جامعة أكلي محند اولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

مكافحة جريمة القرصنة الالكترونية في القانون الجزائري

مذكـــرة لنيـــل شهـــــادة الماستر في القانون العام

تخصص: القانون الجنائي و العلوم الجنائية

إعداد الطالبة:
- بوديسة إيمان

تحت إشراف الأستاذ:
- د/ خالدي فتيحة

لجنة المناقشة

الأستاذ:خنيمي طارق.....رئيسا

الأستاذ: د/ خالدي فتيحة.....مشرفا ومقررا

الأستاذ:صغير يوسف.....ممتحنا

السنة الجامعية: 2020/2019

شكر وعرفان

بسم الله الرحمن الرحيم

" فَتَبَسَّمَ ضَاحِكًا مِّن قَوْلِهَا وَقَالَ رَبِّ أَوْزِعْنِيٓ أَنْ أَشْكُرَ نِعْمَتَكَ ٱلَّتِيٓ أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَٰلِدَيَّ وَأَنْ أَعْمَلَ صَٰلِحًا تَرْضَىٰهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ ٱلصَّٰلِحِينَ".

سورة النمل الآية 19

الشكر لله عز وجل على نعمه

أتقدم بالشكر الجزيل إلى أستاذتي الفاضلة **" خالدي فتيحة"** على نصائحها وتوجيهاتها التي أنارت دربي والتي لم تبخل علي بمراجعها ومعلوماتها القيمة.

كما لا يفوتني أن أتقدم بالشكر والتقدير إلى لجنة المناقشة.

كما أتوجه بالشكر إلى كل الزملاء والأصدقاء خصوصا الأخت " بوزيدي آسيا"، و" رشيدة".

وكل شكر إلى كل من ساهم في إنجاز عملي هذا سواء بمعلومة أو نصيحة أو كلمة طيبة.

إهداء

ربي إذا أعطيتني نجاحا فلا تأخذ تواضعي، وإذا أعطيتني تواضعا فلا تأخذ اعتزازي بكرامتي.

أهدي هذا العمل المتواضع إلى الصدر الدافي والقلب العطوف رمز الصبر والتضحية الجوهر الثمينة :" أمي" الغالية.

إلى من علمني أن أرسم الوجوه المستنيرة وسقاني كؤوس الكفاح وكان القدوة في النضال وحسن مثال صاحب الشهامة " أبي" وجدي رحمهما الله وأسكنهما فردوس الجنة والنعيم.

إلى تيجان رأسي ومصدر همتي وفخري إخوتي وأخواتي الأعزاء " فارس، سيد أحمد، وشمس الدين، وإلى إبنتا أخي الكتكوتة الصغير " أسيل إليس".

إلى زوجي وعائلته، وإلى عائلة بوديسة وطير وزياني.

والى جميع طلبة السنة الثانية ماستر قانون جنائي،

والى جميع هؤلاء أهدي ألف شكر

المقدمـــة :

تتوالى العصور والأزمات على البشرية ويتوالى معها لتطور والازدهار وزيادة المعرفة بما يحيط بالإنسان ومدى قارئه على الاستفادة مما هو متوفر في بيئته.

وبعد الثورة الصناعية الكبرى في القرن التاسع عشر كان لابد من تتويج هذه المرحلة بالاكتشافات تخدم الإنسانية جمعاء أو تحقق ذلك فعلا باختراع الحاسوب الآلي الذي ولج صالحا كل الميادين الصناعية والتجارية والطبية والعلمية وحتى العسكرية بل وتعدى الأمر ذلك بكثير لدرجة أصبح من المستحيل الاستغناء عن الحواسيب في أي مكان حتى في المنازل.

ومع اختراع الحاسوب كان هناك اختراع آخر لا يقل شأنا وأهمية عنه ألا وهو وسائل الاتصالات وكان هذان الاختراعان يتطوران ويتقدمان بخطى ثابتة نحو الأفضل كلا على حده، لحين اندماجها في خط واحدمع استخدام تقنيات الشبكات السلكية واللاسلكية .

وبعد أن تحول العمل اليدوي إلى الحاسوب الذي يرتبط عادة بحواسيب أخرى عبر شبكات صغيرة أو كبيرة، أصبحت المعلومات في خطر دائم لأن اختراق أي جهاز يعني إمكانية الدخول إلى الأجهزة الأخرى التي ترتبط عبر شبكة واحدة، هذا الأمر جعل العالم ينفتح على نوع جديد من الجرائم والتي تعرف بسرقة المعلومات أو كما يصطلح عليها "بالقرصنة الالكترونية"، التي أصبحت تشكل جناية لا تقل خطورة وتأثيرا عن باقي أنواع الجرائم.

والقرصنة الالكترونية عدة أشكال منها ما يهدف إلى سرقة بيانات من حاسوب معين ومنها ما يهدف إلى التخريب فقط كمسح البيانات على سبيل المثال، وهذه الأهداف تعتمد على طبيعة المخترق فإذا كان هاويا فإن أعماله لا تجاوز

التجربة ومحاولته التعلم أكثر أو حتى مجرد الاطلاع وهذا النوع يكون خطيرا جدا لأنه قد يتسبب بحذف أنظمة كاملة دون أن يعلم كما أنه يترك اثرا محسوسا على النظام الذي اخترقه، أما إذا كان محترفا فإن الأمر يختلف كثيرا لأنه يدرك جيدا ما يفعله ويكون له هدف محدد فعلى سبيل المثال يستطيع وعبر ثغرة معينة الدخول على أرقام الحسابات المصرفية في بنك ما ويستطيع عبر عدة إجراءات تحويل مبالغ مالية إلى رصيده الشخصي أو إلى أي زبون آخر لذلك المصرف دون أن يشعر الآخرين بذلك، أو العبث في الأنظمة الالكترونية التي تستخدم في المطارات مما يسبب ارباكا كبيرا في حركة الطيران. كما يمكن اعتبار النسخ غير المشروع لبرامج الحاسوب شكلا من أشكال القرصنة كونه يسلب حق المنتج الأصلي ويعرضه لخسائر كبيرة.

وبوجود الشبكات الدولية "الانترنت" أو المحلية أصبحت الحواسيب المرتبطة بهذه الشبكات عرضة للاختراق وأن كافة محتوياتها عرضة للسرقة أو التخريب.

وسنحاول في هذا البحث التطرق للقرصنة كجناية خطيرة ومؤثرة على جميع أطياف المجتمع تصل إلى حدود فوق التصور.

تتمثل أسباب اختيار الموضوع في رغبة الباحث في التعرف على جريمة القرصنة الالكترونية بالنظر لكونها تمثل خطورة وهي من العمليات البارزة في هذا الميدان، حيث تعتبر القرصنة سلاحا والقراصنة جنودا تقنيين يخترقون الشبكات والمواقع.

يرجع سبب اختيار الموضوع من الناحية الموضوعية إلى الدور الهام في دراسة جريمة القرصنة الالكترونية باعتبارها من الجرائم التي تشهد الجديد كل يوم مع المخاطر الأمنية المتزايدة.

ينبع الهدف من دراسة ضاهرة القرصنة الالكترونية و التعرف على جوانبها بإعتبارها عملية خطيرة و غير شرعية و غير أخلاقية و محاولة الوصول لطرق لمكافحة هته الجرائم، و يجد المحقق نفسه في حيرة أمامها و كيفية التعامل معها و أسلوب التحقيق فيها، إذ لاشك أن إجراءات التحقيق و جمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

و بصدد البحث في هذه الإشكالية الجوهرية يعتبر البحث فيها أمرا ضروريا للإجابة عن جوهر موضوع الدراسة، و من هذا المنطلق نطرح الإشكالية التالية:

كيف تصدى المشرع الجزائري لجريمة القرصنة الالكترونية ؟

من أجل الإجابة عن التساؤل المطروح اعتمدنا على المنهج الوصفي التحليل الذي يتناسب مع موضوع الدراسة من خلال وصف جريمة القرصنة الالكترونية وتحليلها لتحديد أشكالها وأركانها وأساليب البحث والتحري في جريمة القرصنة الالكترونية ومحاولة الوصول إلى آليات لمكافحتها.

و سأقسم هذا البحث إلى فصلين، نتناول في الفصل الأول الاطار المفاهيمي لجريمة القرصنة الالكترونية، و اخصص الفصل الثاني إلى الجوانب الموضوعية و الجوانب الإجرائية لجريمة القرصنة الالكترونية.

الفصل الأول:

الإطار ألمفاهيمي لجريمة القرصنة الالكترونية

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشرع للكمبيوتر كأداة لارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها لتنصب بالقول أننا أمام عولمة الجريمة وإن كان في نطاق تطبيق نصوص القانون الجنائي إلا أنه يجب ان نعترف أننا بصدد ظاهرة إجرامية ذلك طبيعة خاصة تتعلق بالقانون الجنائي سواء من حيث محل الجريمة أو أسباب ارتكابها الأمر الذي يصوغ لهدم محاولة اختراق نظم الشبكات المتخصصة ما يطلق بالقرصنة الالكترونية والتي أصبحت اليوم هاجسا أمنيا يتحدى قيام الحكومة.

سنتعرف من خلال هذا الفصل على الإطار المفاهيمي لجريمة القرصنة الالكترونية من خلال مبحثين، نتطرق في المبحث الأول على مفهوم جريمة القرصنة الالكترونية وفي المبحث الثاني خصائص وأنواع جريمة القرصنة الالكترونية.

المبحث الأول:

مفهوم جريمة القرصنة الالكترونية :

كثر الحديث في عصرنا الحاضر عن القرصنة الالكترونية فأصبح من الطبيعي سماع هذا المصطلح أو قرصنة البرامج أو القرصنة المعلوماتية وغيرها من المصطلحات المرادفة لهذه التسميات والقرصنة بمعناها الدقيق هي كل عمل عنف غير مرخص به، إلا أن لفظ القرصنة في وقتنا الحاضر أصبح وصفا يطلق على نهب المصنفات المنشورة للغير من خلال الحصول على نسخة منها دون الحصول على موافقة مالكها.

المطلب الأول :

تعريف جريمة القرصنة الالكترونية :

تعددت التعريفات التي تناولت جريمة القرصنة الالكترونية ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة وهذا ما سنحاول التطرق اليه نشأة القرصنة الالكترونية.

الفرع الأول :

نشأة القرصنة الالكترونية :

بدأت ظاهرة القرصنة والاختراق مع بداية ظهور المحاسبة الالكترونية وازدادت بشكل كبير مع استخدام قنية الشبكات[1]، حيث يشمل الاختراق الهجوم على شبكات الحاسوب من قبل مخترقي الأنظمة والمواقع الالكترونية ومنتهكي القوانين، غير أن القرصنة لا تمس الشبكة العنكبوتية فقط، بل تمتد إلى تقنيات أخرى كالاتصالات، والبرمجيات، ذلك أن عمليات القرصنة

[1] عبابسة فاروق ، عبوب خديجة، القرصنة الالكترونية فب الجزائر و أثرها على المستخدم ، مذكرة لنيل شهادة الماستر في علوم الاعلام و الاتصال ، جامعة مستغانم، ص41.

تطورت بسرعة فائقة، وأصبح من الشائع جدا العثور على مواقع بالأنترنت خاصة لترويج البرامج المقرصنة مجانا او بمقابل مادي رمزي.[1]

في هذا الاطار تشير البيانات إلى أن قرصنة البرامج أدت إلى خسائر مادية باهضة جدا، لذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وانشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات، من أبرز هذه التنظيمات، اتحاد برمجيات الأعمال Bisines Saftware Allionceأو ما تعرف اختصارا بـ ASA والتي أجرت دراسة تبين منها ان القرصنة على الانترنت ستطغى على أنواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الانترنت، ومنا تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الانترنت لمعرفة مدى استخدام المتصفح للمواقع لبرامج مقرصنة، إلا أن تلك الشركات تراجعت عن هذا التهديد إثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الانترنت.

قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لإبلاغهم عن أي الموقع مخصصة للبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكاوي ضدهم ومقاطعتهم إن أمكن أو اقفال تلك المواقع على الأقل.

إن القرصنة كظاهرة عالمية لا تختلف عن تلك التي يعرفها العالم العربي إذ أنها لم تسبقها بخطوات كبيرة، خاصة في ظل عدم حقوق الحماية الفكرية أو عدم جدية تطبيق هذه القوانين إن وجدت.

إن تاريخ القرصنة معروف جدا، حيث تم تسجيل العديد من الحالات التي أخذت زحما إعلاميا كبيرا، في هذا الاطار يمكن سرد أهم حالات القرصنة التي حدثت عبر التاريخ كما يلي

- في عام 1985 قتم شخص يدعى "روبيرتو سوتر" كولومبي الجنسية بسرقة على تيلكس حكومي، ليرسل مجموعة رسائل عبره على مصاريف في المملكة المتحدة وكنها على

[1]عبابسة فاروق ، عبوب خديجة، المرجع نفسه، ص42.

دول أخرى ونتج عن هذه الرسائل نقل 13,5 مليون دولار من أرصدة الحكومة الكولومبية Worm.

- وفي عام 1988 قام أحد طلاب جامعة "كورل" بزراعة برنامج في شبكة حواسيب حكومية انتشر خلالها في حاسوب وبعد ان تم كشفه تم طرده من الجامعة وحكم عليه بإيقافه على العمل 3 أعوام وتغريمه بمبلغ 10000 عشرة آلاف دولار.
- تعتبر« cirty bonus» مجموعة من القراصنة الروس قامت بنقل مبلغ 10 ملايين دولار إلى حسابات مصرفية في مختلف دول العالم في عام 1994، حيث كان زعيم العصابة "فلادمير ليفين" باستخدام حاسوبه الشخصي لتحويل الأموال على حسابات في كل من فلندا وإسرائيل، وقد تم بإيقافه في الولايات المتحدة الامريكية وحكم عليه بالسجن لمدة ثلاث سنوات[1].

الفرع الثاني :

التعريف القانوني للقرصنة الالكترونية :

يشير مفهوم القرصنة الالكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة(المصنفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها. عبارة أخرى القرصنة ماهي سوى عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الالكترونية أي أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته. بقصد المساس بالسرية او المساس بسلامة المحتوى والتكاملية. أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها. فهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله. فالقرصنة إذن تعني الوصول بطريقة غير مشروعة من خلال ثغرات في نظام الحماية الخاص بالهدف.

[1] .عبابسة فاروق، عبوب خديجة، "القرصنة الالكترونية في الجزائر واثرها على المستخدم"، شهادة الماستر في علوم الاعلام والاتصال، مستغانم، ص41/40.

ويقم بعملية القرصنة أشخاص هواة او مترفين، تم تعريفهم كالتالي: أشخاص لهم القدرة على التعامل مع أنظمة الحاسوب الآلي والشبكات، بحيث تمون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية، اتخذت لحماية تلك الحاسبات أو الشبكات، "وهؤلاء المخترقون يتم تصنيفهم إلى نوعين: أولهما هم الهاكرز "HAKERS" وهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات، أيا كانت إجراءات وبرامج الحماية التي تم اتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من تم على الإضرار نتيجة اختراق جهازه أو شبكته. أما الكراكز "CRACKERS" فهؤلاء يطلق عليهم المخربين، هم يتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحماية، إلا أهم يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحسابات والشبكات[1].

كما يمكن كذلك تعريف القرصنة الالكترونية على أنها" عملية اختراق الأجهزة الحاسوب أو المواقع تتم عبر شبكة الانترنت غالبا لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط بها اكثر من جهاز حاسب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في اختراق برامج الحاسوب وطرق ادارتها أي أنهم عبر مجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين للتعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة[2].

المطلب الثاني:

مظاهر وأسباب جريمة القرصنة الالكترونية :

من خلال دراستنا لجريمة القرصنة الالكترونية و نشأتها سوف نتطرق في هذا المطلب على إبراز مظاهر القرصنة الالكترونية في (الفرع الأول)، و أسباب القرصنة في (الفرع الثاني)، و تفصيل كل نقطة على حدة.

[1]. منير محمد الجنبهي، ممدوح محمد، "جرائم الانترنت والحاسب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، الاسكندرية، ص28.
[2]. عبابسة فاروق، عبوب خديجة، نفس المرجع السابق، ص43.

الفرع الأول :

مظاهر القرصنة الالكترونية :

من خلال ما سبق يتضح لنا عدة مظاهر للقرصنة الالكترونية تتمثل في تقليد برامج الحاسوب ،نسخ برامج الحاسوب و أخيرا أسلوب الهندسة العكسية.

أولا:

تقليد برامج الحاسوب : يقصد بتقليد برامج الحاسوب محاكاة برنامج معين يصنع أو انتاج نسخ على مثاله بحيث تبدو عند تسويقها كالأصل.

ثانيا:

نسخ برامج الحاسوب: وتعد هذه المصورة أهم صور القرصنة على البرامج وتتمثل في عملية النسخ الكلي أو الجزئي سواء عن طريق المحاكاة أم النسخ المباشر، حيث تقوم بعض الشركات بنسخ البرامج وبيها دون ترخيص الشركات المنتجة، ويتم كذلك سرقة البرنامج الأصل عن طريق إزالة معالم وتغيير هيئته وإعادة تجهيزه على نحو يبدو كمنتج جديد[1].

هناك نوعان يمكن أن يرد بها نسخ البرامج هما النسخ المباشر أو ما يطلق عليه النسخ الحرفي، ويقصد به قيام مرتكب هذا الفعل بنسخ البرنامج بصفة كاملة أو بيعه دون الحصول على ترخيص بذلك من الجهات المعنية، كما تشمل القرصنة النسخ غير القانوني للبرامج ويقصد به كل استخدام غير مسموح به للبرامج.

ثالثا:

أسلوب الهندسة العكسية: يقصد به قيام بعض الشركات المتخصصة في تصنيع وإنتاج أجهزة لأداء وظائف معينة تؤديها أجهزة أخرى موجودة في الأسواق، حيث تكون الطريقة

[1] منير محمد الجنبيهي، ممدوح محمد، جرائم الانترنت و الحاسب الالي و وسائل مكافحتها ، دار الفكر الجامعي ،الإسكندرية، ص28.

المتبعة في تصنيع وإنتاج الأجهزة الجديدة مختلفة عن طريقة تصنيع أو انتاج الأجهزة الأصلية[1].

الفرع الثاني :

أسباب جريمة القرصنة الالكترونية :

يختلف مرتكبو جرائم المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الاجرامي، لكن النهاية يبقى الطرفان مخالفين للقانون لذى يستحقوا العقاب بما اقترفوا من الجرائم ونام عدة أسباب تدفع لارتكاب الجرائم المعلوماتية يمكن أن نختصرها في الآتي :

أولا:

- **حب التعلم :**

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع لارتكاب مثل هذه الجرائم لأن المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب أن لا تبقى في المعلومات حكرا على أحد أي أن للجميع الحق بالتعرف والاستفادة من هذه المعلومات.

ثانيا:

- **التسلسل واللهو :**

عدد غير قليل من مخترقي الأنظمة يعتبرون من عملهم هذا وسيلة للمرح والتسلية وتقضية أكبر وقت ممكن في مواقع وحواسيب آخرين ويكون هذا الاختراق غالبا سلبيا يحدث تأثير على المستخدم.

[1].عايد رجا الخلايلة، "المسؤولة التقصيرية الالكترونية، المسؤولة الناشئة من إساءة استخدام الفرد الحاسوب والانترنت"، دار الثقافة للنشر والتوزيع، ط1، الإصدار الأول، 2006، ص3/2/1.

ثالثا:

- **الدوافع الشخصية :**

يعتبر محيط الانسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته وغالبا ما تدفع المشاكل الشخصية إلى رغبة بالانتقام ووجود أنظمة الكترونية تسهل له القيام برغباته فيعبث بمحتوياتها إلى درجة التخريب أو يكون الدافع التحري واثبات الجدارة أمام الآخرين بحيث يفتخر هذا الشخص بأن استطاعته اختراق أي حاسوب أو أي موقع ولا يستطيع أحد الوقوف بوجهه[1].

المبحث الثاني:

تصنيف جريمة القرصنة الالكترونية :

من خلال ما سبق ذكره عن مفهوم القرصنة الالكترونية في المبحث الأول سوف نتطرق في هذا المبحث على دراسة أنواع القرصنة الالكترونية في (المبحث الأول)، و دراسة القرصنة الالكترونية في الجزائر و أشهرها في (المبحث الثاني).

المطلب الأول:

أنواع جريمة القرصنة الالكترونية :

إن أفضل تصنيفات قرصنة الانترنت هو ذلك التصنيف الذي أورده "ويليم فوستروخو دافيدكوف" في مؤلفهم جرائم الكمبيوتر، حيث تم تقسيم قراصنة الانترنت إلى قسمين :

1. الهاكار:

وهم المتطفلون الذين يتحدون أمن النظم المعلوماتية والشبكات من خلال الدخول على أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية

[1].عبابسة فاروق، عبوب خديجة، المرجع السابقً 22.

