

تأثير تطور تكنولوجيا المعلوماتية على تنامي الجريمة

د. محمود شرقي

د. صلاح الدين جبار

جامعة لونيبي علي البليدة2

كلية الحقوق والعلوم السياسية

كلية الحقوق والعلوم السياسية

جامعة لونيبي علي البليدة2

ملخص:

يساهم التطور التكنولوجي في مجال المعلوماتية بطرق مختلفة وأساليب منها المعقدة والسهلة، في تطور اشكال الاجرام على كافة المستويات الاجتماعية والاقتصادية والثقافية والسياسية ...، ومما أضاف خطورة هذه التكنولوجيا هو تجاوزها للحدود الوطنية التقليدية وانتشار شبكاتها عالميا، ورغم ما تقدمه تكنولوجيا المعلومات من خدمات عديدة إيجابية للبشرية في جميع المجالات، وما حققت من انفتاح عالمي لم يسبق له مثيل من قبل ، في هذا المقال سوف نتناول الأجراء القانونية والوطنية الدولية التي بدأت تتسع دائرتها نظرا لكون الجريمة الالكترونية أصبحت عابرة للحدود، ولا تعترف بعنصر المكان والزمان، فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والجني عليهم وما نجم على هذا التطور من انعكاسات سلبية على الافراد والمجتمعات عبر العالم أجمع.

Sammur

The technological development in the field of IT (Information Technology) contributes in different complex and easy ways and methods, in the evolution of different forms of crime on all social, economic, cultural and political levels ... in addition to the seriousness of this technology, it overcome the traditional national borders and the proliferation of the golbal networks, despite what information technology offer as positive services for humanity in all areas, and achieved a global openness that is never seen before.

In this article, we will address the national and international legal proceedings, which began spraiding since the cyber-crime has become transboundary, and does not recognize the element of space and time, however it is characterized by geographical Baltbaeid and different timings between the perpetrator and victims, and the social and individual negative implications of this development on societies all over the world.

مقدمة :

إن الثورة التكنولوجية المعلوماتية قد أحدثت الكثير من التغيرات الأساسية في العالم فلا يكاد أي قطاع من قطاعات المجتمع يخلو من تغيير (سارة خلف، ماي 2010)، فتكنولوجيا المعلومات عمت تقريبا كل جانب من جوانب الأنشطة البشرية وأكثرها تطورا هو قطاع الاتصالات السلكية واللاسلكية. فقد أضحت الاتصالات أيسر بين البشر وأجهزة الكمبيوتر وهذا أدى إلى سهولة الحصول على المعلومات ، بالإضافة إلى إمكانيات غير محدودة عمليا لتبادلها ونشرها بغض النظر عن المسافات الجغرافية، وقد أدت هذه التطورات إلى ارتفاع لم يسبق له مثيل في التغيرات الاقتصادية والاجتماعية، ولكن هناك الجانب المظلم من هذا التطور وهو ظهور أنواع جديدة من الجريمة فضلا عن ارتكاب الجرائم التقليدية من خلال التكنولوجيات الجديدة وعلاوة على ذلك فإن الآثار المترتبة على السلوك الإجرامي تكون أبعد أثرا من ذي قبل لأنها لا تقتصر على قيود وطنية أو حدود جغرافية ، وقد أدى انتشار شبكة الانترنت والحاسب إلى فتح مجالات عديدة للاستفادة منها ولكن في نفس الوقت أدى إلى نشر ثقافة منافية لعادات وطبائع الكثير من المجتمعات وخصوصا العربية نتيجة للانفتاح الذي فرضته هذه التقنيات، وكذلك نتيجة

توفيرها المعلومات التي يمكن استخدامها فيما يحقق مصلحة للبشرية وأيضاً ما يحقق ضرراً لها، مؤسسة لانتشار نوع جديد من الجريمة وهو "الجريمة الالكترونية"، والجرائم الالكترونية تختلف عن أنواع الجرائم الأخرى في وسائلها وأهدافها إلا أن الضرر الناجم عنها لا يمكن فصله عن الأضرار الناجمة عن مختلف الجرائم الأخرى، من خلال ما تقدم سوف نحاول في هذا المقال الإجابة على الإشكالية الآتية: ما مدي ملائمة الإطار القانوني الوطني والدولي في مجال محاربة الجرائم الإلكترونية؟ وهل حققت اتفاقية بودابست (2001) لمكافحة الجريمة الالكترونية، الإطار الأمثل للتعاون الدولي حتى الآن ضد تنامي هذه الجرائم أولاً: تعريف الجريمة الإلكترونية.

