الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –الطارف
كليّة الحقوق والعلوم السياسية
قسم الحقوق

الرقم التسلسلي:.....

مذكرة بعنوان:

الجريمة الإلكترونية في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون الأعمال

إعداد الطالب(ة):
حسام زغيدة
عمر بعلوج

إشراف الأستاذ:
أحمد حسين

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
سارة قريمس	أستاذ مساعد أ	الشاذلي بن جديد -الطارف	رئيسا
أحمد حسين	أستاذ محاضر أ	الشاذلي بن جديد -الطارف	مشرفاً ومقرراً
بن نولي زرزور	أستاذ محاضر أ	الشاذلي بن جديد -الطارف	ممتحنا

السنة الجامعية: 2023/2022

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق و العلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : حسام زغيدة

الحامل لبطاقة التعريف الوطنية رقم: 109270751032600004

الصادرة بتاريخ: 2016/10/10

عن دائرة: سكيكدة

المسجل بقسم : الحقوق تخصص قانون الأعمال

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

الجريمة الإلكترونية في التشريع الجزائري

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2023/06/04

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BEND/EDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : .....بصلوح عمر.....

الحامل لبطاقة التعريف الوطنية رقم: 109720367003080000.....

الصادرة بتاريخ: 2020/10/27.....

عن دائرة: .....بائنة ولاية باتنة.....

المسجل بقسم : .....قسم الحقوق تخصص قانون أعمال.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

.....الجريمة الالكترونية في التشريع الجزائري.....

.....

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2023/06/04

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –الطارف
كليّة الحقوق والعلوم السياسية
قسم الحقوق

الرقم التسلسلي:.....

مذكرة بعنوان:

الجريمة الإلكترونية في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون الأعمال

إعداد الطالب(ة):
حسام زغيدة
عمر بعلوج

إشراف الأستاذ:
أحمد حسين

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
سارة قريمس	أستاذ مساعد أ	الشاذلي بن جديد -الطارف	رئيسا
أحمد حسين	أستاذ محاضر أ	الشاذلي بن جديد -الطارف	مشرفاً ومقرراً
بن نولي زرزور	أستاذ محاضر أ	الشاذلي بن جديد -الطارف	ممتحنا

السنة الجامعية: 2023/2022

قال تعالى :

" وَيَرَى ٱلَّذِينَ أُوتُواْ ٱلْعِلْمَ ٱلَّذِيٓ أُنزِلَ
إِلَيْكَ مِن رَّبِّكَ هُوَ ٱلْحَقَّ وَيَهْدِيٓ إِلَىٰ
صِرَٰطِ ٱلْعَزِيزِ ٱلْحَمِيدِ "

سورة سبأ

إهداء

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

أهدي ثمرة جهدي إلى والدي الكريمين حفظهما الله و رعاهما و أطال في عمرهما و متعهما بالصحة و العافية .

إلى رفيقة دربي و سندي زوجتي حفظها الله بحفظه التام و عينه التي لا تنام و أبعد عنها كل مكروه .

إلى صديقي بوصيدة فيصل الذي رافقني بكل صدق .

إلى كل من ساعدني من قريب أو بعيد في إنجاز هذا العمل المتواضع

إلى جميع الزملاء و الأصدقاء .

حسام

إهداء

أهدي ثمرة جهدي إلى كل من ساعدني من قريب أو بعيد .

إلى عائلتي الكريمة ، الزوجة الغالية و الأبناء البررة الذين كانوا نعم السند

و نعم المشجع و خاصة إبني عبد الوهاب .

إلى كل أساتذتي و زملائي .

عمر

كلمة شكر و عرفان

يسرنا أن نتقدم بجزيل الشكر و الإمتنان الى اللجنة الموقرة التي قبلت مناقشة هذه المذكرة المتواضعة

كما نتقدم بالشكر الجزيل إلى الذي شجعنا ووقف وراء هذا العمل المتواضع بمجهوداته و نصائحه القيمة و سعة صدره التي كانت لها الأثر الكبير في إتمام هذا العمل .

إلى أستاذنا المشرف الدكتور

" أحمد حسين "

حسام و عمر

قائمة المختصرات

إ.أ.م.إ.م	الإتفاقية الأوروبية لمكافحة الإجرام المعلوماتي
إ.ع.م.ج.ت.م	الإتفاقية العربية لمكافحة جرائم تقنية المعلومات
ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري
ق.إ.ج.ف	قانون الإجراءات الجنائية الفرنسي
ق.ع.ج	قانون العقوبات الجزائري
ق.ع.ف	قانون العقوبات الفرنسي
ق.م.ج	القانون المدني الجزائري
OCDE	منظمة التعاون الاقتصادي والتنمية

مقدمة

يشهد العالم اليوم تطورا تكنولوجيا و معلوماتيا كبيرا ساهم في تسهيل الحياة اليومية للأفراد في جميع الميادين ، إذ أضحت أجهزة الكمبيوتر ، الهواتف الذكية و الأنترنت عناصر ضرورية في حياة كل جل المجتمعات و أضحى استخدام الأجهزة الذكية بمختلف أنواعها و أحجامها و وظائفها سواءا لإنشاء قواعد بيانات و تسييرها أو الوصول إلى المعلومة أو المشاركة في مختلف الأنشطة التي لا تعد أو تحصى و بأقل تكلفة .

غير أن هذا التطور الذي تعرفه البشرية في الفترة الأخيرة جراء ثورة المعلوماتية أدى إلى ظهور نوع جديد من الجرائم ، تستهدف المعلومات و البرامج والأجهزة أو تستعملها كوسيلة ، وهو الجانب السلبي لتكنولوجيا المعلوماتية ، وهو ما أعطى مفاهيم جديدة للجريمة و المجرم .

فالجريمة الإلكترونية ترتكب متى توفرت بيئة افتراضية تتعدد فيها الوسائل و تختلف فيها الأهداف ، بيئة لا تعترف بالزمان و المكان فيها فأصبحت المعلوماتية وسيلة لارتكاب أنشطة إجرامية مختلفة كالاعتداء على الحياة الخاصة للأفراد و بياناتهم الشخصية ، و كذلك الجرائم المرتبطة بالأنظمة الإلكترونية و الشبكة المعلوماتية .

إن التزايد المستمر للجريمة الإلكترونية يعود لتطور تقنية و أسلوب ارتكابها و كذلك ضخامة الخسائر التي تحدثها ، و صعوبة اكتشاف الجاني لا يقتصر على الدراية و الذكاء و الاستغلال المحكم لمسرح الجريمة ، لأن الجريمة الإلكترونية ترتكب في بعض الأحيان دون وجود مسرح للجريمة أو قد تتعدد المسارح لجريمة واحدة ، و هو ما يستوجب طرق تحري تتلائم و خصوصيتها مما جعل الدول تدق ناقوس الخطر بسبب تنامي الجريمة الالكترونية و السعي للحد منها من خلال السياسة التشريعية و الوسائل الوقائية اللازمة من أجل مواكبة التطورات الحاصلة في ارتكاب الجريمة الإلكترونية و أساليبها حيث ترتكب و تمحى أثارها أو تتلف الأدلة في زمن قصير جدا مما يصعب إكتشافها أو إثباتها .

والجزائر و على غرار أغلب الدول عملت من أجل الاستفادة من التكنولوجيا الحديثة و العمل على الانتشار الواسع لاستعمال شبكات الانترنت ورقمنة نظامها المالي و الإداري و بما أن الجريمة

الإلكترونية منتشرة في جميع دول العالم باختلاف أنظمتها أو توجهاتها الاقتصادية فانها تزداد انتشارا في المجتمعات الحديثة بشكل عام و البلدان النامية بشكل خاص بسبب خصوصية التحولات الاجتماعية و الاقتصادية .

ووعيا من المشرع الجزائري بخطورة الجريمة الالكترونية على جميع الأصعدة عمل على مكافحة هذا النوع المستحدث من الجرائم من خلال نصوص تنظيمية و أخرى اجرائية و نصوص عقابية لمحاربة الجرائم التي تستعمل الوسائل الالكترونية في الاعتداء على الأشخاص و المعلومات .

أهمية الموضوع :

تعتبر الجريمة الالكترونية ظاهرة اجتماعية ناتجة عن التحولات التقنية و الاقتصادية و الثقافية دوليا و وطنيا ، فالتطور التكنولوجي و تقنية المعلومات صاحبتها أفعال إجرامية خطيرة بسبب الاستخدام الغير مشروع لهذه التقنية ، تستدعي دراسة هذه الجريمة المستحدثة ذات الأساليب المتجددة ، لذى رأينا البحث في الجريمة الالكترونية و اعطاء صورة عامة عليها من خلال شرح و تحليل المفهوم القانوني للجريمة الالكترونية و كيف تعامل المشرع الجزائري إجرائيا مع هذا النوع من الجرائم .

الهدف من الدراسة :

تكمن أهداف هذه الدراسة في السعي إلى تقديم صورة واضحة للجريمة الالكترونية و كذا النصوص القانونية المتعلقة بها في التشريع الجزائري و التي هي في تعديل مستمر بما يتماشى و التطور الذي يشهده هذا النوع من الجرائم كما أن التوجه العام للدولة و المجتمع الى الادارة الالكترونية و تعميم استعمال التكنولوجيا في جميع الميادين مما يتطلب الأخد بعين الاعتبار لتهديدات الجريمة الالكترونية و خطورتها على المجتمع و أمن و سيادة الوطن ، ومن الناحية العلمية اضافة دراسة أخرى بطريقة مختلفة و أسلوب مغاير مع اضافة كل المستجدات العلمية و القانونية في سبيل إثراء الوسط العلمي .

الإشكالية :

إن التنامي المستمر لوسائل و أساليب التعامل بين الأشخاص والتطور الرهيب لتكنولوجيات الاتصال جعل من البيئة الرقمية و الافتراضية فضاءا خصبا للتعدي على الأموال و الأشخاص و بطرق حديثة و متطورة ، وهذا ما دفع بالتشريعات المختلفة إلى السعي في إستحداث سبل و أليات مختلفة لمكافحة هذه الظاهرة ، ومن خلال ما سبق يمكن صياغة الاشكالية على النحو التالي :

كيف تعامل المشرع الجزائري موضوعيا و إجرائيا مع التهديد المتنامي للجرائم الإلكترونية ؟

ويتفرع عنها التساؤلات التالية :

1- ما مفهوم الجريمة الإلكترونية و ماهي أهم صورها ؟

2- ماهي الإجراءات الجزائية التي وضعها المشرع الجزائري لمكافحة الجريمة الإلكترونية ؟

المنهج المتبع :

قصد الإجابة على الاشكالية و الاحاطة بجميع جوانبها فإننا اعتمدنا في دراستنا على المنهج الوصفي من أجل توضيح الاطار المفاهيمي للجريمة الالكترونية و المنهج التحليلي من خلال تحليل مختلف النصوص القانونية التي لها علاقة بالموضوع و تحليل الطبيعة الاجرائية و نجاعتها في ردع و كبح هذه الجريمة .

أسباب إختيار البحث :

1- أسباب موضوعية :

على ضوء ما تقدم فقد اخترنا دراسة موضوع الجريمة الالكترونية كونها من الجرائم الحديثة و المتجددة التي تتطور باستمرار ما يعطي دائما مجالا للبحث و الدراسة حيث أن التطور التكنولوجي المستمر يصاحبه تطورا في أساليب الجريمة و هو ما يتطلب دائما تطورا في اليات المكافحة ، وهذا ما يجعل موضوع الجريمة الإلكترونية خصبا للدراسة و البحث .

2- أسباب ذاتية :

إن حاجة الأفراد للتطور التكنولوجي لتسهيل حياتهم على جميع الأصعدة جعل حاجتهم للوسط الرقمي جد كبير و هذا ما جعلهم عرضة لأنواع جديدة و متجددة للجرائم و بما أن ارتباط المعلوماتية بحياتنا اليومية وثيق إرتأينا دراسة هذا النوع من الجرائم ،كما أن دراساتنا السابقة في مجال الإعلام الألي أعطانا رغبة لدراسة هذا النوع من الجرائم .

خطة البحث :

للإجابة على هذه الإشكالية و الاشكاليات المتفرعة إرتأينا تقسيم بحثنا إلى فصلين أين تطرقنا في الفصل الأول إلى ماهية الجريمة الإلكترونية و تناولنا فيها مبحثين ، المبحث الأول تعرضنا فيه لمفهوم الجريمة الإلكترونية بصفة عامة حيث تضمن مطلبين (مفهوم الجريمة الإلكترونية ، خصائص الجريمة الإلكترونية ، و أركانها) ، أما المبحث الثاني فتناولنا فيه أنواع و صور الجريمة الإلكترونية من خلال مطلبين .

في الفصل الثاني تطرقنا للجانب الإجرائي في معالجة الجريمة الإلكترونية في التشريع الجزائري ، فتناوناه في مبحثين ، فتعرضنا لإجراءات المتابعة والعقوبات المقررة في المبحث الأول الذي تناولناه في مطلبين وتناولنا في المبحث الثاني أساليب مكافحة المشرع الجزائري للجريمة الإلكترونية ، في المطلب الأول تعرضنا للمكافحة وفق قوانين عامة و في المطلب الثاني تناولنا المكافحة وفق قوانين و هياكل خاصة .

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

يعيش العالم ثورة معلوماتية على جميع المستويات و هذا ما ألقى بضلاله على الجانب القانوني لسلوكات الأشخاص فضهرت مجموعة جديدة من الجرائم لها علاقة بالعالم الافتراضي الرقمي ، لا تعترف بحدود أو وقت ، فسعت كل التشريعات الى مجابهة هذه الضاهرة ، ومن أجل ذلك وجب التعريف بهذه الضاهرة و إضهار مختلف سماتها و مميزاتها ، ومن أجل ذلك سنتناول بحثنا في مبحثين ، نتناول في المبحث الأول مفهوم الجريمة الإلكترونية ، ويكون ذلك من خلال مطلبين ، في المطلب الأول نتناول تعريف الجريمة الإلكترونية و في المطلب الثاني نتناول فيه الخصائص و الأركان ، أما في المبحث الثاني فنتطرق إلى أنواع و صور الجريمة الإلكترونية .

المبحث الأول: مفهوم الجريمة الإلكترونية :

تعتبر الجريمة الإلكترونية من الجرائم الحديثة التي انتشرت بشكل كبير في السنوات الأخيرة، فهي تنشأ من استخدام تقنيات المعلومات بطريقة غير قانونية للقيام بأفعال تسبب الإعتداء على الأموال والأشياء المعنوية. وما يمكن الاشارة له هو وجود تعاريف متعددة للجريمة الإلكترونية ، وعدم الاتفاق على تعريف محدد وموحد لها راجع للتطور المستمر في هذا المجال. و ظهرت تسميات متعددة لهذا النوع من الجرائم، جرائم الحاسوب الآلي والانترنت أو الجرائم المتصلة بالكمبيوتر أو الجريمة المعلوماتية [1] أو جرائم تكنولوجيا المعلومات أو إساءة استخدام تكنولوجيا المعلومات ، و ظهرت تسميات أخرى مثل جرائم أصحاب الياقات البيضاء وجرائم الهاكر والسبرانية[2]، وذلك بسبب المنطلقات المختلفة في التطرق لموضوع الجريمة الالكترونية, وسنتناول في هذا المبحث مفهوم الجريمة الالكترونية في نظر الفقه و موقف المشرع الجزائري (المطلب الأول) والخصائص المميزة للجريمة الإلكترونية و أركانها (المطلب الثاني).

المطلب الاول: تعريف الجريمة الإلكترونية :

إن جرائم الحاسبات الالكترونية أو كما تسمى بجرائم المعلوماتية هي ظاهرة إجرامية حديثة النشأة، وبسبب تعلقها بتكنولوجيا الحاسبات الآلية فقد اكتنفها الغموض ، وهذا ما صعب من عملية تحديد مفهومها , فإذا كانت التشريعات المختلفة قد ركزت على سن الجزاءات فإن الفقه تناول مفهوم الجريمة الالكترونية وفق نظريات مختلفة , فتعددت الآراء والأفكار بشأن المفهوم، فهناك من اعتمد في تعريفه على الجانب الفني وهناك من اعتمد على الجانب القانوني وهناك من اعتمد على معايير أخرى مختلفة[3]

---

[1] نهلا عبد القادر المومني ،"*الجرائم المعلوماتية*" ، الطبعة 01 ، دار الثقافة للتوزيع و الانتاج , عمان , الاردن , 2010 , ص 46 .

[2] حسن بن احمد الشهري , "*قانون دولي موحد لمكافحة الجرائم الالكترونية*" , المجلة العربية للدراسات الامنية والتدريب , العدد 53 , المجلد 27 , ص 12 .

[3] مختارية بوزيدي ,*" ماهية الجريمة الالكترونية* ", الملتقى الوطني اليات مكافحة الجرائم الالكترونية في التشريع الجزائري , مركز جيل البحث العلمي , 2017 , ص 9 .

الفرع الأول : تعريف الفقه للجريمة الإلكترونية :

هناك غموض كبير يحيط بالمصطلحات المستخدمة التي تحيل الى الجرائم الإلكترونية نتيجة عدم وجود اتفاق قانوني أو فقهي شامل يحدد المصطلح المناسب لهذه الجرائم. يعود هذا الغموض إلى تطور التقنية المتسارع وظهور جرائم جديدة تختلف في معالجتها وتحديد المفاهيم المطلوبة لها من بلد إلى آخر. هذا الوضع يشكل تحديات كبيرة.

وعلى الرغم من هذا الوضع، يعمل الفقهاء على وضع مفهوم واضح لهذه الظاهرة، حيث يوجد اتجاهان بارزان في هذا الصدد ، و سيتم دراسة هذين الاتجاهين وسنقوم كذلك باستعراض موقف المشرع الجزائري في هذا السياق. [1]

أولا: الاتجاه الضيق لمفهوم الجرائم الإلكترونية :

يتجه العديد من فقهاء القانون إلى تحديد تعريفات ضيقة للجرائم الإلكترونية، ويربطونها بمجموعة من المعايير مثل الحاسوب، أو المستخدم، أو طبيعة الجريمة. على سبيل المثال، فقد وصف الفقيه (Merwe) الجريمة الإلكترونية بأنها "أي فعل غير قانوني يشتمل على استخدام الحاسوب في تنفيذه، سواء كان الحاسوب هو الأداة الرئيسية المستخدمة في تنفيذ الجريمة، أو تشمل سلوكيات إجرامية متعددة يتم تنفيذها باستخدام معالجة بيانات آلية"[2].

كما يرى أنصار هذا الإتجاه أنها "كل فعل غير مشروع يكون العلم و تكنولوجيا الحاسبات الالية بقدر كبير لازم لارتكابه من ناحية و ملاحقته و تحقيقه من ناحية أخرى"[3] , وكذلك يعرفونها بأنها "الجرائم التي يتم ارتكابها باستخدام الحاسوب أو الإنترنت"[4]، وفي نظر مكتب تقييم التقنية في الولايات

[1] يزيد بوحليط , "*الجرائم الالكترونية و الوقاية منها في القانون الجزائري*" , دار الجامعة الجديدة , الاسكندرية , 2019 , ص31 .

[2] عبد العال الديربي ، محمد صادق اسماعيل،" *الجرائم الالكترونية-دراسة قانونية قضائية مقارنة* " ، المركز القومي للاصدارات القانونية القاهرة، مصر، ط1 ،2012 , ص 40 .

[3] خالد ممدوح ابراهيم , "*أمن الجريمة الالكترونية* " , الدار الجامعية , الاسكندرية , 2008 , ص42

[4] علي جبار الحسيناوي , "*جرائم الحاسوب و الانترنت*" , دار اليازوري العلمية للنشر والتوزيع , 2018 , ص23 .

المتحدة، يعتبر استخدام بيانات الكمبيوتر والبرامج المعلوماتية بشكل أساسي هو العنصر المميز في تعريف الجريمة الإلكترونية[1].

كما عرفها الاستاذ Mass بأنها :"" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح" ، و يصف الفقيه روزنبلات (Rosenblatt) الجريمة الإلكترونية على أنها "أي نشاط غير قانوني يشمل الوصول إلى أو تغيير أو حذف المعلومات المخزنة داخل الحاسوب، أو المعلومات التي تم نقلها عبره". ويعرفها تادمان(Tiedemann) ، الفقيه الألماني، بأنها "كل أشكال السلوك غير المشروع التي يتم ارتكابها باستخدام الحاسوب[2]" .بالتالي، يعتقد أتباع هذا التوجه في تعريف الجرائم الإلكترونية أن وجود الحاسوب يعد عنصرًا أساسيًا يستخدم كأداة أو هدف في ارتكاب الجريمة. فالحاسوب يمكن أن يكون الوسيلة التي يستخدمها الجاني لتنفيذ جريمته، سواء كان ذلك عبر الوصول غير المشروع إلى معلومات أو القيام بتلاعبات في البيانات أو تنفيذ هجمات إلكترونية أخرى. وبالإضافة إلى ذلك، يمكن أن يكون الحاسوب هدفًا للجريمة، مثل تعطيل الخدمات المعلوماتية أو اختراق أنظمة الأمان[3].

بالنسبة للأشخاص المعنيين بالتحقيق والتطبيق القانوني، فإن فهم تقنية الحاسوب والمعرفة المسبقة بمفاهيمها وأساليبها تعتبر ضرورية. فذلك يمكن أن يساعدهم في جمع الأدلة الرقمية وتتبع المتورطين في هذه الجرائم. علاوة على ذلك، فإن فهمهم لتقنية الحاسوب يمكن أن يسهم في وضع تدابير أمنية وقانونية فعالة للحماية من الجرائم الإلكترونية والحد من تأثيرها .

ومع ذلك، يجب أن نلاحظ أن هناك بعض الجرائم الإلكترونية التي لا تتطلب معرفة خاصة بتقنية المعلومات. فبعض الأفعال غير المشروعة مثل إرسال رسالة نصية أو بريد إلكتروني غير مرغوب فيه ، أو نسخ بيانات من الحاسوب يمكن أن تتم بدون معرفة متقدمة بتقنية الحاسوب[4]. ولذلك، يعتبر تقييد

[1] عبد الفتاح بيومي حجازي ," *جرائم الكمبيوتر و الانترنت* ", دار الكتب القانونية , مصر , 2007 , ص24

[2] نهلا عبد القادر المومني , المرجع السابق , ص 49 .

[3] يزيد بوحليط , المرجع السابق , ص32 .

[4] المرجع نفسه, ص33

الجرائم الإلكترونية بأفعال مرتبطة بالنظام المعلوماتي غير منطقي ، حيث أن هناك العديد من الأفعال غير القانونية التي يمكن أن تتم باستخدام الحاسوب ولا تدخل تحت تعريف الجرائم الإلكترونية ، مثل جرائم الاحتيال الإلكتروني[1].

