المواقع والقوائم البريدية الإباحية:

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

أما القوائم البريدية فهي أسهل إنشاءً، وغالباً مجانية ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية وربما تكون القوائم البريدية ابعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية والتي تكون من الصعوبة بمكان منعها عن أعضاء أي مجموعة، حتى وأن تم الانتباه إلى تلك القائمة لاحقا وتم حجبها، فان الحجب يكون قاصرا على المشتركين الجدد واللذين لا يتوفر لديهم وسائل تجاوز المرشحات، أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يردونه دون أن تستطيع وسائل الحجب التدخل. ويشترك في القوائم البريدية ألاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعنى كم هائل من الرسائل والصور الجنسية التي يتبادلها مشتركي القائمة بشكل يومي.

واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التي تقدمها 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)، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الإنترنت الذي لا يعترف بأي حدود دولية أو جغرافية فهو يشكل خطرا حقيقيا للأطفال فضلا عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة (موثق في الزغاليل، ١٤٢٠هـ: ٧٨). ويوجد على الإنترنت ألاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية والتي أصبحت أكثر تخصصا فهناك قوائم خاصة للشواذ من الجنسين وهناك قوائم أخرى تصنف تحت دول محددة ومن المؤسف انه وجدت بعض المواقع الشاذة بمسميات عربية بل وسعودية والأدهى والأمَرّ أن يربط بين بعض القوائم الإباحية والإسلام كموقع أسمى نفسه " السحاقيات المسلمات " وهكذا.

وكشفت إحدى الدراسات أن معدل التدفق على الواقع الإباحية في أوقات العمل التي تبدأ من الساعة التاسعة صباحا إلى الخامسة عصرا تمثل (٧٠؟) من إجمالي نسبة التدفق على تلك المواقع (بي بي سي، ٢٠٠١م).

كما كشفت دراسة قام بها الدكتور مشعل القدهي (القدهي،١٤٢٢هـ) بان هناك إقبال كبير جدا على المواقع الإباحية حيث تزعم شركة (Playboy) الإباحية بأن (٤,٧) مليون زائر يزور صفحاتهم على الشبكة أسبوعياً، وبأن بعض الصفحات الإباحية يزورها (٢٨٠,٠٣٤) زائر يوميا وأن هناك مائة صفحة مشابهة تستقبل أكثر من (٢٠,٠٠٠) ألف زائر يوميا وأكثر من ألفين صفحة مشابهة تستقبل أكثر من (١٤٠٠) زائر يوميا، وأن صفحة واحدة من هذه الصفحات استقبلت خلال عامين عدد (٤٣,٦١٣,٥٠٨) مليون زائر، كما وجد أن (٨٣,٥؟) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية، وبأنّ أكثر من (٢٠؟) من سكان أمريكا يزورون الصفحات الإباحية حيث تبدأ الزيارة غالبا بفضول وتتطور إلى إدمان، وغالبا لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الإباحية بها أو شراء مواد خليعة منها

وقد بلغت مجموعة مشتروات مواد الدعارة في الإنترنت في عام (١٩٩٩م) ما نسبته (٨؟) من دخل التجارة الإلكترونية البالغ (١٨) مليار دولار أمريكي في حين بلغت مجموعة الأموال المنفقة للدخول على المواقع الإباحية (٩٧٠) مليون دولار ويتوقع ارتفاع المبلغ ليصل إلى (٣) مليار دولار في عام (٢٠٠٣م)، وقد أتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين (١٢) و (١٥) عام في حين تمثل الصفحات الإباحية أكثر صفحات الإنترنت بحثا وطلبا.

كما وضحت دراسة أدست (Adsit) (Adsit، ١٩٩٩) أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر، ويمكن أن يلمس أثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدوا أن لكثرة المواقع الإباحية على الإنترنت والتي يقدر عددها بحوالي (٧٠,٠٠٠) ألف موقع دور كبير في إدمان مستخدمي الإنترنت عليها حيث أتضح أن نسبة (١٥؟) من مستخدمي الإنترنت البالغ عددهم(٩,٦٠٠,٠٠٠) مليون شخص تصفحوا المواقع الإباحية في شهر ابريل عام (١٩٩٨م).

وقد جرى حصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقع على شبكة الإنترنت ومنها موقع الياهو (YAHOO) فوجد أنها تصل إلى (١٧١) قائمة، بلغ عدد أعضاء اقل تلك القوائم (٣) في حين وصل عدد أكثرها أعضاء إلى (٨٦٨٣) أما موقع قلوب لست (GLOBELIST) فقد احتوى على (٦) قوائم إباحية عربية، في حين وجد عدد (٥) قوائم عربية إباحية على موقع توبيكا (TOPICA) وقد قامت مدينة الملك عبدالعزيز للعلوم والتقنية مشكورة بإغلاق تلك المواقع.

فارتياد مثل هذه المواقع ومشاهدة المواد الجنسية بها من المحظورات الشرعية التي حرص الشارع الحكيم على التنبيه عليها وتحريمها، بل أن الشارع الحكيم امرنا بغض البصر وحرّم النظر إلى الأجنبيات سواء بصورة أو حقيقة وليس فقط تجنب النظر إلى الحرام فقال عز وجل في كتابه الحكيم في سورة النور: (قُلْ لِلْمُؤْمِنِينَ يَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَلِكَ أَزْكَى لَهُمْ إِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ) (٣٠) .

فهناك ولا شك علاقة بين " ارتكاب الأفعال الجنسية المحرمة والنظر إلى الصور الجنسية العارية، فالدين الإسلامي الحنيف حذر من ظاهرة النظر للعراة، لما تحدثه من تصدعات أخلاقية في الفرد والمجتمع" (السيف، ١٤١٧هـ: ١٠٠).

ويذهب الشارع إلى ابعد من ذلك لعلمه بمخاطر النظر وما يمكن أن يوصل إليه، فحرّم رسول الله صلى الله عليه وسلم أن تصف المرأة لزوجها جمال امرأة أخرى لا تحل له وكأنه ينظر إليها 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 إِلَيْهَا".

كل هذه الأمور اهتم بها الشارع وحرمها كونها موصلة لجريمة الزنا التي تعد من الكبائر والتي متى ما اجتب الأفراد هذه الأفعال فلن يقعوا في الزنا. ولعل من حكمة الشارع ومعرفته بالغرائز البشرية التي يساهم الشيطان في تأجيجها ليوقع الإنسان فيما حرم الله، ولعظمة جريمة الزنا فانه لم يحرم الزنا فقط بل حرم الاقتراب منه فقال تعالى في سورة الإسراء: ؟ وَلَا تَقْرَبُوا الزِّنَى إِنَّهُ كَانَ فَاحِشَةً وَسَاءَ سَبِيلًا (٣٢) ؟

يقول القرطبي رحمه الله في تفسير هذه الاية " قال العلماء قوله تعالى "ولاتقربوا الزنى" ابلغ من ان يقول ولا تزنوا فإن معناه فلا تدنوا من الزنا. فاي اقتراب من المحظور هو فعل محظور في حد ذاته، ومن ذلك مشاهدة المواد الجنسة فضلا عن الاشتراك في تلك القوائم الاباحية أو شراء مواد جنسية منها أو،وهو الاخطر ضررا، انشائها كون الفعل الاخير متعدي ضرره للغير ويدخل فاعله في وعيد الله عز وجل حين قال في سورة النور: (إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ) (١٩)

وقد اثبتت بعض الدراسات في المجتمع السعودي ان (٦٨,٨) من مجموعة المبحوثين يرون ان هناك علاقة بين الانحراف والجرائم المرتبكة وبين مشاهدةاشرطة الفيدوا الجنسية، كما اثبتت احدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي والتي اجريت

في الاصلاحيات المركزية بالمملكة ان (٧, ٥٣ ؟) من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية وان فئة كبيرة منهم كانوا يميلون إلى مشاهدة الافلام الجنسية الخليعة وقت فراغهم، كما تبين من الدراسة قوة تأثير مثل هذه الصور في ارتكاب جرائم الاعتداء الجنسي من قبل مجرمي اغتصاب الاناث وهاتكي اعراض الذكور بقوة (السيف، ١٤١٧هـ: ٩٩).