تعرف الجريمة على أنها "ذلك النشاط الذي يصدر من الشخص إيجابياً كان أم سلبياً، ويقرر له القانون عقوبة من العقوبات المقررة في قانون العقوبات" (جلال الدين عبد الخالق والسيد رمضان، 2001، ص181).

كما تعرف من المنظور الشرعي أنها ارتكاب ما فيه مخالفة لأوامر الله تعالى أو نواهيه، بمعنى أن الجريمة سواء كان لها عقوبة دنيوية أم اقتضت على العقاب الآخرة (الجريمة النسوية في الجزائر)، أما من منظور السوسيولوجي فيعرفها راد كليف براون بأنها "انتهاك العرف السائد، مما يستوجب توقيع الجزاء على منتهكيه..." (جلال الدين عبد الخالق والسيد رمضان، المرجع السابق، ص184)، كما تعرف بأنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب (عمرو حسين عباس، 2008، ص70)، وتسمى الجرائم الالكترونية، الجرائم التي تلعب فيها البيانات التكنولوجية والبرامج المعلومات دوراً رئيسياً (يونس عرب، 2002)، وهي أية جريمة يكون متطلباً لاختراقها توافر لدى فاعلها معرفة تقنية الحاسوب (مناني فراح، 2010، ص23)، وتعرف بأنها كل فعل أو امتناع من شأنه الاعتداء على الأحوال المادية أو المعنوية يكون ناتجاً بطريقه مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية (معجل نبيل، ماي - 2011)، وباختصار، أي جريمة تنطوي على جهاز كمبيوتر وشبكة الانترنت، حيث أن أجهزة الكمبيوتر لعبت دوراً أساسياً في ارتكاب الجريمة مثل سرقة المعلومات وإرسال الفيروسات وابتكارها وسرقة أموال عن طريق المواقع الالكترونية للبنوك والشركات ومواقع البيع الوهمية والتجسس، أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة: فإن أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، من هذه التعريفات يعرفها الأستاذ جون فورستر وكذلك الأستاذ Esly D. Ball أنها: "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تاديمان Tiedemaun بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً، فالجريمة بمفهومها الواسع، فعلاً اجتماعياً صاحب السلوك الإنساني منذ بدء الخليقة، مما أعطى للفعل الإجرامي أبعاده التاريخية والدينية والتشريعية والعلمية.

ثانياً: خصائص السلوك الإجرامي:

يرى هول في دراسته "الخصائص العامة للقانون الجنائي" أنه للحكم على سلوك ما بأنه جريمة لابد من توفر سبع خصائص، تمثلت فيما يلي: (محمد سعدي، 2007، ص83).

- 1- الضرر هو المظهر الخارجي للسلوك، فالسلوك الإجرامي يؤدي إلى الإضرار بالمصالح الفردية أو الاجتماعية، أو بهما معاً.
- 2- يجب أن يكون هذا السلوك الضار محرماً قانوناً ومنصوصاً عليه في قانون العقوبات.
- 3- ضرورة وجود تصرف سواء كان إيجابياً أو سلبياً، عمدياً أو غير عمدي يؤدي إلى وقوع الضرر.
- 4- توافر القصد الجنائي، فالجريمة التي يرتكبها الإنسان العاقل عن قصد ورغبة وحرية، تختلف عن تلك التي يكره الإنسان عليها أو التي يرتكبها الطفل أو المجنون.
- 5- التوافق بين القصد الجنائي والتصرف حتى نميز مثلاً بين القتل الخطأ والقتل العمدى.

6- توافر العلاقة العلية بين القصد الجنائي والضرر.

7- يجب النص على عقوبة للفعل المجرم قانونا.

والجريمة هي كذلك كل انحراف عن المعايير الجماعية التي تتصف بقدر هائل من الجبرية و النوعية والكلية، و معنى هذا أنه لا يمكن أن تكون جريمة إلا إذا توافرت فيها الأركان الآتية: (ما هي الجريمة؟).

-القيمة التي تقدرها الجماعة وتحترمها؛

-انعزال حضاري أو ثقافي داخل طائفة من طوائف تلك الجماعة، فلا تعود تقدر تلك القيمة ولا تصبح مهمة لهم؛

-تجاه عدائي والضغط من جانب أولئك الذين يقدرون تلك القيمة الجمعية، ضد الذين لا يقدرونها.

ثالثا: خصائص الجريمة الإلكترونية. من أبرز خصائص وسمات الجرائم الالكترونية ما يلي:

1-سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية؛

2-صعوبة التحكم في تحديد حجم الضرر الناجم عنها قياسا بالجرائم التقليدية؛

3-مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا؛

4-تنطوي على سلوكيات غير مألوفة عن المجتمع؛

5-سهولة إتلاف الأدلة من قبل الجناة؛

6-جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والجني عليه.

