستخبارات والتجسس في كندا،بريطانيا،استراليا ونيوزيلندا ويطلق عليها اسم (ECHELON)لرصد المكالمات الهاتفيةوالرسائل بكافة انواعها سواء ماكان منها برقيا، تلكسيا، فاكسيا أو الكترونيا.

وخصص هذا النظام للتعامل مع الاهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلةجدا من الاتصالات والرسائل الالكترونية عشوائيا باستخدام خاصية الكلمة المفتاحيةبواسطة الحاسبات المتعددة والتي تم انشاء العديد من المحطات السرية حول العالمللمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الاقمار الصناعيةالواقعة في منطقة واي هوباي بجنوب نيوزيلندا، ومحطة جير الدتون الموجودةباستراليا، والمحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول ببريطانيا،والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة شوجرجروف وتبعد (250)كيلومترا جنوب واشنطن دي سي، وايضا المحطة الموجودة بولاية واشنطن على بعد(200)كيلومتر جنوب غرب مدينة سياتل.

ولا يقتصر الرصد على المحطات الموجهة إلى الاقمار الصناعية والشبكات الدوليةالخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة الاتصالاتالارضية وكذا الشبكات الإلكترونية.

أي انه يرصد جميع الاتصالات التي تتم بأي وسيلة. ويعتبر الافراد والمنظماتوالحكومات اللذين لا يستخدمون أنظمة الشفرة التامينية أو أنظمة كودية لحمايةشبكاتهم واجهزتهم، اهدافا سهلة لشبكة التجسس هذه، وأن كان هذا لا يعنى بالضرورة انالاهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتيةلهذه الشبكة ومثيلاتها، ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بلتعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية (عبدالمطلب، 2001م :30-45).

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلوماتإلى اهداف للتجسس التجاري ففي تقرير صدر عن وزارة التجارة والصناعة البريطانيةأشار إلى زيادة نسبة التجسس على الشركات من (36٪) عام (1994م) إلى (45٪) عام(1999م)، كما اظهر استفتاء اجرى عام (1996م) لمسؤلي الامن الصناعي في الشركاتالامريكة حصول الكثير من الدول وبشكل غير مشرع على معلومات سرية لانشطة تجاريةوصناعية في الولايات المتحدة الأمريكية(داود،1420هـ: 62).

ومن الاساليب الحديثة للتجسس الإلكتروني اسلوب إخفاء المعلومات داخل المعلومات وهوأسلوب شائع وإن كان ليس بالامر السهل، ويتلخص هذا الاسلوب في لجوء المجرم إلىإخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومنثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك احد في ان هناكمعلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبسا، كما قد يلجأ إلى وسائلغير تقليدية للحصول على المعلومات السرية (داود، 1420هـ : 67).

وبعد الاعتداءات الاخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدةلأقمارالتجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بنلادنوالجماعات التابعة **له**،وقررت السلطات الأمريكية الاستعانة في عمليات التجسسعلى أفغانستان بقمريناصطناعيين عسكريين مصممان خصيصا لالتقاط الاتصالات التي تجريعبر أجهزة اللاسلكيوالهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطانصورا فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانةبقمرين تابعينلهما لرصد الاتصالاتومن ثم تحول بعد ذلكإلى الولايات المتحدة حيثتدخل في أجهزة كمبيوتر متطورة لتحليلها.
وتشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسس على المكالماتالهاتفيةورسائل الفاكس والبريد الإلكتروني، الأمر الذي يتيح تحليل الإشارات التيتلتقطهاالأقمار الصناعية حتى إن كانت واهنة أو مشفرة (BBC,2001).

2.الارهاب الإلكتروني:
في عصر الازدهار الإلكتروني وفي زمن قيام حكومات الكترونية كما في الاماراتالعربية المتحدة، تبدل نمط الحياة وتغيرت معه اشكال الاشياء وانماطها ومنها ولا شكانماط الجريمة والتي قد يحتفظ بعضها بمسماها التقليدي مع تغيير جوهري أو بسيط فيطرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها جريمة الارهابوالتي اخذت منحنى حديث يتماشى مع التطور التقنى.

وقد انتبه الغرب إلى قضية الارهاب الإلكتروني منذ فترة مبكرة، فقد شكل الرئيسالامريكي بيل كلنتون لجنة خاصة (www.nipc.gov)مهمتها حماية البنية التحتية الحساسة في

امريكا، والتي قامت في خطوة أولى بتحديدالاهداف المحتملة استهدافها من قبل الارهابين ومنها مصادر الطاقة الكهربائيةوالاتصالات إضافة إلى شبكات الحاسب الآلي، ومن ثم تم انشاء مراكز خاصة في كل ولايةللتعامل مع احتمالات أي هجمات ارهابية الكترونية.

