جامعة محمد خيضر – بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق

دور الأمن المعلوماتي في الحد من الجريمة المعلوماتية

مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

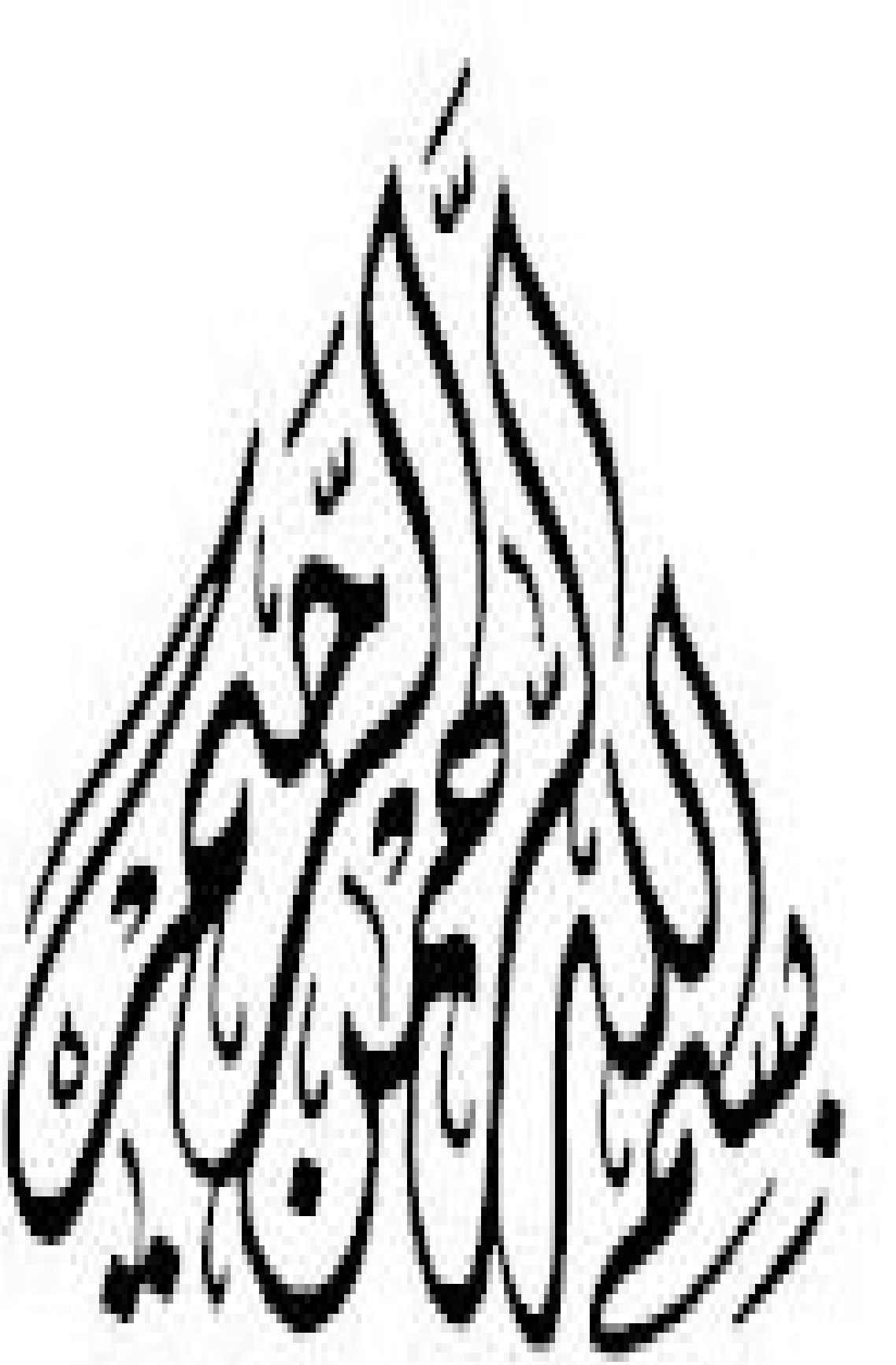
إعداد الطالب:

علاوي محمد

تحت إشراف :

الدكتور: عبد الرؤوف دبابش

الموسم الجامعي: 2017/2016



شكر وعرفان

يسرني أن أتقدم بجزيل الشكر والعرفان إلى من
قدم لي يد المساعدة ووقف وراء هذا العمل المتواضع
بمجوداته و نصائحه القيّمة

أستاذتي وأخي المشرف:الدكتور عبد الرؤوف دبابش فلولا ما
جدتم به علي من توجيه رشيد ورأي سديد ونصح مفيد ما كان
ليتهيأ لي الأمر لأنجز هذا العمل، فلا أملك عرفانا بما تفضلتم
به علي إلا أن أسدي لكم وافر الشكر وأتقدم لكم بعميق
الإمتنان، وخالص
التقدير عسى الله أن يديمكم في خدمة العلم، وينفع بكم البحث
العلمي، فحياكم الله أستاذنا الفاضل وسدد خطاكم

كما يسرني أن أتقدم بجزيل الشكر إلى اللجنة
الموقرة التي قبلت مناقشة هذا البحث المتواضع

إهداء

إلى التي أهدتني نور الحياة و سقتني من دفيء حبها و رعايتها

إلى التي قدمت لي آيات الحب و الحنان، إلى أعذب كلمة رددها لساني إلى من وضعت الجنة تحت قدميها، إلى أمي الحبيبة أطال الله في عمرها.

إلى الذي استلهمت منه معاني الثبات وزرع في قلبي حب العلم ووضع بين جنباتي القوة والعزيمة،إلى الذي وهبني كل رعايته واهتمامه،إلى أبي العزيز أدامه الله لي

الى النور البهي الذي سطع على حياتي بمسرة وضياء لتكون معي في مشواري وسر نجاحي زوجتي الغالية ادامها الله نور يضيء حياتي

إلي أجمل ما أهداني الله إلى فواتح الخير ومفاتيح السعادة أولادي الأحباء حفظهم الله

الى اخي الغالي و استاذي المحترم التي تعجز الكلمات وتتوارى الحروف ويخجل القلم ان يقف هذا الموقف فقد تخونه العبارات وتتشتت الجمل لارد اليك بعض مما تعودته عنك من العطاء فحروفي لا توفيك حقك اخي واستاذي والمشرف على هذا العمل المتواضع الدكتور

عبد الرؤوف دبابش امطرك بوافر دعواتي لك بالتوفيق

إلى من أشد بهم أزري أختي واخواتي حفظهم الله

إلى جميع الأصدقاء

مقدمـــــة

مقدمة :

إن الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا ساهمت و بشكل كبير في تطور معاملات الأفراد ، وتسهيليها ذلك في شتى مجالات الحياة المختلفة ؛ لاسيما بعد ظهور الأنترنت التي وضعت العالم كله في قرية صغيرة ،نظراً لما ميزها من سرعة في تبادل البيانات والمعلومات ، فتطورت بها المعاملات بين الأفراد ، وكان هذا التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات و الاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد، هو المحور الأساسي الذي قامت عليه ثورة جديدة أطلق على تسميتها بالثورة المعلوماتية ،والتي تعد طفرة علمية وتكنولوجية نشهدها اليوم ،حتى بات يطلق على هذا العصر عصر المعلوماتية، والمعلومة هي من أهم ممتلكات الإنسان اهتم بها على ممر العصور فجمعها ودونها وسجلها على وسائط متدرجة التطور؛ بدأً بجدران المعابد والمقابر إلى أن وصل بها المطاف إلى أقراص إلكترونية ممغنطة ، إلا أن هذه الأخيرة ورغم ما تركته من أثار إيجابية نتيجة للتقنيات العالية التي تقوم عليها ، بتوفيرها للراحة والمساهمة في رفع المستوى المعرفي والاقتصادي لمختلف شعوب العالم ، فقد جرّت معها عيوبا استفاق عليها العالم وأدرك خطورتها و بات أثرها ملموسا ومحسوسا ، فهذه الإساءة لاستخدام شبكة الأنترنت والحاسوب مهد الطريق لأصحاب النوايا الخبيثة من المجرمين ، باستخدام هذه التقنية وتطويعها لإشباع رغباتهم وتحقيق نواياهم الإجرامية .

ومن هنا ولدت جرائم جديدة اختلفت عن الجرائم التقليدية اتسمت بخطورتها الكبيرة نظراً لطابعها الخاص سواءاً ما ميز الجريمة أو مرتكبها وصعوبة الإثبات فيها ، وقبل ذلك تثار مشكلة الأمن المعلوماتي الذي يعد مهمة صعبة في ظل الجريمة المعلوماتية التي لا تعترف بالحدود و الأوطان ويعيش محتروفوها في عالم افتراضي ، فتطور الأمن المعلوماتي بات أمراً حتميا وهاجساً أمام رجال القانون ، فكان من الضرورة التصدي لبوادره كي لا يستفحل مع وتيرة النمو المتسارع الذي تشهده دول عربية عدة – ومن بينها الجزائر – في

استخدام النظم المعلوماتية فضلا عن ظروف العولمة والتبعية التكنولوجية من مناخ موات لانتهاك حرمة البيانات الشخصية والمساس بالأمن القومي لهذه الدول و سيادتها الوطنية.
ومن هنا تتجلى أهمية موضوع " **الجريمة المعلوماتية**

أهمية الموضوع :

– تبرز أهمية الموضوع في حداثته ومدى مساسه بالواقع وامتداد خطره ، مما يستدعي ضرورة المعالجة القانونية السريعة و الفورية

– كما تجلت أهمية البحث في بيان طرق و أساليب الحماية المعلوماتية أو ما عرف بالأمن المعلوماتي ، ودوره في قمع الجريمة .

– كما تبرز الأهمية من خلال السيطرة على الوضع بواسطة قوانين حديثة ، ولعله من اللازم الإشارة إلى أن نظام الحماية لم يعد مقتصراً على خصوصية الأفراد وحمايتهم ، بل أنه امتد إلى الدول ذاتها .

– وبالتالي يمكن الاستفادة من هذه الدراسة في مواجهة جرائم الأنترنت والتعامل معها ومكافحتها ، كما يمكن أن تساهم هذه الدراسة بطرح اقتراحات تصورية وتلفت انتباه الباحثين في العلوم الجنائية و الاجتماعية والإنسانية بشكل عام إلى كثير من الظواهر السلوكية المتعلقة باستخدام الانترنت التي تتطلب البحث و الدراسة فيها ، ولفت انتباه كلاً من الجهاز القضائي و القانوني و الأمني إلى سلوكيات و أفعال جنائية ترتكب ضد الآخرين بواسطة الحاسب اللآلي ومن خلال شبكة الأنترنت ، لابد من مواجهتها بضوابط قانونية وقضائية وأمنية .

ومن هذا جاء سبب اختيارنا لهذا الموضوع رغم ما يكتنف هذا الموضوع من صعوبات جمة ترجع إلى حداثة استخدام الحاسب الآلي وما يتسم به من صبغة علمية بحتة غريبة في

تصورنا على رجال القانون نحن نسعى أساسا من خلال هذه الدراسة إلى تحقيق هدفين أساسيين:

– على المستوى النظري التركيز على تحديات القانون الجنائي في مواجهة الإعلام الآلي حيث أن ظهور المعلوماتية و تطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في نطاق القانون الجنائي يفرض حلها البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل ؟

– على المستوى التطبيقي نهدف من هذه الدراسة إلى تغطية الفراغ القانوني الملحوظ في هذا المجال وتوجيه أنظار المشرع الجزائري إلى ضرورة مسايرة قانون العقوبات للتطورات التكنولوجية وما تطرحه من مشاكل قانونية

وهذا برجوع إلى جملة من الدراسات السابقة في هذا المجال منها المذكرات والرسائل التالية:

1– أمال قارة ، الجريمة المعلوماتية ،مذكرة لنيل شهادة الماجستير .

2– سعيد نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في قانون الجزائري ،مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية جامعة الحاج لخضر باتنة .

3– عبد الطيف المعتوق ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة لنيل شهادة الماجستير وعلوم الجنائية .

4– يوسف مناصرة ، جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية .

محاولين الإجابة على الإشكالية الرئيسية :

– **ما هي آليات مكافحة الجريمة المعلوماتية ؟**

وجملة من التساؤلات الفرعية :

- هل يمكننا إعطاء تعريف جامع مانع للجريمة المعلوماتية ؟

- وهل أن الجريمة المعلوماتية تشترك من حيث الأركان مع الجريمة التقليدية ؟

- وكيف واجه المشرع الجزائري هذه الجريمة ؟

لذلك سنعالج موضوع الجريمة المعلوماتية متبعين منهجا يتماشى وطبيعة الموضوع والمنهج الأفضل للخوض في هذا البحث هو المنهج الوصفي التحليلي لأن دراستنا ستعتمد على وصف الجريمة المعلوماتية ، وتحليل أهم النصوص القانونية المنظمة للجريمة المعلوماتية في التشريع الجزائري ولذلك قسمنا الموضوع إلى فصلين حيث تناولنا في الفصل الأول الإطار ألمفاهيمي للجريمة المعلوماتية ثم تطرقنا آليات مواجهة الجريمة المعلوماتية كفصل ثاني بإتباع الخطة التالية:

مقـــدمـــة.

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية .

المبحث الأول : مفهوم الجريمة المعلوماتية .

المبحث الثاني : أركان الجريمة المعلوماتية .

الفصل الثاني : آليات مواجهة الجريمة المعلوماتية .

المبحث الأول : الآليات التشريعية .

المبحث الثاني: الآليات المؤسساتية.

الخـــاتمـــة .

الفصل الأول:الإطار المفاهيمي للجريمة المعلوماتية

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية

منذ ظهور أول الحواسيب في خمسينات القرن الماضي عرفت المعلوماتية تطورا مذهلا ، كما ساعد إقترانها بتكنولوجيات أخرى ، الإلكترونيك ، الرقمنة ...إلخ ، على تعميم إستعمالها وتعدد وظائفها ، والحديث اليوم لم يعد عن الحاسوب و قدراته في إختزال الوقت وتخزين المعلومات وإنجاز عمليات معقدة بقدر ماهو عن تكنولوجيات الإعلام والإتصال ، والفضاء الإفتراضي الذي نشأ نتيجة إرتباط المعلوماتية بمختلف شبكات المواصلات السلكية و اللاسلكية ،ومع التغلغل المتزايد للمعلوماتية و تكنولوجيات الإتصال في مختلف مجلات النشاطات البشرية كان و لابد من وضع أطر قانونية ملائمة لتحديد شروط إستعمال هذه الوسائل الجديدة في مختلف المعاملات ، كما ظهرت أيضا ضرورة وضع نصوص جزائية لحماية الأنظمة المعلوماتية وردع إساءة إستعمالها .

لذلك فالجريمة المعلوماتية باعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية بخصوص تحديد ماهيتها و الأفعال الإجرامية التي تدخل في نطاقها و لذلك ارتأينا التعرض لماهية الجريمة المعلوماتية كمبحث أول و الخصائص المميزة لها والتي خصصنا لها المبحث الثاني وذلك كالأتي:

المبحث الأول: مفهوم الجريمة المعلوماتية

بداية و قبل التكلم عن الجريمة المعلوماتية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات و استخدامها فالبعض يطلق عليها جريمة الغش المعلوماتي، و البعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتلال المعلوماتي ، و آخرون يفضلون تسميتها بالجريمة المعلوماتية ، و حتى نتعرف على هذا النوع من جرائم إرتأينا أن نقسم هذا المبحث إلى ثلاثة مطالب بداية التعرف على الجريمة المعلوماتية كمطلب أول ثم معرفة خصائصها في المطلب الثاني أما المطلب الثالث خصصناه لطبيعة القانونية للجريمة المعلوماتية.

المطلب الأول: تعريف الجريمة المعلوماتية

نتيجة للتطور المذهل في الاتصالات و تكنولوجيا المعلومات ، و ظهور الانترنت فالانتشار الواسع و السريع لها أدى إلى ظهور أشكال و أنماط جديدة من الجرائم ،لاسيما المتعلقة منها بشبكة الانترنت ، والتي باتت تشكل خطرا ليس على سرية النظم الحاسوبية أو سلامته فحسب ،بل تعدت إلى أمن البنى الأساسية الحرجة (1)

فهناك من يرى أن هذه الجريمة القائمة أساسا على التقدم التكنولوجي ،المتطور و المتجدد بصفة دائمة و مستمرة خاصة في مجال تكنولوجيا المعلومات ، و يفضل أن يطلق عليها إصطلاح "جرائم التكنولوجيا الحديثة"،كونها جرائم باعتبارها مرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسيب و غيرها من أجهزة تقنية التي لازالت في تطور و التي قد تظهر في المستقبل ، وهي كذلك جرائم حديثة نظرا لحدثتها النسبية من ناحية ولارتباطها الوثيق بما قد يظهر من أجهزة حديثة ذات طاقة تخزينية و سرعة فائقة و مرونة في التشغيل .

و لكن يبقى إصطلاح الجريمة المعلوماتية على جرائم المتعلقة بالحاسوب و الإنترنت

---

1 عادل عبد العالي إبراهيم خراشي ، اشكالية التعاون الدولي في مكافحة الجرائم، المعلوماتية و سبل التغلب عليها ، دار الجامعة الجديدة، الاسكندرية 2015 ، ص7

إصطلاحا عام و يشمل التقنيات الحالية و المستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب و شبكة الانترنت.

وفي هذا الإطار آثر المشرع الإنجليزي في قانون إساءة استخدام الحاسوب عام 1990 عدم وضع تعريف محدد لجرائم الحاسوب ، بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسبا للتطور العلمي و التقني في المستقبل و حتى يسهل إعطاء تعريف للجريمة المعلوماتية فقد تراوحت التعريفات المقدمة بين المفهوم الواسع و الضيق و جاءت التعريفات كالآتي:

الفرع الأول:المفهوم الواسع

هناك العديد من التعريفات الواسعة من بينها:أن الجريمة المعلوماتية تتمثل في كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية و المعنوية و شبكات الاتصال الخاصة به بإعتبارها من المصالح و القيم المتطورة التي تمتد نصوص قانون العقوبات لحمايتها(1)

كما عرفها الفقيه الألماني (TIEDEMANN) الجريمة المعلوماتية بأنها"تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب

و عرفها الفقيه (Ball.D Leslie) بأنها "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية ".(2)

عرفها الفقيهان (hardcastle et Totty) بأنها تلك الجرائم التي يكون قد وقع في مراحل ارتكبها بعض العمليات الفعلية داخل نظام الحاسب، و بعبارة أخرى هي تلك الجرائم

1- طعباش أمين،الحماية الجنائية للمعلومات الالكترونية ، مكتبة الوفاء القانونية،الاسكندرية،الطبعة الأولى2015، ص16.

2- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي،دار الفكر الجامعي ،الإسكندرية،2006ص2

التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا.

ويوسع البعض مفهوم الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط بأي وجه بالحاسبات ، يتسبب في تكبد أو إمكانية تكبد المجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب.

ويوسع الخبير الأمريكي (Parker) في تعريفها بأنها "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الجاني (1)

ويتبين من خلال هذا التعريف انه ربط الفعل الإجرامي بالخسارة أو الربح أيا كانت الصلة التي تربطه بالمعلوماتية

كما ذهب الفقيهان (credo–michel) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لإرتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته ،كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، و انتهاك ماكينات الحاسب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية و تزييف المكونات المادية و المعنوية للحاسب ،بل و سرقة الحاسب في حد ذاته وأي من مكوناته. (2)

ومن أنصار هذا الاتجاه الموسع من عرفها بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

و يذهب البعض إلى أنه عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة إعتبارات مهمة منها:

1– أن يكون هذا التعريف مقبول و مفهوم على مستوى العالمي .

1– نهلا عبد القادر المومني،الجرائم المعلوماتية ماجستير في القانون الجنائي المعلوماتي ،دار الثقافة للنشر و التوزيع 1429هـ.2008م،الطبعة الأولى،الإصدار الأول–2008،ص49

2– طعباش أمين،مرجع سابق،ص16

2- أن يراعي هذا التعريف التطور السريع و المتلاحق في تكنولوجيا المعلومات .

3- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي

4- أن يفرق هذا التعريف بين الجريمة العادية و الجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

و يمكن القول أن إعطاء هذا التعريف الواسع للجريمة المعلوماتية يدخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسوب أيا كانت هاته العلاقة و أيا كان دور الحاسوب فيها سواء كان وسيلة أو مناسبة لارتكاب التصرفات غير المشروعة أو كان موضوعا لها ،ولذلك فهي كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ،ترتب عنه خسارة تلحق بلصحية أو مكسب يحققه الجاني (1)

ويمكن حصر هذه الحالات كالتالي:

- الحالات التي يكون فيها الإعلام الآلي كمناسبة لارتكاب الجريمة.
- الحالات التي تكون فيها المعلوماتية كأداة لارتكاب الجريمة.
- الحالات التي تكون فيها المعلوماتية كموضوع للجريمة.

إن الإعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكابها أو المناسبة التي ارتكبت في إطارها منتقد لأنه لتعريف الجريمة المعلوماتية و جب الرجوع إلى العامل الأساسي المكون لها، وليس فقط إلى الوسائل المستخدمة لارتكابها ، أو لمجرد أن الحاسب قد استخدم في الجريمة أن نعتبرها من جرائم المعلوماتية وهذا ما أدى إلى ظهور التعريف الضيق

الفرع الثاني:المفهوم الضيق

من بين التعريفات الضيقة للجريمة المعلوماتية بأنها تلك التي يكون الغرض منها موجه ضد الأموال المعلوماتية متى كانت مرتبطة باستخدام نظام المعالجة الآلية للمعطيات ،مع

[1]- المقدم عزالدين عزالدين ،الإطار القانوني للوقاية من جرائم المعلوماتية ومكافحتها ،ملتقى حول الجرائم المعلوماتية بسكرة في 2016/11/16

إقصاء تلك الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير،سواء الأشخاص أو الثقة.

و قد انطلق أنصار التعريف الضيق للجريمة المعلوماتية من النقطة المتعلقة بضرورة تحديد العلاقة بين المعلوماتية و الأفعال غير المشروعة لتحديد ما إذا كانت تلك الأفعال تدخل في نطاق الجريمة المعلوماتية أم لا ؟

أو بعبارة أخرى حتى تشكل الأفعال غير المشروعة جريمة معلوماتية يجب أن تكون موجهة ضد"الأموال المعلوماتية" مع إقصاء تلك الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير سواء الأشخاص أو الأموال، و من أهم التعريفات التي وردت فيه مايلي:

تعريف الفقه (merwe) حيث يرى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي–أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية.

فيما ذهب الفقيه(ros blat) بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه.

وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي. (1)

ويرى البعض أن تعريف كلا من (marwe) و(ros blat) جاء مقصورين على الإطاحة بأوجه الظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع،لأنه يدخل فيه كل سلوك غير مشروع أوضار بالمجتمع.

1–مناصرة يوسف ،جرائم المساس بأنظمة المعالجة الآلية للمعطيات ،رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي و العلوم الجنائية ،قسم العلوم القانونية.جامعة الجزائر ،السنة الجامعية.2008–2009،ص10

وتبنى الفقه الفرنسي تعريفا أضيق من ذلك حيث عرفهابأنها كل الأفعال غير المشروعة الموجهة ضد نظام المعالجة الآلية للمعطيات.

في حين يرى الأستاذ (massa) أن المقصود منها هو الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح .

و يدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة ،تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية،حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا. (1)

الفرع الثالث : التعريف القانوني للجريمة المعلوماتية في القانون الجزائري

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته و ما يحتويه من مكونات غير مادية محلا للجريمة و يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث ، و لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها مسميا إياه:"المنظومة المعلوماتية"وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين"

وقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل و

1-محمد علي العريان،الجرائم المعلوماتية، دار الجامعة الجديدة ،الاسكندرية 2004، ص44

2- مناصرة يوسف ، المرجع السابق ، ص 11

هذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في العاشر من نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات .

