ألجريمة ألالكترونية عبر الانترنيت أثرها وسبل مواجهتها[+]

CYBER-CRIME THROUGH INTERNET AND THE SOLUTIONS TO FACE IT.

سمير سعدون مصطفى [*] محمود خضر سلمان [**] حسن كريم عبد الرحمن [***]

المستخلص:

ألجريمة ألالكترونية هي كل فعل ضار بالآخرين عبر استعمال الوسائط الالكترونية مثل ألحواسيب ، أجهزة الموبايل، شبكات الاتصالات ألهاتفية، شبكات نقل ألمعلومات، شبكة ألانترنيت أو ألاستخدامات غير ألقانونية للبيانات ألحاسوبية أو ألالكترونية عموما. هذه ألدراسة تعرض أثر ألجريمة ألالكترونية على ألمجتمع وعلى ألأخلاق من خلال استغلال مرتكبو هذه الجريمة للوسائط الالكترونية. وتقدم هذه الدراسة التوصيات بوضع التشريعات والقوانين اللازمة لمعاقبة وردع مرتكبي الجرائم الالكترونية وتقديم النصائح والحلول الفنية لمستخدمي الوسائط الالكترونية للتقليل من خطورة واثر هذه الجريمة.

Abstract:

Cyber-crime is any act detrimental to others through the use of electronic media such as computers, mobile phones, telephone networks, information transfer network, the Internet or illegal uses of computer or electronic data in general. This study was the impact of electronic crime on society and the ethics of taking advantage of the perpetrators of this crime to electronic media. The study provides recommendations to legislation and laws to punish and deter the perpetrators of cyber crimes and providing advice and technical solutions for users of electronic media to reduce the risk and the impact of this crime.

ألمقدمة:

مع دخول الحاسوب والانترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم الالكترونية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية ومتابعة هذا النوع من الجرائم وسن القوانين والتشريعات اللازمة لمكافحة الجرائم الإلكترونية نظراً لما تسببه من خسائر مادية ومعنوية كبيرة. تُعرف الجريمة في القوانين الوضعية بأنها كل فعل يعاقب عليه القانون أو امتناع عن فعل يقضي به القانون ويحدد القانون الوضعي عقوبات محددة للمخالفات بمعنى أنه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لا يعتبر جرماً.

[+] تاريخ استلام البحث ٢٠١٠/٩/٢٠ / تاريخ قبول النشر ٢٠١١/٥/٤

[*] أستاذ مساعد/ ألكلية التقنية كركوك / قسم هندسة ألإلكترونيك والسيطرة

[**] مدرس/ المعهد التقني كركوك / قسم التقنيات الكهربائية

[***] مدرس مساعد/ المعهد التقني كركوك / قسم أنظمة الحاسبات

من ناحية أخرى الجريمة هي كلّ فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين. وبالتالي فالجرائم الإلكترونية أي فعل ضار يأتيه المواطن عبر استعماله الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموماً. لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه "جرائم" يمكن أن تنتهك على الشبكة ، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين وأساتذة الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. [1]

لكن مع توسع استخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها.

فمع تطور الانترنت وتوسع استخداماته وازدياد أعداد المستخدمين لها في العالم (حوالي ١,٦ مليار مستخدم يمثلون ربع سكان العالم) أصبح الانترنت وسطاً ملائماً للتخطيط ولتنفيذ عدد من الجرائم بعيداً عن رقابة وأعين الجهات الأمنية. إذن الجريمة الالكترونية هي استخدام الوسائط الحاسوبية والشبكات وشبكات الإنترنت لارتكاب جريمة أو التخطيط لها ساهمت التكنولوجيا منذ نشأتها بتغيير الكثير من المفاهيم التي اعتاد الناس عليها، وتباينت هذه التغييرات بين السلبية والإيجابية. ففي الوقت الذي قامت فيه التكنولوجيا على سبيل المثال بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية(Internet Hackers) ، ويقومون من خلالها باقتحام خصوصية الفرد رغما عنه.