المواقع المتخصصة في القذف وتشويه سمعة الاشخاص:

تعمل هذه المواقع على ابراز سلبيات الشخص المستهدف ونشر اسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الاخبار عنه. وهناك حادثة مشهورة جرىتدأولها بين مستخدمى الإنترنت في بداية دخول الخدمة للمنطقة حيث قام شخص في دولة خليجية بإنشاء موقع ونشر صور احدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل علي تلك الصور بعد التسلل إلى حاسبها الشخصي وحأول ابتزازها جنسيا ورفضت فهددها بنشر تلك الصور على الإنترنت وفعلا قام بتنفيذ تهديده بانشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وادى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها.

كما وقعت حادثة تشهير أخرى من قبل من اسموا نفسهم " الامجاد هكرز " حيث اصدروا بيان نشر على الإنترنت بواسطة البريد الالتكروني ووصل العديد من مشتركي الإنترنت أوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر على التطاول في احدى المنتديات بالقدح والسب 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 ثم تم نشر صوره وكشف اسراره في موقعهم على الإنترنت حيث خصصوا 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 المسئولة عن متابعة السلبيات التي تحدث اثناء

إستخدام الإنترنت، متنفسا لاحقداهم ومرتعا لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديما "من أمن العقوبة أساء الادب".

والقذف مُجَّرم شرعاً، ونظرا لشناعة الجرم ومدى تاثيره السلبي على المجنى عليه والمجتمع كونه يساعد على اشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعل عقوبته من الحدود والتي لا يملك احد حق التنازل عنه ولا يجوز العفو عنها بعد طلب المخاصمة امام القضاء،كما جعلها عقوبة ذات شقين الأول عقوبة بدنية بجلده ثمانين جلدة لقوله تعإلى 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 تعإلى في ذات الاية وذات السورة: ؟ وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُ الْفَاسِقُونَ (٤) ؟ وشدد رسول الله صلى الله عليه وسلم في جريمة القذف حيث اعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفق عليه "اجتنبوا السبع الموبقات، قالوا يارسول الله، وما هن؟ قال الشرك بالله، والسحر، وقتل النفس التي حرم الله الا بالحق، وأكل الربا، واكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات". ولا تعاقب الشريعة على القذف الا اذا كان كذبا واختلاقا فان كان حقيقة واقعية فلا جريمة ولاعقوبة (عودة، ١٤٠١هـ: ٦٤٥-٦٤٦؛ فرحات، ١٤٠٤هـ: ١٥١-١٦٤).

استخدام البروكسي للدخول إلى المواقع المحجوبة:

البروكسي هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدي مستخدمي الانترنت للبروكسي هو ما يستخدم لتجأوز المواقع المحجوبة وهو ما نقصده في هذه الدراسة حيث يستخدم البروكسي من قبل مستخدمي الإنترنت في المجتمع السعودي لتجأوز المواقع المحجوبة من قبل مدينة الملك عبدالعزيز للعلوم والتقنية والتي عادة ما تكون هذه المواقع المحجوبة اما مواقع جنسية أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر احصائيات عن الجرائم أو حتى بعض المواقع العادية ويعود ذلك للالية التي يتم بها عملية ترشيح المواقع وربما 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 ان الغالبية العظمى تستخدم البروكسي للدخول إلى المواقع الجنسية أو المواقع السياسية ولكن بدرجة اقل.

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

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

أ- ان النظام أُقِّر من ولي الامر و مخالفة ولي الامر من المحظورات الشرعية، ما دامت تلك الأنظمة لا تخرج عن تعاليم الشرع، والدليل على ذلك قوله تعإلى في سورة النساء ﴿يَاأَيُّهَا الَّذِينَ آمَنُوا 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 وان عبدا حبشيا مجدعا فاسمعوا وأطيعوا ما أقام فيكم كتاب الله» وفي الحديث الذي رواه احمد في مسنده « قد تركتكم على البيضاء ليلها كنهارها، لا يزيغ عنها بعدي إلا هالك، ومن يعش منكم فسيرى اختلافا كثيرا، فعليكم بما عرفتم من سنتي و سنة الخلفاء الراشدين المهديين، و عليكم بالطاعة و إن عبدا حبشيا عضوا عليها بالنواجذ، فإنما المؤمن كالجمل الأنف حيثما انقيد انقاد».

ب- اذا كان مشاهدة المواقع الجنسية حرام، فإن إستخدام البروكسي للدخول إلى تلك المواقع

حرام ايضا فما بني على باطل فهو باطل، والفعل اذا كان محرماً فان الوسيلة الموصله اليه تكون محرمة. وتنطبق هنا قاعدة سد الذرائع أي «دفع الوسائل التي تؤدي إلى المفاسد، والاخذ بالوسائل التي تؤدي إلى المصالح» (ابوزهرة، ١٩٧٦م: ٢٢٦)، كما انه «من المقرر فقهياً أن دفع المفاسد مقدم على جلب المصالح» (ابوزهرة، ١٩٧٦م : ٢٢٨).

إخفاء الشخصية:

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

إنتحال الشخصية:

وهي تنقسم إلى قسمين:

أ- انتحال شخصية الفرد:

تعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة الا ان التنامي المتزايد لشبكة الإنترنت اعطى المجرمين قدرة اكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الإنترنت الكثير من الاعلانات المشبوهة والتي تداعب عادة غريزة الطمع الانساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلا اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال

الافصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من ان مثل هذا الاعلان من الوضوح بمكان انه عملية نصب واحتيال الا انه ليس من المستبعد ان يقع ضحيته الكثير من مستخدمي الإنترنت. ويمكن ان تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الاساءة إلى سمعة الضحية (داود، ١٤٢٠هـ: ٨٤-٨٩).

ب- انتحال شخصية المواقع:

مع ان هذا الاسوب يعتبر حديث نسبياً، الا انه اشد خطورة واكثر صعوبة في اكتشافه من انتحال شخصية الافراد، حيث يمكن تنفيذ هذا الاسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الامن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الامني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحأول المجرم اختراق موقع لاحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع ان يكثر استخدام اسلوب انتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها (داود، ١٤٢٠هـ:٨٩-٩٣).

والمحاذير الامنية والمخالفات النظامية والشرعية واضحة في هذه الفقرة سواء ماكان منها قاصرا على انتحال شخصية الافراد أو المواقع، فقد حفظت الشريعة السماوية والأنظمة الوضعية الحقوق الشخصية وصانت الملكيات الفردية وجعل التعدي عليها امرا محظورا شرعيا ومعاقب عليه جنائياً.

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

ومهما كان حجم هذه الاضرار الناتجة عن هذا الفعل غير النظامي فانه لا يمكن الا ان يتضرر

المجنى عليه من هذا الفعل وخاصة ان الهدف الغالب من وراء انتحال الشخصية لن يكون حميدا أو بحسن نية أو لخدمة شخص اخر خلاف منتحل الشخصية.

وتتفق الشريعة مع القوانيين الوضعية في جعل الانسان مسئولا عن كل فعل ضار بغيره، سواء اعتبر القانون ذلك الفعل جريمة ام لم يعتبره (عودة، ١٤٠١هـ:٧٧)،

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

جرائم الاختراقات:

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

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

وتتفق التشريعات السماوية والأنظمة الوضعية على ضرورة احترام خصوية الفرد ويعتبر مجرد التطفل على تلك المعلومات سواء كانت مخزنة في الحاسب الآلي أو في بريده الالتكروني أو في أي مكان اخر انتهاكاً لخصوصيته الفردية وحقوقه.

ومن المعلوم "ان الفقهاء يقسمون الحقوق إلى حقوق لله وحقوق للافراد إلا أن الكثيرين منهم يرون بحق ان كل ما يمس حق الجماعة الخالص أو حق الافراد الخالص يعتبر حقا لله تعإلى أي من حقوق الجماعة ونظامها" (عودة، ١٤٠١هـ:٢٠٦)، ومن هنا يعتبر التعدى على حقوق الافراد وانتهاك خصوصياتهم الشخصية مخالفة شرعية وجريمة نظامية كونه ينظر اليه شرعا تعدياً على حق الله.

