الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية المرجع: .....

قسم : القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة الإلكترونية في التشريع الجزائري

ميدان الحقوق و العلوم السياسي

الشعبة: حقوق التخصص: القانون الجنائي

من إعداد الطالب(ة):

مسعود شهيرة

تحت إشراف الأستاذ(ة):

بلحنافي فاطمة

الأستاذ(ة) .رئيسا

الأستاذ(ة) مشرفا مقررا

الأستاذ(ة) .مناقشا

السنة الجامعية : 2021/2020

نقشت في 2021/07/14

شكر و عرفان

بسم الله الرحمان الرحيم :

" رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَ عَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِين "

سورة النمل اية 19 .

قال رسول الله صلى الله عليه و سلم " و من لا يشكر الناس لا يشكر الله " .

نشكر الله عز و جل على أنه هدانا بالقوة لإتمام هذا العمل المتواضع .

كما أتقدم بالشكر الجزيل إلى الأستاذة " بلحنافي فاطمة " على نصائحها و توجيهاتها التي أنارت دربي ، و التي لم تبخل علي بالمراجعة و المعلومات القيمة .

كما لا يسعدني إلا أن أتقدم بالشكر و العرفان لكل من ساعدني في هذا العمل بدءا بكل إنسان علمني في هذه الدنيا على مدار حياتي الدراسية خاصة أساتذتي على مستوى كل الأطوار الدراسية وصولا إلى الطور الجامعي .

الإهداء

الحمد و الشكر لله رب العرش العظيم الذي وفقني في إعداد هذه المذكرة و أزكى الصلاة و سلام على صفيه و خليله خاتم الأنبياء و الرسل .

أهدي ثمرة جهدي ،

إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم .... إلى قرة عيني و صديق أحلامي و رجل حياتي

أبـــي

إلى الجوهرة المصونة و اللؤلؤة المكنونة .... إلى من أرضعتني الحب و الحنان ... إلى لذة عيشي و جنة حياتي .... إلى أغلى الحبايب

أمـــــي

إلى القلوب الطاهرة الرقيقة و النفوس البريئة إلى رياحين حياتي أخوتي : **توفيق ، صورية ، تواتية ، حسيبة ، خيرة .**

المقدمة

مقدمـة

بقدر ما يحققه تطور التقنيات من فوائد كبيرة في مجال الرقي و التقدم الانساني ، فإنها في الوقت ذاته مهدت السبيل الى بروز اشكال جديدة من الجرائم ، لاسيما بعد أن تم ربط العالمية للأنترنيت حيث وجد المجرم تقنية عالمية و أساليب حديثة الحاسب الالي بالشبكة تساعده في ارتكاب العديد من الجرائم دون أن يترك أثرا واضحا لتلك الجريمة ، و المجرم يستطيع باستغلال هذه المخترعات العالمية و الأجهزة الإلكترونية و ما تقدمه من وسائل مقدمة في ارتكاب العديد من الجرائم من خلال الامكانيات الهائلة لهذه التقنيات ، و يصل إلى أي مكان يرغب فيه ، و إلى أعداد بشرية هائلة في نفس الوقت ، فلا مكان و لا زمان يستطيع وضع حدود لهذه الشبكة .

و لقد تطورت الظاهرة الإجرامية في الآونة الاخيرة تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها ، و الذي يتمثل في استعمال آخر ما توصل اليه العلم و تطويعه في خدمة الجريمة ، فقد أصبحت المعلومات تجوب في سرعة كبيرة فشبكة المعلومات التي تصل بين الحاسبات الالية في مختلف انحاء العالم جعلت اعتماد المعلومات المالية بشكل أساسي على هذه الحاسبات الالية التي أصبحت مستودع أسرار الأشخاص ، سواء تلك المتعلقة بأسرارهم الخاصة أو أموالهم أو نشاطهم الاقتصادي .

كما تتميز الجرائم الالكترونية بصعوبة متابعتها حيث أنها في الغالب لا تترك أثرا فليست هنالك أموال أو ممتلكات مفقودة ، و إنما هي أرقام تتغير في السجلات ، و معظم الجرائم

الالكترونية ربما يتم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها ، كما أن الجرائم الالكترونية تتميز بالدقة و التعقيد التقني ، و غالبا من يرتكب تلك الجرائم يتمتع بالذكاء.

و تكمن أهمية دراسة هذا الموضوع فيما يكتسبه من جد و غموض ، أمام انتشار ظاهرة الجريمة الإلكترونية ، أو جرائم الأنترنيت ، مقابل الفراغ القانوني خاصة في التشريع الوطني موازاة بما تعرفه مقاهي الانترنيت من إقبال واسع و إدمان شبابنا على شاشات الكمبيوتر ، و ربط أغلب بيوتنا و إداراتنا بالشبكة العنكبوتية ، مما يدفعنا للبحث عن الأسلوب الأمثل للتعامل مع هذه الظاهرة بسبب ما خلفت من حيرة لدى رجال القانون لعدم امكانية تطبيق النصوص القانونية السارية لعدم تناسبها مع طبيعة الجريمة الإلكترونية التي تغزو مجتمعنا بمختلف فئاته ، رغم أن ملفات المتابعة القضائية لها تعد شبه معدومة مما يتطلب تبيين نصوص تشريعية لمكافحة هذه الجريمة التي أرهقت كل الميادين و الأسس القانونية كما تكمن أهميته في اتساع مجاله و كلما تناولنا فكرة منه بقي الكثير منه يحتاج للتوضيح لأنه موضوع جديد من جهة ، و يحتاج لإيجاد إجراءات جديدة لمتابعته من جهة أخرى.

و المشرع الجزائري كغيره من التشريعات المقارنة نظم الجريمة الإلكترونية ووضع الآيات المختصة بالمتابعة للحد منها و تهدف إلى تطوير التنظيم القضائي الرامي إلى مكافحتها و ردع مرتكبيها لحماية الاقتصاد الوطني على وجه الخصوص ، و عليه فالإشكال الاساسي المطروح يتمثل في: تحديد ماهية الجريمة الإلكترونية ، والتي تتفرع عنها مجموعة من تساؤلات تتمثل في: ماهي أركان مكونه لهذا النوع من الجرائم ؟ فيما تتمثل خصائصها ؟

و ماهي طرق مكافحة الجريمة الالكترونية في القانون الجزائري ؟

و بما أن دراستي للموضوع مقيدة بعدد من الصفحات فتناوله سيكون بشكل ضيق ، مع محاولة الإلمام بأكبر قدر من المعلومات لتقريب الفكرة لذهن كل من يقرأ هذه المذكرة لإزالة اللبس بالإجابة عن الإشكالات المطروحة من خلال التطرق إلى تعريف الجريمة الإلكترونية ، و دوافع ارتكابها ، خصائصها و أنواعها ، في الفصل الأول ، ليصل بنا الحديث في الفصل الثاني عن مكافحة الجريمة الإلكترونية في التشريع الجزائري ، من خلال نصوص جرائم الأموال و نصوص الملكية الفكرية و النصوص المستحدثة ، لتكون مذكرتنا هذه تطبيقية أكثر منها نظرية .

الفصل الأول

ماهية الجريمة الإلكترونية

الفصل الأول : ما هي الجريمة الالكترونية

لقد شهد العالم في الآونة الاخيرة تطورا ملحوظا في مجال التقنية , مما نتج عنه استعمال الحاسب الألي و شبكة الانترنيت في جميع الميادين , لكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة , الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال , و هو ما يعرف بالجريمة الالكترونية , و نظرا لحادثة هذه الجريمة , فقد اختلف الفقهاء في وضع تعريف موحد لها , كما اتسمت بمجموعة من الخصائص و عرفت نوعا جديدا من المجرمين لهم عدة دوافع لارتكاب هذه الجريمة و سأحاول التطرق في هذا الفصل الى مفهوم الجريمة الالكترونية و أركانها في المبحث الأول و بيان خصائص و أنواع الجريمة الإلكترونية في القانون الجزائري من خلال المبحث الثاني .

❖ المبحث الأول : مفهوم الجريمة الالكترونية

من خلال هذا المبحث سأحاول التعرض إلى التعاريف المختلفة للجريمة الالكترونية و كذا الأركان التي ترتكز عليها و بيان الدوافع المؤيدة لارتكابها نظرا لطبيعتها الخاصة باعتبارها تقع في العالم الافتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس , و ذلك من خلال المطلبين المواليين :

○ المطلب الأول: تعريف الجريمة الالكترونية و أركانها

لم يتفق الفقه الجنائي على ايجاد تسمية موحدة للجريمة الالكترونية , فهناك عدة تسميات لها منها الجريمة المعلوماتية , جرائم إساءة استخدام , تكنولوجيا المعلومات و الاتصال , جرائم الكمبيوتر و الانترنيت، الجرائم المستحدثة [1]، الجريمة الناعمة ، إجرام ذوي الياقات البيضاء ، و تجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الالي و ميدان جرائم الانترنيت ، فبينما تتحقق الأولى باعتداء على مجموعة الأدوات المكونة للحاسب الالي و برامجه و المعلومات المخزنة به , فإن جرائم الانترنيت تتحقق بنقل المعلومات و البيانات بين أجهزة الحاسب الالي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميادين (الحوسبة و الاتصالات) و ظهور مصطلح [2] **Cybercrime** .

الفرع الاول : تعريف الجريمة الالكترونية

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الالكترونية و يعود ذلك الاختلاف حول تحدي نطاق هذه الجريمة ، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق و البعض الاخر ينظر إليها بمفهوم واسع.

أولا الاتجاه المضيق من تعريف الجريمة الالكترونية :

[1] – عادل يوسف عبد النبي الشكري ، بحث بعنوان الجريمة الإلكترونية و أزمة الشرعية الجزائرية ، جامعة الكوفة ، 2006 ، ص 112.

[2] – مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، مجلة علمية ، 2012 ، العدد 21 ، ص 08 .

يرى انصار هذا الاتجاه الجريمة الالكترونية بأنها" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الالية بقدر كبير لازم لارتكابه من ناحية ، و لملاحظته و تحقيقه من ناحية اخرى " .

يرى الأستاذ **Mass** أن المقصود بالجريمة الإلكترونية هو الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح [1].

و يرى الأستاذ **Rosenblatt** بأن الجريمة الالكترونية هي " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسب أو تغييرها أو حذفها أو التي تحول عن طريقه "[2] .

الفقيه الالماني **Tie de mann** يرى أن " كل أشكال السلوك غير المشروع و الضار بالمجتمع الذي يرتكب باستخدام الحاسب ، فهو يرتكز في تعريفه على وسيلة ارتكاب الجريمة " .

يعرفها مكتب تقييم التقنية في الولايات المتحدة الامريكية من خلال تعريف جريمة الحاسب **Cybercrimme** أنها : الجرائم التي تلعب فيها بيانات الكمبيوتر و البرامج المعلوماتية دورا رئيسيا ، و ارتكز كذلك في تعريفه على الوسيلة المرتكبة بها الجريمة.

تعريف **David Thompson** لجريمة الحاسب بأنها : أي جريمة يكون متطلبا لاقترافها

[1] – نهلة عبد القادر المومني ، الجرائم المعلوماتية ، ماجيستير القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع 1429 هـ – 2008 ، الطبعة الأولى ، الإصدار الأول ، 2008 ، ص 20.

[2] – حمزة بن عقون ، السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية ، تخصص علم الإجرام و العقاب ، جامعة باتنة ، 2019 ، ص 213 .

أن تتوافر لدى مرتكبها معرفة بتقنية الحاسب ، و هذا الفقيه ارتكز في تعريفه على توافر المعرفة بتقنية المعلومات [1].

