الجلسة السادسة

الجريمة المعاصرة: والاستخدامات السلبية للتقنية

الورقة الرابعة

جرائم الكمبيوتر والانترنت

إعداد

ملازم أول / سعود وصل الله سعد الثبيتي

الـــورقـــة الـرابـــعـــة

جرائم الـكـمـبـيـوتر والانـتـرنـت

إعـــــــداد

ملازم أول / سعود وصل الله سعد الثبيتي

شرطة محافظة الطائف

مـقـــدمـــة

الحمد لله الذي خلق الإنسان من عدم وعلمه ما لم يعلم ورغبه في العلم والتعلم والصلاة والسلام على سيدنا محمد ورسوله البشير النذير، السراج المنير، المبعوث إلى كافة الخلق من غني وفقير ومأمور وأمير. وحسبنا الله ونعم الوكيل، نعم المولى ونعم النصير.

الجريمة كما يعلم الجميع، بدأت منذ بداية وجود الإنسان على سطح الأرض فهي ليست حديثة ولكن ما يمكن القول بأنه متغيراً أو متطور في الجريمة هو أساليب تنفيذها، وكذلك اختلاف أدواتها وأهدافها. ولا شك أن الجريمة تتطور بتطور التكنولوجيا فالمجرمين يحاولون الاستفادة من هذا التقدم لذلك نرى أنه ليس مستغرب أن تظهر أنماط من الجرائم لم تكن موجودة في السابق.

وفي عصرنا هذا نلاحظ أن العالم قد شهد تقدما تكنولوجياً لم يسبق له مثيل وقد نتج عن ذلك ظهور وسائل اتصال متطورة جعلت العالم قرية واحدة مفتوحة، وتلاشت معها الحدود الجغرافية وكذلك الحدود السياسية للدول، والانترنت سلاح ذو حدين فيمكن استخدامها في الخير والتطور، وبالإمكان استخدامها في الشر والتخريب. ويتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، ومن الوجهة التقنية بين الحاسوب أداة الجريمة وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدف.

مشكلة البحث:

تتحدد مشكلة البحث في تحديد حجم وأنواع جرائم الانترنت ومعرفة الأكثر شيوعا بين مستخدمي الانترنت في المجتمع السعودي. وكذلك المساهمة في وضع عقوبات لمرتكبي هذا النوع من الجرائم.

أهمية البحث:

تنبثق أهمية هذا البحث من حيث أنها محاولة لإلقاء الضوء على حجم وأنواع جرائم الانترنت في المجتمع السعودي وبالتالي يمكن من خلالها الاستفادة في مواجهة هذه الجرائم الحديثة والتعامل معها ومكافحتها، وكذلك لفت انتباه رجال القضاء والقانون إلى هذه الجرائم لوضع لوائح قانونية وقضائية تتناسب مع هذه الجريمة ومرتكبيها.

أهداف البحث:

١- التعرف على أنواع جرائم الانترنت الأكثر شيوعاً في المملكة ودراستها دراسة مستفيضة.

٢- الكشف عن الآثار المختلفة للظاهرة الإجرامية المعاصرة سواءً الظواهر الاجتماعية أو الاقتصادية أو الأمنية أو النفسية.

٣- لفت انتباه الجهاز القضائي والقانوني إلى جرائم جديدة قد ترتكب ضد الآخرين والمجتمع بواسطة الحاسب الآلي ومن خلال الشبكة العنكبوتية والانترنت، من أجل وضع لوائح وأنظمة قانونية وقضائية رادعة لهؤلاء المجرمين.

٤- نشر الوعي بين منسوبي السلطات الأمنية والقضائية ورفع مستوى الكفاءة لديهم من خلال عقد الدورات المتقدمة في هذا النمط من الجرائم. وتأهيلهم على كيفية التعامل معها وتدريبهم على دراسة وتحليل الأدلة.

جرائم الكمبيوتر والانترنت مفهومها وتاريخها وأنواعها

المبحث الأول: تعاريف ومصطلحات:

هناك تباين كبير بشأن الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر، وهذا التباين بلا شك رافق سيرة نشأة وتطور ظاهرة الإجرام المرتبطة أو المتصلة بتقنية المعلومات، فابتداء من اصطلاح إساءة استخدام الكمبيوتر واصطلاح احتيال الكمبيوتر، ووصولاً إلى جرائم الهاكرز أو الاختراقات وجرائم الانترنت.

ولأن الدقة العلمية تقتضي انطباق الوصف على الموصوف فقد شاعت هناك مصطلحات وتعبيرات كثيرة مع بدايات الظاهرة واتسع استخدامها حتى عند الدارسين القانونيين كالغش المعلوماتي أو غش الحاسوب وإساءة استخدام الكمبيوتر واصطلاح جرائم أصحاب الياقات البيضاء والجرائم الاقتصادية المرتبطة بالكمبيوتر والانترنت، وهذه جرائم منها المتعدي الذي يشمل أكثر من جرائم الكمبيوتر والانترنت، جرائم أصحاب الياقات البيضاء، ومنها الذي يقتصر على نوع من الأنواع كالجرائم الاقتصادية. لذلك فإن الاصطلاح لا يكون دقيقاً في التعبير عن الظاهرة.

واستخدام اصطلاح جرائم الكمبيوتر والانترنت أو استخدام اصطلاح (cyber crime) هو اصطلاح شامل لجرائم الكمبيوتر وجرائم الشبكات. وفي مضمونة يشمل هذا الاصطلاح الجرائم التي تستهدف النظم والمعلومات كهدف (جرائم الكمبيوتر). والجرائم التي تستخدم الكمبيوتر وسيلة لارتكاب جرائم أخرى (الجرائم المتعلقة بالكمبيوتر).

ونريد هنا إيضاح بفعل المفاهيم الرئيسية التي سيتعرض لها البحث.

٢) الحاسب الآلي: يمكن أن يعرف بأنه مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة من الأجهزة التي تعمل طبقاً لبرنامج تم

وضعه مسبقاً للحصول على نتائج معينة (تشفوش، ١٩٩٢م:٦).

في نطاق القانون الجنائي: (فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً).

١) الجريمة: محظور شرعي زجر الله عنه بحد أو تعزيز.

٢) الانترنت: تعني لغوياً ترابط بين شبكات حيث يتكون الانترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء العالم ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الانترنت (الفنتوخ ١٤٢١١: ١١).

٣) جرائم الكمبيوتر والانترنت: هو ذلك النوع من الجرائم الذي يتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق منها ومقاضاة فاعليها (مندوره، ١٤١٠: ٢١).

كما يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً.

ويعرّفها تاديجان بأنها: (كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب).

المبحث الثاني: لمحة تاريخية

يعتبر الانترنت هو ثمرة التقدم العلمي العالمي في مجال الاتصالات وتبادل المعلومات، وتعتبر شبكة الانترنت

هي الشبكة الرئيسية التي تجتمع تحت كافة الشبكات الأخرى أيا كان نوعها أو الغاية منها.

وبدأ العمل بالانترنت بتاريخ ١٩٦٩/١/٢م عندما كونت وزارة الدفاع الأمريكية فريقاً بحثياً من العلماء يهدف لإنشاء مشروع بحثي كان موضوعه هو تشبيك الحاسبات. وكان أساس البحث في هذا المشروع البحثي بجانب إنشاء الشبكات هو تجزئة الرسالة المراد إرسالها إلى موقع معين في الشبكة ومن ثم يتم نقل كل جزء من تلك الأجزاء بطريق مختلف عن الطريق الذي تسلكه الأجزاء الأخرى من الرسالة مرة أخرى، كما كانت مرسله. وكان ذلك إبان الحرب التي أطلق عليها مصطلح (الحرب الباردة) التي كانت قائمة بين الاتحاد السوفيتي والولايات المتحدة الأمريكية.

ثم تطور المشروع بعد ذلك إلى الاستعمال السلمي بجانب الاستعمال العسكري حيث أنقسم عام ١٩٨٣م إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي وبالغرض الذي نشأت من أجله وهو خدمة جهاز المخابرات المركزية الأمريكية ويرمز إليها بـ (CIA) وسميت الشبكة الأخرى باسم (MAIL NET)، وخصصت هذه الشبكة للاستخدام المدني ومن ثم ظهر اسم انترنت.

وفي عام ١٩٨٦م تمَّ ربط خمس مراكز للكمبيوترات العملاقة وأطلق عليها اسم (NSF NET) وأصبحت فيما بعد العامود الفقري والأساسي لنمو وازدهار شبكة الانترنت في الولايات المتحدة الأمريكية ثم دول العالم بعد ذلك.

وقد كان الانترنت آنذاك ملكاً للحكومة الأمريكية، والآن هناك مالك لهذه الشبكة. لذلك فقد اتسعت هذه الشبكة بشكل كبير جداً، ففي عام ١٩٨٥م كان هناك أقل من ألفي حاسب آلي مرتبط بالشبكة، وفي عام ١٩٩٥م وصل العدد إلى خمسة ملايين حاسب آلي مرتبط بالشبكة، وفي عام ١٩٩٧م وصل العدد إلى ستة ملايين حاسب. وهي تستخدم حوالي ثلاثمائة ألف سيرمز متناثرة في كافة أنحاء العالم. وفي استطلاع أجرته شبكة (NUA) الأمريكية قدر عدد مستخدمي شبكة الانترنت عالمياً عام ١٩٨٨م حوالي مائة وأربعة وثلاثين مليون مستخدم. ونشرت أيضاً ذات الشبكة تقريراً صدر بتاريخ ٢٠٠٠/١٠/٢٦م يوضح أن عدد المستخدمين للشبكة في هذا العام ٢٠٠٥م سيكون حوالي مائتان وخمسة وأربعون مليون مستخدم.

وقد أشار الرئيس السابق للولايات المتحدة الأمريكية (بيل كلينتون) إلى مشروع مستقبلي لتطوير شبكة الانترنت أطلق عليه اسم (الانترنت ٢)، فقال:

(لابد أن نبني الجيل الثاني من شبكة الانترنت لتتاح الفرصة لجامعاتنا الرائدة ومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة عن سرعات اليوم وذلك لتطوير كل من العلاجات الطبية الحديثة ومصادر الطاقة الجديدة وأساليب العمل الجماعي).