الموضوعة لهذا الغرض، وفي الغالب لا يكون لديه دوافع حاقدة وتخريبية وإنما ينطلقون من هدف اكتساب الخبرة أو بدافع الفضول أو بمجرد التحدي واثبات الذات.

2. الكراكر:

هم أشخاص يقومون بالتسلل على أنظمة المعالجة الآلية للاطلاع على المعلومات المخزنة بها لإلحاق الضرر أو العبث بها أو سرقتها وذلك بهدف التحدي الإبداعي، تتميز هذه الفئة بصفة الخبرة والإدراك الواسع للمهارات التقنية لذلك فقد أثبت الواقع العلمي أن الهاكر يستعين بالكراكر إذا ما صادفه أي نوع من أنواع الحماية، وغاليا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة[1].

حيث يعتمد الكثير من مستخدمي الانترنت من الفضوليين إلى التسلل أو اختراق أجهزة أشخاص أو مؤسسات دون إستأذان، فيبدأ بعضهم على سبيل التجربة والفضول، وعندما يتمكن من يعجبه الأمر وينساق فيه إلى حد بعيد، فيدخل أجهزة مستخدمي الانترنت لا يعرفهم شخصيا ولا يعرف حتى مكان تواجدهم لسرقة أسرارهم والاستيلاء على ملفاتهم الخاصة أو للتخريب، ويتحول بذلك فضول عابث على اختراق احترافي قد لا تصده حتى برامج باكتشاف حدوث الاختراقات والحماية منها [2].

ولقد كثر الحديث عن وقائع عملية كما في حالته اختراق أحد الصبية الذي يبلغ من العمر 14 سنة نظام الكمبيوتر العائد للبنتاغون، و الأخر لا يتجاوز 17 سنة تمكن من إختراق كمبيوتر العديد من المؤسسات الاستراتيجية في أوروبا و الو.م.أ.

و لعلى البسمة المحيّرة لقراصنة الانترنات هو تبادلهم المعلومات فيما بينهم و تحديد التشارك في وسائل الاختراق و آليات نجاحها و اطلاعهم لبعضهم البعض على مواطن الضعف في نظم الشبكات و الكمبيوتر، حيث تجري عمليات التبادل للمعلومات فيما بينهم و بشكل رئيسي عن طريق النشرات الإعلامية الالكترونية و مجموعات الأخبار.

[1].مصطفى حمد موسى، "التحقيق في الجرائم الالكترونية"، مطابع الشرطة، ط1، ص15.
[2]. عمر يوسفي، "التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة دراسة وصفية تحليلية"، شهادة الماجستير، 2008، ص127.

أهم طرق اختراق الحاسوب:

تتم اغلب عمليات الاختراق عن طريق زرع برنامج معين في جهاز الضحية، يقوم هذا البرنامج بعمل معين كما يلي :

* الفيروسات: هو برنامج له القدرة على نسخ نفسه أكثر من مرة و يمتاز بقدرته على التخفي و له أثار تدميرية على أنظمة تشغيل الحاسوب لان عملية النسخ و التكرار الدائم لملفاته تجعل هاته الملفات تحل محل الملفات الأصلية الموجودة على القرص الصلب للحاسوب.

* أحصنة طروادة: هو برنامج تجسسي بعمل معين يحدده الشخص الذي صممه أو زرعه في جهاز الضحية يمكنه منت الحصول على مبتغاه.

* الديدان: هو برنامج ينتقل غالبا عبر البريد الالكتروني و يمتاز بقدرته على التنقل عبر شبكات الانترانت لغرض تعطيلها أو التشويش عليها عن طريق شل قدرتها على تبادل المعلومات.

4.القنبلة المعلوماتية information Bomp:

هو برنامج يصنعه مصمم النظام نفسهن لغرض انهاء مدة عمل ذلك النظام خلال وقت معين، أو في حال استخدام أرقام او أحرف معينة يحددها المصمم.

5.الفخ Trappe:

هو منفذ يتركه مصمم البرنامج يسهل له عملية الدخول إليه وقت ما يشاء واجراء التعديلات التي يريدها[1].

[1].عبابسة فاروق، عبوب خديجة، نفس المرجع السابق

المطلب الثاني :

القرصنة الالكترونية في الجزائر و أشهرها:

القرصنة الالكترونية في الجزائر يمكن أن تدخل على المدى القريب والمتوسط من مؤثراتها، فتأثيرها يشابه الزمة المالية العالمية المستفعلة حاليا فقد تم دق ناقوس الخطر بمناسبة احتفال تسليم شهادات الكفاءة لممثلي شركة lp baick في ميدان أمن الشبكات المعلوماتية حيث أوضح ممثلوا هذه الشركة أن خدماتها تضمن أقصى الأمن في تسيير شبكات المؤسسات[1].

أما في الجزائر فأرادوا ممثلوا شركة LP Baick، اجراء عملية تحسيس حول ظروف واشكالية تأمين شبكات المعلوماتية في الجزائر ثم مناقشتها بقوة، حيث اوضحوا أن في الجزائر خطر الاعتداء المعلوماتي، واضحوا أن خطر الاعتداءات المعلوماتية ضد مواقع رسمية جزائرية يشكل تهديدا واقعا، ولحد الآن لا يوجد أي برنامج خاص بالجزائر مما يثير مخاوف أن تكون منظومتنا المعلوماتية لدى المؤسسات المقرصنة أو معتدي عليها، وأضافوا أن أخطار القرصنة في الجزائر موجود في أي زمان ومكان ومنذ عامين تمكن الجزائريون من حل شفرةTps رغم أنه حتى ذلك الحين كان الروس هم في الطليعة هذا الميدان.

كما أوضح الرئيس المدير العام لشركة التعليم والتكوين "نوار حرز الله" بأنه منذ وقت قريب فإن المواقع الالكترونية لمؤسسات الدولة كانت مستهدفة في كل حين موضحا بأن عدد الاعتداءات على مختلف مواقع Web قد بلغت 3000 اعتداء في الشهر، وفي هذا الميدان فإن بعض المعقدين أو الهاكرز يظهرون وبعضهم يبدي افتخارا بإمضاء قرصنة لأكبر عدد من المواقع وذلك الغرور تسبب لهؤلاء الأشخاص بعقوبات مستحقة[2].

إن المتتبع لظاهرة القرصنة الالكترونية في الجزائر يدرك التناقض الذي يميز هذه الظاهرة، ففي حين لا يزال تصنيفها في مؤخرة التقنية التكنولوجية، تبقى تحتل المراتب الأولى

[1] عبابسة فاروق، عبوب خديجة، المرجع نفسه ص28.
[2] عبابسة فاروق، عبوب خديجة، المرجع نفسه ص29

في مجال القرصنة الالكترونية، حيث تشير التقارير والمعطيات المنشورة من قبل الهيئات المختصة والصحافة الوطنية إلى أن الجزائر تأتي على رأس البلدان العربية في ميدان القرصنة.

كما أنه اختراق البرامج المعلوماتية يهم القراصنة الجزائريين وذلك لنزع الشفرة لباقات القنوات التلفزيونية الرقمية مثلا، فعلى سبيل المثال فإن منتدى التبادل شفرات الدخول للباقات التلفزيونية المشفرة فإن الجزائريون يوجدون على رأس القائمة، في متوسط 40 ألف متصل يوميا، 9 الاف منهم جزائريون ويستعملون القرصنة كلمات سرية عن طريق برامج معروفة في هذا الميدان والمتواجدة في السوق الوطنية.

ويرى الخبير في مجال التكنولوجيا الاعلام والاتصال السيد "قرار يونس" أ تطور تقنيات الاعلام والاتصال صاحبته أضرار منها القرصنة الالكترونية وفي السياق ذكر المتحدث أن درجة خطورة القرصنة في الجزائر قليلة مقارنة بمثليتها من الدول خاصة في مجال التجارة الالكترونية التي لم تشرع بعد في استعمالها، إلا أنه ألم بضرورة التفكير من الاف في تنظيم هذه العملية وتحصين المواقع وتأمينها من خلال التطبيق الصارم للإجراءات خاصة ما تعلق بقرصنة البرامج، حيث يبقى تطبيق عقوبات على المخالفين متفاوت رغم أن القانون يمنع أي نوع من القرصنة سواء كانت الكترونية أو كلاسيكية.

وحسب السيد "قرار" فإن التكتم عن ظاهرة القرصنة وعدم التبليغ وتقديم شكاوي عن حالات القرصنة خوفا من المشكل التي قد يواجهها القائمون على الانترنت يبقى عائقا أمام محاربة الظاهرة[1].

من جهتها قالت باحثة هجيرة بودر بمركز البحث في الاعلام العلمي والتقني أن القرصنة الالكترونية في الجزائر منتشرة بصفة واسعة وبأن معظم البرامج المستعملة من قبل الجزائريين هي برامج مقرصنة ابتداءا من أنظمة التشغيل منها نظام "الونداوس" ومختلف طبعاته المستعملة وذكرة المساء أن استعمال البرامج الغير المقرصنة يعد جد ضئيل في الجزائر ويقتصر عن بعض مؤسسات الدولة والذي يبقى غير كاف لأن البرامج المقرصنة تباع في

[1] عبابسة فاروق، عبوب خديجة، المرجع نفسه ص30.

الأماكن العمومية بدون حسيب أو رقيب وتقتني بسهولة، كما أن الاقبال عليها واسع نظرا لثمنها الزهيد مقارنة بتلك الأصلية.

يعود ذلك كما أضافت إلى عدم استيعاب أهمية الأمن المعلوماتي والثغرات والعيوب التي تحتوي عليها البرامج المقرصنة والتي تصدر أمن الأنظمة المعلوماتية بينما يجب حسبها التهاب نحو مصادر المجانية "Open Sonrce" المعروفة بأمنها وإمكانية معرفة ثغراتها[1].

يعد الهويات المستعارة على غرار موريش، ماستر، أوكسيد، ماكسي32، هيزوكا4، أنجل25، دي زاد، من أشهر الأسماء المستعارة والرموز التي تشير إلى قراصنة الانترنت في الجزائر، كما أنهم معروفين في العالم اجمع عبر الشبكة العنكبوتية بفريق "دي زاد:Team x"، وقد استطاع هذا الفريق وهم من الشباب العبقري في مجال التحكم شبه الكامل في تقنيات وأسرار الاعلام الآلي إلى درجة سمحت لهم باختراق أكثر المواقع تحصينا في أي بقعة على الكرة الأرضية، لاسيما منها الإسرائيلية والصهيونية العنصرية.

القرصان "أنجل" الذي يسكن بإحدى ضواحي عاصمة الشرق قسنطينة وهو من مواليد 1976 حيث بلغ عدد اختراقاته في هذا المجال أزيد من 150 موقع دمرها جميعا ووضع بديلها عبارات نفكس موقفة من تلك المواقع، ومن بين المواقع المخترقة هي مواقع إسرائيلية، وماقع دانماركية، وقد أوضح القرصان "أنجل" المتخرج من جامعة قسنطينة في مجال الطاقة والذي تعلم وأتقن تقنيات الاعلام الآلي أنه اخترق مواقع هولندية مساندة لإسرائيل المغتصبة للأراضي العربية، إضافة إلى مواقع شيعية إيرانية .

هناك أيضا القرصان الجزائري "Hisok 4" "هيزوكا" والقاطن بولاية مستغانم هذا القرصان تمكن بمفرده من اختراق آلاف المواقع في العالم أجمع وهو من أخطر وأقوى القراصنة المعروفين في العالم والدليل على ذلك ورود اسمه في مئات المواقع المدمرة من طرفه[2].

[1]. عبابسة فاروق، عبوب خديجة، مرجع سابق، ص29.
[2] عبابسة فاروق، عبوب خديجة، المرجع نفسه ص31-32.

كما يوجد قرصان جزائري آخر والذي يعرف بـ"CO2" وهذا أيضا يعد من أشد القراصنة ذكاء وفتكا، ويبقى زها أخطر القراصنة الجزائريين على الاطلاق هو الذي رسم لاسمه أيضا بـ"Crusty" حيث تمكن هذا القرصان من تدمير أزيد من ثمانية ألاف موقع في مدة زمنية محدودة وبإبلاغ صوت المستضعفين إلى العالم من المظلومين في فلسطين خاصة، هناك أيضا قرصان من مدينة المدية والذي يملك شهادة في الدراسات التطبيقية الجامعية لإعلام الآلي للتسيير حيث يملك ألقاب عديدة يعرف بها من بينها Danki، ناس ملاح وقباح، سرمد، ذبيح القدر، أما في قرصنة الأجهزة فيعرف باسم فتة لم يرد أن يفضحعن الاسم وعن أسباب قيامه بعمليات القرصنة قال لنا "سرمد" أن الدوافع الأولى هو حب التطفل والاطلاع على المعطيات الشخصية للآخرين.

أما بالنسبة إليه فلقد كانت بينه وبين مجموعة من الشباب التحدي حيث أنهم استهانوا به وانقصوا من قدراته العلمية وبأنه شخص غير كفؤ لممارسة الاعلام الآلي وكانت تلك البداية وقد وضح "سرمد" أنه يوجد أنوع للقرصنة ، فهناك قرصنة على الأجهزة والقرصنة على المواقع، وقد أعطى لنا مثال تطبيقي على كيفية قرصنة موقع الكتروني كما صرح الهاكر عن المواقع الأكثر استهدافا من طرفه حيث قال بأنه استهدف المواقع التي تهين شخص النبي صلى الله عليه وسلم، إضافة إلى مواقع مصرية عندما كانت الحرب الالكترونية بيننا وبينهم، إضافة إلى بعض المستندات والمواقع الإباحية.[1]

المطلب الثالث:

خصائص جريمة القرصنة الالكترونية و ما يشابهها من جرائم أخرى:

إنما نقصد به من ذاتية الجرائم المعلوماتية و استقلاليتها و تمييزها عن غيرها من الجرائم، لاسيما التقليدية منها و ذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية و الإجرائية التقليدية القائمة إلا أن موضوع الدراسة يتمحور حول جريمة

[1]www.echoroukinline.com

القرصنة الالكترونية، إذ أن خصائص القرصنة تندرج ضمن خصائص الجريمة المعلوماتية و سوف نحاول ان نبرز أهم هذه الخصائص فيما يلي:

الفرع الأول:

خصائص جريمة القرصنة الالكترونية:

تتميز جريمة القرصنة الالكترونية عن غيرها و ما يشابهها من الجرائم الأخرى و هذا ما سوف نحاول ابراز اهم هذه الخصائص فيما يلي:

أولا:

الجريمة المعلوماتية المتعدية للحدود (عابرة للوطنية): إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مفادها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدا .

فالجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهى بذلك شكل حديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة،[1] ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعيني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذا أن الفاعل لا يتواجد على مسر ح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول

[1] خالد ممدوح إبراهيم . الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الأولى 2009 . ص 88

إلى ذا كرة لحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث[1]، أو القيام بإعداد احد البرامج الخبيثة (vérus) في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم[2]. وتظهر

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم[3] ، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى. ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجرعة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث تتواءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الاتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في محال الجرائم المعلوماتية، بالإضافة إلى تنو ع واختلاف النظم القانونية والإجرائية.

ثانيا:

صعوبة اكتشاف الجريمة المعلوماتية وإثباتها: تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنّها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من انحن عليهم. كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعد أمر كشف الجريمة و إثباتها وإذا ما قورنت حالات اكتشاف الجرعة

[1] نائلة محمد فريد قورة ، المرجع السابق ص 52

و من الأمثلة عن القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية قضية عرفت بإسم مرض نقص المناعة المكتسبة (الإيدز) . و تتخلص وقائعها أنه عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة.إلا أن هذا البرنامج في يترتب على حقيقته كان يحتوي على فيروس vérusمجرد تشغيله تعطيل جهاز .[2]

[3] أنظر في هذا المجال مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاقبة المجرمين المنعقد في هافانا عام 1990 .

المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي أيه يحتاج إلى عنف أو جثث أو اقتحام وإنما هي معلومات وبيانات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي [1] فلا ترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها[2] فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن

الاستدلال بأقوالهم ولا أدلة مادية بمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداوها بواسطة نبضات إلكترونية غير مرئية.

كما ذهب البعض للقول بان صعوبة اكتشاف الجريمة المعلوماتية و كذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والى تتسم ف أغلب الحالات بالطابع التقني الذي يضفى عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها. فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الإستدلالية و الإجراءات التقليدية مع هذا النوع من الجرائم . بالإضافة إلى صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية[3] .

ويمكن اعتبار أنه من بين الأسباب أيضا الي تقف وراء صعوبة اكتشاف الجرعة المعلوماتية وإثباتها المجني عليهم أنفسهم، ذلك أن هؤلاء قل يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حدى بين موظفيها

[1] عادل يوسف عبد النبي الشكري _ الجريمة المعلوماتية و أزمة الشرعية الإجرائية _ جامعة الكوفة كلية قانون ، ص 116.
[2] محمد حماد البهيتي ، التكنولوجيا الحديثة و القانون الجنائي . دار الثقافة للنشر و التوزيع عمان 2004 ، ص 165 .
[3] هشام محمد فريد رستم الجوانب الإجرائية للجرائم المعلوماتية, مكتبة الآلات الحديثة الطبعة الأولى 1994. ص 16

عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها[1]. ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض .حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه ، و هو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها . [2]

وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل الجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة الجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الالتزام.وعرض ذات الاقتراح على لجنة خبراء بمجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة.

الفرع الثاني:

مميزات جريمة القرصنة و ما يشابهها عن الجرائم الأخرى:

تعتبر جريمة القرصنة نوع من أنواع الجريمة المعلوماتية فالمشرع الجزائري ادرج جريمة القرصنة ضمن جريمة الانترنت و القرصنة تعتبر نوع من أنواع الجريمة المعلوماتية، فجريمة الانترنت هي سلوك إرادي غير مشروع صادر عن شخص لدراية فائقة لامور الحوسبة المعاقب

أشارت بعض التقديرات في الو.م.أ أن ما يتراوح بين 20 و25 من جرائم الحاسبات لا يتم الإبلاغ عنها خشية الإساءة إلى السمعة وق

أظهرت نتائجها أن 02 فقط من كل جرائم fortune 500دراسة أجريت على ألف شركة من الشركات المنتجة لجهاز المعلوماتية التى يتم

[1]التبليغ عنها للشرطة أو لمكتب التحقيقات الفدرالي. مشار إليه لدى رشيدة بوكر مرجع سابق،ص 472

[2] نهلا.عبد القادر المومني، المرجع السابق، ص 55

عليه قانونا بجزاء جنائي تكون شبكة الانترنت محل له أو وسيلة لارتكابه، أما فيما يميز الجريمة التقليدية عنها بانها كل سلوك انساني غير مشروع صادر عن إرادة إجرامية يفرض له القانون جزاءا جنائيا و انطلاقا من هذا يمكن استخراج نقاط الاختلاف بين الجريمتين و سيتم ذلك عن طريق استخلاص أوجه التشابه و الاختلاف و ذلك كما يلي:

أولا:

أوجه التشابه بين الجريمتين (جرائم الانترنت و الجرائم التقليدية): و يمكن حصر أوجه التشابه بين الجريمتين في النقاط التالية:

- ❖ غياب التعريف القانوني لكلا الجريمتين: فالمشرع كما هو متعارف عليه في لغة القانون لا يعرف الجريمة لان ذلك ليس من اختصاصه بل من اختصاص الفقه و القضاء في بعض الأحيان غير انه و للضرورة الملحة يجد نفسه مضطر لذلك، إما لتحديد اركان الجريمة العامة و او الخاصة أو تحديد السلوك الاجرامي المستحدث للجريمة[1].
- ❖ كلاهما يمثل جريمة تهدد مصالح و كيان المجتمع: إذ يعتبر كلا منها سلوكا ارداديا إنسانيا غير مشرع يهدد مصلحة أو مال محمي قانونا بجزاء جنائي.
- ❖ يفرض القانون مقابل ارتكابها جزاءا جنائيا، إي يعاقب على اقترافهما إما بعقوبة (إعدام) سالبة للحرية، غرامة مالية أو بتدابير أمن.
- ❖ يشترط لقيام كلا الجريمتين أركان: و أن اختلف الفقه الجنائي حول عددها من ركنين إلى ثلاثة أركان أي عدم اعترافهم بوجود ركن شرعي يعتبر شرطا اوليا للتجريم او أنه من شروط التجريم التي يتعين البحث في توافرها قبل البحث في اركان الجريمة ذاتها و مبررين ذلك بانه لا يمكن أن يكون هذا الأخير ركنا في هذه الجرائم، المهم يعترف بوجود ركنين فقط و هما الركن المادي و المعنوي.