وقد أدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية سواء عمدا أو مصادفة، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع على شبكة الإنترنت حتى يقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة باجهزتهم (Cookies) وهي نصوص صغيرة يرسلها العديد من مواقع الويب لتخزينها في جهاز من يزور تلك المواقع لعدة اسباب لعل منها التعرف على من يكرر الزيارة للموقع أولاسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك أو

حتى الاستئذان منه! وفورا يتم اصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وارسالها إلى مصدرها أو احدى شركات الجمع والتحليل للمعلومات وهي عادة ما تكون شركات دعاية وإعلان وكلما قام ذلك الشخص بزيارة الموقع يتم ارسال المعلومات وتجديد النسخة الموجودة لديهم ويقوم المتصفح 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 اصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا حيث يكون الشخص عادة اقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي بعكس لو كان الذي يتعامل معه انسان اخر (موقع مجلة الأمن الإلكترونية، ١٤٢١هـ ؛ داود،١٤٢٠هـ: ٥٠- ٥٢).

هذا وان كانت هناك وسائل لحماية الخصوصية اثناء تصفح الإنترنت، الا انه " من الصعب جدا السيطرة على مايحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي) وعلى ذلك فان حماية الخصوصية يجب ان تبدأ من البداية بتحديد نوعية البيانات التي لاينبغي ان تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلك المعلومات" (داود،١٤٢٠هـ:٥٣).

يتضح من كل ما تقدم ان هذه الافعال غير شرعية أو حتى اخلاقية ولا تتمشى مع تعاليم ديننا الحنيف الذي حرّص على احترام الحقوق الشخصية وحفظ الملكية الفردية وراع خصوصية الافراد والجماعات، بل اعتبر التعدي على الحقوق الشخصية تعدي على حقوق الله، مما يعنى انها افعال اجرامية وتصرفات لا اخلاقية يعاقب عليها الشرع بعقوبات تختلف بحسب نوع الفعل المرتكب وبحسب الضرر الواقع على المجنى عليه، وقد يدخل الفعل وعقوبته تحت جرائم الحدود أو القصاص أو التعازير وليس المجال هنا مجال تفصيل لهذه الانواع بقدر ما هو مجال تحديد وايضاح ان هذه الافعال مجرّمة وان هناك عقوبة شرعية بحق من يرتكب هذه الافعال.

وقد اجْمَلْتُ ايضاح التكييف الشرعي والنظامي لهذه الافعال كونها متشابهة ومتداخلة إلى حد كبير، الا انه ونظرا لخطورتها وشيوعها فيلزم الامر التطرق وبشيئ من التفصيل إلى شرح فني لهذه الافعال واضرارها لعله يضيف بعدا اخر يساهم وبوضوح اكثر في التَعَّرُفْ على كونها مجرَّمة

الاقتحام أو التسلل:

يشمل هذا البند جرائم الاختراقات سواء للمواقع الرسمية أو الشخصية أو إختراق الأجهزة الشخصية، إختراق البريد الإلكتروني أو الاستيلاء عليه، الاستيلاء على اشتراكات الآخرين وأرقامهم السرية. وهي افعال اصبحت تنشر يوميا في الصحف والاخبار فكثيراً ما " تتدأول الصحف والدوريات العلمية الان أنباء كثيرة عن الاختراقات الأمنية المتعددة في اماكن كثيرة من العالم ليس اخرها اختراق اجهزة الحاسب (الآلي) في البنتاجون (وزارة الدفاع الأمريكية)

ولكي يتم الاختراق فان المتسللون إلى اجهزة الاخرين يستخدممون ما يعرف بحصان طروادة وهو برنامج صغير يتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص التي يقوم بها على حاسوبه الشخصي فهو في أبسط صورة يقوم بتسجيل كل طرقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل 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 إستخدامها 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 تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلا كل من وزارة العدل والمخابرات المركزية والقوات الجوية، كما تعرض له حزب العمال البريطاني" (داود، ١٤٢٠هـ: ٨٣).

وقد قام قراصنة اسرائيلين باقتحام صفحة الإنترنت الاعلامية الخاصة ببنك فلسطين المحدود ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى الغاء الصفحة ومحوها كليا، كما تعرضت العديد من الشركات الخاصة في مناطق الحكم الذاتي للهجوم والعبث ومنها شركة اقتحم المتسللون اجهزتها ووضعوا صورة زوجة مدير الشركة وهي عارية بعد تجريدها من الملابس بواسطة الحاسب الآلي (ابوشامة، ١٤٢٠هـ: ٣٧).

وفي عام (١٩٩٧م) قدّرَتْ وكالة المباحث الفدرالية الأمريكية (FBI) تعرض(٤٣؟) من الشركات التي تستخدم خدمة الإنترنت لمحولة تسلل تتراوح مابين (١-٥) مرات خلال سنة واحدة (Wilson، ٢٠٠٠)، ولا يقتصر التسلل على المحترفين فقط بل انه قد يكون من الهواة ايضا حيث يدفعهم إلى ذلك الفراغ ومحاولة اشغال الوقت، كما حدث مع مراهقة في الخامسة عشر من عمرها قامت بمحاولة التسلل إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة وذلك بسبب انها لم تكن تحب مشاهدة التلفزيون لذلك فكرت ان تكون متسللة (Koerner) (Hacker، ١٩٩٩).

وهو ايضا ما اتضح لوكالة المباحث الفدرالية (FBI) اثناء حرب الخليج الأولى عندما اجروا تحقيقا حول تسلل اشخاص إلى الصفحة العنكبوتية الخاصة باحدى القواعد العسكرية الأمريكية، وكانت الشكوك قد اتجهت بداية إلى ارهابين دوليين الا ان الحقيقة تجلت بعد ذلك في ان المتسللين هما مراهقان كانا يعبثان بجهاز الحاسب الآلي في منزلهما (Wilson، ٢٠٠٠).

وفي عام (١٩٩٧م) قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماشيتيوشش (Massachusetts) مما ادى إلى تعطيل نظام الملاحة الجوية وأنظمة أخرى حيوية لمدة ستة ساعات، وبالرغم من فداحة الضرر الذي تسبب فيه الا ان عقوبته اقتصرت على وضعه تحت الرقابة لمدة سنتين مع الزامه باداء خدمة للمجتمع لمدة (٢٥٠) يوما (Wilson، ٢٠٠٠)، وبهذا فان القانون الامريكي يلعب دورا غير مباشر في تشجيع المراهقين على اعمال التسلل حيث نادرا ما يعاقب المتسللين دون سن الثامنة عشر، كما يساهم أولياء امور المراهقين في ذلك ايضا حيث يعتبرون ابنائهم اذكياء اذا مارسوا انشطة حاسوبية تتعلق بالتسلل إلى اجهزة الاخرين (Koerner، ١٩٩٩).

وأوضحت دراسة اجريت عام (١٩٧٩م) على عدد (٥٨١) طالب جامعي امريكي ان (٥٠؟) منهم قد اشترك في اعمال غير نظامية اثناء استخدام الإنترنت خلال ذلك العام، وأن (٤٧) طالبا أو مانسبته (٧,٣؟) سبق وقبض عليه في جرائم تتعلق بالحاسب الآلي، وأن (٧٥) طالبا أو مانسبته (١٣,٣؟) قبض على اصدقائهم في جرائم تتعلق بالحاسب الآلي (Skinner & Fream، ١٩٩٧).

فالعقوبات الحالية لاتساعد على تقليص الارتفاع المستمر للجرائم المتعلقة بالحاسب الآلي، ففي خلال عام واحد تضاغفت تلك الجرائم على مستوى الولايات المتحدة الأمريكية، ففي عام (١٩٩٩م) تحرت وكالة المباحث الفدرالية (FBI) عن (٨٠٠) حالة تتعلق بالتسلل(Hacking) وهو ضعف عدد الحوادث التي قامت بالتحرى عنها في العام السابق أي عام (١٩٩٨م)، أما الهجوم على شبكات الحاسب الآلي على الإنترنت فقد تضاعف (٣٠٠؟) في ذلك العام ايضا (Koerner، ١٩٩٩).