لذلك فإن مفهوم جرائم الكمبيوتر مرّ بتطور تاريخي تبعاً لتطور التقنية واستخدامها، ففي المرحلة الأولى من شيوع استخدام الكمبيوتر في الستينات والسبعينات ظهرت أول معالجات لما يسمى جرائم الكمبيوتر واقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي بالاستخدام غير المشروع للبيانات المخزنة في أنظمة الكمبيوتر. ومع تزايد عدد المستخدمين في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عدد من القضايا الإجرامية الفعلية، وبدأ الحديث عنها بوصفها ظاهرة جرمية لا مجرد سلوكيات

مرفوضة. وفي الثمانينات ظهر مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وأنشطة نشر وزراعة الفيروسات الالكترونية التي تقوم بعمليات تدميرية للملفات أو البرامج وشاع اصطلاح الهاكرز. وشهدت التسعينات ثورة هائلة في حقل الجرائم الالكترونية بل امتدت ليظهر تغيرا واضحاً في نطاقها ومفهومها ، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات فظهرت الجرائم التي تمارس ضد مواقع الانترنت التسويقية الناشئة والتي يؤدي انقطاعها عن الخدمة لساعات خسائر مالية بالملايين، وانتشرت جرائم نشر الفيروسات عبر مواقع الانترنت حيث يسهل انتقالها إلى ملايين المستخدمين في ذات الوقت.

تنامي حجم جرائم الكمبيوتر ومفاسدها منذ مطلع التسعينات:

أشرنا إلى أن شبكة الانترنت قد نمت خلال العشر سنوات الأخيرة بشكل مذهل، فأصبحت هذه الشبكة تضم الآن ملايين المستخدمين في كافة المدن حول العالم وتحولت من مجرد أن كانت شبكة تستخدم في الأغراض العسكرية أو الأكاديمية إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وبالفعل لم يكن هناك قلق مع بدايات إنشاء شبكة الانترنت نحو جرائم يمكن أن ترتكب بواسطة الشبكة وذلك نظراً لمحدودية مستخدميها ناهيك عن كونها مقصورة على شرعية معينة من المستخدمين وهم الباحثين وطلاب العلم.

لذلك فإن الشبكة لم تكن آمنه في تصميمها وإنشائها كما أن الاهتمام في بداية الأمر كان منصباً على الاهتمام بالبناء وتوسيع النشاط دون النظر إلى مسائل الأمن. وفي ١٩٨٨/١١/٢م وبحدوث قضية موريس الشهيرة تغيرت النظرة السابقة حيث استطاع هذا الشخص أن ينشر فيروساً الكترونياً عرف (بدودة موريس) تمكن بواسطته من مهاجمة آلاف الكمبيوترات عبر الانترنت، ونجم عنه أضراراً بالغة حيث أوقف آلاف الأنظمة عن العمل وتسبب في تعطيل وإنكار الحزمة. وبدأ المستخدمون يحاولون إيجاد حلول آمنه تقفل الثغرات ونقاط الضعف.

وفي عام ١٩٩٥م نجم هجوم مخطط له عرف باسم (IP-SPOOFING) وقد أدى هذا الهجوم إلى وقف عمل كمبيوترات موثوقة وتشغيل أخرى وهميه.

وفي عام ١٩٩٦م ظهرت هجمات إنكار الخدمة واستطرقت الصحف في الحديث عنه ونشر عناوين رئيسية حول إخبار تلك الهجمات. والأحداث الشهيرة في هذا الحقل كثيرة ومتعددة ولعلنا نبرز بعضاً منها:-

١. قضية موريس: وهي أول الهجمات الكبيرة والخطيرة في بيئة الشبكات. حيث أطلق هذا الشخص فيروس عُرِفَ باسم (دودة موريس) أدى إلى تعطيل عدد كبير من الأجهزة وقدرت الخسائر المادية لإعادة النظام حوالي مائة مليون دولار.

٢. قضية الجحيم العالمي: تعامل معها مكتب التحقيقات الفدرالية وحيث تمكنت هذه المجموعة من اختراق موقع البيت الأبيض والجيش الأمريكي.

٣. فيروس ميلسا : وهو فيروس شرس أطلق من قبل مبرمج كمبيوتر أتهم باختراق اتصالات عامة.

٤. حادثة شركة أوميغا : حيث تمكن مصمم ومبرمج يدعى (تيمون ألن) من إطلاق قنبلة الكترونية بعد ٢٠ يوم من فصله من ذات الشركة استطاعت أن تلغي كافة التصاميم وبلغت الخسائر بحوالي عشرة مليون دولار وهذه الجريمة تعتبر أكثر جرائم تخريب الكمبيوتر خطورة.

المبحث الثالث: إثبات جرائم الانترنت

جرائم الانترنت كثيرة ومتنوعة ويصعب حصرها لأن هذه الجرائم لا تترك أثراً، بمعاينته يتم التوصل إلى مرتكبها مثل الجرائم التقليدية التي دائماً تترك أثراً يقود إلى مرتكبها ؛ ولعل أسباب صعوبة إثبات جرائم الحاسب الآلي والانترنت تعود للآتي:-

١- أنها جريمة لا تترك أثراً لها بعد ارتكابها.

٢- صعوبة الاحتفاظ الفني بآثارها إن وجدت.

٣- تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها والتحقيق فيها.

٤- تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

٥- تعتمد على قمة الذكاء في ارتكابها.

٦- أنها ترتكب في دولة ما ويتحقق الفعل الإجرامي في دولة أخرى أي أنها جريمة ليس لها حدود.

٧- غياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم. لذلك فإن الأمر ليس بكل تلك الصعوبة لكنه لابد من الأخذ بعدة خطوات ليكون في الإمكان الإمكان مكافحة جرائم الانترنت وتلك الخطوات هي: -

١. تحديد الجريمة من البداية.

٢. تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل منسوبيها بما يتناسب مع الأسلوب الذي يمكنهم من العمل لمواجهة هذا النوع من الجرائم.

٣. وضع قوانين وتعليمات لمكافحة هذا النوع من الجريمة ووضع العقاب الشديد لها لتكون مانعاً من موانع ارتكابها.

٤. التركيز على مواجهة تلك الجرائم بصفة دولية بإقرار اتفاقات دولية تجرّم تلك الجرائم وتعمل كل الدول على متابعة مرتكبيها.

المبحث الرابع: إيجابيات الانترنت للأجهزة الأمنية

أن شبكة الانترنت ليس فقط أرضاً خصبة لارتكاب الجرائم وإنما هي أيضاً تقدم خدمات جليلة للأمن لعل أبرزها ما يلي: -

١) تلقي البلاغات بطريقة فورية وسريعة.

٢) إيصال التعاميم والتعليمات بسرعة فائقة.

٣) عدم تعريض المتعاونين مع الأجهزة الأمنية للخطر.

٤) إتاحة الفرصة لجميع المواطنين للتعاون مع الأجهزة الأمنية.

٥) مخاطبة الإنتربول ومحاصرة المجرمين بصورة سريعة.

٦) نشر صور المطلوبين أمنياً.

٧) نشر الأنظمة والقوانين التي تهم المواطنين.

٨) توعية الجمهور بطرح التعليمات أو الإنذارات لمنعهم من التعامل مع الجهات المشبوهة.

٩) نشر الوظائف من خلاله للقضاء على البطالة.

١٠) عمل الاستفتاءات على جميع القضايا سواءً الوطنية أو العالمية ليتم قياس رأي الجمهور والاستفادة منه

في الدراسات.

١١) من خلال الانترنت يتم التواصل فيما بين الشعوب لنقل التقدم التكنولوجي والعلمي من الدول المتقدمة إلى الدول النامية.

١٢) الانترنت أصبح طريقة من طرق التعليم الحديث عن بعد وبواسطته يتم تدريب العاملين بمختلف المجالات.

ففي دراسة أمنية لشرطة دبي حول الاستخدامات الأمنية للانترنت حُددت عشر خدمات أمنية يمكن تقديمها للجمهور عن طريق شبكة الانترنت. ((البيان – ٢٠٠٠م)).

كما حددت دراسة الدكتور فايز الشهري الإيجابيات الأمنية لشبكة الانترنت في تلقي البلاغات وتوفير السرية للمتعاونين..... الخ.

كما بادرت الدول الأوربية إلى الاستخدام الفعلي لشبكة الانترنت في البحث عن المجرمين والقبض عليهم حيث تمكنت العديد من الدول وفي مقدمتها ألمانيا وبريطانيا وفرنسا من استخدام شبكة الانترنت في السعي نحو ضبط المجرمين والتعرف على كل الحالات المشابهة في كل أنحاء أوروبا والاتصال فوراً بالانتربول عبر شبكة الانترنت.

المبحث الخامس: دور الكمبيوتر في الجريمة

يمكننا تصنيف الأدوار التي يقوم بها الكمبيوتر في حقل ارتكاب الجرائم كالآتي:

الأول: قد يكون الكمبيوتر هدفاً للجريمة وذلك مثل الدخول غير المصرّح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها أو إرسال الفيروسات بواسطة البريد الالكتروني أو بواسطة برنامج مسجل في أحد الوسائط المتنوعة ولعل من أوضح المظاهر لاعتبار أن الكمبيوتر يكون هدفاً للجريمة عندما تكون السرية والسلامة والقدرة هي التي يتم الاعتداء عليها. بمعنى أن توجه هجمات الكمبيوتر إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، ويستهدف هذا النمط الإجرامي مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها أو السيطرة على النظام دون تصريح أو تمويل وهذه الأفعال الجرمية تتضمن ابتداءً الدخول غير المصرح به إلى النظام الهدف والتي تعرف بأنشطة الهاكرز كتابة عن فعل الاختراق. لذلك يجب وضع برامج لحماية هذه الأجهزة من الفيروسات وتحديث قاعدة بيانات هذه البرامج لضمان أقصى درجة من الحماية. ورغم أن وجود مثل هذه البرامج في جهاز الحاسب الآلي لا يمثل إطلاق الحماية التامة من أي هجوم فيروسي قد يلحق الضرر بالنظام وإنما هو سبب من أسباب الوقاية حيث أن الفيروس إذا كان حديث وغير معروف من السابق قد يتسلل إلى الجهاز.

الثاني: قد يكون الكمبيوتر أداة الجريمة لارتكاب جرائم تقليدية ما في حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان بنكية مخزنة في الجهاز ويستدعي الجاني رقماً معيناً لإحدى البطاقات ويحصل بواسطته على مبالغ من حساب مالك البطاقة، أو استخدام التقنية في عمليات التزييف والتزوير، حتى أن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها أو العبث في عمل الأجهزة الطبيعية والمخبرية والتلاعب في برمجياتها. وكذلك العبث في إتباع الوسائل

الالكترونية للتأثير على عمل الطائرات أو السفن.