و الذي أفرد القسم السابع مكرر منه تحت عنوان:المساس بأنظمة المعالجة الآلية للمعطيات ،و الذي تضمن08 مواد من المادة 394 مكرر و حتى المادة 394 مكرر07 و قد وفق المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى حيث اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها أما فيما يخص الشرط الثاني لمجلس الشيوخ الفرنسي و المتعلق بضرورة توافر النظام على حماية فنية فيبدو أن النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية. (1)

المطلب الثاني: خصائص الجريمة المعلوماتية

إن ظاهرة جرائم المعلوماتية ظاهرة جديدة مستحدثة تقرع في جنباتها ناقوس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر و هول الخسائر الناجمة عن جرائم المعلوماتية التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات و معلومات و برامج بكافة أنواعها)، وبما أن الجريمة المعلوماتية هي جريمة ذات ارتباط بجهاز الحاسوب و شبكة الانترنت أضفى عليها مجموعة من خصائص و السمات المميزة لهذه الجريمة عن الجرائم التقليدية هي: (2)

الفرع الأول:الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول:

-فما يعرف بالمجتمع المعلوماتي هو مجتمع منفتح لا يعترف بالحدود الجغرافية فهو عالم شاسع عبر شبكات يخترق الزمان و المكان دون الخضوع لحرس الحدود فبعد ظهور شبكات

المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة ،فالمقدار التي تتمتع بها الحواسيب و شبكاتها في نقل كميات كبيرة من المعلومات

1- سعيد نعيم ،آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، جامعة الحاج لخضر باتنة 2012-2013 ،ص 41

2- نهلا عبد القادر المومني ،المرجع السابق ،ص50

و تبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد

فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل الإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى .

هذه الطبيعة المميزة للجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول موضوع الاختصاص القضائي للجريمة،وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية ، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام. (1)

و تعتبر القضية المعروفة باسم مرض نقص المناعة المكتسبة (الايدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية ،تتلخص وقائع هذه القضية التي حدثت عام1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة ، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طرواده) ، إذا كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس(2).

وفي الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، و تقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي ، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة ، وبالفعل وافق القضاء الأمريكي على تسليم المتهم ، وتم توجيه إحدى عشرة تهمة إبتزاز إليه وقعت معظمها في دول مختلفة ،إلا أن إجراءات محاكمة المتهم لم تستمر بسب حالته العقلية

1–عبد الله عبد الكريم عبد الله ،جرائم المعلوماتية و الانترنت (الجرائم الالكترونية) دراسة مقارنة،منشورات الحلبي الحقوقية لبنان 2007،ص18

2–مناصرة يوسف ،المرجع السابق ، ص13

و مهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

الأولى:أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية

الثانية:أنها المرة الأولى التي يمثل فيها شخص المحاكمة بتهمة إعداد برنامج خبيث

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية ونظرا للخطورة التي تشكلها على المستوى الدولي،و الخسائر التي قد تتسبب بها تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم .والتعاون الدولي يتمثل في المعاهدات و الاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية و تقديمهم للقضاء العادل ،ومن صعوبة ملاحقة مرتكبي جرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.(1)

أما بالنسبة لأهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة . بالإضافة إلى أن نقص الخبرة لدى الشرطة و جهات الادعاء و القضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت و جمع الأدلة عنها لإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم وبالتالي من أجل التصدي لإجرام المعلوماتي لابد أن تعمل الدول في اتجاهين: **الأول:داخلي** حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم .

الثاني:دولي عن طريق عقد اتفاقيات دولية ،حتى لا يستفيد مجرموا المعلوماتية من عجز التشريعات الداخلية من ناحية ،وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج و آثار هذه الجرائم . (2)

1–هشام محمد فريد،الجوانب الإجرائية للجرائم المعلوماتية ،مكتبة الآلات الحديثة ،أسيوط،ط1،1994 ص82

2– عبد الله عبد الكريم عبد الله ، المرجع السابق ص 21

الفرع الثاني: صعوبة إكتشاف الجريمة المعلوماتية

كذلك يعتبر من أهم ما تتميز به الجريمة المعلوماتية هو صعوبة اكتشافها و إذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا ما قورنت بما يتم اكتشافه من الجرائم التقليدية ، وتعود الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية .كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول و قارات أخرى، إذ أن الجريمة المعلوماتية كما سبق و أشرنا –جريمة عابرة للدول (دولية)، وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم ، ويصعب في جرائم المعلوماتية العثور على دليل مادي للجريمة و ذلك راجع إلى استخدام الجاني وسائل فنية و تقنية معقدة في كثير من الأحيان ،وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل و التلاعب به.(1)

فالجرائم المعلوماتية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها و الإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة و الخبرة في مجال الحسابات غالبا لدى مرتكبها كما أن المجني عليه يلعب دورا رئيسا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك إلى عدم الكشف حتى لا يتبين لموظفيها عما تعرضت له و تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها و مكانتها و هز الثقة في كفاءتها. (2)

1- هلال عبد الله أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية، القاهرة، ط1، 1997 ص22

2- هلال عبد الله أحمد ، المرجع السابق ، ص23

و يرى البعض أن للمجني عليه دورا مثيرا للريبة في بعض الأحيان ،فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل ،وذلك بسبب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي .

ويترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية هي أن هناك إمكانية الحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم ،إذ يعتمد ذلك أساسا على تطور نظم الأمن الخاصة بأنظمة الحاسبات و شبكاتها.(1)

و في الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدو أكثر وضوحا في المؤسسات المالية مثل البنوك و المؤسسات الادخارية و مؤسسات الإقراض و السمسرة حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القاضية حيالها إلى تضاؤل الثقة من جانب المتعاملين معها.

حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحتها .

و قد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي و إلى جانب ذلك فإن المجني عليه يتردد أحيانا في إبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار و قوعها بناء على تقليدها من قبل الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه و نظامه المعلوماتي مما يسهل عملية اختراقه . (2)

1- هشام محمد فريد، المرجع السابق ،ص 82

2- نفس المرجع

الفرع الثالث: صعوبة إثبات الجريمة المعلوماتية

في حال اكتشاف وقوع الجريمة المعلوماتية و الإبلاغ عنها و هو الأمر الذي كما سبق و أشرنا أنه ليس بالأمر السهل فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب.

فالجريمة المعلوماتية لا تترك آثارا ملموسة و بذلك لا تترك شهودا يمكن الاستدلال بأقوالهم و لا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات و تناولها بواسطة نبضات الكترونية غير مرئية.(1)

لذلك فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب و الإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن و أجهزة التحقيق و الملاحقة .ففي هذه البيئة تكون البيانات و المعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل و محوه كليا من قبل الفاعل أمرا في غاية السهولة.

ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من محاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي و ذلك إذا تم إختراقه من قبل الغير أما بالنسبة لإثبات الجريمة فتجدر الإشارة إلى أن وسائل المعاينة و طرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية فالأخيرة لها مسرح تجري عليه الأحداث ،حيث تخلف آثار مادية تقوم عليها الأدلة و هذا المسرح يعطي المجال أمام سلطات الاستدلال و التحقيق الجنائي في الكشف عن الجريمة و ذلك عن طريق المعاينة و التحفظ على الآثار المادية التي خلفتها الجريمة (2)

لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة ذلك ولسببين:

1- سعيد نعيم ، المرجع السابق،ص34

2- نفس المرجع

أولا: إن الجريمة المعلوماتية لا تخلف آثارا مادية.

ثانيا: إن كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان و وقوع الجريمة و حتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبيا ، الأمر الذي يعطي مجالا للجاني أو للآخرين أن يغيروا أو يتلفوا و يعبثوا بالآثار المادية إن وجدت ، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية .

–بالإضافة إلى ذلك فإن نقص الخبرة الفنية و التقنية لدى الشرطة و جهات الإدعاء و القضاء يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية ذلك أن هذا النوع من جرائم يتطلب تدريبا و تأهيلا لهذه الجهات في مجال تقنية المعلومات و كيفية جمع الأدلة و التفتيش و الملاحقة في بيئة الحاسوب و الانترنت، ونتيجة لنقص الخبرة و التدريب كثيرا ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبذل لكشف غموضها و ضبط مرتكبيها جهودا تتناسب و هذه الأهمية .بل إن المحقق قد يدمر الدليل بمحوه محتويات الاسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة . (1)

الفرع الرابع:أسلوب ارتكاب الجريمة المعلوماتية

ما يعرف بذاتية الجرائم المعلوماتية التي تبرز بصورة أكثر وضوحا في أسلوب ارتكابها و طريقتها .، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف و الإيذاء كما هو الحال في جريمة القتل أو الاختطاف ،أو في صورة الخلع أو الكسر و تقليد مفاتيح كما هو الحال في جريمة السرقة فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (soft crime) لا تحتاج إلى العنف ،بل كل ما تحتاج إليه هو القدرة على تعامل مع الجهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة فتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته

1– معتوق عبد الطيف ،الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن ،مذكرة لنيل شهادة الماجستير و علوم الجنائية،2011–2012،ص 24

أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو تغرير بالقاصرين كل ذلك دون حاجة لسفك الدماء .

الفرع الخامس:الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

–تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني علها ، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب و الانترنت يقوم بالجانب الفني من المشروع الإجرامي ،وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب و تحويل المكاسب إليه ،و الاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكا سلبيا و هو الذي يترجم بصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها ،و قد يكون اشتراكا إيجابيا و هو غالبا كذلك يتمثل في مساعدة فنية أو مادية (1)

الفرع السادس: خصوصية مجرمي المعلوماتية

– المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي) فإذا

كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي و المعرفي للمجرم في عملية ارتكابها

–باعتبارها قاعدة عامة –فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات ،أو على الأقل شخص لديه حد أدنى من المعرفة و القدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت . فعلى سبيل المثال فإن الجرائم المعلوماتية ذات طابع الاقتصادي مثل تحويل الالكتروني غير المشروع للأموال يتطلب مهارة و قدرة فنية تقنية عالية جدا من قبل مرتكبها.(2)

1– نهلا عبد القادر المومني ، المرجع السابق ، ص 56

2–نفس المرجع ، ص 57

كذلك فإن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد يكون مختلفا عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي .

ومن أهم سمات المجرم المعلوماتي أنه يمكن أن نستخلص مجموعة من السمات التي

يتميز بها مجرم المعلوماتي ، و التي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين .

ويعد الأستاذ (parker) واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة و المجرم المعلوماتي بصفة خاصة ، وير (parker) ان المجرم المعلوماتي وان كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه ، حتى ولو كان غير عادي كونه يرتكب جريمة متخصصة خاصة إذا تمثلت في سرقة المعلومات المشفرة ما يلزم خبرة تقنية عالية في هذا المجال .(1)

و فيما يلي عرضا لبعض السمات العديدة للمجرم المعلوماتي و التي في الغالب تميزه عن غيره من المجرمين العاديين:

أولا :المجرم المعلوماتي مجرم متخصص

تبين في عديد من القضايا أن عددا من المجرمين لا ترتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم ، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى ،مما يعكس أن المجرم الذي يرتكب الإجرام المعلوماتي هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا:المجرم المعلوماتي مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلومات إلى إرتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت التعرف عليهم و أدت إلى تقديمهم إلى المحاكمة المرة السابقة ، و يؤدي ذلك إلى العودة إلى الإجرام ،وقد ينتهي بهم الأمر كذلك في المرة التالية

1–طعباش أمين ، مرجع سابق ،ص22

إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم المعلوماتي محترف

يتمتع المجرم المعلوماتي بإحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضي الكثير من الدقة و التخصص و الاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك و المؤسسات العسكرية(1)

رابعا:المجرم المعلوماتي مجرم غير عنيف

المجرم المعلوماتي من المجرمين الذين لا يلجأون إلى العنف بتاتا في تنفيذ جرائمهم و ذلك

لأنه ينتمي إلى إجرام –الحيلة –فهو لا يلجأ إلى العنف في ارتكاب جرائمه ،وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

فضلا عما تقدم ، فالمجرم المعلوماتي مجرم ذكي يتمتع بالتكيف الاجتماعي ،أي لا يناصب أحد العداء و أيضا يتمتع بالمهارة و المعرفة وأحيانا كثيرة على درجة عالية من الثقافة.

خامسا:المجرم المعلوماتي له سمات خاصة

يتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين، وهي: (2)

أولا :المهارة

يتطلب تنفيذ الجريمة المعلوماتية قدرا من المهارة يتمتع بها الفاعل ، و التي قد يكتسبها عن

1–طعباش أمين،مرجع سابق،ص22

2– طعباش أمين ، نفس المرجع

طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في المجال

التكنولوجي ، أو بمجرد التفاعل الاجتماعي مع الآخرين ،وهذه ليست قاعدة في أن يكون المجرم المعلوماتي على هذا القدر من العلم ،وهذا ما أثبته الواقع العملي أن جانبا من أنجح مجرمي المعلوماتية ، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.(1)

ثانيا:المعرفة

تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة المواد و تنفيذها ، و إمكانيات نجاحها ، واحتمالات فشلها،فالجناة عادة يمهدون لارتكاب جرائهم بالتعرف على كافة الظروف المحيطة بهم ، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم و الكشف عنهم، و تميز المعرفة بمفهومها السابق مجرمي الانترنت ، حيث يستطيع مجرم الانترنت أن يكون تصورا كاملا لجريمته

ثالثا :الوسيلة

ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتي لإتمام جريمته.

و هذه الوسائل قد تكون في غالب الأحيان ،وسائل بسيطة وسهل الحصول عليها خصوصا إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة الشائعة أما كان النظام من الأنظمة غير المألوفة فتكون هذه الوسائل معقدة و على قدر من الصعوبة . (2)

رابعا: السلطة

يقصد بالسلطة،الحقوق و المزايا التي يتمتع بها المجرم المعلوماتي و التي تمكنه من ارتكاب جريمته ،فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة

1- طارق إبراهيم الدسوقي عطية ، (الأمن المعلوماتي ،النظام القانوني للحماية المعلوماتية) ، دار الجامعة الجديدة للنشر،2009،ص176،177

2- طارق إبراهيم الدسوقي عطية ،مرجع سابق ، ص 177 .

المعلومات محل الجريمة .

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي و إجراء المعاملات .

كما أن السلطة قد تكون شرعية من ممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

خامسا :الباعث

و هو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويضل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية .

ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى في الغالب تكون هي الانتقام من رب العمل أو أحد الزملاء .

حيث يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية اللأخلاقية،وبين الإضرار بمؤسسة أوجهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم،(1).

والانتقام موجود داخل النفس البشرية، فكثير من الأفراد يفضلون تعسفيا أو بغير وجه حق من الشركة أو منظمة حكومية أو حتى مصرف ،وهم يملكون المعلومات والتدريب اللازم والمعرفة الكافية بخفايا هذه الجهة لذا يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر لإصلاحه إلى وقت لا بأس به .

فقد دفع الانتقام بمحاسب شاب إلى أن يتلاعب في برامج الكمبيوتر الخاصة بالشركة التي يعمل بها،حيث برمجها على أن تختفي كل البيانات الخاصة بديون الشركة بعد

1–طارق إبراهيم الدسوقي عطية ،مرجع سابق ،ص177

مضي ستة أشهر من تاريخ تركه للعمل وحدث ما أراد بالفعل فبعد أن ترك العمل ومرت ستة أشهر اختفت البيانات الخاصة بديون الشركة نهائيا عن جهاز الكمبيوتر(1)

وبناءا على ما تقدم يمكن أن ينقسم مجرمي المعلوماتية إلى مجموعة من الطوائف المختلفة ،حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرد الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يأتي:

الطائفة الأولى(pranksters):

وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم ، ومن أمثلة هذه الطائفة صغار مجرمي المعلوماتية .

الطائفة الثانية(hackers):

وتضم الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول ، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

الطائفة الثالثة (malicious hackers):

وهم أشخاص هدفهم إلحاق خسائر بالمجني عليهم ، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف ، ويندرج تحت هذه الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها . (2)

1–هشام محمد فريد رستم –المرجع السابق،ص38

2–محمد أمين الرومي ،جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية ، الإسكندرية ، 2003 ،ص 24

الطائفة الرابعة (personal problem solvers):

وهم الطائفة الأكثر شيوعا من مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه، ويكون الباعث في هذه الجريمة إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية.

الطائفة الخامسة (career criminals):

وهم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الإجرامي تحقيق ربح مادي بطريق غير مشروع ، ويقترب المجرم المعلوماتي من هذه الطائفة في سماته إلى المجرم التقليدي ومن جانب آخر ، أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين

(أو الجناة) تنحدر من : 1-مستخدموا الحاسب بالمنازل.

2-الموظفون الساخطون على منظماتهم.

3-المتسللون ومنهم الهواة أو العابثون بقصد التسلية .

4-المحترفون الذين يتسللون إلى مواقع مختارة بعناية و يعبثون أو يتلفون النظام أو يسرقون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها.

5-العاملون في الجريمة المنظمة . (1)

ويتمتع هؤلاء الجناة بصفات أخرى غير متوفرة في الجناة العاديين نذكر منها:

1-أعمارهم تتراوح عادة بين 18 إلى46 سنة والمتوسط العمري لهم 25 عاما .

2-المعرفة والقدرة الفنية الهائلة.

3-الحرص الشديد وخشية الضبط وافتضاح الأمر.(2)

1- محمد أمين الرومي المرجع السابق،ص25

2- نائلة عادل محمد فريد قورة جريمة الحاسب كصورة الجرائم الاقتصادية المستحدثة ، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين ، مجلة الأمن العام العدد 151-1995، ص58

– **صعوبة التعرف على هوية الجاني،** فهو لا يترك أثرا لجريمته، وإن وجد فقد لا تدل عليه .

– **وجود بعض العقبات في محاكمة الجاني،** حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرما.

– **إتساع شريحة الجناة لتشمل صغار مستخدمي الانترنت،** بسبب توفر الوسائل والبرامج المستخدمة في التخريب لصغار مستخدمي الإنترنت، مما جعل جرائم الإنترنت لا تتطلب خبرة عالية.

– **نقص الوعي بسلبية الإستخدام السيئ للإنترنت** ، مما يجعل البعض ينظر للأعمال التخريبية على الإنترنت –كاختراق المواقع – عمل بطولي . (1)

أما **الطائفة السادسة** "**Extreme Advocates** "

فتدخل في عدادها الجماعات الإرهابية أو المتطرفة ، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار إجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه .

وإن اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحاسبات الآلية في انجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات ، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوروبا باسم "**The Red Brigades** " (الكتيبة الحمراء) بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها. (2)

1–محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقرن، دار الجامعة الجديدة ، الإسكندرية 2007، ص33

2–نائلة عادل محمد فريد قورة ، الحاسب الآلي دراسة نظرية وتطبيقية ، منشورات الحاتي الحقوقية ، 2005 ص59

الطائفة السابعة "**The Criminally Negligent** " والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية ،ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح ، ففي نيوزلندا على سبيل المثال قام إثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة بهذه التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ . (1)

المطلب الثالث: الطبيعة القانونية للجرائم المعلوماتية

إن دراسة الجريمة الإلكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو القسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حدا متناولا كل عناصرها الأساسية والعقوبة المقررة ، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة ، ولقد ساهم التطور التقني للتكنولوجيا المعلوماتية في ظهور الجرائم المعلوماتية ، إلا أن إنتشار هذا النوع من الجريمة بالشكل الذي نراه اليوم ، والتي أصبحت تأخذ أبعادا جديدة وأشكالا مختلفة،إنما بفعل ربط تكنولوجيا الحواسيب بشبكات الاتصال العالميةInternet .

ومحاولة لإبراز طبيعة هذا النمط الجديد من الإجرام ، يتطلب البحث عن صور و أشكال هذا النوع من الجرائم التي تطال الأشخاص في حياتهم وأموالهم وتخل بقيم المجتمع و آدابه العامة ، وتهدد أمن وكيان الدولة.(2)

الفرع الأول :الجرائم المعلوماتية جرائم إعتداء على الأشخاص والأموال

إن الجريمة المعلوماتية بقدر ما هي إعتداء على الأشخاص فهي إعتداء كذلك على الأموال

1–نائلة عادل محمد فريد قورة ، الحاسب الآلي دراسة نظرية وتطبيقية ، المرجع السابق ،ص 63

2– نفس المرجع

وهذا ماسنتطرق له فيمايلي :

أولا: الجرائم المعلوماتية جرائم إعتداء على الأشخاص

تم وصف الجرائم المعلوماتية بأنها جرائم أشخاص بالنظر إلى الدور الذي يلعبه الحاسوب والإنترنت في الجرائم التي يكون الهدف من ارتكابها الاعتداء على الأشخاص عن طريق إفشاء ما يعتبرونه أسرارا ، وهو يشكل تحريضا على الانتحار أحيانا ، أو يتسبب في إحداث ضرر عاطفي قد تمس الحياة العائلية ، أو عن طريق التحريض على الفساد كتحريض القاصرين أو نشر المعلومات عنهم من أجل أنشطة جنسية غير مشروعة ،أو عن طريق القدح والذم والتحقير وبث المعلومات المزيفة و المضللة أو غير المرغوب فيها .

ثانيا : الجرائم المعلوماتية جرائم إعتداء على الأموال

إن وصف الجرائم المعلوماتية بأنها جرائم أموال راجع إلى ضخامة السلوكيات غير المشروعة والناتجة عن استخدام الحواسيب الآلية لتحقيق مكاسب مالية ، كالغش والاحتيال والمضاربات غير المشروعة، وجميع أعمال التخريب والهدم ، كتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب نظام المعالجة الآلية للمعطيات ، وزرع البرامج الخبيثة والضارة (الفيروسات والبكتيريا) (1)

الفرع الثاني : الجرائم المعلوماتية جرائم تفسد الأخلاق وتمس بأمن الدولة

لم تعد مخاطر الجرائم المعلوماتية تهدد الأفراد وأموالهم فحسب، وإنما تطال كذلك الأخلاق والقيم الاجتماعية وتمس بأمن الدولة .

أولا : الجرائم المعلوماتية جرائم مخلة بالقيم والآداب الاجتماعية

لا يختلف إثنان عن الدور السلبي الذي يلعبه الحاسوب الآلي المتصل بالشبكة العنكبوتية

1–محمد زكي أبو عامر وعلي عبد القادر القهوجي ، قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة ، 1993 ، ص9

Intranet بخصوص جرائم الأخلاق ، حيث ساهم ولا زال يساهم بشكل كبير في انتشارها عن طريق الصور الخليعة الإباحية سواء من حيث إنتاجها وعرضها وتوزيعها، ولعل ما سهل هذا الانتشار الكبير عدم تجريم بعض الأفعال الجنسية لدى بعض الدول في إطار ما يسمى بالحرية الشخصية ، وهي ظاهرة عرفتها الكثير من المحاكم .

ثانيا : الجرائم المعلوماتية جرائم تمس أمن الدولة

مع تزايد عدد العارفين والمستعملين للحواسيب الآلية التي أصبحت المخازن الأساسية للمعلومات الحساسة من قبيل المعلومات العسكرية والملفات المتعلقة بالحالة الجنائية وخطط الأمن، لم تعد المؤسسات حتى الحكومية منها بمنأى عن الجناة والمنظمات الإرهابية ،والجهات المخابراتية الأجنبية، وغيرها من الجهات التي تشكل خطرا وتهديدا على أمن الدول سواء الداخلية منها و الخارجية . (1)

1– عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، دار الفكر الجامعي ، الإسكندرية ، 2005،ص 325

المبحث الثاني :أركان الجريمة المعلوماتية

الأصل أن كل جريمة تتكون من ركنين الركن المادي والركن المعنوي و إذ تخلف أحدهما أعتبر الفعل غير مجرم كما تطلب القانون لبعض الجرائم قصدا خاصا ، ويقصد بالركن المادي للجريمة هو توفر مجموعة الانشطة التي يقوم بها الجاني ويستعملها في التنفيذ الفعلي للجريمة أما الركن المعنوي للجريمة فيقصد به العمد أو الخطأ .

