الفصل الأول

الإطار النظري للدراسة

مقدمة - تعريف الإنترنت وبداياته واستخداماته:

"الإنترنت هو جزء من ثورة الاتصالات، ويعرّف البعض الإنترنت بشبكة الشبكات، في حين يعرّفها البعض الآخر بأنّها: شبكة طرق المواصلات السريعة" (أبو الحجاج، ١٩٩٨م : ١٨)، كما أنّ الإنترنت " تعنى لغوياً ((ترابط بين شبكات)) وبعبارة أخرى ((شبكة الشبكات)) حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحّد يسمى ((بروتوكول تراسل الإنترنت)) (TCP/IP)"(الفنتوخ، ١٤٢١هـ:١١).

بدأ الإنترنت في ١٩٦٩/١/٢ عندما شكّلتْ وزارة الدفاع الأمريكية، فريقاً من العلماء، للقيام بمشروع بحثي عن تشبيك الحاسبات، وركّزت التجارب على تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة، ومن ثَمّ نقل هذه الأجزاء بأشكال وطرق مستقلة، حتى تصل مجمّعة إلى هدفها، وكان هذا الأمر يمثّل أهمية قصوى لأمريكا وقت الحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإن الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها، عن أي طريق آخر بديل، إلى خط النهاية، ومن ثَمّ تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم عام (١٩٨٣م) إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبغرضها الأساسي، وهو خدمة الاستخدامات العسكرية، في حين سُمِّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية ،أي تبادل المعلومات، وتوصيل البريد الإلكتروني، ومن ثَمّ ظهر مصطلح ((الإنترنت)) حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام (١٩٨٦م) أمكن ربط شبكات خمسة مراكز للكمبيوترات العملاقة وأطلق عليها اسم (NSFNET) والتي أصبحت فيما بعد العمود الفقري، وحجر الأساس، لنمو وازدهار الإنترنت في أمريكا، ومن ثَمّ دول العالم الأخرى (الفنتوخ،١٤٢١هـ : ٢١ - ٢٤).

من يملك الإنترنت؟

لا أحد في الوقت الراهن يملك الإنترنت، وإنْ كان يمكن القول في البداية بأنّ الحكومة الأمريكية ،ممثلة في وزارة الدفاع، ثُمّ المؤسسة القومية للعلوم، هي المالك الوحيد للشبكة، ولكن بعد تطّور الشبكة، ونمّوها، لم يعد يملكها أحد، واختفى مفهوم التملُّك، ليحلّ محلّه ما أصبح يسمي بمجتمع الإنترنت، كما أنّ تمويل الشبكة تحوّل من القطاع الحكومي، إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية –ذات الصبغة التجارية– والتي يمكن الاستفادة من خدماتها مقابل اشتراك (أبو الحجاج، ١٩٩٨م : ١٨). وهذه الخصوصية أي عدم وجود مالك محدد أو معروف للانترنت يجعل مهمة رجال الأمن أكثر صعوبة (Thompson, 1999).

توسع الشبكة:

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

وفي استطلاع أجرته شبكة (NUA) الأمريكية (NUA, 1998) قُدّر عدد مستخدمي الشبكة عالمياً في العام (١٩٩٨م) بحوالي (١٣٤,٠٠٠,٠٠٠) مئة وأربعة وثلاثين مليون مستخدم، وتصدرت أمريكا وكندا الصدارة من حيث عدد المستخدمين الذي بلغ (٧٠,٠٠٠,٠٠٠) سبعين مليون مستخدم (NUA ,6/1998).

وفي تقرير صدر بتاريخ ٢٠٠٠/١٠/٢٦م قدّر أنّ عدد المستخدمين للشبكة عام (٢٠٠٥م) سيكون حوالي (٢٤٥,٠٠٠,٠٠٠) مائتين وخمسة وأربعين مليون مستخدم، وقدّر أنّ غالبية هذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ,10/2000).

وقدّرت دراسة أجراها موقع عجيب (Ajeeb.com,25/3/2001) تجاوز عدد المستخدمين العرب الـ(٥,٠٠٠,٠٠٠) الخمسة ملايين مستخدم مع نهاية عام (٢٠٠١م)، وأنْ يصل العدد إلى (١٢,٠٠٠,٠٠٠) اثني عشر مليون مستخدم عربي مع نهاية عام (٢٠٠٢م)، وقدرّت الدراسة عدد مستخدمي الإنترنت في المملكة العربية السعودية بـ(٥٧٠,٠٠٠) خمسمائة وسبعين ألف مستخدم.

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

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

خدمات الإنترنت :

يوفّر الإنترنت خدمات عديدة من أهمها:

١. **البريد الإلكتروني:** لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي إلكتروني بصورة سريعة جداً لا تتعدّى ثواني في الغالب.
٢. **القوائم البريدية:** تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة.
٣. **خدمة المجموعات الإخبارية:** تشبه خدمة القوائم البريدية غير أنّ كلّ عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.
٤. **خدمة الاستعلام الشخصي:** يمكن الاستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الإنترنت والمسجلين لديها.
٥. **خدمة المحادثات الشخصية:** يمكن التحدث مع طرف آخر صوتاً وصورة وكتابة.
٦. **خدمة الدردشة الجماعية:** تشبه الخدمة السابقة إلا أنّه –وفي الغالب– يمكن لأي شخص أن يدخل في المحادثة، أو يستمع إليها، دون اختيار الآخرين.
٧. **خدمة تحويل أو نقل الملفات:** (FTP) لنقل الملفات من حاسب إلى آخر وهي اختصار كلمة (FILE TRANSFER PROTOCOL).
٨. **خدمة الأرشيف الإلكتروني:** (ARCHIVE) تُمكّن البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة في حاسب المستخدم.

٩. **خدمة شبكة الاستعلامات الشاملة:** (GOPHER) تفيد في خدمات كثيرة كنقل الملفات، والمشاركة في القوائم البريدية، حيث تفهرس المعلومات الموجودة على الشبكة.

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

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

١٢. **الصفحة الإعلامية العالمية:** (WORLD WIDE WEB) أو الويب (WEB) تجمع معاً كافة الموارد المتعددة التي يحتوي عليها شبكة الإنترنت للبحث عن كلّ ما في الشبكات المختلفة وإحضارها بالنص والصوت والصورة، وتعدّ الويب نظاماً فرعياً من الإنترنت، لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة.

مستلزمات الاتصال بالشبكة:

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

١. حاسب آلي.
٢. جهاز مودم.
٣. خط هاتفي.
٤. الاشتراك في الخدمة.
٥. برامج تصفح الشبكة وأشهرها (INTERNET EXPLORER) و (NETSCAPE)

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

المبحث الأول: جرائم الحاسب الآلي والإنترنت.

المبحث الثاني: جرائم الإنترنت من منظور شرعي وقانوني.

المبحث الثالث: الأبعاد الشرعية والقانونية للأفعال الجنائية المرتكبة من قبل مستخدمي الإنترنت في المجتمع السعودي (تصوّر إسلامي).

المبحث الأول: جرائم الحاسب الآلي والإنترنت

اشْتُقّتْ كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأَجْرَم فهو مجرم وجريم (ابن منظور، بدون : ٦٠٤ – ٦٠٥). وعَرَّفت الشريعة الإسلامية الجريمة بأنها"محظورات شرعية زجر الله عنها بحدّ أو تعزير"(الماوردي، ١٤١٧هـ : ١٩).

وتعرّف جرائم الحاسب الآلي والإنترنت فنياً بأنها: " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها" (مندورة،١٤١٠هـ : ٢١)، كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني " (محمد، ١٩٩٥م : ٧٣)، وهناك من عرّفها بأنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة" (البداينة، ١٤٢٠هـ : ١٠٢).

أمّا التعريف الإجرائي لدراسة الباحث فيُعَرِّفُ جرائم الإنترنت بأنّها : جميع الأفعال المخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية، المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسيّة والممارسات غير الأخلاقية، وجرائم الاختراقات، والجرائم المالية، وجرائم إنشاء أو ارتياد المواقع المعادية، وجرائم القرصنة.

وأطلق مصطلح جرائم الإنترنت (Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في استراليا للفترة من ١٦– ١٩٩٨/٢/١٧م (بحر، ١٤٢٠هـ : ٢)، وهذه الجرائم" لا تعترف بالحدود بين الدول ولا حتى بين القارات، فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة "(عيد، ١٤١٩هـ: ٢٥٢)، وهي تعدّ من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت باعتبارها أداة لارتكاب الجريمة أو تسهيل ارتكابها (Vacca , 1996).

وبالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبياً، إلا أنها لقيتْ اهتماماً من قبل بعض الباحثين، حيث أُجريتْ العديد من الدراسات المختلفة، لمحاولة فهم هذه الظاهرة، ومن ثَمّ التحكم فيها، ومنها دراسة أجرتها منظمة (Business Software Alliance) في الشرق الأوسط، حيث أظهرت أنّ هناك تبايناً بين دول منطقة الشرق الأوسط، في حجم خسائر جرائم الحاسب الآلي، حيث تراوحت ما بين (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دولار أمريكي في المملكة العربية السعودية، والإمارات العربية المتحدة، و (١,٤٠٠,٠٠٠) مليون وأربعمائة ألف دولار أمريكي في لبنان (البداينة، ١٤٢٠هـ : ٩٨).

وأظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأنّ (٢٤–٤٢٪) من منظمات القطاع الخاص، والعام، على حدٍّ سواء، كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت (البداينة، ١٩٩٩م : ٥).

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

وأظهر مسح أُجري من قبل (the computer security institute) في عام (١٩٩٩م)، أنّ خسائر (١٦٣) مئة وثلاث وستين شركة أمريكية –من الجرائم المتعلقة بالحاسب الآلي– بلغت أكثر من (١٢٣,٠٠٠,٠٠٠) مئة وثلاثة وعشرين مليون دولار أمريكي، في حين أظهر المسح الذي أُجري في عام (٢٠٠٠م) ارتفاع عدد الشركات الأمريكية المتضررة من تلك الجرائم، حيث وصل إلى (٢٧٣) مائتين وثلاث وسبعين شركة، بلغ مجموع خسائرها أكثر من (٢٥٦,٠٠٠,٠٠٠) مائتين وستة وخمسين مليون دولار(Rapalus,2000).

كما بيّنت إحصائيات الجمعية الأمريكية للأمن الصناعي أنّ الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد تصل إلى (٦٣,٠٠٠,٠٠٠,٠٠٠) ثلاث وستين بليون دولار أمريكي، وأنّ (٢٥٪) من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي، وقد أصيب (٦٣٪) من الشركات الأمريكية والكندية بفيروسات حاسوبية، ووصل الفقد السنوي بسبب سوء استخدام الحاسب الآلي (٥٥٥,٠٠٠,٠٠٠) خمسمائة وخمسة وخمسين مليون دولار(Reuvid,1998).

ومن الصعوبة بمكان، تحديد أي جرائم الحاسب الآلي المرتكبة هي الأكبر من حيث الخسائر، حيث لا يعلن الكثير عن مثل هذه الجرائم، ولكن من أكبر الجرائم المعلنة هي جريمة

لوس انجلوس، حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية (EFI) للإفلاس، وبلغت خسائرها (٢,٠٠٠,٠٠٠,٠٠٠) ملياري دولار أمريكي. وهناك أيضاً حادثة انهيار بنك بارينجر البريطاني في لندن، إثر مضاربات فاشلة في بورصة الأوراق المالية في طوكيو، حيث حاول البنك إخفاء الخسائر الضخمة، باستخدام حسابات وهمية، أدخلها في الحسابات الخاصة بالبنك، بمساعدة متخصصين في الحاسب الآلي، وقد بلغت إجمالي الخسائر حوالي مليار ونصف دولار أمريكي (داود، ١٤٢٠هـ: ٣١).

وتعدّ هذه الخسائر يسيرة نسبياً، إذا ما قورنت بالخسائر التي تسببها جرائم نشر الفيروسات، والتي تضرّ بالأفراد والشركات، وخاصة الشركات الكبيرة، حيث ينتج عنها توقف أعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وقد يصل الضرر في بعض المنشآت التجارية والصناعية إلى تكبّد خسائر مادية تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلت خسائر فيروس (Code Red) إلى (٢,٠٠٠,٠٠٠,٠٠٠) ملياري دولار أمريكي، في حين وصلت الأضرار المادية لفيروس الحب الشهير (٨,٧٠٠,٠٠٠) ثماني مليون وسبعمائة ألف دولار، واستمّر انتشار الفيروس لخمسة شهور، وظهر منه (٥٥) خمسة وخمسون نوعاً. وتتراوح أضرار الفيروسات ما بين عديمة الضرر إلى اليسير الهين، وقد تصل إلى تدمير جميع محتويات الجهاز، وإن كان الأكثر شيوعاً من هذه الفيروسات، هو ما يسبب ضرراً محصوراً في إتلاف البيانات التي يحتويها الجهاز (Ajeebb.com,8/8/2001).

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

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

غير أنّ متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها صعب جداً لأن أمثال" هذه الجرائم لا تترك أثراً، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات. ومعظم جرائم الحاسب الآلي تمّ اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنّ الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها" (مندورة ، ١٤١٠هـ : ٢٢).

وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أمور (موثق في شتا،٢٠٠١م : ١٠٣) **هي :**

أولاً: عدم ترك أثر لها بعد ارتكابها.

ثانياً: صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ثالثاً: احتياجها إلى خبرة فنية، ممّا يَصْعُبْ على المحقق التقليدي التعامل معها.

رابعاً: اعتمادها على الخديعة في ارتكابها والتضليل في التعرف على مرتكبيها.

خامسا: اعتمادها على قمة الذكاء في ارتكابها.

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

والإنترنت ليس قاصراً على السلبيات الأمنية فقط، بل له إيجابيات أيضاً، فهو مفيد جداً في النواحي الأمنية، كأنْ يُستخدم الإنترنت في إيصال التعاميم والتعليمات بسرعة، وإمكانية الاستفادة من قواعد البيانات المختلفة والموجودة لدى القطاعات الأخرى، وتبادل المعلومات مع الجهات المعنية، ويفيد أيضاً في مخاطبة الإنتربول ومحاصرة المجرمين بسرعة.

وفي دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت (البيان،٢٠٠٠م)، حددت (١٠) عشر خدمات أمنية يمكن تقديمها للجمهور عن طريق شبكة الإنترنت، وأبرزت (١٥) خمس عشرة سلبية، أبرزها الإباحية والمعاكسات والاحتيال والتجسس والتهديد والابتزاز.

كما حددت دراسة الشهري (الشهري، فايز، ١٤٢٢هـ) الإيجابيات الأمنية لشبكة الإنترنت في تلقي البلاغات، وتوفير السرية للمتعاونين مع الأجهزة الأمنية، وطلب مساعدة الجمهور في بعض القضايا، ونشر صور المطلوبين للجمهور، ونشر المعلومات التي تهم الجمهور، وتكوين جماعات أصدقاء الشرطة، وتوعية الجمهور أمنياً، واستقبال طلبات التوظيف، ونشر اللوائح والأنظمة الجديدة، وتوفير الخدمة الأمنية خارج أوقات العمل الرسمي، وسهولة الوصول إلى العاملين في الجهاز الأمني، وإجراء استفتاءات محايدة لقياس الرأي العام، ووسيط فاعل في عملية تدريب وتثقيف منسوبي القطاع، وأخيراً وسيط مهم للإطلاع على خبرات الدول المتقدمة والاتصال مع الخبراء والمتخصصين في مختلف دول العالم.

وقد بادرت بعض الأجهزة الأمنية في الدول الأوروبية إلى الاستفادة من شبكة الإنترنت، في البحث عن المجرمين والقبض عليهم " فقد تمكنت العديد من الدول وفي مقدمتها ألمانيا، وبريطانيا، وتأتي في المرتبة الثالثة فرنسا، من استخدام شبكة الإنترنت في السعي نحو ضبط المجرمين، بل التعرف على كل الحالات المشابهة في كل أنحاء أوروبا، والاتصال فورا بالإنتربول عبر شبكة الإنترنت" (الشهاوي، ١٩٩٩م : ٢٥).

فئات الجناة في جرائم الحاسب الآلي :

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

الفئة الأولى : العاملون على أجهزة الحاسب الآلي في منازلهم، نظراً لسهولة اتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد، أو نظام معين، يحدّ من استعمالهم للجهاز.

الفئة الثانية : الموظفون الساخطون على منظماتهم التي يعملون بها، هؤلاء يعودون إلى مقرّ عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتى سرقته، وقد يجد الموظف نفسه أحياناً مرتكباً لجريمة حاسوبية، مصادفة، ودون تخطيط مسبق لها.

الفئة الثالثة : فئة المتسللين (Hackers) وينقسمون قسمين: فمنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفون الذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز، وتقع أغلب جرائم الإنترنت حالياً تحت هذه الفئة بقسميها.

الفئة الرابعة: العاملون في الجريمة المنظمة، كعصابات سرقة السيارات، حيث يحددون بواسطة شبكة الإنترنت، الأماكن التي ترتفع بها سعر بيع قطع غيار السيارات، ومن ثَمّ يبيعون القطع المسروقة في تلك الأماكن ليضمنوا أكبر ربح ممكن.

خصائص وأنواع جرائم الحاسب الآلي والإنترنت :

بطبيعة الحال فإنّه من الصعب جداً الفصل بين جرائم الحاسب الآلي وجرائم الإنترنت، فكلاهما وجهان لعملة واحدة، إذ لابدّ من وجود الحاسب الآلي لارتكاب جرائم الإنترنت.

