الجريمة الإلكترونية ومدى مكافحتها في التشريع المصري والسعودي

إعداد
طه السيد أحمد الرشيدي

المقدمة

إن التطور التكنولوجي المعاصر في مجال تقنية المعلومات وشبكات الاتصالات عمل على التقارب بين ملايين البشر وأتاح فرصا جديدة للاطلاع على المعلومات وتبادلها ؛ حتى وصف هذا العصر بعصر المعلومات ، إلا أن هذه التقنية جلبت معها كثير من الآثار السلبية ، تمثلت في استغلال بعض المجرمين هذا التطور في تقنية المعلومات وما يقدمه من وسائل حديثة ومتقدمة في ارتكاب العديد من الجرائم التقليدية ، كالسرقة والنصب وخيانة الأمانة، وتزوير المحررات، والاعتداء على حرمة الحياة الخاصة، وغير ذلك من الجرائم(١).

ومع شيوع الانترنت ووسائل الاتصالات الحديثة بزغ فجر ظاهرة إجرامية جديدة، تعرف بالإجرام ألمعلوماتي أو جرائم المعلومات؛ فتم السطو على البنوك بمساعدة هذه الوسائل ، ونمت الجريمة المنظمة وترعرعت في ظل هذه الثورة العلمية في مجال المعلومات والاتصالات، وخصوصاً في مجالات الإرهاب وتجارة المخدرات، والاتجار بالسلاح والدعارة المنظمة باستخدام الإنترنت(٢).

وعلي الرغم من هذا الكم الرهيب من الجرائم التي ترتكب علي شبكة الانترنت إلا أن هناك فراغا تشريعيا في مواجهة هذه الجرائم التي مازالت تخضع لقانون الإجراءات العادي الذي أصبح غير قادر علي مواجهة هذه النوعية من الجرائم المستحدثة التي تحتاج إلي تكييفها قانونا محددا.

خاصة وأن الجريمة المعلوماتية لها طبيعتها الخاصة وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

وهذه الطبيعة الخاصة وهذا الاختلاف يعني أن الإجراءات الجنائية التقليدية لا تتناسب بالقدر الكافي لمكافحة هذه الجرائم وتثير مشكلات كبيرة في مجال إجراءات تحقيق الدعوى الجنائية ، ومنها صعوبة التحري والتفتيش والضبط وجمع الأدلة الجنائية وإثبات هذه الجرائم ،وهذا يتطلب صدور قوانين إجرائية خاصة بهذه الجرائم تعالج هذه المشكلات تتواكب مع طبيعة هذه الجرائم ،وتضمن تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة.

وتقتضي مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام تحقيق أمور عدة، منها : ضرورة إعداد كوادر أمنية وقضائية للبحث والتحقيق والمحاكمة في هذا النوع من الجرائم، كذلك تطوير التشريعات الجنائية الحالية سواء الموضوعية أو الإجرائية بإدخال نصوص التجريم

---

(١) د/ محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة دار الثقافة للنشر والتوزيع ، عمان، سنة سنة ١٤٣٠ هـ - ٢٠٠٩م ، ص ٦٠٥.

(٢) د/ محمد أبو العلا عقيدة "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية" بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي ، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع كلية الحقوق جامعة المنصورة - http://www.f-law.net ص ١ ، د/عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي ، مصر سنة ٢٠٠٦م ، ص ١٩.

والعقاب والنصوص الإجرائية اللازمة لمواجهة هذا الإجرام المستحدث. فضلا عن ذلك فإن التعاون الدولي في مجال الأمن والتحقيق وتسليم المجرمين وتنفيذ الأحكام يعد ضرورة لا مفر منها (١).

وقد أحسن المشرع العربي بوضع القانون العربي النموذجي الموحد في شان مكافحة سوء استخدام وسائل تكنولوجيا المعلومات والاتصالات، وأفرد الباب الرابع منه لبعض قواعد الإجراءات الجنائية في شأن جرائم الكمبيوتر والانترنت، وهي القواعد الأكثر أهمية ، محيلاً فيما عداها إلى القواعد العامة في قانون الإجراءات الجنائية المصري ، والذي يشكل القواعد في الإجراءات التي تحكم الدعوى الجنائية سواء في مرحلة الاستدلالات أو التحقيق الابتدائي ، وكذلك مرحلة المحاكمة والطعن على الأحكام .

وركزت المادة ٢٣ من القانون العربي النموذجي الموحد على وجوب الاستعانة بالخبير ألمعلوماتي المتخصص في البرامج واستخدام الانترنت ، تلافيا لحدوث أضرار بالبرامج والبيانات كما ألزم مأمور الضبط القضائي بالبحث عن الجرائم الإلكترونية ومرتكبيها وجمع الاستدلالات اللازمة للتحقيق ، شرط أن يكون مؤهلا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية . وهذا الأمر ينسحب بطبيعة الحال على تأهيل أعضاء النيابة العامة ، وقضاة الحكم في هذا النوع من الجرائم

كما ركزت المادة ٢٦ من ذات القانون على ضمانات حماية سرية البيانات المخزنة في الحاسب الآلي أو الوسيط الإليكتروني ، وعدم المساس بحقوق الغير التي تتعلق بالبيانات والبرامج المخزنة، وذلك عند القيام بعمليات التفتيش والضبط في نطاق الجريمة الإلكترونية.

وقد ساهمت بعض الدول العربية في هذا الشأن فأصدر المقنن المصري قانون التوقيع الاليكتروني رقم ١٥ لسنة ٢٠٠٤م كما أصدر المقنن الإماراتي القانون رقم ٢ لسنة ٢٠٠٦ لمكافحة جرائم المعلومات ، كما أصدر المقنن السعودي نظام مكافحة جرائم المعلوماتية سنة ١٤٢٨هـ ٢٠٠٧م (٢).

---

(١) د/ محمد أبو العلا عقيدة ، مرجع سابق ص٢، ٣. ، د/ نبيله هبة هروال ، الجوانب الاجرائية في مرحلة جمع الاستدلال، طبعة دار الفكر الجامعي ، مصر سنة ٢٠٠٦م، ص ١٣، د/ عبد الله حسين علي محمود" إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات" بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي ، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع منتدى هيئة التحقيق والادعاء السعودي ص ١ .

(٢) د/عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي الموحد ، دار الفكر الجامعي ، مصر سنة ٢٠٠٦م ، ص ٨، ٩.

مشكلة البحث:-

تتمثل المشكلة الرئيسية لهذا البحث في أن الجريمة الإلكترونية لها طبيعتها الخاصة وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

وهذه الطبيعة الخاصة وهذا الاختلاف يعني أن التشريعات الجنائية الخاصة بمواجهة الجرائم التقليدية، لا تصلح للمواجهة الفعالة لهذا النوع من الجرائم؛ وينبغي أن يكون هناك تشريع خاص لمواجهة هذه الجرائم.

كما أن الإجراءات الجنائية التقليدية لا تتناسب بالقدر الكافي لمكافحة هذه الجرائم وتثير مشكلات كبيرة للمحقق في مجال إجراءات تحقيق الدعوى الجنائية ، ومنها صعوبة التحري والتفتيش والضبط وجمع الأدلة الجنائية وإثبات هذه الجرائم ، في إطار تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة ، خاصة وأن نصوص قانون الإجراءات الجنائية وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجميع الأدلة المتعلقة بها .

أهمية البحث :

تكمن أهمية البحث في تنامي دور التعاملات الالكترونية الأمر الذي طرح تحديات عديدة أمام رجال القانون في مجال مكافحة جرائم المعلومات؛ ذلك أن هذه الجرائم تنوعت أساليب ارتكابها و تزايدت مخاطرها و حجم الخسائر الناجمة عنها حتى باتت تهدد الاقتصاد و الأمن القومي للدول التي ترتكز مصالحها الحيوية على التقنية بشكل عام وعلى المعلوماتية بشكل خاص؛ فقد أجرت منظمة ال Alliance Business Software دراسة عن أضرار جرائم الانترنت في بعض دول الشرق الأوسط. أظهرت هذه الدراسة آن هناك تباين بين الدول في حجم خسائرdamages جرائم الانترنت جرائم الحاسب الآلي حيث تراوحت بين ثلاثين مليون دولار أمريكي في المملكة العربية السعودية و الإمارات العربية المتحدة و مليون و أربعمائة ألف دولار أمريكي فقط في لبنان.

وجاء في صحيفة عكاظ السعودية يوم السبت ١٤٣٣/١٠/٢٨ العدد٤١٠٨ ص١٩ شئون وطن

قدر الخبراء في ختام مؤتمرهم ملتقى الجودة الشاملة في الأمن العام تحت شعار «الجودة والتميز واجب وإبداع»بجدة حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا، و بالإضافة لما سبق فانه من الضروري التعرف على جرائم المعلومات ودراسة خصائصها و طبيعتها الخاصة وما تتميز به عن الجرائم التقليدية، في أسلوب و طريقة ارتكابها للعمل على إيجاد تعاون إقليمي ودولي لمكافحتها.

أسباب اختيار البحث:

اختارت هذا البحث للأسباب الآتية:

١- أن الأخذ بمستجدات العصر من وسائل الاتصالات الحديثة أصبح ضرورة عصرية وأن جرائم المعلومات تنوعت أساليب ارتكابها و تزايدت مخاطرها و حجم الخسائر الناجمة عنها حتى باتت تهدد الاقتصاد و الأمن القومي للدول التي ترتكز مصالحها الحيوية على التقنية بشكل عام وعلى المعلوماتية بشكل خاص، وأن المصلحة المجتمعية داعية إلى تذليل كل الصعاب نحو مكافحة هذه الجرائم.

٢- صدور القانون العربي النموذجي الموحد في شان مكافحة سوء استخدام وسائل تكنولوجيا المعلومات والاتصالات، وقانون التوقيع الاليكتروني المصري رقم ١٥ لسنة ٢٠٠٤م والقانون رقم ٢ لسنة ٢٠٠٦ م الإماراتي لمكافحة جرائم المعلومات ، ونظام مكافحة جرائم المعلوماتية السعودي سنة ١٤٢٨هـ ٢٠٠٧م .

دراسة مدى نجاح النظام الجزائي المصري والسعودي في مكافحة هذا النوع من الجرائم.

منهج البحث:

سوف أعتمد في هذا البحث على منهج الاستقراء والتحليل لموضوعات البحث، وعلى البحث المكتبي فيما يتعلق بدراسة عناصر خطة العمل في ضوء التشريعات المختلفة ، مع التركيز على النظام الجزائي المصري، والسعودي، والأبحاث والدراسات التي تناولت مجالات الدراسة ، فضلا عن الاستعانة بالتقارير الصادرة عن الجهات الحكومية المعنية ٠

خطة البحث:

سوف أتناول هذا البحث من خلال مقدمة وفصلين وخاتمة كالتالي:

المقدمة: وتشتمل على أهمية موضوع البحث، وأسباب اختياره، والمنهج العلمي المتبع فيه، وخطة البحث.

الفصل الأول : ماهية الجرائم الإلكترونية ؛ وفيه ثلاثة مباحث كالتالي:

المبحث الأول : التعريف بالجريمة الإلكترونية ، وخصائصها.

المبحث الثاني: سمات المجرم في الجرائم الإلكترونية، ودوافع ارتكابه الجريمة.

المبحث الثالث: أنوع الجرائم الإلكترونية وطرق ارتكابها.

الفصل الثاني : مكافحة الجرائم الإلكترونية ، وفيه ثلاثة مباحث:

المبحث الأول : مكافحة الجرائم الإلكترونية في التشريعات الدولية

المبحث الثاني : مكافحة الجرائم الإلكترونية في التشريع الجنائي المصري.

المبحث الثالث : مكافحة الجرائم الإلكترونية في التشريع الجزائي السعودي.

الخاتمة ، وتشتمل على أهم النتائج والتوصيات .

الفصل الأول
ماهية الجرائم الإلكترونية

تمهيد وتقسيم:

إن الجرائم الإلكترونية (١).لها طبيعة خاصة؛ وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

كما أن هذه الجرائم تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها). وهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، توجه للنيل من الحق في المعلومات ، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت . هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة ، وهذا وحده - عبر دلالته العامة - يظهر مدى خطورة جرائم الكمبيوتر ، فهي تطال الحق في المعلومات ، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري(٢).

لذا فان إدراك ماهية هذه الجرائم ، وخصائصها ، وسمات مرتكبيها ودوافعهم ، وبيان أنواع هذه الجرائم، وطرق ارتكابها وكيفية مواجهتها؛ يتخذ أهمية بالغة لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية، وهذا ما سأتناوله في المباحث التالية:

---

(١) يوجد تعدد بشان الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر وفيما بعد بيئة الشبكات ، وهو تعدد رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط أو المتصل بتقنية المعلومات ، فابتدءا من اصطلاح إساءة استخدام الكمبيوتر ، مرورا باصطلاح احتيال الكمبيوتر ، الجريمة الإلكترونية ، الجريمة المعلوماتية ، فاصطلاحات جرائم الكمبيوتر أو جرائم الحاسب الآلي ، والجريمة المرتبطة بالكمبيوتر ، جرائم التقنية العالية ، والجرائم المعلوماتيّة، وغيرها ، إلى جرائم الهاكرز أو الاختراقات فجرائم الانترنت فجرائم الكمبيوتر والانترنت، والجرائم الرقمية، وجريمة أصحاب الياقات البيضاء ، والجرائم الناعمة ، والجرائم النظيفة ، وأخيرا السيبر كرايم ، وهذا التعدد في ألألفاظ، والمصطلحات المعبرة عن الجريمة الإلكترونية أو جرائم تقنية المعلومات تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد. د/ محمد الأمين البشري "تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت" بحث مقدم إلى الحلقة العلمية (الانترنت والإرهاب) خلال الفترة من: ١٧-٢١ /١٤٢٩/١١هـ الموافق ١٥-١٩ /٢٠٠٨/١١م بالتعاون مع جامعة عين شمس ، منشور على موقع جامعة نايف العربية للعلوم الأمنية ، ص٨ ، "دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول" إعداد:إدارة الدراسات والبحوث ، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز،التعقيب) في الدول العربية المنعقد في جمهورية السودان خلال الفترة ٢٣-٢٥/٩/م الموافق ٧-٩/١١/١٤٣٣هـ، "جرائم الكمبيوتر والانترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية" ، بحث منشور على موقع: WwW.Lawyers-Gate.CoM

(٢) يونس عرب "جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات" ورقة عمل ٢ مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ /٢٠٠٢/٢ ص٢.

المبحث الأول
التعريف بالجريمة الإلكترونية وخصائصها

تقسيم:
سوف أتناول هذا المبحث من خلال مطلبين : أتحدث في المطلب الأول عن التعريف بالجريمة الإلكترونية ، وأتحدث في المطلب الثاني عن خصائص الجريمة الإلكترونية.

المطلب الأول
التعريف بالجريمة الإلكترونية

إن تعريف الجريمة الإلكترونية أو جرائم المعلومات كان محلاً لاجتهادات الفقهاء ، وذهبوا في ذلك مذاهب شتى ووضعوا تعريفات مختلفة ، وبالتالي فليس هناك اتفاق على تعريف فلا نجد تعريفاً محدداً للجريمة الإلكترونية، نتيجة للاجتهادات الفقهية المتشعبة في هذا المجال.

فهناك من تناول تعريف هذه الجريمة من زاوية تقنية(فنية) وهناك من تناولها من زاوية قانونية؛ فالتعريفات القائمة على معيار قانوني ، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة ، وتعريفات قائمة على معيار شخصي ، وتحديدا متطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها. وهناك تعريفات تنظر إلى موضوع الجريمة وأنماطها وبعض العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو سمات مرتكبها وهذه التعريفات كالتالي(١).

