وزارة التعليم العالي و البحث العلمي

جامعة تبسة

كلية الحقوق والعلوم السياسية

قسم الحقوق

تخصص : قانون جنائي

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر الموسومة بـ

القرصنة الإلكترونية

الطالبة:

قحايريــة وســام

لجنة المناقشة:

-د /دربال عبد الرزاق - جامعة تبسة - رئيسا

-د /دلـــول الطاهـــر - جامعة تبسة – مشرفا ومقررا

-أ /مقـــران ريمـــة - جامعة تبسة - عضوا

السنة الجامعية 2014/2013

شكر وعرفان

لا بدّ و أنا أخطو خطوتي الأخيرة في رحاب الجامعة، من وقفة تعود بي إلى أعوام قضيتها في رحاب الجامعة مع أساتذتي الكرام الّذين قدّموا لنا الكثير باذلين بذلك جهودا كبيرة،لذاوقبل أن أمضي أقدّم أسمى معاني الشّكر و التّقدير للّذين حملوا أقدس رسالة، و أخصّ بالشّكر و التّقدير أستاذيو مثلي الأعلى الدكتور "**دلول الطاهر**"

و أقول لها بشراك قول رسول الله "إنّ الحوت في البحر،و الطّير في في السّماء ليُصلّون على معلّم النّاس الخير"

و أشكره بتفضله بالاشراف على هذه المذكرة وعلى ما قدمه لي من مساعدات منهجية وعلمية قيمة كانت لي نبرا منيرا ومرشدا .

كما أتقدم بفائق الاحترام والتقدير الى لجنة المناقشة والى الدكتور " **درويال عبد الرزاق** " الذي تقبل رئاسة لجنة المناقشة في هذه المذكرة ، والى الاستاذة الكريمة " **مقران ريمة** " التي قبلت أن تكون عضوا مناقشا لهذا العمل المتواضع .

والشكر موصول الى كل الاساتذة والعاملين في كلية الحقوق .

و كذلك أشكر كلّ من ساعدني على إتمام هذا العمل

المتواضع

إهداء

إلى من بلغ الرسالة وأدى الأمانة .. ونصح الأمة .. إلى نبي الرحمة ونور العالمين..

سيدنا محمد صلى الله عليه وسلم

إلى من كلله الله بالهيبة والوقار .. إلى من علمني العطاء بدون انتظار .. إلى من أحمل أسمه بكل افتخار .. أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد. إلى اليد الطاهرة التي أزالت من أمامي أشواك الطريق

ورسمت المستقبل بخطوط من الأمل والثقة

إلى الذي لا تفيه الكلمات والشكر والعرفان بالجميل إلى

والدي العزيز"علي "

إلى من ركع العطاء أمام قدميها

وأعطتني من دمها وروحها وعمرها حبا وتضحيا ودفئا لغدٍ أجمل

إلى الغالية التي لا أرى الأمل إلا من عينيها.إلى ملاكي في الحياة .. إلى معنى الحب وإلى معنى الحنان والتفاني

.. إلى بسمة الحياة وسر الوجود

إلى من كان دعائها سر نجا حي وحنانها بلسم جراحي

إلى أغلى الحبايب أمي الحبيبة "يمينة "

إلى إخواتي ورفقاء دربي وسندي على طول الأيّام .. في نهاية مشواري أريد أن أشكر على مواقفك النبيلة يا من تطلعتو لنا جحي بنظرات الأمل "جمال " و "بلال "

إلى من به كبرت و عليه اعتمدت...إلى شمعة أنارت أحلك اللّحظات...إلى من بوجوده أكتسب قوّة و إرادة لا مثيلها...إلىمن علّمني معنى التّفا ئل"وليد"

إلى من أرجو من الله أن ينزل على قبرهما الضياء والنور والسرور

ويجازيهما بالإحسان إحسانا وبالسيئات مغفرة ورضوانا

اللهم خلصهما من ضيق اللحود إلى جنّات الخلود وارحمهما واغفر لهما يارب العالمين

إلى "روح جدّتي الطّاهرة" و "روح جدي الطّاهرة" رحمهما الله

إلى الأخوات اللواتي لم تلدهن أمي .. إلى من تحلو بالإخاء وتميزوا بالوفاء والعطاء إلى ينابيع الصدق الصافي

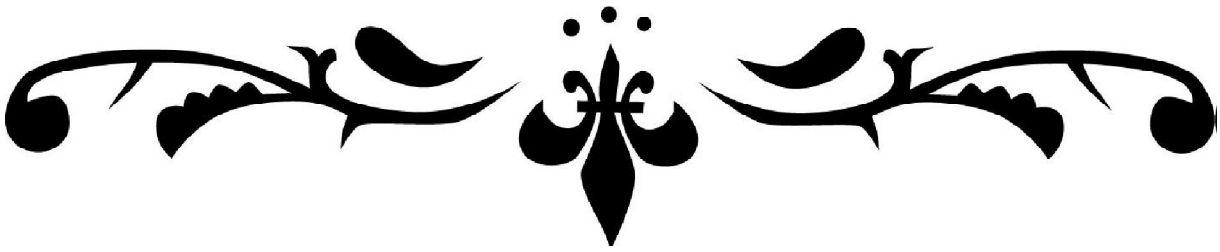
إلى من معهم سعدت ،وبرفقتهم في دروب الحياة الحلوة والحزينة سرت إلى من كانوا معي على طريق النجاح والخير

إلى من عرفت كيف أجدهم وعلموني أن لا أضيعهم"أسماء،مريم ،أميمة "

إلى كل من ساندوني و أعانوني وكانوا خير معين لي وخير دعم، و كانوا سببا في تمهيد الطّريق

وإلى كلّ منلم يذكرهمّ قلمي و يذكرهم قلبي

المقدمة



يعيش العالم اليوم عالمًا متغيرًا جديدًا يمتاز بالديناميكية و سعة التغير والتطور و اتساع المفاهيم و بأدق التفاصيل ،ومن لا يتعامل مع التفاصيل سيسقط في توجهاته الحضارية دون إدراك أبعادها ،ومع ازدياد التطور السريع و المذهل في تقنيات الاتصالات الحديثة،أدى بالعالم بالدخول إلى عصر المعلومات أو الثورة الإلكترونية ،واقترانه بأعظم تقنيات الاتصال الحديثة المتمثلة في شبكة الانترنت و التي تختزن معلومات الأرض الاقتصادية و العلمية و الثقافية و الاجتماعية، وكل ما يمت إلى النشاط و الحضارة البشرية ، كما أن هذه التقنية فعلت ما لم تفعله السياسة في توحيد الشعوب و الثقافات.

لكن، وكما أن لتقنيات الإلكترونية الحديثة دورها الإيجابي في حياة الشعوب ،فلها دور سلبي كذلك ، وهو أثر مترتب على إساءة استعمال الوسائل الإلكترونية الحديثة ، فأصبحت الشبكات الإلكترونية أداة لارتكاب الجريمة أو محلاً لها مما أدى إلى ظهور جرائم جديدة عابرة للحدود سميت حاليًا بالجرائم القرصنة الإلكترونية ، والتي تتسم بالحداثة و الأسلوب التقني في ارتكابها و سرعة التنفيذ، ومع ازدياد تمخض ثورة المعلومات الإلكترونية تزداد معها خطورة الاعتداءات الإلكترونية الكامنة في هاته الجريمة على المجتمعات بكافة نواحيها،مما يبرز الأهمية الملحة لجدارة البحث والدراسة والتحليل لجريمة القرصنة الإلكترونية.

أولا_ أهمية الموضوع : وتبرز من خلال جانبين هما :

أ - الأهمية العلمية :

تبدو أهمية الموضوع على وجه الخصوص في خطورة القرصنة الإلكترونية في الوقت الحاضر و الحاجة الملحة للتعاون القضائي الدولي لمواجهتها باعتبارها جريمة عالمية أخذت بالانتشار و الامتداد لتطال دولاً كانت بعيدة في الماضي عن هذه الظاهرة مثل الدول العربية ، و غيرها من البلدان النامية ، و يستدعي مكافحتها كظاهرة حديثة جهود عالمية و علمية يتم من خلالها التعرف على واقعها و سبل و دوافع ارتكابها ، و مخاطرها الاقتصادية و الاجتماعية و تهديدها للأمن الدولي ، خاصة في ظل قلة الدراسات العربية المتعمقة في هذا المجال .

ب - الأهمية العملية :

تبرز أهمية الموضوع عمليًا كونه من المواضيع التي تثير أكبر التحديات التي تواجهها دول العالم على المستوى التكنولوجي و الأمني و القانوني ، و كونه من المسائل التي تشغل بال أكبر الحكومات تطورًا و الأقل على حد سواء ، و كما تبرز الأهمية العملية للموضوع في التعرف على أهم الصعوبات القائمة التي تواجه مكافحة هذه الظاهرة الإجرامية الإلكترونية ، و بالتالي تحديد مدى ملائمة تطبيق القوانين التقليدية على هذه الظاهرة المستجدة .

ثانيا_ أسباب اختيار الموضوع: و يمكن ردها إلى :

أ - الأسباب الموضوعية :

من الأسباب الموضوعية التي دفعتني للبحث في الموضوع هو ظهور ما أطلق عليه "القرصنة الإلكترونية " في وقت ظلت فيه وجهات النظر الحالية متعارضة بشأن الاتفاق على تعريف لها ، بالإضافة إلى أن هذا الموضوع من المواضيع التي تدخل ضمن تخصصنا وكونه يجمع بين القانون الجنائي الداخلي إذ تدخل هذه الجريمة في صميم قانون العقوبات ، و كونها من الجرائم العابرة الحدود والتي تدخل في نطاق دراسات القانون الجنائي الدولي .

ب - الأسباب الشخصية :

فتمكن في قناعتي الخاصة بمدى خطورة القرصنة الإلكترونية ، فمن يطالع واقع الدول والأفراد اليوم عبر الوسائل الإلكترونية ، لا بد و أن يسمع و يعرف مدى معاناة هذه المجتمعات من هذه الظاهرة ، كما أنها لم تعد مجرد تهديد لدولة دون أخرى بل هي مأساة إنسانية و ثقافية وكارثة اقتصادية و سياسية و دينية ،إضافة إلى أن هذا الموضوع يتسم بالحداثة نسبيًا خاصة في دول العالم الثالث التي تعاني من فراغ في تشريعاتها القانونية ،و بالإضافة إلى أن هذه الظاهرة الإجرامية تصاعدت على مسرح الحياة بشكل يستدعي البحث و الدراسة من مختلف التخصصات .

ثالثا_ أهداف الموضوع :

من جملة الأهداف التي وددت الوصول إليها من خلال هذه الدراسة، هو نشر الوعي القانوني و التقني و الأمني عن القرصنة الإلكترونية للحد من تأثيراتها، وذلك من خلال التعرف على مفهوم القرصنة الإلكترونية ، و أهم الخصائص التي تتصف بها و أيضًا التعرف على الوسائل التقنية المستخدمة في ارتكابها ، بالإضافة لتعرف إلى أهم الجهود المبذولة في مواجهة هذه الظاهرة .

رابعًا _ تساؤلات الدراسة:

تعتبر القرصنة الإلكترونية من الموضوعات التي تكتسي أهمية خاصة، حيث أصبحت تستقطب اهتمام الباحثين و الدارسين في هذا المجال، كون أن هذا الموضوع يثير العديد من المشكلات القانونية، وأهم مشكلة محورية هي :

- ما مدى اعتبار القرصنة الإلكترونية من قبيل الإجرام ألمعلوماتي أم أنها جريمة من نوع خاص وفقا لقوانين خاصة ؟

وينبثق عن هذه الإشكالية أسئلة فرعية هي :

- ما هي القرصنة الإلكترونية ؟ وفيما تتمثل أهم التقنيات الإلكترونية في تنفيذها ؟ ، وماهي أهم معالم الصعوبات التي تعرقل إثبات وقوعها ؟ .

- ما مدى كفاية القوانين والجهود المبذولة في الحد من القرصنة الإلكترونية ؟ وما أهمية التعاون في مكافحتها ؟

خامسًا _ المنهج المتبع

بالنظر إلى طبيعة الموضوع و حداثته النسبية ، و للإجابة على الإشكالية المطروحة اعتمدت في دراستي هذه المنهج الوصفي التحليلي، **فالمنهج الوصفي** إعتمدتة لوصف هذه الجريمة و بيان خصائصها و آليات ارتكابها و مرتكبوها ، و**المنهج التحليلي** من خلال استقراء النصوص القانونية و تحليلها في محاولة الوصول إلى خطة عمل جيدة لمكافحة هذه

الجريمة، مع الاستعانة بالمنهج التاريخي في بداية البحث لدراسة التطور التاريخي للقرصنة الإلكترونية .

سادسًا_ الدراسات السابقة

لم أجد من الدراسات ما تناولت هذا الموضوع بصفة كاملة ، و لكن هناك من دراسات من تناولت أجزاء منه فقط ، أذكر منها :

- جمال وادي، " العلامة و الانترنت " ،(مذكرة ماجستير، فرع الملكية الفكرية ، جامعة الجزائر، 2003- 2006) .

- حفيظة خمايسية، " التعاون الدولي في مكافحة جرائم الانترنت "، (مذكرة لنيل شهادة الماجستير – فرع القانون الجنائي الدولي - ، كلية الحقوق و العلوم السياسية ، جامعة تبسة، 2011ـــــ2012) .

- مليكة عطوي،" الانترنت والملكية الفكرية "،(مذكرة ماجستير، كلية العلوم السياسية و الإعلام ، فرع علوم العلوم و الاتصال، جامعة الجزائر، 2003 - 2004) .

سابعًا _ الصعوبات

صادفتني في إتمام هذه الدراسة صعوبات أذكر منها :

قلة المراجع التي تناولت بصفة خاصة و محددة القرصنة الإلكترونية خاصة العربية منها ،حيث أن معظم المراجع التي تناولت هذه الجريمة تمت دراستها و معاقبتها بصفة عامة ضمن جرائم أخرى ، إضافة لذلك قلة الدراسات التي تناولت الجهود المبذولة لمكافحة القرصنة الإلكترونية بشيء من التفصيل ،بل كانت تشير إليه كحل أو مقترح تنتهي بها تلك الدراسات .

ثامناً_ التصريح بالخطة:

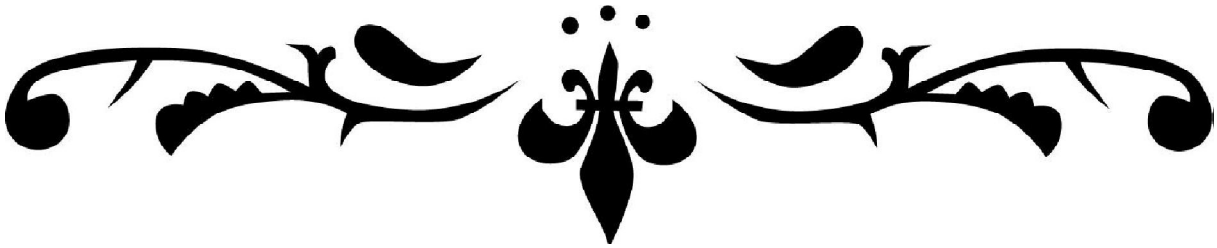
بما أن دراستي للموضوع مقيدة بعدد محدد من الصفحات فتناوله سيكون بشكل ضيق مع محاولة الإلمام بأكبر قدر من المعلومات ، لتقريب الفكرة لذهن كل من يقرا هذه المذكرة و إزالة اللبس بالإجابة عن الإشكالات المطروحة، والوصول إلى الأهداف المتوخاة منه اعتمدت على خطة مكونة من فصلين :

- في الفصل الأول لماهية القرصنة الإلكترونية ، والذي تم تقسيمه إلى ثلاثة مباحث: ليتم التطرق في المبحث الأول لمفهوم القرصنة الإلكترونية،و في البحث الثاني لتقنيات ارتكاب القرصنة الإلكترونية.

- أما الفصل الثاني تمت الدراسة فيه إلى الجهود المقررة لمكافحة القرصنة الإلكترونية، والذي تم تقسيمه إلى ثلاث مباحث عرض في الأول لجهود الوطنية للمشرع الجزائري، و في الثاني للجهود العربي المقررة،وفي الثالث للجهود الدولية.

الفصل الأول

ماهية القرصنة الإلكترونية



الفصل الأول: ماهية القرصنة الإلكترونية

سعت المجتمعات الإنسانية من وراء استخدامها لتكنولوجيا المعلومات الإلكترونية في مرافق الحياة المختلفة،لخلق مجتمع جديد خال قدر الإمكان من الجرائم والسرقات،إلا أن هذا لم يتم، فأصبحت تكنولوجيا المعلومات الإلكترونية في العديد من الأحوال معول هدم وتدمير لبنية المجتمع ، فاخترقت القوانين ليس تحت جنح الظلام ، بل في وسط النهار ، لكن دون أن يراك الآخرون ، فثورة المعلومات قد أتت بآثار السيئة على النظام والقانون ، ولعل أكثر وأكبر هذه الآثار السيئة تكمن في شبكة المعلومات العالمية " الانترنت " ، كون أنها غير خاضعة للمراقبة والتحكم ، وفي هذا فرصة لنشوء وزيادة الجرائم الالكترونية ، والتي من ضمنها ما يعرف بالقرصنة الالكترونية،وهكذا تأتي المخاوف من هذه الظاهرة الإجرامية الالكترونية من واقع فعلي ملموس ، إذ أنها تهدد بخرق الحقوق الخصوصية والحقوق المدنية الأساسية ، ذلك أنها تستخدم عن طريق الأنشطة الإجرامية القضائية ، سواء بارتكاب جرائم التزوير أو السرقة من خلال النفاذ إلى قواعد البيانات الشخصية ، والدخول غير الشرعي على الشبكات والتخريب العمدي للشبكات ، والى غير ذلك من هذه الآثار السلبية والتي قد تكون في بعض الأحيان مهددة لسيادة الدولة وفي بعض الأخر قد تكون قاتلة لعدد من أبناء هذه الدولة أو تلك ، فالقرصنة الإلكترونية ظاهرة إجرامية مستجدة نسبيا تقرع في جنابتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها ، لذا فإن إدراك ماهية هذه الظاهرة الإجرامية الإلكترونية ، تستدعي طرح العديد من الأسئلة التي تظل تشغل فكر الكثير من الناس ، هذه التساؤلات أصبحت حقا مثيرة ، بل تبرز حقيقة لا يمكن تجاهلها أو إغفالها تلك التي تتعلق بحاجة الناس الماسة إلى توفير الأمن للمجتمع من مخاطر القرصنة الإلكترونية ، والأمن في هذا الجانب لا يتأتى إلا من خلال التعرف على ماهية هذه الجريمة، وما هي أهم خصائصها ؟ ومن ثم من يرتكبها ؟ وما هي الوسائل والطرق الإلكترونية التي يتم استخدامها لتنفيذ هذا النوع من الجرائم؟،مع إبراز المحل الإلكتروني التي تقع عليه هذه الاعتداءات،ومن ثم تبيان ما هو الدليل الواجب توافره في هذه الجرائم لإثبات وقوعها؟،وذلك كله يتأتى من خلال إجراء العديد من الأبحاث والدراسات في هذا المجال ، ولهذا سنعمل في هذا الفصل على البحث في ماهية القرصنة الإلكترونية ، وفي هذا سنقسم هذا الفصل إلى ثلاثة مباحث كالأتي:

المبحث الأول: مفهوم القرصنة الإلكترونية.

المبحث الثاني: تقنيات ارتكاب القرصنة الإلكترونية.

المبحث الثالث:الإثبات الجنائي في بيئة القرصنة الإلكترونية.

المبحث الأول : مفهوم القرصنة الإلكترونية :

تعد القرصنة الالكترونية ظاهرة إجرامية مستجدة نسبيا تقرع في جنباتها أجراس الخطر، لتنبه مجتمعات العصر الراهن لحجم والمخاطر وهول الخسائر الناجمة عنها ، بوصفها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة ، من بيانات ومعلومات وبرامج بكافة أنواعها ، فهذه الظاهرة تتخذ أهمية استثنائية لإدراك ماهيتها ومراحل نشأتها وسماتها المميزة عن غيرها،وبناءا على ذلك سوف نقسم هذا المبحث الى ثلاثة مطالب ، نعرض في الأول للتعريفات المختلفة للقرصنة الالكترونية ، ونبرز في الثاني مراحل نشأة وتطور هذه الظاهرة ، وسنوضح في الثالث الخصائص المتعلقة بالقرصنة الالكترونية .

المطلب الأول : التعاريف المختلفة للقرصنة الإلكترونية .

المتتبع لما يقال وما يبحث حول القرصنة الالكترونية ، التي أوجدتها ثورة الاتصالات وتقنية المعلومات عبر العالم ، سواء على نطاق عربي أو دولي ، يلاحظ أن ثمة تباين أو عدم ثبات حول المصطلحات والتسميات التي أطلقت ولازالت تطلق على هذه الظاهرة الإجرامية الجديدة التي باتت تهدد الدول قبل الأفراد ، وقد اختلفت التسميات وتعددت وتطورت حتى لدى الباحث ذاته تبعا لتطور مفهوم هذه الجريمة المستحدثة ووضوح صدورها في الواقع العملي[1] ، ومن تلك التسميات نعتها بجريمة الالكترونية أو جرائم الكمبيوتر والانترنت ، أو جرائم التقنية العالية، أو جرائم الاحتيال ألمعلوماتي أو جرائم الهاكرز ، أو الاختراقات التقنية ، وما قيل الأخير السيبر كرايم (cyber crime) أو أصحاب الياقات البيضاء .[2]

الفرع الأول : التعريف اللغوي.

" ق ر ص " (القرص) بالإصبعين وبأيه نصر و (قرص) البراغيث لسعها ، و(القرص) و (القرصة) من الخبز و (قرص) العجين من باب نصر قطعة قرصة .[3]

---

[1] - د.عبد الحكيم رشيد توبة ، جرائم تكنولوجيا المعلومات ، الطبعة الاولى ، دار المستقبل للنشـــر والتوزيـــع ، الاردن ، 2009.

[2] - مليكة عطوي ، الانترنت والملكية الفكرية ، مذكرة لنيل شهادة الماجستير – فرع علوم والاتصال - ، كلية الحقـــوق ، جامعة الجزائر ، 2002 – 2003 ، ص 91 .

[3] - د.الرازي محمد بن أبي بكر,مختار الصحح,الطبعة الرابعة ,المكتبة المصرية ,لبنان,1418,ص 251.

قرصنة : القرصنة كما عرفتها المادة 111 من اتفاقية جامايكا الجديدة لقانون البحار لعام 1982 هي : " كل عمل من أعمال العنف والاعتقال والسلب غير المشروعة التي يرتكبها ، لأغراض شخصية ، ملاحو أو ركاب سفينة خاصة أو طائرة خاصة [1] ، فمن هذا التعريف اللغوي فإنه يظهر أنه بمجرد سماع كلمة قرصنة فإنه يتبادر إلى أذهاننا عصابات سرقة السفن البحرية والسطو عليها ، ولهن ما فيها ، وهو ما يفعله قرصان الأنظمة الالكترونية لكن بوسائل حديثة . [2]

الفرع الثاني : التعاريف الاصطلاحية .

إن اختيار التعريف الاشمل للقرصنة الالكترونية يكون بارتباط البعدين التقني والقانوني لأنه إذا عدنا للحقيقة الأولى المتصلة بنشأة وتطور تقنية المعلومات نجدها تشمل فرعين يرى بحكم التطور تقاربهما واندماجهما ، هما الحوسبة والاتصالات ، فتقوم الحوسبة على استخدام التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق ، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة هذه الدلالات يحددها الأستاذ Zangeyuexiao بالرسائل والأخبار والبيانات والمعروفة والرموز والعلامات وغير ذلك[3] ، أما البعد القانوني فينصرف إلى نظرية الجريمة من حيث النص التجريمي والعقاب ، ومن حيث قاعدة التكييف ، فليس سهلا وفي ظل تقنية أنظمة المعلومات ووسائلها وتطبيقاتها أن يضبط السلوك البشري خصوصا حيث يكون بصورته السلبية ،وفي هذا دفع قوي نحو البحث في بعد قانوني لتلك السلوكيات,[4] ، وفي هذا تعددت تعاريف القرصنة الالكترونية فختصر تعريفها على : أنها استخدام أو النسخ الغفير المشروع لنظم التشغيل أو البرامج الحاسوبية المختلفة والاستفادة منها شخصيا أو تجاريا.[5]

---

[1]-د. أحمد سعيفان,قاموس المصطلحات السياسية والدستورية والدولية,الطبعة الأول,مكتبة لبنان,لبنان ، 2004، ص 267.

[2]- أنظر المقال المنشور متاح على الموقع : www.alukon.net ، بتاريخ 2014/02/24 ، على الساعة 23:09.

[3]- د .هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، ط 1 ، دار النهضة العربية ، القـاهرة ، 1992 ، ص 20 .

[4]- د . جلال محمد الزعبي وأسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنـة ، الطبعـة الأولى، دار الثقافة للنشر والتوزيع ، الاردن ، 2010 . ص63 .

[5]- د. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية ، 2007 ، ص10.

- أيضا وهي الجرائم الواقعة على المعلومات والبرامج الموجودة داخل الجهاز الكمبيوتر سواء كانت مخزنة على ديسك مورد أو قرص صلب ، أو على أقراص مضغوطة " س د ي " وتتمثل هذه الجرائم في تقليد البرنامج أو سرقته أو إتلافه أو تعطيل حركته أو العبث بالبيانات المخزنة في ذاكرة الجهاز[1] .

وكما أنها تعرف بأنها التوصل إلى كافة المعلومات في الكمبيوتر بصورة غير مشروعة ونسخ البرامج بدون وجه حق ، والذي يرمي إلى الاستيلاء على بعض حقوق الملكية الأدبية أو الصناعية المحمية قانونا للاطلاع على الأسرار الاقتصادية وإمكانية التلاعب بالقيود المصرفية أو مؤسسات إصدار البطاقات الائتمانية ، أو الحصول على المعلومات السياسية والعسكرية والإستراتيجية والخطط ذات الطابع السري[2].

وكما تعرف القرصنة الالكترونية في مجال الاعتداء على العلامة التجارية عبر الانترنت،[3] بأنها السطو الالكتروني وهو أن يقوم شخص أو مشروع لا يمتلك أي حق على علامة تجارية بتسجيل هذه العلامة في صورة عنوان الكتروني على شبكة الانترنت ، وذلك يقصد الأضرار بمالك هذه العلامة ، أو يقصد إعادة بيع العنوان الالكتروني إلى هذا المالك مرة أخرى بثمن مغالي فيه ، ومن ثم نكون أمام قرصنة الكترونية سواء قصد القرصان من تسجيل العنوان الالكتروني إعادة بيعه مرة أخرى للمالك الأصلي للعلامة أو لأحد منافسيه ، أو قصد منه منع المالك من تسجيل هذا العنوان[4] .

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في نيسان 2000 فقد تصدى لوضع محاور استرشادية لبيان تعريفها فقال : " أنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي ، أو شبكة حاسوبية ، أو داخل نظام حاسوبي ، والجريمة التي تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية [5].

---

[1]- د. محمد أمين الرومي ، جرائم الكمبيوتر والانترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2003 ، ص 19 .

[2]- د – عبد الحكيم رشيد توبة ، المرجع السابق ، ص 110 .

[3] - لمزيد من التفاصيل حول العلامة التجارية عبر الانترنت راجع: جمال وادي ، العلامة و الانترنت ، مذكرة لنيل شهادة ماجيستر، كلية الحقوق بن عكنون، جامعة الجزائر ، 2002-2003، ص 03.

[4] د.شريف محمد غنام، حماية العلامات التجارية عبر الانترنت في علاقاتها بالعنوان الالكتروني ، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص 103

[5]- د. جلال محمد الزعبي وأسامة أحمد المناعسة ،المرجع السابق ، ص 65 ، 70.

المطلب الثاني : نبذة تاريخية للقرصنة الالكترونية .

تعد دراسة التطور التاريخي للقرصنة الالكترونية تبعا لتطور التقنية واستخداماتها ، الخطوة الأولى لازدياد تبيان هذه الجريمة وخصائصها، ومن ثم سيتم استعراض من خلال: الفرع الأول لمراحل نشأة القرصنة الإلكترونية و الفرع الثاني حالات تاريخية لوقوع القرصنة الالكترونية .

