جـــامـــعة زيـــــان عـــــاشـــور-الجـــلفة-

كـــلية الحـــقوق والعـــلوم الســـــياسية

قسم القانون العام

الجرائم السيبرانية في القانون الجزائري

مذكرة ضمن متطلبات لنيل شهادة الماستر في الحقوق

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبين :

❖ العيد شعثان

❖ مسعود موفقي

إشراف الأستاذة:

د. فطيمة الزهرة فيرم

لجنة المناقشة:

أ/د مليكة حجاج	**رئيسا**
أ/د فطيمة الزهرة فيرم	**مشرفا و مقررا**
أ/د احمد بن الصادق	**ممتحنا**

الموسم الجامعي : 2022/2021

جـــامـــعة زيـــــان عـــــاشـــور-الجـــلفة-

كـــلية الحـــقوق والعـــلوم الســـــياسية

قسم القانون العام

الجرائم السيبرانية في القانون الجزائري

مذكرة ضمن متطلبات لنيل شهادة الماستر في الحقوق

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبين :

❖ العيد شعثان

❖ مسعود موفقي

إشراف الأستاذة:

د. فطيمة الزهرة فيرم

لجنة المناقشة:

أ/د مليكة حجاج	**رئيسا**
أ/د فطيمة الزهرة فيرم	**مشرفا و مقررا**
أ/د احمد بن الصادق	**ممتحنا**

الموسم الجامعي : 2022/2021

الإهداء

يفنى العباد ولا تفنى صنائعهم

فاختر لنفسك ما يحلو به الأثر

إلى الدكتورة والمشرفة فيرم فطيمة الزهراء

إلى كل من له فضل علـــي

إلى كل طالب علم

أهدي هذا العمل

شكر وعرفان

الدكتورة: فيرم فيطمة الزهراء

لولا ما قدمته لنا من توجيه ورأي سديدين، فلا نملك عرفانا بما تفضلتي به علينا إلا أن نسدي لكِ وافر الشكر ونتقدم لكِ بعميق الإمتنان وخالص التقدير.

ويسرنا كذلك أن نتقدم بجزيل الشكر والعرفان إلى اللجنة الموقرة التي قبلت مناقشة هذه المذكرة

كما لا يفوتنا أن نتقدم بالشكر إلى كل من قدم لنا يد المساعدة من قريب كان ومن بعيد.

مقدمة :

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري و المعرفي الهائل غير المعهود، وذلك بفضل الثورة العلمية التكنولوجية في مجال الاتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة، و وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة، الاقتصادية، الاجتماعية، الثقافية، والعلمية، تهاوت أمامها الحدود السياسية و الحواجز بين الدول و الشعوب، وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت وطوت الأبعاد، بما تتميز به من عنصري السرعة والدقة في تجميع للمعلومات، تخزينها ومعالجتها، ومن ثم نقلها و تبادلها عن بعد بين الأطراف المختلفة داخل الدولة الواحدة أو بين عدة الدول، حتى أضحت فيه الكرة الأرضية قرية صغيرة تسبح في فضاء الكتروني. وهو ما دعا بالكثير من المفكرين إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر، ففي حين كان الهدف من الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فان هدف الثورة الثانية إحلال الآلة محل النشاط الذهني للإنسان.

ولا شك أن هذه الثورة المعلوماتية الهائلة قد انعكست بصورة إيجابية على كثير من جوانب الحياة المعاصرة، بسبب ما توفره من الوقت والجهد والتكلفة عن الإنسان تجعل حياته اليومية أكثر سهولة و يسر، الأمر الذي أدى إلى تضاعف الطلب على التقنيات التي تقوم عليها هذه الثورة والمتمثلة في الحواسيب الآلية والشبكات المعلوماتية، وتوسع ميادين

استعمالها وازداد الاعتماد عليها بشكل مفرط في كل القطاعات العامة أو الخاصة، إلى حد بدا من الصعب على هذه القطاعات أداء نشاطاتها دون الاستعانة بشكل أساسي على هذه التقنيات الحديثة.

وبالرغم من المزايا والفوائد الجّمة التي تحققت وتتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات وسائل تكنولوجيات المعلومات والاتصال، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى، في الوقت ذاته، على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات .الشيء الذي استتبعه ظهور نمطا جديدا من الجرائم، لم يكن معهودا من قبل سمي بجرائم تقنية المعلومات أو الجرائم الإلكترونية او الجرائم السبيرانية .

ولا جدال في اعتبار الجرائم السبيرانة من أخطر و أعقد الجرائم على الإطلاق و تأتي في مقدمة الأشكال الجديدة للجريمة المنظمة ، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها وخصوصية مرتكبيها و وسائل كشفها. فهي جريمة تقنية سهلة الارتكاب، تنشأ في الخفاء وفي بيئة الكترونية افتراضية مكونة من إشارات وذبذبات مغناطيسية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصالات بصورة آلية دون أن تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات

ويتمتعون بمهارات و خبرات تقنية عالية، فضلا على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأية سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي.

وقد أدت هذه الخصائص التي تميز الجريمة الإلكترونية إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية مع ما قد يشكله ذلك من مساس بمبدأ الشرعية الجزائية والتفسير الضيق للنص الجنائي ، وهو ما ألقى مسؤولية كبيرة على عاتق المشرع الجزائري في اتخاذ الخطوات التشريعية الضرورية لمواجهة الجرائم السبيرانية الناشئة عن إساءة استخدام الأنظمة المعلوماتية . وذلك بسن نصوص جنائية جديدة تتوافق مع هذه الأنشطة الإجرامية المستحدثة، وتمّكن مرفق العدالة الجنائية من تطوير آليات ووسائل التصدي للجرائم التي افرزتها تكنولوجية الإعلام و الاتصال، والاستفادة من معطيات هذه التكنولوجيا الحديثة في الكشف عن الجرائم واثباتها وملاحقة مرتكبيها لتقديمهم إلى العدالة.

ولا تقتصر الصعوبات والمشكلات التي تثيرها ظاهرة الإجرام السبيراني فقط على القانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الإجرام، بل امتدت إلى نطاق القانون الجنائي الإجرائي، حيث صيغت نصوصه لتنظم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كثيرة في إثباتها أو

التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتتجسد أولى المشكلات الإجرائية في مجال الجرائم السبيرانية، في التحديات القانونية والعملية التي تثيرها عملية البحث والتنقيب أمام سلطات التحقيق بجميع مستوياتها وباختلاف أدواها . وبالتحديد فيما يخص إثبات هذه الجرائم والآلية المناسبة لمباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية وصولا الى الحقيقة. إذ أن الجهات المكلفة بالبحث والتحري متعودة على التعامل مع الجريمة التقليدية، التي ترتكب في عالم مادي و ملموس يلعب فيه السلوك المادي الدور الأكبر والأهم، ويسهل التحري والبحث فيها بالنظر إلى ما تتضمنه من عناصر مادية يمكن إدراكها بالحواس، وما يمكن أن يخلفه المجرم من أثار محسوسة في مسرح الجريمة من بصمات أو قطرات دم أو محررات مزورة...، على خلاف الجريمة السبيرانية التي ترتكب في مسرح افتراضي الكتروني غير مادي يختلف تماما عن المسرح التقليدي، ولا يخلف مرتكبها أي أثار، بسبب دقة وسرعة اقترافها، وإمكانية محو أثارها، وإخفاء الأدلة المحصلة عقب وقوعها مباشرة .وهو ما يجعل سلطات البحث والتحقيق في حيرة من أمرهم إزاء هذه الوقائع الاستثنائية غير المألوفة.

ويزداد الوضع تعقيدا بالنسبة لجهات الاستدلال حينما يتعلق التحقيق بجريمة سبيرانية امتد أثارها إلى خارج الإقليم الوطني، بحيث تثير مسألة تتبعها و الدخول إليها قصد جمعها

وتحويلها إلى الدولة التي يجري فيها التحقيق مشكلات تتعلق بسيادة الدولة و الولاية القضائية، والتي لا يحتاج حلها إلى تعاون دولي في هذا المجال.

ومع إدراك الصعوبة التي تطرحها المواجهة الإجرائية لأشكال الإجرام الجديدة التي افرزتها بيئة المعالجة الآلية للمعطيات والتنبه لأثارها السلبية، بدأت مهمة معالجتها تحظى باهتمام متزايد من الحكومات وحتى العديد من الهيئات الدولية، فأخذ الفنيون وخبراء الحسابات والإعلام الآلي، يركزون جهودهم البحتة وتجاربهم العلمية على سّد ثغرات الأنظمة الأمنية وتحسين وتطوير أساليب الحماية الفنية للنظم والبرامج المعلوماتية لتصل إلى أقصى درجة ممكنة من الفعالية تجنبا لوقوع اعتداءات عليها أو بواسطتها، وتكّفل الفقه الجنائي بإبراز أوجه القصور التي تعترى تطبيق النصوص الإجرائية للتشريعات التقليدية القائمة على النمط الإجرامي الجديد الذي أسفرت عنه المعلوماتية، وسعى المشرع إلى تدارك هذا القصور باستحداث نصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، تمكن رجال العدالة الجنائية من البحث والتحقيق واستنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم. ومن ثم تحقيق التوازن بين الضرورة الملحة في عصرنا إلى الاستفادة من إمكانات الحسابات و تقنيات التكنولوجيا الحديثة، وبين الحاجة الفردية والاجتماعية إلى الحماية الجزائية من انعكاسات هذه التقنيات.

ومن هنا يظهر لنا الاهمية البالغة لموضوع الجرائم السبيرانية في القانون الجزائري الذي سنتطرق له من خلال بحثا هذا .

- أهمية البحث:

ترجع أهمية هذا البحث إلى أنه من الموضوعات الحديثة المرتبطة بتطور وسائل الاتصالات الحديثة.

إن اختيار موضوع الجرائم السيبرانية في التسريع الجزائري يرجع الى اهمية هذا الموضوع وكذا انه من الموضوعات المستحدثة التي غزت الاوساط الجزائرية مثله مثل باقي الدول، وهو ذا قيمة اقتصادية لا تقل بأي حال من الأحوال عن قيمة الأشياء المادية، ويتعين وضع نظام ملائم لحمايتها.

من الناحية الجنائية والجزائية. ومما زاد من أهمية هذا البحث هو ظهور أنماط إجرامية مستحدثة بشأن الاعتداء على المعلومات على شبكة الانترنت وانتهاك الخصوصية الشخصية. مما جعل الفقه والقضاء المقارن يحاول التصدي لهذه الظاهرة وكذا المشرع الجزائري من خلال وضعه لبعض النصوص التي أدرجها في هذا الشأن.

وهذا ما سوف نعالجه في موضوعنا وذلك ببيان ماهية الجرائم السيبرانية، خصائصها وأنواعها، والجهود المبذولة للتصدي لها وذلك من خلال محاولة المشرع لسد الفراغ التشريعي في القوانين القائمة.

- أسباب اختيار الموضوع :

إن سبب اختيار موضوع " الجرائم السبيرانية في القانون الجزائري " هي الرغبة في التعرف على هذا النوع من الجرائم ،الذي تعاني منه الدول المتقدمة وعرفته الدولة الجزائرية في الآونة الأخيرة حيث ان هذا الأخير قد تفش في مجتمعنا هذا من ، ومن جهة أخرى هو الفضول لمعرفة الآليات والإجراءات وكذا الهيئات التي اتخذتها الدولة الجزائرية لمجابهة ومكافحة هذا النوع من الجرائم .

إن هذا الموضوع مازال محل دراسة وبحث نظرا للتطور التكنولوجي المستمر وتطور استخدامات الانترنت كذلك.

- أهداف البحث:

إن الهدف من هذه الدراسة يتمثل في الآتي:

- التعرف على ماهية الجرائم السيبرانية في التشريع الجزائري.
- بيان مدى صلاحية النصوص التقليدية في التعامل مع جرائم السيبرانية المستحدثة.
- موقف المشرع الجزائري من الجرائم السيبرانية وما استحدثه من قوانين لمواكبة هذه الجرائري .

- إشكالية البحث:

ما هي الخصوصية التي تتميز بها الجريمة السيبرانية وما مدى فعالية النصوص القانونية المقررة لمواجهتها ؟

- المنهج المتبع:

وللاجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي، لان بحثنا هذا سيرتكز على وصف المفاهيم العامة والخاصة بالإجراءات المتبعة للبحث والتحقيق في الجرائم السبيرانية .

- خطة الدراسة

بهدف الإجابة على إشكالية البحث قسم موضوع الدراسة الى فصلين، حيث جاء في الفصل الأول الإطار المفاهيمي للجريمة السيبرانية والذي من خلاله تم التطرق الى مفهوم الجريمة السبيرانية إضافة إلى دوافع ارتكابها وكذا خصائصها بالإضافة إلى أنواعها وكذا تبيان موقف المشرع الجزائري من هذه الجريمة ،ثم ياتي بعد ذلك الفصل الثاني تحت عنوان آليات التصدي للجريمة السبيرانية في القانون الجرائري الذي من خلاله سنتعرف على الهيئات المتخصصة في هذا النوع من الجرائم، وكذا الإجراءات المتبعة للتصدي للجريمة السيبرانية ، وأخيرا خاتمة تضمنت أهم النتائج والتوصيات التي خلص إليها هذا البحث .

الفصل الأول

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشروع للكمبيوتر كأداة لارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به التي ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها لنذهب بالقول أننا أمام عولمة الجريمة، وإن كان في نطاق تطبيق نصوص القانون الجنائي، إلا أنه يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، سواء من حيث محل الجريمة أو أسباب ارتكابها أوصفات المجرم السبيراني فالجريمة هنا جريمة سبيرانية تتعلق بالتقنية المعتمدة على المعالجة الالية للمعطيات ، ومن خلال ما تقدم سنتعرف من خلال هذا الفصل إلى المفاهيم العامة للجريمة السبيرانية وذلك من خلال مبحثين، نتطرق في المبحث الأول إلى مفهوم الجريمة السبيرانية وفي المبحث الثاني إلى خصائص وانواع الجريمة السبيرانية في القانون الجزائري .

ماهية الجريمة السيبرانية

الجريمة السيبرانية جريمة مستحدثة، يعتمد مرتكبها على وسائل تقنية، ويكون ذا دراية كافية باستخدام الّنظم المعلوماتية، لذا فإّن الإحاطة بمفهومها الّدقيق لا يزال محل خلاف فقهي، وعليه نذكر بعض المفاهيم حول الجريمة السيبرانية وكذا موضوعاتها[1].

المبحث الأول: مفهوم الجريمة السيبرانية

الجريمة هي فعل غير مشروع صادر عن إرادة جنائية، ويقّرر القانون لهذا الفعل عقوبة او تدبيرا امنيا، وكان من نتائج التّطور التكنولوجي في الوقت الراهن وجود ثّمة علاقة ارتباط القانون والجريمة[2].

المطلب الأول: المفهوم العام للجريمة السيبرانية

الجريمة السيبرانية هي فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المآدية أو المعنوية أو الاعتداء على خصوصية للأفراد، أو هي عمل أو امتناع يأتيه الإنسان إضرار بمكّونات الحاسب وشبكات الاتّصال الخاصة به، ومن جهة أخرى هي الجريمة التي يكون الّنظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إّما ضّد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضّد الأشخاص كجريمة السب أو القذف عبر

الإنترنت.[3]

أما في الجزائر فقد عالج الأمر10/97 :المتعلق بحماية حق المؤّلف والحقوق المجاورة الملغى بالأمر 05/03مسألة التّعدي على المصّنفات المعلوماتية إْذ أدرج هذه الأخيرة بموجب المآدة 4/أ ضمن المصّنفات المحمية قانونا ، ثم صدر القانون 15/04المدرج في 10-11-2004 المعدل والمتمم لقانون العقوبات [4] ، أدرج فيه المشّرع

[1] نبيل ادريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية، كلية الحقوق والعلوم السياسية. جامعة البليدة 02، ص 29.
[2] نفس المرجع، ص 29.
[3] نفس المرجع، ص 30.
[4] القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الامر رقم 66-156 المؤرخ في 08 يونيو 1966 ، المتضمن قانون العقوبات ، الجريدة الرسمية عدد71 مؤرخة في 10 نوفمبر 2004.