ثانيا: الاتجاه الموسع لمفهوم الجرائم الإلكترونية:

هناك فريق من الفقهاء يسعى لتوسيع مفهوم الجرائم الإلكترونية أو المعلوماتية بمقاربة أوسع. حيث يتم تعريف الجرائم الإلكترونية على أنها : "كل فعل إجرامي أو متعمد ايا كانت صلته بالمعلوماتية ينشأ عنه خسارة بالمجني عليه, او كسبا يحققه الفاعل ".[2] ويشمل هذا التعريف جميع الأنشطة الإجرامية التي يمكن أن تتسبب في ضرر مادي أو معنوي، سواء كانت تتعلق بالمعلوماتية أو لا.

فمنظمة التعاون الاقتصادي والتنمية (OCDE) تعرف الجرائم الإلكترونية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "[3].

أما الفقه الفرنسي يعرف الجرائم الإلكترونية على أساس فكرة الغش المعلوماتي , حيث عرف كل من الفقيه ميشال Michel و الفقيه ريدو Redo الجريمة الإلكترونية بأنها " سوء استخدام الحاسب و يشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته , و كذا الاستخدام غير المشروع لبطاقات الائتمان و انتهاك ماكينات الحاسب الألية بما تتضمنه من شبكات تحويل الحسابات المالية طرق الكترونية و تزييف المكونات المادية و المعنوية للحاسب و سرقة الحاسب الالي في حد ذاته أو أي مكون من مكوناته" .[4]

---

[1] إيمان مكري , *"الجريمة الالكترونية في التشريع الجزائري"* , رسالة ماجستير , كلية علوم الاعلام و الاتصال , جامعة الجزائر 3 , 2015 , ص 138 .

[2] راضية عيمور , *"الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري "*, المجلة الاكاديمية للبحوث القانونية والسياسية , العدد 1 , المجلد 6 , 2022 , ص 90 .

[3] خالد حسن أحمد لطفي , *" الدليل الرقمي و دوره في اثبات الجريمة المعلوماتية "*, دار الفكر الجامعي , الاسكندرية , 2019 , ص 26 .

[4] عبد العال الديربي ، محمد صادق اسماعيل، المرجع السابق , ص 41 .

من جانبه، يعرف القانون العربي النموذجي الجرائم الإلكترونية على أنها "كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني".[1]

هذه التعاريف هي تفسيرات واسعة للجريمة الإلكترونية المرتكبة باستخدام الحاسب الآلي في جوانب مختلفة، سواء كانت الجريمة هي الهدف الأساسي أو وسيلة التنفيذ عبر الإنترنت أو غيرها من الوسائل التي يتم تطويرها في المستقبل، مثل الهاتف المحمول والفاكس وما إلى ذلك .

إن هذا الاتجاه يعطي توسعا كبيرا في تعريف الجريمة الإلكترونية ليشمل جميع الجرائم المرتكبة على أجهزة الكمبيوتر أو بالقرب منها، عبر الإنترنت، أو من خلال الأجهزة الحديثة الأخرى. بناءً على التعريف السابق، يتم استخدام أجهزة الكمبيوتر لارتكاب الجرائم ومهاجمة تلك الأجهزة وأنظمتها، واستخدام الأدوات الإلكترونية الأخرى المتاحة عبر التكنولوجيا الحديثة.

تتضمن الجرائم الإلكترونية عمومًا مزيجًا من الحوسبة وتكنولوجيا الاتصالات الحديثة. يوضح تاريخ تكنولوجيا المعلومات أنها تتكون من قطاعين متقاربين ومتكاملين: صناعة الحوسبة وصناعة الاتصالات. تستخدم الحوسبة الأساليب التكنولوجية لإدارة وتنظيم ومعالجة البيانات لتلبية احتياجات ومنطق أجهزة الكمبيوتر. من ناحية أخرى، يتميز الاتصال بالطريقة التي يتم بها نقل المعلومات بجميع أشكالها: الرسائل والأخبار والبيانات والمعرفة والوثائق والأدب. والأفكار والرموز والتعليمات المخفية والأخبار المفيدة والخصوصية وماشابه ذلك[2].

بدراسة التعاريف المختلفة، نجد أن تعريف منظمة التعاون الاقتصادي والتنمية واضح وشامل للأسباب التالية:

– تحديد لماهية السلوك الإجرامي للجريمة، إذ شمل كل من الفعل الإيجابي والسلوك السلبي المتمثل في الامتناع.

[1] تم إعداد القانون الاسترشادي العربي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب و الامانة العامة لجامعة الدول العربية، وتم إقراره سنة 2003 .

[2] يزيد بوحليط ، المرجع السابق ، ص34 .

– اعتماد تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة كما تتسم هذه التقنية بالتطور المستمر.

– يعبر عن الطابع التقني المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

– يتيح إمكانية التعامل مع التطورات المستقبلية في مجال تقنية المعلوماتية ونظم الاتصالات.

ومما سبق ذكره فسبب اختلاف الفقه في وضع تعريف للجريمة الإلكترونية أو المعلوماتية مرده الاختلاف في المعيار المعتمد وزاوية النظر للإتجاهات المختلفة. ومع ذلك ، يمكن تلخيص التعريف على أنه ، "سلوك غير قانوني , يتم معاقبته بموجب قانون , صادر عن إرادة جرمية ، تحدث في بيانات الكمبيوتر". يشمل السلوك الأفعال الإيجابية والسلبية ، ويعد غير شرعي لأن المشروعية تنفي الصفة الجرمية. وبما أن تحديد الصفة الإجرامية يتم بإرادة المشرع ومن خلال النصوص ، فإن موقع جريمة الكمبيوتر هو بيانات الكمبيوتر بأكملها ، بما في ذلك البيانات المدخلة والمعالجة والمخزنة والبرامج والمعلومات المستخرجة والمتبادلة بين الأنظمة المعلوماتية ... الخ . أما الكمبيوتر فهو "النظام التقني بمعناه الشامل الذي يجمع بين تقنيات الحوسبة والاتصالات ، بما في ذلك شبكات المعلومات"[1].

الفرع الثاني: موقف المشرع الجزائري :

نتيجة لثورة المعلومات الجديدة، ظهرت جرائم جديدة لم يشهدها المجتمع من قبل. وكما هو الحال مع التشريعات الأخرى، قام المشرع الجزائري بتعديل قانون العقوبات بإضافة القسم 07 مكرر من المواد 394 مكرر – 394 مكرر 7 بعنوان " جرائم المساس بأنظمة المعالجة الالية للمعطيات"[2]. وجاء في التعديل الجديد أنه نظراً للتقدم التكنولوجي والتوسع في وسائل الاتصال أدى ذلك الى ظهور أنواع جديدة من الجرائم، ومع هذا التعديل الجديد، تطمح الجزائر إلى توفير حماية قانونية لأنظمة المعلومات

[1] يونس عرب، " *صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية* "، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل ،2006 ، ص 7 .

[2] القانون رقم 04 – 15 المؤرخ في 10 نوفمبر ،2004(ج.ر71 ص11. و12)،القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن المواد من 394 مكرر إلى المادة 394 مكرر 7 .

الحاسوبية وأساليب معالجة البيانات، وسد الفراغ القانوني في بعض المجالات، وكذلك تشديد المسؤولية الفردية وعواقب المحاولة والتآمر ضد القانون .

ما يلاحظ هو استخدام المشرع الجزائري لمصطلح "الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال" لوصف الجرائم الإلكترونية والمعلوماتية، وذلك وفقًا للمادة 02/أ من القانون رقم 09-04، والذي يتضمن قواعد الوقاية ومكافحة هذه الجرائم[1]. وتشمل هذه الجرائم "التدخل غير المصرح به في أنظمة معالجة البيانات، وأي جرائم أخرى يتم ارتكابها باستخدام الأنظمة المعلوماتية أو الاتصالات الإلكترونية". وفيما يتعلق باستخدام المصطلح، فإنه يشير بشكل خاص إلى الأنظمة والمعلومات والشبكات التي تحتوي عليها .

وانطلاقا من فحوى هذه المادة نستنتج أن المشرع الجزائري قسم هذه الجرائم المستحدثة الى الاصناف التالية :

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية.
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الإلكترونية.

وقصد توضيح المصطلحات، نص في المادة (02/ب) نفسها على تعريف المنظومة المعلوماتية على أنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، والملاحظ أن هذا التعريف يتفق مع نص المادة الأولى من الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي (إ.أ.م.إ.م) ببودابيست لسنة 2001 [2] إذ تنص على :" يعتبر النظام المعلوماتي جهاز يتكون من معدات وبرامج قائمة للمعالجة الآلية للبيانات الرقمية ... يمكن أن تكون منفردة أو متصلة . مع أجهزة مماثلة أخرى داخل شبكة..." ، ويتفق أيضا

[1] قانون رقم 09 - 04 المؤرخ في 05 أوت 2009 , جريدة رسمية عدد47 , المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها الصادرة في 16 أوت 2009 .

[2] طرشي نورة ," *مكافحة الجريمة المعلوماتية* ", رسالة ماجيستير , كلية الحقوق , جامعة الجزائر 1 , 2012 , ص68 .

مع نص المادة (5/02) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (إ.ع.م.ج. ت.م) المحرّرة بالقاهرة بتاريخ 2010/12/21 ، والتي صادقت عليها الجزائر[1]. حيث عرفت النظام المعلوماتي على أنه:" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"[2].

فمن خلال استعمال المشرع الجزائري لهذا المصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الالكترونية فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة فالحوسبة تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها[3]، ومن خلال ما سبق يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها" كل السلوكات المجرمة التي يشكل الحاسوب و شبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الالكترونية ."[4]

المطلب الثاني: خصائص و أركان الجريمة الإلكترونية :

تتميز الجرائم الإلكترونية بقدرة شبكات المعلوماتية على نقل وتبادل المعلومات الشخصية والعامة في نفس الوقت، مما يتيح فرصة ارتكاب الجرائم. يعود السبب في ذلك إلى تنوع مراكز المعلومات ورغبة الأفراد في البقاء متصلين بالشبكة، حيث ترتبط هذه الجرائم بشكل كامل بمعالجة البيانات الإلكترونية. وتواجه هذه الجرائم تحديات قانونية نظرًا لطبيعتها الخاصة.[5]

---

[1] مرسوم رئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014 ، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 ، الجريدة الرسمية ، عدد57، مؤرخة في 14 سبتمبر 2014 ، ص 4 .

[2] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ، وافق عليها مجلسا وزراء الداخلية و العدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21-12-2010 ، المادة 2 .

[3] يزيد بوحليط , المرجع السابق ، ص39.

[4] يونس عرب، المرجع السابق ، ص 8 .

[5] فضيلة عاقلي ، "*الجريمة الالكترونية و اجراءات مواجهتها من خلال التشريع الجزائري* " ، أعمال المؤتمر الدولي الرابع عشر الجرائم الالكترونية ، مركز جيل البحث العلمي ، طرابلس ، 2017 ، ص 121 .

فالقوانين التقليدية لم تخصص لهذه الظواهر الحديثة، مما يؤدي إلى تعقيدات في تطبيقها على هذا النوع من الجرائم وتثير مشكلات متعددة، بدءًا من مسألة الإثبات وصولاً إلى متابعة الجناة. وبناءً على ما تم ذكره، يمكن القول إن الجرائم الإلكترونية تتمتع بطبيعة قانونية خاصة.

الفرع الأول: خصائص الجريمة الإلكترونية : تعتبر الجريمة المرتكبة عبر الإنترنت من بين الجرائم المستحدثة، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي ، ولذلك فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل:

أولا : خصائص متعلقة بالجريمة :

أ– تتطلب وجود جهاز الكتروني والتحكم بتقنية استخدامه: تتميز الجرائم الإلكترونية بالحاجة إلى استخدام أجهزة إلكترونية متقدمة كأساس لارتكابها، ومن هنا جاء تسميتها بهذا الاسم. بالإضافة إلى ذلك، يصعب على أي شخص ارتكاب جريمة إلكترونية بدون وجود اتصال بشبكة الإنترنت واستيعاب التكنولوجيا والمعلوماتية والاتصالات. وكلما كان المجرم متمكنًا بشكل أفضل في التحكم في هذه الجوانب الثلاث، زادت خطورته وقدرته على ارتكاب جرائم إلكترونية خطيرة [1].

ب – جريمة حديثة: تمثل الجرائم الإلكترونية نوعًا جديدًا من الجرائم، حيث تتميز بأساليب جديدة لارتكابها تتوافق مع تطور التقنية والحوسبة وتكنولوجيا المعلومات والاتصالات. تعتمد هذه الجرائم على استخدام العلوم والتقنية في تنفيذها، وتشتمل على مشتبهين ومجرمين ينتمون إلى دول مختلفة ويعملون عبر شبكات دولية.[2]

ج – ارتكاب الجريمة الإلكترونية اثناء تشغيل نظام المعالجة الآلية للمعلومات : تحدث الجريمة الإلكترونية عند تشغيل نظام معالجة البيانات ، وعلى الرغم من أنه يمكن ارتكاب هذه الجرائم عند

[1] إسمهان بوضياف ، "*الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر*"، مجلة الاستاذ الباحث للدراسات القانونية والسياسية ، العدد 11 ، سبتمبر 2018 ، ص356 .

[2] خالد ممدوح ابراهيم ، المرجع السابق ، ص51 .

إدخال أو إخراج البيانات، فإن مرحلة معالجة البيانات هي الأسهل والأخطر لارتكاب هذه الجرائم [1]، فعند إيقاف تشغيل الجهاز يكون آمنا، بغض النظر عن نوعه، سواء كان جهاز كمبيوتر أو جهاز إلكتروني ذكي ، و يمكن تلخيص مراحل ارتكاب الجريمة الإلكترونية فيما يلي: [2]

1- مرحلة الإدخال : إن ادخال بيانات ومعلومات غير صحيحة هي أسهل مرحلة كما يمكن أن تكون بعدم ادخال المعلومات المطلوبة والوثائق الأساسية وهي اكثر مرحلة ترتكب فيها الجرائم الإلكترونية.

2- مرحلة تشغيل نظام المعالجة الآلية للبيانات : ترتكب أي جريمة إلكترونية حين يتلاعب المجرم في برامج الحاسوب بإدخالِ تعديلات ونشر معلومات غير مصرح بها. بحيث يتم التسبب بتشغيل برامج تعطل بشكل جزئي أو كلي، ويكون المجرمْ محترفا ويمتلك التقنية لتحقيق هدفه.

3- مرحلة المعالجة الآلية للبيانات والمعطيات : في هذه الحالة تكون البيانات في وضعية نشطة وهي المرحلة المقصودة. حيث يكون الاعتداء على البيانات المخزنة في النظام من أجل معالجتها إلكترونيا ويمكن للمستخدم تصحيحها أو تعديلها أو محوها أو تخزينها أو إسترجاعها أو طباعتها وهذه العملية وثيقة الصلة بارتكاب الجرائم الإلكترونية.

4- مرحلة الإخراج : في هذه المرحلة يتم إرتكاب العمل الإجرامي على النتائج التي يخرجها النظام المعلوماتي للحاسوب وتكون عملية إدخال البيانات صحيحة ومعالجتها صحيحة لكن التلاعب يكون في النتائج ، أي ان النتائج لا تتوافق مع البيانات الموجودة في النظام .

د _ عالمية وعابرة للحدود: تُعد الجريمة الإلكترونية من فئة الجرائم الخاصة، حيث تحدث في العالم الافتراضي ويتم تنفيذها عن طريق أجهزة الكمبيوتر أو الأجهزة الذكية. يحدث ذلك من موقع

---

[1] شوقي يعيش تمام ," *الجريمة المعلوماتية دراسة تأصيلية مقارنة* ", مخبر أثر الاجتهاد القضائي على حركة التشريع , جامعة محمد خيضر , بسكرة , جانفي 2019 , ص27 .

[2] عادل يوسف عبد النبي الشكري ," *الجريمة المعلوماتية وأزمة الشرعية الجزائية* ", مجلة مركز دراسات الكوفة , العراق , العدد 7, المجلد5, 2008 , ص 115.

الجاني في إحدى الدول، حيث يستهدف موقع الجريمة في دولة أخرى أو دول متعددة، وبذلك يتجاوز الحدود الجغرافية. تصبح الحدود الجغرافية غير ذات أهمية مع ظهور الشبكة العنكبوتية العالمية، التي جعلت العالم يتحول إلى قرية صغيرة [1] ، لأنها تقع في عالم افتراضي واتصالها بعالم الانترنات وتقنية المعلومات يسهل الاتصال بين حواسيب لا حصر لها في عدة دول فالجرائم الالكترونية ترتكب عن بعد ، حيث يرتكبها شخص جالس امام شاشة الكمبيوتر ببلد ولا يكون في مسرح الجريمة [2]. إن الجرائم الإلكترونية قد تؤثر على ضحايا في بلدان مختلفة في نفس الوقت، وذلك يعزى بشكل خاص إلى إزالة الحدود الاقتصادية بفضل انتشار التجارة الإلكترونية التي تُزيل الحواجز الجمركية وتُمكّن من سهولة تنقل رؤوس الأموال. هذا يخلق تحديات فيما يتعلق بتطبيق القانون، حيث يتم التخطيط للجريمة في بلد معين، وتنفيذها في بلد آخر، ويكون الضحية في بلد ثالث. تُظهر الطابع العالمي للجرائم الإلكترونية تعقيدات في مجال تنفيذ القوانين المعمول بها، نظرًا للتعامل مع جوانب متعددة تتعدى الحدود الجغرافية.

هـ – قلة الإبلاغ عن الجريمة الإلكترونية : تواجه كشف الجرائم الإلكترونية صعوبات بسبب قلة التبليغ عنها. يُفسر هذا بوجود عدم إبلاغ كافة الجرائم المرتكبة، حيث يتم اكتشافها بعد فترة من ارتكابها عادةً وعن طريق الصدفة. يترتب على ذلك أن الضحايا، سواء كانوا مؤسسات عامة أو خاصة أو ذوو جنسيات مختلفة، قد لا يقومون بالإبلاغ عن تلك الجرائم. و ذلك بسبب مخاوف من التأثير السلبي على سمعتهم أو هز ثقة زبائنهم، وخاصة إذا كانوا بنوكًا أو مؤسسات مالية. كما قد يكونون يخشون التداعيات النفسية والاجتماعية، خاصة في حالة الابتزاز والتهديد بنشر معلومات أو صور خاصة للأشخاص الطبيعيين الضحايا [3] .

---

[1] فتيحة رصاع ، "*الحماية الجنائية للمعلومات على شبكة الأنترنت* "، رسالة ماجيستير, جامعة أبي بكر بلقايد ، تلمسان , 2012 ، ص 43 .

[2] نهلا عبد القادر المومني ، المرجع السابق ، ص 51 .

[3] خالد ممدوح ابراهيم ، المرجع السابق ، ص51 .

و :صعوبة اكتشاف الجريمة الإلكترونية واثباتها : صعوبة متابعتها واكتشافها بحيث لا تترك أثر فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير وذلك راجع لكونها تفتقر إلى الدليل المادي التقليدي كالبصمات و يصعب الاحتفاظ الفني بآثارها إن وجدت ، فضلا عن إمكانية تدمير أي معلومة قد تستخدم كدليل في أقل من ثانية وما جعل الجرائم الإلكترونية صعبة الاكتشاف والإثبات البعد الجغرافي بين الجاني والمجني عليه، استخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم ترتكب في وقت سريع ، ومن الصعوبات التي تواجه إثبات هذه الجرائم عدم اقتناع القضاة بكثير من الجرائم المستحدثة في هذا المجال، إن من الأسباب الكامنة في صعوبة اكتشاف وإثبات هذه الجرائم عدم تقديم شكاوي من قبل أصحاب الشركات التي يتم اختراقها وذلك خوفا على سمعة الشركة وعلى المستثمرين فيها[1].

ي – صعبة الاكتشاف لخصوصية الوسيلة : أي أنها هادئة وناعمة فيصعب اكتشاف حدوثها بسبب طبيعتها التقنية البحتة ، وهي معقدة ليست في متناول الجميع من حيث الاستعمال والتشغيل، فمعظم الجرائم الإلكترونية تكتشف صدفة بعد وقت طويل من اقترافها ، فالجريمة تتم في اقل من بضع ثواني و بمجرد لمسة على لوح المفاتيح ،وتحدث وتنتهي بلا صخب ولا ضجة من طرف مجرم بعيد عن مسرح الجريمة قد يتواجد في بلد آخر وفي قارة اخرى. [2]

ثانيا: خصائص متعلقة بالجاني : يتميز المجرم المعلوماتي عن غيره من المجرمين بصفات وسمات معينة جعلت منه محل العديد من الأبحاث والدراسات، واختلف الباحثون في تحديد هذه الخصائص ومع ذلك يمكن أن نستخلص من هذه الأبحاث مجموعة من السمات التي يتميز بها المجرم المعلوماتي والتي يساعد التعرف عليها في مواجهة هذا النمط الجديد من المجرمين ومن أهم هذه الصفات:

---

[1] نهلا عبد القادر المومني ، المرجع السابق ، ص 54 .

[2] محمد خليفة ، " *خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها* "، مجلة دراسات و ابحاث ، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 1 , 2009 , ص375 .

أ : سمات الجناة الخاصة: يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز لهذه الخصائص الأستاذ Parker بكلمة S.K.R.A.M .[1]

– **الذكاء:** يعتبر الذكاء من أهم صفات مرتكب الجرائم الإلكترونية ، فطريقة دخوله إلى أنظمة الحاسب الألي تتطلب منه المعرفة التقنية والقدرة على التعديل والتغيير في البرامج لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي ، فمن يستعين بجهاز الحاسوب للإستلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع من الذكاء وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة الإلكترونية في عدم استخدامه للعنف في ارتكابه للجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة (soft Sabotage) .

فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج.

–مجرم متخصص ويعود للأجرام : المجرم المعلوماتي يتميز بالعودة إلى ارتكاب الجرائم بشكل مستمر، يستخدم مهاراته في مجال التكنولوجيا لاختراق الأنظمة والتحكم في الشبكات غير المصرح بها. قد لا يكون هدفه الأساسي في الاختراق هو الإيذاء، ولكنه يتمتع بالاستمتاع بمهاراته وقدرته على الوصول إلى المعلومات المحمية. يعود الكثير من المجرمين المعلوماتيين لارتكاب جرائم أخرى في مجال التكنولوجيا، وذلك بسبب رغبتهم في سد الثغرات التي أدت إلى اكتشاف هويتهم ومحاكمتهم في المرات السابقة. هذا الدوران بين الجرائم يمكن أن يؤدي في النهاية إلى محاكمتهم مرة أخرى في المستقبل[2].