حسب هذا التعريف فإن هذه الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم ، ويرى الأستاذ **باركار** أن الجريمة الإلكترونية هي كل فعل إجرامي أيا كانت صلته بالمعلوماتية ، ينشأ من خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل .[2]

ثانيا الاتجاه الموسع من تعريف الجريمة الإلكترونية :

هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية يعرفونها كالآتي : هي كل فعل أو امتناع عمدي ينشأ من الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال أو الأشياء المعنوية ، يرى الخبير الأمريكي **Parker** مفهوما واسعا للجريمة المعلوماتية والمتمثل في كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، وينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل ، كما يعرف الأستاذ **Vivant** و **Hestonc** الجريمة الإلكترونية بأنها مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب .[3]

[1] – سامي علي حامد عباد ، الجريمة المعلوماتية و إجرام الأنترنيت ، ماجستير في القانون ، دار الفكر الجامعي ، 30 شارع سوتر ، الإسكندرية 2008 ، ص 38 – ص 40 .

[2] – محمد العريان ، الجرائم المعلوماتية ، كلية الحقوق ، جامعة الاسكندرية ، دار الجامعة الجديدة للنشر ،الاسكندرية ، 2004 ، ص 43.

[3] – نهلة عبد القادر المومني ، المرجع نفسه ، ص 49.

جرائم الكمبيوتر هو مصطلح أشمل من المصطلح السابق ويقدم فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء كان أداة الجريمة أو كان هدف الجريمة و يدخل من ضمنها الاعتداء على الشبكات المحلية الخاصة بالهيئات والمنشآت الخاصة و العامة .[1]

الجريمة الإلكترونية هي ببساطة استخدام التقنية الرقمية لإخافة الآخرين.

أما البعض من الفقهاء يعرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الالي الرقمي وشبكة للأنترنت) بطريقة مباشرة أو غير مباشرة ، كوسيلة لتنفيذ الفعل الاجرامي المستهدف .[2]

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه ، لأن جهاز الحاسوب الالي قد لا يعدو أن يكون مجالا تقليديا في بعض الجرائم ، كسرقة الحاسب الالي نفسه ، أو الاقراص الممغنطة ، أو الاسطوانات الممغنطة على سبيل المثال ، ومن ثم لا يمكن اعطاء وصف الجريمة الالكترونية على سلوك الفاعل بمجرد أن الحاسب الالي أو أي من مكوناته كانوا محلا للجريمة ، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الالي ، ولا يكون أمام جريمة الكترونية ، كمن يقوم بالاتصال بواسطة حاسب الي وبشركائه في ارتكاب جريمة السطو على بنك .

[1] – أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنيت ، دار المطبوعات الجامعية ، أمام كلية الحقوق ت 4126869 الاسكندرية ، 2009 ، ص 106– ص 107.

[2] – صغير يوسف ، الجريمة المرتكبة عبر الأنترنيت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولود معمري تيزي وزو ، 06 / 03 / 2013 ، ص 09 ، نقلا عن كحلوش علي ، جرائم الحاسوب و أساليب مواجهتها ،مجلة صادرة عن مديرية الأمن الوطني ، العدد 84 ، 2007 ، ص 51 .

أما بالنسبة للتعريف القانوني للجريمة الالكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، وعرفها بموجب أحكام المادة **02** من القانون **04/09** [1] على أنها " جرائم المساس بالأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات ، وأي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية " .

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة ، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الالية للمعطيات ، كما بينها في القانون العقوبات [2] من المادة **394** مكرر إلى **394** مكرر **07** ، وترك المجال واسع لأي جريمة اخرى ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

و حسب المشرع الجزائري فإن قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة ، أو يسهل ارتكابها عن طريق منظومة معلوماتية ، أو نظام الاتصالات الإلكترونية ، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم كما أن التعريف تضمن تكرار [3] ، كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية و من أمثلة

[1] – القانون رقم 09–04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، جريدة رسمية العدد 47.

[2] – القانون رقم 04 – 15 ، الصادر في 10 نوفمبر2004 ، معدل و متمم للأمر رقم 156/66 ، الصادر في جوان 1966 ، المتضمن قانون ع.ج.ر ، العدد 71.

[3] – سوير سفيان ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية و علم الإجرام ، جامعة أبو بكر بلقايد ، تلمسان ، 2010 – 2011 ، ص من 14 إلى 16.

الجريمة الإلكترونية المرتكبة في الجزائر ، تسرب أسئلة الباكالوريا لسنة 2016 ، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية .[1]

الفرع الثاني: أركان الجريمة الإلكترونية

تتكون الجريمة الإلكترونية من ركنين الركن المادي و الركن المعنوي و إذا تخلف أحدهما اعتبر الفعل غير مجرم قانونا.

أ) الركن المادي للجريمة الإلكترونية : يتكون الركن المادي من الجريمة الإلكترونية من السلوك الإجرامي و النتيجة و العلاقة السببية مع العلم أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقق نتيجتها ، مثل إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة فرغم عدم تحقق النتيجة إلا أنه لا مناص من معاقبة الشخص ، و يتخذ الركن المادة عدة صور حسب كل جريمة .

* **جريمة الغش المعلوماتي** : الركن المادي فيها هو تغيير الحقيقة في مستند مادي أو محرر رسمي ، و لكن المستند هنا ليس مستند مادي يدخل ضمن أدلة الإثبات ، بل هي عبارة عن تسجيلات الكترونية أو محررات الكترونية.

[1] – جارية سليماني ، موقع العربي الجديد ، تاريخ الدخول 2017/02/09 الساعة 20:30
http//www.alaraby.co.uk/media news

***جريمة الإرهاب الإلكتروني و المواقع الإباحية و مواقع القمار** : الركن المادي في هذه الجرائم هو إطلاق المواقع التي تحث إما على الانضمام إلى الجماعات الإرهابية ، كما تورد كيفية صنع القنابل اليدوية .

- ✓ أما المواقع الإباحية فتزود مواقعها بالصور، و أفكار الشذوذ الجنسي ، و هنالك مواقع تنشر فكرة الانتحار ، أو تشويه صورة الإسلام .[1]
- ✓ أما مواقع القمار فهي لغسيل الأموال فالركن المادي هنا سلوك المجرم المعلوماتي في تزويد المواقع بالمعلومات اللازمة للانحراف أو القتل و هذا المجرم أقل من المخترق أو المتسلل ، هذا فيما يخص السلوك الإجرامي أما النتيجة فهي الأثر المادي المتمثل في انحراف المجتمع و تدمير الأخلاق و المعتقدات و ظهور عادات غريبة على المجتمع زيادة إلى تفشي العنف فتصميم الموقع من طرف المجرم مرتبطة بالتأثيرات الخطيرة التي يتحمل عبؤها المجتمع من انحراف و هذا ما يعرف بالعلاقة السببية .

ب) الركن المعنوي للجريمة الإلكترونية :

بما أنه العلم بعناصر الجريمة و إرادة ارتكابها [2] و بالتالي يتكون هذا الركن من عنصرين هما العلم و الإرادة .

[1] – أ. السمدان – النظام القانوني لحماية برامج الكمبيوتر ، مجلة الحقوق ، الكويت ، العدد 4 ، سنة 1987 ، ص 51 .

[2] – عبد الله سليمان ، شرح قانون العقوبات ، قسم عام الجزء الأول للجريمة ، الجزائر دار ، 2006 ، الطبعة الخامسة ، ص 43 .

فالعلم هو إدراك الأمور على نحو مطابق للواقع يسبق الإرادة . أما الإرادة ، فهي اتجاه لتحقيق السلوك الإجرامي .

و يتخذ القصد الجنائي عدة صور منها ، القصد العام و القصد الخاص .

القصد الجنائي العام ، هو الهدف الفوري و المباشر للسلوك الإجرامي و ينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها .

القصد الجنائي الخاص ، هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم بطرحنا السؤال : ما هو الهدف الذي يريد الجاني تحقيقه من الجريمة ؟

فأي قصد يجب توافره في الجريمة الإلكترونية ؟

إن المجرم الإلكتروني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة و بالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون و أنهم قد تسللوا صدفة ، فلا انتفاء للعلم كركن للقصد الجنائي ، كان يجب عليهم أن يتراجعوا بمجرد دخولهم و لا يستمروا في الاطلاع عل أسرار الأفراد و المؤسسات [1] لأن جميع المجرمين و الأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية و معرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية .

[1] - أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه الجزائر، ط1، 2007،، ص 124.

فالقصد الجنائي متوافر في جميع الجرائم الإلكترونية دون استثناء و لكن هذا لا يمنع أن هناك بعض الجرائم الإلكترونية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الإنترنيت .

أما جرائم نشر الفيروسات على الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة و في جميع الحالات المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص .

- **المطلب الثاني : دوافع ارتكاب الجريمة الإلكترونية**

إن الجريمة التقليدية و المجرم التقليدي يختلفان تماما عن الجريمة الإلكترونية و المجرم الإلكتروني ، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب و العوامل التي تدفع إلى ارتكاب الفعل غير المشروع ، فالدافع (الباحث) ، الغرض ، الغاية ، مفاهيم لكل منها دلالته في القانون الجنائي ، تتصل بما يعرف بالقصد الخاص في الجريمة ، و هي مسألة تثير جدلا فقهيا و قضائيا واسعا ، ذلك أن القاعدة القضائية تقرر أن الباحث ليس عنصرا من عناصر القصد الجرمي ، و أن الباحث لا أثر له في وجود القصد الجنائي ، و إذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب ، فإنها من حيث الدلالة لا تتمايز ، فالدافع هو العامل المحرك للإرادة ، و الذي يوجه السلوك الإجرامي كالمحبة و الشفقة و البغضاء و الانتقام ، و هو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة ، و هو يختلف من جريمة إلى أخرى ، أما الغرض فهو الهدف الفوري

المباشر للسلوك الإجرامي ، و يتمثل بتحقيق النتيجة التي أصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات ، و أما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام ، أو سلب مال المجني عليه في جريمة القتل .

و بالنسبة للجريمة الإلكترونية فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم [1] ، و أهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين :

الفرع الأول : الدوافع الشخصية لارتكاب الجريمة الإلكترونية :

تصنف هذه الدوافع إلى دوافع مادية ، و أخرى ذهنية ، و ذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية ، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني و دفعه لارتكاب جريمته ، و هذا ما سنتطرق إليه .

أ) الدوافع المادية :

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية ، و ذلك لأن الربح الكبير و الممكن تحقيقه من خلالها يدفع المجرم الإلكتروني تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية و يستغل الفرص و يسعى إلى الاحتراف حتى يحقق أعلى المكاسب و بأقل جهد دون أن يترك وراءه ، فيعتمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الألية للبنوك و المؤسسات المالية إن كان أحد موظفيها ،

[1] – حمزة بن عقون ، المرجع نفسه ، ص 46 – ص 47 .

أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية ، فيعمل على استغلالها و برمجتها لتحويل مبالغ مالية لحسابه ، أو لحساب شركائه ، أو لحساب من يعمل لحسابهم إن كان خارج المؤسسة ، كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو على المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب ، و قد أشارت في هذا الاطار مجلة " ***SECURITE INFORMATIQUE*** " و هي مجلة متخصصة في الأمن المعلوماتي ، أن **43** % من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال ، و **23**% من أجل سرقة معلومات ، و **19** % أفعال أخلاق **15** ، % الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية .

و في حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق أرباح كبيرة في وقت قصير ، و يمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر ، أين أجريت هذه الدراسة بمشاركة **538** مؤسسة أمريكية تضم وكالات حكومية ، و بنوك و مؤسسات صحية و جامعات و التي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية ، حيث تبين أن **85** % من

المشاركين في الدراسة تعرضوا لاختراقات بالنسبة لأنظمة المعلوماتية ، و أن **64** % لحقت بهم خسائر مادية جراء هذه الاعتداءات . [1]

ب) الدوافع الذهنية لارتكاب الجريمة :

تتمثل هذه الدوافع في المتعة و التحدي و الرغبة في فهم النظام المعلوماتي ، و اثبات الذات ، و قد تكون هذه الدوافع مجرد شغف بالإلكترونيات و الرغبة في التحدي و قهر النظام و التفوق على تعقيد وسائل التقنية ، فاختراق الأنظمة الإلكترونية و كسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها و تسلية تغطي أوقات فراغه ، و على صعيد آخر قد يكون اقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية و التغلب عليها ، إذ يميل هذا المجرم إلى اظهار تفوقه على وسائل التكنولوجيا الحديثة ، و في الغالب لا تكون لديهم دوافع حاقدة أو تخريبية ، و إنما ينطلق من دافع التحدي و إثبات المقدرة . [2]

[1] – سعيدان نعيم ، أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، 2012 – 2013 ، ص 60 – ص 61 ، نقلا عن نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة (2) ، 2010 ، ص 90 ، و نقلا عن ضاح محمود الحمود و نشأت مفقي المجالي ، جرائم الأنترنيت ، دار المنار للنشر و التوزيع ، 2005 ، ص 31.

[2] – سعيداني نعيم ، المرجع نفسه ، ص 61 – ص 62 .

الفرع الثاني : الدوافع الموضوعية لارتكاب الجريمة الإلكترونية :

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعه على اقتراف الإجرام الإلكتروني و لا يسعى في ذلك حينها لا للمتعة و التسلية و لا لكسب المال . و يمكن إبراز أهم الدوافع كالآتي :

دافع الانتقام و الحاق الضرر برب العمل :

و يتوفر هذا الدافع نتيجة فصل الموظف من عمله ، أو تخطيه في الحوافز أو الترقية ، فهذه الأمور تجعله يقدم على ارتكاب جريمته [1] ، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الحريمة ، و ذلك أنه غالبا ما يصدر عن الشخص الذي يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها ، و غالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية و من ذلك الشعور بالحرمان من بعض الحقوق المهنية ، أو الطرد من الوظيفة ، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب العمل .

و مثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر ، و قد تحقق هذا الأمر في التاريخ المحدد من طرفه .

[1]. – صغير يوسف ، المرجع نفسه ، ص 42 .

دافع التعاون و التواطؤ:

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية ، و غالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية ، أين يقوم بالجانب الفني من المشروع الإجرامي ، و آخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب و تحويل المكاسب المادية ، و عادة ما يمارسون التلصص على الأنظمة و تبادل المعلومات بصفة منظمة حول أنشطتهم .[1]

و إذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية ، مع ذلك فهي ليست ثابتة و معتمدة لدى الفقهاء و الباحثين لأن السلوك الإجرامي و الدوافع لارتكاب الجريمة الإلكترونية قد تتغير و تتحول بسرعة من حالة العبث و محاولة التحدي و التغلب على الأنظمة ، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز و الحصول على الأموال ، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد ، إذ نجد في كل جريمة جديدة دوافع جديدة ، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة .[2]

[1]. – سعيداني نعيم ، المرجع نفسه ، ص 62 .

[2]. – سعيداني نعيم ، المرجع نفسه ، ص 62 .

❖ المبحث الثاني : خصائص و أنواع الحريمة الإلكترونية في القانون الجزائري

بعد التطرق لمفهوم الحريمة الإلكترونية و بيان الدوافع المؤدية لارتكابها من طرف المجرم الإلكتروني ، أحاول من خلال هذا المبحث بيان خصائص هذه الجريمة و ذلك بالتطرق للبيانات الخاصة بالجريمة الإلكترونية و السمات الخاصة بالمحرم الإلكتروني و تنوع هذه الجريمة في التشريع الجزائري بحسب ما إذا ارتكبت باستخدام النظام المعلوماتي ، أو كانت موجهة ضده ، و هذا ما يتم بيانه في المطلبين الآتيين :

○ المطلب الأول : خصائص الجريمة الإلكترونية :

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية و ذلك نتيجة ارتباطها بتقنية المعلومات و الحاسب الآلي مع ما يتمتع به من تقنية عالمية ، و قد اضفت هذه الحقيقة مع هذا النوع من الجرائم عدد من السمات و الحقائق ، و التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي ، و قد كان لظهور شبكة المعلومات و تطورها إلى الصورة التي أصبحت عليها الأن ما يعرف بالأنترنيت أثره في إعطاء شكل جديد للجريمة المعلوماتية .[1]

[1] – نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية ، دراسة نظرية و تطبيقية ، بيروت ، منشورات الحلبي الحقوقية ، 2005 ، الطبعة الأولى ،ص 29 .

الفرع الأول : السمات الخاصة بالجريمة الإلكترونية :

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية من عدة جوانب ، بمجموعة من الخصائص أو السمات ، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها ، و تتلخص هذه السمات في فيما يلي :

- ✓ خفاء الجريمة و سرعة في التطور في ارتكابها ،حيث تفسر بأنها خفية و مستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الاتصالات ، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة ، مثلا عند ارسال الفيروسات المدمرة و سرقة الأموال و البيانات الخاصة أو اتلافها ، و التجسس عليها و سرقة المكالمات و غيرها [1] و قد تتم في ثانية أو جزء من الثانية في بعض الجرائم .
- ✓ ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية ، أجهزة و معدات و تجهيزات الحاسب الألي ، بمعنى تتم بواسطة المكونات المادية للحاسوب (**Hardware**) ، و مكوناته البرمجيات (**Software**).
- ✓ يقوم بها المجرم ذو طبيعة خاصة و إمكانات خاصة (علمية معلوماتية) ، يستخدم في ارتكاب جريمته الموارد المعرفية و الأساليب الاحترافية .

[1] – صغير يوسف ، الجريمة المرتكبة عبر الأنترنيت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولود معمري ، تيزي وزو ، 2013/03/06 ، ص 09 ، نقلا عن كحلوش علي ، جرائم الحاسوب و أساليب مواجهتها ، مجلة صادرة عن مديرية الأمن الوطني ، العدد 84 ، 2007 ، ص 51.

✓صعوبة الحصول على دليل مادي في مثل هذه الجرائم ، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر[1] . و لعل صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها ، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثارا تدل عليهم .[2]

✓الجريمة الإلكترونية تستلزم طرقا خاصة مستحدثة للإثبات ، قوامها التعليم و التدريب المتخصص المستمر لعلوم الحاسب الآلي ، لذا فإنها تقتضي وجود رجل شرطة إلكتروني ، و محقق إلكتروني ، و قاضي إلكتروني ، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة و تعقب الجناة فيها و محاكمتهم ، و عليه فإن الاستعانة بالخبراء تصبح حتمية لكشف و تحليل و تفسير الدليل الجنائي ، الذي يثبت البراءة أو الإدانة ، هذه الجريمة لا يحدها مكان ، فهي عالمية إذ يمكن عن طريق الآلي أو في هاتف نقال لشخص في الصين مثلا أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ، ضد شخص طبيعي أو معنوي في الو.م.أ أو العكس .

✓ تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات و مؤسسات ، لتجنب الإساءة للسمعة و الرغبة في عدم زعزعة ثقة العملاء ، ففي إحدى الوقائع

[1] – عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماوي ، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية (دراسة مقارنة) ، المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي ، الرياض ، 2007 ، ص 10 .

[2] – موسى مسعود أرحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، ورقة مقدمة لدى المؤتمر المغاربي الأول حول المعلوماتية و القانون الذي تنظمه أكادمية الدراسات العليا ، طرابلس ،28-2009/10/29 ، ص 03 .

تعرض أحد البنوك ، و هو بنك " ***Marchant Bank City*** " في بريطانيا لسرقة ثمانية مليون جنيه إسترليني من إحدى أرصدته إلى رقم في سويسرا ، و تم ضبط الفاعل متلبسا ، يسحب المبلغ المسروق و بدلا من محاكمته ، قام البنك بدفع مليون جنيه إسترليني له ، بشرط التزام الفاعل بعدم الإعلام عن جريمته ، و إعلام البنك عن الألية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي .

- ✓ غالبا ما تكون الخسار الناجمة عنها فادحة للمجني عليه. [1]
- ✓ ذاتية الجريم الإلكترونية تبرز بوضوح في أسلوب ارتكابها و طريقتها ، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد تكون في صورة الخلع أو الكسر ، و تقليد المفاتيح كما هو الحال في جريمة السرقة ، و تحتاج كذلك إلى وجود شبكة المعلومات الدولية – الأنترنيت – مع وجود مجرم يوظف خبراته و قدراته على التعامل مع الشبكة ، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير للتغرير بالقاصرين ، كل ذلك دون الحاجة لسفك الدماء .
- ✓ الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص على ارتكابها اضرارا بالمجني عليه ، و غالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات

[1] – عبد الناصر محمد محمود فرغلي ، محمد عبيد سعيد المسماوي ، المرجع نفسه ، ص 10– ص 11 .

الحاسوب و الأنترنيت يقوم بالجانب الفني من المشروع الإجرامي ، و شخص اخر من المحيط أو من خارج المؤسسة المجني عليها ، لتغطية عملية التلاعب و تحويل المكاسب . [1]

الفرع الثاني : السمات الخاصة بالمجرم الإلكتروني :

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الالي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب ، و إنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين .

و لقد اختلف الباحثون في تحديد هذه السمات [2] ، و يعد الأستاذ **PARKER** واحد من أهم الباحثين الذين عالجوا الجريمة المعلوماتية بالدراسة بصفة عامة و المجرم المعلوماتي بصفة خاصة ، و مع ذلك يعد المجرم المعلوماتي مجرما لارتكابه فعل اجرامي يتطلب توقيع العقاب عليه ، و كل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء ، و إن كانت في رأيه لا تتطابق معها .

فالمحرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه يكون على درجة من العلم و المعرفة . [3]

---

[1] – سمية مزغيش جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر ، بسكرة ، 2013-2014 ، ص 18.

[2] – نائلة فريد عادل قورة ، المرجع السابق ، ص 54 .

[3] – ليس من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء، انظر، suthreland (Eduin H) « whithe collar criminality » Gers (Gilbert) in chate collar criminal the offender in business the professions atherton press 1968.

و يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في كون أن الفاعل في الحالتين يبرر جريمته كونه لا ينظر إلى سلوكه ، باعتباره جريمة أو فعل يتنافى مع الأخلاق .

و يتميز المجرم المعلوماتي بإضافة إلى ذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ **PARKER** بكلمة **S.K.R.A.M** و هي تعني : المهارة **Skills** ، المعرفة ***Knowledge*** ، الوسيلة ***Resources*** ، السلطة ***Anthority*** ، و أخيرا الباعث ***Motives*** .[1]

وتعد **المهارة** : المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي ، و التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال ، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات ، أو بمجرد التفاعل الاجتماعي مع الأخرين .

إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال ، بل إن الواقع العلمي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال .

أما **المعرفة** : فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها بكامل ملابستها ومدى إمكانية نجاحها أو فشلها ، إذ أن المجرم المعلوماتي باستطاعته أن يكون له تصورا كاملا لجريمته ، كون أن مسرح الجريمة المعلوماتية هو النظام

[1] -Parker (DonnB) figding camputer crime A new framework for protecting information 1988 / p 114.

المعلوماتي [1] ، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها و ذلك قبل تنفيذ جريمته .

أما **الوسيلة** : فيراد بها الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية في أغلب الحالات تتميز نسبيا بالبساطة و بسهولة الحصول عليها ، كما أنه نظرا لمهارته و قدرته يستطيع حتى ابتكارها ، إذ أن الواقع أثبت أنه كلما كان النظام المعلوماتي غير مألوف و يتميز بالخصوصية كانت الوسائل المتطلبة لارتكاب الجريمة أكثر صعوبة .

