

الجريمة الإلكترونية... دراسة سوسيو قانونية

أ / بوفاتح محمد بلقاسم ، كلية الحقوق والعلوم السياسية ، جامعة الجلفة

مقدمة :

إن التطور التكنولوجي الهائل أدى إلى انتشار شبكة الانترنت والحاسوب، وفتح مجالات عديدة للاستفادة منها، ولكن في نفس الوقت أدى إلى نشر ثقافة منافية لعادات وطباع الكثير من المجتمعات وخصوصا العربية نتيجة للانفتاح الذي فرضته هذه التقنيات وأيضا نتيجة إلى توفيرها المعلومات التي يمكن استخدامها في ما يحقق مصلحة للبشرية وأيضا ما يحقق ضررا لها مدعاة لانتشار نوع جديد من الجريمة وهو الجريمة الإلكترونية . والجريمة الإلكترونية هي وصف صعب لعمل مادي أصعب، حيث لا يوجد هنا حراس بل توجد حدود مفتوحة بلا حراسة، بل انه يمكن القول حالياً إن زمن الجواسيس الدوليين الذين كانوا يتبادلون الحقائق والملفات والصور السرية أو يقومون بنقل معلومات مهمة قد انتهى دورهم، حيث يمكن حالياً نقل كل المعلومات الخطرة والمختورة من معلومات استخباراتية أو خطط تخريبية أو صور سرية بشكل سهل جداً عبر ضغطة خفيفة على زر لوحة مفاتيح كمبيوتر. فالجمال حالياً مفتوح لكل أنواع الجرائم الإلكترونية التي يصعب حصرها أو تعدادها نظراً لازديادها وتنوع أساليبها كلما أمعن العالم في استعمال شبكة الانترنت، إن الجرائم الإلكترونية تختلف اختلافا جذريا عن أنواع الجرائم الأخرى اعتبارا للضرر الناجم عنها إذ لا يمكن الاستهانة به ولا يمكن بأي حال من الأحوال فصله عن الأضرار الناجمة عن مختلف الجرائم الأخرى مع اختلاف الأهداف طبعا ، كما أن اتساع نطاق الشبكة الدولية للمعلوماتية ، وزيادة عدد مستخدمي هذه الشبكة من الأعمار والأجناس المختلفة ، سرعان ما رافق ذلك بروز ظواهر جديدة وعديدة مثل الجريمة الإلكترونية والحب الإلكتروني ، والدعاية الإلكترونية ، والحرب الإلكترونية ، والفضفضة الإلكترونية أو الدردشة الإلكترونية ، والجنس الإلكتروني إلخ . ولدراسة هذه الإشكالية والوقوف على حيثياتها نصيغ جملة من الأسئلة التالية :

ما ملامح هاته الجريمة ؟ ما مدى تغلغلها بين الفئات ؟ وهل تتعدد أنواعها ؟ كيف يمكن مواجهتها ؟ ولإجابة عن هذه التساؤلات نقترح الخطوة التالية:

المبحث الأول: أشكال الجريمة الإلكترونية :

المطلب الأول : مفاهيم معلوماتية

1 - الاختراق : كأن يخترق شخصا البريد الإلكتروني لشخص آخر ، أو يخترق حسابات شركة معينة ويعرف أسرارها وربما يبيعها للمنافسين ، أو يخترق حسابات أحد البنوك أو يطلع على الأرقام المشفرة لحسابات بعض العملاء ، وربما ينجح في الدخول على الحساب وصرف بعض المبالغ (كما حدث فعلا في

أحد الحسابات البريدية لشخصية جزائرية منذ فترة قريبة) ، وربما تصل عمليات الاختراق إلى جهات أمنية أو استخباراتية أو وزارات الدفاع مما يشكل تهديدا للأمن القومي لبعض الدول .

وعملية الاختراق تشكل هوية محبة لبعض الشباب حيث يجلسون ساعات طويلة يتحينون الفرصة ويجربون طرقا مختلفة حتى يحققوا الاختراق وساعتها يشعرون بنشوة عجيبة ، وهذا الإحساس يشبه إلى حد كبير شعور التلصص والتصنت والتجسس واكتشاف الأسرار ، وهذه مشاعر تقليدية قديمة نحاول القياس عليها لمعرفة الشعور المصاحب للاختراق الإلكتروني .

يضاف إلى ذلك إحساسا بالقدرة والتفوق والسيطرة والانتصار ، وقد يلجأ إلى الاختراق بعض الشخصيات المحبة للمغامرة والاستكشاف أو الشخصيات السيكوباتية (خاصة إذا حاولت الاستفادة من الاختراق) ، أو الشخصيات التي تشعر بالدونية وتريد تحقيق انتصار إلكتروني يعوضها عن تلك المشاعر المؤلمة . وقد يلجأ إليه بعض العباقرة الصغار حين يكتشفون قدرتهم الفائقة على فك الشفرات والدخول على المواقع السرية ، وهذا ما عكسته (وربما شجعت عليه) بعض الأفلام الأجنبية .

2 - الخداع : ويزيد من احتمالات الخداع حالة التخفي التي يتيحها التواصل الإلكتروني ، فقد يتحدث إليك شاب على أنه فتاة والعكس ، وقد تحدثك امرأة عجوز على أنها فتاة مراهقة ، وينبني على كل هذا تكوين صورة ذهنية معينة عن الطرف المخاور قد تكون مخالفة تماما لحقيقته ، وقد ينبني على هذه الصورة الذهنية مشاعر معينة كالحب مثلا أو الصداقة ، ولكن حين تتيح الظروف لمواجهة حقيقية في الواقع فسيختلف الأمر تماما حيث تظهر عملية الخداع والتضليل ، وتكون صدمة لأحد الطرفين (خاصة المخدوع) أو كليهما . وقد يتضمن الخداع معاملات مادية ونصب واحتيال وصفقات وهمية يتورط فيها أصحاب النوايا الحسنة أو السذج من الناس .