الفرع الأول : مراحل نشأة القرصنة الإلكترونية

ارتبط ظهور القرصنة الالكترونية بظهور الانترنت كوسيلة اتصال عالمية وسريعة ، وارتبط ظهورها أيضا بالفكرة السائدة لدى الأغلبية بأن الانترنت فضاء لا يحكمه القانون[1] .

أولا: القرصنة الهاتفية

فقبل عام 1969 من هذه السنوات لم يكن للكمبيوتر وجود ، ولكن كان هناك شركات الهاتف وفي هذا ظهرت القرصنة الهاتفية والتي كانت المكان الأول لظهور ما نسميه الكاكرز في وقتنا الحالي ، وكان ظهوره يعود لعام 1878 ، في الولايات المتحدة الأمريكية وإحدى شركات الهاتف المحلية ، حيث كان أغلب العاملين في تلك الفترة من الشباب المتحمس لمعرفة المزيد من هذه التقنية الجديدة والتي حولت مجرى التاريخ ، فكان هناك الشباب يسمعون الى المكالمات التي تجري في هذه المؤسسة ، وكانوا يتلاعبون بالخطوط الهاتفية ، فنجد مثلا هذه المكالمة الموجهة من السيد مارك تصل السيد جون ، وكل هذا كان بغرض التسلية لتعلم المزيد ، لهذا قامت الشركة بتغيير الكوادر العاملة الى كوادر نسائية .

ثانيا: في الستينيات

في الستينات من هذا القرن ظهر الكمبيوتر الأول ، لكن هؤلاء الهاكزر كانوا لا يستطيعون الوصول إلى الكمبيوترات وذلك لأسباب منها كبر حجم هذه الآلات في ذلك الوقت ووجود حراسة على هذه الاجهزة نظرا لأهميتها ووجودها في غرف ذات درجة حرارة ثابتة، والغريب في الأمر أن في الستينات الهاكزر هو مبرمج قوي أو عبقري ، فالهاكزر في تلك الفترة هو المبرمج الذي يقوم بتصميم أسرع برنامج من نوعه ويعتبر

[1]- د . شريف محمد غنام ، المرجع نفسه، ص 102 .

دينيس ريتشي، وكين تومسون أشهر هاكر على الإطلاق ، لأنهم صمموا برنامج اليونكس ، وكان يعتبر الأسرع وذلك عام 1969[1]

ثالثا : العصر الذهبي للهاكرز 1980 – 1989 .

وفي عام 1981 أصدرت شركة IBM ، جهاز كمبيوتر سمته بالكمبيوتر الشخصي لصغر حجمه ، ولهذا فقد بدأ الهاكرز في تلك الفترة بالعمل الحقيقي لمعرفة طرقة عمل هذه الأجهزة وكيفية تخريب هذه الأجهزة [2]، وفي هذه الفترة ظهرت مجموعات من الهاكرز وكانت تقوم بعمليات تخريب الأجهزة المؤسسات التجارية ، وفي عام 1973 ظهر فيلم سينمائي إسمه (حرب الالعاب) تحدث هذا الفيلم عن عمل الهاكرز وأنهم يشكلون خطورة على الدولة واقتصادها ، وحذر الفيلم من الهاكرز[3] .

رابعا : حرب الهاكرز العظمى 1990 – 1994 .

البيانات الأولى لحرب القرصنة هذه في عام 1984 ، حيث ظهر شخص اسمه ليكس لوثر ، وأنشأ مجموعة إسمها (LOD) وهي عبارة عن مجموعة من الهاكرز والهواة الذين يقومون بالقرصنة على الأجهزة الأجرين ، وكانوا يعتبرون من أذكى الهاكرز في تلك الفترة، إلى أن ظهرت مجموعة اسمها (MOB) وكانت بقيادة شخص يدعى (فيبر) ، وكانت هذه المجموعة منافسة لمجموعة (LOB) ، ومع بداية العام 1990 بدأت المجموعتان بحرب كبيرة سميت بحرب الهاكرز العظمى وهذه الحرب كانت عبارة عن محاولات ، كان طرف اختراق أجهزة الطرف الآخر ، واستمرت هذه الحرب ما يقارب الأربعة أعوام وانتهت بالقبض على (فيبر) رئيس مجموعة (MOB) ، ومع انتهاء الحرب ظهر الكثير من المجموعات والهاكرز الكبار[4] ،وما بعد عام 1994 تم القبض على أعظم هاكرز في التاريخ " كفين متنيك " الذي قام بسرقات كثيرة دوخت الاف بي آي ، ولم يستطيعوا معرفة الهاكرز

---

[1]- د.عبد الصبور عبد القوي ، علي مصري ، الجريمة الالكترونية ، الطبعة الاولى ، دار العلوم للنشر والتوزيع ، القاهرة ، 2008 ، ص 13.

[2]- د . نعيم مغبغب ، مخاطر المعلوماتية والانترنت على الحياة الخاصة وحمايتها ، دراسة في القانون المقارن ، الطبعة الثانية ، منشورات الحلبي الحقوقية ، لبنان ، 2008 ، ص 14 .

[3]- راجع مقال : محمد محمود عمارة ،"تاريخ القرصنة الالكترونية بين العبقرية و انتهاك الفوائد، المتاحة على الموقع: www/sooid.net، بتاريخ2014/03/24 ، على الساعة 03:25.

[4]- د.عبد الصبور عبد القوي على المصري ، المرجع السابق ، ص 56 .

في أغلب شرقاته ، في مرة من المرات استطاع أن يخترق الشبكة الخاصة بشركة BIGTAL EGQIBMENT COMPENY ، وتم القبض عليه في هذه المرة وسجنه لمدة عام ، وبعد خروجه من السجن كان أكثر ذكاء ، ومن أشهر جرائمه سرقة الأرقام الخاصة ببطاقة الائتمان والتي كانت أخر جريمة له تم القبض عليه وسجنه لمدة عام ، ولكن إلى ألان لم يخرج من السجن لان FBI يرون بأن كيفين هذا خطيرا ولا توجد شبكة لا يستطيع اختراقها .

خامسا : الهاكرز في الدول العربية .

للأسف الشديد كثيرا من الناس في الدول العربية يرون بأن الهاكرز هم الأبطال ، بالرغم من أن العالم كله غير نظرته للهاكرز بعد القبض على " كيفين متنيك " ، فمنذ دخول الانترنت للدول العربية في عام 1996 والناس يبحثونه عن طريق القرصنة الجديدة ، وكثيرا من الناس تعرضوا لهذه المشكلة فآخر الإحصائيات ذكرت بأن هناك أكثر من 80 % من المستخدمين العرب أجهزتهم تحتوي على ملف الباتش ، والذي يسهل عمل الهاكرز وكثير من الناس في الدول العربية يجد بأن هناك فرق كبير بين ما يسمى بالهاكرز أو الكراكز ، ولكن الاسمان هما لشخص واحد وهو قرصان ، الفرق البسيط بينهما هو الهاكرز 90 %من عمله يقوم به في فضاء الانترنت ، أما الكراكر أو ما يمكن أن نسميه سارق البرامج فهو يقوم بعمله في أغلب الأحيان دون الحاجة للاتصال بالشبكة ، فهو يقوم بفك شفرة البرامج ، لا توجد مجموعات حقيقية في الدول العربية فيما عدى بعض المحاولات الفردية البسيطة ، منها على سبيل المثال شرقة 10.000 جنيه مصري من قبل هاكرز مصري[1] ، وفي هذه الحقبة تم رصد 1600 حالة لإساءة استخدام الحاسوب وتم تقديم استبيان من قبل معهد ستانفورد للتحضير لمناقشة مشروع قانون الجريمة الاقتصادية ، أما معهد الإجرام وقانون العقوبات الاقتصادي في ألمانيا الاتحادية قام بتقديم دراسة تضمنت وصفا لـــ 31 جريمة ارتكبت بواسطة الحاسوب ، وتوالت الدراسات التي رصدت وسجلت العديد من جرائم الحاسوب[2].

[1]- د.عبد الصبور عبد القوي على ، المرجع السابق ، ص 57 .

[2]- د .يونس عرب ، موسوعة القانون وتقنية المعلومات – جرائم الكمبيوتر والانترنت ، منشورات إتحاد المصارف العغربية ، الجزء الاول ، الطبعة الاولى ، أبو ظبي 2002 ، ص 302 .

وفي القرن الحالي بدأت أنشطة القرصنة الالكترونية باختراق مواقع المعلومات ونظمه عبر الانترنت ، والدخول دون تصريح أو تخويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيه ، وكذلك تعطيل الأنظمة بالبرمجيات الخبيثة أو التدمير المادي لها ، وغيرها من الصور التي تطرح اليوم إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني[1].

الفرع الثاني : حالات تارخية لوقوع القرصنة الالكترونية .

في عام 1986 م ، قام شخص يدعى روبير توسوتو " كولومبي الجنسية " بسرقة خط تيلكس حكومي ليرسل عبره مجموعة رسائل الى مصارف في المملكة المتحدة ومنها الى دول أخرى ونتج عن هذه الرسائل نقل 13.5 مليون دولار من أرصدة الحكومة الكولومبية .

وفي عام 1988 قام أحد طلاب جامعة – كورل بزراعة برنامج – worm - في شبكة حواسيب حكومية انتشر خلالها في 6000 حاسوب ، وبعد أن تم كشفه طرد من الجامعة ، وحكم عليه بإيقافه عن العمل 3 أعوام ، وتغريمه مبلغ 10.000 دولار .

أيضا قد حكمت المحكمة الملكية البريطانية في دينة ردينغ على شركة " سايبر سوفت " بغرامة 12000 جنيه إسترليني بعدما أثبت أنها تتعاطى قرصنة البرامج وبعد أن وجد في مكاتبها 1200 قرص تتضمن برامج منسوخة ، 700 مرجع مستورد من الشرق الأقصى من دون إذن رسمي لذلك .

كذلك نظرت المحاكم البريطانية في دعوى رفعتها جمعيات مكافحة القرصنة في أمريكا وبريطانيا ضد مجموعة بمرور الصحف العائدة لروبرت ماكسويل ، تم الكشف على 90 % من البرامج الآتية ، وكانت الاسطوانات المقرصنة تشغل في الأجهزة الشخصية ، وطالبوا أمام المحكمة محو الاسطوانات ودفع تعويض يتجاوز 250 ألف دولار ، علما بأن ماكسويل كان يشجع على اعتماد القرصنة وكان قد توفي في ظروف غامضة عام 1991 .

[1]- د .علي جبار الحسناوي ، جرائم الحاسوب والانترنت ، دار اليازوري العلمية للنشـــر والتوزيـــع ، الاردن ، 2009 ، ص21 .

المطلب الثالث : خصائص القرصنة الالكترونية .

حين انتشرت شبكات الحاسب والمعلومات بطول العالم وعرضه ودخلت تطبيقاتها بيئة المجتمعات المعاصرة ، وأسهمت ولا شك في تعزيز التواصل الحضاري والثقافي والتفاهم الإنساني وكسر حواجز العزلة الاتصالية بين الشعوب ، إلا أنها في الجانب الأخر ساعدت على شيوع الجريمة بمختلف أشكالها لتقود إلى ما يمكن تسميته بالقرصنة الالكترونية ، والمتأمل في حال شبكة الانترنت على وجه الخصوص ، يدرك ما قدمت هذه الوسيلة من تسهيلات كبرى لأنشطة القرصنة الالكترونية ، جاعلة الكثير من البلدان عرضة لمخاطر وآثار هذه الجريمة الذكية العابرة للحدود التي باتت اليوم يهدد كيان المجتمع الإنساني كله ، وفي سياق هذه الجريمة وظروف ارتكابها من خلال الأنظمة والشبكات ، فقد حدد بعض الفقهاء بيان لأفعالها خصائص متفردة لا تتوافر في أي من أفعال الجرائم التقليدية في أسلوبها وطريقة ارتكابها ، والتي ترتكب يوميا في كافة دول العالم ،و أهم خصائص القرصنة الالكترونية فهي :

أولا :الحاسب الآلي هو أداة لارتكاب القرصنة الالكترونية ، وفحوى هذه الخاصية أن كافة الجرائم الالكترونية ، وبما فيها القرصنة الالكترونية ، يكون الحاسب الآلي هو الأداة لارتكابها، وبه يتم الدخول إلى شبكة الانترنت وبالتالي يتم تنفيذ القرصنة الالكترونية بأي شكل[1]، إضافة إلى ما سبق فإن هذه الجرائم ، تتطلب إلماما كافيا بمهارات ومعارف فنية ، كالمعرفة التقنية بالحاسب الآلي ، وكيفية تشغيله واستخدامه ، وهذا ما تؤكده الدراسات والإحصاءات ، ولعل التطور الحاصل في ميدان البرمجة له من الأثر البالغ لازدياد عدد هذه الجرائم وتتناسب خطورة القرصنة الالكترونية مع المعرفة التقنية تناسبا طرديا ، فكلما تقدمت المعرفة التقنية لدى الأفراد كلما زادت احتمالية توظيف هذه المعرفة بشكل غير مشروع .

ثانيا : تتميز بصعوبة اكتشافها وإثباتها ويرجع السبب في ذلك إلى أنها لا تترك أثر خارجيا، فلا يوجد جثث لقتلى ولا آثار للدماء ، وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة ، ويعد التطور التكنولوجي المتلاحق سببا رئيسيا لصعوبة اكتشافها وإثباتها،

[1]- د .أمير فرج يوسف ، الجريمة الالكترونية والمعلوماتية ، الطبعة الأولى ، الناشر مكتبة الوفاء القانونية ، الإسكندرية ، 2011 ، ص 15 .

حيث أن شبكة الانترنت مثلا انتشرت بواسطتها مكاتب معروفة ومتخصصة ، ترتزق من قيامها بأعمال السطو وبيع المعلومات ، وبالإمكان الاستعانة بها ، أو استئجار القراصنة المحترفين للقيام بالأعمال غير المشروعة ، المتصلة بالحاسب الآلي ، بمقابل مبالغ يتفق عليها ، ومما يزيد الأمر تعقيدا ، أن هؤلاء القراصنة لا يهاجمون ، من أجهزة الحاسب الخاصة بهم وإنما يدخلون إلى شبكات بعيدة عنهم ويهاجمون من خلالها، ويرجع السبب في صعوبة اكتشاف وإثبات أفعال القرصنة الالكترونية إلى عدم وجود إحصائيات دقيقة تحدد الحجم الحقيقي لهذه الظاهرة ، إلى عدم تعاون المجني عليه[1].

ثالثا : إن القرصنة الالكترونية قد ترتكب عن طريق حاسب آلي في دولة ما ، في حين يتحقق الفعل الإجرامي في دولة أخرى ، كما أنها تمتاز بالتباعد الجغرافي بين الفاعل والمجني عليه ، ومن الوجهة التقنية بين الحاسوب أداة الجريمة وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء ، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة ، وبفعل سيادة تقنيات شبكات النظم والمعلومات امتد خارج هذه الحدود ، دون تغيير في الاحتياجات التقنية ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق.

رابعا : تعتبر القرصنة الالكترونية من نوع الجرائم العابر للحدود وبالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات ، والاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض والجرائم الاقتصادية والمالية وجرائم التلوث البيئي[2].

خامسا : تمتاز أيضا القرصنة الالكترونية بسهولة ارتكابها وهذا نظرا لسهولة انتشار شبكة الانترنت في الآونة الأخيرة على مستوى العالمي ، بحيث أصبح قراصنة المعلومات بسهولة أن يقوموا باختراق نظم المعلومات المرتبطة بالشبكة وقد لاحظ " سكوت سارتي " المسؤول عن مكافحة الجريمة على الانترنت ، في وزارة العدل الأمريكية ، أن الكمبيوتر

[1]- د .عبد الحكيم رشيد توبة ، المرجع السابق ، ص 141 .

[2]- د .علي جبار الحيسناوي ، المرجع السابق ، ص 45 .

الموصول بشبكة الانترنت أصبح سلاحا لاقتراف هذه الجرائم في عالم بلا حدود ، وأضاف أن شبكة الانترنت تسهل الجريمة أيضا ، واعترف " دغلاس بيريت " ، أحد المسؤولين في مركز الحماية من جرائم الحاسب الآلي ، التابع للشرطة الفيدرالية الأمريكية بأنه لا يمكننا أن نتوقع كل شيء ، لان تحديد الخطر أمر بالغ الصعوبة .

سادسا : أنها تعتمد على قمة الذكاء ، والمهارة في ارتكابها كما أنها تعتمد على الخداع ، والتضليل في التعرف على مرتكبيها[1] ، وكذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي ، ,ان الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم [2].

[1]- د . نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، ناشر لمنشأة المعارف ،القـاهرة، 2008 ، ص 113 .

[2]- د . منير محمد الجنبهي و د .ممدوح محمد الجنبهي ، جرائم الانترنـت والحاسـب الآلـي ، دار الفكـر الجـامعي ، الاسكندرية ، 2006 ، ص 15 .

المبحث الثاني : تقنيات ارتكاب القرصنة الالكترونية .

لقد أصبح موضوع القرصنة الالكترونية محور اهتمام العديد من المهتمين بشؤون المجتمعات يبد أن الأمر بالنسبة لعامة الناس لا زال يكتنفه الغموض والالتباس ، لاسيما عن أولئك الذين ينفذون هذه الجرائم ، فالعديد من عامة الناس يسألون عن: من هم الأشخاص الذي يقومون بمثل هذه الأعمال الإجرامية ؟ وما الوسائل والطرق التي تتبع في ارتكاب هذا النوع من الجرائم؟ و ماذا تستهدف هذه الظاهرة الإجرامية الالكترونية؟ ، وبناءا على هذا سوف نقسم هذا المبحث إلى ثلاث مطالب ، نعرض في الأول الجاني والمجني عليه الالكتروني ، ونوضح في الثاني المحل الالكتروني المستهدف، و أخيرا نبرز أهم الأسلحة الالكترونية في تنفيذ القرصنة الالكترونية.

المطلب الأول : الجاني والمجني عليه الالكتروني

إن التسارع المذهل الذي يشهده عالم المعلوماتية والتقنيات الرقمية الحديثة انعكس بدوره على الجرائم التي ترتكب في البيئة التقنية الالكترونية فأصبحت أمام جرائم مستحدثة سريعة التطور وهذه الجرائم وغيرها تحتاج لطرفين فاعل أو جاني ومجني عليه ، إلا أن الأطراف هنا يختلفون نوعا ما عن أطراف الجرائم التقليدية إذ المجرم الالكتروني له دراية ومعرفة بالحاسب الآلي كشرط أساسي ويستخدم أدوات خاصة وأجهزة معينة لإتمام جريمته فيما المجني عليه فيها ذو صلة وثيقة بتقنية الالكترونية ومشتملاتها، نبحث ذلك كله في فرعين كالأتي :

في الفرع الأول الجاني الالكتروني و في الفرع الثاني المجني عليه الالكتروني.

- الفرع الأول : الجاني الالكتروني .

الجاني في الجرائم الالكترونية ، ومن بينها القرصنة الالكترونية شخص طبيعي ، يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي ولا نقصد هنا ذلك المستوى الرفيع العالي عن المعرفة ، لأن الحد الأدنى من المعرفة يكفي لظهور الجريمة وإمكان ارتكابها، خصوصا إذا ما اتسعت دائرة الإجرام فاستعان الفاعل ذاته بغيره ممن يساعدوه في ارتكاب الجريمة ، وممن لديهم المعرفة التقنية اللازمة أو الأجهزة الالكترونية اللازمة ، وبصورة التدخل أو المساهمة بمعناها الواسع، هذا الفاعل قد يقوم بعمله غير

المشروع هذا إما بحسن نية أو بسوء نية فيرتكب أعمالا قد تسبب فعلا ضررا عظيم ، وقد لا يسبب منه شيئا [1].

وأمام التطور والتغير السريع في أنماط الجرائم الالكترونية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي القرصنة الالكترونية ، ولكن يمكن لنا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية ، أن نبين بعض هذه الأنماط لهؤلاء المجرمين ولكن لابد من الإشارة أولا إلى أن هذه التصنيفات لا تعني أن كل مجرم إلكتروني يتدرج تحت فئة محددة دون غيرها من الفئات المذكورة ، بل يمكن أن يكون المجرم الواحد مزيجا من اكثر من طائفة أو فئة .

أولا - المخترقون أو المتطفلون :

هذه الطائفة لا تختلف عن طائفة الهاكرز ، علما أن بين الاصطلاحين تباينا جوهريا ، فالهاكرز متطفلون يتخذون إجراءات أمن النظم والشبكات ، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية ، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة ، أما الكريكرز فإن اعتداءاتهم تعكس ميول جريمة خطرة تتبني عنها رغباتهم في إحداث التخريب [2]، ومع أن هذا المعيار غير منضبط إلا أن الدراسات والمعالجات في حقل جرائم الكمبيوتر والانترنت ، ومن بينها القرصنة الالكترونية، أثبتت أن اصطلاح الهاكرز مرادفا في الغالب لهجمات التحدي ، طبعا دون أن يؤثر هذا التمييز على مسؤولية مرتكبي الأنشطة من كلا الطائفتين ومسائلاتهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم والسمة الغالبة على أعضاء هذه الطائفة صغر السن ، وقلة الخبرة ، وعدم التمييز بين الأنظمة محل الاختراق وبرغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم الكمبيوتر التابعة للشركات المالية والتقنية والبنوك ومصانع الألعاب والمؤسسات الحكومية ومؤسسات الخدمة العامة ، وكثر الحديث عن وقائع عملية كما في حالة اختراق أحد الصبية الذي لا يتجاوز عمره السابعة عشر ، لكمبيوترات العديد من المؤسسات الإستراتيجية في أوروبا والولايات المتحدة ، ومن بينها الكمبيوترات المتصلة ببرامج حرب

[1]- د . جلال محمد الزعبي وأسامة محمد المناعسة ، المرجع السابق ، ص 71 .

[2]- د . عبد الحكيم رشيد توبة ، المرجع السابق ، ص 157 .

النجوم الذي كان مخطط لتنفيذه من قبل الولايات المتحدة في حقبة الحرب الباردة [1] ، أما السمة المميزة الأخرى لهذه الطائفة تبادلهم للمعلومات فيما بينهم ، وتحديدا التشارك في وسائل الاختراق وآليات نجاحها وإطلاعهم بعضهم البعض على مواطن الضعف في نظم الكمبيوتر والشبكات ، حيث تجري عمليات التبادل للمعلومات فيما بينهم وبشكل رئيسي عن طريق النشرات الإعلامية الالكترونية ومجموعات الأخبار [2]، وفي تطور حديث لتنظيم هذه الطائفة نفسها يجري عقد مؤتمرات لمخترقي الكمبيوتر يدعى لها الخبراء من بينهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم فيما بينهم ، وبالرغم من أن الخطورة في هؤلاء تكمن بمثابرتهم على أنشطة الاختراق وتطوير معارفهم التقنية وبالرغم من توفر فرصة استغلال هؤلاء من قبل منظمات وهيئات إجرامية فإنه ومن ناحية أخرى ساهم العديد من هؤلاء المخترقين في تطوير نظم الأمن في عشرات المؤسسات في القطاعين الخاص والعام، وعليه فالها كرز الذي يكون دافعهم الأساسي هو التطفل ، فإنهم هاكرز المستقبل ، والذين يحصرون أنفسهم في نطاق استكشاف وفحص النظم بدون محاولة القيام بأية عمليات تخريب كبيرة ، أما الهاكرز الذي يكون دافعهم الأساسي هو التخريب فهم هؤلاء الذين يتعدون تلك الحدود وينصب اهتمامهم على سرقة المعلومات متسببين في إحداث أنواع متعددة من الدمار، وفي بعض الأحيان يتسببون في تدمير نظم بأكملها ، وكما يستخدم بعضهم الآخر البرامج التي تؤدي إلى إحداث التلف والدمار في أنظمة الكمبيوتر والتي يقومون بتنزيلها واستخدامها، ولا يتسم العديد من هؤلاء الهاكرز بالمهارة فهم مجرد مجموعة من المرضى والمنحرفين وعلى العموم توجد علاقة وثيقة بينهم وبين غيرهم من المجموعات الصغيرة السرية الغامضة ، التي تكون في منآى عن مجتمع التبادل الحر والذكي للمعلومات الذي يدعمه الهاكرز الآخرون[3] .

ثانيا – المجرمون المحترفون :

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية ، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها ، ولذلك فإن هذه الطائفة تعد الأخطر من

[1]- د .عبد الحكيم رشيد توبة ، المرجع السابق ، ص 156 .

[2]- د .علي جبار الحسناوي ، المرجع السابق ، ص 49 .

[3]- د . نسرين عبد الحميد نبيه ، المرجع السابق، ص 41 .

بين مجرمي التقنية ، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب القرصنة الالكترونية ، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي ، يتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة إما تبعا لتخصصهم بنوع معين من الجرائم أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم ، فمثلا نجد طائفة محترفي التجسس الصناعي وهم أولئك الذين يوجهون أنشطتهم إلى اختراق نظم الكمبيوتر العائدة للشركات الصناعية ومشاريع الأعمال بقصد الاستيلاء على الأسرار الصناعية والتجارية ، إما لحساب أعمال يقومون بها بذاتهم أو في الغالب لحساب منافسين آخرين في السوق وأحيانا لحساب مجموعات القرصنة الدولية .

إضافة لذلك فإن أفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى ، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورن معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم وحول الأعمال الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنهم من الشباب أكبر سنا من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين 25 – 40 عام[1]

ثالثا - الحاقدون :

هذه الطائفة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين ، فهم لا يسعون إلى إثبات المقدرة التقنية والمهارية ، وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية ، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم ، أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها ، ولهذا فإنهم ينقسمون إما إلى مستخدمي النظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة ، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم ولا يستمر أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية ، ومع ذلك يشقى الواحد منهم في الوصول الى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه وتغلب على أنشطتهم الالكترونية استخدام تقنيات زراعة الفيروسات والبرامج الضارة

[1]- د . نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الثانية ، دار الثقافة للنشـــر والتوزيـــع ، الأردن ، 2010 ، ص 85 .

وتخريب النظام أو إتلاف كل أو بعض معطيات أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنت ، ليس هناك ضوابط محددة بشأن أعمارهم ، كما أنهم لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة ولا يفاخرون بأنشطتهم ، بل يعمدون إلى إخفائها ، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد في ذلك ، وبالرغم من أن سمات هذه الطائفة تضعها من حيث الخطورة في مؤخرة الطوائف المتقدمة، إذ هم أقل خطورة من غيرهم من مجرمي القرصنة، ولكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن الأنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسسات المستهدفة[1] .

رابعا - طائفة صغار السن :

فئة صغار السن ، أو كما يسميهم البعض (صغار نوابغ الإلكترونية) ، ويصفهم بأنهم " الشباب البالغ المقتدون بالمعلوماتية والحسابات الآلية " ، فإن من بينهم في الحقيقة ، فئة لم تزل دون سن الأهلية مولعين بالحوسبة والاتصال ، وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية ، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح " المتلعثمين " ، الدال حسب تعبير الأستاذ توم فروستر ، على " الصغار المتحمسين للحاسوب ، بشعور من البهجة ، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب " ، ويسميهم البعض كذلك بمجانين بالإسناد الى كثرة استخدامهم لتقنية المعدل والمعدل العكسي ، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم .[*]

ويمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة ، وسمات أفرادها ، ومدى خطورتهم في نطاق ظاهرة القرصنة الالكترونية إلى ثلاثة اتجاهات :

---

[1]- د . عبد الحكيم رشيد توبة ، المرجع السابق ، ص 162 .

[*]من الأمثلة الشهيرة لجرائم التقنية التي ارتكبت من هذه الفئة ، العصابة الشهيرة التي أطلقت عليها عصابة " 414 " ، والتي نسب إليها ارتكاب ستون فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحواسيب ، نجم عنها أضرار كبيرة لحقت بالمنشآت العامة والخاصة ، وكذلك تلاميذ المدرسة الثانوية في ولاية " منهاتن " ، الذين استخدموا في عام " 1980 " طرفيات غرف الدرس للدخول الى الشبكة اتصالات وبيانات العديد من المستخدمين ودمروا ملفات زبائن الشركة الرئيسية في هذه العملية ، كما سبب متعلمو ألمانيا الغربية الصغار في عام 1982 فوضى شاملة عندما دخلوا الى الشبكة الفيديو تكس ونجح بعض المتلعثمون الفرنسيون في إيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي: د.محمد طارق عبد الرؤوف الحن ، جريمة الاحتيال عبر الانترنت ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، لبنان ، 2011 ، ص 188 .