والعمد هو اتجاه إرادة الجاني إلى إرتكاب الفعل أو الإمتناع متى كانا مجرمين قانونا وذلك لإحداث نتيجة مباشرة أو نتيجة أخرى مجرمة يتوقعها الجاني ،أما الخطأ فيتوفر بوقوع

النتيجة الإجرامية بسبب خطأ الفاعل سواء بإهماله أو عدم انتباهه أو عدم إحتياطه أو طيشا أو رعونة أو عدم مراعاة للقوانين واللوائح والأنظمة والأوامر وقبل كل هذا لابد من توافر نص قانوني يجرم الفعل أو الامتناع عن الفعل وهذا ما يمثل لنا الركن الشرعي للجريمة فهل هذه الأركان هي نفسها أركان قيام الجريمة المعلوماتية أم أنها جريمة مختلفة الأركان؟

هذا ما سوف نتطرق إليه من خلال المطالب التالية :

المطلب الأول : الركن الشرعي

إن الجريمة المعلوماتية هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان، و هذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه (1)

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لمواجهة الجريمة المعلوماتية خاصة مع ظهور شبكة " الانترنت " التي ساهمت بشكل خطير في تفشي الجريمة و وعيا

بخطورة الوضع، أصدر المجلس الأوروبي سنة 1989 توصية لتشجيع الدول الأعضاء على

1–أحسن بوسقيعة ، الوجيز القانون الجزائي العام ، دار هومه، الجزائر ، ط10،2011 ،ص27

تبني نصوص عقابية خاصة بالجريمة المعلوماتية وقد ترددت العديد من الدول في اختيار التقنية التشريعية المناسبة، فمنها من قام بإدماج نصوص خاصة بالإجرام المعلوماتي في قانون العقوبات التقليدي، ومنها من وضع قانون جنائي مستقل للمعلوماتية يدخل في إطار القانون الجنائي التقني، وعلى المشرع فقط الإلمام بمصطلحات تقنية حتى لا يتم المساس بجريمة تبادل المعارف والحفاظ على الحق في احترام الحياة مما يطرح إشكاليتين أساسيتين هما : إشكالية الموقع وإشكالية المصطلحات (1)

الفرع الأول : إشكالية الموقع

تثور في حالة إدماج النصوص الجديدة في قانون العقوبات التقليدي، يتم إدماجها تحت أي طائفة من الجرائم ؟

هناك عدة فرضيات وآراء : هناك من يقول بإمكانية إدماجها في إطار إحدى الأجزاء التقليدية لقانون العقوبات، و البعض يفضل إدماجها في إطار جرائم الأموال باعتبارها أنه يمكن إسباغ صفة المال على الكيانات المادية والمعنوية للحاسوب، والبعض الآخر يفضل إدماجها في إطار الجزء الخاص بالجرائم ضد الملكية باعتبارها الكيان المادي للحاسوب (عناصر مادية) قابلة للتملك كما أن الكيان المعنوي يدخل في إطار الملكية الفكرية ، و هناك من يرى إضافة جزء آخر خاص بالجرائم المعلوماتية مستقل عن الأجزاء التقليدية بإعتبار أن هذه الجرائم تتعلق بقيمة إقتصادية جديدة لها طابع خاص وهناك رأي ثالث يرى أنه من الأفضل إلحاق كل جريمة معلوماتية بما يقابلها في القانون العقوبات التقليدي مثلا: وضع جريمة التزوير المعلوماتي في باب تزوير المحررات الإعتداء على المعطيات يلحق بالإتلاف...الخ (2)

1- علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الالي ، دار الجامعية للطباعة والنشر، بيروت ، د ط ص24

2-احسن بوسيقيعة، الوجيز في القانون الجزائي العام ،دار هومه، الجزائر،ط10،2011،ص27

الفرع الثاني: إشكالية المصطلحات

نظرا للطابع التقني للجريمة المعلوماتية، فإنها تطرح مشكل المصطلحات التقنية نظرا لغموض مفهومها باعتبارها غريبة عن لغة القانون مثل : Informatique

..Enregistrement Captation...الخ و الإبقاء على بعث المصطلحات الضرورية كالنظام ،المعطيات..الخ.

أما بالنسبة لتعريف المصطلحات التقنية فموقف التشريعات يختلف إزاءها ،فالتشريعات الأنجلوساكسونية تعتمد طريقة إعطاء تعريفات في صلب القانون .

أما الطريقة الفرنسية توكل مهمة تحديد معاني المصطلحات التقنية للقضاء وهي الطريقة الأفضل نظرا لسرعة تطور تقنيات الإعلام الآلي وعدم إمكانية مواكبة القانون الجنائي لهذا التطورهذا بالنسبة للإشكاليات التي يطرحها الركن الشرعي للجريمة المعلوماتية بالنسبة لبحثنا هذا وفي غياب الأساس التشريعي في القانون الجزائري حاليا، وفي انتظار التعديل المقبل لقانون العقوبات الجزائري والذي سيتضمن محورا خاصا بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، ستكون التجربة الفرنسية هي محور دراستنا، خاصة أن مشروع تعديل قانون العقوبات الجزائري قد إعتمد على التشريع الفرنسي فيما يتعلق بالجرائم المعلوماتية. (1)

وقد بدأت المحاولة في فرنسا سنة 1985 حين تقدم وزير العدل وقتئذ بمشروع قانون العقوبات جديد أضاف إلى الكتاب الثالث منه باب رابعا بعنوان" جرائم المعلوماتية" مكونا من ثماني مواد 1/307إلى8/307 والتي كانت تجرم التقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي عمدا واستخدام أو إنتاج برنامج أو معطيات أو أي عنصر من عناصر بدون موافقة من لهم الحق عليه، وتخريب أو تعييب كل أو جزء من نظام المعالجة الآلية للمعطيات، وكذلك عرقلة أدائه لوظيفته والحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق الاستخدام غير المشروع لنظام المعالجة الآلية للمعطيات، ولكن

-د/ 1 -علي عبد القادر القهوجي،المرجع السابق ، ص24

هذا المشروع ظل حبيس الأدراج، ولم ير النور.

وفي05 أغسطس سنة 1986 تقدم إلى الجمعية الوطنية الفرنسية النائب (Codfrain Jacque) مع بعض النواب من أعضاء حزب التجمع من أجل الجمهورية باقتراح مشروع قانون في"الغش المعلوماتي "

وكان هذا الاقتراح مجرد تعديل وتطويع بعض الجرائم التقليدية مثل السرقة والنصب وخيانة الأمانة والإخفاء والتخريب والإتلاف والتزوير واستعمال المحررات المزورة .

ولكن عند نظر البرلمان الفرنسي لهذا الاقتراح، دارت حوله مناقشات طويلة ومعمقة، وأدخلت عليه تعديلات جوهرية وتم إقراره في شكل جديد يختلف عن شكله الأول الذي قدم به، بحيث اقترب من الاقتراح الذي سبق الإشارة إليه في مشروع قانون العقوبات لسنة 1985، وكان ذلك في 1987/12/22وأصبح قانونا منذ1988/01/05 وحمل رقم 19/88بتاريخ1988/01/05 بشان الغش المعلوماتي، وأدمج هذا القانون في قانون العقوبات الفرنسي، وأصبح يشكل بابا جديدا هو الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات حيث يعالج الباب الأول الجنايات ،و يعالج الباب الثاني الجنح ضد الأشخاص ،و يعالج الباب الثالث الجرائم المعلوماتية (1) ويحتوي هذا الباب على المواد من 2/462 إلى 9/462 ويجرم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية المعطيات أو في جزء منه، وشدد عقوبة تلك الجريمة في حالة محو أو تعديل المعطيات الموجودة فيه أو طرق معالجتها أو نقلها سواء تم ذلك بطريقة مباشرة أو غير مباشرة، ويجرم كل من عرقل أو أفسد عمدا أو بدون مراعاة لحقوق الغير أداء النظام لوظيفته. كما يجرم تزوير المستندات المعالجة آليا أيا كان شكلها،وكذلك استعمال تلك المستندات و يجرم أخيرا الشروع في ارتكاب الجرائم السابقة، وكذلك الاتفاق الجنائي على ارتكابها، ويلاحظ على النصوص السابقة أنها تجرم الاعتداء على نظام المعالجة الآلية للمعطيات ماعدا جريمة تزوير المستندات المعالجة آليا واستعمالها،فإنها تحمي نتاج هذا

1–نفس المرجع ، ص24

النظام، أي المعطيات المعالجة وهذا يعني أن المشرع الفرنسي جمع في صعيد واحد حماية النظام وحماية نتاج هذا النظام، ولذلك فقد فصل بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات وبين جريمتي تزوير المستندات المعالجة آليا واستعمالها. ففي الكتاب الثالث من هذا القانون الجنايات والجنح ضد الأموال ، وفي القسم الثاني من هذا الكتاب وفي الاعتداءات الأخرى على الأموال يعالج الباب الأول منه الإخفاء والجرائم الأخرى المشابهة أو القريبة منه . ويخصص الباب الثاني الإتلاف والتخريب والتعييب، أما الباب الثالث، فقد كرسه المشرع للاعتداءات على أنظمة المعالجة الآلية للمعطيات .

أما جريمتا تزوير المستندات المعالجة أليا واستعمالها فقد اختفتا من الباب الثالث المذكور لأن المشرع رأى أن المصلحة المحمية فيهما هي الثقة العامة، وليس نظام المعالجة الآلية للمعطيات، وأضافهما إلى جريمة التزوير العادية بعد تطويع نصوصها بما يتلائم وتلك المستندات حيث نصت المادة 1/441 قانون العقوبات الفرنسي الجديد في باب التزوير على تجريم كل تغيير للحقيقة مكتوب في محرر أو أي دعامة أخرى تحتوي على الأفكار وسوف نعالج الجرائم السابقة كل حدى، فالمشرع الفرنسي من أولى المشرعين الذين بادروا بتجريم أفعال الاعتداء على أنظمة المعالجة الآلية للمعطيات. أما في ما يخص المشرع الجزائري فقد أورد قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيات وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر 7 بمقتضى القانون 04-15 المؤرخ في2004/11/10 ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23/06 المؤرخ في 2006/12/20 والذي مس المادة 303 وإقراره بالمادة 303 مكرر إلى 303 مكرر 03 ، وهذا تصديا للإستخدام السيئ لوسائل التكنولوجيا الحديثة . (1)

1-د/ علي عبد القادر القهوجي،المرجع السابق ، ص24

المطلب الثاني الركن المادي

جرائم المعلوماتية تتخذ عدة أشكال تتعدد بتنوع صور الاعتداء على الإعلام الآلي والتي يمكن إجمالها في صورتين أساسيتين: الاعتداءات على أنظمة المعالجة الآلية للمعطيات و الاعتداءات على منتجات الإعلام الآلي :

الفرع الأول: الاعتداءات على نظام المعالجة الآلية للمعطيات

هذه الصورة الأولى للركن المادي للجريمة المعلوماتية تتضمن الأفعال الآتية:

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

ثانيا: الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات .

ثالثا: الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام، هذه الاعتداءات تتطلب وجود نظام للمعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام (1) وسنتعرض إليها بالتفصيل فيما يلي :

أولا: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات نصت المادة 394 مكرر من قانون العقوبات الجزائري على انه "يعقب بالحبس من ثلاث أشهر إلى سنة، وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين ، والغرامة من 50.000دج إلى 150.000دج (2)

1-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه الجزائر، ط2، 2007 ، ص10

2- مولود ديدان، قانون العقوبات،قانون رقم 01/09المؤرخ في 25 فبراير2009، د ط، ص 120.

كما تنص المادة 1/323من قانون العقوبات الفرنسي على أن فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه يعاقب بالحبس لمدة سنة وبغرامة 100.000 أورو، فإذا نتج عن الدخول أو البقاء سواء محو أو تغيير في المعطيات الموجودة في النظام أم تعيب تشغيل النظام،فان العقوبة تصبح الحبس لمدة سنتين، والغرامة التي تصل200.000 أورو الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع.

بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، وهو يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام.

فعل الدخول:لا يقصد بالدخول هنا الدخول بالمعنى المادي،أي الدخول إلى مكان أو منزل أو حديقة،إنما يجب أن ينظر إليه كظاهرة معنوية،تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان،أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.

ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام،ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر أكثر التقنيات استخداما لارتكاب جريمة الدخول غير المشروع للنظام (1)

إستخدام البرامج الظاهرة المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة إذ

على الرغم من ضرورة تزويد الحاسبات ببعض أنظمة الحماية الفنية للحيلولة دون الاتصال غير المشروع بالبرامج والبيانات المخزنة،إلا أن إدارة وتشغيل البيانات والحاسبات بطريقة آمنة خاضعة للتحكم والسيطرة تقتضي وجود نوع من البرامج يمكن إستخدامه تخطي حواجز الحماية الفنية لمنظومات الحاسب في الحالات الطارئة وحالات إختلال وظائف الحاسب

1– د/ علي عبد القادر القهوجي، المرجع السابق، ص25

أو توقفه عن العمل ، وثمة نوع من برامج الاستخدامات المتاحة مخصص لهذا الغرض، أشهره البرنامج المسمى super zap المستخدم في معظم مراكز حاسبات M.B.I إذا يسمح استخدام هذا البرنامج بالوصول إلى سائر أجزاء نظام معلومات الحاسب على نحو يشابه استخدام المفتاح العمومي في حالة الطوارئ لفتح أقفال الأبواب والمنافذ المغلقة، وتمثل البرامج المخصصة لهذا الغرض إذا ما وقعت في أيدي غير المصرح لهم باستخدامها أداة بالغة الفعالية شديدة الخطر على أمن البرامج والبيانات المخزنة،إذ تسمح لمستخدمها بالتغلغل في منظومات الحاسب حتى لو كان محميا بشكل دقيق،وتمكنه من أداء أية مهام غير مصرح بها Dépiombage وتقع هذه الجريمة من كل إنسان أيا كانت صفته، إذ أنها ليست من جرائم ذوي الصفة إنما ترتكب من أي شخص كان يعمل في مجال الأنظمة أم لا يعمل،وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ليس ممن يكون لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فتتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو الاتفاق،أو مخالفا لإرادة من له الحق في السيطرة على النظام،كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة،أو السرية المتعلقة بالمعلومات الذاتية أو الاسمية أو سر المهنة، أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية أو أي معلومات يجمعها الإنسان في نظام ولا يترك الإطلاع عليها لأي إنسان (1)

ويكون الدخول غير مشروع إذا كان من له حق سيطرة على النظام قد وضع بعض القيود للدخول إليه، ولم يحترم الجاني تلك القيود أو إذا كان يتطلب ضرورة دفع مبلغ من النقود، وتم الدخول دون دفع ذلك المبلغ، ويرتكب الجريمة من يعمل على الحاسب ولكن بنظام معين، فيدخل في نظام آخر.

1–طعباش أمين،المرجع السابق،ص 106

كما تقع الجريمة سواء تم الدخول إلى النظام كله أم إلى جزء منه فقط، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام، أو على عنصر واحد منه، أو منطقة ضيقة منه، كان هذا بشرط أن يكون العنصر الذي تم الدخول إليه فقط يدخل في برنامج متكامل قابل للتشغيل.

وفي النهاية فإن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات، بل إن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام أبواب المصيدة DOORS-TRAP .

من الأمور الشائعة التي يقوم بها واضعي البرامج أن يتركوا فواصل في البرنامج أثناء إعداده تسمى"أبواب المصيدة" تستخدم في إضافة ما يحلو لهم من أوجه التلاعب.

ويتم ذلك أثناء قيامهم بالمعالجة النهائية على اعتبار أن هذا شيء عادي، ويمكن لمهندسي الحاسب أن يقوموا باكتشاف هذه الفواصل من الأجزاء الداخلية للصيانة. (1)

صناديق القمامة POUBELLE تلقى عادة في سلة المهملات أوراق الكربون أو أوراق عادية تحتوي على بيانات أو حتى أشرطة مغناطيسية من قبل العاملين في أقسام الخلية

الإلكترونية ويمكن استخدام هذه الملحقات أول بأول .

طريقة:"raccourci" تتمثل هذه التقنية في استغلال نقاط الضعف الخاصة بالنظام الداخلي للرقابة .

طريقة القناع:" les"déguisements وذلك بأن يقوم القرصان بإقناع الحاسوب بأنه شخص مرخص له بالدخول طريقة "asynchrone acte " هذه التقنية تتمثل في استعمال نقاط الضعف الموجودة على مستوى نظام الاستغلال.

1- طعباش أمين، المرجع السابق، ص106

وجريمة دخول غير مصرح إلى نظام المعالجة الآتية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة، يكفي الوصول إلى المعلومات المخزنة بداخل النظام، فبمجرد الوصول إليها تقوم الجريمة.(1) يرتكب فعل الدخول بأية طريقة أو وسيلة كانت لأن المشرع الجزائري لم يحددها.(2) ويستوي أن يتم الدخول بطريق مباشر يستطيع الجاني للوصول إلى المعلومات المخزنة لدى الأنظمة المعالجة الآلية باستخدام الشاشة النظام والاطلاع بالقراءة على ما هو مكتوب عليه وباستخدام آلة الطباعة مرفقة بجهاز الحاسب الآلي استخراج قائمة البرامج الموجودة داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالالتقاط المعلوماتي بعد التقاط المعلومات المتواجدة في الحاسب الآلي والنهاية الطرفية والتقاط الإشعاعات الإلكترومغناطيسية المنبعثة من الجهاز المعلوماتي **فعل البقاء:** قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام ، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام، وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي، يكون البقاء جريمة في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والاطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه، أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لايكون فيه للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له الحق في سيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي للجرائم وإذا كانت تلك الجريمة على هذه

1–أمال قارة، المرجع السابق، ص101

2–نائلة عادل محمد فريد قورة، المرجع السابق ص 63

الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا وبصورة غير مباشرة حماية للمعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة، وذلك بالنسبة للموظف أو العميل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له حق السيطرة على النظام، ويقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج .(1)

كما يمكن أن تطبق على الاستخدام غير المشروع للبطاقات الممغنطة إما بسرقتها أو التزوير ثم استخدامها أو حتى إذا استخدمها صاحبها في سحب مبالغ دون أن يكون لديه رصيد كاف، أو عند عدم وجود الرصيد.

تكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب البطاقة يعلم مقدما بأن ليس له رصيدا كاف، ويمكن أيضا تطبيقها على التنصت على المحادثات الهاتفية طالما ن أن أرقام الهواتف معالجة آليا في نظام خاص بها هذه الجريمة تعد جريمة سلوك مجرد، أي أنها تقع وتكتمل بمجرد انتهاء سلوك المكون لها وهو دخول أو البقاء دون أن يتطلب المشرع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية.وإذا كان الاتجاه الغالب في فقه يعتبر جريمة الدخول أو البقاء ذات سلوك مجرد، إلا أن الفقه لم يتفق على كون هذه الجريمة وقتية أو مستمرة أو متتابعة الأفعال، وقد ذهب رأي إلى اعتبار كل من جريمتي الدخول والبقاء جرائم مستمرة، بينما ذهب رأي آخر إلى اعتبار جريمة الدخول جريمة متتابعة الأفعال، بينما جريمة البقاء مستمرة . وذهب رأي ثالث إلى أن جريمة الدخول وقتية ذات أثر ممتد وجريمة البقاء جريمة مستمرة، ولكن تثور في هذا الفرض مشكلة : متى تنتهي جريمة الدخول متى تبدأ جريمة البقاء ؟ ذهب رأي في الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، وإن كان الدخول –في نظر هذا الرأي– يفترض في ضرورة البقاء فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل، وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام

1–علي عبد القادر القهوجي،مرجع سابق،ص133

وتنتهي بانتهاء حالة البقاء . ويؤخذ عن هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة، لهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه

المتدخل أن بقاءه داخل النظام غير مشروع، وأخذ على هذا الرأي أيضا صعوبة إثبات علم المتدخل، وذهب رأي ثالث إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع،(1)

فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام وهذا الرأي وإن أمكن توفيره فنيا فإنه لن يكون متاحا إلا بالنسبة للشركات أو المؤسسات الكبيرة فقط .

والرأي الأصوب في مثل هذه الظروف هو الذي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام،أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد،لأن الغرض يتعلق بدخول غير مشروع،أي مع علم الجاني أن ليس له الحق في الدخول،فإذا دخل وظل ساكنا،تظل الجريمة جريمة دخول إلى النظام،أما إذا بدأ في التجول،فان جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله فيه غير مشروع أو أن مبدأ استمراره فيه غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام.ويكفي لتحقيق تلك الجريمة البقاء داخل النظام كله أوفى جزء منه بذات المعنى السابق ويكفي البقاء داخل النظام لتوافر الركن المادي لتلك الجريمة،فلا يشترط أن يضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر،وتظهر أهمية التفرقة بين أنواع الجرائم السابقة والتي تتعلق أساسا بالتقادم والاختصاص المكاني والعفو .

إلا أن تلك الأهمية تبدو ضئيلة لأن الفقه يتفق في مجموعة على أن جريمة البقاء جريمة مستمرة، لأن الفترة الزمنية التي تستمر فيها جريمة الدخول قصيرة نسبيا بحيث يمكن اعتبارها مستمرة أو وقتية ذات أثر ممتد.(2)

1–أمال قارة،مرجع سابق،ص114

2–د/جميل عبد الباقي الصغير،جرائم التكنولوجيا الحديثة، دار النهضة العربية،ص59

أما الاعتداء العمدي علي سير نظام المعالجة الآلية للمعطيات تعاقب المادة 2/323من قانون العقوبات الفرنسي "كل من عطل أو افسد نشاط أو وظائف نظام المعالجة الآلية للمعطيات بالحبس حتى ثلاثة سنوات وبالغرامة حتى 300000أورو"تتعلق هذه الجريمة بتجريم كل فعل من شأنه أن يؤدي إلى توقف تشغيل نظام المعالجة الآلية للمعطيات وان كان المشرع لم ينص صراحة على ضرورة توافر الركن المعنوي في هذه الجريمة إلا أنه يستفاد من الأعمال التحضيرية ضرورة توافر هذا الركن،وان يتخذ صورة القصد الجرمي،ولذلك فان هذه الجريمة يلزم لتحققها توافر الركنين المادي والمعنوي، يتمثل السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظر منه القيام به أو في فعل إفساد نشاط أو وظائف هذا النظام،ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة،بل يكفي أن يؤثر على احد هذه العناصر فقط سوا المادية جهاز الحاسب الآلي نفسه،شبكات الاتصال،أجهزة النقل..... الخ أما المعنوية مثل البرامج والمعطيات،وتتمثل صور الاعتداء العمدي على فيما يلي:

التعطيل:(العرقلة) يفترض وجود عمل إيجابي،ولم يشترط المشرع أن يتم التعطيل بوسيلة معينة،فقد تكون تلك الوسيلة مادية أو معنوية،وتكون وسيلة التعطيل مادية سواء اقترنت بعنف أم لا أذا وقعت على الأجهزة المادية للنظام(1)

أو منعت من الوصول إليها مثل تخزينها أو بكسرها أو تحطيم أسطوانة أو قطع شبكات الاتصال أو سكب كوب شاي أو أي مادة أخرى أو منع وصول العاملين على أنظمة إلى المكان الذي توجد فيه الأنظمة وتكون وسيلة التعطيل معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات وذلك بإتباع التقنيات التالية:

إدخال برنامج فيروسي–.استخدام قنابل منطقية–.استخدام بطاقات الوقف هي بطاقات تسمح بوقف تنفيذ البرنامج بالمرور بمختلف الفيروسات المعلوماتية والقنابل المنطقية–إشباع إمكانية الدخول–جعل النظام يتباطأ في أدائه لوظائفه.