[1] يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة ويرى الأستاذ Parker أن المجرم المعلوماتي، وإن كان يتميز ببعض السمات الخاصة به إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يستوجب توقيع العقاب عليه. ويرمز الأستاذ باركر لهذه الصفات بكلمة SKRAM وهي تعني المهارة(SKILLS) ، المعرفة Knowledg) (الوسيلة (Resources)، السلطة(Autority) وأخيرا الباعث(Motives) .

[2] عادل يوسف عبد النبي الشكري ، المرجع السابق ، ص117 .

–مجرم اجتماعي وهادئ : فلا يلجا الى العنف في ارتكاب جريمته حيث يعتمد على الجهد الذهني و الفكري بدل الجهد العضلي وهو انسان مثقف و عادي يتمتع بحقوقه السياسية والاجتماعية يعيش بين افراد المجتمع ويعمل سواء في مجال المعلوماتية او في مجال آخر، وهو واجتماعي لا تظهر عليه علامات الإجرام فهو يمارس حياته الطبيعية الهادئة ويدخل في تجمعات تظم مجرمين مثله لتبادل المعلومات والمهارات وكل ما هو جديد.[1]

– المجرم المعلوماتي يبرر إرتكاب جريمته: أثبتت بعض الدراسات أنه لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقية ما يقوم به أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها بل لا يعتبر أن ما يقوم به يدخل في عداد الجرائم، خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، لذلك فإن كثيرا من العاملين في مجال المعلوماتية لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة،.وما ساعد على نماء هذا الشعور هو عدم وجود احتكاك مباشر بين الجاني والمجني عليه، فالتباعد في العلاقة الثنائية هذه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل .[2]

ب : طوائف المجرمين الإلكترونيين : إن التطور التكنولوجي والمعلوماتي أدى إلى تطور الإجرام الإلكتروني وبالتالي ظهور أصناف من المجرمين المعلوماتيين ، يختلف الباعث والدافع لارتكابهم الجرم. هذا ما ادى الى تصنيف وتجميع المجرمين الإلكترونيين في مجموعات تجمعهم ميزات مشتركة[3]:

1– القراصنة : هواة ومحترفين وهم هدفهم التسلية والمزاح وليس احداث الضرر ولا الربح المادي وينقسمون الى نوعين بينهما تعاون هما[4] :

---

[1] عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 86 .

[2] مولاي براهيم عبد الحكيم ، " *الجرائم الالكترونية* "، مجلة الحقوق والعلوم الانسانية ، العدد23 ، المجلد 2 ، 2015 ، ص 214.

[3] صغير يوسف ،" *الجريمة المرتكبة عبر الانترنت* "، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، 2013 ، ص25 .

[4] نهلا عبد القادر المومني ، المرجع السابق ، ص83 .

أ – الهاكرز[1] : هو مصطلح أطلقه طلبة أمريكيون على المتميزين والممتعون بقدرة عالية من التقنية، أغلبهم صغار سن ولهم شغف بالحاسوب وهم هواة لا يبغون مالا ولا ضررا انما اثبات قدراتهم ، وهم مقتحمي النظم هواة هم شباب أو طلبة موهوبون هدفهم إثبات مهارتهم على اكتشاف أو إظهار الأنظمة المخترقة بدافع اللهو والفضول والمزاح.

ب – الكراكرز : قراصنة محترفين هم بالغون تتجاوز اعمارهم 25 سنة فاكثر،أو مهنيون ذوي اختصاص هدفهم التخريب والحاق الضرر بالضحية، يعيشون من عائدات جرائمهم ويعاودون فعلهم.

2– الحاقدون المخربون: ليس لهم فئة عمرية محددة فهدفهم ليس المكاسب ولكن الانتقام من أصحاب العمل و الهيئات التي كانوا يعملون لديها ، فهم موظفون سابقون تم الاستغناء عنهم هدفهم احداث الضرر وليس الحصول على مكاسب مالية يستغلون معرفتهم بأنظمة الحواسيب لدى هذه المؤسسات لنشر بيانات أو استعمال البيانات المخزنة في نظامها المعلوماتي او مسحها .

3– المتجسسون: بدل الطرق التقليدية يستخدم المجرم من جهة استخباراتية ويستعمل المعلوماتية في جريمته للحصول على معلومات سرية عن دولة و افشائها لدولة أخرى وتكون عسكرية صناعية او اقتصادية ويكون غالبا أحد مستخدمي الجهاز المستهدف .

4– مخترقو الأنظمة : هم جهاز بحد ذاته يتبادلون المعلومات ويعقدون المؤتمرات لتجديد معلوماتهم ،حول مواطن الضعف في الأنظمة المعلوماتية نشاطهم ليس تخريبيا ولكن تستعملهم الأجهزة المختصة والشركات المنتجة لبرامج معالجة البيانات احيانا لفحصها واختبارها قصد ايجاد برامج او وسائل حماية من الاعتداء ، هدفهم المتعة وليس التخريب .

5– المتطرفون والإرهابيون : ينتمون فيها إلى طائفة معينة ذات أفكار وتوجه خاص بها تستعمل الانترنت لبث أفكارها وترويجها، والتطرف يكون دينيا او عرقيا أو جهويا هدفه تغيير المجتمع وفقا لما

[1] عرفت إتفاقيةالأمم المتحدة لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (63/55) المؤرخة في 12/04/2000 الهاكر (المخترق) بأنه المبرمج المتفوق جدا ولكنه يستخدم جل طاقته في الاتجاه غير شرعي لمحاولة اختراق أنظمة حاسوبية بهدف إثبات قدرته أو التباهي بها وأحيانا لأهداف إجرامية.

يعتقد وليس لتحقيق مكاسب شخصية او معنوية، اما الارهابيون فعادة يرسلون رسائل تهديد و يقومون بتدمير البيانات المخزنة في الأنظمة الحكومية لتسجيل وجهة نظرهم ويستعملون اساليب اقناع وتأثير احيانا يقع ضحيتها المختصون اللذين يدرسونها لمواجهتها.[1]

6- طائفة الربح المادي: وهؤلاء يعملون في مجال الجريمة المنظمة هدفهم الحصول على الأموال بوجه غير مشروع أو حتى الأفراد الذين يعملون لصالحهم فيرتكبون الجريمة بهدف حل مشاكلهم المادية كلما كإنو بحاجة الى ذلك.

7-طائفة صغار السن : او كما يسميهم البعض صغار نوابغ المعلوماتية وفي اصطلاح القانون يطلق عليهم الأحداث[2].

الفرع الثاني: أركان الجريمة الإلكترونية :

لكي تتم معاقبة الجاني على أفعاله لابد من توافر عناصر معينة. هذه العناصر هي الجزء الأساسي لوجود الجريمة ولا يمكن حدوثها بدونها, وتتكون العناصر من الجانب المادي للجريمة والقصد الجنائي والإرادة والنموذج القانوني للجريمة. يجب أن تكون هذه العناصر قائمة سواء كانت الجريمة تقليدية أو إلكترونية[3].

أولا : الـركن الشـرعـي للجـريمة الالكتـرونية: يقصد بالركن الشرعي للجريمة وجود نص يعتبر السلوك مخالفًا للقانون ويتم تحديد الجزاء المناسب له في وقت وقوع الفعل، أي لا يمكن ملاحقة الشخص عن فعل إرتكبه قبل صدور نص التجريم أو بعد إلغائه (إلا ما كان أصلح للمتهم "استثناء") ، ولا يمكن معاقبة سلوكات لم يصرّح المشرع بتجريمها، يجب على القضاة الإلتزام بتفسير النصوص الجزائية وعدم التوسع فيها[4].

---

[1] نهلا عبد القادر المومني , المرجع السابق ، ص ص 85-86 .

[2] فتيحة رصاع ، المرجع السابق ، ص 56 .

[3] يزيد بوحليط ، المرجع السابق ، ص90

[4] أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط18 ، 2019 ، ص64.

لابد ان تكون الجريمة قد حددت اركانها بموجب قانون مطبق وقت ارتكابها, إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين .

-مطابقة الفعل لنص التجريم .

-أن لا يخضع الفعل المرتكب لسبب من أسباب الاباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الاباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة .

خص المشرع الجزائري الجرائم التي تتعلق بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات، وهو القسم السابع المكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات". ويتضمن هذا القسم ثمانية مواد تغطي كل أنواع الاعتداءات على الأنظمة المعلوماتية[1].

كما أنه ومن أجل الحد من هذه الجريمة، أصدر قانون خاص يعمل على وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها طبقا لقانون 04/09 الصادر بتاريخ 2009/08/05، وهذا تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير مجرمة قانونا.

ثانيا: الـركن المـــادي : يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور و القانون وعناصره هي :

[1] بوخبزة عائشة ,"*الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري*" , مذكرة ماجستير في القانون الجنائي , كلية الحقوق , جامعة وهران , الجزائر , 2012-2013 , ص62 .

–السلوك الاجرامي: هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة الإلكترونية يمكن أن نجده بنوعيه السلوك الايجابي او السلبي ، دون أن ننسى التطور الكبير الحاصل في محتوى و طبيعة السلوك الإجرامي بتطور الوسائل التي وضعت بين يدي الفاعل ، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا خلقت صعوبات كثيرة .

– النتيجة الاجرامية: يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى .

– العلاقة السببية بين الفعل والنتيجة: تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجع إلى إسناد النتيجة الى الفعل و هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت غير عمدية فإن نفي رابطة سببية يؤدي إلى انتفاء المسؤولية كلية عنها ذلك أنه لاشروع في الجرائم غير العمدية .

ثالثا : الركن المعنوي: يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس متمثل في توافر الارادة الجرمية لدى الفاعل، وتوجيه هذه الارادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجرمية المترتبة على الافعال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالاثار الضارة الناشئة عنه .

يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الالي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة

أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الالي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الالي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي وفي جريمة الاحتيال الالكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص أخر من ممتلكاته على نحو غير مشروع .[1]

وسنتناول الركن المعنوي لكل جريمة بتفصيل أكبر لما نستعرض صور الجرائم الالكترونية لاحقا .

المبحث الثاني: أنواع الجرائم الالكترونية و صورها :

بما أنه هناك إختلاف في تسمية و تعريف الجريمة الإلكترونية بين التشريعات المختلفة ومختلف المدارس الفقهية ، وكما رأينا سابقا في خصائص الجريمة و المجرم الإلكتروني ، فقد كان لذلك تأثيرا على تقسيم الجرائم الإلكترونية من حيث أنواعها أو تصنيفاتها ، وقد سعى المشرع الجزائري لتسمية مختلف الجرائم الالكترونية ، وسنتطرق في مبحثنا إلى أنواع الجريمة الإلكترونية و بعض الصور المذكورة في التشريع الجزائري .

المطلب الأول : أنواع الجرائم الالكترونية في التشريع الجزائري :

إن الجريمة الإلكترونية لديها تصنيفات مختلفة بسبب الاختلاف في التسميات والمعايير. فمنهم من يصنفها حسب أسلوب ارتكاب الجريمة، وآخرون يستندون إلى دوافع ارتكابها، وبعضهم الآخر يعتمد على محل وحق المعتدى عليه [2], و من الملاحظ أن هذه التقسيمات أو بعضها لم تراع بعض أو كل خصائص هذه الجرائم و موضوعها و الحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم

[1] يزيد بوحليط ، المرجع السابق ، ص 94 .

[2] فتيحة رصاع ، المرجع السابق ، ص 69 .

متناسية معايير أخرى . و يرى البعض من الفقهاء أنه يجب مراعاة في كل محاولة لتقسيم الجرائم الإلكترونية اعتباران هما :

*التطور المستمر الذي يطرأ على الجريمة الإلكترونية بصفة عامة .

*معيار الجريمة الإلكترونية أي ما يدخل في إطار هذه الجرائم و ما يخرج منه [1].

وعليه فقد إرتأينا الأخد برأي تقسيم الجرائم الإلكترونية إلى طائفتين رئيسيتين بالاعتماد على محل الجرائم الإلكترونية التي تنصب على معطيات الحاسوب و تطال الحق في المعلومات بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ يستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسب الآلي . وهذا ماذهب اليه المشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها ولم يحددها ، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات .

الفرع الأول: الجريمة الإلكترونية 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 الآخرى، الجريمة الواقعة على الأسرار .

أولا: الجريمة الإلكترونية الواقعة على الأشخاص:

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

[1] نائلة عادل محمد فؤاد قورة ، " *جرائم الحاسب الآلي الاقتصادية* " ، ط1 ، سوريا ، منشورات الحلبي الحقوقية ، 2005م ، ص 256 .

أ- الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية :

يكون النظام المعلوماتي وسيلة للإعتداء 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 الإختراع، التي تحتوي على حق معنوي وآخر مالي للمخترع[1] . وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 05/03 الصادر في 2003/07/19 , المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو عام 2003 , يتعلق ببراءات الاختراع .

ب- الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة :

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الإعتداء 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[2].

ثانيا: الجريمة الإلكترونية الواقعة على النظم المعلوماتية الآخرى:

تتحقق هذه الجريمة بالولوج المادي في مركز المعالجة المعلوماتية ، استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها داخل نظم معلوماتية الآخرى، بالإضافة إلى إساءة استخدام

[1] أسامة حسين محي الدين عبد العال ، "*جرائم الحاسب الألي دراسة تحليلية* " ، مجلة العلوم القانونية و الاقتصادية ، العدد 2 ، الجزء 2 ، 2013 ، ص 1376 .

[2] سفيان سوير ، "*جرائم المعلوماتية* " ، رسالة ماجستير ، كلية الحقوق و العلوم السياسية ، جامعة أبو بكر بلقايد، تلمسان ،2011/2010 ، ص35 .

البطاقة الإئتمانية [1]. في الحالة الأولى يستطيع الجاني الإستيلاء على المعلومات المخزنة داخل النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة، أو استخدام شاشة النظام، أو الإطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الإئتمانية، وذلك عن طريق عدم احترام العميل الحائز على البطاقة الإئتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة إئتمانية إنتهت مدة صلاحيتها أو تم إلغاؤها، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة إئتمانية للحصول على السلع والخدمات .[2]

ثالثا: الجريمة الإلكترونية الواقعة على الأسرار:

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة[3]. ويتخذ هذا النوع من الجرائم صورتين ، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة ، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والإقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات [4]، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية [5]. وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة61 إلى المادة 96 مكرر من قانون العقوبات، بالإضافة إلى المادة394 مكرر 03 التي تنص على: " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد".

---

[1] خالد ممدوح ابراهيم ، المرجع السابق ، ص63

[2] سفيان سوير ، المرجع السابق ، ص37 .

[3] أمال قارة ،" *الجريمة المعلوماتية*" ، رسالة ماجستير ،كلية الحقوق بن عكنون ، جامعة الجزائر ، 2002/2001 ، ص43 .

[4] صغير يوسف ، المرجع السابق ، ص 54 .

[5] أسامة حسين محي الدين عبد العال ، المرجع السابق ، ص ص 1376 – 1377 .

الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي.

جرم القانون رقم 04-15 الصادر في 10 نوفمبر 2004 المتضمن قانون العقوبات كل أنواع الإعتداءات 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 394 مكرر إلى 394 مكرر7 ، وتأخذ صور الإعتداء صورتين وهما :الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش.[1]

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 الدخول أو البقاء تخريب 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[2].

ثانيا: جريمة المساس بمنظومة معلوماتية.

يقصد بالاعتداء هنا ذلك الاعتداء الذي يهدف إلى الإضرار بمعلومات الكومبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها، تكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم، يتحقق الاعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة، ويتخذ أحد الأشكال التالية :

[1] عطاءالله فشار ، " *مواجهة الجريمة المعلوماتية في التشريع الجزائري* " ، جامع الكتب الإسلامية، المجلد 1 ، ص29 .

[2] حمزة بن عقون،" *السلوك الإجرامي للمجرم المعلوماتي*" ، شهادة ماجستير ، جامعة الحاج لخضر ، باتنة ، 2012/2011 ، ص 182 .

أ-الاعتداء على المعطيات الداخلية للنظام:

جرم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية من خلال المادة 394 مكرر 1 من قانون العقوبات، وحدد في ذات المادة صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر ولم يدع أي مجال للاجتهاد فيها، مما يدل على أن أي اعتداء لا يحمل إحدى هذه الصور : الإدخال، المحو،التعديل فهو مستبعد ولا يخضع لأحكام المادة 394 مكرر .1[1]

ب- الاعتداء على المعطيات الخارجية للنظام :

يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقيق نتيجة معينة تتمثل في المعالجة الآلية للمعطيات[2]، وقد نص عليها المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات ، حيث يتبين لنا من نص هذه المادة أنها جاءت عامة ومطلقة، فهي تقرر الحماية الجنائية لكل من المعطيات الداخلية والخارجية للنظام معا.

ج- الاعتداء على سير نظام المعالجة الآلية:

تجاهل المشرع الجزائري وضع نص واضح لتجريم الاعتداء على نظام المعالجة الآلية للبيانات، ولكن يمكن استخلاص هذا الأمر من خلال النصوص الأخرى التي وضعها فيما يتعلق بتجريم الاعتداءات على نظم المعالجة أو بيانات هذه الأنظمة سواء كانت داخلية أو خارجية. من الممكن القيام بأنشطة مختلفة تؤثر على نظام المعالجة مثل تخريبه بموجب المادة 394 المكررة أو الاعتداء على بيانات النظام الداخلية باستخدام برامج الفيروسات أو القنابل الإلكترونية وذلك يؤدي إلى تأثير سلبي على سير النظام الإلكتروني[3] .

تجدر الإشارة إلى أن المشرع الجزائري جرم كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة وجعل العقوبة لهما تساوي العقوبات المقررة للجريمة ذاتها، وقد تشمل هذه

[1] أمال قارة ، المرجع السابق ، ص120 .

[2] عطا الله فشار ، المرجع السابق ، ص 36 .

[3] أمال قارة ، المرجع السابق ، ص 114 .

العقوبات المذكورة في القسم السابع مكرر من قانون العقوبات عقوبات أصلية تتمثل في الحبس والغرامة، وعقوبات تكميلية هي مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع وأماكن الاستغلال إذا ارتكبت الجريمة بعلم مالكها، كما أن المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي ارتكب إحدى الجرائم الإلكترونية إلى 05 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي مع إقراره المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين و / أو شركاء في نفس الجريمة التي أرتكبها الشخص المعنوي .

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 إحداها 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[1].

المطلب الثاني : صور الجرائم الالكترونية :

يصنف الفقهاء جرائم الكمبيوتر ضمن فئات متعددة، تختلف حسب الاساس والمعيار المتبع، فبعضهم يقسمها إلى جرائم ترتكب على نظام الحاسوب وأخرى ترتكب بواسطته و بعضهم يصنفها ضمن فئات بالاستناد إلى الاسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة ، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدي عليه ، فتوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الاموال بواسطة الحاسوب وتلك التي تقع على الحياة

[1] سفيان سوير , المرجع السابق , ص93 .

الخاصة، والملاحظ أن هذه التقسيمات لم تراعي خصائص هذه الجريمة وموضوعها، والحق المعتدي عليه لدى وضعها لاساس أو معيار التقسيم، وعليه ونظرا لطبيعة هذا النوع المستحدث من الجرائم تعددت تصنيفاتها، وسنتطرق لأربع تصنيفات لهذه الجرائم .[1]

الفرع الأول : الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات :

إن النهج التجريمي من قبل المشرع الجزائري المتبع في الجرائم الماسة بالمعالجة الالية للمعطيات كان واضحا وشاملا ، غير أن ما يطرح الاشكال بهذا الخصوص هو غياب تحديد معاني الركن المادي والمعنوي بشكل دقيق ، مما قد يرتب أثارا إيجابية بالنسبة للمجرمين الذين تسمح لهم الثغرات القانونية بالإفلات من العقاب ، وعلى كل حال فإن جرائم التعدي على النظم المعلوماتية يمكن حصرها في الصور التالية

أ: جريمة التزوير المعلوماتي : نظر للإنتشار الذي يشهده العالم لدور الحاسب الآلي الى أن أصبح يحل محل المحررات والوثائق، والصكوك، في أغلب مجالات نظم المعالجة الالية للمعلومات وتزايد مع ذلك عدد الإعتداءات التي تمس بهذه المعلومات المخزنة داخل الحاسب والتي يكون فيها الإعتداء على حقوق وأموال وحياة الأفراد الخاصة ، وهذا ما وجب فرض حماية له لضمان سلامة وأمن هذا الفعل الذي يعد بمثابة تزوير .

– تعريف جريمة التزوير : التزوير المعلوماتي هو أي تغيير للحقيقة يرد على مخرجات الحاسب الألي سواء تمثلت في مخرجات ورقية مكتوبة كذلك التي تتم عن طريق الطابعة. ويعرف بانه تغيير الحقيقة في محرر باحدى الطرق التي حددها القانونتغييرا من شأنه أن يرتب ضررا للغير , و بنية استعمال هذا المحرر فيما اعده له . [2]

– أركان جريمة التزوير الالكتروني : لا تختلف الجريمة الإلكترونية عن التقليدية كثيرا من حيث الأركان المكونة لهذه الجريمة والتي يمكن تفصيلها فيمايلي :

[1] يزيد بوحليط ، المرجع السابق ، ص61 .

[2] عبد الفتاح بيومي حجازي ، المرجع السابق ، ص197 .