الأول : اتجاه لا يرى إصباغ أية صفة جرمية على هذه الفئة ، أو على الأفعال التي تقوم بها، ولا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب ، استنادا الى أن صغار ة المستهدفة في نشاطهم ولا يستقر أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية السن لديهم ببساطة ميل للمغامرة والتحدي ، والرغبة في الاكتشاف ، ونادرا ما تكون أهدافه ، أفعالهم المحظورة غير شرعية واستنادا الى أنهم لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشآت أو شركة تجارية .

الثاني : الاتجاه الذي يحتفي بهذه الفئة ويناصرها يعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ، ويصفهم بالأخيار ، وأحيانا بالأبطال الشعبيين ، ويتمادى هذا الاتجاه في تقدير هذه الفئة بالمطالبة بمكافئتهم بوصفهم لا يسببون ضررا للنظام ، ولا يقومون بأعمال احتيال ، وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات.

الثالث : اتجاه يرى أن مرتكبي القرصنة من هذه الطائفة يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييزا استنادا إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة ، ودورها أثر على وصف الفعل قانونا من جهة أخرى ، واستنتاجا الى أن خطورة أفعالهم تتميز بانتهاك الأنظمة واختراق الحواسيب وتجاوز إجراءات الأمن والتي تعد بحق من أكثر جرائم الحاسوب تعقيدا من الوجهة التقنية ، عوضا عن مخاطرها المدمرة[1].

خامسا - المجرمون البالغون :

هذه الطائفة وفقا للدراسات المسيحية ينتمون الى فئة عمرية تتراوح بين 25 – 24 عاما ، وبالتالي تمتاز هذه الطائفة بصفات الشباب العمرية والاجتماعية وإذا استثنائيا صغار السن من بينهم الذين تكون أعمارهم دون الحد الأدنى المشار إليه أعلاه ، كما رأينا فيما سلف ، فإن لمجرمي القرصنة إلكترونية سمات عامة ، يتحقق بعضها لدرجة أقل في صغار السن ، وهذه السمات إضافة لما أوردناه في الطوائف المتقدمة تتمثل بما يلي :

[1]- د . محمد طارق عبد الرؤوف الحن، المرجع السابق ، ص 189 .

1 - الصفات الشخصية والتخصص والكفاءة

الجامع بين محترفي القرصنة الالكترونية تمتعهم بقدرة عالية من الذكاء ، وإلمام جدي بالتقنية العالية واكتسابهم معارف علمية وعملية ، وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية ، وهذه السمات مجرمي ذوي الياقات البيضاء ، أما فيما يتعلق بكفاءتهم ، فإن الدراسات القليلة المتوفرة تشير إلى تمتعهم بكفاءة عالية إلى درجة اعتبارهم مستخدمين مثاليين ، من قبل الجهات العاملين لديها ، وممن يسمون بالنشاط الواسع الفاعلة .

2 - من حيث السيكولوجية

إن الدراسات القليلة للجوانب السيكولوجية لمجرمي القرصنة أظهرت شيوع عدم الشعور بلا مشروعية الطبيعية الإجرامية وبلا مشروعية الأفعال التي يقترفونها كذلك لعدم استحقاقهم للعقاب عن هذه الأفعال ، فحددوا الشر والخير متداخلة لدى هذه الفئة، وتغيب في دواخلهم مشاعر الإحساس بالدين ، وهذه المشاعر في الحقيقية تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي الجرائم الالكترونية، من اكتشافهم وافتضاح أمرهم ، لكن هذه الرصدة والخشية يفسرها انتمائهم في الأعم الأغلب إلى فئة اجتماعية متعلمة ومثقفة [1] .

الفرع الثاني: المجني عليه الإلكتروني .

في حين أن من يرتكب جرائم التقنية ومن بينها القرصنة الالكترونية شخص طبيعي ، فإن الضحية هنا يمكن أن يكون شخص طبيعيا أو معنويا ، مع أن الغالبية العظمى من الجرائم تقع على شخص معنوي يتمثل بمؤسسات وقطاعات مالية وشركات ضخمة .

وعلى أساس أن القرصنة الالكترونية تقع في بيئة الحاسب الآلي نفسه في الغالب ، فإن القطاعات المستهدفة هي تلك المعتمدة أكثر من غيرها على أجهزة الحاسب الآلي المختلفة ، وأهم تلك القطاعات البنوك ، في ظل انتشار آلية وتقنية الانترنت أكثر من غيره ، كذلك الإدارات وقطاعات الإنتاج الصناعي[2].

بالإضافة إلى قطاعات المال ، تزداد رقعة الجريمة لتشمل الشركات الخاصة ، كشركات التأمين ، فقد شوهدت لوس أنجلس أشهر الجرائم من هذا النوع عندما تمكن أحد

[1]- د- عبد الحكيم رشيد توبة، المرجع السابق، ص 166.

[2]- د .جلال محمد الزعبي واسامة أحمد المناعسة ،المرجع السابق ، ص 77 .

موظفي شركة تأمين كبرى باستخدام نظامها الحاسوبي ، في خلق عملاء وهميين مؤمن عليهم، وتمكن من بيع (46.000) بوليصة تأمين إلى شركة مناظرة، كما تبرز بشكل ملحوظ جرائم تتعلق بانتهاك حق المؤلف خصوصا في الدول النامية ، كبيع أو عرض برامج الحاسوب مقلدة .

- **دور الضحية في كبح الجريمة :**

في الأغلب الأعم من هذه الجرائم يكون دور الضحية أي المجني عليه ضئيلا وسلبيا إلى حد كبير ، إذ يفضل الكثير من المجني عليهم من إبقاء ما لحقهم من اعتداء سرا خوفا على سمعتهم أو سمعة تجارتهم ، حماية لمركزهم المالي وثقة العملاء بهم ، فلا يرغبون بالكشف عن الاختراقات الحاصلة على أجهزتهم الحاسوبية ونظم المعلومات لديهم حتى لا ينظر إلى تدابير الحماية لديهم على أنها ضعيفة غير فعالة فتسبب ضعف الثقة بالمؤسسة ، وبالتالي عزوف العملاء عنها .

هنا يكون للصدفة فقط دور في كشف الجرائم وملاحقتها ، وهذا الكلام صحيح إلى حد بعيد في بلادنا ، أما في البلاد الغربية فالوعي أكبر ولا يخشى أصحاب المؤسسات التي تم اختراقها الإعلان عن ذلك ، بغية تحصيل حقوقهم ، ومعاقبة المجرمين ، وهو أمر يعود بالفائدة على الأجهزة القضائية ، ومجموع المعتدى عليهم على حد سواء ، فيما يتعلق بزيادة الخبرة وتحديد أطر الجريمة ، وبالتالي وضع أفضل الحلول لمكافحتها مستقبلا .

ومن هنا يمكن القول أن ردة فعل السيئة للمجني عليهم خير معين لمرتكبي الأفعال، ولعل الشيء الذي يبعث على القلق حقيقة إزاء سلبية هؤلاء الضحايا هو إسرارهم على إخفاء الجرائم التي وقعوا ضحية لها [1] .

[1]- د . جلال محمد الزعبي و د.اسامة أحمد المناعسة ، المرجع السابق ، ص 78 .

المطلب الثاني : المعلومات الالكترونية المستهدفة

المعلوم أن هناك معايير متعددة تصنف الجرائم على أساسها، ومن هذه المعايير، المعيار الذي يعتمد في إسباغ الوصف على طائفة من الجرائم وانتسابها إلى تلك الطائفة دون غيرها، هو المحل الذي يقع عليه الاعتداء، فتأخذ مجموعة من الجرائم وصفها لاشتراكها في عنصر واحد يجمع بينها، هو محل الاعتداء ، ولا يكفي أن يكون محل تجريم من قبل المشرع استنادا إلى مقتضيات مبدأ الشرعية، إنما يشترط إلى جانب ذلك أن ينصب الاعتداء على إحدى مكونات الكيان المعنوي للنظام الالكتروني،والتي تتمثل في البرامج والمعلومات سواء المخزنة منها في الحاسب الآلي، أو المرسلة، أو المنقولة عن طريقه، والتي تم السيطرة عليها بوجه غير مشروع [1] ، وأكثر الأساليب انتشارا في مجال الاعتداء على المعلومات هي القرصنة الالكترونية إذ ينتج من خلالها خسائر كبيرة جدا، وبناء علي ما سبق سنتناول ابتداء في الفرع الأول ماهية المعلومات ومدى انطباق وصف الأموال عليها في الفرع الثاني، وسنبرز من الفرع الثالث المعلومات المستهدفة من قبل القرصنة الالكترونية.

الفرع الأول: ماهية المعلومات

الحديث حول ماهية المعلومات يتطلب الإشارة أولا إلى تعريف المعلومات، ثم بيان الشروط الواجب توافرها في المعلومات حتى تتمتع بالحماية القانونية.

أولا: تعريف المعلومات

من الناحية العملية فالواقع العملي لا يقدم تعريفا للمعلومات ولكن هناك جهودا قد بذلت وهدف هذه الجهود هو الاعتراف لبعض المعلومات التي يمكن حمايتها عن طريق حق الملكية الذهنية بطابع القابلية للتملك [2] ،وقد تعددت التعريفات بشأن المعلومات ، فقد عرفها الأستاذ باركر بأنها" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل أو الاتصال، أو الأنظمة الالكترونية، وهي تتميز بالمرونة حيث يمكن تغييرها وتجزئتها ومعها أو نقلها بوسائل وأشكال مختلفة".

[1]- د . سامي علي حامد عياد ، المرجع السابق ، ص 230 .
[2]- د .نهلا عبد القادر المومني ، المرجع السابق ، ص 99 .

وتعرف البيانات أنها" المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما" وتسمى العلاقة بين المعلومات والبيانات بالدورة الاسترجاعية للمعلومات، إذ يتم تجميع وتشغيل البيانات والحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة، [1] ،وبصفة عامة تتميز المعلومات أو البرامج بقابليتها للدمج فقد تضاف معلومة إلى معلومة أخرى لتكونا معا معلومة جديدة تختلف في قيمتها وأهميتها عما كانت عليه قبل الدمج.[2]

ثانيا_ الشروط الواجب توافرها في المعلومات

هناك شروط لا بد أن تتوافر في المعلومة بصفة عامة حتى يمكن أن تتمتع بالحماية القانونية وتتجلى هذه الشروط فيما يلي:

1- أن يتوافر في المعلومة التحديد والابتكار: إن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقة، فالمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون محددة، [3] ,أما فيما يتعلق بالابتكار فانه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة، فمعلومة غير مبتكرة هي معلومة عامة شائعة ومتاحة للجميع ويمكن للجميع الوصول إليها ولا يمكن نسبتها إلى شخص محدد[4] ..

2 - أن يتوافر في المعلومة السرية والاستئثار

كلما اتسمت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومة محددا بمجموعة معينة من الأشخاص ودون هذا التحديد لا يمكن أن تكون المعلومة محلا يعتدي عليه، فالمعلومة غير السرية تكون صالحة للتداول ومن ثم تكون بمنأى عن أي حيازة، وتعد خاصية الاستئثار بالمعلومة أمرا ضروريا لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، وتتوافر

---

[1]- د . سامي علي حامد عياد ، المرجع السابق ، ص 24 .

[2]- على سبيل المثال رقم حساب العميل في البنك معلومة على قدر من الأهمية إلا أنه إذا أضفت إلى هذه المعلومة معلومة أخرى كاسم البنك واسم العميل وحجم الرصيد فإن قيمة المعلومة وأهميتها في هذه الحالة تتضاعف وتتطلب قدرا أكبر من الحماية ، ولهذا السبب تقوم البنوك بإرسال كل معلومة منفردة عن طريق عمليات اتصال مختلفة فهي على سبيل المثال تقوم بإرسال مجموعة كبيرة من أرقام الحسابات عن طريق عملية اتصال وتقوم بإرسال قيمة الأرصدة عن طريق عملية اتصال أخرى ويتم تجميع المعلومات المختلفة في مركز لمعالجتها وذلك بهدف الحفاظ على سرية هذه المعلومات ، أنظر د / نهلا عبد القادر المومني ، المرجع السابق ، ص 103.

[3]- د . خثير مسعود ، الحماية الخبائية لبرامج الكمبيوتر ، دار الهدى ، الجزائر ، 2010 ، ص 16 .

[4]- د .خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية ، الإسكندرية ، 2008 ، ص 31 .

للمعلومة صفة الاستئثار إذا كان الوصول إليها غير مصرح بها لأشخاص محددين ويمكن أن ينبع الانتشار من سلطة شخص أو جهة ما على المعلومة وعلى التصرف فيها[1] .

الفرع الثاني: الطبيعة القانونية للمعلومة

من المسلم به أن الشق المادي للنظام ألمعلوماتي والمتمثل في جهاز الحاسوب والمعدات الملحقة به والدعامات، التي يخزن عليها المعلومات والكابلات وغير ذلك، هي مال مادي منقول له كيان خارجي ملموس، وبالتالي فان جريمة السرقة المنصوص عليها في قانون العقوبات يمكن أن تقع على هذا الجانب من مكونات النظام الالكتروني، أما فيما يتعلق بالشق المعنوي للنظام ألمعلوماتي والمتمثل في المعلومات والبيانات والبرامج وغير ذلك فان التساؤل يقول في ما إذا كان بالإمكان انطباق وصف الأموال عليها بالرغم من طبيعتها المعنوية.

ابتداء نشير إلى أن الاتجاه الذي كان سائدا في تحديد مدى انطباق وصف المال على الأشياء كان يعتمد على صفة المادية في الأشياء لاعتبارها مالا ، وبالتالي فالأشياء المعنوية لا تتمتع من وجهة نظرهم بصفة المال، فقد كان ينظر إليها باعتبارها إما عديمة القيمة أو ذات قيمة منخفضة، الا أن التطورات الحديثة والمستمرة في مجال تكنولوجيا المعلومات أدت إلى ارتفاع قيمة المعلومات عن قيمة الأموال المادية ، وخاصة عند التفاعل الذي تم بين العملاقين وهما : علم المعلوماتية وعلم الاتصالات ، حيث أصبحت المعلومات تنساب بسهولة ويسر بين الأفراد ، وأصبحت تشكل قوة حقيقية لمن يمتلكها ، وهذه التطورات أدت بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال ، حيث تم اللجوء إلى معيار آخر ألا وهو معيار القيمة الاقتصادية للشيء ، ووفقا لهذا الاتجاه يمكن إسباغ صفة المال على المكونات المعنوية للنظام الالكتروني على أساس ما تتمتع به من قيمة اقتصادية وعليه فإن المعلومات تعتبر من قبيل الأموال المعنوية التي يمكن الانتفاع بها واستغلالها ، وكذلك يمكن حيازتها معنويا[2] .

[1] - د .نهلا عبد القادر المومني ، المرجع السابق ، ص 104 .

[2] - د.نهلا عبد القادر المومني ، الجرائم المعلوماتية ، المرجع السابق ، ص 107

الفرع الثالث : المعلومات المستهدفة .

من الواضح أن الانتشار الواسع لاستعمال الكمبيوتر والانترنت في جميع قطاعات الدولة سيعرض هذه الأخيرة بالتأكيد إلى ظاهرة القرصنة الالكترونية ، وقد أكدت هذا بالفعل الإحصاءات في هذا المجال إذ أن هذه الظاهرة تمس نسبة عالية للبنوك ، أو ما يقدر بنسبة 19 % وتأتي الإدارة بنسبة 16 % والإنتاج الصناعي 10 %، وإن الشيء الآخر أيضا يؤكد أن ظاهرة القرصنة الالكترونية تمس الجزء الأعظم بالنسبة للمعلومات الآتية :

أولا : المعلومات العسكرية

الخطط والتدابير العسكرية وأسرار الدولة الحربية والمشروعات النووية وصناعة الأسلحة، كل هذه المعلومات التي تتعلق بالجانب الأمني والاستراتيجي للبلاد التي تعتبر أكثر المعلومات حساسية وسرية في أي دولة التي كانت توضع سابقا في عشرات المجلدات، ويمكن في الوقت الحاضر في ظل الثورة الالكترونية تم تخزينها في ذاكرة الحاسوب ومعالجتها آليا أو وضعها على قرص مغناطيسي سهل الحمل أو تحميلها على مواقع خاصة على شبكة الانترنت ، ويمكن في ظل هذا الوضع للمخترقين أن يقوموا باستخدام الوسائل التقنية خلال فترة زمنية قصيرة من أي مكان في العالم بالوصول إلى هذه المعلومات بل قد يصل الأمر إلى حد تدمير هذه المعلومات العسكرية ومحوها ، الأمر الذي يشكل خطرا على الأمن القومي لأي دولة .[*]

---

[*] ومن أهم الحالات التي تم اكتشافها والتي ترتبط فيها القرصنة الالكترونية بالمصالح العليا للدولة ، تلك الحالة التي تتخلص وقائعها ، بقيام ثلاثة طلبة ألمان بالعمل لحساب المخابرات السوفيتية حيث قاموا بمدها بالشفرات الخاصة بأنظمة حسابات غاية في الأهمية ، ومنها نظام الحاسوب الخاص بوزارة الدفاع الأمريكية ، " البنتاجون "، ومعمل الأبحاث في " لولا موس" وإحدى = =الشركات الفرنسية ومعاهد علمية متفرقة في أوروبا وأمريكا الشمالية واليابان ، وتمكن الجناة في هذه الواقعة من الدخول إلى أنظمة الحاسبات السالفة الذكر ، عبر شبكات المعلومات وتمكنوا من استغلال بعض الثغرات التي تعتري الإجراءات الأمنية لهذه الأنظمة للحصول على الشيفرات الخاصة بها ، ولقد تم اكتشاف الجناة بالصدفة ، استغرقت عملية تتبعهم عاما كاملا قدموا بعده للمحاكمة أمام القضاء الألماني وكان ذلك في عام 1989 ، د – نهلا عبد القادر المومني ، المرجع السابق ، ص 212 .

ثانيا – المعلومات المالية

وهي التي تستهدف المركز الحسابي والإداري والتنقلات الأموال والاستثمارات وفي المنشآت العامة أو الخاصة[1] ، وإن ما حدث في كولومبيا وفرنسا عام 1983 يمثل ولو بشكل واقعي وليس إنفرادي يمكن المتسللين بالمساس أو التجسس على المعلومات المالية ، فقد تمكن مستخدم بالحكومة الكولومبية من اختلاس ليس أقل من 13.5 مليون دولار أمريكي، حيث كان هذا الأخير يتلاعب بحسابات الحكومة ويحول منها مبالغ لحسابه الخاص، وهذا من خلال جملة تنقلات هذه الأموال عبر العالم في مختلف البنوك ، أما تمكن مسؤول الخدمة الخارجية في فرنسا من اختلاس مبلغ مالي قدر بـــ 7 ملايين فرنك فرنسي بعد أن اكتشف زميل له أنه كان يتلاعب بالحسابات ينقل منها مبالغ خيالية لحسابه الخاص[22].

ثالثا – المعلومات الاقتصادية

يقول القاضي الفرنسي " Louis joinet " : إن المعلومات قوة اقتصادية والقدرة على تخزين أنواع معينة من البيانات ومعالجتها ، يمكن أن يعطي بلدا مميزات أساسية وتكنولوجية على البلدان الأخرى ، كما أن التوصية الصادرة عن المجلس الأوروبي الخاصة بجرائم الحاسوب قد عرفت المعلومات الصناعية والتجارية السرية أنها : " مجموعة من الحقائق لها قيمة معلوماتية ولها صلة بشخص أو بمؤسسة وتتميز هذه الحقائق بكونها سرية، أي غير معلومة للجميع، وأن الدخول إلى الأنظمة التي تحتوي عليها مقصور على دائرة محددة من الأشخاص ، وتظل هذه السرية رهنا بإرادة الشخص المسؤول عن المؤسسة ".

وعليه فالقرصنة الالكترونية **في النطاق التجاري**، تسعى للحصول على الأسرار التسويقية والحسابات المالية للمؤسسة المستهدفة ، وكذلك معرفة المعلومات الكافية حول حساب التكلفة وكشف الميزانية وحالة الأسواق والعناوين الخاصة بالعملاء .

أما فيما يتعلق بالقرصنة الالكترونية **في النطاق الصناعي** فيهدف إلى الكشف عن أسرار الإنتاج للصناعات المختلفة بما في ذلك معرفة خطوات الإنتاج وكذلك التوصل إلى الأبحاث العلمية التي تجري لتطوير الصناعات المختلفة,والحاجة إلى توفير سنوات عديدة من

[1] - د – سامي علي حامد عياد ، المرجع السابق ، ص 61

[2] ـــ د .نهلا عبد القادر المومني ، المرجع السابق ، ص 107 .

البحث العلمي الشاق وتجنبا لاستثمار ملايين الدولارات في هذه العمليات ، قد تدفع المؤسسات المختلفة بل حتى الدول إلى اللجوء للقرصنة الالكترونية وذلك من أجل التجسس لغرض الحصول على الأسرار الصناعية دون تحمل الأعباء المادية ويبدو ذلك بشكل واضح في مجال صناعة برامج الحاسوب ، حيث أن صناعة هذه البرامج عادة ما تكلف مبالغ باهظة , وقد كان ذلك سببا وراء لجوء الكثير من الشركات للقرصنة وذلك للحصول على المعلومة الخاصة بإنتاج هذه البرامج ، إما لإنتاج برامج مماثلة وتسويقها ، أو لزيادة الخبرة في هذا المجال ، أو لمجرد التعرف على ما توصلت إليه شركة منافسة[1] .

رابعا – البيانات الشخصية والاجتماعية:

بعد انتهاء جمع المعلومات السكانية والمعلومات المتعلقة بالوضع الاجتماعي للسكان من حيث ديانتهم، وأصولهم ومستوى المعيشة الخاص بهم ، وغير ذلك من المعلومات والتي تبني عليها الدولة خططها التنموية والاقتصادية ، يتم عادة في معظم الدول تخزينها في ذاكرة الحاسوب على مواقع خاصة تابعة للدولة التي تتعلق هذه البيانات بسكانها،إلا أن هذه البيانات والمعلومات قد يتم إساءة استعمالها من قبل جهات داخل الدولة والأغراض الخاصة بها ، أو من قبل جهات خارجية أي من قبل دولة معادية ، تهدف لمعرفة الجوانب المختلفة لدولة ما لتحقيق أهداف خاصة بها .[*]

المطلب الثالث : أسلحة القرصنة الالكترونية

إن ذاتية القرصنة الالكترونية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها، وذلك لتحقيق مختلف أهداف مجرمي القرصنة الالكترونية والذين يلجئون إلى عدة أساليب وأدوات تمكنهم من تحقيق غاياتهم، وإذ لا يمكن حصر الآليات والأساليب التي يستخدمها أو يستعين بها مجرموا القرصنة الالكترونية في تنفيذ اعتداءاتهم الجريمة المختلفة، وذل بسبب عدم وجود نموذج موحد للنشاط الجرمي من جهة، والى عدم إمكانية التنبؤ بالوسائل التي قد تستخدمها التكنولوجيا في هذا الشأن، ورغم تعدد هذه التقنيات الالكترونية المستخدمة في

---

[1]- د . نهلا عبد القادر المومني ، المرجع السابق ، ص 214 .

[*] ومن الأمثلة على القرصنة الالكترونية على هذا النوع من البيانات:قيام موظفين من العاملين بمركز حاسوب في السويد ، بنسخ برامج مسجل عليها إحصاءات وبيانات سكانية ، حيث قاما ببيعها بعد ذلك إلى أحد المكاتب الخاصة بالإحصاءات والبيانات لأغراض استهلاكية مقابل ثمن رخيص، د – نهلا عبد القادر المومني ، الجرائم المعلوماتية ، المرجع السابق ، ص 216 .

تدمير النظم الالكترونية، فإننا سنحاول التعرض الى أهم هذه التقنيات الأكثر خطورة والأكثر استعمالا من قبل المجرم الالكتروني، ويتعين علينا، أن نتعرض بشيء من التفصيل لهذه الأساليب في ثلاثة فروع: الأول" عن الفيروسات الالكترونية"، الثاني "عن برامج الدودة الالكترونية، الثالثة " عن القنابل الالكترونية".

الفرع الأول: الفيروسات الالكترونية

الفيروس المعني في هذا المجال ليس ذلك المعتمد في المجال الطبي، وان كانت التسمية واحدة، وقد تكون النتائج أيضا متشابهة، بحيث إذا كان الفيروس في جسم الإنسان قد يؤدي إلى مشكلة وعدم قدرته على الاستمرار ، فان الفيروس في القرصنة الالكترونية هو عبارة عن جزء ضار يضاف إلى برنامج الكمبيوتر، ويطلب منه إزالة المعلومات الموجودة على الديسك أو مسحها، أو إتلافها ، أو خلط المعلومات ، فلا يمكن معها بالتالي استعمال البيانات والمعلومات[1] .

أولا_ تعريف الفيروس

في الواقع العملي لا يوجد تعريفا موحدا للفيروسات، فقد تعددت التعريفات في هذا الشأن، فقد عرفه الأستاذ الدكتور "محمد سامي الشوا" بأنه:" عبارة عن خلية كحق ومغناطيسية نائمة ومبرمجة تنشط في وقت محدد لتخريب البرنامج الأصلي، ومنتشرة في الأجهزة التي تضمنها الشبكة بحيث تفسره ما تحويه من معلومات [2] .

فالفيروسات عبارة عن برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر ، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنه ينتقل عبر الحدود من أي مكان إلى آخر في العالم ، وهو يسمى عادة باسم أول مكان اكتشف فيه[3] .

ثانيا_ خصائص الفيروسات

_ يتولى إعداد هذه الفيروسات فئة مريضة من خبراء البرامج ، كما يشير الاتهام في بعض الأحيان إلى بعض الشركات الكبرى المتخصصة في مجال إنتاج البرامج .

_ خاصية التخزين في البرامج، فمن المعروف إن صناعة البرامج تمر بعدة مراحل، وتطبيقيا كذلك ففي مرحلة الإنتاج مثلا قد يحدث فيرسة البرنامج، لأن هذه المرحلة يتم فيها

[1]- د . محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر، الاسكندرية، 2004 ، ص 84 .
[2]- د . نهلا عبد القادر المومني ، المرجع السابق ، ص 126 .
[3]- د. نسرين عبد الحميد، الجرائم الاقتصادية، المكتب الجامعي الحجيث، القاهرة، 2009، ص 346.

العديد من الاختيارات للبرنامج للتأكد من خلوه من الأخطاء ، وهنا في هذه المرحلة قد يوجد بينهم من يضمر الشر لهذا النظام عن طريق فيرسته.

_ خاصية القدرة على الاختفاء، فيختفي الفيروس نفسه عن المستخدم ولا يترك أي أثار دالة على وجوده، فالبرامج التي تحمله تضل تعمل بكفاءة مدة طويلة في نفس الوقت الذي يقوم فيه الفيروس بالانتقال من برنامج إلى آخر بسرعة كبيرة، ولا يشعر المستخدم به الا بعد أن يؤدي وظيفته التدميرية، ويتوقف النظام ألمعلوماتي عن العمل[1].

وكان أول من فكر في فيروس الحاسوب هو " جون نيومان" عام 1949 عندما طرح الفكرة الأساسية في تصميم الفيروس الالكتروني في مقال نشر له تحت عنوان" نظرية التعقيد الأوتوماتيكي ومفاده أن جهاز الحاسوب يمكن أن يدمر نفسه، ولم يلق هذا المقال في حينه أهمية لقلة انتشار الحواسيب[2]، ويستخدم الفيروس بشكل عام لتحقيق أحد غرضين:

أ_ الغرض الحمائي:

ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به، فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه، ويعد ذلك بمثابة عقوبة تلحق بالناسخ.