الثالث: قد يكون الكمبيوتر بيئة الجريمة، كما يتم في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين أو اتصال لعصابات ترويج المخدرات وأنشطة الشبكات الإباحية أو تخزين البرامج المجرمة فيه.

الرابع: إساءة استخدام الحاسب الآلي أو استخدامه بطريقة غير قانونية كمن يقوم باستخدام الجهاز بعد انتهاء عمله في أمور لا تخص العمل.

أما من حيث دور الكمبيوتر في اكتشاف الجريمة فإنه من الضروري استخدام نفس وسائل الجريمة المتطورة للكشف عنها ومن هنا يلعب الكمبيوتر ذاته دوراً رئيسياً في كشف جرائم الكمبيوتر وتتبع فاعليها أو التصدي لهم علماً أن الكمبيوتر يستخدم لآن على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم.

المبحث السادس: أهداف جرائم الكمبيوتر والانترنت

من المعروف أن أكثر الجرائم الالكترونية التي يتم ارتكابها يكون الهدف الأساسي منها هو الحصول على المعلومات الالكترونية التي تكون إما محفوظة على أجهزة الكمبيوتر أو المنقولة عبر شبكة الانترنت إلا أن ذلك لا يعني أن هناك جرائم أخرى يكون لها هدف آخر غير الحصول على المعلومات منها كانت أهمية تلك المعلومات لذا فإن أهداف الجرائم الالكترونية كالآتي:-

١- المعلومات: تمثل جرائم الكمبيوتر طائفة الجرائم المنصبة على المعلومات بمفهومها الواسع (بيانات، معلومات، برامج تطبيقية، وبرامج تشغيل) وهناك العديد من الجرائم التي يكون ارتكابها لهدف يتعلق بالمعلومات ويتمثل هذا الهدف إما بالحصول على المعلومات أو تغييرها أو حذفها نهائياً، والجرائم التي يكون الهدف منها المعلومات هي في الغالب أعمّ من الحالات التي يكون الهدف منا جرائم اقتصادية.

٢- أجهزة الكمبيوتر: أما بالنسبة للمكونات المادية للحاسب فالموقف الغالب يتجه إلى اعتبارها من قبيل الجرائم الواقعة عليها مما يندرج في نطاق الجرائم التقليدية حتى تلك التي تستهدف نظام الحاسوب باعتباره المعبّر عن عصر التقنية والغالب يكون الهدف هو تخريب تلك الأجهزة نهائياً أو تعطيل أنظمتها لفترات طويلة وهذا يتم بواسطة نشر الفيروسات.

٣- الأشخاص أو الجهات: حيث أن معظم الجرائم التي تُرتكب عبر الانترنت تستهدف إما أشخاص أو جهات معينة وتكون تلك الجرائم مباشرة تُرتكب في صورة ابتزاز أو تهديد أو تشهير أو جرائم غير مباشرة تُرتكب في صورة الحصول على البيانات أو المعلومات الخاصة بتلك الجهات أو الأشخاص ثم ترتكب بواسطتها الجرائم.

المبحث السابع: فئات الجناة في جرائم الكمبيوتر والانترنت

يمكن حصر أنواع الجناة في جرائم الكمبيوتر والانترنت إلى أربعة فئات: -

الأولى: المستخدمون لأجهزة الحاسب الآلي في منازلهم دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم له.

الثانية: الموظفون الساخطون على منظماتهم التي يعملون بها فقد يعودون إلى مقر أعمالهم بعد انتهاء الدوام ويقومون بتخريب الأجهزة أو إتلافها أو حد سرقتها، أو يقومون بالدخول على الأنظمة في حال كونهم

محترفين ويقومون بتخريبها أو نشر الفيروسات بها.

الثالثة: العابثين أو المتسللين - الهاكرز - وينقسم المتسللين إلى قسمين فمنهم الهواة أو العابثون بقصد التسلية.

الرابعة: العاملون في الجريمة المنظمة كالعصابات العاملة في مجال المخدرات أو غسيل الأموال.

المبحث الثامن: نظريات وأسس تصنيف أنواع جرائم الكمبيوتر والانترنت

يصنف الدارسون والمختصون جرائم الحاسوب ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فالبعض يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدوافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد حمل الاعتداء وكذا تعدد الحق المعتدى عليه تنقسم جرائم الكمبيوتر بهذا المعنى إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة. ومن الملاحظ أن هذه التقسيمات أو بعضها لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم، ولأن جرائم الحاسوب في نطاق الظاهرة الإجرامية المستحدثة جرائم تنصب على الكيانات المادية مما يدخل في نطاق الجرائم التقليدية ولا يتدرج ضمن الظاهرة المستجدة لجرائم الحاسوب.

ولعلنا نقف على أبرز التصنيفات بهدف الإطاحة بمختلف الأنماط:

أولاً: تصنيف الجرائم تبعاً لنوع المعطيات محل الجريمة:-

يمكن تقسيم جرائم الحاسوب بالاستناد إلى هذا المعيار كالآتي:

أ) الجرائم الماسة بقيمة معطيات الحاسوب: وتشمل فئتين: أولهما: الجرائم الواقعة على ذات المعطيات كجرائم الإتلاف وتشويه البيانات ونشر الفيروسا.

وثانيهما: الجرائم الواقعة على ما تمثله المعطيات آلياً من أموال أو أصول، وجرائم التحويل والتلاعب في البيانات المخزنة في الحاسوب، وتزوير المستندات.

ب) الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة:

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على

ثانياً: تصنيف الجرائم تبعاً لدور الكمبيوتر في الجريمة:

حيث أنه قد يكون الكمبيوتر هدف الاعتداء، وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم الجرائم المرتبطة بالكمبيوتر وقد يكون الكمبيوتر أخيراً بيئة الجريمة أو وسطها أو مخزوناً للمادة الجرميه وفي هذا النطاق هناك مفهومان:

البيانات الشخصية المتصلة بالحياة الخاصة.

ج) الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات): وتشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

ثانياً: تصنيف الجرائم تبعاً لدور الكمبيوتر في الجريمة:

حيث أنه قد يكون الكمبيوتر هدف الاعتداء، وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم الجرائم المرتبطة بالكمبيوتر وقد يكون الكمبيوتر أخيراً بيئة الجريمة أو وسطها أو مخزوناً

للمادة الجرميه وفي هذا النطاق هناك مفهومان:

الأول: جرائم التخزين ويقصد بها تخزين المواد الجرميه.

والثاني: جرائم المحتوى ويسمى بالمحتوى غير المشروع أو غير القانوني ولقد أوجد مشروع الاتفاقية الأوربية تقسيماً جديداً نسبياً، فقد تضمن أربع طوائف رئيسية لجرائم الكمبيوتر والانترنت:

أ- جرائم تستهدف عناصر (السرية والسلامة وموفورية) المعطيات والنظم وتضم:

- الدخول غير القانوني.
- الاعتراض غير القانوني.
- تدمير المعطيات.
- إساءة استخدام الأجهزة.

ب- الجرائم المرتبطة بالكمبيوتر وتضم:

- التزوير المرتبط بالكمبيوتر.
- الاحتيال المرتبط بالكمبيوتر.

ج- الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللا أخلاقية.

د- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة، قرصنة البرمجيات.

ثالثاً: تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال:

هذا التصنيف شائع في الدراسات والأبحاث الأمريكية كما نجده المعيار المعتمد لتقسيم جرائم الكمبيوتر والانترنت في مشروعات القوانين النموذجية التي وضعت من قبل جهات بحثية بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع، كما أن مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت الموضوع من قبل فريق بحثي أكاديمي حيث تم تقسيم جرائم الكمبيوتر والانترنت إلى الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال عدا السرقة، وجرائم السرقة والاحتيال، وجرائم التزوير، وجرائم المقامرة، والجرائم ضد الآداب عدا الجرائم الجنسية، والجرائم ضد المصالح الحكومية. ويلاحظ أن هذا التقسيم يقوم على فكرة الغرض النهائي أم المحل النهائي الذي يستهدفه الاعتداء لكنه ليس تقسيم من منضبط وغير محدد الأطر.

فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال. أما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار، والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة، عموماً فإنه تبعاً لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي فإن جرائم الكمبيوتر تُصَنّف على النحو التالي:

أ/ الجرائم التي تستهدف الأشخاص:

١. الجرائم غير الجنسية التي تستهدف الأشخاص مثل التحريض على الانتحار، القتل بالكمبيوتر.

٢. الجرائم الجنسية وتشمل تحريض المراهقين على أنشطة جنسية غير مشروعة ونشر الصور الإباحية.

هـ/ جرائم المقامرة والجرائم ضد الأخلاق والآداب.

ب/ جرائم الأموال عدا السرقة.

ج/ جرائم الاحتيال والسرقة.

د/ جرائم التزوير.

هـ/ جرائم المقامرة والجرائم ضد الأخلاق والآداب.

و/ جرائم الكمبيوتر ضد الحكومة.

المبحث التاسع: المخاطر الأمنية للانترنت

كما يعلم الجميع فإنه لا يمكن بطريقة أو بأخرى حصر المخاطر الأمنية بصفة دقيقة لأسباب متعددة منها أن انتشار الانترنت يعتبر حديثاً نسبياً كما أنه ولطبيعة العمل الأمني فإن المخاطر مستجدة دوماً ولا تقف عند زمن معين أو على نمط محدد فالخير والشر في صراعٍ دائم لا يتوقف منذ قديم الزمن إلا أنه (يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات الأخرى قد تسبب تلوثاً ثقافياً يؤدي إلى تفسخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات).

إنَّ الاستخدام غير الأخلاقي واللا قانوني للشبكة قد يصل إلى فئات المراهقين والهواة مما يؤثر سلباً على نمو شخصياتهم النمو السليم ويوقعهم في أزمات النمو وأزماتٍ قيميه لا تتماشى مع النظام الاجتماعي السائد وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور والمواد الإباحية ولذلك سنتطرق إلى أهم المخاطر الأمنية للانترنت وهي كالتالي:-

أولاً: التجسس الالكتروني:

عمليات التجسس هي عمليات قديمة قدم البشرية وقدم النزاعات البشرية فمنذ تقدم العصور كان الإنسان يتجسس على أعداءه لمعرفة أخبارهم والخطط التي يعدونها لمهاجمته ولهذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة.

وقد تطورت عمليات التجسس طبقاً لما يسود المجتمع من تطورات علمية وتكنولوجية وفي عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي. والعالم العربي والإسلامي كان ولا يزال مستهدف أمنياً وثقافياً وفكرياً وعقدياً.

