مدخل إلى الجريمة الالكترونية

تمهيد:

الجريمة ظاهرة اجتماعية تتواجد بتواجد الانسان والمجتمع وتتطور بتطورهما، خاصة والعالم يشهد تغير وتطور معلوماتي وتكنولوجي سريع، ولاشك أن المجرمين – كما رجال الامن – يحاولون الاستفادة من هذا التقدم التقني خاصة وإننا في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة، وتبعا لذلك فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصرا على أسباب التقدم التقني فقط، بل يحدث دوما وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمر . فمجرم الامس ليس كمجرم اليوم وبالتالي فجريمة الامس ليست كجريمة اليوم، وقد تمخضت ثورة المعلومات والتكنولوجيا المتقدمة عن وسائل اتصالات متطورة جعلت العالم قرية الكترونية مفتوحة للعموم، الغت معها الحدود الجغرافية والسياسية للدول، وهذه التقنية الخاصة بنظام نقل المعلومات السريع أو ما يعرف بالانترنت ليست سيئة في حد ذاتها بل هي سلاح ذو حدين ، فيمكن ان تسخر للخير و المنفعة كما يمكن أن تسخر للشر والمضرة.

ورغم الفوائد العديدة التي لا تحصى للاستفادة من شبكة المعلومات العالمية (الانترنت) ، فقد توسعت الشبكة ولم تعد قاصرة على أغراض البحث العلمي بل امتدت لتشمل المعاملات التجارية و السياسية والأمنية والصحية والرياضية ...الخ، إلا انه في نفس الوقت فقد زادت أساليب إساءة الاستخدام لتلك الشبكة ومنها الاستخدام لارتكاب بعض الجرائم.

واذا كان العصر المعلوماتي أو عصر ثورة المعلومات هو نتاج طفرة الاتصالات وطفرة تقنية المعلومات ، فإن ما جاء به من أنشطة غير مشروعة ، تنطوي بلا شك على أنشطة إجرامية تقليدية تأخذ شكلا مستحدثا.

فشبكة الانترنت– بوصفها نتاج المعلوماتية – كأداة للربط والاتصال بين مختلف شعوب العالم ، تشكل أداة لارتكاب الجريمة، أو محلا لها. وذلك بإساءة استخدامها واستغلالها على نحو غير مشروع، مما أدى إلى ظهور طائفة جديدة من الجرائم عرفت بالجريمة المعلوماتية.

وهذه الجرائم يطلق عليها الجرائم الالكترونية (السيبرانية) أي تلك الاعمال التي تتم عن طريق الانترنت، ومع التطور المستمر للأنترنت وتوفر السرية التامة جعل من الانترنت جهاز التنفيذ للعديد من الجرائم بعيدا عن أعين

الجهات الأمنية , فقد سمحت شبكة الانترنت ومهدت لظهور الجرائم الالكترونية . فأصبحت الانترنت نموذجا صارخا للإجرام تتخلله ثغرات قانونية تتحدى الاجهزة الامنية والقضائية.

وقد أصبحت الجريمة الالكترونية احدى اهم الاخطار التي تواجه الدول المتقدمة والنامية على حدا سواء (حيث تكلف العالم 400 مليار دولار سنويا)، فهي عالمية بلا حدود حيث ان التحقق فيها والحكم عليها عملية معقدة ، ترتكب من قبل الافراد أكثر مما ترتكب من محترفي الحاسوب وشبكات المعلومات، كما يمكن أن ترتكب من مراكز البحوث ومن الاكاديميين ، ومن المدريين يبحثون عن الثراء أو السلطة .أو من قبل منظمات تبحث عن معلومات عن منافسيها أو من وسائل الاعلام تبحث عن معلومات أو اخبار أو من قبل حكومات تبحث عن معلومات تجارية ، أو جريمة منظمة تبحث عن ملفات موثوقة ، ففي ظل التحول إلى الحكومة والإدارة الالكترونية والتجارة الالكترونية ..الخ أصبح لزاما على الجهات المعنية إيجاد حلول لمختلف الصعوبات التي قد تعوق سير إدارة الخدمات الالكترونية والعمل على إصدار تشريعات والقوانين المناسبة التي تمنع من ارتكاب الجرائم الالكترونية .