أولاً : التعريفات التي تنظر إلى زاوية التقنية:

القائلون بالتعريف التقني يذهبون إلى القول بأن الجريمة الإلكترونية هي :"نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود" (٢).

ويذهب أنصار هذا الاتجاه الفقهي إلى القول بان تعريف جرائم الحاسب الآلي من الناحية القانونية وتصنيف صورها يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جريمة الحاسب الآلي وهي : الحاسب الآلي ، برنامج الحاسب الآلي ، البيانات ، الممتلكات ، الدخول ، الخدمات ، الخدمات الحيوية (٣).

---

(١) د/عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر ، مرجع سابق، ص ٢٠ ، عادل يوسف عبد النبي"الجريمة المعلوماتية وأزمة الشرعية الجزائية" بحث منشور بمركز دراسات الكوفة، العدد السابع ٢٠٠٨م ص ١١١ ، ١١٢، عبد الله بن عبد العزيز الخثعمي " التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية" رسالة مكملة لمتطلبات الحصول على الماجستير، مقدمة لجامعة نايف العربية للعلوم الأمنية، ص ٦٣وما بعدها.

(٢) د/ محمد الأمين البشري التحقيق في جرائم الحاسب الآلي، مرجع سابق ، ص ٦.

(٣) د/ عبد الفتاح بيومي حجازي المرجع السابق ص ٢٠.

وهناك جانب آخر من الفقه يذهب إلى تعريف جريمة الحاسب الآلي بأنها : الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنيت (١).
ويرى أنصار هذا الجانب الفقهي أن من سمات هذه الجريمة أنها جريمة مستترة ، وتتسم بالسرعة والتطور في وسائل ارتكابها ، وهي أقل عنف في التنفيذ من الجرائم التقليدية ، وعابرة للحدود ، ويصعب إثباتها لعدم وجود أدلة مادية عليها ، كما يسهل إتلاف الأدلة الخاصة بها ، ونقص الخبرة العلمية لدى الجهات القائمة على ضبطها ، وعدم كفاية القوانين القائمة التي تعالجها (٢).

ثانياً : التعريفات التي تنظر إلى موضوع الجريمة:
من التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم ، تعريفها بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه " (٣). وتعريفها بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "(٤).
الثاً : التعريفات التي تنظر إلى وسيلة ارتكاب الجريمة :
أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة ، فان أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ، من هذه التعريفات ، يعرفها الأستاذ جون فورستر(٥). بأنها " 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 دورا رئيسا" (٦).
رابعاً : التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل :
جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع ، وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل ، وهي تحديدا سمة الدراية والمعرفة التقنية . من هذه التعريفات ، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام ١٩٧٩ ، حيث عرفتها بأنها " أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها " . ومن هذه التعريفات أيضا تعريف

(١) د/ محمد عبد الرحيم سلطان العلماء "جرائم الانترنيت والاحتساب عليها" بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت جامعة الإمارات مايو ٢٠٠٥ ص ٥ .
(٢) د/ محمد عبد الرحيم سلطان ، مرجع سابق، ص ٥.
(٣) د/ هشام رستم، ورقة عمل بعنوان:" جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة" منشورة بمجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، عدد١٧ عام ١٩٩٥م، ص ٣١.
(٤) د/ هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، ١٩٩٢ ، ص ٢٠
(٥) Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, ١٩٨٩, P. ١٠٤
(٦) مشار إلى هذه التعريفات لدى: د. هشام رستم ، مرجع سابق ، ص ٢٩ و ٣٠ .

David Thompson بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب " . وتعريف Stein Schjqlberg بأنها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا " (١).

وهذا التعريف متبنى من قبل العديد من الفقهاء والدارسين(٢). بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية ، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح إمكانية التعامل مع التطورات المستقبلية التقنية.

وكذا تعريف جريمة الكمبيوتر لخبراء منظمة التعاون الاقتصادي والتنمية، بأنها : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" (٣).

وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام ١٩٨٣ ضمن حلقة (الإجرام المرتبط بتقنية المعلومات)، ويتبنى هذا التعريف الفقيه الألماني Ulrich Sieher ، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

وعَرَّف نظام مكافحة جرائم المعلومات السعودي، الصادر بالمرسوم الملكي رقم م/ ١٧ وتاريخ: ١٤٢٨/٣/٨هـ بناءً على قرار مجلس الوزراء رقم: (٧٩) وتاريخ: ١٤٢٨/٣/٧هـ الجريمة المعلوماتية أو الإلكترونية بأنها:" أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" (٤).

وبالنظر إلى جملة التعريفات السابقة يتضح عدم وجود تعريف متفق عليه لهذه الجريمة ولذا فالتعريف الراجح في نظري لهذه الجريمة أنها :"سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية محله معطيات الكمبيوتر" (٥). فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الإجرامية ، ومعاقب عليه قانونا لان إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق . ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها ، المعلومات

---

(١) د. هشام رستم ، مرجع سابق ، ص ٣٢ .
(٢) د. هشام رستم ، مرجع سابق ، ص ٣٥ .
(٣) انظر موقع المنظمة على شبكة الانترنت .
(٤) عبد الله بن عبد العزيز الخثعمي ، التفتيش في الجرائم المعلوماتية مرجع سابق، ص٦٣ وما بعدها.
(٥) قريب من ذلك، تعريف الأستاذ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، طبعة دار الفكر الجامعي، ٢٠٠٦م ص ١٧٩. وتعريف الاستاذ / يونس عرب، جرائم الكمبيوتر والانترنت ، مرجع سابق ص١١ ، وتعريف د/ محمد عبد الله منشاوي ، جرائم الإنترنت من منظور شرعي وقانوني طبقاً للقانون السعودي، منشور على موقع : http://www.f-law.net

المستخرجة ، والمتبادلة بين النظم) وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوج بين تقنيات الحوسبة والاتصال ، بما في ذلك شبكات المعلومات (١).

المطلب الثاني
خصائص الجريمة الإلكترونية

تمهيد وتقسيم:

تعد الجريمة الإلكترونية إفرازا ونتاجاً لتقنية المعلومات ، فهي ترتبط بها وتقوم عليها ، وهذا ما اكسبها لوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الصفات قد يتطابق بعضها مع صفات طوائف أخرى من الجرائم هذا من ناحية ، ومن ناحية أخرى فأن اختلاف الجريمة الإلكترونية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية .

وسوف أقسم هذا المطلب إلى فرعين: أتناول في الفرع الأول خصائص الجريمة الإلكترونية المشتركة مع بعض الجرائم الأخرى، وأتناول في الفرع الثاني الخصائص التي تنفرد بها الجريمة الإلكترونية.

الفرع الأول
الخصائص المشتركة مع بعض الجرائم

من خصائص الجرائم الإلكترونية أو جرائم المعلومات خطورتها البالغة والحجم الكبير للخسائر والأضرار التي تنشأ عنها ، إضافة إلى أنها توصف بأنها من الجرائم العابرة للحدود، وهي بذلك تشترك مع بعض الجرائم الأخرى كالإرهاب، والاتجار بالمخدرات، وغسيل الأموال، وسوف أتناول هذه الخصائص بشيء من التفصيل فيما يلي:

أولاً : خطورة الجرائم الإلكترونية:

تكتسب دراسة الجرائم الإلكترونية أهمية خاصة نظراً لخطورتها، وذلك لأنها تمس الإنسان في فكره وحياته الخاصة، وتمس المؤسسات في اقتصادها ، والبلاد في أمنها القومي والسياسي والاقتصادي.

كذلك فإن الخسائر الناشئة عن هذه الجرائم توصف بأنها فادحة(٢).

فقد جاء في صحيفة عكاظ السعودية (٣) .

:"كشف خبير عالمي أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم يبلغ ١١٤ مليار دولار، وأكد في ختام ملتقى الجودة الشاملة في الأمن العام تحت شعار «الجودة والتميز واجب وإبداع» نحن أمام تحد جوهري يحتم الإسراع في ضخ ثقافة أمن المعلومات لحماية الأفراد من الابتزاز والجهات والممتلكات من الخسائر الناجمة عن

---

(١) المراجع السابقة نفس الموضع.

(٢) د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ١٩٩٤ ، ص١٩ ، د/ محمود عبابنة ، جرائم الحاسوب وأبعادها الدولية طبعة دار الثقافة للنشر والتوزيع ٢٠٠٩، ص٣٢.

(٣) الصادرة يوم السبت١٤٣٣/١٠/٢٨ العدد ٤١٠٨ ص١٩ شئون وطن .

التساهل في أنظمة الحماية. وشدد عدد من الخبراء العالميين المشاركين في الملتقى، على أن الجريمة إلكترونية أكبر عائق يواجه التعامل مع مختلف القضايا، مشيرين إلى أن أمن المعلومات والاختراق والجرائم الإلكترونية، يحتم على وزارت الاتصالات وتقنية المعلومات الإسراع في نشر المعلومات والإحصاءات في سبيل حماية الوطن ومقدراته من الخسائر والجرائم الإلكترونية الناجمة عن عدم نشر تلك الإحصاءات.

وقدر الخبراء في ختام مؤتمرهم بجدة حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا، متوقعين ارتفاع هذه الأرقام نظرا لتزايد استخدام الإنترنت على نطاق واسع للتواصل وعقد المعاملات والصفقات التجارية من قبل كل من الأفراد والمؤسسات على حد سواء.

ودعا الخبراء لضرورة العمل على مراجعة وتطوير قانون الجرائم الإلكترونية وتطوير أقسام أكاديمية في الجامعات للتعامل مع الجرائم الإلكترونية، إضافة إلى التعاون مع شركات عالمية متخصصة لتقديم استشارات في مجالات الحماية وأمن المعلومات.

ومن جهته أكد الدكتور عايض طالع العمري رئيس مجلس الجودة السعودي في المنطقة الغربية أن العالم يشهد اليوم ثورة هائلة في مجال تقنية المعلومات، وانتشار استخدام الشبكة المعلوماتية (الانترنت) على نطاق واسع حول العالم، حيث تشير آخر الإحصائيات أن عدد مستخدمي الانترنت في العالم أكثر من ٢ مليار مستخدم العام الماضي، وأن عدد مستخدمي الإنترنت في الشرق الأوسط ٦٨.٦ مليون مستخدم، مشيرا إلى أن الدولة الأولى في العالم من حيث عدد مستخدمي الإنترنت هي الصين وبين أن هذا الرقم أدى لانتشار الجرائم الإلكترونية بشكل سريع

وأكد عضو مجلس الجودة السعودي الدكتور هاني حسن فتياني ، أن إحصاءات نشرت مؤخرا أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم يبلغ ١١٤ مليار دولار، وقال: كل ذلك يضعنا أمام تحد جوهري يتمثل في الإسراع في ضخ ثقافة أمن المعلومات لحماية الأفراد من الابتزاز والجهات والممتلكات من الخسائر الناجمة عن التساهل في أنظمة الحماية. وأشار إلى أن الجرائم الإلكترونية كبدت دول مجلس التعاون الخليجي خسائر تقدر بـ ٧٣٥ مليون دولار سنويا، لافتا إلى أن تلك الجرائم إذا كانت تستهدف المؤسسات فإنها تنطوي على أضرار وأخطار جسيمة تلحق بالمؤسسات المستهدفة".

وجاء في الأهرام المسائي المصري(١) .:"حذر خبراء من تزايد معدلات الجريمة الالكترونية في مصر واعتبروها تمثل مشكلة كبري لقطاع الاتصالات والتكنولوجيا المتنامي في الفترة الأخيرة. وقدرت إحدى شركات برامج الحماية من مخاطر الإنترنت حجم الخسائر الناجمة عن جرائم اختراق شبكات الإنترنت والكمبيوتر عالميا بـ٤٠ مليار دولار، في حين تصل سوق برامج الحماية المقلدة والمنسوخة إلى ٢٥% من حجم السوق الإقليمية

(١) الصادرة في نوفمبر ٢٠٠٩ العدد٣ ا.محمد رمضان .

من جانبه اعترف المهندس محمد حجازي مدير مكتب حماية الملكية الفكرية التابع لـ إيتيدا بوزارة الاتصالات بأن نسبة القرصنة التي تتعرض لها برامج الحماية والسوفت وير في مصر تصل إلى ٥٩% وفقا لآخر إحصائية تم إجراؤها في ٢٠٠٩م. وبالإضافة لذلك تعتبر البنوك هي الهدف الرئيسي للنسل الجديد من مجرمي التقنية العالية؛ ذلك لأنها تعتمد اعتمادا كليا ورئيسيا على أنظمة نقل التمويل إلكترونيا EFT ؛ إذ أن بنوك نيويورك وحدها تتناقل ٢٠٠ بليون دولار يومياً فما الذي سيكون عليه الحال إذا ما استطاعت الأيدي المنحرفة على الحصول على رموز التخويل الالكترونية المستخدمة في EFT؟ وكم من الأموال يمكن نقلها في ثوان معدودة إلى خارج البلاد؟".

إضافة إلى هذا النوع من الإجرام ، فإن هناك أنواعا أخرى كالقروض الوهمية وفتح اعتمادات وأشكال أخرى من التلاعب ونصب بطاقات التسليف(١).

وخلاصة الأمر أنه يمكن القول أن جرائم المعلومات تطال المعلومات ، ذلك الحق الذي يمس البناء العلمي والثقافي والاقتصادي والذي ينعكس بدوره ، ويقف عائقاً في طريق التنمية ، كما أن هذه الجرائم تطال حياة الأفراد الخاصة ؛ فالاطلاع على خصوصيات الأفراد جريمة كفلتها كل التشريعات، إضافة إلى تهديدها الأمن القومي للدول ، فالاختراقات التي تمت بواسطة الحواسيب التابعة لوزارة الدفاع الأمريكية هددت الأمن القومي الأمريكي ، إضافة لمخاطر متعددة ، كفقدان الثقة بالتقنية وتهديد الملكية الفكرية وقتل روح الإبداع الإنساني(٢).

ثانياً: الجرائم الإلكترونية جرائم عابرة للحدود:

أخذت تكنولوجيا الحاسب الآلي تلعب دوراً بالغ الأهمية في العالم المعاصر ، وغزت الأسواق سواء الخاصة بالدول المتقدمة صناعياً أو دول العالم الثالث؛ فالدول المتقدمة صناعياً تقوم بتصنيع أجهزة الحاسب الآلي وابتكار برامج ومصنفات لتحقيق الربح المادي ، وتقوم دول العالم الثالث باستقبال هذه المبتكرات واستخدامها على نطاق واسع نظراً لصغر حجمها وقلة كلفتها وتزايد الحاجة اليها.

هذا التطور التكنولوجي في مجال الحاسبات وبرامجها وشبكات الاتصال ، وخاصة شبكة الانترنت جعل الإنتاج الذهني يتصف بالعالمية لأنه لا يقتصر على دولة دون أخرى ؛ فالبشرية كلها شريكة في الاستفادة من هذا الإنتاج الأدبي والذهني(٣).

كما ربطت الانترنت العالم بشبكة اتصال متميزة و فعالة من خلال الأقمار الصناعية و الفضائيات، وجعلت الانتشار الثقافي وعولمة الثقافة و الجريمة أمراً ممكناً و شائعاً.و قربت شعوب العالم بأجناسهم و ثقافتهم المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال.