ب_ الغرض التخريبي

يتم إعداد هذه الفيروسات من قبل فئة مريضة من خبراء البرامج وذلك بهدف الدعاية أو الابتزاز ، فيرمي صانع الفيروس إلى التخريب بهدف الحصول على منافع شخصية[3] .

ثالثا_ أنواع الفيروسات

إن أنواع الفيروسات لا يمكن حصرها كون أنها أخذت بالتزايد بشكل متصارع ويعود السبب في ذلك إلى وجود الشبكة العالمية بشكل للمعلومات" الانترنيت"، فقبل هذا الاستعمال المذهل لشبكة الانترنيت كان انتشار الفيروسات في جميع أنحاء العالم يستغرق عامين إلى خمسة أعوام، إما ألان فيستغرق الأمر ساعات محدودة، ومن أشهر واهم هذه الفيروسات:

[1]- د . محمد طارق عبد الرؤوف الحن ، المرجع السابق، ص 188 .
[2]- د . نهلا عبد القادر المومني ، المرجع السابق ، ص 127 .
[3]- د . محمد علي العريان ، المرجع السابق ، ص 90 .

أ_ فيروس مايكل أنجلو

أطلق هذا الفيروس يوم 06مارس عام بمناسبة الاحتفال بذكرى ميلاد الرسام الايطالي الشهير مايكل أنجلو وأصاب هذا الفيروس العديد من أجهزة الحاسوب الشخصية في عدد كبير من دول العالم [1] .

ب - فيروس ناسا:

وهو فيروس أطلق احتجاجا على إنتاج الأسلحة النووية فهو عبارة عن برنامج يحمل رسالة مناهضة للأسلحة النووية وتظل هذه الرسالة تكرر نفسها وتتكاثر بشكل مدمر للبرامج الأخرى ، وكان الهدف منه محاولة اختراق شبكة الحاسب الآلي التابعة لوكالة الفضاء الأمريكية " ناسا ".

ويوجد هناك مصادر متعددة أو محتملة للفيروسات على اختلاف أنواعها ، فقد يكون مصدر هذه الفيروسات :

- الموظفون القائمون على تصميم البرامج أو تشغيلها حيث يقوم هؤلاء الموظفون بصنع فيروسات بهدف الانتقام من المؤسسة التي يعملون بها أو لمجرد إثبات المهارة.
- الجاسوسية العسكرية والصناعية فقد تقوم أجهزة المخابرات في بعض الدول أو الشركات الصناعية بإدخال فيروس إلى البرنامج المراد التجسس عليه ، وذلك للحصول على معلومات صناعية أو عسكرية .
- الإرهاب ، فقد تقوم الجماعات الإرهابية المنظمة باستخدام نظم الاتصالات الحديثة في تنفيذ مخططاتها الإرهابية عن بعد ، فتقوم بصنع فيروسات يهدف تخريب وإتلاف الأهداف التي تعتقد أنها تقف ضد مبادئها ومعتقداتها .
- كذلك فإن قراصنة الحاسوب قد يكون لهم دور في انتشار هذه الفيروسات وكذلك المتنافسين في مجال صناعة الحواسيب وغير هؤلاء ممن لهم مصلحة في انتشار هذه الفيروسات وتدميرها لنظم المعلومات المختلفة [2].

[1]- د . محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 188 .

[2]- د. محمد علي العريان، المرجع السابق، ص 93.

ج – فيروس حصان طروادة Tarjan Horse:

وهو عبارة عن برنامج يتمتع بقدرته الفائقة على الاختفاء داخل البرنامج الأصلي ليعمل أثناء التشغيل ، بحيث يؤدي إلى تعديل البرنامج أو تغييره ومحو المعلومات وتدميرها[1] .

د – فيروس الحب I love you :

ظهر هذا الفيروس في جميع أنحاء العالم وبصفة خاصة في الولايات المتحدة الأمريكية وتقدر خسائر أمريكا منه نحو عشرة مليارات دولار ، وقد اقتحم أنظمة الكمبيوتر العسكرية في وكالة الأمن القومي ، وقد انتشر هذا الفيروس عن طريق فتح البريد الالكتروني للمستخدم User تحت عنوان " Love " ثم لا يلبث أن نفتحه حتى ينشر في أنحاء الحاسب الآلي [2] .

الفرع الثاني : برامج الدودة الالكترونية (Worm Software) .

تعد هذه البرامج من أكثر البرامج المصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر، وهو ما يؤدي إلى عجز النظام إلكتروني عن أداء عمله عن طريق محو عدة أجزاء من المعلومات .

أولا : تعريف برامج الدودة

وهي عبارة عن برامج تستغل أية فجوة في نظم التشغيل ، كي تنتقل من حاسب آلي إلى آخر، ومن شبكة إلى أخرى عبر الوصلات التي تربط بينهما ، وتتكاثر أثناء عملية انتقالها كالبكتيريا بإنتاج نسخ منها[3]، والدودة الالكترونية تنتشر أساسا عبر خطوط التوصيلة الالكترونية وتصدر معلومات غير صحيحة وتؤدي في النهاية إلى إغلاق النظام[4] .

ثانيا : آلية عمل الديدان .

تختلف الديدان في طريقة عملها من نوع إلى آخر فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة بينما بعضها يتخصص في البريد الالكتروني بحيث يقوم بإرسال نفسها في

---

[1] د-.عبد الفتاح البيومي الحجازي، الجرائم المستحدثة، الطبعة الاولى، منشأة المعارف، الإسكندرية، 2008، ص 492.

[2] - د .محمود أحمد عبابنة ، جرائم الحاسوب ، وأبعادها الدولية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيـــع ، الأردن ، 2009 ، ص 102 .

[3] - د . محمود أحمد عبابنة ، المرجع السابق ، ص 103 .

[4] -د. عبد الفتاح البيومي حجازي، الجريمة في عصر العولمة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 148.

رسائل إلى جميع من توجد عناوينهم في دفتر العناوين الموجودة بالجهاز باسم مالك البريد مما يوقعه في حرج بالغ مع من تم إرسال تلك الرسائل إليهم ، وتكمن خطورة الديدان في استقلاليتها ، وعدم اعتمادها على أي برامج أخرى تلتحق بها ، مما يعطيها حرية كاملة في الانتشار السريع ، ومما لا شك فيه أنه توجد أنواع منها في غاية الخطورة ،[1]وفي الواقع العملي، هناك العديد من الأمثلة على حدوث مثل هذه الديدان الالكترونية. [*]

الفرع الثالث : القنابل الالكترونية

القنابل الالكترونية ، أو المعلوماتية وهو اصطلاح يطلق على أنواع من البرامج الالكترونية ، والتي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف .

أولا : تعريف القنابل الالكترونية

وهي عبارة عن برنامج يعده مصمم النظام الالكتروني ويثبته بداخله بغية أن يعمل بعد انقضاء مدة محددة على استعمال النظام الالكتروني ، بهدف تدميره ، أو تعطيله أو محو البيانات التي يحتويها .

ثانيا : أنواع القنابل الالكترونية

1 – القنابل المنطقية : " Logicbonb "

ويمكن القول أنها : " عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة، أو في كل فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع[2] .

والقنابل المنطقية تظل في حالة سكون ، ولا يتم اكتشافها مدة من الزمن ، قد تطول أو تقصر وهذه المدة يحددها المؤشر الموجود داخل برنامج القنبلة ، و هناك العديد من

---

[1]- د .منير محمد الجنبهي ود – ممدوح محمد الجنبهي ، المرجع السابق ، ص 82.

[*] - ومن أشهر القضايا الالكترونية ، التي استعملت فيها تقنية برامج الدودة ، قضية موريس ، حيث في تشرين الثاني عام 1988 تمكن طالب يبلغ من العمر 23 عاما ويدعى " Robermorris " ، من إطلاق دودة موروس عبر الانترنت ، أدت إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 20000 نظام عبر الانترنت ، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية ، ومنها الأنظمة الالكترونية: د – أمير فرج يوسف ،المرجع السابق ، ص 367 .

[2]- د. نسرين عبد الحميد نبيه ، المرجع السابق ، ص 157 .

الأمثلة الواقعية على وضع قنابل منطقية في النظام الالكتروني ، من أجل تدمير الملفات وإتلافها.*

2- القنبلة الزمنية أو الموقوتة Time Bomb

وهي عبارة عن برامج يتم إدخالها بطرق مشروعة متخفية مع برامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام وتغييرها، وهي تعمل في وقت محدد وفي يوم معين [1] .

استخدام القنابل الزمنية(الموقوتة) يحقق أهدافا متعددة لمعديها، فيمكن من خلال هذه القنابل توقيت القيام بعملية التخريب في وقت معين يلحق أكبر ضرر ممكن بنظام الحاسوب، كما يمكن التأجيل في التفجير يتيح انتقال القنبلة للنسخ الاحتياطية للبرامج التي تقوم الجهة المستهدفة بإعادة إنتاجها*.

* - قيام أحد المبرمجين في ولاية تكساس الأمريكية سنة 1985 بوضع قنبلة منطقية في حاسوب الشركة التي كان يعمل بها بعد فصله منها مستغلا عدم تغيير الشركة لكلمة السر التي كان يعرفها ، مما أدى إلى تدمير سجلات عمولة المبيعات مرة كل شهر، تمكن خبير في نظم المعلومات في الدنمارك من وضع قنبلة منطقية في نظام أحد الحواسيب أدت إلى محو أكثر من مائة برنامج، وقد تقدم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال أثر القنبلة إليها، وقد تم ضبط المجرم وحكم عليه القضاء الدنمركي بالسجن لمدة تسعة أشهر: د.نهلا عبد القادر المومني ، المرجع السابق ، ص 133 .

[1]- د .أمير فرج يوسف ، المرجع السابق ، ص 292 .

* - ومن الأمثلة على استخدام القنبلة الزمنية في الواقع العملي من أجل تدمير المعلومات وإتلافها:

قيام أحد المبرمجين الفرنسيين بوضع قنبلة موقوتة في شبكة المعلومات في الجهة التي كان يعمل بها اثر فصله من العمل، وهذه القنبلة كانت تتضمن أمرا بتفجيرها بعد ستة أشهر من تاريخ فصله، الأمر الذي نتج عنه تدمير كل بيانات هذه الجهة د .نهلا عبد القادر المومني ، المرجع نفسه ، ص 134 .

المبحث الثالث : الإثبات الجنائي في بيئة القرصنة الإلكترونية

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا ، فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد عنها ، أفرز إلى حيز الوجود نوعا جديدا من الأدلة يتماشى مع طبيعة القرصنة الإلكترونية،وهو ما يعرف بالدليل الإلكتروني أو الرقمي، فإثبات هذه الجريمة،تحتاج إلى طرق تقنية تتناسب مع طبيعتها،بحيث يمكن ترجمة هذه النبضات والذبذبات الإلكترونية إلى أدلة إثبات أو نفي على ارتكاب القرصنة الإلكترونية، وبناءا على تسلسل هذه الأفكار ، سنقسم هذا المبحث إلى ثلاثة مطالب كالآتي :

- **المطلب الأول : الصعوبات المعيقة لإثبات القرصنة الإلكترونية .**
- **المطلب الثاني: الدليل الإلكتروني.**
- **المطلب الثالث : حجية الدليل الإلكتروني**

المطلب الأول : الصعوبات المعيقة لإثبات القرصنة الإلكترونية

إن القرصنة الإلكترونية هي من إحدى الجرائم التي تتخطى آثارها حدود الدول بل والقارات في الكثير من الأحيان ، مما يعد ذلك عائقا أما إثبات هذه الجريمة ، لتعقب المجرمين ، وتقديمهم للمحاكمة ، فبات الوصول للمجرم الإلكتروني الرقمي يشكل عبء ثقيلا على الأجهزة القائمة بأعمال التتبع والتحليل الإلكتروني لملابسات الوقائع المختلفة ، وعليه فإن هناك من الصعوبات والتحديات ما يقف حائلا دون تحقيق النتائج المرجوة منه على أكمل وجه ، من إن أهم المشكلات التي تقف عائقا أمام إثبات الجرائم الإلكترونية والتي من ضمنها القرصنة الإلكترونية، أنها من الجرائم التي تختلف كليا عن المسرح التقليدي الذي ترتكب فيه الجريمة، حيث يتم الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية والتي هي صيغت لإثبات جرائم ترتكب في عالم ملموس ماديا [1]، إذ في المقابل يستحل الكشف عن وقوع قرصنة إلكترونية بتلك الوسائل كون أنها تقوم على نبضات إلكترونية غير مرئية،لا يمكن قراءتها إلا بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل والتي

[1]- لمزيد من التفاصيل أنظر: حفيظة خمايسية ،"التعاون الدولي في مكافحة جرائم الأنترنت "،(مذكرة لنيل شهادة الماجستير – فرع القانون الجنائي الدولي - ، كلية الحقوق و العلوم السياسية ، جامعة تبسة، 2011ـــــ2012) , ص 155.

يمكن في أقل من الثانية محوها ، ومما يزيد الصعوبة في إثباتها أنه يصعب اكتشافها ، وإذا اكتشفت يصعب ملاحقتها وضبطها ، ومرتكبوها يتسمون بالدهاء والذكاء والسرعة الفائقة في القدرة على إتلاف أو تشويه و إضاعة الدليل في فترة قصيرة، بالإضافة إلى ذلك أن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب على ذلك من دعاية[1] .

المطلب الثاني : ماهية الدليل الإلكتروني

يتطلب منا البحث في ماهية الدليل الإلكتروني التعرض لتعريفه،ثم التعرض إلى تحديد مصادره الإلكترونية.

الفرع الأول : تعريف الدليل الإلكتروني

هناك عدة تعريفات للدليل الإلكتروني أو ما يصطلح عليه بالدليل الرقمي ، نذكر منها:هو"أية بيانات مخزنة أو منقولة بواسطة الحاسوب تدعم أو تدحض أية نظرية حول كيفية ارتكاب الجريمة ، وتتعلق بعناصر هامة في الجريمة " .

أما مجموعة العمل العلمية حول الدليل الإلكتروني SWGDE فقد عرفته بأنه : " أية معلومات ذات قيمة مخزنة أو منقولة بشكل إلكتروني" .

ويمكن تعريف الدليل الإلكتروني بأنه المعلومات أو البيانات الإلكترونية المخزنة في الحاسوب أو المنقولة بواسطته والتي يمكن استخدامها في إثبات أو نفي جريمة ما .

الفرع الثاني : مصادر الدليل الإلكتروني

يمكن الوصول إلى الدليل الإلكتروني المتعلق بالقرصنة الإلكترونية عن طريق البحث في المصدرين التاليين :

أولا : أنظمة الحاسوب وملحقاتها .

تعد الحواسيب مصدرا غنيا بالأدلة الإلكترونية، وخاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة لسلوكية الأفراد،فالملفات الشخصية أو ملفات النظام وغيرها من أنواع الملفات،التي تكون مخزنة عادة في الأقراص الصلبة أو الأقراص الليزرية CD ، الذاكر المعروفة بFlash Memory كثيرا ما تحتوي على معلومات تتعلق بالجريمة ، وتفيد في

[1]- د .علي جبار الحيسناوي ، المرجع السابق ، ص 136 .

عملية التحقيق، وعملية حجز الحاسوب أو ضبطه يقصد تفحصه ، تعد نقطة البداية في الكشف عن خفايا القرصنة الإلكترونية .

ثانيا: أنظمة الاتصال بالانترنت

تشمل عملية فحص أنظمة الاتصال بالانترنت فحص حركة التنزيل والتحميل ودرجة الاستيعاب ، ولعل أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالانترنت هي مسألة تحديد مكان الجريمة، أو الحاسوب الذي ارتكب بواسطته النشاط الجرمي ، حيث يمكن معرفة هذا الحاسوب طريق تتبع الحركة العكسية لمسار الانترنت ، ويستخدم في عملية التتبع هذه نظام فحص إلكتروني يطلق عليه " علم البصمات المعاصر ، أو علم بصمات القرن الواحد والعشرين" ، وهو منهج تم استخدامه في العديد من الجرائم ، مثل تتبع مبتكر فيروس "ميليسا" وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات " بلومبرج " لأخبار المال وهو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع،ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الانترنت ، هو عنوان رقمي أو إلكتروني فقط IP-adress وهذا الدليل الإلكتروني لا يكفي لنسبة الجريمة إلى مالك الحاسوب ، إذ من الممكن أن لا يكون هو مرتكب الجريمة ، كما لو كان حاسوبه مسروقا ، أو مؤجرا في أحد مقاهي الانترنت ، أو أن المشتبه به لا يعرف أي شيء عن الانترنت .... الخ ،الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة ... الخ ، إلى جانب الدليل الإلكتروني ، حتى يمكن أن تنسب الجريمة إلى مرتكبها ، وعلى المحقق أو الخبير الإلكتروني أو يوثق جميع مراحل البحث ، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها .

وقد يتخذ الدليل الإلكتروني المستمد من الحاسوب الانترنت شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات،كما يمكن أن يتخذ الشكل الإلكتروني كالأشرطة والأقراص الليزرية ، والى جانب ذلك يوجد مخرج ثالث وهو عرض المعلومات والبيانات المتعلقة بالدليل الإلكتروني عن طريق شاشة الحاسوب[1] .

[1]- د . محمد طارق الحن ، المرجع السابق ، ص 349.

المطلب الثالث : حجية الدليل الإلكتروني

الدليل الإلكتروني كغيره من الأدلة يستوجب له حجية لكي يعتد به الإثبات وسنوضح ذلك في الفرعين التاليين :

الفرع الأول : حجيته

من المعروف أن للقاضي الجزائي مطلق الحرية في أن يصل إلى الحقيقة،من أي دليل قانوني يستمده متعلق بالجريمة،ومن المعلوم أيضا أنه لابد من توافر شروط في الدليل المستخلص منها :

ــ الانسجام مع أحكام القانون ، وعدم مخالفته للقانون أو الدستور حتى يقبل أمام المحكمة كالإستحصال عليه بوسيلة مشروعة .

ــ إمكانية مناقشته ، فالقناعة الوجدانية تتطلب المناقشة للدليل .

ــ أن يكون غير قابل للشك يقيني ، فالشك يفسر لصالح المتهم .

ومن المعروف أن الأدلة الفنية المضبوطة في نظم المعلومات لها أهمية كبيرة، وقد يكون فيها الفصل بين الإدانة والبراءة للمتهم ، ويجب أن يعتني فريق التفتيش ، وفريق جمع الأدلة الإلكترونية بتخزين هذه الأدلة في بيئة مناسبة إلكترونيا،أدلة إثبات قاطعة وذلك يعتمد على دقة الأجهزة المستخدمة في الكشف عن التلاعب، فالدليل الإلكتروني،يمكن استخدامه دليلا قانونيا قاطعا عندما ينص المشرع أن المعلومات الإلكترونية هي أدلة في الإثبات ، فالدليل الإلكتروني في الجنائي يمكن اعتباره قرينة بسيطة يمكن إثبات عكسها .

الفرع الثاني : الشروط الفقهية المتطلبة في الدليل الإلكتروني

ومن الشروط الفقهية الواجب توافرها في الدليل الالكتروني :

- أن يكون منطويا على اعتداء حق يحميه القانون .
- تحديد دقيقا لمصدر استنباط الدليل الإلكتروني
- تحديد الدليل وفق الجريمة المتعلقة بها والجريمة المصرح بها [1] .

.

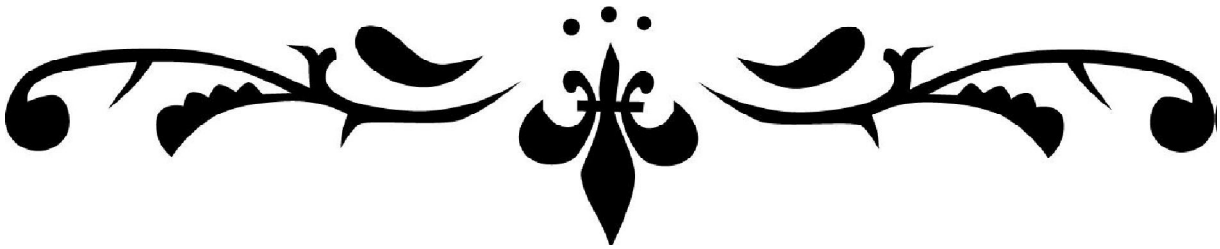
[1]- د .علي جبار الحيسناوي ، المرجع السابق ، ص 143 .

ملخص الفصل الأول

نخلص في ختام هذا الفصل إلى أن القرصنة الإلكترونية هو مصطلح جديد من بين مصطلحات الجرائم التي تعد الإلكترونية فيها هاجساً يقلق الدولة والشعب في آن واحد ولذا كان من الأهمية أن نبدأ بالمبحث الأول بدراسة الإطار التعريف لهذه الجريمة و التي تبين لنا تعدد التعاريف بشأنها مما ينجم عنه تحديد تعريف دقيق لها،ومن خلال تلك التعاريف يمكن تعريفها على أنها الجريمة التي تتم بوسائل غير قانونية لاقتحام نظام الكمبيوتر بدون إذن من المالك الكمبيوتر أو المستخدم ،كما تم توضيح التطور التاريخي لهذه الجريمة والتي كان بدايتها بالقرصنة الهاتفية ومرورا بمراحل تتنوعت وتضاعفت هذه الجريمة يوما بعد يوم إلى أن تطورت في العصر الحالي بفعل ثورة التكنولوجيا لتشكل جريمة مستحدثة ،تتميز بخصائص تختلف تماما عن الجرائم التقليدية حيث تفتقر للدليل المرئي الذي يسهل فهمه ، فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء والذين يختلفون عن المجرمين التقليدين لأنه في الغالب هم على دراية كافيه من العلم والثقافة والمعرفة يمتلكون أدوات المعرفة التقنية والتي يستخدمونها كأسلحة إلكترونية، والتي تستهدف مجني عليه إلكتروني، وذلك لتحقيق أهدافهم أيا كان الدافع من هذا الاعتداء الإلكتروني ، لتوجه لنيل من الحق في المعلومات الإلكترونية ،سواء المتعلقة بمعلومات الحياة الخاصة للأفراد ، أو الاقتصادية ، المعلومات المهددة للأمن القومي ، والسيادة الوطنية،وكما أنها تشيع فقدان الثقة بالتقنية ، وتهدد إبداع العقل البشري، بالإضافة لذلك تم التطرق لنوعية الإثبات الخاصة والتي تتوائم مع طبيعة هاته الجريمة ورغم الصعوبات المعيقة لإثبات وقوعها فهذا لا يعني انتفاء الدليل لذلك الإثبات وهذا كون أن الدليل الإلكتروني يعتبر من الأدلة ذات الدور الفعال المثبت أو المنفي لوقوع القرصنة الإلكترونية.

الفصل الثاني

الجهود المقررة لمكافحة القرصنة الإلكترونية



الفصل الثاني: الجهود المقررة في مكافحة القرصنة الإلكترونية

أدى الانتشار الواسع و المتصارع للإنترنت و الكمبيوتر و التطور الهائل في عالم البرمجيات وتزايد الاعتماد على بنوك المعلومات الإلكترونية ، في تنظيم نواحي الحياة كافة إلى وصول هذه التقنية العالية إلى أيدي الخير و الشر معًا، حيث أستغل البعض معرفتها بالتقنية العلية لارتكاب الجرائم و منها القرصنة الإلكترونية،كما اكتسبت هذه الجريمة طابعًا دوليًا اعتبار أنها من الجرائم العبرة للحدود،في حقيقتها تعتبر من الجرائم الداخلية التي يعاقب عليها قانون العقوبات الوطني.

أما عن حجم هذه الظاهرة على الصعيد العالمي فقد بات أمر ملاحظتها محسوسة، ويتمثل ذلك في الإحصائيات المروعة التي تزايد مخاطرها و الخسائر الناجمة عنها ، حتى باتت تشكل تهديدًا للأمن القومي و للاقتصاد الدولي ، ولذلك فإن التعاون الدولي في مجال مكافحة القرصنة الإلكترونية و الوقاية منها أمرًا لا مفر منه ، إذ تواجه اليوم كل من الدول المتقدمة و الدول النامية على حد سواء خطر هذا التطور، ويغترف العديد من المهتمين بشؤون القرصنة الإلكترونية، بوجود العديد من المشكلات و الصعوبات العملية و الإجرائية التي تعيق مكافحة هذه الظاهرة الإجرامية الإلكترونية، ومن أهم هذه المشكلات :

- يمكن أن تنقضي عدة أشهر أو حتى سنوات قبل اكتشاف الجريمة.
- صعوبة إثبات وقوع القرصنة الإلكترونية، وصعوبة التوصل إلى الجاني، لان أغلب المجرمين الإلكترونين يستخدمون أسم مستعار و يصعب تحديد موقعه.
- تنازع القوانين الجنائية من حيث المكان، فهناك مبادئ تحكم تطبيق القوانين الجنائية من مبدأ إقليمية و العينية و الشخصية و العالمية، و تثور المشكلة في حالة ارتكاب الفعل المؤثم في الخارج، فأي من القوانين الجنائية سوف يخضع لها الجاني الإلكتروني.
- كما أن جهل الناس بثقافة الانترنت وجرائمها،وكذلك جهل المسئولين إدارات المنتديات أو مقاهي الانترنت يفتح المجال لزيادة ارتكاب القرصنة الإلكترونية.

لكن و غم هذه المشكلات و الصعوبات التي واجهت و تواجه المجتمع، لاسيما المعنيون بمكافحة القرصنة الإلكترونية،لم تهبط إرادة أصحاب عقول المعرفة و التقنية التكنولوجية ورجال القانون و الأمن ، في إيجاد أو ابتكار قوانين و طرق و تكنولوجيا

معلومات قادرة على استكشاف المجرمين ، و إمكانية ملاحقتهم لإنزال العقوبة القانونية التي تتواءم و فعلهم الإجرامي، وذلك ببذل جهود على المستوى الوطني ، و الإقليمي، و الدولي ، وهذا ليحقق نتيجة إلا من خلال عقد المؤتمرات و الاتفاقيات والمعاهدات وقائيا و علاجيا ، وهذا ما سيتم دراسته في الفصل الثاني والذي سيتم التطرق فيه إلى أهم الجهود المبذولة على الصعيد الوطني ، و الإقليمي ، و الدولي ، مبرزين مدى نجاعة المجتمعات على حد السواء العربية منها و الدولية ، في مكافحة القرصنة الالكترونية .

وفي هذا الدراسة تم تقسيم الفصل الثاني إلى ثلاث مباحث أساسية كالأتي:

- المبحث الأول: جهود المشرع الجزائري.
- المبحث الثاني: الجهود العربية .
- المبحث الثالث: الجهود الدولية .

المبحث الأول : جهود المشرع الجزائري في مكافحة القرصنة الإلكترونية

إن ظهور التقنيات الإلكترونية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع القرصنة الإلكترونية ، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة ، وعلى مستوى عال من الخطورة الإجرامية ، فما مدى إمكانية استعانة القاضي بقانون العقوبات التقليدي لتوفير الحماية لهذه القيمة الاقتصادية الجديدة ألا وهي أموال الإعلام الآلي ، في ظل النصوص التقليدية خاصة وأن المشرع لم يكن في ذهنه وقت وضع النصوص التقليدية هذا النوع من الجرائم الإلكترونية ألا وهي القرصنة إلكترونية وهنا تكمن المشكلة،فهل يستطيع القاضي الجزائي من خلال النصوص التقليدية التي أقرها المشرع الجزائري أن يحقق حماية جزائية للمعلومات الإلكترونية دول الإطاحة بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي ، وما مدى تطبيق نصوص المستحدثة للمعلوماتية علما أن القرصنة الإلكترونية باعتبارها من إحدى الجرائم الإلكترونية ؟.

ولهذا الغرض ارتأينا تقسيم هذا المبحث إلى مطلبين نوضح في الأول الحماية الجنائية التي أقرها المشرع الجزائري بموجب نصوص حقوق الملكية الفكرية ، ونبرز في الثاني الحماية الجنائية التي أقرها المشرع الجزائري بموجب النصوص الخاصة المستحدثة .