وللحد من تزايد عمليات التسلل(Hacking) ونظرا لان المتسللين عادة يطورون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة، فقد اضطر مسئولوا أمن الحاسبات الآلية وشبكات الإنترنت وكذلك رجال الامن على الاستعانة بخبرات بعض محترفين التسلل ليستطيعوا تطوير نظم الحماية ضد المتسللين (Hackers)، وعلى سبيل المثال يرسل مسئولي امن الحاسبات اسئلة تتعلق باحدث سبل الحماية لغرف الدردشة الخاصة بمواقع المتسللين أو ما تعرف باسم (hacker internet chat room) ولطلب نصائح تقنية حول أحدث سبل الحماية (Staff، ٢٠٠٠، ١٧ February).

بل ان وكالة المباحث الفدرالية (FBI) استعانت ايضا بخبراء في التسلل (Hackers) لتدريب منسوبي الوكالة على طرق التسلل (Hacking) لتنمية خبراتهم وقدراتهم في هذا المجال وليستطيعوا مواكبة خبرات وقدرات المتخصصين من المتسللين (Hackers)، ومنهم أحد أشهر المتسللين (Hackers) ويدعى (Brian Martin) والمشهور باسم (Jericho) وهو متهم حاليا بالتسلل والعبث بمجتويات الصفحة الرئيسية لصحيفة (New Youk Times) على شبكة الإنترنت (Staff، ٢٠٠٠ ٢ April).

واكدت وحدة الخدمات السرية الأمريكية (The US Secret Service) ان الجرائم المنظمة تتجه نحو استغلال التسلل (Hacking) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية (Thomas، ٢٠٠٠).

وفي خبر نشرته صحيفة لوس انجلوس تايمز أوضحوا ان متسللين قاموا باقتحام نظام الحاسب

الآلي الذي يتحكم في تدفق اغلب الكهرباء في مختلف انحاء ولاية كاليفورنيا الأمريكية (موقع ارابيا،١٠/٦/٢٠٠١م).

الاغراق بالرسائل:

يلجأ بعض الاشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني لشخص ما بقصد الاضرار به حيث يؤدى ذلك إلى تعطل الشبكة وعدم امكانية استقبال أي رسائل فضلا عن امكانية انقطاع الخدمة وخاصة اذا كانت الجهة المضررة من ذلك هي مقدمة خدمة الإنترنت مثلا حيث يتم ملء منافذ الاتصال (Communication-Ports) وكذلك قوائم الانتظار (Queues) مما ينتج عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية غير محدودة، ولذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق اعداد كبيرة منها(داود،١٤٢٠هـ:٩٣).

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

الفيروسات الحاسب الآلية:

الفيروسات الحاسب الآلييه هي احدى انواع البرامج الحاسب الآلية الا أن 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 لفيروس أو الرسالة البريدية المرسل معها الفيروس اصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

وقد عرفها احد خبراء الفيروسات (Fred Cohen) بانها نوع من البرامج التي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أن الفيروس ينسخ

نفسه من حاسب آلي إلى حاسب آلي اخر بحيث يتكاثر باعداد كبيرة (Highley، 1999).

ويمكن تقسيم الفيروسات إلى خمسة انواع:

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

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

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

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

الخامس: يعرف بحصان طرواده وهذا النوع يصنفه البعض كنوع مستقل بحد ذاته،الا انه ادرج في تقسيمنا هنا كاحد انواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي الا أن اثره التدميري خطير. وتعمل الفيروسات على اخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيير اشكالها لذلك وجب تحديث برامج الخاصة بمكافحة الفيروسات بصفة دائمة (عيد،١٤١٩هـ: ٦٣-٦٦).

وهناك فريق من الخبراء يضع تقسيما مختلفا للفيروسات على أساس المكان المستهدف بالاصابة داخل جهاز الكمبيوتر ويرون أن هناك ثلاثة أنواع رئيسية من الفيروسات وهي فيروسات قطاع الاقلاع (Boot Sector) وفيروسات الملفات (File Injectors) وفيروسات الماكرو (Macro Virus). كما أن هناك من يقوم بتقسيم الفيروسات إلى فيروسات الاصابة 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 أيضا الفيروسات المتغيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات (الجزيرة،٢٠٠٠).

ومن الجرائم المتعلقة بارسال فيروسات حاسوبية قيام شخص امريكي يدعى (Robert Morris) بارسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (١٩٨٨م) عبر الإنترنت وقد كرر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفايروس وادى ذلك إلى تعطيل ما يقارب من (٦٢٠٠) حاسب إلى مرتبط بالإنترنت، وقدرت الاضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قدر لمصمم الفيروس تصميمه ليكون اشد ضررا لكان قد لحقت اضرار أخرى لا يمكن حصرها بتلك الاجهزة، وقد حكم على المذكور بالسجن ثلاثة سنوات بالرغم من دفاع المذكور بانه لم يكن يقصد احداث مثل تلك الاضرار(Morningstar، ١٩٩٨).

كيف يتم اقتحام الجهاز:

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

١. يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص بإستقباله وتشغيله وقد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى.

٢. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة انتجة اسرائيل.

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

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

٥.في حالة اتصال الجهازبشبكة داخلية أو شبكة إنترانت.

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

٧.كما يمكن الاصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكروز الموجود في برامج معالجة النصوص (Nanoart،٢٠٠٠).

وبصفة عامة فإن برامج القرصنه تعتمد كليا على بروتوكول الـ ((TCP/IP وهناك ادوات (ActiveX) مصممه وجاهزة لخدمة التعامل بهذا البروتوكول ومن اشهرها (.WINSOCK

OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الادوات. ويحتاج الامر إلى برنامجين، خادم في جهاز الضحية وعميل في جهاز المتسلل حيث يقوم الخادم بفتح منفذ في الجهاز الضحية ويكون هذا المنفذ معروف من قبل العميل اصلا في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية حيث يتعرف برنامج الخادم (server) على اشارات البرنامج المخترق ويتم الاتصال ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق حيث يتمكن من العبث بها أو الاستيلاء على ما يريد منها.

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز وهناك وهناك ما يقارب الـ(٦٥٠٠٠) منفذ تقريبا في كل جهاز يميز كل منفذ عن الآخر برقم خاص ولكل منها غرض محدد، فمثلا المنفذ (٨٠٨٠) يخصص احيانا لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعتبر جزء من الذاكرة لها عنوان معين يتعرف عليها الجهاز بأنها منطقة إرسال واستقبال البيانات، وكل ما يقوم به المتسلل هو فتح احد هذه المنافذ للوصول لجهاز الضحية وهوما يسمى بطريقة الزبون/الخادم Client Server)) حيث يتم ارسال ملف لجهاز الضحية يفتح المنافذ فيصبح جهاز الضحية (server) وجهاز المتسلل (Client) ومن ثم يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج ((NetBus أو ((NetSphere ولعل الخطورة الاضافية تكمن في انه عند دخول المتسلل إلى جهاز الضحية فانه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز حيث يصبح ذلك الجهاز مركزا عاما يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ (Portscanning) عن طريق احد 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، الا انه سرعان ما اسيئ استخدامه. وتعد هذه البرامج من أخطر البرامج المستخدمه من قبل المتسللين كونه يتيح للدخيل الحصول على كلمات المرور (passwords) وبالتالي الهيمنه على الحاسب الآلي بالكامل. كما أن المتسلل لن يتم معرفته أو ملاحظته كونه يستخدم الطرق المشروعة التي

يستخدمها مالك الجهاز. كما تكمن الخطورة ايضا في أن معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات إضافة إلى أن الطبيعة الساكنة لحصان طروادة يجعلها اخطر 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 الاحصنة أثناء أدائها لمهمتها التجسسية وبالتالي فإن فرص إكتشافها والقبض عليها تكاد تكون معدومه (Nanoart، ٢٠٠٠).

أهم المنافذ المستخدمة لاختراق الجهاز:

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

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

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

الجرائم المالية

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، غسيل الاموال، ولعل جرائم هذا القسم أوضح من ناحية معرفة كونها مُجَّرَمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمى والتي يعرف الجميع انها مخالفة للنظام وللشرع كونهم من الجرائم التي اشتهر محاربتها جنائيا. ونظرا للاختلاف البسيط في تصنيف كل جريمة من جرائم هذا القسم فسيتم توضيح التكييف الشرعي والقانوني لكل جريمة بشكل مفصل.