و استخدام هذه الشبكة أدى إلى سلبيات تمثلت في انتشار الجريمة، وأصبحت الجرائم المستحدثة و المنتشرة بواسطة الإنترنت مشكلة عالمية لا تعترف بالحدود الجغرافية للدول؛

---

(١) د/ محمود عبابنة ، جرائم الحاسوب ، مرجع سابق، ص٣٣.

(٢) د/ جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي)، الكتاب الأول، دار النهضة العربية، ١٩٩٢، ص ١٧.

(٣) د/ محمود عبابنة ، جرائم الحاسوب ، مرجع سابق، ص٣٣.

لارتباط العالم بشبكة واحدة، فغالباً ما يكون الجاني في بلد و المجني عليه في بلد آخر،كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه.وهذا ملاحظ من خلال نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي(١).

وبذلك أعطى انتشار شبكة الانترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، ونتج عن ذلك أن الاستخدام غير الشرعي الناجم عن الاتصال بالحاسوب أيضاً اتصف بالعالمية أو بالعابر للحدود، فالجرائم لم تعد تقتصر على إقليم ولا تتعداه، بل أصبح بالإمكان ارتكاب الجرائم عن طريق الحواسيب باختراقه لحواسيب في بلد آخر أو إتلاف معطياتها، فالتعدي في بلد وأثره في بلد آخر، وصار من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر كما سبق ، وهكذا (٢).

و لهذا فان جرائم الحاسوب تشترك مع غيرها من الجرائم في إنها تتخطى حدود الدول، كتجارة المخدرات و غسيل الأموال ، إلا أنها تتميز عن الأخيرة حيث يمكن ارتكابها دون مغادرة المقعد المقابل للحاسب الآلي بعكس جرائم المخدرات وغسيل الأموال التي تتطلب حركة بين الدول.

ومن الأمثلة على هذه الجرائم عابرة الحدود، تمكن احد الهواة في أوروبا من حل شفرة احد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) و من ثم أصبح المجال مفتوحا للعبث ببيانات هذا المركز، و كذلك الحال في إنتاج الفيروسات(٣).

هذا التباعد أدى إلى إن تتشتت الجهود في مواجهة هذا النوع من الإجرام، فوجود الجاني على سبيل المثال في أوروبا و المتضرر في أمريكا يجعل التصدي لهذا النوع من الإجرام أمرا عسيرا، و ذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق، الأمر الذي حدا بالبعض للقول" بان المجتمعات المعاصرة في ظل التقنية الحديثة، اقتصادا بلا حدود و ثقافة بلا حدود، عن جريمة منظمة بلا حدود حيث تم استغلال الحاسب الآلي فيها أسوا استغلال، فعن طريق الانترنت تم تحويل الأموال الكترونيا و غسلها" (٤)

□

(١) "الجرائم المعلوماتية ونظام مكافحتها في المملكة العربية السعودية" بحث منشور على موقع: http://www.f٤٤g.com.

(٢) د/ محمود عبابنة ، جرائم الحاسوب ، مرجع سابق، ص٣٤..

(٣) د/ عمر الفاروق الحسيني" تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الآلي" بحث منشور في كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، ١٩٩١م.

(٤) د/ محمود عبابنة ، مرجع سابق، ص٣٥..

الفرع الثاني
الخصائص التي تنفرد بها الجرائم الإلكترونية

تعد الجرائم الإلكترونية إفرازا ونتاجاً لتقنية المعلومات ولذا فهي تتميز عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الخصائص ، وهي كالتالي(١):

أولاً: الحاسب الآلي هو أداة ارتكاب الجرائم الإلكترونية:

الحاسب الآلي هو دائما أداة الجريمة في الجرائم التي ترتكب على شبكة الانترنت وهى خاصية متفردة عن أي جريمة أخرى؛ ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الانترنت و قيامه بتنفيذ جريمته أيا كان نوعها؛ وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الانترنت(٢).

ثانياً: أنها جرائم ترتكب عبر شبكة الانترنت:

تعد شبكة الانترنت هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك و الشركات الصناعية و غيرها من الأهداف التي ما تكون غالبا الضحية لتلك الجرائم و هو ما دعا تلك الأهداف إلى اللجوء إلى نظم الأمن الالكترونية في محاولة منها لحماية نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم(٣).

ثالثاً: مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي:

لاستخدام الحاسب الآلي لارتكاب جريمة على شبكة الانترنت لابد وان يكون مستخدم هذا الحاسب الآلي على دراية فائقة و ذو خبرة كبيرة في مجال استخدامه و إلا فأين له بالخبرة اللازمة التي تمكنه من تنفيذ جريمته والعمل على عدم كشفها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي و أن الشرطة أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم (٤).

رابعاً: صعوبة الكشف عن الجريمة الإلكترونية وإثباتها:

لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الالكتروني إلى أي عنف أو سفك للدماء أو آثار اقتحام لسرقة الأموال ، وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحي كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الالكتروني ، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها(٥)

وهناك صعوبة أخرى تتعلق بإثبات الجرائم الإلكترونية حيث إن هذه الجرائم لا تترك أي اثر خارجي ومرئي لها ، ومما يزيد من صعوبة إثباتها ارتكابها في الخفاء وعدم وجود أي اثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام

---

(١) عادل يوسف عبد النبي، الجريمة المعلوماتية مرجع سابق ،ص ١١٤وما بعدها.
(٢) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ، مرجع سابق، ص١٤.
(٣) د/ نبيله هبه هروال الجوانب الإجرائية ، مرجع سابق ، ص ٣٧ .
(٤) منير محمد الجنبيهي،ممدوح محمد الجنبيهي، مرجع سابق، ص١٤.
(٥) د/شمس الدين إبراهيم احمد"وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري" دراسة مقارنة، طبعة دار النهضة العربية القاهرة ط ١ ٢٠٠٥م ، ص ١٠٤،عادل يوسف عبد النبي، الجريمة المعلوماتية مرجع سابق، ص ١١٤وما بعدها.

النبضات الالكترونية في نقل المعلومات فهذه الجرائم تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا(١)

كما توجد صعوبات أخرى تكتنف إثبات هذه الجرائم تكمن في المجرمين الذين يخططون لمثل هذا النوع من الجرائم هم دائماً أصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة تكفل نجاحهم في ارتكاب الجريمة وفرارهم من أعين السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها بالإضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي لإثبات هذه الجرائم ، بالشكل الذي يوجب البحث عن أدلة جديدة وحديثة ناتجة من ذات الحاسب الآلي، وهنا تبدأ صعوبات البحث والتحري عن الدليل ، وجمع هذا الدليل ، وتبدأ إشكالية قبوله إن وجد ومدى مصداقيته على إثبات جريمة تنصب على عناصر غير مادية معلومات وبرامج(٢)خامساً: أنها جرائم ناعمة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل ، السرقة ، الاغتصاب ، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي(٣).

سادساً: خصوصية المجرم في الجرائم الإلكترونية:

قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة ولكن الأمر مختلف تماما بالنسبة للمجرم في الجرائم الإلكترونية أو المجرم ألمعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات(٤)سابعاً: جريمة مغرية للمجرمين:

نظرا للصفات التي تتمتع بها مثل هذه الجريمة والصعوبات التي تثور عند محاولة اكتشافها أو ملاحقتها فإن ذلك يشكل إغراءً كبيرا للمجرمين وخصوصا أنه يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم ، ونتيجة لكل ما سبق تعتبر مثل هذه الجرائم جريمة تستهوي الكثيرين لسهولتها وكثرة مكاسبها (٥).

---

(١) د/ هشام رستم، "الجرائم المعلوماتية، أصول التحقيق الجنائي الفني" مجلة الأمن والقانون، دبي العدد(٢)، ١٩٩٩م، ص٨،
محمد عبد الله ابو بكر سلامة، موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت منشأة المعارف، الإسكندرية ٢٠٠٦ ص٢٠ .

(٢) د/عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص ٤٢ .

(٣) "مقدمة في الجرائم الالكترونية" بحث منشور على موقع :
http://www.startimes.com

(٤) مصعب القطاونة "الإجراءات الجزائية الخاصة في الجرائم المعلوماتية" بحث منشور على موقع:
http://www.lawjo.net

(٥) د/ نبيله هبه هروال، الجوانب الإجرائية ، مرجع سابق ، ص ٣٧ .

المبحث الثاني
سمات المجرم في الجرائم
الإلكترونية ودوافع ارتكابه للجريمة

تمهيد وتقسيم:

إن أية ظاهرة إجرامية، أو أي نمط إجرامي مستحدث له ما يميزه من الخصائص عن غيره، كما قد تختلف دوافع ارتكاب الجريمة الإلكترونية ، فقد يكون الرغبة الإجرامية، وقد يكون شيئا آخر، وعلى ذلك فإن مرتكبي هذه الجرائم المستحدثة لهم من السمات، والدوافع ما يميزهم عن غيرهم من الجناة، وهذا ما سأتناوله من خلال المطلبين التاليين:

المطلب الأول

سمات المجرم في الجرائم الإلكترونية

تتوافر لدى معظم الجناة مرتكبي الجرائم الإلكترونية أو المعلوماتية مجموعة من الصفات أو الخصائص تميزهم عن سواهم من الجناة المتورطين في أنماط الانحراف الأخرى ، ولعل من ابرز هذه السمات ما يأتي: (١).

أولاً: المجرم في الجرائم الإلكترونية يكون صغير السن:

حيث تتراوح أعمار مقترفي الجريمة الإلكترونية بين ١٨ ، ٤٦ سنة ، والمتوسط العمري لهم ٢٥ سنة وهذا مؤشر على أن المجرم ألمعلوماتي يكون من صغار السن لان كبار السن لم يألفوا التعامل مع الحاسب الآلي . كما أن حداثة الطفرة المعلوماتية الهائلة التي يشهدها العالم المعاصر كانت عاملاً في بلورة هذه السمة (٢).

ثانياً: المجرم في الجرائم الإلكترونية يكون ذكيا:

يوصف الإجرام ألمعلوماتي بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف ، فالمجرم ألمعلوماتي إنسان على مستوى من الذكاء ، إضافة إلى انه مجرم متكيف اجتماعياً لا يناصب العداء للمجتمع(٣).

ثالثاً : المجرم في الجرائم الإلكترونية يكون متخصصا ومحترفا:

لا بد أن تتوافر لدى الجناة مرتكبي الجرائم الإلكترونية قدر من المعرفة المعلوماتية ، أي أنهم متخصصون في هذا الشكل من الانحراف والإجرام (٤) ، ولكن هذه السمة ليست عامة ومطلقة وإنما تقتصر على الجرائم التي يستلزم ارتكابها التعامل مع الحاسب الآلي

---

(١) د/ محمود عباينة ، جرائم الحاسوب ، مرجع سابق، ص٣٥، د/ عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت ، مرجع سابق ص ٨٣، وما بعدها، د/ جميل عبد الباقي الصغير ، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص١٥ وما بعدها . ويقسم المتخصصون في ظاهرة الإجرام ألمعلوماتي المجرمين ألمعلوماتيين إلى سبع طوائف على النحو الأتي : الهواة ، المخربون ، مخترقو الأنظمة ، المهنيون ، الجريمة المنظمة ، المتطرفون ، الحكومات . عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية ، مرجع سابق، ص ١٢٩ هامش ٣١.

(٢) د/حاتم عبد الرحمن منصور الشحات ،الإجرام ألمعلوماتي، دار النهضة العربية القاهرة ط ١ ٢٠٠٣ م ص ٨٩ .

(٣) د/عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت ، مرجع سابق ص ٨.

(٤) د/محمد سامي الشوا ، مرجع سابق ص ٥٤ وما بعدها.

ومعالجة المعلومات ، للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسوب كما في البنوك أو المفاعلات النووية والمؤسسات العسكرية(١).

خامساً: المجرم في الجرائم الإلكترونية مجرم عائد:

غالباً ما يعود مرتكبي الإجرام ألمعلوماتي إلى ارتكاب جرائم أخرى في مجال المعلوماتية رغبة منهم في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحكمة في المرة الأولى ، فيؤدي ذلك إلى العود لارتكاب الجريمة فينتهي بهم الأمر في المرة الثانية إلى كشفهم وتقديمهم للمحاكمة (٢).

ويمكن حصر أنواع الجناة في جرائم الحاسب الآلي في أربعة فئات كالتالي(٣):

الفئة الأولي : العاملون على أجهزة الحاسب الآلي في منازلهم نظرا لسهولة اتصالهم بأجهزة الحاسب الآلي دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

الفئة الثانية : الموظفون الساخطون على منظماتهم التي يعملون بها فيعودون إلى مقار عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو حتى سرقته.

الفئة الثالثة : فئة المتسللين (Hackers) ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين اللذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتويات ذلك الجهاز، وتقع اغلب جرائم الإنترنت حاليا تحت هذه الفئة بقسميها.

الفئة الرابعة:العاملون في الجريمة المنظمة كعصابات سرقة السيارات حيث يحددون بواسطة الشبكة أسعار قطع الغيار ومن ثم يبيعون قطع الغيار المسروقة في الولايات الأعلى سعرا.

المطلب الثاني

دوافع ارتكاب الجرائم الإلكترونية

هناك عدة دوافع إلى ارتكاب الجريمة الإلكترونية ، قد يقف وراءها مصدر واحد هو الرغبة الإجرامية، ويمكن إيجاز هذه الدوافع فيما يلي(٤):

---

(١) د/حاتم عبد الرحمن منصور الشحات، مرجع سابق ص ٩٠.

(٢) د/عبد الفتاح بيومي حجازي ، مرجع سابق ص ٨٣

(٣) محمد عبد الله المنشاوي "جرائم الانترنت في المجتمع السعودي" رسالة ماجستير مقدمة إلى كلية الدراسات العليا بأكاديمية نايف العربية للعلوم الأمنية سنة ٢٠٠٣م ص ٢٨.

(٤) وتجدر الإشارة إلى أن الدافع أو الباعث على ارتكاب الجريمة بصفة عامة لا يعتد به في التشريعات الجزائية المختلفة اكتفاءً بتوافر القصد الجنائي بعنصريه (العلم والإرادة) غير أنه لا يمكن إهمال الدافع والباعث على ارتكاب الجريمة وذلك لأنه يقدم لنا تفسيراً للجريمة وأسباب ارتكابها. د/ محمود عبابنة ، جرائم الحاسوب وأبعادها الدولية مرجع سابق، ص٢٢ .

أولا : الدوافع الشخصية:

يمكن رد الدوافع الشخصية لدى مرتكب الجريمة الإلكترونية إلى السعي لتحقيق الربح ، فهذا الدافع المادي يعد من أهم البواعث إلى ارتكاب الجريمة الإلكترونية لما يحققه من ثراء شخصي فاحش ، وقد تكون الرغبة في تحدي وقهر النظام التقني المعلومات وإثبات الذات وتحقيق انتصار شخصي على نفس الأنظمة المعلوماتية من بين الدوافع الذهنية أو النمطية لارتكاب الجريمة (١).

ثانياً : الدوافع الخارجية:

وعلى رأس هذه الدوافع ، الدوافع السياسية، فقد سخرت الدول شبكة الانترنت في الصراعات السياسية الدائرة اليوم ، وشهدت السنوات القليلة الماضية محاولات دولية لاختراق شبكات حكومية في مختلف دول العالم، فالتجسس عبر الانترنت يتم يومياً، من قبل أجهزة المخابرات ، كذلك فإن بعض الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية(٢).