[1] محمد سامي الشةا، ثورة المعلومات و انعكاساتها على قانون العقوبات ، دار النهضة العربية القاهرة سن 1994، ص5.

❖ تمر الجريمتين بالمراحل التي تمر بها اية جريمة من مرحلة التفكير و التخطيط و التحضير فالتنفيذ.

ثانيا:

أوجه الاختلاف بين الجريمتين: مقابل ذلك يختلفان في النقاط التالية

❖ من حيث الطبيعة القانونية: تعتبر جرائم الانترنت من الجرائم المستحدثة الخطيرة المصنفة ضمن الجرائم التقنية الحالية و بالضبط جرائم نضم المعلومات التي تكون فيها شبكة الام إما وسيلة لإرتكابها و يستخدم فيها الحاسب الالي كأدات لتسهيل ارتكابها على عكس الجرائم التقليدية التي هي من الجرائم العادية و قد تكون خطيرة في بعض المراة و تستخدم في ارتكابها وسائل تقليدية كالاسلحة النارية أو الهدم في جرائم القتل أو المفاتيح المقلدة في سرقة البيوت[1].

❖ من حيث الأدلة : لقد سبق التأكيد على أن جرائم الانترنت تمتاز بمجموعة من الخصائص تميزها عن غيرها من الجرائم لاسيما تلك التقليدية و من أهمها صعوبه اثباتها و اكتشافها لكون الأدلة فيها ادلة الكترونية غير مرئية غير مادية غير ملموسة فهي عبارة عن نبضات الكترونية تنساب عبر أجهزة الحواسيب و شبكة الشبكات، و على هذا يمكن القول بان جرائم الانترنت جرائم تستهدف معنويات و لا الماديات محسوسة على عكس الجرائم التقليدية التي تكون فيها الأدلة مادية محسوسة[2] و مرئية، فعلى سبيل المثال يكون الدليل في جريمة القتل إما وجود بصمات الجاني على سلاح الجريمة أو على الجثة أو على وجود الدليل سلاح الجريمة عبى مسرحها، و كان يكون

[1] الخلقة العلمية ، الدليل الرقمي و التحقيق في الجرائم الالكمترونية المنعقدة من 22 إلى 27 / 1429/12 كلية العلوم الأدلة الجنائية جامعة نايف العربية للعلوم الأمنية ص27.

[2]. عبد الفتاح البيومي الحجازي، الدليل الجنائي في جرائم الكومبيوتر و الانترنت، دراسة متعمقة في جرائم الحاسب الالي و الانترنت، دار الكتب القانونية، مصر، بدون سنة ص36-37

ذلك في جريمة التزوير المحررات التوقيع المزور و في جريمة الاغتصاب نطفة أو بصمة وراثية.[1]

- ❖ من حيث القانون المطبق: تخضع الجرائم التقليدية إلى تطبيق النصوص القوانين الجنائية التقليدية لقانون العقوبات قانون الإجراءات الجزائية على عكس جرائم الانترنت التي تعجز تلك القوانين عن مواجهتها و تعتبر قاصرة عن التطبيق خصوصا قانون الإجراءات الجزائية و ما تتضمنه من إجراءات تمس بحقوق و حريات الأفراد، إذ يجب ان تتعامل هذه الأخيرة بشكل عصري يتناسب مع طبيعة هذا الإجرام المنفرد و خاصة فيما يتعلق بإجراءات التفتيش و المعاينة و المحافظة على الأدلة، و كذا ضبطها و من جهة أخرى فإن جرائم الانترنت تتميز بتعديلها للحدود الجغرافية و القضائية، إذ لا تقتصر على دولة معينة و إنما تتخذ من العالم مسرحا لها المشكلة التي تثير تحديد القانون الجنائي المختصة داخل الدولة الواحدة إذا وقعت الجريمة ضمن اختصاص محكمتين قضائيتين محليتين في هذه الحالة مشكلة التنازع الايجابي في الاختصاص على عكس الجرائم التقليدية التي ترتكب داخل إقليم دولة معينة.
- ❖ من حيث المحل: محل الاعتداء في جرائم الانترنت او وسيلة هذا الاعتداء تتمثلفي مفردات جديدة تختلف عن مفردات الجرائم التقليدية و هي البرامج و البيانات.
- ❖ من حيث صفات الجاني يختلف الجاني في جرائم الانترنت عن مثيله في الجرائم التقليدية، فالجاني في هذه الجرائم يسمى مجرما تقنيا أو هاكر أو مجرما معلوماتيا أو مجرم الانترنت و هو يتمتع بغالب الأحيان بقدر كاف من علم و بالمعرفة التقنية و هو يختلف عن المجرم العادي[2] الذي يرتكب الجرائم التقليدية في كونه يتمتع بشخصية مستقلة، فهو منفرد عن المجرم الذكي في الاختراق و ارتكاب أفعال تقنية عبر العالم الافتراضي لا يمكن للناس العاديين أو العامة القيام بها فإنه يصعب ملاحقة مرتكب هذه

[1] سامح عبد الحكم، جرائم الانترنت الواقعة على الأشخاص في اطار التشريع البحريني، دراسة مقارنة، بالتشريع المصري دار النهظة العربية القاهرة،2007، ص3.

[2] عبد الفتاح البيومي حجازي، المرجع نفسه، ص96.

الجرائم لإستحالة تحديد هويتهم سواء قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها كما ان هؤلاء المجرمين لاحهم ليس ناريا أو ادات حادة إنما عقل و برنامج و فيروسات لغختراق برنامج حاسوبية.

- ❖ من حيث الضحايا: جرائم الانترنت غالبا ما تقيد ضد مجهول و في حالة اكتشافها فمن الصعب إقامة الدليل عليه و محاكمته على عكس الجرائم التقليدية التي قد تقيد ضد المجهول أو ضد المعلوم[1].
- ❖ من حيث النظام القانوني: يشترط للقيام كل هذه الجرائم ثلاث اركان و هي الركن الشرعي ، الركن المادي و الركن المعنوي أي انها كغيرها من الجرائم لها أركانها و عناصرها.
- ❖ من حيث مراحل ارتكابها: تمر هذه الجرائم كغيرها من الجرائم بذات المراحل التي تمر بها أية جريمة من مرحلة التفكير و التخطيط و التحضير فالتنفيذ
- ❖ من حيث إجراءات الملاحقة و الكشف عن مرتكبها: يتطلب الكشف عن مرتكب هذه الجرائم و ملاحقتهم قضائيا استراتيجيات تحقيق و تدريب و مهارات خاصة تسمح بتفهم و مواجهة التقنيات و الأساليب المستخدمة في هذا النوع من الجرائم فكثيرا ما تخفق و تفشل أجهزة الشرطة في ملاحقة و ضبط مرتكبها، كما تتطلب هذه الجرائم ضرورة وجود تعاون دولي لمكافحتها و الحد منها.
- ❖ من حيث الهدف(الغرض المرتكب من أجله): تهدف كل جريمة من هذه الجرائم إلى تحقيق أرباح مادية طائلة في الوقت التي تسبب فيه أضرار و خسائر مادية و معنوية هائلة و ضخمة.

ثالثا:

أوجه الاختلاف بين جرائم الانترنت و غيرها من الجرائم المستحدثة المشابهة لها .

[1] د/حسين المحمدي بوادي، غرهاب الانترنت الخطر القادم، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية، 2006 ، ص76.

سبق التأكيد و بينا نقاط التشابه و الاختلاف بين جرائم الانترنت و الجرائم التقليدية حيث اعتبرت تلك الجرائم المستحدثو و هي التقنية العالية و الخطيرة حيث ان اختلافها هذا لا يقتصر على تلك النوعية من الجرائم بإعتبارها تقليدية و عادية و منحصرة في إقليم معين بل قد تختلف و تتفق نع غيرها من الجرائم المستحدثة و المشابهة لها، كالجريمة المنظمة و جريمة الحاسوب أو ما تسمى الجريمة المعلوماتية و تندرج ضمنها جريمة القرصنة الالكترونية و جريمة التقنية و جريمة الاتصال عن بعد[1]:

1- أوجه التشابه بين جرائم الانترنت و غيرها من الجرائم المستحدثة المشابهة لها: تعرف جرائم الانترنت بأنها كل سلوك إرادي غير مشروع صادر عن شخص ذا دراية فائقة بمجال الحوسبة معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لإرتكابه .

و من خلال ما تم تقديمه يمكننا حصر أوجه التشابه بين جرائم الانترنت و غيرها من الجرائم المستحدثة في النقاط التالية:

- من حيث الطبيعة القانونية: تعتبر هذه الجرائم أو تصنف ضمن الجرائم المستحدثة و الخطيرة و بالتحديد جرائم التقنية العالية أي جرائم نظم المعلومات التي يترتب عنها نتائج وخيمة و ضارة بجميع المستويات سواء اجتماعية أو اقتصادية أو سياسية و سواء كانت شخصية متعلقة بفر او دولية متعلقة بالدولة هذا من جهة و من جهة أخرى ففي كلتيهما تستعمل التقنية العالية لإرتكابهما أي الانترنت و الحاسب الألي الذي يعتبر سلاح الجريمتين و بالأحرى أداة لإرتكاب الجريمتين، كما يجب أن يتمتع مرتكبها بصفات و سيمات عالية تتماشى مع مستوى المحيط الذي تتعامل معه و مع نوع الجريمة الذي يرغب في ارتكابها كما تشترط جريمة الانترنت و الجرائم المعلوماتية في خاصية صعوبة اكتشافها و اثباتها و ذلك راجع إلى الأدلة المتميزة بأنها غير مرئية

[1] د. شريف سيدي كامل الجريمة المنظمة في القانون، الطبعة الأولى، دار النهظة العربية، القاهرة ، ص12.

على العموم، و يمكن محوها و تدميرها في ثوان قليلة معدودة إما من طرف المجرم أو من المحقق في هذه الجرائم بسبب إهماله أو نتيجة التعامل بخشونة مع الأقراص المرنة.

- من حيث العقاب يعاقب القانون على ارتكاب هذه الجرائم بفرض جزاءات جنائية تتلائم مع هذه النوعية من الجرائم.
- من حيث النظام القانوني: يشترط لقيام كل من هذه الجرائم ثلاث أركان و هي: الركن الشرعي الركن المعنوي و الركن المادي كغيرها من الجرائم لها أركانها و عناصرها.
- من حيث الخصائص التي تتمتع بها: تشترك جرائم الانترنت و الجرائم المستحدثة المشابهة لها في خاصية عدم اعترافها بالحدود الجغرافية المتعارف عليها في العالم المادي إذ تعتبر هذه الجرائم جرائم عابرة للحدود الدولية و التي تتخذ شكلا بعيدا عن الطابع الإقليمي، مع الإشارة إلى إمكانية وقوعها داخل إقليم دولة ما أو بين عدة دول في نفس الوقت فتجعل العالم بذالك قرية صغيرة[1].

2-أوجه الاختلاف بين جرائم الانترنت و غيرها من الجرائم المستحدثة المشابهة لها: سبق التأكيد على أن طريقة المعلومات فائق السرعة (انترنت) يتميز بجملة من الخصائص من ابرزها ارتباطه بالحاسوب، إذ يعتبر هذا الأخير النافذة أو البوابة التي يطل عليها على العالم الخارجي الامر الذي أدى بالفقهاء إلى اعتبار أن جرائم الانترنت هي ذاتها جرائم الحاسب الالي أو بالأحرى هي ذاتها جرائم المجريمة المعلوماتية و لكنها في حقيقة الامر ما هي إلا نوع منها هذا من جهة و من جهة أخرى أدت خاصية عبورها و عدم اعترافها بالحدود الجغرافية المرسومة في العالم المادي إلى اشتراكها و تشابهها مع الجرائم المستحدثة.

رابعا:

جرائم الاعتداء على الأشخاص عبر الانترنت: يقصد بجرائم الاعتداء على الأشخاص بصفة عامة تلك الجرائم التي تنال بالاعتداء إو التهديد بالخطر حقوقا ذات طابع شخصي بحت أي

[1] د. شريف سيدي كامل الجريمة المنظمة في القانون،ص-ص 13-14.

تلك الحقوق اللسيقة بالشخص المجني عليه و التي تعبر عن مقومات الأساسية لشخصيته و هي تخرج عن دائرة التعامل الاقتصادي و أهمها الحق في الحياة و في سلامة الجسم و الحق في الحرية و في صيانة العرض الحق في الشرف و العتبار، او هي مجموعة من الجرائم التي تقع الاعتداء على الجوانب الشخصية الإنسانية و من ثم فهي تستهدف اما المساس بشخصية الانسان الطبيعية أو العضوية و تمس بذلك حقه في الحياة أو سلامته البدنية او عرضه أو حريته، و إما تستهدف المساس بشخصية الانسان المعنوية أي بقيمتع المعنوية أو الاعتبارية كجرائم الشرف و الاعتبار و تعد هذه الأخيرة من الجرائم التقليدية الأكثر وقوعا و انتشارا لمجتمعاتنا و التي تصدت لها و تناولتها مختلف التشريعات العقابية و هذا ما نصت عليه النصوص القانونية كقانون رقم 07/18 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، و لكن لما عرفه علمنا من ثورة رقمية اثرت بالسلب عليه بافرازها لجرائم مستحدثة و فريدة من نوعها تختلف عن نظيرتها التقليدية لا سيما وسيلة او محل ارتكابها إذا اتاحت للمجرم المعلوماتي أو ما يعرف الهاكرز و إمكانية تسخير العالم الافتراضي لتحقيق رغباته في ارتكاب اغلب الجرائم و خاصة تلك الواقعة على الأشخاص من جنح بسيطة إلى جنايات كبرى، سواء كان فاعلا اصليا أو فاعلا معنويا و بابسط الأساليب من خلال الالاعب ببرمجة البيانات عن بعد و بضغطة زر واحد هو جالس في مكانه دون الحاجة إلى مبارحته و يمكن تصنيف جرائم الاعتداء على الأشخاص عبر الانترنت على جرائم البث العلني و جرائم الاعتداء على حرمة الحياة الخاصة، و يستم التطرق إلى كل نوع من هذه الجرائم في النقاط التالية: جرائم البث العلني عبر الانترنت و جرائم الاعتداء على حرمة الحياة الخاصة

1-جرائم البث العلني عبر الانترنت[1].

تعد جرائم البث العلني أحد الخصائص التي تتميز بها تقنية الانترنت فهي فضلا عن كونها وسيلة حية و حيوية للبث فهي تعتبر كذلك مضهرا للبث السمعي المرئي لإحتوائها قوة وسائل و أدوات البث التقليدية (المقروءة، المسموعة و المرئية) و لكن ذلك الأخير (البث

[1] محمد محمد حسن، جريمة القذف، دراسة مقارنة بين القانون الجنائي الوضعي و الشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق،1996، ص21.

العلني) لم يرحمه أصحاب النفوس المريضة لقد وجدوا من خلاله متنفسا لاحقادهم و مرتعا لشهواتهم و استعملوه في نشر الشائعات و الأخبار الكاذبة التي تطول ز تمس رموز الشعب سواء كانت تلك الرموز الفكرية او الدينية او السياسية و أيضا في قذف و سب و تشويه سمعة تلك الرموز بهدف تشكيك الناس في مدى مصداقية هؤلاء الأفراد و محاولة فض الناس من حولهم ليخلو لهم الجو في محاولة منهم لتسميم أفكار الناس و تتخذ جرائم البث العلني مظاهر عدة يمكن حصرها في جرائم الماسة بسمعة الشخص و شرفه و اعتباره و جرائم النشر الالكتروني و جرائم العنف و القذف و القتل عبر الانترنت، و تعد جائبالسب و القذف و التشهير من أبرز الجرائب التقليدية الماسة بسمعة الشخص و شرفه و اعتباره إذ تأثر سلبا على شخص الانسان خاصة بعد ظهور شبكة الانترنت الني أصبحت وسيلة تستخدم للنيل من شرف الغير أو كرامته أو اعتباره أو تعرضه لإلى بغض الناس و احتقارهم بما يتم اسناده للمجني عليه على شكل رسالة البيانات.

2-جرائم الاعتداء على حرمة الحياة الخاصة[1].

حظيت الحياة الخاصة للأفراد حماية دستورية و قانونية و دولية في مختلف دول العالم فقد كفل دستور الجزائري تلك الحماية للحقوق و الحريات الفردية في الفصل الرابع من المواد 29 إلى 59 فضلا، فمثلا في المادة 1/34 على : تضمن الدولة عدم انتهاك حرمة الانسان و في المادة 39 منه على : لايجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه و يحميها القانون سرية المراسلات و الاتصالات الخاصة بكل اشكالها مضمونة و هذا ما نصت عليه القوانين الخاصة: قانون 07/18 يتعلق بحماية الأشخاص الطبيعيين و القانون 04/09 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، و قانون العقوبات و هذا حسب ما نصت عليه المواد 394 مكرر إلى 393 مكرر 7 .

[1] فقد كفل الدستور الجزائري تلك الحماية للحقوق و الحريات الفردية في الفصل الرابع من المواد 29 إلى 59. فمثلا نص في المادة 1/34 منه على: تضمن الدولة عدم انتهاك حرمة الانسان و في المادة 39 منه على: "لا يجوز انتهاك حرمة حيتة المواطن الخاصة.

لقد أصبح التطور التكنولوجي الذي يشهده عصر ثورة المعلومات يهدد الأفراد في حياتهم الخاصة، لاسيما بعض شيوع استخدام الانترنت و الحواسيب في شتى كجالات الحياة، حيث تم اعتبارها وسيلة لتخزين بيانات شخصية مختلفة و متعددة –كالبيانات الاسمية[1] و ذلك على ما يصطلح عليه بنوك أو مراكز المعلومات. مما يشكل تهديد و انتهاكا غير مسبق لخصوصيتهم نظرا لسوء استخدامها أو استخدامها لغير الغرض الذي جمعت من أجله من قبل الجهات المختصة بذلك. فتتحمل بذالك حياة الفرد إلى جحيم بعدها كانت هذه المعلومات و البيانات في ضل الطرق التقليدية في مأمن لا يطلع عليها إلا صاحب الشأن نفسه بإتباع إجراءات معينة، لتصبح كالكتاب المفتوح و المقروء من قبل من كان لديه الإمكانية التقنية و الفنية الكافية للوصول إليها سواء أكان تابعا لهذه الجهات أو كان فردا غير مرخص له أساسا بالإطلاع عليها. و هذا ما أكده بعض الخبراء من أن هناك إمكانية في متابعة و مراقبة الواقع التي قد يزورها الشخص على شبكة الانترنت.

فاستخدام الانترنت هو في الحقيقة ظاهر بوضوح أمام من يريد مراقبته و لا يمكنه التنكر. و المثال الواقعي لذلك هو ما نشر مؤخرا من أنه على مدار عام دوام شخص يدعى كريستوفر كانترس على الاشتراك في المناقشات الدائرة في مجموعة المناقشات المنتشرة على الانترنت. حيث أضاف أراءه إلى الأعداد الكبيرة من الأدراء الموجودة في هذه المجموعة. إلى حين اختياره من قبل صحيفة "مينيا بولس ستار تريبيون" بصورة عشوائية لجمع المعلومات الخاصة به من الشبكة بناء على ما نشره بنفسه، مستخدمة في ذلك موقعا على الويب يطلق عليه Dedja News و الذي ينتيح البحث في مجموعات الاخبار الموجودة على الانترنت بواسطة اسم شخص، و تعتبر المعلومات التي تمكنت الصحيفة من جمعها ذات أهمية كبيرة و لا يستهان بها و حيث شملت كل ما هو شخصي من مكان مولده و المدرسة التي ذهب إليها و الجامعة التي درس بها و مكان عمله الحالي و السابق و يمكن لأي شخص جمع كل كلمة بمجموعات الاخبار و معرفة المواقع التي تزورها على

[1] و يقصد بالبيانات الاسمية:"البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية و المالية و الوظيفية و المهنية و العائلية، عندما تكون هذه البيانات محلا للمعالجة الألية" . محمد امين احمد الشوابكة، المرجع السابق، ص63.