أما **السلطة** : فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي و التي تمكنه من ارتكاب جريمته ، و هذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي و التي تعطي للفاعل مزايا متعددة مثل فتح الملفات و محو تعديل محتوياتها ، مجرد قراءتها منها أو كتابتها .

وقد تتمثل هذه السلطة في حق استعمال الحاسب الألي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية لبعض الإدارات مثلا .

وقد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر .

[1]. – نائلة عادل محمد فريد قورة ، المرجع نفسه ، ص 57 .

و أخيرا يأتي **الباعث** لارتكاب الجريمة ، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى ، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث و بعد عرضنا لدوافع ارتكاب الجريمة المعلوماتية نتطرق في المطلب الموالي حتى نضبط مفهومها أكثر .

- **المطلب الثاني : انواع الجرائم الالكترونية في القانون الجزائري**

يمكن تصور الجريمة الالكترونية من زاويتين بحسب اختلاف الزاوية التي ينظر منها إزالة الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي فمن ناحية قد يكون هذا الأخير نفسه موضوع الجريمة الالكترونية ، ومن ناحية أخرى قد يكون النظام المعلوماتي هو أداة الجريمة الالكترونية و وسيلة تنفيذها ، وبالتالي تقسم الجريمة الالكترونية إلى قسمين :

الفرع الأول : الجرائم الواقعة بواسطة النظام المعلوماتي

في هذه الجرائم لا يكون النظام المعلوماتي موضوعا أو محلا للجريمة الالكترونية ولكن الجريمة تقع في هذه الحالة بواسطة النظام المعلوماتي ، أي أنه يستخدم كأداة لارتكاب الجرائم الالكترونية مثل الجرائم التي تقع على الذمة المالية في السرقة والنصب وخيانة الأمانة ، وانتهاك حرمة الحياة الخاصة ، ومن الحالات الواقعية لاستخدام النظام المعلوماتي كوسيلة لارتكاب الجريمة : قيام موظف يعمل في مجال البيانات في أحد البنوك السويسرية الكبرى بالتلاعب في المعلومات المالية الخارجية للمصرف والاستيلاء مع بعض شركائه على مبالغ طائلة ، حيث كان يمنح بحكم عمله كمشتغل ومراجع بيانات ، من وصول بعض الأوامر

التحويل إلى قسم الترميز ليقوم هو بإدخالها إلى الكمبيوتر ، غير أنه بدلا من ادخال القيمة الفعلية إلى الكمبيوتر، لكن أمر التحويل كان يدخل هذه القيمة مضروبة في ألف ، وقد تمكن بهذه الطريقة من الاستيلاء على **700,000** يورو من أموال البنك . [1]

الفرع الثاني : الجرائم الواقعة على النظام المعلوماتي

وهي الجرائم التي يكون فيها النظام المعلوماتي محلا وموضوعا للجريمة الالكترونية وقد يوجه الاعتداء ضد المكونات المادية للنظام المعلوماتي كالأجهزة والمعدات [2]، ولا تثار ثمة أي إشكالية في تطبيق النصوص التقليدية عليها نظرا للطابع الخاص لهذه المكونات المعنوية .

وباعتبار جرائم الاعتداء ضد البرامج أخطر الاعتداءات المكونات المعنوية للنظام المعلوماتي فلا بد من الإقرار بوجوب الحماية الجزائية لبرامج الحاسوب الآلي ولقد بلغت الخسائر الناجمة عن الاعتداء على البرامج **21** مليار يورو بنسبة **20 %** من الخسائر ، وذلك سنة **1993** وفق احصائيات فريق الأمن المعلوماتي الفرنسي كما وصلت نسبة البرامج المزيفة إلى **95%** من مجموعة البرامج المتداولة في الجزائر كما صرحت ممثلة شركة ميكروسوفت ، وقدرت خسائرها بـ **40** مليون دولار سنة **2000** .[3]

هذا وتجدر الإشارة إلى اتفاقية بودابست لعام **2001** بشان جرائم الكمبيوتر والإنترنت أوجدت تقسيما جديدا نسبيا ، فقد تضمنت أربع طوائف لجرائم الكمبيوتر والانترنت :

---

[1]– ز. ط. شحاده، الاعمال الجرميه التي تستهدف الأنظمة المعلوماتية، مطبعة صادر، 2006 ، ص 108.

[2]– أحمد خليفة الملط ، الجرائم المعلوماتية ، الاسكندرية ، دار الفكر الجامعي ، 2006 ، الطبعة الثانية ، ص 72 .

[3] Rose (philippe) , Op-cit , p 58.59 .

الأولى : تتعلق بالجرائم التي تستهدف السرية والسلامة للمعطيات والنظم وتضم الدخول غير مصرح به والاعتراض غير القانوني وتدمير المعطيات ، وإساءة استخدام الأجهزة .

الثانية : تتعلق بالجرائم المرتبطة بالكمبيوتر وتضم التزوير والاحتيال .

الثالثة : تتعلق بالجرائم المرتبطة بالأفعال الإباحية و اللاأخلاقية .

الرابعة : تتعلق بالجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة .

الفصل الثاني

مكافحة الجريمة

الإلكترونية في

القانون الجزائري

الفصل الثاني : مكافحة الجريمة الإلكترونية في القانون الجزائري

بعد التطرق إلى ماهية الجريمة الإلكترونية ، من خلال تعريفها وأنواعها والدوافع المؤدية لارتكابها . أتعرض في هذا الفصل إلى بيان كيفية التصدي للجريمة الإلكترونية من طرف المشرع الجزائري ، وذلك بتوفير الحماية الموضوعية والإجرائية للنظام المعلوماتي ، من خلال مختلف التشريعات التقليدية أو المستحدثة التي تناولت الجريمة الإلكترونية ، وهذا ما سيتم توضيحه في المبحثين الآتيين .

❖ المبحث الأول : الحماية الموضوعية للنظام المعلوماتي

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى ، استوجب ذلك توفير حماية جنائية خاصة بها ، فالمعلومة أصبحت تقوم ماليا ، وبالتالي تدخل في عتاد الأموال الاقتصادية ، وقد تكون المعلومة شخصية وإفشائها يهدد الحياة الخاصة من جوانب متعددة . ونظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات (شبكة الأنترنت) ، أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها الشبكات ، وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم المستحدثة .[1]

[1] – رصاع فتيحة ، رسالة الماجيستير الحماية الجنائية للمعلومات على شبكة الأنترنيت ، مذكرة لنيل شهادة الماجستير في القانون العام ، جامعة أبو بكر بلقايد ، تلمسان، 2011 – 2012 ، ص 88 .

○ المطلب الأول : الحماية في قانون العقوبات .

إن القانون الجنائي التقليدي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الجديدة ، لاسيما أن نصوصه وضعت في عصر لم يكن الأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن استخدامه [1]، لكن نجد أن المشرع الجزائري تدارك الفراغ القانون في مجال الإجرام المعلوماتي ولو نسبيا ، خصوصا بموجب القانون رقم **04-15** المتضمن تعديل قانون العقوبات ، إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات ، وقد سبق ذكرها في المبحث الثاني من الفصل الأول ، أما العقوبات سأتطرق لها من خلال الفروع الموالية .

الفرع الأول : العقوبات الأصلية

نص المشرع الجزائري في القانون رقم **04-15** على عقوبات أصلية لجريمتي الدخول والبقاء غير المشروعان للنظام المعلوماتي ، وكذا جريمة المساس بمنظومة معلوماتية وفق الآتي :

- **عقوبة الدخول أو البقاء غير المشروعان للنظام :** في حالة الدخول غير المشروع من طرف المجرم الإلكتروني للنظام كله أو جزء منه أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه ، ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب

[1] – سمير سعدون مصطفى ، و اخرون ، الجريمة الالكترونية عبر الانترنيت و سبل مواجهتها ، بحث مقدم بتاريخ 2010/09/20 ، بدون سنة بدون صفحة .

النظام ، تكون العقوبة بالحبس من ثلاثة أشهر إلى سنة وغرامة من **50.000 دج** إلى **100.000 دج** طبقا للمادة **394** مكرر من قانون العقوبات رقم**15/04**.

أما في حالة الدخول أو البقاء ونتج عنه حذف أو تغيير لمعطيات المنظومة ، أو انجر عن هذا الدخول أو البقاء تخريب لنظام اشتعال المنظومة ، فإن العقوبة تضاعف إلى الحبس من ستة أشهر إلى سنتين وغرامة من **50.000 دج** إلى **150.000 دج** ، وذلك وفقا للمادة **394** مكرر من قانون العقوبات السابق الذكر .

- **عقوبة المساس بمنظومة معلوماتية** : نص المشرع الجزائري في المادة **394** مكرر **01** من نفس القانون السابق الذكر على عقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام ، وذلك بالحبس من **06** أشهر إلى **03** سنوات وغرامة من **500.000 دج** إلى **2.000.000 دج** ، وذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية ، وفي حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية تكون العقوبة الحبس من شهرين إلى **03** سنوات وغرامة من **1.000.000 دج** إلى **5.000.000 دج** .[1]

[1] – خثير مسعود ، الحماية الجنائية لبرامج الكمبيوتر ، أساليب و ثغرات ، دار الهدى للنشر و التوزيع ، الجزائر، طبعة 2010 ، ص 99 – ص 100 .

الفرع الثاني : العقوبات المقررة للشخص المعنوي

نص المشرع الجزائري في المادة **51** مكرر من القانون رقم **15/04** على مسألة الشخص المعنوي وذلك وفق شروط : – أن ترتكب إحدى الجرائم المنصوص عليها قانونا – أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي – أن ترتكب الجريمة لحساب الشخص المعنوي . كما نصت المادة **394** مكرر **04** من نفس القانون على العقوبات الواجبة التطبيق على الشخص المعنوي في حالة ارتكابه لأي جريمة اعتداء على نظام المعالجة الألية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي .[1]

- **المطلب الثاني : الحماية في نصوص الملكية الفكرية .**

يقصد بالحقوق الذهنية أو الفكرية ، بأنها حقوق ملكية معنوية ترد على أشياء غير مادية وتقسم إلى ثلاثة أنواع :

- **حقوق الملكية الصناعية** ، ويرد على ابتكارات جديدة تمكن صاحبها من احتكار استغلال ابتكاره قبل الكافة ، وهي أنواع ، حقوق تتعلق بابتكار جديد من حيث الشكل والمظهر الخارجي للمنتجات الرسوم أو التصميمات أو النماذج الصناعية) ، حقوق تتعلق بابتكار جديد من حيث الموضوع كالاختراعات ، حقوق ترد على شارات مميزة تمكن صاحبها من احتكار استغلال علامة تستخدم لتمييز المنشآت كالاسم التجاري.

[1] – خثير مسعود ، المرجع نفسه ، ص 100– ص 111 .

- **حقوق الملكية التجارية** وهي تتضمن ما للتاجر من حق على محله التجاري ، باعتباره مال منقول .
- **حقوق الملكية الأدبية والفنية** ، وتعني ما للمؤلف من حق على إنتاجه الذهني في الآداب والفنون والعلوم .[1]
- وقد اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة ، تتمثل في وجود المصنف أولا ثم عدم مخالفته للنظام العام ثانيا ، وأخرى خاصة وهي وجود ابتكار جديد في المصنف أولا ثم القيام بإيداعه القانوني ثانيا .[2]

الفرع الأول : مدى خضوع معطيات الحاسب الألي لنصوص الملكية الصناعية .

ترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالاختراعات ، ومعنى الاختراع إيجاد شيء لم يكن موجودا من قبل ، أو اكتشاف شيء كان موجودا ولكنه كان مجهولا وغير ملحوظا ثم أبرزه في المجال الصناعي ، فالاختراع الذي لا يؤدي إلى تقدم ملموس في الفن الصناعي لا يستحق براءة عنه .[3] ولما كانت البرامج تتضمن استخدامات جديدة الأفكار أو

[1]– محمد عبد الرحيم الناغي ، الحماية الجنائية للرسوم و النماذج الصناعية (دراسة و مقارنة) ، دار النهضة العربية ، القاهرة ، 2009 ، ص 12– ص13 .

[2] – بن زيطة عبد الهادي ، حماية برامج الحاسوب في التشريع الجزائري ، دار الخلدونية للنشر و التوزيع ، الجزائر ، 2007 ، ط 01 ، ص 37 .

[3] – عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، 2000 ، ط 02 ، ص 51 .

مبادئ علمية لتشغيل الحاسب الآلي ، فهي من هذه الزاوية تصبح قابلة للبراءة .[1] وقد نص عليها الأمر رقم **03-07** الصادر في **2003** ، حيث نصت المادة الثالثة منه على الشروط الواجب توافرها حتى يحظى الاختراع بالحماية بقولها : " يمكن أن تحمي بواسطة براءة الاختراع ، الاختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصناعي ... " . [2] وعليه يمكن القول أنه حتى يحظى أي اختراع ما بالحماية ضمن نطاق براءات الاختراع ، وجب توافر شرطي الابتكار والجدة والقابلية للتطبيق الصناعي .[3]

وتجدر الإشارة إلى أنه يمكن الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين :- أن يكون البرنامج جزءا من ذاكرة الحاسوب نفسه ومثاله البرنامج المبني .

- أن يكون البرنامج جزءا ، أي أن طلب البراءة ينصب على وسيلة صناعية جديدة ، يستخدم البرنامج في تحقيق إحدى مراحلها ، فالحماية تبقى رهينة توفر الشرطان المذكوران ، مما يصعب توفرها ، فالمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الاختراع [4] طبقا للمادة **07** من الأمر رقم **03-07** التي تنص على : " لاتعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب ". [5]

---

[1] - بوعناد فاطمة زهرة ، مكافحة الجريمة الإلكترونية في التشريع الجزائري ، مجلة الندوة للدراسات القانونية ، سيدي بلعباس ، 2013 ، العدد 01 ، ص 68 .

[2] - الأمر رقم 03-07 ، الصادر في 19 يوليو 2003 ، المتعلق ببراءات الإختراع ، ج ر العدد 44 .

[3] - خثير مسعود ، المرجع نفسه ، ص 69 .

[4] - بوعناد فاطمة الزهرة ، المجلة السابقة الذكر ، ص 66 .

[5] - الأمر رقم 03-07 ، المرجع نفسه.

الفرع الثاني : خضوع معطيات الحاسب الآلي النصوص الملكية الأدبية و الفنية .

تظهر الملكية الأدبية والفنية من خلال حق المؤلف، وهو حق استئثاري يمنحه القانون للمؤلف أي مصنف للكشف عنه، كابتكار له أو استنساخه أو توزيعه أو نشره على الجمهور، والإذن للغير باستعماله على وجه محدد. [1] وقد انقسم الفقه إلى اتجاهين، اتجاه يرى أن برامج الحاسب الآلي مصنفة ضمن قانون حق لمؤلف وأنه لا حاجة لتعديل النصوص التقليدية في قانون حق المؤلف، باعتبار برامج الحاسب الآلي ما هي إلا طرق مختلفة للتعبير عن الأفكار الإنسانية و هو مثل سائر المصنفات، أما الاتجاه الآخر أقر لبرامج الحاسب الآلي الصفة المميزة عن سائر المصنفات الأخرى المحمية، بموجب قانون حماية حق المؤلف، وتبنى هذا التوجه العديد من الدول التي عدلت قوانينها بما ينسجم و الصفة المميزة لبرامج الحاسب الآلي،[2] ومنهم الجزائر حيث جاء الأمر رقم **03-05** المتعلق بحق المؤلف والحقوق باستخلاص ما يلي: - أن المشرع وسع قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لاسيما المصنفات المعلوماتية ،[3]

[1] - عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، منشورات الحلبي الحقوقية ، بيروت ، 2003 ، ص 75 .

[2] - جلال محمد الزعبي ، أسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية ، دراسة مقارنة ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن ، 2010 ، ط 01 ، ص 189.

[3] - بوعناد فاطمة الزهرة ، المرجع نفسه ، ص66 .

حيث تنص المادة **05** من القانون رقم **03-05** [1] على أنه: " تعتبر أيضا مصنفات محمية الأعمال الآتية.... مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواءا كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى...تكفل الحماية لمؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية ."

و **المادة** رقم **04** من نفس القانون نصت على أنه:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل...وبرامج الحاسوب...."، كما أن مدة الحماية تحدد بـ **50** سنة بعد وفاة المبدع وفقا **للمادة 58** فقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي لمؤلف برنامج فعلا من أفعال التقليد، حيث نص المشرع في المادة **151** من الأمر رقم **05/03** ، على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء فني أو في حالة المساس بسلامة مصنف أو أداء فني، أو في حالة استنساخ مصنف أو أداء فني بأي أسلوب في شكل نسخ مقلدة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول.

وقد قرر المشرع جزاءات لجرائم التقليد، حيث ربط المشرع الجزائري حماية المصنف بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة، كما خول المشرع لصاحب المصنف المعتدى عليه القيام بإجراء تحفظي يتمثل في حجز التقليد، وبواسطته يتم حجز الوثائق والنسخ

[1] – الأمر رقم 03-05 ، الصادر في 19 يوليو 2003 ، يتعلق بحقوق المؤلف و المجاورة ، ج ر العدد 44 .

الناتجة عن الإستنساخ غير المشروع أو التقليد. والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من **156/153** إلى **159** من نفس القانون السابق الذكر، حيث قدرت العقوبة الأصلية بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من **500.000 دج إلى 1.000.000 دج** سواء تمت عملية النشر داخل الجزائر أو خارجها، ومنح المشرع للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة و إتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع، وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبية، كما للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر. [1]

- **المطلب الثالث : الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .**

صدر القانون رقم **09-04** الصادر في **05** أوت **2009** ، ويتضمن **19 مادة** موزعة على ستة فصول ، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية ، كما يتضمن القانون أحكام خاصة بالمراقبة الإلكترونية لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم الأفعال الموصوفة بجرائم

[1] – سوير سفيان ، المرجع نفسه ، ص 75 – ص 78 – ص 80 .

الإرهاب والتخريب ، والجرائم الماسة بأمن الدولة أو حالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام . وينص القانون على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام و الاتصال ومكافحته ، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم ، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج ، علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل . يعتبر القانون رقم **09-04** ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية ، حيث جاء بتحريمه للأفعال المخالفة للقانون و التي ترتكب عبر التي تحديدها وهي وسائل الاتصال عامة ، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا . [1]

❖ المبحث الثاني :الحماية الإجرائية للنظام المعلوماتي.

إن القاعدة الإجرائية ليست غاية في ذاتها ، وإنما هي وسيلة لغاية تتمثل في حسن تطبيق القانون الجنائي الموضوعي ، فبينما تجرى بالدعوى العمومية محاكمة القاضي للمتهم، فإنه بتطبيق القواعد الإجرائية التي خالفتها الدعوى تجرى محاكمة القانون للقاضي، وبالتالي فإن للإجراءات الجنائية خطورة لا تقل بمحال القواعد المقررة في قانون العقوبات ، لأنها تمس

[1] – رصاع فتيحة ، المرجع نفسه ، ص 113– ص 115 .

مباشرة بحريات المواطنين واستقرارهم .[1] وعليه كان لابد من التطرق إلى الجوانب الإجرائية بخصوص الجريمة الإلكترونية ، و مدى توافر الحماية الإجرائية للنظام المعلوماتي، وذلك من خلال المطالب الأتية .

○ المطلب الأول : إجراءات جمع الأدلة التقليدية .

إن التطور التقني الذي لحق نظم المعالجة الآلية ، فضلا عن الطبيعة الخاصة للدليل الرقمي أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل ، وهو ما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية [2]، لذا سأبين مدى اعتماد هذه الإجراءات في مجال الجريمة الإلكترونية للحصول على الدليل الرقمي وفق الفرعين المواليين .

الفرع الأول : الإجراءات المادية (المعاينة ، التفتيش ، الضبط)

أولا : المعاينة : هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه وتقتضي المعاينة إثبات حالة الأشخاص والأشياء [3]، وكل ما يعتبر في كشف الحقيقة ، وبهذا المعنى تستلزم المعاينة الانتقال إلى محل الواقعة أو أي محل توجد به أشياء ، أو آثار يرى المحقق أن لها صلة بالجريمة ، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية

[1] – طارق إبراهيم الدقوسي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة ، الإسكندرية ، 2009 ، ص 342 – ص 343 .

[2] – سعيداني نعيم ، المرجع نفسه ، ص 221 .

[3] – عبد الله دغش العجمي ، المشكلات العلمية و القانونية للجرائم الإلكترونية ، (دراسة مقارنة) رسالة مكملة للحصول على درجة الماجستير في القانون العام جامعة الشرق الأوسط ، 2014 ، ص 77 .

متمثلة في تصور كيفية وقوع الجريمة وظروف ملابساتها وتوفير أدلة مادية ، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية ، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها ، لأن الجريمة التقليدية غالبا لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية ، على خلاف الجريمة الإلكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة ، لأن الجريمة الإلكترونية قلما تخلف آثار مادية ، وأن كثير من الأشخاص يردون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة ، وحتى اكتشافها أو التحقيق فيها وهي طويلة نسبيا ، الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالأثار المادية للجريمة إن وجدت ، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة [1]، و ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي : تصوير جهاز الحاسوب وما قد يتصل به من أجهزة طرفيه ومحتوياته – عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغنطيسية في العالم الخارجي حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية – ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها ، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغييرها.

ثانيا : التفتيش : التفتيش هو إجراء من إجراءات التحقيق ، يستهدف البحث عن الحقيقة في مستودع السر ، لذلك يعتبر من أهم الإجراءات لأنه غالبا ما يسفر عن أدلة مادية تؤدي إلى

[1] – عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية ، مصر ، 2002 ، ص 20– ص 21 .

نسبة الجريمة للمتهم ،[1] والمستهدف من التفتيش هو جهاز الحاسوب بمكوناته المادية (وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل) ، والمكونات المعنوية (الكيانات المنطقية) ، فعندما يستهدف التفتيش الكيانات المادية لا يشكل عائق ، وإنما الإشكال يثور عندما ينصب على المكونات المعنوية (البرامج ، قواعد البيانات ...) ، لأنه هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات .[2]

– **تفتيش مكونات الحاسوب المادية** : لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته ، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب ، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش ، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه ، و حسب **المادة** رقم **45** ف **3** تنص على : " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم ... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات " . و **المادة 47** ف **3** تنص على : " عندما يتعلق الأمر بـ ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... فإنه يجوز إجراء التفتيش ... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل ... " ، و **المادة 64 ف 2** تنص على : " وتطبق فضلا عن ذلك أحكام **المواد 44 ، 47** من

[1] – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 68 .

[2] – زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى للطباعة و النشر ، الجزائر ، 2011 ، ص من 131 إلى 133 .