وعلى كل حال يُصنِّف كل من محمد ومندورة (محمد،١٩٩٥م؛ مندورة، ١٤١٠هـ) تلك الجرائم إلى مجموعات:

المجموعة الأولى : تستهدف مراكز معالجة البيانات المخزّنة في الحاسب الآلي، لاستغلالها بطريقة غير مشروعة، كمن يدخل إلى إحدى الشبكات، ويحصل على أرقام بطاقات ائتمان بنكية مخزّنة لدى البنك، ليحصل بواسطتها على مبالغ من حساب مالك البطاقة.

ومما يميّز هذا النوع من الجرائم، أنّه يصعب اكتشافه، مالم يكن هناك تشابه في بعض أسماء أصحاب هذه البطاقات.

المجموعة الثانية : تستهدف مراكز معالجة البيانات المخزّنة في الحاسب الآلي، بقصد التلاعب بها، أو تدميرها كلياً، أو جزئياً، ويمثّل هذا النوع: الفيروسات المرسلة عبر البريد الإلكتروني، أو بواسطة برنامج مسجل في أحد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي.

ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات، ولكن بشرط تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجات الحماية، علماً بأنّ وجود مثل هذه البرامج في جهاز الحاسب الآلي، لا يعنى إطلاقاً الحماية التامة من أي هجوم فيروسي، وإنما هو أحد سبل الوقاية، لأنّه قد يتسلل الفيروس إلى الجهاز، بالرغم من وجودها، ويلحق أذى بالجهاز ومكوناته، خاصة إذا كان الفيروس حديثاً وغير معروف من قبل.

المجموعة الثالثة :تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحباً على جوائز اليانصيب، حيث قام أحد الموظفين بالشركة، بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو، فذهبت الجائزة إلى شخص دون أن يستحقها نظاماً.

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

المبحث الثاني: مواكبة الأنظمة والتشريعات لجرائم الإنترنت

" يمكن النظر للإنترنت كمهدد للأمن الاجتماعي، وخاصة في المجتمعات المغلقة والشرقية، حيث أنّ تعرُّض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثاً ثقافياً يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات. إنّ الاستخدام غير الأخلاقي واللاقانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلباً على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قِيمّيةٍ لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسيّة وتقديم الصور والمواد الإباحية" (البداينة، ١٩٩٩م : ١٠١).

والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين و" مع دخول الكمبيوتر (الحاسب الآلي) الذكي إلى المنازل فإنّ ذلك سيفتح الباب لأنواع متطورة من الجرائم التي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشبكة الإنترنت، فطالما أنّك تستطيع مثلاً وصل خزانة الأموال في مكتبك بشبكة الإنترنت لإعطاء إنذار عند محاولة فتحها، فربمّا يكون من الممكن فتحها عن بعد بواسطة الكمبيوتر (الحاسب الآلي) ثُمّ الوصول إليها وإفراغها"(داود، ١٤٢٠هـ : ٣٢)

واستلزم التطور التقني، تطوراً في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية من السهولة بمكان –في الغالب– تحديد مكان ارتكابها، بل إنّ ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين أنّه يصعب جداً تحديد مكان وقوع الحادثة عند التعامل مع جرائم الإنترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما أنّه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود دولية أو جغرافية، ونتيجة لذلك فإن تحديد مكان محاكمة الجناة، والقوانين التي تخضع لها كل جريمة، أمر في غاية الحساسية والتعقيد خاصة وأنّ كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلاً قد لا يعتبر جريمة في أمريكا والعكس صحيح، بل إنّ الأمر يصل إلى حدِّ اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما في الولايات المتحدة الأمريكية (Thompson, 1999).

وأدىّ التطّور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، ممّا أجمع معه مشرّعو القانون الوضعي في الدول المتقدمة، على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أنْ تنشأ عن استخدام الحاسب الآلي وشبكة الإنترنت، ودَفَعَهُمْ هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة، وما أثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الاختصاص القضائي ومكان وزمان ارتكاب الجريمة، حيث يَسْهُل على المجرم في مثل هذه الجرائم ارتكاب جريمة ما في مكان غير المكان الذي يتواجد فيه، أو الذي حدثت فيه نتائج فعله (تمّام، ٢٠٠٠م : ١– ٣).

وتطوير القوانين الجنائية وتحديثها أمر يستغرق بعض الوقت فـ"هناك تعديلات كثيرة مطلوب إدخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن استخدام الحاسب الآلي في مجال المعلومات، وعن ظهور شبكات المعلومات العالمية" (داود، ١٤٢١هـ : ٦٨)، وقد لاقت جرائم الحاسب الآلي اهتماماً عالمياً، فعقدت المؤتمرات والندوات المختلفة، ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (١٩٩٣م)، الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنولوجيا المعلومات، وتوصّل إلى توصيات أحاطت بجوانب مشكلة جرائم الحاسب الآلي، إلاّ أنّها لم تتعرض لجزئية هامة وهي التعاون الدولي الذي يعتبر ركيزة أساسية عند التعامل مع هذه النوعية من الجرائم (عيد، ١٤١٩هـ:٥٦ – ٢٥٩).

ويعتبر هذا المؤتمر تحضيراً للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام (١٩٩٤م)، والذي وضع عدة توصيات حول جرائم الحاسب الآلي والإنترنت، والتحقيق فيها، ومراقبتها، وضبطها، وركّز على ضرورة إدخال بعض التعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وإفرازاتها (أحمد،٢٠٠٠م : ٥ – ١٠).

والتعاون الدولي مهمّ عند التعامل مع جرائم الإنترنت، لكونه يطّور أساليب متشابهة لتحقيق قانون جنائي، وإجرائي، لحماية شبكات المعلومات الدولية، خاصة أنّ هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فإنّ عدم التعاون الدولي يؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول، ممّا يعطي الفرصة للمجرمين للإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية (الشنيفي، ١٤١٤هـ :١١٣).

وتعتبر السويد أول دولة تسنّ تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، حيث صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها (الشنيفي، ١٤١٤هـ : ١٠٨؛ عيد، ١٤١٩هـ : ٢٥٥).

وتبعت الولايات المتحدة الأمريكية السويد حيث كانت ثاني دولة تشرّع قانوناً خاصاً بحماية أنظمة الحاسب الآلي وذلك من خلال القانون المعروف بقانون عام (١٩٧٦م – ١٩٨٥م)، ومن ثَمّ قام معهد العدالة القومي عام (١٩٨٥م) بتحديد خمسة أنواع رئيسة للجرائم المعلوماتية هي:

١.جرائم الحاسب الآلي الداخلية، ٢. جرائم الاستخدام غير المشروع عن بعد، ٣. جرائم التلاعب بالحاسب الآلي، ٤. دعم التعاملات الإجرامية، ٥. سرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (١٩٨٦م) صدر قانونٌ تشريعيٌ يحمل الرقم (١٢١٣)، عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خوّلت وزارة العدل الأمريكية في عام (٢٠٠٠م) خمس جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع جرائم الحاسب الآلي والإنترنت (الشنيفي، ١٤١٤هـ: ١٠٩؛ عبدالمطلب، ٢٠٠١م: ٩٢ – ٩٤؛ عيد، ١٤١٩هـ: ٢٥٥).

وتأتي بريطانيا ثالث دولة تسنّ قوانين خاصة بجرائم الحاسب الآلي حيث أقرتّ قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير، وسائط التخزين الحاسوبية المتنوعة، أو أي أدآة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى (الشنيفي، ١٤١٤هـ : ١٠٩؛ عيد، ١٤١٩هـ : ٢٥٥).

وتطبّق كندا قوانين متخصصة ومفصّلة للتعامل مع جرائم الحاسب الآلي والإنترنت، حيث عدّلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت، وحدّد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، ووضّح فيه صلاحيات جهات التحقيق، وجاء في قانون المنافسة (The Competition Act) مثلا ما يخوّل مأمور الضبط القضائي –متى ما حصل على أمر قضائي– حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها (أحمد، ٢٠٠٠م : ٢٦٣؛ الشنيفي، ١٤١٤هـ : ١١٠؛ عيد، ١٤١٩هـ : ٢٥٥).

وفي عام (١٩٨٥م) سنّت الدنمرك أول قوانينها الخاصة بجرائم الحاسب الآلي والإنترنت، حيث شملت العقوبات المحددة لجرائم الحاسب الآلي، كالدخول غير المشروع إلى الحاسب الآلي، أو التزوير، أو أي كسب غير مشروع، سواء للجاني أو لطرف ثالث، أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها، أو تغييرها، أو الاستفادة منها (الشنيفي، ١٤١٤هـ : ١١٠؛ عيد، ١٤١٩هـ : ٢٥٥)

كما اهتمّت فرنسا بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية، فأصدرت في عام (١٩٨٨م) القانون رقم (١٩-٨٨) -الذي أضاف إلى قانون العقوبات الجنائي- جرائم الحاسب الآلي والعقوبات المقررة لها، كما تمّ عام (١٩٩٤م) تعديل قانون العقوبات لديها، ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريّات وسماع الأقوال (تمام، ٢٠٠٠م : ٩١- ٩٢، ١١٥؛ شتا، ٢٠٠١م : ٧٠).

وفي هولندا يحقّ للقاضي إصدار أمر بالتصنّت على شبكات الحاسب الآلي متى كانت هناك جريمة خطيرة، كما يجيز القانون الفلندي لمأمور الضبط القضائي حق التصّنت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام (أحمد، ٢٠٠٠م : ٢٢٢، ٢٦٣)

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والإنترنت تنص على أنّه لا يَلْزَمُ مالك الحاسب الآلي المستخدم في جريمة ما، التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرّت عام (١٩٩١م) شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل (أحمد، ٢٠٠٠م : ٢٢٢، ٢٧٦)، ويوجد في المجر وبولندا قوانين توضّح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهّم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضاً الحقّ في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك سيؤدي إلى إدانته أو إدانة أحد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى أبعد من هذا حيث إنهّا تنصّ على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم (أحمد،٢٠٠٠م : ٢٧٦).

هذا وعلى مستوى الدول العربية فإنّه وحتى تاريخه –وبحسب علم الباحث– لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والإنترنت، ففي مصر مثلاً ،وإنْ كان لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أنّ القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية، ومن ذلك مثلاً اعتبر أنّ قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تمّ تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية (تمام، ٢٠٠٠م : ٩١– ١٠٤، ١٢٦).

وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وإنْ وجد نص قريب من الفعل المرتكب فإنّ العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت. وقد أوكل إلى شركة البحرين للاتصالات السلكية واللاسلكية (بتلكو) مهمة تقديم خدمة الإنترنت للراغبين في ذلك، كما أنيط بها مسؤولية الحدّ من إساءة استخدام شبكة الإنترنت من قبل مشتركيها (بحر، ١٤٢٠هـ : ٣٩، ٤٣).

وعلى المستوى المحلي نجد أنّ المملكة العربية السعودية أيضاً لم تسنّ قوانين خاصة بجرائم الإنترنت، إلاّ أنّ الوضع مختلف هنا، فهي ليست في حاجة لتحديث قوانينها وتشريعاتها لأنّها تنطلق من الشريعة الإسلامية الكاملة، فالمشرّع واحد لا ثاني له، والتشريع أزلي لا تجديد له، وهو مع كونه أزلي فإنّه صالح لكل زمان ومكان لكونه صادر من خالق الكون والعليم بما يَصْلُحُ له ويُصْلِحُهُ. وقد " تركت الشريعة الإسلامية الباب مفتوحاً لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة، منها لا ضرر ولا ضرار، وتركت لولي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاة لمصلحة المجتمع، ويندرج ذلك تحت باب التعازير" (الشهري، عبدالله، ١٤٢٢هـ : ٣٨)، وهناك قاعدة سد الذرائع أي "دفع الوسائل التي تؤدي إلى المفاسد، والأخذ بالوسائل التي تؤدي إلى المصالح" (أبوزهرة، ١٩٧٦م : ٢٢٦). "ومن المقرر فقهياً أنّ دفع المفاسد مُقَدّمٌ على جلب المصالح" (أبو زهرة، ١٩٧٦م : ٢٢٨).

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

لذا فإنّ هذا البحث وعند دراسته لجرائم الإنترنت في المجتمع السعودي فإنّه ينطلق من القوانين الشرعية المعمول بها في المملكة العربية السعودية التي تستمد قوانينها من كتاب الله وسنة نبيه محمد عليه أفضل الصلاة وأزكى التسليم، وليس من القوانين الوضعية التي قد تتّفق في تعريف الجريمة إلا أنّها تختلف حتماً في تقسيمها للجريمة.

وتعّرف الجريمة في القوانين الوضعية بأنّها: كلّ فعل يعاقب عليه القانون، أو امتناع عن فعل يقضي به القانون، ولا يعتبر الفعل أو الترك جريمة إلاّ إذا كان مجرّماً في القانون. أمّا التعريف الشرعي للجريمة فهي: إتيان فعل محرّم معاقب على فعله، أو ترك فعل محرم الترك، معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه (عودة، ١٤٠١هـ : ٦٦). أو بمعنى آخر هي "فعل ما نهي الله عنه، وعصيان ما أمر الله به" (أبو زهرة، ١٩٧٦م : ٢٤).

والشريعة الإسلامية تقّسم الجريمة من حيث جسامة العقوبة إلى حدود، قصاص أو دية، وتعازير، أمّا القوانين الوضعية فتقّسم الجريمة إلى جنايات، جنح، ومخالفات (الدميني، ١٤٠٢هـ، طالب، ١٩٩٨م : ١٦٨). أي إنّ القوانين الوضعية " تُقسّم الجريمة أساساً على مقدار العقوبة، وبذلك فإنّ تحديد الجريمة يعتبر فرعاً من العقوبة، في حين أنّ التشريع الإسلامي يجعل الأساس في العقوبة هو جسامة الجريمة وخطرها من حيث المساس بالضرورات الخمس" (منصور، ١٤١٠هـ : ٢١٣ – ٢١٤).

وبشكل أدقّ فالاختلاف يقع في التقسيم الثالث أي في قسم التعازير في الشريعة، وقسم المخالفات في القوانين الوضعية، ففي الأولي أشمل وأعمّ حيث إنّه يُدْخِلُ في التعازير كلّ الأفعال سواء المجرّمة أو غير المجرّمة، أي التي لها عقوبة محددة أو التي لم ينُصّ علي عقوبة محددة لها، فالعقوبة هنا تقديرية للقاضي وتبدأ من الزجر والتوبيخ وتصل إلى حدِّ إيقاع عقوبة القتل، تبعاً للفعل المرتكب ولنظرة القاضي لذلك الفعل. في حين يحدد القانون الوضعي عقوبات محددة للمخالفات بمعنى أنّه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون و إلاّ لم يعتبر جرماً، ومن هنا تختلف النظرة إلى الجريمة في الشريعة الإسلامية عنها في القوانين الوضعية، حيث إنّها أشمل وأعمّ في الشريعة عنها في القوانين الوضعية، الأمر الذي يجعل معه الشريعة الإسلامية متطوّرة ومتجدّدة دوماً، فهناك عقوبة لكل فعل شاذ أو غير مقبول وإنْ لم ينصّ على تجريمه قانوناً.

ولا يعنى هذا أنّ كل الأفعال مجرّمة في الشريعة، بل المقصود هو أنّ أي فعل شاذ أو منافٍ لتعاليم الدين الإسلامي ولو كان جديداً فإنّ هناك عقاب له في الشريعة، فـ"الأساس بلا شكّ في اعتبار الفعل جريمة في نظر الإسلام هو مخالفة أوامر الدين" (أبوزهرة، ١٩٧٦م: ٣١)، أمّا العقوبة المقررة لكل جريمة فمتفاوتة حيث " تتفاوت الجرائم في الإسلام بتفاوت ما فيها من مفاسد" (أبو زهرة، ١٩٧٦م: ١٨٥)، فالشريعة حدّدت إطاراً عاماً للأفعال المقبولة وغير المقبولة جديدها وقديمها، كما حدّدت العقوبة المناسبة لكل جريمة أو فعل غير مقبول، وهنا سرّ تفوّق الشريعة الإسلامية.

ومن هذا فقضية الجريمة والعقوبة ومستجداتها أمر محسوم في المملكة العربية السعودية ويميزّها عن غيرها من الدول، فالقوانين الجنائية لديها والمستمدة من الشريعة تّتسم "بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل الذي يغطي كلّ جوانب الحياة ويصلح لكلّ زمان ومكان. فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحماية المصالح المعتبرة في الإسلام، وهي الدين والنسل والنفس والمال والعقل، وأيّ اعتداء على مصلحة من تلك المصالح يعتبر جريمة يعاقب فاعلها، ويختلف بالطبع مقدار العقوبة حسب جرامة الفعل الإجرامي" (عجب نور، ١٤١٧هـ : ١٣).

ومع ذلك فالأمر يحتاج إلى وضع أسس تنظيمية فاعلة وشاملة لتحديد الجهة المخوّلة بداية للتعامل مع جرائم الإنترنت والممارسات غير الأخلاقية التي تحدث أثناء استخدام الإنترنت، تحقيقاً، وضبطاً، ووقايةً، فلا بدّ أنْ يواكب استخدام المملكة العربية السعودية لتقنية الإنترنت ظهور أنماط جديدة من الإجرام ،كغيرها من الدول، فهذه الأنماط ليست قاصرة على دولة دون أخرى.