الركن المادي: لا يختلف الركن المادي في جريمة التزوير المعلوماتي عن التزوير في صوره التقليدية ،إلا في مجال ماهو مستجد في إستخدامات الحاسب الآلي ، التي يلجأ لها المجرم في تزوير الوثائق المعلوماتية، وفقا للنظم أو البطاقات المعلوماتية أو دعامات ممغنطة . ولقيام الركن المادي في جريمة التزوير المعلوماتي لابد أن يتكون هذا الركن من عناصر مهمة وأساسية تتمثل في :

1/ المستند المعالج آليا : المستند أوالمحرر في المجال المعلوماتي هو كل قرص أو شريط ...الخ صالح للتسجيل والتحميل وأن يكون محلا للمعلومات ، والمستند المعالج آليا هو كل دعامة مادية مهيأة لإستقبال المعلومات ،ولا يصلح أن يكون محل لجريمة التزوير المعلوماتي المستندات الغير معالجة آلياً حتى ولو كانت معلوماتية ، فتخرج منها الأوراق المعدة لتسطير المعلومات والأقراص الممغنطة التي لم يسجل عليها أي شيء والملاحظات التي تكون في شكل كتب . يعني المعلومات التي مازالت في مرحلة الإعداد فقط.[1]

2/فعل تغيير الحقيقة : وهو التغيير والتحريف لما يرد في محتويات المستندات الاصلية والحقيقية المعالجة آليا ، لأنه من غير المحتمل أن يكون تغيير الحقيقة او التزوير المعنوي ؛ بالمعنى الأصح أن تغيير الحقيقة في جريمة تزوير البيانات المعالجة الآلية ، لايتم الا أذا كانت طرق تزوير مادية فقط دون المعنوية بشرط وجود المستند الأصلي المعالج آلياً ،وموجود سابقا وحقيقي، وفعل التزوير قد يقع داخل نظام المعالجة الآلي أو خارجه أو قبل أو بعد الدخول .[2]

3/ الضرر : لأنه في حال عدم إلحاق أضرار بالغير لا عقاب عن جريمة التزوير ، ولا تقوم المسؤولية بتحقيق الضرر فحسب حتى بإحتمال تحققه وقد يكون فعل التزوير قد ألحق بالمجني عليه ضرراً ،واقع وحقيقي أو مفترض ومحتمل الوقوع , والمشرع الجزائري قد تطرق في قانون العقوبات وذكر على سبيل الحصر صور التزوير، وهذا ما يتضح في المواد 214 و 215 التي نصت كل منهما على

[1] ياسين بوعروة ، " *جريمة التزوير المعلوماتي* " ، مذكرة ماستر ،كلية الحقوق و العلوم السياسية ، جامعة العربي بن امهيدي ، ام البواقي ، 2013-2014 ، ص9 .

[2] عبد الفتاح بيومي حجازي ، المرجع السابق ، ص201 .

مايلي المادة 214 ق.ع حددت لنا أربع طرق للتزوير المادي فنصت على " يعاقب بالسجن المؤبد كل قاضي أو موظف أوقائم بوظيفة عمومية إرتكب تزوير في المحررات العمومية أو الرسمية أثناء تأدية وظيفته .

1- إما بوضع توقيعات مزورة

2- وإما بإحداث تغيير في المحررات أوالخطوط أو التوقيعات

3- وإما بإنتحال شخصية الغير أو الحلول محلها

4- وإما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها"

أما بالنسبة لطرق التزوير المعنوية فنصت عليها المادة 215 من ق.ع "يعاقب بالسجن المؤبد كل قاضي أو موظف عمومي أو قائم بوظيفة عمومية قام أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش وذلك إما بكتابة إتفاقات خلاف التي دونت أو أُمليت من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذباً بأن وقائع قد أُعترف بها أو وقعت في حظوره أو بإسقاطه أو بتغييره عمداً الإقرارات التي تلقاها[1]."

الركن المعنوي لجريمة التزوير المعلوماتي : لقيام جريمة التزوير لابد أن يشترك فيها القصد الجنائي بنوعيه العام والخاص ، فالقصد الجنائي العام الذي يتوجب فيه علم الجاني بأركان الجريمة ، وإتجاه إراداته إلى القيام بالتزوير وإلحاق ضرر ،والقصد الخاص يتمثل في نية الجاني في إستخدام المحرر المزور في فعله الذي بفضله قام بالتزوير ،لذا إجتمع رأي أغلبية الفقهاء والقضاة على أن التزوير هو تعمد تغيير الحقيقة في محرر تغييراً من شأنه أن يسبب ضرراً ونية إستعمال المحرر فيما غيّرت من أجله الحقيقة , فالمشرع الجزائري لم يساير الإتجاه الحديث التي وسّع في مفهوم المحرر ليشمل كل نوع تزوير حديث ،حيث يرجع الى نصوصه التقليدية التي يستعمل فيها مصطلح محرر لكن هذا المصطلح لم يستوعب أفعال التزوير

[1] ياسين بوعروة ، المرجع السابق ، ص12 .

المعلوماتي بالرغم من أن الجزائر كانت قد صادقت على إتفاقية إ ع م ج ت م التي كانت المادة 10 منها تنص على التزوير المعلوماتي[1].

ب:جريمة الإختراق : تعتبر هذه الجريمة الأكثر شيوعا في مجال الإجرام المعلوماتي ، والسلوك الإجرامي المحبب والمفضل لمجرمي المعلوماتية .

– تعريف جريمة الإختراق الإلكتروني : يُعرّف الإختراق في القانون العربي النموذجي الموحد المتعلق بجرائم إستخدام تقنية المعلومات بأنه "الدخول الغير مصرّح به أو غير مشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية". ، ويعرف أنه عملية يتسرب بها البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت وتتم هذه العملية في أي مكان بغض النظر عن وجود شخص في المكان أو البلد الذي يتم فيه الإختراق ، يعني أنه البعد الجغرافي لادخل له في الإختراقات المعلوماتية ، لأن الهدف من الإختراق هو الوصول بطريقة غير مشروعة إلى المبتغى ، والمخترق يدخل الأجهزة دون دخل أو علم صاحبها، مع عدم مبالاته بالأثار السلبية التي يحدثها للأجهزة أو نفسية الأشخاص . وتعرف بشكل عام بأنها : القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريقة الغش) ، عن طريق ثغرات في نظام الحماية الخاص بالهدف ، وهي سمة سيئة يتسم بها المخترق ، لقدرته على دخول أنظمة الاخرين عنوة ودون رغبة منهم ودون علمهم بغض النظر عن الاضرار التي تحدثها ، وتعد هذه الانشطة الجرمية الاكثر انتشارا[2].

– أنواع الإختراق : من أهم الأساليب المرتكبة لقيام جريمة الإختراق وهي :

1–الإختراق بإستخدام البرامج (الفاحص): والفاحص هو برنامج تطبيقي يستعمل للأغراض الكشف الآلي عن مواطن الضعف في المعيقات المحلية والنائية .

---

[1] تنص المادة العاشرة من إ.ع.م.ج.ت.م على : "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة."

[2] عزيزة رباحي ،" *الأسرار المعلوماتية ،وحمايتها الجزائية*" ، أطروحة دكتوراه ،كلية الحقوق والعلوم السياسية ،جامعة أبوبكر بلقايد ،تلمسان ،الجزائر ، 2018/2017 ، ص 112.

2- الشمّام Sniffer: يعرّف الشمام على أنه جزء من عتاد الحاسوب أو برنامجه التي تستسرق السمع وتتجسس على جميع أنواع المرور المعلوماتي ويتألف الشمام من جزئين أحده من عتاد الحاسوب والآخر من برامجه .

3-المسح والنسخ : يعرف على أنه أسلوب تغيير التركيب وتبديل المعلومات ويستخدم تحديداً بشأن إحتمالات كلمة السر أو رقم هاتف الموزع ، وأبسط نمط فيه عندما تستخدم قائمة الإحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى أحدها وإستخدامه موزع للإتصال بالإنترنت .[1]

- أركان جريمة الإختراق الإلكتروني :

الركن الشرعي لجريمة الإختراق الإلكتروني : تحمل جريمة الإختراق عدة تسميات كالقرصنة الدخول غير مصرح به الدخول عن طريق الغش ، الدخول دون حق .. ويظهر الركن الشرعي لهذه الجريمة في التشريع الجزائري في المادة 394 من ق ع ج .[2]

الركن المادي لجريمة الإختراق : الركن المادي لجريمة الدخول والبقاء غير مصرح به في نظام المعالجة الآلية للمعطيات يتطلب نشاط إيجابي , بالنسبة للتشريع الجزائري لم يتطرق ولم ينص على وجود شرط مسبق لقيام هذه الجريمة، والعنصر المفترض في هذه الجريمة يتمثل في النظام الأمني ؛ وحسب المادة 394 من قانون العقوبات الجزائري التي جاءت على عموميتها ولم تحدد طريق للدخول أو البقاء عن طريق الغش ،في جزء او كل نظام معالجة الآلية للمعطيات ، وقد أشارت المذكرة التفسيرية لإتفاقية بودابيست إلى أن الولوج الغير قانوني ، يضم الإختراق الذي يحدث للنظام بأكمله أوجزءه ، والسلوك الإجرامي هنا يرتبط بالنتيجة الإجرامية التي تظهر في صورة أثر مادي ضار ، وهذا مايطلق عليه بالجرائم المادية

[1] عزيزة رباحي ، المرجع السابق ، ص 115

[2] يزيد بوحليط ، المرجع السابق ، ص ص 178-179.

ويختلف في هذا الحال الركن المادي إذا كانت الجريمة بسيطة أو مشددة ، فإذا كانت بسيطة فالمشرع لا يشترط تحقيق نتيجة ،وإذا كانت مشددة فيشترط توافر الحذف أو التغيير .[1]

الركن المعنوي لجريمة الإختراق : بالنسبة لهذه الجريمة تتكون من القصد الجنائي العام والخاص ؛ القصد الجنائي العام الذي يتمثل في العلم والإرادة يجب أن يعلم الجاني كل الوقائع التي تدخل في تكوين الجريمة وأول مايجب العلم به هو علمه بموضوع الحق المعتدي عليه ، ويجب أن يتوفر العلم للجاني أن فعله ينصب على نظام معلوماتي وعلى المعلومات ، ولابد أيضا أن يعلم الجاني أن دخوله هذا غير مشروع وغير مصلح به ، وإذا كان إعتقاده أن الموقع متاح للجميع فالقصد ينتفي بالإضافة إلى الدخول بالصدفة والخطأ، ويجب العلم بالإرادة بإعتبار الإرادة أساس العنصر النفسي للجاني والإرادة هنا مقتصرة على السلوك الإجرامي فقط دون النتيجة .[2]

بالرجوع إلى المشرع الجزائري نجده أنه لم يكتف بتجريم فعل الدخول أو البقاء غير مشروع في نظام معالجة الآلية للمعطيات ،بل إعتبر أن المحاولة فقط جريمة ، وهذا حسب المادة 394 مكرر ق ع ج"... أو يحاول ذلك ..." ." وهذا تأكيد على الخطورة الناجمة عن هذه الأفعال .[3]

الفرع الثاني:جرائم الاعتداء على الحياة الخاصة للاشخاص .

إن تسخير البيئة المعلوماتية لارتكاب مختلف صور الاعتداء على نظم المعالجة الآلية للمعطيات وكذا تلك الجرائم الماسة بالأموال، سمح كذلك للمجرم بتحقيق أغلب صور الاعتداء على الأشخاص سواء نجم عنه أذى معنوي أو ضرر مادي، وتعددت صور الجرائم المعلوماتية المتعلقة بالأشخاص[4].

---

[1] سفيان حديدان ، " *الدخول أو البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات* "،مجلة الاستاذ الباحث للدراسات القانونية والسياسية ،جامعة 8 ماي 1945 ،قالمة،الجزائر،العدد الثامن ، المجلد الثاني ، ديسمبر2017 ، ص306 .

[2] خالد سليمان عبد هللا الحمادي ،" *جريمة الدخول غير مشروع إلى النظام المعلوماتي في القانون القطري-دراسة مقارنة* – " ، رسالة ماجستير، كلية الحقوق ،جامعة قطر ، قطر ،جانفي 2019 ، صص 81-84 .

[3] يزيد بوحليط ، المرجع السابق ، ص 187 .

[4] ابتسام مناع ، " *جريمة الاعتداء الالكتروني على الحياة الخاصة في التشريع الجزائري* " ، مجلة الشريعة والاقتصاد ، الاصدار الاول ، المجلد الثامن ، 2019 ، ص 320 .

أ–جريمة القذف: هناك بعض التشريعات العربية تطلق على القذف تسمية الذم و القدح و التحقير، الذم بمعنى إسناد مادة معينة إلى الشخص و لو في معرض الشك و الاستفهام، أما القدح فنقصد به الاعتداء على كرامة الغير أو شرفه أو اعتباره و لو في معرض الشك و الاستفهام من دون بيان مادة معينة، أما بالنسبة للتحقير فهو كل تحقير أو سباب يوجه إلى المعتدى عليه وجها لوجه بالكلام و الحركات أو الكتابة أو معاملة غليظة[1].

ويمكن تعريف القذف على أنه إسناد واقعة محددة علناً وعمداً تستوجب عقاب من تُنسب إليه، أي بنسبة أمر شائن للمقذوف كإزدرائه واحتقاره بشكل علني ويتوجب العقاب عليه[2] , واجتمع الفقه على تعريف القذف بأنه إسناد واقعة محددة علناً ، وعمداً، أي بنسبه أمر شائن بشكل علني يستوجب في حالة صدق ذلك معاقبته بالعقوبات المقررة قانوناً وإزدراء الناس واحتقارهم له.[3] و جاء في قرار للمحكمة العليا ما يلي: " يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف و اعتبار الاشخاص او اسنادها اليهم ويعاقب على نشر هذا الادعاء وذلك الاسناد حتى و لو تم ذلك على وجه التشكيك او اذا قصد به شخص دون ذكر الاسم و لكن كان من الممكن تحديده من عبارات الكتابة"[4] .

– الركن الشرعي: عرفت المادة 296 من قانون العقوبات الجزائري القذف على أنه "يعد القذف كل إدعاء بواقعة من شأنها المساس بشرف أو اعتبار الأشخاص والهيئات المدعى عليها أو إسنادها إليهم ويعاقب على نشر الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الإسم ولكن كان من الممكن

[1] عادل عزام سقف الحيط ، " *جرائم الذم و القدح و التحقير المرتكبة عبر الوسائط الالكترونية* " ، دار الثقافة للنشر و التوزيع ، ط2 ، 2015 ، ص84 .

[2] يزيد بوحليط ، المرجع السابق ، ص 167-168 .

[3] عادل عزام سقف الحيط ، المرجع السابق ، ص67 .

[4] المحكمة العليا ، ملف رقم 188086 , قرار بتاريخ 1999 .

تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة " .

ما يستنتج أن المشرع الجزائري أخذ بنفس ما أخذ به المشرع المصري حيث نص على جريمة القذف في قانون العقوبات ، هذا عكس المشرع الفرنسي الذي أوردها ضمن قانون الإعلام ...[1]

– **الركن المادي**: يتكون الركن المادي لجريمة القذف من العناصر الأساسية وهي الادعاء بواقعة شائنة أو إسنادها للغير، و النتيجة، و العلانية :

* **السلوك الاجرامي**: **الإدعاء والإسناد (ALLEGATION et IMPUTATION)**: معناه أن ينصب الإدعاء على وقائع تمس الشرف الشخص أو إعتباره ولقيام هذه الواقعة لا يكفي كونها شائنة بل ويجب أن تكون محددة ومعينة حيث يستطيع إقامة الدليل عليها ويجب أن تستوجب عقاب من أُسندت إليه أو إحتقاره ,[2] و يعرف بأنه:"التصريح بتلك الواقعة على ذمة الغير، أو الإدراج الناتج تحت ظل الشك لتلك الواقعة و التي يدعي القاذف بأنه عرفها شخصيا".والإسناد يعني نسبة الأمر إلى شخص المقذوف على سبيل التأكيد، سواء كانت الوقائع المدعى بها صحيحة او كاذبة تمهيدا لمساءلته عن ما أسند إليه[3].

* **النتيجة (المساس بالشرف و الاعتبار)** : و النتيجة أن تكون الواقعة المسندة فيها مساس بالحق في الشرف والاعتبار , فيكون الفعل الذي اسند للمجني عليه يحط من كرامته في محيطه المتمثل

[1] يزيد بوحليط ، المرجع السابق ، ص 118 .

[2] عبد السلام عليلي ، " *جريمة القذف عبر مواقع التواصل الاجتماعي* " ، مجلة الدراسات القانونية و الاقتصادية ، العدد 2 ، المجلد 5 ، 2022 ، ص 578 .

[3] زروقي محمد ،" *الحماية القانونية للحق في الشرف و الاعتبار*" ، مذكرة ماجستير ،كلية الحقوق ، جامعة الجيلالي ليابس ، سيدي بلعباس ، 2014- 2015، ص 51.

في الاهل و الوطن حتى وان كان ذلك لا يعتبر كذلك في مجتمع أخر فالعرف السائد لدى مجتمع المجني عليه يحدده قاضي الموضوع الذي يتولى تحديد ما إذا كانت تلك الواقعة تستوجب العقاب أم لا .[1]

* : **العلانية** : تعرف العلانية على أنّها أن يصل إلى علم الجمهور أمور أو وقائع معينة إتصال حقيقي أو حكمي " , وفي نطاق جريمة القذف فالعلانية تتمثل في إتصال عبارات القذف إلى عالم الجمهور سواء كان هذا الإتصال حقيقيا أو حكمياً وهذا الجمهور لا تربطه أي صلة أو علاقة بالمجرم سواء علاقة مباشرة كالقرابة أو الصداقة فخطورة جريمة القذف تكمن في إعلان عباراته المشينة للجمهور الغير معين لأن الخطر والضرر الذي ينشأ من الجريمة ينشأ من العلانية التي تلحق بعباراته .[2]

ـ **الركن المعنوي**: تعتبر جريمة القذف (الذم) من الجرائم العمدية التي يتطلب لقيامها أن يتخذ الركن المعنوي فيها صورة القصد الجنائي المتمثل في القصد الجنائي العام فقط دون إرتباطها بالقصد الجنائي الخاص[3] فحسب القواعد العامة ،فالقصد الجنائي العام يتمثل في العلم والإرادة وهو أن يعلم الجاني بعناصر الركن المادي للجريمة مع إتجاه إرادته الى إحداث السلوك وأن يعلم الجاني مايرتكبه من فعل مستند إلى المجني عليه ينقص من شرفه وكرامته كما يتعين أن ينصرف علم الجاني إلى علانية عبارات الذم، فإذا إتخذت العلانية صورة القول والصياح يجب أن يعلم الجاني بأنه أجهر بأقواله في أماكن عامة أو قد ينقل بطريق غير مباشر لاسلكي إلى أشخاص آخرين ، وإذا كانت العلانية بالكتابة فيجب أن يعلم بما قام بتدوينه المتضمن للذم والقذف قد يعرض على العامة فنستنتج أن قيامه بفعل الذم كان بارادته الحرة الغير مكرهة ، أوقائمة تحت التهديد ويجب أن لا تكون وليدة إنفعال أو ثورة نفسية[4].

ب جريمة السب: يعرف على انه كل " إلصاق لعيب أو تعبير يحط من قدر الشخص عند نفسه أو يخدش سمعته لدى غيره", ويقصد به كل تعبير به التجريح والاحتقار واللفظ القبيح إلى شخص ما

[1] زروقي محمد ، المرجع السابق ، ص 51.

[2] يزيد بوحليط ، المرجع السابق ، ص 119 .

[3] زروقي محمد ، المرجع السابق ، ص 73.

[4] عبد السلام عليلي ، المرجع السابق ، ص580 .

وأن لا ينطوي هذا التعبير على واقعة محددة", وعليه فالسب هو ذكر العيوب التي تمس بشرف واعتبار الأشخاص بطريقة عمدية، دون أن يتضمن ذلك إسناد واقعة معينة[1]

– **الركن الشرعي** : بالرجوع إلى مانص عليه المشرع الجزائري في المادة 297 من قانون العقوبات الجزائري أنه "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقير أو قدح لا ينطوي إسناد أية واقعة " وقد اقتبس المشرع الجزائري من نص المادة 2/29 من قانون حرية الصحافة الفرنسي .[2]

– **الركن المادي**: يتكون الركن المادي لهذه الجريمة على ثلاث عناصر أساسية وهي كالآتي:

1– خدش الشرف والإعتبار : وهو التعبير الذي يحط من قدر المجني عليه ويمس بسمعته ،فهو يمس بالشرف والإعتبار دون تحقيق واقعة معينة ويكفي لقيامه أن تكون هذه العبارات تحمل عنف وكلاما بذئ وسيئ وماجن ، كالسارق واللصّ والسكير والرّاشي ... وعلى المحكمة أنّ تذكر تلك الألفاظ وإلا كان الحكم قاصرا [3].

2– توجيه السبّ إلى شخص معين أو أشخاص معينين : يجب تعيين الأشخاص الموجه إليهم السب أو من الممكن تعيينهم ، فالسبّ العلني يجب أن تمس عباراته بمذهب أو فكرة معينة ، ولا يشترط لوقوع السب حضور المجني عليه أثناء الواقعة[4].

3 العلانية : تشترك كلاً من جريمتي السب والقذف في عنصر العلانية التي تتحقق بالكتابة ونشر الصور والوسائل السمعية والبصرية أو أي وسيلة إلكترونية ،إذا كانت تقنيات الانترنت تسهل عملية نقل الصوت والصورة من مستخدم إلى آخر في أي مكان في العالم ، فمن الممكن تصور إنتشارها

[1] داود فايز ، مهدي رفيق ، "*جريمة السب في القانون الجزائري*" ، مذكرة ماستر ، جامعة محمد بوضياف ، المسيلة ، 2019–2020 ، ص ص 7–8 .

[2] زروقي محمد ، المرجع السابق ، ص 103.

[3] داود فايز ، مهدي رفيق ، المرجع السابق ، ص29 .

[4] المرجع نفسه ، ص31 .

وعلانيتها في نطاق الإنترنت[1] ، فحسب المادة 297 من قانون العقوبات الجزائري فهي مذكورة على أساس أنّها ليست عنصر وركن أساسي في جريمة السب لأن جريمة السبّ لا تنتفي بإنتفاء العلانية وإنما تتحول من جنحة إلى مخالفة حسب نص المادة 2/463 من قانون العقوبات الجزائري التي تنص "يعاقب بغرامة من 30 إلى 100دج ويجوز أن يعاقب أيضا بالحبس لمدة 10 أيام على الأكثر كل من ألقى بغير احتياط أقذار على أحد الأشخاص ألفاظ سباب علانية دون أن يكون قد إستفزه ."

– **الركن المعنوي** : يجب أن يتوفر على القصد الجنائي العام بأنّ تنصرف فيه إرادة الجاني إلى إذاعة الأمور الماسة بالشرف و الإعتبار مع وجوب توفر علمه بها وبمعناها ،لأنه من الأمر المفترض أن يعلم الجاني بعبارات السب الشائنة ولابد أيضا أن يتوافر له قصد الإذاعة ، يعني أنّ إرادته توجهت إلى غاية الشّر عن ما عبر عليه من ألفاظ تخدش شرف المجني[2].