3 - السطو : وذلك من خلال السطو على مواد علمية أو أدبية أو فنية وادعاء ملكيتها خاصة أنه لا توجد حتى الآن قوانين واضحة لحماية الملكية الفكرية الإلكترونية حيث أن إثبات هذه الملكية يكون صعبا للغاية في هذه الحالة نظرا لمرونة الإضافة والحذف والتغيير لما ينشر من مواد على الشبكة الإلكترونية .

4 - الفيرسة والتدمير : وهي إصابة بريد إلكتروني أو موقع بفيروس معين ، وقد يكون هذا الفعل بهدف التسلية أو بهدف العدوان أو بهدف الإحساس بالقدرة على السيطرة والتأثير في الآخرين ، وقد يكون هذا الفعل موجها لأشخاص معينين معروفين لهذا الشخص (مهدف إغاظتهم أو السخرية منهم أو مداعبتهم أو إظهار التفوق عليهم) ، أو قد يمارس هذه العملية على نطاق واسع تجاه عدد هائل من الناس يستدرجهم هذا الشخص برسالة تنثير الفضول أو بصورة عارية أو مشهد جنسي وعند استقبال هذه الرسالة تتم عملية الفيرسة فتدمر البرامج لدى الشخص المستهدف ، ولا تخفى هنا دوافع العبث والعدوان لدى من يقومون بهذا السلوك إضافة إلى أساليب الخداع والتمويه .

5- الإغواء والإستعراء : وهذه الجريمة تتصل بالرغبات الجنسية وتفرعاتها حيث يمارس بعض الناس عمليات إغواء من خلال إرسال صور أو مشاهد جنسية إلى ضحاياهم للسيطرة عليهم أو اجتذابهم أو التسلي بهم أو ابتزازهم أو إثارة رغبتهم ، أو يمارسون الإستعراء من خلال الحديث الصريح والمكشوف (جدا) عن مشاعر أو ممارسات جنسية ، وهذا الإغواء والإستعراء قد يكشف عن ميول جنسية مثلية إن كان موجها لنفس الجنس ، أما إن كان موجها للجنس الآخر فهو يحمل في طياته رغبة في الاستعراض والاستمتاع بمشاهد الدهشة أو الاستغراب أو الخجل أو الإثارة البادية على الطرف الآخر، وهذا العمل قد يقوم به شخص أو تقوم به مواقع كاملة ، وقد يكون وراءه أهداف ربح مادي وقد يكون مجرد التسلية والتعبير عن الرغبات الجنسية الكامنة سواء كانت مثلية أو غيرية .

6 - الشائعات : وتبدأ برسالة إلكترونية واحدة ثم ما تلبث أن تصل للآلاف بل أحيانا للملايين من الناس بسبب سرعة ومرونة التواصل الإلكتروني ، والشائعة قد تهدف إلى تغيير معين في اتجاهات الناس نحو شيء أو شخص معين بهدف النيل منه أو الضغط عليه، أو إثارة البلبلة تجاه قضايا معينة .

7 - العنصرية : حيث تمارس مجموعة أو مجموعات من الناس حربا إعلامية على الإنترنت ضد مجموعة أخرى من الناس عبر الرسائل الإلكترونية بحيث تشكل رأيا عاما ضدها أو تحط من شأنها أو تشوه صورتها . وقد يكون هذا عملا منظما تحركه بعض الجهات أو يكون تعبيرا عن صراعات ثقافية بين الشعوب يعجزون عن التعبير عنها في الحياة العادية إما خوفا من المواجهة المباشرة أو خوفا من الملاحقة والمساءلة القانونية لذلك يلجئون إلى الوسيلة السرية التي لا يستطيع القانون اكتشافها وملاحقتها حتى الآن .

8 - تبادل الرسائل المشفرة بين أفراد العصابات والجماعات : فكثير من العصابات والجماعات تستفيد من الشبكة العنكبوتية لتبادل الرسائل المشفرة ، وهذا يحميها من التتبع الأمني أو السياسي ، وقد تصدر الأوامر الجماعية لأعضائها على مستوى العالم في لحظة دون أن ينتبه لذلك أحد ، وهذا يساعد كثيرا على تفشي الجريمة المنظمة ، أو الأعمال التي تحتاج لتواصل سريع وسري ومنظم . فقد كشف تقرير نشر مؤخرا حول تطور مفهوم الجريمة عبر الإنترنت أن تلك الصورة التقليدية التي يرسمها البعض لأنماط الجريمة الإلكترونية وأشكالها قد طرأ عليها العديد من التطورات ، وأبدع مخطوطها في ابتكار أساليب تستعصي على الاكتشاف والملاحقة لمركبيها (1).

المطلب الثاني: أنواع وأشكال الجريمة الالكترونية

من الصعوبة تماماً حصر الجريمة الالكترونية حيث أن أشكالها متعددة ومتنوعة وهي تزداد تنوعاً وتعددًا كلما أوغل العالم في استخدام الحاسب الآلي وشبكة الانترنت ،ويمكن تقسيم أنواع الجريمة الالكترونية إلى أربع مجموعات :

المجموعة الأولى :وتشمل الجرائم التي يتم فيها استخدام الكمبيوتر بشكل غير قانوني من قبل الأفراد المرخص لهم باستعماله .

المجموعة الثانية :وتتضمن الجرائم التي يتم من خلالها اختراق الكمبيوتر لتدمير البرامج والبيانات الموجودة في الملفات المخزنة عليه، وتدخل ضمن الفيروسات الالكترونية .

المجموعة الثالثة :تشمل الجرائم التي فيها استخدام الكمبيوتر لارتكاب جريمة معينة أو التخطيط لها .