فلا بد من وضع تنظيمات واضحة للحدّ من سلبيات هذه الأفعال ومحاسبة مرتكبيها وإعطاء الحق للمتضررين منها. فهذه التنظيمات سوف تُفَعِّلُ قوانين وتشريعات المملكة المستمدة من الشريعة الإسلامية لتضع بعض الحواجز والروادع أمام من يرتكب مثل هذه الجرائم من داخل المملكة.

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

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

١. منع انتحال أرقام الإنترنت أو ما يعرف بـ(Ip-spoofing) والتي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة .
٢. منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـ(E-Mail Spamming) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم، وهو ما عرف اصطلاحاً باسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.
٣. الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (٦) أشهر.
٤. الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسي ومزوّد الاتصال، بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.
٥. تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.
٦. ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

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

وهذه التنظيمات مفيدة ولا شك إلا أنها ليست كافية، والمهمّ بداية تحديد جهة متخصصة ومؤهلة للتعامل مع جرائم الإنترنت تحقيقاً وضبطاً ووقاية، خلاف مدينة الملك عبدالعزيز التي تضطلع بمهام كثيرة ومختلفة عن المهام التي ستوكّل للجهة التي ستحدّد لمثل هذا العمل. وعلى كلّ حال فيجب أن لا يركن إلى الأنظمة والتعليمات فقط عند التعامل مع الجرائم والتجاوزات، فالأنظمة ليست وحدها الرادع لأي مخالفات أو سلبيات وخاصة في بيئة دينية محافظة كالمملكة العربية السعودية حيث يلعب الوازع الديني والرقابة الذاتية دوراً مهماً في الردع والحدّ من أي تجاوزات، فمن المهمّ أنْ يؤخذ

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

ولعلنّا لا نغفل العادات والتقاليد المستوحاة من شريعتنا الإسلامية وتقاليدنا العربية الأصيلة، التي تربّي بداخل المواطن الوازع الديني الرادع عن ارتكاب المخالفات والنواهي، ومع كلّ هذه الضوابط فالنفس أمارة بالسوء والشيطان يجري من ابن آدم مجرى الدم، فيجب أنْ يكون هناك ضوابط عقابية تعاقب من يضعف رادعه الإيماني ليجد الرادع السلطاني له بالمرصاد، فإنّ الله ليزع بالسلطان ما لا يزع بالقرآن.

المبحث الثالث:

الأبعاد الشرعية والقانونية للأفعال الجنائية المرتكبة من قبل مستخدمي الإنترنت في المجتمع السعودي (تصور إسلامي)

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

أولاً : الجرائم الجنسيّة والممارسات غير الأخلاقية وتشمل:

١. المواقع والقوائم البريدية الإباحية:

يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية، والشراء منها، والاشتراك فيها، أو إنشائها. وقد" أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الإنترنت يشكّل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل في أعداد مستخدمي الإنترنت حول العالم" (الزغاليل، ١٤٢٠هـ: ٧٦)، وتختلف المواقع الإباحية عن القوائم البريدية التي تخصص لتبادل الصور والأفلام الجنسيّة، فالمواقع الإباحية غالباً ما يكون الهدف منها الربح المادي، حيث يستوجب على متصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم إباحي لوقت محدد، أو دفع اشتراك شهري، أو سنوي مقابل الاستفادة من خدمات هذه المواقع، وإن كانت بعض هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال صور جنسيّة مجانية يومية على عناوينهم البريدية، كما أنّ تصفح الموقع يتطلب في الغالب الاتصال المباشر بشبكة الإنترنت مما يعنى أنّ الموقع قد يتمّ حجبه من قبل مدينة الملك عبدالعزيز للعلوم والتكنولوجيا فلا يمكن الوصول إليه إلا باستخدام البروكسي.

أمّا القوائم البريدية فهي أسهل إنشاءاً، وغالباً ما تكون مجانية، ويقوم أعضاؤها المشتركين بتبادل الصور والأفلام على عناوينهم البريدية، وربمّا تكون القوائم البريدية أبعد عن إمكانية المتابعة الأمنية، حيث يُرَكّزُ نشاطها على الرسائل البريدية والتي يصعب منعها عن أعضاء المجموعة، حتى وإن تمّ الانتباه إلى تلك القائمة لاحقاً وتمّ حجبها، فإنّ الحجب يكون قاصراً على من يحاولون الاشتراك بعد حجب الموقع ولا يتوفر لديهم وسائل تجاوز المرشحات، أمّا الأعضاء السابقون فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يريدونه دون تدخل وسائل الحجب. ويشترك في القوائم البريدية آلاف الأشخاص التي تصلهم جميعاً أي رسالة يرسلها مشترك منهم، مما يعنى أنّ هناك كماً هائلاً من الرسائل والصور الجنسيّة يتبادلها مشتركو القائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة، والمزايا الأخرى التي تقدّمها حيث " تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ" (داود،١٤٢٠هـ : ٩٣)، فكلّ مستخدم معرّض للتأثر بما يعرض على الإنترنت الذي لا يعترف بحدود دولية أو جغرافية، فهو يشكّل خطراً حقيقياً على الأطفال فضلاً عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة (الزغاليل، ١٤٢٠هـ : ٧٨).

ويوجد على الإنترنت ألآف المواقع الإباحية وعدد كبير جداً من القوائم الجنسيّة التي أصبحت أكثر تخصصاً، فهناك قوائم خاصة للشواذ من الجنسين، وهناك قوائم أخرى تصنّف تحت دول محددة. وممّا يندى له الجبين، ويحزن له القلب، أنّ هناك مواقع شاذة بمسميات عربية بل وسعودية، والأدهى والأمَرّ الربط بين بعض القوائم الإباحية والإسلام كموقع أطلق عليه "السحاقيات المسلمات" وهكذا.

وكشفت إحدى الدراسات أنّ نسبة (٧٠٪) من التدفّق على المواقع الإباحية يكون في أوقات العمل التي تبدأ من الساعة التاسعة صباحاً إلى الخامسة عصراً (بي بي سي، ٢٠٠١م).

كما كشفت دراسة القدهي (القدهي،١٤٢٢هـ) بأنّ هناك إقبالاً كبيراً جداً على المواقع الإباحية، حيث تزعم شركة (Playboy) الإباحية بأنّ (٤,٧) مليون زائر يزور صفحاتهم على الشبكة أسبوعياً، وبأنّ بعض الصفحات الإباحية يزورها (٢٨٠,٠٣٤) زائراً يومياً، وأنّ هناك مئة صفحة مشابهة تستقبل أكثر من (٢٠,٠٠٠) عشرين ألف زائر يومياً، وأكثر من ألفي صفحة مشابهة تستقبل أكثر من (١٤٠٠) ألف وأربعمائة زائر يومياً، وأنّ صفحة واحدة من هذه الصفحات استقبلت خلال عامين (٤٣,٦١٣,٥٠٨) مليون زائر، كما وجد أنّ (٨٣,٥٪) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية، وبأنّ أكثر من (٢٠٪) من سكان أمريكا يزورون الصفحات الإباحية، حيث تبدأ الزيارة غالباً بفضول ثُمّ تتطور إلى إدمان، وفي الغالب لا يتردد زوّار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الإباحية بها أو شراء مواد خليعة منها، وقد بلغت مجموع مشتريات مواد الدعارة في الإنترنت في عام (١٩٩٩م) ما نسبته (٨٪) من دخل التجارة الإلكترونية البالغ (١٨) مليار دولار أمريكي، في حين بلغت مجموع الأموال المنفقة للدخول على المواقع الإباحية (٩٧٠) مليون دولار. ويتوقع ارتفاع المبلغ ليصل إلى (٣) ثلاثة مليار دولار في عام (٢٠٠٣م)، وقد اتّضح أنّ أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين (١٢) و (١٥) سنة، في حين تمثّل الصفحات الإباحية أكثر صفحات الإنترنت بحثاً وطلباً.

كما وضّحت دراسة أدست (Adsit) (Adsit, 1999) أنّ المواقع الإباحية أصبحت مشكلة حقيقية، وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون آخر، ويمكن أن تلمس أثارها السيئة في: ارتفاع جرائم الاغتصاب بصفة عامة، واغتصاب الأطفال بصفة خاصة، والعنف الجنسي، وانعدام القيم والمبادئ عند الأسر، وامتهان النساء وعدم احترامهن. ويبدو أنّ لكثرة المواقع الإباحية على الإنترنت التي يقدر عددها بحوالي (٧٠,٠٠٠) ألف موقع دوراً كبيراً في إدمان مستخدمي الإنترنت عليها، حيث اتّضح أنّ نسبة (١٥٪) من مستخدمي الإنترنت البالغ عددهم (٩,٦٠٠,٠٠٠) مليون شخص تصفحوا المواقع الإباحية في شهر أبريل عام (١٩٩٨م).

وقام الباحث بمساعدة آخرين بحصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقع على شبكة الإنترنت، ومنها موقع الياهو (YAHOO) فوجد أنها تصل إلى (١٧١) مئة وإحدى وسبعين قائمة، بلغ عدد أعضاء أقلّ تلك القوائم (٣) ثلاثة، في حين وصل عدد أكثرها أعضاء إلى (٨٦٨٣) ثمانية آلاف وستمائة وثلاثة وثمانين عضواً، أمّا موقع قلوب لست (GLOBELIST) فقد احتوى على (٦) ست قوائم إباحية عربية، في حين وجد عدد (٥) خمس قوائم عربية إباحية على موقع توبيكا (TOPICA) وقد قامت مدينة الملك عبدالعزيز للعلوم والتقنية مشكورةً بإغلاق تلك المواقع.

وارتياد مثل هذه المواقع ومشاهدة المواد الجنسيّة بها من المحظورات الشرعية التي حرص الشارع الحكيم على التنبيه عليها وتحريمها، بل إنّه أمرنا بغضّ البصر، كما حرّم النظر إلى الأجنبيات، فضلاً عن تجنّب النظر إلى الحرام، فقال عزّ وجلّ في كتابه الحكيم في سورة النور: ﴿ قُلْ لِلْمُؤْمِنِينَ يَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَلِكَ أَزْكَى لَهُمْ إِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ(٣٠) ﴾، فهناك ولا شكّ علاقة بين " ارتكاب الأفعال الجنسيّة المحرّمة والنظر إلى الصور الجنسيّة العارية، فالدين الإسلامي الحنيف حذّر من ظاهرة النظر للعراة، لما تحدثه من تصدعات أخلاقية في الفرد والمجتمع" (السيف، ١٤١٧هـ : ١٠٠).

ويذهب الشارع إلى أبعد من ذلك حيث حرّم رسول الله صلى الله عليه وسلم أن تصف المرأة لزوجها جمال امرأة أخرى لا تحلّ له، فقال عليه الصلاة والسلام في الحديث الذي رواه البخاري في صحيحه واحمد في مسنده واللفظ للبخاري: " قَالَ النَّبِيُّ صَلَّى اللَّهم عَلَيْهِ وَسَلَّمَ لَا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَا كَأَنَّهُ يَنْظُرُ إليها". كلّ هذه الأمور اهتّم بها الشارع وحرّمها لأنّها موصلة لجريمة الزنا التي تعدّ من الكبائر، فتجنّب الأفراد لهذه الأفعال هو درع حصين لهم من الوقوع في الزنا وما شابهه.

ومن حكمة الشارع ومعرفته بالغرائز البشرية –التي يساهم الشيطان في تأجيجها ليوقع الإنسان فيما حرم الله– ولعظمة جريمة الزنا فإنّه لم يحرّم الزنا فقط، بلْ حرّم الاقتراب منه، فقال تعالى في سورة الإسراء: ﴿ وَلاَ تَقْرَبُوا الزِّنَى إِنَّهُ كَانَ فَاحِشَةً وَسَاءَ سَبِيلا(٣٢) ﴾.

يقول القرطبي رحمه الله (القرطبي، ١٩٨٦م)، في تفسير هذه الآية:" قال العلماء قوله تعالى "ولا تقربوا الزنا" أبلغ من أن يقول ولا تزنوا فإنّ معناه فلا تدنوا من الزنا. فأيّ اقتراب من المحظور هو فعل محظور في حدِّ ذاته، ومن ذلك مشاهدة المواد الجنسيّة فضلا عن الاشتراك في تلك القوائم الإباحية أو شراء مواد جنسيّة منها أو إنشائها – وهو الأشدّ خطراً – لأنّ الفعل الأخير يتعدّى ضرره للغير ويدخل فاعله تحت وعيد الله عزّ وجلّ حين قال في سورة النور: ﴿ إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ ءامَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لاَ تَعْلَمُونَ(١٩) ﴾.

وقد أثبتت بعض الدراسات في المجتمع السعودي أنّ (٦٨,٨ ٪) من مجموعة المبحوثين يرون أنّ هناك علاقة بين الانحراف والجرائم المرتكبة وبين مشاهدة أشرطة الفيديو الجنسيّة، كما أثبتت إحدى الدراسات المتخصصة في تفسير ارتكاب الجريمة الجنسيّة في المجتمع السعودي والتي أجريت في الإصلاحيات المركزية بالمملكة، أنّ (٥٣,٧٪) من مرتكبي الجرائم الجنسيّة كان لهم اهتمامات بالصور الجنسيّة، وأنّ فئة كبيرة منهم كانوا يميلون إلى مشاهدة الأفلام الجنسيّة الخليعة وقت فراغهم، كما تبيّن من الدراسة قوة تأثير مثل هذه الصور في ارتكاب جرائم الاعتداء الجنسي من قبل مجرمي اغتصاب الإناث وهاتكي أعراض الذكور بالإكراه (السيف، ١٤١٧هـ : ٩٩).

٢ . *المواقع المتخصصة في القذف وتشويه سمعة الأشخاص:*

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف، ونشر بعض أسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه. وهناك حادثة مشهورة جرى تداولها بين مستخدمي الإنترنت في بداية دخول الخدمة للمنطقة، حيث قام شخص ما، في دولة خليجية، بإنشاء موقع على الإنترنت ونشر به صور إحدى الفتيات وهي عارية وفي أوضاع مخلّة مع صديقها، وقد حصل علي تلك الصور أثر التسلل إلى حاسوبها الشخصي والاستيلاء على الصور منه، ومن ثَمّ حاول ابتزازها جنسياً وتهديدها بنشر تلك الصور على الإنترنت، إلاّ أنّها لم تتجاوب معه فنفّذ تهديده بإنشاء الموقع ونشر الصور به، كما قام بتوزيع رابط الموقع على عدد من المنتديات والقوائم البريدية، ممّا أدى إلى انتحار الفتاة لأنّه فضحها بين ذويها ومعارفها.

كما وقعت حادثة تشهير أخرى من قبل من أطلقوا على أنفسهم (الأمجاد هكرز) حيث أصدروا بياناً نُشر على الإنترنت بواسطة البريد الإلكتروني، ووصل إلى عدد من مشتركي الإنترنت، أوضحوا فيه قيام شخص يكنّ (بحجازي نادي الفكر) على التطاول في أحد المنتديات بالقدح والسبّ السافر على شيخ الإسلام ابن تيمية والشيخ محمد بن عبدالوهاب وغيرهم من رموز الدعوة السلفية، وقد استطاع (الأمجاد هكرز) اختراق البريد الإلكتروني الشخصي للمذكور، ومن ثَمّ تمّ نشر صوره وكشف أسراره في موقعهم على الإنترنت حيث خصصّوا صفحة خاصة للتشهير به، وعنوانها على الشبكة هو : **http://216.169.120.174/hijazi.htm** (موقع منتدى الفوائد،١٤٢١هـ).

وحوادث التشهير والقذف في شبكة الإنترنت كثيرة، فقد وجد ضعفاء النفوس في شبكة الإنترنت، وفي ظل غياب الضوابط النظامية والجهات المسؤولة عن متابعة السلبيات التي تحدث أثناء استخدام الإنترنت، متنفساً لأحقادهم ومرتعاً لشهواتهم المريضة دون رادع، أو خوف من المحاسبة، وقد قيل قديما "من أمن العقوبة أساء الأدب".

والقذف مُجَّرم شرعاً، ونظرا لشناعة الجرم ومدى تأثيره السلبي على المجني عليه وعلى المجتمع لكونه يساعد على إشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعل عقوبته من الحدود التي لا يملك أحد حق التنازل عنه، ولا يجوز العفو عنها بعد طلب المخاصمة أمام القضاء،كما جعلها عقوبة ذات شقين، الأول عقوبة بدنية بجلده ثمانين جلدة لقوله تعالى في سورة النور﴿ وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً (٤) ﴾، والشق الثاني عقوبة معنوية بعدم قبول شهادة الجاني بعد ثبوت جلده لقوله تعالى في الآية نفسها: ﴿ وَلاَ تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمْ الْفَاسِقُونَ (٤) ﴾، وشدّد رسول الله صلى الله عليه وسلم في جريمة القذف، حيث اعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفّق عليه "اجتنبوا السبع الموبقات، قالوا يا رسول الله، وما هن؟ قال الشرك بالله، والسحر، وقتل النفس التي حرّم الله إلا بالحق، وأكل الربا، وأكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات". ولا تعاقب الشريعة على القذف إلاّ إذا كان كذباً واختلاقاً فإنْ كان حقيقةً واقعية فلا جريمة ولا عقوبة (عودة، ١٤٠١هـ: ٦٤٥-٦٤٦؛ فرحات، ١٤٠٤هـ : ١٥١-١٦٤).

