وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم القانون الخاص

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

المعالجة الآلية للمعطيات في القانون الجزائري

ميدان الحقوق و العلوم السياسية

التخصص: **قانون قضائي**

من إعداد الطالب(ة):

بن عطية الحبيب

تحت إشراف الأستاذ(ة):

جلـــطي منـــصور

أعضاء لجنة المناقشة

الأستاذ(ة) ..... د/ محمد كريم نورالدين ..... رئيسا

الأستاذ(ة) ..... د/ جلطي منصور ..... مشرفا مقررا

الأستاذ(ة) ..... د/ خالد زواتين ..... مناقشا

السنة الجامعية: 2020/2019

نوقشت يوم: **2020/06/28**

بسم الله الرحمن الرحيم

وَابْتَغِ فِيمَا آتَاكَ اللَّهُ الدَّارَ الْآخِرَةَ وَلَا تَنْسَ نَصِيبَكَ مِنَ الدُّنْيَا وَأَحْسِنْ كَمَا أَحْسَنَ اللَّهُ إِلَيْكَ وَلَا تَبْغِ الْفَسَادَ فِي الْأَرْضِ إِنَّ اللَّهَ لَا يُحِبُّ الْمُفْسِدِينَ.

صدق الله العظيم .(الآية 77 من سورة القصص).

إهـــداء

أهدي هذا العمل المتواضع،

إلى الوالدين الكريمين حفظهما الله،

إلى كل أفراد أسرتي،

إلى روح جدي رحمه الله،

إلى كل من ساهم بتلقيني و لو بحرف في حياتي الدراسية،

إلى كل الأصدقاء، و كل من كان برفقتي و مصاحبتي أثناء دراستي بالجامعة.

شكـــر

*أشكر الله عز و جل و أحمده على توفيقه لي في إنجاز هذا العمل المتواضع،

* كما أتقدم بالشكر الجزيل للأستاذ " جلطي منصور" على قبوله الإشراف على عملي هذا.

* الشكر موصول أيضا إلى أعضاء لجنة المناقشة.

*كما لا يفوتني أن أشكر كل عمال و موظفي كلية الحقوق و العلوم السياسية أساتذة، إداريين و أعوانا .

قائمة المختصرات

ج.ر .....: جريدة رسمية

ط .....: طبعة

ص .....: صفحة

ق.م.ج .....: القانون المدني الجزائري

ق.إ.ج.ج .....: قانون الإجراءات الجزائية الجزائري

ق.ع.ج .....: قانون العقوبات الجزائري

مقدمـــة

تعتبر الجرائم المعلوماتية وليدة عصر العولمة، ذلك أن هذا النوع من الجرائم الواقعة على الحاسب الآلي بكل مكوناته المادية أو المعنوية لم تكن في الحسبان حتى يتسنى دراستها و وضع قواعد و أسس تسييرها قبل انتشارها و تطورها .

هذه الجرائم ولدت نتيجة الاستخدام الهائل للحاسوب في شتى المجالات الخاصة و العامة، بالإضافة إلى الانتشار الواسع للشبكات العنكبوتية التي ظهرت على الساحة الدولية، حيث لم يكن لها وجود قبل ذلك، و نتيجة لظهور تلك الشبكة فقد ظهرت معها الجرائم المعلوماتية التي تمثلت في جرائم الاعتداء على الكمبيوتر، سواء كان هذا الاعتداء يقع على ذات الجهاز أو كان على البيانات (المعطيات) التي يحتويها أو على الشبكة ذاتها .

و لم يعد يخف على أحد ما أصبحت تمثله هذه المعلومات من أهمية حتى باتت سلعة رائجة في سوق المعلومات، فقد غزت مختلف جوانب الحياة و ارتبطت بمختلف الأنشطة و الأعمال، فبات لزاما على كل الدول و المجتمعات التي تنشد التطور و الازدهار و مواكبة التطورات الهائلة أن تولي لها الاهتمام و أن تحقق لها التدفق و الانسياب ممّا يكفل الاستفادة القصوى منها .

هذا و قد ازداد حجم المعلومات في العالم كثيرا كنتيجة لما أفرزته ما يعرف بالثورة التكنولوجية التي ارتبطت بها مجالات شتى، و مع هذا التنامي غير المسبوق للمعلومات نتيجة الاستعمال الواسع للتكنولوجيا، و ازدياد الاعتماد على أجهزة الحاسوب الآلي و على المعالجة الآلية للمعلومات (المعطيات) التي يقدمها، كما تبنت الدول عدة مشاريع مثل " حاسوب لكل أسرة" أو " حاسوب لكل شخص " هذا مع ربط شبكات المعلومات بكل أنواعها، ما أعطى قفزة نوعية وتحولا هائلا و سريعا في المجال المعلوماتي ممّا زاد في الإقبال على هذه الشبكات والخدمات.

لكن و إذا كان هذا هو الجانب المشرق لما يسمى بالمعلوماتية، فإن هذه الأخيرة و ككل تطور قد حملت بين طياتها جانبا مظلما أفرزه استعمالها لأغراض غير مشروعة، و هو ما يسمى بالجرائم المعلوماتية، هذه الجرائم لبست لباس المعلوماتية و اتسمت بما تتسم بها من سمات وسايرت ما تقدمه من تطور، فتميزت عن غيرها من الجرائم بخصائص و تقنيات عديدة، وقد اتخذت هذه الجرائم صورتان، كانت المعلوماتية في الأولى وسيلة لارتكاب الجريمة وفي الثانية محلا للجريمة حيث تقع جرائم المعطيات.

كل هذا دفع المشرع الجنائي في الجزائر و في العديد من الدول إلى التدخل لحماية المصالح المهمّة المتعلقة بهذه المعلوماتية فجرّم ما يسمى بالغش المعلوماتي، كما أضاف طائفة من الجرائم الجديدة في ق.ع.ج جرم من خلالها العديد من الأفعال التي تشكل عدوانا على المعطيات، و هذه الجرائم هي : الدخول أو البقاء غير المصرح بهما لأنظمة المعالجة الآلية للمعطيات، التلاعب بمعطيات الحاسوب الآلي و أيضا التعامل في معطيات غير مشروعة .

تكمن أهمية الدراسة في القيام بالتعريف بظاهرة جديدة تعدّ من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني و الدولي على حد سواء، هذه الظاهرة يزداد انتشارها يوما بعد يوم مع الانتشار الهائل للحاسبات الآلية، و ازدياد الاعتماد عليها في شتى المجالات. وموضوع الجرائم الواقعة على نظام المعالجة الآلية للمعطيات موضوع كبير، كما أن المشرع الجزائري لم يتناول هذا الموضوع إلا حديثا عكس التشريعات الأوربية و الأمريكية التي كانت سباقة في هذا المجال.

وسنسلط الضوء في هذا الموضوع من خلال الطبيعة الفنية للموضوع فارتباط الجرائم محل الدراسة والبحث بالحاسب الآلي يتطلب الإحاطة بمكونات هذا الأخير و بنظام المعالجة الآلية للمعطيات وما يميزها من خصائص وتقنيات الاعتداء عليها ، فضلا عن خصائص الجريمة والمجرم المعلوماتي وهذه من الصعوبات التي اعترضت البحث باعتبارها أمور فنية تحتاج إلى جهد ناهيك عن الجهد القانوني .

إضافة إلى حداثة الموضوع في المجالات القانونية فكل المواضيع السابقة و المعتمدة في البحث تناولت الجريمة الإلكترونية بالمفهوم الواسع لها و لم تتعلق بالمعطيات على وجه الخصوص وهو جزء من الجريمة المعلوماتية، و نتيجة لذلك فقلة البحوث و المراجع في هذا المجال خاصة على المستوى الوطني أو العربي صعب من الإحاطة بالموضوع بكل جزئياته.

انطلاقا من هذا نتناول موضوع الحماية الجنائية للمعطيات التي تناولها المشرع الجزائري في ق.ع.ج وفق الإشكالية التالية :

هل الترسانة القانونية للمشرع الجزائري كافية للتصدي للجريمة المعلوماتية وردع مرتكبيها، أم لابد من إعادة النظر في فحواها لتواكب خصوصيات الجريمة المعلوماتية ؟

اعتمدنا في هذا البحث المنهج التحليلي و ذلك بتحليل كل جريمة من الجرائم المنصوص عليها في ق.ع.ج الخاصة بالجرائم موضوع البحث على حدا إلى عناصرها التي تكونها قمنا بتقسيم البحث إلى فصلين الأول بعنوان ماهية المعطيات الرقمية و الجرائم الماسة بها، و يتضمن مبحثين، في المبحث الأول تناولنا مفهوم المعطيات الرقمية ، في المبحث الثاني تناولنا أركان الجرائم الماسة بالمعطيات. هذا فيما يخص الفصل الأول أمّا الفصل الثاني فخصصناه لإثبات الجرائم الماسة بالمعطيات الرقمية و الجزاءات المقررة لها وقسمناه كذلك إلى مبحثين، تناولنا بالدراسة في المبحث الأول إثبات الجرائم الماسة بالمعطيات الرقمية وفي المبحث الثاني الجزاءات المقررة للجرائم الماسة بالمعطيات الرقمية و انهينا البحث بخاتمة تضمنت أهم النتائج التي توصلنا إليها (خلاصة).

الفصل الأول : ماهية المعطيات الرقمية و الجرائم المتعلقة بها

مع بداية انتشار شبكة الإنترنيت لم يكن هناك قلق تجاه الجرائم التي يمكن أن ترتكب على الشبكة، و ذلك نظرا لمحدودية استخدامها حيث كانت قاصرة على أغراض البحث العلمي فقط و ذلك لكونها مقتصرة على فئة معينة من المستخدمين و هم الباحثين و العلماء و طلبة الجامعات و مع ظهور الثورة المعلوماتية و توسع استخدام شبكة الإنترنيت و بدء إستخدامها في المعاملات التجارية و الإقتصادية و الثقافية و دخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة إزدادت مع الوقت و تعددت صورها و أشكالها، و هذه الجرائم يطلق عليها إسم الجرائم المعلوماتية أي تلك أي تلك الأعمال و الأفعال المجرمة من إختراقات و تلاعب بالبيانات الرقمية لمستخدمي هذه الشبكة و التي عادة تتم عن طريق الإنترنيت باعتبارها شبكة عالمية من جهة و أسرع طريق لنشر المعلومات و حذفها في أسرع وقت ممكن لذلك تعتبر من أهم و أخطر التحديات التي تواجه المعلومات الإلكترونية، و نظرا لكثرة الإعتداءات عل البيانات المتواجدة في الشبكة المعلوماتية ظهرت عدة تعريفات حول هذا الموضوع، لذلك قسمنا هذا الفصل إلى مبحثين تناولنا في المبحث الأول مفهوم المعطيات الرقمية و في المبحث الثاني أركان جريمة المساس بالمعطيات الرقمية.

المبحث الأول: مفهوم المعطيات الرقمية

لقد مهدت الثورة الصناعية التي تفجرت في منتصف القرن التاسع عشر لبزوغ ثورة جديدة هي ثورة المعلومات التي تقترن دائما بفكرة الحاسوب، و الذي بفضله يعيش العالم الآن عصر المعلومات الذي يتسم بالتطور السريع لتكنولوجيا الحاسبات، فقد أخذت المعلومات الآن في التزايد و التفاعل مع التقدم العلمي و التطور التكنولوجي و بسبب كثرة المعلومات بدأت الدول تهتم بأساليب جمع هذه المعلومات و تبويبها و تصنيفها و تحليلها بغية الإستفادة منها في الوقت الذي تطورت فيه المستحدثات التكنولوجية التي استهدفت التحكم في هذه المعلومات و تخزينها و استرجاعها.

و هذا الكم الهائل من المعلومات كان لابد من إدراجه في الكمبيوتر، و لمن في ظل بيئة المعلومات المخزنة آليا كان لابد من أن تضعف قبضة الأمن و الرقابة و التحكم و أن تزدهر عمليات التجسس على المعلومات المعالجة إلكترونيا و قرصنتها و تخريبها و إتلافها، حتى باتت تشكل تهديدا بالغا لسائر المنظمات الحكومية التي تعتمد أعمالها على الحاسبات و الشبكات الاتصالية، و ترفع مخاطر إساءة استخدام الحواسيب و التلاعب بالبرامج و ملفات المعلومات المخزنة آليا بقصد الحصول على أموال و خدمات غير مستحقة هذا من جهة، و من جهة أخرى تثير المعلومات باعتبارها أهم عنصر في عالم المعالجة الآلية للمعطيات عدة مشاكل قانونية فقد ساء إستخدامها لإرتكاب الجريمة عن بعد من ناحية أو كونها محلا للإعتداء عليها من ناحية أخرى مما يثير مسألة الإعتداء و ما إذا كان يشكل جريمة أم لا، لذلك قسمنا المبحث إلى مطلبين، الأول لتعريف المعطيات الرقمية و الثاني لخصائص جرائم الإعتداء على المعطيات.

المطلب الأول: تعريف المعطيات الرقمية

إن التطور التقني الحاصل في عالم تكنولوجيا المعلومات و ما يتطلبه من ضرورة القيام بمهام توفير و جمع و معالجة و تبادل المعلومات في نفس الوقت أدى إلى إرتكاب جرائم نظام

المعالجة الآلية، و الذي نشأ في الحقيقة بهدف وصف الحالة التي انبثقت عن اندماج تقنية نظام المعلومات و تقنية الإتصالات عن بعد، و قد تم تعريفه على أنه عبارة عن آلية و إجراءات منظمة تسمح بتجميع و تصنيف و فرز البيانات و معالجتها و من ثم تحويلها إلى معلومات يستخرجها الإنسان عند الحاجة ليتمكن من إنجاز عمل واتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي يحصل عليها من المعلومات المسترجعة من النظام الذي يحتوي على ما يسمى بالمعطيات و عليه فإننا سنتطرق إلى تعريف المعطيات[1].

1-تعريف المعطيات:

لقد اجتهد فقهاء و دارسي القانون محاولين في ذلك إيجاد تعريف للمعطيات فعرفها البعض بأنها عبارة عن مجموعة من الأرقام و الكلمات و الرموز أو الحقائق أو الإحصائيات الخام التي لا علاقة بين بعضها البعض و لم تخضع بعد للتغيير أو التجهيز أو الإستخدام، أما المعلومات فهي المعنى الذي يستخلص من هذه المعطيات.

و قد عرفت الوكالة الفرنسية المعطيات "Les donnes" بأنها كل حدث مفهوم أو تعليمة تقدم في شكل متفق عليه قابلة للتبادل عن طريق البشر أو بواسطة الحاسوب أو ينتجها الحاسوب[2] ، و لقد اعتمدت إتفاقية بودابست للجريمة المعلوماتية في تعريف المعطيات ذات التعريف الذي ذهبت إليه هيأة التوصيف العالمية الإيزو، حيث نصت في مادتها الأولى على أن المعطيات هي كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل و تكون مهيأة للمعالجة بما في ذلك برنامج معد من ذات الطبيعة و يجعل الحاسوب يؤدي مهمته.

و قد أخذت التوصية الصادرة عن منظمة التعاون الاقتصادي و التنمية في 26-11-1992 الخاصة بحماية أنظمة الحاسبات الآلية و شبكات المعلومات بالتفرقة السابقة، حيث عرفت المعطيات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددا يجعلها قابلة للتداول و التغيير أو للمعالجة بواسطة الأفراد أو بوسائل إلكترونية، أما المعلومات فهي المعنى المستخلص من هذه المعطيات[3] .

1.هشام محمد فريد رستم، ق.ع.ج و محاضر تقنية المعلومات، مكتبة الآلات الحديثة 1992، ص26.

2. مفتاح محمد دباب، معجم المصطلحات و تكنولوجيا المعلومات و الاتصال، الدار الدولية للنشر، القاهرة 1995،ص42.

3.إنتصار عريب، أمن الكمبيوتر و القانون، دار الراتب الجامعية، بيروت، ص81.

و تأسيا على هذا المعنى فإن المعطيات تعتبر المواد الخام التي تستخرج منها المعلومات باستخدام معالجة آلية في عملية الاستخراج، إذ يتم تجميع و تشغيل المعطيات للحصول على المعلومات ثم تستخدم في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات و التي يحصل تجميعها و معالجتها مرة أخرى للحصول على معلومة إضافية.

2- تعريف المعطيات في القانون الجزائري:

لقد أخذ المشرع الجزائري بما أخذت به باقي التشريعات فبالرجوع إلى ق.ع.ج القسم الرابع مكرر3 بعنوان المساس بأنظمة المعالجة الآلية للمعطيات نجد أن المشرع لم يعرفها و قد أحسن بعدم تعريفه للمعطيات و ذلك نظرا للتطور التكنولوجي المستمر و التطورات السريعة و المتلاحقة على التقنيات الذي حال دون ذلك فما نراه اليوم من برامج أو بيانات خاضعة للحماية قد لا يكون غدا و العكس صحيح، فكان مصطلح المعطيات مقصود به البيانات الرقمية و غير الرقمية و المعطيات ..الخ، حيث يعتبر هذا المصطلح أشمل و أعم.

بينما جاء مصطلح المعطيات المعلوماتية في قانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بأنها "أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[1] .

و بهذا التصور تكون المعطيات عبارة عن حقائق رقمية أو غير رقمية تتم بطريقة منهجية يمكن فهم دلالتها مباشرة دون الدخول في عمليات استنتاجيه استقرائية لدلالتها المعقدة من خلال أكثر من بيان[2] ، لأن ذلك يعني أن التحول من كون الأمر مجرد معطيات إلى بيانات و معلومات لذلك و جب تعريف البيانات و المعلومات على أنها:

---

1. أنظر المادة 02 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج ر، العدد 47.

2.رشيدة بوبكر،جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن و منشورات الحلب الحقوقية،الطبعة الأولى، سنة 2012، ص67.

الفرع الأول: تعريف البيانات:

إن دراسة الطبيعة القانونية للبيانات أمر هام و ضروري إذ أن تطور و تنوع هذه البيانات غير تماما وسائل تحليل القوانين المعاصرة، فليس من الغريب أن المسائل الخاصة بقواعد البيانات أصبحت محل جدل و يعود الأمر إلى سببين هما :

– التطور التكنولوجي في وسائل الإتصالات و عملية إدراج هذه البيانات في الأجهزة الإلكترونية.

– عدم إدراك الأفراد للمعنى الحقيقي للبيانات و مدى خطورة استغلالها و هي مشاكل في تزايد مستمر لذلك سنتطرق في دراستنا لهذه الجزئية إلى تعريف البيانات لغة ثم اصطلاحا.

تعريفها لغة: هي مجموعة المؤشرات و الأفكار المختلفة.

أما اصطلاحا: فيقصد بها الحقائق أو المشاهدات أو القياسات التي تكون على صورة أرقام أو حروف أو رموز أو أية أشكال خاصة و تصنف فكرة أو موضوع أو حدث أو هدف أو أية حقائق أخرى كمواد خام غير مرئية أو مقومة أو مفسرة أو غير معدة للاستخدام إذا ما قومت و فسرت و نظمت و رتبت، أصبح لها مضمون ذا معنى يؤثر في الإتجاه و رد الفعل و السلوك أي أنها في هذه الحالة تصبح معلومات و على سبيل المثال بيانات داخلية و أخرى خارجية.