1–د/جميل عبد الباقي،مرجع سابق،ص60

تقنيات التعييب والإفساد:التلاعب في المدخلات:إدخال بيانات مختلفة أو محرفة في نظام معلومات الحاسب أو تغيير مسار البيانات الصحيحة المدخلة أو الجمع بين الأمرين معا،أمور يسهل القيام بها في أولى مراحل تشغيل نظام معلومات الحاسب وهي مرحلة إدخال البيانات لمعالجتها،فحيث تجهز البيانات و تحول في هذه المرحلة إلى لغة مقروءة من قبل الآلة المستخدمة في المعالجة،ويكون سهلا تغذية الحاسب ببيانات مغلوطة أو زائفة أو منع إدخال بيانات وثائق معينة،وأكثر من نصف الجرائم المعلوماتية يقع باستخدام هذه الطريقة للتلاعب في البرامج ومن أبرز صوره:

إدخال تعديلات عير مرخص بها غلى البرامج المستخدمة:تمر معظم البرامج بعد إعدادها واختيارها بعدد من التعديلات الثانوية أثناء فترة تنفيذها لتصحيح ما قد تتضمنه من أخطاء لم يتم من قبل اكتشافها وفي بعض الأحيان قد يقتضي الأمر تطويرها ومن المتاح في هاتين المرحلتين،إدخال تغيرات غير مرخص بها على البرامج تسمح بارتكاب جرائم الاعتداء على المال وإخفائها(1)

ومن قبيل هذه التغيرات ما يعرف باسم حيلة أو خدعة التقريب البرامج الخبيثة ظهرت البرامج الخبيثة إلى الوجود بعد الشروع في استخدام الحاسبات بفترة ليست كبيرة وهي تتخذ صورا عدة وتستهدف أغراضا شتى فمنها ما يعد بهدف الاحتيال والاستيلاء بواسطة الحاسبات على المال،ومنها ما يعد بهدف التمييز والتبرير ومن أخطرها برنامج حصان طروادة و القنابل المنطقية وبرامج الدودة والفيروسات ويستوي أن يكون التعطيل دائما أو مؤقتا، فقد يؤدي إلى توقف دائم للنظام كما في حالة إدخال فيروس وقد يكون التوقف مؤقتا أو منقطعا على فترات منتظمة،كما إذا تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شل النظام عند البدء في تشغيله مثلا،أو عند استخدام أحد برامج التطبيق كما يستوي أن يكون التوقيف بالنسبة لجميع مستعملي النظام أم بالنسب لأحدهم فقط، ولكن يشترط في التعطيل أن يكون إيجابيا أي أن يصدر عن الجاني نشاطا إيجابيا يؤدي إلى توقيف النظام أو الامتناع عن التدخل بقصد تعطيل النظام .

1–د/جميل عبد الباقي،مرجع سابق،ص60

برنامج حصان طروادة:هو برنامج خادع يخفي ظاهره عرضا غير مشروع يضمره إذ يظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدمه بينما يكون موجودا بطريقة خفية داخله بعض الأوامر أو التعليمات التي تؤدي عند تشغيله مهاما ضارة غير متوقعة تمثل أغراضه الحقيقة المضمرة، وهكذا قد يبدو البرنامج كما لو كان معدا لتنظيم البيانات بالملفات أو تكثيفها،بينما الهدف الحقيقي من وراء تشغيله قد يكون محو هذه البيانات من ذاكرة الحاسب أو التهديد بذلك.أو الاستيلاء على المال بتحريف البيانات المدخلة أو المخزونة.

بدأ هذا البرنامج في الظهور،حسب ما يقرر البعض في الولايات المتحدة الأمريكية في أواخر عقد السبعينات نتيجة لانتشار استخدام اللوحات الالكترونية للبيانات التي تنتج تخفيف أو زيادة تحميل البرامج،هذا النوع من البرامج يعرف باسم ZAXOON يبدو عند بداية تشغيله،كأحد ألعاب التسلية ثم يقوم بعد ذلك بمحو أقراص النظام.

ومن نفس النوع أيضا برنامج يسمى FILER يبدو في ظاهرة كما لو ينظم بيانات الملفات مع أنه يقوم في الحقيقة بمحوها.ومن هذا النوع تعليمات يجري رسمها خفية في البرامج المستخدمة لإصدار شيكات لمستحقيها بصفة دورية(كأرباب المعاشات)مثلا وإرسالها إليهم عن طريق البريد مهمتها تحريف الإخطار الذي يجري إدخاله إلى الحاسب بوفاة مستحق الشيك،الذي يترتب عليه وقف إصدار الشيكات بتغيير عنوانه مؤقتا لمدة ثلاثة شهور متتالية،وهكذا يصدر الحاسب خلال هذه الشهور شيكات ترسل إلى العنوان المؤقت، وعند انقضاء الشهور الثلاثة تعيد التعليمات المخفية في البرنامج البيانات لتجري بطريقتها الأصلية لتكون إخطار بوفاة مستحق الشيك وهو ما يجعل اكتشاف التلاعب أمر في غاية الصعوبة(1)

1-امير فرج يوسف،الجرائم المعلوماتية على شبكة الانترنيت،دار المطبوعات الجامعية،الاسكندرية2009،ص88

وعادة ما توجد برامج أحصنة طروادة في برامج العمال،كبرامج معالجة النصوص، وبرامج إدارة قواعد البيانات.وغالبا ما تكون مختفية في منتصف البرامج أو في مكان غير مستعمل منه والبرنامج الذي يتضمنها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر الأوامر غير المتوقعة،وقد تظهر هذه الأوامر وتنفذ مباشرة عند تشغيله،وهي بخلاف ما يسمى بفيروسات الحاسب.لا تنسخ بنفسها واكتشافها بالغ الصعوبة وكذلك أيضا محاولة اقتفاء أثر معدها القنابل المنطقية أو الموقوتة وهي برامج محمية بحيث تبقى ساكنة وغير فعالة،وغير مكتشفة لمدة قد تصل إلى أشهر أو حتى أعوام وهذه المدة يحددها عادة مؤشر زمني يحتويه البرنامج كتاريخ معين بحيث ينشط البرنامج عند حلوله،ويؤدي مهامه الهدامة وقد لا يرتبط مؤشر التفجير بالزمن،وإنما بشروط منطقية معينة داخل نظام التشغيل أو داخل برنامج أو ملف وذلك حسبما يحدده مبرمج القنبلة،يمكن أن يكون مؤشر التفجير إدخال أو عدم إدخال بيان ما إلى نظام معلومات الحاسب أو مجرد الاتصال بنظام الحاسب لإعلام مستخدميه بوجود قنبلة منطقية فيه،وتحقق القنابل المنطقية لمعدها أغراضا متعددة، أبرزها تأجيل التفجير لجعل اقتفاء أثر معدي القنابل وتعقبهم أكثر صعوبة أو متعذرا وتوقيف التفجير يرتبط بأحداث معينة كالوقت الكافي لتسرب القنبلة إلى النسخ الاحتياطي للبرامج التي تقوم الجهات المجني عليها عادة بإعدادها برامج الدودة (1)

وهي برامج تشغيل تنقل من حاسب إلى آخر مغطية شبكة بأكملها وقد تنتقل من شبكة إلى أخرى عبر الوصلات التي تربط بينها وأثناء عملية انتقالها تتكاثر كالبكتيريا بإنتاج نسخ منها ومن أهدافها شغل أكبر مجال ممكن من سعة الشبكة وبالتالي: تقليل أو حفظ كفاءتها وقد تتعدى أهدافها ذلك لتبدأ بعد التكاثر والانتشار في التخريب الفعلي للملفات والبرامج ونظم التشغيل الأخيرة ذاع صيت برنامج الدودة الذي أطلق عليه اسم انترنيت نسبة إلى الشبكة التي أصابها وبروتوكولات الاتصال،وفي الآونة وأسماه آخرون باسم دودة موريس،وقد ادخل هذا البرنامج إلى الشبكات الانترنيت مساء 1988/11/03 من خلال إحدى وسائل التدقيق في حزمة البرامج الخاصة بالبريد الإلكتروني حيث دخل عن طريق باب خفي بكلمة سر بسيطة ليصل إلى النظم المرتبطة .

1-أمال قارة،المرجع السابق،ص117

الفيروس المعلوماتي:

أ-تعريفه:يمكن أن نعرف الفيروس في كلمات قليلة بأنه برنامج مكتوب بإحدى لغات البرمجة بطريقة خاصة والقدرة عل التحكم في البرامج الأخرى ويقدر على تكرار نسخ نفسه.(1)

ب-خصائصه:نستطيع أن نعرف برنامج الفيروس بصورة مكملة للتعريف السابق بأن الفيروس هو البرنامج الذي يستطيع أن يلحق نسخ تنفيذية من نفسه في برامج أخرى تصبح بدورها هي أيضا قادرة على إلحاق نسخ من الفيروس وهكذا نستخلص مما سبق أنه ليسمى برنامج ما بأنه برنامج فيروس يجب أن تتوافر فيه عدة شروط هي-:القدرة على نسخ نفسه في البرنامج الذي يصيبه بالعدوى-القدرة على التحكم في البرنامج المصاب والتعديل فيه-القدرة على تمييز البرامج التي تم إصابتها بالعدوى .

والامتناع هنا ليس امتناعا مجردا،وإنما هو امتناع مختلط بنشاط إيجابي يتمثل في تعسف الجاني ورفضه القيام بما يفرضه عليه القانون أو الاتفاق من واجب تشغيل النظام.الإفساد:Fausser يقصد بالإفساد كل فعل وإن كان لا يؤدي إلى التعطيل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

والإفساد من هذه الزاوية يقترب من التعييب الذي سبق الإشارة إليه عند التعرض للظرف المشدد لجريمة الدخول والبقاء غير المشروع،ولعل الفارق بينهما يكمن في إن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة للجريمة التي نحن بصدد دراستها.وتقنيات التعييب والإفساد متعددة منها-:استخدام القنبلة المعلوماتية التي يدخل عن طريقها معلومات تتكاثر داخل النظام تجعله غير صالح للاستعمال .(2)

1-خالد أبو الفتوح: فيروس الكمبيوتر، مقال منشور في مجلة قضايا الدولة،ص6

2- خالد أبو الفتوح ، نفس المرجع

أما إستخدام البرنامج الذي يحمل فيروس يطلق عليه اسم "حصان الطراودة" والذي يقوم بتغيير غير محسوس في لبرامج أو المعطيات ،وغير ذلك من الفيروسات التي تجعل مخرجات النظام غير تلك التي كان يجب عليه أن يخرجها،بل إن الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادية في النظام ،هذا ويلاحظ أنه و إن كان من الناحية النظرية يمكن التمييز بين فعل التعطيل أو التوقيف وفعل الإفساد أو التعييب، إلا أنه من الناحية العملية كثيرا ما يتطابقان، ويكفي هنا مجرد النظر إلى الوسائل التي يتحقق بها كل فعل منهما، كما يلاحظ أن فعل التعطيل أو الإفساد بالمعنى السابق يشترك في جانب منه مع جريمة الإتلاف أو التخريب العادية ،ولما كان نص هذه الجريمة عاما بينما نص المادة 2/323 نصا، فإن تجاوز التنازع الظاهري بين هذين النصيين يكون على أساس تغليب النص الخاص العام لأن نص المادة2/323 يتعلق بنظام للمعالجة الآلية للمعطيات فقط وليس مطلق الأشياء التي يمكن أن تقع عليها جريمة الإتلاف والتخريب العادية (1)

-ثالثا:الاعتداءات العمدية على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات تعاقب المادة323 من قانون العقوبات الفرنسي"كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات،أو محا أو عدل بطريق الغش تلك المعطيات بعقوبة الحبس حتى ثلاث سنوات، وبعقوبة الغرامة حتى300000أورو النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات(2)

يتجسد في إحدى الصور الثلاث التالية: الإدخال (L intrusion) ، المحو (L effacement) ، التعديل (Modification) لا تشترط إجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي،وأفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة،أو محو أو تعديل معطيات موجودة من قبل،هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد وهو المعطيات أو التي تمت معالجتها آليا والتي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات ،

1-أمير فرج يوسف،المرجع السابق:ص88-89

2-خالد أبو الفتوح،مقال منشور في مجلة قضايا الدولة،ص6.

و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة،كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام،أي التي يحتويها النظام وتشكل جزاءا منه، لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت،ولم تتخذ حيالها إجراءات المعالجة الآلية أما تلك التي في طريقها إلى المعالجة حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية،ويكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.(1)

المادة:4/462 قانون 1988 كل من أدخل المعطيات بغير قصد وعن تجاهل حقوق الغير بطريقة مباشرة أو غير مباشرة،أو أوحى أو عدل هذه المعطيات في نظام المعالجة الآلية الموجودة فيه،وطرق المعالجة أو الاتصال يعاقب بالحبس من 3أشهر إلى 3سنوات وبغرامة من2000إلى5000 أورو أو بإحدى هاتين العقوبتين.

تجدر الإشارة إلى أن الحماية الجنائية للمعطيات طالما أنها تدخل في نظام المعالجة الآلية للمعطيات أي طالما كان يحتويها ذلك النظام وكانت تكون وحدة واحدة مع عناصره يترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها،وحتى ولو لفترة قصيرة،كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام .

والحماية الجنائية تقتصر على تلك التي توجد داخل النظام أو تلك التي في طريقها إلى الدخول إليه،أو تلك التي دخلت بعد خروجها، ولا يشترط أن تقع أفعال إدخال ومحو وتعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء عن بعد أم بواسطة شخص ثالث، ونحدد فيما يلي المقصود بكل من الأفعال الثلاثة السابقة .(2)

1–عبد الفتاح بيومي حجازي التجارة الالكترونية وحمايتها القانونية،دار الفكر الجامعي الاسكندرية2004،ص365،

2–نفس المرجع ، ص366

الإدخال: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية،أم كان يوجد عليها معطيات من قبل ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا(التاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له .

وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير ،كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب(فيروس–حصان طراودة–قناة معلوماتية زمنية)يضيف معطيات جديدة. المحو يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام،أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة (1)

التعديل:يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى،ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزيا أم بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة effacement d gomme ، أو برامج الفيروسات بصفة عامة،وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينها، كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل بالمعنى السابق.

الفرع الثاني–الصورة الثانية–الاعتداءات على منتجات الإعلام الآلي هذه الصورة الثانية للركن المادي للجريمة المعلوماتية تتمثل في المساس بمنتجات الإعلام الآلي ويتجسد هذا المساس في فعل التزوير المعلوماتي،هذه الصورة من صور الجرائم المعلوماتية لا تشترط

1–عبد الفتاح بيومي حجازي التجارة الالكترونية وحمايتها القانونية،دار الفكر الجامعي الاسكندرية2004،ص365

بدلا من ذلك أن تشدد عقوبة جريمة الاعتداء العمدي على المعطيات إذا نتج عن الإدخال أو التعديل أو المحو تغيير الحقيقة لكن مجلس الشيوخ اقترح تعديلا يتمثل في اعتبار تزوير المستندات المعالجة آليا جريمة مستقلة عن التزوير في المحررات وكذلك جريمة استعمال تلك المستندات المزورة،وتمت الموافقة في البرلمان بمجلسه على هذا التعديل وتضمن القانون رقم 19/88 الصادر في 1988/01/05 بشأن غش المعلوماتية المادتين 5/462-6/462 حيث نصت الأولى على تجريم تزوير المستندات المعالجة آليا،بينما جرمت المادة الثانية استعمال تلك المحررات.ولكن بصدور قانون العقوبات الفرنسي الجديد في 1992/12/16 ألغيت المادتين السابقتين،حيث قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا واستعمالها والاكتفاء بإضافته إلى جريمة التزوير العادية،أي العودة إلى الاقتراح القديم الذي تقدم به النائبCodfrain وقد تم تعديل المادة 441/1 من الكتاب الرابع من قانون العقوبات الفرنسي لكي تفي بهذا الغرض.وقد نصت بعد تعديلها على أنه يعد تزويرا "كل تغيير بطريق الغش للحقيقة...في مكتوب أو في أي دعامة أخرى تحتوي التعبير عن الفكر"وهكذا تطورت جريمة التزوير في المعلوماتية من مجرد جريمة تزوير المستندات المعالجة آليا واستعمالها إلى جريمة تزوير المستندات المعلوماتية واستعمالها وسوف نتكلم عن الركن المادي لهاتين الجريمتين بشيء من التفصيل قبل وبعد التعديل. (1)

قبل التعديل: تزوير المستندات المعالجة آليا نصت المادة5/462 قانون العقوبات الفرنسي قبل إلغائها على معاقبة أي شخص يرتكب عمدا تغييرا للحقيقة في المستندات المعالجة آليا أيا كان شكلها متى ترتب على ذلك ضرر للغير.يتكون الركن المادي من عدة عناصر هي:محل يرد عليه فعل تغيير الحقيقة وهو المستند المعالج آليا-فعل تغيير الحقيقة -الضرر المستند آليا،ويقصد بالمستند في الاصطلاح القانوني كل دعامة مادية(مكتوب أو أي شيء) تصلح لأن تدون عليها المعلومات أو الآراء والتي هي غير مادية، أو هي الشيء المادي

1-د/خالد أبو الفتوح:مرجع سابق،ص9

الذي يكمن أن يدون عليه شيء معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز(قرص أو شريط ممغنط أو خلافه)يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة،وتم تصنيفه أم أنه مازال بداخلها انتظارا لاستخراجه أو تعديله،ويقصد بالمستند المعالج آليا كل دعامة مادية مهيأ لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية المعلوماتية،أي من خلال نظام المعالجة الآلية للمعلومات، وبعبارة أخرى يقصد بالمستند المعالج آليا الدعامة المادية التي تم تحويل المعطيات المسجلة عليها إلى لغة الآلة.ويستوي بعد ذلك لوقوع فعل تغيير الحقيقة على هذا المستند الشكل الذي يكون عليه،فيدخل فيه إلى جانب الشرائط أو الأقراص الممغنطة المسجل عليها البرامج أو المعطيات بطاقات الائتمان المزورة أو البطاقات البنكية بصفة عامة والوثائق والخطابات، خلاف جريمة التزوير العادية، كما لا تتحقق تلك الجريمة من خلال اصطناع لا أساس له أو من مجرد تصوير أو نسخ أصلي موجود. (1)

طرق التزوير: إن فعل تغيير الحقيقة في جريمة تزوير المستندات المعالجة آليا لا يتحقق إلا باستخدام طرق التزوير المادية فقط دون المعنوية،بشرط أن يقع هذا الفعل عل محتوى مستند أصلي معالج آليا موجودا سلفا وحقيقيا،ويستوي بعد ذلك أن يقع هذا الفعل داخل نظام المعالجة الآلية للمعطيات أم خارجه كما يستوي أن يقع ذلك قبل أم بعد دخوله إلى ذلك النظام.

الضرر بخصوص عنصر الضرر،فلا يوجد جديد يضاف إلى مضمون هذا العنصر مما هو مسلم به في جريمة تزوير المحررات فيستوي أن ماديا أو معنويا حالا أم محتملا فرديا أم جماعيا ، ويقاس ضابط الضرر على أساس ما للمستند المعالج آليا من قيمة قانونية في الإثبات أي يصلح لأن يحتج به في مواجهة الغي أو التمسك به في مواجهته، ويستوي بعد ذلك أن يكون هذا المستند قد أعد من البداية لهذا الغرض أم أنه يتمتع بتلك القيمة على نحو عارض وعلى سبيل المصادفة ، بعد التعديل تزوير المستندات المعلوماتية منذ تعديل قانون

1–د/علي عبد القادر القهوجي،المرجع السابق،ص151

العقوبات الفرنسي الجديد في1992/12/16 حذفت جريمتي تزوير المستندات المعالجة آليا واستعمالها من بين جرائم الاعتداء على أنظمة المعالجة لآلية للمعطيات .

وهذا الحذف له ما يبرره وهو إختلاف المصلحة التي يحميها القانون في هاتين المجموعتين من الجرائم.المشرع عند تجريمه للاعتداء على نظام المعالجة الآلية للمعطيات هي هذا النظام ذاته أو بمعنى فالمصلحة التي يحميها أدق هي مصلحة صاحب الحق في هذا النظام أو مصلحة من له السيطرة عليه،بينما المصلحة التي يحميها القانون بصدد جريمة ولهذا السبب وأيضا بسبب الاختلاف حول نطاق التزوير العادية هي الثقة العامة في المستندات ذات القيم القانونية أيا كان شكلها،تزوير المستندات المعالجة آليا قرر المشرع الفرنسي إلغاء نصوص التزوير المعلوماتي .

وتجسيدا لهذا الاتجاه تم تعديل المادة 1/441 قانون العقوبات الفرنسي بحيث تغطي كل صور التزوير التي تنشأ عن استخدام الحاسب الآلي وأصبحت تنص على أنه "كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن فكر Godfrain."