الفرع الثالث : جرائم الاعتداء على بالأموال:

أ : جريمة غسيل الأموال :

– **تعريفها** : ويقصد بغسيل الأموال أو تبييض الأموال وهي العبارة التي استعملها المشرع الجزائري في قانون العقوبات "إخفاء المصدر الاجرامي للممتلكات والاموال، لاسيما ما يسمى بالمال القذر وتمر عملية التبييض تقنيا بثلاث مراحل، توظيف المال، التمويه والادماج [3], و بإستقراء قوانين التشريع الجزائري نجد أن المشرع الجزائري لم ينص على إعطاء تعريف لجريمة تبييض الأموال ، بل حدد الأفعال التي يمكن إعتبارها كجريمة لغسيل الأموال عند ارتكابها وأظهر أيضا الآليات القانونية لمكافحتها فنص في العديد من القوانين على ذلك .

[1] داود فايز ، مهدي رفيق ، المرجع السابق , ص ص31-32 .

[2] زروقي محمد , المرجع السابق , ص 107.

[3] زهيرة كيسي ، أحمد حمي ، " *صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014* " ، مجلة العلوم القانونية و السياسية ، العدد 10، المجلد 10 ، 2019 ، ص 788 .

– **أركانها** : لقيام جريمة تبييض الاموال لابد من تحقق ثلاث أركان الشرعي , المادي و المعنوي بالاضافة الى الركن المفترض والمتمثل في وجود جريمة سابقة، أي أن تكون الاموال محل الغسيل "عائدات إجرامية".[1]

الركن الشرعي : من خلال استقراء المادة 389 مكرر من قانون رقم 15/04 نصت على المراحل الأساسية التي تمر بها جريمة تبييض الأموال من تحويل ونقل وإخفاء وتمويه أو مساعدة أي شخص متورط في نفس الجريمة أو اكتساب الممتلكات أو حيازتها أو استخدامها[2].

الركن المادي: يظهر السلوك الإجرامي في الركن المادي لجريمة تبييض الأموال من خلال أهم صور هذا النشاط هو الاعتماد والإستعانة بالبيئة الالكترونية في غسيل الأموال ويظهر ذلك وفقا لمراحل وهي:

1/ مرحلة الإيداع : وهي المرحلة التي تأتي بعد الحصول على الأموال القذرة وتوضع في مكان معين لفترة من الزمن قصد نسيانها وفي هذه المرحلة يستغل الجاني لفتح حسابات بإسمه أو إسم مستعار أو بشراء أسهم لمؤسسات مالية أو تجارية.

2/ مرحلة التكديس: التي يخرج فيها المال من مكانه ويدخل في فترة الغسيل كأن يوضع في مشروعات عقارية أو شركات، وهذه المرحلة هدفها تضليل الجهات الرقابية بأسلوب التمويه والتعتيم، ثم تأتي المرحلة الأخيرة التي يدمج فيها المال القذر مع المال المشروع .

الركن المعنوي : إن هذه الجريمة تقوم على القصد الجنائي العام القائم على العلم والإرادة ،أي أن يعلم الجاني بالسلوك الجرمي المعاقب عليه قانوناً ، وعلمه مبني على قاعدة لا عذر بجهل القانون، بالإضافة إلى إتجاه إرادته لإرتكاب الفعل مع العلم بأنه مجرم وجريمة تبييض الأموال تتم بأساليب إلكترونية وتكون هذه الأساليب عن طريق وسائل الكترونية متمثلة في بطاقات الإئتمان والتحويل الإلكتروني

[1] زهيرة كيسي ، أحمد حمي، المرجع السابق ، ص 788 .

[2] يزيد بوحليط ، المرجع السابق ، ص 287.

للنقود حديث سري ومؤمن عكس الطريق القديم التقليدي ، أو عن طريق الهاتف المحمول ، لذا كان موقف المشرع من تعريف الأموال الخاضعة لجريمة التبييض أنه لم يفرق بين المال المادي والمال المعنوي المنقول والغير منقول ، المشرع الجزائري إعتبر أن الجريمة التي ترتكب بالوسيلة التقليدية لاتختلف عن الوسيلة الالكترونية ويعتبر ذلك رأيا صائبا من أجل تشجيع المشرع للسياسة الجنائية لقمع الجرائم الإلكترونية .[1]

ب : جريمة الإحتيال الإلكتروني:

– **تعريف الإحتيال الإلكتروني:** تعددت تعريفات الإحتيال الإلكتروني أو ما يعرف بالاحتيال المعلوماتي و شمل أيضا الإختلاف العناصر الواجب توفرها لإثباتها وتحقيقها كجريمة و أغلب التعريفات والمفاهيم ربطت الإحتيال الإلكتروني بفكرة الإستخدام الغير مشروع للحاسبات الآلية لتحقيق ربح مادي غير مشروع بصفة عامة وبين الإحتيال الإلكتروني ؛ وتعرف بصفة عامة جريمة الإحتيال بأنها كل فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبير إحترازي [2]."

وقد وضعت نصوص قانونية خاصة بهذا النوع من الجرائم المستحدثة كالولايات المتحدة وتشريعات عربية أيضا ، وقد حدث الإختلاف في تسميتها فاتجاه أطلق عليها جريمة النصب كالتشريع الجزائري والليبي والمصري والكويتي والبحريني والمغربي ، والإتجاه الثاني أبقى على نفس التسمية "الإحتيال" كالتشريع الأردني والسوري والعراقي والقطري ..... [3]

على الرغم من الإختلاف في تسمية النصب والإحتيال لكن يبقى المعنى واحد أي أن النصب معناه الإحتيال القائم على تشويه الحقيقة والكذب والخداع ، وجريمة الإحتيال قد عبر عليها المشرع

---

[1] يزيد بوحليط ، المرجع السابق ، ص 291 .

[2] خديجة صبايحية دحمان ،" *جرائم السرقة والاحتيال عبر الانترنت –دراسة مقارنة –بين الفقه الاسلامي والقانون الجزائري* " ، مذكرة ماجستير ،كلية العلوم الاسلامية ، جامعة الجزائر 2012-2013، ص 16 .

[3] سويح دنيا زاد ، " *الاحتيال الالكتروني* " ، مجلة الدراسات القانونية و الاقتصادية ، المركز الجامعي سي الحواس بريكة ، باتنة ، العدد 04 ، 2019 ، ص38 .

الجزائري في قانون العقوبات وأُطلق عليها "النصب "ودليل ذلك مانصت عليه المادة 372 ق.ع " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الإلتزامات أو الحصول على أي منها أو شرع في ذلك وكان ذلك بالإحتيال لسلب كل ثروة للغير " .

– أركان جريمة الإحتيال الإلكتروني:

الركن المادي : يتضح النشاط الإجرامي لجريمة الإحتيال والنصب المتمثل في الإستلاء على الحيازة الكاملة لمال مملوك للغير بطرق محددة قانونا فإذا إعتمد الجاني على طرق إحتيالية ، وحمل المجني عليه على تسليمه دعامة مادية مثبت عليها أحد البرامج التي تخصه ، وبعدها يخدعه ويستولى عليها الجاني لأنه من غير المتوقع أن ينقل المجني عليه معلوماته ومحتوياته وبرامجه بطريق شفهي لعدم وجود شيء ملموس مادي يتحقق فيه التسليم والإستلاء ، حتى ولو إفترض وقوع التسليم قولا فإنه لن ينتج عن ذلك حرمان المجني عليه بالمعلومات التي نقلها بالقول بل يبقى تحت تصرفه وتحت سيطرة من نقلها هذا ما يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي لفعل الإحتيال .[1]

ويشترط لتحقيق الركن المادي ان يرتبط بافعال اساسية وهي :

1–فعل النصب : ويتم عن طريق تغذية بيانات النظام المعلوماتي ببيانات غير صحيحة، أو عن طريق التلاعب بالبرامج والإدخال والإتلاف والمحو والطمس ..

2– وقد يكون الفعل بإرتكاب طرق إحتيالية التي تعتبر مجموعة من الأفعال المادية والمظاهر الخارجية التي يلجا اليها الجاني ليصحح الإعتقاد لدى المجني عليه بصدق ما صدر عنه من كذب مما يدفعه إلى تسليم المال طواعية أو إختيار ، ومن هنا يظهر أنه أولا لابد أن يصدر فعل الكذب أي جعل الواقعة غير صحيحة على أنها صحيحة سواءا بالكتابة أو القول أو بالإشارة ولايمكن أن تنصب جريمة

[1] تيسير أحمد حسين الزعبي ،" *جريمة الاحتيال الالكتروني* " ، مذكرة ماجستير ، جامعة جدارا ، فلسطين ، 2010 ، ص ص 95-96 .

النصب والإحتيال على الصمت والسكوت ،أي أن الكذب لايكفي لوحده بل لابد أن يستعمل وسائل إحتيالية ومن بينها الوقائع الخارجية التي يحيط بها الجاني وهي لا تعد ولا تحصى ؛ فقد تكون مظاهر خارجية يحيط بها الجاني نفسه أو يستعين بشخص من الغير أو سوء إستخدام الجاني لصفة حقيقية ، كحمل المجني عليه الى الثقة فيه .

الركن المعنوي: تعتبر جريمة النصب والاحتيال من الجرائم العمدية والقصدية اي انها تتوفر على القصد الجنائي العام بالاضافة الى القصد الجنائي الخاص ؛ والقصد العام في جريمة النصب يجتمع فيه عنصري العلم والإرادة يعني علم الجاني بالركن المادي للجريمة ، أي أن فعله يقوم على الإستيلاء على منقول غير مملوك له بل مملوك للغير بل أخذه دون رضا مالكه ، والإرادة هنا تتجه إلى إمتلاك الشيء المستولي عليه وهو نفس المعنى المدروس في جريمة السرقة ومن هنا نعلم أن جريمة الإحتيال تتوفر على نية إرتكاب الجرم لدى الجاني ، وأن كل تلاعب يحدثه بالمعلومات يمس بالحاسب الآلي ومن شأن هذا التلاعب الوصول إلى غاية يريد تحقيقها ، وجريمة الإحتيال تطبق بشكل واسع في عمليات تحويل الأموال الإلكترونية كنقلها من مصدر إلى مصدر أي من مصدر شرعي إلى مصدر غير شرعي ، وقد تتوفر أيضا هذه الجريمة في مجال بطاقات الإئتمان الممغنطة واجهزة الصرف الآلي ، وبمجرد الشروع في سحب هذه الاموال يعتبر فعلا جرمياً في حد ذاته , والباعث في إرتكاب جريمة النصب والإحتيال متى توافر القصد الجنائي العام والخاص وقام الركن المعنوي بغض النظر عن الباعث والسبب ،فمن المعلوم أن يكون الدافع هو حب المال أو رغبة الانتقام أو التشفي أو السخرية أو الإستهزاء إوإثبات غفلة المجني عليه[1].

الفرع الرابع : الجرائم الماسة بأمن الدولة :

تحتل الجرائم الماسة بأمن الدولة مكانة هامة في كل التشريعات وكذلك المعاهدات الدولية، وبالرغم من أنّ مرتكبيها هم أفراد وماتتميز به هذه الجرائم بخصائص خطيرة تميزها عن بقية الجرائم من أبرزها

[1] تيسير أحمد حسين الزعبي ، المرجع السابق ، ص ص 97-99 .

الطابع الدولي ،ففي كل دولة المشرع يعمل ويلتزم بسن قوانين تحمي الدولة كشخص معنوي قانوني وسياسي ،وهذا الإعتداء لم يكن داخلي فقط بل تعدى إلى الخارج عن طريق الإختراق مايعرف بالعالم الإفتراضي .

أ: جريمة التجسس (التنصت) : معظم دول العالم مع إرتباط بالشبكة العنكبوتية وخاصة في العقدين الأخيرين مما جعل الإتصالات ونظم المعلومات تتكاثف وتزداد، وأصبحت هذه الأخيرة عاملاً أساسياً في كل الإدارات وفي مختلف القطاعات كالقطاع المصرفي ، والتجاري ، والأمني ،والسياحي ... إلخ، بالإضافة إلى المشاريع الحيوية والحساسة كالنقل والمواصلات .... أدى إلى ظهور جريمة كانت أساسا موجودة منذ القدم إلا أن عصر المعلوماتية نمى وزاد في إنتشارها ، وهذه الجريمة تمثلت في التجسس أو مايعرف بالتنصت المعلوماتي ومن خلال ماسنحاول التطرق إليه سوف نعرف التعاريف التي توضحها والأركان التي تقوم عليها.

– تعريف التجسّس الإلكتروني : هو إستخدام الوسائل التقنية الحديثة للدخول الغير مصرح به والغير مسموح وغير مشروع إلى أنظمة معلومات إلكترونية خاصة بهيئة أو حكومة أو دولة ما بغرض التنصت عليها بهدف الحصول على ماتملكه من أسرار ومعلومات تتعلق بنظامها ، وهذه المعلومات قد تتعلق بالجانب العسكري أو السياسي أو الإقتصادي [1], عرفه بعض من الفقه بأنه" :الإطلاع على معلومات خاصة بالغير محفوظة على جهاز إلكتروني وليس مسموحاً لغير المخولين بالإطلاع عليها" , أما الفريق الأخر من الفقه فيرى بأنه استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلّق بنظامها وأسرارها، حيث تشمل عملية التجسس جميع المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية والاجتماع .[2]

[1] نجاري بن حاج علي فايزة ،" *جريمة التجسس الالكتروني* "، ستراتيجيا، مجلة دراسات الدفاع والاستقبالية ، العدد 11 ، 2019 ، ص 66

[2] بن بادة عبد الحليم ، "*جريمة التجسس الالكتروني*" ، الملتقى الدولي الأول الموسوم أمن المعلومات في الفضاء الالكتروني ،كلية الحقوق و العلوم السياسية ، جامعة غرداية ، 2020 ، ص 05 .

– أركان جريمة التجسّس الإلكتروني :

الركن المادي :يقوم الركن المادي لجريمة الإعتراض الغير قانوني للبيانات في فعل الإعتراض الذي يجب أن يقوم به الجاني في الجريمة دون وجه حق وبإستخدام وسائل فنية غير علنية ، المشرع الجزائري لم يعرف ولم يحدّد هذا السلوك، إلا أنّه في الفقرة (و) من قانون رقم 09-04 الفصل الأول منه المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ،أورد المشرع تعريف للإتصالات الإلكترونية على أنّها "أي تراسل أو إرسال أو إستقبال "علامات أو إشارات أو كتابات أو صور أو أصوات ، أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، نلاحظ أن المشرع وسع في مفهوم الإتصالات الإلكترونية عند إستخدامه مصطلح "الوسائل الإلكترونية "يقصد وسائل نقلها ، ومصطلح علامات وإشارات يقصد إنبعاثات الإشعاعات الكهرومغناطيسية أو الضوئية أو الرقمية المنبعثة أثناء إنتقال المعلومات[1].

الركن المعنوي : تعتبر جريمة التجسّس الإلكتروني من الجرائم العمدية لذا لابد من وجود القصد الجنائي ؛وهو قصد الحصول على معلومات تمس أمن الدولة من جهة الداخل أو الخارج سواء كانت عسكرية أو أمنية أو سياسية , أما القصد الخاص هنا يتمثل بقصد الفاعل إيقاع ضرر بالدولة أو الإساءة لها أو بأجهزتها أو شخصياتها[2].

ب :الإرهاب الإلكتروني :

تعريف جريمة الإرهاب الإلكتروني : إختلفت التعريفات التي تخص الإرهاب عبر الإنترنت ؛ أو كما يسمى بالإرهاب الرقمي ، فعرّف أنّه "هو جماعات غير مشروعة أو تهديدات بهجمات ضد الحاسيبات أو الشبكات أو المعلومات المخزنة إلكترونياً،توجه من أجل الإبتزاز أو الإجبار أو التأثير في

[1] إلهام بن خليفة ، "*التجسس الالكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري* " ، دفاتر السياسة والقانون ، العدد 01 ، المجلد 14 ، 2022 ، ص156 .

[2] المرجع نفسه ، ص 157 .

الحكومات أو الشعوب ،أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة والإرهاب المعلوماتي يتمثل في إستخدام الموارد المعلوماتية في شبكات المعلومات وأجهزة الكمبيوتر ،للتخويف والإرغام لإغراض وأهداف سياسية ،وقد يسبب الإرهاب المعلوماتي شلل في أنظمة القيادة والسيطرة على الإتصالات ... وعرفه باري كولين :" هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها , سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية , وأن الهجمة يجب أن تكون ذات أثر مدمر و تخريبي مكافئ للأفعال المادية للإرهاب " [1].

– أركان جريمة الإرهاب الإلكتروني :

الركن المادي : تتنوع صور الركن المادي في جريمة الارهاب الالكتروني ، والفعل يقع بإستخدام تقنية أنظمة معلومات ولتتحقق هذه الجريمة ركنها المادي يشترط ان يستخدم قدر كافي من العنف التهديدي، وأن يهدف إستخدامه للعنف أو التهديد به إيقاع الرعب بين الناس أو تعريض حياتهم للخطر، وقد ينفذ فعله إلى إشكال من الإجرام في شكل معنوي القادر على إظهار الإرهاب الإلكتروني إلى حيز الوجود كجرائم واجبة العقاب عند إرتكابها كإستخدامها للعنف والتهديد بغرض تعريض أمن المجتمع للخطر، أو الإخلال بالنظام العام ، ولا يشترط وقوع الضرر بل يكفي حدوثه ،كتلاعب الفاعل بانظمة إدارة وتشغيل الإشارة الضوئية ، وإختراق الانظمة ...، وقد يكون العنف ملحق بالبيئة أو المرافق العامة كالتلاعب بأنظمة ضخ المياه ، أو قد يمس العنف الموارد الوطنية أو الدستور والقوانين، أو تعطيل الاتصالات وأنظمة الحاسوب ، أو قد يكون الهدف من العنف تعريض نظام الحكم للخطر ،او تغيير كيان الدولة إقتصادياً أو إجتماعياً[2].

الركن المعنوي : لقيام جريمة الإرهاب الإلكتروني لايكفي في ذلك القصد العام ،أي لايكفي لقيامها علم الجاني بالسلوك الإجرامي المرتكب ، وإرادة إرتكابه ،بل لابد من إقتران القصد الجنائي العام

[1] غلاف كريمة ، جرلال زهرة ، " *جريمة الإرهاب الالكتروني* " ، مذكرة ماستر ، جامعة عبد الرحمان ميرة ، بجاية ، 2018-2019 ، ص 14 .

[2] خلفي عبد الرحمن ," *القانون الجنائي العام* ", دار بلقيس للنشر دار البيضاء , الجزائر, 2017 , ص 203 .

بالقصد الجنائي الخاص ، والقصد الخاص يتمثل في إقتران الإرهاب الإلكتروني بالغرض الإرهابي فلابد من وجود نية للفاعل ، عند إستخدامه لتقنية نظم المعلومات أن يهدد بإحداث أحد الأغراض المعلنة في النص القانوني التجريمي ، إذا لم يتوافر ذلك لاتقوم الجريمة[1] .

وفي ظل عصر السرعة والثورة المعلوماتية لا يستطيع أحد أن ينكر أهمية الانترنت لأنها احد أهم دعائم تكنولوجيا الاتصال والمعلومات ، و لكن هناك على الجانب الآخر أثار سلبية من أهمها ظهور نوع جديد من الجرائم الالكترونية، ونتيجة لهذا فقد كانت هناك التشريعات المقارنة التي عرفت الجريمة الالكترونية وبينت كيفية التصدي الى هذا الشبح، وكذلك المشرع الجزائري الذي عرفها كذلك وبين سماتها ونطاقها وطبيعتها ، وهذه الجريمة كأي جريمة أخرى لها أركان تقوم بقيامها وتزول بزوالها وفي هذا الفصل تناولنا مفهوم الجريمة الالكترونية في التشريعات المقارنة كما تطرقنا كذلك الى الجريمة الالكترونية في التشريع الجزائري وكذا تناولنا أركانها المتعارف عليها والمتمثل في الركن الشرعي والركن المادي والركن المعنوي و إضافة الى ذلك تحدثنا عن الركن المفترض لهذه الجريمة.

[1] غلاف كريمة ، المرجع السابق ، ص 47 .

خلاصة الفصل الأول:

وفي نهاية هذا الفصل ، يتضح لنا أن الجريمة الالكترونية هي جريمة وليدة التطور العلمي والتكنولوجي الذي وصلت إليه المجتمعات، فبرغم من الايجابيات التي تطغى على هذا التقدم إلا أن الجانب السلبي له يعرف انتشار كبيرا خاصة في أوساط الجيل الصاعد، فالمجرم المعلوماتي له قدرة كبيرة على التكيف بالمجتمعات الأخرى وكذا يتميز بالذكاء والفطنة وهي اكبر مقومات ارتكاب هذا النوع من الجرائم.

كما أن الصعوبة التي تحيط بالجريمة الالكترونية تتجلى في مسألة سرعة اكتشافها وكذا صعوبة إثباتها شكل أكبر عوائق التي تواجهنا في مكافحة هذا النوع من الجرائم.

إجراءات المتابعة و أساليب المكافحة للجريمة الالكترونية في التشريع الجزائري

تثير الجرائم الإلكترونية العديد من الاشكالات تتعلق بقانون الاجراءات الجنائية، حيث أن نصوص هذا القانون سنت لحماية القواعد المرتبطة بالجرائم التقليدية ، فلا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها أو جمع الأدلة المرتبطة بها كما تخضع لمبدأ حرية القاضي الجنائي في الاقتناع بشأن الجريمة والمجرم. و في المقابل تظهر صعوبات كثيرة فيما يخص البحث والتحري واثبات الجريمة الإلكترونية والوقاية منها على أساس أنها تتم في وسط افتراضي غير مادي و لا محدود ، وهو ما حاول أيضا المشرع الجزائري التكيف معه في سياسته الجنائية الهادفة إلى مكافحة هذا النوع من الجرائم .

ومن خلال ما ذكر سنقسم بحثنا إلى مبحثين نتناول في الأول إجراءات متابعة الجريمة الإلكترونية و العقوبات المقررة لها ، أما في المبحث الثاني سنتناول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري .

المبحث الأول : إجراءات متابعة الجريمة الإلكترونية و العقوبات المقررة لها :

تعد الجرائم الإلكترونية من أخطر الظواهر الإجرامية التي تحدث في المجتمع الجزائري ، حيث صاحب الفترة الأخيرة انفجار هائل للتكنولوجيا ، جاء معه اختلاف في سلوك الأفراد بين من يحسن استخدامها ومن يستغل استخدامها لأغراض إجرامية ، وعليه كان على المشرع الجزائري التدخل من خلال عدد من الإجراءات والعقوبات الموضوعة لمكافحة الجريمة وردع المجرم الإلكتروني. وهذا ما سنتناوله في هذا المبحث من خلال دراسة اجراءات البحث و التحري (المطلب الأول) , و مرحلة التحقيق المحاكمة (المطلب الثاني) .