فالبيانات الداخلية : هي بيانات تتداول داخل المؤسسة حيث تسجل و تحلل العمليات الداخلية لها، و تكون بصفة متكررة و دورية مثل بيانات عن حجم النشاط اليومي.

أما البيانات الخارجية : فهي بيانات تنتشر خارج المؤسسة مثل المتعاملين، حيث تقوم بوصف منتجات، و خدمات المؤسسة و تأخذ أشكال نشر عديدة مثل المجلات، تقارير ...

و قد تعددت التعريفات حول البيانات منها العربية و الغربية[1] .

---

1. التعريفات العربية:" لقد عرف المشرع المشرع المصري البيانات: بأنها أي تجميع متميز للبيانات يتوفر فيه عنصر الابتكار أو الترتيب أو أي مجهود شخصي يستحق الحماية و بأي لغة أو رمز و بأي شكل من الأشكال و يكون مخزن بواسطة حاسب و يمكن استرجاعه بواسطته أيضا.

أما المشرع اللبناني: فقد عرف البيانات باعتبارها مجموعة أعمال و معلومات سواء كانت في شكل مقروء أو آلي أو أي شكل آخر تكون منجزة من طرف صاحب حق المؤلف.

و قد نص المشرع الجزائري للبيانات في معرض تعريفه للمعطيات ذات الطابع الشخصي و ذلك في القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]، حيث جاء في نص المادة الثالثة من هذا القانون أن المعطيات ذات الطابع الشخصي هي كل معلومة بغض النظر عن دعامتها تكون متعلقة بشخص طبيعي معين تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة آلية،و تتمثل هذه البيانات على وجه الخصوص في رقم التعريف، أو أحد عناصر الهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الاجتماعية[2].

الفرع الثاني: تعريف المعلومات.

هي من المصطلحات التي تكاد تفقد وزنها الدلالي من كثرة الإستعمال حيث أن جميع التعريفات التي ذكرت في المعلومات تعبر بشكل كبير عن آراء ووجهات نظر أصحابها، و هذه التعريفات قد تكون مقبولة عند بعض التخصصات و مرفوضة عند البعض الآخر، و قبل التطرق إلى تعريف المعلومات سنتطرق إلى تعريفها لغة ثم إصطلاحا.

تعريفها لغة: المعلومات من حيث المدلول اللغوي مشتقة من المادة اللغوية "علم" و هي مادة غنية بالكثير من المعاني كالعلم و الإحاطة ببواطن الأمور و الوعي، والإدراك و اليقين، الإرشاد، الإعلام، الشهرة، المعرفة، التعليم، الدراية...و كل المعاني المتصلة بوظائف العقل،"INFORMATION" هي المقابل الإنجليزي لكلمة معلومات و هي بدورها مشتقة من اللاتينية "INFORMATION" التي تعني في الأصل عملية الإتصال أو ما يتم ايصاله أو تلقيه[3].

أما تعريفها اصطلاحا: فقد عرفت المعلومة بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل أو الإتصال أو التفسير أو التأويل أو المعالجة و

1.القانون رقم 07/18 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر ب ج.ر رقم 34 لسنة 2018.

2.المادة 03 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،القانون السابق.

3.حتمت قاسم، مدخل لدراسة المكتبات و علم المعلومات، القاهرة، دار غريب، سنة 1990، ص15.

تجزئتها و جمعها أو نقلها بوسائل أو أشكال مختلفة[1].

و قد عرف الأستاذ Calte المعلومات بأنها رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير[2].

و عرفت أيضا أنها النقل المجرد لوقائع معينة ثم الحصول عليها من مصادر متعددة.

و رغم اجتهاد فقهاء القانون و محاولاتهم لوضع تعريف شامل يتكفل بوضع تعريف محدد للمعلومات إلا أنهم لم يتمكنوا بعد من ذلك[3].

إذا فالمعلومات وفقا لذلك عي النتيجة المبدئية أو الذهنية المترتبة على تشغيل المعطيات و تعليلها أو استقراء دلالتها و استنتاج ما يمكن استنتاجه منها وحدها أو مترافقة مع غيرها أو تفسيرها على نحو يعتري معرفة مستخدمي القرار و يساعدهم في الحكم السديد على الظواهر و المشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية[4].

– فالمعلومات تكون قابلة للدمج حيث تضاف معلومة إلى معلومة أخرى ليكونا معا معلومة جديدة تختلف في قيمتها و أهميتها و بالتالي تثار مسألة مقدار الحماية اللازمة لها، و هو ما يطلق عليه بالنظرية التكاملية للمعلومات.

و هنا يطرح السؤال نفسه ما هو الفرق بين البيانات و المعلومات؟

الفرع الثالث: الفرق بين البيانات و المعلومات.

عادة ما يخلط الباحثين و الدارسين بين البيانات و المعلومات و قد جرت العادة على استخدام كل منهما مكان الآخر، إلا أنه يوجد فرق بين المصطلحين و يكمن في:

1.نائلة محمد فريد فورة،جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة 01، سنة 2005، ص 97.

2.رشيدة بوكر، المرجع السابق، ص 65.

3.خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الاسكندرية، سنة 2008، ص27.

4. محمد محمد شتا، فكرة الحماية الجنائية لبرنامج الحاسب الالي، دار الجامعة الجديدة للنشر 2002، ص61.

1- يبدأ أي نظام للمعلومات بالبيانات data و ينتهي بالمعلومات information.

2- البيانات هي حقائق تم تسجيلها، أو سيتم تسجيلها مستقبلا بشأن أحداث معينة، و قد تكون هذه الحقائق مستقلة و غير مرتبطة ببعضها و غير محددة العدد، و تعرف أيضا بالمداخلات أو المادة الخام للمعلومات، و بمعنى آخر هي مجموعة من الحقائق و المشاهدات التي يتم جمعها من مجتمع إحصائي معين، و يتم إدخالها إلى الحاسوب و إخراج النتائج، و من أمثلة البيانات الاسم، السن، المهنة ...الخ.

3- المعلومات هي ناتج تشغيل البيانات، أو مجموعة النتائج التي تم التحصل عليها من الحاسوب و بمعنى آخر هي مجموعة البيانات التي جمعت و أعدت بطريقة ما جعلتها قابلة للاستخدام أي مفيدة بالنسبة لمستقبلها أي مستخدمها، و هي تمثل المخرجات في نظام المعلومات و لها تأثير في اتخاذ القرارات المختلفة.

4- يقوم المستخدم بإدخال البيانات للحاسب ثم بتشغيلها و ترتيبها، ثم تجرى عليها بعض العمليات لتحصل على معلومة ذات قيمة و فائدة، و كل مجموعة من المعلومات تشكل معرفة ما و هذه هي وظيفتها النهائية، و تستخدم في تأكيد معلومة سابقة، أو في إضافة حقائق أو أفكار جديدة لمستقبل أو مستخدم المعلومات.

5- عادة ما تكون البيانات على شكل أرقام و جداول و أشكال بيانية بينما تكون المعلومة على شكل نص و عبارات أو صور توضيحية، و يمكن أن تكون البيانات نصوصا أو أرقام أو صور أو أي شكل آخر.

6- يرى الباحثون أنه من الصعب أن نضع حدا فاصلا بين البيانات و المعلومات، فما يعتبر معلومة في بعض المراحل، تعتبر بيانات في المرحلة التي تليها، و أن المعلومة قد لا تكون في صورة كمية أي يعبر عنها بالأرقام، و إنما قد تكون معلومة عبر كلمة أي وصفية[1].

---

1. Word.acc.net/vb/shotthread k php ?t7187

المطلب الثاني: خصائص الجرائم الواقعة على المعطيات الرقمية

من البديهي أننا أصبحنا في عصر بات كل شيء فيه خاضعا للعلم و الخبرة و المعرفة، و يبرز ذلك خاصة في المعاهد و الكليات... بوصفها عنصرا أساسيا في الجانب الأمني، و توفير مقومات السلام و الاستقرار في البلاد، لذلك فإن عالم الجريمة ليس معزولا عن التحولات الهامة الخاصة الالكترونية منها التي يشهدها العالم، بل يمكن القول أن جماعات الجريمة المنظمة تكون السباقة أحيانا فيه إحداث مثل هذه التحولات من خلال ابتكار أنماط إجرامية تستدعي جهدا كبيرا و تقنيات متقدمة لمواجهتها و درء أخطارها على الإنسانية.

كما تعاني المجتمعات الإلكترونية في الآونة الأخيرة من انتهاكات للحقوق و الخصوصيات الإلكترونية، و ذلك في ظل انتشار الجريمة الإلكترونية أو جريمة التعدي على المعطيات و هذا النوع من التقنيات و التكنولوجيا، الأمر الذي دفع الدول إلى العمل مليا للحد من هذه الجرائم التي تلحق الضرر بالأفراد من خلال التوعية و الرسائل الوقائية و الأمنية، و من خلال ما تقدم يتبين لنا أن الجريمة الماسة بالمعطيات لها عدة خصائص سواء الخاصة بالحاسب الآلي كجهاز أو الأشخاص الذين يقومون بهذه الجرائم لذلك قسمنا هذا المطلب إلى فرعين .

الفرع الأول: سمات الجرائم المتعلقة بالمعطيات الرقمية

إن الجرائم التي تمس المعطيات تعد من الجرائم المعلوماتية فهي ترتبط بها و تقوم عليها و قد أدى اتساع هذه الجرائم إلى إلحاق ضرر بالمجتمع، كما أن ازدياد و ازدهار حجم تقنية المعلومات في القطاعات المختلفة أدى إلى إعطاء الجرائم المعلوماتية لونا أو طابعا قانونيا خاصا يتميو عن غيرها من الجرائم سواء التقليدية منها أو المستحدثة بمجموعة من الخصائص و لعل أبرز خصائص الجرائم التي تمس المعطيات الإلكترونية هي:

1- جريمة تمس معطيات الحاسب الآلي:

أ- الحاسب الآلي أداة لارتكاب هذه الجرائم: تتميز الجرائم الماسة بالمعطيات أو المعلومات بخاصية منفردة تميزها عن الجرائم التقليدية، و باعتبار أن الحاسب الآلي هو الوسيلة الرئيسية الأكثر استخداما في الجريمة[1] و من جهة أخرى يتم الاعتداء على الحواسيب الأخرى و الدخول إلى البرامج و سرقتها أو العبث ببيانات الحاسوب أو إتلافها و الاطلاع على المعلومات المخزنة[2]، لذلك اشترط الفقهاء وجود شبكة الإنترنيت حتى يتم الربط بين هذه الحواسيب، و قد شهد العالم وسائل إلكترونية غير الحاسب الآلي كالهواتف النقالة الذكية التي استطاع البعض استغلالها في التعدي على المعلومة الخاصة.

ب- أن يقع الاعتداء على الحاسب الآلي أو ملحقاته: و هنا يكون الهدف من ارتكاب تلك الأفعال عبر شبكة الانترنيت هو الاعتداء على معطيات الحاسب الآلي، كالمعلومات و البيانات المخزنة في الذاكرة و هذه المعطيات ليست ذات طبيعة مادية منقولة ملموسة، حتى نجزم بخضوعها لنصوص قانون العقوبات التقليدي، و هي أقرب إلى الكيانات الذهنية أو المعنوية التي تم إدخالها إلى الحاسب الآلي[3]، فالغالب يكون الهدف هو تخزين تلك الأجهزة نهائيا أو على الأقل تعطيلها لأطول فترة ممكنة و معظم تلك الجرائم تتم بواسطة استخدام فيروسات[4].

2- جرائم ترتكب على شبكة الإنترنيت:

لم يكن هناك قلق مع بدايات شبكة الإنترنيت من جرائم يمكن أن ترتكب عليها أو بواسطتها ليس لأنها آمنة في تصميمها و بنائها، بل لمحدودية مستخدميها، و لكون الانترنيت عبارة عن شبكة كبيرة تربط بين شبكات منفردة متواجدة عبر مختلف دول العالم للملايين من أجهزة الكمبيوتر التي يمكنها الاتصال بنفس المواقع في اللحظة ذاتها و سرعة فائقة لكم هائل من

1-منير محمد الجنبهي، ممدوح الجنبيهي، جرائم الانترنيت و الحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، دون طبعة، 2006، ص25.

2- محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة و النشر و التوزيع الأردن، 2009، ص36.

3- محمود أحمد عبابنة، نفس المرجع، ص39.

4- أمير فرج يوسف، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية للمكافحة، الطبعة 01، مكتبة الوفاء القانونية، الإسكندرية، سنة 2011، ص20.

المعلومات و الخدمات، بهذا صارت شبكة الانترنيت مجالا للاعتداءات الإجرامية على الأموال و البنوك و الشركات ...الخ[1].

3- جرائم عابرة الحدود:

مع التطور الذي شهدته تكنولوجيا الاتصالات ظهرت شبكة الإنترنت التي ألغت كل الحدود الجغرافية ما جعلها تكتسب طبيعة دولية كاختراق الشفرات البنكية ، تبييض الأموال و سرقتها، تزوير وإتلاف المعلومات و البيانات ، تخريب أجهزة الحاسب الآلي عند الضرورة ، وهنا يطرح الإشكال حول تحديد الدولة صاحبة الاختصاص القضائي وماهية القوانين الواجبة التطبيق.

4- جريمة يصعب اكتشافها و إثباتها:

و من بين هذه الخصائص صعوبة اكتشافها و صعوبة إثباتها و السبب في ذلك أنها لا تترك أثرا خارجيا، و إذا اكتشفت يكون ذلك بمحض الصدفة، و مما يزيد الأمر تعقيدا أن هؤلاء القراصنة لا يهاجمون من أجهزة الحواسيب الخاصة بهم و إنما يدخلون إلى شبكات بعيدة عنهم و يهاجمون من خلالها[2]، فالجاني يتمتع بقدرات فنية تمكنه من إتمام الجريمة بدقة، و مثال ذلك إرسال فيروسات مدمرة و سرقة الأموال و البيانات الخاصة أو إتلافها و التجسس و سرقة المكالمات و غير ذلك من الجرائم[3]، كما له القدرة على أن يمنع الوصول للدليل بشتى الوسائل فيقوم بإدخال برنامج أو وضع كلمات سرية و رموز تعوق الوصول إلى الدليل و يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه.

و قد يكون سبب صعوبة اكتشافها و إثباتها راجع إلى:

أ- خفاء الجريمة: تتسم الجرائم الماسة بالمعطيات و البيانات بميزة الخفاء على عكس الجرائم التقليدية و التي عادة تكون علنية، فالمجني عليه لا يلاحظها رغم انها قد تقع أثناء و جوده على الشبكة لأن الجاني يتمتع بقدرات تقنية تمكنه من الجريمة بدقة عالية[4].

1-محمد أمين الشوابكة،جرائم الحاسوب و الانترنيت،الجريمة المعلوماتية،دار الثقافة و النشر،عمان،الطبعة 01،سنة2007،ص26.

2-محمد عبيد الكعبي،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت،دار النهضة العربية،القاهرة،ص32.

3-محمد أحمد عبابنة، المرجع السابق، ص37.

4- محمد عبيد الكعبي، المرجع نفسه، ص32.

ب – سرعة محو الآثار و الأدلة: فجريمة المعطيات تقع خارج إطار الواقع المادي الملموس في بيئة إلكترونية يتم فيها نقل المعلومات و تداولها بطريقة غير مرئية علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت[1]. فهي معلومات و بيانات و أرقام تتغير بسرعة فائقة و لا تترك أي أثر أو دليل على ذلك و هنا تأتي صعوبة الكشف عن هذه الجريمة.

5– جريمة ناعمة:

من المتعارف عليه في التقليدية أنه يستعمل فيها أدوات و سبل لتحقيق النتيجة الإجرامية، كجريمة السرقة مثلا فإن الأمر يتطلب كسر، و خلع، أو حتى الحرق...الخ و كذلك جرائم الإرهاب أو جرائم المخدرات...الخ بينما في الجرائم الماسة بالمعطيات فالأمر مختلف تماما و هذا ما يميز هذا النوع من الجرائم و يجعلها من الجرائم الناعمة، لأنها لا تتطلب عنفا لسرقة المعلومات و البيانات أو نقلها من حاسب لآخر أو معرفة الشفرات الخاصة بالبنوك و السطو على أرصدتها، فرغم غياب العنف إلا أن النتيجة المراد تحقيقها تحققت و هذا سبب تسميتها بالجريمة الناعمة.

6– نقص الخبرة لدى الأجهزة الأمنية و القضائية:

تحتاج جرائم المعطيات أو المعلومات غلى خبرة فنية عالية يصعب على المحقق التقليدي التعامل معها، و نظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلب لاكتشافها و البحث عنها كفاءات عالية، لذلك يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية و الإجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة إجراء التحريات السرية، و تتبع مسار العمليات الالكترونية العابرة للحدود[2]، كما أنر رجال الشرطة قد لا يتعاملون بمهارة واحترافية مع الدليل الالكتروني المستمد من الجريمة و إن وجد فقد يتلفونه من غير قصد.

1– خالد ممدوح إبراهيم، المرجع السابق، ص45،46

2– خالد ممدوح إبراهيم، المرجع نفسه، ص45،46

7- مرتكب الجريمة شخص ذو خبرة فائقة:

لاستخدام الحاسب الآلي و ارتكاب جريمة على شبكة الانترنيت لابد أن يكون مستخدم هذا الحاسوب على دراية و خبرة كبيرة في مجال استخدامه و التي تمكنه من تنفيذ جريمته و العمل على عدم اكتشافها، فهذا الشخص يتمتع بذكاء، إذ يمكنه التغلب على كثير من العقبات التي تواجهه أثناء ارتكاب الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل و تطوير في الأنظمة الأمنية حتى لا يستطيع أحد أن يلاحقه و يتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب فالمجرم المعلوماتي يعتمد على الذكاء[1]، فهو شخص ذو مهارات تقنية عالية متخصص في الإجرام المعلوماتي و يستغل مداركه و مهاراته في اختراق الشبكات و كسر كلمات المرور أو الشفرات و يسبح في عالم الشبكات للحصول على ما يريد من البيانات و المعلومات بحيث يستطيع الاختراق و تغيير المعلومات و له القدرة على تغيير البرامج أو تحويل الأموال، لذلك نجد أن معظم من يرتكبون هذه الجرائم هم خبراء في مجال الحاسب الآلي أو المعلوماتي و أن المصالح الأمنية تبحث أولا عن خبراء الكمبيوتر عند ارتكاب الجرائم المعلوماتية.