والجريمة الالكترونية تمس الحياة الخاصة للأفراد وتهدد الاعمال التجارية بخسائر فادحة، كما تنال من الامن القومي والسيادة.

ان الجرائم الالكترونية امتدت وتوسعت بالتشهير بالشخص وتشويه سمعته وكذا جرائم النصب والاحتيال والابتزاز وغيرها من الأفعال الاجرامية. وسنحاول من خلال هذه المحاضرة تناول موضوع الجريمة الالكترونية من حيث تعريفها ونشأتها وخصائصها وانواعها و أسبابها ، ....الخ

1-تحديد المفاهيم:

أولا – الجريمة :

لغة :

– الجريمة مفردها الجرم وهو في اللغة التعدي والذنب , وتعني أيضا الجناية وهي كل فعل محظور يتضمن ضررا.

(صليبا، 1982، صفحة 398) .

اصطلاحا:

التعريف الشرعي للجريمة: تعرف الجريمة شرعا بأنها " إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه"

التعريف القانوني للجريمة: يعرف القانون الجريمة بأنها " إما عمل يجرمه القانون، أو امتناع عن عمل يقضي به القانون ، ولا يعتبر الفعل أو الترك جريمة في نظر القوانين الوضعية، إلا إذا كان معاقبا عليه طبقا للتشريع الجنائي.(عياد، 2006، صفحة 12)

ثانيا– الجريمة الالكترونية :

– لغة:

– الكتروني و الكترونيات نسبة للإلكترون , وبدأ ينتشر العقـل الالكتروني في كل المكاتب : الة الحاسوب وتعتمد على مادة الالكترون لأجراء ادق العمليات الحسابية وبأسرع وقت ممكن ويسمى أيضا كمبيوتر (المعاني).

اصطلاحا :

لم يتفق العلماء على تسمية موحدة للجـريمة الالكترونية فهناك عدة تسميات منها : الجريمة المعلوماتية , جرائم إساءة استخدام تكنولوجيا المعـلوماتية والاتصال , جرائم الكمبيوتر و الانترنت , الجرائم المستحدثة , الجريمة الناعمة , جرائم الحاسب الآلي والانترنت...الخ

وتجدر الإشارة ان هناك فارق في ميدان جرائم الحاسب الالي وميدان الانترنت . فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب الالي وبرامجه والمعلومات المخزنة فيه . فان جرائم الانترنت تتحقق بنقل المعلومات والبيانات بين الأجهزة الحاسب الالي عبر خطوط الهاتف او الشبكات الفضائية الا ان الواقع التقني للحوسبة أدى اندماج الميدانيين (المطرودي، 2012، صفحة 13).

ويمكن عرض بعض التعريفات :

– الجريمة الالكترونية " كل فعل غير مشروع يكون العلـم بتكنولوجيا الحاسبات الالية بقدر كبير لازم لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى ".

كما يمكن تعريفها بأنها "ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقق فيها ومقاضاة فاعليها". (عياد، 2006، صفحة 12)

حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة. بل كذلك لملاحقتها والتحقق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة الالكترونية بمعنى يجب ان يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة والمتخصصين بملاحقتها من قضاة وضباط الشرطة وغيرهم.

ويعرفها روزبلات بأنها:" هي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي، والتي تحول طريقه" (الشوابكة، 2009، صفحة 8)

الجريمة المعلوماتية في منطلق هذا التعريف ، ليست هي التي يكون الحاسب أداة ارتكابها، بل التي تقع على الحاسب أو داخل نظامه.

ويرى الأستاذ باركر ان الجريمة المعلوماتية هي: " كل فعل اجرامي متعمد، أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل. "

والحقيقة ان التعريفات السابقة للجريمة المعلوماتية قاصرة عن الإحاطة بأوجه ظاهرة الاجرام المعلوماتي، إذ ركز البعض على موضوع الجريمة، وركز البعض الآخر على وسيلة ارتكابها، بينما ركز آخرون على فاعل الجريمة، بينما نرى ان الجريمة المعلوماتية قد تقع على الحاسب الآلي بشقيه المادي و المعنوي ممثلا بالكيان المنطقي، بالاعتداء على البيانات المخزنة و المتبادلة بين الحاسب الآلي وشبكاته –الخاصة والعامة– عبر خطوط قنوات الاتصال.