كما قامت وكالة الاستخبارات المركزية بانشاء مركز حروب المعلوماتية وظفت به الفامن خبراء امن المعلومات، كما شكلت قوة ضاربة لمواجهة الارهاب على مدار الساعة ولميقتصر هذا الامر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحثالفدرالية والقوات الجوية.

وحذّر تقرير صدر من وزارة الدفاع الأمريكية عام (1997م) من ((بيرل هاربورالكترونية)) وتوقع التقرير ان يزداد الهجوم على نظم المعلومات في الولايات المتحدةالأمريكية من قبل الجماعات الارهابية أو عملاء المخابرات الاجنبية وأن يصل هذاالهجوم إلى ذروته عام (2005م)، وأوضح التقرير ان شبكة الاتصالات ومصادر الطاقةالكهربائية والبنوك وصناعات النقل في امريكا معرضة للهجوم من قبل أي جهة تسعىلمحاربة الولايات المتحدة الأمريكية دون ان تواجه قواتها المسلحة (داود، 1420هـ).

وبعد الهجمات الاخيرة على الولايات المتحدة الأمريكية ارتفعت اصوات البعض بممارسةالارهاب الإلكتروني ضد المواقع الاسلامية والعربية التي يشتبه بانها تدعم الارهاب،وأوردت شبكة (CNET) الاخبارية خبرا عن اتفاق (60) خبيرا في امنالشبكات ببدء تلك الهجمات الارهابية على مواقع فلسطينية وافغانية.

3.جرائم ذوي الياقات البيضاء:
هذا المصطلح من الجرائم حديث نسبياً، وأول من اطلقته عالم الاجتماع سذرلاند (Sutherland) حيث وضّح أن هذهالجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الادارية الكبيرة،وتشمل انواعا مختلفة من الجرائم كالرشوة والتلاعب بالشيكات والاختلاس والسرقةوتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات محلية أو عالمية غيرمشهورة وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها.

وهذا النوع من المشاكل يصعب ارتكابها أو كشفها والتحقيق فيها دون المام جيد بظروفالانتاج والحسابات الجارية والعمل التجاري ومبادي التقنية الحسابية الالتكرونية.وقدرت خسائر المجتمع الامريكي بمبلغ (12– 42) مليون دولار سنويا نتيجة خداعالمستهلكين باستخدام جميع وسائل التكنلوجيا المتقدمة(اليوسف،1420هـ: 209-211).

واستفاد الجناة من انتشار الإنترنت في تطوير جرائمهم وتوسعة الرقعة الجغرافية لهابحيث اصبحت عالمية بعد ان كانت محلية.

4.الجرائم الاقتصادية:
تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال فيالدول الراسمالية نجد ان اغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهربالضريبي والجمركي والسطو على المصارف وتجارة الرقيق الابيض والاطفال، في حينتتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء.
وهذا لا يعنى بالضرورة انه لايمكن ارتكاب كل انواع هذه الجرائم في مجتمع واحد حيثيمكن ان تجد في المجتمع الراسمالي مثلا جرائم رشوة واختلاسات والعكس صحيح.وكما فيالجرائم الأخرى فان الإنترنت ساهم في تطوير طرق واساليب ارتكاب هذه الجرائم ووسّعمنطقة عملها ،خاصة مع توجه الكثير من الدول في التحول إلى الحكومات اللالكترونيةكما في دولة الامارات العربية المتحدة مثلا، حيث استفاد المجرمون من التقدم التقنيفي اختلاس الاموال وتحويل الارصدة النقدية وكذلك في سرقة التيار الكهربائي والمياهوخطوط الهاتف والعبث بها واتلافها (اليوسف،1420هـ : 211-214).

<--[supportLineBreakNewLine! if]--!>
<--[endif]--!>

الخاتمة
وبعد، فهذا جهد المقّل في محاولة لتحديد جرائم الانترنتالمرتكبة أثناء استخدام الشبكة العنكوبيتية،مع تكيفها قانوينا وشرعيا، والتى آملان تساهم هذه الدراسة في مواجهة هذه الجرائم الحديثة والتعامل معها ومكافحتها، وفيطرح افتراضات تصورية تلفت انتباه الباحثين في العلوم الشرطية والعلوم الاجتماعيةوالعلوم الإنسانية، بشكل عام، إلى كثير من الظواهر السلوكية المتعلقة باستخدامالإنترنت، والتي تتطلب البحث والدراسة.