٣. استخدام البروكسي للدخول إلى المواقع المحجوبة:

البروكسي هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحّد، والمعنى المتعارف عليه لدي مستخدمي الإنترنت للبروكسي هو ما يستخدم لدخول المواقع المحجوبة، وهو ما نقصده في هذه الدراسة، حيث يستخدم البروكسي من قبل مستخدمي الإنترنت في المجتمع السعودي لدخول المواقع المحجوبة من قبل مدينة الملك عبدالعزيز للعلوم والتقنية، وهذه المواقع تكون محجوبة إمّا لأنّها مواقع جنسيّة، أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية التي تنشر إحصائيات عن الجرائم أو بعض المواقع العادية، ويعود ذلك للآلية التي تتمّ بها عملية ترشيح المواقع، وربمّا لخطأ بشري في حجب موقع غير مطلوب حجبه، ولذلك فقد تجد من يستخدم البروكسي للدخول إلى موقع علمي أو موقع عادي حجب خطأً، وهذا في حكم النادر، والشاذ لا حكم له، في حين أنّ الغالبيةَ العظمى تستخدم البروكسي للدخول إلى المواقع الجنسيّة، أو المواقع السياسية ولكن بدرجة أقلّ.

ومن هنا فاستعمال البروكسي للدخول إلى المواقع المحجوبة يعتبر أمراً مخالفاً للنظام الذي أقرّ حجب تلك المواقع، حتى لو افترضنا جدلاً أنّ هناك نسبة بسيطة جداً قد تستخدم البروكسي للدخول إلى المواقع التي قد تكون حجبت بطريق الخطأ، إلا أنّ هذه النسبة سواء من الأفراد أو من المواقع التي تحجب بالخطأ تكاد لا تذكر وهي في حكم الشاذ، أضف إلى ذلك أنّه يُفترض في المواطن والمقيم احترام النظام والتقيّد به وعدم تجاوزه لأي مبرر حتى وإنْ شاب النظام خلل أثناء تنفيذه، فَفَتْحُ مثل هذه الثغرة والسماح للأفراد بتجاوز التعليمات التي أقرّها النظام لمبرر قد يكون واهياً أو لخطأ قد يكون واكب تنفيذ أمر فيه من الخطورة الشيء العظيم حيث سيجرئ الأفراد على تجاوز النظام لأيّ مبررّ، وتعمّ الفوضى وتسود الجريمة.

هذا من ناحية مخالفة استخدام البروكسي للنظام، أمّا من ناحية مخالفة استخدام البروكسي للشرع فهو من شقيين :

أ- أنّ النظام أُقِرَّ من ولي الأمر، و مخالفة ولي الأمر من المحظورات الشرعية، ما دامت تلك الأنظمة لا تخرج عن تعاليم الشرع، والدليل على ذلك قوله تعالى في سورة النساء ﴿ يَا أَيُّهَا الَّذِينَ ءامَنُوا أَطِيعُوا اللَّهَ وَأَطِيعُوا الرَّسُولَ وَأُولِي الْأَمْرِ مِنْكُمْ(٥٩) ﴾، وقوله صلى الله عليه وسلم في الحديث الذي روي في المعجم الكبير " يا أيها الناس اتقوا الله واسمعوا وأطيعوا لمن كان عليكم، وإنْ عبداً حبشياً مجدعاً، فاسمعوا وأطيعوا ما أقام فيكم كتاب الله" وفي الحديث الذي رواه أحمد في مسنده " قد تركتكم على البيضاء ليلها كنهارها، لا يزيغ عنها بعدي إلا هالك، ومن يعش منكم فسيرى اختلافاً كثيراً، فعليكم بما عرفتم من سنتي و سنة الخلفاء الراشدين المهديين، و عليكم بالطاعة وإن عبداً حبشياً عضُّوا عليها بالنواجذ ، فإنما المؤمن كالجمل الآنف حيثما انقيد انقاد".

ب- إذا كانت مشاهدة المواقع الجنسيّة حراماً، فإنّ استخدام البروكسي للدخول إلى تلك المواقع حرامٌ أيضاً، فما بني على باطل فهو باطل، والفعل إذا كان محرّماً فإنّ الوسيلة الموصلة إليه تكون محرّمة. وتنطبق هنا قاعدة سد الذرائع أي "دفع الوسائل التي تؤدي إلى المفاسد، والأخذ بالوسائل التي تؤدي إلى المصالح" (أبوزهرة، ١٩٧٦م : ٢٢٦)، كما أنّه "من المقرر فقهياً أنّ دفع المفاسد مقدّم على جلب المصالح" (أبوزهرة، ١٩٧٦م : ٢٢٨).

٤. *إخفاء الشخصية:*

توجد الكثير من البرامج التي تمكّن المستخدم من إخفاء شخصيته، سواء أثناء إرسال البريد أو أثناء تصفح المواقع. ولا شك أنّ أغلب من يستخدم هذه البرامج هدفهم غير نبيل، فهم يسعون من خلالها إلى إخفاء شخصيتهم خوفاً من مسائلة نظامية، أو خجلاً من تصرّف غير لائق يقومون به. ومن الأمور المسلّم بها شرعاً وعرفاً أنّ الأفعال الطيبة لا يخجل منها الأشخاص بل يسعون عادة -إلا في حالات معينة- إلى الإعلان عنها والافتخار بها، أمّا الأفعال المشينة فيحرص الغالبية على إخفائها. وإخفاء الشخصية غالباً أمر مشين وتهرّب من المسؤولية التي قد تلحق بالشخص متى ما عُرفت شخصيته، ولعلّ ما يدلّ على ذلك حديث رسول الله صلى الله عليه وسلم الذي رواه مسلم في صحيحه "البِرُّ حسنُ الخُلُق، والإثمُ ماحاكَ في صدرِك وكَرِهْتَ أن يطّلعَ عليه الناسُ".

٥. انتحال الشخصية:

وهي تنقسم إلى قسمين:

أ- انتحال شخصية الفرد :

تُعدّ جرائم انتحال شخصية الآخرين من الجرائم القديمة، إلاّ أنّ التنامي المتزايد لشبكة الإنترنت أعطى المجرمين قدرةً أكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تداعب عادةً غريزة الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلاً إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وهذا يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهّم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من أنّ مثل هذا الإعلان يمثّل عملية نصب واحتيال واضحة، إلا أنّه ليس من المستبعد أن يقع ضحيته الكثير من مستخدمي الإنترنت. ويمكن أن تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الإساءة إلى سمعة الضحية (داود، ١٤٢٠هـ: ٨٤-٨٩).

ب- انتحال شخصية المواقع :

ومع أنّ هذا الأسلوب يعدّ حديثاً نسبياً، إلاّ أنّه أشدّ خطورةً، وأكثر صعوبةً في اكتشافه، من انتحال شخصية الأفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الآمن (Secured Server). حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثَمّ يقوم بتحويله كموقع بيني، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين، ثُمّ يقوم بتركيب البرنامج الخاص به هناك، مما يؤدي إلى توجّه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع أن يكثر استخدام أسلوب انتحال شخصية المواقع في المستقبل، نظراً لصعوبة اكتشافها(داود، ١٤٢٠هـ:٨٩-٩٣).

والمحاذير الأمنية والمخالفات النظامية والشرعية واضحة في هذه الفقرة، سواءً ما كان منها قاصراً على انتحال شخصية الأفراد أو المواقع، فقد حفظت الشريعة السماوية والأنظمة الوضعية الحقوق الشخصية وصانت الملكيات الفردية، وجُعل التعدي عليها أمراً محظوراً شرعياً ومعاقباً عليه جنائياً.

وفي انتحال شخصية الآخرين تعدٍّ صارخ على حقوقهم وانتهاكاً لملكياتهم التي صانها الشرع لهم، كما أنّه يترتب على انتحال شخصية الآخرين أضرارٌ متنوعة قد تلحق بهم، وتتفاوت هذه الأضرار بتفاوت نتيجة الفعل، فقد تقتصر على أضرار معنوية كتشويه سمعة الشخص، وقد تصل إلى أضرار مادية كالاستيلاء غير المشروع على ممتلكات ومقتنيات مادية للمجني عليه.

ومهما كان حجم هذه الأضرار الناتجة عن هذا الفعل غير النظامي، فإنّ المجني عليه لا بدّ أنْ يتضرر من هذا الفعل، وخاصة أنّ الهدف الغالب من انتحال الشخصية لن يكون حميداً، ولن يكون بحسن نية، أو لخدمة شخص آخر خلاف منتحل الشخصية.

وتتّفق الشريعة مع القوانين الوضعية في جعل الإنسان مسؤولاً عن كل فعل ضارّ بغيره، سواء اعتبر القانون ذلك الفعل جريمة أم لم يعتبره (عودة، ١٤٠١هـ :٧٧)، ولا شكّ أنّ انتحال شخصية الأفراد أو المواقع مضرّ بأصحابها الأساسيين، ولذلك فهي جريمة قانونية ومخالفة شرعية

ثانيا: جرائم الاختراقات:

يشمل هذا القسم جرائم تدمير المواقع، واختراق المواقع الرسمية أو الشخصية، واختراق الأجهزة الشخصية، واختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه، أو إغراقه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية، و إرسال الفيروسات والتروجنات.

ولعلّ جميعَ هذه الجرائم والأفعال مع اختلافها يجمعها أمر واحد، وهو كونها جميعاً تبدأ بانتهاك خصوصية الشخص، فضلاً عن إلحاق الضرر المادي والمعنوي بالمجني عليهم، وهذا سببٌ كافٍ لتجريمها.

وتتّفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوصية الفرد، ويعدّ مجرّد التطفّل على تلك المعلومات، سواءً كانت مخزنّة في الحاسب الآلي، أو في بريده الإلكتروني، أو في أي مكان آخر، انتهاكاً لخصوصيته الفردية ولحقوقه.

ومن المعلوم "أنّ الفقهاء يقسّمون الحقوق، إلى حقوق لله، وحقوق للأفراد، إلا أنّ الكثيرين منهم يرون –بحقّ– أنّ كل ما يمس حقَّ الجماعة الخالص أو حقّ الأفراد الخالص يعتبر حقّاً لله تعالى، أي من حقوق الجماعة ونظامها" (عودة، ١٤٠١هـ :٢٠٦)، ومن هنا يعدّ التعدي على حقوق الأفراد وانتهاك خصوصياتهم الشخصية مخالفة شرعية وجريمة نظامية، لأنّه يعدّ شرعاً تعدّياً على حقّ الله.

وقد أدى انتشار الإنترنت إلى تعرّض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية سواء عمداً أو مصادفةً، فبكّل بساطة ما أنْ يزور مستخدم الإنترنت أيّ موقع على شبكة الإنترنت حتى يقوم ذلك الموقع بإصدار نسختين من الكعكة الخاصة بأجهزتهم (Cookies) وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة أسباب، لعلّ منها التعرف على من يكرّر الزيارة للموقع أو لأسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم، والأخرى يتمّ تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات دون أن يشعر صاحب الجهاز بذلك أو حتى يستئذن منه! وفوراً يتم إصدار رقم خاص ليميّز ذلك الزائر عن غيره من الزوار، وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وإرسالها إلى مصدرها أو إحدى شركات جمع وتحليل المعلومات، وهي عادةً ما تكون شركات دعاية وإعلان، وكلّما قام ذلك الشخص بزيارة الموقع يتم إرسال المعلومات وتجديد النسخة الموجودة لديهم، ويقوم المتصفّح لديه بعمل المهمة المطلوبة منه مالم يقم صاحب الجهاز بتعديل وضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة أو بأخرى. كما قد يحصل أصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعاً حيث يكون الشخص عادة أقلّ تردّداً عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي، بعكس ما لو كان الذي يتعامل معه إنساناً آخرَ (موقع مجلة الأمن الإلكترونية، ١٤٢١هـ ؛ داود،١٤٢٠هـ: ٥٠- ٥٢).

هذا وإنْ كانت هناك وسائل لحماية الخصوصية أثناء تصفح الإنترنت، إلاّ أنّه "من الصعب جداً السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي)، وعلى ذلك فإنّ حماية الخصوصية يجب أنْ تبدأ من البداية، بتحديد نوعية البيانات التي لا ينبغي أنْ تصبح عامة ومشاعة، ثُمّ بتقييد الوصول إلى تلك المعلومات"(داود،١٤٢٠هـ:٥٣).

يتّضح من كلّ ما تقّدم أنّ هذه الأفعال غير شرعية وغير أخلاقية، ولا تتمشى مع تعاليم ديننا الحنيف الذي حرص على احترام الحقوق الشخصية وحفظ الملكية الفردية، وراعى خصوصية الأفراد والجماعات، بل اعتبر التعدي على الحقوق الشخصية تعدياً على حقوق الله، مما يعنى أنّها أفعال إجرامية وتصرفات لا أخلاقية، يعاقب عليها الشرع بعقوبات تختلف بحسب نوع الفعل المرتكب، وبحسب الضرر الواقع على المجني عليه، وقد يدخل الفعل وعقوبته تحت جرائم الحدود، أو القصاص، أو التعازير. وليس المجال هنا مجال تفصيل لهذه الأنواع بقدر ما هو مجال تحديد وإيضاح أنّ هذه الأفعال مجرّمة وأنّ هناك عقوبة شرعية بحقّ من يرتكب هذه الأفعال.

وقد أجملت إيضاح التكييف الشرعي والنظامي لهذه الأفعال لأنّها متشابهة ومتداخلة إلى حدٍ كبير، إلاّ أنّه ونظراً لخطورتها وشيوعها فيلزم الأمر التطّرق وبشيء من التفصيل إلى شرح فني لهذه الأفعال وأضرارها، لعلّه يضيف بعداً آخر يساهم وبوضوح أكثر في التَعَّرُفِ على كونها مجرَّمة، وهذه الأفعال هي:

١. الاقتحام أو التسلل :

يشمل هذا البند جرائم الاختراقات، سواء للمواقع الرسمية، أو الشخصية، أو اختراق الأجهزة الشخصية، واختراق البريد الإلكتروني، أو الاستيلاء عليه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية. وهي أفعال أصبحت تنشر يومياً في الصحف والأخبار فكثيراً ما " تتداول الصحف والدوريات العلمية الآن أنباءً كثيرة عن الاختراقات الأمنية المتعددة في أماكن كثيرة من العالم ليس آخرها اختراق أجهزة الحاسب (الآلي) في البنتاجون (وزارة الدفاع الأمريكية)" (داود، ١٤٢٠هـ: ٩٩).

ولكي يتم الاختراق فإنّ المتسللين إلى أجهزة الآخرين يستخدمون ما يعرف بحصان طروادة وهو برنامج صغير يتمّ تشغيله داخل جهاز الحاسب، لكي يقوم بأغراض التجسس على الحاسوب الشخصي، فهو ببساطة يقوم بتسجيل كلّ طرقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل، ويشمل ذلك كلّ بياناته السرية، أو حساباته المالية، أو محادثاته الخاصة على الإنترنت، أو رقم بطاقة الائتمان الخاصة به، أو حتى كلمات المرور التي يستخدمها لدخول الإنترنت، والتي قد يتم استخدامها بعد ذلك 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 تعرضّت لهذا النوع من الجرائم في الولايات المتحدة مثلاً كلٌ من وزارة العدل والمخابرات المركزية والقوّات الجوية، وكذا حزب العمّال البريطاني"(داود، ١٤٢٠هـ:٨٣).

وقد قام قراصنة إسرائيليون باقتحام صفحة الإنترنت الإعلامية الخاصة ببنك فلسطين المحدود، ووضعوا بها صوراً وشعارات معادية، مما اضطّر البنك إلى إلغاء الصفحة ومحوها كلياً، كما تعرضت العديد من الشركات الخاصة في مناطق الحكم الذاتي للهجوم والعبث، ومنها شركة اقتحم المتسللون أجهزتها ووضعوا صورة زوجة مدير الشركة وهي عارية بعد تجريدها من الملابس بواسطة الحاسب الآلي (أبوشامة، ١٤٢٠هـ: ٣٧).

كما قام بعض المخترقين فجر الثلاثاء الموافق ١٤٢٣/١٠/٦هـ بتخريب أجزاء من موقع مدينة الملك عبدالعزيز للعلوم والتقنية بالمملكة، واستبدال صفحة الحجب التي تظهر لكلّ من يحاول الدخول لموقع محجوب من قبل المدينة، بصورة إباحية فاضحة (موقع صحيفة الرياض، ١٤٢٣/١٠/١٠هـ).

وفي عام (١٩٩٧م) قدّرَتْ وكالة المباحث الفدرالية الأمريكية (FBI) تعرّض (٤٣٪) من الشركات التي تستخدم خدمة الإنترنت لمحاولة تسلل تتراوح مابين (١-٥) مرات خلال سنة واحدة (Wilson,2000)، ولا يقتصر التسلّل على المحترفين فقط بل إنّهم قد يكونون من الهواة أيضاً، حيث يدفعهم إلى ذلك الفراغ ومحاولة شغل الوقت، كما حدث مع مراهقة في الخامسة عشرة من عمرها، قامت بمحاولة التسلل إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة، لأنّها لاتميل لمشاهدة التلفاز، لذلك فكرّت أنّ تكون متسللة (Hacker) (Koerner,1999).