<u>الاتجاه الموسع من تعريف الجريمة الالكترونية :</u>

على عكس الاتجاه السابق يرى فريق اخر من العلماء ضرورة توسيع من مفهوم هاته الجريمة وبالتالي هي:" كل جريمة تتم بوسائل الكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الانترنت من خلال : غرف الدردشة واختراق البريد الالكتروني ومختلف وسائل التواصل الاجتماعي بهدف الحاق الضرر للفـــرد او المجموعة وحتى الدول ضمن برنامج استهداف حربي او اقتصادي او الاضرار بسمعتها او العكس . ويبقى الهدف هو الكشف عن قضايا متستر عليها او نشر معلومات لفائدة طرف او اطراف أخرى من باب التسريب

وفي تقرير الجـرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام مخالفة الجـريمة في كل حالة يتم فيها تغيير المعطيات او البيانات او البرامج او محوها او كتابتها او أي تدخل اخر في مجال انجاز البيانات او معالجتها وتبعا لذلك تسبب في ضرر اقتصادي، او فقد ،او حيـازة ملكـية شخص، او بقصد الحصـــول على كسب اقتصادي غير مشروعه او لشخص اخر .

من خلال هاته التعاريف يتضح لنا صعوبة قبول هذا التوجه لأن الحاسب الالي نفسه لا يعدو ان يكون محلا تقليديا في بعض الجرائم كسرقة الحاسوب نفسه او الأقراص الممغنطة على سبيل المثال .

ومن ثم لا يمكن إعطاء وصف للجريمة الالكترونية على سلوك الفاعل لمجرد ان الحاسب الالي او أي من مكوناته كانوا محل للجريمة , كما انه قد ترتكب الجريمة ويستعمل الحاسب الالي ولا نكون امام جريمة الكترونية , كمن يقوم بالاتصال بواسطة حاسب الآلي بشركائه في ارتكاب جريمة سطو على بنك .

وحديثا تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته ، حيث عرف الجريمة المعلوماتية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية ".ويعد هذا التعريف – وبحق– من أفضل التعريفات التي تناولت ظاهرة الاجرام المعلوماتي، إذ أنها تشمل كلا الجانبين: المادي والمعنوي للحاسب الآلي ومنها شبكة الانترنت. وكذلك فإنه لا يقتصر على مجرد كون الحاسب الآلي وشبكاته محلا للاعتداء، بل أيضا وسيلة للاعتداء وارتكاب الجرائم. (عطوي، 1991، صفحة 15)

ثالثا– الحاسب الآلي: يمكن ان يعرف بأنه مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة"

وهناك من يعرف الحاسب الآلي بأنه:" جهاز آلي أو آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون (سلفا في الجهاز الانترنت: تعني لغويا (ترابط بين شبكات) وبعبارة أخرى (شبكة الشبكات) حيث تتكون الانترنت من عدد كبير من شبكات الحاسب المترابطة و المتناثرة في انحاء كثيرة من العالم. ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الانترنت

TCP/IP

الشبكة النسيجية WORLD WIDE WEB.وتسمى ايضا

تمثل مدخلا ميسرا للانترنت وتمثل واجهة استخدام موحدة للعديد من أدوات الشبكة المتاحة وتعمل عن طريق تأسيس WEBروابط نصية متشعبة بين الوثائق الموجودة في أي مكان عل الشبكة.، (عياد، 2006، صفحة 10)

رابعا – الانترنت: عبارة عن شبكة تتألف من العديد من الحاسبات الآلية المرتبطة ببعضها البعض، إما عن طريق خطوط التلفون، أو عن طريق الأقمار الصناعية، وتمتد عبر العالم لتؤلف في النهاية شبكة هائلة، بحيث يمكن للمستخدم لها الدخول إليها من أي مكان وفي أي وقت، طالما كان جهاز الحاسب الآلي مزودا بمودوم يربطه بخط الهاتف لتلقي وارسال البيانات عبر مزود الخدمة. (الشوابكة، 2009، صفحة 7)