رابعا: أهداف الجريمة الإلكترونية. يمكننا تصنيف أهداف الجريمة الالكترونية إلى التالي:

1-الوصول إلى المعلومات بشكل غير قانوني، كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم؛

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

3-الحصول على معلومات تغيير عناوين مواقع الانترنت بهدف التخريب على المؤسسات العامة وابتزازها.

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

5-الإستفادة من تقنية المعلومات من اجل كسب مادي أو معنوي أو سياسي غير مشروع كعمليات تزوير بطاقات الائتمان وعمليات اختراق مواقع الكترونية على الشبكة العنكبوتية

6-استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة أو نشر الأفكار التي يمكن أن تؤسس إلى فكر تكفيري (وليد عاكوم،

2009 ، ص 6).

ولتحقيق هذه الأهداف يعتمد القائمون بهذه العمليات على عدة أساليب وأدوات كمثال عليها:

1-صناعة ونشر الفيروسات وهذه تعد الجرائم الأكثر تأثيرا وانتشارا معتمدة في أكثر الأحيان على شبكة الانترنت التي أصبحت تدخل في أعمالنا 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؛

2-حصان 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؛

3- إيقاف خدمات الخادمتين من خلال إغراق أجهزة الخادمتين في المؤسسات (وخاصة تلك المرتبطة في الانترنت) بعدد هائل من طلبات التشكيك، مما يؤدي إلى إيقاف عملها وتحقق الحسائر التي يهدف إليها القائم بهذا العمل؛

4- 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 (عمرو حسين عباس، ص 21)؛

5- الملاحق والمضايقة والابتزاز والتغريب باستخدام أساليب عدة مما ذكر وعادة ما يكون الضحية من قبلي الخبرة أو المعرفة الالكترونية أو من الأطفال أو النساء وتستخدم أيضا لهذا الهدف مواقع المواعدة على الانترنت أو البرامج الحوارية؛

6- تشويه السمعة وذلك بنشر معلومات حصل عليها المجرم بطريقة غير مشروعة أو معلومات مغلوطة وتهدف إلى كسب مادي أو سياسي أو اجتماعي معين؛

7- النصب والاحتيال كبيع السلع أو الخدمات الوهمية أو سرقة معلومات بطاقات الائتمان واستخدامها وتوفر الانترنت مجالا واسعا للقيام بهذه الأعمال حيث أن الإطار الوهمي الذي يمكن أن تغلف فيه الانترنت من يقوم بهذه العملية تسمح له بالاختفاء في أي وقت يشاء وبعد قيامه بالجريمة.

خامسا: المجرم المعلوماتي (الإلكتروني).

المجرم المعلوماتي أو (الهاكرز) هو الذي يقوم بكل هذه الجرائم حيث اختلف الكثير في تعريفه وتحديد هويته وتقدير مدى عقوبته لقد تنوعت الدراسات التي تحدد المجرم، وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة، ولكن يمكن تلخيص سماته بأنه مجرم متخصص: له قدرة عالية في المهارات الحاسوبية والتقنية ويستغل هذه المهارات في اختراق نظم التشغيل واكتشاف كلمات المرور أو الشفريات ليحصل على المعلومات الموجودة علي أجهزة الحواسيب ومن ثم يقوم بتخزينها للاستفادة منها. وكذلك السرقة والنصب والاعتداء علي حقوق الملكية الفكرية وغيرها من الجرائم، مقابل المال، كما أنه يقوم بإخفاء أي اثر له لكي لا تكتشفه الأنظمة الأمنية حتى لا تستطيع مراقبته أو ملاحقته من خلال أي شبكة ويمكن إجمال خصائص وسمات المجرم المعلوماتي كما يلي:

. شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي (عمرو حسين عباس، المرجع السابق، ص 11)؛