وهذا ما اتّضح أيضاً لوكالة المباحث الفدرالية (FBI) أثناء حرب الخليج الأولى، عندما أجروا تحقيقاً حول تسلل أشخاص إلى الصفحة العنكبوتية الخاصة بإحدى القواعد العسكرية الأمريكية، وكانت الشكوك قد اتجهت في البداية إلى إرهابيين دوليين، إلا أنّ الحقيقة تجلّت بعد ذلك في أنّ المتسللين هما مراهقان كانا يعبثان بجهاز الحاسب الآلي في منزلهما (Wilson,2000).

وفي عام (١٩٩٧م) قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماسيتيوسش (Massachusetts) مما أدى إلى تعطيل نظام الملاحة الجوية، وأنظمة حيوية أخرى لمدة ست ساعات، وبالرغم من فداحة الضرر الذي تسبب فيه، إلاّ أنّ عقوبته اقتصرت على وضعه تحت الرقابة لمدة سنتين مع إلزامه بأداء خدمة للمجتمع لمدة (٢٥٠) مائتين وخمسين يوماً (Wilson,2000)، وبهذا فإنّ القانون الأمريكي يلعب دوراً غير مباشر في تشجيع المراهقين على أعمال التسلّل لندرة عقاب المتسللين دون سن الثامنة عشرة، كما يساهم أولياء أمور المراهقين في ذلك أيضاً حيث يعدّون أبناءهم أذكياء إذا مارسوا أنشطة حاسوبية تتعلق بالتسلل إلى أجهزة الآخرين (Koerner,1999).

وأوضحت دراسة أجريت على (٥٨١) خمسائة وواحد وثمانين طالباً جامعياً أمريكياً، أنّ (٥٠٪) منهم اشترك بأعمال غير نظامية أثناء استخدام الإنترنت ذلك العام، وأنّ (٤٧) سبعة وأربعين طالباً أو ما نسبته (٧,٣٪) سبق وقبض عليه في جرائم تتعلق بالحاسب الآلي، وأنّ (٧٥) خمسة وسبعين طالباً أو ما نسبته (١٣,٣٪) قبض على أصدقائهم في جرائم تتعلق بالحاسب الآلي (Skinner & Fream, 1997).

فالعقوبات الحالية لا تساعد على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسب الآلي، ففي خلال عام واحد تضاعفت تلك الجرائم على مستوى الولايات المتحدة الأمريكية،وفي عام (١٩٩٩م) تحرّت وكالة المباحث الفدرالية (FBI) عن (٨٠٠) ثماني مائة حالة تتعلق بالتسلل (Hacking)، وهو ضعف عدد الحوادث التي قامت بالتحري عنها في العام السابق أي عام (١٩٩٨م)، أمّا الهجوم على شبكات الحاسب الآلي على الإنترنت فقد تضاعف (٣٠٠٪) في ذلك العام أيضاً (Koerner,1999).

وللحدّ من تزايد عمليات التسلل (Hacking)، ونظراً لأنّ المتسللين عادة يطوّرون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة، فقد اضطّر مسؤولو أمن الحاسبات الآلية، وشبكات الإنترنت، ورجال الأمن، الاستعانة بخبرات بعض محترفي التسلل، ليستطيعوا تطوير نظم الحماية ضد المتسللين (Hackers)، وعلى سبيل المثال يرسل مسؤولو أمن الحاسبات أسئلة تتعلق بأحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف باسم (hacker internet chat room) ولطلب نصائح تقنية حول أحدث سبل الحماية (Staff, 2000, February 17).

بلْ إنّ وكالة المباحث الفدرالية (FBI) استعانت أيضاً بخبراء في التسلل (Hackers) لتدريب منسوبي الوكالة على طرق التسلل (Hacking) لتنمية خبراتهم وقدراتهم في هذا المجال، وليستطيعوا مواكبة خبرات وقدرات المتخصصين والمحترفين من المتسللين (Hackers)، ومنهم أحد أشهر المتسللين (Hackers) ويدعى (Brian Martin) والمشهور باسم (Jericho) والمتّهم بالتسلل والعبث بمحتويات الصفحة الرئيسية لصحيفة (New York Times) على شبكة الإنترنت (Staff, 2000 April).

وأكدّت وحدة الخدمات السرية الأمريكية (The US Secret Service) أنّ الجرائم المنظّمة تتجه نحو استغلال التسلل (Hacking) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية (Thomas,2000).

وأوضح خبر نشرته صحيفة لوس انجلوس تايمز أنّ متسللين قاموا باقتحام نظام الحاسب الآلي الذي يتحكم في تدفق أغلب الكهرباء في مختلف أنحاء ولاية كاليفورنيا الأمريكية (موقع أرابيا،١٠/٦/٢٠٠١م).

٢. الإغراق بالرسائل :

يلجأ بعض الأشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني لشخص ما، بقصد الإضرار به، حيث يؤدي ذلك إلى تعطّل الشبكة، وعدم إمكانية استقبال أيّ رسائل فضلاً عن إمكانية انقطاع الخدمة، وخاصة إذا كانت الجهة المتضررة من ذلك هي مقدمة خدمة الإنترنت مثلاً، حيث يتم ملء منافذ الاتصال (Communication-Ports) وكذلك قوائم الانتظار (Queues) مما ينتج عنه انقطاع الخدمة، وبالتالي تكبّد خسائر مادية ومعنوية غير محدودة، ولذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفّق أعداد كبيرة منها(داود، ١٤٢٠هـ:٩٣).

وإذا كان هذا هو حال الشركات الكبيرة فلنا أنْ نتصور حال الشخص العادي إذا تعرّض بريده لمحاولة الإغراق بالرسائل، حيث لن يصمد بريده طويلاً أمام هذا السيل المنهمر من الرسائل عديمة الفائدة، أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، خاصة إذا علمنا أنّ مزود الخدمة يعطي عادة مساحة محددة للبريد لا تتجاوز عشرة ميغا كحدّ أعلى.

٣. الفيروسات الحاسب آلية :

الفيروسات الحاسب آلية هي إحدى أنواع البرامج الحاسب الآلية، إلاّ أنّ الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما، أو حتى مجرد فتح البرنامج الحامل للفيروس، أو الرسالة البريدية المرسل معها الفيروس، إصابة الجهاز به ومن ثَمّ قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. وقد عرّفها أحد خبراء الفيروسات (Fred Cohen) بأنّها نوع من البرامج التي تؤثّر في البرامج الأخرى، بحيث تعدّل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أنّ الفيروس ينسخ نفسه من حاسب آلي لحاسب آلي آخر، بحيث يتكاثر بأعداد كبيرة (Highley,1999)

ويمكن تقسيم الفيروسات إلى خمسة أنواع :

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

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

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

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز.

الخامس: يعرف بحصان طروادة، وهذا النوع يصنّفه البعض كنوع مستقّل بحد ذاته، إلاّ أنّه أدرج في هذا التقسيم كأحد أنواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي إلا أنّ أثره التدميري خطير. وتعمل الفيروسات على إخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيّر أشكالها، لذلك وجب تحديث برامج مكافحة الفيروسات بصفة دائمة (عيد،١٤١٩هـ : ٦٣-٦٦).

ويختلف الخبراء في تقسيمهم للفيروسات، فمنهم من يقسمّها على أساس المكان المستهدف بالإصابة داخل جهاز الكمبيوتر، ويرون أنّ هناك ثلاثة أنواع رئيسة من الفيروسات هي: فيروسات قطاع الإقلاع (Boot Sector) وفيروسات الملفات (File Injectors) وفيروسات الماكرو (Macro Virus). وهناك من يقسّمها إلى: فيروسات الإصابة المباشرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها، أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفة تندرج تحت هذا التقسيم، وهناك أيضاً الفيروسات المتغّيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلّل برامج مكافحة الفيروسات (موقع جريدة الجزيرة ،٢٠٠٠).

ومن الجرائم المتعلقة بإرسال فيروسات حاسوبية قيام شخص أمريكي يدعى (Robert Morris) بإرسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (١٩٨٨م) عبر الإنترنت، وقد كرّر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفيروس وأدى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) ستة آلاف ومائتي حاسبٍ آلي مرتبط بالإنترنت، وقد قدرّت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قُدّر لمصمم الفيروس تصميمه بحيث يكون أشدّ ضرراً، للحقت أضرار أخرى لا يمكن حصرها بتلك الأجهزة، وقد حُكم على المذكور بالسجن ثلاث سنوات بالرغم من دفاع المذكور عن نفسه أنّه لم يكن يقصد إحداث مثل تلك الأضرار(Morningstar, 1998).

كيف يتم اقتحام الجهاز؟

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

١. يرسل عن طريق البريد الإلكتروني باعتباره ملفاً ملحقاً حيث يقوم الشخص باستقباله وتشغيله، وقد لا يرسل وحده حيث من الممكن أن يكون ضمن برامج، أو ملفات أخرى.

٢. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة أنتجته إسرائيل.

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

٤.طريقة أخرى لتحميله، تتلخّص في مجرد كتابة كوده على الجهاز نفسه في دقائق قليلة.

٥.في حالة اتصال الجهاز بشبكة داخلية أو شبكة إنترانت.

٦.يمكن نقل الملف أيضاً بواسطة برامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

٧.كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص (Nanoart,2000).

وبصفة عامة فإن برامج القرصنة تعتمد كلياً على بروتوكول الـ (TCP/IP) وهناك أدوات (ActiveX) مصمّمه ومجهّزة لخدمة التعامل بهذا البروتوكول، ومن أشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات. ويحتاج الأمر إلى برنامجين، خادم في جهاز الضحية، وعميل في جهاز المتسلل، فيقوم الخادم بفتح منفذ محدد مسبقاً في جهاز الضحية ، في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية، حيث يتعرف برنامج الخادم (server) على إشارات البرنامج المخترق، ويتم الاتصال، ومن ثَمّ يتمّ عرض كامل محتويات جهاز الضحية عند المخترق، حيث يتمكّن من العبث بها أو الاستيلاء على ما يريد منها .

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز، وهناك ما يقارب الـ(٦٥,٠٠٠) منفذ تقريباً في كل جهاز، يميّز كلّ منفذ عن الآخر برقم خاص ولكلّ منها غرض محدد، فمثلاً المنفذ (٨٠٨٠) يخصص أحياناً لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعدّ جزءاً من الذاكرة، لها عنوان معين يتعرف عليها الجهاز بأنّها منطقة إرسال واستقبال البيانات، وكلّ ما يقوم به المتسلل هو فتح أحد هذه المنافذ للوصول لجهاز الضحية وهو ما يسمى بطريقة الزبون/الخادم (Client\Server) حيث يتمّ إرسال ملف لجهاز الضحية، يفتح المنافذ فيصبح جهاز الضحية (server)، وجهاز المتسلل (Client)، ومن ثَمّ يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج (Net Bus) أو (Net Sphere).

ولعلّ الخطورة الإضافية تكمن في أنّه عند دخول المتسلل إلى جهاز الضحية فإنّه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز، حيث يصبح ذلك الجهاز مركزاً عاماً يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ (Port scanning) عن طريق أحد البرامج المتخصصة في ذلك.

خطورة برامج حصان طروادة:

بداية تصميم هذه البرامج كان لأهداف نبيلة، كمعرفة ما يقوم به الأبناء، أو الموظفون، على جهاز الحاسب في غياب الوالدين، أو المدراء، وذلك من خلال ما يكتبونه على لوحة المفاتيح، إلا أنّه سرعان ما أسيء استخدامه. وتعدّ هذه البرامج من أخطر البرامج المستخدمه من قبل المتسللين، لأنّه يتيح للدخيل الحصول على كلمات المرور (passwords)، وبالتالي الهيمنة على الحاسب الآلي بالكامل. كما أنّ المتسلّل لن يتمّ معرفته أو ملاحظته لأنّه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة أيضاً في أنّ معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات، إضافة إلى أنّ الطبيعة الساكنة لحصان طروادة يجعلها أخطر من الفيروسات، فهي لا تقوم بتقديم نفسها للضحية مثلما يقوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج، أو الأضرار التي يقوم بها للمستخدم، وبالتالي فإنه لا يمكن الشعور بهذه الأحصنة أثناء أدائها لمهمتها التجسسية، وبالتالي فإنّ فرص اكتشافها، والقبض عليها تكاد تكون معدومة (Nanoart,2000).

أهم المنافذ المستخدمة لاختراق الجهاز:

إذن فأهمّ مورد لهذه الأحصنة هي المنافذ (Ports) التي تقوم بفتحها في جهاز الضحية ومن ثَمّ التسلل منها إلى الجهاز والعبث بمحتوياته. فما هذه المنافذ؟ سنحاول هنا التطرّق بشكل إجمالي إلى أهم المنافذ التي يمكن استخدامها من قبل المتسللين، والبرامج المستخدمة في النفاذ من هذه المنافذ :

المنفذ	اسم البرنامج
21	blade Runner , doly Trojan ,FTP Trojan , Invisible FTP , Larva ,WebEX , Win Crash
23	Tiny Telnet Server
25	Antigen , Email Password Sender , Haebu Coceda , Kauang 2 , Pro Mail trojan , Shtrilitz , Stealth , Tapirs ,Terminator , Win Pc ,Win Spy ,Kuang20.17A-0.30
31	Agent 31 , Hackers Paradise , Master Paradise
41	Deep Throat
58	DMSetup
79	Fire hotcker
80	Executor
110	Pro Mail trojan
121	Jammer Killah
421	TCP wrappers
456	Hackers Paradise

531	Rasmin
555	Ini Killer , Phase Zero , Stealth Spy
666	Attack FTP ,Satanz BackDoor
911	Dark Shadow
999	Deep Throat
1001	Silencer , WEBEX
1011 1012	Doly Trojan
1024	Net Spy
1045	Rasmin
1090	Xtreme
1095 1097 1098 1099	Rat
1170	Psyber Stream Server , Voice
1234	Ultors Trojan
1243	Back Door -G , SubSeven
1245	VooDoo Doll
1349	UPD – BO DLL
1492	FTP99CMP
1600	Shivka – Burka
1807	Spy Sender
1981	Shockrave
1999	Back Door
2001	Trojan Cow
2023	Ripper
2115	Bugs
2140	Deep Throat , The Invasor
2565	Striker
2583	Win Crash
2801	Phineas Phucker
3024	Win crash
3129	Master Paradise
3150	Deep Throat , The Invasor
3700	Portal Of Doom
4092	Win crash
4567	File Nail
4590	ICQ Trojan
5000	Bubbel , Back Door Setup , Sockets de troie
5001	Back Door Setup , Sockets de troie
5321	Fire hotcker
5400 5401 5402	Blade Runner
5555	ServeMe

5556 5557	Bo Facil
5569	Robo-Hack
5742	Win Crash
6400	The Thing
6670	Deep Throat
6711	SubSeven
6771	Deep Throat
6776	Back Door-G , SubSeven
6939	Indoctrination
6969	Gate Crasher , Priority
7300 7301 7306 7307 7308	Net Monitor
7000	Remote Grab
7789	BacK Door Setup , ICKiller
9872 9873 9874 9875 10067 10167	Portal of Doom
9989	iNi – Killer
10520	Acid Shivers
10607	Coma
11000	Senna Spy
11223	Progenic trojan
12223	Hack 99 Key Logger
12345	Gaban Bus Net busPie Bill Gates , X -bill
12346	Gaban Bus Net Bus X-bill
12361 12362	Whack – a – mole
12631	WhackJob
13000	Senna Spy
16969	Priority
20001	Millennium
20034	NetBus 2 Pro
21544	Girl Friend
22222	Prosiak
23456	Evil Ftp , Ugly FTP
26274	UPD – Delta Source
29891	UPD - The Unexplained
30029	AOL Trojan
30100 30101	NetSphere

30102	
30303	Sockets de Troie
31337	Baron Night , BO client ,Bo2 , Bo Facil UPD - BackFire , Back Orifice , DeppBo
31338 31339	NetSpy DK
31338	UPD - Back Orific , Deep BO
31666	Bo Whack
33333	Prosiak
34324	Big Gluck , TN
40412	The Spy
40421	Agent 40421 , Master Paradise
40422 40423 40426	Master Paradise
47262	UPD –Delta Source
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
54321	School Bus
60000	Deep Throat
61466	Telecommando
65000	Devil

المصدر موقع (http://www.nanoart.f2s.com/hack/ports3.htm)

ثالثا: الجرائم المالية

تشمل جرائم السطو على أرقام البطاقات الائتمانية، ولعب القمار، والتزوير، والجريمة المنظّمة، والمخدّرات، وغسيل الأموال. ولعلّ جرائم هذا القسم أوضح من ناحية كونها مُجَرَّمة، حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمّى، والتي يعرف الجميع أنّها مخالفة للنظام وللشرع، لأنّها من الجرائم التي اشتهر بمحاربتها جنائياً. ونظراً للاختلاف البسيط في تصنيف كلّ جريمة من جرائم هذا القسم، فسيتم توضيح التكييف الشرعي والقانوني لكل جريمة بشكل مفصّل.

١. جرائم السطو على أرقام البطاقات الائتمانية:

بدأ مفهوم التجارة الإلكترونية ينتشر في السبعينيات الميلادية، وذلك لسهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية، فضلاً عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل، والأهم هو إيجاد أسواق أكثر اتساعاً. ونتيجة لذلك فقد تحوّل عدد من شركات الأعمال إلى استخدام الإنترنت والاستفادة من مزايا التجارة الإلكترونية، كما تحوّل تبعاً لذلك الخطر الذي كان يهدد التجارة السابقة، ليصبح خطراً متوافقاً مع التجارة الإلكترونية.

