

## مفهوم الجريمة باستخدام شبكة المعلومات الدولية<sup>(\*)</sup>

السيد آدم سميان ذياب الغريزي

مدرس القانون الجنائي المساعد

كلية القانون / جامعة تكريت

### أقدمة :

أصبحت الجرائم في ظل العصر المتطور في تزايد مستمر يستخدم مرتكبيها تقنية العصر الرقمي مثل ما يستخدمه الآخرون لخدمة الإنسانية ، والشبكة الدولية للمعلومات (الإنترنت) كوسيلة من وسائل التطور في العصر الحديث أصبحت كأحدى وسائل الجرائم المرتكبة عن طريق استخدام هذه الشبكة . بحيث أصبحت كثيرة ومتنوعة ، وواسعة النطاق بسعة هذه الشبكة ، بحيث أصبحت الشبكة هدفا للمجرمين المجيدين لاستخدامها ، أو أصبحت وسيلة لإرتكاب سلوكيات مجرمة، ومنها الواقعة على الأموال ومنها الواقعة على الأشخاص ، والجرائم الواقعة على الملكيات ومنها حقوق المؤلفات والمخترعات .... وغيرها في تعدد مستمر ، بإستمرار التطور التقني المتسارع الذي يشهده العصر التقني الذي نعيش فيه . فهل نحتاج إلى أطار قانوني ينظم العمل على هذه الشبكة ؟ وهل إن قوانيننا الجنائية قادرة وكافية لمعالجة هذه السلوكيات المتنامية والمتطورة بشكل يومي ؟ بشقيها الموضوعي العقابي ، والشكلي الإجرائي .

فنحن في القانون الجنائي محكومون بمبدأ الشرعية الذي يميز قانوننا العقابي عن غيره من القوانين ، والقياس محظور في الجانب العقابي ، والتفسير لا يمكن التوسع به ، فكيف سنستطيع مع المحافظة على هذه المبادئ ، فرض العقاب على هذه السلوكيات التي تنتهك الحقوق والمصالح؟ هل نستطيع القياس على الجرائم الأخرى؟ ونعتبر هذه الجرائم صورا لها؟ أم نستطيع التوسع في التفسير لنشملها بغيرها من السلوكيات المجرمة ؟ أم أن هذه السلوكيات تحتاج إلى تجريم جديد يحدها ، ويعاقب عليها ؟

فاستخدام الشبكة شائع بمجتمعنا العراقي ليس للمثقفين فقط ، بل أصبح حتى الأميون الذين لا يجيدون القراءة والكتابة يستخدمون الشبكة كوسيلة للإتصال

(\*) أستلم البحث في ٢٣/٩/٢٠٠٩ \*\*\* قبل للنشر في ١١/٣/٢٠٠٩ .

الصوتي والصوري، بل أصبحت الشبكة ولعا ليس للبالغين فقط بل حتى الأطفال الأحداث ، فالكثير اليوم يمتلكون الحواسيب الشخصية ، ولكننا لم نسأل أنفسنا ، من أين هذه النظم التشغيلية والتعريفية المثبتة عليها ؟ فنظام التشغيل الشهير Windows والذي يشغل كل حواسيبنا في العراق ، القليل منه نسخة أصلية ، والبقية الكثيرة مستنسخة ، فما هو العقاب على هذا التصرف هل نحن في مجال المسؤولية الجنائية جميعا ، باستعمالنا برامج مسروقة ، لم ندفع ثمنها لشركتها المصنعة ، وعند ولوجي لموقع الشركة المصنعة وجدت أن سعر النسخة الواحدة ٤٠٠ يورو . فكيف هو الحال مع عشرات البرامج التي نستخدمها في حواسيبنا الشخصية؟

وعند سؤالي عن النظم التشغيلية والبرامج التطبيقية للمختصين حاسوبيا وجدت أن أغلبها مستنسخة ، والكثير منها يستطيع إختراق الحواسيب الشخصية القريبة أو البعيدة المرتبطة بالشبكة وليس فيها برنامج الحماية الكافي ، فالبرنامج المعروف (Mac address change) والذي يستطيع سرقة الخدمة من كل شخص قريب بمسافة ثلاثين كيلو مترا متوفر لدى حتى الأطفال ، وهناك برامج موجودة على الشبكة تشتري بالبطاقات المالية Master card وغيرها وبأثمان زهيدة تستطيع إن تنزع داخل حاسب المتلقي للخدمة ، يستطيع زارعها تصفح وإمتلاك كل ما في الحاسب من صور عائلية وأفلام شخصية أو حتى بحوث علمية !!! فما هو الإجراء الذي ستتخذه السلطات التشريعية في العراق الذي أسس في ٢٠٠٠/١/١ الشركة العامة لخدمات الشبكة الدولية للمعلومات<sup>(١)</sup> . وليس لديه نص يعاقب على أي إنتهاك بصورته الصريحة .

وكتمهيد تاريخي ، فقد ظهرت شبكة المعلومات الدولية إلى الوجود كثمرة لمشروع حكومي أمريكي بدء تنفيذه عام ١٩٦٠ وتحقق وجوده النهائي عام ١٩٦٩ وقد سمي ( الإربانت - ARPA net ) كلفت بتنفيذه وكالة مشروعات البحوث المتقدمة ARPA- Advanced Research Projects Agency التابعة لوزارة الدفاع الأمريكية ومن هنا اكتسبت الشبكة التسمية المشار إليها ، وقد استخدمت في البداية للأغراض المتعلقة بعلم الكمبيوتر والمشروعات الهندسية المرتبطة بشكل مباشر بالأمور العسكرية وقد أصبحت هذه الشبكة رابطة اتصال حيوية فيما بين المتعاونين من أماكن نائية في تنفيذ المشروعات ، لكنها ظلت من الناحية العملية غير معروفة خارج نطاق نشاط وكالة مشروعات البحوث المتقدمة . وفي عام ١٩٨٩ قررت الحكومة الأمريكية وقف تمويل الإربانت ووضعت

(١) الوقائع العراقية - رقم العدد: ٣٨١٢ بتاريخ: ٢٠٠٠/٠٧/٠٢ .

خطط لإنشاء خلف تجاري لها في شكل شبكة تقرر تسميتها (الانترنت) وقد اشتق الاسم من اسم البروتوكول الأساسي للاتصالات وظل اغلب مشتركى الانترنت من بين العلماء داخل الجامعات والشركات العاملة في صناعة الكمبيوتر الذين استخدموها لتبادل البريد الالكتروني .

وبالرغم من أن هذه الخدمة ليست بالخدمة الحديثة حيث بدأ استخدامها منذ عام (١٩٦٩م) إلا أن استخدامها كان آنذاك مقتصرًا على الأغراض العسكرية وفي دولة واحدة هي أمريكا، ومنذ فترة ليست بالطويلة بدأ انتشار استخدام الشبكة على المستوى العالمي وفي كل المجالات إذ غزت هذه الخدمة العالم بشكل سريع جدا وعلى كافة مستويات المجتمع. ويقدر عدد مستخدمي هذه الشبكة عالميا في العام (١٩٩٨م) بحوالي (١٣٤) مليون مستخدم وتوقعت إزدياد هائل في عدد المستخدمين لها سنويا يمكن أن يصلوا في العام (٢٠٠٥ م) إلى حوالي ( ٢٤٥ ) مليون \* مستخدم وستكون غالبية هذه الزيادة في خارج الولايات المتحدة الأمريكية، بمعنى أن انتشار الشبكة لن يكون محصورا في أمريكا فقط بل سيشمل جميع دول العالم وهذا يوضح وبجلاء سرعة انتشار استخدامها كظاهرة يتحول إليها الجميع بصورة سريعة وشبه حتمية حيث سيعتبر من يتخلف عن مواكبتها في عداد المتخلفين عن مواكبة تقنية العصر وبالتالي سيَتَخَلَّفُ عن الركب.

ولم يكن هناك قلق مع بدايات عمل الشبكة من جرائم يمكن أن ترتكب عليها أو بواسطتها لا لأنها آمنة في تصميمها وبنائها ، بل نظرا لمحدودية مستخدميها ، علاوة على كونها كانت مقصورة على فئة معينة من المستخدمين – الباحثين ومنتسبي الجامعات- إلا أنه ومع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة .

وفي هذا الإطار فان أول حالة موثقة لإساءة استخدامها ترجع إلى عام ١٩٥٨ وفقا لما نشره معهد ستانفورد في الولايات المتحدة الأمريكية ، ليبقى الحديث من ذلك الوقت وحتى مطلع السبعينات في إطار البعد الأخلاقي وقواعد السلوك المتعين أن تحكم استخدامها ، ولتنتج الجهود والمواقف نحو حسم الجدل باعتبار إساءة الاستخدام فعلا موجبا للمسؤولية القانونية ، ولتتطلق التشريعات الوطنية في حقل جرائم الشبكة مع نهاية السبعينات ( تحديدا في الولايات المتحدة ابتداء من ١٩٧٨ ) . أما الجهد الدولي فقد تحقق ابتداء في حقل الخصوصية ، ففي عام ١٩٦٨ ، شهد مؤتمر الأمم المتحدة لحقوق الإنسان ، طرح موضوع مخاطر التكنولوجيا على الحق في الخصوصية ، إذ بالرغم من أن الحق في الخصوصية نشأ قبل هذا التاريخ وحظي بجدل قانوني وقضائي وفكري منذ مئات

السنين ، فانه لم يكن ثمة إثارة لما يتصل بهذا الحق متعلقا بالمعلومات الشخصية المعالجة آليا بالقدر الذي أثير في المؤتمر المشار إليه ، والذي استتبعه إصدار الأمم المتحدة قرارات في هذا الحقل لتشهد بداية السبعينات ( تحديدا عام ١٩٧٣ في السويد ) انطلاق تشريعات قوانين حماية الخصوصية مع الإشارة إلى أنها نوقشت في نظم قانونية أجنبية كثيرة - كدول أوروبا الغربية مثلا - ضمن مفهوم حماية البيانات Data Protection.<sup>(١)</sup> فأين نحن من هذا الركب المتسارع ؟ ومتى سنعالج هذه المشاكل التي يفرزها العمل على هذه الشبكة وقد سبقتنا الدول بعشرات السنين.

ولبيان مفهوم الجريمة باستخدام شبكة المعلومات الدولية ، وللإجابة عن التساؤلات السالفة، نتناول في بحثنا هذا بيان مفهومها ، بتقسيم بحثنا هذا إلى مبحثين ، نخصص الأول منه لمعرفة تعريف الجريمة والمجرم في الجرائم التي تتم عن طريق هذه الشبكة ، وكذلك بيان خصائص الجريمة والمجرم فيها ، ونخصص المبحث الثاني لبيان أهم صور الجرائم باستخدام هذه الشبكة ، سواء كانت كصور للجريمة الخاصة بها ، أو كانت الشبكة وسيلة في ارتكاب السلوك الإجرامي لغيرها من الجرائم ، نطمح أن يكون بحثنا هذا بذرة لدراسات موسعة ، أو حافزا لتشريع عقابي يتناولها بصورة قانونية ، نستطيع أو نستطيع غيرنا بيان أركان الجرائم فيها ، وبيان العقاب المفروض عليها .

## المبحث الأول

### ماهية الجريمة باستخدام شبكة المعلومات الدولية .

نستطيع تعريف شبكة المعلومات الدولية أو الشبكة العنكبوتية (الانترنت) بأنها مجموعة حاسبات آلية متصلة مع بعضها من خلال وصلات تشعبية تسمح للمستخدمين أن يتصفحوا العديد من صفحات النشاط وكذلك التنقل من موقع إلى آخر وكذلك استخدام البريد الإلكتروني وتبادل الملفات وإجراء المحادثات والألعاب والتجارة والإلكترونية وغيرها . وهي اكبر شبكة اتصالات ، وهي ليست شبكة اتصالات تجارية ، كما أنها ليست شبكة اتصالات واحدة بالمعنى

(١) للمزيد ينظر: الحمادي يونس عرب - الخصوصية وامن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي-

ورقة عمل مقدمة إلى منتدى العمل الالكتروني ، اتحاد المصارف العربية . عمان- الأردن ، أيار ٢٠٠١ . ص ٢ وما بعدها .

الحرفي بل هي عدة شبكات اتصالية فردية وجماعية ومجموعة كمبيوترات متناثرة وموزعة في شتى أنحاء العالم مرتبطة معا في كتلة لم يتبلور لها شكل معين حتى الآن ، والشبكة مملوكة لكل الأفراد والمؤسسات لكنها ليست مملوكة لأحد . فهي مجموعة كبيرة من الشبكات تبرم بينها إتفاقيات الكترونية تنظم عمل ملايين - إن لم أقل مئات الملايين - من الحواسيب ، للإرتباط سوية بعملها التقني .