١. جرائم السطو على أرقام البطاقات الائتمانية:

بدأ مفهموم التجارة الإلكترونية ينتشر في السبعينات الميلادية وذلك لسهولة الاتصال بين

الطرفين ولامكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في ارسال البيانات وتخفيض تكلفة التشغيل والأهم هو ايجاد اسواق اكثر اتساعا. ونتيجة لذلك فقد تحول العديد من شركات الاعمال إلى استخدام الإنترنت والاستفادة من مزايا التجارة الإلكترونية، كما نحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطرا متوافقا مع التجارة الإلكترونية.

فالاستيلاء على بطاقات الائتمان عبر الإنترنت امر ليس بالصعوبة بمكان اطلاقا، فـ" لصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الالوف من ارقام البطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات للاخرين " (داود، ١٤٢٠هـ: ٧٣)، وقد وقعت بالفعل عدة حوادث ومن ذلك حادثة شخص الماني قام بالدخول غير المشروع إلى احد مزود الخدمات واستولى على ارقام بطاقات ائتمانية الخاصة بالمشتركين ومن ثم هدد مزود الخدمة بافشاء ارقام تلك البطاقات ما لم يستلم فدية وقد تمكنت الشرطة الالمانية من القبض عليه. كما قام شخصان في عام (١٩٩٤م) بانشاء موقع على الإنترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها الكترونيا، ولم تكن الطلبات لتصل اطلاقا حيث كان الموقع وهمي قصد منه النصب والاحتيال وقد قبض على مؤسسيه لاحقا (موثق في عبدالمطلب، ٢٠٠١م: ٨٥)

واثبت شبكة (MSNBC) عمليا سهولة الحصول على ارقام بطاقات الائتمان من الإنترنت، حيث قامت بعرض قوائم تحتوي على اكثر من (٢٥٠٠) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بيانات متوفرة تجاريا، ولم يكن يصعب على اي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على ارقام تلك البطاقات واستخدامها في عمليات شراء يدفع قيمتها اصحابها الحقيقين. ويقترح بعض الخبراء باستخدام بطاقة ائتمان خاصة بالإنترنت يكون حدها الائتماني معقول بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الامر الذي بدأت بعض البنوك الدولية والمحلية في تطبيقه اخيرا (عبدالمطلب،٢٠٠١م: ٨٦ - ٩٠).

ويتعدى الامر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الإلكترونية (Electronic Cach) أو (Cyber Cash) والتي يتنبأ لها ان تكون

مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان) وأن يزداد الاعتماد عليها والثقة بها، كما ان هناك الاسهم والسندات الإلكترونية المعمول بها في دول الاتحاد الأوروبي والتي اقر الكونجرس الامريكي التعامل بها في عام ١٩٩٠م، وبالتالي فان التعامل معها من خلال الإنترنت سيواجه مخاطر امنية ولا شك.

ولذلك لجأت بعض الشركات والبنوك إلى العمل سويا لتجاوز هذه المخاطر كالاتفاق الذي وقع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC) وهي من اكبر المؤسسات المصرفية في هونج كونج وشركة كومباك للحاسب الآلي وذلك لتطوير أول نظام الي آمن للتجارة الالتكرونية والذي يمنح التجار خدمة نظام دفع امن لتمرير عمليات الشراء عبر الإنترنت (داود، ١٤٢٠هـ : ١٢٣ - ١٢٤).

وجرائم السطو على أرقام البطاقات الائتمانية مُجَّرمة شرعا وقانونا حيث تصنف ضمن جرائم السرقات، "فالشارع الاسلامي يرغب في المحافظة على اموال الناس وصيانتها من كل اعتداء غير مشروع بحيث يهدد الامن والاستقرار" (فرحات،١٤٠٤هـ:٢٩).

والسرقة من الكبائر المحرمة التي نصت الايات القرآنية والاحاديث النبوية على تحريمها ووضعت عقوبة رادعة لمرتكبها. قال تعإلى في سورة المائدة ?السَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ (٣٨) ?

بل لعن رسول الله 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 الايمان 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".

القمار عبر الإنترنت:

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

ويوجد على الإنترنت اكثر من الف موقع للقمار يسمح لمرتاديه من مستخدمى الإنترنت ممارسة جميع انواع القمار التي توفرها المواقع الحقيقية، ومن المتوقع ان ينفق الامريكيون ما يزيد عن (٦٠٠) مليار دولار سنويا في اندية القمار وسيكون نصيب مواقع الإنترنت منها حوالي مليار دولار.

وقد حاول المشرعون الامريكيون تحريك مشروع قانون يمنع المقامرة عبر الإنترنت ويسمح بملاحقة اللذين يستخدمون المقامرة السلكية أو اللذين يروجون لها سواء كانت هذه المواقع في امريكا أو خارجها (عبدالمطلب، ٢٠٠١م: ٧٨ - ٨٢).

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

ينظر الاسلام إلى القمار كمحظور شرعي منهي عن فعله وماعقب على ارتكابه، وقد وردت ادلة متعددة في كتاب الله وفي كتب الاحاديث، اما دليل تحريم القمار من القرآن فهو قوله تعإلى في سورة المائدة (يَاأَيُّهَا الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالْأَنصَابُ وَالْأَزْلَامُ رِجْسٌ مِنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ) (٩٠)

ولم يكتفي الشرع بالنهي عن هذا الفعل بل وضح لاتباعه ان هذا العمل انما هو من اعمال الشيطان التي يسعى من خلالها إلى ايقاع العداوة والبغضاء بين الناس ووضح ان في اجتاب هذا الفعل فلاح وصلاح وفوز في الدنيا والاخرة، قال تعالى في سورة المائدة: (إِنَّمَا يُرِيدُ الشَّيْطَانُ أَنْ يُوقِعَ بَيْنَكُمُ الْعَدَاوَةَ وَالْبَغْضَاءَ فِي الْخَمْرِ وَالْمَيْسِرِ وَيَصُدَّكُمْ عَنْ ذِكْرِ اللَّهِ وَعَنِ الصَّلَاةِ فَهَلْ أَنْتُمْ مُنْتَهُونَ) (٩١)

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

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

تزوير البيانات:

تعتبر من اكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من اشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك. وقد وقعت حادثة في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي بحث تصبح باسم احد لصوص

السيارات والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للابلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تقوم تلك الفتاة باعادة تسجيل السيارة باسم مالكها وكانت تتقاضي مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى ان قبض عليها، وفي حادثة الخرى قام مشرف تشغيل الحاسب باحد البنوك الأمريكية بعملية تزوير حسابات اصدقائه في البنك بحيث تزيد ارصدتهم ومن ثم يتم سحب تلك المبالغ من قبل اصدقائه وقد نجح في ذلك وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك الا ان طمع اصدقاءه اجبره على الاستمرار إلى ان قبض عليه (داود، ١٤٢٠هـ:٤٥- ٤٧).

ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة اهدافهم الإجرامية. وجرائم التزوير ليست بالجرائم الحديثة، ولذا فانه لاتخلوا الأنظمة من قوانيين واضحة لمكافحتها والتعامل معها جنائيا وقضائيا و" تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها" (داود، ١٤٢١هـ: ٦٧).

وعالجت أنظمة المملكة العربية السعودية جرائم التزوير بشكل مفصل حيث صدر المرسوم الملكي رقم (١١٤) وتاريخ ١٣٨٠/١١/٢٦هـ بالمصادقة على نظام مكافحة التزوير، ومن ثم تم التعديل على هذا النظام ليواكب المستجدات وذلك بالمرسوم 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).

الجرائم المنظمة:

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من اشهر المؤسسات الإجرامية المنظمة والتي بادرت بالاخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ اعمالها، ومن ذلك انشاء مواقع خاصة بها على شبكة الإنترنت لمساعدتها في ادارة العمليات

وتلقي المراسلات واصطياد الضحايا وتوسيع اعمال وغسيل الاموال، كما تستخدم تلك المواقع في انشاء مواقع افتراضية تساعد المنظمة في تجاوز قوانين بلد محدد بحيث تعمل في بلد اخر يسمح بتلك الانشطة.