المجموعة الرابعة :وتشمل الجرائم التي تتمثل في استغلال البيانات المخزنة على الكمبيوتر بشكل غير قانوني .

ونفس التصنيف ينسحب للفاعل الجنائي، فيمكن أيضاً تصنيف الجرم الالكتروني في أربع فئات رئيسية وهي :

الفئة الأولى :الأفراد الذين يعملون في مجال الجريمة المنظمة عبر استخدام الكمبيوتر.

الفئة الثانية :الموظفون الساخطون على مؤسساتهم أو شركاتهم والذين يستغلون معرفتهم بأنظمة الحاسب الآلي في شركاتهم وسيلة لإيقاع الضرر بهم عبر نشر البيانات أو استعمالها أو مسحها **الفئة الثالثة** :الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي الجرائم الالكترونية وذلك بحكم سهولة اتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية.

الفئة الرابعة : فئة العابثين مثل الهاكرز أو الكراكرز (crackers) وهم الذين يستغلون الكمبيوتر من أجل التسلية في أمور غير قانونية وليس بغرض التخريب .

وتحدث الجريمة الالكترونية عادة في إحدى ثلاث مراحل هي :

المرحلة الأولى :مرحلة إدخال البيانات، ومن ذلك على سبيل المثال قيام الجرم الالكتروني بتغيير أو تزوير البيانات مثل التسلل الالكتروني إلى البيانات المتعلقة بفاتورة الهاتف قبل طبعها في شكلها النهائي بحيث يتمكن من حذف بعض المكالمات من الفاتورة قبل طباعتها وإرسالها، ومثل قيام أحد الطلاب بتغيير درجاته المسجلة على الكمبيوتر في مادة معينة أو تغيير تقديره الفصلي أو العام

المرحلة الثانية :مرحلة تشغيل البيانات كقيام الجرم الالكتروني بتغيير أو تعديل البرامج الجاهزة (soft

wear) التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة بطريق غير شرعي من قبل الجاني، ومن ذلك مثلاً استخدام برنامج معين لتقريب الأرقام المتعلقة بالعمولات البنكية على حساب أحد الأشخاص، أو تجميع الفروق بين الأرقام المقربة والأرقام الفعلية وإضافتها لحساب سري آخر لنفس العميل.. وقد تبدو هذه الفروق بسيطة ولكنها ستكون كبيرة إذا تمت إضافتها خلال عدة سنوات .

المرحلة الثالثة :مرحلة إخراج البيانات، ومثل ذلك سرقة بعض البيانات الالكترونية أو المعلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات (2).

المطلب الثالث:تصنيف أهداف الجريمة الالكترونية :

يمكن حصر أهداف الجريمة الالكترونية إلى ما يلي:

1 - الوصول إلى المعلومات بشكل غير قانوني ، كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف الجرم

2 - الولوج إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها وعادة ما تتم هذه العملية على مواقع الانترنت .

3 - التمكن من معلومات عن عناوين مواقع الانترنت للمؤسسات العامة بهدف تغييرها وتخريبها وابتزازها .

4 - الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الابتزاز كالبثوث والدوائر الحكومية والأجهزة الرسمية والشركات بكافة إشكالها .

5 - الاستفادة من تقنية المعلومات من اجل كسب مادي أو معنوي أو سياسي غير مشروع كعمليات تزوير بطاقات الائتمان وعمليات اختراق مواقع الكترونية على الشبكة العنكبوتية ،أو التخطيط والتواصل للجريمة عبر الوطنية...الخ

6 - استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة أو نشر الأفكار التي يمكن أن تؤسس إلى فكر تكفيري وهذا ما هو معمول به من القاعدة(3).

المبحث الثاني: خطر وضرر الجريمة الالكترونية:

المطلب الأول :الفئات الأكثر تضررا:

الفئة الأول :الأطفال أول المتأثرين :

يقول الدكتور رياض إبراهيم أستاذ علم الاجتماع أن استخدام الانترنت قد تكون له تأثيرات على العلاقات الاجتماعية ، وإن أول هذه التأثيرات تظهر عند الأطفال تحت سن العاشرة إذ تبين أن الانترنت يؤدي إلى عزل الطفل اجتماعيا وعدم تفاعله مع بقية أفراد أسرته ، وبقية الأقران والأصدقاء مما يفقده ظرف بناء المهارات اللازمة للتفاعل مع الآخرين ويحد من امتداد جسور التواصل والتلاحق مع الغير.

إن وجود الانترنت قد افقد الوحدات التقليدية أو ما يعرف بمؤسسات التنشئة التي كانت مسئولة عن تنشئة الإنسان كثيرا من وظائفها وأهميتها فأصبح الانترنت مصدرا أساسيا في عملية التنشئة .ولذلك تفرض أهمية المراقبة والمتابعة.

أهمية المراقبة :

ويبحث عدد من الباحثين في مجال علم النفس والتربية على ضرورة مراقبة مضامين الانترنت من قبل الأسرة للتأكد من ضبط الجانب السلبي الذي يمكن أن تحمله تلك المضامين ،إذ أن الانترنت أصبح بديلا للتفاعل الاجتماعي الصحي مع الرفاق والأقارب ، كما إن قضاء الأشخاص ساعات الطويلة في استكشاف مواقع الانترنت المتعددة يعني تغيرا في منظومة القيم الاجتماعية للأفراد حيث يعزز هذا الاستخدام المفرط القيم الفردية

بدلاً من القيم الاجتماعية وقيم العمل الجماعي المشترك ، وهي التي تمثل عنصراً هاماً في ثقافتنا ، ويسبب في الوحدة.