وهذا التعديل الجديد يكشف على أن المشرع الفرنسي قد تحول مما سبق أن رفضه بشدة إبان عرض اقتراح وأصبح التزوير في مجال المعلوماتية يخضع لما يخضع له التزوير في مجال المحررات العادية،طبقا للتعديل الجديد فإن جريمة التزوير في مجال المعلوماتية يكون لها نفس أركان وعناصر جريمة التزوير في المحررات (1)

أي يلزم لتحققها توافر محرر أو أي دعامة أخرى تحتوي تعبيرا عن الفكر ويترتب عنه ضرر للغير والركن المعنوي وهو القصد الجنائي العام والخاص ويصدق نفس الشيء أيضا بالنسبة لجريمة استعمال الدعامات المزورة والجديد الذي استحدثه التعديل فيما يتعلق بما يلي:

1–د/علي عبد القادر القهوجي،المرجع السابق،ص151

محل التزوير إذا كان يقتصر قبل التعديل على المحرر أو المكتوب الذي يتخذ شكل الكتابة أي العبارات الخطية أو العلامات أو الرموز التي تصلح لنقل المعني من شخص إلى آخر، وكان يستبعد استناد إلى هذا التحديد الأسطوانة أو أشرطة التسجيل وغيرها من الدعامات التي لا تتخذ شكل الكتابة الجديد الذي استحدثه التعديل أنه وسع من محل التزوير بحيث أصبح لا يقتصر على ما يصدق عليه وصف المكتوب فقط،تعبير مطلق ويدخل فيه بلا جدال" support autre وإنما يمتد ليشمل أيضا أي دعامة أخرى تحتوي على الفكر.وتعبير دعامة أخرى"كل الدعامات المستخدمة في مجال الحاسب الآلي والتي يسجل عليها تعبيرا عن الفكر يصلح لأن يرد عليه التزوير بأن يكون مجرد سرد للوقائع أو بيانات تعبير عن إرادة،وإنما يلزم فوق ذلك أن تكون تلك الوقائع أو البيانات مما يصلح للتمسك به أو الاحتجاج به وهي لا تكون كذلك إلا إذا كانت تقرر حقا سواء بإنشائه أم بتعديله أم بإلغائه أم بتثبيته . (1)

وهذا يصدق ليس فقط على المستندات المعالجة آليا بل يشمل البرامج أيا كان نوعها والمعلومات المسجلة على أقراص أو شرائط ممغنطة ولو لم يتم معالجتها بعد،أو لم يتم إدخالها بعد إلى جهاز الحاسب الآلي والتعليمات المتعلقة بكيفية تشغيل البرامج والبطاقات البنكية (بطاقات السحب،وبطاقات الائتمان أو الدفع.... الخ) حتى ولو لم تدخل الخدمة،وهكذا يتضح أن التعديل الجديد أفضل من السابق،الذي كان يقتصر فيه التزوير على المستندات المعالجة آليا فقط،ويتجنب الصعوبات للتمييز بين تلك المستندات وغيرها مما لا يخضع لتلك المعالجة.(2)

إن التزوير في مجال المعلوماتية لا يتصور وقوعه بإحدى طرق التزوير المعنوي التي لا تتحقق إلا انتماء التعبير ن الأفكار التي قد تم التعبير عنها من قبل بينما يقع التزوير في هذا المجال

1–د/علي عبد القادر القهوجي، المرجع السابق ، ص152

2–عمر أبو الفتوح عبد العظيم الحمامي ، الحماية الجنائية للمعلومات المسجلة الكترونيا (دراسة مقارنة) ، دار النهضة العربية ، القاهرة 2010 ، ص 886

عن طريق الاستعانة بطرق التزوير المادية اللاحقة وهي التقليد والتوقيع والحذف و الإضافة والتعديل أو التغيير مثل وضع الإمضاء مزور على المستندات المعالجة آليا عن طريق الاستخدام غير المشروع للرقم الشخصي السري للدخول أو تقليد عن مستند معالج آليا

المطلب الثالث:الركن المعنوي: الركن المعنوي للجريمة المعلوماتية يختلف باختلاف أشكالها وعليه ارتأينا التعرض للركن المعنوي لكل جريمة على حدى(1) –الدخول والبقاء بالغش داخل نظام المعالجة الآلية للمعطيات التجول والبقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا إذا تما عن طريق الغش وجريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي والقصد الجنائي يتكون من علم وإرادة فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأن ليس له حق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا دخول الجاني أو بقاؤه داخل النظام مسموحا به أي مشروعا،كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق،كان يجهل بوجود حظر للدخول أو البقاء،أو كان يعتقد خطأ أنه مسموح له بالدخول،فإذا توافر القصد الجنائي بعنصرية العلم والإدارة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام.(2)

من استقراء نص المادة 1/323قانون العقوبات نستنتج أن القصد الجنائي العام لا يكفي إنما يجب توافر قصد جنائي خاص وهو "الغش" ليس المقصود به نية الإضرار و إلا

يكون هناك تناقض بين الركن المادي الذي لا يتطلب النتيجة والركن المعنوي،مفهوم الغش الذي اعتمده الفقه والقضاء بالنسبة لهذه الجريمة هو مفهوم مستعار من الغش في جريمة السرقة

1–أمال قارة،مرجع سابق،ص114

2–علي عبد القادر القهوجي، المرجع السابق،ص152

وقد عرفه الفقهاء كالتالي:عادة يبدو طابع الغش الذي تم به الدخول من خلال الجهاز الرقابي الذي يحمي النظام،أما بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

هذا التعريف المقترح للغش في جريمة الدخول والبقاء يسمح بمواجهة إشكال سبق وأن طرح فيما يخص الحماية الفنية لنظام المعالجة الآلية للمعطيات والسؤال المطروح فيما إذا كان يجب توافر الحماية الفنية حتى يعتبر الدخول أو البقاء غير مشروعين؟

وقد أجاب التعريف المذكور آنفا عن هذه الإشكالية في أن الدخول والبقاء بالغش لا يتضمن معنى خرق فالجهاز الرقابي ما هو إلا وسيلة الجهاز الرقابي للنظام، إنما يظهر من خلال الولوج دون وجه حق إلى النظام لإثبات أن الدخول للنظام غير مرخص، وفي حالة خرق الجهاز الرقابي فجراء عملية إستعجالية لحماية النظام، الدخول هنا تم لمصلحة صاحب النظام في هذه الحالة من الأفضل تأسيس البراءة على أساس نظرية الأفعال المبررة(أسباب الإباحة) وعلى وجه الخصوص على أساس فكرة حالة الضرورة وليس على أساس انعدام الركن المعنوي الاعتداءات علي سير نظام المعالجة الآلية للمعطيات جريمة الاعتداء علي سير نظام المعالجة الآلية للمعطيات نفترض أن الإرادة اتجهت إلى فعل التعطيل أو فعل الإفساد .(1)

كما يجب أن يعلم الجاني بأن نشاطه الجرمي يؤدي إلى تعطيل أو إفساد نظام المعالجة الآلية للمعطيات، وأن يعلم أنّ ذلك بدون رضا صاحب الحق في السيطرة على ذلك النظام أو حتى إرادته وعليه فإن هذه الجريمة المعلوماتية هي جريمة عمدية، لكن الطابع العمدي وحده غير كاف أضاف له المشرع "مع تجاهل حقوق الغير(2) .

-الاعتداء علي سير نظام المعالجة الآلية للمعطيات.وفي هذه الجريمة يفترض أن فعلا العرقلة والتعطيل تما عمدا مع تجاهل حقوق الغير..غياب عبارة"عمديا"من المادة 1/323 من قانون العقوبات ذلك لأنه من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية

1-أمال قارة،مرجع سابق،ص114

2-علي عبد القادر القهوجي، المرجع السابق،ص152

وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء غير المشروع داخل النظام،إذن المقصد الجنائي العام مفترض يستنتج من طبيعة الأفعال المجرمة.(1)

-الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات:كانت هذه الجريمة المعلوماتية في ظل قانون1988ترتكب عمدا أو مع تجاهل حقوق الغير حتى تجرم لكن في ظل القانون الجديد تم تعويضها بعبارة الغش وعليه توافر قصد جنائي عام وقصد جنائي خاص.

-القصد الجنائي العام حيث تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم أن نشاطه الجرمي يترتب عليه التلاعب في المعطيات أو يعلن أن ليس له الحق في القيام وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات أو بدون موافقته.

لكن لا يكفي أن يكون الجاني قد تصرف عمديا بل يجب أن تكون لديه"نية الغش"خاصة وأن أعمال الإضافة والحذف والتعديل هي من صميم النشاط المعلوماتي ولا تقوم الجريمة إلا إذا تمت هذه العمليات بنية الغش وخارج الاستعمال المرخص به الشيء الذي يميز نية الغش كقصد خاص يختلف عن القصد الخاص الذي كانت تتطلبه النصوص السابقة و هو تجاهل حقوق الغير هو أن الغش يتضمن معنى العلم وإرادة إحداث الضرر للغير .(2)

- بالنسبة للتزوير المعلوماتي فإن الركن المعنوي لهذه الجريمة المعلوماتية هو ذات المدلول في جريمة التزوير المحررات وهو ما يتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة ، إلى جانب القصد الخاص فيجب أن ينصرف علم الجاني إلى أنه يغير الحقيقة

1-نهلا عبد القادر المومني،مرجع سابق،ص155

2-أمال قارة،مرجع سابق،ص120

في مستند معلوماتي بإحدى الطرق المحددة في القانون وأن تتجه إرادته إلى فعل تغيير الحقيقة.أما القصد الخاص فهو نية إضافية تتمثل في اتجاه نية الجاني إلى استعمال المستند المزور ويتوافر هذا القصد حتى ولو يستعمل هذا المستند المزور فعلا،ويمكن أن يكون هناك قصد احتمالي عند العلم بإمكانية إحداث ضرر.ما يميز الركن المعنوي للجرائم المعلوماتية بمختلف أشكالها هو صعوبة إثباته.(1)

1-عمر أبو الفتوح عبد العظيم الحمامي،مرجع سابق، ص886-887

الفصل الثاني:آليات مواجهة الجريمة المعلوماتية

الفصل الثاني:آليات مواجهة الجريمة المعلوماتية

الجزائر ليست بمنأى عن الثورة التي أحدثتها المعلوماتية لهذا كان لزاما على المشرع الجزائري أن يسايرها بإحداث تعديل في قانون العقوبات و من أسباب هذا التعديل أن التقدم التكنولوجي و إنتشار وسائل الاتصال الحديثة أدى إلى إبراز أشكال جديدة من الإجرام مما دفع بالكثير من الدول إلى بذل جهود لتوفير الحماية الجزائية للأنظمة المعلوماتية.

وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى النص على معاقبتها وتوفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات وسوف يمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد فكانت المحاولات من الحد من هذه الظاهرة المستحدثة بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها ، فمع التطور التكنولوجي من وسائل تخزين المعلومات و تبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر أصبح أمر أمن تلك البيانات و المعلومات يشكل هاجسا و موضوعا حيويا مهما للغاية.(1)

لذلك كالأول:من توفير أمن للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها و ذلك من خلال توفير الأدوات و الوسائل اللازم توفرها لحماية المعلومات من المخاطر الداخلية أو الخارجية ، والمعايير و الإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ، و لضمان أصالة و صحة هذه الاتصالات .

1–فشار عطا الله (مواجهة الجريمة المعلوماتية في التشريع الجزائري) الملتقى المغربي حول القانون و المعلوماتية ،أكاديمية الدراسات العليا ، ليبيا، أكتوبر ،2009 ص35

المبحث الأول : الآليات التشريعية لمواجهة الجريمة المعلوماتية

إن حماية المعلومات هو أمر قديم و لكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجي و يرتكز أمن المعلومات على:

- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج و التطبيقات
- أنظمة حماية الولوج أو الدخول إلى الأنظمة
- أنظمة حماية قواعد البيانات

ولتوفير هذه الحماية كان لابد من وضع نصوص قانونية تجرم كل الأفعال التي من شأنها المساس بأنظمة المعالجة الآلية للمعطيات و تنظم الجزاءات المقررة لها إما عن طريق قانون الإجراءات الجزائية أو القوانين الخاصة و هذا ما سنتطرق إليه من خلال المطالب التالية:

المطلب الأول: الأمن المعلوماتي في قانون العقوبات

تدارك المشرع الجزائر خلال السنوات الأخيرة و لو نسبيا الفراغ القانوني من مجال الإجرام المعلوماتي عموما و الإجرام عبر الانترنت خصوصا بموجب القانون04-15 المتضمن تعديل قانون العقوبات ، الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات و هي: (1)

<u>الفرع الأول</u>: جريمة التوصل أو الدخول غير المصرح به

حيث أن هذه الجريمة تقوم بمجرد ما يتم الدخول غير الدخول المرخص به أو عن

طريق الغش في المنظومة المعلوماتية ، سواء مس ذلك الدخول أو البقاء في كامل

1-محاضرة ألفيت من طرف بورزام أحمد ،وكيل الجمهورية لدى محكمة باتنة ، تحت عنوان الجرائم المعلوماتية، المجلس القضائي بباتنة يوم20جوان 2006،ص14

المنظومة أو في جزء منها فقط

وهو ما أشارت إليه المادة394 مكرر من قانون العقوبات بنصها على (يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة) ، أورد المشرع طرفين لتشدد عقوبة الدخول غير المشروع إلى المنظومات المعلوماتية ، الطرف الأول حذف أو تغيير المعطيات ، و الطرف الثاني هو تخريب نظام اشتغال المنظومة ، وقد أشار المشرع في المادة المذكورة أعلاه على تجريم فعل الشروع في جريمة الدخول غير المصرح به ، ذلك بقوله أو يحاول ذلك. (1)

الفرع الثاني: جريمة التزوير المعلوماتي:

النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال و المحو و التعديل ، ولا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها إذ يتوفر الركن المادي للجريمة بمجرد قيام أحد هذه الأفعال ، لكن القاسم المشترك في هذه الأفعال جميعا هو انطواؤها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات(2) وذلك بإدخال معطيات جديدة غير صحيحة أو تعديل آخر قائمة.

ولقد أكد المشرع على معاقبة هذه الجرائم في المادة 394مكرر1 بنصها :

(يعاقب بالحبس و الغرامة كل من أدخل بطريق الغش معطيات لنظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها)

1–بوزام أحمد،مرجع سابق ،ص15

2–خثيرمسعود،الحمايةالجنائية لبرامج الكمبيوتر(أساليب و ثغرات)،دار الهدى،عين مليلة،الجزائر،2012،ص123

الفرع الثالث: جريمة الاستيلاء على المعطيات:

تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي ، وهي ما أقرته المادة394مكرر2 بنصها على كل من يقوم عمدا أو بطريق الغش:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو مرسلة أو معالجة عن طريق منظومة معلوماتية

– حيازة أو إنشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم الرابع.

الفرع الرابع: جريمة إتلاف و تدمير المعطيات:

تطرق لها المشرع الجزائري بالمادة 394 مكرر1 من قانون العقوبات والتي تنص على:

–يعاقب بالحبس و الغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تضمنها القسم الخامس .

الفرع الخامس:جريمة الإحتيال المعلوماتي:

بنظر إلى نص المادة 394 مكرر2 على :(يعاقب بالحبس و الغرامة كل من قام بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية...) أي أن يهدف مرتكبها إلى جني فوائد مالية جراء ذلك، في القسم السادس (1)

الفرع السادس: أنشطة الإنترنت المجسدة لجرائم المحتوى الضار و التصريف غير القانوني:

نصت مواد القسم السابع مكرر من ق ع و خاصة المادة 394

مكرر2/ 2 على تجريم أفعال الحيازة، الإفشاء و النشر التي تطرأ على المعطيات

1–الجريدة الرسمية عدد71 الصادرة في10–11–2004 المتضمن قانون العقوبات

الآلية بهدف المنافسة غير المشروعة ، الجوسسة، الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة ،وذلك بعقوبتي الحبس و الغرامة إضافة إلى مانصت عليه المادة 394 مكرر6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات .(1)

تمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية و هي :عقوبة الحبس و الغرامة ، وعقوبات تكميلية بموجب نص المادة 394 مكرر6 و المتمثلة في : إغلاق المواقع و المحل و أماكن الاستغلال و مصادرة الأجهزة و البرامج و الوسائل المستخدمة سواء إن كانت الجريمة قد ارتكبت بعلم مالكها ،ومثال ذلك إغلاق مقهى الانترنت الذي ترتكب فيه هذه الجرائم بشرط علم مالكها وقد أورد المشرع ظروفا نشدد بها العقوبة للجريمة و هي:

–حالة الدخول و البقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام

–إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام المواد: 394،1/152مكرر، و 394 مكرر2 من قانون 15–04 المؤرخ في 2004/11/10 أكد المشرع الجزائري أيضا بموجب المادة 394 مكرر 5 على تجريم

الإشتراك (سواء شخص طبيعي أو معنوي) في مجموعة أو إتفاق بغرض الإعداد

لجريمة من جرائم الماسة بالأنظمة المعلوماتية –بعقوبة الجريمة –بفعل أو بعدة أفعال

مادية وكان التحضير مجسد، أي بمعنى آخر فإن المشرع إستثنى العقاب على الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد. (2)

1–المواد 394 مكرر2 و 394 مكرر6 من قانون 04–15 المؤرخ في:2004/11/10

2–نفس المرجع

كما نصت المادة394 مكرر4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع بغرامة تساوي 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي ، غير أن المسؤولية الجزائية للشخص المعنوي ستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة (1)

والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها و هو مانصت عليه المادة394 مكرر7 من قانون العقوبات ، ونص المشرع الجزائري على حماية الأشخاص من التعدي على حياتهم الخاصة وذلك من خلال المادة303 مكرر، حيث حددت هذه المادة الحالات التي يتم فيها المساس بحرمة الحياة الخاصة و ذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أوسرية أو صور في مكان خاص بغير إذن صاحبها أو رضاه، نخلص إلى أن المشرع الجزائري رغم تداركه من خلال قانون 15-04 و المتضمن تعديل قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث. (2)

-تنص هذه المادة على أنه: كل من شارك في مجموعة أو أكثر من جرائم المنصوص عليها في هذا القسم و كان بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها التحضير مجسد(1)

1-المواد 394 مكرر1 و2 ، 152 من قانون 15/04 المؤرخ في/11/10/ 2004

2-بورزام أحمد، المرجع السابق، ص15

المطلب الثاني:الأمن المعلوماتي في قانون الإجراءات الجزائية

نجد أن المشرع نص على مجموعة من الجزاءات الخاصة بالجريمة المعلوماتية حيث جاءت المادة37 قانون الإجراءات الجزائية بالنص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم المعلوماتية و نص على التفتيش في المادة 45 الفقرة 7، كما نصت المادة 51 الفقرة 6 على توقيف النظر في جريمة المساس بأنظمة المعالجة، ونص على إعتراض المراسلات و تسجيل الأصوات وإلتقاط الصور من المادة 65 مكرر5 إلى65 مكرر10 أما بالنسبة لنصوص إجراءات التحقيق و المحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية (1)

كما تناول قانون الإجراءات الجزائية موضوع الجرائم الافتراضية من خلال:

1-إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجاز لها تمديد اختصاصها للنظر في الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات (المواد37-40-329)

2-تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم التي تمس أنظمة المعالجة الآلية إلى كامل الإقليم الوطني(المادة16)

3-التنصيص على قواعد إستثنائية في التفتيش

أ-جواز التفتيش في المحلات السكنية و غير السكنية و في كل ساعة من ساعات الليل و النهار لمعاينة الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات بناءا على إذن مسبق من وكيل الجمهورية المختص (المادة47) (2)

ب-إمكانية قيام ضباط الشرطة القضائية بالتفتيش داخل المساكن و من دون

1-أمال قارة، مرجع سابق ،ص 130

2-مولود ديدان، قانون الإجراءات الجزائية ،الأمر 11-02 ، دار بلقيس،الجزائر،ص18،22،31،32،33

حضور المشتبه فيه و دون شهود (المادة45 الفقرة الأخيرة)

ج–إمكانية قيام ضباط الشرطة القضائية بتفتيش مسكن أي شخص أن يحوز أوراق وأشياء لها علاقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات من دون حضور صاحب المسكن (المادة45 الفقرة الأخيرة)، إن هذه القواعد الاستثنائية المنصوص عليها في المادة45 لا تعفي من إتخاذ جميع التدابير اللازمة لضمان إحترام السر المهني عندما يجرى التفتيش في محلات يكون أصحابها ملزمون باحترام السر المهني، وجميع تلك الإجراءات الاستثنائية تستوجب الإذن المسبق من وكيل الجمهورية عندما يتعلق الأمر بحالة التلبس أو بتحقيق إبتدائي(1)

4–إمكانية إستعمال أساليب خاصة بالتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات و يتعلق الأمر:

أ–باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية .

ب–بالتقاط و تثبيت و بث و تسجيل الكلام و التقاط صور للأشخاص في الأماكن الخاصة جاءت جميع هذه الصلاحيات الاستثنائية مشروطة بإذن السلطة القضائية كما نص القانون على أن الإذن نفسه ينبغي أن يتضمن الضوابط التي تحول دون التعسف في استعماله .

ج–التسرب: أجازت المادة 65 مكرر11، التسرب كوسيلة لمعاينة جرائم المساس بأنظمة المعالجة الآلية للمعطيات وإيقاف مرتكبيها وذلك من خلال قيام ضباط أو عون الشرطة القضائية أو الأشخاص الذين يتم تسخيرهم لغرض التسرب بإيهام المشتبه فيه أنهم يشتركون معه في إرتكاب الجريمة (كفاعلين أو شركاء أو بإخفاء مصطلحات الجريمة) (2)

1–مولود ديدان ، المرجع السابق،ص18،22،31،32

2–نفس المرجع

5-التنصيص على إمكانية تمديد فترة التوقيف للنظر:

نص قانون الإجراءات الجزائية المعدل سنة 2006 على إمكانية تمديد فترة التوقيف للنظر المحددة ب48 ساعة مرة واحدة عندما يتعلق بالتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات في حالات التلبس.(1)

المطلب الثالث:الأمن المعلوماتي في القوا نين الخاصة

لما نتكلم عن القوانين الخاصة بالأمن المعلوماتي فنحن نكون بصدد التعرف على قوانين الملكية الفكرية و قوانين الملكية الصناعية وكذا النصوص الخاصة بجرائم تكنولوجيا الإعلام و الاتصال و هذا ما سنتطرق إليه على التوالي:

الفرع الأول:الأمن المعلوماتي في قوانين الملكية الفكرية

نظرا للإعتداءات التي تتعرض لها مختلف المنتجات الفكرية عبر الإنترنت إرتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية، و سنفصل ذلك من خلال نقطتين أساسيتين:

-الحماية في إطار قانون الملكية الصناعية

-الحماية في إطار قانون الملكية الأدبية و الفنية

أولا : الأمن المعلوماتي من خلال قوانين الملكية الصناعية

تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين آخرها الأمر رقم 06-03 المؤرخ في 19-07-2003 و المتعلق بالعلامات التجارية -نعلم أن كل برنامج يحمل اسما خاصا به لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج ، ولما كانت هذه الحماية قاصرة على

1-فشار عطاالله، مرجع سابق، ص 35

الإسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الإسم مقترنا به ،غير أن الحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط ، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد(1)

وكذلك الأمر 03-07 المتعلق ببراءة الإختراع: حيث عرفت المادة 02 من الأمر 03-07 الاختراع على أنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية ، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي: (شرط الابتكار ،شرط الجدة ،القابلبية للتطبيق الصناعي، ،المشروعية) يتحصل المخترع في حال توافر هذه الشروط على براءة الاختراع و هي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال إختراعه و التمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة و بشروط معينة و الجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية.(2)

غير أن السؤال المطروح هو هل تستفيد برامج الحاسب من حماية بواسطة براءات الاختراع؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد السببين:

1-إما تجرد البرامج من أي طابع صناعي

2-إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى إستحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات و ليس من الهين إثبات توافر هذا الشرط إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدر معقول من الدارية لتقر ما إذا كان قد سبق تقديم إختراعات مشابهة للإختراع المقدم الطلب بشأنه أم لا،الأمر الذي يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة

1-فشار عطاالله ،مرجع سابق ،ص36

2 -المادة 2 من القانون 03-07المؤرخ في 19 -07-2003 المتعلق ببراءة الاختراع ،الجريدة الرسمية عدد44 صادر في 23-07-2003

و التمييز في المجال التي تتولى بحثه، إضافة على التحفظ العلمي لمنتجي برامج الحاسب على استعمال قوانين براءة المخترع، و يتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة و التكلفة العالية و المدد الطويلة التي يستغرقها هذا التسجيل ،فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر و عليه يمكن للغير الوصول إلى سر البرنامج و استغلاله قبل صدور البراءة ،تجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع و التي نصت على أنه:"تعد من قبل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"(1)

تجسدت هذه القوانين فيما يلي:الامر66-57 المؤرخ في19-03-1966 المتعلق بعلامات المصنع و العلامات التجارية،المعدل و المتمم بالأمر رقم 67-233 مؤرخ في 19-10-1967 المتضمن أحكام العلامات التجارية و المعدل بالأمر رقم 03-06 مؤرخ في 19 جويلية 2003، و المتعلق بالعلامات ، الجريدة الرسمية عدد44 صادر في 23 جويلية 2003

ثانيا:الأمن المعلوماتي من خلال قوانين الملكية الأدبية

شهد النصف الأخير من القرن العشرين تطورا ملحوظا في مجال الاتصال رافقه تطور في وسائل نقل الإنتاج الفكري على إختلاف صوره من علوم و فنون و آداب ،و قبل تعديل قوانين التأليف في بعض الدول ،بادر القضاء إلى إسباغ الحماية على برامج الكمبيوتر كمصنفات فكرية ضمن عمومية النصوص الواردة في شأن المصنفات التقليدية ،فالنصوص في مجموعها و إن كانت لم تذكر صراحة برامج الحاسب الآلي مما أوجد مصنفات بإشراك حياة حقوق صاحب براءة الاختراع كما في القانون التجاري الجزائري(2)

1-أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير ،جامعة الجزائر ،2002 ص17

2-نفس المرجع

جديرة بحماية حق المؤلف كانت محل اهتمام و دراسة من قبل المتخصصين في مجال الملكية الفكرية إتجه المشرع الجزائري صراحة إلى الإعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي وذلك من خلال تعديله للأمر 73- 14 بموجب الأمر 97-10.