وفي بعض المواقف أن يستسلم بعض الأفراد للمؤثرات الخارجية ، ولعل من أبرزها الحاجة إلى اختصار عنصر الزمن ، وتوفير سنوات عدة من البحث ، وتحاشي استثمار الملايين من الدولارات، في مجال البحث العلمي ، إذ تدفع الحاجة بعض المنشآت، بل وحتى بعض الدول، إلى الاتصال بالأفراد، الذين يشغلون أماكن حساسة في إحدى المنشآت، كي يعملوا لصالح منشآت أخرى منافسة، بهدف الاطلاع على بعض المعلومات والتقنيات المتوفرة لديها للاستفادة منها ، وتستخدم في ذلك عدة أساليب ، منها الرشوة أو الإقناع والإغراء المقترن بالتهديد ، والذي قد يصل في بعض الأحيان إلى زرع جواسيس في تلك المنشآت(٣).

وقد يكون دافع جنون العظمة، أو الطبيعة التنافسية، هي التي تدفع بعض العاملين في المنشأة لإظهار قدراتهم الفنية الخارقة لإدارة المنشأة ؛ فيفضي به ذلك إلى ارتكاب مثل هذه الجرائم ، حتى ينافس زملائه للوصول إلى أعلى المراكز المرموقة، وأخيرا قد يكون دافع الانتقام من رب العمل أو احد الزملاء أو الأصدقاء من بين البواعث الدافعة إلى ارتكاب الجريمة (٤).

□

(١) د/ احمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر العربي الإسكندرية ص ٩٨ وما بعدها، عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية ، مرجع سابق، ص ١١٧، وما بعدها ..

(٢) د/ محمود عبابنة ، جرائم الحاسوب وأبعادها الدولية مرجع سابق، ص٢٦ .

(٣) د/ محمد سامي الشوا المرجع السابق ص ٦١ ٦٢.

(٤) د/ احمد خليفة الملط المرجع السابق ص٩٩.

المبحث الثالث
أنواع الجرائم الإلكترونية وطرق ارتكابها

تقسيم:
سوف أتناول هذا المبحث في مطلبين : أتحدث عن أنواع الجرائم الإلكترونية في المطلب الأول، ثم أذكر طرق ارتكابها في المطلب الثاني.

المطلب الأول
أنواع الجرائم الإلكترونية

هناك عدة تصنيفات للجرائم الإلكترونية أو للجرائم الإلكترونية؛ فهناك من الباحثين من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي وجرائم أخرى ترتكب بواسطته، أو بحسب الأسلوب المتبع في الجريمة أو الباعث والدافع لارتكاب الجريمة (١). وعلى ذلك تقسيم الجرائم الإلكترونية بحسب ما يستهدفه المجرمون من هذه الجريمة إلى أربعة أنواع، كالتالي(٢):

النوع الأول : يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية . ومع أن وجود هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقاية والتي قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديث وغير معروف من السابق .

النوع الثاني: يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة ، وما يميز هذا النوع من الجرائم انه من الصعوبة بمكان اكتشافه مالم يكن هناك تشابهه في بعض أسماء أصحاب هذه البطاقات.

النوع الثالث: يشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة.

---

(١) مقدمة في الجرائم الالكترونية، بحث منشور على موقع : **http://www.startimes.com**

(٢) د/علي جبار الحسيني، جرائم الحاسوب والانترنت، طبعة دار اليازوري العلمية للنشر والتوزيع، الأردن، ٢٠٠٩م ص٥٥ ،٥٦، منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ، مرجع سابق ص٢٢،٢٣ ، محمد عبد الله المنشاوي "جرائم الإنترنت من منظور شرعي وقانوني طبقا للقانون السعودي" منشور على موقع : **http://www.f-law.net** ، عبد الله بن عبد العزيز الخثعمي ، التفتيش في الجرائم المعلوماتية ، مرجع سابق، ص ٦٨وما بعدها.

النوع الرابع: يشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل.

وأبرز التصنيفات وأشملها لأنواع جرائم المعلومات ما ذكره بعض الباحثين (١) وهو كالتالي:

تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة .

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات ، وهو التصنيف الذي يعكس أيضا التطور التاريخي لظاهرة جرائم الكمبيوتر والانترنت ؛ ولهذا نجد أن الجرائم الإلكترونية أو جرائم المعلومات بالاستناد إلى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية :-

أولا : الجرائم الماسة بقيمة معطيات الحاسوب. وتشمل هذه الطائفة فئتين، أولهما، الجرائم الواقعة على ذات المعطيات، كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آليا، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات ، وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آليا واستخدامها).

ثانيا : الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة . وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة،

ثالثا : الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) . وتشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.

هذا من جهة، ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج ، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل. وهو في الحقيقة تمييز - ليس مطلقا

(١) يونس عرب، جرائم الكمبيوتر والانترنت ، مرجع سابق ص٥ وما بعدها.

- بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية. ولا بد لنا من الإشارة، أن حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر إلى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم.

تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة .

الكمبيوتر في الجريمة ، قد يكون هدف الاعتداء ، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات ، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم الكمبيوتر) وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر) ، وقد يكون الكمبيوتر أخيرا بيئة الجريمة أو وسطها أو مخزنا للمادة الإجرامية ، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور الأول جرائم التخزين ، ويقصد بها تخزين المواد الإجرامية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها ، والثاني ، جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانوني والاصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الانترنت ، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الالكتروني للأموال وغيرها باعتبار أن مواقع الانترنت تتصل بشكل رئيس بهذه الأنشطة ، والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها . وهذا التقسيم شائع بجزء منه (وهو تقسيم الجرائم إلى جرائم هدف ووسيلة) (١). وتبعا له تنقسم جرائم الكمبيوتر إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها ، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر . أما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا ، وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام ٢٠٠١ – ذلك أن العمل منذ مطلع عام ٢٠٠٠ يتجه إلى وضع إطار عام لتصنيف جرائم الكمبيوتر والانترنت وعلى الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة هذه الجرائم ، وهو جهد تقوده دول أوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا وأمريكا ، وضمن هذا المفهوم نجد الاتفاقية المشار إليها تقسم جرائم الكمبيوتر والانترنت إلى الطوائف التالية – مع ملاحظة أنها تخرج من بينها طائفة جرائم الخصوصية لوجود اتفاقية أوروبية مستقلة تعالج حماية البيانات الاسمية من مخاطر المعالجة الآلية للبيانات – اتفاقية ١٩٨١ م.

(١) د جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الإلى، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، ١٩٩٢، ص٢٥.

ولذا فقد أوجدت الاتفاقية الأوروبية تقسيما جديدا نسبيا ، فقد تضمنت أربع طوائف رئيسة لجرائم الكمبيوتر والانترنت .

الأولى : - الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية) المعطيات والنظم وتضم :-

الدخول غير قانوني (غير المصرح به) .

الاعتراض غير القانوني .

تدمير المعطيات .

اعتراض النظم .

إساءة استخدام الأجهزة .

الثانية : الجرائم المرتبطة بالكمبيوتر وتضم : -

التزوير المرتبط بالكمبيوتر .

الاحتيال المرتبط بالكمبيوتر .

الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية .

الرابعة : الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات .

٣- تصنيف الجرائم تبعا لمساسها بالأشخاص والأموال .
نجد هذا التصنيف شائعا في الدراسات والأبحاث الأمريكية – مع فروق بينها من حيث مشتملات التقسيم ومدى انضباطيته ، كما نجده المعيار المعتمد لتقسيم جرائم الكمبيوتر والانترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع ويعكس هذا الاتجاه التقسيم الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت الموضوع عام ١٩٩٨ الذي تم وضعه من قبل فريق بحثي أكاديمي ، والمسمى **Model State Computer Crimes Code** ، وفي نطاقه تم تقسيم جرائم الكمبيوتر والانترنت إلى ، الجرائم الواقعة على الأشخاص ، والجرائم الواقعة على الأموال عدا السرقة ، وجرائم السرقة والاحتيال ، وجرائم التزوير ، وجرائم المقامرة والجرائم ضد الآداب – عدا الجرائم الجنسية ، والجرائم ضد المصالح الحكومية ويلاحظ ان التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء ، لكنه ليس تقسيما منضبطا ولا هو تقسيم محدد الأطر ، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال ، أما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار ، والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة.

المطلب الثاني
طرق ارتكاب الجرائم الإلكترونية

هناك الكثير من الخطوات التي يجب أن يقوم بها من ينوي مهاجمة الأنظمة الحاسوبية، وهذه الخطوات يتطلب القيام بها الكثير من الوقت والجهد، إلا أن الهكرة المتمكنين يقومون بتطوير برمجيات تتولى تنفيذها بشكل آلى والاستمرار في أداء ذلك ولساعات طوال نيابة عنهم (١).
والأساليب المستخدمة في ارتكاب هذه الجرائم، وكذلك الأدوات التي تستعمل لتنفيذها من الكثرة والتنوع بحيث يصعب الإحاطة بها، ولعل من أشهرها وأكثرها استخدامًا ما يلي(٢) :

أولاً: كسر كلمات السر Password Cracking :
تقوم فكرة كسر كلمات السر بصفة عامة على محاولة تخمين هذه الكلمة وتجربتها فإن كان التخمين موفقًا وإلا تتم تجربة كلمة أخرى حتى التوصل إلى الكلمة المناسبة التي تسمح للهكر بولوج النظام(١).

The Honeynet Project (٢٠٠٢). Know Your Enemy: Revealing The Security
(١) Tools, Tactics, and Motives of The Blackhat Community. Boston: Addison-Wesley.١٠٩

(٢) محمد بن نصير محمد السرجاني"مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت"رسالة ماجستير مقدمه لجامعة نايف العربية للعلوم الأمنية، سنة ٢٠٠٤م ص ٥٢ وما بعدها.

وفي معظم أنظمة التشغيل الحديثة يتم تشفير كلمة السر الخاصة بولوج كل مستخدم إلى النظام ومن ثم حفظها ضمن قائمة تحوى كلمات السر الخاصة بجميع المستخدمين في أحد الملفات الخاصة بنظام التشغيل.

وفي حال نجاح الهكر في اختراق النظام باسم مستخدم عادي فإنه سيحتاج غالبًا إلى محاولة الحصول على صلاحيات أكبر تمكنه من السيطرة الكاملة على النظام ألمخترق وذلك من خلال الحصول على اسم المستخدم و كلمة المرور الخاصة بأحد مدراء النظام وربما كبير مديري النظام root ، وفي سبيل تحقيق هذا الهدف يلجأ الهكر إلى أخذ نسخة من الملف المشفر الذي يحتوي على قائمة كلمات السر ويبدأ في العمل على كسر التشفير الخاص بكلمات السر للتمكن من قراءتها في شكلها النصي واستخدامها للولوج إلى النظام، وربما قام بمحاولة كسر كلمات السر من خلال تجربة كلمات السر المتوقعة مباشرة على الحاسوب المستهدف بالاختراق (٢).

وهناك عدة أساليب للقيام بذلك من أشهرها أسلوب هجوم القاموس Dictionary Attack ، والذي يعتمد على كلمات القاموس اللغوي الموجودة في ملف نصي مرفق بالأداة ويتم تجربة هذه الكلمات بطريقة الية الواحدة تلو الأخرى على أمل أن تكون كلمة السر المستخدمة من بين هذه الكلمات، والأسلوب الثاني هو أسلوب الهجوم الضارب–Brute Force Attackويقوم على تركيب عشوائي للكلمات عن طريق تجربة ترتيب الحروف الأبجدية والأرقام بشكل معين وتجربتها فإن لم تنجح يتم تجربة تشكيلة أخرى من الحروف، وهكذا حتى الوصول إلى كلمة السر وكسرها، ويتميز الأسلوب الأخير بقدرته على كسر أية كلمة سر في حين أن هجوم القاموس لا يمكنه كسر أية كلمة سر غير تلك الموجودة في قاموسه الخاص.

وهناك الكثير من البرامج التي تقوم بعملية كسر كلمات السر، وهي متاحة على الإنترنت والعديد منها مجاني مثل Unsecure و Webcrack وL٠phtCrack (٣).

ثانياً: التجسس على رزم البيانات: Packet Sniffing

ويقوم هذا الأسلوب الشائع، على استخدام نوع من الأدوات البرمجية الخاصة يطلق عليها Sniffers تقوم بالتقاط وتحليل كل حزم البيانات التي تمر عبر الشبكة التي يرتبط بها الحاسوب الذي تعمل عليه تلك الأداة.

***Garfinkel, S., Spafford, G., & Schwartz, A. (٢٠٠٣).*Practical Unix & Internet** (٣)

Security. Sebastopol, California: O'Reilly & Associates.

***Chirillo, John (٢٠٠٢) b.* Hack Attacks Revealed**. Indianapolis, Indiana: Wiley Publishing.

(٤)

***Cole, Eric (٢٠٠٢).* Hackers Beware: Defending Your Network From The Willy** (١)

Hacker. Indianapolis, Indiana: New Riders Publishing.

وهذه الأدوات قادرة على استراق أية معلومات يتم تداولها عبر الشبكة المحلية مثل أسماء المستخدمين وكلمات المرور أو بيانات بطاقات الائتمان وأحيانًا تستهدف محتوى رسائل البريد الالكتروني ومن ثم يتم استخدام المعلومات التي تم الحصول عليها بهذا الأسلوب، في إتمام عملية الاختراق وربما غيرها من جرائم الحاسوب والإنترنت الأخرى، وهناك الكثير من الأدوات المجانية التي يمكن استخدامها للتجسس على حزم البيانات، وهي متوفرة على شبكة الإنترنت مثل Windump و Ethereal و EtherPeek لبيئة النوافذ و tcpdump و sniffit و Etherealو SuperSniffer لبيئة يونيكس (١) .

ثالثاً: مسح تحديد قابلية التعرض للهجوم: Vulnerability Scanning

وهذا الأسلوب شبيه بأسلوب مسح المنافذ إلا أنه في حين يستهدف الأخير معرفة المنافذ المفتوحة ومحاولة تحديد الخدمات التي تعمل من خلالها، يقوم أسلوب تحديد قابلية التعرض للهجوم على مسح الحواسيب المرتبطة بالشبكة أو حاسوب واحد فقط بحثًا عن ثغرات أمنية معروفه في أنظمة التشغيل أو بعض برمجيات الخادم ، وتستخدم لهذا الغرض أدوات برمجية مصممة لكشف نقاط ضعف الأنظمة والبرمجيات ومدى قابليتها للاختراق، وهذه القابلية ترتبط عادة إما بوجود أخطاء برمجية في الشفرة Bugs ، أو سوء الإعداد لمستوى الأمان في الشبكات والحواسيب نتيجة عدم تمّ كن مدير الشبكة أو مدير النظام من عمله ، وهناك العديد من هذه الأدوات متوفرة على الإنترنت، منها , SATAN SAINT,.. Titan وغيرها (٢).

رابعاً: الاتصال الاجتماعي:

وهو أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري تمامًا وليس لها أية أبعاد تقنية. حيث يستخدم الهكر مهاراته في الاتصال مع الآخرين ويستعمل الخداع والكذب ليحصل منهم على معلومات ذات طابع تقني يتمكن بواسطتها من القيام بعملية الاختراق وغالبًا ما تتم هذه العملية من خلال المحادثات الهاتفية

ويعتبر هذا الأسلوب، رغم بعده عن الجانب التقني وربما سهولته في نظر الكثيرين، فن مهم يستطيع من يجيده أن يخترق العديد من الشبكات بسهولة كبيرة .حتى أن واحدًا من أشهر الهكرة ويدعى كيفن ميتينك ذكر في كتاب ألفه بعنوان فن الخداع أن أكثر الاختراقات التي قام بها كانت باستخدام هذا الأسلوب (٣).