المطلب الأول : إجراءات البحث و التحري في سبيل متابعة الجرائم الالكترونية :

وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الماسة بالمعطيات ومنها لا يطبق الا على الجريمة الإلكترونية خاصة في مرحلة جمع الاستدلالات والتحقيق . وتعد هذه المرحلة من اختصاص ضباط الشرطة القضائية الذين ينقسمون الى نوعان , النوع الأول وهو الذي يتمتع باختصاص عام و يتمثل في إجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات،والنوع الثاني هو ذو الاختصاص النوعي المحدود في نوع معين من الجرائم التي حددها القانون على سبيل الحصر هؤلاء المشار إليهم في المادة 12 من قانون الاجراءات الجزائية.

الفرع الأول: الاجراءات العامة لمتابعة الجريمة الإلكترونية :

في مجال المكافحة الاجرائية للجريمة الإلكترونية ، يتعين الاشارة إلى الدور الذي تلعبه الشرطة القضائية كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفة عامة والجرائم الإلكترونية بصفة خاصة، حيث نظرا لطبيعة هذه الاخيرة الخاصة وكيان بيئتها غير الملموس؛ تظهر صعوبة دور الشرطة

في الكشف عنها ومتابعة مرتكبيها، الامر الذي أدى بالدول السباقة في مكافحة الاجرام المعلوماتي إلى إيجاد وحدات من الشرطة متخصصة بالعمل في هذا المجال[1] .

أولا – الإجراءات المادية : وتتمثل الإجراءات المادية في المعاينة التقنية من جهة والتفتيش في بيئة الكترونية و كذا ضبط الدليل الرقمي وبيانها كما يلي :

أ– المعاينة التقنية للجريمة الالكترونية : بما أن مسرح الجريمة هو بداية الوصول لتحديد هوية الجاني ومعرفة كيفية و ظروف ارتكاب الجريمة، فان معاينته تتمثل في المعايشة الفعلية له من قبل الأشخاص المخول لهم اجرائها وهم قاضي التحقيق وكيل الجمهورية و ضباط الشرطة القضائية طبقا لنصوص المواد 66،72،32 من قانون الإجراءات الجزائية ، حيث يخضع مسرح الجريمة و الأماكن الأخرى الملحقة به لمعاينة دقيقة غايتها تحديد الأثار المختلفة بهدف كشف اللبس و السير نحو سبيل الاستدلال على مرتكبيها ومنه وجب الوقوف على تعريف المعاينة و تحديد أنواعها , وبناءا على ما تقدم ذكره يمكن القول أن المعاينة هي رؤية العين لمكان أو سخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[2] , وحتى يكون التفتيش في بيئة الكترونية لابد ان يتم علي مستويين تتمثل في تفتيش المكونات المادية (HARDWARE) للحاسب الالي والتي تمثل مسرح الجريمة التقليدي وأيضا تفتيش المكونات المعنوية (SOFTWARE) للحاسوب والتي تمثل مسرح الجريمة الافتراضية .

1–المسرح التقليدي (الجرائم الواقعة على المكونات المادية) : المسرح التقليدي هو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية، ومن امثلة هذه الجرائم تلك الواقعة على اشرطة الحاسب والكابلات

[1] محمدي بوزينة أمنة،" *إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية* "، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة، 29 مارس ،2017 , ص 60 .

[2] عائشة بن قارة ، "*حجية الدليل الالكتروني في مجال الاثبات الجنائي*" ، رسالة ماجستير ، جامعة الاسكندرية ، مصر ،2009 ، ص 47

الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الالي ذات الطابع المادي الملموس[1] .

2-المسرح الافتراضي (الجرائم الواقعة على المكونات الغير مادية او بواسطتها) : المسرح الافتراضي يقع داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله ، وتتميز المعاينة في العالم الافتراضي بالصعوبة[2] المتمثلة في :

* ندرة الاثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات .

* الاعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال الفترة مابين وقوع الجريمة واكتشافها و بداية المعاينة ولذلك على ضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه ان ينتقل الى العالم الافتراضي للمعاينة سواءا من مكتبه او اللجوء الى مقهى الأنترنت او الى الخبراء وغيرها من الأماكن التي تساعده في اظهار الحقيقة .

* إجراءات المعاينة التقنية : تتسم إجراءات المعاينة التقنية بالدقة و الخبرة في المجال المعلوماتي وتخضع لشروط تقنية وفنية محددة تتمثل في :

- عند العثور على الأجهزة داخل مسرح الجريمة يجب عدم العبث بها، تدوين الحالة التي هي عليها منطفئة او في حالة تشغيل , موصولة بالكهرباء او بجهاز لاحق اخر، و ينبغي ترقيم لواحقها بتسلسل
- يجب تحرير الأوراق المطبوعة على الحاسب الالي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها، ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل وتحرير الأوراق التي تمت طباعتها.
- تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة
- عند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيها (داخل الحاسب الالي او خارجه).[3]

---

[1] عمار حشمان ، "*الجريمة المعلوماتية في التشريع الجزائري* "، مذكرة ماستر ، جامعة قاصدي مرباح ، ورقلة ، 2019 ، ص 47 .

[2] طرشي نورة ،" *مكافحة الجريمة المعلوماتية* "، مذكرة الماجستير ، جامعة الجزائر1 ، 2012 ، ص 113 .

[3] المرجع نفسه ، ص 114 .

– عند الانتهاء من الترقيم يجب تصوير ودمج الأجهزة وملحقاتها في الحالة التي هي عليها .

–يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة كما ينبغي حمايتها من أي سبب من أسباب التلف وارسالها الى المخبر لإجراء الخبرة.

يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية الى الأدلة الرقمية واكتشاف المعلومات التي يحتويها كل دليل ومن هذه الأجهزة والأنظمة والبرمجيات ما يلي :

–أجهزة بقدرة عالية على التحليل وتخزين المعطيات

–نسخ من مختلف أنظمة التشغيل المستعملة لدى الافراد والمؤسسات.

–نسخ من برامج حذف وكسر كلمات المرور لمختلف الحاسبات، برامج نسخ الأقراص المدمجة والمحمولة، برامج الضغط وفك الضغط، برامج التشفير وفك التشفير، برامج حماية الأنظمة والشبكات من الاختراق، برامج كشف الأجهزة المخفية من الأقراص الصلبة، برامج استعادة الملفات المحذوفة وبرامج البحث عن الانترنت. ومن أجل التحقيق في الجرائم الإلكترونية يمكن للخبراء اللجوء الى بعض التقنيات منها [1]:

– تحديد عناوين IP وعناوين البريد الالكتروني المستعملة في ارتكاب الجريمة.

– استخدام تقنيات التخفي عن طريق نظام البروكسي proxy.

– استخدام برامج التتبع، كما يتبع المحقق في تحقيقه مناهج وطرق تحري لإثبات وقوع الجريمة وتحديد شخصية مرتكبها منها :

– إقتفاء الأثر في الجريمة الإلكترونية كون المجرم غالبا ما يعمد الى محو اثاره.

– يجب على المحقق الاطلاع على مختلف الأنظمة المعلوماتية ومكوناتها من شبكات وتطبيقات وخدمات .

[1] مباركية رابح ، " *إجراءات التحري والتحقيق في الجريمة الالكترونية* " ، مذكرة ماستر ، جامعة محمد البشير الابراهيمي ، برج بوعريريج ، ص ص 26-27 .

- يمكن الاستعانة بالذكاء الاصطناعي لحصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج .

ب- التفتيش المعلوماتي (التفتيش في بيئة تقنية) : يعتبر التفتيش اجراء من إجراءات البحث والتحقيق ويهدف الى البحث عن ادلة مادية لجناية او جنحة تحقق وقوعها بمكان يتمتع بالحرمة او تفتيش شخص، وان لإجراء التفتيش أهمية بالغة وخطورة معتبرة على الحياة الخاصة، ولهذا نص عليه المشرع الجزائري بمقتضى قواعد دستورية[1] حيث تضمن الدولة عدم انتهاك حرمة المسكن فلا تفتيش الا بمقتضى القانون. وفي إطار احترامه فلا تفتيش الا بأمر مكتوب صادر عن السلطة القضائية المختصة[2].

1- محل التفتيش : يقصد بمحل التفتيش في الجريمة الإلكترونية هو كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به . ينبغي الاشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال الذكي[3]، وبالتالي ففي جرائم الانترنت يقع التفتيش على موضوعين هما :

أ- تفتيش مكونات الحاسب الالي : قبل الغوص في إجراءات التفتيش لابد من تعريف الحاسب الالي" وهو كل جهاز الكتروني يستطيع ترجمة أواصر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال او اخراج معلومات" [4] . ومنه نستنتج قسمين من مكونات الحاسب وجب تفتيشها :

***- تفتيش المكونات المادية للحاسب الالي Hardware**: تخضع المكونات المادية لنظام المعالجة الالية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 ق.إ.ج.ج أي انه يجب مراعاة مكان وجود ذلك الحاسوب اثناء مباشرة ذلك الاجراء، فيما اذا كان مكانا عاما او خاصا،

---

[1] المادة 40 من الدستور الجزائري 1996 .

[2] برا هيمي جمال ،" *التحقيق الجنائي في الجرائم الالكترونية* " ، أطروحة دكتوراه ، جامعة مولود معمري تيزي وزو ، 2018 ، ص 13-14

[3] لينذا بن طالب ،" *التفتيش في الجريمة المعلوماتية* "، مجلة العلوم القانونية و السياسية ، عدد 16 ، 2017 ، ص 492 .

[4] محمد هماج مرهج الهيتي ، " *جرائم الحاسوب* "، ط 1 ، دار المناهج للنشر والتوزيع ، الاسكندرية ، 2012 ، ص 2 .

ذلك لان لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كان موجود في مكان خاص كمسكن المتهم فلا يجوز تفتيشه الا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات المقررة قانونا وكذا المادة 64 من نفس القانون، فلا يجوز القيام بإجراء التفتيش الا بأذن مكتوب صادر عن وكيل الجمهورية او قاضي التحقيق وبعد الحصول على رضا صريح من صاحب المسكن، ويجب كتابته بخط يد صاحب الشأن وتوقيعه، اما اذا تعذر على صاحب الشأن الحضور وقت اجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، واذا امتنع عن ذلك او كان هاربا استدعى الضابط لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته كما يجب ان يتم ذلك الاجراء في المواعيد المحددة قانون وهي من الساعة الخامسة صباحا الى الساعة الثامنة مساء إلا في الحالات الخاصة خاصة فيما يتعلق بالجرائم الستة الخطيرة والتي من بينها الجريمة الإلكترونية التي لا تشترط المواعيد وانما في كل وقت من الليل والنهار(24 ساعة)[1] .

***–تفتيش المكونات المعنوية لنظام المعالجة الالية Software** : يتعلق الأمر بالتفتيش عن الجريمة التي وقعت على المكونات المعنوية للحاسوب ويقصد بها أنظمة الكمبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات , والرأي المستقر عليه أن معطيات الحاسوب تصلح للتفتيش عن الأدلة الجرمية وضبطها لان الغاية من التفتيش هو الحصول على دليل خاص بالجريمة وكشف الغموض الذي أحاط بها [2].

ويتضح موقف المشرع الجزائري من خلال القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، حيث اجازت المادة 05 منه للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية بغرض التفتيش ولو كان عن بعد كل من المنظومة المعلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها او أي منظومة تخزين معلوماتية.

[1] براهيمي جمال ، المرجع السابق ، ص ص 15-16 .

[2] صغير يوسف ، المرجع السابق ، ص 78 .

يقصد بالتفتيش عن بعد تفتيش حاسوب المتهم عندما يكون متصلا بغيره من الحواسيب عبر شبكة أخري في دولة أخرى .[1]

طبقا للمادة 2/05 من القانون04/09 أجاز المشرع تمديد التفتيش الى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقا بذلك متى حصل الاعتقاد بوجود المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه الأخيرة يمكن الدخول اليها من المنظومة الأولى في إطار إقليم الدولة أما اذا تبين ان المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني. فإن التفتيش او الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة .

2- ضوابط التفتيش : إن الحرص على احاطة التفتيش بشروط وضمانات أساسية بوصفه اجراء يمس صميم الحرية الشخصية الغرض منه تحقيق الموازنة الضرورية بين مصلحة المجتمع وبين حقوق المتهم .ومن الشروط والضمانات التي يجب توافرها لإجراء التفتيش ما هو موضوعي ومنها ما هو شكلي[2] :

أ- الشروط الشكلية: وهي شروط شكلية لصحة التفتيش وهي:

- الحضور الضروري لبعض الأشخاص اثناء اجراء التفتيش في العالم الافتراضي وهي من اهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية وذلك لضمان الاطمئنان على سلامة الاجراء وصحة الضبط، والاصل ان الشخص الذي يستوجب الحضور هو المتهم او أحد أقاربه حيث اشترط المشرع الجزائري انه لا يجوز تفتيش مسكن المتهم الا بالضوابط والضمانات المقررة في نص المادة 45 و 64 ق.إ.ج.ج ، وهو ما استثناه المشرع لتطبيق هذه الضمانات بالنسبة لبعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات بموجب المادة 47 /3 ق.إ.ج.ج .

[1] براهيمي جمال ، المرجع السابق ، ص ص 25-26 .

[2] المرجع نفسه ، ص 31 .

-أن يتم التفتيش بأسلوب آلي.اي ان يكون التفتيش علي دعامة الكترونية وهو بالضرورة الحاسب الالي .

-أن يتم التفتيش من طرف فريق يتكون من خبراء .

-إذن التفتيش لابد ان يكون مسببا .

-ذهب المشرع الجزائري الى حضر التفتيش للمساكن وما في حكمها في أوقات معينة فالاصل ان يكون التفتيش من الساعة الخامسة صباحا الي الساعة الثامنة مساء وإلا كان التفتيش باطلا.

ب- الشروط الموضوعية: يقصد بها الشروط اللازمة لإجراء التفتيش الصحيح [1]، وتتمثل في

- سبب التفتيش: حتى يكون التفتيش صحيحا لابد أن تكون قد وقعت جريمة معلوماتية ، وهو ما أكدته المادة 5 من القانون 04/09 .

- الغاية من التفتيش: لابد ان يكون التفتيش بقصد ضبط أشياء تتعلق بالجريمة او تفيد في كشف الحقيقة والكشف عن أشياء تتعلق بالجريمة او تفيد في اظهار الحقيقة طبقا للنص المادة 44 ق.إ.ج.ج .

- محل التفتيش: هو المستودع الذي يحفظ فيه المرء بالأشياء المادية التي التي تضمن سره .

- إذن التفتيش : وطبقا للتشريع الجزائري فإن الإذن لابد ان يكون مكتوب من طرف إما وكيل الجمهورية او قاضي التحقيق المختص .

ثانيا : الإجراءات الشخصية : وهي إجراءات تتعلق بالشخص في حد ذاته وتتمثل في الخبرة وشهادة شاهد الكتروني والتسرب وهو ما سنتناوله فيما يلي :

أ- الخبرة : الخبرة هي اجراء يستهدف استخدام قدرات شخص الفنية او العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرينة يفيد في معرفة الحقيقة بشأن وقوع الجريمة [2]ولهذا

[1] براهيمي جمال ، المرجع السابق ، ص 31 .

[2] صغير يوسف ، المرجع السابق ، 88 .

فان للخبرة التقنية في الجريمة ونسبتها الى المتهم أو تحديد ملامح شخصيته الإجرامية أهمية بالغة ، ونظرا لأن الجريمة الإلكترونية لها خصوصيتها فإن الخبير المعلوماتي لابد أن تتوافر لديه المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة و لا تكفي الشهادة العلمية للخبير بل يجب مراعاة الخبرة العملية[1] لأنها هي التي تحقق الكفاءة الفنية .

1 – مهام الخبير : ينحصر دور الخبير الفني أو التقني، في تنفيذ المهام الفنية والتقنية التي يتم تكليفه بها من جهات التحقيق أو الجهات القضائية المختصة أو من الجهات المعنية بمكافحة جرائم المعلومات.

2– مجالات الخبرة بالنسبة للجرائم الإلكترونية : تتنوع العمليات الالكترونية بتنوع المجالات التي تستخدم شبكة الانترنت فنجد امثلة لها في الاعمال المصرفية، الإدارة الالكترونية، التجارة الالكترونية، لذلك تتنوع الجرائم التي تقع على هذه العمليات وفقا لنوع العمليات الالكترونية المستخدمة في ارتكابها حيث تقتضي عمليات البحث الجنائي والتحقيق في المعلوماتية الاستعانة بخبرات عديدة ومتنوعة .

3– ضوابط الخبرة : تخضع الخبرة لمجموعة من الضوابط القانونية والفنية :

* **الضوابط القانونية** : وتنحصر في تلك الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء ،واجبات والتزامات الخبير (الحلف اليمين، وخضوعه للرقابة القضائية) [2].

– القيام بمهامه بنفسه واستجابته لطلبات الخصوم .

– ايداعه التقارير خلال المدة المحددة .

[1] صغير يوسف ، المرجع السابق , 89 .

[2] انظر المواد ،143 ،144 ،145 ،148 153 قانون الإجراءات الجزائية الجزائري.

* **الضوابط الفنية:** تشمل خطوات اشتقاق الدليل الالكتروني والتي تتمثل في خطوات ما قبل التشغيل والفحص وخطوات التشغيل وتحديد مدن الترابط بين الدليل المادي والالكتروني ومرحلة تدوين النتائج واعداد التقارير وتتمثل هذه الضوابط في :

– جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز المعتدي

– التحليل الرقمي لمعرفة كيفية اعداد الأدلة الرقمية ونسبتها وتحديد عناصر حركتها، ثم التوصل في النهاية الى معرفة بروتوكول الانترنت (IP) للحاسوب الذي صدرت منه الرسائل والهجمات الالكترونية.[1]

ب– شهادة الشاهد الكتروني (الشهادة في الجريمة الالكترونية) : في مجال الجرائم الالكترونية يقصد بالشهادة ، القدرة على الولوج إلى نظام المعالجة الالية للمعطيات بهدف الحصول على الأدلة الرقمية بطلب من الجهات القضائية المختصة[2].

من ناحية أخرى تنقسم الشهادة إلى عدة أقسام :فهناك الشهادة المباشرة وغير المباشرة والشهادة الشفهية والمكتوبة والشهادة بالتسامع[3]، إضافة إلى ظهور نوع مستحدث يسمى بالشهادة الالكترونية عن بعد التي لا يكون فيها الشاهد حاضرا جسديا انما تتم عبر وسائل إلكترونية أو رقمية من خلال شبكة الأنترنت .

1: تعريف الشاهد الإلكتروني: الشاهد في الجريمة الإلكترونية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الالي، والذي لديه خبرة جوهرية لازمة للدخول الى نظام المعالجة الالية للمعطيات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله[4] ولذلك يطلق على الشخص اسم الشاهد المعلوماتي تمييزا عن الشاهد التقليدي.

---

[1] براهيمي جمال ، المرجع السابق ، ص ص 76 – 78 .

[2] نعيم سعيداني،"*آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري*"، رسالة ماجستير علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012 ، ص 143 .

[3] يزيد بوحليط ، المرجع السابق ، ص 241 .

[4] المرجع نفسه ، ص 242 .

2: فئات الشاهد الإلكتروني : ينحصر الشاهد المعلوماتي في عدة طوائف وفئات وهم[1]:

* **مشغل الحاسب الالي**: عامل تشغيل الحاسب الالي وهو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به .

* **خبير البرمجة**: أو خطوط البرامج وهم الأشخاص المتخصصين في كتابة أوامر البرامج وهم فئتين: الأولى: مخططو برامج التطبيقات و الثانية: مخططو برامج النظم .

* **المحلل** : هو الشخص الذي يحلل الخطوات، ويقوم بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه الى وحدات منفصلة واستنتاج العلاقة الوظيفة بينها .

* **مهندس الصيانة والاتصالات** : وهم المسؤولين عن اعمال الصيانة الخاصة بتقنيات الحاسب بمكونات وشبكات الاتصال المتعلقة به .

* **مدير النظم** : وهم الذين توكل لهم اعمال الإدارة في النظم المعلوماتية .

3: التزامات الشاهد في الجريمة الإلكترونية : يلتزم الشاهد في الجريمة الإلكترونية أن يعلم بها جهات التحقيق القضائي والا تعرض للعقوبات المقررة للامتناع عن الشهادة[2].وترتكز الشهادة على ما يلي :

– طبع البيانات المخزنة في ذاكرة الحاسب الالي او حاملات البيانات الثانوية وتسليمها الى المحقق طالما ان المصلحة العامة اقتضت ذلك .

– الإفصاح عن كلمات المرور السرية

– الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة .

وعموما هناك شروطا يجب توافرها لإلزام الشاهد المعلوماتي بالإعلام في الجرائم الإلكترونية وهي:

– وقوع جريمة إلكترونية فعليا .

[1] بوخبزة عائشة ، المرجع السابق ، ص209 .

[2] يزيد بوحليط ، المرجع السابق ، ص244 .

– علم الشاهد المعلوماتي بالمعلومات الجوهرية المتصلة بالواقعة

– أن تقتضي مصلحة التحقيق هذه الشهادة .

ج– التسرب : التسرب تقنية جديدة بالغة الخطورة في أمن الضبطية القضائية، وتتطلب جرأة وكفاءة ودقة في العمل قننها المشرع الجزائري في التعديل المطبق على قانون الإجراءات الجزائية لسنة 2006 .

1: مفهوم التسرب: إستحدث المشرع الجزائري إجراء التسرب بموجب المادة (65 مكرر 11) من ق.إ.ج.ج التي تنص على:" عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5) يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه."

وبخلاف إجراءات التحري سابقة الذكر التي لم يعرفها المشرع الجزائري ، أورد تعريف التسرب بموجب المادة (65 مكرر 12) من ق.إ.ج.ج التي تنص على:" يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة (65 مكرر14)أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم". كما حدد المشرع نطاق تطبيق التسرب بموجب المادة (65 مكرر 5) سالفة الذكر والتي من بينها جرائم المساس بأنظمة المعالجة الألية للمعطيات.

من خلال التعريف السابق فالتسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية ، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو شريك ، إلا أن المشرع أحاطه بجملة من الضوابط تجعله يتم وفق الشروط الشكلية والقانونية المطلوبة، والتي سنتناولها فيمايلي:

2: الشروط الشكلية والموضوعية للتسرب و اثاره : من أجل إنجاح عملية التسرب وتسهيل مهام الشخص المتسرب لبلوغ الهدف المرجو من هذا الإجراء ، فقد أحاطه المشرع بجملة من الشروط يتعين مراعاتها عندما تقتضي ضرورات التحري والتحقيق اللجوء إليه.