موقع التابع لشبكة الانترنت و الأمر ذالك يستطيع أن يطلع على بريدك الالكتروني و يجري عمليات التسويق و يتعامل مع البنوك باسمك من خلال الانترنت و على هذا فإن شبكة الانترنت قد سهلت الكثير من الأمور الحياتية يتجاوزها لعديد من العقبات التي كانت تعتبر من الضروب المستحيلة إذ اصبح بإمكان أي شخص الإبحار عبرها و الولوج إلى أي موقع يرغب فيه و الحصول على ما يريده من معلومات و بيانات خاصة سواء كانت تتعلق بالافراد أو بمؤسسات بطرق غير مشروعة دون الحاجة لقطع المسافات أو تضييع الأوقات الأمر الذي جعل الحياة الخاصة لهؤلاء الأشخاص تتعرض لجولة من الانتهاكات و أن تلك الشبكة لا تتوفر فيها السرية الكاملة و اللازمة للإحاط بتلك البيانات الخاصة إذ كا اتصال بالانترنت يمكن أن يترك اثرا ما حتى و لو لم يدرك مستخدم الشبكة ذلك، فأصبح بالإمكان بعض الأشخاص الولوج إلى أنظمة و أجهزة تخص الاخرين و الحصول على معلومات و أسرار حياتهم أو اية معلومات أخرى تخصهم يرغب صاحبها في إضفاء الطابع السرية عليها و يمكن تعريف الخصوصية المعلوماتية بأنها حق الأفراد في تحديد متى و كيف و إلى أي مدى تصل المعلومات عنهم للآخرين او بأنها قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم و عليه يمكن تعريف جريمة الاعتداء على خصوصية الآخرين عبر الانترنت بأنها: كا اعتداء على البيانات الاسمية عبر الانترنت و ذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت و العمل على تسجيل و حفظ البيانات المتبادلة بين الأنظمة المعلوماتية و من خلال هذا يمكن ادراج طرق الاعتداء على الحياة الخاصة في النقاط التالية:

*استقراء السمع و التنصت أو الرقابة الالكترونية[1]: أي في التجسس و الاستماع سرا و خلصتا لمراسلة الأفراد و مكامن خصوصيتهم و ذلك دون رضاهم و لا أدلة من الشبكة المعروفة و التي استخدمت كمشروع تنصت على مزودي خدمة الانترنت لمراقبة وسائل البريد الالكتروني و التراسل الفوري لمشتركي الانترنت، و يقصد بالتنصت هنا الاستماع سرا بوسيلة أيا كانت نوعها إلى كلام له صفة الخصوصية صادرة عن شحص ما أو متبادل بين

[1] د. شريف سيدي كامل الجريمة المنظمة في القانون،ص-ص 15-16.

شخصين أو اكثر دون رضاء من هؤلاء، هذا من جهة و من جهة أخرى يعتبر الدخول غير المرخص به للمعلومات أو الدخول غير المشروع أو الاختراق و الاطلاع عليها دون إذن أو ترخيص صورة من صور انتهاك لحقوق الإنسان في خصوصيته عبر الانترنت و يتم ذلك عن طريق الحصول على كلمة السر أو كلمة المرور للملفات المخزنة و بالتالي التسلل إلى شبكة كما لو كان ذلك الشخص المستخدم الحقيقي، و استغلاله لتلك المعلومات الخاصة في غير محلها أو الاطلاع عليها بدون اذن من صاحبها فمثلا مكن اعتراض الرسائل المنقولة بواسطة البريد الالكتروني و قراءة فحواها الذي يفترض انه سري قبل وصوله للمرسل إليه أو يمكن الدخول في موقع بدون ترخيص بقصد الدخول الى البيانات أو المعلومات امنية تمس الامن و الاقتصاد القومي للبلاد أو الغاؤها و يعرف الدخول غير المشروع بأنه الولوج غير المصرح به و بشكل غير مشروع إلى نظام المعالجة الالية للبيانات بإستخدام الحاسوب أو هو دخول شخص بكريقة متعمدة إلى الحاسب الالي أو الموقع الالكتروني أو النظام المعلوماتي أو شبكة حاسبات ألية غير مصرح لذلك الشخص بالدخول اليها أو هو دخول شخص عادي أو موظفا عاما متعما موقعا أو نظام معلومات أو شبكة إلكترونية دون أن يكون له مصرحا له بذلك و يقوم بالاطلاع على البيانات أو نسخها أو إلغائها أو حذفها أو تدميرها أو افشاءها أو تغييرها بشكل يحدث ضررا لصاحب النظام.

و تجدر الإشارة إلى أنه إذا كان هذا الشخص الذي دخل الموقع أو النظام موظفا عاما فهو يدخله دون تفويض من جهة التي يعمل بها او يقوم بتسهيل ذلك الدخول للغير، كما يعد تسجيل المحادثات الخاصة التي تدور في منتديات المناقشة و في مجموعات الاخبار ضربا أخر من الجرائم الماسة بالحياة الخاصة عبر الانترنت فمثلا يقوم www.dejanews.com[1] بنسخ اجمالي لكامل المنتديات المناقشة و يحفظه داخل ملقمات خاصة.

[1] T.G.I Paris,réf 30 avril 1997, D.1998.Somm Convenentes,p 79.

هذا من جهة و من جهة أخرى كذالك فإن التقاط و نقل الصور دون موافقة صاحبها يعد مظهرا خطيرا و أخر من مظاهر التعدي على خصوصية الإنسان كان يكون ذلك عن طريق الكمرا الموصولة بالانترنت التي يستخدها العديد من مستخدمي هذه الشبكة و خاصة الشباب منهم يطلقون عليهم لفظ الكام اختصارا للكميرا، و هي توضع على جهاز الكمبيوتر و تنقل الصورة و الصوت في ذات الوقت للطرف الاخر، و يمكن بالطبع للطرف الاخر تسجيل الصورة كذلك الصوت و من ثم نقله على دعامة الدسك أو قرص ممغنط و الاحتفاظ به أو إذاعته و نشره عبر الانترنت لإفشاء محتوى أسراره و أدق خصوصيته هذا بالنسبة للالتقاط و النقل عبر شبكة الانترنت من طرف لأخر. اما الجديد أيضا فهو الالتقاط و النقل عبر الهاتف المحمول سواء كان الالتقاط لمجرد صورة فحسب و أن يتم الالتقاط كذلك عن طريق تقنية استخدام البلوتوث او خاصية الوسائط المتعددة سواء للهاتف المحمول أو أكثر من هاتف محمول يحتوي على ذات الخاصية و كذلك النقل عبر تحميل تلك الصور أو المواد على جهاز الكمبيوتر عن طريق ذات الخاصية و التي أصبحت متوافرة الأن في أجهزة الكمبيوتر و بالتالي إمكانية إرسالها عن طريق البريد الاكتروني أو نشرها[1].

و تجدر الإشارة أنه يشترط ان يتم ذلك في مكان خاص و المقصود بالمان الخاص هنا المكان الذي لا يمكن دخوله دون إذن الشخص الذي يشغله سواء كان ذلك بطريقة دائمة أو مؤقتة، كما اوجدت شبكة الانترنت برامج رصد متطور تسمى بالكعكات و التي هب عبارة عن ملفات صغيرة يخزنها موقع الانترنت في الذاكرة الرئيسية لجهاز حاسوب المستخدم لإستخدانات كثيرا ما تكون مفيدة مثل أخذ المعلومات الخاصة بالمتصفح كضغط كلمة السر الخاصة به و عدد المرات التي زار فيها الموقع و بذلك أصبحت تلك الشبكة من أنجح الوسائل في تتبع الأشخاص و في كشف أسرار حياتهم كما استخدمت لبناء الدراسات المتعلقة بالتسويق و ملاحقة الزبائن و مضايقتهم، أما الوسيلة الأخطر في تلك المضايقات للخصوصية عبر الانترنت تتمثل في نرمجيات التتبع الشم و هي وسيلة تتبع لجمع اكثر

[1] خالد ممدوح إبراهيم . الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الأولى 2009 . ص 90.

قدر ممكن من المعلومات السرية و الخاصة عن طريق ما يعرف بانظمة جمع المعلومات، و نستخلص مما سبق ان هناك تحديات جديدة أوجدتها شبكة الانترنت في مواجهة خطط حماية الخصوصية أو الحياة الخاصة فهي زادت من كمية البيانات المجمعة و المعالجة و المنشأة و أتاحت عولمة المعلومات و الاتصالات.

و على غرار هذا تجدر الإشارة أنه توجد أنواع جرائم الاعتداء على حرمة الحياة الخاصة بواسطة شبكة الانترنت تورد أساليب إجرامية شائعة في التعدي على الخصوصية و منها:

- استعمال بيانات شخصية غير حقيقية: المحو أو التلاعب في بيانات شخصية بمعرفة افراد غير مصرح لهم بالاطلاع أو استعمال هذه البيانات .
- استعمال بيانات شخصية غير حقيقية بواسطة المسموح لهم قانونا.
- جمع أو معالجة بيانات حقيقية بدون ترخيص[1].

فبخصوص الحالة الأولى فيهدف هذا التلاعب أو المحو للبيانات المختزنة أليا إلى تحقيق غاية مادية للجنات و من الأمثلة الواقعية عن هذا الأسلوب حالة شركة TR.W.COMPAN CREDIT DATA الامريكية إذ تختص هذه الأخيرة بتزويد عملائها من البنوك و المتاجر الكبرى و غيرهم بالمعلومات الكافية عن المركز الائتماني لدى شخص تريد هذه الجهات التعامل معه، الأمر الذي دفع بستتة عاملين في هذه الشركة إلى الاتصال بالافراد و المؤسسات ذوي المركز الائتماني السيئ حتى يحصلوا على مقابل مالي لهم مقابل تعديل البيانات الخاصة بهم و بذلك تورط الكثير من العملاء هذه الشركة في تعاملات تجارية و مالية مع افراد لا يتمتعون بمركز ائتماني جيد، أما الحالة الثانية يكون الإهمال فيها هو السبب وراء عملية حمع أو معالجة أو نشر البيانات الشخصية الغير صحيحة بواسطة المسموح لهم قانونا مع إمكانية تصور حدوث ذلك بصورة عمدية.

[1] هشام محمد فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات ، ص-ص 189-191.

أما الحالة الثالثة تخص جمع او معالجة بيانات حقيقية دون ترخيص حيث تقوم جهات أو أشخاص ليس لهم الحق في تخزين بيانات حقيقية تخص أفراد باستخدام أساليب تتسم بعدم المشروعية كالالتقاط الارتجاجات التي تحدثها الأصوات في الجدران الإسمنتية و معالجتها بحاسوب مزود ببرنامج خاص لترجمتها إلى كلمات و عبارات و مراقبة و اعتراض و تفريغ الرسائل المتبادلة عن طريق البريد الالكتروني و توصيل أسلاك بطريقة خفية إلى الحاسب الذي تخزن بداخله البيانات و التوصل بطريق غير مشروع إلى ملفات تخص الآخرين.

3-موقف التشريعات المقارنة من جرائم الاعتداء على حرمة الحياة الخاصة[1]:

أثارت مسألة حماية الخصوصية الفردية في مواجهة أخطار المعلوماتية قلقا في مختلف الأنظمة القانونية حيث لم تأخذ التشريعات المقارنة مسلكا موحدا لحماية الحق في حرمة الحياة الخاصة في مواجهة الأخطار الناجمة عن استخدام الحاسب الالكتروني و الانترنت كبنك للمعلومات سواء في دساتيرها أو تشريعاتها و يمكننا تقسيم موقف هذه التشريعات المقارنة إلى موقفين موقف التشريعات العامة من هذه الجرائم و موقف التشريع الجزائري من اخطار بنوك المعلومات على الحياة الخاصة، و قبل ذلك يجب التطرق أولا إلى تبيان الجهود الدولية المبذولة لحماية الحياة الخاصة في مواجهة نظم المعلومات فقد أثارة مسألة حرمة الحياة الخاصة للأفراد اهتمامات المنظمات العالمية و الإقليمية و التي اكدت على حق الإنسان في حرمة حياته الخاصة من أخطار الاعتداء على البيانات الشخصية حيث برزت في هذا الإطار جهود منظمة الأمم المتحدة و المجلس الأوروبي و كذا منظمة التعاون الاقتصادي.

أ. موقف التشريعات العربية بصفة عامة من جرائم الاعتداء على حرمة الحياة الخاصة و سنحدد في هذه النقطة الدول العربية التي وضعت قوانين خاصة في مواجهة أخطار بنوك المعلومات ثم نعرج إلى الدول العربية التي التزمت الصمت حيال هذا الإشكال الخطير و الجسيم المهدد لخصوصية المعلوماتية للأفراد، و من الدول العربية التي خصصت حماية قانونية للخصوصية المعلوماتية للأفراد تونس افرد فيه حماية خاصة للمعطيات الشخصية و كذا السعودية من خلال نظام مكافحة الجريمة المعلوماتية و كذا

[1] منير محمد الجنبيهي، ممدوح الجنبيهي، من المعلومات الالكترونية، المرجع نفسه، ص94.

الإمارات العربية المتحدة، و على عكس الدول العربية السابقة فقد اكتفت معضم التشريعات العربية لتوفير تلك الحماية بالنصوص القانونية التقليدية الخاصة بحماية الاسرار المتناثرة ما بين قوانين العقوبات و قوانين الإجراءات الجزائية و قوانين البريد و الاتصالات.

ب.موقف التشريع الجزائري من أخطار البنوك المعلومات على الحياة الخاصة[1]:

أما بالنسبة للجزائر و لما كانت هذه الأخيرة من الدول العربية التي طالها التسوناكمي جرائم الانترنت بجميع أنواعها و لاسيما جرائم التعدي على حرمة الحياة الخاصة بكل اشكالها و لما كانت خصوصية الافراد من أهم الحريات المكرسة في المواثيق الدولية و الدساتير و القوانين ، و كان التعدي عليها و انتهاكها يشكل جريمة و انتهاكا لحقوق و حريات الافراد كان من اللازم على المشرع الجزائري توفير الحماية الواجبة لهذه الحرمة و تجريم كل اشكال الاعتداءات التي يمكن أن تمس و تهز هذه الأخيرة و هذا من خلال المواد الدستورية و كذلك من مواد قانون العقوبات و الإجراءات الجزائية، فأما فيما يخص الحماية الدستورية لهذه الحرمة فقد كفل الدستور الجزائري تلك الحماية للحقوق و الحريات الفردية في الفصل الرابع من المواد 29 إلى 59 و من ذلك ما نص عليه في المادة 1/32 منه على أن الحريات الأساسية و حقوق الانسان و المواطن مضمونة و في المادة 1/34 على انه تضمن الدولة عدم انتهاك حرمة الانسان و في المادة 39 منه على انه لا يجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه و يحميها القانون.

سرية المراسلات و الاتصالات الخاصة بكل اشكالها مضمونة

و تجسيدا لهته الحماية الدستورية لخصوصيات الافراد فقد تدخل المشرع الجزائري و وضع حدا لكل اعتداء على حرمة هته الحياة ة ذلك بتجريم كل أنواع المساس بحرمة الحياة الخاصة و بستخدام وسائل التكنولوجيا الحديثة من المواد 394 مكرر إلى 394 مكرر 7 مضمونا احكام النصوص التي تكفل حماية حرمة الحياة الخاصة و أن المشرع الجزائري قد حدد الجرائم التي

[1] تنص المادة 39 على أنه باستثناء حالة موافقة صاحب الشهادة لايمكن لمزود الخدمات المصادق الالكترونية او أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة إلا ما كان منها ضروريا لغبلام العقد و تحديد محتواه و تنفيذطه و اعداد و اصدار الفاتورة.

تقع على حرمة الحياة الخاصة و هي جريمة الالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص و بغر رضا صاحبها جريمة الالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية و بدون اذن صاحبها جريمة الاحتفاظ أو إذاعة أو استعمال تسجيلات أو الصور أو الوثائق المتحصل عليها من الجريمتين[1].

و المشرع الجزائري بصفة خاصة يسعى دائما إلى خلق نقطة توازن بين قمع الجريمة و حماية حرمة الحياة الخاصة من خلال وضع ضوابط قانونية تجعل من هذه الأساليب الحديثة في البحث و التحري تدخل في اطار الشرعية الإجرائية و ذلك بالنض على ضرورة الحصول على اذن من وكيل الجمهورية المختص و قاضي التحقيق و ان تتم هذه العملية تحت اشرافه.

[1] وضع الترتيبات التقنية دون موافقه المعنيين من أجل التقاظط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة او سرة من طرف شخص او عدة أشخاص في أماكن خاصة أو عمومية او التقاط صور لشخص او عدة أشخاص يتواجدون في مكان خاص "كما انه أجاز بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها من الخلال القانون رقم 04/09. المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

خلاصة الفصل :

نستخلص من هذا الفصل تعدد و تنوع و تباين التعريفات الفقهية حول موضوع القرصنة الالكترونية ، فالامر الذي نتج عنه صعوبة الاتفاق على تعريف فقهي جامع شامل مانع لها في مقابل النيابة التامة بالنسبة للتشريع اذ انه و بالرغم من وجود بعض القوانين و النصوص الخاصة في بعض الدول كالقانون رقم 04/09 الموجود في الجزائر المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الاعلام و الاتصال و مكافحتها إلا انها لم تعرف جريمة القرصنة بالتحديد بل تضمنت تعريفات واسعة تخدم الجريمة المعلوماتية او الجرائم المتصلة بتكنولوجية الاعلام و الاتصال إلا ان جريمة القرصنة موضوع الدراسة، و نستخلص كذالك من خلال ما تم تقديمه ان كل فقيه أو مفكر ركّز على زاوية معينة من زوايا جريمة القرصنة الالكترونية غير ان نقطة التقاطع أو القاسم المشترك بينهم هو تطرقهم لهذا الموضوع كفعل إجرامي غير شرعي ينجر عنه عقوبات و متابعات قضائية جراء الضرر الناجم عنهم ، و نستخلص كذالك ان مرتكب هذه الجريمة شخص ذو خبرة فائقة بمجال الحوسبة يسمى المجرم التقني و تختلف هذه الجريمة عن الجرائم الاخرى في نقاط أن الأدلة فيها غير مرئية غير مادية و غير ملموسة يمكن تدميرها و إخفاء معالم الجريمة فيها في ثوان معدودة لكون أن مسرح الجريمة فيها غير موجود لانه عبارة عن عالم افتراضي و أن مرتكبها يعتمد عبى قوته الذهنية اكثر من قوته الجسدية و ذات الشأن بالنسبة للجرائم المستحدثة المشابهة لجرائم الانترنت كالجريمة المعلوماتية و جريمة التقنية فهي تختلف عنها في انه ليست كل جريمة انترنت هي جريمة معلوماتية بل نوع منها فقط كما سبق ز ان ذكرناه (جريمة القرصنة) فهي موضوعنا المعالج و المراد دراسته.

الفصل الثاني:

الجوانب الموضوعية والإجرائية لجريمة القرصنة الالكترونية

تمهيـــد :

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع جريمة القرصنة الالكترونية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بموضوع هذه الدراسة، سيتم في هذا الفصل المعنون الجوانب الموضوعية والإجرائية لجريمة القرصنة الالكترونية التطرق والتقديم لأركان هذه الجريمة والعقوبات المقررة لمكافحتها وإحاطة الموضوع بالنصوص الواجبة التطبيق وفرض العقاب على مرتكب هذه الجريمة من خلال ما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية لهذه الجريمة، أصبحت هذه الجريمة اليوم شبح يهدد العالم وهاجسا أمنيا يتحدى قيام الحكومة الالكترونية من أجل القضاء ومكافحتها.

ولذلك سنتناول في هذا الفصل الجوانب الموضوعية لجريمة القرصنة الالكترونية من خلال المبحث الأول، والجوانب الإجرائية لمكافحة جريمة القرصنة الالكترونية من خلال المبحث الثاني .

المبحث الأول : الجوانب الموضوعية لجريمة القرصنة الإلكترونية:

من خلال ما سبق التطرق إليه و دراسته جريمة القرصنة الإلكترونية تنتقل لأن إلى دراسة أركان هذه الجريمة وتبرز العقوبات المقدرة لارتكاب هذه الجريمة ونذكر الجرائم التي يكون الحاسوب هدفا لها من خلال نظام المعالجة الآلية للمعطيات وجرائم الاعتداءات الماسة بالأنظمة المعلوماتية.

المطلب الأول :أركان جريمة القرصنة الالكترونية و العقوبات المقررة لها:

الفرع الأول: أركان جريمة القرصنة الالكترونية :

إن أركان هذه الجريمة هي نفسها أركان جريمة معلوماتية تندرج ضمنها سماها المشرع نظام المعالجة الآلية للمعطيات إلا أن لهذه الجريمة أركان ثلاثة وتتمثل في:

الركن الشرعي: وهو الصفة غير المشروعة للفعل وتتمثل قاعدة التجريم والعقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ثم نتناول الركن المادي فيتمثل في : ماديات الجريمة التي يبرز به إلى العالم الخارجي بمعنى أن الركن المادي للجريمة الإتلاف المعلوماتي.