تتنوع نشاطات أولئك القراصنة، ويقابل ذلك التنوع بنشاطات القراصنة تنوعا آخر بمدى الضرر الذي يستطيعون إلحاقه بالمستخدم، حسب النشاط الذي يقومون باستخدامه. في كثير من الأحيان تمكن المعلومات التي يحصل قراصنة الشبكة العنكبوتية عليها من القيام بعمليات احتيال باسم الضحية، كالقيام بالبيع أو الشراء أو طلب قروض مصرفية وغير ذلك من الأمور.لقد سهلت الشبكة العنكبوتية على القراصنة مسألة سرقة الهوية من خلال توفيرها للكثير من الطرق التي تساهم بإنجاح أهدافهم بشكل كبير. فعلى سبيل المثال، تعتبر غرف الدردشة مرتعا خصبا لتنفيذ هذا النوع من السرقات، حيث يقوم القراصنة بتصميم برامج فايروسية تسمى أحصنة طروادة(Trojan Horses) ، التي تستطيع من خلال دخولها على أحد أجهزة الحاسوب، أن تتجسس على صاحبه للحصول على معلومات معينة مثل كلمات المرور التي يستخدمها، لتقوم هذه الأحصنة بعد ذلك بإعادة هذه المعلومات للقرصان. [٢]

بعض ايجابيات الانترنيت

١) المعلومات و المعارف والإحصائيات والتكنولوجيا والأخبار والأفلام.
٢) مجال الطب و الدعم الطبي.
٣) إتصال الأسر والتواصل بين الأقارب والبريد الالكتروني.
٤) التعليم عن بعد و التدريب الثقافي والعلمي.
٥) الاجتماعات التي تتم عن طريق الوسائل المرئية.
٦) التطبيقات المصرفية.
٧) التسوق عبر الإنترنت.
٨) البحث عن فرص العمل والعمل عن بعد.

بعض سلبيات الإنترنت

١) التوجهات الفكرية المختلفة عن عاداتنا و تقاليدنا

٢) المواقع الإباحية و الجنس

٣) ألعاب وتسلية

٤) غرف دردشة غير مجدية

٥) تبادل ملفات و صور غير لائقة

٦) تحميل الأغاني بدون مراعاة حقوق الملكية. [٣]

أنواع الجرائم الإلكترونية

•١ جرائم اختراق الحواسيب ومراكز المعلومات بهدف:

o الوصول للبيانات بشكل غير قانوني والاطلاع عليها أو التلاعب بها (تزويرها مثل تغيير وثيقة ملكية أو تغيير بيانات ضريبية، . . . الخ)

o تدمير البرامج والبيانات المخزنة فيها (تعطيلها عن العمل) من خلال زرع الفيروسات والبرامج الخبيثة.

•٢ جرائم شبكة الانترنت Cyber Crime وتشمل:

o استخدام الحواسيب وشبكة الإنترنت للتخطيط لجريمة (مثل السرقة ، تزوير أوراق ومستندات، اختلاس أموال، الاحتيال، التخطيط لجرائم جنسية ضد الأطفال والقصر والفتيات)

o اقتحام المواقع الإلكترونية على الشبكة وإيقافها عن العمل من خلال إغراقها بالرسائل أو بوسيلة أخرى أو تدميرها.

o جرائم القرصنة (إنشاء مواقع للبرامج المقرصنة، استخدام البرامج المقرصنة وسرقة المواقع)

o التشهير وتشويه السمعة في المواقع الإلكترونية والإخبارية

o انتحال شخصية فرد أو شركة بهدف الاحتيال (مثلاً من خلال البريد الإلكتروني)

o اختراق البريد الإلكتروني للآخرين

o تزوير التوقيع الإلكتروني

o جرائم الأموال: السطو على أرقام البطاقات الائتمانية، اختلاس من البنوك، تزوير وثائق ومستندات مالية.

o الاحتيال للاستيلاء على الأموال من خلال البريد الالكتروني

o جرائم التغرير والاستدراج : التغرير والاستدراج هي من أشهر جرائم الإنترنت ومن أكثرها انتشاراً خاصة بين أوساط صغار السنّ والقصر والفتيات من مستخدمي الشبكة. وهي تقوم على عنصر الإيهام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين. وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها أو ردعها لأنها تُرتكب بشكل متزايد ودون أي حدود سياسية أو اجتماعية، إذ يستطيع كلّ مراسل أو محاور عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية من ذوي طالبي التعارف وإقامة العلاقات عبر الشبكة ومن ثم خارجها. وغالباً لا يتم الإبلاغ عن معظم حالات التغرير والاستدراج لأن معظم ضحاياها هم من صغار السنّ الذين لا يدركون المعنى القانوني للتغرير والاستدراج.

فالقانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الحديثة، لاسيما أن نصوص القانون الجنائي التقليدي وضعت في عصر لم يكن الإنترنت فيه قد ظهر، ولم تظهر بعد المشاكل القانونية الناشئة عن استخدامه، مما يفرض علي رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدام الإنترنت ومواجهة هذا النقص التشريعي، خاصة أنه لا يوجد لدينا نصوص خاصة بهذه الجرائم فلا عقوبة على جرم لم يأت عليه نص قانوني وباعتبار أن لا

عقوبة إلا بنص فهذا يستوجب إعادة النظر بالتشريعات القائمة لدينا لتعديل بعض نصوصها بما يتعلق بهذا الموضوع وإصدار تشريعات مستقلة للإحاطة بجميع الجرائم المتعلقة بجرائم الحاسوب والانترنت.

الجرائم الإلكترونية جديدة ولم يتناولها القانون الجنائي التقليدي، وبالتالي لا يوجد نصوص في قانون العقوبات تتعلق بالجريمة الالكترونية وبالتالي من الصعوبة بمكان إصدار أحكام بحق مرتكبيها.

الأجهزة القضائية وأساتذة القانون ما زالوا عاجزين عن الخروج بتصور واضح عن الجريمة الالكترونية. والقانون لا يعاقب على فعل سرقة المعلومات الإلكترونية لكونها غير مادية.

إن أهم خطوة في مكافحة جرائم الانترنت هي تحديد هذه الجرائم بداية ، ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل القائمين على النظر فيها بما يتناسب وطبيعة هذه الجرائم المستجدة، ويأتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها والعقوبات المقترحة ومن ثم يجري التركيز على التعاون الدولي لمكافحة هذه الجرائم والحاجة إلى وجود تشريع دولي موحد في هذا المجال. فهناك قصور واضح عربيا في مجال جرائم الإنترنت سواء من حيث أساليب التحقيق والرصد أو في مجال التوعية والتثقيف، وظهرت الحاجة إلي تثقيف القائمين بالضبط والخبراء. [٤]

مرتكبو جرائم الحاسوب والانترنت

الهكرز hackers أو المتسللين : هواة بارعون باستخدام الحاسوب يستغلونه للتسلية بشكل غير قانوني لديهم فضول لاكتشاف حواسب الآخرين.

الكراكرز Crackers أو القراصنة المحترفون وهم عصابات أصبحت متخصصة بجرائم الإنترنت.

معدلات الجريمة الالكترونية على المستوى العالمي

القضية كبيرة وأكبر مما نتصور، ففي بريطانيا وفي عام ٢٠٠٧ هناك جريمة الكترونية تقع كل ١٠ ثواني (٣ مليون جريمة بالسنة، أو ٨ آلاف جريمة باليوم). وأكبر نسبة فيها تعود لجرائم التحرش الجنسي (٨٥٠ ألف حالة) ، بينما هناك ٩٢ ألف حالة لسرقة الهوية أي الحصول على معلومات شخصية حول مستخدمي الانترنت، و ١٤٥ ألف حالة لاختراق الحواسيب بهدف سرقة المعلومات أو التخريب، و ٢٠٧ ألف حالة للحصول على الأموال من خلال الاحتيال للسطو على أرقام البطاقات الائتمانية. وتقول إحصائيات شركات التأمين أن ٧٠% من هذه الجرائم تستهدف الأفراد. [٥]

الأطفال هم من أكثر ضحايا الجريمة الالكترونية على الانترنت

الإحصائيات العالمية تقول أن ٨٠% من الأطفال الذين يستخدمون البريد الإلكتروني يستقبلون رسائل بريد إلكتروني دعائية كل يوم وبخاصة خلال فترات العطلة حيث يقضي الأطفال الكثير من الوقت في تصفح الإنترنت. وبعض تلك الرسائل تتضمن محتوىً 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، وغالباً يفتح الطفل الرسالة.