قسما كاملا متعّلقا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما صدر قانونا يتضّمن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، نص على أحكام إجرائية تتعّلق بكيفيات التحقيق في هذه الجرائم ،و ادرج عقوبات تسلط على كل من يعرقل حسن سير التحقيقات القضابية في هذا المجال .

كما نجد ان فقهاء القانون الجنائي قد انقسموا الى أربعة اتجاهات لكل اتجاه اسسه المختلفة التي يعتمد ويرتكز عليها في تعريفه للجريمة السيبيرانية[1] وهي كالاتي :

الفرع الأول: التعريف القائم على أساس محل الجريمة

يرتكز أصحاب هذا الاتجاه على وسيلة ارتكاب الجريمة، طالما أن وسيلة ارتكاب الجريمة هي الكمبيوتر أو إحدى وسائل التقنية الحديثة المرتبطة به، فتعتبر الجريمة من ضمن جرائم الأنترنت[2] حيث يضيق أنصار هذا الاتجاه من نطاق هذه الجريمة، ويحصرونها في الحالات التي تمس مكونات الحاسوب غير المادية، كالبرامج والبيانات والمعطيات المخزنة في ذاكرته[3]،ومن ذلك نجد تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية حيث يرى بأنها " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[4].

وعرفها البعض الآخر بصياغة أخرى وهي: تلك الجرائم الناتجة عن استخدام التكنولوجيا والتقنية الحديثة المتمثلة في الكمبيوتر والأنترنت، بأعمال وأنشطة إجرامية تهدف إلى تحقيق عوائد ضخمة جراء أعمال غير شرعية، يعاد ضخها في الاقتصاد الدولي عبر

[1] ابتسام حمديني، أسلوب التحقيق في الجرائم الالكترونية كآلية لمكافحتها، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج ،الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11و 12افريل 2017، ص 02.

[2] يوسف صغير، الجريمة المعلوماتية المرتكبة عبر الانترنت، مذكرة ماجستير، جامعة تيزي وزوو، كلية الحقوق والعلوم السياسية،2012-2013، ص 7.

[3] عبد العالي الدريبي ومحمد صادق إسماعيل، الجريمة الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة2012، ص 32.

[4] نفس المرجع ، ص 42.

شبكة الانترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية للشراء عبر الإنترنت، أو تداولا لأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة.[1]

يرد في هذا الإطار الأستاذ فاندرسونR. Fanderson. على واضعي هذا التعريف بقوله :"ليس لمجرد أن الحاسب قد استخدم في الجريمة، أن نعتبرها من جرائم الإنترنت " والحجة التي اعتمدها في نقده، مفادها أنه لا يمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العامل الأساسي المكون لها، وأن الاعتماد فقط على الوسائل المستخدمة لتحقيقها، لا يكفي لاعتبار مجرد استخدام الحاسب الآلي في الجريمة أنها من جرائم الإنترنت.[2]

الفرع الثاني: التعريف القائم على أساس المعرفة والتحكم في التكنولوجيا

يستند أنصار هذا الاتجاه إلى معيار شخصي، إذ يجب أن يكون القائم بهذه الجرائم ملما وعارفا بتقنية المعلومات،[3]ومن قبيل هذه التعاريف نجد التعريف الذي قدمه الأستاذ ديفيد تومبسون David Tompsonللجريمة المرتكبة عبر الأنترنت بأنها " أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"، [4]كما قدم الفقيه ستين سكيولبيرجStein Schiolbergتعريفه لجرائم الحاسب بقوله: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا"[5]،ولقد أخذت وزارة العدل الأمريكية بهذا التعريف في التقرير الصادر عنها سنة 1989والمتعلق بجرائم الأنترنت [6].

[1]عبد الله عبد الكريم، جرائم المعلوماتية والانترنيت،منشورات الحلبي الحقوقية بيروت، 2005، ص.15

[2]يوسف صغير، مرجع سابق، ص 10.

[3]رحيمة نميلي، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في المؤتمر الدولي 14، طرابلس،عنوان :الجرائم الالكترونية طرابلس، يومي 24و 25 مارس 2017، ص05 .

[4]هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح آلية حربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون والكومبيوتر والانترنت، جامعة الامارات المتحدة كلية الشريعة والقانون، مجلد الثاني الطبعة الثالثة ،2004،ص407.

[5]عبد اللطيف معتوق، الاطار القانوني لمكافحة جرائم المعلوماتية في التسريع الجزائري والتسريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخضر باتنة ، كلية الحقوق والعلوم السياسية،2011-2012، ص 07.

[6]سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة ابو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية ،-2011 2010 ، ص12.

حسب منظور أصحاب هذا التعريف، لابد من توفر سمات شخصية لدى مرتكب هذه الجريمة، والمحصورة أساسا في الدراية والمعرفة التقنية.

الفرع الثالث: التعريف المرتكز حول موضوع الجريمة

يرى أصحاب هذا الاتجاه أن الجريمة السيبرانية ليست التي يكون الحاسب أداة ارتكابها، بل هي التي تقع عليه أو في نظامه، ومن نماذج مسايرة هذه الفكرة تعريف الفقيه روزنبلات Rosenblatt وبعض الخبراء الآخرين، حيث يعد رفون الجريمة السيبرانية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه "، ومن نفس المنظور يعرفها البعض بأنها غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها[1].

الفرع الرابع : التعريف القائم على أساس الجمع بين عدة معايير

نظرا لعدم نجاح الاتجاهات السابقة في وضع تعريف شامل للجريمة المرتكبة عبر الإنترنت عمد أصحاب هذا الاتجاه إلى تعريفها عن طريق دمج أكثر من تعريف، واعتبروا أن الأنترنت الجريمة المرتكبة عبر الأنترنت هي: " الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها، أو الجريمة التي يكون الحاسب الآلي نف سه ضحيتها".[2]

ورغم الانتقادات التي وجهت لهذا الاتجاه على اعتبار الجمع بين عدة معايير لتعريف الجريمة السيبرانية، إلا أن هذا التعريف يعد التعريف الراجح من الناحية العملية نظرا لتعدد صور الجرائم الإلكترونية وتطورها بتطور تقنية المعلومات.[3]

انطلاقا مما سبق ذكره يتضح أن الجريمة السيبرانية هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينها.

[1] هشام محمد فريد رستم، المرجع السابق، ص 407.
[2] ابتسام حمديني، مرجع سابق،ص05.
[3] ابتسام حمديني، مرجع سابق،ص05.

الفرع الخامس : تعريف المشرع الجزائري للإجرام السيبراني

خلافا للمشرع الفرنسي الذي لم يعط تعريفا للجريمة السيبرانية، فإن المشرع الجزائري قد اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب الفقرة (أ) المادة 02من القانون 04/09على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."[1]

الملاحظ على تعريف المشرع الجزائري أنه قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة السيبرانية، أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكتروني، وثانيها معيار موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[2].

كما اعتمد المشرع على معيار رابع لتحديد نطاق الجريمة الإلكترونية، حيث نص على أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا من شأنه أنيوسع من دائرة التجريم في مجال الإجرام السيبراني في القانون الجزائري[3].

المطلب الثاني: دوافع ارتكاب الجريمة السيبرانية.

يقول الدكتور(ADAM GRAYCAR) مدير المعهد الأسترالي لعلم الإجرام، بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

أولا: دافع معين لارتكاب العمل.

ثانيا: هدف ضحية محاسبة.

ثالثا: الفرصة المواتية

رابعا: غياب عيون الأمن[1]:

[1]القانون رقم 09-04 المؤرخ في 05 اوت 2009يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، الصادرة بتاريخ 16اوت 2009، ص05.
[2]رحيمة نميلي، مرجع سابق، ص 06.
[3]رحيمة نميلي، مرجع سابق، ص06

إذا فالدافع والقصد يشكل أحد الركائز في جميع الجرائم. وبالنسبة لجرائم الحاسب الآلي والإنترنت فهي لا تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية.[2] فثمة دوافع عديدة تحرك العينات لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم، ويمكن تلخيص هذه الدوافع فيما يلي:

الفرع الاول :الدوافع الشخصية.

اولا : الدوافع المادية:

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية. ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب الذي يتيح تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على ذلك ما حدث في فرنسا سنة 1986حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000فرنك فرنسي أي ما يعادل أكثر من 38 مرة.

ومنذ بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الإنترنت هو تحقيق الكسب المالي، ففي دراسة الفقيه Parkerالصادرة في إحدى مجلات المتخصصة بخصوص موضوع الأمن المعلوماتي تبين أن:

34% من جرائم الغش المعلوماتي من أجل اختلاس الأموال.

23% من أجل سرقة المعلومات

19% من أجل الإتلاف.

[1] فايز بن عبد الله الشهري، التحديات الامنية المصاحبة لوسائل الاتصال الجديد دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي arablawinf ، ص 09.

[2] نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، سنة 2005 بيروت، ص 63.

15% من أجل سرقة وقت الحاسوب لأغراض شخصية.

وإذا انتقلنا للدراسات الحديثة، فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات المسحية والإحصائية الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية.

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة

ثانيا: الدوافع الذهنية أو النمطية

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنيت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون إيجاد الوسيلة إلى تحطيمها، أو التفوق عليها.

الفرع الثاني: الدوافع الخارجية

أولا : دافع الانتقام وإلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات و ديون المنشأة ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معنية، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة،

مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل.

وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.[1]

ثانيا : الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية

يميل مرتكبوا هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها وغالبا ما يجدون الوسيلة التي تحيطها، ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات لإظهار تفوقهم على الوسائل التقنية.

إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الإجرامية (مجموعات الجريمة المنظمة)لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة. هذا وإن كان الفعل الواحد قد يعكس دوافع متعددة وخاصة، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات دوافعه سياسية وإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، وقد تتداخل وتشترك هذه الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينها.[2]

المطلب الثالث: أركان الجريمة السيبرانية.

لا تختلف أركان الجريمة السيبرانية عن أركان أي جريمة أخرى فلابد من توافر الركن المادي والركن المعنوي وما يميزه هو الركن المفترض وهذا ما نستعرضه في هدا المطلب وهو كالأتي :

[1] هيام حاجب ، الجريمة المعلوماتية، مذكرة لنيل إجازة المدرسة العليا للقضاء، الجزائر،2005-2006، ص14.
[2] هيام حاجب ، المرجع نفسه، ص 15.

الفرع الأول: الركن المادي

ويعرف بأنه: "النشاط المادي الذي يصدر عن الجاني متخذا مظهرا خارجيا يتدخل من أجله القانون بتقرير العقاب".

ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية، بمعنى أن الركن المادي يتكون من ثلاث عناصر.

أولا: السلوك الإجرامي:

وصوره متعددة كالسلوك الإجرامي الإيجابي وذلك بمخالفته نصا ينهي عن الإتيان بهذا الفعل كسرقة بيت أو جهاز معين، سواء كان التحرك الإيجابي بحركة واحدة كالقتل بالرصاص، أو بحركات متعددة كالمشاجرة التي تنتهي بالوفاة.

وقد يكون سلبيا بمخالفة نص يأمر بإتيان فعل معين، كامتناع ممرضة عن إعطاء جرعة الدواء لمريضها العاجز بما يؤدي لوفاته.

وقد يكون السلوك الإجرامي بصورة بسيطة كما في جريمة القذف، وقد تكون بصورة معقدة كما في جريمة الإرهاب أو السطو المسلح فالقانون الجنائي لا يعول كثيرا على الوسيلة التي ارتكبت بها الجريمة أووقع بها السلوك الإجرامي ولا يعتد بزمان أو مكان وقوع الجريمة إلا عند تقديره للظروف المشددة أو المخففة، فيستوي القتل أن يكون بمسدس أو بالسكين، أو حتى عن طريق الريموت كنترول أو بواسطة أجهزة الحاسوب.

فأهمية هذه الصور المجرمة والظروف المصاحبة لها تظهر مدى توافر القصد الجنائي، كما تفيد تحديد الاختصاص القضائي، والقانون واجب التطبيق، وبدء سريان مدة التقادم في الأنظمة المقارنة.[1]

[1] روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24، شهر 5 سنة 2020، ص 21وما بعدها.

كما يمكن تقسيم وتكييف الجرائم بنفس تقسيم الجرائم التقليدية، وذلك حين تتشابه معها في ذات السلوك الإجرامي.

ثانيا: النتيجة الإجرامية

وتثير مسألة النتيجة الإجرامية في الجرائم السيبرانية جدلا كبيرا بين أنصار المذهب المادي وأنصار المذهب القانوني حول تحديد الجريمة السيبرانية هل هي جرائم مرتكبة سلوكا أو كنتيجة في العالم الافتراضي، أم أن هناك امتدادا للنتيجة لتحقيق وجودها المادي وتنقسم النتيجة الإجرامية إلى قسمين:

1-جرائم الضرر : هي التي يطلب القانون في ركنها المادي حصول ضرر معين، وذلك مثل حصول الضرر في الجرائم السلبية والإيجابية.

2-جرائم الخطر: فهر جرائم السلوك المجرد حتى لو لم تقع النتيجة الإجرامية وكذلك كما في جرائم المشروع والتي تعاقب عليها الأنظمة في حالة كونها جناية ، وذلك لما يمثله السلوك الإجرامي من خطر دون النظر في نتيجة ذلك الفعل، بينما يختلف الأمر في الجنح والمخالفات فلا يعاقب عليها القانون بصفة عامة نظرا لقلة خطورة الدافع الإجرامي في نفس الفاعل[1].

ثالثا: علاقة السببية

لم يحدد القانون الجنائي معيارا لتحديد الرابطة السببية، فناقش علماء القانون واستقر رأيهم على ثلاث نظريات:

1-نظرية تعادل الأسباب: وهي تساوي جميع العوامل التي تساهم في إحداث النتيجة الإجرامية، فهي متعادلة من حيث قوة أثرها في حصول النتيجة.

[1] روان بنت عطية الصحفي ، المرجع السابق ، ص23 وما بعدها .

2-نظرية السبب الأقوى أو السبب المباشر: فهي لا تساوي بين الأسباب المساهمة فيحصول الجريمة، بل تنظر إلى السبب الأقوى سواء كان هو سلوك الجاني أو غيره،وهذه النظرية حصرت النتيجة في عامل واحد هو أقوى الأسباب، وهذا يؤدي بالجاني إلى الإفلات من العقاب.

3- نظرية السببية الملائمة: ومضمونها أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله وذلك حسب المجرى العادي للأمور، ما لم يتدخل لقطع تلك العلاقة سبب شاذ أو غير مألوف، وقد تكون هذه النظرية هي أنسب النظريات ظن (فلو أرسل الجانيفيروسا) إلى بريد المجني عليه الالكتروني مما تسبب في تلف الجهاز بالكامل لدى فتح المجني عليه بريده الالكتروني، فهذا سبب مباشر يسأل الجاني عنه،بينما لو كان المجني عليه قد أُرسلت له عدة فيروسات من عدة أشخاص وتسببت بمجموعها بتلف الجهاز، فإن القضاء حينئذ يعمل إحدى النظريات السابقة[1].

الفرع الثاني: الركن المعنوي

إن الركن المعنوي في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتّخذ صورة القصد الجنائي.

أولا : الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

إن الركن المعنوي لجريمة الدخول والبقاء غير المشروعين، يتّخذ صورة القصد الجنائي من علم و إرادة باعتبارها من الجرائم العمدية، وقد عبر نص المادة 394 مكرر عن القصد الجنائي العام بتطلُّبه أن يكون الدخول أو البقاء "عن طريق الغش"، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات

[1] المرجع السابق، ص 24و 25.

غير مشروع، وهو نفس ما عبر عنه المشرع الفرنسي فينص المادة 1/323 بعبارة **.Frauduleusement**

يتطلّب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وبناء أركانها، واستكمال عناصرها، وخاصة الركن المادي منها، و أو لهذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج، باعتباره محل الحق الذي يحميه المشرع، فإذا اعتقد الفاعل بناء على أسباب معقولة بأنّه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، دون أن يتّجه علمه إلى أنه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات،فإن قصد الدخول أو البقاء لا يتوفّر فيه [1].