ومن الأساليب المشهورة في هذا المجال، أن يتصل الهكر بأحد مدراء الشبكة ويدعي أنه مستخدم جديد منتحً لا صفة أحد الموظفين الجدد، ويطلب معلومات ولوج النظام

Rubin, Aviel (٢٠٠١). **White-Hat Security Arsenal: Tackling the Threat**.

(٢)

Boston: Addison-Wesley.

Cronkhite, C., & McCullough, J. (٢٠٠١). **Access Denied: The Complete Guide**

to (٣)

Protecting Your Business Online. Berkeley, California: Osborne/McGraw-Hill.

Mitnick*, K. & Simon, W (* ٢٠٠٢*).* The Art of Deception: Controlling the

(١) Human Element of Security. Indianapolis, Indiana: Wiley Publishing.

المخصصة لهذا الموظف الجديد، أو أن يتصل الهكر بأحد أقسام العمل في المنظمة التي يريد اختراق شبكتها، ويدعي أنه أحد الفنيين المسئولين عن الشبكة وأنه قدُ كلف بتأكيد اسم المستخدم وكلمة المرور الخاصة بكل موظف في ذلك القسم، وبالتالي قد يحصل على اسم مستخدم وكلمة مرور يتمكن بواسطتها من ولوج الشبكة مستغلا الخداع وعدم معرفة الموظفين بمبادئ أمن المعلومات (١).

خامساً: مسح المنافذ : Port Scanning

وهو عبارة عن محاولة إجراء اتصال شبكي بالعديد من المنافذ على الحاسوب المستهدف بغرض كشف نوع الخدمات الشبكية التي تعمل عليه، ونظام التشغيل الخاص به، أو تطبيقات معينة ذات ثغرات أمنية معروفة ليتم استغلال بعض المنافذ التي تكون في حالة استماع Listening في محاولة الاعتداء على هذا الحاسوب إما بالاختراق أو التعطيل عن العمل .

ويهدف هذا الأسلوب إلى مسح أكبر عدد ممكن من المنافذ في الحاسوب الواحد أو منافذ محددة في حواسيب تقع ضمن نطاق شبكة واحدة أو عدة شبكات وكشف نقاط الضعف في كل حاسوب، حتى أن بعض الأدوات المخصصة للقيام بذلك تحتوي على قاعدة بيانات بالأساليب الشائعة الاستخدام لاستغلال كل نقطة ضعف.

وهناك طرق كثيرة لاستخدام هذا الأسلوب، تتفاوت قليلا من الناحية التقنية، ولكل منها استخدامات خاصة، مثل المسح ألتزامني الخفي Stealth SYN Scan ، والمسح العاطل ،Idle Scanning وأسلوب الطعم الخادع Spoofing Decoys ، وغير ذلك من طرق استخدام هذا الأسلوب.

وهناك العديد من الأدوات البرمجية المصممة للقيام بهذه المهمة وتسمى Port Scannersوأكثرها مجاني ومتاح على شبكة الإنترنت ومنها على سبيل المثال WinScanو Super Scanner وتعمل في بيئة نوافذ مايكروسوفت وكذلك nmap و netcat لبيئة يونيكس (٢).

سادساً : الإدارة عن بعدRemote Administration :

وهذا الأسلوب يقوم على السيطرة الكاملة عن بعد على حاسوب مرتبط بالشبكة المحلية أو بالإنترنت من حاسوب آخر موجود على نفس الشبكة أو على الإنترنت. ويستخدم لهذه العملية برنامج مكون من أداتين منفصلتين إحداهما موجودة في حاسوب الهكر ويقوم من خلالها بإدارة حاسوب الضحية أما الأداة الأخرى فتكون في حاسوب الضحية وتقوم بتلقي الأوامر القادمة من حاسوب الهكر وتنفيذها. ولعل أبرز مثال على هذا النوع من

***Chirillo, John (٢٠٠٢) a*. Hack Attacks Revealed**. Indianapolis, Indiana: Wiley

(٢) Publishing

***McClure, S., Scambray, J. & Kurtz, G. (٢٠٠١)* Hacking Exposed: Network Security** (٣)

البرمجيات برامج حصان طروادة ومن أشهرها Sub و Net Bus و Back Orifice (١).

سابعاً : مسح الخطوط الهاتفية : War Dialing

ويعتمد هذا الأسلوب على استخدام برنامج خاص يشغل على حاسوب موصول بخط هاتفي، بحيث يتم تزويد هذا البرنامج بقائمة أرقام هواتف أو تحديد مدى معين من أرقام الهواتف المتسلسلة، ثم يقوم البرنامج بالاتصال بهذه الأرقام الواحد تلو الآخر وتحديد ما إذا كان يوجد على الطرف الآخر جهاز حاسوب أو جهاز ناسوخ (فاكس) أم مجرد جهاز هاتف صوتي فقط ، ويتم تسجيل أرقام الهواتف التي يرتبط بها جهاز حاسوب ليتم فحصها بشكل دقيق من قبل الهكر في وقت لاحق بحثا عن طريقة لاختراقها .

وهناك العديد من البرامج التي تدعم هذا الأسلوب وهي مجانية ومتوفرة على الإنترنت ومنها برنامج Toneloc وهو من أقدمها ويعمل على نظام دوس، وبرنامج-THC Scanوهي أداة طورها مجموعة من الهكرة الألمان (٢).

ثامناً : التشفير: Cryptography

التشفير هو فن تغيير الشكل الظاهري للمعلومات بحيث يتم إخفاء معناها الحقيقي. وهو عامل مهم في أمن المعلومات إلا أنه متى ما تم استخدامه من قبل المجرمين والإرهابيين لتشفير اتصالاتهم وملفات المعلومات الخاصة بخططهم، فإنه يشكل معضلة بالنسبة لرجال الشرطة، فالتعامل مع الملفات المشفرة أمر صعب خاصة في ظل تطور تقنيات التشفير ووجود برمجيات ذات واجهة رسومية جعلت القيام به أمرًا سهلا بالإضافة إلى التزايد الهائل في قدرة الحواسيب الشخصية على معالجة البيانات وبالتالي سرعة تشفير الملفات مهما كان عددها كثيرًا أو أحجامها كبيرة. (٣)

وعملية كسر التشفير ليست بالأمر الهين، فقد أورد ليتمن Littman في كتابه عن مطاردة الهكر الشهير كيفن متنك، كيف أن الأخير قام بتشفير كامل ملفاته التي تم التحفظ عليها كجزء من أدلة الإدانة باستخدام المواصفات المعيارية DES ، وقد استطاع رجال العدالة التوصل إلى مفتاح التشفير المستخدم، في عملية تمت بواسطة كمبيوتر عملاق تابع لوزارة الطاقة الأمريكية واستغرقت عدة شهور، بتكلفة وصلت إلى مئات الآلاف من الدولارات(٤).

---

(١) ***Tulloch,Mitch (٢٠٠٣)***. Microsoft Encyclopedia of Security. Redmond, Washington: Microsoft Press

(٢) ***Tulloch, Mitch (٢٠٠٣)***. Op.cit.

(٣) محمد بن نصير محمد السرجاني، مرجع سابق ص ٥٨.

(٤) ***Littman, Jonathan (١٩٩٧).*** The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen. Boston: Little, Brown and Company.

وفي دراسة أجراها عام ٢٠٠١ ، المعهد الوطني للعدالة في أمريكا، وشملت ١٢٦ من رجال تنفيذ العدالة، يمثلون ١١٤ وكالة حكومية أو مكتب حكومي، أفاد ٦٢ ٪ من مجموع العينة بأنه ليس لدى مختبراتهم الجنائية القدرة على فك التشفير أو أن قدرتها ضعيفة، بينما أجاب ٢٠ ٪ بأنه لا يدري، وهذا مؤشر على مدى خطورة استخدام هذا الأسلوب وربما عدم جاهزية أجهزة العدالة الجنائية للتعامل معه حتى الآن. (١)

تاسعاً: استراق ضربات لوحة المفاتيح Keystroke Monitoring :

ويتمثل هذا الأسلوب في اعتراض كل مفتاح يتم النقر عليه ضمن لوحة المفاتيح الخاصة بالحاسوب الضحية، وتسجيله في ملف خاص بطريقة خفية ودون معرفة الشخص الذي يستخدم الحاسوب. وتسمى الأدوات المستخدمة للقيام بذلك، لاقطات ضربات لوحة المفاتيح Keystroke Loggers، وتأتي على شكل قطعة حاسوبية Hardware صغيرة الحجم لا يستغرق تركيبها داخل لوحة مفاتيح الحاسوب أكثر من دقيقة واحدة، مثل القطعة المسماه Keyghost ، كما تأتي أيضًا على شكل برامج حاسوبية يتم دسها داخل الحاسوب بطرق عدة بحيث تسجل كل حرف أو رقم يقوم مستخدم هذا الحاسوب بطباعته وتسجيله في ملف خفي ليتم جمعه لاحقًا، بل إن بعض هذه البرامج يقوم بإرسال محتوى هذا الملف إلى الهكر فور اتصال الجهاز المصاب بالإنترنت وبدون علم صاحب الحاسوب، ومن أمثلة هذه البرامج Spector Pro Data Interception (٢).

عاشراً: مولدات أرقام بطاقات الائتمان:

وهي برمجيات تقوم عند استخدامها بتوليد أرقام بطاقات ائتمانية عشوائية تتوافق مع التقسيمات الخاصة بالبطاقات الائتمانية لكل بنك ولكل دولة، وبعضها يولّد معلومات متكاملة تشمل بالإضافة إلى ما ذكر اسما وعنوانًا وهميًا، ويمكن لأي شخص أن يستخدم هذه المعلومات على الإنترنت لشراء البضائع من بعض المواقع التي لا تتوافر لديها تقنيات التحقق الفوري من صلاحية بطاقات الائتمانية(٣).

حادي عشر: اختطاف جلسة الاتصال الشبكي: Session Hijacking

يتم انتقال البيانات خلال أي شبكة على شكل حزم تنتقل بين طرفين على الشبكة بعد أن تتم عملية الاتصال بينهما بما يتطلبه ذلك من شروط تقنية، ولكن يمكن باستخدام هذا الأسلوب وفي ظل الظروف المناسبة التجسس على هذه الحزم ومن ثم خطف الاتصال بتحييد أحد أطراف الاتصال وإيهام الطرف الآخر باستمرارية الاتصال مع الحاسوب الأصلي في حين يكون الاتصال قد أصبح بين الحاسوب الضحية وحاسوب الهكر وبذلك يتمكن المهاجم من تنفيذ أوامر على الحاسوب الضحية ويعتبر هذا الأسلوب بالغ التعقيد من الناحية النظرية،

---

(١) ***Hollis, S., David, S. B., David, J. I., Richard B., Wayne, C., & Wayne, P. W. (٢٠٠١). Electronic Crime Needs Assessment for state and Local Law Enforcement***

Shinder, Debra (٢٠٠٢). Scene Of The Cyber crime: Computer Forensics Handbook. Rockland, MA: Syngress Publishing.

(٢)

(٣) محمد بن نصير محمد السرجاني، مرجع سابق ص ٦٠.

فالأمر يتطلب شخصًا على درجة عالية من المهارة والتمكن في تقنية الشبكات ليتم تنفيذه يدويًا، إلا أنه يوجد عدة برامج تم تصميمها لتجعل من تنفيذه أمرًا أكثر سهولة ومن هذه البرامج برنامج Juggernaut و.Hunt. (١)

ثاني عشر: تمويه العنوان الشبكي: IP Spoofing

ويتمثل هذا الأسلوب في التلاعب في ترويسة حزم البيانات الصادرة من عنوان شبكي خاص بحاسوب ما لتبدو وكأنها قادمة من عنوان شبكي خاص بحاسوب آخر ويتم ذلك من خلال تعطيل أحد الأجهزة الموثوق فيها بالنسبة للجهاز الضحية باستخدام أساليب عديدة لذلك، ومن ثم وباستخدام العنوان الشبكي الخاص بهذا الحاسوب المعطَّل يتمكن مستخدم هذا الأسلوب من إيجاد اتصال شبكي موثوق بين جهازه والجهاز الضحية وبالتالي تنفيذ أوامر تسهل له اختراق الحاسوب المستهدف، ويمكن القيام بذلك أيضًا مع رسائل البريد الإلكتروني فبالإضافة إلى سهولة تمويه العنوان البريدي إلى عنوان يثق فيه الضحية يمكن أيضًا تمويه العنوان الشبكي IP Address لينخدع بذلك حتى المستخدم المتقدم أيضًا .(٢)

ثالث عشر: التخّفي الشبكي : Anonymity

كما يحرص المجرم التقليدي على سرية هويته، كذلك مرتكب جرائم الحاسوب والإنترنت، ونظرًا لأن الهوية على الشبكات بما فيها الإنترنت تتمثل بالدرجة الأولى في العنوان الشبكي IP Address ، فإن التركيز ينصب على أن لا ينكشف هذا العنوان للطرف الآخر من الاتصال تحت أي ظرف من الظروف. وفي سبيل ذلك يتم استخدام العديد من الأساليب لتحقيق هذا الهدف، مثل استخدام معيدات إرسال البريد الإلكتروني Remailers، وهي خوادم تتلقى البريد من شخص ما وتعيد إرساله إلى شخص آخر يحدده، مع ضمان عدم ظهور العنوان الشبكي الخاص بالمرسل، حيث يظهر عنوان الخادم عوضًا عنه.

وكذلك يتم استخدام بعض المواقع على الإنترنت التي تقدم خدمة التخفي، بحيث يستطيع المستخدم تصفح المواقع على الشبكة العالمية دون أن تسجل هذه المواقع عنوانه الشبكي أو غير ذلك من المعلومات عنه، ويطلق على هذه المواقع مساعدات التخفي Anonymizers .

---

(١) ***McClure et al., ٢٠٠١*** **op.cit.**

(٢) ***Schwartau, Winn (٢٠٠٠).*** **Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption**. Broadway, New York: Thunders Mouth Press.

كما يمكن أن يتم استعمال خدمات الإنترنت المختلفة من خلال بعض أنواع الخادم الوكيل الواقعه خارج نطاق الشبكة الوطنية والتي لا تكشف العنوان الشبكي للمستخدم عند طرف الاتصال الآخر وإنما تظهر العنوان الشبكي الخاص بالخادم نفسه(١).

رابع عشر: إخفاء وتمويه الرسائل : Steganography

يقوم هذا الأسلوب على إخفاء رسالة ما بشكل كامل بحيث يحجب وجودها تماما، ويتم ذلك في الرسائل ذات الطابع الرقمي بواسطة دمج الرسالة مع ملف آخر مختلف تمامًا وقد يكون هذا الملف عبارة عن مستند أو صورة أو تسجيل صوتي أو لقطة فيديو، من خلال استبدال أجزاء صغيره من البيانات المكونه للملف المستخدم للإخفاء وإحلال البيانات الخاصة بالرسالة محلها، بحيث يبقى محتوى الملف الأصلي كما هو ولا يتغير حجمه نهائيًا، كما أنه لا يطرأ أي تأثير على جودة الصورة أو الصوت بالنسبة للعين البشرية.