- من خلال استقراء الأمر 97-10 المعدل و المتمم بالأمر 03-05 نستخلص مايلي:

أ-أن المشرع الجزائري و سع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية ، والتي عبر عنها بمصنفات قواعد البيانات و برامج الإعلام الآلي التي تمكن من القيام بنشاط علمي،أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة و تترجم بإندفاعات إلكترونية بالحاسوب ، أما قواعد البيانات فهي عبارة عن مجموعة من المصنفات و الأساليب و القواعد ، كما يمكن أن تشمل الوثائق المتعلقة بسير المعطيات و قد أشارت المادة 5 إلى قواعد البيانات بنصها أنه تعتبر أيضا مصنفات محمية الأعمال الآتية : مجموعة المعلومات البسيطة التي تأتي أصالتها من إنتقاء مواردها أو تنسيقها أو ترتيبها (1)

1-أن الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية بارن، و بالتالي هذه المادة تشمل حتى مصنفات الإعلام الآلي(المادة 58 من الأمر 03-05)

2-تشديد العقوبات الناجمة عن مساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية إذ في السباق تجريم الاعتداءات على الملكية الفكرية تناولته المواد390-394 من قانون العقوبات لكنها أخرجت بموجب الأمر 97-10 من مضلة قانون العقوبات و أصبح لها تجريم خاص إذ أن أمر رقم 97-10مؤرخ في

06 -03-1997 المتعلق بحق المؤلف و الحقوق المجاورة ، الجريدة الرسمية

1-أمال قارة، الجريمة المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم القانونية، مرجع سابق ،ص 18 .

عدد13 صادر في 12-03-1997 ، معدل و متمم بأمر03-05 مؤرخ في 19-07-2003 المتعلق بحقوق المؤلف و الحقوق المجاورة ،،الجريدة الرسمية عدد44 صادر في :2003/07/23 حيث أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة الاعتداء على حق المؤلف ، بينما الأمر 97-10 وكذا الأمر 03-05 يقرران عقوبتي الحبس و الغرامة.

إتضح مما سبق أن المشرع الجزائري سواء بدافع توفير الحماية الجزائية للمعلوماتية أو بدوافع خارجية قد واكب التطورات الحاصلة في المجال المعلوماتي، بأن أخضع المعلوماتية لقانون الملكية الفكرية موسعا بذلك من سلطة القاضي في تقرير العقوبة ،وذلك ضمانا و حماية لحق المؤلف و مالك الحق المجاور.(1)

وتجدر الإشارة إلى أن المستجدات التي إعتمدها المشرع الجزائري من خلال الأمرين 10-97 و05-03 تعود لأسباب أهمها أن من شروط الانضمام إلى المنظمة العالمية للتجارة هو المصادقة على اتفاقية بارن و هو ما فعلته الجزائر بموجب المرسوم الرئاسي 97-341 إضافة إلى تبني أحكام إتفاق جوانب الملكية الفكرية المتعلق بالتجارة.

الفرع الثاني:الأمن المعلوماتي في قانون مكافحة جرائم تكنولوجيات الإعلام والاتصال

سنتطرق فيما يلي إلى أسباب صدور القانون رقم 09-04 مؤرخ في 05اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها،ثم إلى مضمون هذا القانون باختصار

أولا: أسباب صدور قانون مكافحة الجرائم المعلوماتية

من أهم الأسباب التي دفعت بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام و الاتصال و خاصة الجرائم الناشئة عن

1-أمال قارة ، المرجع السابق، ص78-79

الإستخدام غير المشروع لشبكة الانترنت ، خاصة في ظل الثورة التي تعرفها في مجال إستخدام الانترنت ، وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة المرتكبة عبر الانترنت هو القصور الذي عرفه القانون رقم 04-15 و المعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و بين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة هذه و التدخل السريع لتحديد مصدرها و التعرف على مرتكبها.(1)

ثانيا: مضمون قانون مكافحة الجرائم المعلوماتية : يتضمن قانون09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال على ستة فصول نلخصها فيما يلي:

الفصل الأول: نص على الأحكام العامة التي تبين الأهداف المتوخاة من القانون و تحدد مفهوم مصطلح التقنية الواردة وكذا مجال تطبيق أحكامها .

الفصل الثاني: حيث جسد أحكام خاصة بمراقبة الاتصالات الالكترونية ، وقد روعي في وضع هذه القواعد خطوة التهديدات المحتملة وأهمية المصالح المحمية، حيث نص القانون على أربع حالات يسمح فيها للسلطات الأمنية لممارسة الرقابة على المراسلات و الاتصالات الالكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب و الجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو نظام العام ، ولمقتضيات التحريات و التحقيقات القضائية و عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، وفي

1-القانون رقم 09-04 المؤرخ في:2009/05/02 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و مكافحتها،الجريدة الرسمية عدد47لسنة2009،ص14

إطار تنفيذ الطلبات المساعدة القضائية الدولية المتبادلة.(1)

الفصل الثالث: تضمن القواعد الإجرائية،الخاصة بالتفتيش و الحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة وعلى هذا الأساس يجوز للجهات القضائية و ضباط الشرطة القضائية الدخول والتفتيش و لو عن بعد إلى المنظومة المعلوماتية أو جزء منها ، و كذا المعطيات المعلوماتية المخزنة فيها مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي ، و يسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها (2)

الفصل الرابع :تطرق إلى التزامات مقدمي الخدمات في مجال الاتصالات الالكترونية و ذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الالكترونية لاسيما التزام حفظ المعطيات المتعلقة بحرمة السير و التي من شأنها المساعدة في كشف الجرائم و مرتكبها ، يهدف هذا القانون إلى إعطاء للسلطات العمومية و مقدمي الخدمات دورا إيجابيا و مساعدا في مواجهة الجرائم و كشف مرتكبها.

حيث ألزم هذا القانون مقدمي خدمات الانترنت على التدخل الفوري لسحب المحتويات التي تم بإمكانهم الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، و تخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام و الآداب العامة و إخطار المشتركين لديهم بوجودها .

1- الجريدة الرسمية للجمهورية الجزائرية ، العدد47 المؤرخة في 25 شعبان عام1430 الموافق ل16اغسطس 2009م،ص19

2- نفس المرجع،ص15

-**الفصل الخامس:**أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام و الاتصال و مكافحته،إذا نص القانون على إنشاء هيئة وطنية وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها،وقد تم الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل و تنظيم هذه الهيئة.(1) يعتبر القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها نطاقا واسعا في مجال مكافحة الجرائم المرتكبة عبر الانترنت ،حيث جاء كجريمة للأفعال المخالفة للقانون و التي ترتكب عبر وسائل الاتصال عامة .

الفصل السادس: تحدث عن الاختصاص القضائي و كيفية التعاون و المساعدة القضائية (2) الدولية

1- فشار عطاالله ،المرجع السابق،ص39

2- الجريدة الرسمية للجمهورية الجزائرية –العدد47،مرجع سابق،ص14

المبحث الثاني: الآليات المؤسساتية لمواجهة الجريمة المعلوماتية

نتطرق من خلال هذا المبحث إلى الآليات المؤسساتية التي واجهة الجريمة المعلوماتية وهي الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال كهيئة وطنية مستحدثة في مطلب أول و الهيئات القضائية الجزائية المختصة في مطلب ثاني أما المطلب الثالث فيكون التطرق فيه للمعهد الوطني للأدلة الجنائية وعلم الإجرام أما المطلب الرابع فيكون الحديث فيه عن المديرية العامة للأمن الوطني .

المطلب الأول:الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال

تم استحداث هيئة وطنية مهمتها متابعة كل منشورات الإنترنت و مراقبة إتصالات الهاتف الثابت و النقال، في الجزائر من أجل ضمان المراقبة الوقائية للاتصالات الالكترونية و الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و المساس بأمن الدول .

وإعتمدت الجزائر رسميا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و التي تأتي كلبنة جديدة في مسار الإصلاحات التي باشرها رئيس الجمهورية من أجل تعزيز دولة القانون،و التأكيد أكثر على سيادة القانون في كل الأحوال في مرسوم رئاسي رقم15–261 مؤرخ في 08 أكتوبر2015، وذلك في خطوة جديدة نحو مراقبة كل المحتويات المنشورة عبر شبكة الانترنت ، حيث تم وضع هذه الهيئة تحت تصرف وزير العدل، وتتكون لجنتها المديرة من وزير الداخلية ووزير تكنولوجيات البريد و الاتصال و قائد الدرك الوطني و المدير العام للأمن الوطني و ممثلين عن وزارة الدفاع الوطني ورئاسة الجمهورية ،إضافة إلى قاضين من محكمة العليا، وذلك بهدف مكافحة الجرائم المعلوماتية ، وحسب هذا المرسوم فإن هذه الهيئة تعمل على مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و من خلال جمع المعلومات

1– –الجريدة الرسمية للجمهورية الجزائرية–العدد47،مرجع سابق،ص14

والتزويد بها عبر الخبرات القضائية ، وتهدف هذه الهيئة الجديدة تحت سلطة القاضي المختص،إلى تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصادرها و مسارها من أجل استعمالها في الإجراءات القضائية ،كما تسهر الهيئة أيضا على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية و تطوير تبادل المعلومات و التعاون على المستوى الدولي في مجال اختصاصها، موضحا أن هذه الهيئة التي تعد سلطة إدارية مستقلة لدى وزير العدل، ستعمل تحت إشراف و مراقبة لجنة مديرة يترأسها وزير العدل، و تضم أساسا أعضاء من الحكومة معنيين بالموضوع ، و مسؤولي مصالح الأمن ، و قاضين إثنين من المحكمة العليا يعينها المجلس الأعلى للقضاء ،وستضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين

لمصالح الاستعلام العسكرية و الدرك و الأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية ، فيما تكلف بتنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

كما تعنى الهيئة الجديدة بمساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال، و ضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المتخصص .

ومن بين الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية(1)

حيث تمت الإشارة في هذا المجال،إلى أنه "وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية

1-سالم عبد الرزاق،ملتقى حول اللمنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية،بمحكمة سيدي أمحمد،ص11

و في هذا القانون و مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات ،يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية،و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية."و ينص القانون على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، كما يحدد قوانين الإجراءات المتعلقة بتفتيش المنظومة المعلوماتية،حيث "يتعين على مانحي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و ستجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها،و بوضع المعطيات التي يتعين عليهم حفظها".

ويتطرق كذلك لإلتزامات مانحي خدمات الانترنت، و بخصوص التعاون و المساعدة القضائية الدولية، أشار القانون إلى أن "المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني،عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني" ، ويعتبر هذا المسار قد مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة، و لمراجعة الترسانة التشريعية، بما في ذلك المجال الجزائي، من أجل تحسين حماية حقوق و حريات المواطنين ، و تشديد العقوبات على أي تقصير في هذا المجال."كما جاء القانون الذي تم تنفيذه الفعلي بفضل سلسلة من تعليمات الرئاسية ذات الصلة لتحديد صلاحيات السلطة القضائية، ومنها على وجه الخصوص ،التعليمة الصادرة في 28 ماي 2014 التي تحظر بدون أي استثناء، كل قرار بالمنع من مغادرة التراب الوطني ما لم يسلم من طرف قاضي التحقيق أو نيابة الجمهورية.كما ذكر بيان الرئاسة، في هذا السياق بحركة الإصلاحات الأمنية و السياسية الواسعة التي شرع في تجسيدها منذ سنة2011 برفع حالة الطوارئ، وتنفيذ عدة قوانين ذات بعد سياسي، مؤكدا بالمناسبة هذا المسار سيتوج لاحقا بمشروع مراجعة الدستور.(1)

1-نفس المرجع،ص12

المطلب الثاني:الهيئات القضائية الجزائية المختصة

سنتطرق في هذا المطلب إلى الهيئات القضائية الجزائية المختصة في ردع الجريمة المعلوماتية والمتمثلة في كلا من الضبطية القضائية وقاضي التحقيق والمحكمة ودورها في توفير الأمن المعلوماتي .

الفرع الأول:الضبطية القضائية

ويأتي دور الشرطة القضائية في الحماية من الجريمة المعلوماتية من خلال مرحلة جمع الاستدلالات و ضباط الشرطة القضائية نوعان: النوع الأول: و هم ضباط

يتمتعون باختصاص عام و يختصون بإجراءات الاستدلال شأن الجرائم المنصوص عليها في قانون العقوبات أما النوع الثاني: فهم ذوو الاختصاص النوعي المحدود

بخصوص نوع معين من جرائم حددها القانون على سبيل الحصر،هؤلاء المشار إليهم في المادة 21من قانون الإجراءات الجزائية و سلطتهم كذلك محددة لا تمتد إلى مرحلة التفتيش و دخول المنازل و المعامل و المباني أو الأماكن المحاطة بأسوار إلا بحضور أحد ضباط الشرطة القضائية و من بين هؤلاء: رؤساء الأقسام، المهندسون

وأعوان الغابات و حماية الأراضي، وتعد محاضرهم ذات حجية و قوة إثبات كما استقر عليه القضاء الوطني و مايهمنا في هذه الدراسة هو دور الضبطية القضائية و مجال اختصاصها فيما يتعلق بالجريمة المعلوماتية(1)

أولا:الإجراءات التقليدية لجمع الدليل

سنتطرق في هذا الفرع إلى إجرائيين الإجراءات المادية و الإجراءات الشخصية.

أولا:الإجراءات المادية: تتمثل هذه الإجراءات في المعاينة و التفتيش و الضبط **أ-المعاينة**

والمقصود بالمعاينة هي الرؤية بالعين لمكان أو شخص أو شيء لإثبات حالته و ضبط كل مايلزم لكشف الحقيقة.

و تعتبر المعاينة إجراءا من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها ، كما يمكن للمحكمة أن تقوم بإجراءات

1- زبيخة زيدان، المرجع السابق، ص116،117

معاينة إذا رأت ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة(1)

-كيفية إجراء المعاينة التقنية لمسرح الجريمة الالكترونية:

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي إلى مسرح الجريمة، لأن هذا الأخير حجر الزاوية في التحقيق الجنائي و مكمن الآثار و الأدلة المادية،و ينبغي التعامل في الإطار مع مسرح الجريمة الالكترونية على أنه مسرحان هما:

المسرح التقليدي:

يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية و يترك فيها الجاني عدة أثار كالبصمات و بعض متعلقاته الشخصية أو وسائط تخزين رقمية

المسرح الافتراضي:

يقع داخل البيئة الالكترونية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب و شبكة الانترنت في ذاكرة الأقراص الصلبة الموجودة بداخله (2)

ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه الجريمة و ذلك بإتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية و المتمثل:

1- ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها و شبكاتها

2-و جود خريطة توضح الموقع الذي سيتم معاينته و تفاصيل المبنى أو الطابق موضوع البلاغ ، و عدد الأجهزة و الخزائن و الملفات ويحدد ذلك من خلال مصادر سرية لجهات الأمن .

1-عائشة بن قارة مصطفى،المرجع السابق،ص79،80

2-نفسه ،ص84

3- تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة

4-تأمين الأجهزة و المعدات التي سيتم الاستعانة بها في عملية المعانية سواء كانت أجهزة أو برامج.

5-إعداد الفريق المتخصص الذي يتولى المعانية من الخبراء و رجال الضبط و الأمن

6- تحديد البيانات و المهام و الاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدى، وذلك حتى لا تتداخل الاختصاصات.

7-إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل

8-أن تتم هذه المعاينة وفق مبدأ المشروعة و في إطار ماتنص عليه القوانين الجنائية .

9- تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة و مابها من برامج و شبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي (1)

ب-تفتيش في البيئة الإلكترونية:

التفتيش في مدوله القانوني بالنسبة للجرائم المعلوماتية لا يختلف عن مدلوله السائد في فقه الإجراءات الجزائية رغم إختلاف المحل الذي يقع عليه التفتيش، و يقصد به إجراء من الإجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات و تخزين و مخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة و تشكل جناية أو جنحة و التوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة و نسبتها إلى المتهم بارتكابها .

كما تتفق التشريعات العربية على تعريف التفتيش بأنه إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق و كل مايفيد الحقيقة في شأنها.

1-نفسه ص85،86

يثير موضوع التفتيش الذي يقع على نظم الحاسب الآلي مسائل عديدة للبحث كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، و حكم تفتيش الوسائل التي تتصل مع بعضها البعض و تقع في أماكن عامة أو خاصة، و ضوابط هذا التفتيش .

1-مدى صلاحية الكيانات المعنوية كمحل يرد عليه التفتيش.

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة فإن البعض قد شك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنوية للحاسب الآلي و هو ما حذا ببعض التشريعات بأن تنص صراحة على أن تفتيش يتم بالنسبة لأنظمة الحاسب الآلي مثل ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر في سنة 1990 حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي(1).

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

وعلى ضوء هذه الآراء الفقهية، وعلى النحو الذي قننه المشرع الجزائري صراحة في إمكانية وقوع التفتيش على مساكن أشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية فان التفتيش يرد على الكيانات المعنوية في الحاسبات الآلية، بحسب أن هذه الكيانات المعنوية و إن كانت غير مادية إلا أنها في نطاق الأشياء المادية(2).

ويترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسب ووسائط أو أوعية حفظ و تخزين البيانات المعالجة آليا كالاسطوانات و الأقراص و الأشرطة

1-د.هلالي عبدالله أحمد،تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،ص73

2-زبيخة زيدان،المرجع،السابق،ص130،131

الممغنطة و مخرجات الحاسب، ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام و التي يمكن عزلها ككيان قائم بذاته

2–ضوابط التفتيش الذي يقع على نظم و مكونات الحاسب الآلي

لقد تطورت طرق التفتيش بحيث أنها أصبحت لا تقف–فقط–عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، و إنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الالكترونية و خاصة الحاسب الآلي، أو تقع عليه، فيمكن تبعا لذلك تسجيل البيانات المعالجة ألليا بعد تحويلها من نبضات أو ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء محسوسة تسجل و تخزن على وسائل معينة،وعلى هذه الوسائل يرد التفتيش أو الضبط . (1)

ويخضع التفتيش لشروط مقيدة يجب مراعاتها تحت طائلة البطلان.

إذ تنص المادة 44 من القانون الإجراءات الجزائية بعد تعديله بالقانون رقم06–22على عدم جواز إجراء التفتيش من قبل ضباط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل و الشروع في التفتيش .

ثم تنص المادة 45على القيود الذي يتعين على ضباط الشرطة القضائية احترامها أثناء فترة التفتيش بصفة عامة لكن أضاف التعديل وتمم نص المادة45 بأن رفع القيود الواردة فيها فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،إلا ما تعلق منها بالحفاظ على السر المهني وكذا جرد الأشياء و حجز المستندات. (2)

كما أجاز في نص المادة47 إجراء التفتيش و المعاينة و الحجز في كل محل سكني أوغير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة47 من قانون الإجراءات الجزائية،إذ تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن

1–د.هلالي عبدالله أحمد، المرجع السابق، ص89

2–د.هشام رستم، الجوانب الإجرائية، المرجع السابق، ص69

مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

غير أن المشرع لم يتطرق إلى المحل الذي عليه التفتيش بصفة مدققة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، ذلك أن التفتيش هنا يقع على نظام معلومات الحاسب أو الوسائط أو أوعية حفظ و تخزين البيانات المعالجة إلكترونيا كالاسطوانات و الأقراص و الأشرطة الممغنطة و مخرجات الحاسب.

ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام و التي يمكن عزلها ككيان قائم بذاته

والملاحظ أن المشرع الجزائري عندما عدل نصوص المواد المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد خص الحاسبات الآلية داخل الدولة حتي لو إتصلت مع بعضها البعض فيكون ذلك عن طريق شبكة محلية .

لكن يطرح التساؤل هنا في حالة ما إذا اتصلت بحاسبات أخرى خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة،ومنها شبكة الانترنت (1)

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

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

إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة47.

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

1–د.هشام رستم،المرجع السابق،ص69

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

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

لكن الجزائر لحد الآن لم تنضم إلى أي من المعاهدات أو الاتفاقيات الخاصة بجريمة المعلوماتية (1) .

ثانيا-الإجراءات الشخصية

سنتطرق في هذه المجموعة التي هي ذات طبيعة شخصية لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء و الحصول على دليل و تتمثل هذه الإجراءات في :عملية التسرب، الشهادة، والخبرة التقنية، إستجواب المتهم.

1-عائشة بن قارة مصطفى،المرجع السابق،ص201

أ-التسرب:

المادة 65 مكرر12 قانون الإجراءات الجزائية الجزائري عرفت التسرب بأنه"يقصد بالتسرب قيام ضابط أوعون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف يسمح لضابط أوعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة و أن يرتكب عند الضرورة الأفعال المذكورة في المادة65 مكرر14 أدناه و لا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على إرتكاب الجرائم(1)

أما بالنسبة لمواصفات الإذن بالتسرب و طبيعته حددتها المادة65 مكرر15 من قانون الإجراءات الجزائية و هي:

1-أن يسلم فقط لضرورة التحري أو التحقيق القضائي

2-أن يكون مكتوبا.

3-أن يكون مسببا.

4-أن يذكر في الإذن طبيعة الجريمة التي ينص عليها الإذن

5-يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته.

6-يحدد فيه المدة المقررة للعملية و المحددة بأربعة أشهر و هي قابلة للتجديد لمدة أربعة أشهر أخرى كل ما دعت الضرورة ذلك.

7-أن تودع الرخصة أي الإذن في ملف الإجراءات بالانتهاء من عملية التسرب (2)

*و ملاحظة على ذلك أنه إذا أغفل شرط من هذه الشروط يؤدي إلى بطلان الإذن خرج المشرع الجزائري عن الأصل العام في تحقيق القائم بالفصل بين سلطني الاتهام و التحقيق و أوكل لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مهمة إصدار الإذن بالتسرب. (3)

1-بوكثير خالد،المرجع السابق،ص26

2-مولود ديدان،قانون الإجراءات الجزائية،المرجع السابق،ص42

3-زبيخة زيدان،المرجع السابق،ص169

ب-الشهادة في الجريمة المعلوماتية :

-تعريف الشاهد في الجريمة المعلوماتية : يطلق عليه إسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة و المتخصص في تقنية و علوم الحاسب الآلي و الذي يكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات فلذلك نجد أن الشاهد المعلوماتي ينحصر في إحدى الطوائف التالية: مشغلة الحاسب الآلي، خبراء البرمجة ،المحللون، مهندسوا الصيانة و الاتصالات ،مديرو النظم. (1)

وللشاهد إلتزامات لابد من التقيد بها مثل: طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطباعتها و تسليمها إلى سلطات التحقيق و الإفصاح عن كلمات المرور السرية و الكشف عن الشفرات المدونة بها و الأوامر الخاصة بتنفيذ البرامج المختلفة(2)

ج-الخبرة في الجريمة المعلوماتية:

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

وقد أجاز المشرع للمحقق الإستعانة بخبير متخصص في المسألة موضوع الخبرة فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه يجوز لكل جهة قضائية تتولى: التحقيق أو تجلس للحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة أو الخصوم أو من تلقاء نفسها.