الكثير من هؤلاء الأطفال بالطبع ينزعجون من تلك الرسائل ولا يناقشون الموضوع مع أهاليهم، بعضهم الرسائل تثير فضولهم ويطلعون عليها، وحتى عندما يطلعون على محتوى تلك الرسائل فإن الكثير منهم لا يطلعون أهاليهم على ذلك.. ويتم استدراج الأطفال عن طريق غرف الدردشة أو عن طريق طلب صورهم والعبث فيها ونشرها فوق أجسام عارية وخاصة في حالة صور الفتيات. [٦]

الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الانترنت والحاسوب

سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا. كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم.

وعلى مستوى الدول العربية لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية واتخاذ إجراءات فورية تجاه المخالفين في المواقع الالكترونية ويتم تدميرها إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة. شهدت فعاليات المؤتمر الإقليمي الأول حول الجريمة الإلكترونية، «تحديات تكنولوجيا المعلومات والتنمية الاقتصادية»، العديد من المطالب. دعا عدد من رجال القانون والقضاة وأعضاء النيابة العامة والمتخصصين في مجال مكافحة الجريمة الإلكترونية إلي ضرورة وضع تشريعات وقوانين تعاقب مرتكبي جرائم الإنترنت والمعلومات والبيانات، علي شبكة المعلومات الدولية، وتطوير التشريعات الموجودة حاليا بما يواكب التطور العلمي والتكنولوجي ، بما يكفل حقوق المواطنين المستخدمين شبكة المعلومات الدولية، وتحدد واجباتهم.

أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطارا للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال، ويحدد الواجبات تجاهها، فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتا مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال القيم التي يروجها.

و لا يقف دور القانون علي مجرد تنظيم العلاقات المترتبة علي التقدم التكنولوجي بل إنه يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتي لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم، بل يكون علي العكس من ذلك وسيلة لمحاربة هذا الإجرام، وهو ما يوجب على القانون أن تمتد نصوصه إلي الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تحدد الجريمة في نصوص منضبطة واضحة، ولا يترك بحثها إلي نصوص قانون العقوبات التقليدي، التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام.

وقد تتجاوز نتائج هذه الجرائم إلى وقوع جرائم أخرى تهدد الحق في الحياة والسلامة البدنية، إذا ما أدي العبث في المعلومات إلى تغيير طريق العلاج أو تركيبة الدواء.

و قد تؤثر على نطاق الخدمات الإلكترونية وقطاعات التنمية الاقتصادية، وتكنولوجيا المعلومات، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية المستخدمين تكنولوجيا الاتصالات، من خلال إجراءات تتميز بالشفافية الكاملة، خاصة أننا نواجه تحديات جديدة بما يعرف بالجريمة الإلكترونية، التي يجب مكافحتها، لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل عن الثوابت التشريعية والقانونية. [٧]

أن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته.

أوجه القصور التشريعي في كثير من الدول العربية :

(١) إن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب عند انتفاء النص. الأمر الذي يمنع مجازاة مرتكبي السلوك الضار أو الخطر على المجتمع بواسطة الحاسوب (الكمبيوتر) أو الإنترنت ؛ طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب .

(٢) يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان ؛ غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية ؛ التي تتجاوز حدود المكان ؛ فجرائم الإنترنت عابرة للحدود .

(٣) انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الانترنت لكونها من الجرائم الحديثة وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى، ويساعد على ذلك انعدام وجود مركزية وملكية عبر الانترنت .