كذلك يتعين أن يعلم بخطورة الفعل الذي يقوم به، فإذا كان غير ذلك ينتفي القصد الجنائي. يتطلّب القصد الجنائي أيضا أن يتوقّع الجاني النّتيجة الإجرامية التي ستترتّب عن القيام بفعله، فتوقّع النتيجة هو أساس النّفي الذي تقوم عليه إرادتها، فحيث لا يكون التّوقّع لا نتصور الإرادة، والنّتيجة التي يجب أن يتّجه إليها توقّع الفاعل هي النّتيجة التي يحددها القانون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

ولا يشترط أن يتوقّع الضرر الذي سوف يلحق النِّظام أو صاحبه من جراء هذا الدخول[2]، فإذا توقّع الفاعل أنّه بصدد الدخول إلى نظام معين، ثم ترتّب على فعله الدخول إلى نظام آخر، فإن القصد الجنائي يظلُّ متوافراً لديه.

وهناك وقائع يسأل فيها الجاني عن الجريمة دون أن يتطلّب القانون علمه بها، فحين يقرر القانون لبعض الجرائم عقاباً معيناً إذا أحدث الفعل نتيجة ذات جسامة معنية،وإذا ازدادت جسامة هذه النّتيجة فأفضت إلى نتيجة أشد جسامة، شدد القانون العقاب، ويتطلّب

[1] نائلة عادل، مرجع سابق، ص 365.
[2] نفس المرجع، ص 366.

المشرع انصراف القصد الجنائي إلى النّتيجة الأقل جسامة ولكنّه لا يتطلّب انصرافه إلى النّتيجة الأشد جسامة، بحيث يسأل الجاني عنها بالرغم منعدم توقُّعها لها[1].

وهذا ما ينطبق على الفقرة الثّانية والثّالثة من المادة 394مكرر من قانون العقوبات،حيث يعاقب الجاني على النّتيجة الأشد بمجرد ترتُّبها عن الدخول أو البقاء غير المشروع الذي قصده.

ويجب أن يعلم مرتكب جريمة الدخول أو البقاء غير المشروعين داخل نظم المعالجة الآلية للمعطيات، أن دخوله إلى هذا النِّظام غير مشروع أو غير مصرح به، فلا يتوافر القصد الجنائي إذا وقع الجاني في خطأ، كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأً أنّه مسموح له بالدخول أو البقاء.

أما بالنِّسبة لإرادة الجاني فيجب أن تتّجه إلى الدخول أو البقاء غير المشروع يتداخل النّظام، أي أن تتّجه إرادته لتحقيق هذه النّتيجة، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول أو البقاء سواء كان هذا الباعث هو الفضول، أو إثبات القدرة على المهارة والانتصار على النِّظام، حتى وإن كانت الغاية نبيلة كمن يدخل إلى النِّظام غير المصرح له بالدخول رغبةً في الكشف عن أوجه القصور التي تعتري النِّظام الذي تمكّن من الدخول إليه، وذلك لتجنُّب هذا القصور مستقبلا[2].

ثانيا :الركن المعنوي للاعتداءات على سير نظام المعالجة الآلية للمعطيات والاعتداءات على المعطيات خارج وداخل النظام:

إن الاعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التّعطيل أو العرقلة، وإفساد النّظام، لا تكون إلاّ عمدية هذا ما يميزها عن الاعتداء غير العمدي لسير النِّظام الذي يشكِّل ظرفاً مشدداً لجريمة الدخول والبقاء غير المشروعين داخل النِّظام [3].

[1]نفس المرجع، ص 367 .
[2]نائلة عادل ، المرجع السابق ، ص 368.
[3]امال قارة،الحماية الجزائية للمعلوماتية في التسريع الجزائري، الطبعة الأولى، دار هومة الجزائر ، ص 124.

وهذه الاعتداءات تتطلّب القصد الجنائي العام من علم وإرادة، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنّه يقوم بإحدى هذه الأعمال التي أوردها النّص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التّعديل، ويعلم خطورة النّشاط الإجرامي الذي يقوم به وما يترتّب عنه من عقاب.

كما يجب أن تتّجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التّعديل، فلا يسأل من قام بذلك خطأً أو عن غير قصد، بل يسأل طبقاً للمادة 394مكرر 2/**3**التي تتناول الصورة المشددة لجريمة الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات، كونها تعاقب الفاعل عن الحذف والتّغيير المترتّب عن الدخول أو البقاء غير المشروعين حتى وإن كان خطأً، كون أن نص المادة 394 مكرر 1من قانون العقوبات اشترط أن ترتكب هذه الأفعال "بطريق الغش".

وهي العبارة المستعملة كذلك في نص المادة 3/323 من قانون العقوبات الفرنسي **Frauduleusement** أي أن يعلم أنّه ليس له الحق في القيام بذلك، وأنّه يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته . ولا يتطلّب نص المادة 394 مكرر 1 قصداً جنائياً خاصاً، إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التّشريعات المقارنة التي اشترطت قصدا خاصا إلى جانب القصد العام، يتمثّل في اتّجاه نية المتّهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير،وهو ما كان عليه النّص الفرنسي القديم قبل تعديله، ويبرز ذلك في عبارة "ارتكاب الفعل دون مراعاة حقوق الآخرين. "وقد انتُقدت هذه المادة قبل تعديلها بشدة لتطلُّبها القصد الجنائي الخاص، كون أن اشتراط هذا القصد الخاص سوف يؤدي إلى اللاّعقاب في الحالات التي لا تتّجه فيها نية الفاعل إلى تحقيق ربح، على الرغم من أهمية المعلومات التي قد يتم إتلافها، مثل إتلاف معلومات علمية [1].

[1] نائلة عادل، مرجع سابق، ص 368.

وهو ما دعا المشرع الفرنسي إلى استبعاد القصد الخاص من هذه الاعتداءات العمدية، حيث اقتبس المشرع الجزائري نص المادة 394 مكرر 1من نص المادة 3/323 المعدلة من قانون العقوبات الفرنسي.

أما بالنسبة للاعتداءات العمدية الماسة بالمعطيات الموجودة خارج النظام، فيجب لقيام الركن المعنوي أن يتوافر القصد الجنائي العام، وهو ما عبرت عنه المادة 294 مكرر 2 بعبارة "كل من يقوم عمداً وعن طريق الغش".

بالتّالي يجب توافر العلم والإرادة لدى الجاني لقيام الركن المعنوي، فيجب أن يكون عالما أن المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك بتصميمه أو بحثه أو تجميعه أو توفيره أو نشره أو الاتّجار في هذه المعطيات، أي علمه بأن هذه المعطيات يمكن أن تكون وسيلة لارتكاب الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

ويجب أن يعلم الجاني كذلك، أن إتيانه أحد الأفعال السابقة ينصب على معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، وكذلك أن يعلم بخطورة الفعل الذي يقوم به، وأن يتوقّع النّتيجة المترتِّبة عن القيام بأحد الأفعال السابقة.

الفرع الثالث: الركن المفترض

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة من جرائم الاعتداء على هذا النظام.

ويؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية، إذ أن هذا الشرط يعتبر عنصرا لازما، ولذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات ومدى خضوع هذا النظام لحماية فنية.

أولا : تعريف نظام المعالجة الآلية للمعطيات.

هو تعبير فنِّي تقني متطور، يخضع للتطورات السريعة والمتلاحقة في مجال الإعلام الآلي، ولذلك لم يعرف المشرع الجزائري على غرار المشرع الفرنسي نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من الفقه والقضاء.

حيث قدمت المادة الأولى من الاتّفاقية الدولية للإجرام المعلوماتي تعريفا للنّظام المعلوماتي على النّحو التالي[1]:

"قصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتّصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات". ويقصد بـ "بيانات الكمبيوتر" أية عملية عرض للوقائع،أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها"

أماّ الفقه الفرنسي، فقد عرفه من خلال الأعمال التّحضيرية للمادة 1/323 من قانون العقوبات الفرنسي، الذي تبنّى التّعريف الوارد في القانون الخاص بالمعلوماتية وحماية الحريات لسنة ،1978بأنَّه "كلُّ مركّب من وحدة أو مجموعة وحدات للمعالجة،والتي تتكون كل منها من الذّاكرة و البرامج والمعطيات وأجهزة الإدخال والإخراج،وأجهزة الربط التي تربط بين العناصر المختلفة للنظام، كالشّاشة ولوحة المفاتيح والطّابعة والبطاقات المغناطيسية التي تشكِّل وسيلة للدخول، والتي تربط بينها مجموعة من العلاقات التي عن طريقها تتحقّق نتيجة معينة، وهي معالجة المعطيات، على أن يكون هذا المركَّب خاضع لنظام الحماية الفني"[2].

وهذه العناصر المادية والمعنوية التي يتكون منها المركَّب، واردة على سبيل المثال لا الحصر، فيمكن إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التّقني

[1] امال قارة، مرجع سابق، ص 102.
[2] نائلة عادل محمد فريد قورة، مرجع سابق ، ص131.

في هذا المجال. فإذا تم الاعتداء على أحد هذه العناصر بمعزل عن النّظام، فلا تقوم الجريمة، فلا بدمن الاتّصال بينها

ويكون نظام المعالجة الآلية للمعطيات في طور التّشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النِّظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاّحقة [1].

ثانيا : الحماية الفنّية لأنظمة المعالجة الآلية للمعطيات

تكفل بعض القواعد الأمنية الحماية لنظم المعالجة الآلية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها، ويتأتّى ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن بين هذه القواعد، أُسلوب يعتمد على توزيع العملياّت التي يقوم بها نظام المعالجة الآلية للمعطيات ونقلها إلى نظام احتياطي (مركز للمساعدة) عند الضرورة، ويلجأ إلى هذا الأسلوب عادة البنوك وشركات التّأمين، ويظلّ هذا الموقع سرا ويخضع لدرجة عالية من الحماية، ومن الأساليب المستعملة كذلك، الاعتماد على الاختبارات الفيزيولوجية للدخول إلى النِّظام عن طريق التحقّق من شخصية القائم بعملية الدخول عن طريق بصمة الأصبع أو نبرة الصوت أو شكل الأذن أو شبكية العين[2].

لكن يبقى نظام التّشفير لحماية المعلومات هو الأسلوب الواسع الانتشار، خاصة البيانات المتناقلة عبر الشّبكات، كشبكات الإنترنت، لما تنطوي عليه من سرية البيانات الشخصية كالرسائل الإلكترونية وكذا البيانات الخاصة بالأعمال التجارية الرقمية[3].

[1] المرجع نفسه، ص 131.
[2] نائلة عادل، المرجع نفسه، ص353 .
[3] امال قارة، مرجع سابق، ص 103.

ويقوم نظام التّشفير على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحلّ رموزه، يعرفه عادةً مرسل المعلومات والمرسل إليه، وفي داخل جهاز الكمبيوتر توجد أجهزة مهمتها التّحقُّق من شخصية القائم بعملية الدخول عن طريق الشّفرة.

وقد ثار التّساؤل حول ضرورة وجود أو عدم وجود حماية للنّظام كشرط للتمتّع بالحماية الجنائية؟

فبالرجوع إلى نص المادة 394 مكرر[1] من قانون العقوبات، لا نجد إشارة إلى ضرورة خضوع النِّظام للحماية الفنية حتى يتمتع بالحماية الجنائية، وكذلك الشّأن بالنّسبة للمادة 1/323 من قانون العقوبات الفرنسي، ويظهر من خلال الأعمال التّحضيرية لقانون، 1988 المتعلّق بالمعلوماتية والمقتبسة منه المادة، 1/323 أنه كان من المقترح ضرورة شمول النّص بهذا الشرط، ولكن اشتراط وجود حماية أمنية في نظام المعالجة الآلية للمعطيات لم يتم الاتّفاق عليه في المناقشات الأخيرة في البرلمان الفرنسي، ولذلك جاء النّص خالياً من هذا الشَّرط، ووجد أن هذا الشّرط قد يؤدي إلى الحد من الحماية الجنائية للنُّظم غير المشمولة بتجهيزات أمنية داخل النِّظام.

ولذلك اكتفى المشرع الفرنسي في النَّص النِّهائي بأن يكون التوصل قد تم"بطريق الغش"، وهذا التَّعبير يترك تفسيره لقاضي الموضوع[2].

وهذا ما فتح أبواب النِّقاش حول هذه النُّقطة من خلال ظهور رأيين مختلفين:

الرأي الأول: يقول بعدم جدارة الأنظمة التي لا تحميها نظم أمنية بالحماية الجنائية، كون أنّه من غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أي إجراءا تتكفل لها الحماية ويقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية

[1] تنص المادة 394مكرر من قانون العقوبات":يعاقب بالحبس من ثلاثة اشهر الى سنة وبغرامة من 50000 دج الى 100000دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

[2] صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،عين للدراسات والبحوث انسانية والاجتماعية ، القاهرة ، 2003، ص117.

للمعطيات على جريمة انتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بغير رضاء صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوباً باستعمال وسائل تدلّ على عدم رضا صاحب المسكن.

ويستند أنصار هذا الرأي إلى عدة أسباب تنصب جميعها في اتجاه واحد هو ضرورة أن يكون هناك نظم أمنية يتم اختراقها لامتداد الحماية الجزائية للمعلومات، وأول هذه الأسباب يتعلّق بالمادة 28من القانون 07/78 لسنة 1978الخاص بالمعلوماتية وحماية الحريات الفرنسي، حيث تتطلّب أن تكون الأنظمة مشمولة بتدابير أمنية لحمايتها، والسبب الثاني يكمن في إقامة الدليل على قيام الركن المادي للجريمة وكذا التّحقُّق من توافر القصد الجنائي لدى مرتكبها، لأن اختراق الأنظمة الأمنيّة من طرف الفاعل يترك أثراً، ويؤكِّد طريق الغش والاحتيال الذي سلكه.

الرأي الثاني: فهو يذهب إلى أنَّه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائيا بغض النّظر إن كانت تتمتّع بحماية النّظم الأمنية من عدمه، ويقيس أنصار هذا الاتِّجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتُّع المال المسروق بحماية صاحبه أو عدم تمتُّعه بهذه الحماية لا يؤثّر في قيام جريمة السرقة، بغض النّظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كما أن تطلُّب مثل هذا الشّرط يضيق من تطبيق الحماية الجزائية، ويتجاهل الحالات التي يتم فيها الدخول إلى النّظام نتيجة خطأٍ قام به المبرمجون، أو المسؤولون عن أمن النِّظام[1].

هذا الرأي هو الأقرب إلى الصواب استنادا إلى المبادئ العامة المستقرة في القانون الجنائي كحرفية النّص، وعدم جواز تقييد النّص المطلق أو تخصيص النّص العام، إلاّ إذا وجد نص يجيز ذلك، ولا يوجد في حالتنا نص خاص يقيد إطلاق النّص أو يخصص

[1] نائلة عادل، مرجع سابق، ص 355.

عمومه، وبالتّالي يجب التزام حرفية النّص في التّفسير، فعدم ذكر المشرع لشرط الحماية الفنّية يعني أن المشرع أراد استبعاده[1].

وأكّدت محكمة استئناف باريس في حكم صادر لها في 05/04/1994 على أنّه من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النِّظام.

المبحث الثاني: خصائص وأنواع الجريمة السيبرانية في القانون الجزائري.

من خلال هذا المبحث سوف نتعرض إلى كل من خصائص الجريمة السبيرانية وكذا أنواعها بالاضافة إلى موقف المشرع الجزائري في ثلاث مطالب وهي كالأتي :

المطلب الأول: أنواع الجرائم السيبرانية في القانون الجزائري

لقد اختلف الفقه والقانون في تصنيف الجرائم الالكترونية باختلاف الزاوية التي ينظر منها إزاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي.[2]

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية[3]. على خلاف هذه الجريمة، فإن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه[4].

---

[1] امال قارة، مرجع سابق، ص105.

[2] رحيمة نميلي ، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، اعمال المؤتمر الدولي الرابع عشر،الجرائم الالكترونية ، طرابلس، يومي 24و25مارس 2017، ص 08.

[3] حسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 1، الديوان الوطني للأشغال التربوية،الجزائر،2002 ،ص 24.

[4] فتيحة رصاع ، الحماية الجنائية للمعلومات على شبكة الانترنت،رسالة ماجستير ، جامعة ابي بكر بلقايد تلمسان ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، 2011-2012، ص 69.

أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات،وهذا ما سيتم بيانه في الفرعين الموالين.

الفرع الأول: الجريمة السيبرانية المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص،الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار[1]، وسأوضح كل نوع منها في البنود الآتية.

أولا : الجريمة السيبرانية الواقعة على الأشخاص الطبيعية.

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

1-الجريمة السيبرانية الواقعة على حقوق الملكية الفكرية:

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع.وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية

[1]سفيان سوير ،مردع سابق ، ص 33.

وهي الأمر رقم 05/03الصادر في 2003 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، والأمر رقم 07/03الصادر في 2003 المتعلق ببراءات الاختراع[1].

2- الجريمة السيبرانية الواقعة على حرمة الحياة الخاصة:

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة .ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها باطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

ثانيا : الجريمة السيبرانية الواقعة على النظم المعلوماتية الأخرى:

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى ،بالإضافة إلى إساءة استخدام البطاقة الائتمانية.

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الاستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة،أو استخدام شاشة النظام، أو الاطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة إساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة

[1] سفيان سوير ، المرجع السابق، ص 34وما بعدها .

صلاحيتها أو تم إلغاؤها، أما الحالة اما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات[1].

ثالثا : الجريمة السيبرانية الواقعة على الأسرار.

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة .ويتخذ هذا النوع من الجرائم صورتين،الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[2]،حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة فيما يتعلق بالدول التي يكون فيها نزاعات[3]،والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية،والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أوبيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل[4].

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات،بالإضافة إلى المادة 394 مكرر 03 التي تنص على: "تضاعف العقوبات المنصوص عليها فبهذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد"[5].

[1] سفيان سوير ، المرجع السابق، ص ص35 ، 37 .
[2] سفيان سوير ، المرجع نفسه، ص 38 .
[3] يوسف صغير ، مرجع سابق ، ص54.
[4] سفيان سوير ، المرجع نفسه، ص 38 .
[5] الامر 04-15، القانون الصادر في 10 نوفمبر 2010 ،يعدل ويتمم الامر رقم 156/66، الصادر في 08 جوان 1966، المتم قانون العقوبات، ج ر العدد 71 .

الفرع الثاني: الجريمة السيبرانية الواقعة على النظام المعلوماتي.

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 15/04الصادر في 10 نوفمبر 2004 المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات،وذلك في المواد 394مكرر إلى 394 مكرر07 ،وتأخذ صور الاعتداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ما سأتناوله في مايلي .

أولا : جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية.

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخـول أو البقـاء تخريـب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[1].

1- فعل الدخول غير المشروع:

لا نعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الألية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2011-2012، ص 13.

في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أملا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها ،كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول إلى المنظومة.

2- فعل البقاء غير المشروع:

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في 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، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع لشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الاطلاع فقط،ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت

المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أوحصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.[1]

ثانيا :جريمة المساس بمنظومة معلوماتية.

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 15/04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش.هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل ، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل 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، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.

ثالثا : أفعال إجرامية أخرى

جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الأتية : تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر[2] ، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات

[1] حمزة بن عقون، المرجع السابق، ص 183وما بعدها .
[2] حمزة بن عقون، المرجع السابق، ص 184 .

المعلوماتية في حد ذتها[1]، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض[2].

من خلال التعرض إلى ماهية الجريمة السيبرانية، يتضح بأن لهذا النمط من الجرائم طبيعة خاصة ومتميزة، وهي جريمة ناعمة حال ارتكابها، تتجاوز حد الخشونة في نتائجها، إذ بمجرد ملامسة الجاني لزر أو أكثر من لوحة المفاتيح، قد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه، وهذا ما يؤدي إلى صعوبة في مكافحتها، ويعاب على المشرع الجزائري أنه اهتم بالجريمة السيبرانية بالنص على بعض الجرائم السيبرانية وليس كلها وأهمل المجرم السيبراني، إذ لم يتعرض له في أي نص قانوني، بالإشارة إلى تعريفه أو سماته.

كما أن التطرق لماهية الجريمة السيبرانية والتعرف عليها بعمق يفيدنا في إيجاد الحلول لمواجهتها.

المطلب الثاني: خصائص الجريمة السيبرانية.

في هذا المطلب سنحاول عرض جملة من خصائص هذه الجريمة التي سنعرضها في شكل فروع متتابع مبينين بذلك اهم ما اشتملت عليه اهم المراجع في هذا المطلب و ان من أهم هده الخصائص هي كالاتي :

الفرع الاول : جرائم صعبة الإثبات:

إن متابعة جرائم الحاسب الآلي والانترنت والكشف عنها من الصعوبة بمكان حيث إن هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من

[1] نسيم دردور ، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي،جامعة منتوري، قسنطينة،2012- 2013 ص 42 .
[2] حمزة بن عقون، مرجع سابق، ص 184 .

ارتكابها كما إن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها، وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أمور وهي:

أولا: أنها كجريمة لا تترك أثر لها بعد ارتكابها.

ثانيا: صعوبة الاحتفاظ الفني بأثرها إن وجدت.

ثالثا : أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها، والتظليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها [1].

ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص و السيمات المميزة لهذه الجريمة عن الجرائم التقليدية هي:

الفرع الثاني : جريمة عابرة للحدود

أعطى انتشار شبكة الانترنت إمكانية الوصول لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان ،لذلك فان من السهولة بمكان ان يكون المجرم في بلد ما والمجني عليه في بلد أخر، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وربط فاعليها، و حيث ان التنظيمات الداخلية متفاوتة فيما بين كل دولة من دول العالم ، تظهر العديد من المشاكل حول صاحب الاختصاص القاضي لهذه الجريمة متعلقة بإجراءات الملاحقة العقابية، وتتشابه الجرائم الالكترونية في هذه الخاصية مع بع الجرائم مثل جرائم غسيل الأموال وجرائم المخدرات[2].

[1] ياسمينة بونعار، الجريمة االالكترونية ، مجلة المعيار ، جامعة الأمير عبد القادر للعلوم الإسلامية،كلية اصول الدين ،المجلد الثاني ، العدد 39، جوان 2015، ص 280.

[2] عبد الله دغش العجمي ، رسالة ماجستير بعنوان،المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، جامعة الشرق الاوسط ، 2014 ،ص 20.

الفرع الثالث : جريمة ناعمة

تتسم الجرائم الناشئة عن استخدام الأنترنت بأنها ناعمة لخفتها ولكونها متسترة في أغلبها، كما أن الضحية لا يلاحظ ارتكابها رغم أنها قد تقع أثناء وجوده على الشبكة، فالجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، ومثال ذلك إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم[1].

ويستفيد المجرمون في مختلف مناطق العالم من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم، ويظهر ذلك جليا في مختلف المواقع الإلكترونية ومنتديات قراصنة الهاكرز التي تضمن لهم الاتصال فيما بينهم بهدف تبادل الخبرات في مجال القرصنة، من أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن[2].

فهي جرائم لا تمارس بالعنف، ولا تحتاج إلى أدني مجهود عضلي، بعكس بعض الجرائم التقليدية، ومن هنا نلاحظ بأن المجرم السيبراني يتميز بمهارات عالية، فهو يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية لإتلاف البرامج واختراق الحواجز الأمنية، ولعل الدافع للمجرمين السيبرانيين قد يكون بدافع المال بلجوئهم إلى الطرق الغير مشروعة وذلك بسبب ما يعانوه من البطالة، وقد يكون بدوافع عقائدية وسياسية، وقد يكون بدوافع شخصية كقيام الموظف بالانتقام من المؤسسة أو الشركة التي قامت بفصله، أو لتجسس وانتهاك الخصوصية[3].

الفرع الرابع: وقوع الجريمة السيبرانية أثناء المعالجة الآلية للبيانات

من خصائص الجريمة الالكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الربط الأساسي الذي يتعين توافره حتى

[1] يوسف صغير، مرجع سابق ،ص 14 و مابعدها .

[2] عبد المومن بن صغير، ، مداخلة مقدمة من فعاليات الملتقى الوطني 2015-2016، بعنوان : الجريمة المعلوماتية بين الوقاية و المكافحة ، عنوان الملتقى : "الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن" ، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة محمد خيضر بسكرة، ، يومي 16و17نوفمبر2015، ص08.

[3] روان بنت عطية الله الصحفي، المرجع السابق ، ص 13.

يمكن البحث في قيام أو عدم قيام أركان الجريمة الالكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك انه في حالة تخلف هذا الشرط تنتفي الجريمة الالكترونية.

وقد كان هناك اقتراح من قبل مجلس الشيوخ الفرنسي حال تعديل قانون العقوبات الحالي، بنوع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات، ولكن حذف هذا التعريف باعتبار أنها عملية فنية تخضع للتطور السريع، وبالتالي سيكون أي تعريف لها قاصرا ،وكان هذا التعريف ينص على: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة، البرامج، والمعطيات، و أجهزة الإدخال والإخراج، وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات، والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية ".

والجريمة الالكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الإلية للبيانات سوءا عند مرحلة إدخال البيانات أوأثناء مرحلة المعالجة، أوأثناء مرحلة إخراج المعلومات[1].

الفرع الخامس: الجريمة السيبرانية جريمة مستحدثة

تعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعد الجرائم الالكترونية سواء التي تتعرض لها أجهزة الكومبيوتر أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة، حيث ان التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدارته وإمكاناته أجهزة الدولة الرقابية، بل انه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وامن مواطنيها[2].

[1] المرجع نفسه ، ص 24.
[2] روان بنت عطية الله الصحفي ، المرجع السابق ، ص 25.

الفرع سادس: خصوصية المجرم السيبراني

قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة، ولكن الأمر مختلف تماما بالنسبة للمجرم المعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات. وقد تم تصنيف مجرمي الجرائم الالكترونية الى المخترقين والمحترفين والحاقدين.

أ. **المخترقون:** مثل الهاكرز الذي يعد شخصا بارعا في استخدام الحاسب الآلي ولديه فصول في استخدام حسابات الآخرين بطرق غير مشروعة، الامر الذي يدل على أنهم أشخاص متطفلون وغير مرحب لهم لدى الغير، الدخول الى مواقع الحسابات من اجل إثبات الذات.

ب. **المحترفون:** وهم الأكثر خطورة بين مجرمي الانترنت، حيث يهدف البعض منهم إلى الاعتداء لتحقيق الكسب الغير المشروع في الناحية المادية وذلك عبر الدخول في حسابات البنوك، والبعض الأخر يدخل من اجل تحقيق أغراض سياسية والتعبير عن وجهة نظره او فكرة، وغالبا أعمار هؤلاء تكون بين 25و40 سنة.

ج. **الحاقدون:** وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية او مادية ولكن يتحركون لرغبة الانتقام والتأثر كالأمور الطائفية[1].

الفرع السابع: أسلوب ارتكاب الجريمة السيبرانية

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر كما هو الحال في جريمة السرقة..... فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها

[1] روان بن عطية الله الصحفي ، المرجع السابق ، ص 21وما بعدها.

(SOFT) CRIME لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته او قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس او اختراق خصوصيات الغير او التغرير بالقاصرين كل ذلك دون حاجة لسفك الدماء[1].

الفرع الثامن: قلة الإبلاغ عن وقوع الجريمة السيبرانية

في معظم الأحيان لا يتم الإبلاغ عن جرائم الانترنت وذلك راجع لسببين، أولهما هو الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، وأكثر من ذلك يتم اكتشافها بعد فترة طويلة من ارتكابها.

والسبب الثاني هو عدم اكتشاف المجني عليه الحية للجريمة وزد على ذلك ان الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كف الستار عنها.

وما يمكن قوله عن خصائص الجريمة المعلوماتية انها جريمة العالم الافتراضي، الغير ملموس، وما يميزها أكثر الشخص الذي يقوم بهذه الجريمة الذي يختلف اختلافا جذريا عن المجرم التقليدي، فالمجرم المعلوماتي يتميز بذكائه وقدرته مع التعامل مع جهاز الحاسوب والشبكة العنكبوتية، اللذان يساعدانه على ارتكاب جرائمه بدون جهد عضلي اي كسر ولا سفك دماء .

فالجريمة المعلوماتية تتم بتقنيات عالية، وكذلك هناك خاصية بارزة وهي عولمة هذه الجرائم يؤدي إلى تسيب جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم فهذه الجرائم صورة صادقة من صور العولمة[2].

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، الجامعة الأردنية ، دار الثقافة للنشر والتوزيع ، ص57وما بعدها .
[2] فتيحة رصاع ، مرجع سابق ، ص 47وما بعدها .

المطلب الثالث: موقف المشرع الجزائري من الجريمة السيبرانية

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04 المؤرخ في 2004.11.10المتضمن تعديل قانون العقوبات [1]،ولكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي وسنبين بصفة موجزة الأفعال التي جرمها المشرع الجزائري بموجب القانون السالف الذكر:

1-**جريمة التوصل أو الدخول غير المصرح به :** نصت عليه المادة 394 مكرر من قانون العقوبات بقولها" يعاقب بالحبس والغرامة 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." فقد أورد المشرع ظرفي تشديد لعقوبة الدخول غير المشروع وهما:في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة. وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله" أو يحاول ذلك "[2].

2-**جريمة التزوير المعلوماتي :**نص عليها المشرع في نص المادة 394مكرر 1بقوله"يعاقب بالحبس وبالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[3].

---

[1] القانون 15/04 ، مرجع سابق.

[2] أمال قارة، مرجع سابق ، ص99.

[3] تنص المادة 394مكرر 2من قانون العقوبات":يعاقب بالحبس والغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكبها الجرائم المنصوص عليها في هذا القسم.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

3-**جريمة الاستيلاء على المعطيات** :نصت عليها المادة 394مكرر 2بقولها "كل من يقوم عمدا وبطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

4-**جريمة إتلاف وتدمير المعطيات** :نص عليها المشرع الجزائري بالمادة 394مكرر 1من قانون العقوبات "يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها." وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات

5-**جريمة الاحتيال المعلوماتي** :وهو ما نصت عليه المادة 394مكرر 1/2بقولها "يعاقب بالحبس وبالغرامة 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 من جراء ذلك.

6-**نشطة الانترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني** :نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394مكرر 2/2على تجريم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق،وجميع الأفعال غير المشروعة، وقد نصت المواد على توقيع عقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر6[1] بتوقيع عقوبة تكميلية تتمثل في

[1]تنص المادة 394من قانون العقوبات":مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

غلق المواقع les sites التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[1].

أما الجزاءات المقررة بموجب الفصل السابع مكرر فتتمثل في العقوبات **الأصلية** وهي عقوبة الحبس والغرامة. وعقوبات تكميلية بموجب نص المادة 394مكرر 6والمتمثلة في: مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع(les sites) والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت cybercaféالذي ترتكب فيه هذه الجرائم بشرط علم مالكه.وقد أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي: في حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. ونص أيضا بموجب المادة 394مكرر 5على تجريم الاشتراك (سواء شخص طبيعي أو معنوي) في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية– بعقوبة الجريمة –وكان التحضير لهذه الجرائم مجسدا بفعل أو بعدة أفعال مادية. أي بمعنى آخر فإن المشرع استثنى من العقاب الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد[2].

نصت المادة 394 مكرر 4[3] على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 05مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي. غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين فينفس

[1] أمال قارة، مرجع سابق، ص .20.

[2] تنص المادة 394مكرر5من قانون العقوبات":كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبة المقررة للجريمة ذاتها".

[3] تنص المادة 394مكرر4من قانون العقوبات":يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 5مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

الجريمة. والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر 7[1] من قانون العقوبات.

إلى جانب قانون العقوبات التي جاءت نصوصه المستحدثة مجرمة لبعض الاعتداءات على المعلوماتية فإن المشرع الجزائري وبموجب الأمر 03/05 المؤرخ في 2003.07.19المتعلق بحقوق المؤلف والحقوق المجاورة قد عمد إلى توفير الحماية لبرامج الحاسب الآلي وإخضاعها لقوانين الملكية الفكرية وأقر عقوبة الحبس والغرامة على كل من يعتدي على هذه المصنفات[2].