و بالنظر إلى الطبيعة الخاصة بالجرائم المعلوماتية فان إماطة اللثام عنها قد يحتاج إلى خبرة فنية تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر هذه الحاجة في مرحلتي التحقيق و المحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها و الطبيعة المعنوية لمحل الاعتداء(3)

و بالعودة لنص المادة146 نجد أن المشرع بفرض على الجهة القضائية الآمرة بندب الخبير تحديد مهمة الخبير بدقة و هذا يعود بنا إلى ضرورة تأهيل سلطات

1-مولود ديدان،قانون الإجراءات الجزائية،المرجع السابق،ص43

2-زيبخة زيدان،المرجع السابق،ص169

3-بوكثير خالد،المرجع السابق،ص23

التحقيق أو الحكم في الجرائم المعلوماتية لنجاح الهدف المتوخى من التحقيق في هذا النوع المستحدث من الجرائم.

كما تجدر الإشارة على أنه يجب على القاضي إختيار الخبراء ذوي الإمكانيات العلمية و المقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية،إذا يجب مراعاة الخبرة العلمية فالوسائل الالكترونية متعددة و شبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية و علمية دقيقة (1)

وعلى القاضي أن يتناول في أمر ندب الخبير المسائل التالية:

1- تركيب الحاسب الآلي ، طرازه ، نوعه ،نظام تشغيله،الأنظمة الفرعية التي يستخدمها.

2-بيئة الحاسب أو الشبكة من حيث طبيعتها ،تركيزها ،توزيعها و كذلك نمط و وسائط الاتصالات

3-المكان المحتمل لأدلة الإثبات وشكلها و هيئتها .

4-الأثار الاقتصادية و المالية المترتبة عن الجريمة المعلوماتية

5- كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو الأجهزة أو تدميرها

6 -إمكانية نقل أدلة الإثبات لأوعية أو وسائط مادية كالأوراق أو الأسطوانات على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة(2)

د- الإستجواب :

وهو مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق و مطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما،وذلك قصد محاولة كشف الحقيقة وإستظهارها بالطرق القانونية.

أحالت التشريعات استجواب المتهم بضمانات خاصة و ذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية و تتمثل في حق

---

1 – بوكثير خالد،المرجع السابق،ص23

2– زبيخة زيدان،المرجع السابق،ص170

الاستعانة بمحام أثناء الاستجواب.(1)

-الإجراءات الحديثة لجمع الدليل الإلكتروني:

أولا:الإجراءات المتعلقة بالبيانات الساكنة:

1-التحفظ المعجل على البيانات المخزنة:

في المادة 16من اتفاقية بودابست نصت على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالأمور المخزنة بواسطة نظام المعلوماتي(2).

وذلك عندما تكون هناك أسباب تدعو للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير، وهذا خلال مدة 90 يوم كحد أقصى وتكون هذه المدة قابلة للتمديد(3).

-المقصود بمزودي الخدمات:

مزود الخدمات هو من تقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.

-مفهوم التحفظ المعجل على البيانات المخزنة:

يقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، في إنتظار إتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية.

ثانيا :الإجراءات المتعلقة بالبيانات المتحركة:ونجد فيها:

-اعتراض الاتصالات الالكترونية.

-اعتراض المراسلات السلكية و اللاسلكية و المراقبة الالكترونية.

تجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا

1-مولود ديدان، قانون الإجراءات الجزائية، المرجع السابق، ص35

2-د.هشام رستم، المرجع السابق، ص134

3-نفس المرجع ، ص140، 141

التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فانه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها.(1)

وانطلاقا من أهمية حماية الحياة الخاصة نجد الدستور ينص في المادة 39 "لايجوز إنتهاك حرمة حياة المواطن المختصة،وحرمة شرفه، يحميها القانون، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة" وتبعا لذلك نظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك و الإجراءات التي يتم إتباعها حيال هذه المراقبة.(2)

وإذا كانت شبكات الحاسب الآلي تستخدم خطوط الهاتف و تستعين بجهاز معدل الموجات "modem" والذي يستطيع تحويل الإشارات الرقمية المستحدثة بواسطة الحاسب على موجات تناظرية تنقل مع موجات الصوتية خلال خطوط الهاتف، وبذلك فانه يتبن وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك تتم بالوسائل الإلكترونية بحيث يمكن القول أن هناك تنصتا و مراقبة إلكترونية تتم على شبكات الحاسب الآلي.(3)

و من ثمة لا يجوز التنصت عليها أو الإطلاع على الأسرار التي تحتويها إلا بذات الطرق التي ينص عليها قانون الإجراءات الجزائية، فلا يستطيع الشخص إختراق صندوق البريد الإلكتروني أو الدخول إلى أنظمة الحاسب الآلي المخزنة به الرسائل البريدية الإلكترونية و ضبطها إلا عن طريق إتباع إجراءات قانونية محددة في القانون و من قبل أشخاص مخولين قانونا بذلك.

وقد اختلف الفقه في تكييف إجراء إعتراض المراسلات السلكية و اللاسلكية،فذهب رأي إلى أنها تعد تفتيشا و بالتالي تخضع لقيوده،وإستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها هو البحث و ضبط ما يفيد الوصول إلى الحقيقة

1-بوكثيرة خالد،الجرائم المعلوماتية،مذكرة نهاية تدريب،المنظمة الجهوية للمحامين ناحية سطيف دفعة2005-2006،ص24

2- عائشة بن قارة مصطفى،المرجع السابق، ص154

3- هلالي عبدالله،المرجع السابق،ص22

ولا أهمية لأن يكون الشيء المضبوط ماديا أم معنويا،وهي ذات الغاية من المراقبة و التصنت فهي البحث عن دليل معين(1)

في حين ذهب رأي آخر إلى التفرقة بين التفتيش و المراقبة، وأعتبر الأول إجراء غايته العثور على الأدلة المادية و ضبطها بوضع اليد عليها لمصلحة العدالة أما الثانية فليس لها كيان مادي ملموس و القول بأن الرسائل الالكترونية أو الحديث في التلفون يندمج في كيان مادي يمكن ضبطه،فأسلاك التلفون أو التسجيل ليس دليلا في حد ذاته وإنما هي وسيلة أو أداة لسماع الحديث و لا تتأثر طبيعته بوسيلة أو أداة الحصول عليه.(2)

و الرأي السديد أن التفتيش و إعتراض المراسلات إجراءان مختلفان ذلك أن المشرع الإجرائي قد أفرد أحكاما خاصة لكل واحد منها نظرا لإختلاف المحل الذي يقع على كل منهما،فالأخير يقع على حرمة الحياة الخاصة بمطلق القول،أما الأول فقد يمس مصادفة هذه الحياة الخاصة حتى وإن تمت على كيانات معنوية فليس معنى أنه يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائما على كيانات معنوية أن نسوي بينهما من حيث تأثيرهما على حرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش.

وقد تدخل المشرع الفرنسي في10جويلية1991 بإصدار قانون يفرض الرقابة على الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات بعد إختلاف الفقه بشأن ضبط الأشياء المعنوية من مكونات الحاسب الآلي عن طريق التنصت أو اعتراض المراسلات إذا إعتبر جانب من الفقه أن قانون الإجراءات الجزائية عندما نص على إصدار إذن بضبط أي شيء":فانه يشمل بذلك بيانات الحاسب المعنوية. أما الجانب الآخر للفقه فإقترح مواجهة هذا القصور التشريعي بالنص صراحة على
إعتراض المراسلات و يجب أن تشمل المواد المعالجة عن طريق الحاسب الآلي.

1–د.رؤوف عبيد،مبادئ الإجراءات الجنائية في القانون المصري،دار الجيل للطباعة،الطبعة السادسة عشر،1985 ص358

2–د.أحمد فتحي سرور، مرجع سابق،ص147

وعلى ضوء هذا القانون فإن المشرع الإجرائي الفرنسي خص إصدار قرار المراقبة بقاضي التحقيق (المادة1/110) وله أن يندب مأمور الضبط القضائي للقيام به،ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة و كانت هناك إستحالة في الوصول إليها بطرق البحث و التنقيب العادية م(1/100) وتطلب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقب عليها بالحبس الذي يزيد عن سنتين م (2/100) وكذلك حدد ميعادا زمنيا للمراقبة مدته أربعة أشهر في حدها الأقصى و تكون قابلة للتجديد، وأنه يتعين أن يتم التسجيل و تفريغ التسجيل تحت سلطة قاضي التحقيق و رقابته(م100)

وقد خاض المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائية بالقانون رقم06-22 المؤرخ في20 ديسمبر2006 في نص المادة14المتممة للباب الثاني من الكتاب الأول من الأمر رقم66-155 بالفصل الرابع تحت عنوان"إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور"بالمواد 65 مكرر5 إلى المادة 65 مكرر10. (1)

وقد خول المشرع لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة65 مكرر5 ومن بين هذه الجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

فيسمح الإذن بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المنصوص عليها في المادة47 من القانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق على تلك الأماكن و تنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية.(2)

والإذن بالمراقبة أو التنصت أو إعتراض المراسلات محددة بميعاد 4 أشهر

1-بوكثيرة خالد،المرجع السابق،ص24

2-عائشة بن قارة مصطفى،المرجع السابق،ص176،177 .

كحد أقصى قابلة للتجديد المادة65 مكرر7.

كما خول لقاضي التحقيق الإذن أيضا بوضع هذه الترتيبات في حالة فتح تحقيق قضائي و تتم العمليات تحت مراقبته المباشرة.

كما أجاز المشرع في نص المادة65 مكرر8 تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات السابقة المذكورة في نص المادة65 مكرر5، و في الأخير على ضباط الشرطة القضائية تحرير محضر عن أي عملية إعتراض أو تسجيل أو وضع ترتيبات تقنية و عمليات الالتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري و يذكر تاريخ بداية هذه العمليات و الانتهاء منها،ركما يودع أي تسجيل أو إعتراض أو نسخ تم أثناء عملية المراقبة و يودعها بالملف.(1)

الفرع الثاني: دور قاضي التحقيق في توفير الأمن المعلوماتي

ويبرز دور قاضي التحقيق من خلال المرحلة الثانية بعد مرحلة جمع الإستدلالات وهي مرحلة التحقيق

أولا: تعيين قاضي التحقيق

في الجزائر يتعين قاضي التحقيق بمقتضى قرار من وزارة العدل، ثم عدل المشرع عن ذلك بموجب القانون01-08 المؤرخ في 26جوان2001 وأصبح التعيين بموجب مرسوم رئاسي،وفقا لنص المادة39 قانون الإجراءات الجزائية،إلا أنه حتى هذه الأخيرة تم إلغاؤها بموجب القانون رقم06-22 المؤرخ في 20ديسمبر2006 ليرجع من جديد للتعيين(2)

بموجب قرار من وزير العدل بعد استشارة المجلس الأعلى للقضاء من بين قضاة الجمهورية،وهذا رجوعا إلى نص المادة 50 من القانون الأساسي للقضاة ، وتكون مدة التعيين ثلاث سنوات،وتنتهي مهام قاضي التحقيق بنفس الأشكال التي يتعين فيها،أي بقرار من وزير العدل(3)

1-نفس المرجع،ص178

2-عبد الرحمان خلفي،الإجراءاتالجزائية في التشريع الجزائري و المقارن،دار بلقيس لنشر،دط،2015،ص223،224

3-عائشة بن قارة مصطفى،المرجع السابق،ص177

ثانيا:اختصاص قاضي التحقيق

سنتناول في هذا العنصر قواعد الاختصاص الشخصي ثم النوعي وأخيرا المحلي لقاضي التحقيق.

أ-الاختصاص الشخصي.

الأصل أن قاضي التحقيق يحقق مع جميع الأشخاص دون تمييز،إلا أن المشرع الجزائري إستثنى بعض الفئات:

-الأحداث

- العسكريين

-ضباط الشرطة القضائية

-قضاة الحكم و التحقيق و مساعدي و كيل الجمهورية

-قضاة المجالس القضائية ورؤساء المحاكم ووكلاء الجمهورية

-قضاة المحكمة العليا ورؤساء المجالس القضائية و النواب العامون

-أعضاء الحكومة و الولاة ويختص كذلك بالتحقيق في جميع جرائم القانون العام سواء كانت جناية أو جنحة أو مخالفة التي من خلالها تقدم النيابة العامة طلب إفتتاحي أو الجنايات أو الجنح التي من خلالها يقدم الطرف المدني إدعاء مدنيا(1)

ب-الاختصاص النوعي.

يختص قاضي التحقيق بالتحقيق في جميع الجرائم و يكون ذلك وجوبي في الجنايات و جوازي في الجنح إذا كان هناك نص وإختياري في المخالفات طبقا لنص المادة66 من قانون الإجراءات الجزائية: التحقيق الابتدائي وجوبي في مواد الجنايات أما في مواد الجنح فيكون إختياري مالم يكن ثمة نصوص خاصة،كما يجوز إجرائه في مواد المخلفات إذا طلبه وكيل الجمهورية،ويختص كذلك قاضي التحقيق على مستوى المحاكم الجهوية في جرائم : المخذرات و الجريمة المنظمة و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال و الإرهاب و جرائم الصرف طبقا للمرسوم التنفيذي رقم 348 المؤرخ في 2006/10/06

1-عبد الفتاح بيومي حجازي،التوقيع الالكتروني في النظم القانونية ندار الفكر الجامعي،الاسكندرية،2005،ص519

ج-الاختصاص المحلي:

تنص المادة 40 من قانون الإجراءات الجزائية "يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.... (1)

-كذلك يجوز أن يمتد اختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 40 قانون الإجراءات الجزائية.

ثالثا: سلطات قاضي التحقيق و حدود الدعوى الجنائية أمامه

القيام باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة و بالتحري عن أدلة الاتهام وأدلة النفي المادة 68 قانون الإجراءات الجزائية يجوز لقاضي التحقيق أن يأمر بإجراء فحص طبي كما له أن يعهد إلى الطبيب بإجراء فحص نفساني أو يأمر باتخاذ أي إجراء يراه مفيدا المادة 68 قانون الإجراءات الجزائية.

ينسق القاضي المكلف بالتحقيق سير إجراءات التحقيق وله وحده الصفة في مسائل الرقابة القضائية و الحبس المؤقت وإتخاذ أوامر التصرف قي القضية طبقا لنص المادة70 قانون الإجراءات الجزائية.(2)

يستطيع القاضي سماع أقوال كل من يشير إليهم في كل الشكوى بإعتبارهم شهودا طبقا لنص المادة73 من قانون الإجراءات الجزائية.

يستطيع قاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جمع المعاينات اللازمة أو القيام بتفتيشها طبقا لنص المادة79 قانون الإجراءات الجزائية.

إستدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية طبقا لنص المادة88 قانون الإجراءات الجزائية .

1-عبد الرحمان خلفي،المرجع السابق،ص228

2-مولود ديدان،قانون الإجراءات الجزائية،المرجع السابق،ص38،39،40

يجوز للقاضي إستدعاء مترجم طبقا لنص المادة91 قانون الإجراءات الجزائية.

إصدار أمر بإحضار المتهم أو بإيداعه السجن أو بإلقاء القبض عليه حسب نص المادة 109 قانون الإجراءات الجزائية(1)

رابعا:السمات التي يتميز بها قاضي التحقيق بالنسبة للجريمة المعلوماتية

إن الجريمة المعلوماتية تختلف عن الجريمة التقليدية فلذالك لا يمكن أن يحقق فيها أي قاضي تحقيق وإنما لابد أن يكون له صفات خاصة و هذه الصفات هي:

كأن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة وأن يميل إلى تصميم البرامج أكثر من تشغيلها و يجب معرفة الجديد عن هذه البرامج وأن يستطيع تصميم و تحليل البرامج أو أنظمة التشغيل بسرعة وأن يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على الإختراق و الشبكة و كل هذه الأمور لا تتوافر إلا لمن كان لديه إمكانيات عقلية تزيد على متوسط العام المألوف .

خامسا:كيفية اتصال قاضي التحقيق بملف الدعوى الخاص بالجريمة المعلوماتية

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي للطلب الافتتاحي لإجراء تحقيق، وإما عن طريق شكوى مصحوبة بإدعاء مدني"ضمن الشروط المنصوص عليها في المادتين 67 و73

أ-الطلب الافتتاحي لإجراء التحقيق:

يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية أن يطلب فتح التحقيق ما لم ينص القانون على وجوب التحقيق في بعض الجنح،ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا ظهرت وقائع جديدة طبقا للمادة 3/67 من قانون الإجراءات الجزائية الجزائري على أنه "لايجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها .

ويجوز أن يوجه الطلب ضد شخص مسمى أو غير مسمى .

1-عبد الرحمان خلفي ،نفسه

و لقاضي التحقيق سلطة إتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه.

فإذا وصلت لعلم قاضي التحقيق وقائع لم يشر إليها في طلب إجراء التحقيق يتعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع"

ب-الشكوى المصحوبة بالادعاء المدني:

تنص المادة 72 من قانون الإجراءات الجزائية"يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص. (1)

إن إحدى طرق تحريك الدعوى من طرف الأفراد،وهي في نفس الوقت إحدى طرق اتصال قاضي التحقيق بملف الدعوى، و يلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت، وحرصا منه على أن يكون الإشراف على الملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية القضائية التي عادة ما يكون لها تأثير على مجرى التحقيق، كما أنه يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها.

إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء استعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية الكاذبة إذا ما خسر دعواه، ولهذا عليه أن يتأكد من أن إتهامه كان مبنيا على دليل قوي في الدعوى(2)

سادسا :استئناف أوامر قاضي التحقيق.

الجهات التي تستأنف أوامر قاضي التحقيق هي:

أ-النيابة العامة

لوكيل الجمهورية أو أحد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء وذلك طبقا لنص المادة170من قانون الإجراءات الجزائية الجزائري" لوكيل الجمهورية الحق في أن يستأنف أمام غرفة الاتهام جميع أوامر قاضي التحقيق.

1-مولود ديدان،قانون الإجراءات الجزائية،المرجع السابق ص ،42،45،49

2-عبد الرحمان خلفي، المرجع السابق، ص296

و يكون هذا الإستئناف بتقرير قلم مكتب المحكمة و يجب أن يرفع في ثلاثة (3) أيام من تاريخ صدور الأمر

يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة استئناف أمر الإفراج و يفرج على المتهم رغم

استئناف النائب العام مالم يكن وكيل الجمهورية قد إستأنفه بالطبع و يجب أن يبلغ النائب العام عند استئناف الخصوم في الدعوى، وذلك خلال العشرين يوما التالية لصدور الأمر حتى يكونوا على بينة من أمرهم و لايفاجؤا بقرار من غرفة الاتهام في غير صالحهم

طبقا لنص المادة171 من قانون الإجراءات الجزائية الجزائري"يحق الاستئناف أيضا للنائب العام في جميع الأحوال و يجب أن يبلغ استئنافه للخصوم خلال العشرين يوما التالية لصدور أمر قاضي التحقيق و لايوقف هذا الميعاد و لا رفع الاستئناف بتنفيذ الأمر بالإفراج المؤقت. (1)

ب-استئناف المتهم:

إن المتهم لا يجوز له إستئناف جميع أوامر قاضي التحقيق و يرفع الاستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة أيام من تبليغ الأمر إلى المتهم طبقا للمادة 168قانون الإجراءات الجزائية

ج-استئناف المدعي المدني.

كما أجاز المشرع الجزائري للمدعي المدني الحق في استئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية،وبمفهوم المخالفة لايجوز له استئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت و الإفراج و الرقابة القضائية.

ويرفع الاستئناف خلال ثلاثة أيام من تاريخ تبليغ الأمر المراد استئنافه إلى المدعى المدني،وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا لنص المادة173 الإجراءات الجزائية(2)

1-مولود ديدان، قانون الإجراءات الجزائية، المرجع السابق،ص106

2-عبدالرحمان خلفي، المرجع السابق، ص298

الفرع الثالث:المحكمة

أولا:الاختصاص المحلي في الجريمة المعلوماتية

طبقا لنص المادة37 من قانون الإجراءات يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط أو مكان إقامة المتهم أو مكان الضبط(1)

كما نصت أحكام المرسوم التنفيذي رقم348 –06 المؤرخ في 5 أكتبور2006 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق

إلى دائرة إختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي امحمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران وفي نطاق الجرائم المعلوماتية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان أخر،فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة،وتعد جريمة معلوماتية إذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر أنها أرتكبت في جميع الأماكن التي إمتدت الجريمة فيها، ومتى كانت الجريمة المعلوماتية،أيا كان نوعها فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام و الاتصال إذ ارتكبت خارج الإقليم الوطني،أو إذا كان مرتكبيها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي(2)

ثانيا:الاختصاص النوعي في الجريمة المعلوماتية.

يتحدد الاختصاص النوعي للمحكمة الفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي ينظر فيها،حيث تختص محكمة الجنايات في الفصل في الجنايات و الجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الإتهام حسب نص المادة248 من قانون الإجراءات الجزائية الجزائري.(3)

1–مولود ديدان،قانون الإجراءات الجزائية،المرجع السابق،ص79

2–نفس المرجع،ص17

3– جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجي الحديث،دار النهضة العربية،القاهرة 1992،ص63

كما تختص المحاكم في النظر في الجنح و المخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 01 من المرسوم التنفيذي رقم 348-06 المؤرخ في 28 أكتوبر 2006 المتضمن تحديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.(1)

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخذرات والجريمة المنظمة العابرة للحدود وجرائم تبييض الأموال والإرهاب ، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذ جعل الإختصاص ينعقد إلى دائرة إختصاص أخرى وهذا مانصت عليه المواد 37 ،40 ، والمادة 329 من قانون الإجراءات الجزائية إثر التعديل الذي جاء به القانون 04-14 المؤرخ في 10نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06- 348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات إقليم موسع لدى المحاكم بكل من : الجزائر العاصمة ، قسنطينة ، وهران ، ورقلة . (2)

1-الجريدة الرسمية للجمهورية الجزائرية ، العدد 63 ، المرجع السابق ،ص29

2-القانون رقم 04-14، المرجع السابق، ص 4

المطلب الثالث:المعهد الوطني للأدلة الجنائية و علم الإجرام

المعهد الوطني للأدلة الجنائية و علم الإجرام مقره ببوشاوي بالعاصمة و يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة،جميعها تضمن،التكوين و التعليم تقديم المساعدات التقنية،الدراسات و التحاليل في علم الجريمة وإنجاز الخبرة، البحوث

دائرة الإعلام الآلي و الإلكتروني مكلفة بمعالجة،تحليل و تقديم كل دليل رقمي و تمثالي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة ،أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف،التقنيات و الطرق المستعملة في مختلف الخبرات العلمية،لإنجاز المهام المنوطة بها

الفرع الأول:تشكيلته

كما سبق و أشرنا أن المعهد الوطني للأدلة الجنائية و علم الإجرام يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة وتنقسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات سمعية،بصرية،والإعلام الآلي.

كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات و ضمان نزاهة وشرعية الدليل وهذه المخابر هي:

1-مخبر الإعلام الآلي 2-مخبر الفيديو 3-مخبر الصوت

أولا:مخبر الإعلام الآلي

يختص مخبر الإعلام الآلي بتحليل ومعالجة حوامل المعطيات الرقمية، الهاتف ،الشريحة،القرص الصلب،ذاكرة الفلاش و تحديد التزوير الرقمي للبطاقات البنكية. يتوفر على وجود محطة ترميم و تصليح الأجهزة و الحوامل المعطلة وكذلك الشبكات الإعلامية ، خبرات الإعلام الآلي و التجهيزات البيانية .

كما يضم الشبكات الإعلامية خبرات الإعلام الآلي و التجهيزات البيانية و جهاز إقتناء معلومات الهواتف و الحواسيب(1)

1-هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية،المعهد الوطني للأدلة الجنائية وعلم الإجرام،جامعة بسكرة كلية الحقوق،2013،ص3

والقاعات التي يحتوي عليهاهى7 قاعات: مكتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، فصيلة إقتناء المعطيات، قاعة موزع وقاعات تخزين(1)

ثانيا:مخبر الفيديو

من مهام مخبر الفيديو مقارنة الأوجه وشرعية الصورة و الفيديو و إعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية

الصورة فيديو – صورة بمختلف التقنيات.