8- توفر وسائل تقنية تعرقل الوصول للدليل:

فالمجرم المعلوماتي عادة ما يتميز بذكاء خارق على اختراق المواقع و قد يرتكب عدة جرائم كسرقة بيانات أو تغييرها أو اختلاسات فهناك أدلة الكترونية و هي على الغالب الأعم هي أدلة دقيقة جدا، و حتى لا يتمكن شخص آخر من الوصول إلى هذه الأدلة التي قد تبين المجرم، فيقوم هذا الأخير بدوره بمنع الوصول للدليل بشتى الوسائل فيقوم بإرسال برامج أو وضع كلمات سرية و رموز أو يلجأ لتشفير التعليمات لمنع الوصول إلى دليل يدينه.

الفرع الثاني: تصنيف المجرمين المتعديين على المعطيات الرقمية.

من المعلوم أن الإجرام الالكتروني يستهدف أجهزة الحاسوب أو البريد الالكتروني أو المواقع

1- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعية، الاسكندرية،سنة2008،ص32.

الالكترونية على شبكة الانترنيت و خصوصا المواقع الالكترونية للشركات المعروفة مثل شركة مايكروسوفت و غيرها من الشركات العالمية و التي غالبا ما تكون مستهدفة من قبل شركات منافسة لها، و التي قد تتسبب في خسارة الكثير من الأموال، و قد تستهدف المواقع الالكترونية للبنوك بهدف الدخول لحسابات أحد العملاء و سرقة الأموال.

فهذه الجرائم ليست بالضرورة أن يقوم بها المجرم و الضحية داخل بلد واحد فقد يكون هناك بعدا جغرافيا في هذا النوع من الإجرام، فيكون الفاعل في بلد و النتيجة في بلد آخر أو قارة أخرى هذا ما يطلق عليه بالمجرم التقني أو المجرم المعلوماتي لذلك عرف البعض هذا الأخير بانه كل شخص يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة[1].

و من خلال ماتقدم فقد أطلق البعض على هؤلاء بالهاكرز لذلك سنتطرق لتعريه.

تعريف الهاكرز: تسمى باللغة الانجليزية "hacking" و تسمى باللغة العربية التجسس أو اختراق أو قرصنة، حيث يقوم شخص غير مصرح به باختراق نظام تشغيل جهاز ما بطريقة غير شرعية بغرض التجسس أو السرقة أو التخريب حيث للشخص المتجسس أن ينتقل أو يسمح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أمر بالطباعة أو التصوير أو التخريب[2].

دوافع المجرمين المتعدين على المعطيات:

مما لا شك فيه أن السلوك الإنساني أيا كان له ما يفسره، و ما الذي بعث على ارتكابه، و هو الذي يطلق عليه الدوافع إلا أن صورة الدافع فكرة تشوبها بعض الغموض و عدم اتفاق من جانب الفقه و لذلك تعددت الاتجاهات واختلفت فمنهم من أطلق عليه الغاية و منهم النية، و منهم الغرض و منهم الباعث.

1- عبد الفتاح يومي حجازي، التزوير في جرائم الكمبيوتر و الانترنيت، دار الكتب القانونية،مصر،سنة 2008،ص105.

2- ياسر رجب التهامي، خدع الهاكرز، دون طبعة، سنة 2008، ص03.

و مهما يكن الأمر، فإن دراسة دوافع هذا النمط من الإجرام قد تكون لها فائدة مزدوجة فهي:

* أولا قد تساعدنا في إيجاد الحلول المناسبة لمقاومتها و التغلب عليها.

* و ثانيا المساهمة في تحديد التكييف القانوني الذي قد تضفيه عليها، لذلك قد تكون هذه الدوافع شخصية و دوافع خارجية.

أ- الدوافع الشخصية:

بعد دراسات عديدة توصل العلماء و الباحثون إلى أن هناك العديد من الدوافع الشخصية التي يرى فيها مرتكبو الجريمة أسبابا منطقية لتبرير أفعالهم و أنها هي التي تقوم بتحفيزهم على ارتكاب مثل تلك الأفعال و الاعتداءات غير المشروعة في الفضاء السيبراني[1]، و يمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى عدة دوافع منها المالية و أخرى ذهنية:

1- الدوافع المالية:

يعتبر السعي إلى تحقيق الربح في المرتبة الأولى و يمثل في الحقيقة غاية الفاعل و من بين أكثر الدوافع تحريكا للجناة للتعدي على المعطيات المتواجدة في الحاسوب حيث يقوم مرتكبو هذه الجريمة ذوي الكفاءة العالية، بما لديهم من خبرة في المجال التكنولوجي بتوجيه هذه الإمكانات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المالية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك، فيستطيع المجرمون بمجرد دخولهم إلى أنظمة البنوك معرفة أرقام الحاسب و سرقتها أو تحويلها، و يكون المكسب المادي أيضا هدفا لمن هم أقل في المعرفة التقنية و قد يكونون غير مؤهلين على الاطلاق في المجال المعلوماتي و لا يمكنهم الدخول إلى أنظمة تلك الحواسيب و يكون أسلوب ارتكابهم للجرائم أسلوب محدد في مجال معين لا يحتاج إلى خبرة و مهارة[2].

ووفقا للدراسات فغن القطاع المالي يعد أكثر القطاعات استهدافا من قبل الجناة و يرجع ذلك

1-لقد عرف الفضاء السيبراني بأنه: مجال شامل يتكون من شبكة محبكة تضم المنشآت التكنولوجية للإعلام، بما فيها الانترنيت، شبكات الاتصال السلكي و اللاسلكي، أنظمة الإعلام الآلي، دارات مدمجة و معالجات دقيقة و يضم المعلومة الرقمية المنقولة و كدا متعاملي الخدمات على الخط. و للمزيد من التفاصيل أنظر: بلفريد لطفي لمين،الفضاء السبراني:هندسة و فواعل مقال منشور بالمجلة الجزائرية للدراسات السياسية، العدد05، سنة 2016، ص148.

2- أيمن عبد الحفيظ ، الإتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية ،بدون نشر،2005، ص18.

إلى أن هذه البنوك تعتمد و بشكل أساسي على أنظمة التمويل الإلكتروني المستخدمة في الأيدي الخاطئة و بالتالي فإن ملايين الدولارات يمكن أن تنقل في ثواني معدودة إلى الجاني دون أن يترك أي دليل ضده[1].

2- الدوافع الذهنية:

تعد الصورة الذهنية لمرتكبي الجرائم الماسة بالمعطيات أو جرائم الحاسوب و الانترنيت هي صورة البطل الذكي الذي يستحق الإعجاب لا صورة المجرم الذي تستوجب محاكمته فمرتكبو هذه الجرائم يسعون في إظهار تفوقهم و مستوى ثقتهم ببراعتهم لدرجة أنه إزاء أي ظهور لأي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة فيحاولون إيجاد وسيلة إلى تحطيمها أو التفوق عليها[2].

ب- الدوافع الخارجية:

1- دوافع سياسية:

تعد الدوافع السياسية من أبرز بواعث المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية لذلك أصبحت شبكة الانترنيت مجالا خصبا لنشر أفكار العديد من الأفراد و المجتمعات و وسيلة لترويج الأخبار و أمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو نظام الحكم أو بالرموز الدولية و الإساءة لهم بالذم و التشهير ...[1].

2- دوافع الإنتقام:

يعد هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها و

1- محمود أحمد عبابنة، المرجع السابق، ص24.

2- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف ، الأردن ، ص44.

3-تركي عبد الرحمن الموشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته، أطروحة دكتوراه، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، سنة2009، ص39.

غالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية، و من ذلك الشعور بالحرمان من بعض الحقوق المهنية أو الطرد من الوظيفة فيتولد لدى المجرم المعلوماتي الرغبة في الانتقام من رب العمل[1].

3- الأشخاص أو الجهات:

هناك بعض الجرائم التي ترتكب عبر شبكة الانترنت يكون الدافع من وراء ارتكابها إلحاق الأذى بالأشخاص أو جهات بعينها و غالبا ما تكون تلك الجرائم مباشرة ترتكب في صورة ابتزاز أو تهديد أو تشهير مثل ما حصل بإمارات دبي بدولة الإمارات العربية المتحدة عندما قام أحد الأشخاص بقرصنة صور الفتيات و السطو على البريد الإلكتروني الخاص بمجموعة من فتيات تلك الدولة و سرقة صورهن الشخصية و نشرها على موقع خاص بشبكة الإنترنت مع مجموعة صور إباحية ، أيضا ما حصل في المملكة العربية السعودية حينما قام أحد الأشخاص باختراق البريد الإلكتروني الخاص بإحدى الفتيات بالسعودية و الحصول على بعض الصور الشخصية الخاصة بها و ابتزازها فيما بعد ، و قد تكون غير مباشرة تتمثل في الحصول على البيانات و المعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة.

4- دوافع تجارية و اقتصادية:

تعد شبكة الإنترنت مجالا جديدا تماما للعمل التجاري ، إذ سمحت للشركات بالعمل بسرعة و دون استخدام قنوات الاتصال التقليدية عالية التكاليف ، و وفرت إمكانيات متساوية للجميع في كل أنحاء العالم ، وفرضت حدود اقتصادية ، ووفرت فرصا للأمن في عملية تبادل المعلومات داخل المؤسسة الواحدة أو بين مختلف المؤسسات و الشركات و المنظمات البعيدة جغرافيا عن بعضها البعض مما وسع من دائرة المستهلكين ، بالإضافة للحركية التي وفرتها الشبكة وسمحت من جديد بالنظر في الأشكال الجديدة من الخدمات و البضائع ومن أمثلة ذلك إمكانية القيام من خلال الشبكة بحجوزات في الكثير من دول العالم من ذلك حجز التذاكر لحضور الألعاب

1- محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات،دار النهضة العلابية، سنة 2003،ص52.

الرياضية و النشاطات الترفيهية و السفر بالطائرات و السفن و القطارات، و يعمل بنجاح في روسيا نظام للحجز المسبق لبطاقات خطوط السكك الحديدية للسفر على خطوط دول رابطة الدول المستقلة ، ووفر ظهور التسويق عبر شبكات الإنترنت إمكانيات جديدة و رخيصة ، وسريعة و عملية من خلال الشبكات ، لأنه يمكن تحديث صفحات الواب خلال ثوان لا أكثر، و تعتبر بعض صفحات الواب أنه كلما وصلت المعلومات بسرعة للمشترين، كان اتخاذ القرار بالشراء أسرع في هذا المجال. و أظهرت الدراسات أن الكثير من المستخدمين يزورون الصفحات في البداية من أجل التعرف على المنتجات الجديدة و سرعان ما يتخذون قرارات من خلال المعلومات التي يحصلون عليها[1].

رغم الإيجابيات التي حصلت عليها الإنسانية من تطور تكنولوجيا المعلوماتية كشبكة الانترنت و المعلومات الرقمية ، إلا أن العالم اليوم يواجه مشكلة نتيجة زيادة نسبة الجرائم المرتكبة عن طريق الحاسبات الإلكترونية ، وخاصة في المجالات الاقتصادية و الإقراض المالي ، ومن المعلومات التي نشرتها وزارة الداخلية الروسية عام 1997 أن حصة الجرائم المرتكبة عن طريق الحاسبات الإلكترونية بلغت نسبة 0.02 %من عدد الجرائم في المجال المالي و أن الخسائر المادية بلغت أكثر من 20 مليار روبل ، ووفر انفتاح الشبكات إمكانيات أكبر للمقتحمين الذين استطاعوا من خلالها الوصول لإمكانية معرفة كلمة السر، و عناوين الصفحات الإلكترونية و غيرها وحتى الدخول إلى الشبكات بأسماء مسجلة لمستخدمين آخرين ، ونتيجة لتلك التصرفات تضررت شركات معروفة بشكل كبير، وتضررت قدرتها التنافسية و عرضتها لفقدان ثقة الزبائن[2].

5- الدوافع الأمنية و العسكرية:

والتجسس الإلكتروني و الإرهاب الإلكتروني، هذا وقد وقعت في الفترة الأخيرة العديد من الحوادث التي تؤكد ذلك، مثل ما حصل في الفترة ما بين عامي 1990-1991 عندما استطاع

1- محمد البخاري، و مبادئ الأمن ألمعلوماتي الدولي: الدورة المعلوماتية فجرت الحواجز القائمة بين الشعوب، شبكة الضياء للمؤتمرات و الدراسات أنظر الموقع " www.diae.net" تاريخ الإطلاع على الموقع 04-03-2020.

2- محمد البخاري، و مبادئ الأمن ألمعلوماتي الدولي، الموقع السابق.

خمسة متسللين من هولندا التسلل إلى 19 نظاما من أنظمة الحاسب الآلي في مواقع الجيش الأمريكي على شبكة الانترنت، بما في ذلك المواقع التي كانت موجهة مباشرة لعملية عاصفة الصحراء حيث استطاعوا الحصول على معلومات في غاية الأهمية من مواقع دقيقة للقوات الأمريكية و أنواع الأسلحة التي تملكها تلك القوات و قدرة الصواريخ و حركة السفن الحربية الأمريكية في منطقة الخليج. و مثال آخر يتمثل في سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها القوات العسكرية التابعة للدول الأعضاء من حلف شمال الأطلنطي من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية خلال صيف 1994، و مثل ما حصل في إيطاليا عام 1998 م عندما تعرضت عدة وزارات و جهات حكومية و مؤسسات مالية لهجوم من جماعات الأيدي الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها. وكذالك ما حصل عندما قامت مراهقة في الخامسة عشرة من عمرها بمحاولة تسلل إلى موقع خاص بإحدى القواعد العسكرية للغواصات الحربية بسنغافورة ، وفي عام 1999 تمكن مراهق أمريكي عمره 16 عاما من اختراق حاسبات وكالة الفضاء الأمريكية (ناسا) ووزارة الدفاع الأمريكية (البنتاجون) و تمكن من نسخ برامج من إدارة الطيران و الفضاء قيمتها حوالي 7.1 مليون دولار، و في عام 2001 اخترق متسللون حاسبات شبكة كهرباء كاليفورنيا بالولايات المتحدة الأمريكية و خلال شهر ماي 2008 تعرضت العديد من المواقع الإلكترونية البلجيكية إلى عمليات قرصنة، كما أن موقع الأمم المتحدة أيضا تعرض لعملية قرصنة من قبل أحد القراصنة و ذلك في بداية شهر أغسطس 2007 الذي طالب اسرائيل و أمريكا بالتوقف عن شن الحروب و قتل الأطفال، كذلك موقع الكهرباء السورية الذي تعرض لعملية قرصنة في منتصف عام 2007 و ذلك على خلفية الإنقطاعات الدائمة و المتكررة للتيار الكهربائي في معظم المدن السورية و التي تجاوزت أحيانا السبع ساعات.

المبحث الثاني: أركان الجرائم التعلقة بالمعطيات.

استقر الفقه على ضرورة وجود نصوص قانونية تجريمية خاصة لمواجهة الجريمة عبر الوسائط الالكترونية، خاصة بعد ظهور شبكة الانترنيت التي ساهمت بشكل كبير في تفشي الجريمة ووعيا بخطورة الوضع أصدر المجلس الأوربي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص تشريعية عقابية خاصة بالجريمة المعلوماتية[1]، و منذ ذلك الحين و الدول في سعي حثيث لإرساء قواعد قانونية تجريمية تتفق و هذه الظاهرة المستحدثة، و قد سعى المشرع الجزائري في تعديله ق.ع.ج بإضافته للقسم السابع بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" و قد أرسى هذا القسم حماية فعالة لأنظمة المعالجة الآلية للمعطيات، و ذلك رغبة منه في وضع حد للاعتداءات الواقعة على المعطيات من جهة و مواكبة العصرنة و السير قدما نحو تطوير منظومته التشريعية تأسيا بذلك بغيره من التشريعات من جهة أخرى، ومن ثمة نص على مجموعة من الجرائم، و أوجب لها عقوبات قاسية للحد من اقترافها، و كما هو معلوم فإن المشرع يتطلب لقيام جريمة ما توافر أركان الجريمة .

المطلب الأول: الركن المادي للجرائم المتعلقة بالمعطيات الرقمية

يعد الركن المادي للجريمة الجانب الذي يدخل في تكوينها، و يبرز هذا الجانب إلى العالم الخارجي بمظهر مادي يعبر عن سلوك و نتيجة[2]، و يتكون الركن المادي من ثلاث عناصر هي السلوك الإجرامي والنتيجة التي تحققت و العلاقة السببية التي تربط بين السلوك و النتيجة، و قد لا يتوفر الركن المادي دائما على هذه العناصر في جميع الجرائم، فقد يكتفي المشرع بالسلوك وحده للقول بقيام الركن المادي للجريمة دون اشتراطه أن تتحقق النتيجة و صور ذلك ما يسمى بالجرائمالشكلية[3].

و في الحقيقة يصعب الفصل بين العمل التحضيري و البدء في النشاط الإجرامي الماسة

1- قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، سنة 2002، ص37.

2- عبود السيراج، قانون العقوبات، القسم العام، الطبعة الرابعة، مطبوعات جامعة دمشق، سنة 1990، ص143.

3-عبد الله سليمان،شرح ق.ع.ج القسم العام،الجزء الأول،ديوان المطبوعات الجامعية،الجزائر،سنة1998،ص145 .

بالمعطيات، فحتى لو كان القانون لا يعاقب على الأعمال التحضيرية في الجرائم العادية إلا أن الأمر يختلف بعض الشيء في جرائم تكنولوجيا المعلومات، فشراء برنامج الاختراق أو تصميمه أو شراء معدات لفك الشفرات و كلمات المرور، و حيازة صور مخلة بالحياء لأطفال صغار في السن كلها أشياء تشكل جريمة في حد ذاتها، لذلك نجد أن المشرع الفرنسي قد وسع من مفهوم الشروع في الجرائم المعلوماتية باعتبار هذه الأفعال هي مقدمة الفعل غير المشروع و بالتالي فإن الجزء الأكبر من الأعمال التحضيرية يدخل في نطاق الشروع في السلوك المجرم و يعاقب عليه بنفس عقوبة الجريمة التامة[1].

لذلك تحديد الركن المادي في الجرائم الماسة بالمعطيات أو الجرائم المرتكبة عبر الانترنيت يثير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة و المتمثل في الجانب التقني، و هذا ما يميز ركنها المادي الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو شبكة الانترنيت و تبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه، و مكان البداية واكتمال الركن المادي، و أجهزة السلوك الإجرامي المرتكب في العالم المادي أو العالم الافتراضي و غيرها من التساؤلات التي تتعلق بطبيعة الجريمة[2].

الفرع الأول: الركن المادي في جريمة الدخول غير المصرح به و جريمة البقاء الاحتيالي

أولا- في جريمة الدخول غير المصرح به: بالرجوع إلى ق.ع.ج نجده أنه يعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك[3].

و من خلال ذلك نجد أن المشرع نص على فعل مادي و هو الدخول عن طريق الغش، إلا أنه لم يقدم تعريفا له، و بالرجوع إلى بعض التشريعات العربية نجدها تعرف هذا الفعل على أنه دخول شخص بطريقة معقدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة

1- أحمد حسام طه تمام،الجرائم الناشئة عن استخدام الحاسب الآلي،دار النهضة العربية،القاهرة،الطبعة1،سنة2000،ص596

2-منصور بن صالح السلمي،المسؤولية المدنية لانتهاك الخصوصية في نطاق مكافحة جرائم المعلوماتية،السعودية،جامعة نايف العربية للعلوم الأمنية،كلية الدراسات العليا ، سنة2010، ص76.