المطلب الأول : الحماية الجنائية بموجب نصوص الملكية الفكرية

اختلف الفقه والقضاء الغربي اختلافا بينا في ما مدى حماية البرامج والمعلومات الإلكترونية من خطر الجرائم الإلكترونية والتي من بينها القرصنة الإلكترونية ، وإدراج هذه البرامج والمعلومات الإلكترونية ضمن نطاق الملكية الفكرية بشقيها المتمثلين في :

الملكية الصناعية والملكية الأدبية والفنية ، ومن هنا كان الاهتمام لمعرفة أي من النظامين الأكثر ملائمة لحماية هذا الإنتاج الذهني وهذا الجدل القائم بين هذين النظامين هو حديث الساعة ، في حول أي نظامين كفيل بمكافحة هذه الظاهرة وحماية لهذه المعلومات الإلكترونية ومن هنا سيتم استعرض فيما يلي لهذين النظامين كبيئتين لحماية البرامج ، مبينا أن النظامين أنجع لذلك لدى الموقف الجزائري وذلك في الفرعين التاليين :

الفرع الأول : الحماية بموجب نصوص الملكية الصناعية

بسط المشرع الجزائري حمايته على الابتكارات والاختراعات ، والتي تكون نتيجتها منتوج جديد وطريقة جديدة ذات تطبيق صناعي وذلك بواسطة قانون براءة الاختراع[1].

أولا : مفهوم براءة الاختراع

براءة الاختراع فهي وثيقة تمنحها الدولة للمخترع فتخول له حق استغلاله ماليا والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة

أما الاختراع فهو" فكرة المخترع تسمح عمليا باتجاه حل لمشكل محدد في مجال التقنية" [2] .

كما نص أيضا: " يمكن أن تقع تحت حماية براءات الاختراعات الجديدة الناتجة عن نشاط اختراعي والقابلة للتطبيق صناعيا " [3] ، ومنه فإننا نقول حتى يحظى اختراع ما بالحماية ضمن نطاق براءة الاختراع ، وجب توافر شرطي الابتكار والجدة ، والقابلية للتطبيق الصناعي ومن هذا المنطلق فهل من المتصور توافر هذه الشروط وامتداداها إلى الكيان المعنوي للأنظمة الالكترونية والتي تكون محلا للقرصنة الإلكترونية [4]؟ وهو ما سأبحثه في العنصر الثاني الموالي :

ثانيا : مدى انطباق الشروط الخاصة بالاختراع على الكيان المعنوي للكمبيوتر

تضاربت الآراء والفقهاء في مدى اعتبار هذا الكيان المعنوي للكمبيوتر ، تنطبق عليها شروط الاختراع لكي يتم حمايتها ومكافحة الجرائم الإلكترونية من خلال قانون براءة الاختراع ، وخلاصة هذا الجدل أنه وبالرغم من مناداة الجانب الأكبر من الفقه لاستعمال هذه المعلومات والبرامج الإلكترونية تحت حماية بقانون براءة الاختراع ، متى كان الغرض منها هو إظهار فكرة صناعية جديدة ، فإن المشرع الجزائري قد استبعد برامج الكمبيوتر صراحة من نطاق الحماية بواسطة قانون براءة الاختراع ، بقوله :" لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب" [1]. ومن هذا المنطلق فإنه يمكننا القول بأن المشرع قد تبنى حق المؤلف كبيئة لمكافحة هذه الجرائم ، وهو ما سيأتي توضيحه في الفرع الموالي .

---

[1] ـ الأمر رقم 03-07 ،المؤرخ في 19 جمادى الأول الموافق 19 جويلية 2003، المتعلق ببراءات الاختراع .
[2] ـ المادة الثانية من قانون براءة الاختراع .
[3] ـ المادة الثالثة من قانون براءة الاختراع.
[4] ـ د.سمير جميل حسين الفتلاوي ، الملكية الصناعية وفق القوانين الجزائرية ، ديوان المطبوعات الجامعية، الجزائر ،2006، ص217.
[1] ـ المادة السابعة من قانون براءة الاختراع.

الفرع الثاني : الحماية بموجب نصوص حقوق المؤلف

ترتب على عدم حماية الكيان المعنوي الإلكتروني للكمبيوتر، من نطاق براءة الاختراع أن اتجه الفقه إلى قانون حماية حق المؤلف ، أما بالنسبة للمشرع الجزائري وإذا كان لم يدرج هذه البرامج والمعلومات الإلكترونية صراحة ضمن المصنفات الخاضعة لحماية حق المؤلف،فإن هذا التعدد قد ورد على سبيل المثال لا الحصر فنجد أن المشرع قد وسع قائمة المؤلفات المحمية ، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية ، حيث نص على ذلك في القانون حق المؤلف وحقوق المجاورة [2] " تعتبر على الخصوص ومصنفات أدبية أو محمية ما يأتي : المصنفات الأدبية المكتوبة مثل .... ، ومصنفات وقواعد البيانات" .

وانطلاقا من أن قواعد البيانات هي عبارة عن تجميع للبيانات بشكل متميز فهي أحد مصنفات الكمبيوتر التي تحتل مكانة مهمة في صناعة المعلومات الإلكترونية ، ومن هنا فالمشرع قد أدرج برامج تحت نطاق المصنفات المحمية بحق المؤلف بشروط ، وهو توافر شرط الابتكار وإن لم يكن منصوصا عليه صراحة [3] ، كما يجب أن تشتمل هذه البرامج على نوع من الأصالة بحيث تبرز من خلالها شخصية المؤلف [4]، والمنتقد في المشرع الجزائري أنه قد بالغ في إعطائه البرمجيات نفس مدة الحماية المقررة لباقي المصنفات الأدبية لمدة 50 سنة ، وكان الأجدر به أن يخفف من هذه المدة ذالك أن هناك تطورا دائما في المجال التكنولوجي ، مما قد يؤدي إلى صدور وإدخال تعديلات بصفة شبه يومية على البرمجيات ، وهذا الاتجاه لا ينافي اتفاقية جنيف[1] ، كما يذهب البعض إلى ذلك في انتقادهم الموجه للمشرع الجزائري ، على اعتبار سمو هذه الاتفاقيات عن الدستور وبالتالي فمخالفته يعني مخالفة صريحة للدستور ولكن في واقع الأمر فإن الاتفاقية نصت في المادة 3/4 على أنه لا تقل حمايتها عن 10 سنوات ، مصنفات التصوير الفوتوغرافي ومصنفات الفن

---

[2] -الأمر رقم 03-05 ، المؤرخ في جمادى الأولى 1424 الموافق ل 19 جويلية 2003 ،المتعلق بحقوق المؤلف و الحقوق المجاورة ، الجريدة الرسمية رقم 61 ، الصادرة ب 2003/01/13 .

[3] - د. بن زيطة عبد الهادي ، حماية برامج الحاسوب في التشريع الجزائري ، الطبعة الأولى ، دار الخلدونية ، الجزائر ، 2007 ، ص 34 .

[4] - André Bertrand. , Thierry piète cou dol , Internet et le droit ,édit Dalloz , 1997, p 33 .

[1] - المرسوم الرئاسي رقم 97 – 341 ، المؤرخ في 1997/09/13، المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية في 1886/09/09 ، والمتممة في باريس في 1896/05/04 ، المعدلة في 1979/09/28،الجريدة الرسمية رقم 61، المؤرخة في 1997/09/14.

التطبيقي، وباعتبار البرامج كذلك ذات طبيعة خاصة فوجب مراعاة هذا الاستثناء تحويل هذه المدة بما يتلاءم وطبيعتها[2] .

ومن هذا المنطلق نجد أن هذه الحماية للبرامج ضمن نطاق حق المؤلف وإن كانت قد أعنتنا لفترة من الفترات عن البحث عن حماية أخرى لهذه البرامج ، كما أنه كان لها الفضل أن تبنها لفترة من الزمن ، إلا أنه لا يمكن الأخذ بذلك أكثر من هذا ، ذلك أن الجزائر اليوم تحتل مكانة مرموقة داخل المنظومة المعلوماتية ، كما أنه تطور استخدام الإعلام الآلي وتزايدت معه الاعتداءات والتي من بينها القرصنة الإلكترونية ومن هنا فلابد من تطوير المنظومة التشريعية للبحث عن حماية أفضل وآمن لهذه البرامج ،وهو ما حاول المشرع تثمينه من خلال قانون العقوبات الجزائري، وانطلاقا من ظللك فسأتعرض لدراسة النصوص المستحدثة ،ضمن قانون العقوبات الجزائري .

المطلب الثاني : الحماية الجنائية في إطار نصوص خاصة

إن المشرع الجزائري ومسايرة منه للتطور التكنولوجي ، فقد أصدر مؤخرا نصوصا تجريمي للحد من الاعتداءات الصادرة ضد الأنظمة الإلكترونية ، وذلك بموجب قانون العقوبات الجزائري [1]، والذي منع بذلك الدخول غير المصرح بت إلى نظام المعالجة الآلية للمعطيات ، وعاقب كل تخريب لمحتويات النظام ، أو إعاقة تشغيله ، وتأسيسا على هذه الحالة الجنائية الخاصة سنعالج في الفروع الآتية ما تداركه المشرع في النصوص الخاصة لحماية الأنظمة الإلكترونية من الاعتداءات ، والتي تعد القرصنة الإلكترونية من قبيل هذه الاعتداءات.

الفرع الأول : الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

أول ما يجب تبيانه أن المعالجة الآلية للمعطيات هي المسألة الأولية الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء، وعلى هذا النظام وبالرجوع إلى الفقهاء، فتم تعريف المعالجة الآلية للمعطيات بأنها كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، والتي تتكون من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط ، والتي يربط بينها مجموعة من العلاقات التي

[2] - د – خثري مسعود ، المرجع السابق ، ص 87 .

[3]- قانون رقم 23-06 ,المؤرخ في ذي القعدة 1427 –الموافق ل 20 ديسمبر 2006، المعدل و المتمم للأمر رقم 66-156، المؤرخ في 18 صفر 1386 –الموافق ل8 جوان 1966 ، المتضمن قانون العقوبات الجزائري .

عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات ، على أن يكون هذا المركب خاضع لنظام الحماية الفنية[1].

وبالرجوع إلى المشرع الجزائري نجده نص على جريمة دخول أو البقاء بطريق الغش في المادة 394 الفقرة الأولى من قانون العقوبات الجزائري ، ويمكن القول انطلاقا من نص المادة أنه يمكن اعتبار السلوك المجرم في هذه المادة من احد صور السلوك الإجرامي للقرصنة الإلكترونية،و هذا كون أن هذه الجريمة ذو سلوك مجرد ، أي أنها تبدأ أو تنتهي بانتهاء السلوك المكون لها ، وهو الدخول أو البقاء دون أن يتطلب المشرع في نموذجها القانوني حسب نصوص التجريم أي نتيجة إجرامية .

ويتحقق **فعل الدخول إلى النظام** ، متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج ، كذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج ورغم ذلك تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه ، فلو فرضنا أن الجاني دخل إلى موقع – أمازون دوت كوم – وهو موقع للبيع الإلكتروني معد للجمهور ، لكنه تجاوز الموقع إلى البيانات الخاصة بإعداد الموقع وتنظيمه في صفحة " Home page " وتنطوي على معلومات لا يجوز للجمهور الدخول إليها ، وبالتالي يكون فعل الجاني مكونا للجريمة الدخول غير المشروع رغم أن الموقع في ذاته مفتوحا للجمهور .

وفعل البقاء في النظام، يتحقق متى اتجهت إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول ، وفي كلتا الصورتين فإن القصد الجرمي قائما حتى ولو كان الباعث من الدخول أو البقاء الفضول ، أو إثبات القدرة على الانتصار على النظام[2].

الفرع الثاني : جريمة الاعتداء ألعمدي على المعطيات

لم يتعرض المشرع الجزائري لهذه الجريمة ، بل اكتفى بالنص على جريمة الاعتداء على المعطيات فقط، بنصه : " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دح إلى 2.000.000 دح ، كل من أدخل بطريق الغش معطيات في نظام

[1]- د – آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الأولى ، دار هرمة ، الجزائر ، 2006 ، ص 102 .

[2]- د . خثري مسعود ، ، المرجع السابق ، ص 118 .

المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1]، فهذا النشاط الإجرامي المنصوص هنا،يشكل بطبيعته أحد السلوكات الإجرامي للقرصنة الإلكترونية ، و ينحصر صور هذا السلوك في أفعال الإدخال والمحو والتعديل ويكفي توافر إحداها لقيام الجريمة، سواء ذلك بك :

- إدخال بيانات لم تكن موجودة من قبل ، يقصد التلاعب أو التشويش على صحة البيانات القائمة .
- أو بفعل المحو بإزالة جزء من المعطيات المسجلة على دعامة داخل النظام أو تحطيم تلك الدعامة .
- أو بفعل التعديل وذلك بتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ، ويتحقق هذا الفعل عن طريق محوها كليا أو جزئيا أو تعديلها ، وذلك باستخدام القنابل الإلكترونية أو ببرامج الفيروسات .

و مما سبق نجد أن هاته الأفعال (الإدخال ، المحو ، التعديل) جاءت على سبيل الحصر ، وبالتالي فلا يقع تحت طائلة أي فعل آخر غيرها وتتحقق هذه الجريمة بعلم الجاني وإرادته في ارتكابها ، ولا يشترط توافر نية إضرار بالشخص مالك البرنامج أو صاحب النظام .[2]

الفرع الثالث : العقوبات المقررة على الاعتداءات الإلكترونية

نص المشرع الجزائري لردع هذه الاعتداءات بمجموعة من العقوبات المتمثلة في :

أولا : عقوبات الأصلية

- عقوبة الدخول أو البقاء داخل النظام : حدد المشرع عقوبة هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة والغرامة من 50.000 دج إلى 100.000 دج[3] ، وأما الصورة المشددة لهذه الجريمة فتنص عليها المادة 394 مكرر 3/2 على مضاعفة

[1] ـ المادة 394 مكرر2 من قانون العقوبات الجزائري .
[2] - د .خثري مسعود ، المرجع السابق ، ص 125 .
[3] ـ المادة 394 مكر 3/2 من قانون العقوبات الجزائري .

العقوبة بالحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج .

- عقوبة الاعتداء العمدي على المعطيات :

حدد المشرع عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام ، بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة 500.000 دج إلى 2.000.000 دج[1] ، كما عاقب على استخدام هذه المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية ، وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج[2].

ثانيا : العقوبات التكميلية

نصت المادة 394 مكرر 3 من قانون العقوبات، على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في :

1 – المصادرة : وتشمل الأجهزة والبرامج المستخدمة في ارتكاب جريمة من الجرائم الماسة بالنظام ، مع مراعاة حقوق الغير حسن النية .

2 – إغلاق المواقع : والأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية .

3 – إغلاق المحل أو مكان الاستغلال : إذا كانت الجريمة قد ارتكبت بعلم مالكها ، ومثال ذلك المقهى الإلكتروني الذي ترتكب في مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها.

ثالثا : العقوبات المقررة للشخص المعنوي

عاقب المشرع الشخص المعنوي ،في حالة ارتكابه لإحدى جرائم الاعتداء على نظام المعالجة الآلية لبيانات بغرامة تعادل خمس مرات الحد الأقصى للغرامة للشخص الطبيعي .

[1] .المادة 394 مكرر1 من قانون العقوبات الجزائري.

[2] -المادة 394 مكرر2 من قانون العقوبات الجزائري .

رابعا : عقوبة الاشتراك والشروع في الجريمة

- عقوبة الاشتراك نص عليها المشرع بأنها: " كل من شارك في مجموعة أو اتفاق تآلف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم ، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها"[1]، ومن خلال استقراء نص المادة أعلاه نجد أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك حيث رصد لها نفس عقوبة الجريمة التامة .
- عقوبة الشروع : نصت المشرع على " يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "[2] ، وبالرجوع إلى القواعد العامة للقانون الجنائي نجد أن الشروع في الجنح لا يعاقب عليه إلا بنص، وبذلك نجد أن المشرع الجزائري قد تبنى فكرة العقوبة على الشروع في ارتكاب الجنح الماسة بنظام المعلوماتي للمعطيات ، وذلك رغبة منه في توفير حماية فعالة لهذا النظام، إذ جعل الشروع معاقب عليه بنفس عقوبة الجريمة التامة[3] .

ومن خلال استعراض الحماية الجنائية للبرامج من خلال نصوص خاصة والتي تبناها المشرع الجزائري في نصوص قانون العقوبات الجزائري , يمكن القول أن المشرع الجزائري قد هدف من وراء ذلك إلى حماية النظام ككل متكامل (الكيان المادي – الكيان المعنوي) ، وبالتالي فإنه لم يتعرض في تعديله هذا لحماية البرامج أو المعلومات بنصوص صريحة لحل الجرائم ومن بينها القرصنة الإلكترونية ، مما أضحى هناك فراغ قانوني واضحا إزاء ردع هذه الجريمة ، رغم أن الجزائر في الوقت الحالي متضررة بالإصابة ببرمجيات خبيثة و تهديدات إلكترونية ، و غيرها من صور الاعتداءات الإلكترونية .

[1] ـ المادة 394 مكرر5 من قانون العقوبات الجزائري.
[2] ـالمادة 394 مكرر 7 من قانون العقوبات الجزائري.
[3] - د – خثير مسعود ، المرجع السابق ، ص 130 .

المبحث الثاني : الجهود العربية لمواجهة القرصنة الإلكترونية

تعد القوانين والتشريعات العربية متأخرة في مواكبة المستجدات التشريعية العالمية المتعلقة بالجرائم الإلكترونية ، الهادفة إلى حماية المنظومة الإلكترونية وقد يعزي ذلك إلى التأخير التقني في مجال المعلوماتية للدول وإذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس خطر القرصنة الإلكترونية المحتمل في البيئة العربية يمكن أن يكون كبيرا لكون الجاهزية الأدائية والتقنية والتشريعية لمواجهتها ليست بالمستوى المطلوب .

وبناءا على ذلك سوف نبرز في هذا المبحث الجهود العربية لمواجهة ظاهرة القرصنة الإلكترونية وهذا في ثلاثة مطالب نعرض في الأول الجهود التعاون العربي ونبرز في الثاني دور الاتفاقيات العربية لحماية حقوق المؤلف ، وسنوضح في الثالث إلى بعض التشريعات والقوانين الوطنية والعربية لمواجهة القرصنة الإلكترونية .

المطلب الأول : جهود التعاون العربي

في ظل شيوع شبكات المعلومات ونقل و تدفق المعلومات إضافة إلى التشديد على أهمية بذل جهود عربية لمكافحة كافة الأنشطة المكونة للاعتداءات الإلكترونية فبرزت على هذا المستوى جهود التعاون العربي محاولة منها لسعي من اجل وضع قواعد لمنع وردع مرتكبي هذه الجرائم ، وفي هذا سوف يتم التطرق إلى أهم تلك الجهود في الفروع الآتية

الفرع الأول: القانون الجزائي العربي الموحد .

لعل أبرز ما يمكن أن يقال عن الجهود العربية المبذولة ، من أجل الحماية من الجرائم الالكترونية ومن بينها القرصنة الالكترونية خصوصا ، هو اعتمادهم على القانون الجزائي العربي الموحد[1]، وبالرجوع إلى المذكرة الإيضاحية لهذا القانون ، وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص ، نجد أن هذا القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتجة عن المعالجات المعلوماتية ،وذلك في المواد 461 – 464 ، وحيث أشارت المواد 161 – 163 على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر الجرائم الالكترونية ،أما المادة 464 منه ، فلقد نصت على عقوبات لمجرمي الإلكترونيون وذلك من يقوم بفعل الدخول بطريق الغش إلى كامل أو جزء

[1] ـ القانون الجزائي العربي الموحد، المعتمد بموجب القرار رقم 229،المؤرخ في 19 نوفمبر 1996.

من نظام المعالجة الآلية للمعلومات ، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة ، وتغيير المعلومات داخل النظام وسرقة المعلومات .

وتعد هذه المحاولة على الرغم من تواضعها أبرز ما تم على صعيد تعزيز التعاون على مستوى وطننا العربي من الناحية التشريعية [1] .

الفرع الثاني : جمعية القانون الجنائي

أكدت الجمعية المصرية للقانون الجنائي في مؤتمرها السادس المنعقد في القاهرة من 25 – 28 أكتوبر1993م حول جرائم الكمبيوتر والجرائم المتعلقة بالجرائم الإلكترونية ، والتي من بينها القرصنة الإلكترونية وذلك اعتبارا أنها من الجرائم الإلكترونية ، كما أكدت هذه الجمعية على وجوب تكاتف الجهود لمكافحتها لأنها تمثل وجها سلبيا للتقدم الحضاري ، ووجوب تعديل نصوص قانون العقوبات التقليدية ، أو إضافة نصوص جديدة لأن النصوص الحالية لا تحيط معظمها بالجرائم الحديثة المراد تجريمها .

كما خرج المؤتمر بتوصيات خاصة بهذه الطائفة من الجرائم الإلكترونية ، وتوصيات بالتعاون الدولي في مجال أنظمة المعلومات الإلكترونية ، وتنفيذ ما تقره من قواعد ووجوب تحقيق التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وذلك في مجال الإنابة القضائية وتسليم المجرمين وتنفيذ الأحكام ، كما وصى المؤتمر بوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات وطرق الاستدلال والتحقيق وجمع الأدلة في الجرائم المتعلقة بها.

أما بالنسبة لمسألة الحماية القانونية للبيانات الاسمية و الحياة الخاصة من الاعتداءات الإلكترونية عبر شبكة الانترنت ، فلم تتناوله الدول العربية في تشريعاتها وقوانينها المعمول بها حاليا ، ورغم هذا ، فلم تتطرق بعد التشريعات والقوانين العربية لجريمة القرصنة الإلكترونية الواقعة على الأنظمة الإلكترونية مباشرة ، ولم تتناولها في تشريعاتها وقوانينها ، على الرغم من الحاجة الملحة إلى تجريمها و الوقاية منها ، ولضمان تحقيق سبل الحماية والأمن لمنظومة المعلومات والاتصالات الحديثة وفي مقدمتها شبكة الانترنت[2].

[1]- د – على جبار الحيسناوي ،المرجع السابق ، ص 159 .

[2]- د – على جبار الحيسناوي ، المرجع السابق ، ص 162 .

المطلب الثاني : الاتفاقيات العربية

إن الجهود العربية المبذولة في إطار حماية الملكية الفكرية وحق المؤلف خصوصا ، تتمثل في عدة من الاتفاقات أبرمت في مجال حماية حقوق الملكية الفكرية في ظل التقنيات الجريمة الحديثة ومنها القرصنة الالكترونية وسنتناول في الفروع الآتية أهم الاتفاقيات العربية المبرمة في هذا المجال .

الفرع الأول : الاتفاقية العربية لحماية حقوق المؤلف

أبرمت الاتفاقية العربية لحماية حقوق المؤلف والتي أوصى مؤتمر الوزراء المسئولين عن الشؤون الثقافية المنعقد في بغداد 1981 م الدول العربية بالمصادقة عليها ، وجاء في ديباجة الاتفاقية أن الدول العربية إذ تحزوها الرغبة على حد سواء في حماية حق المؤلفين على المصنفات الأدبية والفنية بطريقة فعالة وموحدة ، وتجاوبا مع المادة 21 من ميثاق الوحدة الثقافية العربية الصادرة عام 1964 م ،والتي حثت الدول العربية على وضع تشريعات لحماية الملكية الأدبية والفنية والعلمية،من الاعتداءات الإلكترونية .

و إن كان هذا يعد جهدا متواضعا، إلا أن هذا له ما يبرره فوضع الدول العربية يختلف عن الدول الغربية المتقدمة التي تعتمد على التكنولوجيا في شتى مناحي الحياة،ولا تزال أقل تأثر بالجرائم الإلكترونية الماسة بالملكية الفكرية كما هو الحال في الغرب[1] .

الفرع الثاني : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تأتي ضمن الجهود العربية الحثيثة التي تقوم بها جامعة الدول العربية لحشد التدابير الأمنية اللازمة تجاه مكافحة الجرائم الإلكترونية،في شتى أشكالها وصورها ، ومنها جرائم القرصنة الإلكترونية عبر إيجاد الأسس النظامية والبيئة القانونية ،كما أنه تنادي على ضرورة تعزيز التعاون بين الدول العربية في مجال المكافحة،.وتسعى هذه الاتفاقية إلي تحقيق توازن ضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره، والمساعدة على تحقيق النظام الإلكتروني و حفظ الحقوق المترتبة على الاستخدام المشروع

[1]- د – محمود أحمد عبانية ، جرائم الحاسوب وأبعادها الدولية ، المرجع السابق ، ص 173 .

للحاسبات الآلية والشبكات المعلوماتية، كما يهدف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني[1].

الفرع الثالث : المؤتمرات العربية لحماية الملكية الفكرية

إلى جانب الجهود العربية المبذولة في ظل الاتفاقيات العربية للحماية من مساوئ التكنولوجيا الحديثة ، فهناك مؤتمرات دولية عربية عقدت لتساهم أيضا في تلك الحماية ، ومن أهم هذه المؤتمرات :

أولا : المؤتمر العربي الدولي الأول للملكية الفكرية

يعتبر المؤتمر الدولي العربي الأول للملكية الفكرية[2]،من المؤتمرات الساعية لحماية الملكية الفكرية حيث نوقشت فيه حماية الملكية الفكرية ، والإجراءات المطلوبة من الأقطار العربية لتنفيذ اتفاقية تربس وأثر حماية الملكية الفكرية على مستقبل الاستثمار في الشرق الأوسط .

ثانيا : المؤتمر العربي الدولي الثاني للملكية الفكرية

أما المؤتمر الدولي العربي الثاني للملكية الفكرية ، الذي عقد عام 1998 م ، طالب بضرورة توجيه توصية حول تسهيل نقل التكنولوجيا من الدول الصناعية ، إلى الدول العربية لحماية الاختراعات ومكافحة القرصنة الإلكترونية ، وتسهيل نقل اختراعات العلماء العرب إلى أوطانهم[3] .

المطلب الثالث: التشريعات والقوانين الوطنية والعربية لمواجهة القرصنة الإلكترونية

لم تزل التشريعات والقوانين العربية تخطو خطوات خجولة في مواكبة التطورات التشريعات العالمية المتعلقة بالقرصنة الإلكترونية ،فالدول العربية لازالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي .

و في هذا المطلب سيتم الاستعراض لبعض التشريعات والقوانين العربية التي تبين الجهود التي قامت بها تلك الدول لمواجهة الجرائم الإلكترونية والتي من ضمنها القرصنة الإلكترونية.

[1] - إنتصار إلياس إبراهيم،"الإتفاقية العربية لمكافحة جرائم تقنية المعلومات"،دراسة تطور جرائم تقنية، مجلة شرطة الخرطوم، العدد22، 28 أكتوبر2013،ص15.

[2] - المؤتمر العربي الدولي الأول للملكية الفكرية، المنعقد ب28-30 -1995 في عمان، بموجب التنظيم المشترك العربي لحماية الملكية الفكرية.

[3] - د – علي جبار الحيسناوي ، جرائم الحاسوب والانترنت ، المرجع السابق ، ص 161 .

الفرع الأول : في تونس

أفرد المشرع التونسي حماية خاصة للمعطيات الالكترونية في مواجهة التطور التقني في المواد من 38 – 42 من قانون التجارة الالكترونية[1]، وفرض عقوبات أصلية وعقوبات تكميلية على الأفعال المخالفة لتلك المواد فتنصص المادة 38 على أنه : " لا يمكن لمزود خدمات المصادقة الالكترونية ، معالجة المعطيات الشخصية إلا بعد موافقة صاحب الشهادة المعني " ، وتجد المادة 41 تنصص على أنه : " يتعين على مزود خدمات المصادقة الالكترونية قبل كل معالجة للمعلومات الشخصية إعلام صاحب الشهادة بواسطة إشعار خاص بالإجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية ".

وكذلك تنص المادة 42 على : " يمكن لصاحب الشهادة في كل وقت يطلب ممضي بخط اليد أو الكترونيا النفاذ إلى المعلومات الشخصية المتعلقة بصاحب الشهادة ، ويتعين على المزود وضع الإمكانيات اللازمة لتمكين صاحب الشهادة من إرسال مطلبه الممضي لتعديل المعلومات ، أو مسحها بطريقة إلكترونية " .