كما اتمنى لفت انتباه المعنيين والمسئولين عن الأجهزة والتنظيمات التربوية،والإعلامية، وخطباء المساجد، والمؤسسات العلمية، للمساهمة في مكافح هذه الانماطالحديثة من الجرائم والحد منها، ولتحذير أولياء الأمور وكافة شرائح المجتمع منالتعامل معها، ولبيان عظيم خطورتها بشكل عام.

واخيراً ارجوا ان اكون قد وفقت في ابراز الصورة الحقيقية لجرائم الانترنت، فإن كانذلك فمن الله وحده وله الفضل والمنة، وان لم اوفق فمن نفسي والشيطان ولكن عذريانني اجتهدت ولكل مجتهد نصيب.

محمد عبدالله منشاوي

باحث في جرائم الانترنت

mohammed@minshawi.com

<--[supportLineBreakNewLine! if]--!>
<--[endif]--!>

المراجع:

اولاً- المراجع العربية:

1.ابن منظور، أبي الفضل جمال الدين محمد بن مكرم.(بدون). لسان العرب .بيروت: دار صادر.

2.أبو الحجاج، أسامة.(1998م). دليلك الشخصي إلى عالم الإنترنت . القاهرة :نهضة مصر.

3.ابوزهرة، محمد.(1976م). الجريمة والعقوبة في الفقة الاسلامي. القاهرة :دار الفكر العربي.

4.احمد، هلالي عبدالاله.(2000م). تفتيش نظم الحاسب الآلي وضمانات المتهمالمعلوماتي. عابدين : النسر الذهبي للطباعة.

5.بحر، عبدالرحمن محمد.(1420هـ). معوقات التحقيق في جرائم الإنترنت : دراسةمسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير غير منشورة، أكاديميةنايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

6.البداينة، ذياب.(1420هـ). جرائم الحاسب والإنترنت، أبحاث الندوة العلميةلدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلومالأمنية ، تونس، تونس (93-124).

7.البداينة، ذياب.(1988م). الأمن الوطني في عصر المعلومات. الجزيرة، 9421.

8.البداينة، ذياب.(1999م). التطبيقات الاجتماعية للإنترنت، ورقة قدمت فيالدورة التدريبية حول شبكة الإنترنت من منظور أمنى، أكاديمية نايف العربية للعلومالأمنية ، بيروت، لبنان.

9.تمّام، احمد حسام طه. (2000م). الجرائم الناشئة عن استخدام الحاسب الآلي.القاهرة : دار النهضة العربية .

10.الجنيدي، ماهر (أ). (1999م). النصر للأقوى والأذكى والقذر، مجلة إنترنتالعالم العربي ، (نوفمبر)، 36.

11.الجنيدي، ماهر (ب). (1999م). رائحة الماريجوانا تنبعث من أوكار إنترنت ، مجلةإنترنت العالم العربي ، (نوفمبر)، 39 – 40.

12.داود، حسن طاهر. (1420هـ). جرائم نظم المعلومات. الرياض : أكاديمية نايفالعربية للعلوم الأمنية.

13.داود، حسن طاهر. (1421هـ). الحاسب وامن المعلومات. الرياض : معهدالادارة العامة.

14.الدمينى، مسفر غرم الله.(1402هـ). الجناية بين الفقه الإسلامي والقانونالوضعي. (ط.2) الرياض : دار طيبة للنشر والتوزيع.

15.الزغاليل، أحمد سليمان.(1420هـ). الاتجار بالنساء والأطفال، أبحاثالندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايفالعربية للعلوم الأمنية ، تونس، تونس (43-90).

16.السيد، سمير.(1997م). محاضرات في شبكة المعلومات العالمية . القاهرة :مكتبة عين شمس.

17.السيف، محمد ابراهيم.(1417هـ). الظاهرة الإجرامية في ثقافة وبناء المجتمعالسعودي : بين التصور الاجتماعي وحقائق الاتجاه الاسلامي. الرياض :مكتبة العبيكان.

18.شتا، محمد محمد.(2001م). فكرة الحماية الجنائية لبرامج الحاسب الآلي.الإسكندرية: دار الجامعة الجديدة للنشر.

19.الشنيفي، عبدالرحمن عبدالعزيز.(1414هـ). أمن المعلومات وجرائم الحاسب الآلي.(ط1) الرياض : بدون.

20.الشهاوي، قدري عبدالفتاح.(1999م). اساليب البحث العلمي الجنائي والتقنيةالمتقدمة. الاسكندرية :منشأة المعارف.

21.الشهري، عبدالله محمد صالح.(1422هـ). المعوقات الإدارية في التعامل الأمنيمع جرائم الحاسب الآلي : دراسة مسحية على الضباط العاملين بجهاز الأمن العامبمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكةالعربية السعودية.