3- أنظر المادة 394 مكرر من الأمر رقم 66-150 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الجزائري المعدل.

حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها[1]. يتبين لنا أن المشرع الجزائري اكتفى بذكر فعل الدخول فنص على ذلك "... كل من يدخل أو يبقى عن طريق الغش" و لم يذكر الأفعال المادية لفعل الدخول و لم يحدد الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام، لذلك جرم أي وسيلة أو طريقة سوى تم الدخول بطريقة مباشرة أو غير مباشرة على عكس بعض التشريعات الأخرى التي وسعت من دائرة التجريم و ذكرت مجموعة كبيرة من الأفعال التي قد تحدث نتيجة فعل الدخول[2]، و قد تم تجريم تلك الأفعال لعدم وجود حماية قانونية صريحة للبيانات و المعلومات الالكترونية في التشريعات العقابية إضافة إلى لزوم معاملتها معاملة المال و الوثائق و الحقوق الأخرى التي يحظر القانون المساس بها، فالمعلومات و البيانات الالكترونية لها قيمة مادية و معنوية لا تقل عن قيمة الوثائق و الأموال و الحقوق الأخرى المحمية بموجب التشريعات النافذة، و لا إمكانية لتصور وقوع إتلاف إلكتروني لا يكون محله مال إلكتروني معنوي و هو أمر لا يتوفر إلا في بيئة الكترونية قوامها تقنين نظم معلومات، كما قد تحتوي هذه البيانات على دراسات و معلومات خاصة أو أنها برامج تتحكم بأنظمة أو مؤسسات و تسيرها مما يترتب على ما تقدم أن أي من تلك الأفعال قد ينجم عنها تعطيل خدمات ، و قد ينجم عنها تعطيل الأجهزة ووقوع خسائر مادية أخرى، مما يتطلب وجود حماية تشريعية خاصة للمعلومات و البيانات المخزنة في نظام معلومات أو شبكة معلومات لسهولة الوصول إليها و إلغائها و حذفها و إضافتها و تدميرها و إتلافها[3].

فإن الجريمة تقوم بمجرد فعل الدخول إلى النظام دون ضرورة حدوث أية جريمة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمالها تلك

1- أنظر المادة الأولى من المرسوم الملكي السعودي المتعلق بنظام مكافحة الجرائم المعلوماتية السعودية،لـ 27-04-2008.

2-و قد حولت بعض التشريعات معالجة فعل الدخول غير المصرح به،و من بين هذه التشريعات ما نص عليه القانون الأردني: كل من دخل قصدا إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح يعاقب بالحبس ...

3- بهاء فهمي الكبيجي،مدى توفق أحكام جرائم أنظم المعلومات في القانون الأردني، رسالة ماجستير في القانون العام،جامعة الشرق الأوسط،2013، ص26.

المعلومات، بل أن الجريمة تتوافر حتى و لو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام[1].

ثانيا: في جريمة البقاء الاحتيالي.

اعتبر المشرع أن البقاء الاحتيالي جريمة نص عليها في قانون العقوبات بقوله ، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات.....[2] فيتحقق الركن المادي في جريمة البقاء الاحتيالي إذا اتخذ صورة البقاء داخل النظام و يقصد بفعل البقاء " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[3]" .

وقد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام و يدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه، ثم يبقى داخل النظام بعد ذلك و يتحقق في هذا الفرض في الاجتماع المادي لجريمتي الدخول و البقاء غير المشروع في النظام[4].

لذلك تعد هذه الجريمة من الجرائم المستمرة ، فالجريمة تستمر كلما زادت مدة البقاء الغير مشروع داخل النظام المعلوماتي[5]، كما أن جريمة البقاء الاحتيالي لم يشترط فيها القضاء الفرنسي أن تتوافر لدى المجرم نية الإضرار بالنظام المعلوماتي بل يكفي أن يقوم بمجرد البقاء فقط إذا كان غير مشروع، و قد يتسبب المجرم زيادة عن بقائه الغير مشروع في النظام إلى الإضرار بهذا الأخير[6].

1- قارة أمال، المرجع السابق، ص43.

2-انظر المادة 394 مكرر فقرة أولى من ق.ع.ج، المرجع السابق.

3- علي عبد القادر قهوجي،الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية القاهرة،سنة 1999، ص133.

4-علي عبد القادر قهوجي، المرجع نفسه، ص133.

5- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الجزائر،2002، ص85،68.

6- قارة أمال، المرجع السابق، ص43.

وقد نص قانون العقوبات على أنه ، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة...[1].

يتبين أن المادة نصت على ظرفي تشديد لعقوبة الدخول أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام على تأدية وضيفته ، و يكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع و بين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته، أو تعديل البيانات.

الفرع الثاني: الركن المادي في جريمتي الغش المعلوماتي و الإتلاف المعلوماتي

أولا - في جريمة الغش المعلوماتي : تعد جريمة الغش المعلوماتي في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش التي تقع في هذا المجال و لاسيما بعد تراجع المحررات و المستندات و الوثائق و الصكوك الورقية في حين غزت المحررات الإلكترونية كل المجالات مما زاد صعوبة اكتشاف و إثبات الغش في هذا المجال ، أو هو تغيير الحقيقة في مستند رسمي و لكن المستند هنا ليس مستندا عاديا بل هي عبارة عن تسجيلات إلكترونية أو محررات إلكترونية.

وقد أشار المشرع بخصوص الغش بقوله : ... عن طريق الغش ....خاصة مع تزايد حجم الاعتداءات الواقعة عل المعطيات المخزنة داخل الحاسب الآلي التي تمس الأفراد في حقوقهم و أموالهم و حياتهم الخاصة و أمام تزايد فرص الأشخاص للعبث و التلاعب في معطيات الحاسب بتبديلها و تحويرها بالشكل الذي يفقد الثقة بالتقنية و يمس مراكز الأفراد بات من الواجب بسط الحماية لهذه المعلومات و ضمان أمنها و سلامتها من كل تبديل وغش[2].

و يتمثل الركن المادي لجريمة الغش المعلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون وهو تغيير من شأنه أن يسبب ضرار ومن هنا و لقيام هاته الجريمة لا بد من توافر ثلاثة عناصر أساسية:

1- أنظر المادة 492 مكرر 2-3 ق.ع.ج ، القانون السابق.

2- محفوظ أحمد عبابنة، المرجع السابق، ص 107.

- وجود محرر
- تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا.
- أن يترتب على ذلك ضررا.

1- وجود محرر:

لعل من أهم العقبات التي واجهت تطبيق النص الخاص بالغش المعلوماتي هي وجود محرر، فمستند المعلومات ينتج عن إصدار أمر من مشغل الجهاز إلى الطابعة و ذلك بطبع المعلومات التي تم معالجتها آليا داخل جهاز الكمبيوتر، حيث أن البيانات بإدخالها تتم معالجتها و تتحول إلى معلومات مفيدة، و يشترط أن يظهر مستند المعلومات لحيز الوجود، فلا يشترط أن يتم الغش على المستندات المطبوعة على أوراق بواسطة طباعة، فيمكن أن يتم التزوير على المعلومات المعالجة آليا داخل جهاز الكمبيوتر و المسجلة على قرص صلب أو قرص مرن و من هنا يمكن القول بتطبيق ذلك على برنامج كمبيوتر، عندما يكون هذا البرنامج قد دون على أسطوانة أو شريط ممغنط محررا، ومن ثم فإن تغيير الحقيقة فيه يعد غشا أو تزوير لانتقال المعطيات المخزنة إلى جسم مادي، يأخذ صفات المحرر المكتوب، الذي يمكن قراءته بالعين عن طريق الكمبيوتر و الكشف عن مضمونه من قبل الغير[1].

2- تغيير الحقيقة:

يقصد بتغيير الحقيقة هو إبدالها بما يغايرها، و بالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر طالما ظل مضمون المحرر على حالته قبل الإضافة أو الحذف، و يقوم ذلك بصدد المستندات المعلوماتية في حالة حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزءا من برنامج التشغيل أو برنامج التطبيق و يجب في هذه الحالة أن تكون محلا للتجريم.

3- الضرر:

و هو عنصر أساسي في جريمة الغش المعلوماتي، فإذا تخلف الضرر انتفى التزوير و لو توافرت كل أركانه، فالضرر عنصر جوهري في جريمة الغش المعلوماتي، و لا يشترط القانون

1- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات، دار الهدى، الجزائر، طبعة 2010، ص134-135.

وقوع ضرر بالفعل بل يكفي احتمال وقوعه، و يكفي لقيام التزوير أن يكون الضرر ماديا أو أدبيا أو فرديا أو اجتماعيا، و البحث في توافر الضرر من عدمه مسألة تتعلق بالوقائع يفصل فيها قاضي الموضوع، و نظرا لعدم كفاية النصوص المتعلقة بالغش في المحررات لمواجهة الغش المعلوماتي الذي يقع في مجال المعالجة الآلية للمعطيات، فقد عاقب المشرع الفرنسي على الغش المعلوماتي الذي يقع في المستندات المعالجة آليا، سواء كانت داخل الجهاز أو خارجه[1].

ثانيا– الركن المادي في جريمة الاتلاف المعلوماتي:

قد يتخذ الركن المادي لجريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة لها، أو تدميرها أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية:

1– التعديل غير المشروع للمعلومات: يشكل التعديل غير المشروع للمعلومات المبرمجة آليا واحد من أكثر صور إتلاف المعلومات شيوعا، و يمكن تعريفه بأنه كل تغيير غير مشروع للمعلومات و البرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي.

و قد فرقت التوصية الصادرة عن المجلس الأوربي المتعلقة بجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات و البرامج و بين التعديلات غير المصرح بها و التي لا تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي و نظامه[2].

2– تدمير المعلومات : يعد تدمير المعلومات بدوره صورة من صور الإتلاف و إن كان أبعد أثرا من مجرد إجراء بعض التعديلات للمعلومات، و قد أوصى التقرير الصادر عن المجلس الأوربي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات، و لقد ميزت التوصية الصادرة عن المجلس الأوربي بين شكلين من أشكال التدمير الذي يلحق بالمعلومات، الأول يتعلق بمحو المعلومات تماما، و الثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محو تماما، و يذهب البعض إلى أن إخفاء المعلومات

1–خثير مسعود، المرجع السابق، ص137.

2– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي،الإسكندرية، سنة2010،ص418.

دون محوها لا يمكن أن يشكل تدميرا لها، و هو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو أن يكون يكون تعديلا و ليس تدميرا[1].

المطلب الثاني: الركن المعنوي في الجرائم المتعلقة بالمعطيات الرقمية.

لا يكفي للقول بوجود جريمة ما مجرد قيام الواقعة المادية التي تخضع بنص جريمة و لا تخضع لسبب من أسباب الإباحة، بل لا بد من أن تصدر هذه الواقعة عن إرادة فاعلها و ترتبط بها ارتباطا معنويا و هو ما يعبر عنه بالركن المعنوي للجريمة بمعنى وجود رابطة معنوية أو صلة نفسية تربط بين ماديات الجريمة و نفسية فاعلها بحيث يمكن القول بأن الفعل هو نتيجة لإرادة الفاعل، فالركن المعنوي هو المسلك الذهني و النفسي للجاني باعتباره محور القانون الجنائي، ذلك لأنه في إطار هذا الركن تتحقق كافة مقومات المسؤولية الجنائية من إسناد و إذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات[2].

لذلك يتكون الركن المعنوي لجرائم المعطيات الرقمية من عنصريها أي العلم و الإرادة، فالعلم هو إدراك الفاعل للأمور، أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة طبقا للمبادئ العامة المعروفة في قانون العقوبات، و قد يكون القصد عاما أو خاصا، فالقصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي و ينحصر في حدود ارتكاب الفعل، أم القصد الخاص فهو الغاية من تحقيق النتيجة مثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه.

و الأصل أن الفاعل في جريمة المعطيات الرقمية يوجد سلوك إجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه و قاصدا ذلك و مهما يكن لا يستطيع إثبات انتفاء علمه كركن للقصد العام، إذن فالقصد الجنائي العام متوافر في جميع الجرائم المعلوماتية أو الإلكترونية دون أي استثناء و لكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد

1- خالد ممدوح إبراهيم، المرجع نفسه، ص 419.

2- خمايسية حفيظة،التعاون الدولي في مكافحة جرائم الانترنيت،رسالة ماجستير، المركز الجامعي خنشلة،سنة2012،ص24.

الجنائي الخاص مثلا جرائم تشويه السمعة عبر الإنترنيت، جرائم نشر الفيروسات عبر الشبكة[1].

الفرع الأول: الركن المعنوي في جريمة الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية:

بالرجوع إلى ق.ع.ج نجده قد نص على:"كل من يدخل أو يبقى عن طريق الغش[2]"، حيث للركن المعنوي أهمية في قيام جريمة الدخول غير المصرح به إلى نظام كمبيوتر، فالأفعال التي تقوم عليها هذه الجريمة يقوم بها كل مستخدمو الكمبيوتر، و من بين كل هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي، فالركن المعنوي في جريمة الدخول و البقاء غير المشروع يتطلب دراسة القصد العام و الخاص لدلك سنتطرق إلى:

القصد العام: يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة و استكمال عناصرها يتعين أن يشمله علم الجاني، و لكن علم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، و إنما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقائع و تكتسب به أهميتها في نظر القانون، حيث أن عددا من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون، إلا إذا اكتسبت وصفا معينا، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية و لم تعد صالحة لتقوم بها الجريمة[3].

أما القصد الخاص: فهو أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على الفعل، فتوقع النتيجة هو الأساس النفسي الذي تقوم عليه إرادتها، فحيث لا يكون التوقع لا نتصور وجود الإرادة، و النتيجة التي يجب أن يتجه إليها توقع الفاعل هي النتيجة التي يحدده القانون، و هي الدخول غير المصرح به إلى النظام و لا يشترط أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجة، فالقصد الجنائي يتوافر و لو لم يتوقع الجاني هذه الآثار، فيتعين إذن أن يتوقع الجاني أنه سوف يدخل إلى نظام غير مصرح له

1- فضيلة عاقلي،الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري، مقال منشور على الموقع الآتي:www.jilrc.com بتاريخ 10-04-2017 و تم الاطلاع يوم 21-02-2020.

2- انظر المادة 394 مكرر ، ق.ع.ج، القانون السابق.

3- خالد ممدوح، الجريمة المعلوماتية، المرجع السابق، ص260.

بالدخول إليه و لا يشترط أن يتوقع الضرر الذي سوف يلحق النظام من إجراء هذا الدخول.
كذلك من الدخول غير المصرح به، أن يكون مالك النظام قد وضع قيودا للدخول إلى النظام و لم يلتزم الجاني بهذه القيود، أو كان الأمر يتطلب سداد مبلغ نقدي لم يسدده الجاني و قام بالدخول غير المشروع إلى النظام، و يلاحظ في هذا الصدد أن المشرع الجزائري يعاقب على الدخول المجرد غلى النظام المعلوماتي، فبمجرد الدخول تقوم به الجريمة حتى ولو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول نفع أو فائدة طالما الدخول غير مشروع.
و يتحقق فعل الدخول كذلك، كلما دخل الجاني إلى النظام كله أو جزء منه الدخول إلى شبكة الاتصال أو البرامج، و يتحقق الدخول غير المشروع كذلك متى كان مسموحا للجاني بالدخول لجزء معين في البرامج فيتجاوزه إلى جزء آخر غير مسموح له بالدخول فيه مثلا أو أن الجاني دخل على موقع www.amazon.com و هو موقع للبيع الالكتروني معد للجمهور، و لكنه تجاوز الموقع إلى البيانات الخاصة بإعدادات الموقع و تنظيمه، في حين أن هذه البيانات و المعلومات لا يجوز للجمهور الاطلاع عليها، فهنا يكون فعل الجاني مكونا لجريمة الدخول غير المشروع رغم أن الموقع مفتوح للجمهور[1].

الفرع الثاني: الركن المعنوي في جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات و إتلافها.

أولا: في جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات: نص قانون العقوبات على " كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان التحضير مجسدا بفعل أو عدة أفعال مادية ....[2] لذلك تعتبر جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات جريمة عمديه لأن أفعال الاعتداء المتمثلة في أفعال العرقلة و التعطيل تعد من الأفعال العمدية، و هذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يعتبره ظرف مشدد لجريمة الدخول و البقاء غير المشروع داخل النظام، و عليه فالقصد الجنائي المفروض ينتج من طبيعة الأفعال المجرمة[3].

1- خالد ممدوح، الجريمة المعلوماتية، المرجع السابق، ص269.

2- انظر المادة 394 مكرر 5 من ق.ع.ج ، القانون السابق.

3- قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر،الطبعة2،سنة 2007،ص125.

و جريمة الاعتداءات العمدية على المعطيات يتخذ فيها القصد الجنائي بعنصريه العلم و الإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، و يعلم أيضا أنه ليس له الحق في القيام بذلك، و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، و يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي نية الاعتداء، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة و يتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، و إن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

ثانيا: في جريمة إتلاف المعلومات:

يشترط لقيام هذه الجريمة توافر القصد العام فيكفي هذا القصد لثبوت علم الجاني بأن الأموال التي يتعدى عليها بالإتلاف هي ملك للغير و أن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للاستعمال أو ينقص قيمته، و يجب أيضا أن تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل و ينتج عن فعله تحقق الضرر المترتب على جريمته مع علمه أن فعله غير شرعي.

و فعل الإتلاف يتطلب وجود القصد الجنائي و يكفي قيام القصد العام في اتجاه نية الجاني إلى إتلاف الأموال الثابتة أو المنقولة و يتطلب علم الجاني بأن فعله يؤدي إلى إتلاف أموال مملوكة للغير، فإن عدم العلم هنا ينفي القصد الجنائي، و يجب أيضا اتجاه الإرادة للفعل الذي يؤدي إلى الإتلاف، لأن الجريمة عمدية ففي الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بالاعتداء على المعلومات الموجودة داخل الجهاز تتجه إرادة الجاني إلى إتلاف المال و ذلك بوضع برنامج من شأنه أن يغير المعلومات أو يقوم بمحوها[1]، فمن يعمل هذا العمل الإجرامي فهو على درجة عالية من الناحية التقنية ، و بناءا على ذلك فهو يعلم بالفعل بأن هذه الأموال التي تتجه إرادته إلى إتلافها مملوكة للغير فإن القصد الجنائي يكون

1- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، المرجع السابق، ص420.

متوافر و تقوم الجريمة المنصوص عليها باكتمال أركانها أما لو كان الإتلاف ناتج عن حدث غير مقصود، كما لو وقع شئ من العامل أو الموظف على الجهاز أدى إلى إتلاف جزء منه فلا تقوم جريمة الإتلاف العمدي التي تسبب عنها إعاقة النظام المعلوماتي[1].