وعليه فقد تنبه المشرع التونسي إلى خطورة القرصنة الإلكترونية على بنوك المعلومات ، وعلى المعطيات الشخصية مما حذا به إلى فرض نصوص خاصة تكفل الحماية لحرمة الحياة الخاصة[2].

الفرع الثاني : الإمارات

تعد في طليعة البلدان العربية ، التي تسعى لمواكبة المستجدات الحديثة في مجال التشريعات والقوانين المتعلقة بالمنظومة الإلكترونية ،حيث عالجت في قانون المؤلف القضايا الخاصة بالقرصنة وسرقة المؤلفات[3]،وطبقت قانون حماية الملكية الفكرية الصادر عن الدولة عام 1994[4] ،والذي يوجه إلى مستخدمي البرامج غير الشرعية عقوبة الغرامة المالية التي تصل إلى 50 ألف درهم إماراتي،ومصادرة أجهزة الحاسوب والبرامج ، بالإضافة إلى العقوبة الحبس التي تصل مدتها إلى ثلاث سنوات .

---

[1] ـ القانون التونسي، رقم 83/20، المؤرخ في 09 أوت 2000،المتعلق بالمبادلات و التجارة الإلكترونية .

[2] - د – محمد أمين أحمد الشوابكة ، جرائم الحاسوب والانترنت ، دار الثقافة ،الأردن ،2006،ص 82 .

[3] ـ القانون الاتحادي الإماراتي ، رقم 40/92،المؤرخ في 16 أفريل 1992،المتعلق بحماية المصنفات الفكرية و حقوق المؤلف،الجريدة الرسمية رقم 3821 .

[4] ـ القانون الاتحادي الإماراتي،رقم 36/94، المؤرخ في 24 فيفري ،المتعلق بالملكية الأدبية و الفنية، المعدل و المتمم بالأمر رقم 33/09.

وتعد دولة الإمارات في صدارة القائمة الإقليمية في مكافحة قرصنة البرمجيات في الشرق الأوسط لعام 2000 ويجري العمل من أجل وضع الأطر القانونية للتجارة الإلكترونية ففي 2001 في أسبوع الحكومة الإلكترونية الثالث ، تم تأكيد على ضرورة وضع صياغة قانونية وتشريعية لإثبات القانوني ، والتوقيع الإلكتروني ، وكل ما يتعلق بالتجارة الإلكترونية[1]، ووضع جميع التدابير اللازمة لحمايتها من القرصنة الإلكترونية ،كما أنها تعد من أول الدول التي سنت قانونا مستقلا بالجرائم المعلوماتية و ذلك عام 2006 [2] .

الفرع الثالث : مصر

نجد أن مصر لم تعمل على سن قوانين جديدة خاصة بتا ، في هذا المجال فالقانونين في مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي على الجرائم الالكترونية ، والتي تفرض نوعا من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة للجرائم الالكترونية[3].

كما اتجها القانونين إلى تعديل قوانين الملكية الفكرية للتناسب مع التطورات التقنية المستحدثة عالميا ، بسن قوانين تحمي البرمجيات وحقوق المستهلكين من الجرائم الالكترونية، فقد عملت جمعيات خاصة من أجل تثبيت حماية حقوق الملكية الفكرية في مجال البرمجيات وعلى رأسها " إتحاد منتجي البرامج التجارية،وقد أسفر ذلك على انخفاض في نسبة القرصنة إلى نحو 19 % في عام واحد ، فوصلت إلى 56 % في عام 2001 ، بعد أن كانت تلك النسبة 75 % خلال العام 1999 ، وألان وفي مصر تدرس مسألة الدفع الالكتروني في مجال التجارة الالكترونية ، من خلال لجان متخصصة في وزارة الاتصالات والمعلومات وذلك من أجل إصدار قوانين منظمة له .

وفي ظل مواكبة النهضة التكنولوجية و الإلكترونية والمعلوماتية التي يعيشها العصر، فقد أصدر المشرع المصري قانون خاص للاتصالات[4]، لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكتروني[5] ، لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية

[1] ـ لمزيد من التفاصيل أنظر: قانون الاتحادي الإماراتي رقم 01/05 ،المتعلق بالمعاملات و التجارة الإلكترونية ،على الموقع: www.oman.legal.net، تاريخ الإطلاع:2014/ 20/04 ،30:20 .

[2] - د – علي جبار الحيسناوي ، المرجع السابق ، ص 173 .

[3] - د – عبد الحكيم رشيد توبة ، جرائم تكنولوجيا المعلومات ، المرجع السابق ، ص 232 .

[4] ـ المرسوم الرئاسي رقم 10/03، المؤرخ في 14 فيفري 2003،المتضمن قانون الإتصالات المصري.

[5] ـ المرسوم الرئاسي رقم 15/04،المؤرخ في 21 أفريل 2004 , المتضمن قانون التوقيع الإلكتروني .

"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 القرصنة الإلكترونية.

الفرع الرابع : المملكة العربية السعودية

على الرغم من حداثة القرصنة الالكترونية نسبيا، إلا أن الدراسة التي أجرتها منظمة (business software alliance) في الشرق الأوسط في حجم خسائر القرصنة الالكترونية،وصلت إلى ثلاثين مليون دولار أمريكي في المملكة العربية السعودية،والإمارات العربية المتحدة[1] .

لم تسن السعودية قوانين خاصة بجرائم الالكترونية إلا أن وضعها يختلف فهي ليست بحاجة لتحديث قوانينها وتشريعاتها كونها تنطلق من الشريعة الإسلامية الكاملة، فهو مشرع واحدا لا ثاني له والتشريع أزلي لا جديد له ، فهو صالح لكل زمان ومكان وقد تركت الشريعة الإسلامية الباب مفتوحا لتجريم الجرائم المستحدثة تحت قواعد فقهية واضحة منها وتركت لوالي الأمر تقرير العقوبات لبعض الجرائم المستحدثة مراعاة لمصلحة المجتمع ، ويندرج ذلك تحت باب التعازير ، وهناك قاعدة سد الذرائع : دفع الوسائل التي تؤدي إلى المفاسد والأخذ بالوسائل التي تؤدي إلى المصالح[2] .

ولقد صدر في المملكة العربية السعودية نظام حماية حقوق المؤلف، حيث توضح هذه المادة الثالثة منه [3] ، الأنواع المشمولة بالحماية ورد في البند عاشرا : برامج الحاسب الآلي، ومما تجدر الإشارة إليه أن عقوبة نسخ البرامج في السعودية تصل إلى إغلاق المحل المخالف 15 يوما وتغريمه (10.000) ريال ، مع مضاعفة هذه العقوبة في حالة تكرار المخالفة للاتفاقية العالمية لحقوق المؤلف التي وقعت في باريس ، والتي أصدرت تعليمات بشأن تطبيق حماية حقوق التأليف على المصنفات الأجنبية ، والتي تضم برامج الحاسوب الإلكترونية ، وبرامج ألعاب الحاسوب الإلكترونية ،وقد نصت التعليمات على ضرورة

[1] - د – علي جبار الحيسناوي ، المرجع السابق ، ص 174 .
[2] - د – عبد الحكيم رشيد توبة ، المرجع السابق ، ص 233 .
[3] - المرسوم الملكي رقم م/11، المؤرخ في 19 ماي 1410 هـ ،المتعلق بنظام حماية حقوق المؤلف السعودي .

الالتزام بالتوقف الكلي والنهائي عن ممارسة أعمال نسخ البرامج الإلكترونية بأي شكل أو حجة[1] .

وقد اتخذت مدينة الملك عبد العزيز للعلوم والتقنية من خلال وحدة الانترنت المشرفة على عمل مقدمي خدمة الانترنت ، في المملكة عددا من الإجراءات الفنية التي تهدف إلى محاصرة أعمال المخربين والمتسللين ومنعهم ، وقد أوضحت الوحدة أنها قد ألزمت جميع مقدمي خدمة الانترنت في المملكة بتطبيق عددا من الإجراءات الفنية ، لمنع القرصنة الإلكترونية ، وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الانترنت في المملكة ، ومن بين هذه الإجراءات :

1 – منع انتحال أرقام الانترنت والتي يقوم من خلالها مجرمي القرصنة الالكترونية باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة .

2 – العمل على منع إساءة استعمال البريد الالكتروني ، سواء للتهديد أو إرسال عروض أسعار أو دعايات لا يقبل بتا المستخدم ، ما عرف اصطلاحا بالبريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة .

3 – الحصول على خدمة الوقت " 4TP " عن طريق وحدة البر وكسي ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات الالكترونية .

4 – ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية[2] .

[1]- د – علي جبار الحيسناوي ، المرجع السابق ، ص 175 .

[2]- د .منير محمد الجنبهي ود ممدوح محمد الجنبهي ، المرجع السابق ، ص 193 .

المبحث الثالث : الجهود الدولية

مع تزايد الخسائر الناجمة عن القرصنة الإلكترونية ، وتزايد حجم الأضرار الناشئة ، والتي تتخطى في أغلب أحيانها حدود الدول ، فبات أمر التعاون الدولي لمواجهتها ضرورة حتمية.، وعليه فالتعاون الدولي هو من أهم سبل مكافحة الجرائم الإلكترونية والتي من ضمنها القرصنة الالكترونية ، فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها ما ارتكبوه من جرائم ، وفي إطار الجهد الدولي المبذول ، فإن هناك العديد من الهيئات والمنظمات والمجالس الدولية التي تؤدي دورا ملحوظا في إبرام الاتفاقيات في محاولة منهم لترسيخ وجوب التعاون الدولي لمواجهة القرصنة الإلكترونية.

وفي ظل هذه الدراسة سيتم تقسيم هذا المبحث إلى أربعة مطالب نعرض في الأول للجهود الدولية للأمم المتحدة ، وفي الثاني نعرض الجهود الدولية لحماية الملكية الفكرية ، ونبرز في المطلب الثالث جهود المجلس الأوروبي ونوضح في المطلب الرابع إلى أهم التشريعات والقوانين الوطنية لمواجهة القرصنة الإلكترونية .

المطلب الأول : جهود الأمم المتحدة على النطاق الدولي

تبذل الأمم المتحدة جهودا لا يستهلان بها في مجال التصدي لجرائم الحاسب الآلي والانترنت ، ألا والتي من ضمنها القرصنة الإلكترونية ، وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشارها وتعاظم أثارها .

وفي هذا سنبين في الفروع التالية لأهم الجهود الأمم المتحدة من خلال المؤتمرات الدولية كالآتي:

الفرع الأول : مؤتمر الأمم المتحدة السابع

كلف مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو في ايطاليا في عام 1985 م ، لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي، فأقرت مجموعة من المقترحات والتوصيات لمكافحة الظواهر الإجرامية الحديثة، وقد تبنى مؤتمر " هافانا " الثامن هذه التوصيات بعد أن أدخل عليها بعض التعديلات، ويمكن إجمال توصيات مؤتمر " هافانا " عام 1990 في المبادئ التالية :

1 – تحديث القوانين الجنائية الوطنية بما في ذالك التدابير المؤسسية .

2 – تحسين أمن الحاسب الآلي والتدابير المعنية .

3 – اعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم الالكترونية .

4 – اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم .

5– زيادة التعاون الدولي من أجل مكافحة هذه الجرائم [1] .

الفرع الثاني : مؤتمر الأمم المتحدة التاسع

وفي المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين برعاية الأمم المتحدة، المنعقد في القاهرة عام 1995 م ، أكدت توصياته على وجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية ، من تزايد مخاطر التكنولوجيا ووجوب التنسيق ، والتعاون بين أفراد المجتمع الدولي ، لاتخاذ الإجراءات المناسبة للحد منها .

الفرع الثالث : مؤتمر الأمم المتحدة العاشر

وفي العام 2000 عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين بودابست في المجر ، وأكدت على وجوب العمل الجاد للحد من جرائم الحاسب الآلي المتزايدة والمستحدثة ، واتخاذ التدابير للحد من أعمال القرصنة .

وتوجهت جهود منظمة الأمم المتحدة في ميدان حماية الحياة الخاصة في مواجهة التقدم التقني ، وحماية الأفراد وحرياتهم من خطر التعدي ، وذلك في المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان ، وأبرز ما جاء في توصياتها أن الحاسبات الإلكترونية تمثل أكبر تهديد للحياة الخاصة والحرية الشخصية .

إذ أنها تعد من أدوات المراقبة وأجهزة التطفل الحديثة وخاصة إذا تم تخزين البيانات الشخصية على الحاسب الوالي[2]

المطلب الثاني : الجهود الدولية لحماية الملكية الفكرية

مما لاشك أن حقوق الملكية الفكرية ، هي من أكثر الحقوق التي يتم انتهاكها يوميا على شبكة الانترنت ، أو على كافة الشبكات الاتصالات والمعلومات على مستوى العالم وعليه فوجود معاهدات دولية تمنع تلك الانتهاكات ، وإصدار كل دولة قوانين خاصة بها

[1]- د – محمود أحمد عبابنة ، المرجع السابق ، ص 152 .

[2]- د – علي جبار الحيسناوي ، المرجع السابق ، ص 148 .

تعمل على حماية حقوق الملكية الفكرية كل يؤدي ذلك يؤدي إلى الحفاظ على تلك الحقوق من الانتهاك اليومي[1] ، وعليه سيتم التوضيح في الفروع الآتية إلى أهم الاتفاقيات الدولية التي تم إبرامها في مجال حماية حقوق الملكية الفكرية من القرصنة الإلكترونية كالأتي :

الفرع الأول : دور المنظمة العالمية للملكية الفكرية

تعتبر المنظمة العالمية للملكية الفكرية "الويبو" [2] ، من إحدى الوكالات المتخصصة في شبكة وكالات منظمة الأمم المتحدة ولها دور مهم في تحديد و تعزيز الحلول الدولية للمشاكل القانونية و الإدارية التي تفرضها التقنية الرقمية و بشكل خاص الإنترنت ،وتلك الناتجة عن النشر الإلكتروني و ما تحتويه مواقع الإنترنت والتي تكون محل مستهدف من قبل القراصنة الإلكترونيون والذين يقومون بالاعتداءات على الأفكار و الممارسات التقليدية للملكية الفكرية، و هو الأمر الذي دفع بالمنظمة لتعزيز جهودها في الاهتمام بوضع قواعد و معايير جديدة تساير ما شهده عالمنا الحالي من ظهور شبكة المعلومات و ثورة المعلومات[3]، ولتحقيق ردع لهذه الجرائم الحديثة تم التنسيق و التعاون في ما بين المنظمة العالمية و منظمة التجارة الإلكترونية من أجل توحيد الأهداف التي تسعى إليها كل واحدة منهما وهي حماية الملكية الفكرية من مساوئ التكنولوجيا الإلكترونية [4].

ومن خلال استعراض بنود تضامن الاتفاقيتان فقد أكد الأعضاء حرصهم على دعم الملكية الفكرية في جميع أنحاء العالم بهدف تشجيع النشاط الإبتكاري ، وتطوير ورفع كفاءات الاتحادات المنشأة في مجالات حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية ، ووضع مجموعة عمل تصمم عدد من الخبراء يهدف حماية برامج الحاسوب الآلي، وعبر الاجتماعات المتكررة ، ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف ، ومنذ ذلك العام وحتى الآن عدلت معظم تشريعاتها الخاصة بحق المؤلف ، وزادت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية قانونا [5] .

---

[1]- د .عبد الحكيم رشيد توبة ، المرجع السابق ، ص 238 .

[2] ـ الاتفاقية العالمية للملكية الفكرية،المنعقدة في إستوكهولم بالسويد ، المنعقدة في 14تموز 1967 و التي دخلت حيز التنفيذ 1970 .

[3] ـ د. عبد الله عبد الله ، الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت ، دار الجامعة الجديدة ، الإسكندارية ، 2008 ، 258 .

[4] ـ د. فاتن حسين حواء ، المواقع الإلكترونية و حقوق الملكية الفكرية ،الطبعة الأولى ، دار الثقافة، الأردن ، 2010، ص118.

[5]- د . محمود أحمد عبابنة ، المرجع السابق ، ص 239 .

الفرع الثاني : معاهدة برن لحماية المصنفات الأدبية والفنية

تعد معاهدة "برن" هي حجر الأساس في مجال الحماية الدولية لحق المؤلف [1] ، وتعد المادة التاسعة من تلك الاتفاقية هي أساس تلك الاتفاقية ، لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان ، فضلا عن ذلك تمنح اتفاقية برن صاحب حق المؤلف ، الحق أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور المصنفة ، وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدي عليه وطنيا أم أجنبيا [2] .

الفرع الثالث : معاهدة تريبس

معاهدة تريبس[3] ، هي من المعاهدات التي تم انجازها في مجال حماية الملكية الفكرية من السطو عليها لاسيما مع انتشار عمليات السطو الالكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية [4].

تلك الاتفاقية تم التوقيع عليها من قبل دول الأعضاء بها وقد عالجوا من خلال الاتفاقية العامة للتعريفات و التجارة (الجات) حقوق الملكية الفكرية ، فربطوا بذلك بين المعايير الدولية والمعايير المحلية وتتضمن تلك الاتفاقية العديد من الإجراءات الهامة والفعالة لردع الاعتداءات على حقوق الملكية الفكرية ، كما أنها ومن وجه آخر تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع ، ومن تلك التدابير على سبيل المثال لا الحصر ، إعطاء الحق للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة ، والتي عادة ما تكون سهلة التخلص منها لو لم تكن هناك سرعة في محاولة ضبطها ، فضلا عن فرض عقوبات جنائية رادعة ، كما تعمل على إبطاء عجلة التقنيات في الدول النامية لاسيما الدول العربية ، وذلك بتعزيزها لسيطرة مفهوم الربح على المصنفات الأدبية والفكرية بعيدا عن توخي مفاهيم التوزيع العادل في نشر تلك التقنيات ، كذلك فرض حصار التكنولوجيا عليها ، وفي حالة تراخي الدولة العضو عن اتخاذ مثل تلك الإجراءات ، تكون عرضة لان تتخذ ضدها العديد من الإجراءات العقابية من باقي الدول الأعضاء [5] .

---

[1] ـ إتفاقية برن لحماية المصنفات الأدبية و الفنية المؤرخة في 9/ 11/ 1886 م.

[2] - د – عبد الحكيم رشيد توبة ، المرجع السابق ، ص 239 .

[3] ـ إتفاقية تريبس المتعلقة بالتجارة من حقوق الملكية الفكرية المؤرخة في 15 أفريل 1994 .

[4] ـ لمزيد من التفاصيل أنظر: د. محمد قطب ، الجرائم المستحدثة ، الطبعة الأولى ، دار الفجر للنشر و التوزيع ، القاهرة ، 2009 ، ص 387 .

[5] - د.منير محمد الجنبهي ، ود.ممدوح محمد الجنبهي ، جرائم الانترنت والحاسب الآلي ، المرجع السابق ، ص 201 .

المطلب الثالث : دور المجلس الأوروبي .

يقوم المجلس الأوروبي بدور مهم في محاولة الحد من الجرائم الالكترونية ومن ضمنها القرصنة الالكترونية وذلك من خلال إقراره للعديد من التوصيات الخاصة لحماية البيانات والبرامج ، وحماية تدفق المعلومات ، وسنوضح في الفروع التالية لدور المجلس الأوروبي في مكافحة ظاهرة القرصنة الالكترونية كالآتي :

الفرع الأول : اتفاقية حماية المعلومات الإلكترونية .

توج المجلس الأوروبي جهوده بإصدار إتفاقية شاملة تتعلق بالجرائم الإلكترونية وحماية للمعلومات الإلكترونية [1].

وجاء في مقدمة تلك الاتفاقية أن الدول الأعضاء وحرصا منها على حماية مجتمعاتها من الجرائم الإلكترونية يجب عليها وضع التشريعات الملائمة وتعزيز التعاون الدولي لاسيما مع تزايد معدلات الجرائم المرتبطة بالتقنية من جرائم شبكات الحاسب الآلي ، والاعتداء على المعلومات الإلكترونية والتي تستلزم جهود مضنية للبحث عن الأدلة و الإثبات نظرا للطبيعة الخاصة التي تتمتع بها هذه الجرائم ، لإن الأدلة فيها تخزن وتنتقل بواسطة الشبكات، كما نصت هذه الإتفاقية على ضرورة التعاون الدولي واتخاذ الإجراءات والتشريعات الكفيلة لمكافحة هذه الظاهرة [2] .

الفرع الثاني : إرشاد لحماية قواعد البيانات

باعتبار أن البيانات تعد نتاجا فكريا يتطلب حمايتها فقد أصدر الإتحاد الأوروبي إرشادا [3] يتعلق بالحماية القانونية لقواعد البيانات بما في ذلك غير الإلكترونية ، من الاعتداءات الإلكترونية ، وقد حدد هذا الإرشاد مدة حماية مضمون قاعدة البيانات بهذا الحق الخاص بـــ 15 سنة ، تبدأ من تاريخ انتهاء صناعة قاعدة البيانات ، وكل تعديلا مهما أو تغييرا تاليا في المضمون من شأنه أن يمنح القاعدة ذاتها حماية قانونية جديدة [4] .

---

[1] ـ الإتفاقية الأوروبية المتعلقة بالجرائم الإلكترونية و حماية المعلومات الإلكترونية المؤرخة في 25 / 04 / 2000 .

[2] ـ د. كوثر مازوني ، الشبكة الرقمية و علاقاتها بالملكية الفكرية ، دار الجامعة الجديدة ، الجزائر، 2008 ، 292 .

[3] ـ الإرشاد الأوروبي،رقم CEE/9/96 ،المتعلق بحماية قواعد البيانات المؤرخ في 1996/03/11.

[4] ـــ د .علي جبار الحيسناوي ، المرجع السابق ، ص 152 .

الفرع الثالث : معاهدة مكافحة جرائم الشبكات الإلكترونية

وقعت اللجنة الخاصة المعنية بقضايا الجريمة ، بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة الجرائم الإلكترونية وسط انتقادات من دعاة حماية الحرية الشخصية ، وبعد أن يتم المصادقة عليها من مقر رئاسة المجلس وتوقيعها من قبل البلدان المعنية ، ستلزم الاتفاقية الدول المعنية بسن القوانين الضرورية للتعامل مع جرائم القرصنة الالكترونية ، بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وانتهاكات حقوق النسخ الرقمي والصور الأخرى للجرائم الالكترونية ، كما تلزم المعاهدة الدول بمساعدة بعضها في جمع الأدلة وفرض القانون وتعزيز التعاون الدولي [1] .

المطلب الرابع : التشريعات والقوانين الوطنية الأجنبية لمواجهة القرصنة الالكترونية

اتجهت كافة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم الجرائم الإلكترونية الجديدة ، و التي تعتبر القرصنة الإلكترونية من إحدى صورها على قوانينها التقليدية القديمة، وصاغت نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجيا .

وفي هذا المطلب سيتم التطرق في إلى أهم الدول المتقدمة التي سعت إلى مكافحة الجرائم الإلكترونية وسنبحث في مجمل نصوصها القانونية على مجرمته من سلوكيات إجرامية المكونة لفعل القرصنة الإلكترونية .

الفرع الأول : السويد .

تعد السويد أول دولة تسن تشريعات خاصة بجرائم الإلكترونية ، حيث صدر أول قانون خاص بها (The spécial low) ، وسمي بقانون البيانات ، عام 1973 ، وقد عالج هذا القانون قضايا القرصنة الالكترونية ، من حيث أنه جرم سرقة المعلومات الالكترونية والدخول غير المشروع على البيانات الالكترونية ، أو تحويلها أو الحصول غير المشروع عليها .

[1] - د – عبد الحكيم رشيد توبة ، المرجع السابق ، ص 228 .

الفرع الثاني : الولايات المتحدة الأمريكية .

تعد الولايات المتحدة الأمريكية من الدول الثانية ، في إصدار قوانين خاصة بها (Spécial Laws) تجرم الجرائم الإلكترونية ، وقد قدرت الولايات المتحدة الأمريكية خسائرها من القرصنة الإلكترونية ، ما بين ثلاثة وخمسة ملايين دولار سنويا ، وبينت دراسة أجرها أحد مكاتب المحاسبة الأمريكية أن 240 شركة أمريكية تضررت من القرصنة الإلكترونية .

و قد أظهر المسح الذي أجري عام 2000 أن مئتين وثلاث وسبعين شركة بلغ مجموع خسائرها أكثر من (256.000.000) دولار .

وفي عام 1986 صدر قانونا آخر يحمل الرقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم الإلكترونية ، ووضعت المتطلبات الضرورية اللازمة لتطبيقه ، وقد قولت وزارة العدل الأمريكية في عام 2000 م خمس جهات حكومية للتعامل مع الجريمة الإلكترونية منها مكاتب للتحقيقات الفيدرالي [1]

الفرع الثالث : بريطانيا

بينت دراسة أجريت في بريطانيا ، أنه حتى أواخر الثمانينات أرتكب ما يقارب من 262 جريمة إلكترونية ، وقد كلفت حوالي اثنين وتسعين مليون جنيه إسترليني سنويا ، وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الإلكترونية ، حيث أقرت قانون مكافحة التزوير والتزييف الإلكتروني عام 1981 م .

الفرع الرابع : فرنسا .

فرنسا من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة ، حيث أصدرت أول قانون خاص بها في عام 1988 م ، الذي زاد على قانون العقوبات الجنائي جرائم الحاسب الآلي ، وفي عام 1994 م تم تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية بالجرائم الإلكترونية وإقرار عقوبات لها .

وفي سنة 1978 ، أصدر المشرع الفرنسي القانون رقم 7 ، الخاص بالمعالجة الإلكترونية للبيانات ، والذي اشتهر باسم قانون معالجة المعلومات الإلكترونية والحريات ، ووضعت عدة قوانين روعي فيها التطور التكنولوجي في عالم الاتصالات والكمبيوتر ومنها :

[1] - د .منير محمد الجنبهي و د.ممدوح محمد الجنبهي ، المرجع السابق ، ص 188 .

- قانون 1980/07/12 ، والمتعلق بإثبات التصرفات القانونية ذات المعالجة الإلكترونية.
- قانون 1982/06/29 ، الذي أقر فيه مبدأ حرية الاتصال السمعي والبصري .
- قانون العقوبات الجديد لعام 1992 ، المعمول به منذ عام 1994[1] .

ونرى مما تقدم أن الجهد المبذول الداخلي أو الدولي لحماية نظم المعلومات الإلكترونية ركز على استظهار ومواجهة الأخطار التي يمثل اعتداء على الحياة الخاصة للأفراد وبياناتهم الشخصية المخزنة باستخدام الحواسيب ونظمها وشبكات المعلومات ، ونرى أن الحاجة ملحة إلى تضافر الجهود لوضع قواعد عامة لحماية البيانات والمعلومات الإلكترونية لاسيما مع تزايد تطور تقنيات القرصنة الالكترونية .

[1]- د – علي جبار الحيسناوي ، المرجع السابق ، ص 165 .

ملخص الفصل الثاني

نخلص في ختام هذا الفصل المتعلق بالجهود المقررة لمكافحة القرصنة الإلكترونية، إلى أنه ومع مدى تزايد مخاطر القرصنة الإلكترونية على كافة مجالات الحياة أصبح من المهم التعاون بإقرار جهود وطنية و إقليمية و دولية للحد من هذه الجريمة ، مما أصبح معه ضرورة تطوير القوانين أمرا لا مفر منه بحسبان أنه المرآة الحقيقية التي تعكس واقع المجتمع بصدق و أمانة ، وعلى الرغم من التحديات والصعوبات التي تواجه نظام مكافحة القرصنة الإلكترونية والتي من أهمها صعوبة التوصل إلى مرتكبي القرصنة الإلكترونية الذين يرتكبون الجريمة في دولة ما، ضد المجني عليه الذي يكون في دولة أخرى ، ومن صعوبة تعين الجاني الحقيقي ، و صعوبة إيجاد أدلة ملموسة تدين الجاني، إلى غيرها من الصعوبات المتجددة ، ولكن ورغم ذلك فالمجتمعات لم تفقد الشجاعة و الأمل في إيجاد أنظمة وقوانين صارمة لمكافحة جرائمهم ، وإذلال جميع العقبات وإيجاد جميع الحلول الممكنة لمواجهة التحديات التي تقف ضد تطبيق أنظمة لمكافحة القرصنة الإلكترونية .