والاستيلاء على بطاقات الائتمان عبر الإنترنت أصبح سهلا، فـــ" لصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثَمّ بيع هذه المعلومات للآخرين " (داود، ١٤٢٠هـــ: ٧٣)، وقد وقعت بالفعل عدة حوادث، ومن ذلك حادثة شـــخص ألماني قام بالدخول غير المشـــروع إلى أحد مزودي الخدمات، واستولى على أرقام بطاقات ائتمانية خاصة بالمشتركين، ومن ثَمّ هددّ مزود الخدمة بإفشاء أرقام تلك البطاقات مالم يستلم فدية، وقد تمكنت الشرطة الألمانية من القبض عليه. كما قام شـخصـان في عام (١٩٩٤م) بإنشـاء موقع على الإنترنت مخصـص لشـراء طلبات يتم بعثها فور تســديد قيمتها إلكترونياً، إلاّ أنّ الطلبات لا تصــل إطلاقاً لأنّ الموقع وهميٌّ هدفه النصب والاحتيال، وقد قبض على مؤسسيه (عبدالمطلب، ٢٠٠١م : ٨٥).

وأثبتت شبكة (MSNBC) سهولة الحصول على أرقام بطاقات الائتمان، حيث قامت بعرض قوائم تحتوي على أكثر من (٢٥٠٠) رقم بطاقة ائتمان، حصـــلت عليها من ســـبعة مواقع للتجارة الإلكترونية باســتخدام قواعد بيانات متوفرة تجارياً، ولم يكن يصــعب على أي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على أرقام تلك البطاقات واستخدامها في عمليات شـــراء يدفع قيمتها أصـــحابها الحقيقيون. وتلافياً لذلك بدأت بعض البنوك الدولية والمحلية في إصـــدار بطاقة ائتمان خاصـــة بالإنترنت يكون حدُّها الائتماني معقولاً ليقلّل من مخاطر الاستيلاء عليها (عبدالمطلب،٢٠٠١م : ٨٢– ٩٠).

ويتعدّى الأمر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان، فنحن في بداية ثورة نقدية تُعرف باسم النقود الإلكترونية (Electronic Cash)، أو (Cyber Cash)، والتي يتنبّأ لها أنْ تكون مكمّلة للنقود الورقية والبلاســـتيكية (بطاقات الائتمان)، وأنْ يزداد الاعتماد عليها والثقة بها، كما أنّ هناك الأســـهم والســـندات الإلكترونية المعمول بها في دول الاتحاد الأوروبي، والتي أقرّ الكونجرس الأمريكي التعامل بها في عام ١٩٩٠م، وبالتالي فإنّ التعامل مع هذه الأسهم والسندات الإلكترونية من خلال الإنترنت، سيواجه مخاطرَ أمنية ولا شك.

ولذلك لجأت بعض الشـــركات والبنوك إلى العمل ســـوياً لتجاوز هذه المخاطر كالاتّفاق الذي وُقّع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC)، وهي من أكبر المؤسسات المصرفية في هونج كونج، وشركة كومباك للحاسب الآلي، وذلك لتطوير أول نظام آلي آمن للتجارة الالكترونية، والذي يمنح التجّار خدمة نظام دفع آمن لتمرير عمليات الشـــراء عبر الإنترنت (داود، ١٤٢٠هـ : ١٢٣ – ١٢٤).

وجرائم السطو على أرقام البطاقات الائتمانية مُجرَّمة شرعاً وقانوناً حيث تصنّف ضمن جرائم السرقات، "فالشرع الإسلامي يرغب في المحافظة على أموال الناس وصيانتها من كل اعتداء غير مشروع بحيث يهدد الأمن والاستقرار" (فرحات،١٤٠٤هـ:٢٩).

والسرقة من الكبائر المحرّمة التي نصت الآيات القرآنية والأحاديث النبوية على تحريمها، ووضعت عقوبة رادعة لمرتكبها. قال تعالى في سورة المائدة ﴿ السَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالاً مِنْ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ (٣٨) ﴾

ولعن رسول الله صلى الله عليه وسلم السارق نظراً لشناعة فعله وعظيم جرمه، ففي الحديث الذي رواه البخاري 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 الإيمان عن السارق، فروى البخاري في صحيحه عن ابن عباس رضي الله عنهما، عن النبي صلى الله عليه وسلم، قال: " لا يزني الزاني حين يزني وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن".

٢. القمار عبر الإنترنت:

كثيراً ما تتداخل عملية غسيل الأموال مع أندية القمار المنتشرة، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الإنترنت محل اشتباه ومراقبة من قبل السلطات الأمريكية. وبالرغم من أنّ سوق القمار في أمريكا يعدّ الأسرع نمواً على الإطلاق، إلاّ أنّ المشكلة القانونية التي تواجه أصحاب مواقع القمار الافتراضية على الإنترنت أنها غير مصرّح لها حتى الآن في أمريكا، بعكس نوادي القمار الحقيقية، كالمنتشرة في لاس فيجاس وغيرها، ولذلك يلجأ بعض أصحاب تلك المواقع الافتراضية على الإنترنت إلى إنشائها وإدارتها من أماكن مجاورة لأمريكا وخاصة في جزيرة انتيجوا على الكاريبي. ويوجد على الإنترنت أكثر من ألف موقع للقمار يسمح لمرتاديه من مستخدمي الإنترنت ممارسة جميع أنواع القمار التي توفّرها المواقع الحقيقية، ومن المتوقّع أن ينفق الأمريكيون ما يزيد عن (٦٠٠) ستمائة مليار دولار سنوياً في أندية القمار، وسيكون نصيب مواقع الإنترنت منها حوالي مليار دولار. وقد حاول المشّرعون الأمريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت، ويسمح بملاحقة الذين يستخدمون المقامرة السلكية أو الذين يروجّون لها، سواء أكانت هذه المواقع في أمريكا أم خارجها (عبدالمطلب، ٢٠٠١م : ٧٨ – ٨٢).

هذا هو حال القمار ونظرة القوانين الوضعية له، ولكن ما هي نظرة الشرع له؟ وهل يوجد في تعاليم الدين الإسلامي ما يُجرّم لعب القمار ويجعله من الأفعال المحرّمة شرعاً، والمعاقب عليه قانوناً؟

ينظر الإسلام إلى القمار باعتباره محظوراً شرعياً منهياً عن فعله ومعاقباً على ارتكابه، وقد وردت أدلة متعددة في كتاب الله عزّ وجلّ وفي كتب الأحاديث، أمّا دليل تحريم القمار من القرآن فهو قوله تعالى في سورة المائدة ﴿ يَاأَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالأَنْصَابُ وَالأَزْلاَمُ رِجْسٌ مِنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ (٩٠) ﴾.

ولم يكتف الشرع بالنهي عن هذا الفعل، بلْ وضّح لأتباعه أنّ هذا العمل إنمّا هو من أعمال الشيطان، التي يسعى من خلالها إلى إيقاع العداوة والبغضاء بين الناس، ووضّح أنّ في اجتاب هذا الفعل فلاحاً وصلاحاً وفوزاً في الدنيا والآخرة، قال تعالى في سورة المائدة ﴿ إِنَّمَا يُرِيدُ الشَّيْطَانُ أَنْ يُوقِعَ بَيْنَكُمْ العداوة وَالْبَغْضَاءَ فِي الْخَمْرِ وَالْمَيْسِرِ وَيَصُدَّكُمْ عَنْ ذِكْرِ اللَّهِ وَعَنْ الصَّلاَةِ فَهَلْ أَنْتُمْ مُنتَهُونَ (٩١) ﴾.

واتّفق المفسّرون على أنّ الميسر هو القمار، فورد توضيح كلمة الميسر في تفسير الجلالين بأنهّا القمار، أمّا ابن كثير فقد أورد في تفسيره لهذه الآية، حديثاً رواه أحمد في مسنده عن أبي هريرة رضي الله عنه أنّ أمير المؤمنين عمر بن الخطاب رضي الله عنه فسَّر الميسر هنا بالقمار (ابن كثير، ١٤٠٨هـ)، كما ورد تفسير كلمة الميسر أيضاً في فتح القدير بأنها قمار العرب بالأزلام، وكذلك أكد تفسير البغوي بأنّ المراد بالميسر هو القمار (البغوي، ١٤٠٩هـ)، أمّا البيضاوي فقد وضّح أنّ الميسر سمي به القمار لأنه أخذ مال الغير بيسر(البيضاوي، بدون).

وفي كتب الحديث ورد ذكر القمار أيضاً، فورد في مصنف ابن أبي شيبة عن وكيع، قال "حدثنا حماد بن نجيح قال: رأيت ابن سيرين مرّ على غلمان يوم العيد المربد و هم يتقامرون بالجوز، فقال: يا غلمان! لا تقامروا فإن القمار من الميسر"، كما أورد في مصنفه أيضاً عن ابن سيرين قال: "كل شيء فيه قمار فهو من الميسر"، وفيه أيضاً عن عبد الله بن عمرو قال: "من لعب بالنرد قماراً كان كآكل لحم الخنزير، ومن لعب بها من غير قمار كان كالمدهن بودك الخنزير" (ابن أبي شيبة، ١٣٨٦هـ). كما أخبر عبد الرزاق في مصنفه عن معمر عن ليث عن مجاهد قال: "الميسر القمار كله، حتى الجوز الذي يلعب به الصبيان" (بن همّام، بدون).

٣. تزوير البيانات:

تعدّ من أكثر جرائم نظم المعلومات انتشـــاراً، فلا تكـاد تخلو جريمة من جرائم نظم المعلومات من شـــكل من أشـــكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات، وتعديل البيانات الموجودة بها، أو إضـافة معلومات مغلوطة بهدف الاسـتفادة غير المشـــروعة من ذلك. وقد وقعت حادثة في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السـيارات، وبناء على اتفاقية مسـبقة، بتغيير ملكية السـيارات المسـجلة في الحاسـب الآلي بحيث تصـبح باسـم أحد لصـوص السـيارات والذي يعمد إلى سـرقة السـيارة وبيعها، وعندما يتقدم مالك السيارة للإبلاغ يتّضح عدم وجود سجلات للسيارة باسمه وبعد بيع السـيارة تقوم تلك الفتاة بإعادة تسـجيل السـيارة باسـم مالكها، وكانت تتقاضـي مقابل ذلك مبلغ مائة دولار واســـتمرت في عملها هذا إلى أن قبض عليها، وفي حادثة أخرى قام مشـرف تشـغيل الحاسـب بأحد البنوك الأمريكية بعملية تزوير حسـابات أصـدقائه في البنك بحيث تزيد أرصـدتهم، ومن ثَمّ يتم سـحب تلك المبالغ من قبل أصـدقائه، وقد نجح في ذلك، وكان ينوى التوقف قبل موعد المراجعة الدورية لحســابات البنك إلاّ أنّ طمع أصــدقائه أجبره على الاستمرار إلى أن قبض عليه (داود، ١٤٢٠هـ :٤٥- ٤٧).

ومما لاشك فيه أنّ البدء التدريجي في التحول إلى الحكومات الإلكترونية، سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سـترتبط الكثير من الشـركات والبنوك بالإنترنت، مما يسـهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة، وتزوير البيانات، لخدمة أهدافهم الإجرامية.

وجرائم التزوير ليســـت بالجرائم الحديثة، ولذا فإنه لا تخلو الأنظمة من قوانين واضـــحة لمكافحتها والتعامل معها جنائيا وقضائيا و" تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها" (داود ، ١٤٢١هـ : ٦٧).

وعالجت أنظمة المملكة العربية السـعودية جرائم التزوير بشـكل مفصّـل، حيث صـدر المرسوم الملكي رقم (١١٤) وتاريخ ١٣٨٠/١١/٢٦هـ بالمصادقة على نظام مكافحة التزوير، ومن ثَمّ تمّ التعديل على هذا النظام ليواكب المسـتجدات وذلك بالمرسـوم الملكي رقم (٥٣) وتاريخ ١٣٨٢/١١/٥هـ،كما صدر نظام جزائي خاص بتزوير وتقليد النقود وذلك بالمرسوم الملكي رقم (١٢) وتاريخ١٣٧٩/٧/٢٠هـ(موقع السوق الخليجي، ١٤٢٣هـ).

٤. الجرائم المنظمة*:

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصـــابات المافيا لأنّها من أشـــهر المؤسسـات الإجرامية المنظمة، والتي بادرت بالأخذ بوسـائل التقنية الحديثة سـواء في تنظيم أو تنفيذ أعمالها، ومن ذلك إنشـاء مواقع خاصـة بها على شـبكة الإنترنت لمسـاعدتها في إدارة العمليات، وتلقي المراسـلات، واصـطياد الضـحايا، وتوسـيع أعمالها، وغسـيل الأموال، كما تسـتخدم تلك المواقع في إنشـاء مواقع افتراضـية تسـاعد المنظمة في تجاوز قوانين بلد محدد، بحيث تعمل في بلد آخر يسمح بتلك الأنشطة.

ويوجد على الشـبكة (٢١٠) مائتين وعشـرة موقع، يحتوي اسـم نطاقها على كلمة مافيا، كما وجد بالشـبكة (٤) أربعة مواقع للمافيا اليهودية. وقد خُصّـص بعض هذه المواقع للأعضـاء فقط ولم يسـمح لغيرهم بتصـفح تلك المواقع، في حين سمحت بعض المواقع للعامة بتصـفح الموقع، وقامت مواقع أخرى بوضـع اسـتمارة تسـجيل لمن يرغب في الانضـمام إلى العصابة من الأعضاء الجدد (الجنيدي (أ)، ١٩٩٩م : ٣٦).

والجريمة المنظمة ليسـت وليدة التقدم التقني وإن كانت اسـتفادت كثيراً منه، فـــ" الجريمة المنظمة وبسـبب تقدم وسـائل الاتصـال والتكنولوجيا والعولمة أصـبحت غير محدّدة لا بقيود الزمان ولا بقيود المكان، وإنمّا أصـبح انتشـارها على نطاق واسـع وكبير وأصـبحت لا تحدّها الحدود الجغرافية"(اليوسف، ١٤٢٠هـــ ، ص : ٢٠١)، كما اسـتغلّت عصـابات الجريمة المنظمة " الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية، وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة " (حبوش،١٤٢٠هـ: ٢٥٣).

وهناك من يرى أنّ الجريمة المنظمة والإرهاب هما وجهان لعملة واحدة، فأوجه التشـــابه بينهما كبير حيث يسـعى كلاهما إلى إفشـاء الرعب والخوف، كما أنهما يتفقان في أسـلوب العمل والتنظيم، وقد يكون أعضاء المنظمات الإرهابية هم أساساً أعضاءً في عصابات الجرائم المنظمة حيث يسـعون للاسـتفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صـلة وتعاون وثيق بينهما(عزالدين، ١٤١٤هـ : ٢٣- ٣٥).

وحظيت مكافحة الجريمة المنظمة باهتمام دولي بدأ بمؤتمر الأمم المتحدة السـابع عام (١٩٨٥م) لمنع الجريمة، حيث اعتمد خطة عمل ميلانو التي أوصـت بعدة توصـيات حيال التعامل مع الجريمة المنظمة والقضاء عليها.

---

* للمزيد ارجع إلى كتاب الإجرام المعاصر للدكتور محمد فتحي عيد، (ص ٧٧- ١٣١).

وتبع ذلك الاجتماع الأقاليمي التحضيري عام (١٩٨٨م) الذي أقر فيه المبادئ التوجيهية لمنع الجريمة المنظمة ومكافحتها، ثُمّ المؤتمر الثامن لمنع الجريمة بفنزويلا عام (١٩٩٠م)، فالمؤتمر الوزاري العالمي المعني بالجريمة المنظمة عبر الوطنية في نابولي بإيطاليا عام (١٩٩٤م)، والذي عبّر عن إرادة المجتمع الدولي بتعزيز التعاون الدولي وإعطاء أولوية عليا لمكافحة الجريمة المنظمة.

ووضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الإرهاب، والتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة، وفي عام (١٩٩٦م) وافق المجلس في دورته الثالثة عشرة على مدونة سلوك طوعية لمكافحة الإرهاب، ووافق في عام (١٩٩٧م) وفي الدورة الرابعة عشرة على استراتيجية عربية لمكافحة الإرهاب، وفي عام (١٩٩٨م) تمّ إقرار الاتفاقية العربية لمكافحة الإرهاب من قبل مجلس وزراء الداخلية والعدل العرب (عيد، ١٤١٩هـ :٧٧-١٩٤).

٤. تجارة المخدرات عبر الإنترنت:

يحذّر أولياء الأمور أبناءهم من رفقاء السوء خشية تأثيرهم السيء عليهم، وخاصة في تعريفهم على المخدرات. فالصاحب ساحب كما يقال، وهذا صحيح ولا غبار عليه، ولكن وفي عصر الإنترنت أُضيف إلى أولياء الأمور مخاوف جديدة لا تقتصر على رفقاء السوء فقط، بل يمكن أنْ يضاف إليها مواقع السوء - إن صح التعبير- ومن تلك المواقع طبعاً المواقع المنتشرة في الإنترنت، والتي لا تتعلق بترويج المخدرات وتشويق النشء لاستخدامها فقط، بل تتعداه إلى تعليمهم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة.