ولا تكمن خطورة التجسس الالكتروني في استخدام الانترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولا يمكن حتماً الاعتماد على وسائل الحماية التي تنتج من قبل الشركات الأجنبية المعادية. كما أن خطورته لا تكمن إذا ما كان القائم به هم بعض الهواة العابثين وكان الغرض من اختراقهم لأجهزة الكمبيوتر والشبكات هو العبث بالمحتويات أو إلغاء بعضها أو كلها إلا أن الأهمية تكمن فيما إذا كان القائم بتلك الاختراقات هي أجهزة المخابرات في بعض الدول للتجسس على الدول الأخرى.

وقد وجدت بعض حالات التجسس الدولي وفيها ما أكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكية (NSA) والتي قامت بزراعته في نظام التشغيل الشهير ويندوز وربما يكون هذا هو أحد الأسباب الرئيسية التي دعت الحكومة الألمانية بإعلانها في الفترة الأخيرة عن استبدالها لنظام التشغيل ويندوز بأنظمة أخرى. كما كشف أخيراً النقاب عن شبكة دولية ضخمة للتجسس الالكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كل من كندا وبريطانيا واستراليا ونيوزيلندا ويطلق عليها اسم: (ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة أنواعها سواءً ما كان

فيها برقياً، أو تلكس أو فاكس أو الكترونياً. وخصص هذا النظام للتعامل مع الأهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلة جداً من الاتصالات والرسائل الالكترونية عشوائياً باستخدام خاصية الكلمة المفتاح بواسطة الحسابات المتعددة والتي تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الأقمار الصناعية الواقعة في منطقة (واي هوباي) بجنوب نيوزلندا ومحطة جيرالدتون الموجودة بأستراليا، وكذلك المحطة الموجودة في منطقة مورونيستو بمقاطعة كورنول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة شوجر جروف، وأيضاً المحطة الموجودة بولاية واشنطن.

ولا يقتصر الرصد على المحطات المرتبطة بالأقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية بل يشمل أيضاً رصد الاتصالات الأرضية وكذلك الشبكات الالكترونية أي أنه يرصد جميع الاتصالات التي تتم بأي وسيلة ويعتبر الأفراد والمنظمات والحكومات الذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمة كوديه لحماية شبكاتهم وأجهزتهم أهدافاً سهلة لشبكة التجسس الالكتروني وإن كان هذا لا يعني بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتيه لهذه الشبكة ومثيلاتها. ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية.

فمع توسع التجارة الالكترونية عبر شبكة الانترنت تحولت 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 اظهر استفتاء أجري عام ١٩٩٦م لمسئولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول وبشكل غير مشروع على معلومات سريه لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية.

ومن الأساليب الحديثة في التجسس الالكتروني أسلوب اختصار المعلومات داخل المعلومات وهو أسلوب شائع وإن كان ليس بالأمر السهل ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومة أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً كما قد يلجأ إلى وسائل حديثه للحصول على المعلومات السرية.

ومن أحدث وأشهر أمثلة التجسس الالكتروني أنه بعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطة الأمريكية الاستعانة في عمليات التجسس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصاً لالتقاط الاتصالات التي تجري عبر الأجهزة اللاسلكية والهواتف النقالة. بالإضافة إلى قمرين اصطناعيين يلتقطان صوراً 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 العلميات شبكة اشيلون المستخدمة في التجسس على المكالمات الهاتفية ورسائل الفاكس والبريد الالكتروني، الأمر الذي يتيح تحليل الإشارات التي تلتقطها الأقمار الصناعية حتى إن كانت راهنه أو مشفرة.

ثانياً: الإرهاب الالكتروني:

في الماضي كان الإرهاب يعني قيام بعض الإرهابيين بتفجير قنبلة في مكان ما. وقد اعتاد رجال الأمن في جميع الدول على مواجهتها، أما في عصر الازدهار الالكتروني، وفي زمن قيام حكومات الكترونية كما في الإمارات العربية المتحدة تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها، ومنها ولا شك أنماط 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 الإرهاب، والتي أخذت منحنى حديث يتماشى مع التطور التقني.

وقد تنبه الغرب إلى قضية الإرهاب الالكتروني منذ فترة مبكرة فقد شكل الرئيس الأمريكي بيل كلينتون لجنة خاصة مهمتها حماية البنية التحتية الحساسة 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 ثم تم إنشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات أي هجمات إرهابية الكترونية كما قامت وكالة الاستخبارات المركزية بإنشاء مركز حرب المعلومات وظفت به ألفاً من خبراء أمن المعلومات، كما شكلت قوة ضاربة لمواجهة الإرهاب على مدار الساعة ولم يقتصر هذا الأمر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحث الفيدرالية والقوات الجوية. وبعد الهجمات الأخيرة على الولايات المتحدة الأمريكية ارتفعت أصوات البعض بممارسة الإرهاب الالكتروني ضد المواقع الإسلامية والعربية التي يشتبه بأنها تموّل الإرهاب وتدعمه، وأوردت شبكة: (CNET) الإخبارية خبراً عن اتفاق ستين خبيراً في أمن الشبكات ببدء تلك الهجمات الإرهابية على مواقع فلسطينية وأفغانية.

وحذّر تقرير صدر من وزارة الدفاع الأمريكية عام ١٩٩٧م من: (بيريل هاربور الالكتروني) في إشارة للهجوم المفاجئ الذي شنّه سلاح الجو الياباني على الأسطول الأمريكي في ميناء بيريل هاربور أثناء الحرب العالمية الثانية وتوقع أن يزداد الهجوم على نظم المعلومات في الولايات المتحدة الأمريكية من قبل الجماعات الإرهابية أو عصابات الإجرام المنظم أو عملاء المخابرات الأجنبية وأن يصل هذا الهجوم إلى ذروته عام ٢٠٠٥م وأوضح التقرير أن شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في الولايات المتحدة الأمريكية معرضه للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية دون أن توجه قواتها المسلحة.

ثالثاً: جرائم القرصنة:

هي الاستخدام أو النسخ غير المشروع لنظم التشغيل أو البرامج الحاسوبية. ولقد وفرت شبكة الانترنت في ظل ما توفره من تقنيات حديثة مجالاً خصباً لنمو نوع جديد من أنواع الجرائم لم يكن معروفاً من السابق ألا وهو الاستخدام غير المشروع والنسخ غير المشروع لنظم تشغيل وبرامج الحاسب الآلي. فمن المعروف أن النسخ غير القانوني يؤدي إلى خسائر فادحة لمنتجي تلك البرامج ونظم التشغيل كما أن جرائم القرصنة على البرامج الأصلية تؤدي إلى إبطاء عمليات التطوير والبحث العلمي نظراً لخسائر تلك الشركات المادية الباهظة، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الأعمال أو ما تعرف اختصاراً بـ (BSA) والتي أجرت دراسة تبين منها أن القرصنة على الانترنت ستطغى على أنواع القرصنة الأخرى ودق هذا التقرير ناقوس الخطر للشركات المعنية

فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الانترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الانترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة إلا أن تلك الشركات تراجعت عن هذا التهديد أثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الانترنت، كما قامت بعض تلك الشركات مع مزودي الخدمة لإبلاغهم عن أي مواقع مخصصة للبرامج المقرصنة التي تنشأ لديهم وذلك لتقديم شكوى ضدهم ومقاضاتهم إن أمكن أو إقفال تلك المواقع كأقل تقدير.

وقد أدت قرصنة البرامج إلى خسائر مادية باهظة جداً وصلت في عام ١٩٨٨م إلى حوالي إحدى عشر مليار دولار أمريكي في مجال البرمجيات وحدها، والقرصنة عربياً لا تختلف كثيراً عن القرصنة عالمياً إن لم تسبقها بخطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين إن وجدت.

رابعاً: المواقع المعادية:

مصطلح المواقع المعادية هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي الذي نعيشه حالياً، ومصممي تلك المواقع المعادية قد استغلوا هذه التكنولوجيا لخدمة أغراضهم الشخصية في عرض أفكارهم المغرضة التي لم تمتلك الشجاعة الكافية في سلك الطرق الشرعية المباحة في عرض تلك الأفكار والآراء، والغرض من تلك المواقع المعادية الآتي:

١. الإساءة إلى الدين الإسلامي ونشر الأفكار السيئة عنه وحث الناس على الابتعاد عنه.
٢. الإساءة إلى بلد معين وإلى مواقف قادته السياسيين.
٣. الإساءة إلى شخص معين بما يمثله من مواقف سواءً دينية أو سياسية أو وطنية.

خامساً: الجرائم والممارسات الجنسية وغير الأخلاقية:

أ- المواقع الإباحية: لقد وفرت شبكة الانترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية. إن الانترنت جعلت الإباحية بشتى وسائل عرضها من صور وفيديو وحوارات في متناول الجميع ولعل هذا يعد أكبر الجوانب السلبية للانترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا السعودي. إن صناعة ونشر الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال. لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر ١٩٩٨م تتعلق هذه الجرائم بتغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال. ومما لاشك فيه بأن هذه المواقع الموجودة بكثرة على شبكة الانترنت تريد تحقيق الكثير من المكاسب المادية عن طريق زيادة عدد مرتاديها 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 وإن كانت هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يومية على عناوينهم البريدية.

ب- المواقع المتخصصة في القذف وتشويه سمعة الأشخاص:

مع انتشار الشائعات والأخبار الكاذبة والتي تحل رموز الشعوب سواءً كانت تلك الرموز فكرية أو سياسية أو دينية ظهرت شبكة الانترنت بعض المواقع المشبوهة والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة. ولكن تلك المواقع ليست منتشرة انتشار المواقع الأخرى وتركز هجومها في

الغالب على إبراز سلبيات الشخص المستهدف ونشر بعض أسراره سواءً التي يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه والعبث به أو بتلفيق تهم كاذبة عنه. هذا من جهة ومن جهة أخرى فقد يكون الهدف من تلك المواقع هو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم إذا لم يرضخوا ويدفعوا مقابل مادي لعدم التعرض لهم وتركهم دون تشويه سمعتهم. ومثال ذلك ما وقع في بداية دخول الانترنت وجرى تداولها بين مستخدميه حول قيام شخص في دولة بإنشاء موقع خاص بفتاة وقام بنشر صورها وهي عارية إضافة إلى صور أخرى مع صديقها وهي في أوضاع مخلة والتي حصل عليها بعد التسلل إلى حاسوبها الشخصي وسرقة تلك الصور ومن ثم حاول ابتزازها جنسياً ومادياً، وعندما رفضت هددها بنشر تلك الصور في مواقع على الانترنت فأصرت على الرفض وأصرَّ على التنفيذ ووزع الرابط لذلك الموقع على عدد من المنتديات والمواقع البريدية مما أدى إلى انتحار تلك الفتاة لأنه فضحها بين أهلها وذويها.