[1]تنص المادة 394مكرر7من قانون العقوبات":يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".
[2]أمال قارة، مرجع سابق،ص20.

الفصل الثاني

لوضع حماية جزائية للجريمة لمعلوماتية استجابت عدة دول لها، فمثلا الولايات المتحدة الأمريكية التي أصدرت قانون فيدرالي سنة 1984 متعلق بالاحتيال وإساءة استخدام الكمبيوتر، كما أصدرت فرنسا قانون رقم 19/88 الموافق لـ1988/01/05 بشان الغش المعلوماتي، والذي ادمج في قانون العقوبات الفرنسي وأصبح يشكل باب جديد هو الباب الثالث من قانون العقوبات الفرنسي، ثم صدر تعديل جديد لهذا القانون 1993/03/01.

أما عن التشريعات العربية فقد تبنى المشرع الجزائري في القسم السابع مكرر نصوص الجريمة المعلوماتية أو ما يصطلح عليه بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك بالقانون رقم 15/04 المؤرخ في 2004/11/10 متضمن قانون العقوبات الجزائري

وقد شهد العالم مولد أول معاهدة دولية لمواجهة جرائم الكمبيوتر وذلك في سبتمبر 2001 في مدينة بودابست بتوقيع 26 دولة من الاتحاد الأوروبي إضافة إلى كندا وجنوب إفريقيا والولايات المتحدة الأمريكية، والحقيقة أن تلك المعاهدة وإن كانت أوروبية المنشأ فهي دولية النزعة فهي مفتوحة للدول الأخرى التي تطلب الانضمام أو الترشح للانضمام لها.

ولهذا سنتناول في هذا الفصل من خلال المبحث الأول آليات التصدي للجرائم السبيرانية أما المبحث الثاني فسنتطرق إلى الإجراءات المتخذة لمتابعة الجرائم السبيرانية في التشريع الجزائري .

آليات التصدي للجريمة السيبرانية في القانون الجزائري :

إن التطور المتسارع لتكنولوجيا الإتصال والمعلومات أدى إلى حصول نوع من الفراغ التشريعي المنظم للجرائم السيبرانية التي تتميز بنوع من الحداثة في الفضاء الإلكتروني بحيث لا يمكن إخضاعها بأي حال من الأحوال إلى القواعد التقليدية الواردة في النصوص التشريعية العقابية،وهو الأمر الذي يؤدي إلى سن تشريعات جديدة تطبق على هذا النوع من الجرائم ،وبناء على ذلك استحدثت الجزائر على غرار العديد من الدول آليات لمكافحة الجرائم السيبرانية . وهذا ما يتم توضيحه في المبحثين الآتيين.

المبحث الأول:آليات التصدي للجرائم السيبرانية

سنتناول في هذا المبحث شرح لبعض القوانين العامة والخاصة والهيئات والأجهزة المساعدة لمكافحة الجرائم السيبرانية ، من خلال المطلبين الآتيين .

المطلب الأول: مكافحة الجرائم السيبرانية في التشريع الجزائري

من خلال هذا المطلب سنتطرق لمختلف القوانين الشاملة في التصدي والمواجهة لمثل هذه الجرائم المستحدثة في الجزائر وذلك من خلال الفرعين الآتيين.

الفرع الأول: مكافحة الجرائم السيبرانية بموجب القوانين العامة

- **الدستور الجزائري:** لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وهذا ما ضمنه تعديل دستور 2020 ، على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

المادة 37: كل المواطنين سواسية أمام القانون ،ولهم الحق في حماية متساوية ولا يمكن ان يُتذرع بأي تميز يعود سببه إلى المولد، أو العرق، أو الجنس، أو الرأي، أو أي شرط أو ظرف أخر شخصي أو اجتماعي .

المادة 74: حرية الإبداع الفكري، بما في ذلك أبعاده العلمية والفنية مضمونة.

لا يمكن تقييد هذه الحرية إلا عند المساس بكرامة الأشخاص او بالمصالح العليا للأمة أو القيام والثوابت الوطنية .

يحمي القانون الحقوق المترتبة على الإبداع الفكري . في حالة نقل الحقوق الناجمة عن الإبداع الفكري ،يمكن للدولة ممارسة حق الشفعة لحماية المصلحة العامة .

إذ لا يجوز إنتهاك حرمة حياة الموطن الخاصة، وحرمة شرفه،كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكاله مضمونة. ان القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل او أية وسيلة اخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.[1]

– **قانون العقوبات الجزائري** :لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر2004 المتمم للأمر رقم 22/15المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هدا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر7 .[2]

[1] فضيلة عاقلي ،الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري ،المؤتمر الدولي الرابع عشر (الجرائم الاكترونية)،طرابلس ،25/24مارس 2017،ص127

[2]فضيلة عاقلي، المرجع السابق ،ص127

وبغرض تدارك الفراغ القانوني ، فقد قام المشرع الجزائري بموجب القانون رقم 15/04. [1] باستحداث جملة من النصوص والتي جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات ،وحدد لكل فعل منها ما يقابله من الجزاء ، إذ قام المشرع بسن جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة [2]، وإلى جانب ذلك فقد قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الالكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22.[3]

إذ نصت المادة 394 مكرر منها مايلي: "يعاقب بالحبس من ثلاثة اشهر الى سنة وبغرامة من50000 الى100000دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات او يحاول ذلك". وتتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة واذا ترتب عن الأفعال المذكورة اعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 الى 150000دج "،وذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن ان تتدرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة ، ونصت المادة 394 مكرر 2 على انه "يعاقب ... كل من يقوم عمدا وعن طريق الغش بما ياتي :

- 1- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مراسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم .

[1] قانون رقم 15/04،مرجع سابق .

[2] قانون رقم 06-22مؤرخ في2006/12/20،يعدل ويتمم بالامر رقم 66-155 ، يتضمن قانون اجراءات الجزائية ،ج-ر،عدد84،الصادر في 2006/12/24

[3] جمال براهيمي ،مكافحة الجريمة الالكترونية في التشريع الجزائري ،المجلة النقدية للقانون والعلوم السياسية،كلية الحقوق والعلوم السياسية ،جامعة مولود معمري ،تيزي وزو،العدد2،الصادر في2006/11/15،ص124و مابعدها.

- 2- حيازة او افشاء او نشر او استعمال لأي غرض كل المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم ".

وتضيف المادة 394 مكرر6 انه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية :يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على اغلاق المحل او مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها [1]

- قانون الإجراءات الجزائية الجزائرية:

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية ،كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة .[2]

نجد ان المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية في المادة 37 قانون إجراءات جزائية ،ونص على التفتيش في المادة 45الفقرة 7. [3]من نفس القانون المعدلة حيث اعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه ،في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية ،فالتفتيش وان كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة ، وبالتالي لا تطبق الأحكام الواردة في المادة 44من قانون الإجراءات الجزائية اذا تعلق الأمر بالجرائم الالكترونية ،ونص على توقيف النظر في جريمة المساس

[1] نوارة حسين ،آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا ،الملتقى الوطني (آليات مكافحة الجرائم الالكترونية في التشريع الجزائري)،كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ،الجزائر ،29 /2017/03 ، ص118ومابعدها.

[2] فضيلة عاقلي ،مرجع سابق ،ص130

[3] مولود ديدان،قانون الاجراءات الجزائية المادة 37والمادة 45 ، الامر 11-02،دار بلقيس ، الجزائر ،ص33 .

بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5 [1].

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية ، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية ، والتي من شانها ان تفادى وقوع الجريمة أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها ،وهو ما استدركه المشرع بتضمين القانون رقم 06- 22 المعدل لقانون الإجراءات الجزائية تدابير اجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها والتسرب .

يقصد اعتراض المراسلات بإعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للانتاج والتوزيع،التخزين ،الاستقبال والعرض،التي تتم عن طريق قنوات أووسائل الاتصال السلكية واللاسلكية في اطار البحث والتحري عن الجريمة وجمع الأدلة عنها .

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء لهدا الإجراء في المادة 65 مكرر5 من قانون الإجراءات الجزائية على النحو:"إذا اقتضت ضرورات التحري في الجريمة المتلبس بها ،أو التحقيق الابتدائي في ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن :

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسكية .

- وضع الترتيبات التقنية ،دون موافقة المعنيين ،من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص او عدة أشخاص في أماكن مخصصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص "، فموجب هذه المادة المشرع الجزائري يسمح لسلطات التحقيق والاستدلال اذا استدعت التحري في

[1] فضيلة عاقلي ،مرجع سابق ،ص130

الجريمة المتلبس بها ،والتحقيق في الجريمة الالكترونية ، اللجوء الى إجراء إعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والاصوات والتقاط الصور ، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول الى الكشف عن ملابسات الجريمة واثباتها دون ان يتقيدوا بقواعد التفتيش والضبط المألوفة .

أو مع هذا فإن المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء ، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.[1]

الفرع الثاني :مكافحة الجرائم السيبرانية بموجب القوانين الخاصة

1- **القانون الخاص بحماية حق المؤلف والحقوق المجاورة** :يرى معظم الفقه أن "الموقع الإلكتروني مصنف متعدد الأغراض "،يتم استخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الانترنت ، أو كإسم تجاري أو شعار لجدب الجمهور ،كما يمكن ان يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السنمائية أو لوحاتهم الزيتية او...وغيره ،وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة ،وبمجرد تسجيل اسم الموقع يحضى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه ،أي بتحديد القانون الواجب التطبيق حسب الوضعية القانونية للمواقع فعند تسجيل الموقع كمصنف أدبي أو فني لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد كاستعمال اسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها او استغلال صورة أي شخص في الموقع دون الموافقة منه،...وبهذه الصورة فان حماية مواقع الانترنت التي تستغل مصنفا أدبيا أو فنياعلى شبكة الانترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الأدبي

[1] براهيمي جمال ،مرجع سابق ، ص ص138-140.

والمالي للموقع المسجل كمصنف ،وحماية قانونية لأي حق آخر يتم الإعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الإسم والصورة والمعلومات الخاصة ...وفي كل الأحوال لا يمكن الفصل بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف والحقوق المجاورة في الوقت نفسه ،لان حماية الموقع تؤدي بالضرورة إلى عدم محتوياته بما ذلك المصنف .[1]

2-القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها :

صدر القانون رقم 09-04 بتاريخ 05أوت2009 ،ويتضمن 19 مادة موزعة على ستة فصول ،وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين ،وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء و مهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية ،كما يتضمن هذا القانون أحكام خاصة بالمراقبة الإلكترونية التي لا يجوز اجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تمّ تحديدها وهي الأفعال الموصوفة بجرائم 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 والإتصال 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 نظيرتها في الخارج ،علما أن 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 تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو

[1] نوارة حسين ،مرجع سابق ،ص120ومابعدها .

يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا .[1]

3- القانون الخاص المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية :

حيث استحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الإفتراضي منها،استحداث سلطة ضبط من بين مهامها السهر على احترام متعاملي البريد والإتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والإتصالات الإلكترونية والأمن السيبراني[2].

تجريم إنتهاك سرية المراسلات المرسلة عن طريق البريد أو الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو إستعمالها دون ترخيص من المرسل أو المرسل إليه أو الإخبار بوجودها،وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة ،وسنّت مجموعة من العقوبات ضمن المواد من 164 إلى 188من هذا القانون

4- القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي إيجازها في عدة نقاط :

-استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي .

[1] عائشة نايري ،الجريمة الالكترونية في التشريع الجزائري،رسالة ماستر حقوق ،تخصص قانون اداري ،جامعة ادرار،2017/2016،ص 39 ومابعدها .

[2] المادة 13من القانون18-04المؤرخ في 10مايو 2018،الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية ،ج ر ،عدد27،الصادرة بتاريخ 13مايو 2018،.

-وضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي .

- إتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من المسؤول عن المعالجة .

- يمكن للسلطة الوطنية القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة بإستثناء محلات السكن ،كما يمكنها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها .

- تأهيل أعوان رقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات طابع شخصي تحت إشراف وكيل الجمهورية .

- يمكن للمدعي بالمساس بحق من الحقوق المنصوص عليها في هدا القانون أن يطلب من الجهة القضائية إتخاذ أي إجراءات تحفظية للحد من التعدي أو الحصول على تعويض .

- تختص الجهة القضائية الجزائرية بمتابعة الجرائم التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري ،كما تختص بمتابعة الجرائم المنصوص عليها في هدا القانون وفقا لقواعد الإختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية[1] .

- تجريم الإعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية وأخرى سالبة للحرية وفقا للمواد من 54 إلى 74 من هذا القانون [2]

[1] المادة 53من القانون 18-07،المؤرخ في 10 يونيو 2018،المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ،ج ر ،عدد34،الصادرة بتاريخ 10 يونيو 2018،ص 22 .

[2] مهدي رضا،الجرائم السيبرانية وآلية مكافحتها في التشريع الجزائري ،مجلة إيليزا للبحوث والدراسات ،جامعة المسيلة ،المجلد06، العدد02(2021)،ص121و ما بعدها .

المطلب الثاني :الهيئات المتخصصة في الجرائم السيبرانية في التشريع الجزائري

سنتناول في هذا المطلب أهم الهيئات المتخصصة والفعالة في مواجهة الجرائم السيبرانية في الجزائر والتي خصصنا لها اربعة فروع وهي كالآتي .

الفرع الاول:الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

نصت على إنشاء هذه الهيئة المادة 13من القانون 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته.تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم " ،أما مهامها فقد أوردتها المادة 14 من نفس القانون .

- تنظيم الهيئة:

بالرغم من الأهمية المرجوة من هذه الهيئة إلا أنه لم يتم إلى حد الساعة إنشاءها ،وباستقراء نصوص القانون 09-04 فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة ،وهو نفس الأمر في فرنسا إذ أنشأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيا الإعلام و الإتصال .

- مهام الهيئة :

1. الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والإتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الإتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو بطاقات إئتمانهم، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...

2. مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: بحسب نص المادة 14 من القانون 09-04 فهناك نوعان من المكافحة تقوم بهم هذه الهيئة :

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التئ تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة ب من القانون 09-04، وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيا ت الإعلام والاتصال بفرنسا ، فإن لها مهام أدرجها المرسوم رقم 2000-405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة تتمثل في:

- تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

- القيام بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة لتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال ،ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون .

- تقديم المساعدة لمصالح الأمن والدرك الوطنيين ،ولجميع إدارات ومصالح الدولة المركزية فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة ،إذا طلبت منها هذه المصالح ذلك ،ودون أن يؤدي ذلك رفع يد هذه المصالح .

- التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة –المادة 4 فقرة2 من القانون 09-04- في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به .

- من أجل القيام بمهامها فلها تركيز، تحليل، إستقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والإتصال ، والاتصال بكل من مصالح الأمن والدرك الوطنيين ،إدارات ومصالح الدولة ،كذا كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها .

- يجب على كل مصالح الأمن والدرك الوطنيين ،إدارات ومصالح الدولة في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال فيما تسمح به القوانين – وخاصة منها ما يتعلق بالسر المهني – بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيا الإعلام والاتصال .

3/ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم :في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها المنظمات أو الهيئات المماثلة لها على مستو الدول ، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل ،كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم .[1]

الفرع الثاني :المعهد الوطني للأدلة الجنائية وعلم الإجرام

يتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام من إحدى عشرة دائرة متخصصة في مجالات مختلفة ، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، البحوث، الدراسات والتحاليل في علم الجريمة .

[1] عبد الفتاح بيومي حجازي ،الاثبات الجنائي في جرائم الكومبيوتر والانترنت ،دار الكتب القانونية ،مصر ،2007،ص232 وما بعدها.

دائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة تحليل وتقديم كل دليل رقمي وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة ،أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف ،التقنيات والطرق المستعملة في مختلف الخبرات العلمية ،لإنجاز المهام المنوطة بها ،تنقسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات (سمعية ، بصرية، والإعلام الآلي). كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي : [1]

أولا: مخبر الإعلام الآلي : من مهامه:

– تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف ، الشريحة، القرص الصلب ، ذاكرة الفلاش).