ويوجد على الشبكة (٢١٠) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (٢٤) موقعا يحتوى على كلمة مافيا، كما وجد (٤) مواقع للمافيا اليهودية. وقد خصص بعض هذه المواقع للاعضاء فقط ولم يسمح لغيرهم بتصفح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفح الموقع وقامت مواقع أخرى بوضع استمارة تسجيل لمن يرغب في الانضمام إلى العصابة من الاعضاء الجدد (الجنيدي(أ)، ١٩٩٩م: ٣٦).

والجريمة المنظمة ليست وليدة التقدم التقني وإن كانت استفادت كثيرا منه فـ" الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنلوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان وأن ما أصبح إنتشارها على نطاق واسع وكبير وأصبحت لاتحدها الحدود الجغرافية" (اليوسف، ١٤٢٠هـ، ص: ٢٠١)، كما أستغلت عصابات الجريمة المنظمة " الامكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة " (حبوش،١٤٢٠هـ: ٢٥٣).

وهناك من يرى ان الجريمة المنظمة والارهاب هما وجهان لعملة واحدة، فأوجه التشابه بينهما كبير حيث يسعى كلاهما إلى إفشاء الرعب والخوف، كما انهما يتفقان في اسلوب العمل والتنظيم وقد يكون اعضاء المنظمات الارهابية هم اساساً من محترفي الجرائم المنظمة حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صلة وتعاون وثيق بينهما (عزالدين، ١٤١٤هـ: ٢٣- ٣٥).

وحظيت مكافحة الجريمة المنظمة باهتمام دولي بدأ بمؤتمر الامم المتحدة السابع عام (١٩٨٥م) لمنع الجريمة حيث اعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة والقضاء عليها.

وتبع ذلك الاجتماع الاقاليمي التحضيري عام (١٩٨٨م) الذي أقر فيه المبادئ التوجيهية لمنع الجريمة المنظمة ومكافحتها، ثم المؤتمر الثامن لمنع الجريمة بفنزويلا عام (١٩٩٠م)، فالمؤتمر الوزاري العالمي المعنى بالجريمة المنظمة عبر الوطنية في نابولي بايطاليا عام (١٩٩٤م) والذي عبّر عن ارادة المجتمع الدولي بتعزيز التعاون الدولي واعطاء أولوية عليا لمكافحة الجريمة المنظمة.

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

تجارة المخدرات عبر الإنترنت:

كثيرا ما يحذّر أولياء الامور ابنائهم من رفقاء السوء خشية من تأثيرهم السلبي عليهم وخاصة في تعريفهم على المخدرات فالصاحب ساحب كما يقول المثل وهذا صحيح ولا غبار عليه ولكن وفي عصر الإنترنت اضيف إلى أولياء الامور مخأوف جديدة لا تقتصر على رفقاء السوء فقط بل يمكن ان يضاف اليها مواقع السوء - ان صح التعبير- ومن تلك المواقع طبعا المواقع المنتشرة في الإنترنت والتي لاتتعلق بالترويج للمخدرات وتشويق النشئ لاستخدانها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة اصنافها وأن واعها وبأبسط الوسائل المتاحة.

والامر هنا لايحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى اي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخأوف أحد الخبراء التربوين في بتسبيرج بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات وانترنت.

ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تسأهم المنتديات وغرف الدردشة في ذلك ايضا. وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها الا ان هذه

المواقع لم تدق جرس الانذار بعد ولم يهتم باثارها السلبية وخاصة على النشئ كما فعلته المواقع الاباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة.

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

وبالإضافة إلى هذا الموقع توجد مواقع أخرى تحارب المخدرات وتساعد المدمنين على تجاوز محنتهم ومن ذلك الموقع الخاص بجماعة (Join-Together) وعنوانهم على النت هو http://٢١,١٩١,١٢,١٩٢ إلا أن هذه المواقع قليلة العدد والفائدة مقارنة بكثرة وقوة المواقع المضادة (الجنيدي(ب)، ١٩٩٩م: ٣٩-٤٠).

واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات وعقدت المؤتمرات والاتفاقيات الدولية المختلفة ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (١٩٦١م)، اتفاقية المؤثرات العقلية عام (١٩٧١م)، واتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية عام (١٩٨٨م).

وعلى المستوى العربي تم عام (١٩٩٦م) اقرار الاتفاقية العربية لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، كما تم عام (١٩٨٦م) اقرار القانون العربي النموذجي الموحد للمخدرات.

اما على المستوى المحلي فقد صدر نظام مكافحة الاتجار بالمواد المخدرة في المملكة العربية السعودية بقرار مجلس الوزراء رقم (١١) عام (١٣٧٤هـ) والحق به قرار هيئة كبار العلماء رقم (١٣٨) وتاريخ ١٤٠٧/٦/٢٠هـ الخاص باعدام مهربي المخدرات أو من يقبض عليه في قضية ترويج للمرة الثانية، والموافق عليه بالامر السامي رقم (٤/ب/٩٦٦) وتاريخ ١٤٠٧/٧/١٠هـ (عيد، ١٤٢٢هـ:٩٤-١١٠)

غسيل الاموال:

مصطلح حديث نسبيا ولم يكن معروفا لرجال الشرطة فضلا عن العامة وقد بدأ استخدام المصطلح في امريكا نسبة إلى مؤسسات الغسيل التي تملكها المافيا، وكان أول استعمال قانوني لها في عام (١٩٣١م) إثر محاكمة لاحد زعماء المافيا تمت في امريكا واشتملت مصادرة اموال قيل انها متأتية من الاتجار غير المشروع بالمخدرات.

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

ومن البديهي ان ياخذ المجرمون باحدث ما توصلت اليه التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التي استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسعة وتسريع اعمالها في غسيل اموالها غير المشروعة، ويجد المتصفح للانترنت مواقع متعددة تتحدث عن غسيل اموال ومنها الموقع:http://www.laundryman.u.net.com كما يجد ولا شك ايضا المواقع التي تستخدم كساتر لعمليات غسيل الاموال ومنها المواقع الافتراضية لنوادي القمار والتي قام مكتب المباحث الفدرالية(FBI) الامريكي بمراقبة بعض هذه المواقع واتضح انها تتواجد في كاراكاو، جزر الانتيل، جزيرة أنتيجوا وجمهورية الدومينكان وقد اسفرت التحريات التي استمرت خمسة اشهر عن اعتقالات واتهامات للعديد من مدراء تلك المواقع.

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

كل هذا جعل عمليات غسيل الاموال عبر الإنترنت تتم بسرعة اكبر وبدون ترك اي اثار في الغالب. ويقدر المتخصصون المبالغ التي يتم تنظيفها سنويا بحوالي (٤٠٠) مليار دولار (عبدالمطلب،٢٠٠١م: ٦٨ - ٧٢).

وإلى عهد قريب لم تكن جرائم غسيل اموال تشكل جرما بذاتها إلى ان تضخمت الاموال المتحصلة من الجرائم وخاصة من تجارة المخدرات فاصدرت بعض الدول قوانين خاصة تسمح بتعقب وتجميد ومصادرة عائدات الجرائم الخطرة، فأصدرت الولايات المتحد الأمريكية عام (١٩٧٠م) قانون المنظمات القائمة على الابتزاز والنساء، وقانون منع ومكافحة جرائم اساءة إستخدام العقاقير المخدرة، كما اصدرت مصر عام (١٩٧١م) القانون رقم (٣٤) والخاص بتنظيم فرض الحراسة على الاموال المكتسبة بطرق غير مشروعة، كما اقر القانون العربي النموذجي الموحد للمخدرات الصادر عن مجلس وزراء الداخلية العرب عام (١٩٨٦م) مكافحة جرائم غسيل الاموال وخاصة في مادته التاسعة والاربعون والتي سمحت للمحكمة المختصة بحجز الاموال المتحصلة من تجارة المخدرات والتحقق من مصادر تلك الاموال. كما اصدرت بريطانيا وايرلندا عام (١٩٨٦م) قانون يسمح بمصادرة عائدات الجريمة. واصدرت استراليا عام (١٩٨٧م) قانونا يسمح بمصادرة اموال الشخص المدان في جرائم اتحادية.