الفرع الثالث: الركن المعنوي في جريمة السرقة في نظام المعالجة الآلية للمعطيات.

كما سبق فإن جانب من الفقه الجنائي يسلم بأن المعلومات تصبح لأن تكون محلا للسرقة بالاعتداء عليها و اغتصابها من حوزة صاحبها فالمعلومات لها قيمة تقدر بثروات طائلة، و المعلومات من الأموال المعنوية و لذلك فهي تصلح محلا للسرقة و يتم الحصول على هذه المعلومات عن طريق الحصول على كلمة السر و السرقة المعلوماتية يترتب عليها ضرر للغير فقد تكون السرقة بهدف إفشاء سر و يكون ذلك بدخول الجاني إلى نظام معلوماتي خاص و يلتقط المعلومة أو يسرقها بطريقة نسخ شريط أو بطباعتها أو نقلها و الاستيلاء عليها[2].

و في كل الأحوال فإن السرقة المعلوماتية لا يترتب عليها خروج المعلومات من حيازة صاحبها أو الحائز القانوني لها و لكن تخرج فقط من هذه المعلومات.

فالقصد العام: إن الخطأ الذي ينصب على رضا المجني عليه ينفي فعل العلم و ينفي القصد الجنائي كمن يأخذ برنامجا معتقدا أن صاحبه راض عن ذلك فينتفي هنا عنصر العلم و من يستولي على دعائم بها معلومات أو من دخل خطأ على برنامج بالرقم السري فإنه لا يعد مرتكبا لجريمة السرقة.

القصد الخاص: تعد السرقة جريمة عمدية يفترض لإثباتها توافر قصد جنائي خاص و هو الذي يعبر عن نية التملك، لأنها هي التي تكشف عن نية الجاني في حيازة الشئ المعلوماتي و يستدل على توافر القصد من القرائن و الظروف، و نية التملك التي تتجه إليها إرادة الجاني هو عنصر يضاف إلى عنصر القصد العام (العلم و الإرادة) فبالإضافة إلى ضرورة اتجاه الإرادة إلى سرقة الشئ المعلوماتي مع علم الجاني أنه يسرق شئ مملوك للغير يضاف إليهما عنصر نية الاستحواذ على الشئ المسروق[3].

1- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، المرجع السابق، ص421.

2- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، المرجع السابق، ص304.

3- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، المرجع السابق، ص306.

الفصل الثاني: إثبات الجرائم المتعلقة بالمعطيات الرقمية و الجزاءات المقررة لها

لما كان الارتكان إلى القضاء يعتبر من حيث الترتيب الزمني آخر مرحلة يمكن اللجوء إليها، فإن ذلك يجب أن يكون ممن كانت مصالحه مهددة سواء أكانت تلك المصالح محمية بمقتضيات زجرية أو غير زجرية كما يجب أن يكون ذلك اللجوء مقرونا بوسائل مثبتة للاعتداء على تلك المصالح أو مهددة للمراكز.

و كما هو معلوم فإن فكرة الإثبات بصفة عامة يمكن أن تتدرج في سياق الصراع القائم بين كل من مدرسة الإثبات الحر و مدرسة الإثبات المقيد و مدرسة الإثبات المختلط ، و لذلك يبدو من المفيد جدا أن نقف عند نطاق الأخذ باتجاهات تلك المدارس في المجال الجنائي عموما و مجال إثبات الجريمة الماسة بالمعطيات الرقمية على وجه الدقة على اعتبار أن حداثة ظهور هذا النوع من الجرائم يطرح العديد من الإشكالات التي تنبع من صميم طبيعة الجريمة الرقمية ذاتها، و هكذا يمكن القول بأن الطبيعة المادية للجريمة الإلكترونية تفرض على الجهات المكلفة بإنفاذ القانون ضرورة التعامل مع الوسائل الجديدة و الكفيلة بالكشف عن تلك الجرائم من جهة و تحديد مرتكبيها من جهة أخرى.

و في ظل الصعوبات التي تطرحها الجريمة الإلكترونية سواء على المستوى الواقعي أو القانوني يبدو البحث في نظام إثبات هذا النوع من الجرائم مجازفة نظرا لوجود هوة فارقة بين مستوى التنظيم التشريعي للجريمة الماسة بالمعطيات الرقمية و التطور الذي يشهده هذا النوع من الجرائم ، و هي الهوة التي يمكن و صفها بالمتطورة وفق متتالية هندسية تجعل من المستحيل على المشرعين الإحاطة بجميع حيثياتها و جوانبها.

وقد قسمنا هذا الفصل إلى مبحثين تناولنا في المبحث الأول :إثبات الجرائم الماسة بالمعطيات الرقمية، وفي المبحث الثاني الجزاءات المقررة للجرائم الماسة بالمعطيات الرقمية.

المبحث الأول: إثبات الجرائم المتعلقة بالمعطيات الرقمية

إذا كان البحث في مسألة إثبات الجريمة المتعلقة بالمعطيات الرقمية أمرا صعبا، فإن الصعوبة تبدأ انطلاقا من تعريف الجريمة الإلكترونية ذاتها على اعتبار أن التعريف يعتبر مدخلا أساسيا لتحديد نطاق اعتماد وسائل إثبات معينة دون غيرها و مدى السلطات التي يتمتع بها القاضي في تقدير القيمة القانونية لتلك الوسائل أو ما يملكه الأطراف من حرية في التعامل مع نفس وسائل الإثبات، لذلك يذهب معظم المهتمين إلى القول بأن الجريمة الإلكترونية باعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها و على رأسها قاعدة المعطيات و البيانات أو البرامج المعلوماتية، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر مثلا بالنسبة لجرائم الصحافة.

وقد قسمنا هذا المبحث إلى مطلبين تناولنا في المطلب الأول: دور المعاينة في إثبات الجرائم الماسة بالمعطيات الرقمية، في حين تناولنا في المطلب الثاني: دور الشهادة و الخبرة في إثبات الجرائم الماسة بالمعطيات الرقمية.

المطلب الأول: دور المعاينة في إثبات الجرائم المتعلقة بالمعطيات الرقمية

مع تزايد استخدام الكمبيوتر و الانترنيت و الشبكات الداخلية و الخارجية تزايدت نسبة الاعتداء على المعطيات بشكل كبير باستخدام تقنيات جديدة و متطورة يعمد إليها مرتكبو الجرائم، سواء كانت جريمة تمت عبر الكمبيوتر أم جريمة تمت على الكمبيوتر و لذلك كان من الواجب على ضابط الشرطة القضائية الانتقال إلى ذلك المكان، لمعاينة و إثبات الآثار المادية للجريمة و المحافظة عليها و إثبات حالة الأماكن و الأشخاص و كل ما يفيد في كشف الحقيقة، و كذا

إخطار وكيل الجمهورية فورا لكي ينتقل بدوره إلى محل الجريمة في حالة الجناية المتلبس بها[1].

الفرع الأول: تعريف معاينة الدليل الالكتروني في الجرائم المتعلقة بالمعطيات الرقمية

يقصد بالمعاينة: مشاهدة و إثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها.

و المعاينة من إجراء التحقيق الابتدائي، و يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، و الأصل أن يحضر أطراف الدعوى الجزائية للمعاينة، و قد يقرر المحقق أن يجربها في غيابهم، و لا يلتزم المحقق بدعوة محامي المتهم للحضور[2].

كذلك عرفت المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه و يجمع الآثار المتعلقة بالجريمة و كيفية وقوعها و كذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة[3].

- إجراءات معاينة مسرح الجريمة المتعلقة بالمعطيات:

تكون معاينة مسرح الجريمة أول إجراء يقوم به المحقق بعد تلقي البلاغ أو الإخطار به و ذلك في ظروف قد لا يكون فيها عنصر الخصوم أو المتهمين قد ظهر بعد بهذه الصفة على ساحة التحقيق، لذلك عرف مسرح الجريمة بأنه: هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة و مركزها بحيث تكون ميدانا لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند ارتكاب الأفعال المؤثمة جنائيا و التي تدخل في إعداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها.

و حتى تكون للمعاينة في الجرائم المتعلقة بالمعطيات الرقمية فائدة في كشف الحقيقة عنها و

1-نصت المادة 42 من ق.إ.ج.ج" يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية و يتخذ جميع التحريات اللازمة.

2- محمود نجيب حسني، شرح قانون الإجراءات الجنائية،ط3، دار النهضة العربية، القاهرة، سنة1998،ص529.

3- مأمون سلامة، قانون الإجراءات الجنائية، دار الفكر العربي، الطبعة الأولى، سنة 1980، ص374.

عن مرتكبها ينبغي مراعاة عدة قواعد و إرشادات أهمها ما يلي:

– تصوير الحاسبة الإلكترونية و الأجهزة الطرفية المتصلة بها و المحتويات و الأوضاع العامة بمكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسبة و ملحقاتها و مراعاة تسجيل وقت و تاريخ و مكان التقاط كل صورة.

– العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال و نوع الجهاز الذي تم عن طريق الولوج إلى النظام أو الموقع[1].

– ملاحظة و إثبات التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة و التحليل عند عرض الأمر فيها على القضاء.

– وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي للمسؤولين عليها و دور كل واحد منهم.

– فصل الكهرباء عن موقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شأنه التأثير على آثار الجريمة.

– إبعاد الموظفين عن أجهزة الحاسبة الإلكترونية، و كذلك عن الأماكن الأخرى التي توجد بها أجهزة إلكترونية[2].

– عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الجهاز الالكتروني من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة.

1– علي عدنان الفيل، المرجع السابق، ص 32، 33.

2– علي عدنان الفيل، المرجع السابق، ص 34.

– التحفظ عما قد يوجد بسلة المهملات، من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة و الأشرطة و الأقراص الممغنطة غير السليمة و فحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

– التحفظ على مستندات الإدخال و المخرجات الورقية للجهاز ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد بها من بصمات.

الفرع الثاني: حجية الدليل الإلكتروني في إثبات الجرائم المتعلقة بالمعطيات

1– موقف المشرع الجزائري من حجية الدليل الإلكتروني:

لم ينص المشرع الجزائري صراحة على قبول الدليل الالكتروني، و على هذا الأساس يمكن الإعتماد على نص المادة 212 من ق.إ.ج.ج الذي ينص على مبدأ حرية الإثبات في المواد الجنائية تطبيقا لنظام الإثبات الحر، حيث يقابله نص المادة 427 من قانون الإجراءات الفرنسي الذي ينص على ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات، و يحكم القاضي بناءا على اقتناعه الشخصي، و في المقابل ينص قانون الإجراءات بجواز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي نص فيها القانون على خلاف ذلك، و للقاضي أن يصدر حكمه وفقا لاقتناعه الخاص، و لا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه[1].

و من جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات، مما لا يدع مجالا للشك في تطبيقها أمام كل الجهات القضائية، و بالتالي اعتمد المشرع الجزائري نظام الإثبات الحر كأصل عام و نظام الإثبات المقيد كاستثناء[2]، وقد ساير المشرع الجزائري

1– أنظر المادة 212 من ق.إ.ج.ج، القانون نفسه.

2– بوحليط يزيد،السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر، أطروحة دكتوراه،كلية الحقوق،قسم القانون الخاص،جامعة باجي مختار عنابة، سنة 2016، ص285.

الاتجاه العالمي نحو الإتراف أكثر فأكثر بحجية الأدلة الالكترونية على إخلاف أنواعها مثل الإثبات بالكتابة في الشكل الالكتروني[1]، و التوقيع و التصدي الالكترونيين[2].

كذلك نص المشرع الجزائري على مراقبة الاتصالات على مراقبة الاتصالات الالكترونية و حفظ المعطيات المتعلقة بحركة السير و إلزام مؤدي الخدمات بحفظ الأدلة الالكترونية و الاستعانة بكل شخص له مؤهلات لمساعدة الجهات القضائية المختصة[3].

يتبين لنا جليا أن المشرع الجزائري قد أخذ بحجية الأدلة الالكترونية في الإثبات الجنائي، نتيجة لانتشار الجرائم الالكترونية بكافة أنواعها، و قصد تحقيق الفعالية في مكافحتها، و هناك اتجاه دولي للاعتراف بحجية المراسلات الالكترونية بمختلف أنواعها و الاعتراف بحجية الملفات المخزنة في الأنظمة و مستخرجات الحاسوب و البيانات المسترجعة، و حجية الملفات ذات المدلول التقني و البحث و الإقرار بالإثبات بالكتابة في شكلها الالكتروني و تساويه في الحجية مع التوقيع الفيزيائي، و التخلي شيئا فشيئا عن أدلة قيود تحد من الإثبات في البيئة التقنية و مع كل هذا يجب مراعاة المبادئ و الشروط التي تحكم الأدلة الالكترونية، كمبدأ المشروعية، و مبدأ وجوب مناقشة الأدلة، و تأمين الدليل الرقمي ضد التلاعب إضافة إلى صحة الوقائع الواردة بالدليل[4].

1- أنظر المادة 323 مكرر 01 من الأمر رقم 75-58 المؤرخ في 26-09-1975 و المتضمن ق.م و التي تنص على" يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون معدة و محفوظة في ظروف تضمن سلامتها.

2- أنظر المادة 02 الفقرة الأولى من القانون 15-04 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ج.ر رقم 06 الصادرة في 10-02-2015.

3- أنظر المواد 12،04 من القانون رقم 09-04- المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج.ر 47 المؤرخة في 16-08-2009.

4- بوحليط يزيد، المرجع السابق، ص 285،286.

2- موقف التشريعات المقارنة من حجية الدليل الإلكتروني.

تناولت عدد من التشريعات الدليل الإلكتروني و حدد حجيته في الإثبات الجنائي، في حين طبقت بعض التشريعات القواعد العامة في الدليل الإلكتروني ومن بين هذه التشريعات:

- موقف المشرع الايطالي: نص قانون الإجراءات الجنائية الايطالي على الأدلة المعلوماتية و طبق القواعد العامة في الإثبات على الأدلة المعلوماتية إذ أعطى المشرع الايطالي الحرية للقاضي في قبول الأدلة[1]، و منح المشرع الايطالي سلطة تقديرية للقاضي في قبول أي دليل لم ينص عليه القانون إذا اقتنع به ووجد أنه ملائم و يساهم في كشف الحقيقة، واشترط القانون أن تكون الأدلة مشروعة أي تم الحصول عليها بصورة قانونية، و أعطى الحق للأطراف بتقديم أدلتهم و تخضع هذه الأدلة أيضا للسلطة التقديرية للقاضي[2].

كما نص المشرع على أنها:

- تقبل الأدلة بناءا على طلب الأطراف و يتخذ القاضي القرار بدون تأخير و يستبعد الأدلة المحظورة من القانون و تلك التي تبدو تافهة أو عديمة الأهمية.

- يحدد القانون الحالات التي يجوز فيها للقاضي قبول الدليل من تلقاء نفسه.

- يجوز إلغاء القرارات الصادرة بقبول الدليل بعد سماع الأطراف في الخصومة[3].

و أجاز القانون قبول الأوراق المكتوبة أو الوثائق الأخرى التي تمثل وقائع أو تشير إلى أشخاص مسجلة عن طريق التصوير الفوتوغرافي أو السينمائي، أو أية وسيلة أخرى و ذلك إذا

1- نصت المادة 189 من قانون الإجراءات الجنائية الايطالي رقم 447 لسنة 1988 على أنه للقاضي عند طرح دليل لا ينظمه القانون الأخذ به إذا تبين أنه ملائم لضمان التحقيق من الوقائع و لا يؤثر على حرية الإرادة ، و يعمل القاضي على قبول الدليل بعد سماع أقوال الأطراف حول طرق الحصول عليه.

2- سامي جلال فقي حسين،التفتيش في الجرائم المعلوماتية، دراسة تحليلية ، دار الكتب القانونية ،مصر ، 2011. ص229.

3- أنظر المادة 190 من قانون الإجراءات الجنائية الايطالي، المرج نفسه.

تلفت الوثيقة الأصلية لأي سبب أو ضاعت أو سرقت و لم يكن من المستطاع استعادتها جاز استخدام صورة لها[1]، كما أكد في نص المادة على قبول الوثائق التي تشكل الجريمة بأنه: يجب قبول الوثائق التي تشكل جسم الجريمة[2].

و من خلال ما تقدم يمكن تبين القواعد العامة للإثبات التي جاء به القانون الايطالي و ذلك لعدة أسباب منها أن المشرع الايطالي ترك الحرية للقاضي في تقدير الدليل أ منحه السلطة التقديرية الواسعة في الأخذ بالدليل من عدمه، كما أجاز لأطراف الدعوى تقديم الأدلة التي لديهم و التي سيدرسها القاضي و يتخذ القرار بقبوله أو رفضها، كذلك أجاز القانون قبول الأوراق المكتوبة أو الوثائق الأخرى التي تم الحصول عليها عن طريق التصوير أو أية وسيلة أخرى، و هذه العبارة يمكن أن تندرج ضمنها الأدلة المعلوماتية المفرغة على ورق أو المسجلة على أقراص مغناطيسية أو أية دعامة تخزين أخرى[3].

– موقف المشرع الألماني:

أما قانون الإجراءات الجنائية الألماني فلم يورد نصا يحدد حجية الأدلة المعلوماتية، و بالتالي تطبق القواعد العامة في الإثبات الجنائي الواردة في القانون، و قد نص القانون على أنه تفصل المحكمة فيما يتعلق بالأدلة المقدمة وفقا لاقتناعها الحر تبعا للمناقشات في مجموعها، وحدد القانون الألماني الأدلة التي يمكن للمحكمة قبولها حسب قناعتها، و هي الاعتراف و الشهادة، و تقارير الخبراء، و المعاينة، و المستندات، و على الرغم من أن القانون الألماني قد حدد الأدلة إلا أن القضاء الألماني يميل إلى التوسع في قبول الأدلة فقد قبل الشهادة المسموعة بشرط تعزيزها بأدلة أخرى إلا أن المستندات التي اعتبرها القانون أدلة إثبات جرى تحديدها على وجه العموم و لم تحدد ماهية تلك المستندات التي يمكن قبولها، لذلك أعطى القانون الألماني

1– أنظر المادة 234 الفقرة 01، 02 من قانون الإجراءات الجزائية الايطالي، القانون السابق.

2– أنظر المادة 235 من قانون الإجراءات الجزائية الايطالي، القانون السابق.

3– سامي جلال فقي حسين، المرجع السابق ، ص 300.

للقاضي الجنائي الحرية في قبول الأدلة و يمكن قبول الأدلة المعلوماتية إذا تم تفريغها على الورق فتقبل كأدلة مستندات عادية[1].

– موقف المشرع المصري:

لم ينص المشرع المصري على الدليل الالكتروني و بالرجوع إلى القواعد العامة في الإثبات الجنائي الواردة فيه يلاحظ أنه ينص على أنه يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته و مع ذلك فلا يجوز أن يبني حكمه على دليل لم يطرح أمامه في الجلسة، كما نص على أن للمحكمة أن تأمر و لو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة، و يتبين أنه يمكن تطبيق القواعد العامة للإثبات في قانون الإجراءات الجنائية المصري على الأدلة المعلوماتية و تخضع هذه الأدلة للسلطة التقديرية للقاضي في الأخذ بالدليل أو رفضه.