خامسا – المعلوماتية: وهي اختصار مزجي لكلمتي معلومة، وكلمة آلي أو آلية ، وهي تعني المعالجة الآلية للمعلومة. اذن المعلوماتية: يقصد بها ذلك العلم الذي يهتم بالموضوعات و المعارف المتصلة بأصل المعلومات أو البيانات وتجميعها، وتنظيمها واختزالها. واسترجاعها ثم بتفسيرها وإعادة بثها أو تحويلها واستخدامها، وبالتالي هي عملية ديناميكية غاية في التعقيد تتم بدقة متناهية وبسرعة فائقة بهدف إعادة تدويرها أو توظيفها في مجال محدد سواء كان هذا المجال اداري أو صناعي أو تجاري أو سياسي أو امني وذلك باستخدام رموز خاصة ""كود"" عند نقل أو بث البيانات والمعلومات.

(عياد، 2006، صفحة 37)

سادسا – القرصنة: يقصد بالقرصنة هنا استخدام أو النسخ غير المشروع لنظم التشغيل أو البرامج الحاسوبية المختلفة والاستفادة منها شخصيا أو تجاريا.

سابعا – الفيروسات الحاسوبية: هي احدى أنواع البرامج الحاسوبية إلا أن الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية تلحق ضرارا بنظام المعلومات أو البيانات، ولدى البرنامج القدرة على التضاعف والانتشار بحيث يزرع عند تشغيله نسخة منه في البرامج المصابة، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها فيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

ثامنا – حصان الطراودة: هو برنامج صغير ظاهره النفع وباطنه الدمار وينتقل عبلا الشبكات ويتم تشغيله داخل جهاز الحاسب لكي يقوم بأغراض التجسس على أعمال الشخص التي يقوم على حاسوبه الشخصي.

تاسعا– المتسلل: شخص بارع في استخدام الحاسب وبرامجه ولديه فضول في استكشاف حاسبات الآخرين وبطرق غير مشروعة.

عاشرا– المقتحم: شخص مخالف للنظام يقوم بالتسلل إل نظم الحاسب الآلي للاطلاع على المعلومات المخزنة فيها أو لالتحاق الضرر أو العبث بها أو سرقتها.

حدى عشر– البروكسي: برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الانترنت في جهة واحدة ضمن جهاز واحد. (عياد، 2006، صفحة 10، 11)

التعريف الاجرائي لجرائم الانترنت (الجريمة الالكترونية): جميع الأفعال التي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت، وتشمل ذلك:

– الجرائم الجنسية: (ارتياد المواقع الإباحية ، الشراء منها، الاشتراك فيها، أو انشائها، إنشاء القوائم الإباحية أو الاشتراك فيها، إنشاء المواقع أو الصفحات الخاصة بالقذف والتشهير بالاشخاص، استخدام البروكسي لتجاوز المواقع المحجوبة، إخفاء الشخصية أثناء التصفح أو أثناء إرسال البريد الالكتروني، انتحال شخصية الآخرين).

– جرائم الاختراقات: (تدمير المواقع، اختراق المواقع الرسمية أو الشخصية، اختراق الأجهزة الشخصية، اختراق البريد الالكتروني للآخرين ، إغراق البريد الالكتروني للآخرين، الاستلاء على اشتراكات الآخرين وارقامهم السرية، وارسال الفيروسات والتروجنات).

– جرائم الأموال: (السطو على ارقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، جرائم المخدرات وغسيل الأموال).

– جرائم انشاء أو إرتياد المواقع المعارضة أو المعادية (إنشاء، ارتياد أو الاشتراك في المواقع السياسية أو الدينية أو الشخصية المعادية).

– جرائم القرصنة(انشاء مواقع للبرامج المقرصنة، استخدام البرامج المقرصنة وسرقة المواقع)

(عياد، 2006، صفحة 13)

2– واقع الجريمة الالكترونية:

ظهرت الانترنت كثمرة لمشروع حكومي امريكي بدء تنفيذه في الستينات من القرن العشرين، يسمى الآربا نت، وكان ذلك عندما كلفت وكالة مشروعات البحوث المتقدمة بوازرة الدفاع الامريكية بتنفيذ المشروع، والذي استخدم بداية للأغراض المتعلقة بعلوم الكمبيوتر والمشروعات الهندسية.