ويوجد الكثير من البرامج التي تجعل تنفيذ هذا الأسلوب غاية في السهولة حتى بالنسبة لأقل المستخدمين خبرة ومن أشهرها، Hide and Seek و Steganos و StegoDos ، وتعمل في بيئة النوافذ، أما بيئة يونيكس فهناك برنامجSFS . ويستخدم هذا الأسلوب لإخفاء الكثير من المعلومات ذات الصلة بجرائم عده .مثل ذلك الشخص الذي اعتاد على إخفاء أرقام البطاقات الائتمانية المسروقة في صور أزرار التنقل الموجودة على موقعه في الإنترنت . كما يعتقد مكتب التحقيقات الفيدرالية الأمريكي أن تنظيم القاعدة يستخدم هذا الأسلوب بالتزامن مع أسلوب التشفير لتمرير المعلومات بين أعضائه على مواقع الإنترنت والمنتديات وداخل غرف الدردشة (٢).

خامس عشر: إغراق الذاكرة المؤقتة: Buffer Overflows

يعتمد هذا الأسلوب على استغلال طبيعة تعامل البرمجيات مع ذاكرة الحاسوب، بحيث يتم استغلال المخازن المؤقتة التي يستخدمها المبرمج في ذاكرة الحاسوب لتمكين برنامجه من تخزين متغيرات ذات أطوال محدده يحتاجها البرنامج أثناء عمله، حيث يقوم الهكر بتزويد البرنامج ببيانات تفوق في طولها الحد الأقصى الذي يمكن أن يستوعبه المخزن، مما يؤدي إلى ارتباك أداء البرنامج بطريقة تجعل من الممكن تنفيذ الشفرة الزائدة عن حجم المخزن داخل الحاسوب الضحية دون رغبة صاحبه، وهذه الشفرة غالبًا ما تكون لتسهيل عملية اختراق هذا الحاسوب من قبل الهكر، ويتطلب استخدام هذا الأسلوب أن يكون الهكر ملمًا بشكل جيد بلغتي البرمجة، لغة التجميع) لغة الآلة (ولغة سي++، بالإضافة إلى المعرفة الجيدة بنظام التشغيل الذي يعمل على الحاسوب المراد اختراقه (٣).

Jamsa, Kris (٢٠٠٢). **Hacker Proof: The Ultimate Guide to Network**

(٣)

Security. Albany, New York: Delmar Learning.

Vacca, John (٢٠٠٢). **Computer Forensics: Computer Crime** .

(١)

Scene Investigation

Chuvakin, A. & Peikari, C. (٢٠٠٤). Security Warrior. Sebastopol, California

(٢)

الفصل الثاني
مكافحة الجرائم الإلكترونية

تمهيد وتقسيم:

انتهينا فيما سبق إلى أن الجرائم الإلكترونية جرائم عالمية وعابرة للحدود ولذلك من المهم لمواجهة هذه الجرائم ومكافحتها وجود التعاون الدولي لتطوير أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية ، لاسيما وأن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية .

وفي واقع الأمر فقد لاقت الجرائم الإلكترونية اهتماما عالميا فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (١٩٩٣م) الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنولوجيا المعلومات وتوصل إلى توصيات أحاطت بجوانب مشكلة جرائم الحاسب الآلي إلا أنها لم تتعرض لجزئية هامة وهي التعاون الدولي الذي يعتبر ركيزة أساسية عند التعامل مع هذه النوعية من الجرائم .

وهذا المؤتمر يعتبر تحضيرا للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام (١٩٩٤م) والذي وضع توصيات حول جرائم الحاسب الآلي والانترنت والتحقيق فيها ومراقبتها وضبطها وركز على ضرورة إدخال بعض التعديلات في القوانين الجنائية لتواكب مستجدات هذه الجريمة وإفرازاتها .

وكذلك اتفاقية الإجرام السيبيري (الإجرام عبر الانترنت) (٢٠٠١م) والتي صدرت عن المجلس الأوربي، ووُقِّعَت في العاصمة المجرية بودابست في ٢٣ نوفمبر (٢٠٠١م)، وقعت عليها ٣٠ دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في ٢٢ سبتمبر (٢٠٠٦)م، ودخلت حيز النفاذ في الأول من يناير (٢٠٠٧م). واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال (١). وسوف أتناول هذا المبحث من خلال ثلاثة مطالب كالتالي:

المبحث الأول: مكافحة الجرائم الإلكترونية في التشريعات الدولية

المبحث الثاني: مكافحة الجرائم الإلكترونية في التشريع الجنائي المصري

المبحث الثالث: مكافحة الجرائم الإلكترونية في التشريع الجزائي السعودي

O'Reilly & Associates.

(١) د/ عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الآلي، طبعة أولى الرياض ١٤١٤هـ ص ١٠٨، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص ٤، محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي، مرجع سابق، ص٤١.

المبحث الأول
مكافحة الجرائم الإلكترونية في التشريعات الدولية

تزايدت خطط مكافحة الجرائم الإلكترونية ،وانصبَّت الجهود على دراستها المتعمِّقة،وخلق اليات قانونيّة للحماية من أخطارها، ومواجهتها من خلال حماية استخدام الكمبيوتر، أو ما يُعرَف أحيانًا بجرائم الكمبيوتر ذات المحتوى الاقتصادي. وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية). وحماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية).

وإدراكًا لقصور القوانين الجنائيّة بما تتضمّنه من نصوص التجريم التقليديّة عن أن تحيط بالجرائم الإلكترونية ، كان لا بد للعديد من الدول من وضع قوانين وتشريعات خاصّة، أو العمل على تعديل قوانينها الداخلية من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.

وسوف أتناول مكافحة الجريمة الإلكترونية في التشريعات الغربية والعربية في المطلبين التاليين:

المطلب الأول
مكافحة الجرائم الإلكترونية في التشريعات الغربية

اهتمت التشريعات الغربية بظاهرة الجرائم الإلكترونية، وكيفية مكافحتها ، وتعد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها(١).

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (١٩٧٦م – ١٩٨٥م)، وفي عام (١٩٨٥م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية أو الإلكترونية، وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (١٩٨٦م) صدر قانونا تشريعاً يحمل الرقم (١٢١٣) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم الإلكترونية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام (٢٠٠٠م) خمسة جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع جرائم الحاسب الآلي والانترنت.

---

(١) دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص ٤.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى (١).

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (١٩٨٥م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (Competition Act The) مثلا الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها

وفي عام (١٩٨٥م) سنّت الدنمرك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها (٢).

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (١٩٨٨م) القانون رقم (١٩-٨٨) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (١٩٩٤م) تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم الإلكترونية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال (٣).

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته،كما أقرت عام (١٩٩١م) شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل .

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما

---

(١) د/ عبد الرحمن الشنيفي ، أمن المعلومات، مرجع سابق ص١٠٩.
(٢) محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي، مرجع سابق، ص٤١.
(٣) د/ احمد حسام طه تمام الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص٩١،٩٢.

كان ذلك إلى إدانته أو إدانة احد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى ابعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم (١).

المطلب الثاني

مكافحة الجرائم الإلكترونية في التشريعات العربية

لم تتطرق معظم البلاد العربية إلى وضع تشريعات خاصة بالجريمة الإلكترونية إلا منذ زمن يسير ، اكتفاء بالتشريعات التقليدية لمكافحة هذه الجرائم ؛ ولعل السبب في ذلك يعود إلى أن ثورة الحاسب الآلي إن جاز لنا هذا الوصف في البلدان العربية لم تتعد العقد الواحد أو تزيد قليلاً ، ذلك أن الاعتماد على تطبيقات الحاسب الآلي في البلدان العربية قد بدأ منذ نهاية العقد الأخير من القرن الماضي ، وبدأ معه وتيرة الحركة التشريعية لضبط المعاملات الالكترونية ومواجهة الجرائم الإلكترونية.

وبعد أن تم استعراض موقف التشريعات الغربية لمواجهة أو التصدي لهذه الظاهرة الإجرامية الخطيرة المتمثلة بالجرائم الإلكترونية بات واضحاً لنا مدى قصور التشريعات الجزائية في بعض البلدان العربية التي تتصدي لهذا النمط من الجرائم ، الأمر الذي يستدعي أن يسارع المشرع في هذه البلاد لسن تشريعات جديدة أو تعديل التشريعات القائمة حتى تلائم في تطبيقها ثورة الاتصالات المعلوماتية التي تحياها البشرية بالشكل الذي يجعلها كفيلة بحماية النظام ألمعلوماتي ومكافحة الإجرام الناشئ عن استخدامه أو الواقع عليه. (٢)

ومن التشريعات العربية التي تناولت الجرائم الإلكترونية ما يلي(٣):

١- قانون التجارة والمبادلات الالكترونية التونسي:

ففي تونس صدر عام ٢٠٠٠ قانون التجارة والمبادلات الالكترونية وقد عاج فيه المشرع التونسي أحكام العقد والمعاملات الالكترونية كما عالج الجرائم التي تقع على هذه التجارة والمعاملات الالكترونية.

٢- قانون مكافحة الجرائم الإلكترونية (مواده مستحدثة ضمن أحكام قانون الجزاء العماني)، بسلطنة عُمَان (٢٠٠١م):

أصدرت سلطنة عمان جملة من التشريعات لمكافحة الجريمة الإلكترونية تحت مسمى: قانون سلطنة عمان لمكافحة جرائم الحاسب الآلي ، فقد صدر المرسوم السلطاني رقم (٧٢) لسنة (٢٠٠١ م) بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي(الكمبيوتر)، وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني تحت عنوان(جرائم الحاسب الآلي). وكذلك أضيفت مواد إلى قانون الاتصالات العماني تحرم تبادل رسائل تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة

---

(١) محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي، مرجع سابق، ص٤١.

(٢) عادل يوسف عبد النبي، الجريمة المعلوماتية ، مرجع سابق، ص ١٢٦، ١٢٧.

(٣) د/عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت ، مرجع سابق ص ٨، ٩، د/ محمود عبابنة ، جرائم الحاسوب وأبعادها الدولية ، مرجع سابق، ص١٢٧، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص ٤.

أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد ، وأسست السلطنة قانوناً ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة.

٣- المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي:
أدخل المشرِّع المغربي الفصول التي تعاقب على الأفعال التي تشكل جرائم عنوان (المس بنظام المعالجة الآلية للمعطيات) وذلك بموجب القانون رقم ٠٣-٠٧ الصادر بتاريخ ١٦ رمضان ١٤٢٤ الموافق ١١ نوفمبر ٢٠٠٣.
القانون العربي النموذجي أو الاسترشادي:
صدر القانون العربي النموذجي أو الاسترشادي في شان مكافحة جرائم الكمبيوتر و الانترنت – كثمرة عمل مشترك -بين مجلس وزراء الداخلية العرب و مجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد اجتماعها في ٢٢/٥/ ٢٠٠٣م.
وقد وضع هذا القانون الاسترشادي القواعد الأساسية التي يتعين على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجرائم حيث صدر هذا القانون مشيرا للجرائم التي تقع عن طريق الكمبيوتر و الانترنت بصفة عامة محددا عقوباتها لكنه أحال إلى التشريع الوطني فيما يتعلق باركان هذه الجرائم و العقوبات الخاصة التي تطبق عليها.
وبعد إقرار هذا المشروع فليس هناك عذر لأي مشرع عربي في أن يتقاعس عن المبادرة بإصدار التشريع الوطني اللازم لمواجهة جرائم الكمبيوتر و الانترنت و التي تجد تطبيقاتها على مستوى العالم و في أي دولة من الدول أيا كان نصيبها من استعمال الحاسب الآلي و شبكاته و شبكة الانترنت و أيا كانت درجة التقدم لديها.
٥- قانون مكافحة الجرائم الإلكترونية الإماراتي (٢٠٠٦م):
تعتبر دولة الإمارات العربية أول دولة عربية تسن قانونًا مستقلًا لمكافحة الجرائم الإلكترونية رقم ٢ لسنة(٢٠٠٦م).
وفي دولة الإمارات العربية المتحدة صدر عام ٢٠٠٢ قانون حقوق المؤلف وأصحاب الحقوق المجاورة. وفي إمارة دبي صدر قانون التجارة الالكترونية رقم (٢) لسنة ٢٠٠٢ وهو قانون يضبط المعاملات الالكترونية والتوقيع الالكتروني والحماية القانونية المقررة لها في نطاق إمارة دبي .
٦- القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة (٢٠٠٨م):
اعتمده مجلس وزراء العدل العرب بقرار رقم (٧٧١/د٢٤ – ٢٠٠٨/١١/٢٧).
وبالنسبة لمصر والمملكة العربية السعودية فسوف أتناول مكافحة الجرائم الإلكترونية في كل منهما فيما يلي:

□

المبحث الثاني
مكافحة الجرائم الإلكترونية في التشريع الجنائي المصري

حرص المشرع المصري على مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العصر(١)؛ فأصدر قانون خاص للاتصالات(٢) (رقم١٠ /٢٠٠٣م) لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكتروني (رقم ٢٠٠٤/١٥م) لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"، فضلاً عن أنّ هناك جهودًا تبذل لإصدار قانون خاص بالمعاملات الإلكترونية لسلامة وتأمين المعاملات المختلفة من كافة جوانبها القانونية والجنائية، وهناك دراسات جادة لإعداد مشروع قانون لمكافحة الجريمة الإلكترونية.

وفيما عدا القوانين المذكورة، فإنه تطبق قواعد القانون الجنائي التقليدي على الجرائم الإلكترونية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة الإلكترونية، ومن ذلك مثلا اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم الإلكترونية، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية (٣).

وعلى ذلك فهناك فراغ تشريعي في هذا المجال خاصة في قضايا النشر الالكتروني وقوانين جرائم الانترنت الخاصة باقتحام النظم وغيرها ، ويخلو التشريع المصري من أية عقوبات خاصة بجرائم الانترنت ، وما يطبق حاليا علي جرائم الانترنت هو قانون تعامل مع سرقة المعلومات مثل أي سرقة ويعاقب مرتكبها بالحبس مدة لا تقل عن ٢٤ ساعة ولا تزيد علي ثلاث سنوات.. وإذا كانت نصب يعاقب بعقوبة النصب المدرجة في قانون العقوبات..

وإذا كانت سب وقذف تكون جنحه وإذا كانت تركيب صور فاضحة كما يحدث البعض توجه لمرتكبي تهم خدش الحياء وهتك العرض والتحريض علي الفسق.. أما إطلاق الشائعات والسطو علي أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إليه تهم تكدير

---

(١) دخلت خدمة الانترنت مصر عام ١٩٩٣ علي يد مركز المعلومات ودعم اتخاذ القرار بالتعاون مع شبكة الجامعات المصرية ومع بداية عام ١٩٩٧ بدأ المركز في خصخصة خدمات الانترنت في مصر وكانت البداية من خلال ١٦ شركة زادت إلى ٦٨ شركة في عام ٢٠٠٠ وانتهت إلى ٢١١ شركة هي إجمالي الشركات التي تقدم خدماتها في مجال الانترنت داخل مصر. وكان عدد مستخدمي الانترنت في مصر في العام الأول لاستخدامه لم يتجاوز ٧٥ ألف شخص ولكنه بعد تطبيق حملة حاسب لكل بيت وانخفاض أسعار خدمات الانترنت السريع وصل عدد مستخدمي الانترنت حاليا إلى خمسة ملايين و٣٠٠ ألف مستخدم يحصلون علي خدماتهم من خلال ٢١١ شركة تعمل في هذا المجال داخل حدود مصر. د/ عادل عمر "جرائم الانترنت في مصر" على موقع: http://www.adelamer.com

(٢) وعُرِّفت الاتصالات فى هذا القانون فى (م١/ف٣) بأنها: (أية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أياً كانت طبيعتها، وسواء كان الاتصال سلكياً أو لاسلكيًا).