وأخيرا الركن المعنوي من خلال النصوص المختلفة إضافة على بعض التطبيقات القضائية، فالركن المعنوي هو الإرادة التي يقترن بها الفعل سواء في صورته القصد أو الخطأ، كما أن لهذه الجريمة كغيرها من الجرائم أطراف تتمثل في الجاني (المجرم الالكتروني) وبهذا المعنى يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي إما عليه يكون في الغالب الأعم شخص معنوي كالبنوك والشركات وغيرها من المنظمات والهيئات

التي تعتمد في إنجاز أعمالها على الحاسب الآلي، إن للجريمة محلا يتمثل في المعلومات، الأجهزة، الأشخاص، الجهات[1].

الركن المادي لجريمة القرصنة الالكترونية :

يتخذ الركن المادي في جريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة بها modification أو تدميرها distruction أو إدخال غير مشروع للمعلومات داخل أنظمة الحاسبات الآلية.

1. **التعديل غير المشروع للمعلومات المبرمجة آليا:** هو أكثر صور إتلاف المعلومات شيوعا وقد فرقت التوصية الصادرة عن المجلس الأوروبي لعام 2001 المتعلقة بالجرائم المعلوماتية[2] بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات والبرامج، وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث هذه النتائج، بل قد ساعد على تحسين المكونات المنطقية للحاسب الآلي ونظامه. وقد تضمنت التوصية بندا يطالب بإدراج التعديلات الأولى ضمن القائمة الأساسية لجرائم المعلوماتية ولكنه اكتفى في خصوص الثانية بإدراجها ضمن القائمة الاختيارية غير أن الدول التي جرمت إتلاف المعلومات لم تعتد بهذه التفرقة، فمثلا في المملكة المتحدة حددت المادة 17 قانون إساءة استخدام الحاسبات الآلية لعام 1990: أن تعديل المعلومات المعاقب عليه هو التعديل غير المصرح به لمحتوى الحاسب الآلي سواء كان مؤقتا أو دائما[3] .
2. **تدمير المعلومات:** ويعد تدمير المعلومات بدوره صورة من صور الإتلاف وإن كان أبعد أثرا من مجرد إجراء بعض التعديلات للمعلومات، وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى

---

[1] عبد الله دغش، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص27/26.

[2] The recmmendation n°2 (89) on compter – related crime , op.cit , p46

[3] مشار إليه لدى د/ نائلة عادل المرجع السابق، ص 218/ 221 Verguth (pascal) op.cit

تدمير المعلومات وميزت بين شكلين الأول يتعلق بمحو المعلومات تماما، والثاني إخفاء المعلومات حتى لا يمكن الوصول إليها دون أن يترتب عن ذلك محوها تماما. غير أننا نرى إخفاء المعلومات دون محوها لا يمكن أن يشكل إتلافا لها، باعتبار أنه يؤدي فقط إلى تعديل في قائمة الملفات فحسب ولا يترتب محوها كليا من ذاكرة الحاسب.

3. **الإدخال غير المشروع للمعلومات :**

أحسانا يكون لإدخال غير المشروع للمعلومات مسببا في تعديل المعلومات أو تدميرها كليا بذاكرة الحاسب مثلما هو الحال في إدخال البرامج الخبيثة إلى نظام الحاسب الآلي. وقد نصت العديد من الدول في قوانينها على جريمة الإتلاف المعلوماتي، على الإدخال غير المشروع للمعلومات كصورة من صور الركن المادي لهذه الجريمة مثل فرنسا، والسويد، هولندا، أستراليا.

الركن المعنوي في جريمة الإتلاف المعلوماتي:

من خلال استعراض صور الركن المادي لجريمة الإتلاف المعلوماتية تبين لنا أنها جريمة عمدية تتطلب القصد العام، أي علم المتهم أنه يقوم بإحدى الأعمال التي أوردها النص القانوني والتي من شأنها أن تؤدي إلى إتلاف المعلومات، وأن تتجه إرادته إلى ارتكاب الفعل وإلى تحقيق هذه النتيجة.

غير أن هناك تشريعات يتطلب فعل الإتلاف فيها الدخول غير مصرح به إلى نظام الحاسب الآلي كالقانون الإنجليزي، هنا يجب انصراف علم المتهم أولا على الدخول الذي يقوم به إلى نظام الحاسب الآلي غير مصرح به.

وهنا بعض التشريعات التي تتطلب إلى جانب القصد العام قصدا خاصا مثلا القانون البرتغالي يتطلب أن تتجه نية المتهم إلى الإضرار بالغير أو تحقيق الربح غير مشروع له أو للغير.

وقد تم انتقاد تطلب القصد الخاص في جريمة الإتلاف المعلوماتي، ذلك أن في كثير من الحالات يتم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية لمجرد التسلية، ثم ينتج عن ذلك أضرارا بليغة مثلما حدث في قضية موريس والتي كلفت الحكومة لإعادة تشغيل الأنظمة التي خربها عدة ملايين من الدولارات.

أما فيما يخص المشرع الجزائري فإننا نجد نص المادة 407 قانون العقوبات تنص على أن "كل من خرب أو أتلف عمدا أمال الغير المنصوص عليها في المادة 396 بأي وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى 5 سنوات وبغرامة من 500 إلى 5000دج".

ونستخلص من نص المادة أنه يمكن تطبيقها على جريمة الإتلاف المعلوماتي باعتبار أن النص جاء عاما، ومع ذلك فقد حسم المشرع الجزائري فيما يخص جريمة إتلاف المعلومات في تعديله الأخير لقانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 151/66 القسم السابع مكرر عنوانه:" المساس بأنظمة المعالجة الآلية للمعطيات" والتي سوف يتم دراستها في مبحث ثاني.

وفيما يخص التطبيقات القضائية بخصوص جريمة الإتلاف فقد ذهب القضاء الفرنسي في تطبيق جريمة الإتلاف للمكونات المنطقية لأنظمة الحاسبات الآلية إلى اعتبار إدخال المعلومات والبرامج على نحو غير مشروع مكونا لهذه الجريمة.

الفرع الثاني: العقوبات المقررة لجريمة القرصنة الالكترونية:

طبقا للمادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة لإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات سالبة للحرية، وتتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناءا على تبني مبدأ مساءلة الشخص المعنوي الوارد في المادة 12 من الاتفاقية [1].

[1] قارة أمال، الحماية الجزائية للمعلومات في التشريع الجزائري، دار هومة، 126.

وفي فرنسا فإن الجريمة المعلوماتية بصورها المتعددة معاقب عليها بالحبس والغرامة أو أحدهما وسنقدم بمناسبة كل جريمة على حدا.

أولا: العقوبات المطبقة على كل من الشخص الطبيعي والمعنوي:

1) العقوبات المطبقة على الشخص الطبيعي:

- ✓ **العقوبات الأصلية:**

المادة 1/323 من قانون العقوبات الفرنسي الجديد عاقبت على فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه بالحبس مدة سنة وغرامة قدرها 100000 فرنك فرنسي أما نص المادة 394 مكرر من قانون العقوبات الجزائري فإنها عاقبت على جريمة الدخول أو البقاء غير المشروع في صورته البسيطة بـ 3 أشهر إلى سنة حبس وغرامة من 50000 دج إلى 100000 دج.

أما جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات في صورتها المشددة فقد نصت عليها المادة 323 من قانون العقوبات الفرنسي في فقرتها الثانية، إن نتج عن الدخول أو البقاء محو أو تغيير في البيانات الموجودة في النظام، أو حدث تعييب لتشغيل ذلك النظام فإن العقوبة تضاعف، وقد حذا المشرع الجزائري حذو المشرع الفرنسي بأن ضاعف العقوبة إذا ترتب عن الأفعال حذف أو تغيير للمعطيات المنظومة فتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب النظام.

وفيما يخص جريمة إعاقة أو تحريف تشغيل نظم المعالجة البيانات فإن المشرع الفرنسي قد جرم هذا السلوك في نص المادة 2/323 ويعاقب عليه

بالحبس مدة ثلاث سنوات وغرامة 300000 فرنك فرنسي لكل من قام بإعاقة أو إفساد تشغيل نظم معالجة البيانات.

أما المشرع الجزائري فإنه لم يتطرق إلى هذه الجريمة كما سبق وإن أشرت بل نص على جريمة التلاعب في بيانات نظم المعالجة الآلية للمعطيات طبقا للمادة 394 مكرر 2 وعاقب عليها بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، فعقوبتها هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 إلى5000000 دج.

✓ **العقوبات التكميلية :**

نص القانون الفرنسي الجديد على مجموعة من العقوبات التكميلية:

- وفقا لنص المادة 5/323 من قانون العقوبات الفرنسي فإنه يجوز أن يقضى بالحرمان من الحقوق السياسية والمدنية والعائلية مدة لا تتجاوز 5 سنوات، والحرمان من تقلد الوظائف العامة أو أي نشاط مهني تكون الجريمة قد ارتكبت بسببه، وغيرها من العقوبات التكميلية المنصوص عليها في المادة 131 من قانون العقوبات الفرنسي.

أما في قانون العقوبات الجزائري فقد نصت المادة 394 مكرر 3 على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في :

- **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير، حسن النية.
- **إغلاق المواقع:** والأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

- **إغلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها.

2) **العقوبات المطبقة على الشخص المعنوي:**

نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي، أن يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا، كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

وحسب نص المادة 6/323 من القانون الفرنسي فإنه يجوز مساءلة الأشخاص المعنوية وتتحدد هذه المسؤولية حسب أحكام المادة 2/21 من ذات القانون ويسأل عنها الشخص المعنوي بصفته فاعلا أو شريكا كما يسأل عن الجريمة التامة وتلك التي تقف عند حد الشروع المادة 2/122 ونصت الفقرة 3و 2 من المادة 121 على أن المسؤولية الجزائية للأشخاص الاعتباريين هي الأخرى لا تخل بالمسؤولية الجزائية للأشخاص الطبيعيين كفاعلين أو شركاء متى توافرت شروطها.

أما المشرع الجزائري فقد أقر هو الآخر في تعديل قانون العقوبات في القانون 15/04 بالمسؤولية الجزائية للشخص المعنوي في نص المادة 18 مكرر تنص على العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح وهي:

- ✓ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.
- ✓ واحدة أو أكثر من العقوبات التالية :
  - حل الشخص المعنوي.
  - غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات.

وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكب الجريمة بمناسبته.

بالنسبة لعقوبة الغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم المعلوماتية فهي تعادل خمس مرات الحد الأقصى للغرامة المطبقة على الشخص الطبيعي طبقا للمادة 394 مكرر 4.

ثانيـا: الجزاءات المقررة للاتفاق الجنائي والشروع:

- **الجزاء المقرر للاتفاق الجنائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيـــات:**

نصت المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي على الاتفاق الجنائي في الجريمة المعلوماتية أما المادة 4/323 قانون العقوبات الفرنسي، فقد عاقب على المساهمة المادية الجماعية أو مجرد الاتفاق الجنائي على ارتكاب الأعمال التحضيرية لهذه الجرائم، ويعد ذلك خروجا عن القواعد العامة التي تقضي بعدم العقاب إلا على الجرائم التامة أو تلك التي تقف عند حد الشروع المعاقب عليه، وهذا بالطبع يتطلب على الأقل البدء في التنفيذ الذي يرمي مباشرة إلى ارتكاب الجريمة.

أما الأعمال التحضيرية التي تسبق البدء في التنفيذ، فإنه لا عقاب عليها كقاعدة عامة ولكن الخروج عن هذه القاعدة قد يجد مبرره في رغبة المشرع لأن يقرر نوعا من الحماية الوقائية

المتقدمة لنظم المعالجة الآلية للمعطيات ضد المخاطر التي تنشأ عن النشاط غير المشروع لجناة المعلوماتية، والذين قد يحضرون لارتكاب جرائم المعلوماتية، وكذلك لمواجهة القرصنة المعلوماتية.

وقد حذا المشرع الجزائري حذو المشرع الفرنسي في نص المادة 394 مكرر 4 والذي عاقب الاتفاق الجنائي بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، ولم يخضعها للمادة 176 قانون العقوبات المتعلقة بجمعية الأشرار، حيث نصت المادة 394 مكرر 5 "كل من شارك في مجموعة أو في اتفاق تألف 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".

والحكمة ذاتها التي أثارها المشرع الفرنسي من توسيع نطاق العقوبة بإخضاع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي بمعنى الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالعقاب، وذلك أن الإعداد للإجرام المعلوماتية تتم عادة في إطار جماعات خاصة منها القرصنة.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي لإعداد جريمة معلوماتية بعقوبة الجريمة ذاتها وشروط العقاب على الاتفاق الجنائي يمكن استخلاصه من نص المادة 394 مكرر 5 قانون العقوبات:

- اشتراط المشاركة في مجموعة أو اتفاق.
- الغرض من المشاركة، الإعداد للجريمة أو أكثر من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل أو عدة أفعال مادية.
- القصد الجنائي.

ثالثا :الجزاءات المقررة للشروع في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات:

نصت عليها المادة 7/323 من قانون العقوبات الفرنسي والذي عاقب على الشروع في الجرائم الماسة بالأنظمة المعلوماتية بالعقوبة المقررة للجريمة في صورتها الكاملة وهذا ما نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي.

وبالرجوع إلى قانون العقوبات الجزائري نجد المادة 394 مكرر 7 تعاقب على الشروع في ارتكاب الجنح المنصوص عليها في القسم الخاص بالمساس بالمعالجة الآلية للمعطيات بالعقوبات ذاتها المقررة للجنحة.

المطلب الثاني: الجرائم التي يكون الحاسوب هدفا لها :

من أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية عندما تكون السرية والتكاملية أي السلامة هي التي يتم الاعتداء عليها، بمعنى أن توجه هجمات الكمبيوتر إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها وغالبية هذه الأفعال المجرمة تتضمن ابتداء الدخول أو البقاء غير المصرح به إلى النظام الهدف والتي توصف بشكل شائع في هذه الأيام بأنشطة "الهاكرز" كناية عن جرائم الاختراق Haching.

وكان هناك اتجاه في الفقه الفرنسي يرى أنه يمكن أن تطوع النصوص الجزافية التي تتعلق بجرائم الأموال في صورتها التقليدية مثل السرقة، النصب، خيانة الأمانة والإتلاف، وتعدل هذه النصوص حتى تتفق وطبيعة المال في صورته المعلوماتية، غير ان هذه المحاولات لم يكتب لها النجاح في كثير من الدول باعتبار أنها يمكن أن تشوه المبادئ المستقرة التي تقوم عليها تلك الجرائم.

فضلا أنها لا تحقق الحماية الكافية للمال المعلوماتي والذي تختلف طبيعته عن المال التقليدي، والقول بغير ذلك يؤدي إلى ثغرة في نظم حماية المال المعلوماتي [1].

وعليه استقر الفكر القانوني لدى المشرعين، ومنهم فرنسا، أنه لا بد من وجود نصوص خاصة لتجريم الأفعال التي تمثل إساءة لاستخدامات الحاسب الآلي والانترنت، كما سارعت الدول التي سبقت في استخدام هذه التكنولوجيا في إصدار تشريعات ومنها الولايات المتحدة الأمريكية، ألمانيا، السويد، النرويج.....الخ.

وقد أدمج المشرع الفرنسي مشروعا في قانون العقوبات الفرنسي أصبح يشكل الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات، وهو يتعلق بالجرائم المعلوماتية، وذلك في المواد(9/462-2/462) ومضمونها تجريم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو جزء منه، وتشدد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل هذا النظام أو إفساد وظيفته [2].

كما جرم أيضا كل من تعمد بدون مراعاة لحقوق الغير، إدخال معطيات في النظام أو محو أو تعديل المعطيات الموجودة فيه أو طرق معالجتها أو نقلها، سواء تم ذلك بطريقة مباشرة أو غير مباشرة، كما أن هذه تجرم أي فعل من شأنه أن يعرقل أو يفسد عمدا، دون مراعاة حقوق الغير، أداء النظام أو وظيفته، كما يجرم تزوير المستندات المعالجة آليا، أيا كان شكلها وكذلك استعمال تلك المستندات، ويجرم أخيرا الشروع في ارتكاب الجرائم السابقة وكذلك الاتفاق الجنائي على ارتكابها[3].

غير أنه بعد صدور قانون العقوبات الفرنسي الجديد عام 1994 عدلت المادة 1/441 من قانون العقوبات جريمة التزوير، وبهذا التعديل أصبحت جريمة –التزوير المعلوماتي– ليست

---

[1] . د.علي عبد القادر القهوجي، المرجع السابق، ص28 وراجع كذلك الخلاف في شأن طبيعة المال المعلوماتي د/محمد سامي الشوا ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1998، ص174 وما يليها.

[2] د/ أحمد حسام طه تمام، المرجع السابق، ص40.

[3] د/ أحمد حسام طه تمام، المرجع السابق، ص261، د/ علي عبد القادر القهوجي، المرجع السابق، ص40 وكذلك مؤلفنا –الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت مرجع سابق، ص116 وما بعدها.

مجرد جريمة تقع على المستندات المعالجة آليا فقط، بل أصبحت جريمة تزوير للمستندات المعلوماتية واستعمالها [1].

وبذلك أخرج المشرع الفرنسي جرائم التزوير للمستندات المعالجة آليا وأخضع أفعال التزوير المعلوماتي للنصوص التقليدية وهذا ما غفل عنه المشرع الجزائري إذ رغم تعديله الأخير لقانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 بقسم سابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات" إلا أنه لم يتطرق إلى التزوير المعلوماتي ولم يحدث نصوصا خاصة به بل حتى أنه لم يحذ حذو المشرع الفرنسي بتعديل نصوص التزوير التقليدية وهذا ما يجعلنا أما فراغ قانوني.

أما بخصوص الجرائم الماسة بالأنظمة المعلوماتية فإننا نجده قد تمم الفصل الثالث من الباب الثاني بقسم سابع مكرر يشمل المواد من 394 مكرر سبعة، والتي تحقق حماية جزئية لنظم المعالجة الآلية للمعطيات على غرار المشرع الفرنسي وعليه تدرج مفهوم نظام المعالجة الآلية للمعطيات نظرا لكونه تعبيرا تقنيا يصعب على رجال القانون إدراكه ونبين كذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ونقصد بمفهوم نظام المعالجة الآلية للمعطيات سبق وان أشرت أن اشتراط وجود نظام معالجة البيانات أو المعالجة الآلية للمعطيات بمثابة الشرط الأول الذي يلزم تحقيقه حتى يتم بحث ما إذا كان هناك اعتداء على نظم المعالجة الآلية للبيانات من عدمه.

وقد كان مجلس الشيوخ الفرنسي قد اقترح تعريفا لنظام المعالجة الآلية للبيانات بأنه:"كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال و الإخراج وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية" [2].

[1] راجع مفهوم الوثيقة المعلوماتية أو المستند الالكتروني.
[2] د/ علي عبد القادر القهوجي، المرجع السابق، ص43- د/ أحمد حسام طه تمام المرجع السابق، ص204.

ويلاحظ على هذا التعريف أنه أشار للعناصر المادية والمعنوية التي يتكون منها المركب، أساس نظام المعالجة الآلية للبيانات، وهذه العناصر وردت على سبيل المثال لا الحصر[1]،كما تعرف المادة رقم 14/1 من القانون العربي النموذجي الموحد نظام المعالجة الآلية للمعطيات بأنه:" يقصد به كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة".

وقد أثار الفقه الفرنسي سؤالا فيما إذا كان النظام يشترط حماية فنية حتى تقوم الجريمة أم لا والرأي الغالب في الفقه الفرنسي يرى أن الشرط ليس ضروريا، ذلك أن هذا الشرط وجوده لا يكون له سوى دور واحد وهو إثبات سوء نية من قان بانتهاك النظام والدخول إليه بطريقة غير مشروعة ويدخل في ذلك عبء إثبات القصد الجنائي وهذه مسألة أخرى[2].

أما الرأي الآخر فإنه يرى ضرورة وجود نظام أمني، ذلك أن القانون يجرم الاعتداء على نظم الأمن المتضمنة في النظام المعلوماتي[3].

ويستند الرأي الثاني إلى عدة أسانيد منها أن الاعتداء على النظام الأمني شرط مفترض لقيام الجرائم التي تتعلق بنظم المعلوماتية، ويبين ذلك من الأعمال التحضيرية عند مناقشة القانون والعدالة تقتضي عدم العقاب على نص يعد اعتداء على حق لم يحتط له صاحبه، فضلا على التسليم برأي غالب الفقه يعني التوسع في مجال التجريم، فكل دخول غير مشروع يعد جريمة وذلك أمر غير منطقي[4].

غير أننا نرى أن الإشكال مفرغ من محتواه ولا يحتاج إلى أي اجتهاد وذلك أن المبدأ المستقر في القانون الجزائري "مبدأ الشرعية" وعليه فإن عدم ذكر المشرع أو عدم اشتراطه لشرط الحماية الفنية يعني أنه أراد استبعاد هذا الشرط صراحة.