وتضم الأجهزة التالية: جهاز فيديو بوكس و حوامل الفيديو الرقمية و الممغنطة و حبكات إعلامية .

كونيتك ستوديو ،ماكس ثلاثي الأبعاد وموزع لحفظ شرائح الفيديو.

أما بالنسبة للقاعات يحتوي مخبر الفيديو على4رقاعات قاعتان للتحليل، قاعة التخزين و قاعة موزع .

ثالثا: مخبر الصوت

يعمل على تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

ومن أجهزته أجهزة الازدواجية و السماع و حبكات إعلامية معالجة وتحسين التسجيلات الصوتية،نسخ الأقراص المضغوطة وأجهزة التصليح و التعبير.

أما بالنسبة للقاعات فإنه يحتوي مخبر الصوت على05 قاعات :03 قاعات للتحليل، قاعة تخزين و قاعة موزع(2)

الفرع الثاني: مهام المعهد الوطني للأدلة الجنائية و علم الإجرام

على غرار الدول الأخرى لم تعد الجزائر بعيدة عن الإجرام المعلوماتي حيث أضحى هذا النوع الجديد من الجريمة الخفية و العابرة للأوطان يشكل تهديدا جديا و حقيقيا على الأفراد و مؤسسات الدولة الاقتصادية .

1–هواري عياش، المرجع السابق،ص3

2–حوار مع العقيد بن رجم جمال مدير مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية و مكافحتها مجلة الجيش،عدد599،جوان2013 ص 14،15

وبموجب النص الذي تم سنة2004 و المتعلق بمكافحة الجريمة المعلوماتية تم إنشاء مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية و مكافحتها من أجل القضاء أو الحد من هذه الآفة و ذلك من خلال:

-مساعدة و حدات الدرك الوطني الممارسة لمهام الشرطة القضائية في البحث و التوصل إلى مرتكبي المخالفات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات وكذا المخلفات المتعلقة بإستخدام الأنظمة المعلوماتية لتكنولوجيا الإعلام و الاتصال.

-ومن أجل تحقيق ذلك يحوز أفرادها الذين يطاردون الجريمة المعلوماتية أحدث الأنظمة والأجهزة و البرمجيات المتطورة من أجل استخدامها في عمليات الوقاية من الإجرام المعلوماتي ومكافحتها وهذا ما يعد تحديا في حد ذاته حيث يتعلق الأمر بحماية المنظومة الوطنية للمعلومات من خلال تطبيق القانون وقد نجحت خلال السنوات الأخيرة في حل العديد من القضايا منها65 في المائة متعلقة بالمخلفات المرتكبة ضد الأشخاص و8 في المائة ضد الأمن العام وكذا 27 في المائة متعلقة بمخالفات مرتكبة ضد المؤسسات في إطار ممارسة مهامه و نشاطه و يقوم المركز بالتعاون والتنسيق مع المصالح الأمنية الوطنية وعدد من متعاملي الخدمات الهاتفية من أجل الاستجابة للطلبات التي تأتيها من مختلف وحدات الدرك الوطني و المتعلقة بالتشخيص و التعرف على العناوين الالكترونية أو أرقام المرسلين محل التحقيق كما أن المركز يتعاون مع مختلف السلطات القانونية و التشريعية في مجال طلبات التعامل مع الهيئات القانونية الدولية(1)

أما فيما يخص أفاق المركز فيمكن القول أن المركز يسعى إلى :

-تعميم و إستكمال نشر فرق المحققين في الجريمة المعلوماتية وتعميم نظام لليقظة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني

-تكوين مجموعة مختصة في مهام أمن الأنظمة المعلوماتية وحمايتها .

-تكوين المكونين في المجال وإعداد برامج المواد المتعلقة بالتكنولوجيات الجديدة و مكافحة الجريمة المعلوماتية على صعيد كافة مستويات التكوين .

1-حوار مع العقيد بن رجم جمال ،المرجع السابق،ص15

المطلب الرابع: المديرية العامة للأمن الوطني:

لقد تنبهت المديرية العامة للأمن الوطني لخطر الإجرام المعلوماتي في مطلع الآلفية الثانية، وكان ذلك من خلال مشاركة إطاراتها في الملتقيات الدولية التي كانت تنظمها الدول الأجنبية خاصة الأوربية حول الإجرام المعلوماتي ،فمن خلال دق ناقوس الخطر في تلك الدول حول هذه الظاهرة الإجرامية المتسحدثة،إتضح إنتشار و تعميم إستعمال تكنولوجيا الإعلام و الاتصال في تلك المجتمعات كانت لها أثار جانبية سلبية، من جراء إستغلال هذه التكنولوجيا من طرف المجرمين وهو ما جعل الجوانب السلبية لتكنولوجيا الإعلام و الاتصال ستعرف لا محالة طريقها إلى مجتمعنا، بالموازاة مع تعميم و إستعمال هذه التكنولوجيا في بلدنا(1)

ولقد واجهت هذه المديرية الجريمة المعلوماتية بمختلف الوسائل منها:

الفرع الأول: الوسائل القانونية

أ/-القانون 22-06 المؤرخ في 2006/12/10، المعدل و المتمم لقانون الإجراءات الجزائية والذي صنف جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن الجرائم الخطيرة ووضع لها تدابير إجرائية خاصة،منها:

*تمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كافة التراب الوطني.

*مراقبة الأشخاص و التسليم المراقب .

*إمكانية اللجوء إلى الأساليب الخاصة في التحري،لاسيما إعتراض المراسلات،إلتقاط و تسجيل الصور و الأصوات،التسرب.

ب/-القانون 05-03 الخاص بحماية الملكية الفكرية الذي صنف برامج الحاسوب ضمن المصنفات المحمية وإعتبر نشر المصنفات عبر أنظمة المعالجة الآلية للمعطيات كوسيلة من وسائل التقليد المعاقب عليها .

1-مصطفاوي عبد القادر، محافظ الشرطة، الشرطة الوطنية و مكافحة الجريمة المعلوماتية، ملتقي دولي حول محاربة الجريمة المعلوماتية،الجزائر 5-6 ماي2010، مركز البحوث القانونية و القضائية، ص 122

ج/–القانون المدني الذي أقر بأن المعطيات الرقمية يعتد بها كوسيلة إثبات مثلها مثل الوثائق المكتوبة

د/–القانون 04–09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و الذي من أهم ما جاء فيه:

–المراقبة الالكترونية

–تفتيش المنظومات المعلوماتية مع إمكانية تمديد التفتيش من منظومة إلى أخرى ولو خارج الوطن

–حجز المعطيات المعلوماتية– إلزام مقدمي الخدمات بمساعدة السلطات و حفظ المعطيات، – إلزام مقدمو خدمة الانترنت بسحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن،–وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و إخبار المشتركين لديهم بوجودها

الفرع الثاني:الوسائل العملياتية

تتركز إستراتجية المديرية العامة للأمن الوطني في مجال مكافحة الجريمة المعلوماتية على الأعمدة التالية (1)

أ/–التكوين:

أ/1–التكوين الأولي: في مجال التكوين الابتدائي تم إدراج موضوع الجريمة المعلوماتية ضمن البرامج التكوينية المخصصة لضباط الشرطة القضائية

أ/2–التكوين المتواصل والمتخصص:أصبح موضوع الجريمة المعلوماتية من بين الجرائم المستحدثة و التي أدرجت في برامج التكوين المتخصص الموجه للإطارات و الرتباء التابعين للشرطة القضائية.

ب/–إعادة تنظيم مصالح الشرطة القضائية :في إطار سياسة التخصص في مجال الشرطة القضائية،شرعت المديرية العامة للأمن الوطني في إدخال تعديلات على الهياكل التنظيمية الخاصة بمصالح الشرطة القضائية ، وذلك من أجل جعل المصالح

1–مصطفاوي عبد القادر،المرجع السابق،ص123

المكلفة بمكافحة الجريمة أكثر تناسبا مع الواقع و أكثر إستعدادا لما تشير إليه التنبؤات المستقبلية ففي الجريمة المعلوماتية بات من الضروري وضع آليات عملياتية، لذا تم إنشاء مصالح مختصة في مكافحة هذه الجرائم .

ب/1-على مستوى مخابر الشرطة العملية: إثر تفاقم ظاهرة إستخدام التكنولوجيا في مختلف أشكال الإجرام تم سنة2007 تدعيم مخابر الشرطة العلمية و التقنية بأقسام مختصة في الأدلة الرقمية على مستوى المخابر الثلاثة المتواجدة بكل من العاصمة ،وهران و قسنطينة، تكمن مهامها في إستغلال الأجهزة الإلكترونية التي يشتبه إستعمالها في إرتكاب الجرائم و ذلك بهدف إستخراج المعطيات المخزنة بداخلها و التي من شأنها أن تساعد المحققين في التحقيق و التي تشكل في ذاتها أدلة إقناع.

ب/2-أهم الأجهزة التي تتكفل بإستغلالها هذه الأقسام:-أجهزة الكمبيوتر و لواحقها-أدوات التخزين الرقمية مثل (أقراص مضغوطة،أقراص صلبة،أقراص وماضية ،أجهزة الهواتف النقالة،أجهزة التصوير الرقمية)،إلى جانب القضايا المتعلقة بالجرائم الإلكترونية تساعد الأقسام المختصة في الأدلة الرقمية.(1)

1-حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية ، جامعة محمد خيضر بسكرة كلية الحقوق، 2016 ، ص5 ، 6

الخاتمـــــــة

الخاتمة

تعد هذه الدراسة حصيلة جهد متواضع قمنا به من خلال التعرض لأحد الجرائم الخطيرة ذات الطبيعة الخاصة المختلفة عن الجرائم التقليدية وكذا كيفية التصدي لها لما فرضته خصوصيتها على الجهات الخاصة ، بوضع قوانين وطرق أمنية لمكافحة الجريمة ألا أوهي الجريمة المعلوماتية و التعرف على الإختلافات في وصف هذه الجريمة المستحدثة وإعطاء تعريفات مختلفة لها لتميزها بطابع العابرة للحدود و التطور السريع الذي أضعف القائمين على مكافحتها وبالتالي فإن هذه الخصائص وغيرها كان لها الدور الكبير في إبراز النشاط الإجرامي لهذه الجريمة وتوضيح الإختلاف الجوهري الذي ميزها عن الجريمة التقليدية وقبل التطرق لما توصلنا إليه من نتائج وتوصيات حول هذه الجريمة وسبل مكافحتها يجدر بنا الحديث عن الصعوبات التي واجهتنا وفي مقامها الأول طبيعة الموضوع ذاته كونه موضوع فني أكثر منه قانوني وهذا ماأدى بالكثير من الباحثين في المجال القانوني للعزوف عن الحديث في هذا المجال، وعلى كل فإنه يمكن الوقوف على النتائج والتوصيات التالية :

النتائج :

أهم النتائج التي توضحت لنا من خلال خوضنا في موضوع دراستنا هذا هي:

بالنسبة لتعريف الجريمة

تبين لنا أن كل الإعمال والأنشطة الإجرامية متى مست المكونات المادية أو المعنوية لنظام المعلومات وألحقت إضرار بأشخاص عدت جريمة معلوماتية إلا انه لا يوجد إجماع على تعريف موحد للجريمة المعلوماتية حتى قيل أنها تقاوم التعريف

بالنسبة للحماية الجنائية

فكرة الحكومة المستحدثة التي تقوم أساسا على توفير الحماية الجنائية للمعاملات الالكترونية و الهدف من إنشاها هو ربط المواطن بأجهزة الحكومة للحصول على الخدمات بشكل آلي وتخفض كلفة المعاملات الإدارية ويسرع في وتيرتها ولحسن أداءها ولن يأتي ذلك مالم تكن هناك حماية قانونية تجرم الإعتداء على كل المعاملات

بالنسبة للنصوص المستحدثة

-فما يتعلق بالنصوص المستحدثة في هذا المجال فإن أهم نتيجة تمحص عنها هو الإعتراف الضمني للمشرع الجزائـري عن مالية المكونات المعنـــوية لنظام المعلوماتـــــــي

لحماية أنظمة المعالجة الآلية للمعطيات ، وبتعديله لقانون العقوبات ونصه على تجريم الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات وذلك دون التطرق لبعض الجرائم الأخرى كالسرقة أو النصب مرده أن جريمة الدخول والبقاء غير المشروع هي بوابة أغلب الجرائم الواقعة في مجالات المعاملات الالكترونية ، فاختلاس المعلومات أو إتلافها أو الإحتيال للحصول عليها لا يتم إلا بدخول في النظام المعلوماتي وبتجريم الدخول الغير المشروع يكون المشرع غلق باب وقوع جرائم أخرى .

-كما تبين لنا وجود قصور في النصوص المستحدثة فيما تعلق بالمساس بأنظمة المعالجة الآلية للمعطيات حيث أنها لا تكفل المعاملات الالكترونية بحماية جنائية من كل جوانب بل تحميها من بعض الإعتداءات دون الأخرى .

التوصيات والاقتراحات

أما بالنسبة لبعض التوصيات المقترحة فنرى الأخذ بأهم التوصيات المقدمة من المديرية العامة للأمن الوطني وبعض الإقتراحات التي تسد الثغرات المستنتجة وهي كالتالي:

-ضرورة إعطاء تعريف موحد للجريمة المعلوماتية يشمل فيه كل السلوك المجرمة

-ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحقيق التعاون مع التقنيين من أصحاب الخبرة.

- وضع إجراءات كالتحقيق والمحاكمة للجريمة المعلوماتية تختلف عن الجريمة التقليدية.

-إدراج مواد تحسيسية في البرامج التكوينية للأطوار الأولى من التعليم المدرسي ، بهدف توعية الأطفال والمراهقين.

-إدراج مواد تحسيسية في الشعب الجامعية المتخصصة في الإعلام الآلي بهدف إعلام الطلبة بالقوانين المجرمة للإستعمال السيئ لتكنولوجيا الإعلام والاتصال ، من أجل لفت إنتباههم وخاصة المتفوقين في هذا المجال حول خطر الإنسياق وراء هواياتهم لتفادي التورط في قضايا إجرامية .

-تشجيع إنتاج وتسويق البرامج التأمينية وبرامج الرقابة الأبوية .

-كذلك مراعاة الإقتصار عند التجريم و العقاب على أنماط السلوك المحظور حاليا بل يجب مراعاة الأبعاد المستقبلية لأن تكنولوجيا المعلومات و الحواسيب في تطور سريع بل يكاد يكون مذهل.

قائمـــــة المراجـــع

قائمة المراجع

أولا- قائمة المصادر

1-القوانين:

1-قانون رقم 03-07المؤرخ في:2003/07/19المتعلق ببراءة الاختراع الجريدة الرسمية عدد44 الصادرة في 2003/07/23

2-قانون رقم 09-04المؤرخ في 14 شعبان عام 1430 الموافق ل 5غشت سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصة بتكنولوجيا الإعلام والاتصال و مكافحتها ج ر ع 47 صادر بتاريخ 16 أوت 2009

3-قانون رقم 04-14 المؤرخ في 10نوفمبر2004المعدل والمتمم للأمر 155/66 المتضمن قانون الجزائية ،جريدة عدد.71

4-قانون رقم 2000-03 المؤرخ في 2000/8/5 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية

5-قانون العقوبات الفرنسي رقم 97-1159 المؤرخ في 19 ديسمبر 1997 المتضمن قانون العقوبات الفرنسي

2- المراسيم:

المرسوم التنفيذي رقم 06-348 المؤرخ في أكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض ووكلاء الجمهورية وقضاة التحقيق ج ر عدد 63.

ثانيا - قائمة المراجع:

1-الكتب:

1-أحسن بوسقيعة ،الوجيز في القانون الجزائي العام ،دار هومة الجزائر ،ط10،

2-أحمد فتحي سرور

3-أمين طعباش ،الحماية الجنائية للمقالات الالكترونية ،مكتبة الرفاء القانونية الاسكندرية، الطبعة الأولى 2015

4-أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة الجزائر ،ط 2 ،2007

5-أمين فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت،دار المطبوعات الجامعية ،كلية الحقوق ، الإسكندرية ،2009

6-جميل عبد الباقي ، الجوانب الإجرائية للجرائم ،بالأنترنت ،دار النهضة العربية ،القاهرة،2001

7-جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجي الحديثة دار النهضة العربية ،القاهرة ، 2009

8-خيثر مسعود ،الحماية الجنائية لبرامج الكمبيوتر ، أساليب وثغرات دار الهدى ،عين مليلة الجزائر

9-رؤوف عبيد مبادئ الإجراءات الجنائية في القانون المصري ، دار الجيل للطباعة الطبعة السادسة عشر 1985

10-طارق إبراهيم الدعسوقي عطية ،لأمن المعلوماتي ، النظام القانوني لحماية المعلوماتية ، دار الحاسمة الجديدة الإسكندرية 2009

11-عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن ، دار الجامع الجديد ،كلية الحقوق ،جامعة الإسكندرية ، د ط ، 2006

12-عادل عبد العالي إبراهيم خراشي ، اشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية عليها ، دار دار الجامعة الجديدة ، الإسكندرية 2015

13-عمر أبو الفتوح عبد العظيم الحمامي ، الحماية الجنائية للمعلومات المسجلة إلكترونيا (دراسة مقارنة) ، دار النهضة العربية ، القاهرة2010

14-عمر أبو الفتوح عب العظيم الحمامي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الأنترنت دار الفكر الجامعي الإسكندرية 2008

15-عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، الإسكندرية 2006

16-عبد الفتاح بيومي حجازي ، التوقيع الإلكتروني في النظم القانونية ، دار الفكر الجامعي ، الإسكندرية ، 2005

17-علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعية للطباعة والنشر ، بيروت ، د ط، د س

18-عبد الرحمان خلفي ، الإجراءات الجزائية في التشريع الجزائري –دراسة مقارنة ، دار بلقيس لنشر ، دط ، 2015.

19-عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والأنترنت ، منشورات الجلبي الحقوقية ، بيروت ، د ط،2007.

20-محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن ، دار الجامعة الجديدة الإسكندرية 2007

21-محمد زكي أبو عامر وعلي عبد القادر القهوجي ،قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، القاهرة ، 1993.

22-محمد علي العريان ،الجرائم المعلوماتية ،دار الجامعة الجديدة ، الإسكندرية ، د ط ،2004

23-محمد أمين الرومي ، جرائم الكمبيوتر و الإنترنت ، دار المطبوعات الجامعية ، الإسكندرية ،2003

24-مولود ديدان ، دستور ، تعديل نوفمبر 2008 ، دار بلقيس ، الجزائر.

25مولود ديدان ،قانون العقوبات رقم 09-01 مؤرخ في 25 فبراير 2009

26-مولود ديدان ، قانون الإجراءات الجزائية رقم11-02 ، د ط ، ديسمبر 2014

27-نائلة عادل محمد فريد قورة ، الجرائم الحاسب الآلي والاقتصادية ، منشورات الحلبي الحقوقية ، ط1 ، 2005

28-نبيلة هبة هروال ،الجوانب الإجرائية لجرائم الإنترنت ، في مرحلة جمع إستدلالات ،دراسة مقارنة ، دار الفكر الجامعي الإسكندرية ، د ط ، 2013

29-نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، ط1 ،الإصدار الأول 2008 ، 1429هـ- 2008م

30- هشام محمد فريد ، الجوانب الإجرائية للجرائم المعلوماتية ،مكتبة الآلات الحديثة ، أسيوط ، ط 1 ، 1994

31-هلالي عبد الله أحمد ، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، القاهرة ، ط1 ،1997

2-المجلات:

1-مجلة جامعة بابل ، العلوم الإنسانية ، المجلد 14 ، العدد 2 ،2008

2-مجلة الجيش حوار مع العقيد ابن رجم جمال ، مدير مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها عدد 599 ، جوان 2013

3- المدخلات:

1-المقدم عزالدين عزالدين ، ملتقى حول الجرائم المعلوماتية ، الإطار القانوني للوقاية من الجرائم بمكافحتها ، جامعة محمد خيضر بسكرة ، 10 نوفمبر 2015

2-حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، جامعة محمد خيضر بسكرة ، كلية الحقوق ، 2016

3-سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، بمحكمة سيدي محمد.

4-هواري عياش ،مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ، المعهد الوطني للأدلة الجنائية وعلم الإجرام ،جامعة بسكرة كلية الحقوق ،2016

5-مصطفاوي عبد القادر محافظ الشرطة الشرطة الوطنية ومكافحة الجريمة المعلوماتية ملتقى دولي حول محاربة الجريمة المعلوماتية ، الجزائر 5-6 ماي 2010، مركز البحوث القانونية والقضائية

6-بورزام أحمد ،وكيل الجمهورية لدى باتنة ، الجرائم المعلوماتية المجلس القضائي بباتنة

7-مشار عطا الله ،مواجهة الجريمة المعلوماتية في التشريع الجزائري ، الملتقى المغربي حول القانون والمعلوماتية ،أكاديمية الدراسات العليا ، ليبيا ، أكتوبر 2009

8-مجلة الأمن العام ،نائلة محمد فريد ،جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة ،بحث مقدم للمؤتمر التاسع لمنع الجريمة ومعاملة المجرمين ، العدد 151، 1995

4-الرسائل الجامعية:

1-رسائل الماجستير:

1-أمال قارة ، الجريمة المعلوماتية ،مذكرة لنيل شهادة الماجستير ، جامعة الجزائر ،2002.

2-سعيد نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في قانون الجزائري ،مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية جامعة الحاج لخضر باتنة ، 2012-203.

3-عبد الطيف المعتوق ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة لنيل شهادة الماجستير وعلوم الجنائية ، 2011-2012

4-يوسف مناصرة ، جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، رسالة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية ، قسم العلوم القانونية ، جامعة الجزائر ،السنة الجامعية 2008-2009

2-رسائل الماستر:

1-خالد بوكثيرة ، الجرائم المعلوماتية ، مذكرة نهاية التدريب ، المنظمة الجهوية للمحامين ناحية سطيف ، الدفعة 2005-2006

2-مراد ماشوش ،مكافحة جرائم المعلوماتية في التشريع الجزائري ، مذكرة مقدمة لاستكمال نيل شهادة ماستر أكاديمي في مسار الحقوق تخصص ، قانون الجنائي ، 2003

الفهـــــــرس

الفهرس

إن التقدم العلمي في المجال الإلكتروني و ما يتبعه من تنمية معلوماتية قائمة على السرعة في المعاملات و الذي أثر وبشكل كبير في الكثير من جوانب العلاقات التبادلية بين الإفراد ومنها التأثير البالغ على المراكز القانونية وأسس المسؤولية المدنية والجزائية وإنشاء نتيجة ذلك ما يعرف بالمعلومات الإلكترونية التي تتطلب حماية جنائية ذات نوع خاص لخصوصية الأعمال الإجرامية المرتكبة عليها وهذا ما ركز عليه المشرع الجزائري من خلال إستحداث نصوص وأحكام تشريعية خاصة في قانون العقوبات إذا خص الأمر الإعتداءات على الأنظمة المعلوماتية وترك المجال لإجتهاد القاضي في حالة غياب النصوص المستحدثة في أمر ما بمحاولة إخضاعها للنصوص العقابية التقليدية مع مراعاة مبدأ الشرعية وحضر القياس في المجال الجزائي حتى ليترك ثغرة لمرتكب الجريمة للإفلات منها

أما في ما يخص الإعتداءات الواردة على الهيئات المعلوماتية فعلى القاضي الإحاطة بإجراءات الأمر 03-05 المتعلق بالاعتداءات الواردة على حقوق الملكية الفكرية والأدبية والفنية

وما زاد أهمية للموضوع مواكبته لصدور قانون 04-15 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات المستحدثة لنصوص خاصة بالإجرام المعلوماتي وهذا ما حاولنا معالجته من خلال هذا العمل المتواضع .