وإزاء نجاح هذا المشروع، أخذت وزارة الدفاع الامريكية تتعمق بالبحث والدراسة لتغطي بذلك مساحات أكبر، وكان عام 1973 عند انشاء وكالة الدفاع الامريكية لمشاريع الأبحاث المتطورة (دابرا) برنامجا عرف بمشروع التشبيك الدولي، وذلك لغايات تطوير بروتوكولات الاتصال والتي تسمح لشبكات الحاسوب بالاتصال بالشبكة العالمية وهما: برتوكول النقل والسيطرة أو برتوكول الانترنت.

وقد اخذت شبكة الانترنت بالانتشار من خلال ربطها بشبكة العلوم الوطنية ، والتي شكلت دعما قويا لخدمة الاتصالات والانترنت، بالإضافة إلى مشاركة أوروبا في تطوير الانترنت من خلال ربطها بشبكاتها الدولية مثل نورد نت .

وفي عام 1989 قررت الحكومة الامريكية وقف تمويل الآربانت ، ووضعت خططا لإنشاء خلفا تجاريا لها في شكل شبكة تقرر تسميتها الانترنت، تؤدي إلى الاستفادة من المعلومات المخزنة عليها بشكل تجاري وعلى نطاق واسع من خلال برتوكولات الاتصال وتحديدا مع برتوكول نظام الربط المفتوح أوزي، الذي أدى إلى تدويل شبكة الانترنت، وعولمة المعلومات، بحيث يستفيد منها كل مستخدم في أية بقعة على الأرض.

وترتبط الانترنت عبر مجموعة متنوعة من المسارات عالية ومنخفضة السعة، ويستخدم أغلب المستهلكين الكمبيوترات الشخصية للدخول إلى النظام عبر شبكة التلفونات، والتي تتسم بعرض نطاق ترددي ضيق بواسطة جهاز موديم .

ويمثل أحد التحديات التقنية التي تواجه الانترنت في كيفية معالجة محتوى الوقت الفعلي للنقل الالكتروني السمعي (بما في ذلك الصوت) و المرئي على وجه الخصوص، إذ تسمح التكنولوجيا الأساسية للانترنت إلا بنقل البيانات من موضع لآخر بمعدل ثابت من السرعة ، حيث يعد كم الازدحام داخل الشبكة المعيار المحدد لمدى السرعة التي ترسل بها الحزم الصغيرة للبيانات أو حزمة البيانات . (الشوابكة، 2009، صفحة 15، 16، 17)

فمع تطور الانترنت وتوسع استخداماته وازدياد اعداد المستخدمين لها في العالم، ففي عام 2011 كان هناك 2.3 مليار شخص على الأقل كان لهم وصول إلى شبكة الانترنت، أي ما يعادل أكثر من ثلث اجمالي سكان العالم، وان أكثر من 60 في المائة من جميع مستخدمي الانترنت هم من البلدان النامية. وهناك 45 بالمائة من جميع مستخدمي

الانترنت دون سن 25 عاما. كما تشير التقديرات أنه قبل عام 2017 فإن اشتراكات المتنقل سوف تقترب من 70 في المائة من اجمالي عدد سكان العالم. وبحلول العام 2020 فإن عدد أجهزة الشبكة (انترنت الأشياء) سيفوق عددا الناس بمعدل(6، 1) ستة إلى واحد، محولين المفاهيم الحالية للانترنت ، في عالم الغد عالم الشبك فائق السرعة ، سيصبح من الصعب أن نتخيل " الجريمة الالكترونية"، وربما أي جريمة، لا تنطوي على أدلة الالكترونية مرتبطة مع برتوكول الانترنت.

تميز القرن 21 باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسعت الانترنت أضعافا مضاعفة. حاليا هناك 820 مليون شخص يستخدمون الانترنت، بزيادة قدرتها 126 في المئة من 2000– 2005. لقد وفرت السهولة النسبية لاستخدام الانترنت، والحصول على الانترنت على نحو متزايد أكثر للانترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة ، كل ذلك مكن الناس من التواصل وتكوين الصداقات الجديدة والتجارة ، والترفيه ، والتعليم ، والقيام باعمال تجارية ، ودفع الفواتير عبر الانترنت وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الالكتروني ، والذي يعرف بأنه " مكان لأجل غير مسمى حيث يتفاعل الافراد والتجمعات. ويتصف الفضاء الالكتروني بأنه مكان بلا حدود مادية أو اجتماعية تحرم الافراد من العيش فيه.