* الميل إلى الانعزال:

إن الاستخدام الفردي للانترنت يعزز الرغبة والميل للوحدة والعزلة للمراهقين والشباب مما يقلل من فرص التفاعل والنمو الاجتماعي والانفعالي الصحي الذي لا يقل أهمية عن النمو المعرفي وحب الاستطلاع والاستكشاف . و تشير بعض الدراسات إلى أن استخدام الانترنت يعرض الأطفال والمراهقين إلى مواد ومعلومات خيالية وغير واقعية تساهم في إعاقه تفكيرهم وتكيفهم وينمي بعض الأفكار غير العقلانية خصوصاً ما يتصل منها بنمط العلاقات الشخصية وأنماط الحياة والعادات والتقاليد السائدة في المجتمعات الأخرى مؤدياً إلى تدمير نسيج الموروث الاجتماعي الوطني، وهذا ما يتجلى في بروز ضغط رهيب على مستعملي الانترنت (4).

* مصدر للضغط النفسي :

إن استخدام الانترنت أصبح يشكل مصدراً للضغط النفسي والاجتماعي والاقتصادي على الأفراد بسبب تعرض فرد غير المنتمي إلى ثقافة الانترنت للنقد من رفاقه لعدم مواكبته لعناصر هذه الثقافة ناهيك عن كون استخدام الانترنت ممارسة قد تكون مكلفة مادياً خصوصاً للأفراد محدودي الدخل ، ويرى الباحثون أن دخول الانترنت مجالات الحياة الواسعة أصبح عاملاً مساعداً في تقوية الفجوة بين الأجيال فيما يتعلق بثقافة الاتصال مع العالم الخارجي.

● الضرر الأكبر :

أما مستخدمو الانترنت فتفاوتت تقييماتهم لمنافع ومضار الانترنت، فيرى البعض أن استخدام الانترنت يؤثر على العلاقات الاجتماعية ، خاصة الذين يقضون ساعتين فأكثر يومياً في استخدام الانترنت ، إن الوقت المخصص لعلاقتهم مع أسرهم وأصدقائهم يقل تدريجياً ويزداد في المقابل الوقت برفقة جهاز الكمبيوتر.

ففي دراسة تحت عنوان واقع مقاهي الانترنت في مدينة الرياض للدكتور إبراهيم بن سعد الجماد وزملاؤه فقد تحدثت عن أهمية الانترنت وكونه خدمة حيوية وضرورية في عصر التقدم العلمي والتقني وقد أدى الاتصال بالشبكة العالمية (الانترنت) إلى شيوع أنماط جديدة من السلوكيات والقيم والأفكار التي تساهم بشكل كبير في التأثير على المجتمع بشكل عام سواء كان سلبياً أو إيجابياً. و توصلت الدراسة إلى نتائج وتوصيات منها :

- (1) - تنبه إدارة المقهى المرتادين إلى عدم استخدام البريد الإلكتروني لتبادل أي معلومات تتعارض مع الدين وأنظمة الدولة بنسبة 24 بالمائة.
- () - تحت إدارة المقهى المرتادين إلى احترام حقوق النشر والبراءة الفكرية بنسبة 32 % .
- (3) - تحت إدارة المقهى المرتادين من المواقع التي تتضمن القذح أو التشهير بالآخرين بنسبة 35 % (5).

الفئة الثانية: الشباب أكثر إغواء

إن زيادة نسبة جرائم استخدامات الشباب للإنترنت، وتنوع أساليبها وتعدد اتجاهاتها زاد من أخطارها على الأمن القومي لدى الدول ، حيث تحولت هذه الجرائم من مجرد انتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة ينخرط فيها الكثير ممن تتوافر لديهم المهارة والمعرفة في مجال الحاسبات ، ولا شك أن تلك الأنماط من الجرائم تزداد علي مستوى كافة الدول مما يستدعي التعامل معها علي المستوى الفني والقانوني والاجتماعي .

ولعل فئة الشباب والمراهقين هي الفئة الأكثر تعرضاً للإنترنت ، والتي أصبحت الشغل الشاغل لهم يتابعون ما تقدمه من أفكار منحرفة ومذاهب هدامة ، وأنماط سلوكية تتنافى مع مبادئنا وقيمنا وتقاليدنا ، ولا يقرها شرعنا الحنيف مما يحتم علينا مواجهة هذا الخطر والتصدي له ، وقد أوضحت الدراسات والتقارير أن أكثر المستخدمين للمواد الإباحية على الإنترنت كانت من الشباب والشابات والمراهقين والمراهقات ، بل الأدهى والأمر أن ذلك يتم في غفلة من أولياء الأمور، ومن ثمة جاءت أهمية الكشف عن دور الأسرة وتنبيه أولياء الأمور لمواجهة ووقاية الأبناء من الجرائم الناجمة عن الاستخدامات السلبية لشبكة الإنترنت . إن القدرات والفرص التي تؤمنها شبكة الإنترنت طورت العديد من النشاطات التجارية المشروعة من خلال زيادة سرعة وسهولة ومجالات إجراء المعاملات إضافة إلى تخفيض الكثير من النفقات . ولقد اكتشف المجرمون أيضاً أن شبكة الإنترنت تستطيع أن تؤمن فرصاً جديدة وفوائد متضاعفة للأعمال غير المشروعة(6).