. شخص قادر على استخدام خبراته في الاختراقات وتغيير المعلومات؛

. شخص قادر على تقليد البرامج أو تحويل الأموال.. الخ؛

. شخص محترف في التعامل مع شبكات الحاسبات؛

. شخص غير عنيف لان تلك الجريمة لا تلجأ للعنف في (فؤاد جمال، 2010، ص 65)؛

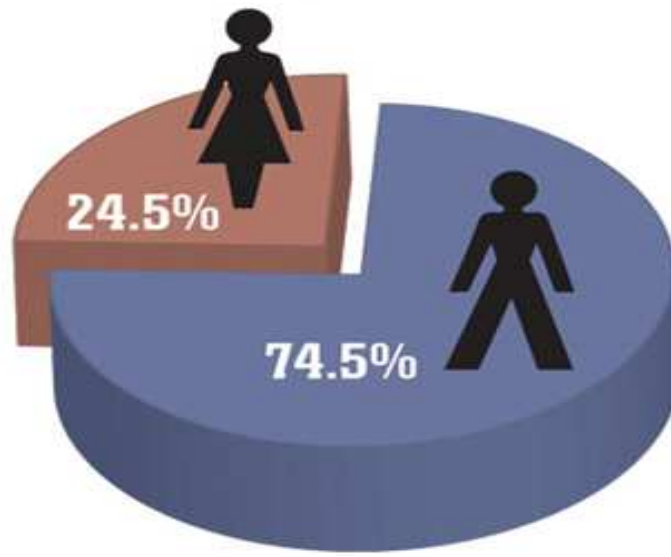
. شخص يتمتع بذكاء حيث يمكنه التغلب على كثير من العقوبات التي تواجهه أثناء ارتكابه الجريمة؛

. شخص اجتماعي له القدرة على التكيف مع الآخرين.

- مجرم متخصص: له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفريات، ويسبح في عالم الشبكات ليحصل علي كل غالي وثمين من البيانات والمعلومات الموجودة علي أجهزة الحواسيب ومن خلال الشبكات.

- مجرم عائد للإجرام: يتميز الجرم المعلوماتي بأنه عائد للجريمة دائما، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات. فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق (فؤاد جمال، المرجع السابق ص 8).
- مجرم محترف: له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.
- مجرم ذكي: حيث يمتلك هذا الجرم من المهارات ما يؤهله لأن يقوم بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعمالها الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب (وليد عاكوم، المرجع السابق ص 5).

Who's Doing the Crimes?*



نسبة مجرمي الإنترنت من الجنسين

سادسا: أنواع الجرائم الإلكترونية.

بسبب انتشار الجريمة الإلكترونية بشكل كبير وواسع فللجريمة الإلكترونية أنواع مختلفة، نتطرق لها ضمن هذا المبحث الذي قسمناه إلى أربعة فروع، على التوالي، الجريمة المالية، ثم الجريمة الثقافية، ثم الجريمة السياسية والإقتصادية، وأخيرا، الجريمة الأخلاقية وجرائم الإرهاب.

1/ الجريمة المالية (Financial Crime):

وهي التي تسبب أضرارا مالية للضحية أو المستهدف من عملية النصب، وتأخذ أحد الأشكال الثلاثة التالية:

- عملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك كتلك التي المنتشرة الآن في الكثير من الدول وفيها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية؛
- إنشاء صفحة انترنت ماثلة لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة (phishing) لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها (خالد العنزي، الخامس ماي 2011 ص 33)؛

. رسائل البريد الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحويل الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي.

2 / الجريمة الثقافية (Cultural Crime):

هي استيلاء المجرم على الحقوق الفكرية ونسبتها له من دون موافقة الضحية، وقد تتخذ إحدى الصور التالية:

. قرصنة البرمجيات: وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل.

. التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت بواسطة تقنية (soft copy) (سارة خلف، المرجع السابق، ص 4، 5)؛

. نسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة.

3 / الجريمة السياسية والاقتصادية (Political and Economic crime):

. يستخدم المجرمون حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم؛

. الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجاناً؛

- نشر الأفكار الخاطئة بين الشباب، كالإرهاب والإدمان والزنا، لفساد الأنظمة لأسباب سياسية واقتصادية بالدرجة الأولى.؛

. تزوير نتائج الانتخابات.