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي ، وكذلك انتقلت الجريمة ولنا ان نتصور حجم التفاعلات التي تتم في الواقع الافتراضي سواء كانت شخصية أو مؤسسية أو في مجال الاعمال أو الخدمات أو الثقافة... فعلى سبيل المثال على الفيس بك وضع صورة احد المشاهير فيما سمي لحظة الفوز 3 مليون شخص، ومتوسط عدد الأصدقاء على حساب الفيس بوك 130 صديق و23 بالمائة من المشتركين 850 مليون منهم 21 بالمائة من آسيا و 488 مليون يستخدمون الفيس بوك و 23 بالمائة من المشتركين يتفقدون حسباتهم 5 مرات في اليوم وهناك أكثر من مليون موقع متصل مع الفيس بوك وتوضع 250 مليون صورة يوميا، وفي عام 2012 تم تشغيل 210000 سنة من الموسيقى من المشتركين.

واذا اجئنا نتحدث عن معدلات الجريمة على المستوى العالمي فالقضية اكبر مما نتصور، ففي بريطانيا وفي عام 2007هناك جريمة الكترونية تقع كل 10 ثواني (3 مليون جريمة بالسنة أو 8 آلاف جريمة في اليوم). واكبر نسبة فيها تعود

لجرائم التحرش الجنسي(850 ألف حالة) ، بينما هناك 92 ألف حالة لسرقة الهوية أي الحصول على معلومات شخصية حول مستخدمي الانترنت ، و145ألف حالة لاختراق الحواسيب بهدف سرقة المعلومات أو التخريب ، و207 حالة للحصول على الأموال من خلال الاحتيال للسطو على ارقام البطاقات الائتمانية ، وتقول احصائيات شركات التأمين أن70 بالمئة من هذه الجرائم تستهدف الافراد. (مايكروسوفت"، 2007)

الأطفال هم اكثر ضحايا الجريمة الالكترونية على الانترنت فالإحصائيات العالمية تقول ان 80 بالمئة من الأطفال الذين يستخدمون البريد الالكتروني يستقبلون رسائل بريد الكتروني دعائية كل يوم، وبخاصة خلال فترات العطلة حيث يقضي الأطفال الكثير من الوقت في تصفح الانترنت. وبعض تلك الرسائل تتضمن محتوى لا ينبغي عليهم أن يطلعوا عليه في أي حال من الأحوال .

والمشكلة تكمن في أن معظم الأطفال لا يتجاهلون الرسائل الطفيلية ويفتحونها مدفوعين بالفضول الذي تحركه لديهم العناوين الرنانة لتلك الرسائل، وغالبا يفتح الطفل الرسالة. الكثير من هؤلاء الأطفال بالطبع ينزعجون من تلك الرسائل ولا يناقشون الموضوع مع اهاليهم...ويتم استدراج الأطفال عن طريق غرف الدردشة أو عن طريق طلب صورهم والعبث بها ونشرها .

والاحداث شهيرة في هذا الحقل كثيرة ومتعددة لكننا نكتفي في هذا المقام بايراد ابرز الحوادث التي حصلت خلال السنوات الماضية ، بحيث نعرض لحوادث قديمة نسبيا وحديثة كأمثلة على تنامي خطر هذه الجرائم وتحديدا في بيئة الانترنت.

** قضية مورس: هذه الحادثة هي احد الهجمات الكبيرة والخطرة في بيئة الشبكات ففي تشرين الثاني عام 1977 تمكن طالب يبلغ من العمر 23 عام ويدعى روبرت مورس من اطلاق فيروس عرف باسم دودة مورس عبر الانترنت، أدى إلى إصابة 6 آلاف جهاز معها حوالي 60000 نظام عبر الانترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لاعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ اكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على مورس بالسجن لمدة 3 أعوام وعشرة آلاف غرامة.

** قضية الجحيم العالمي: تعامل مكتب التحقيقات الفدرالية مع قضية اطلق عليها اسم مجموعة الجحيم العالمي، فقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفدرالية الامريكية والجيش الأمريكي ووزارة الداخلية

الامريكية، وقد ادين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات ان هذه المجموعات تهدف الى مجرد الاختراق اكثر من التدمير أو التقاط المعلومات الحساسة، وقد امضى المحققون مئات الساعات في ملاحقته ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها ، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.