(٤) رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التي تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية في القانون ؛ إلا أنه مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها . [٨]

ألاستنتاجات:

- في الوقت الذي قامت فيه التكنولوجيا بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية.
- الجرائم الإلكترونية جديدة ولم يتناولها القانون الجنائي التقليدي، وبالتالي لا يوجد نصوص في قانون العقوبات تتعلق بالجريمة الالكترونية وبالتالي من الصعوبة بمكان إصدار أحكام بحق مرتكبيها.
- الأجهزة القضائية وأساتذة القانون ما زالوا عاجزين عن الخروج بتصور واضح عن الجريمة الالكترونية. والقانون لا يعاقب على فعل سرقة المعلومات الإلكترونية لكونها غير مادية.
- فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته.
- مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها

التوصيات:

أولا في مجال استخدام ألانترنيت

١-استخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري على جهازك خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي ..

٢- لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس أو التي تحوي أفلاماً وصوراً خليعة لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً

في الجهاز بمجرد دخولك إلى الموقع!!

٣- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا.

٤- عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد exe أو أن تكون ملفات من ذوي الامتدادين مثلpif. jpg. وتكون عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك.

٥- عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل والصور الخاصة أو الملفات المهمة وغيرها من معلومات بنكية.

٦- قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت

٧- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق .

٨- حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.

٩- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.

١٠- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق .

١١- حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.

١٢- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.

١٣- لا تقم باستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره.

١٤- لا تقم باستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره.

١٥.لابد لمؤسسات المجتمع المدني المعنية بالمعلوماتية من القيام بحملات التوعية للتحذير من مخاطر شبكة الإنترنت.

١٦. تثقيف الآباء بشأن كيفية حماية أطفالهم من قناصي الإنترنت.

١٧. حملات إعلانية لتحذير المراهقات من الارتباط بعلاقات مع مجهولين عبر الإنترنت.

١٨. دعوة مزودي خدمة الانترنت والجهات الناظمة إلى اتخاذ الإجراءات اللازمة لوضع فلتر لحماية الأطفال ١٩. توعية مستخدمي الإنترنت لمخاطر الانترنت وحجب المواقع الإباحية.

٢٠. وضع تجهيزات وبرمجيات لمكافحة الرسائل المزعجة والحد من وصولها إلى صناديق البريد الإلكتروني.

٢١. أما المؤسسات فلابد لها من اتخاذ مختلف إجراءات الحماية الأمنية الموصى بها وفق المعايير العالمية لحماية بياناتها وأنظمتها الحاسوبية من الاختراق ووضع سياسة أمنية يتم مراجعتها بشكل دوري.

٢٢. إضافة إلى الاحتياطات التي ينبغي على المستخدم إتباعها للتقليل من خطورة تعرضه لسرقة هويته ما يلي:

•ضرورة الاطلاع على سياسة الخصوصية(Privacy Policy) الخاصة بالموقع الذي تريد استخدامه.

•التأكد من أن الموقع المستخدم يوفر إمكانية تشفيرencryption)) البيانات كي تضمن أمن بياناتك الشخصية.

•عدم إعطاء أي معلومات شخصية، مثل البيانات الخاصة أو أرقام الحسابات، عبر الهاتف ما لم يتم التأكد من أن الخطوط التي تستخدم آمنة.

<u>ثانيا ألتوصيات في مجال العلاقات الأسرية</u>

الإنترنت ــ مثل الأدوات الإعلامية الأخرى – سلاح ذو حدين، يمكن أن يكون مفيدا جدا إذا عرفنا كيف نستغله أحسن استغلال، و هو في نفس الوقت أداة تخريب للنفوس والأرواح عن طريق المواقع التافهة و الإباحية التي لا تجدي ،

وبشيء من المراقبة، وبشيء من التوجيه والإرشاد و التوضيح، يمكن أن نستفيد من هذه الآلة ونحفظ مجتمعاتنا و أبناءنا من شرورها لذا نوصي بما يلي

١. تعزيز الحوار الودّي بين الآباء و الأبناء.

٢. رفع مستوى الوعي والإدراك لدى الأطفال تجاه ما يمكن أن يصلهم من محتوى غير لائق.