المطلب الثاني: صور ونماذج من الجرائم الإلكترونية:

فالجانب المظلم من الإنترنت لا يشمل فقط الاحتيال والسرقة ، ونشر المواد الإباحية ، وشبكات المنحرفين جنسياً ممن يستهدفون الأحداث ، بل أيضاً منظمات الاتجار بالمخدرات والمنظمات الإجرامية التي تركز على استغلال ما توفره الشبكات الإلكترونية من تسهيلات وفرص أكثر مما تركز على تعطيل عمل الشبكات كما يفعل الآخرون المهتمون بهذا الأمر ، في عالم الشبكات الإلكترونية ، كما في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة ، وقد يكون أفضل ما توصف به هذه الأعمال بأنها جرائم غير منظمة ، رغم ذلك هناك أدلة متزايدة على أن مجموعات الجريمة المنظمة تستغل الفرص الجديدة التي توفرها

شبكة الانترنت ، ولن تصبح الجريمة المنظمة مترادفة و مساوية للجريمة التي تُرتكب من خلال الشبكات الإلكترونية ، فمعظم مجموعات الجريمة المنظمة ستواصل العمل في العالم الحقيقي بدلاً من عالم الشبكات الإلكترونية ، ومعظم الجرائم التي تقع في هذا المجال يرتكبها أفراد لا منظمات إجرامية ومع ذلك، من المحتمل أن يزداد مقدار التداخل بين الظاهرتين بدرجة كبيرة خلال السنوات القليلة القادمة حيث أن مستخدمي الشبكة في البلاد العربية 52 مليوناً نهاية السنة ... وعليه بات الدخول في الشبكة العنكبوتية «مخاطرة» بعد انتشار الجرائم الإلكترونية مثل النصب والتجسس وغسل الأموال وتزوير بطاقات الائتمان وتسريب المواد الإباحية ودعارة الأطفال والتشهير واقتحام الحواسيب الخاصة والدخول إلى البريد الإلكتروني للجمهور وانتحال الهوية وغيرها. وكشفت دراسات قدمت في مؤتمر متخصص استضافته القاهرة مؤخراً ، أن جريمة واحدة تحدث كل ثلاث دقائق على الانترنت التي تضم 500 مليون موقع وأكثر من 15 بليون صفحة وملايين قواعد المعلومات وغيرها. ويقدر الخبراء قيمة الخسائر المادية للاعتداءات على حقوق الملكية الفكرية بنحو 72 بليون دولار سنوياً. ولعل أهم خطر وضرر يترصد هو تهديد سيادة الدول .

لقد سعى خبراء في القضاء والأمن والاجتماع لاستنباط طرق تحدّ من انتشار جرائم المعلوماتية ، التي تؤثر أيضاً في سيادة الدول لأنها تصدر من فاعلين «عابرين للأوطان» بحيث تضرب أيديهم شبكة «الويب» التي لا تعترف بالحدود الجغرافية .

ويقول خبراء مكافحة الجرائم الدولية والأنتربول أن هناك تطورا ملحوظا طرأ على أساليب جرائم الإنترنت التقليدية والتي تشمل صناعة ونشر الفيروسات ، الاختراقات ، تعطيل الأجهزة ، انتحال الشخصية ، المضايقة والملاحقة ، التغيرير والاستدراج ، التشهير وتشويه السمعة ، صناعة ونشر الإباحية ، وجرائم النصب والاحتيال.

وهذه الجرائم الالكترونية تكلف الاقتصاد الأمريكي على سبيل المثال ما يقارب (250) مليار دولار سنوياً، أي ما يعادل ميزانيات أغلب دول العالم الثالث تقريباً، بسبب عمليات القرصنة الالكترونية من نسخ برامج أو أفلام أو مواد موسيقية أو بسبب هجمات تعطيل المواقع، وقد قالت السلطات الاتحادية في الولايات المتحدة الأمريكية إن جرائم الاحتيال عبر الانترنت التي تم إبلاغ السلطات الأمريكية عنها زادت بنسبة 33 بالمائة العام الماضي، وذلك في أول ارتفاع لها خلال ثلاث سنوات، وهي ترتفع هذا العام مع تفاقم أزمة الركود الاقتصادي. وارتفعت خسائر الاحتيال عبر الانترنت في الولايات المتحدة إلى رقم قياسي 264.6 مليون دولار في 2008 وفقا لما ورد في تقرير عن مركز شكاوى الاحتيال عبر الانترنت، الذي يديره مكتب التحقيقات الفيدرالي والمركز الوطني لجرائم ذوي الياقات البيضاء. وتزايد جرائم الاحتيال التي يكون مصدرها من مختلف أنحاء العالم - في الأغلب من الولايات المتحدة وكندا وبريطانيا ونيجيريا والصين - هذا العام مع زيادة نسبتها 50 بالمائة تقريبا في الشكاوى التي تم إبلاغ السلطات الأمريكية عنها في مارس فقط. وقال جون

كاني الذي وضع التقرير للصحفيين في إفادة هاتفية "2009 يتجه لأن يكون عاما مزدحما جدا في مجال الجريمة الالكترونية." وبلغت الخسائر بسبب جرائم الاحتيال على الانترنت 239.1 مليون دولار عام 2007 وكانت تبلغ 18 مليون دولار فقط في 2001. ووفقا للتقرير فإن الشكوى الأكثر شيوعا في 2008 كانت عدم توصيل البضائع المشتراة عبر الانترنت تلتها المزايدات الوهمية ثم الاحتيال ببطاقات الائتمان والاحتيال بزعم الاستثمار(7).