ومثال آخر: عندما تمكن جهاز المباحث بجمهورية مصر العربية من ضبط مهندس كمبيوتر مصري الجنسية بتهمة نشر معلومات كاذبة على الانترنت للتشهير بعائلة مسئول مصري وتصميمه موقع على شبكة الانترنت لهذا الغرض، وأشارت الصحف إلى أن ابنة المسئول المصري كانت عرضةً للتشهير بعد أن قام

أحد الأشخاص بنشر موقع على الانترنت باستخدام بيانات عن الضحية بغرض التشهير بها ولكن إدارة مكافحة جرائم الكمبيوتر وشبكات المعلومات بوزارة الداخلية المصرية تمكنت بالتنسيق مع المباحث العامة في ضبط الشخص الذي قام بالتشهير بابنة المسئول المصري وعائلته، وتبيّن بعد التحريات والمتابعة الالكترونية التي قامت بها إدارة مكافحة الجرائم الالكترونية بوزارة الداخلية أن المتهم مهندس كمبيوتر ومصمم برامج.

ج- الدخول إلى المواقع المحجوبة:

بعض الدول تعمل على حجب المواقع غير المناسبة وغير المتماشية مع تقاليدها الاجتماعية والدينية، حيث أن بعض الدول تعمل على حجب المواقع الجنسية الإباحية حتى لا يستطيع زائري شبكة الانترنت الدخول إلى تلك المواقع وهذه الدول تعمل على حماية تقاليدها مما يمكن أن يسببه الدخول على تلك المواقع، إلا أن بعض الأشخاص يعملون جاهدين على تخطي تلك المواقع المحجوبة باستخدام بعض البرامج المخصصة لذلك. أما المواقع المحجوبة والمعادية للعقيدة فمنها ما يكون موجه من قبل أعداء حاقدين من أتباع الديانات الأخرى، كالمواقع التي تنشئها الجاليات اليهودية أو النصرانية تحت مسميات إسلامية بقصد بث معلومات خاطئة عن الإسلام والقرآن، أو بهدف الدعاية للأديان الأخرى ونشر الشبهة والافتراءات حول الإسلام. ويرى كثير من الباحثين أن حجب تلك المواقع هو تصرف صحيح بالنسبة للأطفال الذين يمكن أن تؤثر فيهم تلك المواقع.

د – إخفاء الشخصية: نظراً للتطور الهائل في مجال البرمجيات على مستوى العالم والذي نشهده اليوم ويزداد كل فترة قصيرة فقد ظهرت بعض البرامج المتخصصة التي يمكن استخدامها في إخفاء هوية الشخص عند الدخول على شبكة الانترنت ولكن غالباً ما يتم استخدام برامج إخفاء الشخصية عند الدخول على برامج التحدث حتى يتمكن الشخص المتحدث من الحديث في المواضيع التي يريدها دون إعلان شخصيته الحقيقية حتى لا يتعرف عليه أحد دون التزام بتقاليد أو قوانين وهو ما يخجل من الحديث فيه في حال ما إذا عرفت شخصيته الحقيقية وكذلك عند إرسال البريد الالكتروني في معظم الأحوال قد يمكن معرفة الرقم أو المكان الذي تمكن منه هذا الشخص من الدخول على الانترنت دون معرفة بياناته الحقيقية التي أخفاها.

هـ- انتحال الشخصية:

هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصةً في الأوساط التجارية، تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى، إن ارتكاب هذه الجريمة على شبكة الانترنت أمر سهل، وهذا من أكبر سلبيات الانترنت الأمنية.

وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الانترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة.

سادساً: جرائم الاختراق:

أ) الاختراقات: تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. إن جل عمليات الاختراقات أو محاولات الاختراقات تتم من خلال برامج متوفرة على الانترنت وهذه البرامج تم تصميمها لتمكن المخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أن يتم ذلك الاختراق وأن غالبية البرامج المصممة كان بها نقطة ضعف أساسية تقلل كثيراً من إمكانياتها وهي إمكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه. وتختلف الأهداف المباشرة للاختراقات فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته الاختراقية أو لإثبات وجود ثغرات في الجهاز المخترق. مع العلم أنه يمكن متابعة تلك البرامج والقضاء عليها فيما عدا برنامج واحد تمكن مصمموه من التغلب على كافة الاحتياطات المعدة وأطلق عليه اسم (حصان طرواده) ويعتبر هذا البرامج من البرامج الخطيرة على الإطلاق التي تستخدم في عمليات الاختراق نظراً لتمتعه بعدة مميزات منه الأقدر على عمليات الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه لذلك فقد اكتسب هذا البرنامج شهرة كبيرة وحصان طرواده هو برنامج صغير ظاهره النفع وباطنه الدمار وينتقل عبر الشبكات ويتم تشغيله داخل جهاز الحاسب ليقوم بأغراض التجسس على أعمال الشخص التي يقوم بها على حاسوبه الشخصي. وبواسطته يتمكن المخترق أن يحصل على كلمة سر الدخول على الجهاز ويدخل بطريقة لا تثير أي ريبه ولا شك وهذا ما يزيد من خطورة هذا البرنامج.

ب) الإغراق بالرسائل: هي تلك الطريقة التي تعني إرسال كم هائل من الرسائل عبر البريد الالكتروني لأجهزة الحاسبات الآلية المراد العمل على تعطيلها وتوقفها عن العمل حيث يؤدي إلى تعطيل الشبكة وعدم إمكانية استقبال أي رسائل فضلاً عن إمكانية انقطاع الخدمة خصوصاً إذا كانت الجهة المتضررة من ذلك هي مقدمة خدمة الانترنت فمثلاً يتم ملء منافذ الاتصال وقوائم الانتظار مما ينتج عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية غير محدودة وكذلك لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق أعداد كبيرة منها.

ج) الفيروسات: هي إحدى أنواع البرامج الحاسوبية إلا أن الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية تلحق الضرر بنظام المعلومات أو البيانات وهذا البرنامج لديه القدرة على التضاعف والانتشار بحيث يزرع عند تشغيله نسخه في البرامج المصابة فيمكن كتابة كلمة أو أمر أو حتى مجرد فتح البرنامج

الحامل للفيروس أو الرسائل البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام

الفيروس بمسح محتويات الجهاز والعبث بالملفات الموجودة به. ويبدأ عملها طبقاً للأسلوب الذي صممت من أجله فقد يبدأ عملها بمجرد فتح الرسالة الموجودة بها والتي وصلت عن طريق البريد الالكتروني وقد تبدأ العمل بمجرد تشغيل البرنامج الموجودة عليه في الجهاز.

سابعاً: الجرائم المالية:-

تنقسم الجرائم المالية التي تتم عبر شبكة الإنترنت إلى أنواع وهي كالتالي:-

أ) جرائم السطو على أرقام البطاقات الائتمانية:-

أن البطاقات الائتمانية تعد نقوداً إلكترونية والاستيلاء عليها يعد استيلاء على مال الغير، ونظراً لسهولة الاستيلاء على تلك الأرقام فقد تزايدت حوادث الاستيلاء عليها كما تزايدت عمليات الابتزاز المصاحبة لارتكاب مثل تلك الجرائم وعمليات الابتزاز تكون إما لإعادة تلك الأرقام أو لعدم نشرها أو استخدمها من قبل من استولى عليها وقد وقعت بالفعل عدة حوادث من ذلك النوع، فمنها قيام شخص ألماني بالدخول غير المشروع إلى أحد مزودي الخدمة واستيلائه على أرقام البطاقات الائتمانية الخاصة بالمشتركين ومن ثم بدأ في ابتزاز صاحب الخدمة بنشر تلك الأرقام أو دفع فدية مالية، إلا أن الشرطة الألمانية نجحت في القبض على ذلك اللص عند استلامه الفدية.

وقد أثبتت شبكة (MSNBC) عملياً مدى سهولة الحصول على أرقام البطاقات الائتمانية من شبكة الإنترنت حيث قامت بعرض قوائم تحتوي على أكثر من ٢٥٠٠ رقم بطاقة ائتمانية حصلت عليها من سبع مواقع للتجارة الإلكترونية وذلك عن طريق استخدام قواعد بيانات متوافراً تجارياً ولم يكن من الصعب على أي متطفل استخدام تلك الوسيلة البدائية الوصول والاستيلاء على تلك الأرقام واستخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون.

ويتعدى الأمر المخاطر الأمنية التي يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن في بداية ثورة نقدية يطلق عليها اسم النقود الإلكترونية والتي يتنبأ لها أن تكون مكملة للنقود الورقية أو البلاستيكية (بطاقات الائتمان)، ومن المتوقع أيضاً أن يزداد الاعتماد على هذا النوع الجديد والحديث من النقود وأن تحوز على الثقة التي تحوزها النقود التقليدية، هذا بجانب الأسهم، السندات الإلكترونية المعمول بها حالياً في دول الإتحاد الأوروبي والتي أقر الكونغرس الأمريكي العمل والتعامل عام ١٩٩٠م، فإذا كانت البطاقة الائتمانية تواجه تلك المخاطر فما الحال عند استخدام الأنواع الجديدة من النقود الإلكترونية فنحن بحاجة إلى تدعيم الثقة في تلك الأنواع من النقود التي يتم استخدمها حالياً عبر شبكة الإنترنت حتى تجد الأنواع الجديدة من النقود الإلكترونية الثقة اللازمة ليتعامل معها الأفراد دون خوف من اعتداء اللصوص عليها وإفشاء بياناتها وسرقتها.

ب) لعب اليانصيب:

مع ظهور شبكة الإنترنت على مستوى العالم لأصبح لعب اليانصيب أسهل وأصبح يجمع اللاعبين على مستوى العالم في مكان واحد أسهل من الماضي على الإطلاق وأدى انتشار المواقع على الإنترنت إلى توفر ما يحتاجه اللاعبين من برامج ليتمكنوا من لعبه، ولذلك بدأت الرغبة الجادة في ملاحقة القائمين على تلك المواقع لمخالفتهم القانون الذي يجرم لعب اليانصيب عبر الشبكة إلا أن الأرباح الخيالية التي يجنيها أصحاب

تلك المواقع تدفعهم إلى المرواغة والهرب من تلك الملاحقة حتى لا يغلقوا تلك المواقع التي يربحون من ورائها مليارات الدولارات من اللاعبين الذين يدخلون على مواقعهم من كافة دول العالم دونما خوف من مخالفة القانون في بلادهم. ويوجد على الإنترنت أكثر من ١٠٠٠ موقع لليانصيب يسمح لمرتاديه من مستخدمي الإنترنت ممارسة جميع أنواع القمار التي توفرها المواقع الحقيقية.