22.الشهري، فايز عبدالله.(1422هـ). استخدامات شبكة الإنترنت في مجال الاعلامالامني العربي. مجلة البحوث الأمنية ، 10(19)، 165-214.

23.صحيفة عكاظ، العدد 12789، 1422/6/13هـ، الصفحة الأولى.

24.طالب، احسن.(1998م). الجريمة والعقوبة والمؤسسات الاصلاحية. الرياض :دار الزهراء.

25.عبدالمطلب، ممدوح عبدالحميد.(2001 م). جرائم استخدام الكمبيوتر وشبكةالمعلومات العالمية : الجريمة عبر الإنترنت . الشارقة: مكتبة دار الحقوق.

26.عجب نور، اسامة محمد.(1417هـ). جريمة الرشوة في النظام السعودي. الرياض: معهد الادارة العامة.

27.عزالدين، أحمد جلال.(1414هـ). أساليب التعاون العربي في مجال التخطيطلمواجهة جرائم الارهاب. الرياض : أكاديمية نايف العربية للعلوم الأمنية.

28.عودة، عبدالقادر.(1401هـ). التشريع الجنائي الإسلامي. بيروت : مؤسسةالرسالة، (المجلد الأول).

29.عيد، محمد فتحي.(1419هـ). الإجرام المعاصر. الرياض : أكاديمية نايفالعربية للعلوم الأمنية.

30.فرحات، محمد نعيم.(1404هـ). التشريع الجنائي الاسلامي. جدة : مكتبةالخدمات الحديثة.

31.الفنتوخ، عبدالقادر.(1421هـ). الإنترنت للمستخدم العربي. الرياض: مكتبةالعبيكان.

32.القدهي، مشعل عبدالله. (1422هـ). المواقع الإباحية على شبكة الإنترنت وأثرهاعلى الفرد والمجتمع. [1422/7/29هـ] http://www.minshawi.com/gadhi.htm

33.الماوردي، محمد حبيب.(1407هـ). الاحكام السلطانية. القاهرة : دار التراثالعربي.

34.مجلة أفاق الإنترنت. (1997)، إنترنت 2، المؤلف، السنة 1 (3)، 38-41.

35.محمد، عادل ريان. (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي ،(440)، 73 – 77 .

36.مندورة، محمد محمود.(1410هـ). الجرائم الحاسب الآلية، دورة فيروس الحاسبالآلي، مكتب الأفاق المتحدة : الرياض ، 19 – 26.

37.منصور، عبدالمجيد سيد احمد.(1410هـ). السلوك الاجرامي والتفسير الاسلامي.الرياض : مركز ابحاث الجريمة.

38.موقع صحيفة الجزيرة - القرية الإلكترونية (1421/2/2) http://www.al-jazirah.com/2000/may/6/ev.htm#evt3

39.موقع أرابيا (2001/6/10م) http://www.arabia.com/tech/article/arabic/0,4884,48801,00.html

40.موقع السوق الخليجي (1423/4/1هـ)http://www.gulfforum.com/ksa1/20/1.html

41.موقع بوابة عجيب (2001/3/25م)category=34&http://it.ajeeb.com/viewarticle=1662

42.موقع بوابة عجيب (2001/8/8م) category=17&http://it.ajeeb.com/viewarticle.asp...976

43.موقع صحيفة البي بي سي (2001) http://news.bbc.co.uk/hi/arabic/news/newsid_1550000/1550726.stm

44.موقع صحيفة البيان (2000/5/19) http://www.albayan.co.ae/albayan/2000/05/19/mhl/2.htm

45.موقع صحيفة الجزيرة (2000) http://www.al-jazirah.com/

46.موقع مجلة الأمن الإلكترونية (1421/7/22هـ)
http://safola.com/security.chtml

47.موقع مجلس التعاون لدول الخليج العربية (1423/4/2هـ)-http://www.gcc
sg.org/index.html

48.موقع محامو المملكة (1423/4/2هـ)-http://www.mohamoon
Status=1&ksa.com/dir.asp?DirID=1

49.موقع منتدى الفوائد (14/8/ 1421هـ)
.forum&number=1&...http://216.122.89.86/muntada/postin

50.موقع وزارة التجارة
(1423/4/2هـ)
http://www.commerce.gov.sa/aboutus/leg1.asp?print=true

51.النشرة التعريفية عن مدينة الملك عبدالعزيز للعلوم والتقنية. (1419هـ).الرياض:
الإدارة العامة للتوعية العلمية والنشر.

52.اليوسف، عبدالله عبدالعزيز.(1420هـ). التقنية والجرائم المستحدثة، أبحاثالندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايفالعربية للعلوم الأمنية ، تونس، تونس (195- 233)

المصدر : www. Arab E Law.com