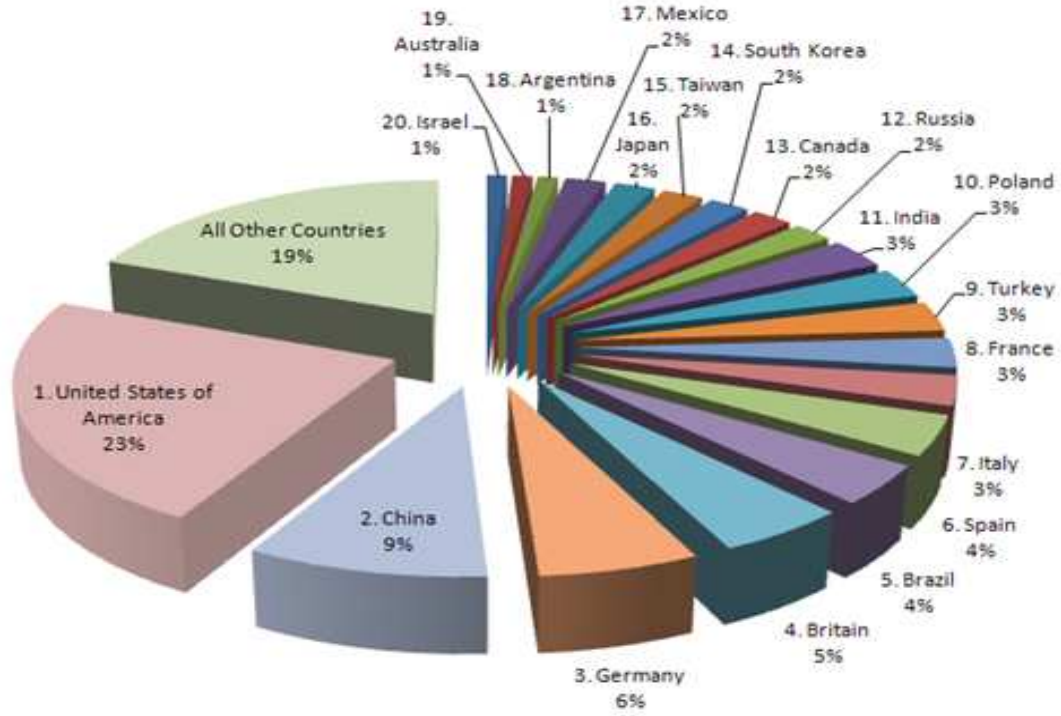
4 / الجرائم الأخلاقية وجرائم الإرهاب:

أ- الجريمة الأخلاقية (Sexual Crime):

هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية: الابتزاز، ومن أشهرها عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وبه مجموعة من صورها، وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور.

. التغير والاستدراج: في العادة تتواجد هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات في الشات أو في برامج المحادثة ويكون علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها بالزواج لكي تثق به، ومن ثم يقوم بتهديدها وفضحها بما يملكه من صور أو تسجيلات لصوتها إن لم تستجيب لطلباته، ويوجد العديد من الحالات المبلغ عنها نجحت المصالح الأمنية في الجزائر في إيقافها والتعامل معها (سارة خلف، المرجع السابق، ص 19).

. انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الانترنت من قبل الغزو الفكري لتيداولها الشبان والشابات وإفساد أفكارهم وإضعاف إيمانهم. وتمثل الصورة التالية أكثر 20 دولة تنتشر فيها الجريمة الإلكترونية .



مجسم: انتشار الجريمة الإلكترونية في أكثر الدول

ب- الجريمة الإرهابية:

قد تستعمل البيانات والمعطيات المعلوماتية في الجرائم الإرهابية، كاتباع الوسائل الإلكترونية للتأثير على برمجيات التحكم في الطائرات المدنية لنقل المسافرين وإسقاطها وقتل ركابها، أو توجيهها عبر التعديل الإلكتروني الإجرامي، لاستعمالها في تدمير العمارات السكنية والإدارية والمطارات المدنية والعسكرية، كما يمكن للإرهابيين الدوليين اختراق برمجيات التحكم في سفن النقل المدنية وتعديلها قصد إغراقها وقتل ركابها، وقد يتسلل الإرهاب الإلكتروني إلى برمجيات المطارات المدنية وأبراج المراقبة وإعطاء تعليمات خاطئة للطيارين، لإحداث خلل في الإقلاع والهبوط، وإحداث كوارث جسيمة، كما قد تستغل برامج الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة تستخدم في الدعم المادي للإرهاب (معجل نبيل، المرجع السابق)، وغيرها من الجرائم الإرهابية التي تتطور أساليبها بسرعة.

سابعاً/استراتيجية مكافحة الجريمة الإلكترونية:

هناك العديد من الصعوبات العملية، في تحديد استراتيجية فعالة، على الأقل في الوقت الراهن لمكافحة الجريمة الإلكترونية للأسباب التالية:

- صعوبة التوصل إلى الأدلة الرقمية والتحفظ عليها؛
- القصور التشريعي في تعريف مفهوم الجريمة الإلكترونية؛
- عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية؛

. قصور النصوص التشريعية الخاصة بمواجهة تلك الجرائم؛

. قصور التعاون الدولي بين الدول في مجالات المكافحة.