ج) تزوير البيانات:

إن تزوير البيانات يكون بالدخول على قاعدة البيانات الموجودة وتعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل، وسواء كان الدخول بطريقة شرعية أو غير شرعية. وتعتبر من أكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات ومن تلك الحوادث التي تم فيها الدخول على قاعدة البيانات بطريقة شرعية، تلك الحادثة التي وقعت في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء على إتقان مسبق بينهما وبين صديقها بتزوير البيانات الخاصة بملكية السيارات والمسجلة بالكمبيوتر بحيث تصبح باسم صديق الفتاة وهو أحد لصوص السيارات والذي يعمد إلى سرقة السيارات وبيعها، وبالتالي عندما يتقدم مالك السيارة الحقيقي للإبلاغ عن سرقة سيارته وبالبحث في قاعدة البيانات في الحاسب الآلي يتضح عدم وجود سجلات للسيارة باسمه، وبعد أن يقوم صديق الفتاة ببيع السيارات تقوم ذات الفتاة بإعادة تسجيل السيارة باسم صاحبها الأصلي أي إعادة البيانات كما كانت عليه، ومن غير أي تعديل. وقد كانت تلك الفتاة تتقاضى عن كل عملية مائة دولار لا غير حتى تم اكتشافها والقبض عليها. هذا من جهة ومن جهة أخرى فإن اتجاه الحكومات على مستوى العالم إلى الاتجاه للحكومات الالكترونية وكذلك انتشار التجارة الالكترونية عبر دول العالم وصدور القوانين المنظمة له سيزيد من فرص ارتكاب تلك الجرائم وفي نفس الوقت سيعمل على إضعاف فرصة القبض على مرتكبي تلك الجرائم، والحكومات الالكترونية هي المناخ الأنسب لارتكاب مثل تلك الجرائم.

د) الجرائم المنظمة: عصابات المافيا: هم أشهر من قام بالجرائم المنظمة على مستوى العالم، وكانت شبكة الانترنت من أهم الوسائل التي ساعدت كثيراً أعضاء عصابات المافيا على تطوير وتحسين عملياتهم على مستوى العالم حيث قامت بإنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع أعمالهم وقد أقامت تلك العصابات مواقع على شبكة الانترنت لتفادي القوانين في بلد ما، بحيث تعمل في بلد آخر يسمح بتلك الأنشطة. والجريمة المنظمة ليست وليدة التقدم وإن كانت استفادت منه فالجريمة المنظمة وسبب تقدم وسائل الاتصال والتكنولوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا قيود المكان وإنما أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها أي حدود جغرافية، كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الانترنت في تخطيط وتحرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة. ولاشك بأن الجريمة المنظمة في الأساس تسعى للإفادة المادية أو تحقيق الأرباح من خلال مواصلة العمل بوسائل جرمية ولذا كما تستعين الشركات العادية بشبكة الانترنت بحثاً عن فرص جديدة لتحقيق الأرباح كذلك تقفل المنظمات الإجرامية، والمنظمات الإجرامية ليست اللاعبات في أسواق الأعمال غير المشروعة ولكنها تكون في أحيان كثيرة أهم اللاعبين وذلك بسبب قدرتها الكبيرة على المنافسة التي يوفرها لها سوق العمل. كما أن

المنظمات الإجرامية تميل إلى مهارة كبيرة في اكتشاف واستغلال فرص القيام بأعمال ومشاريع جديدة غير مشروعة في هذا السياق توفر الانترنت والنمو المتواصل للتجارة الالكترونية مجالات هائلة جديدة لتحقيق أرباح غير مشروعة. وبعض المتخصصين في مجال الجريمة المنظمة يربط بينها وبين الإرهاب على أساس أن العمل الأساسي لكلاهما هو إنشاء الخوف والترويع فيما بين الناس كما أن هناك توافق كبير جداً في طريقة العمل وأساليب التنفيذ مما أدى بهؤلاء الخبراء إلى الاعتقاد إلى وجود تناسق كبير وتخطيط مشترك فيما بين كل من أعضاء منظمات الجرائم المنظمة والإرهابيين، فالإرهابيون يستفيدون من خبرة هؤلاء الأشخاص في تنفيذ مخططاتهم والعكس صحيح فأعضاء منظمات الجرائم المنظمة يستفيدون من الإرهابيين الأموال الطائلة منهم مقابل تنفيذ مخططاتهم.

هـ) تجارة المخدرات:

نجد أن كثيراً من أولياء الأمور يحذرون أبنائهم من مخالطة رفقاء السوء لما لهم من أثر سلبي عليهم خاصة بعد انتشار ظاهرة المخدرات في أوساط الشباب ولكن ما يغفل عنه كثير من الآباء في عصرنا الحديث هي المواقع السيئة ومنها المواقع المنتشرة في الإنترنت. وتعد تجارة المخدرات هي أحد أهم وأخطر أنواع التجارة المحرمة على مستوى العالم ويأتي بعدها تجارة الرقيق الأبيض ثم تجارة السلاح. فتجارة المخدرات هي أكثر أنواع التجارة المحرمة على مستوى العالم ولم تفلح كافة الجهود المبذولة على مستوى العالم إلا في تقليلها دون القدرة على منعها نهائياً نظراً لوجود بعض دول العالم التي تتركز فيها تصنيع وتهريب تلك المخدرات إلى باقي دول العالم ولما تدره تلك التجارة على العاملين فيها من ربح وفير. وقد كان تجار المخدرات يلاقون صعوبات كثيرة في الاتفاق على عمليات التدريب على مستوى العالم إلا أنه بعد التطور التكنولوجي الكبير على مستوى العالم والمتمثل في اتساع شبكة الإنترنت قد استغل مصنعي ومهربي المخدرات شبكة الإنترنت واستخدموها في الاتفاق على عمليات تهريب المخدرات من بلد إلى آخر. كما أن الإنترنت ساهم بنشاط آخر في انتشار ذلك الوباء وهو عن طريق الترويج لها ليزيدوا من السوق الاستهلاكية والطلب على منتجاتها.

كما أنه ظهر في الآونة الأخيرة مواقع تقوم بتعليم الناس بكيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأيسر الوسائل المتاحة.وفي تقرير نشرته شبكة (CNN) الإخبارية ذكر فيه قيام السلطات الاتحادية والمحلية في عدد من الولايات المتحدة الأمريكية بحملة واسعة بهدف متابعة مروجي المخدرات الذين يوزعون العقار المسمى (GHB) عبر شبكة الإنترنت وألقت القبض على العشرات منهم في مختلف المدن الأمريكية في محاولة من السلطات في الحد من انتشار هذا العقار المخدر لما له من آثار مدمرة على الجهاز العصبي لمن يتعاطاه.

و (GHB) هو عقار مخدر مكون من خليط من عدد من المواد الكيميائية الصناعية. وكان الكونغرس الأمريكي قد أصدر قانون بتحريمها قبل عدة سنوات ويعمل هذا العقار وكذلك مشتقاته كعامل مؤثر على النظام المركزي للأعصاب مما يسبب في الإحساس بالدوار والغثيان وعدم القدرة على التركيز وقد قدرت الأجهزة الأمنية الأمريكية أن هذا العقار ومشتقاته تسبب في وفاة أكثر من اثنين وسبعين شخصاً وفقاً للأوراق الرسمية وتحاول الأجهزة الأمنية والحكومية الأمريكية عقد دورات تثقيفية الهدف منها تحذير الجميع بصفة عامة والنساء بصفة خاصة من الوقوع في فخ المروجين الذين يخلطون المواد المخدرة بالمشروبات.

و) غسيل الأموال:

غسيل الأموال يعني في أبسط صورة هو تحويل المصدر غير المشروع للأموال إلى مصدر مشروع فمثلاً تحويل الأموال الناتجة من عمليات غير مشروعة لتجارة المخدرات إلى أموال مشروعة كتجارة السيارات. ومصطلح غسيل الأموال هو مصطلح حديث إلى حدٍ ما وقد بدأ استخدامه في الولايات المتحدة الأمريكية عام ١٩٣١م حيث تمت محاكمة أحد زعماء المافيا ومصادرة أمواله على أساس أن مصدرها تجارة غير مشروعة.

وهناك عدة تعريفات لهذا المصطلح منها أنه تحويل مصدر الأموال غير المشروع إلى مصدر مشروع وقد أعطت شبكة المجرمون مجالاً لتطوير أساليبهم الإجرامية بما في ذلك الاستفادة من الشبكة لتوسعة وتسريع أعمالهم في غسيل أموالها غير المشروعة، ويجد المتصفح للإنترنت مواقع متعددة عن غسيل الأموال ومن المميزات التي يعطي بالانترنت لعمليات غسيل الأموال السرعة، إغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما تساهم البطاقات الذكية والتي تشبه في عملها بطاقات البنوك المستخدمة في أجهزة الصرف الآلية في تحويل الأموال بواسطة المودم أو الإنترنت مع ضمان تشفير وتأمين العملية.

وأيضاً كان انتشار التجارة الالكترونية عبر شبكة الإنترنت خير معين لهؤلاء القائمين على عمليات غسيل الأموال، فالتجارة الإلكترونية وانتشارها حول أنحاء العالم أجمع قد ساعد كثيراً في عمليات غسيل الأموال نظراً لسرعة الاتفاق على الصفقات، وإتمامها من خلاله دون أن تكون في معظم الأحيان تمت رقابة قانونية صارمة بل أنه في حالة وجود رقابة قانونية يكون من الممكن تفادي تلك الرقابة وإتمام تلك الصفقات دون أي تأثير. كما ساهمت بعض الجرائم التي ترتكب عبر الانترنت مثل تزوير البيانات والمواقع الافتراضية التي وفرتها شبكة الانترنت في ازدياد عمليات غسيل الأموال.

المبحث العاشر: مكافحة جرائم الكمبيوتر والانترنت

إن مكافحة الجرائم الالكترونية لن يكون له أي تأثير إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق والتعاون وعليه فإن أي مجهود أو إجراءات فردية تقوم بها الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم فتلك الجرائم لها طابع خاص وسمات مميزة لها عن غيرها من الجرائم وهي كالتالي:-

١- أن تلك الجرائم تستهدف معنويات وليست ماديات محسوسة، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير.