المطلب الثاني: دور الشهادة و الخبرة في إثبات الجرائم المتعلقة بالمعطيات الرقمية

إن الشهادة في مجال الجريمة الرقمية لا يختلف من حيث ماهيتها عنها في الجريمة التقليدية، و أمر سماع الشهود متروك لفطنة المحقق و مرتبط بظروف التحقيق، و بما أن الشهادة من أقدم وسائل الإثبات كان لزاما الرجوع إليها حتى في هذا النوع من الجرائم، كما تعاظم دور الإثبات العلمي للدليل مع ظهور الجرائم الرقمية، و ضرورة اشتقاق الأدلة الرقمية المطلوبة للإثبات في هذه الجرائم و كشف أنماط الجرائم المرتكبة باستخدام الحاسب الآلي، و هو الدور الذي يضطلع به الخبراء القضائيين فأصبح إنشاء المعامل الجنائية مطلبا ملحا لفحص الأدلة الرقمية، و لتقييم عملية الإثبات الرقمي و تحليل الجرائم في نطاق ما يعرف باسم نظم الخبرة الأمنية، و نظرا لحداثة الجرائم الرقمية فإنها لم تأخذ القدر الكافي من الشرح و تقنين إجراءات

1– سامي جلال فقي حسين، المرجع السابق ، ص 301.

إثباتها، سواء من الناحية القانونية أو الفنية و هو ما ألقى على عاتق المعنيين بكشف و تحقيق هذه الجرائم عبئا ثقيلا، حيث تلعب الخبرة القضائية دورا مهما في إثبات هذه الجرائم فهي تنير الطريق للقاضي الذي يهتدي به لتحقيق العدالة[1].

الفرع الأول: دور الشهادة في إثبات الجرائم المتعلقة بالمعطيات الرقمية.

الشهادة في إطار القاعدة الجنائية هي إدلاء الغير (الشهود) بأقوالهم عن وقائع ترتبط بالجريمة موضوع الإجراء الجنائي، فهي بحسب الأصل أقوال يدلي بها الشهود تبين كيفية حدوث ما يؤدي إلى بتكامل (شهود إثبات) أو عدم تكامل (شهود نفي) أركان الجريمة، و الأقوال التي يدلي بها الغير ليست محل رأي أو معتقد شخصي، و إنما مصدرها حقيقة ما، لذلك يتفق الفقه و القضاء على أن إدلاء الشاهد بشهادته إنما هو تقرير لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، لذلك قيل أن الشهود عم عيون القضاء و آذانهم.

و تعد الشهادة من أقدم و أبرز وسائل الإثبات و الحصول على الأدلة حتى أنه يكاد لا يخلو منها تشريع إجرائي على مدار تاريخ القانون الجنائي، و تتنوع الشهادة بحسب الجهة التي يتم الإدلاء بها أمامها، و هذا التنوع ليس له تأثير على قناعة محكمة الموضوع في نظام التنقيب و التحري حيث، يملك القاضي صلاحية كبيرة في بناء قناعته بحسب ما يرتئيه و يتوافق مع ما هو مقرر في أوراق الدعوى[2].

- تعريف الشهادة:

الشهادة في الأصل هي إخبار الشخص بما يكون قد ره أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، ومن ثم فإن الشهود يعتبرون دليل مباشر في الدعوى، و الشهادة بمفهومها التقليدي قد تكون معلومات ناتجة عن استعمال الشخص لحواسه، مثل استعمال حاسة السمع

1- عبد الناصر محمد محمود فرغلي،محمد عبيد سيف سعيد المسماري،الإثبات الجنائي في الأدلة الرقمية من الناحيتين القانونية و الفنية، دراسة تطبيقية و مقارنة، الرياض، 2008، ص23.

2- عبد الأحد جمال الدين، المرجع السابق، ص949.

فقد تأتي الشهادة نتيجة سماع الشخص لأقوال صدرت عن شخص آخر، و قد تكون ناتجة عن حاسة البصر كأن يشاهد الواقعة التي يدلي عنها الشاهد، و على العموم فإن ذلك كله يرجع إلى تقدير قاضي الموضوع في الأخذ بهذه الشهادة أو عدم الأخذ بها.

- الشهادة في الجرائم الالكترونية:

تعد شهادة الشهود في نوعية الجرائم المرتكبة عبر الانترنيت، أو تلك الناتجة عن الحاسوب عامة، من الأدلة الهامة التي يمكن تقديمها للمحكمة، لكونها عاملا حاسما يمثل منطق التعامل مع نوعية هذه الجرائم، فقيام أحد العاملين في أحد الشركات مثلا بالإدلاء بأقوال محددة، و إن كانت تتخذ صفة العمومية أثناء التحقيق في موضوع آخر يمكن أن يكون ذو دلالة في هذا الشأن، ففي جرائم العدوان على حقوق المؤلف فإن الشهادة التي تصلح أن تكون صادرة عن العاملين الذين تم تكليفهم بالقيام بارتكاب النسخ الغير مشروع، إذ يمكن مثلا أن يتولى النسخ أحد المهندسين العاملين في الشركة التي تتولى العدوان على حقوق المؤلف، مثل السماح لمتخصص في نسخ أجزاء من برمجية لكي يتم رصدها في برمجية أخرى[1].

- الشاهد الإلكتروني:

يقصد بالشاهد في الجرائم المتعلقة بالمعطيات هو التقني صاحب الخبرة و التخصص في تقنية و علوم الكمبيوتر و الشبكات، و الذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقضي ذلك، و يطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي، و يشمل عدة طوائف أهمها: مشغلو الحاسب، المبرمجون، المحللون، مهندسو الصيانة، مديرو الصيانة ...الخ[2].

- التزامات الشاهد الإلكتروني:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا للبحث عن أدلة الجريمة بداخله، و السؤال

1- عبد الأحد جمال الدين، المرجع السابق، ص950،951.

2- هلالي عبد الله أحمد، التزامات الشاهد بالإعلام في الجرائم المعلوماتية،دار النهضة العربية، 1997،ص23.

الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات و الإفصاح عن كلمات المرور و الشفرات؟
هناك اتجاهان في هذا الصدد هما:

– الاتجاه الأول: و يرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، و يميل إلى هذا الاتجاه الفقه الجنائي الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشاهد لا يتضمن هذا الواجب، كما أن في القانون التركي نص على أنه لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[1].

– الاتجاه الثاني: و يرى أنصار هذا الاتجاه أنه من بين الالتزامات التي يتحملها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات الجنائية تحتفظ بسلطاتها في مجال الإجراءات المعلوماتية و من ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم، و من ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، و لكن رفض إعطاء المعلومات المطلوبة غير معاقب عليها جنائيا إلا في مرحلة التحقيق و المحاكمة.

و في هولندا يتيح قانون الحاسبة الإلكترونية لسلطات التحري و التحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه و الولوج إلى داخله، كالإفصاح عن كلمات في داخله، كالإفصاح عن كلمات المرور السرية و الشفرات الخاصة بتشغيل البرامج المختلفة، و إذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسوب و كانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.

1– علي عدنان الفيل، المرجع السابق، ص64.

و في اليونان يمكن الحصول من القائم على تشغيل نظام الحاسبة على كلمة المرور السرية للولوج في نظام المعلومات ، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسبة و ذلك لأنه يجب أن يشهد على المعلومات التي حازها بالفعل و ليس عن معلومات جديدة.

يعتبر جوهر الالتزام بالإعلام في الجرائم المعلوماتية أنه متى كان الشاهد المعلوماتي حائزا لمعلومات جوهرية لازمة للبحث عن الأدلة تتطلبها مصلحة التحقيق فإنه يكون مطالبا بأن يعلم بها سلطات التحقيق و التحري على سبيل الإلزام و إلا تعرض للعقوبات المقررة للامتناع عن الشهادة[1].

الفرع الثاني: دور الخبرة في إثبات الجرائم المتعلقة بالمعطيات الرقمية.

يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة و فاعليتها باتخاذ الكثير من الإجراءات و الوسائل المتنوعة اللازمة لتحقيق هدفه، ولما كان ذلك يحتاج إلى جهد لا يستطيع القيام به و تيسيرا عليه لأداء عمله مما اقتضى الاستفادة من أهل الخبرة و الاستعانة بهم، ومنذ بدء ظهور الجرائم ذات الصلة بالحاسبة الإلكترونية، تستعين الشرطة و سلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسبة الإلكترونية، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها و التحفظ عليها أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، حيث تكتسب الخبرة أهمية بالغة في مجال الجرائم الماسة بالمعطيات الرقمية كذلك فإن العلوم و التقنيات المتصلة بها تنتمي إلى تخصصات عملية دقيقة و متنوعة و التطورات في مجالها سريعة و متلاحقة لدرجة قد يصعب معها على المتخصص استيعابها و يمكن القول بصفة عامة بأنه لا

1- هلال عبد الإله أحمد،التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص25.

يوجد حتى الآن خبير لديه معرفة معمقة في سائر أنواع الحاسبات و برامجها و شبكتها كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها و نظرا لأهمية الخبرة في هذا المجال سنتطرق إلى:

1- تعريف الخبرة:

يقصد بالخبرة، بصفة عامة المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الاثنين معا أي العمل و الدراسة.

أما الخبرة القضائية فهي إجراء التحقيق يعهد به القاضي إلى شخص ينعت بالخبير، تتعلق بواقعة أو وقائع مادية يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علميا أو فنيا لا يتوافر في الشخص العادي ولا يستطيع المحقق الوصول إليه وحده[1]، و الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق و المحكمة تحديدا التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها دليل مستقل عن الدليل القولي أو المادي، وإنما هي تقديم فني لهذا الدليل فهي في مجملها تقرير أو رأي فني صادر عن الخبرة في أمر من الأمور المتعلقة بالجريمة و عادة ما يطلق على الخبير في مجال جرائم الإنترنت "بالخبير الإلكتروني الرقمي" و لا يشترط في الخبير الكفاءة العملية في مجال التخصص فحسب بل يجب أن تضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه و على وجه الخصوص الجرائم ذات الصلة بالحاسب الآلي فقد يتعلق الأمر بتزوير المستندات أو التلاعب في البيانات أو بالغش أثناء نقل أو بث البيانات أو جريمة الأموال أو الاعتداء على حرمة الحياة الخاصة أو عرض صور أو أفلام مخلة بالآداب العامة[2].

1- محمود جمال الدين زكي،الخبرة في المواد المدنية و التجارية،مطبعة جامعة القاهرة،1990،ص11.

2- محمد أبو علاء عقيدة،التحقيق و جمع الأدلة في مجال الجرائم الالكترونية، بحث علمي مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية،أكاديمية شرطة دبي مركز البحوث و الدراسات،دبي،2003،ص127.

و يحدد المحقق للخبير مهمته و الميعاد الذي يقدم فيه تقريره، و الأصل أن يباشر الخبير عمله في حضور المحقق و تحت إشرافه و استثناءا أن يتم ذلك في غيابه، وبعد الحصول على المستندات خلال عملية التفتيش يصبح الأمر سهلا حيث يمكن التعرف على بالرؤية و لن يحتاج المحقق لأي مساعدة من قبل الخبير و هذه المستندات مثل أدلة عمل النظام، سجلات إدارة الحاسبة الإلكترونية، وثائق البرامج، السجلات، صيغ مداخلات البيانات و البرامج، وكذلك صيغ مخرجات الحاسبة الإلكترونية المطبوعة و يتم التخطيط على هذه المستندات و يمكن تحديد ما إذا كانت كاملة أصلية، أو صورا من خلال استجواب القائمين على حفظها.

وقد يكون التخطيط على المواد المتعلقة بوسائل الحاسبة الإلكترونية الأخرى أمرا أكثر تعقيدا مثل الأشرطة الممغنطة ، الأسطوانات ، البرامج ، و يحتاج إلى معونة أحد الخبراء الموثوق فيهم حتى يتمكن المحقق من الإلمام بمحتويات الأشرطة أو الأسطوانات دون إحداث أي تغير فيها ، و بالطبع فإن البحث عن المعلومات داخل جهاز الحاسب الإلكتروني ذاته يعد أمرا بالغ التعقيد و يحتاج إلى وجود خبيرا[1].

2- الاستعانة بالخبراء في الجرائم المعلوماتية:

إن الاستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجنائية يرتبط في الحقيقة بمنطق تقليدي يجب أن يعتمده المشرع الجزائري بحيث يسمح بتجاوزه في إطار الجرائم الماسة بالمعطيات و ذلك فضلا عن قاعدة أنه ليس في القانون ما يمنع محكمة الموضوع من ندب خبراء غير مقيدين بجدول المحكمة فإن هذا التوجه القضائي يجب أن يتم تطويره لكي يمكن الاستعانة بخبراء في العالم الافتراضي دون حاجة لإبداء أسباب في منطوقها للاستعانة بالخبراء من خارج الجدول، على أن يشمل التطور إمكانية أن تكون الاستعانة بالخبراء ممتدا إلى أبعد

1- علي عدنان الفيل، المرجع السابق، ص29.

من النطاق الإقليمي والمادي ممثلا في الحدود المادية بين الدول ويمكن أن يكون هؤلاء الخبراء في خارج الإقليم وهو أمر تسمح به مقومات العالم الافتراضي كونه يعد بيئة اتصالية رقمية. فيمكن مثلا الاستعانة بمراكز وهيئات ومؤسسات حكومية أو خاصة تعمل في بيئة تكنولوجيا المعلومات حيث كانت قصد استجلاء الغموض الفني في نظم الإنترنت ودون أن يكون ذلك مكلفا على النحو الذي يفترض حدوثه في العالم المادي وإنما كل ما يحتاج إليه هو توافر بيئة اتصالية رقمية بتكنولوجيا المعلومات والإنترنت فإذا كان توافر مثل هذه البيئة الرقمية أمكن استصدار تشريع يحقق المقصود القانوني من هذا النظام[1].

على أن الأمر هنا على درجة كبيرة من الأهمية تتعلق بالدراية الفنية للقائم بالتحقيق، سيما حالة عدم وجود مثل هذه الدراية الفنية لديه بهذه النوعية من الجرائم ، فهل يجوز له الاستعانة المتواصلة بالخبير الرقمي طوال فترة التحقيق؟.

هذه المسألة على درجة من الخطورة حيث أن القائم بالتحقيق يتواصل عمله بعمل الخبير الذي يستعين به في كافة مراحل التحقيق فيظهر الأمر كما لو كان القائم بالتحقيق يستعين بخبير استشاري هنا، في حين أن بعض التشريعات منحت المتهم صلاحية الاستعانة بخبير استشاري.

كما منح القانون صلاحية التحقيق لغرفة الاتهام باعتبارها درجة ثانية من درجات التحقيق إذ تمتلك سلطات قاضي التحقيق بالإضافة إلى سلطاتها القانونية في مراجعة التحقيق الذي قام به قاضي التحقيق أو النيابة العامة، ومن ثم يكون لها الاستعانة بالخبراء فضلا عن ذلك كله فإنه لما كان الأصل في القانون هو مرحلة التحقيق التي تتم في جلسة المحاكمة فإن محكمة الموضوع تعد السلطة الأصلية التي يمنحها القانون الحق في إجراء تحقيق في الجلسة[2].

1- خالد ممدوح إبراهيم،فن التحقيق الجنائي في الجرائم الالكترونية،المرجع السابق،ص292.

2- خالد ممدوح إبراهيم، المرجع السابق،ص293.

3- أنواع الخبرة التقنية:

إن الاعتماد على الأسلوب الحكومي للتعامل مع ظاهرة الإنترنت سيما في إطار نظم الإثبات، ليجعل من منطق المفاضلة و التبعية هو المنطق السائد ، ومثل هذا الأمر سوف يجعل الجريمة تتفوق على العدالة و أجهزتها بشكل يؤدي دون شك إلى سيادة منطق الجريمة و في ما يلي بيان لذلك:

أ/ الخبرة الخاصة:

و هذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنضمات الخاصة و هي تضم في جنباتها الخبرة الفردية التي تعد من أقوى و أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات و الإنترنت، ويكفي هنا أن نذكر أن المؤسسات الكبرى المتخصصة في الكمبيوتر و الإنترنت تسعى بكل جهودها إلى الاستعانة بأشخاص بينوا كفاءاتهم في مجال الكمبيوتر و الإنترنت، حتى عصاة القانون منهم فهناك اقتصادي يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون و إنما يلزم اللجوء إلى الحلول الاقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الاقتصادية بل أن من الدول من تسعى جاهدة إلى محاولة التعرف على قراصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الإنترنت، و إلى جانب الأفراد توجد المنظمات الخاصة في كافة المحاولات و التي سوف يكون لها السبق في مجال الخبرة[1].

و تختلف المنظمات الخاصة ما بين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الإلكترونية، وبين نوعية من المنظمات التي تسعى إلى فك طلاسم العلم

1- حسين سعيد بن يف الغافري،السياسة الجنائية في مكافحة جرائم الانترنيت، رسالة دكتوراه، كلية الحقوق،عين شمس، سنة 2005،ص443.

الافتراضي على أسس تجارية، فقد استطاعت إحدى الشركات الاسكتلندية المتخصصة في برمجيات الحاسوب و الإنترنت من إعداد مشروع خريطة للعالم الافتراضي على غرار الخريطة الجينية للإنسان، فقد قام بإعدادها مجموعة من خبراء البرمجة الاسكتلنديين كانوا قد شرعوا في إعداد هذا العمل في عام 1998 و استغرق إعدادها ثمانية عشرة شهرا ، و لقد كان من أهم نتائج هذه الخريطة أن تمكنت الخبرة الخاصة من رصد حركة الجريمة عبر الإنترنت ومعرفة تطوراتها في كافة مظاهرها و أشكالها ، حيث برز أكثر من أربعين مظهر من مظاهر الإجرام عبر الإنترنت ، ولقد أمكن من خلال ما تم رصده في إطار خريطة الجريمة عبر الإنترنت إدراك الخبراء لوجود ما يربو عن مائتي ألف موقع جديد للدعارة عبر الإنترنت و لقد استفاد أهل الخبرة الخاصة من رصد هذه الخريطة في التعريف على التهديدات الحقيقية التي تواجه الدول و الأفراد ، مثلا عن إخفاء النصوص بإضافة نصوص أخرى حيث يعد ذلك من أخطر المشاكل التي تواجه العالم الافتراضي فمثل هذه المشكلة تعد ثالث أخطر مشكلة تواجه النظام الأمني في الولايات المتحدة الأمريكية بعد العدوان البيولوجي و الكيمائي[1].

ب/ الجهات التعليمية:

لما كانت شبكة الإنترنت تعد أحد منتجات العلم في حركته التقنية فإنه يمكن القول و بحق أن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات و الجهات التعليمية، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل و هذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية، كما أن التفكير العلمي لا يمكن تجنيه في رصده للظاهرة الإنسانية، والاتجاه العالمي في رصد تطورات الجريمة عبر الإنترنت يتجه إلى

1- عبد الأحد جمال الدين،المرجع السابق، ص1036.