إن جرائم الإنترنت في الدول العربية تختلف عن مناطق أخرى في العالم، فيجب أن ندرك بأن أمن المعلومات في هذه المنطقة يتأثر بكثير من العوامل مثل نمو قاعدة المستخدمين، وضعف الوعي الأمني، وانعدام التدريب اللازم للقائمين على هذا المجال، وعدم وجود اللوائح الأمنية والقوانين التي تعاقب مرتكب هذا النوع من الجرائم وسوف نستعرضها فيما يلي:

أ- نمو قاعدة مستخدمي الإنترنت:

مع تزايد وتوفر وصلات الإنترنت وانخفاض رسوم الاشتراك ازداد عدد مستخدمي الإنترنت في البلدان العربية، لذلك أصبح الإنترنت في هذه البلدان له شعبية كبيرة للاتصال والتواصل وإيجاد فرص جديدة للإعمال التجارية.

ب- عدم وجود برامج للتوعية الأمنية:

يرجع السبب بازدياد ضحايا الجرائم الحاسوبية لعدم وجود برامج توعية لمستخدمي شبكة الإنترنت (خسائرها بالمليارات، ماي -2011).

ج- الهياكل الأساسية للمعلومات:

في المنطقة العربية يكثر الاستثمار في الهيكل الأساسي لتكنولوجيا المعلومات. ومن الضروري أن يؤخذ بعين الاعتبار للصيانة المستمرة في نظام الأمان والحماية حيث أشارت معظم الإحصائيات إلى أن معظم البنوك معرضة للهجوم الإلكتروني من قراصنة الإنترنت، فيجب تخصيص العديد من الاستثمارات في مجال أنظمة تكنولوجيا المعلومات الأمنية والتوعية.

د- ضعف برامج التوعية الأمنية:

من الضروري زيادة الإرشاد والتوعية حول أمن المعلومات فهو أمر لا مفر منه لمكافحة الجريمة الإلكترونية، ففي الدول العربية هناك نقص كبير في الوعي الأمني سواء بين المؤسسات أو المنظمات أو بين عامة الناس مقارنة بأوروبا. فإننا نجد أن الدول العربية جهودها في رفع مستوى الوعي بين الناس قليلة، فعلى سبيل المثال: نجد أن المملكة العربية السعودية تعتبر من الدول المستهدفة لمرتكبي الجريمة الإلكترونية حيث أنها تحتل المرتبة الأولى في الشرق الأوسط وتحتل المرتبة الثامنة والثلاثون على العالم.

و- نمو النشاط المصرفي:

يرجع سبب في زيادة غسيل الأموال المكتسبة بصورة غير مشروعة إلى نمو العمل المصرفي الدولي الذي أعطى سهولة في نقل الأموال النقدية إلى أي بلد، ففي الشرق الأوسط والمغرب العربي يوجد العديد من حالات غسل الأموال التي كان ضحيتها من ضلل بهم باستخدام الحيل والخدع الإلكترونية، التي يرد عليها بعض المستخدمين فيكونون ضحية لبداية عملية غسيل أو استخدام حسابه المصرفي في أغراض أخرى.

ثامنا: السبل الوقائية لمكافحة جرائم الإنترنت:

. تنمية دور الأسرة والمجتمع في مواجهة الجريمة الإلكترونية وذلك من خلال النشرات التوعوية وعقد مؤتمرات وبث ورق عمل إرشادية على صفحات الإنترنت كذلك إقامة حملات إعلانية للتحذير؛

. مواكبة التقنية الحديثة وتأمينها فور انتشارها وتسخيرها للعمل في مجال الوقاية من الجريمة ومكافحتها مثال على ذلك تشديد الرقابة على أكثر البرامج المتداولة بين الشباب مثل Facebook ونشر إرشادات بصفة مستمرة عليه ودعوة مزودي خدمة الانترنت إلى اتخاذ الإجراءات اللازمة لوضع فلتز لحماية الأطفال وتوعية مستخدمي الإنترنت لمخاطر الانترنت وحجب المواقع الإباحية.

. توفير القوى البشرية المؤهلة والمدرية للعمل على هذه الأجهزة الحديثة وتحقيق أداء عالٍ من خلالها وذلك بالتدريب على تحديد مخاطر حقيقة في الشبكة العنكبوتية (الجرائم الإلكترونية، المرجع السابق)، وكيفية مواجهتها، (مواجهة الهاكرز) كذلك تصميم الكثير من البرامج التي تعمل على حائط صد هجمات تلك القرصنة ولعل أشهرها برنامج McAfee كذلك التطبيق العملي على الوقاية من مخاطر معينة (جريدة الرياض، 2010).