** قضية مليسا: وفي حادثة هامة أخرى انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول اطلاق فايروس شرير عبر الانترنت عرف باسم فايروس ميلسا حيث تم التمكن من اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في عام 1999 ةاتهم باختراق اتصالات عامة والتآمر لسرقة خدمات الكمبيوتر، وتصل العقوبات في الاتهامات الموجهة له إلى السجن لمدة 30 يوما والغرامة التي تقدر بحوالي 500دولار وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة.

** الأصدقاء الأعداء: وفي حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الامريكية والكيان الصهيوني، فقد تمكن أحد المبرمجين الإسرائيليين في مطلع عام 1998، من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل ، وتم متابعة نشاطه من قبل عدد من المحققين في الولايات المتحدة الامريكية حيث أظهرت التحقيقات ان مصدر الاختراقات هي كمبيوتر موجود في الكيان الصهيوني فانتقل المحققون إلى الكيان الصهيوني وتعاونت معهم جهات تحقيق إسرائيلية حيث تم التوصل للفاعل وضبطت كافة الأجهزة المستخدمة في عملية الاختراق، وبالرغم من ان المحققين أكدوا ان المخترق لم يتوصل إلى معلومات حساسة إلا ان وسائل الاعلام الامريكية حملت أيضا اخبارا عن هذا الشخص كان في الأساس يقوم بهذه الأنشطة بوصفه عميلا (لإسرائيل) ضد الولايات المتحدة الامريكية .

(عياد، 2006، صفحة 98، 99، 100)

رابعا : خصائص الجريمة الالكترونية :

أولا : خصائص الجريمة الالكترونية :

لما كانت الجريمة الالكترونية هي نتاج التطور العلمي وتكنولوجي وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس , لذا نجد لها مجموعة من الخصائص او سمات تجعلها منفردة مع غيرها من الجرائم سواء من حيث الجريمة ذاتها او من حيث المرتكب وهذا ما يتم بيانه من خلال الفرعين المواليين :

الفرع الأول : السمات الخاصة بالجريمة الالكترونية

– تتسم بسهولة الوقوع في فخها، حيث ان غياب الرقابة الأمنية تساهم وتسهل ذلك، ان الضرر الناجم من الجريمة الالكترونية غير قابلة للقياس، إذ إنها تلحق أضرارا جسيمة.

–لا يتم في الغالب الاعم الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها. فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة، والعدد الذي تم اكتشافه، هو رقم خطير وبعبارة أخرى الفجوة بين عدد الجرائم الحقيقي، وما تم اكتشافه فجوة كبيرة.

– من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني، كما من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.

– إخفاء الجريمة والسرعة في ارتكابها، وأيضا التطور في الأساليب وتقنيات الفعل الاجرامي، حيث لا يتطلب تنفيذ الجريمة الالكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنقل ملايين الدولارات من مكان إلى آخر، وهذا لا يعنى انها لا تتطلب الاعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

– ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية وأجهزة ومعدات الحاسب الالي.

– يقوم بها مجرم ذو طبيعة خاصة وامكانيات خاصة يستخدم في ارتكاب جريمته بموارد معرفة وأساليب احترافية.

– تعتمد هذه الجرائم على قمة الذكاء في الذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها فهي جرائم تتسم بالغموض واثباتها بالصعوبة بمكان فيها يختلف عن التحقيق في الجرائم التقليدية. أي صعوبة الحصول على الدليل المادي في هاته الجرائم، إلا بأساليب امنية وتقنية عالية.

– هاته الجريمة لا يحدها مكان فهي عالمية عابرة للحدود. بمعنى عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، فهذه الجرائم هي صورة صادقة من صورة العولمة، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة، ومن الناحية الزمنية تختلف المواقيت بين الدول، الامر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة.

–.التنفيذ عن بعد، حيث لا تتطلب الجريمة الالكترونية في أغلبها (إلا جرائم سرقة معدات الحاسوب)، وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعينة أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب .

– الجاذبية ، نظرا لما تمثله سوق المعلومات والحاسب و الانترنت من ثورة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال و غسيلها، وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات ...الخ