هذا القانون . " [1]، بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الإلكترونية ، حيث لا يشترط حضور الشخص المشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه ، وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء .[2]

– **مدى خضوع مكونات الحاسوب المعنوية للتفتيش** : عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراءات التفتيش ، وانقسم إلى اتجاهين ، إتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب ، وقد عملت الدول التي تبنت هذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية ، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل حيزا ماديا في فراغ معين ، هذا الحيز يمكن قياسه والتحكم فيه ، وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ، ويمكن قياسه بمقياس معين هو " البايت " و " الكيلوبايت " و " الميغابايت " ، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها ، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية ، لذا فإن طبيعة البيانات و المعطيات المعالجة تتطلب قواعد خاصة

[1] – المواد 45 ، 47 ، 64 ، من الأمر رقم 22/06 ، الصادر في 20 ديسمبر 2006 ، المعدل و المتمم لقانون الإجراءات الجزائية ، ج ر العدد 84 .

[2]. – سعيداني نعيم ، المرجع نفسه ، ص145 .

تحكمها ، فالنصوص التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية ، لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية .[1]

– **مدى خضوع شبكات الحاسوب للتفتيش عن بعد** : نفرق هنا بين فرضين .

الفرض الأول : إتصال حاسوب المتهم بحاسب موجود في مكان آخر داخل الدولة : لقد أجاز المشرع في **المادة 05** من القانون رقم **09-04** إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى ، فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك [2]، حيث تنص **المادة 05** منه على : " ... في الحالة المنصوص عليها في الفقرة " أ " من هذه المادة إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى ، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ... "

الفرض الثاني : إتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة .

ويكون بالدخول إلى منظومة معلوماتية أو جزء منها ، وكذا المعطيات المخزنة فيها ولو عن بعد ، وذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ، ووفقا لمبدأ المعاملة بالمثل ،

[1]. – سعيداني نعيم ، المرجع نفسه ، ص 147 .

[2] . – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 69 .

تسخير كل شخص من له دراية بعمل المنظومة المعلوماتية محل البحث ، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها [1]، حيث تنص **المادة 05** من القانون رقم **09-04** على أنه : " ... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل ".[2]

ثالثا – ضبط الأشياء : يختلف ضبط الأشياء في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل ، ففي هذه الأخيرة يكون المحل أشياء مادية ، أما في الجريمة الإلكترونية تكن الأشياء ذات طبيعة معنوية كالبيانات ، المراسلات الإلكترونية ، وتجدر الإشارة إلى أن ضبط الأشياء قد يرد على عناصر معلوماتية منفصلة مثل الأسطوانات الممغنطة ، وهنا لا يثور أي إشكال عند القيام بالضبط ، لكن الصعوبة تكون عندما يلزم ضبط النظام كله ، أو الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها . أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية : – وحدات الإدخال (لوحة المفاتيح ، الفأرة ، نظام القلم الضوئي) ، وضبط وحدة الإخراج (الشاشة ، الطابعة ، الرسم

[1] – بن دعاس فيصل ، إجراءات التحري في الجرائم المعلوماتية ، محاضرة في إطار التكوين المحلي المستمر للقضاة ، مجلس قضاء قسنطينة ، ص 33 .

[2] – المادة 05 من القانون رقم 04/09 ، المرجع نفسه.

والمصغرات الفيلمية) ، وكل ما يتم ضبطه من بيانات إلكترونية يتعين تحريزها وتأمينها فنيا [1]، تنص **المادة 06** من القانون رقم **04-09** على أنه : " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ، أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ...".[2]

الفرع الثاني : الإجراءات الشخصية (الشهادة ، الخبرة)

أولا : الشهادة : في الجريمة الإلكترونية الشاهد هو الفني صاحب الخبرة و التخصص في التقنية عن وعلوم الحاسب الآلي ، لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات ، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ، ويطلق عليه اسم الشاهد الإلكتروني ، تمييزا له عن الشاهد التقليدي .[3] نتيجة لقصور أحكام الشهادة في الحصول على الدليل الإلكتروني ، يرى بعض الفقهاء ضرورة البحث عن وسيلة قانونية جديدة ، ما لم تستطيع فكرة الإلتزام بالشهادة أن تؤديه ، وهذه الوسيلة هي الإلتزام بالإعلام في الجريمة الإلكترونية ، و ذلك بضرورة وجود نص صريح في القانون يفرض تقديم أي معلومات

[1] – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 69 .

[2] – المادة 06 من القانون رقم 09-04 ، المرجع نفسه.

[3] – كوثر فرام ، الجريمة المعلوماتية على ضوء العمل القضائي المغربي ، بحث نهاية التدريب المعهد العالي للقضاء ، فترة التدريب 2007 – 2009 ، ص 93 .

ضرورية من أجل إعانة سلطات التحقيق و الإستدلال في الحصول على الدليل ، وفرض مثل هذا الإلتزام قد يلعب دور وقائي في حفظ النظام المعلوماتي .[1]

ثانيا : الخبرة : تكون الخبرة في مجال المعلوماتية بتحري الحقيقة ، عن طريق جمع معلومات من الأدلة الرقمية ، وتحصيلها من خوادم المواقع ، ومن الجهاز المعتدى عليه بعد التوصل إلى تحديده ، ثم يقوم الخبير بعملية تحليل رقمي لها ، لمعرفة كيفية إعدادها البرمجي ، ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها ، ثم التوصل إلى معرفة بروتكول الإنترنت للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية [2]، غير أنه قد تواجه سلطات الإستدلال و التحقيق بعض المشاكل الفنية والتقنية التي تستلزم خبير إلكتروني مختص ، وهنا قد لا تتوافر مثل هذه النوعية من الخبرة في من يحملون جنسية الدولة ، وهنا يثور التساؤل حول مدى إمكانية الإستعانة بخبير إلكتروني أجنبي ؟[3] فالبعض يرى أن الإستعانة بخبير أجنبي يشكل تهديد وخطر على سيادة الدولة وأمنها ، والبعض يرى أنه ليس هناك مانع باللجوء إلى خبير إلكتروني أجنبي ، و هو أمر تسمح به مقومات العالم الافتراضي ، باعتباره بيئة اتصالية رقمية عالمية .[4]

[1] – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 70 .

[2] – سعيداني نعيم ، المرجع نفسه ، ص 171 .

[3] – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 70

[4] – سعيداني نعيم ، المرجع نفسه ، ص 168

○ المطلب الثاني : التحقيق في الجريمة الإلكترونية .

يعرف التحقيق بأنه إجراء يتخذ بعد وقوع الجريمة ، لما له من أهمية في التأكد من وقوع الجريمة ، وإسنادها إلى مرتكبيها بأدلة الإثبات بأنواعها ، وبالتالي تتجلى الحقيقة التي تهدف إلى إدانة المتهم من عدمه . وتمر الدعوى الجنائية بمرحلتين ، مرحلة التحقيق ومرحلة المحاكمة ، وتمر عملية التحقيق بدورها بمرحلتين ، مرحلة التحقيق الأولي (الضبطية القضائية) ومرحلة التحقيق الابتدائي (قاضي التحقيق) ، وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية ، فإذا كان التحقيق يعتمد على ذكاء المحقق وقوة ملاحظته ، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى ذلك تطوير لأساليبه ، وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطورها [1] و هذا ما سيتم بيانه في الفروع الموالية .

الفرع الأول : الأجهزة المكلفة بالبحث والتحري .

نظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر ، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية ، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني ، بالنسبة لجهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران ، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي ، بالإضافة إلى فرق متخصصة

[1] – سعيداني نعيم ، المرجع نفسه ، ص 102 – ص 103 .

مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر توجد على مستوى مراكز الأمن الولائي ، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني ، قسم الإعلام و الإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية ، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني .[1]

الفرع الثاني : خصائص التحقيق والمحقق .

للتحقيق الإلكتروني مميزات خاصة عن التحقيق الجنائي التقليدي وكذا المحقق الإلكتروني ، لمسايرة متطلبات الجريمة الإلكترونية بما فيها العالم الإفتراضي الذي ترتكب فيه .

أولا : خصائص التحقيق الإلكتروني

منهج أو أسلوب التحقيق الإبتدائي : – وضع خطة عمل التحقيق : وذلك وفق المعلومات المتوفرة لدى المحقق ، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك بوضع خطة مناسبة ، ولا تبتدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة ، ثم التخطيط الفني للتحقيق من أجل الوصول إلى أفضل الطرق للتعامل مع هذه الجريمة بالتفصيل والوضوح ، وبعدها عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها

[1] – سعيداني نعيم ، المرجع نفسه ، ص 106 – ص 107 .

العاملون في فريق التحقيق ، تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل ، وهو ما يؤدي إلى ضمان مستوى جيد من الأداء ، تحديد الإجراءات المسبقة التي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبراء أو نقص المعرفة ، و بالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة .

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية ، يتم الارتكاز عليها أثناء تنفيذ الخطة وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب إيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق ، بالإضافة إلى مراعاة الظروف المحيطة بالواقعة ، إذ أن هذه الظروف قد تشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها : مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة – مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها – مدى الاختراق الأمني الذي تسبب فيه الجاني .

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش ، وذلك بتحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها .[1]

[1] . – سعيداني نعيم ، المرجع نفسه ، ص 110 – ص 111

– **تشكيل فريق التحقيق :** يجب أن يتشكل الفريق من فنيين وأخصائيين ذوي الخبرة في مجال الحاسوب والأنترنت ما يكفي لمكافحة هذا النشاط الإجرامي ، وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين في مجال المعلوماتية ، والمعرفة باللغات الأجنبية [1]، ولهم مهارات في التحقيق الجنائي بشكل عام و التحقيق الجنائي الإلكتروني بشكل خاص ، ولهم الاستعانة بخبراء ليتمكنوا من فك التعقيدات التي تفرضها ملابسات كل جريمة ، ويتكون الفريق من المحقق الرئيسي ، ويكون ممن لهم خبرة في التحقيق الجنائي ، خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم ، خبراء ضبط و تحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب ، خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية – خبراء التصوير والبصمات والرسم التخطيطي .

– **إجراءات التحقيق : – إجراءات سابقة على بدء التحقيق الابتدائي :** – تحديد نوع نظام المعالجة الآلية للمعطيات ، أي هل الحاسوب معزول أم متصل بشبكة معلومات – وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة ، مع كشف تفصيلي عن المسؤولين بها ودور كل واحد منهم – إذا وقعت الجريمة على شبكة ، فإنه يجب حصر طرفيات الاتصال بها أو منها ، لمعرفة الطريقة التي تمت بها عملية الإختراق من عدمه ، وهل هناك حواسب آلية خارج هذه المشكلة ولها إمكانية الاتصال بها أم لا ؟ – مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة الإلكترونية – مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات

[1] – كوثر فرام ، المرجع نفسه ، ص 88 .

المخزنة – يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الإستدلال لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته – فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق – التأكد أن من خط الهاتف يخص الحاسوب محل الجريمة ، لأنه من الخدع التي يستعملها الجاني عند الإختراق أن يتم ذلك بخط هاتفي مسروق (الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة والتخطيط) – إبعاد الموظفين عن أجهزة الحاسب الآلي بعد حصول المتهم على كلمة السر ، وكذا الشفرات في حالة وجودها – تصوير الأجهزة المستهدفة – التي وقعت بها أو عليها الجريمة – من الأمام والخلف لإثبات أنها كانت تعمل [1].

إجراءات أثناء التحقيق الإبتدائي : – عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها ، والتأكد فنيا من دقة النسخ عن طريق الأمر – نزع غطاء الحاسب الآلي المستهدف ، والتأكد من عدم وجود أقراص صلبة إضافية – أن يكون الهدف من

نسخ محتوى الأسطوانة و الأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة ، ويمكن استعادتها من سلة المهملات ، وكذا معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب – العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد

[1] – سعيداني نعيم ، المرجع نفسه ، ص من 111 إلى 113 .