وسوف نعمد إلى تقسيم مبحثنا هذا إلى مطلبين نتناول في أولهما تعريف الجريمة باستخدام الشبكة الدولية ، من خلال بيان تعريف هذه الجريمة ، ثم نبين في القسم الثاني تعريف المجرم المستخدم لشبكة الإنترنت ، ثم نبين في المطلب الثاني من مبحثنا هذا ، خصائص الجريمة المرتكبة باستخدام الشبكة من خلال توضيح خصائص هذه الجرائم التي تميزها عن غيرها من الجرائم الأخرى ، ثم نوضح خصائص المجرم في هذه الجرائم ، من خلال توضيح ما يمتاز به المجرم من خصائص تميزه عن غيره من المجرمين في الجرائم الأخرى .

### المطلب الأول

#### تعريف الجريمة والمجرم باستخدام شبكة المعلومات الدولية .

إن شبكة المعلومات الدولية (World Wide Web) أو نظام الويب الذي ابتكره العالم الإنجليزي بيرنرس عام ١٩٨٩م ، يرتكز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت ، ومن هنا أطلقت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجاناً عبر الشبكة العنكبوتية في عام ١٩٩١م ، واعتمد في المرحلة الأولى عام ١٩٩٣م ، من خلال برامج التصفح<sup>(١)</sup> . وهي وسيلة اتصال عالمي تتيح ربط نظم الحاسوب - سواء مفردة أو نظماً مرتبطة ضمن شبكات اصغر محلية أو إقليمية أو دولية - ببعضها البعض ، أما وجه الإبداع فيها فهو أن أي مستخدم لحاسوب مرتبط بها ( أي مرتبط بالشبكة ) يمكنه الوصول إلى المعلومات ( أيما كان شكلها ) المخزنة ضمن الحواسيب ونظم التقنية الأخرى والتشارك مع الآخرين في العمل في نفس الوقت ، وإن آلية الوصول غير محددة بمسار اتصالي معين ( أي من نقطة إلى نقطة كما في الهواتف بوجه عام ) ، وإنما بصورة عشوائية بحيث وبمجرد طلب عنوان موقع

(١) د. عبد الرحمن بن عبد الله السند - وسائل الإرهاب الإلكتروني ، حكمها في الإسلام وطرق مكافحتها -

معلوماتي معين يمكن لحاسوب المشترك أن يصل إليه من أي مدخل اتصالي بصفة أن كافة المشتركين على شبكة دولية اتصالية واحدة تتكون من مجموع شبكات الاتصال العامة<sup>(١)</sup>. ولتوضيح تعريف الجريمة باستخدام شبكة المعلومات ، نقسم مطلبنا هذا اقسامين ، تعريف الجريمة ، وتعريف المجرم في جرائم شبكة المعلومات الدولية .

### أولاً : تعريف الجرائم باستخدام شبكة المعلومات الدولية :

لا يوجد تعريف رسمي للجرائم الواقعة باستخدام شبكة المعلومات الدولية . ومع ذلك ، فإن هذا النوع من الجرائم يمكن وصفها بأنها أنشطة إجرامية تقع باستخدام الشبكة ، وقد اختلفت تعريفات الفقهاء في العديد من الدول ، فمنها ما ذهب إليه خبراء متخصصون من بلجيكا بتعريفها بأنها ( كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية ) ، في حين يذهب الفقيه الفرنسي الأستاذ ( Massa ) إلى أن المقصود بها ( الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح ) ويذهب رأي ثالث إلى أنها كل ( فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحول عن طريقه ) في حين يذهب رأي رابع إلى أنها : " سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها "<sup>(٢)</sup>.

والجريمة باستخدام شبكة المعلومات الدولية في نظر فقهاء الشرطة البريطانية هي استعمال أي شبكة حاسوب لإرتكاب الجريمة من قبل المجرمين التقنيين<sup>(٣)</sup>. وتعنى عبارة خدمات المعلوماتية، استخدام الاتصالات السلكية واللاسلكية وإمكانية الوصول لشبكة المعلومات لتزويد الآخرين بالقدرة على إنتاج المعلومات أو اكتسابها أو تخزينها أو تحويلها أو معالجتها أو استردادها أو استخدامها أو إتاحتها للآخرين، ويشمل ذلك المعلومات المسموعة، والبيانات الصوتية والمرئية، ويشترط أن لا يتضمن تعريف عبارة خدمات المعلوماتية،

(٢) يونس عرب - التشريعات والقوانين المتعلقة بالإنترنت في الدول العربية - مؤتمر التكنولوجيات المصرفية العربية والدولية، عمان - الأردن ٢٠٠٢، ص ٤.

(١) ينظر: د. محمود صالح العادلي - الجرائم المعلوماتية ، ماهيتها - صورها - ورشة العمل الإقليمية حول : تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، مسقط ابريل ٢٠٠٦ ، ص ٢.

(٣) Bbc.co.uk- Source: CSI/FBI Computer Crime and Security Survey, 2000.

خدمات البث والإرسال أو خدمات الاتصالات السلكية واللاسلكية.<sup>(١)</sup> والجرائم باستخدام شبكة المعلومات الدولية ، نشاط إجرامي ينطوي على البنية التحتية لتكنولوجيا المعلومات ، بما فيها الحصول بصورة غير مشروعة (الدخول غير المصرح به) ، والتدخل غير القانوني ، عن طريق وسائل تقنية بنقل البيانات إلى جهاز الحاسب، أو من داخل نظامه ، وإدخال البيانات غير المصرح بها، ما يسبب ضررا به ، كحذف ، تخريب ، تعديل، أو تدمير بياناته ، أو تسبب إساءة في استخدامه ، أو سرقة هويته بالاحتيال الإلكتروني.<sup>(٢)</sup>

وشبكة المعلومات أو بالمفهوم المتناقل حاليا ( سايبيرسبيس Cyberspace ) لدى غالبية خبراء التقنية بيئة غير آمنة إذا تخلفت وسائل الحماية التقنية وغابت أدوات الحماية القانونية ، إذ تشير إحصائيات مجموعة غارتنر للأبحاث إلى حقيقة مفادها أن نسبة تتراوح ما بين ٥٠ إلى ٧٥ بالمائة من خدمات الشبكة " مكشوفة " وان الوضع الأمني على الشبكة غير مستتب البتة طبقا لجون بسكاتور ، مدير قسم أبحاث امن الشبكة ، في غارتنر . أضف إلى ذلك ، أن عدد البرمجيات المجانية المتاحة على الشبكة والتي يمكن استخدامها في عمليات الاختراق قد نما بشكل كبير . وهذه البرمجيات تجعل من الممكن لأي شخص أن يقوم بإجراء مسح تلقائي لمواقع الشبكة والبحث عن نقاط الضعف فيها ، ويشبه ذلك التجول في حي ما وفحص كل بيت فيه بحثا عن نافذة غير موصدة أو باب غير مغلق . ويقول بسكاتور (إن المواقع التي يتم الهجوم عليها واستغلالها ليست بالضرورة المواقع الكبرى ولا يقتصر الأمر عليها ) ، ويضيف في هذا الصدد بقوله ، ( بالطبع الشركات الكبرى يتم مهاجمتها أكثر من غيرها ، فموقع مايكروسوفت يهاجم في كل دقيقة من اليوم ولكن باستخدام برامجيات التلصص المؤتمتة فان بإمكان العابثين أن يقوموا بمسح كافة مواقع الشبكة بشكل تلقائي بحثا عن الثغرات . في حين إن المؤسسات صاحبة هذه المواقع يمكنها الانتباه إلى حدوث الاختراق وسد الثغرات بشكل مباشر ، فان البرمجيات المتوفرة الآن تزيد بشكل كبير من احتمالية اكتشاف العابثين لهذه الثغرات ) .<sup>(٣)</sup>

وقد مثلت شبكة المعلومات بالنسبة للعديد من المجرمين ، المكان الذي يمكن فيه تدمير سمعة الشخص أو العمل ، فمجرد خبر عبر موقع ويب ( web site ) أو من خلال المجموعات الإخبارية ( News Group ) يمكن أن يحدث ضررا

(٢) قانون المفوضية العراقية للاتصالات والإعلام رقم ٦٥ لسنة ٢٠٠٤-٣-٢٠٠٤ .

(٢) Computer crime Wikipedia - October 2008 .

(٣) ينظر: يونس عرب - التشريعات والقوانين المتعلقة بالإنترنت في الدول العربية - مصدر سابق - ص ٦ .

كبيراً ، وذلك بسبب الانتشار الواسع للخبر بفعل مميزات الشبكة وسرعة انتقال المعلومات عبرها . إن القانون لا يمكنه أن يقف صامتاً أمام الضرر الذي تحدثه أنشطة الافتراء وإساءة السمعة Defamation عبر موقع (الويب سايت ) والبريد الإلكتروني ومجموعات الأخبار ، ويتعين أن تنشأ مسؤوليات قانونية عن هذه الأفعال تعرض مرتكبيها للمقاضاة كي لا يبقى الاعتقاد السائد لدى ممارسي هذه الأنشطة انه لا مسؤولية على أفعالهم المرتكبة عبر الخط Online . والجريمة على شبكة المعلومات نشاطات إجرامية توصف بأنها الأسرع من الجرائم الأخرى ، وهي في تزايد. تمثل بشكل واسع نشاط غير شرعي يتضمن ذلك الغش المالي ، قطع الخدمة ، تحمّل الصور الإباحية، هجمات الفيروس، مراقبة البريد الإلكتروني وإنشاء مواقع تُروّج للكراهية العرقية.<sup>(١)</sup>

إن القياس في النصوص الجنائية الموضوعية محظور وغير جائز ، ويكاد ينحصر في الحقل الجنائي بنصوص الإجراءات الجنائية كلما كانت أصلح للمتهم ، ومؤدى ذلك امتناع قياس أنماط جرائم الحاسب على الجرائم التقليدية التي تستهدف الأموال والاعتبار المالي . ومن جهة أخرى لا يصلح القياس على نصوص خاصة بنوع من الجرائم كقياس سرقة المعلومات أو سرقة وقت الحاسب على الاستيلاء على القوى المحرزة كالكهرباء لتخلف علة القياس ، ولأن هكذا نصوص شرعت خصيصاً لتطال الأنماط التي تنظمها وهي نصوص خاصة لا يتوسع في القياس عليها بل لا نبالغ إن قلنا أن جزءاً من النصوص الخاصة يعد استثناء على الأصل والاستثناء لا يتوسع فيه .<sup>(٢)</sup>

ومن كل هذا يمكننا تعريف الجريمة باستخدام شبكة المعلومات الدولية بأنها القيام بعمل جرمه القانون أو الامتناع عن عمل أمره به القانون ، يضر بشبكة المعلومات الدولية أو يسيء إستخدامها .

### ثانياً: تعريف المجرم المستخدم لشبكة المعلومات الدولية :

المجرم في الجرائم المرتكبة بإستخدام شبكة المعلومات الدولية ، والمسمى (هاكرز) هو شخص يمتلك من الموهبة بحيث تمكنه من ارتكاب جريمته على الشبكة ، ويمتلك مع موهبته جهاز حاسب ، قد لا يكون ملكه

(١) Bbc.co.uk \_ Source: CSI/FBI Computer Crime and Security Survey, 2000.

(٢) ينظر : يونس عرب - مصدر سابق - ص ٤ .



الشخصي ، بل قد يكون مؤجراً له بالساعات كما يحدث بمقاهي الحاسوب ، ويكون هذا الحاسوب مرتبطاً بالشبكة الدولية للمعلومات ، فكثيراً ما نسمع من وسائل الإعلام بمخترقي النظم ، إلى درجة اختلطت بها المفاهيم فأصبح البعض يقتصر إدراكه بشأن جرائم الحاسب على أنشطة (الهكرز) ، أي مخترقي مواقع المعلومات ونظمها عبر شبكة المعلومات . بالرغم من أنها ترجع إلى السبعينات ، وقد اتخذت عدة أشكال وتطورت أنماطها خلال الثمانينات والتسعينات . ولم يعد الخطر مقتصرًا على محاولة اختراق الشبكات والمواقع من العابثين ( مخترقي الأنظمة HACKERS ) فمخاطر هؤلاء محدودة وتقتصر غالباً على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعارة نسخة أخرى مخزنة ، أما الخطر الحقيقي فيمكن في عمليات التجسس التي تقوم بها الأجهزة الإستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدولة أخرى تكون عادة معادية ، أو استغلالها بما يضر المصلحة الوطنية للدولة . فالمجرم في جرائم الشبكة كما يمكن إن يكون فرداً ، كما يصح إن يكون مجموعة أفراد ، وقد يكون منظمة أو مؤسسة رسمية الغرض من وجودها ارتكاب الجرائم بإستخدام شبكة المعلومات .