*: **الشروط الشكلية:** يجب توفر شروط شكلية[1] معينة في التسرب وهي :

– الإذن القضائي: و هذا ما نصت عليه المادة 65 مكرر 11 [2] فالجهة المختصة لإصداره إما وكيل الجمهورية أو قاضي التحقيق حماية للحقوق الأساسية المكرسة دستورا .

–يجب أن يكون الإذن مكتوبا: وهذا وفق نص المادة (65 مكرر15) التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر11)أعلاه، مكتوبا... وذلك تحت طائلة البطلان" ذلك أن الأصل في العمل الإجرائي هو الكتابة. وفقا لنص المادتين (138-139) من (ق.إ.ج)

–ذكر اسم الضابط المشرف: وهو ما نصت عليه المادة(65 مكرر15)بقولها:" يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا... وذلك تحت طائلة البطلان. تذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء و هوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته."...

–مدة التسرب: حددتها المادة(65 مكرر3/15)حيث تنص على:"...ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر..."، غير أنه ومراعاة لمقتضيات التحقيق الإبتدائي يمكن تجديد هذه المدة ضمن نفس الشروط الشكلية والزمنية السابقة. وحفاظا على حياة العون المتسرب من الخطر إضافة إلى الأشخاص المسخرين، أجاز المشرع للقاضي الذي رخص بعملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها .

---

[1] يزيد بوحليط ، المرجع السابق ، ص 168-170 .

[2] المادة (65 مكرر11)من (ق.إ.ج.ج):" عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر5) أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه".

– إبقاء الإذن بالتسرب خارج ملف الاجراءات إلى غاية الانتهاء من العملية : و الهدف من ذلك هو الحفاظ على السرية المطلوبة لنجاح عملية التسرب والتي حصرها المشرع بين القاضي الامر بها (وكيل الجمهورية أو قاضي التحقيق) وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب

–وجود تقرير مسبق: يتم تحريره من طرف الضابط المسؤول عن الجريمة بشكل مفصل لاطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها وكذا جدوى عملية التسرب، وهذا وفق نص المادة (65 مكرر13) من ق.إ.ج.ج.

–الصفة: نستخلص من المادتين(65 مكرر12 و 65 مكرر14) على أن المخولين قانونا للعمل بنظام التسرب هم ضباط وكذا أعوان الشرطة القضائية وكذا الأشخاص المسخرين لذلك . بعد الانتهاء من عملية التسرب يجب ايداع رخصة التسرب في ملف الاجراءات وهذا وفقا لنص المادة (65 مكرر 6/15) التي تنص على :"....توضع الرخصة في ملف الاجراءات بعد الانتهاء من عملية التسرب ".

* **الشروط الموضوعية:** تتمثل الشروط الموضوعية لعملية التسرب في شرطين رئيسين[1] هما:

–التسبيب : يعتبر التسبيب أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية، وهذا طبقا لنص المادة (65 مكرر 1/15) التي تنص على:" يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا ومسببا وذلك تحت طائلة البطلان."... فالقصد من هذا الإجراء هو الوصول إلى الحقيقة والوصول إلى الأدلة القانونية والموضوعية[2].

[1] براهيمي جمال ، المرجع السابق ، ص86 .

[2] مهدي شمس الدين ، " *النظام القانوني للتسرب في القانون الجزائري* " ، مذكرة ماستر ، جامعة محمد خيضر، بسكرة ، 2013-2014 , ص68 .

–نوع الجريمة: وقد حصرتها المادة(65 مكرر5)من (ق.إ.ج.ج) في سبعة أنواع هي :جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، جرائم تبييض الأموال، الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد. وعليه يجب أن تكون الجريمة جناية أو جنحة.

الفرع الثاني : الاجراءات الخاصة بمتابعة الجريمة الإلكترونية :

إن القواعد الإجرائية التقليدية للتحقيق في الجرائم المعلوماتية هي قواعد عامة لا بد منها و لا يخلو أي تحقيق من اللجوء إليها إلا أنها و أمام الثورة المعلوماتية لا يمكن أن تكون الإجراءات الوحيدة التي تقود المحقق إلى العثور على الدليل لما تميز به هذه الجرائم المستحدثة من خاصية تختلف عن الجرائم العادية ومن ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية ما جاء به في القانون رقم 06-22 مؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 جوان سنة 1966 والمتضمن قانون الإجراءات الجزائية من خلال إجراء اعتراض المراسلات ثم من خلال القانون 04/09 استحداث إجرائين آخرين وهما المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير .

أولا– مراقبة الإتصالات الإلكترونية : تعتبر المراقبة من اهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم سواء تلك التقليدية او المستحدثة كجرائم الانترنت وهي ما يعرف بالمراقبة الإلكترونية وقد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية الجزائري في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور . من خلال هذا يتضح أن أساليب التحري الخاصة هي إجراءات خطيرة تمس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا , ومن اجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 الذي طرأ عليه وفق لقانون 22/06 الذي حصر وجوبية اللجوء الى مثل هذا الإجراء على الجرائم الستة الخطيرة ومن بينها الجريمة الإلكترونية الذي أعطاها اسم "جريمة المساس بأنظمة المعالجة الالية للمعطيات" وتتمثل هذه الأساليب في :

أ- إعتراض المراسلات :

1- مفهوم إعتراض المراسلات: يقصد باعتراض المراسلات على أنه:" إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى إستراق السمع على الأحاديث وتتم بواسطة الوسائل السلكية و اللاسلكية[1] .

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 التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...".

2- إجراءات اعتراض المراسلات:

* **تحديد مجال اعتراض المراسلات** : نصت المادة(65 مكرر 5)من (ق.إ.ج.ج) على الجرائم التي يجوز القيام فيها بهذه العملية وهي:

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية .
- الجرائم الماسة بأنظمة المعالجة الالية للمعطيات .
- جرائم تبييض الأموال .
- جرائم الإرهاب .
- الجرائم المتعلقة بالتشريع الخاص بالصرف[2]:

[1] قادري سارة ،"*أساليب التحري الخاصة في قانون الإجراءات الجزائية* " ، مذكرة ماستر، جامعة قاصدي مرباح ، ورقلة ، 2014 ، ص 28

[2] الأمر رقم: 96-22 المؤرخ في 1996/07/09 المتمم والمعدل بالأمر رقم: 03-01 المؤرخ في:2003/02/19 .

– جرائم الفساد المحددة بالقانون رقم:06-01 المؤرخ في: 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته.

***الجهة القضائية التي يجوز لها بمنح الإذن للقيام بهذه العملية:** حسب ما ورد في نص المادة (65 مكرر 5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

–وكيل الجمهورية: يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة له.

–**قاضي التحقيق:** في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65مكرر5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65 مكرر5/6).

* **الأماكن التي يسمح فيها بالإعتراض:** لم يحدد المشرع الجزائري بدقة الأماكن التي تتم فيها عملية الإعتراض، بل جاء النص على عمومه، حيث نصت المادة (65 مكرر 05)على: " ...في أماكن خاصة أو عمومية..." دون استثناء فقد يكون منزلا أو مقهى الأنترنت أو شركة...إلخ ، حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن ووضع الوسائل اللازمة لاعتراض المراسلات حتى بغير علم وموافقة أصحابها وحتى خارج الأجال المنصوص عليها في المادة (47) من (ق.إ.ج.ج).

* **مضمون الإذن ومدته** : يتضمن الإذن المذكور في المادة (65 مكرر 5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها والأماكن المقصودة ، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65 مكرر7) على:" يجب أن يتضمن الإذن المذكور في المادة 65 مكرر5 أعلاه كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية."

من خلال هذه المادة يمكن أن نستخلص الشروط الشكلية والزمنية للإذن وهي:

– أن يكون الإذن مكتوبا .

– ذكر جميع العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها والأماكن المقصودة.

– ذكر الجريمة التي تبرر اللجوء إلى هذه العملية و هي إحدى الجرائم المذكورة على سبيل الحصر في نص المادة (65 مكرر 5) من (ق.إ.ج.ج).

– ذكر المدة التي تتم خلالها العملية على ألا تتجاوز مدة أربعة أشهر قابلة للتجديد بالشروط نفسها.

***كيفية القيام بالعملية:** يتم اعتراض المراسلات بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر8) . كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية اعتراض وتسجيل المراسلات ، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والإنتهاء منها، كما يمكن ترجمة المراسلات التي تتم باللغات الأجنبية، ويسجل كل هذا في محضر يودع بالملف وهذا وفقا لنص المادتان (65 مكرر9 –65 مكرر10)من (ق.إ.ج.ج).

يعتبر البريد الإلكتروني e-mail من أهم وسائل الإتصال الحديثة التي توفرها شبكة الإنترنت، لما يمتاز به من أمان وسرعة في نقل المستندات والرسائل والملفات وتخزينها، كما أنه يتمتع بالحماية القانونية نظرا لأهميته البالغة، حيث صار مستخدما بكثرة مما يجعله عرضة للإختراق من قبل قراصنة الحاسوب، كما أنه يستعمل أيضا من قبل المجرمين للتواصل فيما بينهم وإعداد خططهم بعيدا عن أعين الأجهزة الأمنية، و لذلك فقد أجاز المشرع اعتراض المراسلات التي تتم عن طريق البريد الإلكتروني حينما يتطلب الأمر كشف الجرائم الإلكترونية ومرتكبيها[1] .

ب – تسجيل الأصوات واجراءات القيام به: يعتبر إجراء تسجيل الأصوات من الإجراءات الخفية مثل اعتراض المراسلات، الهدف منه تمكين أجهزة البحث والتحري من اكتشاف الحقيقة.

1– مفهوم تسجيل الأصوات : يعرف تسجيل الأصوات بأنه:" النقل المباشر والألي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق إلى شريط

[1] سعيداني نعيم ، المرجع السابق ، ص 177 .

التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه" . أو هي تلك:" المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام، ويتم ذلك عن طريق حفظ الحديث على جهاز معد لذلك للاستماع إليه مرة أخرى . وعليه واستنتاجا من التعريفين السابقين يعتبر التسجيل الصوتي نقل الموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية إلى شريط تسجيل بحيث يمكن إعادة سماع الصوت للتعرف على مضمونه و إدراك خواصه التي تشكل عناصر المقارنة عند مضاهاتها على صوت الشخص المنسوب إليه، مما يتيح تقرير إسناده أو نفي ذلك، وهو من الوسائل الملائمة لضبط الحقيقة [1].

بالرجوع إلى نص المادة(65 مكرر5)من(ق.إ.ج.ج) التي تنص على:" اذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الالية للمعطيات أو جرائم تبييض الاموال أو الارهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكالم المتفوه به بصفة خاصة أو سرية، من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية" .

2- اجراءات تسجيل الأصوات: ويتم ذلك كما يأتي:

* **تحديد مجال تسجيل الأصوات:** نصت المادة(65 مكرر5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي: جرائم المخدرات- الجريمة المنظمة العابرة للحدود الوطنية -الجرائم الماسة بأنظمة المعالجة الالية للمعطيات...إلخ .

* **منح الإذن للقيام بهذه العملية:** حسب ما ورد في نص المادة(65 مكرر 5)فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من :

[1] يزيد بوحليط ، المرجع السابق ، ص 260-261 .

وكيل الجمهورية : يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها تحت مراقبته المباشرة .

قاضي التحقيق : في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة(65 مكرر5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة(65 مكرر5/6)من (ق.إ.ج.ج)

* **أماكن تسجيل الاصوات**: لم يحدد المشرع الجزائري بدقة الاماكن التي ستتم فيها عملية تسجيل الاصوات، بل جاء النص عاما ، فقد سمح المشرع الجزائري بالدخول إلى تلك الأماكن ووضع الوسائل اللازمة لتسجيل الأصوات كتركيب الميكروفونات حتى بغير علم وموافقة أصحابها وحتى خارج الأجال المنصوص عليها في المادة (47) من (ق.إ.ج.ج) .

* **مضمون الإذن ومدته** : يتضمن الإذن المذكور في المادة(65 مكرر 5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم، وكذا الأماكن المقصودة سواء كانت عامة أو خاصة وكذا اللجوء إلى هذه التدابير ومدتها.

* **كيف تتم العملية**: تتم عملية تسجيل الأصوات بتسخير أعوان مصالح الإتصالات السلكية و اللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة(65 مكرر8) حيث يقوم القاضي المختص بتحرير محضر عن كل عملية تسجيل الأصوات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الإلتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والإنتهاء منها.

ج– التقاط الصور : إن عملية التقاط الصور باعتبارها إحدى وسائل البحث والتحري الحديثة، هي استثناء عن المبدأ العام الذي يمنع التقاط الصور دون رضا صاحبها لما فيها من مساس بحرمة الحياة الخاصة المحمية قانونا .

1- مفهوم التقاط الصور: تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية. يقوم هذا الإجراء أساسا على استخدام الكاميرات، أو أجهزة خاصة التقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل مادي[1] .

بالرجوع لنص المادة (65 مكرر5) من (ق.إ.ج.ج) التي تنص على:" اذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الألية للمعطيات...يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي : وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ."...وعليه يربط هذا الإجراء الشخص أو الأشخاص في مكان واحد وفي وقت واحد.

2- إجراءات التقاط الصور: نتطرق إليها كما يأتي :

* **تحديد مجال التقاط الصور** : نصت المادة (65 مكرر 5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي :

-جرائم المخدرات .

-الجريمة المنظمة العابرة للحدود الوطنية .

-الجرائم الماسة بأنظمة المعالجة الألية للمعطيات .

-جرائم تبييض الأموال .

-جرائم الإرهاب .

-الجرائم المتعلقة بالتشريع الخاص بالصرف .

[1] زوزو زوليخة ، " *ضوابط المراقبة الالكترونية في التشريع الجزائري* "، مجلة المفكر ، العدد 18 ، 2019 ، ص ص 408-409 .

-جرائم الفساد .

* **منح الإذن للقيام بهذه العملية** : حسب ما ورد في نص المادة(65 مكرر 5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

-وكيل الجمهورية: يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس وتحت المراقبة المباشرة له .

-قاضي التحقيق: في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65 مكرر 5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65 مكرر 5/ 6).

* **أماكن التقاط الصور:** على خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة استثنى المشرع الجزائري التقاط الصور في الأماكن العمومية، غير أنه سمح بهذا التدبير بموجب المادة (56) من القانون 06-01 المتعلق بالوقاية من الفساد و مكافحته.

* **مضمون الإذن ومدته:** يتضمن الإذن المذكور في المادة(65 مكرر 5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط الصور لهم والأماكن المقصودة سواء كانت عامة أو خاصة .

* **كيف تتم العملية:** تتم عملية التقاط الصور بتسخير أعوان مصالح الإتصالات السلكية اللاسلكية للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية التقاط الصور، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والإنتهاء منها، و هذا بموجب المادتين (9- 10) من (ق.إ.ج.ج.) .

ثانيا- حفظ المعطيات المتعلقة بالسير : قررت التشريعات الحديثة ومنها المشرع الجزائري الزام مقدمي خدمات حفظ المعطيات المتعلقة بحركة السير ضمان الوصول الى اثار الجريمة مهما كانت .

أ- تعريفها : ويقصد بمقدمي الخدمات أي كيان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية او نظام اتصالات وأي كيان اخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او مستعمليها[1] .

ويقصد بالمعطيات المتعلقة بحركة السير، هي تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة باعتبارها جزء من حلقة الاتصال توضح مصدر الاتصال، والوجهة المرسلة اليها والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة [2].

ب- المعطيات الواجب حفظها : وقد حدد المشرع الجزائري المعطيات التي يجب على مقدمي الخدمات حفظها فيما يلي:

-المعطيات التي تسمح بالتعرف على مستخدمي الخدمة .

-المعطيات التي تسمح بالتعرف على المرسل اليه او المرسل إليهم وكذا عناوين المواقع .

-الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال وتكون مدة الحفظ لا تتجاوز سنة، والا تعرض مقدمي الخدمة للعقوبات المقررة في المادة 11 من القانون 04/09.

المطلب الثاني : مباشرة التحقيق و المحاكمة :

يبدأ التحقيق في الجريمة الإلكترونية بمجرد وصول البلاغ الى المحقق بشأن وقوع الجريمة حيث يتخذ المحقق الاجراءات اللازمة للكشف عن غموضها وضبط الفاعل وإسناد الاتهام قبله وتقديمه للمحاكمة، أما القواعد الفنية فهي تلك التي تحكم المحقق منذ تلقيه البلاغ حتى ضبط المتهم وتقديمه للمحاكمة بعد إسناد الاتهام إليه ، ويقصد بالتحقيق في مجال القانون هو مجموعة الإجراءات التي تباشرها سلطة التحقيق عند وقوع جريمة أو حادث ما يهدف التنقيب عن الأدلة التي تفيد في كشف الحقيقة, خاصة في الجريمة الإلكترونية .

[1] ابتسام بغو ،" *إجراءات المتابعة الجزائية في الجريمة المعلوماتية* "، مذكرة ماستر ، جامعة العربي بن مهيدي ، أم البواقي ، 2016 ، ص 36

[2] المرجع نفسه ، ص 36 .

وبطبيعة الحال لن يتوقف الأمر عند أدراج التحقيق او التحري إذ لابد لها أن تدخل في مرحلة جديدة وهي أروقة المحاكم التي تختص بمحاكمة أو متابعة مرتكبي الجريمة الإلكترونية وبالتالي وجود جهاز قضائي من أجل محاكمة هؤلاء المجرمين من أجل ذلك وجد جهاز قضائي جديد يختص بالفصل في نوع معين من الجرائم وذلك نظر لخطورتها .

الفرع الأول : اجراءات التحقيق :

يعرف التحقيق الجنائي بأنه العلم الذي يضم مجموعة من الاجراءات النظرية و العملية التي يقوم بها محققو هيئة التحقيق و الادعاء العام بما يوصلهم لكشف الجريمة الإلكترونية و توفير الادلة [1]. و يمكن تعريفه كذلك بأنه: عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمه إلى السلطات التحقيق القضائي في هذه الجرائم لاقامة العدل [2]. وتمر الدعوى الجنائية بمرحلتين، التحقيق و المحاكمة، وتمر عملية التحقيق بدورها بمرحلتين، مرحلة التحقيق الأولي(الضبطية القضائية) مرحلة التحقيق الإبتدائي(قاضي التحقيق) وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية، فإذا كان التحقيق يعتمد على ذكاء المحقق وقوة ملاحظته، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى ذلك تطوير لأساليبه، وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطورها وسنتناول ذلك فيمايلي :

أولا : تعيين قاضي التحقيق : في الجزائر يعين قاضي التحقيق بمقتضى قرار من وزارة العدل ، ثم عدل المشرع عن ذلك بموجب القانون 01 - 08 المؤرخ في 26 جوان 2001 .وأصبح التعيين بموجب مرسوم رئاسي ، وفقا لنص المادة 39 قانون الإجراءات الجزائية ، إلا أنه حتى هذه الأخيرة تم إلغاؤها بموجب القانون رقم 06 - 22 المؤرخ في 20ديسمبر 2006 ليرجع من جديد للتعيين رجوعا

[1] فالح عبد القادر، آيت عبد المالك نادية، " *التحقيق الجنائي في الجرائم الالكترونية و اثباتها في التشريع الجزائري*"، مجلة الاستاذ الباحث للدراسات القانونية و السياسية، جامعة الجيلالي بونعامة، خميس مليانة ، العدد 02 ، مجلد 04 ،2019, ص 1964 .

[2] مصطفى محمود موسى،" *التحقيق الجنائي في الجرائم الالكترونية* "، مطابع الشرطة ، القاهرة ، 2009 ، ص 322.

إلى نص المادة 50 من القانون الأساسي للقضاة ، وتكون مدة التعيين ثلاث سنوات ، وتنتهي مهام قاضي التحقيق بنفس الأشكال التي يتعين فيها ، أي بقرار من وزير العدل[1].

ثانيا : إختصاص قاضي التحقيق: سنتناول في هذا العنصر قواعد الإختصاص الشخصي ثم النوعي وأخيرا المحلي لقاضي التحقيق.

أ: الإختصاص الشخصي : الأصل أن قاضي التحقيق يحقق مع جميع الأشخاص دون تمييز ، إلا أن المشرع الجزائري إستثنى بعض الفئات كالأحداث ـ العسكريين ـ ضباط الشرطة القضائية ـ قضاة الحكم والتحقيق ومساعدي وكيل الجمهورية ـ قضاة المجالس القضائية ـ ورؤساء المحاكم ووكلاء الجمهورية ـ قضاة المحكمة العليا ورؤساء المجالس القضائية ـ والنواب العامون ـ وأعضاء الحكومة والولاة[2].

ويختص بالتحقيق مع جميع جرائم القانون العام سواء كانت جناية أو جنحة أو مخالفة التي من خلالها تقدم النيابة العامة طلب إفتتاحي أو الجنايات أو جنح التي من خلالها يقدم الطرف المدني إدعاءا مدنيا.

ب : الإختصاص النوعي : يختص قاضي التحقيق بالتحقيق في جميع الجرائم ويكون ذلك وجوبي في الجنايات وجوازي في الجنح إذا كان هناك نص وإختياري في المخالفات طبقا لنص المادة 66 من قانون الإجراءات الجزائية التحقيق الإبتدائي وجوبي في مواد الجنايات أما في مواد الجنح فيكون إختياري مالم يكن ثمة نصوص خاصة ، كما يجوز إجراءه في مواد المخالفات إذا طلبه وكيل الجمهورية. إن قاضي التحقيق يختص في المحاكم الجهوية في الجرائم التي إختصها المشرع بالنظر في الجرائم المخذرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الالية للمعطيات وجرائم تبييض الأموال والإرهاب وجرائم

---

[1] المرسوم التنفيذي رقم 06-348 المؤرخ في 05-10-2006 المتعلق بتحديد الاختصاص الاقليمي لبعض المحاكم ووكلاء الجمهورية أو قضاة المحكمة .

[2] ابن الضب فاطنة ، حبي فتيحة ،" *الاليات المستحدثة للحد من الجريمة الالكترونية في التشريع الجزائري* "، مذكرة ماستر ، جامعة غرداية ،2019 ، ص61 .

الصرف طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 05-10-2006 المتعلق بتحديد الاختصاص الاقليمي لبعض المحاكم ووكلاء الجمهورية أو قضاة المحكمة .