. أنشئت عام 2006 منظمة تدعى (مجموعة العمل للتحالف الإستراتيجي ضد الجريمة الإلكترونية) مهمتها وضع قوانين للحد من الجريمة الإلكترونية في العالم وذلك بمساعدة منظمات حكومية عالمية مهمتها تتمثل فيما يلي (الجرائم الإلكترونية وأنواعها، ماي -2011):

- تحديد المخاطر الفكرية الأمنية التي تهدد مستخدمي الانترنت جراء استخدامهم لها؛
- التعرف على أشهر وسائل الإرهابيين في الانترنت وكيفية القضاء عليها؛
- معرفة طرق استخدام وتركيب شهادات الأمان؛
- الوعي بما يحيط بالمستخدم من مخاطر فكرية أمنية جراء استخدام الانترنت؛
- الإطلاع على وسائل وأساليب الاستغلال الفكري الأمني المستخدمة على الإنترنت؛
- الإطلاع على وسائل الوقاية من المخاطر الفكرية الأمنية المبثوثة في الانترنت؛
- التواصل مع الجهات والأشخاص ذوي الصلة في حالة التعرض لأحد مخاطر الإنترنت؛
- بث الوعي في الأوساط الاجتماعية فيما يتعلق بمخاطر الإنترنت وأساليب الوقاية منها؛
- الإلمام والإطلاع على نظام مكافحة الجريمة الإلكترونية؛
- معرفة طرق التجسس وكيفية رصدتها وإزالتها؛
- تعميم الوعي ليشمل جميع مستخدمي الانترنت من طلاب وطالبات الجامعات ومن في مستواهم.

تاسعا: السبل القانونية للحد من الجرائم الالكترونية:

إن للجريمة الالكترونية صدى كبير جدا في العالم، حيث أصبحت تشكل تهديد خطير لاقتصادها ونموها، فالجريمة الإلكترونية أصبحت أمرا مرعبا لدى الدول العربية لما تسببه من أضرار كثيرة في مختلف الأصعدة وذلك يرجع بسبب انتشار الكم الهائل من شبكات الانترنت وخدماتها التي أصبحت في متناول الجميع. لذلك لابد من وضع قوانين وأنظمة صارمة لردع مرتكبي الجرائم الالكترونية بأسرع وقت ممكن، كما يوجد الآن في بعض الدول العربية التي قامت ببعض المحاولات المطبقة للحد من مرتكبي الجريمة، كالجنازير، حيث جاء تعديل قانون العقوبات بالأمر رقم 97 / 10 المؤرخ في 06 مارس 1997، الذي نص على قمع الجرائم الإلكترونية في المواد من 394 مكرر إلى 394 مكرر 7، تحت عنوان: (المساس بأنظمة المعالجة الآلية للمعطيات). غير أن المشرع الجزائري اعتبر كل الجرائم الإلكترونية من فئة الجنح، مهما كانت درجة خطورتها، كما جرم الشروع (المحاولة) بالنسبة لتلك الجنح، وهكذا نصت المادة 394 مكرر على أن: يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من

50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، كما نصت المادة 394 مكرر 2 على أن: يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 إلى 5000000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإبحار في معطيات مخزنة أو معالجة أو مرسلية عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

كما نصت المادة 394 مكرر 7، على أن: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

الخاتمة:

يتضح من خلال الدراسة السابقة أن وجود هذا انتشار الجرائم الإلكترونية يدعو بدون شك إلى خلق إطار قانوني يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية البشر من تأثيرها وحماية النشاطات بكافة أنواعها.

فالانترنت والتكنولوجيا مصادر معرفية لا يمكن التحكم بكيفية انتشارها أو على أقل تقدير استخدام مصادرها، لذا أصبح محتملا على الحكومات والمشرعين سن القوانين التي يمكن من خلالها ضبط استخدام الانترنت في أغراض خارجة عن القانون لأن القوانين الوضعية الحالية المطبقة في عالمنا العريلا تزال قاصرة عن احتواء الأوضاع التي يمكن أن تنشأ جراء استخدام التكنولوجيا الحديث في الإجرام.

إن الجزائر، رغم أنها كانت سباقة بالنسبة للدول العربية في النص على الجريمة الإلكترونية ومعاقبة مرتكبيها بالحبس والغرامة، وذلك سنة 1997، إلا أنها اليوم في حاجة إلى مراجعة تشريعاتها في هذا المجال بما يواكب التطور الملحوظ في الإجرام الإلكتروني.

إن مشروع الحكومة الإلكترونية، رغم فوائده الجمة التي تعود على المواطن والدولة في المجالين الخدمتي والاقتصادي، فلا مناص له من إحاطة معطياته وبرامجه بتشريعات صارمة لحمايته ضد كل هجوم إلكتروني أو سرقة أو ابتزاز.