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكي NSA والتي قامت ببراءته في نظام التشغيل الشهير ويندوز، كما كشف أخيراً النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات للتجسس في كندا وبريطانيا وأستراليا ونيوزلندا. برصد المكالمات الهاتفية والرسائل بكافة أنواعها ويطلق عليها اسم "ECHELON" . فمع توسع التجارة الإلكترونية عبر شبكة المعلومات 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 ١٩٩٤ إلى ٤٥% عام ١٩٩٩ ، كما أظهر استفتاء أجري عام ١٩٩٦ لمسئولي الأمن الصناعي في الشركات الأمريكية عن حصول الكثير من الدول وبشكل غير مشروع على معلومات سرية لأنشطة تجارية صناعية في الولايات المتحدة الأمريكية<sup>(١)</sup> .

والمجرم في جرائم الشبكة يستطيع في استخدامه لها التوصل إلى جريمته ، سواء كانت الشبكة هي الهدف من ارتكاب الجريمة ، عن طريق جرائم الإختراق

(١) INTERPOL - Convention on Cybercrime -Budapest, 23.XI.2001 .

والتدمير البرامج والمواقع وغير ذلك ، أو تكون الشبكة وسيلة في ارتكاب جريمته كوسيلة دعائية لبث الفضائح أو وسيلة لإقناع المقابل بالإحتيال وغيرها من الجرائم التي تصل إلى درجة القتل .

ففي ١٩٩٩/٢/٢٨ في شمال كارولينا ، قتلت " لوباتكا شارون " ٣٥ عاما ، من قبل رجل تعرفت عليه عن طريق الشبكة ، بعد إن تعرضت للإغتصاب والتعذيب ، وكانت قد أخبرت زوجها أنها ذاهبة لزيارة أصدقاءها في جورجيا . فعثر على جثتها ملقاة خلف المنزل الذي إتفقت على لقاء الشخص فيه .<sup>(١)</sup>

والمجرمون في الشبكة كثيرون بسعة الشبكة واستخداماتها ، وقد تتحد الفكرة لديهم بالإرتكاب رغم كونهم من عدة دول ، فيرتكبون جرائمهم بشكل متواصل رغم كل الجهود التي تبذلها بعض الدول للحد أو السيطرة على هؤلاء المجرمين فإنهم يبذلون لإرتكاب جرائمهم كل الجهد الذي لا يعني بالضرورة الكسب أو الربح من وراءه ، ولكن قد يكون التحدي وإثبات الذات في قوة التقنية والتحكم بها ، هو الدافع لإرتكابها ، فعالبا ما تتفاخر الكثير من الشركات العالمية بقوة برامجها الواقية من الإختراق ، فينبيري أصحاب التقنية لإختراق هذه الأنظمة الواقية ، وقد لا يعلم الكثير منهم أنهم يرتكبون سلوكا إجراميا .

فقد تعرض الموقع (AOL) للإغلاق بعد تعرضه للقرصنة التقنية ، واعتقل مكتب التحقيقات الفيدرالي الأمريكي في أثرها أكثر من ٨٩ شخصا في أكثر من ٢٠ دولة تم توجيه الاتهام لهم ، وفي حملة لمكافحة انتشار الصور الإباحية للأطفال عبر الشبكة . خلال عملية " Candy man " ، كانت عمليات البحث تجري على ما يزيد عن ٢٦٦ شخصا ، وتم القبض على ٢٧ شخصا منهم . اعترفوا بقيامهم بالاعتداء على أكثر من ٣٦ طفل . تمكن مكتب التحقيقات الاتحادي من إغلاق مواقع لترويج الدعارة ، مع توجيه اتهامات جنائية ضد ٨٦ شخصا في ٢٦ ولاية . كان بينهم ، ٢ من القساوسة الكاثوليك ، و ٦ أعضاء من رجال الدين الآخرين ، ومدرسة ، وسائق حافلة ، وضابط شرطة.<sup>(٢)</sup> وهذه الفئات ليست حصرية فالعديد من الأنشطة التي يمكن وصفها بأنها تندرج تحت أحكام جرائم الشبكة ، أو التي يتم النشاط الإجرامي فيها بإستخدام الشبكة ، أو هي جزء أساسي من الجريمة ، وتشمل أيضا الجرائم التقليدية ، مثل الغش والسرقة والابتزاز ، والتزوير والاختلاس ، في أجهزة الحاسب أو الشبكات التي تستخدم لتسهيل النشاط غير المشروع . بحيث أصبح المجرمون بإستخدام الشبكة قضية رئيسية في

(١) Kari Sable Burns - Computer & Internet Crimes - Olympia 2007.

(٢) Kari Sable Burns - Computer & Internet Crimes - Olympia 2007.

هذه الأيام في أنحاء عديدة من العالم ، يرتكبها عدد كبير من الناس بالدخول إلى أنظمة المعلوماتية.<sup>(١)</sup>

ومع ذلك ، هناك العديد من الجرائم التي تتناول على وجه التحديد أنواع معينة من السلوك الإجرامي باستخدام الشبكة. وكمثال على ذلك ، تعد جريمة بموجب القانون الجنائي في كندا الحصول على خدمة الشبكة أو امتلاك جهاز مصمم أساسا للحصول على هذه الخدمة بطرق احتيالية. وفي عام ٢٠٠٢ ، أدخلت تعديلات على أجزاء من قانون العقوبات التي تتناول استغلال الأطفال في المواد الإباحية.<sup>(٢)</sup>

وبالرغم من أن الشبكة هي مسرح الجريمة أو بيئتها للمجرم في هذه الجرائم ، أو هي هدفه الذي يسعى لإثبات ذاته فيه ، إلا إنها ومن جانب آخر قد تكون الوسيلة التي تتوصل الجهات المعنية بالمتابعة والعقاب من إلقاء القبض عليه ، عن طريقها ، أو تتوصل إلى تحديد مكانه بواسطتها .

فقد أثبتت المؤشرات أن شبكة المعلومات الدولية حققت كثيرا من المنجزات في ضبط المجرمين ومعرفة مكانهم والتبليغ عنهم ، فلم يعد الأمر كالماضي بنشر صور المجرمين في الصحف أو التلفاز ، بل أخذت الكثير من الدول وفي مقدمتها ألمانيا وبريطانيا وتأتي فرنسا بالمرتبة الثالثة في استخدام الشبكة في السعي نحو ضبط المجرمين ، والتعرف على الحالات المشابهة في كل أنحاء أوروبا والاتصال فورا بالشرطة الدولية (الإنتربول ) التي تقوم بنشر صور المجرمين عبر الشبكة وإظهار جميع صفات المجرم بمجرد الضغط على الصورة . وأنتجت الإحصاءات في فرنسا التي تأتي بالمرتبة الثالثة بإجراء أكثر من ١١,٨٠٠ إتصال خلال خمسة عشر يوما فقط بدخول الشبكة والتعرف على المشتبه فيهم إجراميا.<sup>(٣)</sup>

ومما تقدم يمكننا تعريف المجرم المستخدم للشبكة بأنه كل من يرتكب جريمة تمس بشبكة المعلومات الدولية وتضر بها.

## المطلب الثاني

(١) Computer crime Wikipedia - October 2008 .

(٢) Tushar K. Pain - What is a computer or Internet crime - Criminal Defiance Articles University Avenue ~ Suite 2000.

(٣) ينظر : د. قدرى عبد الفتاح الشهاوي - الإستدلال الجنائي والتقنيات الحديثة - دار النهضة العربية ، القاهرة

### خصائص الجريمة والجرم باستخدام شبكة المعلومات الدولية .

تمتاز الجرائم المرتكبة باستخدام شبكة المعلومات الدولية بتعددتها وكثرة أنواعها فمنها الجرائم الإباحية كجرائم نشر الأفلام والصور الخليعة<sup>(١)</sup>، ومنها جرائم الاتجار بالسلع الوهمية وجرائم القرصنة وإرسال البرامج التخريبية على الأرصدّة المصرفية وجرائم سحب الأموال من البطاقات الإلكترونية وجرائم السب والقذف وجرائم التجسس وجرائم التحريض ضد امن الدولة وجرائم نشر الأفكار الإرهابية والهدامة داخل المجتمع .

وقد صرح وزيرُ الخارجية الألماني فيشر ، بأن الكلفةَ التي تسببها هذه الجرائم تتراوح بأكثر من ٤٠ \$ بليون دولار في السنة الواحدة "بدون شك، هذه فقط البداية " وتمثلت في التجسس على البيانات ، سرقة البيانات ، الإحتيال ببطاقات الإئتمان، صور إباحية، تطرّف وإرهاب.<sup>(٢)</sup> وللجريمة باستخدام الشبكة الدولية للمعلومات خصائص أو مميزات تميزها عن غيرها من الجرائم ، ولتوضيح هذه الخصائص ، نقسم مطلبنا هذا إلى قسمين نركز فيهما على أبرز ما تمتاز به هذه الجرائم في الأول منهما ، وتوضيح أبرز خصائص المجرم المستخدم للشبكة في الثاني منهما .

#### أولاً : خصائص الجريمة باستخدام الشبكة الدولية للمعلومات :

تمتاز الجرائم المرتكبة باستخدام شبكة المعلومات الدولية بالكثير من المميزات والخصائص ، السيئة بكل أحوالها ، والتي يحول المجرمون فيها نعمة التقنية والتطور العلمي إلى نقمة للعدوان على مصالح الآخرين ، أو إنتهاك حقوقهم ، وهذه الخصائص تتزايد بتزايد التطور الحاصل بهذه الشبكة ، فلكل فعل رد فعل ، ولكل جانب جيد ومضيء ، آخر سيء ومظلم ، وندناول توضيح أبرز هذه الخصائص ، وليس كل خصائصها ، بالنقاط التالية :-

١- إنها جرائم عالمية الإرتكاب ، فهي ليست مقتصرة على بلد معين أو فئة أو إقليم ، بل إنها جرائم أصبحت ترتكب بأغلب أنحاء العالم ، إن لم نقل كله ، وحتى الدول الأفريقية الفقيرة أصبحت ملبئة بالمحتالين عن طريق شبكة

(1) Tushar K. Pain - What is a computer or Internet crime - Criminal Defiance Articles , University Avenue ~ Suite 2000.

(2) Bbc.co.uk \_ Source: CSI/FBI Computer Crime and Security Survey, 2000.

المعلومات . فكما إن الشبكة تغطي العالم بأسره ، فالجريمة فيها تكاد ترتكب في كل مكان وجدت فيه هذه الشبكة ، دون إن يشعر مرتكبوها بذلك .  
٢- إنها الجرائم الوحيدة - برأينا - التي يمكن ارتكابها من قبل أكثر من شخص في وقت واحد دون أن تؤثر بمحل الجريمة ، فسرقه برنامج معين من موقع عالمي من قبل شخص في العراق ، يمكن إن يتزامن مع عمل شخص آخر في روسيا ، وآخر في تنزانيا ، دون أن يتأثر محل الجريمة - أي البرنامج - بالنقصان ، ولا تختلف جودته ، ولو تزامن الآف السراق بنفس اللحظة .

فهي جرائم تقع على مال غير قابل للنفاد ، ولا يفقد قيمته التقنية بالاستعمال - وان كان يفقد قيمته التجارية- ويمكن استعماله لأكثر من شخص في نفس الوقت ، ونفقات نقله من شخص لآخر ضئيلة . كما يرى قسم من الفقه الفرنسي<sup>(١)</sup> إنها سرقة استعمال إذا لم يتم استعمال البرامج لأغراض المتاجرة والربح .

٣- تحتاج بعض هذه الجرائم إلى قمة الذكاء في ارتكابها ، ومنها تخريب مواقع معينة ، أو نشر البرامج التي تقوم بالتجسس ، أو تصنيع الفيروسات ونشرها ، أو تدمير البرامج الأخرى . الخ . فسعة المجال الذي تقسحه الشبكة ، يفرز كثرة من الإنتهاكات من جانب المجرمين .

٤- إنها جرائم سهلة الإرتكاب ، لكل من يجيد استخدام التقنية ، يستطيع إن يرتكب كثيرا" منها ، فتحميل الصور الإباحية ، أو نشر الأفكار الإرهابية ، أو تنزيل البرامج المسروقة من الشبكة إلى الحاسب الشخصي ، جرائم أصبحت شائعة الإنتشار ، لأغلب المستخدمين . فهذه الجرائم يمكن ارتكابها من أقصى بقاع الأرض بنفس سهولة ارتكابها من أقرب مكان . وهي لا تحتاج عادة إلى بذل الجهد الكبير ، فيما عدا بعض صورها التي تتمثل بإنشاء البرامج التخريبية وغيرها ، فمجرد ضغطة زر لنشر جرثومة معينة ، أو برنامج تدميري في موقع أو منتدى ، يخلف وبجهد يسير أثارا كارثية على أصحابها والمشاركين فيها ، قد تتسبب أحيانا بإغلاقها .