٢- كما أنها تتسم بالخطورة البالغة نظراً لأغراضها المتعددة. ونظراً لحجم الخسائر الناجم عنها قياساً بالجرائم التقليدية. ونظراً لارتكابها بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمراً صعباً. ونظراً لأنها بذاتها تنطوي على سلوكيات غير مألوفة. وبما أتاحته من تسهيل ارتكاب الجرائم الأخرى تمثل إيجاد وسائل تجعل ملاحقة الجرائم التقليدية أمراً صعباً متى ما ارتكبت باستخدام الكمبيوتر.

٣- التحقيق والتحري في تلك الجرائم والمقاضاة في نطاقها تنطوي على مشكلات وتحديات إدارية وقانونية تتصل ابتداء بمقتضيات ومتطلبات عمليات ملاحقة الجناة، فإن تحققت مكنت الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم.

٤- أن هذه الجرائم من الجرائم العابرة للحدود فهي لا تتم من داخل دولة ويكون تأثيرها منحصر في تلك الدولة وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دولة أخرى وتكون آثارها ممتدة لتصل إلى عدد

غير محدود من الدول وعليه فإن الأساس الذي يرتكز عليه مجال مكافحة الجرائم الالكترونية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج البشعة على اقتصاديات الدول والكيانات الاقتصادية.

ولمواجهة مثل هذه الجريمة (جرائم الكمبيوتر والانترنت) العابرة للحدود مواجهة فعّالة يجب تجريم صورها في القانون الوطني للمعاقبة عليها وان يكون هناك تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وإيجاد الحلول لمشكلاتها الأساسية وأبرز تلك المشكلات:

أ- غياب مفهوم عام متفق عليه بين الدول حول نماذج النشاط المكون للجريمة المتعلقة بالكمبيوتر والانترنت.

ب- غياب الاتفاق حول التعريف القانوني للنشاط الإجرامي المتعلق بهذا النوع من الإجرام.

ج- نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع المعلومات والأدلة عنها للإدانة فيها.

د- عدم كفاءة وملائمة السلطات التي ينص عليها القانون بالنسبة للتحري واختراق نظم الكمبيوتر لأنها عادة متعلقة بالضبط والتحري بالنسبة لوقائع مادية هي الجرائم التقليدية وغير متوائمة مع غير الماديات كاختراق المعلومات المبرمجة وتغييرها في الكمبيوتر.

هـ- عدم التناسب بين قوانين الإجراءات الجنائية للدول المختلفة فيما التعلق بالتحري في الجرائم المتعلقة بالحاسوب.

و- السمة الغالبة للكثير من جرائم الكمبيوتر هي أنها من النوع العابر للحدود وبالتالي كثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض والجرائم الاقتصادية والمالية وجرائم التلوث البيئي.

ز- عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها أن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وديناميكية التحريات فيها وكفالة السرعة بها.

ويمثل مشروع الاتفاقية الأوروبية لجرائم الكمبيوتر في الوقت الحاضر المشروع الأكثر نضجاً لمواجهة جرائم الكمبيوتر بل وواحداً من أهم أدوات التعاون الدولي في هذا الحقل.

والتي سنتطرق لها بإذن الله في هذا المبحث.

عليه فسيكون تناولنا لمكافحة الجرائم الالكترونية من خلال التركيز على التعاون الدولي والعناصر التي يرتكز عليها هذا التعاون والتي تنحصر في الأتي:

- المعاهدات والمؤتمرات الدولية.
- إصدار قوانين جديدة تجرم الجرائم الالكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التجانس.
- التعاون الدولي.
- اتحاد الشركات والكيانات الاقتصادية الكبرى في مجال حماية أمنها الالكتروني.

- المعاهدات والقوانين الخاصة بحق الملكية الفكرية.

١/ المعاهدات والمؤتمرات الدولية:

سبق وأن أشرنا بأن المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة جرائم الكمبيوتر والانترنت وقد عقدت العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الالكترونية ومن تلك المعاهدات.

أ- المعاهدة الأوربية لمكافحة جرائم الانترنت:

وقّعتْ اللجنة الخاصة المعنية لقضايا الجريمة بتكليف من المجلس الأوربي على المسودة الثنائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الانترنت وسط انتقادات من دعاة حماية الشخصية وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيها من قبل البلدان المعنية ستلزم الاتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي بها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

وتتضمن بنود المعاهدة التي تم تعديل مسودتها (٢٧ مرة) قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلة وفرض القوانين لكن الصلاحيات الدولية الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومات استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يسيئون استخدامها.

ب- معاهدة بودابست لمكافحة جرائم الانترنت:

بعد أن وصلت جرائم الانترنت إلى حد خطير أصبح يهدد الأشخاص والممتلكات فقد شهدت العاصمة المجرية بودابست في أواخر عام ٢٠٠١م ميلاد أولى المعاهدات الدولية التي تكافح تلك الجرائم ويعد التوقيع على تلك المعاهدات الدولية هو الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الانترنت واستخدامها الاستخدام الأسوأ.

ويعد التوقيع على تلك الاتفاقية هو نتاج مباحثات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الاتفاقية.

وقد أجريت العديد من الدراسات على مجال التضامن الدولي في مكافحة جرائم الانترنت أوضحت أن العديد من الدول لا تستطيع بمفردها مواجهة تلك الجرائم التي ترتكب عبر الانترنت مهما وضعت من قوانين ومهما غلّظت من عقوبات تلك الجرائم نظراً لكون تلك الجرائم هي من الجرائم عابرة الحدود كما أسلفنا.

٢/ إصدار قوانين جديدة تجرم الجرائم الالكترونية في كافة أنحاء العالم بحيث يكون بينها قدر كبير من التناسق:-

إن الدول المتقدمة تكنولوجياً صاغت نصوصاً قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجياً.

أ. على المستوى العالمي:

أولاً: دولة السويد: تعتبر السويد من أول الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الكمبيوتر والانترنت لتستطيع أن تعاقب المتهمين بارتكاب تلك الجرائم الالكترونية وصدر أول

قانون خاص بها وسمي بقانون (البيانات) وقد صدر هذا القانون عام ١٩٧٣م، وقد عالج هذا القانون قضايا الاحتيال عن طريق الشبكة، وجرائم الدخول غير المشروع على البيانات الالكترونية أو تحويلها أو الحصول غير المشروع عليها.

ثانياً: الولايات المتحدة الأمريكية: كانت الولايات هي الدولة الثانية التي تبعت السويد في إصدار قوانين خاصة بها تجرم الجرائم الالكترونية حيث شرّعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي (١٩٦٧م – ١٩٨٥م)، وحدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية:

- جرائم الحاسب الآلية الداخلية.
- جرائم الاستخدام غير المشروع عن بعد.
- جرائم التلاعب بالحاسب الآلي.
- دعم التعاملات الإجرامية.
- سرقة البرامج الجاهزة.
- مكونات الحاسب المادية.

وقد خولت وزارة العدل الأمريكية في عام ٢٠٠٠م خمس وجهات حكومية للتعامل مع جرائم الانترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي (FBI).

ثالثاً: بريطانيا: فهي ثالث دولة تسن قانوناً خاصاً بها بجرائم الانترنت حيث أقرت قانوناً لمكافحة التزوير والتزييف عام ١٩٨١م الذي شمل في تعاريفه الخاصة تعريف أداة التزوير ووسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الالكترونية أو التقليدية أو أي طرق أخرى.

رابعاً: كندا: فهي تطبق قوانين متخصصة ومفصلة للتعامل مع جرائم الانترنت حيث عدلّت في ١٩٨٥م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الكمبيوتر والانترنت لما شمل القانون الجديد أيضاً تحديد للعقوبات المطبقة على المخالفات الالكترونية كما أوضح القانون صلاحيات جهات التحقيق وخول لمأمور القبض القضائي حق التفتيش على أنظمة الحاسب الآلي والتعامل معها وضبطها.

خامساً: الدانمرك: فقد شرعت أول قانون خاص بها في مجال مكافحة جرائم الكمبيوتر للانترنت في عام ١٩٨٥م وقد. شمل القانون العقوبات المحدودة على ما يرتكب من جرائم مثل الدخول غير المشروع أو تزوير البيانات سواءً كان التزوير بالحذف أو الإضافة.

سادساً: فرنسا: فتعتبر من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع جرائم الانترنت، وأصدرت في عام ١٩٨٨م القانون رقم: (١٩ – ٨٨) والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم كما تم في عام ١٩٩٤م تعديل قانون العقوبات الخاصة بالجرائم المعلوماتية وقد أوكل هذا القانون إلى النيابة العامة - سلطة التحقيق – بما في ذلك طلب عمل التحريات وسماع الشهود.

سابعاً: هولندا: فقد أصدرت قوانين خاصة بها للتوائم مع تلك الجرائم الحديثة ليكون في وسعها التعاون معها ومحاولة السيطرة عليها وقد قامت بتعديل القوانين الخاصة بها وخولت للقاضي إصدار أوامره بالتصنت على شبكات الحاسب متى ما كانت هناك جريمة خطيرة ومتى كان هذا التصنت قادراً على كشف تلك الجريمة.

ثامناً: فنلندا: أصدرت قوانين خاصة لتلائم حاجة تلك الجرائم الحديثة لتكفل تلك القوانين الروع والعقوبة.

تاسعاً: اليابان: قامت بإصدار قوانين خاصة بها لتستوعب المستجدات الإجرامية المتمثلة في جرائم الكمبيوتر والحاسب الآلي وقد نصت على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إنشاء كلمة السر التي يستخدمها إذا كان ذلك سيؤدي إلى إدانته، وشرعت قانوناً عام ١٩٩١م يجيز التصنت على شبكات الحاسب الآلي إذا ما كان ذلك في مجال البحث عن الأدلة الخاصة بأحدث الجرائم الالكترونية.

عاشراً: دولة المجر: قامت بسن قوانين خاصة بها لتجرم الجرائم الالكترونية وقد تضمنت تلك القوانين التي شرعتها على كيفية التعامل مع مثل هذا النوع من الجرائم وأيضاً كيفية التعامل مع المتهمين بارتكاب الجرائم وهي الإجراءات التي تسهل عمل الجهات المنوط بها مواجهة مثل تلك الجرائم والقبض على المتهمين بارتكابها.