---

[1] د/ علي عبد القادر القهوجي، المرجع السابق، ص43، د/ أحمد حسام طه تمام، المرجع السابق، ص205.

[2] M.Andre , rapport ou nom de la commision de lois, n° 144P 13 مشار إليه لدى دم أحمد حسام طه تمام، المرجع السابق،ص264.

[3] من أنصار هذا الرأي الفقيه الفرنسي allerman et blach مشار إليه لدى د/ أحمد حسام طه تمام، المرجع السابق، ص265.

[4] د/ علي عبد القادر القهوجي، المرجع السابق، ص44 وما بعدها.

كما أنه من الناحية العملية فإن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية ووجود مثل هذا النظام يساعد في إثبات أركان الجريمة وبصفة خاصة الركن المعنوي[1].

الفرع الأول :جرائم الاعتداءات الماسة بأنظمة المعلوماتية :

بعد أن تطرقنا إلى الركن المفترض في جرائم اختراق نظم المعالجة الآلية للمعطيات يأتي الحديث عن الركن المادي والمعنوي لكل جريمة على حدا.

أولا :الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

قد نصت عليها المادة 1/323 قانون العقوبات الفرنسي الجديد ونص المادة 394 مكرر قانون العقوبات الجزائري.

كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي .

وباستقراء هذه النصوص نجد صورتين للركن المادي لهذه الجريمة .

الصورة الأولى: وهي الصورة البسيطة لفعل الدخول أو البقاء غير المشروع.

الصورة الثانية: هي الصورة المشددة للعقاب على فعل الدخول أو البقاء غير المشروع وفيها تضاعف العقوبة المقررة للجريمة في صورتها البسيطة[2].

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام أو اختراقه فيجوز إذن الدخول إلى النظام بأي وسيلة تقنية ومن ذلك انتهاك كلمة السر الحقيقية "Pass word" متى كان الجاني غير مخول في استخدامها أو عن طريق استخدام برنامج أو شفرة خاصة.

كما يمكن كذلك استخدام الرقم السري لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول، ومن صور الدخول الغير المشروع كذلك أن يكون مالك النظام قد وضع قيودا على الدخول إليه، ولم يحترم الجاني هذه القيود ، أو كان الأمر يتطلب سداد مبلغ من النقود لم يسددها الجاني، وتحايل وقام بالدخول غير المشروع إلى النظام.

[1] د/ علي عبد القادر القهوجي، المرجع سابق، ص123.
[2] سأتطرق على الجزاء في الفصل الثاني.

والملاحظ أن المشرع يعاقب على الدخول المجرد إلى النظام المعلوماتي، ذلك أن مجرد الدخول إلى النظام تقوم به الجريمة حتى لو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول فائدة، طالما أن الدخول غير مشروع [1].

ويتحقق فعل الدخول متى دخل الجاني إلى النظام كله أو جزء منه، كالدخول إلى طرفية الحاسب أو شبكة الاتصال أو البرنامج، كما يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول إلى جزء معين من البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه[2].

أما فعل البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فقد كان الهدف من تجريمه هو تجريم البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات لمن كان دخوله إلى النظام بطريق الصدفة البحتة، وانتفى لديه القصد الجنائي ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك، حيث يعاقب الجاني على الجريمة العمدية لأن إرادته انصرفت إلى البقاء داخل النظام رغم علمه بأن دخوله غير مشروع [3]، وذلك الحكم ينصرف إلى من هو مسموح له بالدخول على جزء من النظام ثم يدخل إلى جزء آخر غير مصرح له بالدخول فيه. وهناك جانب من الفقه يعرف البقاء غير المشروع بأنه: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[4].

كما يعد صورة للبقاء غير المشروع أيضا أن يظل الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة من المعلومات، في الوقت الذي كان مسموحا له بالرؤية والاطلاع فقط.

ومفهوم الدخول والبقاء غير المشروع على النحو السابق يمثل مفهوما للنشاط الإجرامي سواء في صورته البسيطة أو المشددة وهو ما سنبحثه حالا:

[1] د/ علي عبد القادر القهوجي، المرجع السابق، ص52.
[2] د/ أحمد حسام طه تمام، المرجع السابق، ص30.
[3] د/ أحمد حسام طه تمام، المرجع السابق، صَ299.
[4] د/ علي عبد القادر القهوجي، المرجع السابق، ص52.

أولا: الصورة البسيطة : تتحقق الصورة البسيطة بفعل الدخول غير المشروع أو البقاء غير المشروع في النظام الذي تم اختراقه، وقد عدت هذه الجريمة بمثابة الصورة البسيطة لأن المشرع الفرنسي عاقب عليها بالحبس مدة سنة وغرامة مائة ألف فرنك فرنسي، وضاعف العقوبة متى اقترن بها ظرف مشدد أما المشرع الجزائري فقد حذا حذوه، إذ نص في مادة 1/394 مكرر على الصورة البسيطة وفي الفقرة الثانية ضاعف العقوبة إذا اقترنت بظرف مشدد وحتى يتحقق الركن المادي لهذه الجريمة في صورتها البسيطة يجب تحقق فعل الدخول غير المشروع أو البقاء غير المشروع، على النحو السابق بيانه، أو يتحققان معا، وذلك حتى يقوم الركن المادي لهذه الجريمة في صورته البسيطة.

وجريمة الدخول على النظام أو البقاء فيه، هي من الجرائم العمدية التي تقوم على القصد الجنائي العام الذي يتكون من عنصري العلم والإرادة.

ذلك أنه يجب أن يعلم الجاني بأنه لا يحق له الدخول او البقاء داخل النظام، وأن ذلك ضد رغبة مالك النظام أو صاحب السيطرة عليه، ومع ذلك تنصرف إرادته إلى إتيان هذا الفعل بالمخالفة للقانون وبالمخالفة لإرادة صاحب النظام أو صاحب الحق فيه[1].

ولهذا يرى جانب من الفقه يرى أن الدخول يكون مشروعا متى كان بطريق الصدفة أو السهو أو الخطأ وعلى الشخص الذي دخل بهذه الطريقة أن ينسحب فورا، فإذا لم ينسحب منذ هذه اللحظة توافر في حقه القصد الجنائي العام، لارتكاب هذه الجريمة ويعاقب، ونرى مع جانب آخر من الفقه أن الدخول بطريق السهو أو الخطأ أو المصادفة هو سلوك يتسم بعدم المشروعية لكن المشرع لا يعاقب عليه لانتفاء القصد الجنائي[2].

ووفقا للتحديد السابق للقصد الجنائي، فإن الركن المعنوي لا يتوافر متى كان الدخول الجاني أو بقائه داخل النظام مسموح به أي مشروعا، كذلك لا يقوم القصد الجنائي إن وقع الجاني في خطأ يتعلق بحقه في الدخول أو حقه في البقاء أو في مدى نطاق هذا الحق كأن يجهل وجود حظر للدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول.

[1] د/ علي عبد القادر القهوجي، المرجع السابق، ص53.
[2] د/ علي القهوجي، المرجع السابق، ص54.

ولذلك فمتى توافر القصد الجنائي بعنصرية العلم والإرادة، فإنه لا محل للاعتداد بالباعث على ارتكاب الجريمة، وبالتالي تقوم الجريمة ولو كان الباعث على الدخول إلى النظام أو البقاء فيه، محاولة الفضول أو النزهة أو إثبات القدرة على الانتصار على النظام المعلوماتي.

ثانيا :الصورة المشددة : تحقق هذه الجريمة في صورتها المشددة، متى ترتب على الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام ذاته لأن يؤدي وظيفته.

ويكفي لتوافر هذا الظرف المشدد، أن يكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات، وهذه النتيجة ذاتها هي التي اعتبرها المشرع ظرفا مشددا في هذه الجريمة[1].

وهذه الجريمة عمدية يتعين لقيامها توافر القصد الجنائي العم لدى الجاني بعنصريه العلم والإرادة، فإذا أثبت الجاني انتفاء علاقة السببية بين السلوك الإجرامي الدخول أو البقاء غير المشروع، والنتيجة الإجرامية التي هي ذات الظرف المشدد في الجريمة، كأن يثبت أن تعديل محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ، انتفى السلوك الإجرامي وكذلك القصد الجنائي لدى الجاني، وإذا توافرت أركان جريمة الدخول أو البقاء غير المشروع في صورتها المشددة، عوقب الجاني بالعقوبة المقررة لها.

ثانيا: جريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات:

نصت عليها المادة 1/323 من قانون العقوبات الفرنسي الجديد التي عاقبت على هذا السلوك بعقوبة الحبس والغرامة على كل من قام بإعاقة أو إفساد تشغيل نظم المعالجة الآلية

[1] د/ جميل عبد الباقي الصغير، القانون الجبائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسوب اللي، دار النهضة العربية، القاهرة، 1992، ص20.

للمعطيات، كما نصت عليه المادتين 5و 8 من الاتفاقية الدولية لإجرام المعلومات أما المشرع الجزائري فإنه لم بورد نصا خاصا بجريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات واكتفى بجريمة التلاعب في بيانات نظم معالجة البيانات.

والتعطيل أو التوقيف، الذي يندرج ضمن إعاقة النظام المعلوماتي يقع بأي وسيلة، فالمشرع لم يشترط وسيلة معينة، وقد يتم التعطيل بإدخال فيروس على البرنامج أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة ما على سبيل المثال، لأن يتبطأ هذا النظام عن أداء وظيفته المعلوماتية داخل النظام المعلوماتي[1].

أما التعييب فيقصد به الإفساد، وهو لا يعطل نظام معالجة البيانات، لكنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[2].

وقد لاحظ جانب من الفقه أن التعييب المعاقب عليه في نص المادة 2/323 يكاد يقترب من التعييب الذي يعد ظرفا مشددا حسب المادة 1/323 والفرق بينهما إن الإفساد في حال الظرف المشدد لا يشترط أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة لهذه الجريمة التي نحن بصدد دراستها، فالقصد الجنائي في المادة (1/323) ينصرف لفعل الدخول غير المشروع أو البقاء غير المشروع وذلك في صورته البسيطة أو صورته المركبة، أما القصد الجنائي في فعل التعييب في المادة 2/323 من قانون العقوبات الفرنسي، ينصرف إلى إفساد النظام، وعلى ذلك لا يكون الإفساد نتيجة، بل هو مضمون السلوك الإجرامي في هذه الجريمة.

ومن وسائل التعييب أو الإفساد استخدام القنبلة المعلوماتية أو استخدام البرنامج الذي يحمل فيروس يطلق عليه "حصان طروادة" وغير ذلك من الفيروسات التي تجعل مخرجات النظام غير تلك التي كان يجب عليه أن يخرجها، بل أن الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادية في النظام، ويستوي أن يؤدي نشاط الجاني إلى توقف النظام

[1] د/ علي عبد القادر القهوجي، المرجع السابق، ص56.
[2] د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي وشبكة الانترنت، دراسة مقارنة دار النهضة العربية، 2000، القاهرة.

عن العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أو بأي وسيلة من شأنها أن تعيق حسن سير النظام كالاعتداء المادي على النظام أو نشر فيروس به، حيث يستوي لدى المشرع الوسيلة المستخدمة، ولا يشترط أن تكون الإعاقة أو الإفساد بصورة كلية، بل يمكن أن يؤدي النشاط إلى إعاقة أو إفساد جزئي للنظام [1].

ويتعين كذلك الإشارة إلى أن هذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصريه العلم والإرادة.

ويرى جانب من الفقه الجنائي الفرنسي أنه إذا قام الشخص الذي يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات، ينفي القصد الجنائي لديه، ولا يسأل عن هذه الجريمة [2].

الفرع الثاني : جريمة التلاعب في بيانات نظم المعالجة الآلية للمعطيات:

نصت عليها المادة 462-4 من قانون العقوبات الفرنسي القديم قبل تعديله عام 1994، لكن المشرع عاد ونص على مضمون ذات النص من المادة 3/323 من قانون العقوبات الجديد وعاقب على "إدخال البيانات" في نظام معالجة البيانات أو إلغاء أو تعديل البيانات المثبتة فيه.

ما نصت عليها المواد 03، 04، 08، من الاتفاقية الدولية للإجرام المعلوماتي، والمادة 394 مكرر 2 من قانون العقوبات الجزائري تعاقب على كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدم بطريق الغش المعطيات التي تتضمنها.

وعليه يبدو واضحا أن المشرع لا يحمي نظام البيانات من الناحية المادية بقدر ما يوفر الحماية للمعلومات الموجودة داخل النظام ذاته، وذلك ضد أي نشاط إجرامي وهو ما يطلق

[1] د/ مدحت رمضان، الحماية الجنائية الالكترونية، ص54.
[2] د/ مدحت رمضان، المرجع السابق، ص55.

عليه القرصنة المعلوماتية، علما أن هدف الجاني من هذه الجريمة، أن يحقق النظام المعلوماتي نتائج أو معطيات غير تلك التي كان يجب أن يحققها[1].

والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال، المحو والتعديل، ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها ومن ثم قيام الركن المادي في الجريمة.

وجريمة التلاعب في بيانات نظم المعالجة الآلية للمعطيات تقع على المعطيات أي بيانات المعالجة دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج بعد.

وصور الركن المادي في هذه الجريمة كما يلي :

1. فعل الإدخال.
2. فعل المحو.
3. فعل التعديل.

أولا : فعل الإدخال :

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل[2].

ومن صور إدخال المعلومات المصطنعة "اختلاس النقود عن طريق الغش المعلوماتي"، ويتحقق كذلك فعل الإدخال في القرض الذي يتمكن فيه الحامل الشرعي لبطاقة السحب الممغنطة والتي تسحب النقود من البنوك وتحديدا أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص–السري– للدخول كي يسحب مبلغا أكثر من ذلك المبلغ المسموح به لصاحب البطاقة.

[1] د/ مدحت رمضان، المرجع السابق، ص356 وما بعدها.
[2] د/ علي عبد القادر القهوجي، المرجع السابق، ص59.

أو في حالة إدخال فيروس "حصان طروادة" أو "قنبلة معلوماتية" تؤدي إلى إضافة معطيات جديدة.

ثانيا : فعل المحو :

يقصد به إزالة جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[1].

ثالثا: فعل التعديل :

ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطياتها أخرى[2] وقد يتم التلاعب في المعطيات عن طريق استبدالها أو عن طريق التلاعب في البرنامج، وذلك بإمداده بمعطيات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها.

وكقاعدة عامة فإن المحو أو التعديل للمعطيات الموجودة في النظام، كصورتين للركن المادي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات، يتم عن طريق برامج خبيثة تتلاعب في هذه المعطيات وذلك بمحوها كليا أو جزئيا أو بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات، سواء أكانت منطقية أو زمنية.

والملاحظ أن الأفعال السابقة سواء الإدخال أو المحو أو التعديل قد وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها، فلا يخضع مثلا للتجريم فعل النسخ أو النقل أو التنسيق أو التقريب للمعطيات.

لأن كل هذه الأفعال لا تنطوي على إدخال أو محو أو التعديل بالمفهوم السابق [3] وهذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي بركنيه العلم والإرادة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل وعلمه بأن نشاطه غير مشروع وأنه

[1] د/ علي عبد القادر القهوجي، المرجع السابق، ص 59.
[2] د/ علي عبد القادر القهوجي، المرجع السابق، ص51.
[3] د/ علي عبد القادر القهوجي، المرجع السابق، ص60.

يعتدي على صاحب الحق في المعطيات–محل الاعتداء– ومع ذلك تتجه إرادته إلى ذلك الفعل رغما عن إرادة صاحب الحق في المعطيات أو من له السيطرة عليها[1].

المبحث الثاني: الجوانب الإجرائية لجريمة القرصنة الالكترونية:

تمهـيد :

من خلال ما سبق تطرقنا في المبحث الأول إلى دراسة الجوانب الموضوعية لجريمة القرصنة الالكترونية، وهذا المبحث خصصناه للجوانب الإجرائية لهذه الجريمة، فالمشرع الجزائري سارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية وذلك بتعديل بعض المواد في قانون إ.ج وإصدار قوانين خاصة وجديدة في مجال الإجراءات قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والقانون رقم 18/07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المطلب الأول :المكافحة الإجرائية في القانون الجزائري:

المكافحة الإجرائية في القانون الجزائري المشرع الجزائري سارع لمواكبة هذا التطور لحق الجريمة لمكافحتها من الناحية الإجرائية وذلك بتعديل بعض الموارد في قانون الإجراءات الجزائية و إصدار قوانين خاصة وجديدة مجال الإجراءات .

الفرع الأول :المكافحة الإجرائية في القانون 09/04:

نظم المشرع الجزائري في القانون رقم **09/04** المؤرخ في 5 أوت 2009 والمتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة لتكنولوجية الإعلام و الاتصال ومكافحتها أحكاما جديدة وخاصة بمعالجة الجريمة المعلوماتية تتماشى و التطور الذي لحق بهذه الجريمة من هذه القواعد ما نص عليه في المادة 03 منه التي تضمنت إجراءات جديدة التي تتطلبها التحريات و التحقيقات القضائية .

[1] د/ مدحت رمضان، المرجع السابق، ص56.

- مراقبة الاتصالات الإلكترونية وتجميعها حيث نجد أن المشرع الجزائري الإجرام رغم ضمانته لسرية المراسلات و الاتصالات بكل أشكاله المادة المحدد حصرا .
- قيام بإجراءات التفتيش وحجز المنظومة المعلوماتية ، كما يبين قانون 04/09 في المادة الرابعة الحالات التي يسمح بتطبيق الإجراء الجديد المتمثل في مرا قبة الاتصالات الالكترونية وذلك على سبيل الحصر وهذه الحالات هي :
- الوقاية من الأفعال الموصوفة بجرائم التخريب ، أو الجرائم الماسة بأمن الدولة .
- في حالة توفير معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة و الاقتصاد الوطني .
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة تنص المادة 16 من القانون 04/09على إمكانية تبادل المساعدة القضائية على مستوى الدولي لنجاح عمليات التحقيق التحريات لمكافحة الجرائم المعلوماتية[1] .

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجأ المحقق إلى مجموعة إجراءات بعضها يهدف الحصول على الدليل وتسمى إجراءات جمع الدليل كالتفتيش و الضبط و المعاينة و الشهادة والخبرة أو بعضها لآخر يمص للدليل و يؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المختصم كالقبض و الحبس المؤقت [2].

- وسوف تقتصر دراستنا على إجراءات جمع الأدلة المادية التي يكون منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل و المنطق فهي فهي أقوى مفعول حتى الاقتناع من الأدلة القولية على أن نخص بالدراسة التفتيش وضبط الأشياء باعتبارها أهم التحديات الإجرائية لجرائم الكمبيوتر .

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة ماجستير في القانون الجنائي، جامعة الجزائر 1، كلية الحقوق 2011/2012، ص13.

[2] محمد الأمين البشري، ص373.

- كما قرر المشرع الجزائري بموجب المادة45 من القانون رقم22/06 المؤرخ في 20 ديسمبر 2006 في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو قرر له بعض الضوابط والقواعد .

ويجب أن يقوم بتفتيش نظام الحاسوب الآلي سلطة مختصة بالتحقيق [1].

الفرع الثاني :المكافحة الإجرائية في قانون الإجراءات الجزائية:

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا نع التطور المعلوماتي الذي لحق بالجريمة ، محاولة منه الحد من انتشارها ، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام ، وضع قواعد و أحكام خاصة لسلطة المتابعة و الاختصاص الغرض عنها هو مواجهتها وهذه الأحكام هي [2]:

- جواز تمديد الاختصاص المحلي للمحكمة: حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .
- توسيع مجال اختصاص النيابة العامة: حيث بموجب المادة 37 من قانون الإجراءات الجزائية تم توسيع مجال اختصاص النيابة العامة حيث نصت هذه المادة على تمديد لاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم آخر .
- العمل بنظام المشروعية في تحريك الدعوة العمومية :

حيث سحب نظام الملائمة من النيابة في مجال اختصاص النيابة العامة في مجال متابعة بض الجرائم حيث يلتزم وكيل الجمهورية بتحريك الدعوى بقوة القانون .

وإضافة إلى ما سبق في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث و التحري عن هذه الجرائم بمنح الإذن بالتفتيش، و القيام باعتراض المراسلات وتسجيل الأصوات و التقاط الصور حيث

[1] أمال قارة ، ص59.

[2] طرشي نورة، المرجع السابق،ص134.

نصت المادة 65 مكرر5 في إطار تعديل قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20.

الفرع الثالث : إثبات الجريمة أمام الجهة المختصة :

أولا: إجراءات الحصول على الدليل الالكتروني والتحقيق فيها:

1. التفتيــش:

التفتيش في مدلوله القانوني بالنسبة للجرائم المعلوماتية لا يختلف عن مدلوله السائد في فقه الإجراءات الجزائية رغم اختلاف المحل التي يقع عليه التفتيش.