٥- تتميز الجرائم باستخدام الشبكة بسرعة انتشارها ، فمجرد إشاعة خبر كاذب في أي دولة يمكن إن ينتشر خلال لحظات ، لكل أنحاء العالم . وتحميل فلم إباحي ، أو برامج مسروقة ، أو أفكار إرهابية ، خلال لحظات ، يمكن لكل فرد في العالم مرتبط بالشبكة الإطلاع عليه ، وحتى الإحتفاظ به .

(١) A. Bretrant. La ceiminaltie , informatique : (2) les delits relatives au material , 1984,no62 . P149.

٦- إنها جرائم الرقم المظلم ، فهي لا تترك أثرا" يمكن للجميع إكتشافه . كذلك صعوبة الاحتفاظ بالدليل إن وجد ، فالرقم المعروف عالميا لمرتكبها ما زال مجهولا" ، إذ إن أغلب هذه الجرائم غير مبلغ عنها ، والمكتشف منها قليل جدا" ، قياسا مع كثرة إنتشارها ، وأغلب الشركات العالمية لا تعلن أنه تعرضت للإختراق أو السرقة أو التدمير خوفا من إهتزاز ثقة عملائها بها .

٧- الخسائر الكبيرة التي تخلفها ، فالشركات التي تصنع البرامج ، والمواقع التي تباع الكتب والأفلام ، أو أي شيء آخر ، تحرم من المقابل المادي لمصنوعاتها أو سلعها ، فبسبب لها جرائم الشبكة خسائر فادحة تقدر بمئات المليارات.

ومما لا شك فيه إن الجناة في الجرائم التي تتم باستخدام الشبكة الدولية للمعلومات تكون أفعالهم منصبة على جانب البرامج وما تتضمنه من معلومات ، والتي تسمى (النظم التشغيلية والبرامج التطبيقية) والتي تم تخزينها أو التي يقوم بتفعلها ، أو معالجتها ،. لذلك ينصب اهتمام الجناة على الاستيلاء عليها أو تدميرها أو إتلافها.<sup>(١)</sup> إذ تنتج هذه الجرائم من حيث أثرها الاقتصادي خسائر جدية تقدر بمبالغ طائلة تفوق بنسب كبيرة الخسائر الناجمة عن جرائم المال التقليدية مجتمعة. ولو أخذنا على سبيل المثال بريطانيا ، التي تعد الدولة الثانية في حجم الخسائر التي تلحقها جراء جرائم الشبكة بعد الولايات المتحدة، فإنه ، وعلى لسان وزير التكنولوجيا البريطاني "Lord Reay" أعلن في عام ١٩٩٢ أن (الجرائم التي تتعرض لها أجهزة وأنظمة الحاسوب كالتطفل التشغيلي hacking والفيروسات Viruses تضر بأعمال أكثر من نصف الشركات الصناعية والتجارية في بريطانيا بتكلفة سنوية تقدر بحوالي (١.١) بليون جنيه إسترليني)..وفي الولايات المتحدة فقد بلغ معدل الخسارة بالنسبة للحالة الواحدة (٨٣٣.٢٧٩) دولار أما أقصى خسارة فقد بلغت (٣٧) مليون دولار، وفي ٦% من الحالات المذكورة كان مرد الخسارة هو الاحتيال (غش الحاسوب) للاستيلاء على المعلومات (الإثبات الجنائي فيها ، فهي جرائم غالبا ما تكون غامضة ، لصعوبة إكتشاف مرتكبيها ، والتحقق فيها يختلف عن التحقيق في الجرائم التقليدية ، فيصعب على المحقق التقليدي التعامل مع هذه الجرائم كما يصعب عليه متابعة الجرائم عن طريق الشبكة والكشف عنها وإقامة الدليل عليها ،

(١) ينظر: د. محمد حماد مرهج الهيتي - التكنولوجيا الحديثة والقانون الجنائي - ط ١ ، دار الثقافة للنشر ، عمان - الأردن ، ٢٠٠٤ ، ص ١٥٩ .

(٢) ينظر : يونس عرب - الخصوصية وامن المعلومات - مصدر سابق - ص ٧ .

فالوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى . كما إن من المشكلات القانونية الإجرائية في جرائم الشبكة هي صعوبة إثبات وقوع الجريمة إذ يتم الفعل الإجرامي غالباً بدون علم المجنى عليه كدخول البرامج التخريبية ، وكذلك صعوبة التوصل إلى الجاني لأنه غالباً ما تستخدم تحت اسم مستعار وعن طريق المقاهي فبذلك يصعب التوصل إلى مكانه . ومن المشاكل التي تثار في الإجراءات الجنائية هي صعوبة إلحاق العقوبة بالجاني المقيم خارج القطر وكذلك دخولنا في مشكلة تنازع القوانين الجنائية من حيث المكان وبالتالي نعود إلى مبادئ التحكيم في تطبيق القانون الجنائي من حيث مبدأ إقليمية القانون الجنائي أو عينيته أو شخصيته أو عالميته .

ومن الصعوبات أيضاً مشكلة تحديد المسؤول جنائياً عن الفعل الإجرامي كمن يدخل إلى موقع إباحي أو إرهابي فهل نسأل عن الجريمة عامل الاتصال أم مورد المنافذ أم مورد المعلومات أم منشئ الموقع . وكذلك صعوبة السيطرة على أدلة الإثبات للجريمة لأنها مما يمكن إتلافها بسرعة . وكمثال على ذلك فقد طالبت المحكمة العليا في ولاية فرجينيا بقانون " لمكافحة البريد المزعج " يهدف إلى منع إرسال أعداد كبيرة من البريد الإلكتروني غير المرغوب فيه . وتجريمها كجناية ، وتكون الجريمة جنائية إذا وصل عدد المتلقين لأكثر من ١٠,٠٠٠ شخص أو حاسب ، وكانت ترسل في غضون ٢٤ ساعة<sup>(١)</sup> .

٩- تعدد أنواع الجرائم المرتكبة عن طريق الشبكة ، فمنها ما يتصل بذات الأجهزة والأدوات كشبكات الربط و الآت الطباعة والشرائط التي تسجل عليها البرامج والبيانات وهذه تتعرض للأفعال التي تنسجم مع طبيعتها كالسرقة والإتلاف ، أو قد يكون الإعتداء كما يرى البعض<sup>(٢)</sup> منصبا على الكيان المعنوي كسرقة البرامج أو المعلومات أو نسخها وتقليدها أو إدعاء ملكيتها أو إتلافها أو تعطيلها أو العبث بالبيانات المخترنة في ذاكرة الحاسب .

#### ثانياً : خصائص المجرم المستخدم لشبكة الدولية للمعلومات :

أظهر نمو الاتصالات عبر الشبكة معتمدين عليها من ذوي المهارة التقنية ، أو من صغار المجرمين ، أو من جماعات الجريمة المنظمة . ففي أيلول ١٩٩٩ مثلاً ، حُكم على عضوين من جماعة تعمل انطلافاً من الولايات المتحدة ، عرفت باسم "أساتذة الهاتف" ، بالسجن لاختراقهم شبكات أنظمة الحاسب لشركات الاتصالات اللاسلكية MCI و SPRINT و AT&T و EQUIFAX . وقد تمكن أحد

(١) Washington Post. SEPTEMBER 12TH, 2008.

(٢) د. محمد حماد مرهج الهيتي - مصدر سابق - ص ١٥٨ - ص ١٥٩ .

هؤلاء، كالفين كانتريل، من الحصول على الآلاف من بطاقات إجراء الإتصالات الهاتفية من شركة SPRING وبيعها إلى شخص كندي أعاد تمريرها إلى الولايات المتحدة بواسطة بيعها إلى شخص آخر في سويسرا. وفي النهاية وصلت تلك البطاقات إلى أيدي مجموعات الجريمة المنظمة في إيطاليا. التي بدورها تستخدم، الشبكة لإتصالات (تكون مرمزة عادة) لأغراض أخرى عندما ترى أنها مفيدة ومريحة. وقد أثبتت الجماعات الإجرامية أنها مرنة وقابلة للتكيف في طرق استغلالها للفرص التي يوفرها عالم الشبكات الإلكترونية، كما تستغل أي فرصة أخرى لنشاطاتها غير القانونية، التي تكون بدورها متعددة المستويات، ومتعددة الأطراف، وبطبيعتها عابرة لحدود الأوطان.<sup>(١)</sup>

وللمجرم في جرائم الشبكة مميزات تفرده بطابع خاص عن غيره من مرتكبي الجرائم الأخرى، فكما يمتاز مرتكبو القتل عادة بقسوة القلب وجسامة الجريمة، ومرتكبو السرقة بالخفة والسرعة بالتنفيذ، فإن هؤلاء المجرمين في جرائم الشبكة لهم أوصاف خاصة بهم، تفرزها لهم طبيعة الجريمة المرتكبة، أو الحيز الذي ترتكب فيه، أو شخصيتهم الإجرامية نفسها، ونلخص أبرز هذه الخصائص بالنقاط التالية :-

١- إنه مجرم يستخدم الوسائل التقنية ولديه القدرة على إستباق الزمن والتطورات التشريعية البطيئة، والكثير منهم خريجين لجامعات ومؤسسات علمية هامة. فالمجرم في هذه الجرائم يستخدم الوسائل الفنية اللازمة لإتمام جريمته كأن يكون مرسل لها أو مستقبل. ويدخل في عداد المجرمين موصلي المعلومات أو متعهدي التوصيل، وكذلك منشئي المواقع الإلكترونية التي تعتبر إجرامية كالمواقع الخليعة والمواقع الإرهابية ومواقع نشر الجرائم ومواقع الجريمة المنظمة وغيرها.

٢- لا يحد هذا المجرم عمر معين، فهذه الجرائم كما يمكن للبالغين إرتكابها من ذوي الفئات العمرية المختلفة، يمكن أيضا للصغار الأحداث ارتكابها، فالهوس والولع بهذه الشبكة الساحرة، لا يحتاج إلى عمر معين، ولا تحده ثقافة معينة.

٣- سعة العمل الذي يقوم به - فكما أسلفنا - أن الجريمة باستخدام الشبكة لها صور عديدة، فإن هذه الصور تفرز مجالاً واسعاً " لتحرك المجرم وتنقله

(١) ينظر: فيل وليامز- الجريمة المنظمة وجرائم الشبكات الإلكترونية- الترابطات، والاتجاهات، والاستجابات - مركز

خبرات أمن الإنترنت في جامعة ميلون كارنيجي، ٢٠٠٢.



بينها ، فعندما تواجهه صعوبة بنشر الجرائم أو إختراق المواقع ، يستطيع إرتكاب صور أخرى من نسخ البرامج المسروقة ، أو نشر الصور الإباحية ، أو نشر الأفكار الهدامة في المجتمع ، ثقافية كانت أو دينية أو غيرها .  
ومثالها أدانت هيئة المحلفين الإتحادية في فينيكس - أريزونا ، جيفري كلبرد من كاليفورنيا ، وستشفر جيمس من أريزونا ، بثماني تهم ، بينها التآمر والاحتيال وغسيل الأموال ونقل المواد الفاحشة... وقد وجهت إليهم عقوبات تصل مدتها إلى خمس سنوات في السجن عن كل جريمة ، وتصل إلى ٢٠ سنة لجريمة غسيل الأموال ، ودفع غرامة تصل إلى ٥٠٠ ألف دولار.<sup>(١)</sup> ومثالها المضايقة لشخص ما عن طريق استخدام الشبكة ، فهناك أنماط من السلوك تنطوي على تهديدات تنتشر الخوف والرعب لدى المتلقي، وكثير منهم في السجن اليوم أدينوا لإرسالهم تهديدات عبر البريد الإلكتروني أو المحادثة عن طريق الشبكة.<sup>(٢)</sup>

٤- لا يهدف المجرم في جرائم الشبكة إلى الربح غالبا ، فقد يكون هدفه من الحصول على البرامج للاستعمال الشخصي فقط ، أو توزيعها ونشرها مجانا للآخرين ، وقد يكون الهدف من جريمته التحدي فقط وإثبات الذات بأنه يمتلك القدرة على إختراق التطور في التقنية ، مهما بذلت الشركات من جهد في تطويره.