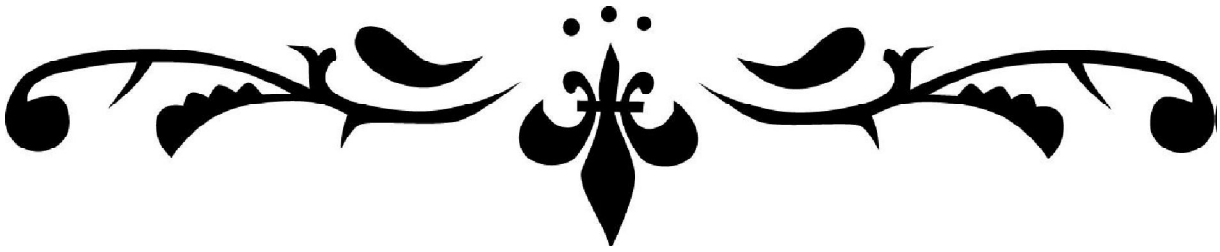
وفي بداية المبحث الأول من هذه الدراسة تم التعرض لجهود المشرع الجزائري و الذي عالج الحماية الجنائية للبرامج والمعلومات و البيانات، أولا من خلال حماية جنائية من خلال نصوص الملكية الفكرية والتي يستخلص منها أن المشرع قد تبنى حق المؤلف كبيئة لمكافحة الاعتداءات إلا أن هذه الحماية ضعيفة كون أنها لم تلم باعتداءات القرصنة الإلكترونية ،مما دفع بالمشرع الجزائري إلى إقرار حماية من خلال نصوص خاصة والتي تبناها المشرع الجزائري في نصوص قانون العقوبات الجزائري و من خلالها يتبين أن المشرع هدف من وراءها إلى حماية الكيان المادي والكيان المعنوي ، وبالتالي فإنه لم يتعرض في تعديله هذا لحماية البرامج أو المعلومات بنصوص صريحة للحماية من القرصنة الإلكترونية ، مما أضحى هناك فراغ قانوني واضحا إزاء ردع هذه الجريمة ، رغم أن الجزائر في الوقت الحالي متضررة بالإصابة بالاعتداءات الإلكترونية .

فيما توالت الدراسة فيما بعد إلى التعرض لجهود العربية المبذولة في هذا المجال والتي تباينت بين التعاون العربي و المصادقة على اتفاقيات بهذا الخصوص، ورغم هذا الجهد المبذول فهناك من الدول العربية التي أدركت خطورة هذه الجرائم مما أسرعت إلا سن قوانين تتواءم مع طبيعة هذه الجريمة المستحدثة ولكن ذلك دون أن يتم بتجريم

القرصنة الإلكترونية بصفة محددة ودقيقة ، ولكن وفي مقابل ذلك فهناك العديد من التشريعات والقوانين العربية مازالت تخطو خطوات خجولة في مواكبة التطورات التشريعات العالمية المتعلقة بالقرصنة الإلكترونية ،فالدول العربية لازالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي ، و لهذا يعتبر تحول الدول العربية إلى مجتمع المعلومات الإلكترونية نمطا من أنماط الحتمية التاريخية ، الغرض منها التطبيق الفعال لتكنولوجيا المعلومات و الاتصالات و التنمية .

كما تم التعرض من خلال هذه الدراسة للجهود الدولية و التي تعد هي من أول الجهود السباقة لمكافحة الجرائم الحديثة ومن خلاله نخلص إلى أن المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة لعبت دور مهما في الحفاظ على الأمن والاستقرار, وخاصة في مجال مواجهة القرصنة الإلكترونية و ذلك من خلال إقرار العديد من الاتفاقيات و المعاهدات وعقد المؤتمرات ، بالإضافة لجهود منظمات الإتحاد الأوروبي و إلى جانب هذه الجهود، هناك جهود أخرى تتضح معالمها في الجهود المتعلقة بحماية العالمية للملكية الفكرية كمعاهدة تيبس و برن ، ومن خلال ما تم التطرق له من تشريعات و القوانين الدولية نجد أن هناك قصور نوعا ما أمام وضع نصوص قانونية خاصة بجريمة القرصنة الإلكترونية ، وبالتالي يستوجب إعادة النظر وذلك قصد سد الثغرات و الفراغات القانونية ، رغم التعديلات التي سارعت الكثير من الدول القيام بتا ،وذلك لأنها لم تعد كافية أمام الكم الهائل للمعلومات الإلكترونية المجودة على الشبكة.

الخاتمة



تناولت هذه الدراسة موضوعًا هامًا من موضوعات المستقبل في مجال أمن المجتمع الواقعي و التقنية الإلكترونية ،و شبكاتها المعلوماتية و هي القرصنة الإلكترونية ، و لقد أصبحت هذه الجريمة الحديثة ظاهرة خطيرة تهدد استقرار المجتمع و أمنه العام ، و هذا ما يشكل تحديا كبيرًا أمام هذا الأخير للأخذ بجميع السبل و الوسائل لمكافحتها خاصة وأننا أمام هذا التحول العالمي الكبير من القلم و الكتاب إلى لغة الأرقام، و لا نعرف ماذا بعد .

وقد عرضنا في هذه الدراسة بالنسبة للفصل الأول للإطار العام لماهية القرصنة لإلكترونية ورأينا أن خطورتها تكمن في خصائصها التي تميزها عن الجرائم العادية لذلك إحتار الفقهاء في وضع تعريف كامل ودقيق لها ، كون أنها ترتكب من قبل مجرمين متخصصين إلكترونين لهم سمات خاصة عن غيرهم يمارسون أنشطتها بسرية تامة وثبات واستمرارية تزيد من خطورتها ، التي تتخذ في أغلب صورها الاعتداء على المعلومات الإلكترونية نظرًا لأهميتها و ما تحتويه من الكثير في مجالات الحياة، فمنها ما يمس الجانب السياسي ، ومنها ما يدخل في المجال الاقتصادي، وينعكس ذلك أيضا على جرائم تمس المجال الاجتماعي، مما ظهرت الحاجة الملحة لتوفير الرعاية القانونية لها ، ثم كانت هناك إطلالة على الوسائل الإلكترونية المستخدمة في الاعتداءات الإلكترونية والتي من الواجب توفرها لإحداث التطابق بين النموذج الإجرامي و بين الواقعة ومن ثم اشتقاق العقاب ، ثم عرجنا بعد ذلك لدراسة بصفة عامة إلى الإثبات الجنائي لهذه الجريمة و إلى الصعوبات المعترضة لإثبات وقوع القرصنة الإلكترونية ،كون أنها من الجرائم النظيفة التي ليس لها أثر خارجي مادي ، فإثباتها يحتاج إلى خبرة فنيّة، ودراية فائقة في هذا المجال لان القواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه الجرائم ، وإنما تحتاج إلى دليل إلكتروني يتواءم مع طبيعة هذه الجريمة الخاصة .

فيما خصصنا الفصل الثاني من الدراسة للبحث في الجهود المقررة لمكافحة القرصنة الإلكترونية ، فكان لا بد من تكاثف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ، ولا توجه لمجتمع بعينه ، ورغم تواجدت بعض الصعوبات المعيقة لخطط مكافحة القرصنة الإلكترونية إلا أن الجهود أنصبت في دراستها المتعمّقة ، وخلق آليّات قانونيّة للحماية من أخطارها، وبرز في هذا المجال جهود وطنية و إقليمية و دولية ، فتطرقنا بداية لجهود المشرع الجزائري من خلال نصوص الملكية

الفكرية من جهة ، و من خلال نصوص خاصة من جهة أخرى ، ومما يتبين لنا في الأخير أن الجزائر بدأت تستهلك التكنولوجيا الحديثة من دون أن تحضر نفسها لذلك بجدارة ، ثم تم التعرض إلى أهم الجهود العربية في هذا المجال من خلال ما تم تكريسه بموجب التعاون الدولي و ما في حكمه ، مع إبراز أهم التشريعات الإقليمية العربية التي حاولت الوقاية من هذه الجريمة ، ثم عرجنا بعد ذلك لإبراز أهم الجهود الدولية المبذولة في هذا الخصوص ومنها بإبراز جهود الأمم المتحدة التي تعد السباقة في مكافحة مثل هذه الجرائم.

النتائج :

- ✓ رغم الجهودات المعتبرة التي قام بها الفقهاء في إعطاء تعريف دقيق للقرصنة الإلكترونية ، إلا أن الخصائص التي تميزت بها و إتساع أنشطة إرتكابها ، حال دون ذلك ، بالإضافة إلى أن مختلف التعاريف الموضوعة لهذه الجريمة هي نفس التعاريف المعتمدة بالبنسبة للجرائم الإلكترونية ، جرائم الأنترنت ، جرائم التقنية العالية وغيرها.
- ✓ أن خطورة القرصنة الإلكترونية تكمن في خصائصها التي تميزها عن الجرائم العادية ، وهذا ما أدى إلى صعوبة حصرها و تحديد قواعدها القانونية .
- ✓ إن التطور التقني و التكنولوجي و سهولة التنقل بين الدول ، زاد من أنشطة هذه الجريمة و تطورها ، و تزيد من خطورة أنشطة العصابات الإجرامية نتيجة إستعمال هذه العصابات للتقنيات الحديثة في إرتكابها ، مما أضحت من أكثر الجرائم خطورة على الأمن و الإستقرار العالمي .
- ✓ إن الوسائل الإلكترونية المنفذة لعمليات القرصنة الإلكترونية تعتبر من أخطر الوسائل كون أنها كثيرة و يصعب حصرها،وبإزدياد تطورها فتحت آفاقاً واسعة للقيام لتجسس الإلكتروني والإرهاب الإلكتروني دون الحاجة لإختراق الدول و المؤسسات المختلفة من قبل عناصر بشرية .
- ✓ أن صعوبة الإثبات الجنائي لوقوع القرصنة الإلكترونية لا يمكن أن تكون عقبة في سبل التجريم، فالتجريم مسألة موضوعية و الإثبات يتعلق بمسائل إجرائية،ولا يمكن أن نجعل صعوبة الإثبات في بعض المسائل الجنائية سببا في عدم التجريم .

- ✓ في ظل تزايد التطور السريع لطوائف مرتكبي القرصنة الإلكترونية المتميزون بخصائص معينة ومع إختلاف دوافع الإرتكاب، فإنه يصعب حصر ووضع تصنيف ثابت لهذه الطوائف بالإضافة إلى صعوبة الوصول إليهم، لأن هذا النوعية من الجرائم يمكن ارتكابها من دول أخرى في العالم فالجاني قد يكون في دولة والمجني عليه في دولة أخرى بعكس الجرائم التقليدية ، كما أن دور الضحايا الضعيف في عدم الكشف عما يلحقهوهم من إعتداءات الإلكترونية يعزز الفرص لمجرمي القرصنة من زيادة إقبالهم للكثير من الإعتداءات .
- ✓ من رغم حداثة هذه الجريمة إلى أن هناك من الدول العربية إستحدثت قوانين للوقاية من القرصنة الإلكترونية مما يبرز مدى وعي الحكومات العربية بمدى خطورتها ،مما ترفع هذه الحكومات الوعي للدول العربية الأخرى بمخاطر هذه الجريمة.
- ✓ تعد الجهود الدولية من بينها الأمم المتحدة من الهيئات التي أخذت على عاتقها مهمة مقاومة هذه الجريمة، ووضع السياسات الجنائية الملائمة للتخفيف من أثارها، والتي أعددت دراسات على هذه الظاهرة الإلكترونية ووسائل مقاومتها، لكن مجهوداتها لا تزال متواضعة نظرًا لعدم تفطن بعض الدول لأخطار هذه الجريمة،وعدم تقديم التعاون اللازم لمكافحتها .

التوصيات :

على ضوء النتائج التي أمكن التوصل إليها من خلال هذه الدراسة، أقدم فيما يلي بعض التوصيات التي يمكن أن يكون لها صدى يساهم في إثراء الفكر الجنائي الإلكتروني ولو بالقدر الضئيل ويمكن إجمال التوصيات في النقاط الآتية :

- ✓ تفعيل دور المكافحة الوقائية التي تسبق وقوع القرصنة الإلكترونية، وذلك من خلال تفعيل دَور المؤسسات التوعويَّة (المسجد، الأسرة، دُور التعليم، أجهزة الإعلام)، وذلك بالتوعية بخطورة القرصنة الإلكترونية على الأسرة والمجتمع.
- ✓ إنشاء مدارس ومعاهد وأقسام بحثية في الجامعات خاصّة تعنى بالأمن الإلكتروني والتدريب فيه، ومواكبة كل ما هو حديث في هذا المجال.
- ✓ سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات القرصنة الإلكترونية ، مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها، والنصِّ على طرق ثبوتها ، مع ضمان الحق في المعلومات و الحق في الحياة الخاصة ، مع التحديد الواضح الدقيق لصور السلوك المكون للقرصنة الإلكترونية، مع مراعاة الطابع التقني لهذه الجريمة و إيجاد العقوبات الملائمة على نحو يحقق أهداف العقوبة في الردع العام و الخاص ، و كذلك النص بشكل واضح و صريح على مسؤولية الشخص المعنوي و إفراد العقوبات الخاصة به .
- ✓ يجب أن يكون للضحايا من القرصنة الإلكترونية دورًا فعالا و إيجابيا من خلال المطالبة بحقوقهم المعتدى عليها وبذلك يكونوا قد أسهموا في التقليل من وقوع هذه الإعتداءات الإلكترونية .
- ✓ نوصي أيضا بعقد دورات تدريبية لأفراد الضبطية القضائية العامة و القضاء على أعمدة التحقيق في النظم الإلكترونية، بهدف تأهيلهم ليتمكنوا من التعامل مع هذا النوع من الجرائم ذات التقنية العالية والعمل على ضبطها وإثباتها بالطرق القانونية والفنيّة ، للحد من إنتشارها والتقليل من آثارها السلبية في الحياة .
- ✓ وهنا ندعو خاصة الشرع الجزائري بالذات في هذا الشأن لإيجاد دراسات قانونية تكفل هذه الجريمة بإعطائها حقها عند توجيه المسؤولية الجنائية لها ،دون ترك جريمة

القرصنة الإلكترونية هكذا لا نصوص محددة بشأنها ولا حتى محاولة للتغير في مجالها،فغياب التشريع القائم بها جعلها تدرس تحت طائلة "الجريمة المعلوماتية"

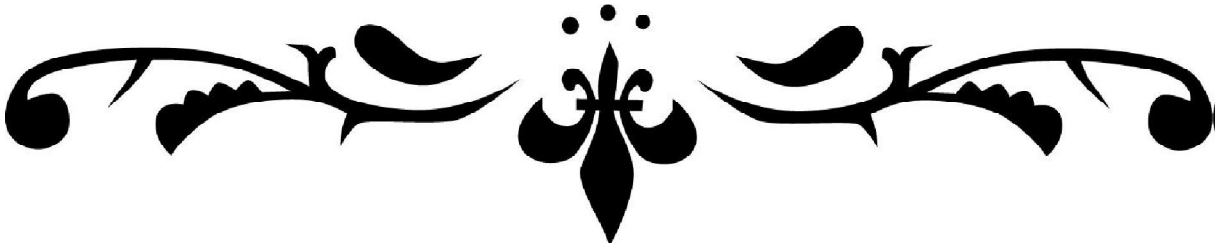
بصفة عامة ، لذلك فأنا أدعو منظومتنا التشريعية بسد هذا الفراغ القانوني.

- ✓ عقد الاتفاقيات بين الدول بخصوص القرصنة الإلكترونية ، وقايةً وعلاجاً وتبادلاً للمعلومات والأدلة.
- ✓ التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعيّة، والقضائيّة، والضبطية، والفنية، وذلك من أجل سد منافذ القرصنة الإلكترونية قدر المستطاع،وتحقيق التعاون مع أصحاب الخبرة الإلكترونية لمعرفة التعامل مع هذه الجربمة .
- ✓ إعداد ندوات و مؤتمرات علمية و بحثية متخصصة تسمح بتزويد الحقل القانوني بكل مستجدات القرصنة الإلكترونية و أساليب إرتكابها، وتعميق أنشطة البحوث و الدراسات في ظل التطورات في ميدان تكنولوجيا الإتصال و المعلومات على نحو يحقق مقتضيات الحماية و التأمين الإلكتروني من جهة وإعتبارات الحرية الفردية و الحق في المعلومة من جهة أخرى .
- ✓ إنشاء قانون دولي مُوَحَّد، ومحاكم خاصَّة دوليَّة محايدة تتولَّى التحقيق في جرائم القرصنة الإلكترونية، ويكون لها سلطة الأمر بضبط وإحضار المجرم الإلكتروني للتحقيق معه أيًّا كان موقع هذا المجرم وبلده، وهذا الاقتراح أو التوصية تتناسب مع مقام جرائم القرصنة الإلكترونية التي تتمثَّل الكرة الأرضيَّة أمامها قرية صغيرة واحدةً قريبة المدى متقاربة الأطراف.
- ✓ التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية للقرصنة الإلكترونية الواقعة في أراضيها ضدّ دول أو جهات أخرى خارج هذه الأراضي،وتعزيز التعاون مع النظمة الدولية للشرطة الجنائية(الأنتربول) لمواجهة كافة أشكال القرصنة الإلكترونية .
- ✓ تفعيل اتفاقيات تسليم المجرمين الإلكترونيين، وتفعيل التعاون الثنائي ومتعدد الأطراف من خلال إبرام المعاهدات وهذا لإتخاذ التدابير اللازمة لحل مشكلة الإختصاص التي تثيرها جريمة القرصنة الإلكترونية العابرة الحدود .

- ✓ الإستفادة من تجارب الدول المتقدمة ذات الخبرة الواسعة حول تدريب القضاة و رجال الجمارك، قصد محاربة القرصنة الفكرية بصفة عامة و القرصنة الإلكترونية بصفة خاصة،مع حث هذه الدول على كشف هذه التجارب من خلال تبادل الخبارات مع ضرورة التعاون العربي في هذا المجال .

وفي نهاية دراستنا فيجب أن نؤكد على أن القرصنة الإلكترونية ما هي إلا الاستخدام غير المشروع لتكنولوجيا المعلومات الإلكترونية وللوقاية منها و وردعها يجب علينا كمجتمع أن نضع يدًا بيدً لنتعاون لأجل الحد من انتشار هذه الجرائم و خصوصًا بزيادة الوعي لدى المجتمع، فيجب أن لا تكون هذه الجرائم بمنأى عن العقاب.

قائمة المراجع والمصادر



أولاً_ المصادر :

أ / القوانين :

1 - قانون رقم 23-06 ،المؤرخ في ذي القعدة 1427 – الموافق لـــ 20 ديسمبر 2006، المعدل و المتمم للأمر رقم 66-156، المؤرخ في 18 صفر 1386 – الموافق لـــ 8 جوان 1966 ، المتضمن قانون العقوبات الجزائري.

2 - القانون الجزائي العربي الموحد، المعتمد بموجب القرار رقم 229،المؤرخ في 19 نوفمبر 1996

3 - القانون التونسي، رقم 83/20، المؤرخ في 09 أوت 2000،المتعلق بالمبادلات و التجارة الإلكترونية .

4 - القانون الاتحادي الإماراتي ، رقم 40/92،المؤرخ في 16 أفريل 1992،المتعلق بحماية المصنفات الفكرية و حقوق المؤلف،الجريدة الرسمية رقم 3821 .

5 - القانون الاتحادي الإماراتي،رقم 36/94، المؤرخ في 24 فيفري ،المتعلق بالملكية الأدبية و الفنية، المعدل و المتمم بالأمر رقم 33/09.

قانون الاتحادي الإماراتي رقم 01/05 ،المتعلق بالمعاملات و التجارة الإلكترونية .

ب / المراسيم :

1 - المرسوم الرئاسي رقم 97 – 341 ، المؤرخ في 1997/09/13، المتضمن انضـــمام الجزائر مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية فـــي 1886/09/09 ، والمتممة في باريس في 1896/05/04 ، المعدلة في 1979/09/28 ،الجريدة الرسمية رقم 61، المؤرخة في 1997/09/14.

2 - المرسوم الرئاسي رقم 10/03، المؤرخ في 14 فيفري 2003،المتضمن قانون الاتصالات المصري.

3 - المرسوم الرئاسي رقم 15/04،المؤرخ في 21 أفريل 2004 , المتضمن قانون التوقيع الإلكتروني المصري .

4 - المرسوم الملكي رقم م/11، المؤرخ في 19 ماي 1410 هـــ ،المتعلق بنظام حماية حقوق المؤلف السعودي .

ج / الأوامر :

1 - الأمر رقم 03-05 ، المؤرخ في جمادى الأولى 1424 الموافق لـــ19 جويلية 2003،المتعلق بحقوق المؤلف و الحقوق المجاورة ، الجريدة الرسمية رقم 61 ، الصادرة بـــ 13جانفي2003

2 - الأمر رقم 03_ 07 ،المؤرخ في 19 جمادى الأول الموافق لـــ 19 جويلية 2003، المتعلق ببراءت الاختراع .

د / الاتفاقيات :

1 - الاتفاقية العالمية للملكية الفكرية،المنعقدة في إستوكهولم بالسويد ، المنعقدة في 14تموز 1967 و التي دخلت حيز التنفيذ 1970 .

2 - إتفاقية برن لحماية المصنفات الأدبية و الفنية ،المؤرخة في 9/ 11/ 1886.

3 - اتفاقية تريبس المتعلقة بالتجارة من حقوق الملكية الفكرية، المؤرخة في 15 أفريل 1994

4 - الإرشاد الأوروبي،رقم CEE/9/96 ،المتعلق بحماية قواعد البيانات، المؤرخ في 03/11/ 1966 .

ثانياً - المراجع العربية :

أ/ الكتب:

1 - د. الشواء محمد سامي ،ثورة المعلومات و إنعكاستها على قانون العقوبات ،الطبعة الثانية،دار النهضة العربية، القاهرة، 1988 .

2 - د. آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الأولى ، دار هرمة ، الجزائر ، 2006.

3 - د. أمير فرج يوسف ، الجريمة الالكترونية والمعلوماتية ، الطبعة الأولـــى ، الناشـــر مكتبة الوفاء القانونية ، الإسكندرية ، 2011.

4 - د.ـــبن زيطة عبد الهادي ، حماية برامج الحاسوب في التشريع الجزائـــري ، الطبعـــة الأولى ، دار الخلدونية ، الجزائر ، 2007 .

5- د . جلال محمد الزعبي وأسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، الطبعة الأولى، دار الثقافة للنشر والتوزيع ، الأردن ، 2010
6- د . خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية ، الإسكندرية ، 2008 .

7- د . خثير مسعود ، الحماية الخبائية لبرامج الكمبيوتر ، دار الهدى ، الجزائر ، 2010.
8- د. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية،2007.
9 - د.سمير جميل حسين الفتلاوي ، الملكية الصناعية وفق القوانين الجزائرية ، ديوان المطبوعات الجامعية، الجزائر ،.2006
10 - د. شريف محمد غنام ، حماية العلامات التجارية عبر الانترنت في علاقاتها بالعنوان الالكتروني ، دار الجامعة الجديدة ، الإسكندرية ، 2007.

11- د.عبد الحكيم رشيد توبة ، جرائم تكنولوجيا المعلومات ، الطبعة الأولى ، دار المستقبل للنشر والتوزيع ، الأردن ، 2009.
12 - د.عبد الصبور عبد القوي ، علي مصري ، الجريمة الالكترونية ، الطبعة الأولى ، دار العلوم للنشر والتوزيع ، القاهرة ، 2008 .
13- د .علي جبار الحسيناوي ، جرائم الحاسوب والانترنت ، دار اليازوري العلمية للنشر والتوزيع ، الأردن ، 2009
14 - د.عبد الفتاح البيومي الحجازي، الجرائم المستحدثة، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2008
15 - د. عبد الفتاح البيومي حجازي، الجريمة في عصر العولمة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.

16 - د. فاتن حسين حواء ، المواقع الإلكترونية و حقوق الملكية الفكرية ،الطبعة الأولى ، دار الثقافة، الأردن ، 2010 .
17 - د. كوثر مازوني ، الشبكة الرقمية و علاقاتها بالملكية الفكرية ، دار الجامعة الجديدة، الجزائر، 2008

18 - د. محمد أمين الرومي ، جرائم الكمبيوتر والانترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2003 .
19 - د. محمد أمين أحمد الشوابكة ، جرائم الحاسوب والانترنت ، دار الثقافة ،الأردن، 2006.
20 - د. محمد طارق عبد الرؤوف الحن ، جريمة الاحتيال عبر الانترنت ، الطبعة الأولى، منشورات الحلبي الحقوقية ، لبنان ، 2011 .
21 - د. محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر، الإسكندرية، 2004 .
22 - د. محمد قطب ، الجرائم المستحدثة ، الطبعة الأولى ، دار الفجر للنشر و التوزيع ، القاهرة ، 2009.
23 - د .محمود أحمد عبابنة ، جرائم الحاسوب ، وأبعادها الدولية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، الأردن ، 2009.
24- د نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم ألمعلوماتي ، ناشر لمنشأة المعارف ،القاهرة، 2008.
25 - نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلومات ، ناشر لمنشأة المعارف ،القاهرة، 2008.
26 - د. نسرين عبد الحميد، الجرائم الاقتصادية، المكتب الجامعي الحديث، القاهرة، 2009.
27 - د. نعيم مغبغب ، مخاطر المعلوماتية والانترنت على الحياة الخاصة وحمايتها ، دراسة في القانون المقارن ، الطبعة الثانية ، منشورات الحلبي الحقوقية ، لبنان ، 2008 .
28 - د. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الثانية ، دار الثقافة للنشر والتوزيع ، الأردن ، 2010.
29 - د. هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، ط 1 ، دار النهضة العربية ، القاهرة ، 1992.
30 - د. يونس عرب ، موسوعة القانون وتقنية المعلومات – جرائم الكمبيوتر والانترنت، منشورات إتحاد المصارف المغربية ، الجزء الأول ، الطبعة الأولى ، أبو ظبي ،2002.

ب/المعاجم اللغوية:

1 - د. أحمد سعيفان،قاموس المصطلحات السياسية والدستورية والدولية، الطبعة الأول، مكتبة لبنان ، لبنان ، .2004

2 - د. الرازي محمد بن أبي بكر، مختار الصحح، الطبعة الرابعة ، المكتبة المصرية ، لبنان، 1418

ثالثًا_ المراجع الفرنسية:

1 _ André Bertrand. , Thierry piète cou dol , Internet et le droit ,édit Dalloz , 1997.

رابعاً - المؤتمرات:

1ــ المؤتمر العربي الدولي الأول للملكية الفكرية، المنعقد ب28-30 -1995 في عمان، بموجب التنظيم المشترك العربي لحماية الملكية الفكرية.

خامسًا - الرسائل الجامعية :

1 - جمال وادي، " العلامة و الانترنت "،(مذكرة ماجستير ، فرع الملكية الفكرية ، جامعة الجزائر، 2003- 2006.

2 - مليكة عطوي ، "الانترنت والملكية الفكرية "، مذكرة لنيل شهادة الماجستير ، كلية الحقوق ، جامعة الجزائر ، 2002 – 2003.

3ــ حفيظة خمايسية ،"التعاون الدولي في مكافحة جرائم الانترنت "،(مذكرة لنيل شهادة الماجستير – فرع القانون الجنائي الدولي - ، كلية الحقوق و العلوم السياسية ، جامعة تبسة، 2011 – 2012) .

سادسًا - المقالات :

1 - د. محمد محمود عمارة ،"تاريخ القرصنة الالكترونية بين العبقرية و إنتهاك الفوائد"، المتاحة على الموقع: www/sooid.net، بتاريخ2014/03/24 ، على الساعة 03:25.

سابعاً - المجالات :

1 - انتصار إلياس إبراهيم،"الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"،دراسة تطور جرائم تقنية، مجلة شرطة الخرطوم، العدد22، 28 أكتوبر2013.