ويمكن القول ببساطة أن الانترنت ستكون ساحة إجرام مثالية تتحدى الأجهزة الأمنية والقضائية بثغرات قانونية ضخمة، فيمكن حالياً القيام بعملية احتيال انترناتية ترتكب بين أستراليا وكندا بينما المنفذون الحقيقيون موجودون في لندن أو ساوباولو أو في وسط قرية هندية أو على أطراف غابة استوائية، وهذا الأمر يثير مشاكل قانونية مثل الاختصاص القضائي والإثبات، ومازالت الأجهزة القضائية وأساتذة القانون في العالم، دون استثناء عاجزين عن الخروج بتصور واضح عن الجريمة الالكترونية وتفرعاتها الكثيرة المختلفة، وإن كانت الأنظمة القانونية المختلفة تحاول إيجاد وتأسيس أرضية قانونية واضحة للجرائم الالكترونية. ونستذكر في هذا المجال المجرم تيم كورادو أشهر لصوص البطاقات الائتمانية على شبكة الانترنت الذي لا يزال حراً طليقاً لأنه كلما اقتادته الشرطة إلى المحكمة كلما ازدادت ضحكته ذلك لأنه لا يوجد دليل واحد ضده، فقد قام هذا البريطاني باقتحام عشرات المواقع في شبكة الانترنت واستولى على أرقام وبيانات ما يزيد على (124) ألف بطاقة ائتمانية تخص عملاء هذه المواقع، وقام بنشر أرقامها وبياناتها على شبكة الانترنت، وقام أيضاً بإرسال بعض بيانات هذه البطاقات إلى بعض المواقع الشخصية لأفراد آخرين لا يعرفهم ولا يعرفونه، وقال (تيم كورادو) حين إلقاء القبض عليه للمرة الأولى، أن رهان رجال الشرطة ضده هو رهان خاسر لأنهم لا يملكون دليلاً واحداً ضده، وقال أيضاً أن هدف من قام بهذه العمليات التي يتهم بها هو إيقاظ الشركات التجارية التي يوجد لها مواقع على شبكة الانترنت من سباتها العميق ودفعها لانجاز المزيد من إجراءات الحماية لمواقعها الالكترونية وبالتالي حماية أموال زبائنهم، وأفلت كورادو من العقاب بسبب واحد وهو أن الموقع الذي تقول الشرطة انه استعمله في عملياته مسجل في شركة (Great solution) التي يوجد مقرها في مقاطعة ويلز البريطانية، ولكن كل البيانات الموجودة في هذا الموقع لا تدل أبداً على أي شيء يتعلق بشخصية تيم كورادو. حيث أن هذه الأنماط لم تعد هي الأشكال الوحيدة للجريمة عبر الإنترنت.

كما أن الإنترنت أيضاً لعبت دوراً أكثر خطورة عن طريق التشجيع على الانتحار، فنشير إلى دخول الانترنت ساحات جرائم القتل والاعتصاب أيضاً ، عن طريق عصابات دولية أنشأت مواقع تعرض من خلالها خدماتها لمن يريد تصفية الخصوم أو إذلالهم و إهانتهم عن طريق اغتصاب زوجاتهم أو بناتهم!.

وتؤكد إحدى منظمات مكافحة جرائم الشبكة الأوروبية أن إحدى هذه العصابات حققت أرباحا هائلة من وراء أنشطتها الإجرامية ، ويقدر التقرير أرباح هذا الموقع بـ 3.6 مليون يورو خلال سنتين فقط ، مقابل 58% من الجرائم التي تم اكتشافها !.

ففي مصر اكتشفت الشرطة أن إحدى هذه العصابات وراء لغز اختفاء طفل كان قد حير أجهزة البحث طويلا ، حيث قامت أمه الأمريكية بتأجير محترفين عبر الإنترنت لاختطاف ابنها من مصر وإحضاره بجواز سفر مزور إلى أمريكا انتقاما من والده الذي طلقها وحصل على حكم قضائي بحضانة الطفل. وتشير المعلومات إلى أن هذه الأنشطة لم تعد تمارس من وراء الستار كما كان الحال سابقا، حيث كانت العصابات تضطر إلى التخفي وتمارس نشاطها عبر مواقع الزواج أو غرف الدردشة ، فقد أصبحت الآن تعرض خدماتها عيانا بيانا وتحصل على المقابل عن طريق الدفع بالفيزا كارد، وإن تعذر ذلك بسبب كثافة الملاحقة الأمنية، فيمكن الاتفاق على وسائل أخرى، وقد سجل العام الماضي نشاطا تجاريا من هذا النوع حجمه 500 مليون يورو.

ويعرض أحد هذه المواقع "في جنوب أفريقيا" خدمات القتل والاختطاف للزبائن من رواده ، ويؤكد أن لديه أعضاء مدربين جيدا على القيام بعمليات التصفية الجسدية دون ترك أي آثار، تدل فرق البحث إلى مرتكب الجريمة، ويؤكد الموقع أن خطط تنفيذ الجرائم لا يضعها أشخاص عاديون، بل هم خبراء في هذا النوع من التخطيط ، ومعظمهم من رجال الشرطة والمخابرات السابقين!! . وتصل تسعيرة الرأس المراد "ذبحها" طبقا لهذا الموقع إلى 5 آلاف دولار للشخص العادي الذي يقع في المحيط الجغرافي، بينما قد يصل الثمن إلى 50 ألف دولار إذا كان مكان تنفيذ الجريمة بعيدا، أما الشخصيات البارزة فيصل سعر رأسها إلى 100 ألف دولار، وقد يرتفع الثمن إلى أكثر من ذلك حسب التكاليف!!، ويشير تقرير آخر إلى أن هناك أيضا مواقع يديرها أشخاص محترفون لحساب أنفسهم، وليس عصابات، فقد اعتقلت الشرطة في كوريا الجنوبية شابا جامعا بسبب إدارته لموقع يقدم فيه خدمات القتل بالأجر، وقد تقاضى في آخر عملية 9 آلاف دولار فقط من سيدة لا يعرفها مقابل قتل صديقها السابق وزوجته، وقد تم اكتشاف طلبات أخرى على موقعه منها الاغتصاب وتهريب السلاح، أما أطرف ما وجدته الشرطة في بريده الإلكتروني فهو طلب من مراهق، يطلب فيه التخلص من والده وزوجته، واعد القاتل المحترف بإعطائه 90% من أموال التأمين الذي كان سيحصل عليه بعد وفاة والده! (8).