٥- انه مجرم قابل للتكيف مع تطور التقنية ، يستغل الفرصة بوجود الثغرات في المواقع الخاصة بالشركات أو الأفراد ، وغالبا ما يأخذ الأمر بصورة التحدي الكبير لأجهزة ووسائل الحماية ضد جرائمه وكذلك لفرق المكافحة التي تحاول السيطرة على نشر الفيروسات ، فيكون هو في تجدد مستمر ، بحيث تمكنه مرونته من التفاعل مع هذا التطور بإستمرار .

٦- يتميز بالقدرة على التخفي والعمل السري ، فيعمد إلى عدم تمكين المجني عليه من ملاحظته أو اكتشافه وإبقاء جريمته في إطار البريد أو الموقع الإلكتروني المجهول الهوية والعنوان، والذي يصعب العثور عليه بين الملايين من المواقع الإلكترونية المنتشرة على الشبكة ، فإن أغلب هذه المواقع أو المنتديات تتطلب دخولا" بأسماء مستعارة ، والبريد الإلكتروني كذلك لا

(١) Internet Crime - is really a group of online related crimes18 May 2008.

(٢) Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.

يحتاج إلى اسم حقيقي أو معلومات صادقة ، فذلك يتمكن المجرمون من ارتكاب جرائمهم بقدر كاف من السرية والكتمان ، دون الإفصاح عن معلوماتهم الحقيقية .

٧- لا يتقيد هؤلاء المجرمين بمشكلة الحدود الدولية وكيفية عبورها ، أو الحصول على التأشيرة للدخول ، فيستطيع مجرم مرتكب لجريمته في مصر مثلاً ، من نشر الجرائم إلى المواقع والمنتديات والبريد الإلكتروني ، في كل أنحاء العالم دون إذن من دولة معينة ، أو التقيد بإجراءات محددة .

فالمشكلة في تطبيق القانون الخاص بالجريمة على الشبكة ، مثل الشبكة نفسها ، لم يُحدّد بالحدود الوطنية. والتحقيق الذي يبدأ في بلادٍ واحدة قد يَفُودُ بسرعة إلى مكان آخر، لكن بدون تعاون الدول الأخرى ، قد يَكُونُ مستحيلًا تَعَقُبُ الجناة وضمانُ الإتهامات. ففي المملكة المتحدة، تحت الحكومة الشرطة والوكالات الأخرى لمتابعة الجريمة على الشبكة. وأعلن وزير الداخلية، جاك سترو، قال: (إن تُقَدِّمُ التقنيات الحديثة مثل الإنترنت فيه منافع مشروعة ضخمة، لكن فيه فرص قويّة أيضاً للمجرمين، كالإحتيال مالي و النشاطات الغير قانونية للشواذ جنسياً، وأعلنُ بأنّي سأرفعُ قابلية خدمة الشرطة لتحرّي الجريمة المرتكبة باستخدام الحاسبات، لكشف، الإحتيال، والإبتزاز وغيرها.)<sup>(1)</sup> وتنشأ المشكلة الأكبر عندما توجه تهمة انتهاك القوانين الاتحادية ، من خلال استخدام الشبكة لارتكاب الجرائم العابرة للدولة ، والتي تسعى الدول لأن تكون العقوبات على ارتكابها شديدة.<sup>(2)</sup>

٨- إن ضعف الإجراءات القانونية المتخذة بحق هؤلاء المجرمين ، وقلة التشريع المعاقب لمثل هكذا جرائم ، نتيجة لتأخر الكثير من الدول في تحصين مجتمعاتها منها ، وصعوبة الإثبات الجنائي فيها ، تجعلهم غالباً ، لا يهتمون بالعقوبات المفروضة بحقهم . فالقليل من الدول من لديها فرق شرطة خاصة بمتابعة هؤلاء المجرمين ، أو لديها الخبراء المختصين بملاحقتهم .

وقد شكلت الولايات المتحدة فرقة خاصة بمتابعة هؤلاء المجرمين تسمى IC3 ، وتشير الشكاوى الجنائية التي تلقتها بشأن التوسع السريع في ساحة الجريمة عبر الشبكة . وهي بدورها تمنح ضحايا الجريمة إجراءات مريحة

(1) Bbc.co.uk \_ Source: CSI/FBI Computer Crime and Security Survey, 2000.

(2) Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.

وسهولة الاستخدام ، عبر آلية تقديم التقارير ، إلى وجود الإنتهاكات على الشبكة جنائية كانت أم مدنية.<sup>(١)</sup> ولديها وكلاء متخصصون في مجالات التقنية ، وهم في تعاون مستمر مع مكتب التحقيقات الاتحادي والمخابرات الأمريكية على حد سواء لمكافحة مثل هذه الحالات الجنائية.<sup>(٢)</sup>

## المبحث الثاني

### صور الجريمة باستخدام شبكة المعلومات الدولية

تتعدد الجرائم المرتكبة باستخدام الشبكة الدولية للمعلومات ، بحالة يمكننا القول فيها إن أغلب الجرائم الموجودة حالياً على وجه الأرض ، الخاضعة للتجريم منها ، والتي لم تتناولها التشريعات بعد بالتجريم ، يمكن إرتكابها بواسطة هذه الشبكة . وتصنيفها يعد بالأمر الصعب على غير ذوي الإختصاصين ، الجنائي والحاسوبي الإلمام به ، ولو دخلنا في مجال المساهمة الجنائية ، فلا أرى – برأيي المتواضع – أن هناك جريمة لا يمكن إرتكاب ولو مرحلة منها باستخدام الشبكة الدولية ، فمن أجسم الجنايات وهي القتل والإبادة وجرائم الحرب ، يمكن التحريض والإتفاق والمساعدة على إرتكابها ، عن طريق الشبكة ، إلى أبسط المخالفات بالامتناع عن ترميم الدور الأيالة للسقوط ، أو رمي المواد القذرة والضارة في الأنهر .. الخ . ولكننا سنتناول في مبحثنا هذا تصنيف هذه الجرائم تبعا للمساهمة الأصلية فيها ، إلى قسمين ، نتناول في الأول منهما صور الجرائم الخاصة بشبكة المعلومات الدولية ، ونتناول في ثانيهما الجرائم التي تعد الشبكة وسيلة فيها لتنفيذ السلوك الإجرامي ، بصورها الخاصة ، وليس بإعتبارها نوعا من جرائم أخرى ، فالقياس في التجريم محذور ، والتفسير في القانون الجنائي لا يمكن للقاضي التوسع به .

### المطلب الأول

(١) Internet Crime - is really a group of online related crimes 18 May 2008

(٢) United States Department of Justice -Computer Crime & Intellectual Property Section – 2009.

### صور الجرائم الخاصة بشبكة المعلومات الدولية

تتميز هذه الجرائم<sup>(1)</sup> بصفة خاصة وهي وقوعها وارتكابها عن طريق شبكة المعلومات الدولية ، فالشبكة فيها تمثل مسرح الجريمة ، إضافة إلى أن الشبكة هي نفسها وسيلة السلوك الإجرامي في التنفيذ ، إذ أنها تبدأ وتنتهي فيها ، وصورها عديدة ، وهي في تزايد مستمر ، ولكن يمكننا بصورة مبسطة حصر أغلب صورها بالنقاط التالية :-

**أولاً - جرائم الجرائم :-** أو ما تسمى " الفيروسات" وذلك بتصنيعها أو نقلها أو نشرها ، وهي أكثر جرائم الإنترنت انتشارا وتأثيرا. وأصبحت الشبكة مسرحا واسعا لإرتكاب مثل هذه الجرائم. والجاني فيها يقوم بتصنيع مادة تخريبية تؤثر تقنيا على أي حاسب تدخل إليه ولو بالصدفة ، بل وليس الحاسب فقط ، وحتى أجهزة نقل المعلومات الصغيرة منها والكبيرة ، وأقراسها الصلبة والمرنة ، وهذه الجرائم تمتاز بالقدرة على الدخول والانتشار أحيانا دون إن يشعر مستخدم الحاسب بها .

ولا يخفى على الكثير سرعة توغل ما يسمى بـ "الدودة الحمراء" إذ استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في ١٩ يوليو 2001 م. كان الهدف المباشر لها المعلومات المخزنة على الأجهزة المفتحة حيث تقوم بتغييرها أو حذفها أو سرقتها و نقلها إلى أجهزة أخرى.<sup>(٢)</sup>

وكان مجرد عمل يدوي لبعض مروجي جرائم الحاسب، قد أفرز أثره بنتائج كارثية. فقد سُئِلَت جرثومة " بقعة الحب"<sup>(٣)</sup> على الأقل ٤٥ مليون حاسبة حول العالم وتسببت بخسارة ما قيمته بلايين الدولارات في أواخر عام ٢٠٠٠ عندما استعملت هذه الجرثومة في محاولة للوصول إلى كلمات السر للحسابات في بنك أوف سويتزرلاند، وفي ما لا يقل عن مصرفين آخرين في الولايات المتحدة. ومع إن الجرثومة انتشرت في العالم اجمع وكلفت المؤسسات التجارية آلاف الملايين من الدولارات، لكنه عندما تمكن مخبرو مكتب التحقيقات الفيدرالي من تحديد هوية مرتكب العمل، تبين انه طالب في الفلبين، واكتشفوا أيضاً أنه ليس

(١) للمزيد ينظر : د. إياس ألهاجري - جرائم الإنترنت - مكتب خدمات البوابة ، يناير ٢٠٠٢ .

(2) for more see , Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.

(3) for more see , Bbc.co.uk -Source: CSI/FBI Computer Crime and Security Survey, 2000.

هناك من قانون يمكن من خلاله محاكمة المرتكب في بلاده . بعد ذلك، عمدت دولة الفلبين إلى إصدار قوانين تحرمّ الجرائم التي تُرتكب عبر الشبكات الإلكترونية، وتبعتها في هذا السياق دول أخرى.<sup>(١)</sup>

وتعرض موقع Yahoo لهجوم جرثومي في ٢٠٠٠/٢/٧ الساعة ١٠:٣٠ بتوقيت المحيط الهادي ، استمر لثلاث ساعات. وكانت خسائر الشركة في معدل واحد جيجابايت في الثانية، أي ما يؤدي إلى إضعاف نشاطها بشكل كبير لا يمكن تداركه . و في ٢٦ / ٣ / ١٩٩٩ ، انتشرت في الموقع نفسه " دودة ميليسا"<sup>(٢)</sup> التي تدخل إلى الوثائق الخاصة المخزنة بحاسب الضحية ، ثم ترسلها تلقائياً عبر البريد الإلكتروني إلى الآف الأشخاص الآخرين خلال ثواني.

ثانياً - جرائم الاختراق :- ومفادها الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. يتم أغلبها عن طريق برامج متوفرة على الشبكة يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير ، وهنا تكمن الخطورة. و تختلف الأهداف المباشرة للاختراقات ، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغييره ، 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 " الإخترافية " أو لإثبات وجود ثغرات في الجهاز المخترق . وغالبا ما يكون المخترق متخفياً بدخوله نظام الشبكة أو الحاسب بأنه شخص مصرح له ، ويتمثل سلوكه الإجرامي بسرقة المعلومات ، أو الحصول على كلمات السر الخاصة بالشركات ، أو الحصول على البرامج بدون تصريح ، وغيرها من الأغراض الإجرامية.

إن احد اشهر قضايا الاختراق تضمنت في نهاية الثمانينات مجموعة من المراهقين الألمان الذين تمكنوا من الدخول إلى أنظمة العديد من الشركات الأمريكية وجمع معلوماتها بقصد بيعها إلى المخابرات السوفيتية ( سابقا ) وقد اكتشفت هذه القضية عن طريق تعاون احد ( الهكرز) مع جهات التحقيق بحيث قدم لها كافة معلوماته بشأن كيفية حدوث الاختراقات والأنظمة المستهدفة ، وقد كانت هذه القضية من أكثر القضايا أهمية بالنسبة لجهات التحقيق فيما بعد ، لما

(٢) فيل وليامز - الجريمة المنظمة وجرائم الشبكات الإلكترونية: الترابطات، والاتجاهات، والاستجابات - مركز خبرات أمن الإنترنت في جامعة ميلون كارنيجي. ٢٠٠٢ .

(٢) Computer crime Wikipedia - October 2008.