– تحديد التزوير الرقمي للبطاقات البنكية .

ومن تجهيزاته:

– محطة ترميم وتصليح الأجهزة والحوامل المعطلة، الشبكات الإعلامية (خبرات الإعلام الآلي والتجهيزات البيانية).

– محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي .

– جهاز إقتناء معلومات الهواتف والحواسب والقاعات التي يحتوي عليها : تتمثل في 07 قاعات (مكتب التوجيه ، فصيلة الأنظمة المشحونة، فصيلة إقتناء المعطيات ، قاعة موزع وقاعة تخزين).[2]

[1] هواري عياش ، " مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية"، المعهد الوطني للأدلة الجنائية وعلم الإجرام ،كلية الحقوق ،جامعة بسكرة ،2016،ص03

[2] سالم عبد الرزاق ،ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ،بمحكمة سيدي امحمد ،الجزائر ،ص ص4–6.

ثانيا: مخبر الفيديو : يختص مخبر الفيديو بمقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة (فيديو – صورة) بمختلف التقنيات .

ومن تجهيزاته : جهاز فيديو بوكس وحوامل فيديو الرقمية والممغنطة وحبكات إعلامية (كونيتك ستوديو ، ماكس ثلاث أبعاد) وموزع لحفظ شرائح الفيديو. أما بالنسبة للقاعات يحتوي مخبر الفيديو على 04 قاعات (قاعتان للتحليل ، قاعة التخزين وقاعة موزع)[1].

ثالثا: مخبر الصوت : ومن مهام التي يؤديها :تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية .ومن أجهزته: الأجهزة الإزدواجية والسماع وحبكات إعلامية (معالجة وتحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة وأجهزة التصليح والتعبير). أما بالنسبة للقاعات فإنه يحتوي مخبر الصوت على 05 قاعات03 قاعات للتحليل، قاعة تخزين وقاعة موزع .[2]

الفرع الثالث :المعهد الوطني للبحث في علم التحقيق الجنائي :

بالإضافة إلى المعهد الوطني للأدلة الجنائية وعلم الإجرام، تم استحداث أيضا المعهد الوطني للبحث في علم التحقيق الجنائي تحت وصاية المديرية العامة للأمن الوطني، بموجب المرسوم الرئاسي رقم 432-04 المؤرخ في 29-12-2004 والذي نص أيضا في المادة 05 منه على مجموعة من المهام من بينها إعداد تقارير الخبرة ، وأيضا القيام بالتكوين وتجديد المعارف في ميدان علم التحقيق الجنائي والإجرام.

[1] سالم عبد الرزاق ،المرجع السابق،ص7

[2] سالم عبد الرزاق .،نفس المرجع ،ص8

ويحتوي هذا المعهد على مصلحة الخبرات الخاصة بالدلائل التكنولوجية، بحيث تكلف بتحليل الدلائل المادية التي تم جمعها إثر معاينة المخالفات والتحريات في ميدان الجريمة المعلوماتية وإعداد تقارير الخبرة .

الفرع الرابع :الهيئات القضائية الجزائية المتخصصة:

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04-14 المؤرخ في 01 نوفمبر 2004 ،[1] وتختص هذه الجهات القضائية بموجب المواد37- 40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم .[2]

ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية :دعم حقوق الإنسان وتسهيل حق اللجوء على القضاء وإعادة الاعتبار لنظام التكوين والتأهيل ،بإحداث تغيرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة ، ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايد في العمليات الإرهابية وتزايدا في أعمال

[1] القانون رقم 04-14،مرجع سابق .

[2] سعيدة بعرة ، مذكرة لنيل شهادة الماستر، بعنوان :الجريمة الاكترونية في التشريع الجزائري ، دراسة مقارنة ،2015-2016،ص52 .

المنظمات الإجرامية واستعمالها القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية .

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي : جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف .[1]

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3-4-5 المعدلة للمواد3-4-5 من المرسوم السابق وجاء التقسيم كالتالي :[2]

- محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : (الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، البويرة، عين الدفلى.)

[1] كريمة علة ، الجهات القضائية الجزائية ذات الاختصاص الموسع ، المجلة الاكادمية للبحث القانوني ، المجلد11، عدد01/2015، ص117.

[2] سعيدة بوزنون ، مكافحة الجريمة الالكترونية في التشريع الجزائري ، مجلة العلوم الانسانية ، المجلد ب،عدد52، ديسمبر2019، ص54 .

– محكمة قسنطينة ويمتد إختصاصها للمجالس القضائية : (قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف ، خنشلة، سوق أهراس، ميلة)

– محكمة ورقلة ويمتد إختصاصها للمجالس القضائية التالية : (ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، غرداية.)

– محكمة وهران ويمتد الإختصاص بها إلى المجالس القضائية التالية: (وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، البيض، تيسمسيلت، النعامة، عين تيموشنت، غيليزان)

بحيث يشمل اختصاص كل جهة قضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنوبا، شرقا، وغربا، وذلك لدى أربع محاكم تسمى أقطابا جزائية ،كما تم تدعيم هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترنية .[1]

المبحث الثاني:الإجراءات المتخذة لمتابعة الجرائم السيبرانية في التشريع الجزائري.

تعتبر الجرائم السيبرانية من أحدث الجرائم التي ظهرت مؤخرا ومما جعلها تشكل خطرا على المجتمع ،وذلك لابد من مواجهتها وردعها بأعنف وأجدى الإجراءات والوسائل الفعالة للقضاء عليها ،ومن هذه النقطة حيث سنتطرق في هذا المبحث إلى المطلبين الآتيين.

المطلب الأول :الإجراءات التقليدية لمتابعة الجرائم السيبرانية

من خلال هذا المطلب سنتناول في فروعه اهم الاجراءات المتخذة لمتابعة هدا النوع من الجرائم وهي كالاتي :

[1] سعيدة بوزنون ، مرجع سابق ،ص55

الفرع الأول :المعاينة في البيئة الإلكترونية :

يقصد بالمعاينة في علم التحقيق الجنائي "مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له ،سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير ،لإثبات حالته كما تركه الجاني "[1] ،لذا يعتبر إجراء المعاينة في الوسط الإلكتروني من أهم الإجراءات والوسائل لتكوين الفكرة الأولى عن كيفية إرتكاب الجرائم السيبرانية ،وبالإضافة إلى أنها تعد من أهم مصادر الأدلة الجنائية المادية .

أولا : دور المعاينة في الكشف عن الجرائم السيبرانية :

تعتبر المعاينة من أهم إجراءات التحقيق ،إلا أن دورها في الكشف عن الجرائم السيبرانية يتضاءل، وسبب ذلك أن الجريمة التقليدية تجري غالبا على مسرح جريمة وتخلف آثار مادية،هذا المسرح يفتح المجال أمام جهات البحث والتحري للكشف عن غموض الجريمة،على عكس مسرح الجريمة السيبرانية الذي يتضاءل فيه دور المعاينة ، بسبب أن هذا النوع من الجرائم قلما يترك آثار مادية ، بالإضافة إلى إمكانية التلاعب بالأدلة عن بعد عن طريق محوها أو إتلافها أو تغييرها ،وعليه يمكن القول أنه ينبغي على القائمين بالمعاينة التعامل مع مسرح الجريمة السيبرانية على أنه مسرحان،مسرح مادي وآخر معنوي ، فالأول يشمل جميع المكونات المادية للحاسب الآلي التي يمكن أن تحوي آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية أو أوراق ....الخ ،أما الثاني فهو مسرح إفتراضي ما يقع داخل البيئة الإلكترونية لجهاز الحاسب الآلي ،ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي قد تفيد في التحقيق .[2]

[1] خالد ممدوح ابراهيم ،فن التحقيق الجنائي في الجرائم الالكترونية ،الطبعة الاولى ،دار الفكر الجامعي ،الاسكندرية،2010،ص149

[2] فاطمة زهرة بوعناد،مكافحة الجريمة الاكترونية في التشريع الجزائري ،،مجلة الندوة للدراسات القانونية جامعة سيدي بلعباس ،العددالاول،2013،ص68

ثانيا :إجراءات المعاينة في البيئة الإلكترونية :

1/ الإجراءات المتخذة قبل إجراء المعاينة :

عادة ما تكون هذه الإجراءات والخطوات التحضيرية ،غرضها تهيئة الوسائل البشرية والمادية للقيام بإجراء المعاينة ،ويتم ذلك بإعداد خطة عمل تحتوي على إعداد شامل للأدوات المستعملة في المعاينة ،وتقسيم المهام بين الفنيين والقائمين على هذا الإجراء [1]، بالإضافة إلى توفير معلومات مسبقة عن مكان الجريمة وعن نوع وعدد الأجهزة المراد معاينتها ،وذلك لتحديد إمكانية التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات ،وتأمين التيار الكهربائي تجنبا لتلفها ،كما انه يجب في هذه المرحلة توفير الإحتياجات الضرورية من الأجهزة والبرامج للإستعانة بها في الفحص والتشغيل وفك التشفير [2]

2/ الإجراءات المتخذة أثناء القيام بالمعاينة :

بعد القيام بالإجراءات التحضيرية التي سبق ذكرها ، يقوم الفنيون القائمون على إجراء المعاينة بتصوير جهاز الحاسب الآلي وكافة مكوناته المادية [3]، مع التركيز على تصوير الأجزاء الخلفية له ومراعاة تسجيل وقت وتاريخ ومكان إلتقاط كل صورة [4]،زيادة على ذلك القيام بملاحظة وإثبات حالة توصيلات الأسلاك المتصلة بكل ملحقات الحاسب الآلي ،وأيضا التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة ،وكذا الشرائط والاقراص المضغوطة وفحصها ،بعد ذلك يتم البحث في جهاز الحاسب الآلي عن الآثار الرقمية التي خلفها المستخدم ،وفي هذه المرحلة يجب تعطيل حركة الإتصالات السلكية واللاسلكية بشبكة الأنترنت تجنبا لتلف الدليل الجنائي الرقمي **أو** التلاعب به وتخريبه عمدا

---

[1] كاظم محمد عطيات ، محمد رضوان هلال،كيفية التعامل التقني والآمن مع اوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص ، المجلة العربية الدولية للمعلوماتية ، العدد الخامس ،المجلد 3،السعودية 2014،ص45

[2] نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، الطبعة الاولى ، دار الفكر العربي ،الاسكندرية ، 2007، ص199.

[3] كاظم محمد عطيات ،محمد رضوان هلال ،مرجع سابق ،ص45 .

[4] خالد ممدوح ابراهيم ،مرجع سابق ،ص172 .

عن بعد،وفي حالة ضبط المعلومات أو البيانات الرقمية ،يجب مراعاة قواعد تحريز الأدلة الجنائية الرقمية التي يتطلب تخزينها عناية فائقة للدعائم المادية وفحصها وإستعمالها لاحقا.[1]

ثالثا:أهمية المعاينة في مجال الجرائم السيبرانية :

للمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق والقضاء ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة ،وبكل ما تحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به .

وبإعتبار المعاينة من أهم إجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من الناحية القانونية أو الفنية ،فمن الناحية القانونية تبدوا أهميتها من عدة إتجاهات منها تأكيد وقوع الجريمة أو نفيها ،أي صدق أقوال الواقعة وكذلك تحديد الوصف القانوني لها ،كما تساعد القاضي في تكوين إقتناعه ،أما من الناحية الفنية فهي تساعد المحقق على تحديد وقت إرتكاب الواقعة الإجرامية ومعرفة علاقة الجاني بالمجني عليه وتحديد الأسلوب الإجرامي الذي إستعان به الجاني .

الفرع الثاني :التفتيش في البيئة الإلكترونية:

معنى 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 نسبة الجريمة إلى المتهم [2]، والمستهدف من التفتيش هو جهاز الحاسوب بمكوناته المادية (وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل)، والمكونات المعنوية (الكيانات

[1] سليمان النحوي ،آليات مكافحة الجريمة السيبرانية في التشريع الجزائري ،مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية ،قسم الحقوق،جامعة برج بوعريريج ،الموسوم بعنوان الاجرام السيبراني المفهوم والتحديات ،يومي 12/11افريل 2017،ص06.

[2] فاطمة زهرة بوعناد ،مرجع سابق ،ص68 .

المنطقية)، فعندما يستهدف التفتيش الكيانات المادية لا يشكل عائقا، وإنما الإشكال يثور عندما ينصب على المكونات المعنوية (البرامج، قواعد البيانات ...)، لأنه هذا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات .[1]

كيفية إجراء التفتيش :

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 ،وحسب المادة رقم 45 ف3 تنص على "لاتطبق هذه الأحكام إذا تعلق الأمر بجرائم ... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات."والمادة 3/47 تنص على :" عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ...فإنه يجوز إجراء التفتيش ... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل ..."، والمادة 2/64 تنص على: "وتطبق فضلا على ذلك أحكام المواد 44،47 من هذا القانون" [2] بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الإلكترونية ،حيث لا يشترط حضور الشخص المشتبه في أنه ساهم في إرتكاب 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.[3].

---

[1] زيبجة زيدان ،الجريمة المعلوماتية في التشريع الجزائري والدولي ،دار الهدى للطباعة والنشر ،الجزائر ،2011،ص ص131–133.

[2] المواد45–47–64،من الامر رقم 06–22،الصادر في 2006/12/20،المعدل والمتمم لقانون اجراءات جزائية ج–ر العدد84،الصادرة في 2006/12/24.

[3] سعيداني نعيم اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ،رسالة ماجيستير،جامعة الحاج لخضر باتنة ،2012–2013،ص145.

مدى خضوع مكونات الحاسوب المعنوية للتفتيش :

عرف الفقه إختلاف حول مدى خضوع 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 من 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 فطبيعة البيانات والمعطيات المعالجة تتطلب قواعد خاصة تحكمها، فالنصوص الخاصة بالتفتيش لايمكن إعماله 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: اتصال 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 للاعتقاد 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 أذا كانت هناك أسباب تدعو بالاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى ، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ..."

[1] سعيداني نعيم ، المرجع نفسه،ص147.

[2] فاطمة زهرة بوعناد ،المجلة السابقة الذكر،ص69 .

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

ويكون بالدخول إلى منظومة معلوماتية أو جزء منها ، كذا المعطيات المخزنة فيها ولو عن بعد، ذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها إنطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ،فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ،ووفقا لمبدأ المعاملة بالمثل ،تسخير كل شخص 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 إنطلاقا من المنظومة الأولى ،مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ،فإن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقية الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل."[2]

الفرع الثالث :الخبرة في مجال الجرائم السيبرانية

الخبرة القضائية هي إستشارة فنية يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي تحتاج تقديرها إلى معرفة أو دراية علمية خاصة [3]،ومنه فالخبرة هي وسيلة لتحديد التفسير الفني للأدلة عن طريق ربطها بالعلوم ،وهي في حقيقتها ليست دليلا مستقلا وإنما هي تقييم فني لهذا الدليل[4].

الخبير هو لابد أن يكون صاحب مقدرة وامكانيات علمية وفنية في مسألة موضوع الخبرة ،ويستطيع القيام بدوره وعليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والآثار الإقتصادية والمالية المترتبة دون إتلاف الأدلة أو الأجهزة أو تدميرها .

---

[1] بن دعاس فيصل ،اجراءات التحري في الجرائم المعلوماتية ،محاضرة في اطار التكوين المحلي المستمر للقضاة ،مجلس قضاء قسنطينة ،ص33.

[2] المادة 05من القانون رقم 09-04،القانون السالف الذكر.

[3] فاطمة زهرة بوعناد،مرجع سابق ،ص71.

[4] عبد الفتاح بيومي حجازي ،مرجع سابق ،ص321 .

قيمة الخبرة في مجال الجرائم السيبرانية:

يستطيع الخبير من خلال ما لديه من معلومات وخبرة إبداء رأي أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية خاصة [1]،وإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمرا ضروريا ، فإن الإستعانة به في مجال الجريمة السيبرانية أكثر من الضروري [2]،وذلك الطبيعة التقنية للجريمة من جهة ،وخصوصية الأدلة الفنية التي تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي من جهة أخرى ،ولهذا كان لزاما أن يتم اللجوء إلى خبير فني و متخصص.