المؤسسات العلمية بحيث يتم دعمها ماديا و معنويا، لتكون أفضل سبل المواجهة، و لقد قامت عدة مؤسسات تعليمية بتكوين قاعدة تتكون من مجموعة خبراء يتمتعون بخبرة كبيرة في مجال الجرائم المعلوماتية لتكون على أهبة الاستعداد لمواجهة الجريمة عبر الإنترنت ، و كذلك دراسة الكمبيوتر بشكل دقيق في الجامعات ومن ذلك جامعة ستانفورد أمريكا، كذلك معهد التكنولوجيا في "ماساتشوستس"[1] الذي قدم للبشرية خبراء على درجة عالية من التفوق[2].

ج/ جهات الضبط القضائي:

شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الإنترنت و في الحقيقة هو نشاط تتزعم الولايات المتحدة الأمريكية في قائمة أجهزة الضبط القضائي في العالم، بحيث تجاوز نشاطها في هذا المجال الإطار الوطني نحو الدولي المتمثل في منظمة الإنتربول أيضا، وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفدرالية الأمريكية FBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب، ومقره سان دييجو، و الذي تم افتتاحه في نوفمبر 2000 وهو بمثابة بيت خبرة عام متعدد الاستشارات في النواحي القضائية غرضه مكافحة التصعيد الخطير في الجريمة عبر الإنترنت، و ذلك بتحليل و تصنيف الدليل الرقمي بحيث يتم إعداد محللين شرعيين للحاسوب ليكون لهم أهمية كبرى في نطاق العمل على تكثيف مواجهة الجريمة عبر الإنترنت، وبين تعدد النواحي التي يتعامل معها المعمل الشرعي الجديد الذي يتكون من التقاء العديد من منظمات الضبط القضائي تتعاون فيما بينها لكي تحقق الفائدة المرجوة منها مثل إدارة مكافحة المخدرات، ووحدة التحقيقات لمكافحة المجرمين ووحدة تحقيقات الجريمة في البحرية، ووحدة الجمارك و مكتب النائب العام للمقاطعة ومكتب حاكم المقاطعة و إدارة شرطة كاليفورنيا.

1- ماساتشوستس: هي جامعة بمدينة كامبريدج بولاية ماساتشوستس تأسست عام1891..

2- حسين بن سعيد بن سيف الغفاري،المرجع السابق، ص453.

د/ التعاون الدولي: قد يكون مفيدا في هذا الإطار التعرض لمنطق التعاون الدولي في مجال الخبرة التقنية، و الحقيقة أن مجال التعاون الدولي إنما يعد تقريرا مسبقا بأهمية اللجوء إلى المنظمات الحكومية في الإطار الإقليمي إذ يكون بين الحكومات المعترف بها في هذا الشأن[1].

4- دور الخبير التقني في حفظ الأدلة الإلكترونية:

في إطار الجرائم المتعلقة بالمعطيات الرقمية نميز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الآلي و بين تلك التي يلزم بقائها في العالم الافتراضي و بين تلك النوعية من الأدلة التي تنتمي إلى العالم الرقمي، و مع ذلك يمكن اللجوء إلى إخراجها في إطار الحاسوب و العالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة و كذلك في البراءة إن التحفظ على الأدلة داخل جهاز الكمبيوتر من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، و هذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف بداية على المدى الذي تكون عليه صحة حركة الكمبيوتر سيما من حيث الخلل و العطب، و يعطي العدوان الفيروسي مثالا حيويا هنا، إذ يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستفادة من هذا الكمبيوتر، ومثال هذا الاتجاه نجده في التشريع الإنجليزي، وتتم عملية حفظ الأدلة داخل جهاز الكمبيوتر بأساليب متعددة تتمثل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي و أقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه ذلك، إن الدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل إلى مظهر آخر بإجراء تعديلات رقمية في البيانات المذكورة[1].

1- عبد الأحد جمال الدين، المرجع السابق، ص 1038، و ما بعدها-

2- خالد ممدوح ابراهيم،عن التحقيق في الجريمة المعلوماتية، المرجع السابق، ص309.

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي فإنه يتطلب من الخبير التقني القيام برصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة و التي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف و السب في غرف المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن التوصل إلى تحديد موضوع السب و القذف و تاريخه و إذا كانت الجريمة من جرائم النشر عبر الإنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسب الآلي المستخدم هنا دون حاجة إلى تحديد الخادم.

وفي مثل هذه الحالة يقوم خبير باستخدام برمجيات مساعدة للتوصل إلى القيام بالحفظ في العالم الرقمي، كما هو الشأن في حجز و تشفير هذه المواقع بعد تحديد جديتها و دقتها ومسارها و هذا أمر يترتب عليه عدم إمكانية حذفها من العالم الرقمي، وإذا قام أحدهم بذلك فإن ذلك يعد قرينة على أنه هو من ارتكب الجريمة، و تستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة، كما هو شأن حال عرض الدليل المقدم إلى محكمة الموضوع أمام جهة قضائية أعلى كالاستئناف أو النقض.

و درءا للمشكلات التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي فإن العديد من المحاكم لجأت إلى ميكنة إدارتها رقميا، حيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى بدورها حفظ الأدلة في العالم الرقمي لعرضها على القضاء كلما تطلب الأمر ذلك[1].

1- خالد ممدوح إبراهيم ، المرجع السابق ، ص 310.

المبحث الثاني: الجزاءات المقررة للجرائم المتعلقة بالمعطيات الرقمية.

إن الجرائم المعلوماتية تعد من الموضوعات الحديثة التي فرضت نفسها بقوة على المستوى الوطني والدولي على حد سواء، والتي تطرح على المشرع الجنائي ضرورة مواجهتها بترسانة قانونية حاسمة ورادعة لمكافحتها وعقاب مرتكبيها.

لذلك قسمنا هذا المبحث إلى مطلبين: تناولنا في المطلب الأول: الجزاءات المقررة للشخص الطبيعي ، وفي المطلب الثاني الجزاءات المقررة للشخص المعنوي.

المطلب الأول: الجزاءات المقررة للشخص الطبيعي.

تنقسم العقوبات المقررة للشخص الطبيعي في الجرائم الماسة بالمعطيات الرقمية إلى عقوبات أصلية وأخرى تكميلية لذلك تناولنا في الفرع الأول: العقوبات الأصلية، و في الفرع الثاني: العقوبات التكميلية.

الفرع الأول: العقوبات الأصلية.

تختلف العقوبات الأصلية باختلاف الجريمة لكونها تضم في كل الحالات الحبس والغرامة، وهذا على النحو الآتي:

أولا – العقوبات الواردة في قانون العقوبات:

– العقوبة المقررة لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات: يعاقب على هذه الجريمة في صورتها البسيطة أي على الدخول أو البقاء الذي لا يترتب عنه أي ضرر بالحبس أي كل من يدخل عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات

المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام تشغيل المنظومة تكون العقوبة الحبس[1]، بينما تضاعف العقوبة على الجريمة في صورتها المشددة إذا ترتب عن الجريمة حذف أو تغيير المعطيات المنظومة، أو إذا ترتب عن الجريمة تخريب نظام تشغيل المنظومة[2].

تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للنظام العام دون الإخلال بتطبيق العقوبات الأشد، فتتشدد العقوبة في جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير للمعطيات التي يحتويها النظام وإما تخريب نظام إشغال المنظومة ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر.

أما في الحالة الثانية فإن هذا الظرف المشدد هو ظرف مادي حيث يكفي أن يقوم الدخول أو البقاء غير المشروع.

– العقوبة المقررة لجريمة الاعتداء على المعطيات:

يعاقب فاعل هذه الجريمة بالحبس[3] وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام[4].

1– يعاقب بالحبس من ستة أشهر إلى سنتين و بغرامة من 50.000 دج إلى 150.000 دج (أنظر المادة 394 مكرر الفقرة 1) من ق.ع.ج ، القانون السابق.

2– أنظر المادة 394 مكرر فقرة 2 من ق.ع.ج (الحبس من ثلاثة أشهر إلى سنة و بغرامة مالية من 50.000 دج إلى 100.000 دج)، القانون السابق.

3– من ستة أشهر إلى ثلاثة سنوات و بالغرامة من 500.000 دج إلى 2.000.000 دج(المادة 394 مكرر)،القانون السابق

4–أنظر المادة394 مكرر 1 من ق.ع.ج (الحبس من سنة إلى ستة سنوات و الغرامة من 1.000.000دج إلى 4.000.000 دج) ، القانون السابق.

– العقوبة المقررة لجرائم التعامل غير المشروع في المعطيات:

يعاقب فاعل هذه الجرائم بغض النظر عن صورها المحددة سابقا بالحبس[1] وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[2].

ثانيا – العقوبات الواردة في قانون التصديق والتوقيع الإلكترونيين.

كذلك يعاقب بالحبس كل أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة[3]. ويعاقب بالحبس[4]، كل مؤدي لخدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة.

كذلك يعاقب بالحبس[5]، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير[6].

ويعاقب بالحبس[7] كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوف، ويعاقب بالحبس[8]، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون

1–من شهرين إلى ثلاثة سنوات و بغرامة من 1.000.000دج إلى 5.000.000دج، من قانون العقوبات، القانون نفسه.

2–يصبح الحبس من أربعة أشهر إلى ستة أشهر و الغرامة من 2.000.000دج إلى 10.000.000دج ، القانون نفسه.

3– المادة 66 من قانون 15–04 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين.(من ثلاثة أشهر إلى ثلاث سنوات و بغرامة من 20.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين) ، القانون نفسه.

4– من شهرين إلى سنة و بغرامة من 200.000دج إلى 1.000.000دج أو بإحدى هاتين العقوبتين فقط،القانون السبق.

5–من ثلاثة أشهر إلى ثلاثة سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين فقط، القانون السابق.

6–أنظر المادة 67،68 من قانون رقم 15–04 ، القانون السابق.

7–من سنة إلى ثلاث سنوات و بغرامة من 200.000دج إلى 2.000.000دج أو بإحدى هاتين العقوبتين من شهرين إلى ثلاث سنوات و بغرامة من 20.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين،القانون السابق.

8– المادة 69،72 من قانون 15–04، القانون السابق.

ترخيص أو كل مؤدي لخدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه، بالرغم من سحب ترخيصه.

ويعاقب بالحبس[1] كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق، ويعاقب كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها[2].

ثالثا: العقوبات المقررة في قانون حق المؤلف والجزائري والحقوق المجاورة.

كذلك يعاقب مرتكب جنحة تقليد مصنف أو أداء فني كما هو منصوص عليها في المادتين 151و 152 أعلاه بالحبس، سواء كان النشر قد حصل في الجزائر أو في الخارج[3].

و نفس القانون نص على أنه " يعد مرتكبا الجنحة المنصوص عليها ....يستوجب العقوبة المقررة في المادة 153 أعلاه كل من يشارك بعمله أو الوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة"[4].

عليها في المادة 153من هذا

ونص كذلك على أنه في حالة العود " تضاعف في العقوبة المنصوص الأمر"[5].

1–من ثلاثة أشهر إلى سنتين و بغرامة من 20.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين فقط(المادة 73) من قانون رقم 15–04.

2– يعاقب بغرامة من 2000دج إلى 200.000دج (انظر المادة 74 من قانون 15–04)، القانون السابق.

3–أنظر المادة 153 من الأمر 03–05 الصادر بتاريخ 19–07–2003 المتعلق بحق حماية المؤلف و الحقوق المجاورة المعدل و المتمم للأمر 14–37.

4– يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000دج إلى 1.000.000دج(انظر المادة 154 من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة ، للأمر نفسه).

5– أنظر المادة 156 الفقة الأولى من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة ، للأمر نفسه.

وبناء على ما تقدم و بتحليل هذه المواد يتبن أن القاضي لا يملك السلطة التقديرية في فرض الغرامة مع الحبس وحده فقط، بل لا بد من الجمع بينهما، إلا أن هذا لا يمنع من القول بوجود سلطة تقديرية للقاضي في تحديد مدة العقوبة المتناسبة مع الفعل الإجرامي، وهذه السلطة ليست مطلقة لأنها بدورها تخضع لرقابة المحكمة العليا[1].

رابعا – العقوبات الواردة في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

وفقا للقانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي فإنه ودون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول[2]، يعاقب كل موظف لا يحترم الكرامة الإنسانية والحياة الخاصة والحريات العامة أو يتعدي على حقوق الأشخاص وشرفهم وسمعتهم بمناسبة أدائه لمهامه المتعلقة بمعالجة المعطيات ذات الطابع الشخصي[3]، وتكون العقوبة هي الحبس.

كما يعاقب بالحبس[4]، كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي دون الحصول على الموافقة الصريحة للشخص المعني[5]، أو يطلع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة خارج إطار أدائه لمهامه.

1- خثير مسعود ، المرجع السابق ، ص 100.

2- المادة 54 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي القانون السابق، (الحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.00دج).

3- المادة 07 من القانون رقم 18-07، القانون نفسه.

4- من سنة إلى ثلاثة سنوات وبغرامة من 100.000 دج إلى 300.00 دج من القانون رقم 18- 07، القانون نفسه.

5- وإذا كان الشخص المعني عديم أو ناقص الأهلية تخضع الموافقة للقواعد المنصوص عليها في القانون العام، ويمكن للشخص المعني أن يتراجع عن موافقته في أي وقت.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية.

كما يعاقب بالحبس كل من ينجز أو يأمر بإنجاز معطيات ذات طابع شخصي دون الحصول على تصريح أو ترخيص مسبق من طرف السلطة الوطنية[1].

ويعاقب بنفس العقوبات كل من يقدم تصريحات كاذبة أو يواصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له من طرف السلطة الوطنية.

ويعاقب بالحبس كل من يقوم بمعالجة المعطيات الحساسة[2] دون الموافقة الصريحة من الشخص المعني وفي غير الحالات المنصوص عليها في القانون[3].

كما يعاقب بالحبس كل من قام بإنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها والمرخص لها.

ويعاقب بالحبس كل من يقوم بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة[4].

1- المادة 12 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي (يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 دج إلى500.000 دج، المادة 56).

2- المادة 03 الفقرة رقم 06 هي معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الأراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو تكون متعلقة بصحته ، بما فيها معطياته الجينية

3- المادة 57 من القانون المتعلق بحماية المعطيات ذات الطابع الشخصي، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من200 . 000 إلى 500. 000 دج

4- المادة 59 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي. (يعاقب بالحبس من سنة إلى ثلاثة سنوات وبغرامة من100 . 000 دج إلى 300. 000 دج)

كما يعاقب بالحبس كل من سمح لأشخاص غير مؤهلين بالولوج إلى معطيات ذات طابع شخصي.

ويعاقب بالحبس كل من يعرقل عمل السلطة الوطنية:

- بالاعتراض على إجراء عملية التحقيق في عين المكان.

- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات.

- والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة المعلومات.

المذكورة. - عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح[1].

ونصت القانون المتعلق بحماية الأشخاص الطبيعيين في مجال حماية المعطيات ذات الطابع الشخصي[2]، على أنه ودون الإخلال بالأحكام الجزائية التي يستدعي تطبيقها طبيعة المعلومات المعنية، يعاقب أعضاء السلطة الوطنية الذين يفشون معلومات محمية بموجب هذا القانون العقوبات المنصوص عليها في المادة 301 من ق.ع.ج.

ويعاقب بالحبس كل من يلج إلى السجل الوطني لحماية المعطيات ذات الطابع الشخصي دون أن يكون مؤهلا لذلك.

كما يعاقب بالحبس، كل مسؤول عن المعالجة يرفض دون سبب مشروع، حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المتعلقة بالمعطيات ذات الطابع الشخصي.

1- المادة 61 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي (يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 60.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط)

2- المادة 62 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي. القانون نفسه.

ودون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول يعاقب المسؤول عن المعالجة الذي يخرق الالتزامات المتعلقة بسرية وسلامة المعالجة[1].

كما يعاقب بنفس العقوبة كل من يقوم بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول وتلك الواردة بالتصريح أو الترخيص.

كما يعاقب بالحبس، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية.

ويعاقب بالحبس كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام القانون[2].

ويعاقب بالحبس من كل من يقوم بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي المتعلقة بجرائم أو إدانات أو تدابير أمن في غير الحالات المنصوص عليها في القانون.

و يعاقب بالحبس كل مسؤول عن المعالجة وكل معالج من الباطن، وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل ولو عن إهمال الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك. ويعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات.

1- المواد 66-67-68 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي، القانون السابق.

2- يعاقب بغرامة من 200.000 دج إلى500.000 دج (المادة 44 من القانون رقم 18-07) المتعلق بحماية المعطيات ذات الطابع الشخصي، القانون نفسه.

يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات[1].

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب جريمة، يؤهل أعضاء ومستخدمو السلطة الوطنية لمعاينة مسح هذه المعطيات.

ويصادر محل الجريمة بغض إلى إعادة تخصيصه أو تدميره في إطار التشريع الساري المفعول، ويتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير.

ويعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون بنفس العقوبات المقررة للجريمة التامة. في حالة العود تضاعف العقوبات المنصوص عليها[2].

الفرع الثاني: العقوبات التكميلية.

نص المشرع الجزائري على عقوبات تكميلية إلى جانب العقوبات الأصلية لذلك نص في قانون العقوبات على أنه " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها[3] ".

1- المواد 71- 70 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي. القانون نفسه.

2- المادة 73-74 من القانون رقم 18-07. المتعلق بحماية المعطيات ذات الطابع الشخصي، القانون السابق.

3- المادة 394 مكرر6 من ق.ع.ج ، القانون السابق.

أما المصادرة فتشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالمعطيات الرقمية ، أما إغلاق المواقع فيتعلق بالمواقع التي تكون محلا للجريمة الماسة بالمعطيات الرقمية و إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عنصر العلم لدى مالكها.

المطلب الثاني: الجزاءات المقررة للشخص المعنوي.

أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي عن ارتكاب أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك في المادة 394 مكررة 5 من ق.ع.ج وتنقسم العقوبات المقررة للشخص المعنوي إلى عقوبات أصلية وأخرى تكميلية.

الفرع الأول: العقوبات الأصلية.

لقد أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي وذلك لنص المادة 18 من قانون العقوبات حيث نصت على " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح وهي:

– الغرامة التي تساوي مرة إلى خمسة مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي من القانون الذي يعاقب على الجريمة.

– واحدة أو أكثر من العقوبات التالية:

* حل الشخص المعنوي.

* غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

* الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

* المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمسة سنوات.

* مصادرة الشيء الذي أستعمل في ارتكاب الجريمة أو نتج عنها.

* نشر أو تعليق حكم الإدانة.

* الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة القضائية على ممارسة النشاط الذي أدى إلى الجريمة، أو الذي ارتكبت الجريمة بمناسبته.

* وبالنسبة للغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية تعادل خمسة مرات الحد الأقصى للعقوبة المقررة للشخص الطبيعي، ونص القانون على أنه " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم الماسة بالمعطيات الرقمية كالدخول والبقاء بالغش وإذا ترتب عن هذه الأفعال حذف أو تغيير المعطيات المنظومة، أو الاعتداء العمدي على المعطيات، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعية"[1].

يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في القانون الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

الفرع الثاني: العقوبات التكميلية.

لم يكتفي المشرع الجزائري بالنص العام والذي يحدد مقدار الغرامة المقررة للشخص تكرار نفس العقوبة حيث نص على " العقوبات المطبقة على الشخص المعنوي والجنح وهي:

المعنوي بل أعاد في مواد الجنايات

1-أنظر المادة 394 مكرر 4 من ق.ع.ج ، القانون السابق.

– الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي من القانون الذي يعاقب على الجريمة.

– واحدة أو أكثر من العقوبات التالية:

* حل الشخص المعنوي.

* غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمسة سنوات.

* الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمسة سنوات.

* المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.

* مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

* نشر أو تعليق حكم الإدانة.

* الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة القضائية على ممارسة النشاط الذي أدى إلى الجريمة، أو الذي ارتكبت الجريمة بمناسبته.

* وبالنسبة للغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية يعاقب بغرامة تعادل خمس مرات الحد الأقصى للعقوبة المقررة للشخص الطبيعي، ونص القانون على أنه" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم كالدخول والبقاء بالغش وإذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، أو الاعتداء العمدي على المعطيات، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1].

1– أنظر المادة 394 مكرر 4 من ق.ع.ج ، القانون السابق.

يعاقب الشخص المعنوي الذي إرتكب إحدى الجرائم المنصوص عليها في القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

وتختلف هذه الغرامة باختلاف تلك المقررة للشخص الطبيعي وذلك تبعا لوجود أو عدم وجود ظروف التشديد وعليه تشدد غرامة الشخص المعنوي تبعا لتشديد غرامة الشخص الطبيعي وتصادر التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعمول به[2].

كما وسع المشرع من دائرة التجريم فنص على العقوبات المطبقة في حالة الاشتراك والشروع " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها[3]، وذلك بشرط:

* اتفاق مجموعة.

* تحضير مسبق مجسد بفعل مادي للجماعة فإذا ارتكبها واحد فقط فلا يعاقب.

* فعل المشاركة في الاتفاق.

بينما تقرر المادة 394 مكرر 7 من قانون العقوبات أنه يعاقب على الشروع في ارتكاب الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات بالعقوبات المقررة للجريمة ذاتها.

وقد نص الأمر المتعلق بحماية حق المؤلف على العقوبات التكميلية بالنسبة للشخص المعنوي كالغلق و المصادرة و نشر ملخص الحكم الصادر في الدعوى لذلك سنتطرق إلى:

1- أنظر الفقرة الثانية من المادة 72 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، القانون السابق.

2- أنظر المادة 394 مكرر5 من ق.ع.ج ، القانون السابق.

* الغلق:

للمحكمة الحكم بغلق المؤسسة التي يستغلها المقلدون سواء كانت مملوكة لهم أو مستأجرة، ويجوز كذلك الحكم بالغلق المؤقت أو النهائي لهذه المؤسسة و ذلك بالموازاة مع حجم الخسائر أو نوع الجريمة القائمة و يرجع الفصل لمحكمة الموضوع[1]، وقد نص على ذلك بأنه" يمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت لمدة لا تتعدى ستة (06) أشهر للمؤسسة التي يستغلها المقلد أو الشركة أو أن تقرر الغلق النهائي عند الاقتضاء[2].

* المصادرة :

تعتبر المصادرة وجوبيه مما يلزم القاضي بأن يحكم بمصادرة و إتلاف جميع الوسائل و العتاد المستخدم في هاته الجريمة، لذلك نص المشرع على أنه" تقرر الجهة القضائية المختصة: مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي مصادرة و إغلاق كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة[3]، وقد حددت المادة 159 من قانون حماية حق المؤلف الجهة التي يمكن أن تؤول إليها هذه الأموال، والوسائل محل المصادرة بحيث قررت تسليمها للمؤلف أو مالك الحقوق أو ذوي حقوقهما، وهي بذلك تعتبر بمثابة تعويض عن الضرر اللاحق بهم.

* نشر ملخص الحكم :

نصت المادة 58 من قانون حماية حق المؤلف على نشر ملخص الحكم، ويقصد بهذه العقوبة التشهير بالمحكوم عليه و التأثير على شخصيته الأدبية فهي ماسة بالشرف و الاعتبار، وهي

1- خثير مسعود، المرجع السابق ، ص 101.

2 - أنظر المادة 156 الفقرة 02 من الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة، القانون السابق.

3- أنظر المادة 157 الأمر المتعلق بحق حماية المؤلف و الحقوق المجاورة، القانون نفسه.

عقوبة تكميلية وجوبية يجب الحكم بها دائما في حال صدور حكم بالإدانة حتى ولو وقف تنفيذ الحكم[1].

1- خثير مسعود، المرجع نفسه، ص 102.

الخاتمة

من خلال دراستنا لموضوع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات عرفنا أنها جريمة مستحدثة، يكون الحساب الآلي فيها أداة لارتكاب الجريمة، وترتكب من مجرم ذو خبرة فائقة في مجال الحاسب الآلي بحيث تعتمد على قمة الذكاء في ارتكابها، وكما نعلم أنها جريمة لا حدود جغرافية لها فهي تتخطى حدود الدولة التي ارتكبت فيها لتتعدى أثارها كافة البلدان على مستوى العالم.

وعرفنا كذالك أن أكثر تلك الجرائم يكون ضمن أهدافها الأساسية، الحصول على المعلومات الالكترونية التي تكون إما محفوظة على أجهزة الحاسبات الآلية وإما منقولة عبر شبكة الانترنت، وأخرى هدفها إما الاستيلاء على الأموال وإما تستهدف الأفراد والجهات الأخرى.

حيث أن من أبرز المشكلات التي أفرزتها جريمة الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات هي التحديات الإجرائية في ميدان التحري والتحقيق والمحاكمة من حيث الاختصاص والقانون الواجب التطبيق خاصة وأن الجريمة المعلوماتية هي جريمة عالمية لا تعترف بالحدود الدولية والإقليمية.

وأنه رغم توفر النصوص القانونية الموضوعية فإن مكافحة جرائم المعلوماتية رهين بالمعيقات الإجرائية التي أفرزتها هذه الجرائم، فبالنسبة لمرحلة التحري والتحقيق فإن أول معيق يواجه حسن سيرها هو غياب القدرات المؤهلة والوسائل الفنية التي تتيح سرعة إدراك ما حصل وأن غياب التأهيل قد يؤدي إلى إتلاف الدليل على الجريمة، فيكون الأثر هو إفلات مرتكبي هذه الجرائم من العقاب. هذا إضافة إلى قصور النصوص الإجرائية التقليدية للضبط و التفتيش لتلاءم المعلوماتية التي تتميز بسهولة إخفاء الدليل، وإلى حين انتهاء التحقيق تبدأ مشكلات المحاكمة وأولها هو الاختصاص، كالاختصاص المتعلق بمكان ووقوع الجريمة أو الاختصاص بناء على معيار إلحاق الضرر،إضافة إلى القانون الواجب التطبيق باعتبارها جريمة عالية عابرة للحدود كما سبق وأن وضحنا.

ورأينا أن التشريع حاول التصدي لهذه الجريمة سواء من خلال النصوص التقليدية في قانون العقوبات أو من خلال النصوص خاصة بها، فبعض الجرائم المعلوماتية كيفت على أنه يمكن إخضاعها للنصوص الجنائية التقليدية في حال غياب نص خاص بها، لهذا يكون من الضروري الإسراع بسن قواعد إجرائية تتلاءم مع طبيعة الجريمة حتى تكون القواعد الموضوعية المجرمة لها أكثر فعالية هذا من جهة، ومن جهة أخرى فإنه لابد من تكاثف الجهود الدولية والإقليمية في حقل الجرائم المعلوماتية لتخطي العقوبات التي تطرحها هذه الجرائم.

إذ يلعب البعد الزمني والمكاني والقانوني، دورا هاما في تشتيت جهود التحري والتنسيق الدولي لتعاقب مثل هذه الجرائم. وهي جرائم تتسم بالغموض حيث يصعب إثباتها والتحقيق فيها ليس كما هو الحال في الجرائم التقليدية وكثير من الجرائم المعلوماتية لا يتم الإبلاغ عنها إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير.

أما من حيث إجراءات التحقيق فيلاحظ غياب نصوص إجرائية تتكفل بوضع ضوابط لتفتيش وضبط المعلومات، وفرض ضمانات قانونية للمتهم المعلوماتي أثناء التفتيش.

أما نطاق استنباط الأدلة وإثبات الجريمة المعلوماتية فإن العديد من الدول لم تتبنى مخرجات الحاسوب الآلي كدليل أمام القضاء، لذلك فإن تطوير أدلة الإثبات بما يتلاءم مع هذا الشكل من الجرائم بات أمر ضروري.

وفي ضل قصور الحماية الجزائية للجرائم المعلوماتية وبرامج الحاسوب الآلي من خلال نصوص الجريمة المعلوماتية والذي يرجع إلى حداثة هذا النوع من الإجرام، أصبحت هناك ضرورة لتكاثف الجهود الدولية وتوافق السياسات الجنائية في مواجهة هذه الجرائم المعلوماتية بوضع اتفاقية دولية تستمد منها التشريعات الجنائية الداخلية ضوابط نصوصها لتحقيق تنظيم جنائي موضوعي وإجرامي شامل.

ولمواجهة الصعوبات المثارة في مجال الجريمة المعلوماتية لا يسعنا في نهاية هذا البحث سوى لتوصية كالآتي:

* وجوب التوسع في إسباغ الحماية الجنائية لبرامج الحاسوب.

* وجوب تجريم الصور الجديدة للاعتداءات التي لم ينص عليها القانون ليومنا هذا.

* ضرورة تجريم الوقائع الإجرامية ذات الصبغة الدولية أو عبر الوطنية كتهريب متحصلات جرائم المخدرات باستعمال الحاسوب الآلي وغسيل الأموال وتمويل الجماعات الإرهابية عبر الانترنت.

* استحداث نص خاص بالاعتداء على سير نظام المعالجة الآلية للمعطيات.

* استحداث نص خاص بالتزوير المعلوماتي، وكذا توسيع مفهوم المحرر ليشمل أية دعامة أخرى.

* حماية البرامج و المعلومات المعالجة بصفة مستقلة عن طريق معاقبة الاستيلاء عليها دون المساس بسلامتها أو أصالتها أو نسخ صور منها عند تشغيل الجهاز.

* إيجاد العقوبات الملائمة على نحو يحقق أهدافها في مجال الردع العام و الخاص.

* مراجعة قواعد إجراءات التحقيق الابتدائي كتلك المتعلقة بالتفتيش والضبط وتحديثها بما يتلاءم مع الطبيعة الخاصة للجرائم المعلوماتية، وتحديث نظرية الإثبات الجنائي للتوصل إلى إثبات الجرائم المعلوماتية التي يصعب إثباتها.

* ضرورة إحالة هذا النوع من الجرائم إلى قضاء متخصص في الجرائم المعلوماتية.

و مع ما نراه من تطور و تقدم في التكنولوجيا و الرقمنة، فهل سيتمكن المشرع الجزائري من مواكبة هذا التطور و توفير الحماية الجزائية و الإجرائية في البئة الرقمية؟

قائمة المصادر و المراجع

النصوص القانونية:

- الأمر رقم 66-156 المؤرخ في 08 جوان المتضمن قانون ق.ع.ج المعدل و المتمم.
- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو 1966 و المتضمن ق.إ.ج.ج.
- الأمر رقم 75-58المؤرخ في 26 سبتمبر 1975 المتضمن ق.م.ج المعدل و المتمم
- المرسوم التشريعي رقم 92-03 المؤرخ في 30 سبتمبر 1992 المتعلق بمكافحة الإرهاب و التخريب، ج.ر عدد 70 بتاريخ 01-10-1992.
- الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، ج.ر عدد 44 المؤرخة في 23-07-2003.
- القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج.ر عدد 47 المؤرخة في 16-08-2009.
- القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين، ج.ر عدد 06 بتاريخ 10-02-2015.
- القانون رقم 18-07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
- القانون الأردني رقم 85 المتعلق بالمعاملات الإلكترونية الصادرة في 2001.
- المرسوم الملكي السعودي المتعلق بنظام مكافحة الجرائم المعلوماتية السعودية،الصادر في 27-04-2007

المراجع :

1- أيمن عبد الحفيظ ، الإتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية ،بدون نشر،2005.

2- أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي، دراسة مقارنة)، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، 2000.

3- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الجزائر،2002.
4- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعية، الاسكندرية، سنة2008 .
5- أمير فرج يوسف، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية للمكافحة، الطبعة 01، مكتبة الوفاء القانونية، الإسكندرية، سنة 2011.
6- إنتصار نوري الغريب، أمن الكمبيوتر و القانون، دار الراتب الجامعية، بيروت، 1994.
7- بهاء فهمي الكبيجي،مدى توفق أحكام جرائم أنظم المعلومات في القانون الأردني، رسالة ماجستير في القانون العام،جامعة الشرق الأوسط،2013.
8- بوحليط يزيد،السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر، أطروحة دكتوراه،كلية الحقوق،قسم القانون الخاص،جامعة باجي مختار عنابة، سنة 2016.
9- تركي عبد الرحمن الموشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته، أطروحة دكتوراه، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، سنة2009.
10- حتمت قاسم، مدخل لدراسة المكتبات و علم المعلومات، القاهرة، دار غريب، سنة 1990.
11- حسين سعيد بن يف الغافري، السياسة الجنائية في مكافحة جرائم الانترنيت، رسالة دكتوراه، كلية الحقوق،عين شمس، سنة 2005.
12- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الاسكندرية، سنة 2008.
13- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي،الإسكندرية، سنة2010.
14- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات، دار الهدى، الجزائر، طبعة 2010.
15- خماسية حفيظة،التعاون الدولي في مكافحة جرائم الانترنيت،رسالة ماجستير، المركز الجامعي خنشلة،سنة2012.
16- رشيدة بوبكر،جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن و منشورات الحلب الحقوقية،الطبعة الأولى، سنة 2012.
17- سامي جلال فقي،التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، 2011.
18- على عدنان الفيل ، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية دراسة مقارنة ، المكتب الجامعي الحديث، 2011.
19- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر و الانترنيت، دار الكتب القانونية،مصر،سنة 2008.
20- عبود السيراج ، قانون العقوبات، القسم العام، الطبعة الرابعة، مطبوعات جامعة دمشق، سنة 1990.

21- عبدالله سليمان، شرح قانون العقوبات الجزائري القسم العام،الجزء الأول،ديوان المطبوعات الجامعية،الجزائر،سنة 1998 .
22- عبد الناصر محمد محمود فرغلي،محمد عبيد سيف سغيد المسماري،الإثبات الجنائي في الأدلة الرقمية من الناحيتين القانونية و الفنية، دراسة تطبيقية و مقارنة، الرياض، 2008.
23- علي عبد القادر قهوجي،الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية القاهرة،سنة 1999.
24- قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، سنة 2002.
25- قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر،الطبعة2،سنة 2007.
26- مفتاح محمد دباب، معجم المصطلحات و تكنولوجيا المعلومات و الاتصال، الدار الدولية للنشر، القاهرة 1995.
27- محمد محمد شتا، فكرة الحماية الجنائية لبرنامج الحاسب الالي، دار الجامعة الجديدة للنشر 2002.
28- محمود نجيب حسني، شرح قانون الإجراءات الجنائية،ط3، دار النهضة العربية، القاهرة، سنة1998.
29- محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة و النشر و التوزيع الأردن، 2009.
30- محمد أمين الشوابكة،جرائم الحاسوب و الانترنيت،الجريمة المعلوماتية،دار الثقافة و لنشر،عمان، الطبعة 01،سنة2007.
31- محمد عبيد الكعبي،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت،دار النهضة العربية،القاهرة.
32- محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات،دار النهضة العلابية، سنة 2003.
33- محمود جمال الدين زكي،الخبرة في المواد المدنية و التجارية ،مطبعة جامعة القاهرة،1990.

34- محمد أبو علاء عقيدة،التحقيق و جمع الأدلة في مجال الجرائم الالكترونية، بحث علمي مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية،أكاديمية شرطة دبي مركز البحوث و الدراسات،دبي،2003.

35- منصور بن صالح السلمي،المسؤولية المدنية لانتهاك الخصوصية في نطاق مكافحة جرائم المعلوماتية،السعودية،جامعة نايف العربية للعلوم الأمنية،كلية الدراسات العليا ، سنة2010 .
36- مأمون سلامة، قانون الإجراءات الجنائية، دار الفكر العربي، الطبعة الأولى، سنة 1980.
37- منير محمد الجنبهي، ممدوح الجنبيهي، جرائم الانترنيت و الحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، دون طبعة، 2006.
38- نائلة محمد فريد فورة،جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة 01، سنة 2005.

39- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف ، الأردن.
40- هلالي عبد الله أحمد، التزامات الشاهد بالإعلام في الجرائم المعلوماتية،دار النهضة العربية، 1997.
41- هشام محمد فريد رستم،قانون العقوبات و محاضر تقنية المعلومات، مكتبة الآلات الحديثة 1992.
42- ياسر رجب التهامي، خدع الهاكرز، دون طبعة، سنة 2008.

الأطروحات و المذكرات:

1- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة ماجستير في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح ، نوقشت بتاريخ 23-04-2013 .
2- بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا، أطروحة دكتوراه، جامعة باتنة، الجزائر، 2015.
3 - بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظم المعلومات في القانون الأردني، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2013 .
4- بوحليط يزيد، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه، ، كلية الحقوق ، قسم القانون الخاص ، جامعة باجي مختار عنابة، 2016.
5- عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، أطروحة دكتوراه ،جامعة قسنطينة، الجزائر،2012.
6- قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، سنة 2002.
7- مباركي دليلة، غسيل الأموال أطروحة دكتوراه علوم تخصص، قانون جنائي باتنة، الجزائر 2008.

المراجع الإلكترونية:

1- فضيلة عاقلي، الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري، مقال منشور على الموقع التالي www.jilrc.com بتاريخ 10-04-2017 و تم الاطلاع يوم 21-02-2020.
2- محمد البخاري،الأنترنيت و مبادئ الأمن ألمعلوماتي الدولي: الدورة المعلوماتية فجرت الحواجز القائمة بين الشعوب، شبكة الضياء للمؤتمرات و الدراسات أنظر الموقع " www.diae.net" تاريخ الإطلاع على الموقع 04-03-2020.

الفهـرس