ولم تتخلف المملكة العربية السعودية عن ركب محاربة جرائم غسيل الاموال فقد كانت المملكة من ضمن دول العالم الـ(١٠٦) اللذين وقعوا عام (١٩٨٨م) على اتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية والتي كانت أول خطوة دولية مهمة لتعريف غسيل الاموال وتحديد الافعال الواجب تجريمها (عيد، ١٤١٩هـ: ٢٦٣-٣١٩)

المواقع المعادية:

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

ففي المواقع السياسية المعادية يتم غالبا تلفيق الاخبار والمعلومات ولو زورا وبهتانا أو حتى الاستناد إلى جزيئ بسيط جدا من الحقيقة ومن ثم نسج الاخبار الملفقة حولها، وغالبا ما يعمد اصحاب تلك المواقع إلى انشاء قاعدة بيانات بعناوين اشخاص يحصلون عليها من الشركات

التي تبيع قواعد البيانات تلك أو بطرق أخرى ومن ثم يضيفون تلك العناوين قسرا إلى قائمتهم البريدية ويبدأو في اغراق تلك العناوين بمنشوراتهم، وهم عادة يلجئون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولايصال اصواتهم إلى اكبر قدر ممكن.

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

موقع http://www.answering-islam.org/

وموقع http://www.aboutislam.com/

وموقع http://www.thequran.com/

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

وهناك مواقع معادية لاشخاص أو جهات وهي قد تكون شبيهة وإلى حد كبير بالمواقع المخصصة للقذف التي سبق التحدث عنها سابقا في القسم الخاص بالجرائم الجنسية، حيث تهدف اساسا لتشويه سمعة الشخص أو الجهة ولذلك فسيكتفى بما سبق التطرق اليه في هذا المجال وسيركز على الحديث عن المواقع السياسية والدينية والتي لم يتم التطرق لها.

والمواقع المعادية بانواعها مخالفة نظامية وجريمة جنائية وتفصيل ذلك كالاتي:

أ. المواقع السياسية المعادية: قد ينظر البعض إلى إنشاء هذه المواقع كظاهرة حضارية تتمشي مع الديموقراطية والحرية الشخصية، وهذا غير صحيح فللديموقراطية والحرية الشخصية حدود يجب ان لاتتجاوزها والا اصبحت سوء ادب وبغي. وهناك ولا شك طرق واساليب يمكن معها التعبير عن الاراء الشخصية وضّحتها الشريعة الاسلامية قبل الديمقراطية الوضعية، وحددتها عاداتانا

وتقاليدنا المنبثقة من قيمنا العربية الاصيلة في حين غفلت عنها قيم الدول الغربية وابسط هذه القواعد ان 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 ال عمران (فَبِمَا رَحْمَةٍ مِنَ اللَّهِ لِنْتَ لَهُمْ وَلَوْ كُنْتَ فَظًّا غَلِيظَ الْقَلْبِ لَانْفَضُّوا مِنْ حَوْلِكَ فَاعْفُ عَنْهُمْ وَاسْتَغْفِرْ لَهُمْ وَشَاوِرْهُمْ فِي الْأَمْرِ فَإِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى اللَّهِ إِنَّ اللَّهَ يُحِبُّ الْمُتَوَكِّلِينَ) (١٥٩) ، كما ان من الآداب ان يكون النقد أو النصيحة في السر لا في العلن وفي هذا يقول الامام الشافعي: تعمدني بنصحك في انفراد وجنبني النصيحة في الجماعة

فإن النصح بين الناس نوع من التوبيخ لا ارضى استماعه

وان خالفتني وعصيت قولي فلا تجزع إذا لم تعط طاعة

وهذه الاداب هي ابسط الاداب الواجب اتباعها مع العامة فما بالك مع ولي الامر الذي قرن الله طاعته بطاعة الله ورسوله – مالم يأمر ولي الامر بأمر مخالف لله – ولذلك فليس في إنشاء المواقع السياسية المعادية أي حرية رأي أو ديمقراطية بل هي سوء ادب ان لم يكن بغي يعاقب عليه الشرع بالقتل فـ" جريمة البغي موجهة إلى نظام الحكم والقائمين بأمره، وقد تشددت فيها الشريعة؛ لإن التساهل فيها يؤدي إلى الفتن والاضطرابات وعدم الاستقرار وهذا يؤدي بدوره إلى تأخر الجماعة وانحلالها. ولا شك ان عقوبة القتل أقدر العقوبات على صرف الناس عن هذه الجريمة التي يدفع اليها الطمع وحب الاستيلاء" (عودة، ١٤٠١هـ:٦٦٣).

والدليل على ان البغي محرم شرعا ومعاقب عليه بالقتل قوله تعالى في سورة الحجرات (وَإِنْ طَائِفَتَانِ مِنَ الْمُؤْمِنِينَ اقْتَتَلُوا فَأَصْلِحُوا بَيْنَهُمَا فَإِنْ بَغَتْ إِحْدَاهُمَا عَلَى الْأُخْرَى فَقَاتِلُوا الَّتِي تَبْغِي حَتَّى تَفِيءَ إِلَى أَمْرِ اللَّهِ فَإِنْ فَاءَتْ فَأَصْلِحُوا بَيْنَهُمَا بِالْعَدْلِ وَأَقْسِطُوا إِنَّ اللَّهَ يُحِبُّ الْمُقْسِطِينَ) (٩) ؟، وفي الحديث الشريف الذي رواه مسلم "إنه ستكون هنّات وهنّات، فمن أراد أن يفرق أمر هذه الأمة، وهي جميع، فاضربوه بالسيف، كائناً من كان" كما ورد عن رسول الله صلى الله عليه وسلم

حديثا رواه مسلم وابي داود واللفظ لابي دواد: عن عبد الله بن عمرو أن النبي صلى الله عليه و سلم قال" من بايع إماماً فأعطاه صفقة يده وثمرة قلبه فليطعمه 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 القوانيين الوضعية وإلى عهد قريب تعتبر الجريمة السياسية أشد خطرا من الجريمة العادية، بل كانت تعامل المجرم السياسي معاملة تتنافى مع ابسط قواعد العدالة حيث تشدد عليه العقوبة وتصادر امواله وتعاقب اهله بجريمته (عودة، ١٤٠١هـ: ١٠٧).

ب. المواقع الدينية المعادية: الدين الاسلامي هو خاتم الاديان السماوية وبه أكمل رسوله صلى الله عليه وسلم تعاليم الدين قال تعالى في سورة المائدة (الْيَوْمَ أَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتْمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمُ الْإِسْلَامَ دِينًا فَمَنْ اضْطُرَّ فِي مَخْمَصَةٍ غَيْرَ مُتَجَانِفٍ لِإِثْمٍ فَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ) (٣) ، ولذلك فلا يقبل أي دين غير الاسلام قال تعالى في سورة ال عمران (وَمَنْ يَبْتَغِ غَيْرَ الْإِسْلَامِ دِينًا فَلَنْ يُقْبَلَ مِنْهُ وَهُوَ فِي الْآخِرَةِ مِنَ الْخَاسِرِينَ) (٨٥) ، ليس ذلك فحسب بل عاقب من بدل دينه بعد اسلامه ففي الحديث الذي رواه البخاري قال النبي صلى الله عليه وسلم: «من بدل دينه فاقتلوه»

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

جرائم القرصنة:

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

وقدتطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت

واصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي.

وادت قرصنة البرامج إلى خسائر مادية باهضة جدا وصلت في العام (١٩٨٨م) إلى (١١) مليار دولار امريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وأن شاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الاعمال (Busines Software Alliance) أو ما تعرف اختصارا بـ(BSA)، والتي اجرت دراسة تبين منها ان القرصنة على الإنترنت ستطغى على انواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة الا ان تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت.

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

والقرصنة عربيا لا تختلف كثيرا عن القرصنة عالميا ان لم تسبقها بخطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين ان وجدت (الجنيدي، نوفمبر ١٩٩٩م: ٢٨-٣٥).