٣. توعية الأطفال بأهمية عدم ذكر أي معلومات شخصية أو أسماءهم الحقيقية أو أرقام تليفوناتهم وعناوينهم أو حتى عنوان البريد الإلكتروني لأي أحد على الشبكة دون أذن الوالدين.

ومن هنا كان من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية ؛ فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا الإجرام غير التقليدي .

مواجهة تتعامل بشكل عصري متقدم مع جرائم المعلوماتية المختلفة التي يأتي في مقدمتها بناء ونشر برامج فيروسات الحاسب الآلي والدخول غير المشروع علي شبكات الحاسبات، والتحايل علي نظم المعالجة الآلية للبيانات وإتلاف البرامج وتزوير المستندات المعالجة الكترونيا، فضلا عن الجرائم التي تحدث في مجال المصارف.

<u>ثالثا ألتوصيات في محور التشريع</u>

١- ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم .

٢- ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية .

٣- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت .

٤- يتعين تدريب وتحديث رجال الادعاء العام – أو النيابة العامة – والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت.

- 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 .

٦- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة .

٧- يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب ألي أخرى ؛ يمكن أن تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات.

٨- يتعين أن تكون للسلطات القائمة بالضبط والتفتيش : سلطة توجيه أوامر لمَنْ تكون لديه معلومات خاصة للدخول على ما يحويه الحاسب الآلي والإنترنت من معلومات للإطلاع عليها .

٩- 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 .

١٠- يتعين اعتبار نشر وطباعة الصور الجنسية عن طريق الانترنت مما يدخل ضمن زمرة جرائم الآداب .

١١- ضرورة تجريم استخدام الأطفال في تصوير أفلام تمثلهم في أوضاع مخلة بالآداب العامة ؛ وعرضها على شبكة الإنترنت وباستخدام البريد الإلكتروني .

١٢- يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية ؛ أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الإنترنت .

١٣- 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 .

١٤- 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.

١٥- ضرورة إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ما قبل الجامعي.

١٦- إنشاء قسماً جديداً بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية للمعلوماتية ؛ أو تحت مسمى آخر (قانون المعلوماتية والإنترنت) أو(قانون الحاسب الآلي والإنترنت) .

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

١٨- من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية ؛ وخصوصا الإنتربول ؛ 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 .

ألمصادر :

١- فراس اللبن ألاصطلاحات المستخدمة في عالم جرائم الكمبيوتر والإنترنت محاضرة http://Faculty.ksu.edu.sa/feras

٢- عبد الله عبد الكريم عبد الله2007جرائم المعلوماتية والانترنت (الجرائم الالكترونية) منشورات الحلبي الحقوقية 2007

٣- علي أنيس الإنترنت و أثره على الشباب و الأسرة الجهاز القومي لتنظيم الاتصالات القاهرة نوفمبر ٢٠٠٦

٤- «تحديات تكنولوجيا المعلومات والتنمية الاقتصادية» من فعاليات المؤتمر الإقليمي الأول٢٠٠٧ القاهرة حول الجريمة الإلكترونية، مصر.

٥- معهد التدريب والدراسات القضائية بالتعاون مع شركة " مايكروسوفت " في أبو ظبي يوم ١٨ حزيران/يونيو ٢٠٠٧، المؤتمر العلمي حول " مكافحة الجرائم الإلكترونية في دول مجلس التعاون الخليجي " المؤتمر الخليجي العلمي حول مكافحة الجرائم الإلكترونية ــ أبو ظبي

٦- أعمال مؤتمر أمن المعلومات وزارة الاتصالات والتكنولوجيا سوريا/http://www.moct.gov.sy

٧- الأدلة القضائية في امن الفضاء الحاسوبي إحصاءات وزارة الاقتصاد الوطني في مجال الاتصالات حتى ديسمبر , 2007سلطنة عمان وزارة العدل

٨- موضي بنت عبد الله آل سعود،دور مراكز المعلومات في دعم القرار السياسي ورقة عمل مقدمة إلى مؤتمر تقنية المعلومات والأمن الوطني الرياض 2007