كشفته من تفاصيل عن الآليات التقنية والوسائل التي استخدمها هؤلاء الهكرز في الحصول على المعلومات.<sup>(١)</sup>

ومن أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الشبكة ، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع . (Defacing) إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة ، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.<sup>(٢)</sup>

ثالثاً- جرائم تعطيل الأجهزة :- ومفادها قيام المجرم التقني بتعطيل أجهزة أو شبكات عن القيام بعملها دون أن يقوم بعملية اختراق حقيقية لتلك الأجهزة. وتتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها ، فيسبب بعمله هذا دمارا لها لا يمكنها من متابعة عملها إلا بإعادة تنصيب برامجها من جديد ، وهذه العملية تأخذ جهدا كبيرا ووقتا طويلا في إعادتها إلى هيئتها السابقة ، والتي هي بدورها عرضة للتعطيل من جديد، وبسهولة كبيرة بنفس عملية التعطيل السابقة .

رابعاً- جرائم تدمير المواقع :- ومفادها أن الجاني يقوم بالدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بالشبكة من خلال نظام آلي (PC-Server) أو مجموعة نظم مترابطة شبكياً (Intranet) بهدف تخريب نقطة الاتصال أو النظام، فيسبب عملها هذا تدميراً للموقع ، يكلف إعادة تشغيله كثيرا من الوقت والجهد والمال ، وقد تكون إجراءات تدميره لمرة ثانية أسهل من المرة الأولى وأسرع ، إلا إذا تجاوز أصحابه أو مالكيه نقطة الدخول بنظام حماية جديد ، أو بتغيير الأرقام السرية الخاص به.<sup>(٣)</sup>

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم ، فالمتغيرات التقنية ، وإمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source) سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو

(1) for more see , Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.

(٢) يونس عرب - الخصوصية وامن المعلومات - مصدر سابق - ص ٢٣ .

(٣) For more see: Legal Information Center – Criminal Law - Legal Information Institute , Cornell Law School. 2009.

الشبكة أو البرمجة، جعلت الحيلولة دون الاختراقات صعبة جداً، إضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانيات والقدرات ما ليس لدى الأفراد.<sup>(١)</sup>

**خامساً** - جرائم خرق الإتفاقيات :- غالبا ما يتم العمل عن طريق الشبكة بالإنتساب للمواقع أو المنتديات ، وحتى عمل البريد الإلكتروني ، عن طريق اتفاقية محددة من قبل الشركة أو الشخص صاحب الموقع ، وبمجرد الضغط على حقل الموافقة بالإنتساب ، وملئ حقول المعلومات - التي هي غالبا ما تكون مزيفة - تنشأ إتفاقية بين الموقع والمستخدم تخوله من التنقل بين صفحات الموقع وتنزيل البرامج المتاحة فيه ، من برامجيات أو أفلام أو أغاني أو غيرها ، فيقوم هذا الشخص المخول بموجب الإتفاقية الألكترونية باستخدام الموقع في غير هذا الغرض دون أن يحصل على التحويل بذلك ، وهذا الخطر يعد من الأخطار الداخلية في حقل إساءة استخدام الإتفاقية مع أصحاب الموقع ، وقد يكون أيضا من الأخطار الخارجية ، كاستخدام المخترق حساب شخص مخول له باستخدام الموقع ويمتلك مميزات أخرى قد تكون بمقابل ، كتخمينه لكلمة السر الخاصة به أو باستغلاله نقطة ضعف بالنظام البرمجي للموقع ، بالدخول إليه بطريق مشروع ومن ثم القيام بسلوكيات غير مشروعة .

ومثال على ذلك تمكن اثنين من طلبة الجامعات بأمريكا، من الدخول إلى موقع الكلية الخاص بمنتدى الطلبة، بموجب أنهم طلاب فيها، ويمتلكون حق الدخول للموقع ، بسرقة هوية الدخول (الاسم والرقم السريين) لأحد موظفي الإدارة، وقاما بإنتهاك إتفاقية الدخول، وغيرها في درجات تخرجهم النهائية بالكلية ، وهما يواجهان الآن عقوبة السجن لمدة ٢٠ عاما، وغرامة قدرها ٢٥٠,٠٠٠ دولار أمريكي.<sup>(٢)</sup>

**سادساً** - جرائم الإضعاف :- وتتم هذه الصورة من الجريمة ، بدخول شخص يملك حق الدخول ويتجاوز الحدود المصرح بها حسب الإتفاقية ، أو عن طريق الاختراق ، فيقوم بزرع مدخل له يخوله الدخول إلى الصفحات المحجوبة عنه ، أو تسهل له الإختراق مستقبلا" ، فيتضرر الموقع بضعف إداء عمله ، وهذه الصورة لا تسبب التعطيل أو التدمير ، فإضعاف المواقع يسبب ترك كثير من

(١) د. عبد الرحمن بن عبد الله السند - مصدر سابق - ص-١٣

(٢) Internet Crime - is really a group of online related crimes 18 May 2008

مشتركيها العمل معها ، لأن غالبية العاملين على الشبكة يحتاجون إلى خدمة سريعة ، وهذه توفر متعة العمل .ومن اشهر الأمثلة على جرائم الإضعاف هو (حصان طروادة) ، فهو عبارة عن برنامج يستخدم لمعالجة كلمات أو برامجات ظاهريا ، لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام ، وهو بدوره يسبب أيضا ضعفا في عمل الموقع أو الحاسب الموجود فيه.

سابعا"- الجرائم الواقعة على الإتصالات : - وهذه الصورة من الجريمة تتم بدون اختراق حاسب المجنى عليه فيتمكن الجاني من الحصول على معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق الموقع أو الحاسب وذلك ببساطة من خلال مراقبة الاتصالات في إحدى نقاط الاتصال أو حلقاتها . أو بصورة اعتراض الاتصالات، وتتم كذلك بدون اختراق الموقع أو الحاسب فيقوم الجاني في هذه الصورة باعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ، ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي .<sup>(١)</sup>

فهناك عقوبات تصل إلى "ما مجموعه ٦٠ عاما في السجن وغرامة قدرها ١.٧٥ مليون دولار" تواجه المستخدم بوتنت جون ، أدين بها عن ٤ جنایات ، لحصوله على حماية أجهزة الحاسب ، والكشف بشكل غير قانوني عن اعتراض الاتصالات الالكترونية ، والتحايل والغش المصرفي) لبعض أصدقاءه من المراهقين.<sup>(٢)</sup> ومنها الجرائم الناجمة عن القرصنة على الإتصالات ، والتعدي على حقوق المؤلف من خلال الاتصالات ، والشعارات التي تظهر على مواقع الشبكة "cyber stalking" والمضايقات التي يمكن أن تؤثر على الحياة اليومية. ومشاكل الكشف عن المعلومات السرية والخصوصية وفقدانها ، ومنها أيضا ، عندما يكون البريد الإلكتروني هو سبيل الإعتراض سواء من خلال القرصنة غير المشروعة ، أو عندما تقع عليه مجرد قراءة من قبل شخص غير مأذون له بذلك.<sup>(٣)</sup>

(1) For more see: Legal Information Center – Criminal Law - Legal Information Institute , Cornell Law School. 2009.

(2) Internet Crime - is really a group of online related crimes 18 May 2008

(3) Computer crime Wikipedia – October 2008.



ثامنا"- الجرائم الواقعة على الخدمات :- ومفاد هذه الصورة من الجرائم يتم من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة وابرز هذه الصور هو إنكار خدمة الإرسال ، عندما يقوم المتلقي بالاحتجاج بعدم وجود خدمة الشبكة ويمتنع عن دفع المستحقات المالية عن ذلك ، أو مثالها إرسال عدد كبير من رسائل البريد الالكتروني دفعة واحدة إلى موقع معين بهدف تعطيل النظام المستقبل لعدم قدرته على احتمالها ، أو توجيه عدد كبير من عناوين المواقع المجرثمة على نحو لا يتيح عملية تجزئة حزم المواد المرسله فتؤدي إلى اكتظاظ الخادم المستقبل وعدم قدرته على التعامل معها . وكصورة أخرى منه هو عدم الإقرار بالقيام بالتصرف ، ويتمثل هذا الخطر في عدم إقرار الشخص المرسل إليه أو المرسل بالتصرف الذي صدر عنه ، كأن ينكر انه ليس هو شخصيا الذي قام بإرسال طلب الشراء عبر الشبكة فيمتنع من دفع الأموال المستحقة جراء ذلك .

وهذه الجرائم تضم كافة الأفعال التي يقوم بها المورد أو المتعهد المستضيف أو متعهد الإيواء لخدمات الشبكة، ومثال ذلك ، مواقع الاستضافة وشركات توفير الخدمة وغيرها من الجهات التي يفترض أن تقوم بتوفير وتأمين الخدمة وبتنظيم وتخزين المضمون الذي يسمح للموردين المستخدمين بالوصول إلى الجمهور، وذلك من خلال توريد الخدمات إلى مواقع خارجية ، وهذه الخدمات من الممكن أن تكون خدمات إجبارية أو علمية ، كما أن هذه الأفعال يمكن أن تتطوي على تقديم مواد غير مصرح بها للجمهور أو إفشاء أسرار أو مساساً بحق الإنسان في احترام حياته الخاصة<sup>(١)</sup>.

تاسعا" - جرائم التجسس :- وتتم هذه الصورة من الجرائم بزرع برامج خاصة في حاسب الموقع أو الشخص أو الشركة ، وهي تطور لمرحلة ما بعد الإختراق ، وهذه البرامج تسمى ( Patch ) تمكن المخترق من الإطلاع على كافة محتويات الحاسب من صور شخصية وأفلام عائلية ، وحتى أرقام الحسابات الشخصية ، وأسماء العملاء المتعاملين مع الشركة ، وهي أكبر صور جرائم الشبكة خطورة وجسامة ، ولا تتحدد بالحوايب الشخصية بل تتعداها إلى حوايب الشركات الكبرى والمواقع الحكومية الرسمية ، وهي بصورتها حرب معلنة على الشبكة بين شركات المواقع وبين الجواسيس.

ومن اشهر دعاوى التجسس حادثة الاستيلاء على المعلومات المرسله إلى شركة سيمنس الألمانية من قبل إحدى الشركات الصناعية الفرنسية والمتعلقة

(١) ينظر: د. محمود صالح العادلي - مصدر سابق - ص ٦ - ص ١٠ .

بعروض تنفيذ شبكة القطارات السريعة في كوريا الجنوبية ومن الحوادث التي حصلت مؤخرا واقعة تجسس شهيرة بين شركتي طيران عالميتين ( البوينغ وإيرباص<sup>(١)</sup> ) ، فجرائم الشبكة شملت أنشطة التجسس الصناعي والأمني ، بالاستيلاء على البيانات والمعلومات ذات القيمة الاقتصادية أو التي تمثل قيما مالية كالقيود المصرفية ، وإجراء تحويلات وهمية للنقود ، وتدمير المعطيات وتشويهها أو اصطناع بيانات ووثائق الكترونية وهمية ، والاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستيلاء على المال ، والإساءة لسمعة الأفراد وتحقيرهم عن طريق نشر صورهم العائلية أو كشف أسرارهم أو معلوماتهم الخاصة على كل المستخدمين للشبكة.

عاشرا - الجرائم الواقعة على البريد الإلكتروني :- فقد يكون هذا البريد وسيلة لإرتكاب صور أخرى ، وقد تكون الجرائم بالصور الأخرى واقعة عليه ، تسبب الضرر بعمله أو فقدانه ، وبالتالي فإن الرسالة التي يمكن أن تكون أكثر سهولة في الكتابة تعد فعلا " إجراميا" أو تفسر بأنها مهينة ، كذلك إرسال رسائل تبدو في ظاهرها أنها رسائل دعوة أو عمل أو تهنئة في حين أن المضمون قد يكون هجوما غير محدد ، مفاده توجيه الشتائم والتحرش والتعليقات المهينة على أفراد معينين موجهة ضد الجنس أو العرق أو الدين أو الجنسية أو الميول الجنسية ، ويحدث هذا غالبا في غرف الدردشة ، بنشر الكراهية من خلال إرسال البريد الإلكتروني إلى الأطراف المعنية.

فضلا عن استخدام تجار المخدرات الشبكة لبيع المواد غير المشروعة من خلال تشفير البريد الإلكتروني. أو ترتيب الصفقات عن طريق مقاهي الشبكة، واستخدام المواقع على الشبكة كساعي لتتبع الطرود غير المشروعة للحبوب ، وتبادل وصفات للأمفيتامينات في تقييد الوصول إلى غرف الدردشة، وعلاوة على ذلك ، وصفات العقاقير التقليدية التي أدت إلى انتعاش تجارة المخدرات والتي أصبحت اليوم متاحة لأي شخص لديه حاسوب موصول بالشبكة.<sup>(٢)</sup>

## المطلب الثاني

### الجرائم التي تكون الشبكة وسيلة في ارتكابها

تعد شبكة المعلومات الدولية وسيلة لإرتكاب السلوك الإجرامي لكثير من الجرائم - إن لم أقل كلها - إذا دخلنا في مجال المساهمة الجنائية في التحريض

(١) الخامي يونس عرب - الخصوصية وامن المعلومات - مصدر سابق - ص ٢٢ .