ونظرا لطبيعة عمل الخبير في هذا المجال ،إهتم المشرع الجزائري بتنظيم أعمال الخبرة وكيفية اللجوء إليها وذلك من خلال المواد من 143 إلى المادة 156 قانون إجراءات جزائية بحيث نصت المادة 143منه على أنه "لجهات التحقيق أو الحكم عندما تعرض عليها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها ".

ومن جهة أخرى نص المشرع من خلال نص المادة 04/05 المستحدثة بالقانون رقم 09- 04 أ، أنه "يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها " .[3]

ومنه يمكن القول أنه يوجد دائما هناك حاجة ماسة إلى خبراء وفنيين من أجل القيام بالعديد من المهام التقنية مثل الكشف عن الأدلة الجنائية الرقمية وتحليلها ،أو إصلاح الدليل

[1] خالد ممدوح ابراهيم ،مرجع سابق ،ص285.

[2] سعيداني نعيم ،مرجع سابق ،ص166 .

[3] القانون رقم 09-04الصادر بتاريخ 2009/08/05يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ،ج-ر عدد47،بتاريخ 2009/08/16،ص05.

وإعادة تجميعه من المكونات المادية للحاسب الآلي ، أو التأكد من أن الدليل لم يتم العبث به[1].

المطلب الثاني :الإجراءات الحديثة لمتابعة الجرائم السيبرانية

من خلال هذا المطلب سنتعرض الى الاجراءات التي اتخذها المشرع الجزائري لمتابعة الجرائم السبيرانية وذلك من خلال الفرع الاتية:

الفرع الأول: إجراء التسرب

نظم المشرع الجزائري هذا الإجراء من خلال المواد 65 مكرر11إلى غاية المادة 65 مكرر18 وسنتناوله فيما يلي :

أولا: مفهوم إجراء التسرب :

عرفت المادة 65 مكرر 12 من قانون الإجراءات الجزائية التسرب بأنه :"قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ،بمراقبة الأشخاص والمشتبه في إرتكابهم جناية أو جنحة ،بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"، فالتسرب إذن هو تلك العملية المحضر لها مسبقا ،تهدف إلى التوغل داخل خلية إجرامية ومعرفة نشاطاتها ،والكشف عن الأشخاص المتورطين سواء كانوا فاعلين أو شركاء، وذلك بتوفير جميع الوسائل البشرية والتقنية اللازمة [2]

ثانيا : شروط القيام بعملية التسرب:

تتمثل شروط القيام بعملية التسرب وفقا لنصوص قانون الإجراءات الجزائية في الإجراءات التالية :

[1] خالد ممدوح ابراهيم ،مرجع سابق،ص302.

[2] سليمان النحوي ،مرجع سابق ،ص12 .

مباشرة التسرب من طرف ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية، والواضح بالنسبة لهذا الشرط أن المشرع الجزائري قد وسع المجال من حيث الأشخاص المعتمد عليهم في نظام التسرب ، على عكس نظام المراقبة الإلكترونية ، أين حصره في نطاق ضباط الشرطة القضائية دون غيرهم من الأعوان بعد استصدار إذن مكتوب بالتسرب، فطبقا لنص المادة 65 مكرر11 من قانون الإجراءات الجزائية "يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ،وكغيره من الأذون المتعلقة بالإجراءات ، فهو إذن مقيد بالشروط التالية :

– ضرورة أن يكون الإذن مكتوبا لا شفاهة،

– ضرورة أن يكون الإذن محددا لأسباب إصداره ،

– ضرورة أن يشتمل الإذن على كل البيانات المطلوبة من تحديد نوع الجريمة وهوية الفرد المتسرب والإجراءات المطلوبة ،

– ضرورة تحديد المدة في الإذن ،والتي لا يمكن أن تتجاوز أربعة (4)أشهر قابلة للتمديد.

– ضرورة إيداع نسخة من الإذن بالتسرب في ملف الإجراءات بعد إنتهاء عملية التسرب[1].

ثالثا: طرق التسرب وصوره :

1/ طرق التسرب :

تتم عملة التسرب في الأوساط المحددة قانونا عبر أسلوبين وهذا جاء في نص المادة 65 مكرر12 وهذا من خلال:

أ/ الجهة المخولة بمنح هذا الإذن

ب/ الجهة القائمة بتنفيذ هذه العملية

[1] زيدان زيبجة ،مرجع سابق ،ص169و ما بعدها.

الطريقة الأولى:

التي يصدر فيها الإذن بالتسرب من وكيل الجمهورية إلى ضابط الشرطة القضائية والذي يتولى أساليب التحري والتحقيق الواردة في المادة 65 مكرر 05والتي جاء فيها إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود ...[1]

وهذا يتم في إطار التحقيق لنص المادة 41من قانون الإجراءات الجزائية تشكل إطار لإجراءات التحري في حالة التلبس التي يصدر فيها الإذن من وكيل الجمهورية إلى ضابط الشرطة القضائية الذي يتولى العملية والتي نجد إطارها القانوني في نص المادة 63من قانون الإجراءات الجزائية والتي ينفذها ضابط الشرطة القضائية بمجرد علمهم بوقوع الجريمة أو بناءا على تعليمات نيابة أو بناءا على تعليمات رؤسائه والتي يصدر فيها الإذن بالتسرب من قاضي التحقيق إلى ضابط الشرطة القضائية والتي يحكمها نص المادة 38من قانون الإجراءات الجزائية الجزائري [2].

الطريقة الثانية :

والتي يصدر فيها الإذن بالتسرب من وكيل الجمهورية إلى ضابط الشرطة القضائية منسق العملية وتحت مسؤولية ينفذها عون الشرطة القضائية وهذا يتم في إطار حالتي التلبس والتحقيق الأولي .

والتي يصدر فيها الإذن بالتسرب إلى ضابط الشرطة القضائية منسق العملية وينفذها تحت مسؤولية عون الشرطة القضائية في إطار الإنابة القضائية[3].

---

[1] انظر نص المادة 65مكرر05 من ق ا ج ج .

[2] جوهر قوادري صامت ،رقابة سلطة التحقيق على اعمال الضبطية القضائية ،في القانون الجزائري والمقارن ،دار الجامعة الجديدة الاسكندرية ، سنة 2010،ص53.

[3] يتم في ظل نص المادة 41من ق ا ج ج ،في حالتي التلبس والتحقيق الاولي ،ونص المادة 138 من ق اج ج في حالة الانابة القضائية

2/ صور التسرب :

ونعني بذلك الطرق التي يمارس في ظلها القائم بعملية التسرب عمله والأفعال التي أذن له القانون القيام بها ويتم من خلال الصور التالية :

أولا: المتسرب كفاعل: طبقا لنص المادة 6 مكرر 10: "يقصد بالتسرب قيام ضابط أو عون 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[1].

والمقصود بالفاعل هو ما جاء بيانه في نص المادة 41 قانون العقوبات :"كل من يساهم مساهمة في تنفيذ الجريمة أو حرض على إرتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة إستعمال السلطة الولائية أو التحايل أو التدليس الإجرامي ".

ومنه يقصد به أن يوهم المتسرب الفاعل المشتبه فيهم بأنه فاعل يحتل مركزا مباشرا في تنفيذ العمل الإجرامي، ومنه يجب ان يميز بين من يقوم بإيهام غيره ومن يحرضهم على القيام بذلك لأن المقصود بالإيهام هو مسايرة المشتبه فيه في مسلكه الإجرامي حتى يضبط ويداه في الجرم [2].

وهذا ما تبناه المشرع الجزائري في قانون الإجراءات الجزائية في نص المادة 65 مكرر12 منه عبارة (لا يجوز بأي شكل تحت طائلة البطلان هذه الأفعال تحريضا على إرتكاب الجرائم .).

[1] زغينة وليد ،اساليب التحري الحديثة وأطر تطبيقها في الجزائر ،مذكرة نهاية الدراسة لنيل إجازة المدرسة العليا للقضاء ،الدفعة 21 ، 2010-2013 ،ص40

[2] احمد عوض بلال ،قاعدة استبعاد الأدلة المتصلة بطرق غير شرعية في الاجراءات الجنائية المقارنة ،الطبعة الثانية،دار النهضة العربية للنشر والتوزيع، القاهرة ،سنة 2013، ص390.

ثانيا : المتسرب كشريك: وهي التي يتم فيها من أجل كشف مرتكب الجرائم المنصوص عليها قانونا حيث يقوم المتسرب بإيهامهم بأنه شريك معهم حسب ما جاء في نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري [1]

وبالرجوع إلى نص المادة 42 من قانون العقوبات التي تعرف الشريك كالآتي :" يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا ولكنه ساعد بكل الطرق وعاون الفاعل أوالفاعلين على ارتكاب الأعمال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك " (كما يدخل في حكم الشريك من اعتداء أن يقدم مسكنا أو ملجأ أو مكانا للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون العنف ضد امن الدولة والأمن العام أو الأشخاص أو الأموال مع علمه بسلوكهم الإجرامي .).

وعليه فالمتسرب في صور الشريك يقوم بإيهام المشتبه فيهم من خلال قيامه بالأعمال التحضيرية أو المساعدة أو المنفذة لهذه الجرائم أو تقديم مسكن أو ملجأ...الخ ،أو مسايرتهم في السلوك الإجرامي إلى حين الإيقاع بهم متلبسين بجرمهم[2].

ثالثا:المتسرب كخافٍ : وهي الصورة الثالثة التي يقوم فيها المتسرب بهمته من خلال إيهام مرتكب الجرائم السالفة الذكر واحد منهم وذلك من خلال إخفائه للأشياء التي تتم عملية إختلاسها أو تبديد فيها وقد تم تحصيلها من خلال إرتكاب هذه الجرائم سواء كليا أو جزئيا وطبقا لنص المادة 387 من قانون العقوبات الجزائري التي قد تعرف فعل الإخفاء كالتالي ("كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصل عنها من جناية أو جنحة في مجموعها أو جزء منها يعاقب عليها ....").

كما وردت صورة إخفاء في نص المادة 43 من قانون 01/06 المؤرخ في 2006/02/20 .[1]

[1] راجع نص المادة 65مكرر 12 منّ ق ا ج ج .

[2] راجع نص المادة 42-43 من قانون العقوبات الجزائري.

الفرع الثاني :إعتراض المراسلات

تعتبر عملية إعتراض المراسلات من بين أهم الإجراءات المستحدثة ،لما لها من أهمية وفائدة في جمع الأدلة الجنائية الرقمية ،ومنه وجب التطرق لهذا الإجراء من خلال :

أولا : مفهوم إعترض المراسلات:

ان إعتراض المراسلات والتسجيل وإلتقاط المراسلات والأصوات والصور ،من بين أهم الآليات المعتمدة من قبل المشرع الجزائري ،حيث أنه بالرجوع لنص المادة 65 مكرر5 من القانون رقم 22/06،والتي جاء فيها "إذا إقتضت ضرورات التحري في الجريمة المتلبس بها ،أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود أو الجرائم الماسة بالمعالجة الآلية للمعطيات أو ....، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي :

– إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.

– وضع الترتيبات التقنية ،دون موافقة المعنيين من أجل إلتقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه به أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص..."يتضح من خلال نص المادة أن المشرع الجزائري لم يعرف نظام إعتراض المراسلات هذا من جهة ، ومن جهة أخرى قام بتحديد مجال تطبيق هذا النظام ،حيث جعله يطبق على جرائم محددة بذاتها ،من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات .حيث يمكن أن يتعدى هذا النظام إلى جرائم أخرى فهو يتعلق فقط بالجرائم المذكورة في المادة السالفة الذكر ، ويبدو أن المشرع الجزائري قد راعى الكثير من الإعتبارات للأخذ بالمفهوم الحصري للجرائم في هذا الخصوص وذلك يعود للأسباب التالية :

[1] قانون 06-01المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته ،كل شخص أخفى عمدا كل أو جزء من العائدات المحصل عليها من إحدى الجرائم المنصوص عليها في هذا القانون .

– أن الجرائم المذكورة تعد الأخطار بذاتها، وهي جرائم يرتكبها أشخاص محترفون وتتوافر لديهم مؤهلات خاصة بالإضافة إلى صعوبة إثبات هذه الجرائم .

– أن نظام إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور ، يعد من الناحية الشكلية إعتداء واضحا على الكثير من المبادئ الدستورية المستقرة ،وخاصة حرمة الحياة الخاصة والحق في الخصوصية وضرورة الحصول على الأدلة بالطرق المشروعة وغيرها[1].

ثانيا : شروط إعتراض المراسلات:

بالرغم من أن عملية إعتراض المراسلات تشكل إنتهاكا لحرمة الحياة الخاصة للأفراد ،وإعتداء على سرية مراسلاتهم والتي كفلها في دستور 1996المعدل بموجب القانون رقم 16-01 وذلك من خلال المادة 46 فقرة 2 التي نصت على"سرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة "[2] إلا ان المشرع الجزائري قد وضع شروط قانونية تنص على منع التعسف في إستعمالها وكذلك حماية الحرية الفردية وتتمثل هذه الشروط في الحصول على إذن من وكيل الجمهورية ،أو من قاضي التحقيق إذا تم فتح تحقيق قضائي [3] زيادة على ذلك أن يكون الإذن الصادر عن وكيل الجمهورية أو عن قاضي التحقيق مكتوبا لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات البحث والتحري ،وأيضا وجوب تضمنه كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إلتقاطها والأماكن المقصودة [4]وفي الأخير أن يكون هذا الإجراء في الجرائم المحددة بموجب المادة 65 مكرر 5 والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

[1] سليمان النحوي ،مرجع سابق ،ص10.

[2] انظر المادة 2/46من الدستور الجزائري المؤرخ في 1966/12/08المعدل والمتمم بالقانون رقم 16-01 المؤرخ في 2016/03/06 المعدل والمتمم في دستور 2020من خلال 46 التي تنص على ان "لكل شخص كان محل توقيف او حبس مؤقت تعسفيين او خطا قضائي الحق في التعويض ، يحدد القانون شروط و كيفيات تطبيق هذا الحكم ،العدد14 .

[3] انظر المادة 65مكرر05 ، من الامر 66-155 المتضمنٌ ق ا ج ج ،المعدل والمتمم السالف الذكر .

[4] انظر المادة 65مكرر 07 ،المتضمن ق ا ج ج ،السالف الذكر.

ثالثا : طرق إعتراض المراسلات :

يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني ومن ثم فعملية الإعتراض تنصب عليه والتي تمثل مصدرا غنيا للأدلة الرقمية للإثبات الجرائم الإلكترونية ومن المعلوم أن الرسالة إلكترونية يظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه ،ولكن هذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إطلاق رسائله من صناديق بريد مسجلة بأسماء وهمية ،كما أن هناك وسائل تتيح للمرسل أن يرسل رسالته دون أن يظهر فيه عنوان بريده الإلكتروني الصحيح لذلك لا بد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الإلكتروني والتي يطلق عليها مصطلح (email header)،وهي أول خطوة للبدء بالتحري عن مرسل الرسالة الإلكترونية وهذه الأخيرة لا تظهر بصورة مباشرة وإنما يتطلب الأمر من المستخدم إجراء بعض الخطوات للحصول عليها[1].

الفرع الثالث :المراقبة الإلكترونية

تعتبر المراقبة الالكترونية من أهم إجراءات التحري التي غالبا ما يستعان بها في البحث والتقصي في مجال الجرائم السيبرانية ،حيث إستحدث المشرع الجزائري هذا الإجراء بموجب القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ،وسوف نتناول بالشرح هذا الإجراء في مايلي:

أولا : مفهوم المراقبة الإلكترونية :

من خلال إستقراء نصوص القانون رقم 09-04 نجد أن المشرع لم يعرف المراقبة الإلكترونية بل ترك أمر تعريفها للفقه ،حيث أنها "عمل أمني سياسي له نظام معلومات

[1] لامية بن دالي ،قروط سميرة ،النظرية العامة للاثبات الجنائي العلمي ،مذكرة ماستر حقوق ،تخصص قانون خاص وعلوم جنائية ،كليةالحقوق والعلوم السياسية ،جامعة عبد الرحمان ميرة ،بجاية ،2015-2016 ،ص67 .