(٣) محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي، مرجع سابق، ص٤٣.

الأمن العام وتهديد الاقتصاد القومي والإضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها إلى محاكم الجنايات مباشرة (١).

وعن الآلية التي يتم بها مواجهة الجرائم الإلكترونية في مصر:

يقول حبيب العدلي وزير الداخلية الأسبق في كلمته التي ألقاها نيابة عنه اللواء مصطفي راضى مساعد أول وزير الداخلية في مؤتمر الجرائم المستحدثة تحدٍ جديد أمام الأجهزة الأمنية (٢): " أننا نحتاج إلى تشريعات تواكب عملية التطور والحداثة في الجرائم في العقدين الأخيرين.

وأضاف أنه في مصر تمثلت المحاور الرئيسية للسياسة الأمنية المصرية في مواجهة الجرائم الإلكترونية، في مواكبة التقدم التقني والتكنولوجي، وتطوير قدرات العنصر البشرى ببناء أنظمة وصياغة تطبيقات في مجال تفعيل تكنولوجيا المعلومات لخدمة العمل الأمني، نحن بذلك أمام الانتقال من نمط أنظمة وتطبيقات ضيقة، يغلب عليها الطابع الإداري إلى الأنظمة العلمية المستحدثة والتطبيقات الأمنية التي تدخل في صلب المهام الأمنية بقطاعاتها وتخصصاتها المتعددة.. وفق الأولويات التي تستهدف تحقيق المبادأة والفاعلية الأمنية في مواجهة الجرائم المستحدثة وعبر الوطنية، وفي مجال حماية حقوق الملكية الفكرية، وواكبت وزارة الداخلية منذ سنوات المستجدات بالتصدي لأنماط التعدي على حقوق المفكرين والمبدعين، فكانت مصر من أوائل الدول التي أنشأت جهازا شرطيا. متخصصا لمكافحة جرائم المصنفات الفنية في عام ١٩٨١ وعقب انضمام مصر لمنظمة التجارة العالمية «الجات»، أنشأت إدارة رئيسية لمكافحة جرائم المصنفات تم تطوير البناء التنظيمي للإدارة الفنية والمطبوعات، لتصبح في عام ٢٠٠٥ إدارة عامة لمواكبة المستجدات والالتزامات الدولية، ويكون الهدف الرئيسي لها هو حماية حقوق الملكية الفكرية.. بالتنسيق مع الجهات الأخرى المعنية كما أنه في عام ٢٠٠٢م تم إنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق للأخذ بزمام المبادرة لمواجهة تلك الجرائم..وأسهمت جهودها على سبيل المثال بالتكامل مع قطاعات الوزارة المختلفة في ضبط أكثر من شبكة في مجال جرائم بطاقات الائتمان امتداداً لتشكيلات إجرامية بالخارج.الجرائم المستحدثة

واختتم المؤتمر أعماله بالتوصل إلى مجموعة من التوصيات تهدف إلى تنمية الوعي بالجرائم المستحدثة وأساليب مواجهتها، أهمها الاستمرار في الجهود التي تهدف إلى نشر الوعي بكيفية التعامل مع شبكة الإنترنت، والعمل على وضع قواعد سلوكية وإرشادية للمستخدمين لشبكة الإنترنت للالتزام بأخلاقيات الشبكة.

---

(١) د/ عادل عمر ، جرائم الانترنت في مصر، على موقع:
http://www.adelamer.com

(٢) منشور على موقع :
http://www.masress.com
، وكذلك في مجلة أكتوبر يوم ٠٢ – ٠١ – ٢٠١١ ونفس المعنى في ندوة " المواجهة الأمنية للجريمة المعلوماتية" بتاريخ ٢٠١١/٤/٧م على موقع:
http://www.alfanonline.com

وإيجاد أساليب تكنولوجية متطورة لزيادة لحماية من المخاطر التي تصاحب استخدام التكنولوجيا المصرفية عبر الإنترنت. وتوثيق التعاون الدولي والإقليمي بين الهيئات والمؤسسات المختلفة لنشر الوعي لدى مسئولي ومستخدمي المعلومات وتعريفهم بالأخطار والتهديدات التي يمكن أن تتعرض لها تلك النظم وكيفية حمايتها، مع ضرورة العمل على إيجاد إجماع عالمي حول نوعية السلوك الذي يشكل ، بالإضافة إلى تعزيز التعاون الإقليمي لتوحيد مفاهيم الجرائم الإلكترونية وكيفية مواجهتها بصفة عامة، وفي القطاع المصرفي بصفة خاصة، على غرار مشروع الاتفاقية الأوروبية لمواجهة جرائم الحاسب الآلي، وقيام هيئة تنمية صناعة تكنولوجيا المعلومات بالتوعية المستمرة بشأن التجارة الإلكترونية والتوقيع الإلكتروني.

وذلك من خلال وسائل الإعلام المختلفة، وضرورة العمل على تحسين أمن الشبكة مع الأخذ في الاعتبار حماية الخصوصية واحترام حقوق الإنسان والحريات الأساسية، طبقاً للمواثيق الدولية ومقاصد الأمم المتحدة وأوصى المؤتمر المؤسسات التعليمية والمراكز البحثية بضرورة نشرة التوعية في قطاعات التعليم بمراحلها المختلفة بمساوئ وأضرار الجرائم الإلكترونية وذلك من خلال إضافة تدريس الجرائم الناشئة عن استخدام الحاسب الآلي والإنترنت ضمن المناهج الدراسية الخاصة بالحاسب الآلي في المدارس والجامعات، وحث الجامعات والمراكز البحثية لدراسة الجرائم الإلكترونية، والجرائم عبر الإنترنت، ومحاولة إنشاء دراسة متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.

وعقد الندوات والمؤتمرات لتبادل الخبرات وإبرام اتفاقيات تعاون مشترك في مجال مكافحة هذه الجرائم وتسليم المجرمين، وإجراء دراسات متخصصة حول الآثار الاجتماعية والاقتصادية للجرائم المعلوماتية أو الإلكترونية في المجتمع المصري، وتغيير المناهج الدراسية في كلية الحقوق بما يتلاءم مع تطور الجرائم وأساليب مواجهتها.

كما أوصى المؤسسات القانونية والتشريعية بسرعة إدخال التعديلات التشريعية اللازمة لتتلاءم مع الجرائم المستحدثة وتساعد في تقديم مرتكبيها إلى العدالة. والتوصية بإنشاء إدارات متخصصة لمتابعة ودراسة الظواهر السلبية التي تثبت على الشبكة العالمية للمعلومات ووضع التصورات المستقبلية لها ومدى إمكانية تأثيرها على مستخدمي الشبكة، ومقترحات معالجتها ومواجهتها.

وطالب المؤتمر وسائل الإعلامي بضرورة العمل على نشر الوعي إعلامياً لخلق رأي عام ضد الجرائم الإلكترونية، ولتعريف مستخدمي الشبكة بمخاطر التعامل مع المواقع المشبوهة، وخاصة الشباب، وتشجيع الضحايا في جرائم الحاسب الآلي والإنترنت على الإبلاغ عن هذا الجرائم.والتوعية بخطورة الظواهر السلبية الحديثة على شبكة الإنترنت ومنها تنامي ظاهرة المخدرات الرقمية.

وضرورة مراقبة الأسرة للأطفال والشباب مستخدمي شبكة الإنترنت، وتوعيتهم بصفة مستمرة من مخاطر الدخول إلى المواقع المشبوهة الإباحية في حين أكد على المجتمع المدني وأهمية قيامه بتوعية الشباب من الوقوع في الممارسات والسلوكيات الخاطئة عبر شبكة الإنترنت، وكيفية الاستفادة من الجوانب الإيجابية لاستخدام وسائل التقنية الحديثة.

وفي "ندوة" عن الإرهاب الإلكتروني، ومخاطر جرائم الإنترنت على استقرار النظام الدولي، تحت عنوان "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المُواجهة" (١). والتي اهتمت بمُناقشة ظهور العديد من الجرائم الإلكترونية التي يأتي في مُقدمتها ما يُعرف بـ "الإرهاب الإلكتروني "CyberTerrorism" والذي يُمثل تهديداً على الأمن القومي للدول، حيثُ أصبحت البنية التحتية لأغلب المُجتمعات الحديثة تُدار عن طريق أجهزة الحاسب الآلي والإنترنت، مما يُعرضها لهجمات مُتعددة من"الهاكرز" و"المُخترقين" بشكل عام. تلك الهجمات التي تستطيع أن تتسبب في خسائر مادية ومعنوية هائلة، حيث يُمكنها إغلاق الاتصالات الدولية، وإعاقة حركة الملاحة الجوية أو البحرية، وإلحاق الضرر بخدمات عامة مثل شبكات الكهرباء والمياه، وأيضاً بالنظام المالي للدول من خلال الإضرار بالبنوك والمؤسسات المصرفية.

يقول اللواء محمود الرشيدي، مُدير إدارة التوثيق والمعلومات بوزارة الداخلية سابقاً، :" إن جهود جمهورية مصر في مجال مكافحة الإرهاب التكنولوجي، والتي تمثل أهمها في : تفعيل التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المُجرمين، أيضاً إصدار عدد من القوانين التشريعية الجديدة لتجريم أي استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، مثل (قانون التوقيع الإلكتروني رقم ٢٠٠٤/١٥، وقانون تنظيم الاتصالات رقم ٢٠٠٣/١٠، وقانون حماية حقوق الملكية الفكرية رقم ٢٠٠٢/٨٢). بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادُل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المُستمر من خلال عناصرهِ الإجرامية المُحترفة والمُنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية. هذا إلى جانب إنشاء إدارة مُتخصصة بوزارة الداخلية عام ٢٠٠٢ ، وهى إدارة مكافحة جرائم الحاسبات وشبكات المعلومات لرصد وتتبُع كافة أنواع الاستخدام غير الأمن وغير المشروع لشبكة الإنترنت، وضبط مُرتكبيها، والعمل على نشر الوعي المعلوماتي بين أفراد المُجتمع بخطورة تلك النوعية من الجرائم على المُجتمع المصري وأنشطته المُختلفة . وأخيراً، أشار الرشيدي إلى مُبادرة وزارة الاتصالات وتكنولوجيا المعلومات عام ٢٠٠٨ بإنشاء أول جهاز فني مُتخصص في حماية وتأمين البلاد من أي هجمات إلكترونية مُحتلة عبر شبكة الإنترنت"

وعن كيفية التصدي لجرائم الهاكرز والمخترقين: يقول: د.مصطفي جاد، وكيل كلية حاسبات ومعلومات جامعة عين شمس، مؤكداً ضرورة بعض أساليب الحماية، التي لخصها في أهمية تشفير البيانات، وإخفاء البيانات، والاهتمام ببروتوكولات الحماية، وجُدر الحماية، ونُظم منع المتطفلين. أما عن أهداف وطُرق الحماية، فقد ذكرها جاد في بعض النقاط التي تتمثل في الوثوقية: أي الاحتفاظ بسرية المعلومات عن الجميع باستثناء الذين

(١) نظمها المركز الدولي للدراسات المُستقبلية والإستراتيجية في ١١ أبريل ٢٠١٢ منشورة على موقع : http://www.siyassa.org.

لديهم صلاحية للاطلاع عليها، وتكامُل البيانات: بمعنى التأكُد من أن المعلومات لم تتغير من قبل أشخاص غير مخولين، والتحقُق من الشخصية، حيثُ يجب التأكُد من هوية الأطراف المعنية بعملية تبادُل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنُب أي شكل من أشكال الخداع (مثل عمليات التزوير، وانتحال الشخصيات)، أيضاً عدم الإنكار: بمعنى منع أي شخص من أن يُنكر أي تعهُد أو عمل سابق تم إجراؤه .

وبالنسبة للموقف القانون من مرتكبي الجرائم الإلكترونية: يقول : د.جميل عبد الباقي، عميد كلية حقوق عين شمس، الذي أكد ضرورة تخصيص دوائر قضائية مُعينة للنظر في الجريمة الإلكترونية، والاستفادة مما انتهى اليه الاتحاد الأوروبي والدول الأخرى في مجال التشريعات الجنائية. كما أكد أهمية تعاون وتوافُق دولي على قانون مُوحد خاص بعقوبات الجرائم الإلكترونية. في حين تحدث د.نشأت الهلالي، مُساعد أول وزير الداخلية الأسبق، ورئيس أكاديمية الشرطة سابقاً، عن أسباب اللجوء للإرهاب الإلكتروني، والتي لخصها في: ضعف بنية الشبكات المعلوماتية، وقابليتها للاختراق، وغياب الحدود الجغرافية، وتدني مُستوى المُخاطرة، وسهولة الاستخدام، وقلة التكلفة، وأخيراً صعوبة اكتشاف وإثبات الجريمة في هذا النوع من الإرهاب. كما أكد الهلالي أهمية حقوق الإنسان الرقمية، وأهمية وجود مُنظمة دولية تعمل على ذلك. وأشار الكاتب والباحث أ.سمير العركي إلى ضرورة تبني الأزهر ودار الإفتاء كُل الجهود التي تهدف إلى التوعية في مُواجهة دعاوى الجماعات المُتطرفة عبر الإنترنت.

وأخيراً، خلصت الندوة إلى بعض التوصيات، من أهمِها ضرورةُ وضع مفهومٍ دولي مُوحَّد للإرهاب بصفةٍ عامة، والإرهابِ الإلكتروني بصفةٍ خاصة، وضرورةُ تأكيد أهمية دور وسائل الإعلام في بلورة استراتيجيات للتصدي لمزاعم الإرهابيين، وأهمية أنْ تعملَ الدولُ على ضرورة توحيد جهودها نحو وضع تشريعات داخلية صارمة لِمُكَافحة الجرائم التي تتعلّق بالإرهاب الإلكتروني، وتعزيز إجراءات الأمن والحراسة بأنواعها (بشرية، تكنولوجية) على مراكز ونُظم المعلومات التكنولوجية، وفق أحدث تكنولوجيا مُتقدمة في مجالات التأمين والتشفير بأنواعِها المُختلفة، ودراسة إمكانية إنشاء غرفة إدارة للأزمات التكنولوجية، يُشارك فيها أخصائيون وخُبراء من مُختلفِ التخصُصات التكنولوجية والأمنية لإعداد ووضع سيناريوهات وأد ومُواجهة أي هجمات إلكترونية مُحتملة تتعرض لها البلاد، والتصدي لمُحاولات تغيير أنماط التفكير الخاصة بالمُجتمعات العربية، والتي تتقبل المعلومة دون نقد أو مُراجعة، وعدم العمل في جُزر مُنعزلة، بمعنى أهمية الاتحاد والتوافُق والتنسيق بين جميع الأطراف.

المبحث الثالث
مكافحة الجرائم الإلكترونية في التشريع الجزائي السعودي

اهتمت المملكة العربية السعودية بمكافحة الجرائم الإلكترونية ، وسارعت بإصدار قانون جديد لمكافحة جرائم المعلوماتية، التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الانترنت وإنشاء مواقع الإنترنت الإرهابية، بالإضافة لحماية التعاملات الإلكترونية التي أصبحت ضرورة من ضرورات التطور التقني في العصر الحديث بسبب تطور تقنيات الاتصالاتِ.

وإدراكا لأهمية تنظيم التعاملات الإلكترونية، وافق مجلس الوزراء في المملكة في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م على نظامي مكافحة جرائم المعلوماتية والتعاملات الالكترونية، وكان ذلك للحد من وقوع الجرائم الإلكترونية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات.