أما ما عانته صحفية مشهورة سقطت ضحية الابتزاز الرخيص عبر الإنترنت فقد شهدت جرائم الإنترنت واقعة مؤسفة عندما تعرضت إحدى الصحفيات الشهيرات بصحيفة كبرى لجريمة سب وقذف تكاد أن تدمر حياتها تماما... فقد انشئوا لها موقعا يدعو إلى ممارسة الرذيلة حيث التقط لها شخص مجهول صورا وقام بتركيب وجهها على أجساد عارية ثم صمم موقعا عبر شبكة الإنترنت يعلن عن رغبتها في ممارسة الجنس مع راغي

المتعة الحرام بمقابل مادي، ولم تكن السيدة تدرى شيئاً عن هذا الأمر حتى فوجئت بجرس هاتف منزلها لا يتوقف عن الرنين، وتجد من يطلب منها تحديد موعد للقائهما الغرامي فظنت أن هناك لبس في بداية الأمر حتى أخبرها أحدهم من الخارج انه شاهد موقعها وفتن بصورها العارية لذا قرر الحضور إلى مصر لمشاركتها بعض الليالي ، وهنا كادت أن تفقد صوابها ، وأصبحت بأزمة نفسية سيئة هرعت على أثرها لرجال الإدارة العامة لمباحث المعلومات والتوثيق بوزارة الداخلية تستغيث لنجدتها وهنا كان لابد من وجود تنسيق بين وزارة الاتصالات المصرية ووزارات الدول الأخرى حيث تبين أن مصمم الموقع استخدم حاسب آلي مرتبط بهاتف متواجد بدولة الإمارات العربية ومرات محددة استخدم هاتفه بالخلترا(9). وهكذا يتضح بصورة أكيدة دخول هذه الجرائم عالمنا العربي؟؟؟!. وهو للأسف الشديد ما تؤكد مختلف التقارير الأمنية.

المطلب الثالث: الأساليب والأدوات المستخدمة في الجريمة الالكترونية وسبل التصدي لها:

الفرع الأول: الأساليب الإجرامية المستعملة في الجريمة:

نذكر: ولتحقيق هذه الأهداف يعتمد الفاعلون لهذه العمليات على عدة أساليب وأدوات وكمثال علي ذلك (أ)- صناعة ونشر الفيروسات وهذه تعد الجرائم الأكثر تأثيراً وانتشاراً معتمدة في أكثر الأحيان على شبكة الانترنت التي أصبحت تدخل في أعمالنا وبيوتنا وحياتنا اليومية، وتؤدي إلى تحقيق بعض أهداف الجريمة الالكترونية كحذف المعلومات أو تعديلها أو نقلها إلى أجهزة أخرى وإحداث بلبلة وخسائر اقتصادية ومادية كبيرة وتعطيل الأجهزة وعمل المؤسسات بكافة أنواعها.

(ب)- حضان طروادة وهو البرنامج الذي يقوم على توفير مدخل للمخترقين إلى أجهزة تحتوي معلومات غير مصرح لهم بالولوج إليها ولا يتطلب استخدام هذا النوع من البرامج إلى خبرات تقنية لتحقيق الهدف، ويكثر استخدام هذا الأسلوب على مواقع الانترنت بحيث يقوم المخترق بتعديل أو تغيير المعلومات الموجودة في الموقع بما يخدم هدفه.

(ج)- إيقاف خدمات الخادما من خلال إغراق أجهزة الخادما في المؤسسات (وخاصة تلك المرتبطة في الانترنت) بعدد هائل من طلبات التشكيك مما يؤدي إلى إيقاف عملها وتحقق الخسائر التي يهدف إليها القائم بهذا العمل.

(د)- انتحال الشخصية وهي جريمة العصر والتي تقوم على مبدأ انتحال شخصية أخرى والقيام بممارسات وأعمال غير مشروعة أو استخدام هوية الشخص الضحية لتحقيق استفادة مادية بطريقة تجعل من الصعب اكتشاف الفاعل الحقيقي.

(ه)- الملاحقة والمضايقة والابتزاز والتغريب باستخدام أساليب عدة مما ذكر وعادة ما يكون الضحية من قليلي الخبرة أو المعرفة الالكترونية أو من الأطفال أو النساء وتستخدم أيضاً لهذا الهدف مواقع المواعدة على الانترنت أو البرامج الحوارية.

(و)- تشويه السمعة وذلك بنشر معلومات حصل عليها الجرم بطريقة غير مشروعة أو معلومات مغلوطة وتهدف إلى كسب مادي أو سياسي أو اجتماعي معين .

ويواجه الإنسان العصري العديد من المغريات التي تشغله يوماً بعد يوم عن العلاقات الاجتماعية حتى أصبح التندر "بأيام زمان" وضرب المثل بها من العوامل المشتركة في كثير من المجالس ، وعلى الرغم من كثرة الأمور التي تشغلنا عن حياتنا الاجتماعية في عصرنا الحالي إلا أن أكثرها تأثيراً هو الانترنت .

الفرع الثاني :الإجراءات والخطوات العملية لمكافحة هذه الظاهرة:

للإجابة عن السؤال المطروح المتضمن الخطوات والإجراءات اللازمة للحد من الجرائم الالكترونية.. نحدد عدداً من هذه الإجراءات وهي:

- القيام بمزيد من برامج التوعية والتثقيف وإعلاء القيم الأخلاقية.. ويجب أن تقوم المؤسسات والهيئات بتوعية العاملين بها بهذه الجريمة.

- تكثيف أعمال الرقابة والسيطرة لكشف المنحرفين ومنع المخربين والتنسيق بين مسؤولي الاتصالات والأمن.

* التنسيق بين التشريعات الوطنية في دول العالم المختلفة فيجب أن تتعاون الدول لمحاربة الإجرام الالكتروني.

* لا بد أن نشير إلى جهود المنظمات الدولية للوصول إلى اتجاه متناسق في التشريع ومنها مجلس أوروبا.

* ضرورة تزويد سلطات التحقيق بوحدات متخصصة تساعد على استجلاء الحقيقة التي تقود إلى كشف الجريمة الالكترونية ومعرفة مرتكبيها نظراً لصعوبة البحث والاستدلال.