استخدمت في اختلاس معلوماتي – العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها – حفظ المعدات والأجهزة التي تضبط بطريقة فنية سليمة .[1]

ثانيا : خصائص المحقق الإلكتروني : تتمثل في الخصائص الفنية للمحقق الإلكتروني ، وتأهيل وتدريب المحقق الإلكتروني .

الخصائص الفنية للمحقق الإلكتروني : – معرفة الجوانب الفنية والتقنية الأجهزة الحاسوب والأنترنت ، لأن افتقار ضابط الشرطة القضائية إلى التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل – إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك ، و منع حذفها و الحرص على عدم تعريض وسائط التخزين كالأقراص المرنة لأي مؤثرات خارجية ، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها– معرفة آلية عمل تشكيلات الحاسوب والانترنت – معرفة المحقق بالأنظمة المختلفة ، لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة – معرفة معطيات الحاسوب المعرفة صيغ الملفات وما تحتويه – معرفة وإدراك أساليب ارتكاب الجريمة الإلكترونية ، وتقنيات الأمن المعلوماتي .

تأهيل وتدريب المحقق الإلكتروني : لابد من وضع سياسة جنائية رشيدة ، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة ، ويمتد هذا التدريب إلى العاملين بأجهزة

[1]. – سعيداني نعيم ، المرجع نفسه ، ص 113 – ص 114 .

الضبطية القضائية . ويرى الفقه الجنائي أنه في حالة التدريب على التحقيق يتعين مراعاة شخص المتدرب ، ومنهج الدورة التدريبية ، وصفة وأسلوب التدريب ، كما يجب أن يشمل منهج التدريب تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة ، والمتعلقة بالكشف عنها وكيفية اتباعها ومعاينتها وفحصها فنيا [1]. و من العقبات التي تعيق عمل الأجهزة حتى على فرض أنه تم إعدادها الإعداد المناسب ، ضخامة حجم البيانات محل الفحص ، ما يتعذر على المحقق الكفء الوصول إلى الدليل المناسب .[2]

الفرع الثالث : الدليل المناسب لإثبات الجريمة الإلكترونية .

الدليل هو أثر يولد ، أو حقيقة تنبعث من الجريمة المرتكبة ، فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر مثلا . وبالنسبة للجريمة الإلكترونية فإنها تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها ، وهي تعرف بالدليل الرقمي المتواجد في أماكن افتراضية ، ويعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الحاسب الآلي ، ويكون في شكل مجالات ، أو نبضات مغناطسية أو كهربائية ، يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء ، أو أنه ذلك الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة . ويتميز الدليل

[1]. – سعيداني نعيم ، المرجع نفسه ، ص 116 – ص 117 – ص 119 .

[2] – موسى مسعود أرحومة ، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية و القانون ، الذي تنظمه أكادمية الدراسات العليا ، طرابلس ، خلال الفترة 28-2009/10/29 ، ص05 .

الرقمي بجملة من الخصائص :- أنه دليل علمي يحتاج إلى بيئته التقنية التي يتكون فيها ، لكونه من طبيعة تقنية المعلومات – أنه من طبيعة تقنية إذ ما تنتجه هذه الأخيرة هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب ، وبالتالي لا وجود للدليل الرقمي خارج بيئته الرقمية ، ويتميز الدليل الرقمي بقابليته للنسخ مطابق الأصل مع نفس القيمة العلمية ، وهذا ما لا نجده في الدليل المادي – أنه دليل متنوع ومتطور ، حيث يشمل كافة البيانات الرقمية الممكن تداولها رقميا ، وتطوره يظهر في حركة الإتصال عبر الأنترنت و مدى تطورها- أنه دليل صعب التخلص منه ، إذ أنه كلما حدث اتصال بتكنولوجيا المعلومات بإدخال بيانات إلى هذا العالم ، فإنه من الصعب التخلص منها ، إذ تتوفر برمجيات ذات طبيعة رقمية ، يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب – أنه ذو طبيعة رقمية ثنائية " 1-0 " ، حيث تعتمد تكنولوجيا المعلوماتية الحديثة على تقنية الترقيم ، التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي ، قوامه الرقمان " 0 و 1 " ، فالكتابة مثلا في العالم الرقمي ليس لها وجود مادي ، وإنما هي مجموعة أرقام لها أصل واحد وهو الرقم الثنائي " 0 و 1 " . والدليل الرقمي نوعان ، الدليل الرقمي الأصلي والدليل الرقمي المكرر ، وهذا الأخير هو استنساخ رقمي لجميع المستمسكات البيانية التي يحتويها الدليل الرقمي الأصلي .[1]

[1] – سعيداني نعيم ، المرجع نفسه ، ص 119 – ص 120 – ص 121 – ص 123 – ص 124 – ص125 – ص 126.

○ المطلب الثالث : إجراءات الأدلة الحديثة .

تتمثل هذه الإجراءات في حفظ المعطيات والتسرب واعتراض المراسلات الإلكترونية .

الفرع الأول : حفظ المعطيات .

ألزم المشرع الجزائري مقدي الخدمات بحفظ المعطيات ، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ، ووضعها في ترتيب معين ، في حين اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش و غيره ، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة ، و هي المعطيات المتعلقة بحركة السير (معطيات المرور) ، وهي كما عرفتها المادة الثانية من قانون رقم **09-04** تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة ، باعتبارها جزءا في حلقة الاتصالات توضح مصدر الإتصال ، الوجهة المرسل إليها ، والطريق الذي يسلكه ، ووقت وتاريخ وحجم ومدة الإتصال و نوع الخدمة . وقد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في **المادة 11** القانون رقم **09- 04** و تتضمن : - المعطيات التي تسمح بالتعرف على مستعملي الخدمة - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال - الخصائص التقنية و كذا تاريخ و وقت ومدة كل اتصال - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها - المعطيات التي تسمح بالتعرف على المرسل إليه ، الإتصال وكذا عناوين المواقع المطلع عليها وبما أن حفظ المعطيات إجراء وقتي ، واحتراما للحق في الخصوصية ، فإن المشرع الجزائري فرض على مزودي الخدمات بإزالة المعطيات

التي يقومون بتخزينها بعد سنة من تاريخ التسجيل ، إن مزودي الخدمات يعتبرون مصدرا لجهات التحقيق ، للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها ، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها .[1]

الفرع الثاني : التسرب واعتراض المراسلات الإلكترونية .

أولا : التسرب : استحدث المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات ، وذلك بسبب عجز الأساليب التقليدية ، ومن بينها إدراج المشرع لعملية التسرب بموجب القانون رقم **06-22** ، مؤرخ في سنة **2006** ، المتضمن قانون الإجراءات الجزائية ، حيث خص الفصل الخامس منه تحت عنوان " في التسرب " ، **المواد** من **65** مكرر **11** إلى **المادة 65** مكرر **18** ، إذ تناول من خلالها مفهوم هذه العملية وشروط إجراءها ، و الحماية الجنائية للقائم بعملية التسرب .

تعريف التسرب : قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك ، وهذا ما نصت عليه **المادة 65** مكرر **12** من قانون الإجراءات الجزائية ، ومثاله في الجريمة الإلكترونية اشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال أو كلام يدور حول قيام أحدهم باختراق شبكات

[1]- سعيداني نعيم ، المرجع نفسه ، ص من 139 إلى 141 .

بث فيروسات ، فيتخذ المتسرب أسماء استعارة ، و يحاول الاستفادة حول كيفية اقتحام الهاكرز لموقع ما حتى يتمكنوا من اكتشاف و ضبط الجرائم.[1]

شروط صحة التسرب:- صدور إذن من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية- أن يكون الإذن مكتوبا ومسببا- يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة- يحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 04 أشهر ، غير أنه من يمكن أن تجدد ، حيث تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على : " ... يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن ... حسب الحالة بمباشرة عملية التسرب . " [2]

ثانيا : إعتراض المراسلات الإلكترونية : يقصد بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء بثها ، وليس الحصول على اتصالات إلكترونية مخزنة ، وقد استحدث المشرع الجزائري هذا الإجراء من خلال القانون رقم **09-04** المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، حيث حدد الحالات التي يجب فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام ، أو مؤسسات الدولة أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ، أو لمقتضيات التحريات و التحقيقات القضائية ، وهذا طبقا **للمادة 04** من القانون رقم **09-04** ، ويترتب على

[1] - بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 69 - ص 70 .

[2] - بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 70 .

المراقبة السرية للإتصالات عموما ، ومن ضمنها الإتصالات الإلكترونية في الغالب تسجيل محتوى تلك الإتصالات وتخزينها على وسائط مادية قابلة للنقل ، بغية استخدامها فيما بعد لإثبات الجريمة الواقعة ، وتختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الإلكترونية المراقبة هي عبارة عن اتصال صوتي فقط ، أو أنها اتصال صوتي مرئي ، ففي الأول يكون التسجيل صوتي فقط ، في حين أنه يكون في الثاني تسجيل صوتي مرئي ، كما تجدر الإشارة إلى أن المراقبة السرية للإتصالات الإلكترونية ، ومن ضمنها المحادثات الهاتفية ، لا يمكن اعتبارها نوع من أنواع التفتيش ، لأن المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة (الإتصالات الإلكترونية حال إجرائها) ، دون التي انتهت وخزنت ، في حين التفتيش يرد فقط على البيانات الإلكترونية الساكنة أو المخزنة (الإتصالات الإلكترونية التي تمت وخزنت) ، وتكون عملية المراقبة في جميع الحالات بإذن مكتوب من السلطة القضائية المختصة طبقا **للمادة 04** من القانون الرقم **09-04** التي تنص على : " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه ، إلا بإذن مكتوب من السلطة القضائية المختصة ... " [1]

الفرع الثالث : صعوبات مكافحة الجريمة الإلكترونية .

يعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية وذلك للأسباب التالية : – يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة .

[1] – بوعناد فاطمة الزهرة ، المرجع نفسه ، ص 72 .

– صعوبة التوصل إلى الجاني ، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام اسم مستعار ، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت ، فيصعب معرفة الجاني وتحديد موقع اتصاله .

– تنازع القوانين الجنائية من حيث المكان ، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي ، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين سوف يخضع لها الجاني ؟

– صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي ، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية ، فهل يسأل عن هذه الجريمة عامل الإتصال ، أم مورد المنافذ ، أم مورد المعلومات ، أو غيرهم من العاملين في مجال الأنترنت .

– إفتراض العلم بقانون جميع الدول، ففي حالة ارتكاب الجريمة في بلد ما، وتحقق النتيجة في بلد آخر يجد الجاني نفسه يخضع لقانون هذه الدولة، وقد يكون هذا الفعل المرتكب مباح في بلده.

– صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص.

– جهل الناس بثقافة الأنترنت يجعلهم يقومون بأفعال لا يعرفون بأنها تشكل جريمة يعاقب عليها القانون .[1]

– عدم ظهور الجليل المادي للجريمة الإلكترونية أو اثار مادية ملموسة .

[1] – جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة) ، دار البلدية ، عمان ، الأردن ، 2007 ، ط 01 ، ص من 220 إلى 223 .