وقوانيين حماية الملكية تعتبر من الأنظمة الحديثة في الدول العربية حيث بدأت الفكرة من الدول الرأسمالية ومن ثم بدأت الدول الأخرى تطبيقها وادراجها في انظمتها، وقد اهتمت دول الخليج بحماية الملكية الفكرية ايضا فقامت امانة مجلس التعاون الخليجي وفي الاجتماع الثاني للوزراء المسئولين عن الثقافة المنعقد بالرياض في ١٩٨٧/٩/١٥م بوضع لائحة استرشادية للنظام الموحد لحماية حقوق المؤلف في دول المجلس (موقع مجلس التعاون لدول الخليج العربية، ١٤٢٣هـ).

ولم يكن هذا هو اخر المشوار بل البداية حيث توالت دول الخليج في اصدار قوانيين الحماية الفكرية، ففي سلطنة عمان 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.

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

ووافق مجلس الوزراء الموقر في جلسته بتاريخ ١٤٢٠/٦/١٧هـ على تشكيل اللجنة الدائمة لحقوق الملكية الفكرية من ممثلين عن وزارات التجارة، الإعلام، الداخلية، الخارجية، العدل، الصناعة والكهرباء، البترول والثروة المعدنية، المالية والاقتصاد الوطني (مصلحة الجمارك)، ديوان المظالم، ومدينة الملك عبدالعزيز للعلوم والتقنية، ويكون مقرها ورئاستها بوزارة التجارة، وحددت 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 إتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (موقع وزارة التجارة، ١٤٢٣هـ).

جرائم اختراقات أخرى لم تتطرق اليها الدراسة:

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

الا انه ونظرا لاهمية هذه الجرائم على المستوى الامني وجب اخذ الاحتياطات اللازمة للتوقي منها واخذها في الحسبان عند وضع الضوابط النظامية للتعامل مع جرائم الإنترنت وللفت نظر الباحثين في هذا المجال، ولذا وجب التطرق اليها هنا بالشرح والايضاح وهذه الجرائم:

١. التجسس الإلكتروني:

" في عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي" (البداينة، ١٩٨٨م)، والعالم العربي والاسلامي كان ولا يزال مستهدف امنيا وثقافيا وفكريا وعقديا لاسباب لاتخفى على احد.

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

ولا تكمن الخطورة في استخدام الإنترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولايمكن حتما الاعتماد على وسائل الحماية التي تنتجها الشركات الاجنبية فهي ليست في مأمن ولا يمكن الاطمئنان لها تماما.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحا (hackers) فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو اتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع امن، اما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على اسرار ومعلومات الدولة ومن ثم افشائها لدول أخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية للدولة.

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

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

وخصص هذا النظام للتعامل مع الاهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلة جدا من الاتصالات والرسائل الالكترونية عشوائيا باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة والتي تم انشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الاقمار الصناعية الواقعة في منطقة واي هوباي بجنوب نيوزيلندا، ومحطة جير الدتون الموجودة باستراليا، والمحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة شوجرجروف وتبعد (٢٥٠) كيلومترا جنوب واشنطن دي سي، وايضا المحطة الموجودة بولاية واشنطن على بعد (٢٠٠) كيلومتر جنوب غرب مدينة سياتل.

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

أي انه يرصد جميع الاتصالات التي تتم بأي وسيلة. ويعتبر الافراد والمنظمات والحكومات اللذين لا يستخدمون أنظمة الشفرة التامينية أو أنظمة كودية لحماية شبكاتهم واجهزتهم، اهدافا سهلة لشبكة التجسس هذه، وأن كان هذا لا يعنى بالضرورة ان الاهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها، ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية (عبدالمطلب، ٢٠٠١م: ٣٠-٤٥).

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى اهداف 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 اظهر استفتاء اجرى عام (١٩٩٦م) لمسؤلي الامن الصناعي في الشركات الامريكة حصول الكثير من الدول وبشكل غير مشرع على معلومات سرية لانشطة تجارية وصناعية في الولايات المتحدة الأمريكية(داود،١٤٢٠هـ: ٦٢).

ومن الاساليب الحديثة للتجسس الإلكتروني اسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وإن كان ليس بالامر السهل، ويتلخص هذا الاسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك احد في ان هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبسا، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية (داود، ١٤٢٠هـ: ٦٧).

وبعد الاعتداءات الاخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطات الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصا لالتقاط الاتصالات التي تجرى عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صورا فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة 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 الصناعية حتى إن كانت واهنة أو مشفرة (BBC،٢٠٠١).

الارهاب الإلكتروني:

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

وقد انتبه الغرب إلى قضية الارهاب الإلكتروني منذ فترة مبكرة، فقد شكل الرئيس الامريكي بيل كلنتون لجنة خاصة (www.nipc.gov) مهمتها حماية البنية التحتية الحساسة في امريكا، والتي قامت في خطوة أولى بتحديد الاهداف المحتملة استهدافها من قبل الارهابين ومنها مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الحاسب الآلي، ومن ثم تم انشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات أي هجمات ارهابية الكترونية.

كما قامت وكالة الاستخبارات المركزية بانشاء مركز حروب المعلوماتية وظفت به الفا من خبراء امن المعلومات، كما شكلت قوة ضاربة لمواجهة الارهاب على مدار الساعة ولم يقتصر هذا الامر 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 الكترونية)) وتوقع التقرير ان يزداد الهجوم على نظم المعلومات في الولايات المتحدة الأمريكية من قبل الجماعات الارهابية أو عملاء المخابرات الاجنبية وأن يصل هذا الهجوم إلى ذروته عام (٢٠٠٥م)، وأوضح التقرير ان شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في امريكا معرضة للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية دون ان تواجه قواتها المسلحة (داود، ١٤٢٠هـ).

وبعد الهجمات الاخيرة على الولايات المتحدة الأمريكية ارتفعت اصوات البعض بممارسة الارهاب الإلكتروني ضد المواقع الاسلامية والعربية التي يشتبه بانها تدعم الارهاب، وأوردت شبكة

(CNET) الاخبارية خبرا عن اتفاق (٦٠) خبيرا في امن الشبكات ببدء تلك الهجمات الارهابية على مواقع فلسطينية وافغانية.

جرائم ذوي الياقات البيضاء:

هذا المصطلح من الجرائم حديث نسبياً، وأول من اطلقته عالم الاجتماع سذرلاند (Sutherland) حيث وضّح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الادارية الكبيرة، وتشمل انواعا 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 المشاكل يصعب ارتكابها أو كشفها والتحقيق فيها دون المام جيد بظروف الانتاج والحسابات الجارية والعمل التجاري ومبادي التقنية الحسابية الالتكرونية. وقدرت خسائر المجتمع الامريكي بمبلغ (١٢- ٤٢) مليون دولار سنويا نتيجة خداع المستهلكين باستخدام جميع وسائل التكنلوجيا المتقدمة(اليوسف،١٤٢٠هـ: ٢٠٩-٢١١).

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

الجرائم الاقتصادية:

تتنوع الجرائم الاقتصادية بتنوع النظام السائد في الدولة فعلى سبيل المثال في الدول الراسمالية نجد ان اغلب الجرائم الاقتصادية تتمحور حول الاحتكارات والتهرب الضريبي والجمركي والسطو على المصارف وتجارة الرقيق الابيض والاطفال، في حين تتمحور تلك الجرائم في النظام الاشتراكي على الرشوة والاختلاس والسوق السوداء.

وهذا لا يعنى بالضرورة انه لايمكن ارتكاب كل انواع هذه الجرائم في مجتمع واحد حيث يمكن ان تجد في المجتمع الراسمالي مثلا جرائم رشوة واختلاسات والعكس صحيح.وكما في الجرائم

الأخرى فان الإنترنت ساهم في تطوير طرق واساليب ارتكاب هذه الجرائم ووسّع منطقة عملها،خاصة مع توجه الكثير من الدول في التحول إلى الحكومات اللالكترونية كما في دولة الامارات العربية المتحدة مثلا، حيث استفاد المجرمون من التقدم التقني في اختلاس الاموال وتحويل الارصدة النقدية وكذلك في سرقة التيار الكهربائي والمياه وخطوط الهاتف والعبث بها واتلافها (اليوسف،١٤٢٠هـ: ٢١١-٢١٤).