إلكتروني يقوم فيه المراقب بمراقبة المراقَب بواسطة الأجهزة الإلكترونية عبر شبكة الأنترنت، لتحقيق غرض محدد وإفراغ النتيجة في ملف إلكتروني ،وتحرير تقارير بالنتيجة " [1] وعليه يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه ، بحيث يقوم بها ضابط من ضباط الشرطة القضائية ذو كفاءة تقنية عالية وبإستخدام تقنيات وبرامج إلكترونية .

ومن جهة أخرى بالرجوع لذات القانون نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الأدلة الجنائية الرقمية فقط ،بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة السيبرانية حماية للنظام العام من التهديد ،وهذا وفقا لما نصت عليه المادة 04 من القانون ، إذ يمكن القيام بهذا الإجراء للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، وكذا في حالة توفر معلومات عن إحتمال الإعتداء على منظومة معلوماتية ، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإ قتصاد الوطني[2].

ثانيا : شروط إجراء المراقبة الإلكترونية

بالرجوع إلى نص المادة 04من القانون رقم 09-04 ، نجد أن المشرع الجزائري قد حدد شروطا للجوء إلى إجراء المراقبة الإلكترونية ، وهي أن يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن منه ، بحيث لا يجوز إجراء عملية المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة ، حيث جاء في المادة "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطات القضائية المختصة ".

[1] سليمان النحوي ،مرجع سابق ،ص14 .

[2] زيدان زيبجة ،مرجع سابق ،ص127وما بعدها .

وقد حدد المشرع الجزائري في نفس المادة الحالات التي يطبق فيها إجراء المراقبة الإلكترونية [1]وهي :

" يمكن القيام بعمليات المراقبة الإلكترونية المنصوص عليها في المادة 03:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني .

ج- المقتضيات التحريات والتحقيقات القضائية ،عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية .

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ".

يتم منح الإذن لمدة 06 أشهر قابلة للتجديد ،على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها ،زيادة على ذلك أن تكون هناك ضرورة تتطلب هذا الإجراء وذلك عندما يكون من الصعب مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية ،وهو ما نصت عليه المادة 4 من خلال الفقرة "ج" من نفس القانون[2].

ثالثا : طرق المراقبة الإلكترونية :

تنفذ عادة عملية المراقبة الإلكترونية في مجال الجرائم المعلوماتية من خلال الإستعانة ببعض الوسائل التقنية نذكر منها :

[1] سليمان النحوي ،مرجع سابق ،ص06 .

[2] آمنة امحمدي بوزينة ،إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية ،مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمه مركز جيل البحث العلمي بالجزائر ،الموسوم بعنوان :اليات مكافحة الجرائم الالكترونية في التشريع الجزائري ،يوم 2017/03/29 ،ص74ومابعدها .

1- **تقنية تتبع بروتوكول الأنترنت (ip):** أو ما يسمى بعنوان الأنترنت هو العنصر المسؤول عن التراسل الحزم البيانية عبر شبكة الأنترنت وتوجيهها إلى أهدافها فهو موجود بكل جهاز إلكتروني مرتبط بشبكة الأنترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات ،ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية ،والثاني لمزود الخدمة ، والثالث لمجموعة الأجهزة الإلكترونية المرتبطة ،والرابع يحدد الجهاز الذي تم الإتصال منه ،وفي حالة وقوع جريمة إلكترونية فيمكن للخبير إتباع المسار التراسلي للبروتوكول(ip)للبحث عن رقم الجهاز المستعمل في إرتكاب الجريمة ،ومن ثم تحديد موقعه ومنه معرفة الجاني[1].

2- **إستخدام تقنية فحص البروكسي (proxy):**البروكسي هو الوسيط العامل بين الشبكة والمستخدم ،تستخدمه الشركات المقدمة لخدمة الإتصال لأجل إدارة الشبكة ، وضمان أمنها وتوفير حزمة الذاكرة الجاهزة **(Cache Memory)** يعمل البروكسي على تلقي طلب المستخدم للبحث عن صفحة ما فيتحقق البروكسي ضمن الذاكرة الجاهزة عما أذا جرى تنزيل الطلب من قبل فيقوم بإعادة إرسالها للمستخدم دون الحاجة إلى طلبها من الشبكة العالمية للمعلومات (web) من أجل تزويد المستخدم بها ، ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات والعمليات ، وهو ما يمنح للخبير فحصها واستخلاص الدلائل ضد المتهم وذلك من خلال تقفي آثاره بمساعدة مزود الخدمات.

3- **استعمال برامج التتبع المعلوماتية:** تقوم برامج التتبع على شاكلة برنامج **(Hack Tracer)** بالتعرف على محاولات الاختراق ومن قام بها ،وإشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ساكنة في خلفية المكتب ، عندما ترصد أي محاولة للقرصنة أو الاختراق وتسارع بغلق منافذ الدخول للمخترق ،ثم تبدأ بعملية مطاردته واقتفاء أثره

[1] ربيعي حسين ،آليات البحث والتحقيق في الجرائم المعلوماتية ،أطروحة دكتوراه في الحقوق ،كلية الحقوق والعلوم السياسية ،قسم الحقوق ،جامعة باتنة 1، 2015-2016،ص228

وصولا إلى تحديد عنوانه الإلكتروني(ip) واسم الشركة المزودة بخدمة الأنترنت ومعلومات أخرى[1].

4- **الإستعانة بنظام كشف الإختراق:** وهو النظام الذي يرمز له **(I –D –S)** وهو نظام يعتمد على مجموعة من البرامج التي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة مع تحليلها بحثا عن إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب والشبكة من خلال مقارنة نتائج التحليل مع الصفات المشتركة للإعتداءات المعلوماتية ،ففي حال استئناف أي منها يبادر لتسجيلها في سجلات حاسوبية خاصة **(Registre)** وهي السجلات التي يسعى لها ضابط الشرطة القضائية لتحليل أسلوب إرتكاب الجريمة وربما مصدرها[2].

[1] خالد ممدوح ابراهيم ،مرجع سابق ،ص306.

[2] ربيعي حسن ،مرجع سابق ،ص229ومابعداها.

الخاتمـــــــــــــــــة :

الجرائم السيبرانية هي من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث، حيث تعتبر من الجرائم الخطيرة والتي يصعب التحكم فيها والتصدي لها نظرا لخصوصيتها بإعتبارها جرائم عابرة للحدود، والسبب يعود إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كومبيوتر وشبكات الانترنت والمواقع الإلكترونية، ومن خلال هذا التطور التكنولوجي الحاصل في العالم الافتراضي الجديد، والذي صارت فيه المعلومة سيدة ومصدرا للقوة والمعرفة والسلطة والمال، بل وأكثر من هذا اصبحت معيارا لتطور الشعوب، ومع هذا فإن الأنترنت ومالها من مزايا إلا أنها جلبت معها مخاطرا جمة طورها المجرم السيبراني وصارت سلاحا لا يستهان به لممارسة نشاطاته الإجرامية، ورغم التزايد المستمر لمثل هذة الجرائم حيث وضعت الجزائر مجموعة من القوانين والتشريعات للحد منها، وخصصت لها اجهزة وهيئات لمواجهتها، ورغم ذلك فإن الجزائر مازالت عاجزة وغير قادرة لمثل هذا النوع من الجرائم ، وهذا راجع لارتفاع الخسائر وتزايد حجم الاضرار الناتجة عنها مما ادى إلى فكرة ترسيخ التعاون الدولي من خلال ابرام الإتفاقيات الدولية لمواجهة الجرائم السيبرانية .

ومن خلال هذه الدراسة توصلنا إلى النتائج التالية:

– لم يتفق الفقهاء على تعريف جامع وموحد للجرائم السيبرانية .

– تبين من خلال دراسة خصائص الجريمة السيبرانية انها تتمتع بطبيعة قانونية مغايرة تمام اللجريمة التقليدية .

– قصور القوانين التقليدية أمام هذه الجرائم المستحدثة .

– رغم إجتهاد المشرع الجزائري للتصدي لهذه الجرائم ،إلا انه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة .

– إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في البيئة الرقمية .

– ان حماية حقوق المؤلف والحقوق المجاورة فيما يتعلق بالمصنفات الرقمية تعتبر غير كافية لمواجهة الإعتداءات الواقعة عليها عبر الأنترنت، وبالأخص قرصنة البرامج وإستعمالها.

ومن خلال ما تقدم ،وبهدف مواصلة السير في إتجاه تفعيل مكافحة الجرائم السيبرانية ،تم إقتراح بعض التوصيات بخصوص هذا الموضوع :

– ضرورة مراجعة التشريعات الوطنية من خلال تشديد الوصف الجنائي والعقوبات المقررة للانماط الإجرامية للجريمة المعلوماتية و السيبرانية ،بغية تحقيق الردع والقضاء على الإجرام المعلوماتي .

– مساعدة شركات التقنية والأنترنت في إتخاذ إجراءات أمنية مناسبة سواءا من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة ، والبرامج .

– الإستعانة بمختصين وخبراء قادرين على تشخيص الجريمة السيبرانية والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء مهامها على أحسن صورة.

– عقد دورات مكثفة للكوادر البشرية العاملين في حق التحري والتحقيق ،والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب ،والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات ،ومعاهد تدريب الشرطة موضوعات عن جرائم الأنترنت.

– ضرورة إبرام إتفاقيات عربية ودولية في مجال مكافحة الجرائم السيبرانية .

قائـــــمة المراجـــــــــع :

الكـــــــتب:

- ممدوح ابراهيم خالد ، فن التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الاولى ،دار الفكر الجامعي، الاسكندرية.
- بيومي حجازي عبد الفتاح ، الاثبات الجنائي في جرائم الكومبيوتر والانترنت ،دار الكتب القانونية ،مصر ،2007.
- عبد العالي الدريبي ومحمد صادق إسماعيل، الجريمة الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- بوسقيعة حسن ، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الطبعة الاولى 2002.
- نهلا عبد القادر المومني، الجرائم المعلوماتية.
- نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت.
- قارة امال ، الحماية الجزائية للمعلوماتية في التسريع الجزائري، الطبعة الأولى، دار هومة.
- صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى، 2003.
- ديدان مولود ،قانون اجراءات جزائية ، الامر 11-02،دار بلقيس ، الجزائر.
- هروال نبيلة هبة ،الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، الطبعة الاولى ،دار الفكر العربي ،الاسكندرية ،2007.

أطروحات الدكتوراة والمجاستير:

- صغير يوسف ، الجريمة المعلوماتية المرتكبة عبر الانترنت، مذكرة ماجستير، جامعة تيزي وزوو، كلية الحقوق والعلوم السياسية،2012-2013.
- براهيمي جمال ،مكافحة الجريمة الالكترونية في التشريع الجزائري ،المجلة النقدية للقانون والعلوم السياسية،كلية الحقوق والعلوم السياسية ،جامعة مولود معمري ،تيزي وزو،العدد2.

- معتوق عبد اللطيف ، الاطار القانوني لمكافحة جرائم المعلوماتية في التسريع الجزائري والتسريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخصر بباتنة ، كلية الحقوق والعلوم السياسية،2011-2012، ص 07.
- سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير، جامعة ابو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية ،2010-2011.
- رصاع فتيحة، رسالة الماجستير، الحماية الجنائية للمعلومات على شبكة الانترنت.
- بن عقون حمزة، السلوك الإجرامي لمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علمالإجرام والعقاب، جامعة باتنة، -2012 2011.
- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي،جامعة منثوري، قسنطينة،2012- 2013.
- دغشى العجمي عبد الله ، رسالة ماجستير بعنوان،المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة.
- سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير فيالعلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، ،2012-2013.

مذكـــــــــرات المـــــــــاستر

- بعرة سعيدة ،الجريمة الاكترونية في التشريع الجزائري ،دراسة مقارنة، مدكرة ماستر، 2016.
- نايري عائشة ، الجريمة الالكترونية في التشريع الجزائري ، مذكرة ماستر ، جامعة ادرار ، 2016-2017.

مذكـــــــرات القضـــــــاء

- حاجب هيام، الجريمة المعلوماتية، مذكرة لنيل إجازة المدرسة العليا للقضاء، الجزائر،2005-2006.
- بن دعاس فيصل ،اجراءات التحري في الجرائم المعلوماتية ،محاضرة في اطار التكوين المحلي المستمر للقضاة ،مجلس قضاء قسنطينة.

المقـــــــــالات

- روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24، سهر 5سنة 2020.
- عبد الله عبد الكريم، جرائم المعلوماتية والانترنيت، منشورات الحلبي الحقوقية بيروت، 2005
- فايز بن عبد الله الشهري، التحديات الامنية المصاحبة لرسائل الاتصال الجديد دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي.
- كريمة علة ، الجهات القضائية الجزائية ذات الاختصاص الموسع ،المجلة الاكادمية للبحث القانوني ،المجلد11، عدد2015/01.
- فاطمة زهرة بوعناد،مكافحة الجريمة الاكترونية في التشريع الجزائري ،،مجلة الندوة للدراسات القانونية جامعة سيدي بلعباس.
- كاظم محمد عطيات ،محمد رضوان هلال،كيفية التعامل التقني والآمن مع اوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص ، المجلة العربية الدولية للمعلوماتية ،العدد الخامس ،المجلد 3،السعودية 2014.
- سعيدة بوزنون ،مكافحة الجريمة الالكترونية في التشريع الجزائري ،مجلة العلوم الانسانية، المجلد ب،عدد52/ديسمبر 2019.

النصـــــــوص القـــــانـــــــونية

- القانون رقم 04-14 المؤرخ في 2004/11/10 المعدل والمتمم للامر66-155المؤرخ في 1966/06/08 ، المتضمن قانون اجراءات جزائية، الصادر في ج—ر عدد71، تاريخ 2004/11/10.
- قانون رقم 15/04المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156،يتضمن قانون العقوبات ،ج –ر،عدد71، الصادرة في 2004/11/10،معدل ومتمم.
- قانون رقم 06-22مؤرخ في2006/12/20،يعدل ويتمم بالامررقم 66-155 ، يتضمن قانون اجراءات جزائية ،ج—ر،عدد84،الصادر في 2006/12/24.
- القانون رقم 09-04المؤرخ في 2009/08/05يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ،ج-ر عدد47،بتاريخ 16/،2009/08 .
- الامر 04-15، القانون الصادر في 10 نوفمبر 2010 ،يعدل ويتمم الامر رقم 156/66، لصادر في 08 جوان 1966، المتم قانون العقوبات، ج ر العدد 71.

الملتقيـــــــــــــــات

- نبيل ادريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية، كلية الحقوق والعلوم السياسية. جامعة البليدة 02.
- ياسمينة بونعار، الجريمة المعلوماتية، جامعة الأمير عبد القادر للعلوم الإسلامية.
- ابتسام حمديني، أسلوب التحقيق في الجرائم الالكترونية كآلية لمكافحتها، مداخلة بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11و 12افريل2017.
- رحيمة النميلي، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في المؤتمر الدولي 14، طرابلس،عنوان :الجرائم الالكترونية طرابلس، يومي 24و 25 مارس 2017.
- هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح آلية حربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون والكومبيوتر والانترنت، جامعة الامارات المتحدة كلية السريعة والقانون، الطبعة الثالثة مجلد الثاني ،2004.

- عبد المومن بن صغير، "الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في الترجيع الجزائري والترجيع المقارن، "مداخلة مقدمة من فعاليات الملتقى الوطني، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة ممد خيضر بسكرة، بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16و17نوفمبر2005.
- حسين نوارة ،آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا ،الملتقى الوطني (آليات مكافحة الجرائم الالكترونية في التشريع الجزائري)،الجزائر.
- فضيلة عاقلي ،الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، مؤتمر الدولي الرابع عشر (الجرائم الاكترونية)،طرابلس.
- هواري عياش ،مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية المعهد الوطني للادلة الجنائية وعلم الاجرام ،كلية الحقوق ،جامعة بسكرة ،2016.
- سالم عبد الرزاق ،ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ،بمحكمة سيدي امحمد ،الجزائر.
- سليمان النحوي ،آليات مكافحة الجريمة السيبرانية في التشريع الجزائري ،مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية ،قسم الحقوق، جامعة برج بوعريريج ، الموسوم بعنوان الاجرام السيبراني المفهوم والتحديات ، يومي 12/11 افريل 2017.

فهرس المحتويات