ثامنًا - المواقع الإلكترونية :

1 _ www.alukon.net

2_ www.oman.legal.net

الملاحق

الملحق رقم 01

الكشف عن تفاصيل مثيرة في قضية القرصنة الالكترونية على البنوك الأمريكية

المصدر – موقع شبكة الإعلام العربية – محيط

في الوقت الذي تجري فيه السلطات الأمريكية التحقيق مع نحو 70 مشتبها به من الأمريكيين في القضية واصلت نيابة الأموال العامة بمدينة المنصورة استجوابها للمتهمين المصريين ، وقالت مصادر قريبة من التحقيقات إن عددا من المتهمين اعترفوا بالتهم المنسوبة إليهم وأن بعضهم كشف تفاصيل عن شبكة القرصنة المصرية الأمريكية منذ تأسيسها منذ 5 سنوات حتى القبض عليها في مصر وأمريكا .

وأضافت المصادر أن المجموعة المقبوض عليها في مصر ليست هي المجموعة الأساسية التي أنشأت شبكة القرصنة ، وأن من أسسها هم محترفون كانوا بالفعل ثروات بعد أن تمكنوا من سحب أكثر من 7 ملايين دولار من ثلاثة بنوك أمريكية وأنهم هاجروا خارج مصر بعد أن بدت عليهم معالم الثراء وتحولوا إلى حديث الأهالي من منطقتي دكرنس والمنصورة بدلتا مصر .

وتابعت مصادر التحقيقات قائلة إن المقبوض عليهم ساروا على نهج المجموعة المصرية القديمة وتمكنوا من تسيير عجلة شبكة القرصنة والاتصال بالقرصنة الأمريكيين وأنهم تمكنوا بالفعل من الحصول على مبالغ مالية كبيرة تقدر بمئات الألوف من الدولارات سددوا بها ديونهم واشتروا سيارات وشققا قبل أن يتم كشفهم بالتعاون بين السلطات المصرية والأمريكية .

الملحق رقم 02

القبض على مجموعة أشخاص ارتكبوا قضايا قرصنة الكترونية .

ألقت إدارة البحث الجنائي / شعبة بحث جنائي أمن إقليم العاصمة القبض على مجموعة أشخاص من جنسية أجنبية قاموا بعمليات قرصنة الكترونية على أجهزة الصراف الآلي العائدة للبنوك وسحب أرصدة عملائها من خلال استخدام تقنيات حديثة مكنتهم من الحصول على بيانات بطاقات الصراف الآلي .

وأوضح الناطق الإعلامي باسم مديرية الأمن العام الرائد محمد الخطيب أن عملية المتابعة استمرت لأسابيع إثر وقوع عدد من حالات القرصنة الالكترونية على حسابات عملاء بنوك تم حصر نشاط مجموعة أشخاص ومراقبتهم ليتم ضبطهم بالجرم المشهود وبالتعاون مع موظفي أحد البنوك أثناء عملية زرع الأجهزة المستخدمة في هذه الجريمة في صراف ألي خارج أحد البنوك في منطقة الصويفية في عمان .

وبحسب الرائد الخطيب فإن مختلف أقسام إدارة البحث الجنائي عملت على مراقبة كابينات الصراف الآلي بشكل مستمر للحيلولة دون تمكين هؤلاء الأشخاص من تنفيذ مخططاتهم وكانت قد ضبطت عددا من الأجهزة المستخدمة في سرقة بيانات بطاقة الصرف الآلي التي عثر عليها داخل الفتحة المخصصة لإدخال البطاقة إضافة لكاميرات صغيرة مثبتة في أعلى الكابينة لغايات تسجيل عملية إدخال الأرقام السرية الخاصة بالبطاقة .

وأكد الناطق الإعلامي أن جهود البحث والتحري مكنت شعبة بحث جنائي إقليم العاصمة من ضبط ثلاثة أشخاص تورطوا في هذه العملية عملوا على زرع أجهزة لنسخ بيانات بطاقات الصراف ومن ثم نقلها على بطاقات مقلدة واستخدامها من جديد لسحب كامل الرصيد في حساب العميل الأصلي والحصول على الرقم السري عبر تصوير عملية الإدخال بواسطة كاميرا صغيرة مثبتة أعلى لوحة المفاتيح في الجهاز فيما أشار إلى أن التحقيقات مستمرة لتحديد إن كان قد تورط آخرون حيث سيعلن قريبا عن نتائج هذه التحقيقات والأساليب المستخدمة في مثل هذا النوع من عمليات القرصنة وهوية الأشخاص المتورطين.

ونوه الرائد الخطيب إلى أن اسلم الطرق لتجنب الوقوع ضحية لمثل هذا الأسلوب

تتمثل في أن يقوم العميل بالتأكد من عدم وجود اية إضافات غير مألوفة على جسم جهاز الصراف الآلي سواء في فتحة إدخال البطاقة أو لوحة المفاتيح أو سقفها الداخلي وتغطية لوحة المفاتيح باليد عند وضع رقم استخدام البطاقة السري وإبلاغ البنك أو البحث الجنائي ذلك لقطع الطريق على كل من تسول له نفسه التعدي على ممتلكات الآخرين واتخاذ الإجراءات الكفيلة بصون حقوقهم .

الملحق رقم 03

مجموعة قرصنة الكترونية تعلن اختراق بريد رئيس الحكومة التونسية وتهدد بنشرها ، احتجاجا على سياسة الحكومة

أعلنت مجموعة تطلق على نفسها " أبو نيمس تونس " اختراق البريد الالكتروني لرئيس الحكومة التونسية حمادي الجبالي ، وقالت إن ذلك يأتي احتجاجا على " عدم احترام الحكومة حقوق الإنسان وحرية التعبير " ، مهددة بنشر المزيد من الوثائق السرية .

أعلنت مجموعة متخصصة في اختراق مواقع الانترنت عن اختراق البريد الالكتروني لرئيس الحكومة التونسية حمادي الجبالي ، وسربت المجموعة ، التي تطلق على نفسها اسم : أبو نيموس تونس " ، على موقعها في شبكة الانترنت 2725 رسالة قالت إنها من سجل البريد الالكتروني الشخصي لحمادي الجبالي ، وقالت المجموعة في رسالة صوتية نشرتها أمس الأحد على شبكة التواصل الاجتماعي " يوتوب " : " قررنا نشر وثائق سرية لحركة النهضة ، تتضمن عناوين بريد الكتروني شخصية ، وأرقام هاتف ومعاملات مصرفية إضافة إلى فواتير (مالية) تم استخلاصها خلال الحملة الانتخابية " ، للحركة وأضافت أنها " احتفظت بجزء كبير من المعطيات السرية " للحكومة التونسية مهددة بنشرها على الانترنت " إن لم تحترم (الحكومة) حقوق الإنسان وحرية التعبير في تونس " ، ومن بين الوثائق التي سربت برقية من حمادي الجبالي إلى السفارة التركية تتضمن مرفقا بالسيرة الذاتية لرفيق عبد السلام ، وزير الخارجية الحالي ، ورسالة من عضو النهضة إلى حمادي الجبالي يقول فيه إن " التونسيين يمكنهم التصويت مرتين في الانتخابات مرة في الخارج ومرة في تونس " .

وقالت مجموعة " أنونيموس تونس " إن اختراق البريد الالكتروني للجبالي يأتي " احتجاجا " على " اعتداء " رجال الأمن السبت على عاطلين من خريجي الجامعات خلال تظاهرهم في العاصمة تونس تعيين محافظين موالين لحركة النهضة " وعلى " سكوت الحكومة " إثر "مهاجمة" سلفيين لفنانين ومسرحين تونسيين نهاية آذار / مارس الماضي ، وأضافت المجموعة أنها " احتفظت بجزء كبير من المعطيات السرية " للحكومة التونسية مهددة بنشرها على الانترنت " إن لن تحترم الحكومة حقوق الإنسان وحرية التعبير في تونس " .

وكانت المجموعة قد شنت هجوما الكترونيا الشهر الماضي على عدة صفحات إسلامية تونسية على " فيسبوك " ، من بينها صفحة لسلفيين ، وقالت المجموعة آنذاك في

رسالة صوتية نشرتها على موقعها الالكتروني إن عمليات القرصنة تأتي ردا على " سكوت الحكومة عن تجاوزات " الجماعات السلفية في تونس ، وأضافت في رسالتها مخاطبة السلفيين : " سنناضل ضدكم (....) سنترصد بريدكم الالكتروني وحساباتكم ومعاملاتكم البنكية ، وسنستنسخ أقراصكم الصلبة ، وهذه مجرد بداية (...) إن لم توقف الحكومة أعمالكم في الأسابيع القادمة ، سنقوم نحن بذلك " .

من جهتها ، لم تنف الحكومة التونسية اختراق الحساب الشخصي لحمادي الجبالي على الانترنت لكنها لم تؤكدها أيضا ، وفي سياق متصل قال رضا الكزدغلي ، المستشار الإعلامي لحمادي الجبالي ، لرويترز " ندرس الموضوع وسيتم إعطاء موقف في وقت لاحق (...) وسنحاول التأكد إن كان الحساب البريدي المقرصن (اخترق) قبل تولي السيد الجبالي رئاسة الحكومة أو بعدها " .

وتواجه الحكومة الحالية في تونس انتقادات واسعة بالتضييق على حرية التعبير والصحافة لكنها تؤكد أن تسعى لحماية الحريات وفقا لأهداف الثورة وأنها لا تسمح بتجاوز الخطوط الحمراء مثل المقدسات الإسلامية ، وقد تمت محاكمة صحفي بسبب نشر صورة امرأة عارية إضافة إلى استمرار محاكمة قناة نسمة الخاصة بعد بث فيلم إيراني يصور الذات الإلهية .

الملحق رقم 04

تأجيل محاكمة 43 شابا في قضية القرصنة الالكترونية الى أبريل .

قضت محكمة جنايات المنصورة الدائرة السادسة بتأجيل قضية القرصنة الالكترونية الى جلسة 2 أبريل القادم والمتهم فيها 43 مصريا بالاستيلاء على أموال من ثلاثة بنوك أمريكية عن طريق تزوير محررا الكترونية وتهمة غسل الأموال .

وتقدم عدد من أسر المتهمين بالتماس المحامي العام الأول بالمنصورة لتقديم موعد جلسة المحاكمة خلال شهر مارس القادم وذلك لتقصير فترة المحاكمة قبل بدء منتصف العام، حفاظا على مستقبلهم حيث يوجد بينهم 27 طالبا بالجامعة .

وأصدرت أسر المتهمين بيانيا قالوا فيه : " نناشد كل ذي صوت حر بعد أن رفع المواطن رأسه بعد ثورة التحرير من الفساد فلم يعد أمامنا سوى أن ننظر للمستقبل بأمل وهؤلاء الشباب المحبوسين الذين ضاعت عليه سنة من عمرهم الدراسي ومضى نصف العام الآخر بعد أن مكثوا في الحبس من تاريخ 2009/10/7 حتى الآن وذلك إرضاء للسطوة والهيمنة الأمريكية ، ولذلك فإننا نطالب بالإفراج عن هؤلاء الشباب فورا فلم يعد هناك مجال للشك في أنهم جزء من مستقبل مصر الحرة حتى لا تتأثر عقولهم الذكية من مجتمع الإجرام الذي يعيشون فيه داخل السجن " .

وأكد محمد نعمة الله ، المحامي ووالد أحد المتهمين ، أن النائب العام استجاب لإخلاء سبيل 5 شباب يوم 13 فبراير الجاري رغم اتهامهم بنفس الاتهامات في قضية أخرى تحمل رقم 14260 لسنة 2010 وتم تنفيذ القرار من رئيس المحكمة استئناف المنصورة " إلا أن أبناءنا محبوسون في سجن المنصورة ومر عليهم سنة ونصف تحت بند التحقيق ولم يتم اتخاذ قرار بشأنهم وكان أمامهم فرصة للهروب أثناء أحداث الثورة إلا أنهم لم يحاولوا الهروب وظلوا في السجن لأنهم متأكدون من براءتهم ولانهم كانوا أدوات لأيادي خفية .

الملحق رقم 05

قضية القرصنة الالكترونية بالدقهلية : دفاع المتهمين يطالب بالإفراج عنهم والكشف عن أسماء المجني عليهم وأرقام بطاقات انتمائهم .

الدقهلية رامي القناوي نشر في الأسبوع أنلاين يوم 02-10-2010 .

باشرت محكمة جنايات المنصورة صباح اليوم برئاسة المستشار أحمد رضا وعضوية المستشارين عفيفي منوفي وشريف محمد إبراهيم وحضور أحمد عبد الجواد رئيس النيابة وسكرتارية وليد العزاوي محاكمة 43 شابا في القضية المعروفة إعلاميا بـــ " القرصنة الالكترونية " .

حيث وجهت لهم المحكمة تهمة الاشتراك في جريمة غسيل الأموال والاستيلاء على أموال ثلاث بنوك أمريكية وتزوير محررات الكترونية وحيازة أسلحة ومخدرات ونفي المتهمين جميع الاتهامات الموجهة إليهم ، حيث طالبت هيئة الدفاع في الجلسات السابقة السماع للشهود الإثبات الواردين بأدلة الثبوت وهم العقيد وليد عبد السلام " رئيس التحريات بإدارة مكافحة الجرائم الحاسبات والمعلومات بوزارة الداخلية " وهم المقدم عبد الرحمن مصطفى حامد " بالإدارة العامة للتوثيق بإدارة مكافحة جرائم الحاسب الآلي " وايمن نبية عبد الفتاح وهدان والسيد وليد زكريا علي أحمد " مهندس كمبيوتر بالجهاز القومي لتنظيم الاتصالات وهؤلاء جميعا أعدوا تقارير للقضية .

كما صرحت المحكمة برئاسة المستشار أحمد رضا وعضوية المستشارين عفيفي منوفي وشريف محمد إبراهيم عاطف عباس وعبد المعطي صبري للدفاع عن المتهمين بتسلم صور من المرفقات الخاصة بتقرير اللجنة المشكلة من وزارة الاتصالات على أن يتم استبعاد الصفحات الواردة بها والتي تخص أرقام الحسابات البنكية والبطاقات الائتمانية ، وكذا تسلم صورة من مرفقات التقرير الفحص الفني بوزارة الداخلية إدارة مكافحة جرائم الحسابات وشبكات المعلومات بقسم المساعدات الفنية بعد سداد الرسم المقرر وعلى النيابة العامة ضم إيصال التحويل المنسوب إلى المتهم الثالث فريد أحمد البراوي المنوه عنه بمحضر جلسة أمس الأول وكذا ضم إيصالات التحويل الخمسة المنسوبة إلى المتهم السابع محمد عبد العزيز رضوان المنوه عنه بذات محضر الجلسة وعلى النيابة العامة إرفاق ترجمة من مرفقات خطاب الملحق القانوني بالسفارة الأمريكية المتضمن كشوفا بأسماء المتهمين الأمريكيين الذين تم ضبطهم بالولايات المتحدة الأمريكية والمؤرخ في 27 فبراير

الماضي وبما أنه تم بشأن التحقيقات معهم وما إذا كانت قد انتهت الى تقديمهم الى المحاكمة من عدمه .

وطالبت هيئة الدفاع من أخذ صور رسمية من المحكمة بالتحقيقات التي أجرتها كما طالبت سماع باقي الشهود النفي وهم لجنة الرقابة على البنوك وسؤالهم مع وجود لجنة حسابية من خبراء وزارة العدل وتسليمهم كشف للمتهمين الأمريكان باللغتين العربية والانجليزية بالإضافة إلى الإفراج عن المتهمين حيث أنهم طلاب خوفا على مستقبلهم الدراسي كما أنهم قضوا ما يقرب من السنة داخل الحبس وقانون الحبس الاحتياطي ينص على أنه لا يجوز الحبس أكثر من ستة أشهر على ذمة القضية واتهمت هيئة الدفاع هيئة الرقابة على البنوك بالفساد نظرا لوجود خلافات في إجراءات الفحص للمتهم الحادي عشر .

أوضحت التحقيقات أن السيناريو الكامل لتنفيذ الجريمة بدأ عن طريق استعمال المتهمين طرق احتيالية تبدأ بتزوير الصفحات الرئيسية للمواقع الالكترونية لبنكي " أوف أمريكا وويلز فاركو " بالولايات المتحدة الأمريكية واصطناع رسائل الكترونية وإرسالها إلى العملاء بحجة طلب تجديد البيانات الشخصية للعملاء ومن ثم استخدام تلك البيانات في الدخول على الحسابات البنكية الشخصية للعملاء وإجراء حجوزات فندقية وشراء تذاكر طيران وتحويلات بنكية بقيمة مليون و 117 مليون دولار أمريكي .. وكشف الفحص الفني للحواسب الشخصية للمتهمين عن احتواء الأجهزة على بيانات البطاقات الائتمانية لعملاء البنكين الأمريكيين وعشرات من الصفحات المزورة للبنكين ومئات من الرسائل الالكترونية المتبادلة بينهم وبين العملاء فضلا عن الايميلات الشخصية لعملاء البنكين وعشرات الأسئلة والأجوبة عن كيفية التعامل مع المواقع الالكترونية واختراقها ، فيما كشف الفحص الفني للهواتف المحمولة للمتهمين عن مراسلات بين المصريين والأمريكيين تتضمن اتفاقيات بشأن تحويل مبالغ مالية بين مصر وأمريكا وشمل قرار الإحالة كل من أيمن محمد إبراهيم " 20 سنة – طالب بكلية الحقوق " من محافظة الشرقية ، وإبراهيم صالح " 23 سنة – حاصل على بكالوريوس إدارة أعمال " ، وفريد احمد محمد أحمد " 27 سنة حاصل على بكالوريوس تجارة " ، ومحمود علي أحمد "هارب"، ومحمد فتحي السيد البسيوني"هارب"، ومحمد نهرو حمزة المهدي محمد21"ينة_ حاصل على معهد فني تجاري" ومحمد عبد العزيز محمد رضوان"19 سنة_ طالب بأكاديمية الدلتا"، ومحمد إسلام حمدي"21 سنة_ حاصل على بكالوريوس تجارة ونظم معلومات"، ومحمد حسن مصباح أحمد" 20 سنة_طالب بكلية

التربية"، ومحمد العربي راشد جاب الله"هارب"، وعمرو أحمد السيد أبو المعاطي" 25 سنة حاصل على بكالوريوس تكنولوجيا المعلومات"، ومحمد فكري محمد محمود"هارب"، ومحمد عبد الهادي طاهر"هارب".

كما شمل القرار كل من خالد جمال سعد حبيب "22سنة_طالب بكلية التجارة"، وحمدي حافظ عمر "هارب"، وحامد محمد توفيق"هارب"، وأحمد محمد أمين إبراهيم"24سنة_محاسب ببنك مصر"، وعصام علي ناصف عبد الصمد"23 سنة_حاصل على بكالوريوس علوم إدارية"، ودينا عبد الفتاح أبو الحسن"هاربة"، ومحمد أحمد راشد "24سنة_حاصل على الثانوية العامة"، وأحمد السيد أحمد العوضي" هارب"، وسامح يحي سعد يوسف"27سنة_سائق"، وحسام حسن محمود"هارب"،وعادل علاء الدين محمد الغريب"22سنة_طالب بكلية التجارة"، وهاني محمد أحمد سمرة 25سنة_حاصل على ليسانس حقوق"، ومعتز محمد جبر عبد الفتاح"21سنة_طالب بكلية التجارة ونظم المعلومات" وحسن حسن معوض"22 سنة_طالب بكلية العلوم"، وياسر مجدي شوقي"23سنة_ طالب بكلية الحقوق"، ومحمد سمير حلمي 20سنة طالب"

بالإضافة إلى ما سبق فقد شمل القرار أيضا كل من هيثم فتحي أحمد"22سنة حاصل على معهد الدراسات متخصصة، وعلي فكري علي محمد"هارب"، وإبراهيم جمال إبراهيم"هارب"، وخالد حمدي مصباح 21سنة طالب، ونادر مجدي شوقي" هارب"، وعبد الرحمان جاد أحمد محمد"هارب"، وأسامة محمد عطية 23سنة حاصل على بكالوريوس نظم معلومات"، ومحمد احمد إبراهيم 22 سنة حاصل على بكالوريوس إدارة أعمال، وبيشوي أوزوريس يوسف 19 سنة طالب بكلية الهندسة، وهشام صالح عبد العال" هارب"، ومحمد محمد محمود أحمد "22سنة عامل بشركة تركيبات أنترنت، ومصطفى أمين حسين"23سنة صاحب مصنع، وتعود أحداث القضية إلى 12أكتوبر 2009 عندما تمكنت أجهزة الأمن بوزارة الداخلية بالتنسيق مع قأسم جرائم الحاسبات بالولايات المتحدة الأمريكية بجهاز المباحث الفدرالية الأمريكية"اف ب أ ي" من الكشف عن التشكيل العصابي وضبط عدد كبير منه وإحالته للمحاكمة

الملحق رقم 06

40 قضية قرصنة الكترونية شهريا في المحاكم الأردنية

توقعت دراسة صدرت حديثة حصلت على "السبيل" على نسخة منها، أن تنفق الشركات على مستوى العالم ما يقارب 500مليار دولار خلال عام 2014 للتعامل مع المشكلات الناجمة عن البرمجيات الضارة التي يتم تحميلها بشكل متعمد مع البرمجيات المقرصنة.

ووفق ما وقفت عليه "السبيل" فان هناك نحو 40 قضية قرصنة الكترونية تقدم شهريا إلى المحاكم الأردنية.

وتوقعت الدراسة المشتركة التي أجرتها مؤسسة البيانات العالمية وجامعة سنغافورة الوطنية، أن ينفق المستهلكون على مستوى العالم 25مليار دولار، إضافة إلى 12مليار ساعة خلال هذا العام نتيجة للتهديدات الأمنية والإصلاحات المكلفة لأجهزة الكمبيوتر الناجمة عن البرمجيات الضارة المصاحبة للبرمجيات المقرصنة.

وكشفت الدراسة التي تحمل اسم "العلاقة بين البرمجيات المقرصنة واختراقات الأمن الالكتروني" عن أن 60 بالمائة من المستهلكين ممن تم استطلاع آرائهم قالوا أن أكثر ما يقلقهم من البرمجيات الضارة هو فقدان البيانات أو الملفات أو المعلومات الشخصية، تليها معاملات الانترنت غير المصرح بها بنسبة 51 في المائة، ثم سرقة حسابات البريد الالكتروني وشبكات التواصل الاجتماعي والبنوك بنسبة 50 في المائة، ومع ذلك فان 43 في المائة من هؤلاء المستهلكين لا يقومون بتنزيل تحديثات برامج الأمان والحماية ويتركون أجهزتهم معرضة لهجمات المجرمين الالكترونيين.

وقالت مديرة الملكية الفكرية في مايكروسوفت الأردن سناء جاسر" العديد من المواطنين في المملكة الذي لا يعون مدى الخطورة المترتبة على شراء برمجيات مقرصنة، فلا يدركون بأن استخدام هذه البرامج وبيعها يعد جريمة يعاقب عليها القانون. وفي ضوء ذلك، نحرص على حشد كافة الجهود لتعزيز وعي المجتمع حول القضايا، كما نعمل بالتعاون مع مختلف الأجهزة لإيجاد حلول فاعلة لمكافحة هذه المشكلة".

ومن جانبه قال أندريه جهل، محامي مكافحة القرصنة في شركة لمايكروسوفت": يلجأ العديد من الأفراد والشركات في الأردن لشراء برمجيات وأجهزة حاسوب من مصادر مشبوهة تزودهم ببرمجيات تحتوي على الفيروسات وقد وجدنا بأنه من بين 203 أجهزة حاسوب تضم برامج مقرصنة تم شراؤها في 11 دولة، احتوت على برمجيات خبيثة خطيرة."

الملحق رقم 07

شركة (TFI) :

أولاــ أطراف النزاع و اسم الموقع المتنازع عليه :

ثانيا ــ المدعي هو شركة (TFI) .

ثالثا ــ ضد المدعي عليه شخص قام بتسجيل اسم الموقع (TFI_ Video.com) .

رابعا ــ اسم الموقع المتنازع عليه (TFI_ Video.com) .

ثانيا ــ وقائع القضية :

برفع دعوى أمام مركزا لتحكيم و الوساطة التابع للوبيو و ذلك في 17 جانفي 2002 الشركة (TFI) تملك العلامة (TFI_ Video) و المسجلة سنة 1993 ، وهي المالكة لإسم الموقع (TFI_ Video) المدعى عليه بتسجيل اسم الموقع (TFI_ Video.com) في 06 أفريل 2001 و الذي ليس له أي حق من حقوق الملكية الصناعية على العلامة (TFI_ Video)

ثالثا ــ إدعاءات الطرفين :

1) **طلب المدعى :** أي الشركة (TFI) من الهيئة التحكمية إصدار قرار بنقل اسم الموقع(TFI_ Video.com) إليها أي الشركة (TFI) وكانت الحجج التي قدمتها هي:

- أن الشركة (TFI) تتمتع بالشهرة العالمية في عالم الإنتاج السمعي البصري.
- تقوم الشركة باستغلال العلامة (TFI) اكثر من 40 سنة .
- إن اسم الموقع(TFI_ Video.com) هو مطابق لعلامة و مطابقة لعلامة (TFI) .
- إن شركة (TFI) لم تمنح في أي وقت كان رخصة استغلال علامتها من طرف المدعي عليه .
- إن اسم الموقع(TFI_ Video.com) تم تسجيله بسوء نية ، فالمدعى عليه قام بتسجيل اسم الموقع لهدف وحيد وهو الحصول على أرباح مالية ، ولهذا الأسباب يطالب المدعى الشركة(TFI) من الهيئة التحكيمية إصدار قرار يأمر بنقل إليها اسم الموقع عليه (TFI_ Video.com) .

2) **دفعات المدعى عليه** :

- إن هدف المدعى عليه من قيامه بتسجيل اسم الموقع(TFI_ Video.com) هو إنشاء موقع على شبكة الانترنت خاص بأفلام الفيديو ، وكان في نيته أخبار الشركة التلفزيونية (TFI) لاحقا من أجل وضع شراكة تجارية معها .
- إن المدعى عليه تجهل تماما بوجود العلامة (TFI_ Video) التابعة لشركة(TFI) كما يجهل نشاطاتها على شبكة الانترنت .

رابعا ــ مناقشة القضية من قبل الهيئة التحكيمية :

وفقا لسياسة توحيد إجراءات حل النزاعات الخاصة بأسماء المواقع المنصوص عليها في تقرير المنظمة العالمية للملكية الفكرية بأسماء مواقع الانترنت لسنة 1999 يتوجب على تقديم أدلة ضد المدعى عليه بإن :

- اسم المدعى عليه يطابق أو يشابه العلامة التي للمدعى حقوق عليه.
- المدعى عليه ليس له أي مصلحة شرعية على اسم موقعه.
- اسم الموقع قد تم تسجيله و استعماله بسوء نية .

وبتطبيق هذه القواعد على النزاع يتبين أن :

- اسم الموقع المتنازع عليه يطابق علامة شركة (TFI) التي لها حقوق على العلامة (TFI_ Video) كما أنها تستعمل نفس التسمية لنشاطاتها على شبكة الأنترنت.
- المدعى عليه ليس له مصلحة أو حق شرعي على اسم موقعه ، و يتبين من ملفات الموضوع بأن المدعى عليه ليس له أي حقوق ملكية أو غيرها على العلامة (TFI_ Video) كما أن المدعى عليه لم يحصل على ترخيص من الشركة (TFI) باستغلال علامتها على شركة اسم الموقع .
- اسم الموقع المدعى عليه تم تسجليه بسوء نية .
- إن المدعى عليه قد اقترح شراكة تجارية مع الشركة (TFI) وهذا يدل على أنه لم يكن يجهل و جود الشركة و التي قد تم تسجيل اسم الموقع مع العلم بأن هذا الموقع يتشكل من حقوق هي ملك للغير ، فيعد هذا التسجيل قائم على سوء نية ، كما أن المدعى عليه لم ينفي قيامه بعرض بيع هذا الموقع للشركة (

TFI) كما أن عدم قيام المدعى عليه باستغلال حقيقي لاسم الموقع (_TFI Video.com) كل تسجيل قائم على سوء النية .

خامسا ــ القرار :

إذ يتوافر الشروط التي وضعتها الويبو من خلال سياسة إجراءات حل النزاعات الخاصة بأسماء الموقع على هذا النزاع قرار نقل اسم الموقع (TFI_ Video.com) إلى الشركة (TFI)وهذا بسبب أن تسجيل الشخص لاسم الموقع(TFI_ Video.com) قائم على سوء النية.

الملاحق