والمصلحة التي يحميها القانون بهذه الصور الجديدة من الجرائم هي بلا شك المصلحة العامة التي تقتضي تأمين استخدام أجهزة الكمبيوتر وشبكة المعلومات الدولية (الانترنت) من عبث العابثين الذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف، وجرائم غسيل الأموال(١).

وتتضح أهداف نظام مكافحة جرائم المعلومات في المملكة من نص المادة الثانية منه حيث جاء فيها: "يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الالكترونية، وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:

١- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الالكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات الكترونية يعول عليها.

٢- إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الالكترونية وسلامتها.

٣- تيسير استخدام التعاملات والتوقيعات الالكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم والدفع المالى الالكتروني.

٤- إزالة العوائق أمام استخدام التعاملات والتوقيعات الالكترونية.

٥- منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الالكترونية".

وقد بدأت المملكة بالعمل في هذا الاتجاه قبل صدور النظام السابق حيث أوكلت المهمة مبدئيا إلى مدينة الملك عبد العزيز للعلوم والتقنية لتقديم هذه الخدمة عبر مزودي خدمة تجاريين، كما شكلت لجنة أمنية دائمة برئاسة وزارة الداخلية وعضوية ممثلين من

---

(١) د/ شيماء عبدالغني محمد عطاالله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م بحث منشور على موقع:
http://www.f-law.net

القطاعات الأمنية والدينية والاجتماعية والاقتصادية المختصة للإشراف على أمن خدمة الإنترنت في المملكة وتشمل مهمتها تحديد المواقع غير المرغوبة والتي تتنافي مع الدين الحنيف والأنظمة الوطنية ومتابعة كل ما يستجد منها لحجبها خاصة تلك المواقع الإباحية أو الفكرية أو الأمنية (١).

وفي تقرير صحفي(٢). كشفت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الإنترنت المشرفة على عمل مقدمي خدمة الإنترنت في المملكة عن إجراءات فنية تهدف إلى محاصرة أعمال المخربين أو المتسللين ومنعهم ومخالفتهم. وأوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الإنترنت في المملكة بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين وإساءة استخدام البريد الإلكتروني وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الإنترنت في المملكة ومن بين هذه الإجراءات ما يلي:

١. منع انتحال أرقام الإنترنت أو ما يعرف بـ (Ip-spoofing) والتي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة.

٢. منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـ (E-Mail Spamming) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا باسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.

٣. الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (٦) أشهر.

٤. الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسي ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

٥. تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.

٦. ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

ونقلت وكالة الأنباء الكويتية عن مصدر مسئول بوزارة الداخلية السعودية قوله أن نظام مكافحة جرائم المعلوماتية. يشمل ١٦ مادة تتضمن عقوبات صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و١٠ سنوات سجنا وغرامات مالية تصل إلى خمسة ملايين ريال سعودي، مضيفاً أن النظام تضمن تعريفات المصطلحات والمسميات الواردة في النظام مثل "الشخص" و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات والجريمة المعلوماتية أو الإلكترونية إلى جانب أهداف النظام بالحد من هذه الجرائم والعقوبات المقررة لكل منها. وحددت مواد النظام الأخرى الجرائم الإلكترونية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم الإلكترونية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام " في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ويهدف النظام الجديد إلى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات

---

(١) محمد عبد الله المنشاوي ، جرائم الانترنت في المجتمع السعودي، مرجع سابق، ص٤٦.

(٢) نشر في موقع صحيفة الجزيرة بتاريخ ١٤٢١/٢/٢هـ .

الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني(١).
وعلى مستوى مكافحة الجرائم من الناحية الشرطية تم إنشاء إدارة خاصة – كما في فرنسا وكندا– من رجال المباحث الجنائية تتخصص في جرائم الكمبيوتر وكذلك أجهزة مركزية للمتابعة (٢).

الخاتمة

في ختام هذا البحث أشكر الله سبحانه وتعالى جزيل الشكر وخالصه على أن وفقني ويسر لي أداء هذا البحث.

ولقد تناولت في هذا البحث دراسة الموضوعات المتعلقة بالجرائم الإلكترونية، وذلك في التشريع الجنائي المصري والسعودي .

ولقد تبين لي من خلال هذه الدراسة النتائج والتوصيات التالية:

أولاً: نتائج البحث:

إن الجرائم الإلكترونية لها طبيعة خاصة؛ وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

أنها جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، توجه للنيل من الحق في المعلومات ، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت .

أنها كما تطال الحق في المعلومات ، تمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري..

أن التعريف الراجح في نظري لهذه الجريمة هو أنها :"سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية محله معطيات الكمبيوتر"

أنها جرائم بالغة الخطورة ولها أضرار بالغة ، كما أنها عابرة للحدود، وهي بذلك تشترك مع بعض الجرائم الأخرى كالإرهاب، والاتجار بالمخدرات، وغسيل الأموال؛ فقد قدر الخبراء في أحد المؤتمرات أن حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول

---

(١) السعودية الأولى عربياً في اصدار قانون ضد جرائم الانترنت ، مقال منشورعلى موقع: http://www.traidnt.net .

(٢) د/ شيماء عبدا لغني محمد عطا الله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م بحث منشور على موقع:
http://www.f-law.net

مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا.

تزايدت خطط مكافحة الجرائم الإلكترونية، وانصبَّت الجهود على دراستها المتعمِّقة،وخلق آليات قانونيّة للحماية من أخطارها، ومواجهتها، وتعد السويد أول دولة غربية تسن تشريعات خاصة بمكافحة جرائم الحاسب الآلي والانترنت، وتعد تونس من أول البلاد العربية التي سنت قانون التجارة والمبادلات الالكترونية عام ٢٠٠٠ م عالج فيه المشرع التونسي أحكام العقد والمعاملات الالكترونية كما عالج الجرائم التي تقع على هذه التجارة والمعاملات الالكترونية.

أن هناك قصور تشريعي في بعض البلدان العربية التي تتصدي لهذا النمط من الجرائم ، الأمر الذي يستدعي أن يسارع المشرع في هذه البلاد لسن تشريعات جديدة أو تعديل التشريعات القائمة حتى تلائم في تطبيقها ثورة الاتصالات المعلوماتية التي تحياها البشرية بالشكل الذي يجعلها كفيلة بحماية النظام ألمعلوماتي ومكافحة الإجرام الناشئ عن استخدامه أو الواقع عليه، وتعد تونس من أول البلاد العربية التي سنت قانون التجارة والمبادلات الالكترونية عام ٢٠٠٠ م عالج فيه المشرع التونسي أحكام العقد والمعاملات الالكترونية كما عالج الجرائم التي تقع على هذه التجارة والمعاملات الالكترونية.

أنه في سبيل مكافحة الجريمة الإلكترونية أصدر المشرع المصري قانون خاص للاتصالات (رقم١٠ /٢٠٠٣م) لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكتروني (رقم ٢٠٠٤/١٥م) لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"، فضلاً عن أنّ هناك جهودًا تبذل لإصدار قانون خاص بالمعاملات الإلكترونية لسلامة وتأمين المعاملات المختلفة من كافة جوانبها القانونية والجنائية، وهناك دراسات جادة لإعداد مشروع قانون لمكافحة الجريمة الإلكترونية.

اهتمت المملكة العربية السعودية بتنظيم التعاملات الإلكترونية ومكافحة الجرائم الإلكترونية ، وسارعت بإصدار نظامي مكافحة جرائم المعلوماتية والتعاملات الالكترونية؛ في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م ، وكان ذلك للحد من وقوع الجرائم الإلكترونية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات.

ثانياً : التوصيات

في سبيل الحد من الجرائم الإلكترونية ومكافحتها فإنني أوصي بالاتي:

- يتعين إدخال مادة أخلاقيات الانترنت ضمن المناهج الدراسية في التعليم ما قبل الجامعي.
- نشر الوعي بين صفوف المواطنين خاصة الشباب بمخاطر التعامل مع المواقع السيئة على الانترنت.
- تعزيز التعاون مع المؤسسات الدولية المعنية بمكافحة مثل هذه الجرائم .
- سن قوانين خاصة لمعالجة هذه الجرائم.
- الاستعانة ببرامج أمن قوية ضد الفيروسات.

وأخيراً وليس آخراً، وبعد أن من الله سبحانه وتعالى – عليَّ بإنجاز هذا البحث، فإنني لا أدعي إلمامي بكافة جوانب الموضوع، أو أنني قد أصبت الحقيقة في كل رأي أو اقتراح عرضته، ولكنها مجرد محاولة، فكل فكر يقبل الجدل والنقاش مهما كانت وجاهته ومنطقيته.

وأخيراً اسأل الله العلي القدير أن يوفقنا لما يحبه ويرضاه، وآخر دعوانا أن الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه، أفضل الصلاة وأتم التسليم. تم بحمد الله وتوفيقه

فهرس لأهم مراجع البحث

أولا : المراجع العربية :
- د/ أحمد حسام طه تمام "الجرائم الناشئة عن استخدام الحاسب الإلى" رسالة دكتوراة ، جامعة طنطا، ٢٠٠١ م
- د/احمد خليفة الملط، الجرائم المعلوماتية دار الفكر العربي الإسكندرية، بدون تاريخ.
- د/جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي)، الكتاب الأول، دار النهضة العربية، ١٩٩٢م
- د/حاتم عبد الرحمن منصور الشحات ،الإجرام ألمعلوماتي، دار النهضة العربية القاهرة ط ١ ٢٠٠٣ م
- د/شمس الدين إبراهيم احمد"وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري" دراسة مقارنة، طبعة دار النهضة العربية القاهرة ط ١ ٢٠٠٥م
- د/شيماء عبدا لغني محمد عطا الله" مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م"بحث منشور على موقع: http://www.f-law.net
- د/عادل عمر "جرائم الانترنت في مصر" مقال على موقع: http://www.adelamer.com
- د/عادل يوسف عبد النبي"الجريمة المعلوماتية وأزمة الشرعية الجزائية" بحث منشور بمركز دراسات الكوفة، العدد السابع ٢٠٠٨م
- د/عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الآلي، طبعة أولى الرياض ١٤١٤هـ
- د/عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي ، مصر سنة ٢٠٠٦م
- د/عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي الموحد ، دار الفكر الجامعي ، مصر سنة ٢٠٠٦م
- د/عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، بدون تاريخ.
- عبد الله بن عبد العزيز الخثعمي " التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية" رسالة مكملة لمتطلبات الحصول على الماجستير، مقدمة لجامعة نايف العربية للعلوم الأمنية.
- د/ عبد الله حسين علي محمود"إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات " بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي ، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع منتدى هيئة التحقيق والادعاء السعودي.
- د/علي جبار الحسيني، جرائم الحاسوب والانترنت، طبعة دار اليازوري العلمية للنشر والتوزيع، الأردن، ٢٠٠٩م

- د/عمر الفاروق الحسيني"تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الآلي" بحث منشور في كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، ١٩٩١م
- د/محمد أبو العلا عقيدة "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية" بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي ، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع كلية الحقوق جامعة المنصورة - http://www.f-law.net
- د/محمد الأمين البشري" تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت" بحث مقدم إلى الحلقة العلمية (الانترنت والإرهاب) خلال الفترة من: ١٧-٢١/١١/١٤٢٩هـ الموافق ١٥-١٩/١١/٢٠٠٨م بالتعاون مع جامعة عين شمس ، منشور على موقع جامعة نايف العربية للعلوم الأمنية
- محمد بن نصير محمد السرجاني" مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت" رسالة ماجستير مقدمه لجامعة نايف العربية للعلوم الأمنية، سنة ٢٠٠٤م
- د/محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ١٩٩٤م
- د/محمد عبد الرحيم سلطان العلماء "جرائم الانترنيت والاحتساب عليها" بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت جامعة الإمارات مايو ٢٠٠٥ م
- د/محمد عبد الله ابو بكر سلامة، موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت منشأة المعارف، الإسكندرية ٢٠٠٦.
- د/محمد عبد الله المنشاوي " جرائم الانترنت في المجتمع السعودي" رسالة ماجستير مقدمة إلى كلية الدراسات العليا بأكاديمية نايف العربية للعلوم الأمنية سنة ٢٠٠٣م
- د/محمد عبد الله منشاوي "جرائم الإنترنت من منظور شرعي وقانوني طبقا للقانون السعودي" منشور على موقع : http://www.f-law.net
- د/محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة دار الثقافة للنشر والتوزيع ، عمان، سنة ١٤٣٠ هـ - ٢٠٠٩م
- د/مصعب القطاونة"الإجراءات الجزائية الخاصة في الجرائم المعلوماتية" بحث منشور على موقع: http://www.lawjo.net
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، طبعة دار الفكر الجامعي، ٢٠٠٦م
- د/نبيله هبة هروال " الجوانب الاجرائية في مرحلة جمع الاستدلال" طبعة دار الفكر الجامعي ، مصر سنة ٢٠٠٦م
- د/هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة،١٩٩٢ م
- د/هشام رستم "الجرائم المعلوماتية، أصول التحقيق الجنائي الفني" مجلة الأمن والقانون، دبي العدد(٢)، ١٩٩٩م

- د/هشام رستم، ورقة عمل بعنوان:" جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة" منشورة بمجلة الدراسات القانونية، تصدره كلية الحقوق ، جامعة أسيوط، عدد ١٧ عام ١٩٩٥م.
- د/يونس عرب"جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور القواعد الإجرائية للملاحقة والإثبات" ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ /٢٠٠٢/٢م، منشور على موقع :**WwW.Lawyers-Gate.CoM**

ثانياً : المراجع الأجنبية:

- *Chirillo, John (٢٠٠٢) a.* Hack Attacks Revealed. Indianapolis, Indiana: Wiley Publishing
- *Chuvakin, A. & Peikari, C. (٢٠٠٤).* Security Warrior. Sebastopol, California
O'Reilly & Associates
- *Cole, Eric (٢٠٠٢).* Hackers Beware: Defending Your Network From The Willy
Hacker. Indianapolis, Indiana: New Riders Publishing.
- *Cronkhite, C., & McCullough, J. (٢٠٠١).* Access Denied: The Complete Guide to
Protecting Your Business Online. Berkeley, California: Osborne/McGraw-Hill.
- *Garfinkel, S., Spafford, G., & Schwartz, A. (٢٠٠٣).Practical Unix & Internet*
Security. Sebastopol, California: O'Reilly & Associates.
- *Hollis, S., David, S. B., David, J. I., Richard B., Wayne, C., & Wayne, P. W. (٢٠٠١). Electronic Crime Needs Assessment for*
state and Local Law Enforcement
- *Jamsa, Kris (٢٠٠٢). Hacker Proof: The Ultimate Guide to Network Security. Albany, New York: Delmar Learning.*
- *McClure, S., Scambray, J. & Kurtz, G. (٢٠٠١). Hacking Exposed: Network Security*
- *Mitnick, K. & Simon, W (٢٠٠٢). The Art of Deception: Controlling the Human Element of Security. Indianapolis, Indiana: Wiley Publishing.*
- *Rubin, Aviel (٢٠٠١). White-Hat Security Arsenal: Tackling the Threat. Boston: Addison-Wesley.*
- *Shinder, Debra (٢٠٠٢). Scene Of The Cyber crime: Computer Forensics Handbook. Rockland, MA: Syngress Publishing.*
- *Tulloch,Mitch (٢٠٠٣). Microsoft Encyclopedia of Security. Redmond, Washington: Microsoft Press*
- *Vacca, John (٢٠٠٢). Computer Forensics: Computer Crime . Scene Investigation.*