– عجز الوسائل التقليدية عن ضبط اثار الجريمة الإلكترونية . [1]

– عولمة هذه الجريمة تؤدي إلى تثبيت جهود التحري و التنسيق الدولي ، لتعقب مثل هذه الجرائم ، و هي بمثابة صورة صادقة من صور العولمة .[2]

– صعوبة تقدير حجم الجريمة الإلكترونية ، فالإحصائيات الجنائية لا تعبر عن الإجرام الحقيقي ، إذ منها ما يصل إلى علم السلطات المختصة بصورة دائمة ، و منها ما لا يصل إلى علمها إلا نادرا ، كالجرائم الماسة بالعرض ، و هنا يظهر الفارق بين الحجم الحقيقي للجريمة الإلكترونية ، و بين ما هو مسجل بالإحصائيات .[3]

من خلال التطرق لمكافحة الجريمة الإلكترونية في التشريع الجزائري استنتج أنه لابد من الوقاية من هذا النوع من الجرائم قبل انتشارها ، و اللجوء إلى مكافحتها ، و ذلك بتربية النشأ على الوازع الديني و الأخلاق الفاضلة ، اللذان هما بمثابة واقي للفرد يحول دون ارتكاب أي نوع من الجرائم ، و يجعلان الفرد يعي مدى خطورة التعدي على حقوق الغير ، علاوة على ذلك توعية الأفراد بأخطار و سلبيات الأنترنيت ، من خلال عقد ندوات و دراسات حول مخاطر الأنترنيت في الجامعات و الثانويات ، و جميع الأنشطة من جمعيات و غيرها.

[1] – عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية ، مصر 2007 ،ص 105 .

[2] – عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنيت (الجرائم الإلكترونية) دراسة مقارنة ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ، ط 01 ، ص33 .

[3] – نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الإقتصادية ، دراسة نظرية و تطبيقية ، منشورات الحلبي الحقوقية ، بيروت ، 2005 ، ط 01 ، ص 68 .

الخاتمة

خـــاتمة

في ختام هذه الدراسة المتعلقة بالجريمة المعلوماتية ، فإنني حاولت معالجة الموضوع من خلال فصلين أساسيين حيث تطرقت للفصل الأول إلى ماهية الجريمة الإلكترونية ، و ذلك بالتطرق إلى مفهومها المتضمن الإتجاه المضيق و الموسع لها ، و بيان الدوافع المؤدية لارتكابها ، و كذا خصائصها التي جعلتها تنفرد عن نظيرتها التقليدية ، سواء تعلقت هذه الخصائص بالجريمة ذاتها ، أو بالمجرم الإلكتروني ، كما تتشكل الجريمة من الأركان الثلاثة المعروفة للجرائم التقليدية ، لكن هذه الأركان تتميز بخصوصيات تجعلها متميزة نوعا ما عن الأول ، كما أن هذا النمط من الجرائم يتنوع بحسب ما هو واقع أو مستهدف النظام المعلوماتي ، أو ما يرتكب باستخدام النظام المعلوماتي ، و يجب تصدي هذه الجريمة الإلكترونية خصوصا أن الجرائم تشهد استعمال موسع للتقنية المعلوماتية في جميع القطاعات ، و هذا ما تطرقت إليه بالتفصيل من خلال الفصل الثاني ، حيث تطرقت للحماية الموضوعية و الإجرامية للنظام المعلوماتي في التشريع الجزائري ، إذ أن المشرع الجزائري قام بتعديل قانون العقوبات رقم **15/04** ، و اصدار قانون رقم **04/09** لما يتناسب و الظاهرة المستجدة.

و من خلال هذا البحث توصلنا إلى جملة من النتائج التالية :

خـــاتمة

– بالنظر لحداثة هذا السلوك الإجرامي و الذي يتجسد في الجريمة الإلكترونية ، فإنه لا يوجد لحد الآن اجتماع فقهي موحد على تعريف لها مما أدى بالقول أن الحريمة الإلكترونية تقاوم التعريف .

– رغم تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي و ذلك بتجريم الإعتداءات الواردة على مستويات الإعلام الآلي ، إلا أنه لم يستحدث نصا خاصا بالتجريم المعلوماتي .

– قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم **15/04** ، حيث اعتبر الدخول غير المشرع للنظام المعلوماتي و البقاء فيه ، و المساس بمنظومة معلوماتية و بعض الأفعال الأخرى أفعال إجرامية و سطر لها عقوبات و استدراك النقص في المجال الإجرامي باصدار قانون رقم **04/09** ، اذ تتضمن قواعد إجرائية و أخرى وقائية و هذه خطوة إيجابية إلا أنها غير كافية لمواجهة خطر الجريمة الإلكترونية .

– المشرع الجزائري لم يخصص قانون خاص للجريمة الإلكترونية .

في ضوء النتائج السابقة التي أظهرتها الدراسة تستخلص بعض التوصيات و الاقتراحات تتمثل في ما يلي :

- ✓ ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل كل السلوكات المجرمة .

خـــاتمة

- ✓ الإستفادة من التجارب الدولية في هذا المجال لكسب المهارات اللازمة لمكافحتها .
- ✓ ضرورة تدريب و تأهيل أفراد الضبطية القضائية و كذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم و تحقيق التعاون مع التقنيين من أصحاب الخبرة .
- ✓ وضع إجراءات كالتحقيق ، و المحاكمة للجريمة الإلكترونية تختلف عن الجريمة التقليدية. مع توعية المجتمع و خلق له ثقافة اجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة و يتعرض صاحبها لعقوبات جزائية .

قائمة

المراجع و

المصادر

أولا النصوص القانونية و الأوامر :

1. القانون رقم **09-04** الصادر في **05** أوت **2009** يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، الجريدة الرسمية العدد **47** .

2. القانون رقم **04-15** الصادر في **10** نوفمبر **2004** ، معدل و متمم لأمر رقم **156/66** الصادر في جوان **1966** ، المتضمن قانون ع.ج.إ الجريدة الرسمية العدد **72** .

3. الأمر رقم **03-07** الصادر في **19** يوليو **2003** المتعلق ببراءات الاختراع ج . ر العدد **44** .

4. الأمر رقم **03-05** الصادر في **19** يوليو **2003** ، يتعلق بحقوق المؤلف و المجاورة ج . ر العدد **44** .

ثانيا المواد :

المواد من **45-47-64** من الأمر رقم **06-22** الصادر في **20** ديسمبر **2006** ، المعدل و المتمم لقانون الإجراءات الجزائية .

ثالثا الكتب :

أ. بالعربية :

1. أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر ، مجلة الحقوق ، الكويت ، العدد **4** ، سنة **1987** .

2. أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، ط **1** ، **2007**.

3. أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنيت ، دار المطبوعات الجامعية ، أمام كلية الحقوق ت **4126869** الاسكندرية ، **2009**.

4. بن زيطة عبد الهادي ، حماية برامج الحاسوب في التشريع الجزائري ، دار الخلدونية للنشر و التوزيع ، الجزائر ، **2007** ، ط **01**.

5. جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة) ، دار البلدية ، عمان ، الأردن ، **2007** ، ط **01**.

6. جلال محمد الزعبي ، أسامة أحمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية ، دراسة مقارنة ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن ، **2010** ، ط **01**.

7. خثير مسعود ، الحماية الجنائية لبرامج الكمبيوتر ، أساليب و ثغرات ، دار الهدى للنشر و التوزيع ، الجزائر، طبعة **2010** .

8. ز. ط. شحادة، الاعمال الجرمية التي تستهدف الأنظمة المعلوماتية، مطبعة صادر، **2006** .

9. زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى للطباعة و النشر ، الجزائر ، **2011** .

10. سامي علي حامد عباد ، الجريمة المعلوماتية و إجرام الأنترنيت ، ماجستير في القانون ، دار الفكر الجامعي ، **30** شارع سوتر ، الإسكندرية **2008** .

11. طارق إبراهيم الدقوسي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة ، الإسكندرية ، **2009**.

12. عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية ، مصر ، **2002**.

13. عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنيت ، دار الكتب القانونية ، مصر **2007** .

14. عبد الله سليمان ، شرح قانون العقوبات ، قسم عام الجزء الأول للجريمة ، الجزائر دار ، **2006** ، الطبعة الخامسة.

15. عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنيت (الجرائم الإلكترونية) دراسة مقارنة ، منشورات الحلبي الحقوقية ، بيروت ، **2007** ، ط **01**.

16. عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، **2000** ، ط **02** .

17. محمد العريان ، الجرائم المعلوماتية ، كلية الحقوق ، جامعة الاسكندرية ، دار الجامعة الجديدة للنشر ،الاسكندرية ، **2004**.

18. محمد عبد الرحيم الناغي ، الحماية الجنائية للرسوم و النماذج الصناعية (دراسة و مقارنة) ، دار النهضة العربية ، القاهرة ، **2009**.

19. نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية ، دراسة نظرية و تطبيقية ، بيروت ، منشورات الحلبي الحقوقية ، **2005** ، الطبعة الأولى.

20. نهلة عبد القادر المومني ، الجرائم المعلوماتية ، ماجيستير القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع **1429 هـ – 2008** ، الطبعة الأولى ، الإصدار الأول ، **2008**.

ب.بالفرنسية :

1. Parker (DonnB) figding camputer crime A new framework for protecting information 1988 .
2. Rose (philippe) , Op-cit .

رابعا الرسائل العلمية :

1. حمزة بن عقون ، السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية ، تخصص علم الإجرام و العقاب ، جامعة باتنة ، **2019** .

2. صغير يوسف ، الجريمة المرتكبة عبر الأنترنيت ، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الدولي للأعمال ، جامعة مولود معمري تيزي وزو ، **06 / 03 / 2013** ، ص **09** ، نقلا عن كحلوش علي ، جرائم الحاسوب و أساليب مواجهتها ،مجلة صادرة عن مديرية الأمن الوطني ، العدد **84** ، **2007**.

3. سوير سفيان ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية و علم الإجرام ، جامعة أبو بكر بلقايد ، تلمسان ، **2010 – 2011** .

4. سعيدان نعيم ، أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر ، باتنة ، **2012 – 2013** ، ص **60 – 61** ، نقلا عن نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة (2) ، **2010** ، ص **90** ، و نقلا عن ضاح محمود الحمود و نشأت مفقي المجالي ، جرائم الأنترنيت ، دار المنار للنشر و التوزيع ، **2005** .

5. سمية مزغيش جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر ، بسكرة ، **2013-2014** .

6. رصاع فتيحة ، رسالة الماجيستير الحماية الجنائية للمعلومات على شبكة الأنترنيت ، مذكرة لنيل شهادة الماجستير في القانون العام ، جامعة أبو بكر بلقايد ، تلمسان، **2011 – 2012** .

7. عبد الله دغش العجمي ، المشكلات العلمية و القانونية للجرائم الإلكترونية ، (دراسة مقارنة) رسالة مكملة للحصول على درجة الماجستير في القانون العام جامعة الشرق الأوسط ، **2014** .

خامسا المقالات و المجلات :

1. عادل يوسف عبد النبي الشكري ، بحث بعنوان الجريمة الإلكترونية و أزمة الشرعية الجزائرية ، جامعة الكوفة ، **2006** .

2. مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، مجلة علمية ، **2012** ، العدد **21** .

3. عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماوي ، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية (دراسة مقارنة) ، المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي ، الرياض .

4. موسى مسعود أرحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، ورقة مقدمة لدى المؤتمر المغاربي الأول حول المعلوماتية و القانون الذي تنظمه أكادمية الدراسات العليا ، طرابلس ،**28-2009/10/29** .

5. سمير سعدون مصطفى ، و اخرون ، الجريمة الالكترونية عبر الانترنيت و سبل مواجهتها ، بحث مقدم بتاريخ **2010/09/20** ، بدون سنة .

6. بوعناد فاطمة زهرة ، مكافحة الجريمة الإلكترونية في التشريع الجزائري ، مجلة الندوة للدراسات القانونية ، سيدي بلعباس ، **2013** ، العدد **01** .

7. بن دعاس فيصل ، إجراءات التحري في الجرائم المعلوماتية ، محاضرة في إطار التكوين المحلي المستمر للقضاة ، مجلس قضاء قسنطينة .

8. كوثر فرام ، الجريمة المعلوماتية على ضوء العمل القضائي المغربي ، بحث نهاية التدريب المعهد العالي للقضاء ، فترة التدريب **2007 – 2009** .

الفهرس