(٢) Computer crime Wikipedia - October 2008.

والمساعدة والإتفاق ، فالجرائم عن طريق الشبكة ، أو التي تكون هذه الشبكة وسيلة فيها عديدة ومتنوعة بتعدد الجرائم وتنوعها ، ومجال سردها لا تحتمله وريقات هذا البحث ، ولكننا بصورة موجزة نشير إلى الكثير منها ، ونركز على الجرائم شائعة الإرتكاب ، التي تكون شبكة المعلومات الدولية وسيلة في إرتكابها. فمن الجرائم الواقعة على الأشخاص . وهي الجرائم التي تقع ضد النفس أو جرائم الاعتداء على الأشخاص أي الحقوق اللصيقة بشخص المجنى عليه ، والتي تعتبر لذلك من بين المقومات الشخصية ، وتخرج عن دائرة التعامل الاقتصادي ، وهذه الحقوق بطبيعتها غير قابلة للمبادلة . كالحق في الحياة والحق في سلامة الجسم والحق في الحرية والحق في صيانة العرض والحق في الشرف والاعتبار . فيمكن عن طريق الشبكة إرتكاب جرائم كثيرة منها تصل كما يرى البعض<sup>(١)</sup> إلى القتل عن طريق برمجة جهاز تفجير يتم التحكم به الكترونياً. إضافة إلى ذلك هناك أيضا أنشطة القرصنة الموجهة نحو الأفراد والأسر والجماعات التي تنظمها ضمن الشبكات ، وتميل إلى بث الخوف بين الناس ، بالتهديد وإظهار القوة ، وجمع المعلومات ذات الصلة لتدمير حياة الناس .<sup>(٢)</sup>

ومنها كذلك الجرائم الإرهابية ، إذ يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية. ومما يقوم به الإرهابيون أيضاً اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والإطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.<sup>(٣)</sup>

ومن الجرائم الواقعة على الأموال . وهي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات القيمة المالية ، ويدخل في نطاق هذه الحقوق كل حق ذي قيمة اقتصادية ، ويدخل لذلك في دائرة التعامل ، ومن ثم كان أحد عناصر الذمة المالية . ومنها سرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الحاسب ، وتزوير البريد الإلكتروني أو الوثائق والسجلات والهوية ، وجرائم المقامرة بالتملك والتسهيل والتشجيع عليها ، فضلاً عن استخدام الشبكة لترويج الكحول ومواد الإدمان للقصر والحيازة غير المشروعة للمعلومات وجرائم الاحتيال و استخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون

(١) د. محمد حماد مرهج المهيتي - مصدر سابق - ص ١٥٨ - ص ١٥٩ .

(٢) Computer crime Wikipedia - October 2008.

(٣) د. عبد الرحمن بن عبد الله السند - مصدر سابق - ص ٨

ترخيص و الاختلاس عبر الحاسب أو بواسطته . و جرائم الإلتاف والتدمير والاعتداء على أموال الغير . كذلك تؤمن الشبكة فرصاً للقيام بمختلف أشكال السرقات، سواء كانت من المصارف الموصولة بالشبكة أو من الممتلكات الفكرية، وهي تؤمن أيضاً وسائل جديدة لارتكاب جرائم قديمة كالاختيال، وتوفر مكامن ضعف جديدة تتعلق بالاتصالات والمعلومات، مما يتيح جريمة الابتزاز، وهي الجريمة التي كانت دائماً السلعة الرئيسية لمنظمات المافيا .

وتستخدم مجموعات الجريمة المنظمة الشبكة للقيام بأعمال رئيسية من الاختيال والسرقة. ولعل أبرز مثال على ذلك - رغم عدم نجاحه - ما حصل في شهر تشرين الأول عام ٢٠٠٠ مع بنك صقلية. فقد ابتكرت مجموعة من حوالي ٢٠ شخصاً، بعضهم يرتبط بعائلات المافيا، بمساعدة شخص من داخل البنك، نسخة رقمية طبق الأصل لنظام وصل البنك بالشبكة. بعد ذلك قررت المجموعة استعمال هذه النسخة الرقمية المطابقة للأصل لتحويل مسار حوالي ٤٠٠ مليون دولار كان الاتحاد الأوروبي قد خصصها لتمويل مشاريع إقليمية في صقلية. كان من المقرر غسل الأموال عبر مؤسسات مالية مختلفة منها بنك الفاتيكان وبنوك في سويسرا والبرتغال. أحبطت الخطة عندما باح بالسر شخص من المجموعة إلى السلطات الرسمية. رغم ذلك، كشفت هذه المحاولة الفاشلة بصورة واضحة للغاية أن الجريمة المنظمة تجد فرصاً ضخمة لها لتحقيق أرباح نابعة من نمو العمل المصرفي الإلكتروني والتجارة الإلكترونية.<sup>(١)</sup>

ومن الجرائم الضارة بالمصلحة العامة ، وهي تلك الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع العام ، أي تلك الحقوق التي ليست لفرد أو أفراد معينين بذواتهم ، فالحق المعتدى عليه هو المجتمع في مجموع أفراد ، أو هو الدولة بصفقتها الشخص القانوني الذي يمثل المجتمع في حقوقه ومصالحه كافة ، ومنها جرائم الاعتداء على الأمن الخارجي و الداخلي للدولة و الرشوة و الاختلاس و تزيف العملة و تزوير المستندات الرسمية ، الإخبار الكاذب عن الجرائم و تضليل العدالة و العبث بالأدلة القضائية ، و التأثير فيها ، و تهديد السلامة العامة .... وغيرها الكثير .

ولكننا نفرّد لجرائم شائعة الوقوع باستخدام الشبكة هذا التصنيف لنماذج منها كالآتي:-

(١) فيل وليامز - مصدر سابق - ٢٠٠٢

١- انتحال الشخصية : هي جريمة الألفية الجديدة كما سماها بعض المختصين<sup>(١)</sup>. في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصة 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 الشبكة أمر سهل وهذه من أكبر سلبيات الشبكة الأمنية. وللتغلب على هذه المشكلة ، فقد بدأت كثير من المعاملات الحساسة على الشبكة كالتجارية منها ، في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة.

ومثالها ما يواجهه شخص من سكان ولاية واشنطن يدعى راندي ترافيس (١٩ عاماً)، من الذين اعتادوا الظهور على الشبكة باسم "fireismyplaymate" تهمة بإرتكابه خمس جنایات بعد استعمال الحاسوب للقرصنة والتخيط بإسم مزور لإرتكاب جرائم القتل في ولاية كاليفورنيا". وإذا أدين فإنه يواجه عقوبة تصل إلى السجن ١٨ عاماً.<sup>(٢)</sup>

٢- المضايقة والملاحقة : تتم جرائم الملاحقة على الشبكة غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الأنوية المختلفة ، وتشمل الملاحقة رسائل تهديد وتخويف ومضايقة. تتفق جرائم الملاحقة على الشبكة مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية. لكنها تتميز بسهولة إمكانية المجرم في إخفاء هويته ، علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة ، الأمر الذي ساعد في تقشي هذه الجريمة. ومن المهم الإشارة إلى أن طبيعة جريمة الملاحقة على الشبكة لا تتطلب اتصال مادي بين المجرم والضحية ، والذي لا يعني بأي حال من الأحوال قلة خطورتها، فقدره المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تقضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية.

٣- التغريب والاستدراج : إن ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة. حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الشبكة والتي قد تتطور إلى النقاء مادي بين الطرفين. إن مجرمي التغريب والاستدراج على الشبكة يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون

(١) للمزيد ينظر: د. إياس ألهاجري - مصدر سابق - ٢٠٠٢.

(٢) Internet Crime - is really a group of online related crimes 18 May 2008.

المجرم في بلد والضحية في بلد آخر، وكون معظم الضحايا هم من صغار السن ، فإن كثيراً من الحوادث لا يتم الإبلاغ عنها ، حيث لا يدرك كثير من الضحايا أنهم قد غرر بهم . فالمحتالون دائماً لديهم تقديم صفقات كانت تأتي عن طريق البريد أو في اتصال هاتفي. ومثالها الاحتيال على المستهلكين عن طريق البريد الإلكتروني وذلك بنشر ٣٠٠ ألف نسخة من نماذج التعرير التي يستخدمها المغرورون.<sup>(١)</sup>

٤- التشهير وتشويه السمعة : يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن شخصيته، والذي قد يكون فرداً أو مجتمعاً أو ديناً أو مؤسسة تجارية أو سياسية، وتتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين. ونشر معلومات كاذبة تضر بسمعة الآخرين يمكن أن يكون أساساً لدعوى تعويض عن أضرار الشبكة والاتصالات فيها ، وهو ما يسمى بالاستعمال غير المشروع لتكنولوجيا المعلومات ، باستعمال برامج الحاسب ، البريد الإلكتروني ، البريد الصوتي ، وغيرها.<sup>(٢)</sup>

٥- صناعة ونشر الإباحية : تعد شبكة المعلومات الدولية أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية، بحيث إن الشبكة جعلت الإباحية بشتى وسائل عرضها من صور وفيديو وحوارات في متناول الجميع ، ولعل هذا يعد أكبر الجوانب السلبية لها خاصة في المجتمعات المحافظة . وتعد صناعة ونشر الإباحية جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال، ولقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر ١٩٩٨م ، تتعلق هذه الجرائم بتغريير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال.<sup>(٣)</sup> وثمة قناعة بأن الجنس كجريمة سيكون لها تأثير دائم على الفرد في المستقبل، فبالإضافة إلى العقوبات الجنائية القاسية التي توقع على مرتكبيها ، فإنها

(1) Kari Sable Burns - Computer & Internet Crimes - Olympia 2007.

(2) Internet Crime - is really a group of online related crimes 18 May 2008.

(3) Cyber Investigations - Inside FBI Cyber Operations \_ FBI.gov is an official site of the US Federal Government, 2009.

من المرجح أن تحمل وصمة اجتماعية ، فضلا عن الأضرار التي لحقت بالسمعة المهنية والعلاقات الشخصية للجاني والضحية.<sup>(١)</sup>

وكثير من الاستغلال الجنسي للقصر يمكن أن يحدث على الشبكة. فالجريمة تنطوي على أشكال تبادل صورة أو صور تبين للقاصر الاشتراك في فعل من أفعال السلوك الجنسي. كوسيلة لإستغلال المستخدم في توزيعها<sup>(٢)</sup>. هذا وقد بدأتها شعبة بالتيمور ، بتحقيق واسع النطاق ، لمكافحة الصور الإباحية للأطفال pedophile للحد من نشاط مروجيها على الشبكة ، ووضع أولئك الأفراد الذين يستخدمون الإعلانات التجارية والخاصة لتجنيد القاصرين إلى العلاقات الجنسية غير المشروعة أو توزيع الصور الإباحية للقصر إلكترونيا.<sup>(٣)</sup>

٦- النصب والاحتيال : أصبحت الشبكة مجالاً رحباً لمن له سلع أو خدمات تجارية يريد أن يقدمها ، وبوسائل غير مسبوقه كاستخدام البريد الإلكتروني أو عرضها على موقع معين أو عن طريق ساحات الحوار. ومن الطبيعي أن يُساء استخدام هذه الوسائل في عمليات نصب واحتيال. ولعل القارئ الذي يستخدم البريد الإلكتروني بشكل مستمر تصله رسائل بريدية من هذا النوع. فكثيراً من صور النصب والاحتيال التي يتعرض لها الناس في حياتهم اليومية على الشبكة ، ومثالها بيع سلع أو خدمات وهمية ، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها. وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال. إن ما يميز عمليات النصب والاحتيال على الشبكة عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي<sup>(٤)</sup>.

وبعد هذا الإستعراض المبسط للجرائم التي تتعرض لها الشبكة أو تكون فيها وسيلة للسلوك الإجرامي ، أجد نفسي متسائلاً ، هل إن قوانيننا العقابية في العراق قادرة على التعامل مع هكذا مجرمين ، بإثبات هذه الجرائم وإيقاع العقاب على مرتكبها ؟ وهل لدينا الملاكات التنفيذية الكفوة والقادرة على مكافحة هذه الجرائم ؟ الأمر حقيقة يحتاج إلى تدخل تشريعي حازم للسيطرة على هذا الوباء.

(١) Jack L. Jaffe.- All rights reserved. Disclaimer - Legal Center , Site Map. 2008.

(٢) Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.

(٣) Justice Department's Computer Crime Initiative – Cybercrime ,2009.