ويقصد به إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها[1].

ويثير موضوع التفتيش الذي يقع على نظم الحاسب الآلي مسائل عديدة للبحث كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتقع في أماكن عامة أو خاصة، وضوابط هذا التفتيش.

- **مدى صلاحية الكيانات المعنوية كمحل يرد عليه التفتيش:**

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة فإن البعض قد شكك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنوية للحاسب الآلي وهو ما حذا ببعض التشريعات بأن تنص صراحة على أن التفتيش يتم بالنسبة لأنظمة الحاسب الآلي مثل ذلك قانون إساءة استخدام

[1] د/ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ص73 وما بعدها.

الحاسب الآلي في إنجلترا الصادر في سنة 1990 حيث نص أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي [1].

وهناك تشريعات أخرى قد أجازت تفتيش أي "شيء" له علاقة بالأفعال الإجرامية مثلما هو الحال بالمشرع الجزائري وعلى ضوء ذلك فإن تفتيش المكونات المعنوية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاما دون تقييد.

ثم إن نظرة الفقه في الكثير من دول العالم إلى مصطلح "الأشياء" التي ترد عليها جرائم الاعتداء على المال نظرة واقعية، بحيث أن هذا المصطلح لا يجب ان يظل جامدا عند معناه الحرفي وإنما يجب أن يؤخذ بأكثر شمولية من معناه المادي حتى أن بعض الفقه في فرنسا[2] ذهب إلى أن برامج الحاسبات الآلية المتمثلة في النبضات والإشارات والذبذبات الالكترونية المغناطيسية أو الكهرومغناطيسية لها كيانها المادي الملموس، فالشيء يكون محلا للحماية الجنائية بالنظر إلى القيمة التي يتمتع بها والتي قد تتمثل في منفعة مالية أو اقتصادية ولا فرق بين الأشياء المادية والأشياء المعنوية من حيث المنفعة التي قد يحصل عليها صاحبها، بل إن بعض الأشياء المعنوية قد تكون لها قيمة اقتصادية تعلو بكثير على الأشياء المادية، كالأسرار التجارية والصناعية[3].

وعلى ضوء هذه الآراء الفقهية، وعلى النحو الذي قننه المشرع الجزائري صراحة في إمكانية وقوع التفتيش على مساكن الأشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية فإن التفتيش يرد على الكيانات المعنوية في الحاسبات الآلية، بحسب ان هذه الكيانات المعنوية وان كانت غير مادية غلا أنها في نطاق الأشياء المادية[4].

---

[1] Wasik (martin) , computer crimes and other crimes against information technology in the united kingdom-rev , inter,De,Dr,panal 1993, p,640

[2] Sagros »pierre » et masse « michel » le droit penal et l'informatique journnée d'étude du 15 novombre 1982 publication à l'institue de science criminelle de le faculte IV-p25

[3] Gautal(jean- louis) , la protection penale des logiciel « le droit criminel face aux technologie nouvelles de la communication » p254 et 255

[4] د/ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص89.

ويترتب على ذلك انه يمكن تفتيش نظام المعلومات الحاسب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة آليا كالاسطوانات و الأقراص والأشرطة الممغنطة والمخرجات الحاسب، ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته[1].

2. ضوابط التفتيش الذي يقع على نظم ومكونات الحاسب الآلي:

لقد تطورت طرق التفتيش حيث أنها أصبحت لا تقف–فقط– عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الالكترونية خاصة الحاسب الآلي، أو تقع عليه، فيمكن تبعا لذلك تسجيل البيانات المعالجة آليا بعد تحويلها من نبضات أو ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط[2].

ويخضع التفتيش لشروط مقيدة يجب مراعاتها تحت طائلة البطلان.

إذ تنص المادة 44 من قانون الإجراءات الجزائية بعد تعديله بالقانون رقم 06–22 عدم جواز إجراء التفتيش من قبل ضابط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ثم تنص المادة 45 على القيود التي يتعين على ضابط الشرطة القضائية احترامها أثناء فترة التفتيش بصفة عامة لكن أضاف التعديل وتمم نص المادة 45 بأن رفع القيود الواردة فيها فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا ما تعلق منها بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات.

[1] د/ هشام رستم، الجوانب الإجرائية، المرجع السابق، ص69.

[2] Jean p, spreutels,les crimes informatiques et d’autres crimes dans les domaines de la technologie informatique en Belgique-rev- inter de-dr pen 1993- p170

كما أجاز في نص المادة 47 إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة 47 من قانون الإجراءات الجزائية، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة المالية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

غير أن المشرع لم يتطرق إلى المحل الذي يرد عليه التفتيش بصفة مدققة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ذلك أن التفتيش هنا يقع على نظام معلومات الحاسب أو الوسائط أو أوعية حفظ وتخزين البيانات المعالجة الكترونيا كالاسطوانات والأقراص و الأشرطة الممغنطة ومخرجات الحاسب.

ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته[1].

والملاحظ أن المشرع الجزائري عندما عدل نصوص المواد المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد خص حسب رأيي على الحسابات الآلية داخل الدولة وحتى لو اتصلت مع بعضها البعض فيكون ذلك عن طريق شبكة محلية.

لكن يطرح التساؤل هنا في حالة ما إذا اتصلت بحسابات أخرى خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة ، ومنها شبكة الانترنت.

ففي حالة وقوع جريمة في نظم الحاسب الآلي داخل الدولة الجزائرية فيجوز هنا لوكيل الجمهورية أو قاضي التحقيق إصدار الإذن بالتفتيش.

لكن هذا الإذن بالتفتيش لا ينفذ إلا على الحاسب الآلي الذي صدر من أجله، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن بالتفتيش لا يمك أن يمتد إليه التفتيش حتى لو كان يحتوي على الجريمة.

[1] د/ هشام رستم، المرجع السابق، ص69.

إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة 47.

لكن في حالة الإذن بالتفتيش على حاسب واحد معين، يتعين استصدار إذن جديد بالتفتيش للحاسب الثاني إذا تبين أنه متصل عن طريق شبكة داخلية بالحاسب الذي أذن التفتيش فيه.

لكن هناك حالة أخرى أكثر تعقيدا تواجه التفتيش على الحاسب الآلي وذلك عندما يقوم بعض الجناة بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة الجزائرية مستخدمين في ذلك الاتصالات البعدية أو مواقع خارج الجزائر مستهدفين عدم إمكان الوصول إليها وفي هذه الحالة فإن تفتيش هذه الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الجولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها، غير أنه يمكن اتخاذ هذا الإجراء عن طريق اتفاقات خاصة تعقد بين الدول المعنية.

وكتطبيق لهذا الإجراء فقد حدث في ألمانيا أثناء إجراءات التحقيق عن جريمة الغش وقعت في بيانات حاسب آلي، ذلك أنه قد تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين [1] ولقد أدرك المجلس الأوروبي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الالكترونية في لأكثر من دولة فأصدر التوصية رقمR9513 التي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود Perquisition transfrontière

لكن الجزائر لحد الآن لم تنظم إلى أي من المعاهدات أو الاتفاقيات الخاصة بجريمة المعلوماتية.

[1] Mohrenschlager « manfred » op.cit, P351 www.anablawinfo.com

3. التحقيــق في جريمة القرصنة الالكترونية :

من خلال ما سبق ذكره أن جريمة القرصنة الالكترونية تندرج ضمن الجريمة المعلوماتية وتعتبر نوع من أنواع الجريمة المعلوماتية، وتعتبر نوع من أنواع الجريمة المعلوماتية، فإن التحقيق في هذه الجريمة هو من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له أهمية في التثبيت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه علي استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة، والثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولى ومرحلة التحقيق الابتدائي، فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق، وإنما نؤيد الرأي أو الاتجاه الذي يقسم التحقيق إلى :

- **تحقيق أولي:** والذي يناط به رجال الضبطية القضائية.
- **تحقيق قضائي:** ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيقه النهائي يكون في مرحلة المحاكمة من طرف قضاة الحكم.

وعليه فإنه يمكن القول أن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أو ابتدائيا، والمفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

وإذا كان التحقيق دوما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة فإن التحقيق في البيئة الالكترونية يستوجب

بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطوير أساليب ارتكابها في هذه البيئة .

فإن التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة، وهذه القواعد إما قانونية وإما فنية فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثيرة، وذلك أن الفكر البشري المتعلق بإبرام المعلوماتي يجب أن يقابله فكر من قبل المحقق الجنائي وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا وذلك كنتيجة طبيعية لمواجهة فكر المجرم المعلوماتي[1].

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو من لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية وذلك بغرض مساعدة جهات التحقيق في انجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك[2].

فالعناصر الأساسية للحقيق في مجال جريمة القرصنة الالكترونية تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتتحدد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي [3]. ويمكن أن نسرد الأهم منها :

- تحديد نوع نظام المعالجة الآلية للمعطيات، فهل هو كمبيوتر معزول أو متصل بشبكة المعلومات.

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009،ص57/56.

[2] انظر المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002 ص115.

- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- تصوير الأجهزة المستهدفة التي وقعت بها أو عليها الجريمة من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق، وعند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم مراعاة العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الالكترونية التي تدخل على وقوع الجريمة وتخزينها في الأقراص.

وكما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات[1].

ولهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق دقيقة وذكية، ذلك من خلال الإسراع في أن يطر رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية، وليس بالضرورة أن يكون المحقق في الجريمة القرصنة تندرج ضمن الجريمة المعلوماتية سماها المشرع الجزائري نظام معالجة آلية للمعطيات خبيرا في الحاسوب والنظم المعلوماتية ولكن لابد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي

[1] جميل عبد الباقي الصغير، المرجع السابق.

اتفاقها على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة[1].

وقد كان هناك من يرى أن صعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن يعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال لكن هذا الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد والمجتمع فضلا عن الإخلال بمبدأ سرية التحقيق سيما لو تعلق التحقيق بجرائم عرض الأشخاص وأسرارهم الشخصية أو تعلق الأمر بأمن الدولة وهذا لما أدرجه المشرع الجزائري ضمن النصوص القانونية في القانون 18-07[2].

ثانيـا: الخبـــرة :

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل المادي وإنما هي تقييم فني لهذا الدليل.

وقد أجاز المشرع للمحقق الاستعانة بخبير متخصص في المسألة موضوع الخبرة.

فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه يجوز لكل جهة قضائية تتوالى "التحقيق أو تجلس للحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة أو الخصوم أو من تلقاء نفسها.

وبالنظر إلى الطبيعة الخاصة بالجرائم المعلوماتية فإن إماطة اللثام عنها قد يحتاج إلى خبرة فنية تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر هذه الحاجة في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[3].

---

[1] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الفترة من 1 إلى 03 ماي 2000.

[2] محمد الأمين البشري، المرجع السابق، ص25.

[3] د/ هشام رستم، المرجع السابق، ص137.

وبالعودة لنص المادة 146 نجد أن المشرع يفرض على الجهة القضائية الآمرة بندب الخبير تحديد مهمة الخبير بدقة، وهذا يعود بنا إلى ضرورة تأهيل سلطات التحقيق أو الحكم في الجرائم المعلوماتية لنجاح الهدف المتوخي من التحقيق في هذا النوع المستحدث من الجرائم.

كما تجدر الإشارة على أنه يجب على القاضي اختيار الخبراء ذوي الإمكانيات العلمية والمقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية، إذ يجب مراعاة الخبرة العلمية فالوسائل الالكترونية متعددة وشبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة[1].

على القاضي في رأيي أن يتناول في أمر ندب الخبير المسائل التالية:

1. تركيب الحاسب الآلي، طرازه، نوعه، نظام تشغيله، الأنظمة الفرعية التي يستخدمها.
2. بيئة الحاسب أو الشبكة من حيث طبيعتها، تركيزها، توزيعها، وكذلك نمط ووسائط الاتصالات.
3. المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.
4. الآثار الاقتصادية والمالية المترتبة عن الجريمة المعلوماتية.
5. كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو الأجهزة أو تدميرها.
6. إمكانية نقل أدلة الإثبات لأوعية أو وسائط مادية كالأوراق أو الأسطوانات على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة.

ثالثـا: اعتراض المراسلات السلكية واللاسلكية والمراقبة الالكترونية:

تجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فإنه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها.

[1] د/ هشام رستم، المرجع السابق، ص141/140.

وانطلاقا من أهمية حماية الحياة الخاصة نجد الدستور في نص المادة 39 ينص" لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، يحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

وتبعا لذلك نظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك والإجراءات التي يتم إتباعها حيال هذه المراقبة.

وإذا كانت شبكات الحاسب الآلي تستخدم خطوط الهاتف وتستعين بجهاز معدل الموجات "modem" والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب على موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط الهاتف، وذلك فإنه يتبين وجود

علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالوسائل الالكترونية بحيث يمكن القول أن هناك تنصتا ومراقبة الكترونية تتم على شبكات الحساب الآلي[1].

ومن ثمة لايجوز التنصت عليها أو الاطلاع على أسرار التي تحتويها إلا بذات الطرق التي ينص عليها قانون الإجراءات الجزائية، فلايستطيع الشخص اختراق صندوق البريد الالكتروني أو الدخول إلى أنظمة الحاسب الآلي المخزنة به الرسائل البريدية لالكنرونية وضبطها إلا عن طريق إتباع إجراءات قانونية محددة في القانون ومن قبل أشخاص مخولين قانونا بذلك .

وقد اختلف الفقه في تكييف إجراء اعتراض المراسلات السلكية واللاسلكية ، فذهب الرأي إلى أنها تعد تفتيشا وبالتالي تخضع لقيوده، واستند في ذلك إلىأن هذه المراقبة تتفق مع التفتيش في أن الهدف منها هو البحث وضبط مايفيد الوصول الى الحقيقة ، ولا أهمية لأن يكون الشيء المضبوط ماديا أم معنويا، وهي ذات الغاية من المراقبة و التصنت فهي البحث عن دليل معين[2].

[1]د.هلالي عبد الله، تفتيش نظم الحاسب الآلي ، المرجع السباق، ص221

[2]د.رؤوف عبيد، مبادئ الاجراءات الجنائية في القانون المصري، دار الجيل للطباعة، الطبعة السادسة عشر ، 1985 ص358، ذ/ احمد فتحي سرور، مراقبة المكالمات التلفونية، المجلة الجنائية القوية، ما بين 1963 ص147.

في حين ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة، واعتبر الأول إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها لمصلحة العدالةن أما الثانية فليس لها كيان مادي ملموس والقول بأن الرسائل الالكترونية او الحديث في التلفون يندمج في كيان مادي يمكن ضبطه، فأسلاك التلفون يمكن التسجيل ليس دليلا في حد ذاته إنما هي وسيلة أو أداة لسماعالحديث ولا تتأثر طبيعته بوسيلة أو أداة الحصول عليه[1].

و الرأي عندي أن التفتيش واعتراض المراسلات إجراءان مختلفان ذلك أن المشرع الإجرائي قد أفرد أحكاما خاصة لكل واحد منها نظرا لاختلاف المحل الذي يقع على كل منهما، فالأخير يقع على حرمة الحياة الخاصة بمطلق القول، أما الأول فقد يمس مصادفة هذه الحياة الخاصة حتى وان تمت على كيانات معنوية، فليس معنى أن يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائما على كيانات معنوية أن نسوي بيهما من حيث تأثيرهما على حرمة الحياة الخاصة بما قد لا يتوافربالنسبة لتفتيش.

وقد تدخل المشرع الفرنسي في 10جويلية 1991 بإصدار قانون يفرض الرقابة على الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات [2] بعد اختلاف الفقه بشأن ضبط الأشياء المعنوية من مكونات الحاسب الألي عن طريق التنصت أو اعتراض المراسلات إذ اعتبر جانب من الفقه أن قانون الإجراءات الجزائية عندما نص على إصدار إذن بضبط "أي شيء" فانه يشمل بذلك بيانات الحاسب المعنوية.

أما الجانب الآخر للفقه فاقترح مواجهة هذا القصور التشريعي بالنص صراحة على إعتراض المراسلات ويجب أن يشمل المواد المعالجة عن طريق الحاسب لآلي.

وعلى ضوء هذا القانون فان المشرع الإجرائي الفرنسي خص إصدار قرار المراقبة بقاضي التحقيق (المادة 1/110) وله أن يندب مأمور الضبط القضائي للقيام به، ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة و كانت هناك إستحالة في

[1] د/ عبد المهيمن بكر، المرجع السابق، ص352،353.

[2] Francillon (jacques) , les crimes et d’autres crimes dans le domaine de la technologie informatiqu en France-rev.inter.de.dr.p en 1993 p303

الوصول إليها بطرق البحث و التنقيب العاديمة م (1/100)وطلب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقب عليه بالحبس الذي يزيد عن سنتين (م 2/100) وكذلك حدد مايعادا زمنيا للمراقبة مدته أربعة أشهر في حدها لأقصى وتكون قابلة للتجديد، وانه يتعين أن يتم التسجيل و تفريغ التسجيل تحت سلطة قاضي التحقيق والرقابة (م100).

وقد خاص المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائرية باقانونرقم06-22 المؤرخ ب20ديسمبر2006 في نص المادة 14 المتممة للباب الثاني من الكتاب الأول من الأمر رقم66-155 بفضل الرابع تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" بالمواد65 المكرر 5 إلى المادة 65 مكرر 10.

إذ خول لوكيل الجمهورية أن يأذن باعتراض المراسلات تتم عن طريق وسائل الاتصال السلكية و اللاسلكية إذا اقتضت ضرورات التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة 65 مكرر 5 و من بين هذه الجرائم جرائم المساس بأنظمة المعالجة الآلية للمعطيات .فيسمح الإذن بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المنصوص عليها في المادة 47 من قانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق على تلك الأماكن وتنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية.

والإذن بالمراقبة أو التنصت أو اعتراض المراسلات محددة بمعاد 4 أشهر كحد أقصى قابلة لتجديد المادة 65 مكررة 7.

كما خول لقاضي التحقيق الإذن أيضا بوضع هذه الترتيبات في حلة فتح تحقيق قضائي وتتم العمليات تحت مراقبته المباشرة .

كما أجاز المشرع في نص المادة 65 مكرر 8 تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات السابقة المذكورة في نص المادة 65 مكرر 5.

وفي الأخير على ضابط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل أو وضع ترتيبات تقنية و عمليات الالتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري ويذكر تاريخ بداية هذه العمليات و الانتهاء منها، كما يودع أي تسجيل أو اعتراض أو نسخ تم أثناء عملية المراقبة ويودعها بالملف.

المطلب الثاني: تقدير أدلة الإثبات المتحصلة عن الوسائل الإلكترونية :

تتنوع نظم الأدلة الجزائية في الإثبات، بين التي تأخذ بنظام الأدلة القانونية في الإثبات وأخرى تعتنق الإثبات الحر القائم على حرية القاضي الجزائي في تكوين اقتناعة وتلك التي تجمع بين النظامين بما يسمى النظام المختلط.

ففي نظام الأدلة القانونية يتقيد القاضي في الإثبات بأدلة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأ، يستمد اقتناعه من هذه الأدلة دون غيرها[1].

أما في نظام الأدلة الاقتناعية فأن القاضي لا يقيده المشرع بأدلة إثبات معينة و إنما يترك له حرية الإثبات وفقا للسلطة لتقديرية في تقدير الدليل و يترتب عن ذلك أن للقاضي الجزائي قبول أي دليل يمكن أن يتولد منه اقتناعه[2].

وعلى الغم من سيادة هذا النظام الأخير للإثبات الجاني في جل التشريعات، منها الجزائر إلا أن المشرع قد طبق في إثبات بعض الجرائم نظام الأدلة القانونية عندما نص على تقييد سلطة القاضي في الإثبات أدلة معينة ومثال ذلك إعطاء حجية كاملة لبعض المحاضر كمحاضر الحجز والمعاينة الجمركية التي تكون صحيحة إلى أن يطعن فيها بالتزوير[3] ومحاضر أخرى أعطاها المشرع حجية نسبية فتكون صحيحة إلى أن يثبت العكس وهنا ينتقل عبء الإثبات من النيابة إلى المتهم ومثال ذلك الاعترافات و التصريحات في المحاضر الجمركية[4].

[1] د/ سعيد عبد اللطيف، اثبات الجرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، ط1999، ص147.
[2] د/ عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، مؤسسة العين للطباعة، ص12 و13.
[3] د/ حسن بوسقيعة، المنازعات الجمركية، دار هومة، ط2005، ص191.
[4] غ.ج2 ملف 73553 قرار 1992/06/12 وايضا غ.ج.م.ق 3 ملف 89323 قرار 8-11-92 ص 52و 53.

وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة ومثال ذلك المادة 341 من قانون العقوبات و التي نصت على وسائل إثبات محددة لإثبات جريمة الزنا، وهذه الحجية وتلك القيود التي ترد على ذلك حرية القاضي في الاقتناع ليس المقصود منها افتراض ارتكاب المتهم للوقائع التي تنص على إعطائها الحجية ولكنها تعفي القاضي من إعادة التحقيق فيها.ويظل القاضي هو مالك السلطة التقديرية لهذه الأدلة ليستمد منها اقتناعه ويظل المتهم بريئا إلى حين إثبات عكس ذلك بالأدلة الكافية.

وإذا كان التطور العلمي قد أفرز ثورة الاتصالات عن بعد وجاءت للبشرية بتكنولوجيا جديدة نراها في مختلف مناحي الحياة، كالتجارة الالكترونية، وشبكات الاتصال العالمية (الانترنت) والتحويلات المصرفية الالكترونية، والنقود الالكترونية، وحلول الثورة الرقمية محل الأوراق والكتابة والتوقيعات التقليدية يطرح التساؤل هنا حول الآثار التي ترتبت على ثورة الاتصالات ومدى تأثيرها في الإثبات الجزائي بالاعتماد على الأدلة العلمية الالكترونية ومدى تقييد سلطة القاضي في الاقتناع.

فقد وفرت التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها، مثلما هو الحال بالنسبة للبصمة الوراثية، وبصمة قزحية العين.....الخ.

كما وفرت التقنية العلمية بالمقابل الوسائل الكافية لخلق جرائم أشد تعقيدا زادت من تعقيد الدليل وطرق الوصول إليه، وخلق عناصر تكوينية في الجرائم تغير مفهومها التقليدي كالشيكات الالكترونية مثلا التي تؤثر بدورها في جريمة الشيك ذلك إثباته يعتمد على مسائل فنية لإثبات الشيك كورقة تجارية.

وظهور الكيانات غير المادية التي تكون محلا في جريمة خيانة الأمانة والتي يتطلب البحث فيها عن العقد الذي تسلم الجاني هذا الكيان غير المادي بموجبه.

وتغير مفهوم المستند في جرائم التزوير بظهور المستندات الالكترونية وتغير طرق الإثبات في هذه الجرائم خاصة بعد ظهور التوقيع الالكتروني وتمتعه بالحجية في الإثبات في الكثير

من التشريعات وإذا كانت الغلبة في إثبات الجرائم الالكترونية للخبرة، فإن ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجزائي ويزيد بذلك أهمية دور القاضي في هذا الإثبات بحيث يظل القاضي متمتعا بسلطة تقديرية في تقدير هذه الأدلة حسبانا أنها قد لا تكون مؤكدة على سبيل القطع[1].

أو قد تكون أمارات أو دلالات، أو قد يحوطها الشك،فمنها تظهر أهمية هذه السلطة التقديرية التي يجب أن يتمتع بها القاضي كما تظهر أهمية تأهيل وتكوين القاضي في هذا النوع من الجرائم لأنه من خلال ذلك يستطيع إظهار مواطن الضعف في هذه الأدلة ويستطيع تفسير الشك لصالح المتهم.

فالدليل مهما تقدمت طرقه وعلت قيمته العلمية أو الفنية في الإثبات، فإنه يحتاج إلى قاض يتمتع بسلطة تقديرية، لأن هذه السلطة التقديرية تكون لازمة لتنقية الدليل من الخطأ أو الغلط أو الغش، وهي تكون ضرورية أيضا لكي تجعل الحقيقة العلمية حقيقة قضائية، فالحقيقة تحتاج على دليل وهذه الحقيقة قابلة للتطور والدليل الذي تقوم عليه يصلح للتطور أيضا حتى يقوى على إثباتها ويجب ألا يقف هذا التطور عند طرق الحصول على الدليل بل يلزم أن يتطور أيضا كل من يتعامل مع هذا الدليل خاصة المحققين والقضاة ولأنه بهذا التطور الأخير تتطور الحقيقة القضائية وتستطيع أن تجعل الحقيقة العلمية عادلة.

المطلب الثالث: موقف المشرع الجزائري من المعالجة الآلية للمعطيات :

لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان ذلك موجب القانون رقم 05/04 المؤرخ في 2004/11/10 المتمم و المعدل للأمر 156/66 المتضمن قانون العقوبات و الذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الأبية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدي إلى بروز أشكال جديدة للإحرام، ما دفع بالكثير من الدول إلى النص على معاقبتها. وأن الجزائر على غرار هذه الدول تسعى

[1] Jean pierre ,essai de synthése et libre de cloture le droit des preuves au defi de la modernité. Op.cit.p144

من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني.

خلاصة الفصل:

نستخلص من هذا الفصل و بعد دراستنا للجوانب الموضوعية و الإجرائية لجريمة القرصنة الالكترونية و من هذا المنطلق قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة. لذلك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات و النظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التحريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي أي الجرائم التي يكون النظام المعلوماتي محلا لها ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها[1].

ثم تبين لنا من خلال دراسة الفصل الثاني لهذا البحث قصور قواعد الإجراءات الجزائية في مواجهة الاجرام المعلوماتي كفشلها في مجال الضبط و التحري، التحقيق، تفتيش النظام المعلوماتي، استنباد الأدلة و اثبات الجريمة و صعوبة اثبات الجرائم الالكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها إذ قد يكون هذا الدليل غير مرئي و قد يسهل إخفائه أو تدميره و قد يكون متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها، كما أن هذا الاثبات قد يحتاج إلى معرفة علمية و فنية قد لا تتوافر لضباط الشرطة القضائية و القضاة، و هكذا حاولنا من خلال هذا البحث معالجة إشكالية تطبيق النصوص التقليدية و المستحدثة و النصوص الخاصة في مجال الجرية.

[1] سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية،تخصص علوم جبائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص45.

الخاتمة

بعد هذا العرض المتواضع لموضوع القرصنة الالكترونية لاحظنا تشعب الموضوع وصعوبته لكون هذا النوع من الجرائم يعد حديثا نسبيا يستلزم دراسات مستقبلية في محاولة وضع المبادئ العامة لكل ما يتعلق من جرائم ترتبط بالتطور الالكتروني والمعلوماتي ووسائل الاتصال الحديثة وهذا ما يتطلب تدخلا تشريعيا من أجل حماية قانونية متكاملة وسد الثغرات التي تعتري قوانين العقوبات النافذة والتي تعد صالحة لمواكبة تطور نظم المعلومات.

فيوما بعد يوم تزداد مخاطر القرصنة الالكترونية وتتوسع دائرتها حتى أصبحت الجزائر تحتل المراتب الأولى عالميا، وأصبحت القرصنة ترتكب كأنها روتين يومي يقوم به بعض الأشخاص من نسخ غير مشروع أو تطفل عبر الانترنت أو إرسال فيروسات أو فك للشفرات أو غير ذلك مما يكلف خسائر مادية ومعنوية لضحاياهم.

ولكن ما يمكن ملاحظته أن الجزائر تفطنت مؤخرا إلى الضرورة الملحة للحد والوقوف في وجه الهاكرز، ووضع قوانين صارمة لردعهم ولو أن هذه القوانين التي هي في طور الإنجاز جاءت متأخرة، ولعل من أهم أسباب تأخره هو عدم ثقافة التبليغ لدى أفراد المجتمع الجزائري الذي لم يتعود على الاعتراف بوجودها أصلا.

والملاحظ من خلال دراسته هذا الموضوع نقص المراجع في هذا الميدان، الصعوبات القانونية التي تواجه رجل القانون خاصة القاضي في تطبيق النصوص الجزائية.

وهكذا حاولنا من خلال هذا البحث معالجة إشكالية تطبيق النصوص في مجال جريمة القرصنة الالكترونية، وقد توصل البحث من خلال هذه الدراسة النتائج التالية :

- ✓ أظهر البحث أن هناك قصورا واضحا في الكثير من التشريعات الموضوعية والإجرائية في مواجهة ومكافحة جريمة القرصنة الالكترونية.
- ✓ أظهر البحث كذلك أن هناك صعوبة الدليل بالنسبة لجريمة القرصنة الالكترونية ، سواء من حيث طرق الحصول عليه أو من حيث طبيعته فالحصول عليه قد يحتاج

إلى عمليات فنية وعلمية. كما أن طبيعته قد تكون غير مرئية كالذبذبات والنبضات وأن استخدام التقنية العلمية في إنفائه أو إتلافه وقد يتم ذلك عن طريق التشفير واستخدام الفيروسات المدمرة.

وعلى ضوء هذه النتائج فإن البحث قد توصل إلى التوصيات التالية :

- ✓ ضرورة إيجاد قاعدة تعاون دولي فيما يتعلق بمكافحة جريمة القرصنة الالكترونية لتوفيق بين التشريعات الخاصة لهذه الجريمة.
- ✓ ضرورة تدخل تشريعي لحماية المعلومات والبيانات بنصوص خاصة فلا يكفي التوسع من نطاق تطبيق النصوص التقليدية حتى لا يصدم القاضي بمبدأ الشرعية ولا يجد نفسه أمام أفعال وسلوكات غير مجرمة فيفلت فاعلوها من العقاب رغم أن العديد من الدول كفرنسا، و.م.أ، وكندا وأصدرت تشريعات تتعلق بمكافحة هذه الجريمة.
- ✓ ضرورة استحداث نصوص قانونية جديدة خاصة في قانون الإجراءات الجزائية حتى تتلائم في مجال الضبط والتحقيق لعدم ملائمة الإجراءات التقليدية في مواجهة هذه الجريمة، إضافة إلى تحديد الأساليب والأجهزة المكلفة بالبحث والتحري عن جريمة القرصنة الالكترونية دون أن تتعرض حقوق الأفراد وحرياتهم للخطر عند الإثبات في مجالها.
- ✓ تخصيص وحدات أمنية لديها الإلمام الكافي بتقنيات الحاسب وذلك لا يتأتى إلا من خلال تكوين فرق وتعليمهم مبادئ وعلوم الحاسب الآلي وكيفية التعامل مع هذه الجرائم وتطوير الوسائل البحث.

لذلك فقد توصلت في هذا البحث أن المشرع دعا على إعادة تقييم بعض القواعد الإجرائية المتاحة في استخلاص الدليل التفتيش وهو ما كان فعلا بموجب القانون 04-09 المتعلق بقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فضلا عن استحداث نوع القواعد الإجرائية الأخرى تتلائم مع الطبيعة الرقمية التي يكون عليها الدليل المناسب في الإثبات هذا النوع من الجرائم كاعتراض المراسلات، وبالتالي فإن

إجراءات استخلاص الدليل في البيئة الرقمية قد يؤدي إلى المساس بهذه الخصوصية وإمكانية الاطلاع المحققين على الأسرار الخاصة بالأشخاص قد لا يكون لهم أصلا يد في الجريمة، مما جعل المشرع يحرص كل الحرص على هذه المسألة بأن اشتراط اللجوء على هذه الإجراءات إذا دعت على ذلك ضرورة التحري والتحقيق التي يجب أن تقدر بقدرها.

بالإضافة إلى كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية وهاته الأخيرة في الغالب ما تكون بجرائم تقليدية، وأن أهم مميزات جرائم الاعتداء على النظم المعالجة آليا للمعطيات أنها تنص على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية، فهذه الجرائم تستهدف المساس بالمعلومات المتواجدة في البيئة الرقمية على هيئات الإشارات والنبضات الغير المرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال المعلوماتية.

اقتراحـــــات :

1- ضرورة إيجاد قاعدة تعاون دولي فيما يتعلق بجريمة القرصنة للتوفيق بين التشريعات الخاصة بهذه الجرائم.

2- ضرورة التدخل التشريعي لحماية المعلومات و البيانات بنصوص خاصة فلا يكفي التوسع من نطاق تطبيق النصوص التقليدية حتى لا يصطدم القاضي بمبدا الشرعية و يجد نفسه أمام أفعال و سلوكات غير مجرمة فيفلت فاعلوها من العقاب، رغم أن العديد من الدول كفرنسا و الولايات المتحدة الامريكية و كندا أصدرت تشريعات تتعلق بمكافة الجريمة المعلوماتية إلا ان هذه التشريعات ما تزال في مهدها و لا يمكن اعتبارها جامعة مانعة .

3- ضرورة التنسيق فيما يتعلق بالإجراءات الجزائية المتبعة في شان الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق منها باعمال الاستدلال او التحقيق سيما و أن الحصول على الدليل في مثل هذه الجرائم خارج نطاق الدولة عن طريق التفتيش في

نظام معلوماتي معين هو في غاية الصعوبة فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته.

4-تاهيل القضاة و تكوينهم في مجال الجرائم المعلوماتية حتى يتسنى له الالمام بكافة النصوص و الإجراءات المتبعة في هذا النوع من الجرائم، خاصة في الاحكام المستحدثة و تنشيط دورات تكوينية مستمرة من قبل الخبراء و قانونيين بإعتبار أن هذا يؤثر على العدالة بصفة مباشرة .

5-ضرورة عقد ملتقيات و التعاون المكثف بين التقنيين و الخبراء في الحقول الالكترونية مع ضباط الشرطة القضائية و القضاة بشكل دوري و دائم للاستفادة من خبراتهم و ارشاداتهم ابتداءا من مرحلة التحري و الاستدلال و جمع الأدلة و الانتهاء باحكام المحاكم، خاصة فيما يتعلق بالخبرة و الشهادة في المجال المعلوماتي و تفعيل الدور الوقائي للقضاء المستعجل في مجال الجرائم المتعلقة بالانترنت.

6-انشاء لجنة مختصة على غرار اللجنة الوطنية للمعلومات و الحريات في فرنسا تتولى دراسة ظاهرة الاجرام المعلوماتي بكافة جزانبه و تعمل على سياغة التعديلات التشريعية اللازمة لإحتواء المشكلة بالاضافة الى تكليفها بمراقبة المعالجات الالية للبيانات و نشر التوعية لمستخدمي الحاسوب بفوائد و مخاطر تعامل به.

7-ضرورة استحداث مصوص قانونية جديدة خاصة في قانون الإجراءات الجزائية حتى تتلائم في مجال الضبط و التحقيق لعدم ملائمة الإجراءات التقليدية في مواجهة هاته الجرائم إضافة الى تحديث الأساليب الإجرائية المتبعة في الجرائم المعلوماتية دون ان تتعرض حقوق الأفراد و حرياتهم للخطر عند الإثبات في مجالها.

المصـــادر و المراجـــع

أولا الكتب:

1. منير محمد الجنبهي، ممدوح محمد، "جرائم الانترنت والحاسب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، الإسكندرية.
2. عايد رجا الخلايلة، "المسؤولة التقصيرية الالكترونية، المسؤولة الناشئة من إساءة استخدام الفرد الحاسوب والانترنت"، دار الثقافة للنشر والتوزيع، ط1، الإصدار الأول، 2006.
3. مصطفى حمد موسى، "التحقيق في الجرائم الالكترونية"، مطابع الشرطة، ط1.
4. خالد ممدوح إبراهيم . الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الأولى 2009 .
5. عادل يوسف عبد النبي الشكري _ الجريمة المعلوماتية و أزمة الشرعية الإجرائية _ جامعة الكوفة كلية قانون .
6. محمد حماد البهيتي ، التكنولوجيا الحديثة و القانون الجنائي . دار الثقافة للنشر و التوزيع عمان 2004 .
7. هشام محمد فريد رستم الجوانب الإجرائية للجرائم المعلوماتية, مكتبة الآلات الحديثة الطبعة الأولى 1994.
8. محمد سامي الشةا، ثورة المعلومات و انعكاساتها على قانون العقوبات ، دار النهضة العربية القاهرة سن 1994.
9. الخلقة العلمية ، الدليل الرقمي و التحقيق في الجرائم الالكمترونية المنعقدة من 22 إلى 27 / 1429/12 كلية العلوم الأدلة الجنائية جامعة نايف العربية للعلوم الأمنية .
10. عبد الفتاح البيومي الحجازي، الدليل الجنائي في جرائم الكومبيوتر و الانترنت، دراسة متعمقة في جرائم الحاسب الالي و الانترنت، دار الكتب القانونية، مصر، بدون سنة .

11. سامح عبد الحكم، جرائم الانترنت الواقعة على الأشخاص في اطار التشريع البحريني، دراسة مقارنة، بالتشريع المصري دار النهظة العربية القاهرة،2007، ص1.3
12. د/حسين المحمدي بوادي، غرهاب الانترنت الخطر القادم، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية، 2006 .
13. د. شريف سيدي كامل الجريمة المنظمة في القانون، الطبعة الأولى، دار النهظة العربية، القاهرة .
14. د. شريف سيدي كامل الجريمة المنظمة في القانون.
15. خالد ممدوح إبراهيم . الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الأولى 2009 .
16. هشام محمد فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات.
17. قارة أمال، الحماية الجزائية للمعلومات في التشريع الجزائري، دار هومة.
18. د.علي عبد القادر القهوجي، المرجع السابق، ص28 وراجع كذلك الخلاف في شأن طبيعة المال المعلوماتي د/محمد سامي الشوا ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1998.
19. د/ جميل عبد الباقي الصغير، القانون الجبائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسوب اللي، دار النهضة العربية، القاهرة، 1992.
20. د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي وشبكة الانترنت، دراسة مقارنة دار النهضة العربية، 2000، القاهرة.
21. د/ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي.
22. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009.
23. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.

24. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الفترة من 1 إلى 03 ماي 2000.
25. د.رؤوف عبيد، مبادئ الاجراءات الجنائية في القانون المصري، دار الجيل للطباعة، الطبعة السادسة عشر ، 1985 ص358، ذ/ احمد فتحي سرور، مراقبة المكالمات التلفونية، المجلة الجنائية القوية، ما بين 1963 .
26. د/ سعيد عبد اللطيف، اثبات الجرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، ط1999.
27. د/ عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، مؤسسة العين للطباعة.
28. د/ حسن بوسقيعة، المنازعات الجمركية، دار هومة، ط2005، ص191
29. غ.ج2 ملف 73553 قرار 1992/06/12 وايضا غ.ج.م.ق 3 ملف 89323 قرار 8-11-92.

ثانيا المذكرات:

1-محمد محمد حسن، جريمة القذف، دراسة مقارنة بين القانون الجنائي الوضعي و الشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق،1996.
2-عبابسة فاروق ، عبوب خديجة، القرصنة الالكترونية فب الجزائر و أثرها على المستخدم ، مذكرة لنيل شهادة الماستر في علوم الاعلام و الاتصال ، جامعة مستغانم.
3-عمر يوسفي، "التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة دراسة وصفية تحليلية"، شهادة الماجستير، 2008.
4-عبد الله دغش، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

5-طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة ماجستير في القانون الجنائي، جامعة الجزائر 1، كلية الحقوق 2011/2012.

ثالثا النصوص القانونية:

1-القانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016

2-أمر رقم 156/66 المؤرخ في 18 صفر 1386هـ الموافق ل 08يونيو 1966، المتضمن قانون العقوبات المعدل و المتمم، الجريدة الرسمية العدد47.

3-أمر رقم 155/66 المؤرخ في 18 صفر 1386هـ الموافق ل 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل و المتمم، الجريدة الرسمية،العدد47.

4-انظر المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية العدد47 المؤرخة في 16 أوت سنة 2009.

5-قانون رقم 07/18 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المراجع باللغة الأجنبية:

- Francillon (jacques) , les crimes et d'autres crimes dans le domaine de la technologie informatiqu en France- rev.inter.de.dr.p en 1993 .

- Gautal (jean- louis) , la protection penale des logiciel « le droit criminel face aux technologie nouvelles de la communication » .
- Jean p, spreutels,les crimes informatiques et d'autres crimes dans les domaines de la technologie informatique en Belgique-rev- inter de-dr pen 1993.
- Mohrenschlager « manfred » op.cit, www.anablawinfo.com.
Sagros »pierre » et masse « michel » le droit penal et l'informatique journnée d'étude du 15 novombre 1982 publication à l'institue de science criminelle de le faculte IV.
- The recmmendation n°2 (89) on compter – related crime , op.cit .
- T.G.I Paris,réf 30 avril 1997, D.1998.Somm Convenentes.
- Wasik (martin) , computer crimes and other crimes against information technology in the united kingdom-rev , inter,De,Dr,panal 1993.

المواقع الالكترونية:

https://www.echoroukonline.com/16/10/2020.
https://www.echoroukonline.com/31/10/2020.

فهرس المحتويات

الفصل الثاني: الجوانب الموضوعية و الإجرائية لجريمة القرصنة الالكترونية