* يجب معالجة المشاكل التي تثار عند وقوع الجريمة بين عدة عدول.

* بحث قيمة المحررات الالكترونية في الاثبات.

صياغة أحندة عمل في هذا المجال يشارك فيها خبراء مكافحة الجريمة الالكترونية لإعداد الكوادر المؤهلة.. ودعوة الخبراء لمناقشة استحداث آليات لمكافحة الجريمة..

كما نقترح إنشاء مجلس وطني تنسيقي يكون محور ارتكاز لحماية الخصوصية وتأمين الفضاء الالكتروني. ونقترح أيضاً إنشاء مركز متخصص لتأمين الشبكات المعلوماتية أسوة بما تم في الدول الأخرى حتى يقوم بالتنسيق مع العالم الخارجي في حالة الهجوم على البنية الالكترونية المصرية. مقال من جريدة الرياض بقلم خالد الطويل.

خاتمة : بعد استعراضنا لمختلف جوانب الظاهرة والتي بحق تعد جريمة عالمية والتي أصبحت تهدد عالمنا أجمع يمكن إدراج مجموعة من التوصيات والاقتراحات التي يمكن أن تحد من هذه الظاهرة والتي من بينها:

- 1- ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم .
- 2- تكثيف التنسيق والتعاون الدولي قضائيا وإجرائيا وتبادل الخبرات في مجال مكافحة الجرائم المعلوماتية .
- 3- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ، وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت .
- 4- تحيين تدريب رجال القضاء والشرطة القضائية بشأن التعامل مع أجهزة الحاسوب والإنترنت وجرائمهما .
- 5- الاسراع في تحيين منظومتنا وينبغي أن تنص تشريعتنا على اعتبار أن الانترنت يعتبر وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية ؛ مع الأخذ بعين الاعتبار أن الإنترنت أوسع انتشارا من سائر وسائل النشر والعلانية الأخرى .
- 6- يلزم تعديل قوانين ونظم الإجراءات الجزائية (الجنائية) ؛ بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني ؛ حتى يستمد الدليل مشروعيته . ويشترط في هذه الحالة أن يكون هذا الإجراء ضروريا، والقاعدة العامة - في هذا الشأن - الضرورة تقدر بقدرها .
- 7- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة .
- 8 - ضرورة النص صراحة في القوانين المنظمة للإثبات - الجنائي والمدني - بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والإنترنت في الإثبات ؛ طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة ، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير ؛ وبما يحقق مبدأ المواجهة بين الخصوم .
- 9- يتعين اعتبار نشر وطباعة الصور الجنسية عن طريق الانترنت مما يدخل ضمن زمرة جرائم الآداب .
- 10- ضرورة تجريم استخدام الأطفال في تصوير أفلام تمثلهم في أوضاع مخلة بالآداب العامة ؛ وعرضها على شبكة الإنترنت وباستخدام البريد الإلكتروني .
- 11-تنظيم نشاط مقاهي الانترنت ومراقبته من مراقبين مختصين في هذا الشأن.
- 12- يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية ؛ أو تغيير محتواه أو إعاقه الرسائل أو تحويلها عبر الإنترنت .
- 13- يتعين إتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم المعلوماتية ؛ وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم ؛ ولاسيما الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الإنترنت .

14- ضرورة نشر الوعي بين صفوف المواطنين - ولاسيما الشباب - بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت ؛ مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للإنترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة ومعاشرة البغايا ؛ وذلك بأسلوب غير مباشر من خلال المواد الدرامية .

15- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم.

16- إنشاء قسمٍ جديد بكمليات الحقوق بالجامعات الجزائرية لدراسة الجريمة الالكترونية، وتكريس قانون المعلوماتية والإنترنت أو (قانون الحاسب الآلي والإنترنت) في البرامج البيداغوجية في مختلف الجامعات .

17- تفعيل دور المجتمع المدني والهيئات والمؤسسات ولاسيما الجمعيات الجوارية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الانترنت .

18- من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية ؛ وخصوصا الإنترنت ؛ وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية .

19- نأمل - وفي الأمل رجاء - أن تسعى الدول ولاسيما العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الانترنت ، مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي ؛ ويا حبذا لو تم إنشاء شرطة عربية تهتم بمكافحة الجرائم المعلوماتية. سواء على مستوى الوقاية من هذه الجرائم ؛ وسواء على مستوى ملاحقة الجناة والتحقيق معهم ومحاكمتهم وإنزال العقاب بهم ويجذو جذو ما أتفق عليه وزراء الداخلية العرب في مكافحة الإرهاب ، باعتمادهم مخطط أمني ضد الإرهاب.

التهميش والمراجع:

1/ محمد أمين الرومي ، جرائم الكمبيوتر و الانترنت ، دار المطبوعات الجامعية - إسكندرية ، 2004

2/ <http://omanlover.org/vb/showthread.php?t=73178> على الساعة 21.25

3) محمد حمّاد مرهج الهيتي ، جرائم الحاسوب ، - دار المناهج ، عمان، 2006

4/ أ . محمد عبد الله أبو بكر سلامة ، موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت ، منشأة المعارف بالاسكندرية ، 2006

5/ محمد أمين الشوابكة ، جرائم الحاسوب و الإنترنت : الجريمة المعلوماتية ، دار الثقافة للنشر و التوزيع ،

عمان، 2007

6/ محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، - دار الثقافة للنشر و التوزيع ، عمان، 2005

7 / جريدة الفجر الجزائرية بتاريخ 2009/04/01

21.30 الساعة على <http://Hoo-net.Com/vb/nebvely.02/04/2009> /8

21.39 الساعة على <http://forum.stop55.com/13703.html> 02/04/2009/9