والأمر هنا لا يحتاج إلى رفاق سوء، لأنّه يُمْكِنْ للمراهق الانزواء في غرفته، والدخول إلى أيّ من هذه المواقع ومن ثَمّ تطبيق ما يقرأه، ويؤكّد هذه المخاوف أحد الخبراء التربويين في بتسبيرج بالولايات المتحدة، الذي أكدّ أنّ ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والإنترنت. ولا تقتصر ثقافة المخدرات على تلك المواقع فقط، بل تساهم المنتديات وغرف الدردشة في ذلك أيضاً. وبالرغم من انتشار المواقع الخاصة بترويج المخدرات وتعليم كيفية صنعها، إلا أنّ هذه المواقع لم تدق جرس الإنذار بعد، ولم يُهتم بآثارها السلبية وخاصة على النشء كما فعلته المواقع الإباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة.

وقد اعترف الناطق الرسمي للتحالف المناهض للمخدرات بأنهم خسـروا الجولة الأولى في ساحة الإنترنت، حيث لم ينطلق موقعهم الخاص على الشبكة http://www.cadca.orgإلا منذ عامين فقط. وبالإضـافة إلى هذا الموقع توجد مواقع أخرى تحارب المخدرات وتسـاعد المدمنين على تجاوز محنتهم، ومن ذلك الموقع الخاص بجماعة (Join-Together) وعنوانهم على الإنترنت هو http://192.12.191.21 إلاّ أنّ هذه المواقع قليلة العدد والفائدة مقارنة بكثرة وقوّة المواقع المضادة (الجنيدي (ب)، ١٩٩٩م : ٣٩-٤٠).

واهتمّت دول العالم قاطبة بمكافحة جرائم المخدرات، وعقدت المؤتمرات والاتفاقيات الدولية المختلفة، ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (١٩٦١م)، واتفاقية المؤثرات العقلية عام (١٩٧١م)، واتفاقية الأمم المتحدة لمكافحة الاتجار غير المشـروع في المخدرات والمؤثرات العقلية عام (١٩٨٨م). وعلى المسـتوى العربي تمّ عام (١٩٩٦م) إقرار الاتفاقية العربية لمكافحة الاتجار غير المشـروع في المخدرات والمؤثرات العقلية، كما تمّ عام (١٩٨٦م) إقرار القانون العربي النموذجي الموحد للمخدرات.

أمّا على المستوى المحلي فقد صدر نظام مكافحة الاتجّار بالمواد المخدّرة في المملكة العربية السعودية بقرار مجلس الوزراء رقم (١١) عام (١٣٧٤هـ)، وألحق به قرار هيئة كبار العلماء رقم (١٣٨) وتاريخ ١٤٠٧/٦/٢٠هـ، الخاص بإعدام مهربي المخدرات أو من يقبض عليه في قضـية ترويج للمرة الثانية، والموافق عليه بالأمر السـامي رقم (٤/ب/٩٦٦) وتاريخ ١٤٠٧/٧/١٠هـ (عيد، ١٤٢٢هـ :٩٤-١١٠).

٥. *غسيل الأموال :*

مصـطلح حديث نسـبياً، لم يكن معروفاً لرجال الشـرطة، فضـلاً عن العامة، وقد بدأ اسـتخدام المصـطلح في أمريكا نسـبة إلى مؤسـسـات الغسـيل التي تملكها المافيا، وكان أول اسـتعمال قانوني لها في عام (١٩٣١م) أثر محاكمة تمت في أمريكا لأحد زعماء المافيا، وتضمّن الحكم القضائي مصادرة أموال قيل إنّها متأتّية من الاتجار غير المشروع بالمخدرات.

واختلف الكثير في تعريف غسيل الأموال، وقد يكون التعريف الأشمل لها هو " أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال"(عيد، ١٤٢٢هـ: ١٢٤).

ومن البدهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية، لخدمة أنشطتهم الإجرامية، ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية، فلجأت إلى الإنترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة، ويجد المتصفح للانترنت مواقعَ متعددة تتحدث عن غسيل الأموال ومنها الموقع: http://www.laundryman.u.net.com ، كما يجد ولا شك أيضاً المواقع التي تستخدم باعتبارها ساتراً لعمليات غسيل الأموال، ومنها المواقع الافتراضية لنوادي القمار والتي قام مكتب المباحث الفدرالية (FBI) الأمريكي بمراقبة بعض هذه المواقع، واتَّضح أنها توجد في كاراكاو، وجزر الانتيل، وجزيرة أنتيجوا، وجمهورية الدومينكان. وقد أسفرت التحريات التي استمرت خمسة أشهر عن اعتقالات واتهامات لعدد من مديري تلك المواقع.

ومن المميزات التي يعطيها الإنترنت لعملية غسيل الأموال: السرعة، وإغفال التوقيع، وانعدام الحواجز الحدودية بين الدول، كما تساهم البطاقات الذكية، والتي تشبه في عملها بطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الأموال بواسطة المودم، أو الإنترنت مع ضمان تشفير وتأمين العملية.

كل هذا جعل عمليات غسيل الأموال عبر الإنترنت تتم بسرعة أكبر وبدون ترك أي آثار في الغالب. ويقدّر المتخصصون، المبالغ التي يتم تنظيفها سنوياً بحوالي (٤٠٠) أربعمائة مليار دولار (عبدالمطلب،٢٠٠١م : ٦٨ - ٧٢).

وإلى عهد قريب لم تكن جرائم غسيل أموال تشكّل جرماً بذاتها، إلى أن تضخمت الأموال المتحصّلة من الجرائم وخاصة من تجارة المخدرات، فأصدرت بعض الدول قوانين خاصة تسمح بتعقب وتجميد ومصادرة عائدات الجرائم الخطرة، فأصدرت الولايات المتحد الأمريكية عام (١٩٧٠م) قانونَ المنظمات القائمة على الابتزاز والنساء، وقانون منع ومكافحة جرائم إساءة استخدام العقاقير المخدرة.

كما أصدرت مصر عام (١٩٧١م) القانون رقم (٣٤) والخاص بتنظيم فرض الحراسة على الأموال المكتسبة بطرق غير مشروعة، كما أقرّ القانون العربي النموذجي الموحّد للمخدرات الصادر عن مجلس وزراء الداخلية العرب عام (١٩٨٦م)، مكافحة جرائم غسيل الأموال، وخاصة في مادته التاسعة والأربعين التي سمحت للمحكمة المختصة بحجز الأموال المتحصلة من تجارة المخدرات والتحقّق من مصادر تلك الأموال.

كما أصدرت بريطانيا وايرلندا عام (١٩٨٦م) قانوناً يسمح بمصادرة عائدات الجريمة. وأصدرت استراليا عام (١٩٨٧م) قانوناً يسمح بمصادرة أموال الشخص المدان في جرائم اتحادية.

ولم تتخلّف المملكة العربية السعودية عن رَكْب محاربة جرائم غسيل الأموال، فقد كانت المملكة من ضمن دول العالم الـ(١٠٦) الذين وقّعوا عام (١٩٨٨م) على اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، والتي كانت أوّل خطوة دولية مهمة لتعريف غسيل الأموال وتحديد الأفعال الواجب تجريمها (عيد، ١٤١٩هـ : ٢٦٣-٣١٩).

رابعاً: المواقع المعادية:

كثيراً ما تنتشـــر المواقع غير المرغوب فيها على شـــبكة الإنترنت، ومن هذه المواقع ما يكون موجهاً ضـد سياسـة دولة ما، أو ضـد عقيدة أو مذهب معين، أو حتى ضـد شـخص ما. وهي تهدف في المقام الأول إلى تشويه صورة الدولة، أو المعتقد، أو الشخص المستهدف.

ففي المواقع الســـياســـية المعادية يتم غالباً تلفيق الأخبار والمعلومات، ولو زوراً وبهتاناً، أو حتى الاستناد إلى جزيء يسير جداً من الحقيقة، ومن ثَمّ نسـج الأخبار الملفقة حولها، وغالباً ما يعمد أصـحاب تلك المواقع إلى إنشـاء قاعدة بيانات بعناوين أشـخاص يحصـلون عليها من الشركات التي تبيع قواعد البيانات تلك، أو بطرق أخرى، ومن ثَمّ يضيفون تلك العناوين قسراً إلى قائمتهم البريدية، ويبدؤون في إغراق تلك العناوين بمنشـــوراتهم، وهم عادة يلجؤون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضـون له، ولإيصـال أصـواتهم إلى أكبر قدر ممكن.

أمّا المواقع المعادية للعقيدة فمنها ما يكون موجهاً من قبل أعداء حاقدين من أتباع الديانات الأخرى، كالمواقع التي تنشـــئها الجاليات اليهودية أو النصـــرانية تحت مســـميات إســـلامية بقصـــد بث معلومات خاطئة عن الإســـلام والقرآن، أو بهدف الدعاية للأديان الأخرى ونشر الشُّبَهِ والافتراءات حول الإسلام. ومن أمثلة هذه المواقع:

موقع http://www.answering-islam.org/

وموقع http://www.aboutislam.com/

وموقع http://www.thequran.com/

أمّا القســـم الثاني من المواقع المعادية للعقيدة فهي المواقع التي يكون أفرادها من عقيدة واحدة ولكن يختلفون في المذاهب.

وهناك مواقع معادية لأشـخاص أو جهات وهي قد تكون شـبيهة وإلى حدٍّ كبير بالمواقع المخصصة للقذف التي سبق التحدث عنها سابقاً في القسم الخاص بالجرائم الجنسيّة، حيث تهدف أساساً لتشويه سمعة الشخص أو الجهة، ولذلك فسيكتفى بما سبق التطرق إليه في هذا المجال وسيركّز على الحديث عن المواقع السياسية والدينية والتي لم يتم التطرّق لها.

والمواقع المعادية بأنواعها مخالفة نظامية وجريمة جنائية، وتفصيل ذلك كالآتي:

أ. **المواقع السياسية المعادية:** قد ينظر البعض إلى إنشاء هذه المواقع باعتبارها ظاهرة حضارية تتمشي مع الديموقراطية والحرية الشخصية، وهذا غير صحيح فللديموقراطية والحرية الشخصية حدود يجب ألاّ تتجاوزها، و إلاّ أصبحت سوء أدب وبغي.

وهناك ولا شك طرق وأساليب يمكن معها التعبير عن الآراء الشخصية وضّحتها الشريعة الإسلامية قبل الديمقراطية الوضعية، وحددتها عاداتنا وتقاليدنا المنبثقة من قيمنا العربية الأصيلة في حين غفلت عنها قيم الدول الغربية، وأبسط هذه القواعد أن يكون النصح بالرفق واللين وبالكلمة الطيبة وليس بالشتم والقذف، قال تعالى في سورة النحل ﴿ ادْعُ إِلى سَبِيلِ رَبِّكَ بِالْحِكْمَةِ وَالْمَوْعِظَةِ الْحَسَنَةِ وَجَادِلْهُمْ بِالَّتِي هِيَ أَحْسَنُ إِنَّ رَبَّكَ هُوَ أَعْلَمُ بِمَنْ ضَلَّ عَنْ سَبِيلِهِ وَهُوَ أَعْلَمُ بِالْمُهْتَدِينَ (١٢٥) ﴾،وقال تعالى في سورة آل عمران ﴿ فَبِمَا رَحْمَةٍ مِنْ اللَّهِ لِنْتَ لَهُمْ وَلَوْ كُنْتَ فَظًّا غَلِيظَ الْقَلْبِ لاَنْفَضُّوا مِنْ حَوْلِكَ فَاعْفُ عَنْهُمْ وَاسْتَغْفِرْ لَهُمْ وَشَاوِرْهُمْ فِي الأَمْرِ فَإِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى اللَّهِ إِنَّ اللَّهَ يُحِبُّ الْمُتَوَكِّلِينَ (١٥٩) ﴾، كما أنّ من الآداب أنْ يكون النقد أو النصيحة في السرّ لا في العلن وفي هذا يقول الإمام الشافعي:

تعمدني بنُصْحكَ في انفراد وجَنّبْني النصيحةَ في الجماعة
فإنّ النصحَ بين الناس نوعٌ من التوبيخ لا أرضى استماعه
وإنْ خالفتني وعصيْتَ قولي فلا تجزعْ إذا لم تُعْطَ طاعة

وهذه الآداب هي أبسط الآداب الواجب اتباعها مع العامة، فما بالك مع ولي الأمر الذي قرن الله طاعته بطاعة الله ورسوله –مالم يأمر ولي الأمر بأمر مخالف لله– ولذلك فليس في إنشاء المواقع السياسية المعادية أي حرية رأي أو ديمقراطية بل هي سوء أدب إن لم يكن بغي يعاقب عليه الشرع بالقتل.

فـ" جريمة البغي موجهة إلى نظام الحكم والقائمين بأمره، وقد تشددت فيها الشريعة؛ لأنّ التساهل فيها يؤدي إلى الفتن و الاضطرابات وعدم الاستقرار وهذا يؤدي بدوره إلى تأخر الجماعة وانحلالها. ولا شك أنّ عقوبة القتل أقدر العقوبات على صرف الناس عن هذه الجريمة التي يدفع إليها الطمع وحب الاستيلاء" (عودة، ١٤٠١هـ :٦٦٣).

والدليل على أنّ البغي محرمّ شرعاً، ومعاقب عليه بالقتل، قوله تعالى في سورة الحجرات ﴿وَإِنْ طَائِفَتَانِ مِنْ الْمُؤْمِنِينَ اقْتَتَلُوا فَأَصْلِحُوا بَيْنَهُمَا فَإِنْ بَغَتْ إِحْدَاهُمَا عَلَى الأخرى فَقَاتِلُوا الَّتِي تَبْغِي حَتَّى تَفِيءَ إلى أَمْرِ اللَّهِ فَإِنْ فَاءَتْ فَأَصْلِحُوا بَيْنَهُمَا بِالْعَدْلِ وَأَقْسِطُوا إِنَّ اللَّهَ يُحِبُّ الْمُقْسِطِينَ(٩) ﴾.

وفي الحديث الشريف الذي رواه مسلم "إنهّ ستكون هنّات وهنّات، فمن أراد أن يفرّق أمر هذه الأمة، وهي جميع، فاضربوه بالسيف، كائناً من كان".

كما ورد عن رسول الله صلى الله عليه وسلم حديثا رواه مسلم وأبو داود واللفظ لأبي دواد: عن عبد الله بن عمرو أنّ النبي صلى الله عليه و سلم قال"من بايع إماماً فأعطاه صفقة يده وثمرة قلبه فليطعه ما استطاع، فإن جاء آخر ينازعه فاضربوا رقبة الآخر قلت: أنت سمعت هذا من رسول الله صلى الله عليه وسلم؟ قال: سمعته أذناي ووعاه قلبي، قلت: هذا ابن عمك معاوية يأمرنا أن نفعل ونفعل، قال: أطعه في طاعة الله واعصه في معصية الله"

وقد كانت القوانين الوضعية –وإلى عهد قريب– تعتبر الجريمة السياسية أشدَّ خطراً من الجريمة العادية، بل كانت تعامل المجرم السياسي معاملة تتنافى مع أبسط قواعد العدالة، حيث تشدّد عليه العقوبة وتصادر أمواله وتعاقب أهله بجريمته (عودة، ١٤٠١هـ : ١٠٧).

ب. **المواقع الدينية المعادية**: الدين الإسلامي هو خاتم الأديان السماوية، وبه أكمل رسوله صلى الله عليه وسلم تعاليم الدين، قال تعالى في سورة المائدة ﴿ الْيَوْمَ أَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتْمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمْ الإِسْلَامَ دِينًا فَمَنْ اضْطُرَّ فِي مَخْمَصَةٍ غَيْرَ مُتَجَانِفٍ لِإِثْمٍ فَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ(٣) ﴾، ولذلك فلا يُقْبل أي دين غير الإسلام، قال تعالى في سورة آل عمران ﴿ وَمَنْ يَبْتَغِ غَيْرَ الإِسْلامِ دِينًا فَلَنْ يُقْبَلَ مِنْهُ وَهُوَ فِي الآخِرَةِ مِنْ الْخَاسِرِينَ(٨٥) ﴾، ليس ذلك فحسب، بل عاقب من بدّل دينه بعد إسلامه، ففي الحديث الذي رواه البخاري قال النبي صلى الله عليه وسلم: "من بدّل دينه فاقتلوه".

ج. **المواقع المعادية للأشـــخاص أو الجهات:** لعلّ في التشـــابه الكبير بين هذه المواقع والمواقع المخصصة للقذف –والتي سبق الحديث عنها في الجرائم الجنسيّة– ما يغنى عن تكرار إيضـاح الموقف الشـرعي والقانوني من هذه المواقع، فما ينطبق على تلك المواقع من تجريم قانوني وشرعي ينطبق على هذه المواقع أيضاً.

خامساً: جرائم القرصنة:

يقصد بجرائم القرصنة هنا الاستخدام أو النسخ غير المشروع لنظم التشغيل أو لبرامج الحاسب الآلي المختلفة.

وقد تطوّرت وسـائل القرصـنة مع تطور التقنية، ففي عصـر الإنترنت تطوّرت صـور القرصنة واتسعت وأصبح من الشائع جداً العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجاناً أو بمقابل مادي رمزي.

وأدّت قرصـنة البرامج إلى خسـائر مادية باهظة جداً وصـلت في العام (١٩٨٨م) إلى (١١) أحد عشـر مليار دولار أمريكي في مجال البرمجيات وحدها، ولذلك سـعت الشـركات المتخصصة في صناعة البرامج إلى الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات، ومن ذلك منظمة اتحاد برمجيات الأعمال (Business Software Alliance) أو ما تعرف اختصاراً بـــ(BSA)، والتي أجْرت دراسة اتّضح منها أنّ القرصنة على الإنترنت ستطغى على أنواع القرصـنة الأخرى، ودقّ هذا التقرير ناقوس الخطر في الشـركات المعنية، فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت، ومنها تهديد بعض الشركات بفحص القرص الصـلب لمتصـفحي مواقعهم على الإنترنت لمعرفة مدى اسـتخدام متصـفح الموقع لبرامج مقرصـنة، إلاّ أنّ تلك الشـركات تراجعت عن هذا التهديد أثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت.

كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لإبلاغهم عن أي مواقع مخصصة للبرامج المقرصنة تنشأ لديهم، وذلك لتقديم شكوى ضدهم ومقاضاتهم إنْ أمكن، أو إقفال تلك المواقع على أقلّ تقدير. والقرصـنة عربياً لا تختلف كثيراً عن القرصـنة عالمياً –إنْ لم تَسبقها بخطوات– خاصة في ظل عدم توفّر حقوق الحماية الفكرية، أو في عدم جدّية تطبيق هذه القوانين إنْ وجدت (سالم، نوفمبر ١٩٩٩م : ٢٨-٣٥).

وقوانين حماية الملكية تعتبر من الأنظمة الحديثة في الدول العربية حيث بدأت الفكرة من الدول الرأسمالية، ومن ثَمّ بدأت الدول الأخرى تطبيقها وإدراجها في أنظمتها، وقد اهتمّت دول الخليج بحماية الملكية الفكرية أيضاً، فقامت أمانة مجلس التعاون الخليجي وفي الاجتماع الثاني للوزراء المسؤولين عن الثقافة المنعقد بالرياض في ١٩٨٧/٩/١٥م بوضع لائحة استرشادية للنظام الموحّد لحماية حقوق المؤلف في دول المجلس (موقع مجلس التعاون لدول الخليج العربية، ١٤٢٣هـ).

ولم يكن هذا هو آخر المشوار بل البداية، حيث توالت دول الخليج العربي في إصدار القوانين الخاصة بالحماية الفكرية، ففي سلطنة عُمان مثلاً صدر قانون الملكية الفكرية بالمرسوم السلطاني رقم (٩٧/٦٥) وتاريخ ١٤١٨/٥/٣هـ، وفي الكويت صدر القانون رقم (٦٤) لعام (١٩٩٩م) بشأن حقوق الملكية الفكرية.

أمّا المملكة العربية السعودية فكانت سبّاقة إلى إصدار تنظيمات خاصة لمحاربة القرصنة، فصدر قرار مجلس الوزراء رقم (٥٦) و تاريخ ١٤٠٩/٤/١٤هـ بالموافقة على نظام براءات الاختراع، ثُمّ صدر قرار مجلس الوزراء رقم (٣٠) و تاريخ ١٤١٠/٢/٢٥هـ بالموافقة على نظام حماية حقوق المؤلف (موقع محامو المملكة، ١٤٢٣هـ).

ووافق مجلس الوزراء الموقّر في جلسته بتاريخ ١٤٢٠/٦/١٧هـ، على تشكيل اللجنة الدائمة لحقوق الملكية الفكرية والتي تتكوّن من ممثلين عن وزارات التجارة، والإعلام، والداخلية، والخارجية، والعدل، والصناعة والكهرباء، والبترول والثروة المعدنية، والمالية والاقتصاد الوطني (مصلحة الجمارك)، وديوان المظالم، ومدينة الملك عبدالعزيز للعلوم والتقنية، ويكون مقرّها ورئاستها بوزارة التجارة، وحُدّدت مهام اللجنة بمتابعة ودراسة ما يستجد من أمور في مجال حقوق الملكية الفكرية، وإعداد التوصيات اللازمة بما يتناسب مع متطلبات الاتفاقيات الدولية ذات العلاقة، وفي مقدمتها اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (موقع وزارة التجارة، ١٤٢٣هـ).

سادساً: جرائم اختراقات أخرى لم تتطرق إليها الدراسة:

لقد ركّزت الدراسة على الأفعال الجنائية التي تُرتكب من قبل مستخدمي الإنترنت في المجتمع السعودي، والتي حصرها الباحث من خلال الدراسة الاستطلاعية لمزودي خدمة الإنترنت في المملكة، لكن ينبغي لفت النظر إلى أنّ هناك جرائم أخرى لم يُتبيّن ممارستها من قبل الأفراد في المجتمع السعودي، ولذلك لم تُدْرَجْ ضمن عناصر الدراسة لبحثها، وإنْ كان هذا لا يعنى الجزم بعدم وجودها، أو على أقلّ تقدير عدم إمكانية حدوثها في المجتمع السعودي، ولذا لم تُدرج في الدراسة لأنّ الدراسة تُرَكِّزُ على الجرائم الأكثر شيوعاً في المجتمع السعودي.

إلاّ أنّه ونظراً لأهمية هذه الجرائم على المستوى الأمني، وجب أخذ الاحتياطيات اللازمة للتوقّي منها، وأخذها في الحسبان عند وضع الضوابط النظامية للتعامل مع جرائم الإنترنت، وللفت نظر الباحثين في هذا المجال لها، ولذا وجب التطّرق إليها هنا بالشرح و الإيضاح وهذه الجرائم:

١. التجسس الإلكتروني:*

" في عصر المعلومات، وبفعل وجود تقنيات عالية التقدّم، فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي" (البداينة، ١٩٨٨م)، والعالم العربي والإسلامي كان ولا يزال مستهدفاً أمنياً، وثقافياً، وفكرياً، وعقدياً، لأسباب لا تخفى على أحد.

وقد تحوّلت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية، خاصةً مع استخدام الإنترنت وانتشاره عربياً وعالمياً.

والخطورة لا تكمن في استخدام الإنترنت، ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية، ولا يمكن حتماً الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية فهي ليست مأمونة ولا يمكن الاطمئنان لها تماماً.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحاً بـ(hackers)، فمخاطر هؤلاء محدودة، وتقتصر غالباً على العبث أو إتلاف المحتويات، والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع آمن، ولكنّ الخطر الحقيقي، يكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة، ومن ثَمّ إفشاؤها لدول أخرى تكون عادة معادية، أو استغلالها بما يضرّ بالمصلحة الوطنية للدولة.

---

* للاستفادة يمكن الرجوع إلى كتاب الجريمة عبر الانترنت للدكتور ممدوح عبدالمطلب ص ٣٠ – ٤٥

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكية (NSA) التي قامت بزراعته في نظام التشغيل الشهير وندوز، وربمّا يكون هذا هو أحد الأسباب الرئيسة التي دعت الحكومة الألمانية إلى إعلانها في الآونة الأخيرة، عن استبدالها لنظام التشغيل وندوز بأنظمة أخرى.

كما كشف أخيراً النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا، وبريطانيا، وأستراليا ونيوزيلندا ويطلق عليها اسم (ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة أنواعها سواء ما كان منها برقياً، أو تلكسياً، أو فاكسياً أو إلكترونياً.

وخصّص هذا النظام للتعامل مع الأهداف غير العسكرية، وبطريقة تجعله يعترض كميات هائلة جداً من الاتصالات والرسائل الإلكترونية عشوائياً، باستخدام خاصية الكلمة المفتاح، بواسطة الحاسبات المتعددة المتواجدة في عدد من المحطات السرية التي تمّ إنشاؤها حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية، ومنها محطة رصد الأقمار الصناعية الواقعة في منطقة (واي هوباي) بجنوب نيوزيلندا، ومحطة (جير الدتون) الموجودة بأستراليا، والمحطة الموجودة في منطقة (موروينستو) في مقاطعة (كورنوول) ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة (شوجرجروف)، وتبعد (٢٥٠) مائتين وخمسين كيلومتراً جنوب (واشنطن دي سي)، وأيضاً المحطة الموجودة بولاية (واشنطن) على بعد (٢٠٠) مائتي كيلومتر جنوب غرب مدينة (سياتل).

ولا يَقْتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة الاتصالات الأرضية وكذا الشبكات الإلكترونية.

بمعنى أنّه يرصد جميع الاتصالات التي تتمّ بأيّ وسيلة كانت. ويعدّ الأفراد، والمنظمات، والحكومات، الذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمة كودية لحماية شبكاتهم وأجهزتهم، أهدافاً سهلة لشبكة التجسس هذه، وليس معنى ذلك أنّ الأهداف الأخرى التي تستخدم أنظمة الشفرة، في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها، فالتجسس لا يقتصر على المعلومات العسكرية أو السياسية، بل تعدّاه إلى المعلومات التجارية، والاقتصادية، وحتى الثقافية (عبدالمطلب، ٢٠٠١م : ٣٠-٤٥).

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت، تحوّل الكثير من مصادر المعلومات إلى أهداف للتجسس التجاري، ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من (٣٦٪) عام (١٩٩٤م) إلى (٤٥٪) عام (١٩٩٩م)، كما أظهر استفتاء أجري عام (١٩٩٦م) لمسؤولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول –وبشكل غير مشروع– على معلومات سِرّية لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية (داود، ١٤٢٠هـ: ٦٢).

ومن الأساليب الحديثة للتجسس الإلكتروني، أسلوب إخفاء المعلومات داخل المعلومات، وهو أسلوب شائع مع أنّه ليس سهلاً، ويتلخّص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحسّاسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي، ومن ثَمّ يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها، وبذلك لا يشكّ أحد في أنّ هناك معلومات حسّاسة يتم تهريبها، حتى ولو تمّ ضبط الشخص متلبساً، كما قد يُلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرّية (داود، ١٤٢٠هـ : ٦٧).

وبعد اعتداءات الحادي عشر من سبتمبر على الولايات المتحدة الأمريكية، صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان، والبحث عن أسامة بن لادن والجماعات التابعة له، وقرّرت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممين خصيصاً لالتقاط الاتصالات التي تجرى عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صوراً فائقة الدقة، وفي الوقت نفسه طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثَمّ تُحوّل بعد ذلك إلى الولايات المتحدة الأمريكية لتدخل في أجهزة كمبيوتر متطوّرة لتحليلها.

وتشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسس على المكالمات الهاتفية ورسائل الفاكس والبريد الإلكتروني، الأمر الذي يتيح تحليل الإشارات التي تلتقطها الأقمار الاصطناعية حتى إن كانت واهنة أو مشفرة (بي بي سي، ٢٠٠١م).

واتّفقتْ هيئة أركان الجيش الإسرائيلية مع شركة مايكروسوفت على شراء برنامج حاسوبي خاص للتنصّت على شبكة الإنترنت، حيث قرر الجيش الإسرائيلي إقامة قسم جديد في هيئة الأركان للتنصّت على شبكة الإنترنت، الأمر الذي سيعطي لأجهزة الأمن الإسرائيلية معلومات هامة وجديدة تجمعها من مستخدمي نظام الوندوز دون علمهم!!! (موقع صحيفة الرياض، ١٤٢٣/١٠/١٣هـ).

٢ . *الإرهاب الإلكتروني:*

في عصـــر الازدهار الإلكتروني وفي زمن قيام حكومات إلكترونية، كما في الإمارات العربية المتّحدة، تبدّل نمط الحياة وتغيّرت معه أشكال الأشياء وأنماطها، ومنها ولا شكّ أنماط الجريمة التي قد يحتفظ بعضـها بمسـماها التقليدي مع تغيّرٍ جوهريّ أو يسـير في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها، القديمة في اسمها، جريمة الإرهاب التي أخذت منحنى حديثاً يتماشى مع التطور التقني.

وقد انتبه الغرب إلى قضـــية الإرهاب الإلكتروني منذ فترة مبكّرة، فقد شـــكّل الرئيس الأمريكي الســـابق بل كلينتون لجنة خاصـــة (www.nipc.gov) مهمتها حماية البنية التحتية الحسّاسة في أمريكا، والتي قامت في خطوة أولى بتحديد الأهداف المحتمل استهدافها من قبل الإرهابيين، ومنها مصادر الطاقة الكهربائية والاتصالات، إضافة إلى شبكات الحاسب الآلي، ومن ثَمّ تَمّ إنشـــاء مراكز خاصـــة في كلّ ولاية للتعامل مع احتمالات أي هجمات إرهابية الكترونية.

كما قامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية وظّفت به ألفاً من خبراء أمن المعلومات، كما شكّلت قوة ضاربة لمواجهة الإرهاب على مدار الساعة، ولم يقتصر هذا الأمر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحث الفدرالية والقوات الجوية.

وحذّر تقرير صدر من وزارة الدفاع الأمريكية عام (١٩٩٧م) من (بيرل هاربور إلكترونية)، وتوقّع التقرير أنْ يزداد الهجوم على نظم المعلومات في الولايات المتحدة الأمريكية من قبل الجماعات الإرهابية، أو عملاء المخابرات الأجنبية، وأنْ يصـــل هذا الهجوم إلى ذروته عام (٢٠٠٥م)، وأوضـح التقرير أنّ شـبكة الاتصـالات، ومصـادر الطاقة الكهربائية، والبنوك، وصناعات النقل في أمريكا معرّضة للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية، دون أن تُواجِهَ قواتها المسلحة (داود، ١٤٢٠هـ).

وبعد الهجمات الأخيرة على الولايات المتحدة الأمريكية، ارتفعت أصوات البعض بممارسة الإرهاب الإلكتروني ضد المواقع الإسلامية والعربية التي يشتبه بأنها تدعم الإرهاب، وتناقلت وسـائل الإعلام المختلفة خبراً عن اتفاق (٦٠) سـتين خبيراً في أمن الشـبكات ببدء تلك الهجمات الإرهابية على مواقع فلسطينية وأفغانية.

٣. جرائم ذوي الياقات البيضاء:

هذا المصطلح حديث نسبياً، وأول من أطلقه عالم الاجتماع سذرلاند (Sutherland)، حيث وضّح أنّ هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذي المناصب الإدارية الكبيرة، وتشمل أنواعاً مختلفة من الجرائم كالرشوة، والتلاعب بالشيكات، والاختلاس، والسرقة، وتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات محلية، أو عالمية غير مشهورة، وشراء المعلبات قبل انتهاء صلاحيتها واستبدال تاريخ صلاحيتها.

وهذا النوع من الجرائم يصعب ارتكابها، أو كشفها، والتحقيق فيها، دون إلمام جيد بظروف الإنتاج، والحسابات الجارية، والعمل التجاري، ومبادئ التقنية الحسابية الإلكترونية. كما أنّ خسائر هذه الجرائم ضخمة فقد قُدرّتْ خسائر المجتمع الأمريكي بمبلغ (١٢– ٤٢) مليون دولار سنوياً نتيجة خداع المستهلكين باستخدام جميع وسائل التكنولوجيا المتقدمة (اليوسف،١٤٢٠هـ: ٢٠٩-٢١١).

وقد استفاد الجناة من انتشار الإنترنت في تطوير جرائمهم، وتوسعة الرقعة الجغرافية لها، بحيث أصبحت عالمية، بعد أن كانت محلية.

٤. الجرائم الاقتصادية:

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة، فعلى سبيل المثال: في الدول الرأسمالية، نجد أنّ أغلب الجرائم الاقتصادية، تتمحور حول الاحتكارات، والتهرّب الضريبي، والجمركي، والسطو على المصارف، وتجارة الرقيق الأبيض، والأطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة، والاختلاس، والسوق السوداء.

وهذا لا يعنى بالضرورة أنّ ّه لا يمكن ارتكاب كلّ أنواع هذه الجرائم في مجتمع واحد، حيث يمكن أنْ تجد في المجتمع الرأسمالي مثلاً جرائم رشاوي واختلاسات، والعكس صحيح. وكما في الجرائم الأخرى، فقد ساهم الإنترنت في تطوير طرق وأساليب ارتكاب هذه الجرائم، ووسّع منطقة عملها، خاصة مع توجّه الكثير من الدول للتحوّل إلى الحكومات الإلكترونية، كما في دولة الإمارات العربية المتحدة مثلاً، حيث استفاد المجرمون من التقدم التقني في اختلاس الأموال وتحويل الأرصدة النقدية، وسرقة التيار الكهربائي، والمياه، وخطوط الهاتف، والعبث بها، وإتلافها (اليوسف،١٤٢٠هـ : ٢١١-٢١٤).

خلاصة الفصل الأول:

تطرّق هذا الفصل إلى تعريف الإنترنت، وبداياته، واستخداماته، ثُمّ تحدّث المبحث الأول عن تعريف جرائم الحاسب الآلي والإنترنت وصعوبة إثباتها، وذِكْر فئات الجناة في جرائم الحاسب الآلي وخصائص وأنواع تلك الجرائم.

وفي المبحث الثاني تمّ التحدّث عن مواكبة الأنظمة والتشريعات لجرائم الإنترنت، مع التطرّق إلى القوانين الخاصة التي أصدرتها بعض الدول لمواجهة جرائم الإنترنت، وتمّ توضيح أنّ قوانين المملكة المستمدة من الشريعة الإسلامية لا تحتاج إلى تحديث لأنّها شاملة لكل أنواع الجرائم قديمها وحديثها، وإنْ كان الأمر يحتاج إلى تفعيل تلك الأنظمة، والعمل على إنشاء جهة متخصّصة للتعامل مع هذه الجرائم المستحدثة.

وأخيراً تمّ في المبحث الثالث التحدّث عن الأبعاد الشرعية والقانونية للأفعال الجنائية المرتكبة من قبل مستخدمي الإنترنت في المجتمع السعودي من منظور إسلامي، وتكييف تلك الأعمال قانونياً وشرعياً على أنظمة المملكة العربية السعودية.