ب/ على المستوى العربي:

إن الدول العربية وللأسف الشديد لم تقم بتشريع أي قوانين جديدة خاصة بها لمكافحة جرائم الكمبيوتر والانترنت بل لم تقم بتحديث قوانينها وأنظمتها الخاصة لتستوعب تلك الحقول الإجرامية، حيث أن الدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتقدم الإجرامي بل إنه إذا وقع لدى إحدى الدول العربية جرائم معلوماتية فيحاولون تطبيق قواعد القانون الجنائي التقليدي عليها وفي الغالب فإن عقوبة القوانين الجنائية التقليدية لا تتناسب مع حجم الخسائر الناتجة عن الجرائم الالكترونية وبالتالي لا يكون العقاب المنصوص عليها مناسب.

ج/ على المستوى الوطني:

أما في المملكة العربية السعودية فهي لا تواجه مثل هذه المشاكل على أساس أن كافة تشريعاتها وأنظمتها مستمدة من الشريعة الإسلامية السمحة، والشريعة الإسلامية لا تحتاج إلى تحديث فهي صالحة لكل زمان ومكان. ولكننا نرى أن تضاف مثل هذه الجرائم ضمن القرار الوزاري الصادر من سمو سيدي وزير الداخلية حفظه الله برقم: (١٢٤٥) في ١٤٢٣/٧/٢٣هـ ليكون المحقق على بصيرة من مثل هذه الجرائم وهل هي من القضايا الموجبة للتوقيف من عدمه وليتمكن المحققون من كيفية التعامل معها، كما أننا نرى أن هناك حاجة ماسة لإنشاء إدارات جديدة بوزارة الداخلية تكون مسئولة عن جرائم الكمبيوتر والانترنت بحيث تكون هذه الإدارات جديدة في تكوينها ونوعية العمل المناط بها وأن يكون هناك سعي حثيث لتأهيل العاملين بها ليكونوا على أعلى درجة ممكنة من التخصص والحرفية في تكنولوجيا الحاسبات وشبكة الانترنت. ولعل هذا الأمر يزداد أهميةً بعد أن ازداد عدد مستخدمي شبكة الانترنت في المملكة العربية السعودية، وهذا الازدياد سوف يكون معه وبدون شك من يقومون باستخدام تلك التكنولوجيا استخداماً سيئاً ويستغلونها في ارتكاب جرائمهم معتقدين أنهم بعيدون جداً عن أيدي القانون وبعيدين عن أن ينالوا عقابهم على ما اقترفت أيديهم. وقد اتخذت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الانترنت المشرفة على عمل مقدمي خدمة الانترنت في المملكة عدد من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين والمتسللين ومنعهم، وقد أوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الانترنت في

المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين وإساءة استخدام البريد الالكتروني: (E - MAIL)، وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الانترنت في المملكة ومن بين هذه الإجراءات ما يلي: -

١- منع انتحال أرقام الانترنت والتي يقوم من خلالها المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة.

٢- العمل على منع إساءة استعمال البريد الالكتروني سواءً 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- الحصول على خدمة (LTP) عن طريق وحدة البروكسي ومزوّد الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

٤- تحديث سجلات منظمة رايب الخاصة بمقدمة الخدمة.

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

٦- الاحتفاظ بسجل استخدام مزوّد الاتصال الخاص بالمشتركين وسجل استخدام البروكسي لمدة لا تقل عن ستة أشهر.

٣/ التعاون الدولي:

بما أن جرائم الانترنت هي جرائم عابرة للحدود أي أنها لا تتم وتنتهي في أراضي دولة معينة لذلك فإن التعاون الدولي هو من أهم سبل مكافحة جرائم الانترنت وملاحقة مرتكبيها ، فبغير التعاون الدولي سيزداد معدل ارتكاب تلك الجرائم ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين المطبقة بها ما ارتكبوه من جرائم.

وتعتبر المعاهدات الدولية التي تنضم إليها العديد من الدول هي النموذج الذي يكوّن هذا التعاون الدولي في ذلك المجال، ومثال ذلك التعاون الدولي في مجال مكافحة الجريمة المنظمة وقد بدأ هذا التعاون الدولي بمؤتمر الأمم المتحدة السابع، والذي عُقد عام ١٩٨٥م، ومنع الجريمة المنظمة وأوصى بعدة توصيات حيال التعامل معها والقضاء عليها ، وكذلك المؤتمر الدولي الذي عُقد بمدينة الرياض بالمملكة العربية السعودية مطلع عام ١٤٢٦هـ لمكافحة الإرهاب.

وقد كانت معاهدة المجلس الأوربي حول جرائم الشبكات الالكترونية التي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعملية وضع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها في نهاية الأمر في جهودها التشريعية والتنظيمية وتطبيق القوانين، ويستند نهج هذه المعاهدة إلى اعتراف أساسي بضرورة قيام انسجام بين قوانين الدول المعنية ، حيث أن الانسجام ضروري بالنسبة للقوانين الأساسية وعلى جميع الدول أن تعيد تقييم ومراجعة قواعد الإثبات والتفتيش وإلغاء القبض والتنصت الالكتروني وما شابه ذلك لتشمل المعلومات الرقمية وأنظمة الكمبيوتر الحديثة وأنظمة الاتصالات الحديثة والطبيعة العالمية لشبكة الانترنت.

ومن الضروري أن تطوّر الحكومات أجهزة تطبيق القانون قدراتها على تطبيق هذه القوانين وهذا يحتاج إلى تطوير الخبرات والكفاءات في مجال مكافحة الجريمة التي ترتكب عبر الشبكات الالكترونية.

ولتفعيل التعاون الدولي لابد من التركيز على العناصر الرئيسية التالية وهي:

١- الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مجال مكافحة جرائم الانترنت.

٢- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي، أي تنفيذ ما تنص عليه تلك الاتفاقيات من إجراءات دون أي تأخر.

٣- العمل على وجود أكبر قدر من التناسق والتطابق فيما بين قوانين الدول المختلفة والمتعلقة بمكافحة جرائم الانترنت فلا يكون الفعل الذي ارتكب جريمة في بلدٍ ما وغير معاقب عليه في قانون دولة أخرى، فمن هنا يجد المجرمون الملاذ الآمن الذي يلجئون إليه دون أي اعتبار لما ارتكبوه من جرائم.

٤- تعاون جميع الدول في تسليم المطلوبين أمنياً إلى الدول التي تطالب بهم لارتكابهم جرائم الانترنت.

٤/ الحجب: يتمثل في حجب المواقع الإباحية والإرهابية التي تشجع الجريمة وتظهرها بوجه مشرق، والمملكة العربية السعودية هي من الدول القليلة جداً التي أدركت حكومتها الرائدة أهمية هذا الأمر فطبقت أمثال هذه البرامج على مستوى الدولة ككل فهي بحق تعتبر من الرواد في هذا المجال. أما باقي الدول التي تتبع سياسة الحجب فإنها في الغالب تحجب شيئاً قليلاً جداً من المواد الإباحية بالإضافة إلى أن أجهزة الحجب لديها ضعيفة جداً ومقترنة بثغرات كبيرة والحجب من الأساليب المجدية التي هدانا إليها ربنا عز وجل في كتابه الكريم كما ورد في سورة يوسف عليه السلام، قال تعالى:) قال ربي السجن أحب إليَّ مما يدعونني إليه (الآية. كما أن الأستاذ الدكتور كاس سانستين وجد بان الدول التي تفرض قوانين صارمة في منع المواد الإباحية تنخفض فيها نسبة هذه الجرائم، وهذا ملاحظ في المملكة العربية السعودية ولله الحمد. ولقد قام باحثان من جامعة (نيوهامبشير) بأمريكا بدراسة تفشي ظاهرة الإباحية والدعارة واثر ذلك على جريمة الاغتصاب. وبعد دراسة شملت جميع الولايات الأمريكية وجد أن الولايات التي تكثر فيها وسائل الدعارة والإباحية ترتفع فيها نسبة جرائم الاغتصاب، والعكس صحيح.

٥/ فرض رقابة على المقاهي التي تقدم الانترنت كخدمة لمرتاديها مع التأكيد على منع ارتياد صغار السن لتلك المقاهي وفرض عقوبات وغرامات مالية على المقاهي التي تخالف ذلك، والعمل على تشجيع مرتادي هذه المقاهي في البحث عن المعلومات المفيدة واستخدام الانترنت في مجال البحث العلمي. ونرى إجراء دراسات مقارنة في مقاهي الانترنت لمعرفة أسباب انتشار ظاهرة ارتيادها والانحراف إلى الجريمة بين مرتاديها بجميع مناطق المملكة.

٦/ تفعيل دور وسائل الإعلام في نشر التوعية الوقائية من عواقب النظر في المواقع الإباحية وكذلك تحصين المواطنين فكرياً ودينياً وإفهامهم أن مثل هذه المواقع تستهدف شبابنا وهي محاولة لتصدير الإباحية بدعوى الحرية وان أهل الغرب بقيمهم الفاسدة وأمراضهم الخبيثة ومبادئهم الذميمة لم يكتفوا بإفشاء الرذائل والمنكرات ودواعي غضب الجبار بينهم ولكن تمادى بهم الحال إلى محاولة تصدير هذه المصائب والفتن إلى بلاد المسلمين، كما نرى أن يكون هناك تشهير وإعلان لكل من يقبض عليه في مثل هذه الجرائم لتحقيق الرادع النفسي وإتباعاً لأمر الله تعالى.

٧/ استخدام المناهج التعليمية كأوعية ووسائل لمكافحة جرائم الكمبيوتر والانترنت وربطها بالنواحي الدينية.

٨/ إنشاء هيئة مشابهة لهيئة المواصفات والمقاييس يكون اختصاص هذه الهيئة تكوين مواقع علمية مفيدة

ومتقدمة عالمياً. فعلى سبيل المثال نجد أن موقع (Google) بمجرد وضعك لأي كلمة بحث فستجد أن الصفحة قد امتلأت بالمواقع فمنها المفيد ومنها الضار، ولكن نريد من هذه الهيئة أن تنشيء مواقع مشابهة لهذا الموقع في الهيكل ومخالفه له في المضمون بحيث يكون ما بداخله منقح أمنياً ودينياً ويقصد به البناء لا الهدم.

المراجــع

١- داود حسن طاهر ـ جرائم نظم المعلومات - جامعة نايف العربية للعلوم الأمنية.

٢- منير محمد الجنبيهي - جرائم الانترنت الحاسب الآلي.

٣- موقع العقيد - المنشاوي على الانترنت.

٤- مزيد النفيعي - مقاهي الانترنت والانحراف إلى الجريمة بين مرتاديها.

٥- محمد محي الدين عوض - جرائم غسل الأموال - جامعة نايف العربية للعلوم الأمنية.

٦- إياس الهاجري - جرائم الانترنت.