(٤) د. إياس الهاجري - جرائم الإنترنت - مكتب خدمات البوابة ، يناير ٢٠٠٢.

فقد عمدت الدول الأوروبية إلى ضمان توفير الحماية الكافية لحقوق الإنسان والحريات ، والتي تنشأ وفقا للالتزامات التي تعهدت بها في إطار مجلس أوروبا عام ١٩٥٠ واتفاقية حماية حقوق الإنسان والحريات الأساسية ، لعام ١٩٦٦ في الأمم المتحدة والعهد الدولي الخاص بالحقوق المدنية والسياسية ، وغيرها من صكوك حقوق الإنسان الدولية السارية ، والتي تتضمن التعاون على تسليم المجرمين فيما بين الأطراف من أجل الأفعال المجرمة على وفق المواد من ٢ إلى ١١ من هذه الاتفاقية ، شريطة أن يعاقب عليها بموجب قوانين كل من الأطراف المعنية عن طريق الحرمان من الحرية لمدة لا تتجاوز واحدا على الأقل سنة ، أو يعقوبة أشد. و في حالة اختلاف الحد الأدنى من العقوبة الواجب تطبيقها في إطار الترتيبات المتفق عليها على أساس المعاملة بالمثل أو تشريع أو معاهدة لتسليم المجرمين ، بما فيها الاتفاقية الأوروبية لتسليم المجرمين رقم ٢٤ ، والتي تنطبق بين طرفين أو أكثر ، والحد الأدنى والعقوبة المنصوص عليها بموجب هذا الترتيب أو تطبق المعاهدة. و يجوز لأي طرف أن يطلب إلى الطرف الآخر من أجل الحصول على وجه السرعة والحفاظ على البيانات المخزنة بواسطة نظام حاسوبي ، الواقعة داخل أراضي الطرف الآخر وذلك فيما يتعلق بالطرف الطالب الذي يعتزم تقديم طلب للحصول على المساعدة المتبادلة ، أو لتأمين الحجز ، أو الكشف عن البيانات.<sup>(١)</sup>

ولمكتب التحقيقات الفدرالي الأمريكي فرقة خاصة بمتابعة الجريمة على شبكة المعلومات الدولية تحتوي أكثر من ٢٠٠ وكيل عبر الولايات المتحدة. يستعمل المخبّرين والوكلاء السريين. ويرى إن المشكلة لن تنحصر في لصوص الحاسوب الأحداث، فالمجرمون المحترفون يستغلون الشبكة الآن للربح ونشر أوبئة الفيروس الأخيرة حول العالم ، ومحاولة انتزاع المال أو البيانات من الشركات الرئيسية.<sup>(٢)</sup>

نتمنى من السلطات المختصة في عراقنا الجديد أن تأخذ بعين الاعتبار الجرائم الناجمة عن استخدام الشبكة ، ووضع العقوبات التي تفرض على المجرمين فيها ، وكذلك إيجاد الإجراءات الجنائية اللازمة التي تمكن السلطات التنفيذية من القبض على المجرمين ، وتدريب وتأهيل الفرق الخاصة والتي تمتلك الإمكانيات البشرية والمادية لتخليص المجتمع من هذه الجرائم .

(١) INTERPOL – Convention on Cybercrime -Budapest, 23.XI.2001 .

(٢) Bbc.co.uk \_ Source: CSI/FBI Computer Crime and Security Survey, 2000



**الخاتمة :**

من خلال تناولنا لمفهوم الجريمة باستخدام شبكة المعلومات الدولية ، إستعرضنا في أوراق بحثنا هذا مفهوم الجريمة عن طريق توضيح ماهية هذه الجرائم من خلال تعريفها فضلاً عن تعريف المجرم في هذه الجرائم ثم تناولنا بيان خصائص هذه الجرائم وخصائص مجرميها ، ثم بيان صور هذه الجرائم باعتبارها جرائم خاصة ترتكب على هذه الشبكة ، وكذلك بيان صور الجرائم التي تكون الشبكة وسيلة فيها ، وتوصلنا إلى بعض النتائج نعرض أهمها في النقاط التالية :-

- ١- تعرف الجريمة باستخدام شبكة المعلومات الدولية بأنها القيام بعمل جرمه القانون أو الإمتناع عن عمل أمره به القانون ، يضر بشبكة المعلومات الدولية أو يسيء إستخدامها . ويعرف المجرم في هذه الجرائم بأنه كل من يرتكب جريمة تمس بشبكة المعلومات الدولية وتضر بها.
- ٢- للجريمة المرتكبة باستخدام شبكة المعلومات الدولية خصائص تميزها عن غيرها من الجرائم هي ، إنها جرائم عالمية الإرتكاب ، تقع في بعض صورها على مال غير قابل للنفاد ، تحتاج بعض هذه الجرائم إلى قمة الذكاء في ارتكابها ، وفي بعض صورها تكون سهلة الإرتكاب ، لكل من يجيد إستخدام التقنية ، تتميز بسرعة انتشارها ، وهي جرائم الرقم المظلم ، فهي لا تترك أثراً" يمكن للجميع إكتشافه . كذلك صعوبة الإحتفاظ بالدليل إن وجد ، وتسبب خسائر جسيمة ، سواء كانت منسوبة على الأشخاص أو الأموال ، و يصعب الإثبات الجنائي فيها ، فهي غالباً ما تكون غامضة ، لصعوبة إكتشاف مرتكبيها ، والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية ، ومن الصعوبات أيضاً مشكلة تحديد المسئول جنائياً عن الفعل الإجرامي ، تتعدد أنواعها بشكل يصعب السيطرة عليها لأنها في تزايد مستمر مع تطور التقنية المستمر ، ثم إنها جرائم لا تحتاج عادة إلى بذل الجهد الكبير .
- ٣- المجرم في الجرائم المرتكبة على شبكة المعلومات خصائص تميزه عن غيره من المجرمين أبرزها ، إنه مجرم يستخدم الوسائل التقنية ولديه القدرة على إستباق الزمن والتطورات التشريعية البطيئة ، والكثير منهم خريجون جامعات أو ينتمون لمؤسسات علمية هامة ، ولا يحد هذا المجرم عمر معين ، فهذه الجرائم كما يمكن للبالغين إرتكابها من ذوي الفئات العمرية المختلفة ، يمكن أيضاً للصغار الأحداث إرتكابها ، يقوم بعمل إجرامي واسع بسعة الشبكة التي هدف جريمته أو مسرحها ، لا يهدف في الكثير من جرائمه إلى الربح ، فقد

- يكون التحدي وإثبات الذات هو الدافع لديه ، وهو مجرم مرن وقابل للتكيف مع تطور التقنية ، يستغل الفرصة بوجود الثغرات في المواقع الخاصة بالشركات أو الأفراد ، يتميز بالقدرة على التخفي والعمل السري ، فيعتمد إلى عدم تمكين المجنى عليه من ملاحقته أو إكتشافه وإبقاء جريمته في إطار البريد أو الموقع الإلكتروني المجهول الهوية والعنوان ، ولا ينتقيد هؤلاء المجرمون بمشكلة الحدود الدولية وكيفية عبورها ، أو الحصول على التأشيرة للدخول ، لأن جريمته عالمية ، والعقاب عليها ضعيف في أغلب بلدان العالم .
- ٤- للجريمة باستخدام الشبكة صور خاصة بها من أهمها جرائم ، الجرائم بالإصطناع والنشر والزرع وغير ذلك ، وكذلك جرائم الإختراق ، وجرائم تعطيل الأجهزة ، وجرائم تدمير المواقع ، وجرائم خرق الإتفاقيات الألكترونية ، وجرائم الإضعاف ، والجرائم الواقعة على الإتصالات والجرائم الواقعة على الخدمات ، وجرائم التجسس ، والجرائم الواقعة على البريد الألكتروني ، وغيرها .
- ٥- إذا اعتبرنا شبكة المعلومات الدولية وسيلة من الوسائل التي يتوصل الجاني فيها لتنفيذ سلوكه الإجرامي فإننا نراها تقع على الأشخاص والأموال والمصالح العامة والخاصة على حد سواء ، وهناك من هذه الجرائم ما تعد الشبكة فيها وسيلة أساسية لإكتمال سلوكها الإجرامي ، أو هي الوسيلة الوحيدة فيه ، ومنها التهديد ، وإنتحال الشخصية ، والتغريب والإستدراج ، والملاحقة والمضايقة ، والتشهير بالسمعة ، ونشر الإباحية والمخدرات ، والنصب والإحتيال ، وحتى الجرائم الإرهابية .
- ٦- الجانب التشريعي ضعيف - إن لم أقل معدوماً - في العراق ، الذي يزخر اليوم بالآلاف من هذه الجرائم ، لذلك نهيب بمشرعنا القانوني التصدي لهذه السلوكيات المنحرفة بالعقاب عن طريق تشريع جنائي خاص بها ، أو أفراد مواد قانونية لها في قانون العقوبات الجديد . وقبل هذا الإجراء لا يمكننا أن نعاقب عليها بصورها الصريحة ، لأننا محكومون ، بلا جريمة ولا عقوبة إلا بنص .
- ٧- نوصي بتطوير وتأهيل فرق خاصة ذات كفاءة عالية ، ومدربة تدريباً مهنياً وتقنياً ، تختص بمكافحة هذه الجرائم ، وملاحقة مجرميها ، لكي لا يستشري وبأوهم في مجتمعنا المحافظ .

**مراجع البحث :**

**باللغة العربية :****أولاً : الكتب :**

١. د. قدري عبد الفتاح الشهاوي - الإستدلال الجنائي والتقنيات الحديثة - دار النهضة العربية ، القاهرة ٢٠٠٥.
٢. د. محمد حماد مرهج الهيبي - التكنولوجيا الحديثة والقانون الجنائي - ط ١ ، دار الثقافة للنشر ، عمان - الأردن ٢٠٠٤.

**ثانياً : البحوث :**

١. د. إياس أهاجري - جرائم الإنترنت - مكتب خدمات البوابة ، يناير ٢٠٠٢.
٢. د. عبد الرحمن بن عبد الله السند - وسائل الإرهاب الإلكتروني ، حكمها في الإسلام وطرق مكافحتها - الرياض ٢٠٠٨ .
٣. فيل وليامز- الجريمة المنظمة وجرائم الشبكات الإلكترونية: الترابطات، والاتجاهات، والاستجابات - ، مركز خبرات أمن الإنترنت في جامعة ميلون كارنيجي. ٢٠٠٢.
٤. د. محمود صالح العادلي - الجرائم المعلوماتية ، ماهيتها - وصورها - ورشة العمل الإقليمية حول : تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط ابريل ٢٠٠٦.
٥. المحامي يونس عرب - الخصوصية وامن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي - منتدى العمل الإلكتروني ، اتحاد المصارف العربية عمان - الأردن ٢٠٠١.
٦. \_\_\_\_\_ - التشريعات والقوانين المتعلقة بالإنترنت في الدول العربية - مؤتمر التكنولوجيات المصرفية العربية والدولية، عمان - الأردن ٢٠٠٢.

**ثالثاً : التشريعات :**

١. قانون المفوضية العراقية للاتصالات والإعلام رقم ٦٥ لسنة ٢٠٠٤-٣-٢٠٠٤ .
٢. الوقائع العراقية - رقم العدد: ٣٨١٢ | تاريخ: ٢٠٠٧/٠٧/٢٠٠٠.

**باللغة الأجنبية :**

1. A.Bretrant. La ceiminaltie , informatique : (2) les delits relatives au material ,no62, 1984.
2. Bbc.co.uk - Source: CSI/FBI Computer Crime and Security Survey, 2000.
3. Computer crime Wikipedia - October 2008.

4. Cyber Investigations - Inside FBI Cyber Operations \_\_ FBI.gov is an official site of the US Federal Government,2009.
5. Daniel C. Grupenhagen - Computer and Internet Crimes in Orange County- 2008.
6. Internet Crime - is really a group of online related crimes18 May 2008.
7. INTERPOL - Convention on Cybercrime -Budapest, 23.XI.2001 .
8. Jack L. Jaffe - All rights reserved. Disclaimer - Legal Center , Site Map. 2008.
9. Justice Department's Computer Crime Initiative – Cybercrime,2009.
10. Kari Sable Burns - Computer & Internet Crimes - Olympia 2007.
11. Legal Information Center – Criminal Law - Legal Information Institute , Cornell Law School. 2009.
12. Tushar K. Pain - What is a computer or Internet crime - Criminal Defiance Articles , University Avenue ~ Suite 2000.
13. United States Department of Justice -Computer Crime & Intellectual Property Section – 2009.
14. Washington Post. SEPTEMBER 12TH, 2008.