كما يتطلب برنامج جدي لتوعية العاملين في هذا المجال من مهندسين وتقنيين وموظفين، بدءاً بالوزارات ووصولاً إلى البلدية والمؤسسات الاقتصادية الصغيرة والمتوسطة.

وفي الختام نستطيع القول أن اتفاقية بودابست (2001) لمكافحة الجريمة الإلكترونية، فعلاً تعتبر الأداة الدولية الوحيدة إلى الآن الملزمة بشأن الجرائم الإلكترونية، كما تعد هذه الاتفاقية المصادق عليها من قبل 48 دولة، بمثابة الخطوط التوجيهية لكل دول العالم، والتي تضع تشريعاً يحاول أن يساير التطورات السريعة للجريمة المعلوماتية، كما أنها توفر إطاراً للتعاون الدولي ضد جرائم الانترنت بصفة عامة، غير أن الهوة التكنولوجية بين الشمال والجنوب، سوف يكون لها بالغ الأثر في حسن استغلال هذه التكنولوجيا، وسوف تزداد خطورته مستقبلاً، ولا يمكن الحد منها إلا بتوفر إرادة دولية لا تقصي أحداً من المجتمع الدولي، وذلك بمزيد من التعاون والاجتهاد الجماعي لوضع هياكل تنظيمية مناسبة وتعزيز التشريع الدولي الوطني، والمزيد من التحسيس للفاعلين في المجتمع بأمن الأنظمة المعلوماتية.

قائمة المراجع:

أولاً: الكتب:

(1) - جلال الدين عبد الخالق والسيد رمضان، الجريمة والانحراف من منظور الخدمة الاجتماعية. القاهرة: المكتب الجامعي الحديث، 2001.

(2) - الجريمة الإلكترونية في الجزائر. نشر على الموقع:

[http://www.4shared.com/dir.PDF]. (18.03.2009), 1,16Mo

(4) - محمد سعدي، السلوك الإجرامي للمرأة الجزائرية اتجاه زوجها. (رسالة الماجستير في علم الاجتماع الثقافي)، كلية الآداب والعلوم الاجتماعية، جامعة البليدة، 2007.

(5) - ما هي الجريمة؟ نشر على الموقع:

[http://ejabat.google.com.mhtml] 568ko,(31/12/2009).

(6) - خلف سارة، "الجرائم الإلكترونية والأدلة الجنائية الإلكترونية". مجلة بحوث، م. ع. س. ماي 2010.

(7) - عاكوم وليد، التحقيق في جرائم الحاسوب. لبنان: الدليل الإلكتروني للقانون العربي، 2009.

(8) - عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية. القاهرة: جامعة الدول العربية، 2008.

(9) - مناني فراح، أدلة الإثبات الحديثة في القانون الجزائري. الجزائر: دار النشر الطباعة، 2010.

(10) - يونس عرب، "جرائم الكمبيوتر والانترنت". أبو ظبي: المركز العربي للدراسات والبحوث الجنائية، 2002.

ثانياً: المجلات والدراسات:

(11) - العنزي خالد، "الابتزاز". الصحيفة الإخبارية اللبنانية، العدد الخامس، ماي 2011 ص 33.

(12) - فؤاد جمال، "جرائم الحاسبات والانترنت". الكويت: المجلة القانونية لخدمات المعلومات التشريعية ومعلومات التنمية، 2010.

ثالثاً: المواقع الإلكترونية:

(14) - "الجرائم الإلكترونية. الخطر الداهم على المجتمع والأسرة". على الموقع:

<http://www.zoomkw.com/zoom/Article.cfm?ArticleID=76148>. (13/05/2011).

(15) - "الجرائم الإلكترونية وأنواعها والأنظمة المطبقة في السعودية" الموقع

"<http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-forensic-and-computer-crimes/987-types-of-electronic-crime-and-regulations-in-force-in-saudi-arabia.html>. Mai

2011.

(16) - "حسائرها بالمليارات"... جريمة الكترونية كل 3 دقائق على الانترنت " الموقع:

2011.Mai. <http://www.ensan.net/news/212/ARTICLE/3596/2008-04-22.html>

(17) - "الاحتياال المالي تكلف منطقة الخليج 380 مليون دولار"، جريدة الرياض، العدد الرابع، 2010

(18) - معجل نبيل، "الإرهاب والانترنت". المجلة الإلكترونية للأبحاث: على الموقع:

www.alarabiya.net/views/2005/01/05/9306.html