ج : الإختصـاص المحلي: تنص المادة 40 من قانون الإجراءات الجزائية " يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر» ...يمتد إختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 2/40 مكرر من قانون الإجراءات الجزائية[1].

ثالثا : سلطـات قـاضي التحقيق وحـدود الدعوى الجنـائية أمـامه: تتمثل سلطاته في القيام بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وبالتحري عن أدلة الإتهام وأدلة النفي و يجوز لقاضي التحقيق أن يأمر بإجراء الفحص الطبي كما له أن يعهد إلى الطبيب بإجراء فحص نفساني أو يأمر بإتخاذ أي إجراء يراه مفيدا (المادة 68 قانون الإجراءات الجزائية.) ينسق القاضي المكلف بالتحقيق سير إجراءات التحقيق وله وحده الصفة في مسائل الرقابة القضائية والحبس المؤقت إتخاذ أوامر التصرف في القضية طبقا لنص المادة 70 قانون الإجراءات الجزائية.

يستطيع القاضي سماع أقوال كل من يشير إليهم في الشكوى بإعتبارهم شهودا طبقا لنص المادة 73 قانون الإجراءات الجزائية.

يستطيع قاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جمع المعاينات اللازمة أو القيام بتفتيشها طبقا لنص المادة 79 قانون الإجراءات الجزائية .إستدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية طبقا لنص المادة 88 قانون الإجراءات الجزائية.

يجوز للقاضي إستدعاء مترجم طبقا لنص المادة 91 قانون الإجراءات الجزائية، إصدار أمر بإحضار المتهم أو بإيداعه السجن أو بإلقاء القبض عليه حسب نص المادة 109قانون الإجراءات الجزائية.

[1] ابن الضب فاطنة ، حبي فتيحة ، المرجع السابق ، ص61 .

ولقاضي التحقيق أن يأمر بحبس المتهم إحتياطيا لمدة 15 يوما .

رابعا : كيفية إتصال قاضي التحقيق بملف الدعوى الخاص بالجريمة الإلكترونية : يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب الإفتتاحي لإجراء تحقيق ، وإما عن طريق شكوى جزائية مقدمة من المضرور وهذا ما أكدته 3/38 من قانون الإجراءات الجزائية الجزائري على "... يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73" [1].

أ : الطلب الإفتتاحي لإجراء التحقيق : يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية أن يطلب فتح التحقيق ما لم ينص القانون على وجوب التحقيق في بعض الجنح ، ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا أظهرت وقائع جديدة طبقا للمادة 3/67 قانون الإجراءات الجزائية الجزائري على أنه " لايجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها» .ويتقيد قاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 3/67 و4 من قانون الإجراءات الجزائية «...ولقاضي التحقيق سلطة الإتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المجال تحقيقها إليه. فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع."

ب : الشكوى المصحوبة بإدعاء المدني : تنص المادة 72 قانون الإجراءات الجزائية " يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص. "

يلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت ، وحرصا منه على أن يكون الإشراف على على ملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية

[1] المادة 67/ 73 من قانون رقم 04/14 المؤرخ في 10 نوفمبر 2010 المعدل والمتمم للامر 156/66 المتضمن قانون الاجراءات الجزائية، جريدة رسمية عدد 71 .

القضائية التي عادة يكون لها تأثير على مجرى التحقيق ، كما أنه يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها. إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء إستعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية كاذبة إذا ما خسر دعواه ، ولهذا عليه أن يتأكد من أن إتهامه كان مبنيا على دليل قوي في الدعوى.

خامسا : إستئناف أوامر قاضي التحقيق : الجهات التي تستأنف أوامر قاضي التحقيق هي

أ : النيابة العامة : لوكيل الجمهورية أو أحد مساعديه إستئناف جميع أوامر قاضي التحقيق دون إستثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري " لوكيل الجمهورية الحق في أن يستأنف أمام غرفة الإتهام جميع أوامر قاضي التحقيق.

ويكون هذا الإستئناف تقرير لدى قلم كتاب المحكمة ويجب أن يرفع في ثلاثة أيام من تاريخ صدور الأمر .

يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج ويفرج على المتهم رغم إستئناف النائب العام مالم يكن وكيل الجمهورية قد إستأنفه بالطبع ويجب أن يبلغ النائب العام عند إستئنافه الخصوم في الدعوى ، وذلك خلال العشرين يوما التالية لصدور الأمر حتى يكونوا على بينة من أمرهم ولايفاجؤوا بقرار من غرفة الإتهام في غير صالحهم .

ب : إستئناف المتهم: إن المتهم لايجوز له إستئناف جميع أوامر قاضي التحقيق و يرفع الإستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة (3) أيام من تبليغ الأمر إلى المتهم طبقا للمادة 168قانون الإجراءات الجزائية.

ج : إستئناف المدعي المدني : كما أجاز المشرع الجزائري للمدعي المدني الحق في إستئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية ، وبمفهوم المخالفة لايجوز له إستئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية.

ويرفع الإستئناف خلال (3) أيام من تاريخ تبليغ الأمر المراد إستئنافه إلى المدعي المدني ، وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا لنص المادة 3/173 قانون الإجراءات الجزائية.

الفرع الثاني : مـرحلـة المحـاكمـة :

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي للطلب الإفتتاحي لإجراء تحقيق، وإما عن طريق شكوى جزائية مقدم من المضرور وهذا ما أكدته المادة 3/38 من قانون الإجراءات الجزائية الجزائري على "... يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73 ويتقيد قاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 3/67 و 4 من قانون الإجراءات الجزائية " ... ولقاضي التحقيق سلطة الإتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه . فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع .[1]

أولا : اختصاص المحكمة: يختص القضاء الوطني في الفصل في الدعوى الجزائية كما يقوم بتحديد إطارها الجغرافي او دائرة الإختصاص المكاني.

1/ الاختصاص المحلي في الجريمة الالكترونية: طبقا لنص المادة 40 من ق.إ.ج.ج يحدد الاختصاص المحلي للجريمة في ثلاث ضوابط مكان وقوع الجريمة أو مكان اقامة المتهم أو مكان الضبط كما نصت أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في: 2006/10/05 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق الى دائرة اختصاص محاكم أخرى ويتعلق الأمر بكل من محكمة سيدي امحمد بالجزائر العاصمة و كذا محكمة قسنطينة و محكمة ورقلة و قسم محكمة وهران, و في نطاق الجرائم الإلكترونية فان السلوك الاجرامي قد يتم في مكان معين و

[1] بعرة سعيدة،" *الجريمة الإلكترونية في التشريع الجزائري*" ، شهادة ماستر ، جامعة محمد خيضر ، بسكرة ، 2016/2015 ،ص 92 .

تتحقق النتيجة في مكان اخر ,فان الاختصاص ينعقد إما في مكان السلوك او مكان تحقق النتيجة , تعد الجريمة الالكترونية اذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر انها ارتكبت في جميع الاماكن التي امتدت الجريمة فيها .[1]

2/ الاختصاص النوعي في الجريمة الالكترونية: يتحدد الاختصاص النوعي لمحكمة الفصل في قضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات كالجرائم الموصوفة بأفعال ارهابية تخريبية المحالة اليها بقرار نهائي من غرفة الإتهام حسب نص المادة 248 من قانون الاجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح و المخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب نص المادة 328 من قانون الاجراءات الجزائية .[2]

ثانيا: تشكيلة المحكمة في الجريمة الإلكترونية : تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع قسم الجنح الخاص بالجريمة الإلكترونية ، فعلى مستوى المحكمة تتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه ، أما على مستوى المجلس قضائي فالتشكيلة فيها ثلاثية ، أي تتشكل من رئيس غرفة ومستشارين إثنين بالإضافة إلى كاتب ضبط وبحضور النائب العام أو أحد مساعديه .أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبطوالنيابة العامة أو من يمثله .[3]

ثالثا :اجراءات المحاكمة في الجريمة الإلكترونية : تستهل المحكمة جلستها بالاعلان أولا عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم

[1] بعرة سعيدة، المرجع سابق، ص 93.

[2] بن الضب فاطنة ، حبي فتيحة ، المرجع السابق ، ص 65 .

[3] بعرة سعيدة ، المرجع سابق ، ص 94 .

والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، يتم تدوين ذلك في محضر الجلسة المعد من طرف كاتب الضبط، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه .[1]

إذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب اجراءات المثول الفوري فإنه يساق بواسطة القوة العمومية لحضور الجلسة، ويخطره رئيس الجلسة بأن له الحق في اختيار محام للدفاع عنه فإن طلب ذلك أمهل القاضي مدة لا تقل عن ثلاثة أيام لتحضير دفاعه ، و إذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة، وفي هذه الحالة وطبقا لاحكام المادة (339 مكرر 6)المستحدثة بموجب الامر 15-02 المؤرخ في 23 جويلية 2015 من (ق.إ.ج.ج) تتخذ المحكمة إحدى الاجراءات التالية: ترك المتهم حرا أو إخضاعه لتدابير الرقابة القضائية المنصوص عليها في المادة (125 مكرر 1)من (ق.إ.ج.ج)، أو وضعه في الحبس المؤقت، مع الاشارة أن هذه التدابير لا تقبل الاستئناف.

ثم بعد ذلك و حسب موضوع القضية و بناء على طلب الخصوم أو من تلقاء نفسه يقرر علانية أو سريتها بعد أخذ رأي النيابة العامة، لكن جلسات الأحداث وجوبيا تتم في جلسة سرية طبقا ألحمام المادة (82)من قانون حماية الطفل رقم 15-12 المؤرخ في 15 جويلية 2015.

يواجه المتهم بالادلة الموجودة ضده، وعلى القاضي مناقشته عن كل واقعة بالتفصيل حتى وإن اعترف على فعله ، و بعدها يقوم بسماع شهود الاثبات ثم النفي إن وجدوا، و بعدها بسماع الطرف المدني، ثم تعطى الكلمة للنيابة العامة من أجل توجيه الاسئلة إلى المتهمين أو الشهود أو الضحايا، أما دفاع المتهم أو الضحية فيتم طرح الاسئلة بواسطة رئيس الجلسة ليكون له الحق في الاعتراض على أي سؤال، باستثناء محكمة الجنايات الابتدائية ومحكمة الجنايات الاستئنافية فيمكن للمحامي طرح أسئلة مباشرة مثل النيابة العامة طبقا لنص المادة (288)من (ق.إ.ج.ج) المعدلة بموجب القانون 17-07 المؤرخ في 27 مارس 2017 . بعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني أو محامية للمرافعة

[1] بعرة سعيدة، المرجع سابق، ص95 .

وتقديم طلبات المتمثلة في التعويض المدني فقط دون المطالبة بالعقوبات الجزائية ، تقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساتها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم التماس ، ويكون بعدها للنيابة العامة والمدعي حق الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه ، ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكم في نفس الجلسة أو يحدد تاريخ لاحق للنطق بالحكم، اين يبني هذا الحكم وفقا لقناعته الشخصية الخاصة .[1]

رابعا : العقوبات المقررة على الجريمة الالكترونية : إن العقوبات المقررة عن ارتكاب الجريمة الالكترونية سواء تعلق الأمر بالشخص الطبيعي أو المعنوي أدرجها المشرع الجزائري في قانون العقوبات و خصص لها القسم السابع مكرر وسماه بالأنظمة المعالجة الألية للمعطيات و خصص لها 10 مواد اختلفت ما بين عقوبات أصلية و أخرى تكميلية.

1/ العقوبات المقررة للشخص الطبيعي : وتنقسم إلى جريمة بسيطة تتمثل في الدخول و البقاء الغير مصرح به حيث جاء في أحكام المادة 372 مكرر:" يعاقب بالحبس من ثلاثة أشهر إلى سنة و غرامة مالية من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الألية للمعطيات . وجريمة مشددة تتمثل في الدخول و البقاء حيث نصت المادة 372 مكرر 1-2-3 على أن تضاعف العقوبة إذا ترتب على ذلك تغيير أو حذف في المعطيات أو المنظومة ولقد حدد العقوبة بالحبس من 6 أشهر إلى سنتين و الغرامة من 50.000دج إلى 150.000دج . وكذلك الاعتداء العمدي على المعطيات حيث أنه و استنادا لنص المادة 372 مكرر 1 فالعقوبة المقررة للإعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من شهرين إلى 3 سنوات أو بغرامة مالية من 1.000.000دج إلى 5.000.000 دج .[2]

[1] بعرة سعيدة ، المرجع سابق ، ص95 .

[2] أنظر المادة372 مكرر 1-2-3 من قانون الإجراءات الجزائية.

من خلال نص المادة 372 مكرر نجد أنه إضافة إلى العقوبات الأصلية توجد مجموعة من العقوبات التكميلية و هي كالتالي:

–المصادرة : يقصد بها مصادرة الأجهزة و البرامج و الوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام و ذلك لبيعها أو حجزها مع مراعات حقوق الغير .

– الغلق : يقصد المشرع بها موقع الأنترنت أو الموقع الالكتروني الذي يعتبر وسيلة لارتكاب الجرائم أو تساعد في ارتكابها.

–إغلاق المحل أو مكان الإستغلال:يشترط فيه توفر عنصر العلم بمعنى إذا ارتكبت الجريمة بعلم صاحبه أو مشاركا فيه أو لم يقم بالإخبار عنه أو بمنعه فتكون عقوبته بإغلاق المقهى الإلكتروني.

2/ **العقوبات المقررة للشخص المعنوي** : جاء في أحكام المادة 12 من الاتفاقية الدولية للاجرام المعلوماتي أن عقوبة الشخص المعنوي تتأسس على مبدأ المسائلة بمعنى يسأل الشخص المعنوي عن هذه الجرائم سواء كان فاعلا أصليا أو شريكا أو متدخلا ،كما يسأل عن الجريمة التامة أو الشروع فيها شريطة أن تكون الجريمة لمصلحة الشخص المعنوي أو كانت بواسطة أحد أعضائه أو ممثليه ويكون منصوب عليها قانونا.أما فيما يخص المشرع الجزائري فقد نظم عقوبة الشخص المعنوي من خلال التعديل الأخير لقانون العقوبات وذلك من خلال نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص :

* الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب الجريمة.

* واحدة أو أكثر من العقوبات الاتية:

- حل الشخص المعنوي .
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 13 سنوات .
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 13 سنوات .

– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية مباشرة أو غير مباشرة لمدة لا تتجاوز 13 سنوات .

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

– نشر أو تعليق حكم الإدانة .

– الوضع تحت الحراسة القضائية لمدة لا تتجاوز 13 سنوات.

نصت المادة 394 مكرر 4 [1]من قانون العقوبات على الغرامة المالية المطبقة على الشخص المعنوي،يعاقب الشخص المعنوي الذي يرتكب أحد الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

المبحث الثاني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري:

رغبة من المشرع الجزائري في التصدي لظاهرة الاجرام الالكتروني وما يصاحبها من أضرار معتبرة على الافراد وعلى مؤسسات الدولة من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى ، عمد منذ الالفية الثانية الى تعديل العديد من القوانين الوطنية بمافيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الاجرامية في مجال تكنولوجية الاعلام و الاتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية، ومع هذا فيبقى السؤال مطروح حول مدى فاعلية و فعالية هذه القوانين في مواجهة الجرائم الالكترونية .

المطلب الاول: مكافحة الجريمة الالكترونية وفقا للقوانين العامة :

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الالكترونية، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الالكترونية .

[1] أنظر المادة 372 مكرر2 من قانون الإجراءات الجزائية.

الفرع الأول : مكافحة الجريمة الالكترونية بموجب قانون العقوبات الجزائري :

لقد تطرق المشرع الجزائري إلى تجريم الافعال الماسة بأنظمة الحاسب الالي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الاجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04- 15المؤرخ في 10نوفمبر 2004 المتمم لأمر رقم 22 -15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر الى المادة 394 مكرر 7 [1] . وبغرض تدارك الفراغ القانوني ، فقد قام المشرع الجزائري بموجب القانون رقم 04-15 بإستحدث جملة من النصوص والتي جرم من خلالها الافعال المتصلة بالمعالجة الالية للمعطيات،وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع الجزائري بسن جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الافعال الماسة بنظم المعالجة الالية للمعطيات وما يقابلها من جزاء أو عقوبة و إلى جانب ذلك فقد قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة للجرائم الالكترونية و ذلك من خلال تعديل قانون الاجراءات الجزائية بموجب قانون رقم 06-22 [2]. إذ نصت المادة 394 مكرر بمايلي : "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك"، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة «تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000إلى 150000دج »، وذلك مهما كانت طبيعة المعلوماتية لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض

[1] فضيلة عاقلي، المرجع سابق ، ص 127 .

[2] براهيمي جمال ،" *مكافحة الجريمة الالكترونية في التشريع الجزائري* " ، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد 2 , الصادرة في 15/11/2016 , ص ص 124-125 .

صور الحياة الخاصة، ونصت المادة 394 مكرر 2 على أنه:« يعاقب ...كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

2- حيازة أو إفشاء أو نشر أو استعمال ألي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.»

وتضيف المادة 394 مكرر6 أنه بالاضافة إلى العقوبات الاصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية: »يحكم بمصادرة الاجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون مجال لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو المكان إذا كانت الجريمة قد إرتكبت بعلم مالكها»

الفرع الثاني : مكافحة الجريمة الالكترونية بموجب قانون الاجراءات الجزائية الجزائرية:

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الاجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة و إستجواب المتهم والضبط والتسرب والشهادة والخبرة [1]. نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية في المادة 37 قانون الاجراءات الجزائية، ونص على التفتيش في المادة 45 الفقرة 7 من نفس القانون المعدلة حيث إعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الاجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من اجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الاحكام الواردة في المادة 44 من قانون الاجراءات الجزائية إذا تعلق الامر بالجرائم الالكترونية، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على إعتراض المراسلات وتسجيل الاصوات وإلتقاط الصور من المادة 65 مكرر5 .

[1] فضيلة عاقلي، المرجع سابق ، ص 130 .

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للاجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية،والتي من شأنها أن تتفادى وقوع الجريمة الالكترونية أو على الاقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06 -22 المعدل لقانون الاجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها والتسرب.

المطلب الثاني : مكافحة الجريمة الالكترونية بموجب القوانين والهياكل الخاصة :

سعى المشرع الجزائري إلى العمل من أجل وضع أليات و هياكل في سبيل التصدي للجرائم الالكترونية وقد تم تجسيد ذلك ميدانيا من خلال سن قوانين و إنشاء هياكل متخصصة سنقوم بتوضيحها فيمايلي :

الفرع الاول : مكافحة الجرائم الالكترونية بموجب القوانين الخاصة :

أولا: القانون الخاص بحماية حق المؤلف والحقوق المجاورة: يرى معظم الفقه أن "الموقع الالكتروني مصنف متعدد الاغراض"، يتم إستخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الانترنت، أو كإسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو... 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 إسم الموقع يحضى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه، و المصنف من حيث المفهوم لا ينصرف فقط إلى المادة الملموسة في الخطوط والتماثيل أو اللوحات الزيتية وإنما هي الفكرة المدرجة في المحل الملموس وهي جوهر الابداع الادبي أو الفني لانها الاساس الذي يقوم عليه المصنف، وقياسا لذلك على موضوعنا تصبح مواقع الانترنت الوسيلة المستخدمة لعرض المصنفات على الجمهور، وبهذه الصورة فإن

حماية مواقع الانترنت التي تستغل مصنفا أدبيا أو فنيا على شبكة الانترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الادبي 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 [1].

ثانيا :قانون البريد والإتصالات اللاسلكية: بإستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات، لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة إجراء التحويلات المالية عن الطريق الالكتروني، ذلك ما نصت عليه المادة 4/46 منه، كما نصت المادة 60 منه على إستعمال حوالات دفع عادية أو إلكترونية أو برقية، بينما أتت المادة 165 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات [2].

ثالثا : القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم إتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر،وهي كالتالي:

1- **مراقبة الإتصالات الالكترونية:** لقد نصت المادة 04 من القانون 09-04 على أربع حالات التي يجوز فيها لسلطات الامن القيام بمراقبة المراسلات و الإتصالات الالكترونية،وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية و هي :

---

[1] حسين نوارة،" *آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا*" ، الملتقى الوطني ''اليات مكافحة الجرائم الإلكترونية في التشريع الجزائري''، الجزائر، 29مارس 2017 ، ص ص 120-121 .

[2] قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 15 ماي سنة 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

– للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب و جرائم ضد أمن الدولة.

– عندما تتوفر معلومات عن احتمال وقوع إعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام .

– لضرورة التحقيقات و المعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية .

– في أطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

2– إقحام مزودي خدمات الإتصالات الإلكترونية في مسار الوقاية من الجرائم المعلوماتية:

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10 ،11 ، 12بالشكل التالي:

–الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات و التحقيق.

– الإلتزام بحفظ المعطيات المتعلقة بحركة السير و كل المعلومات التي من شانها أن تساهم في الكشف عن الجرائم ومرتكبيها،وهذين الإلتزامين موجهين لكل مقدمي خدمات الإتصالات الإلكترونية دون إستثناء .

–الالتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون،وتخزينها أوجعل الوصول إليها غير ممكن.

–الإلتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والأداب العامة مع إخطار المشتركين لديهم بوجودها .

تبنى المشرع في القانون رقم 09-04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام والإتصال تتلخص فيمايلي :

–السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها و المعطيات المعلوماتية المخزنة فيها و إستنساخها.

-إمكانية الإستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني.

-توسيع دائرة إختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام والإتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية و الدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.

- السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام و الإتصال عبر الوطنية ومرتكبيها[1].

رابعا : قانون التأمينات : قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له إجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93 مكرر 2[2] .

الفرع الثاني : مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة :

أولا :الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال: في إطار قمع هذا النوع من الجرائم أنشأ المشرع على مستوى محكمة مقر مجلس قضاء الجزائر، قطبا جزائيا متخصصا في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، وبالنظر إلى أهمية الوقاية والمكافحة من هذه الجرائم، حدا المشرع حذو باقي التشريعات المقارنة و كان لزاما عليه

[1] براهيمي جمال ، المرجع السابق , ص ص 151-154 .

[2] قانون رقم 08 - 01 مؤرّخ في 15 محرّم عام 1429 الموافق 23 يناير سنة 2008 يتمّم القانون رقم 83 - 11 المؤرخ في23 رمضان عام 1403 الموافق 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية ، ج.ر ، عدد 04 ، 27 جانفي 2008 .

البحث على هيئات متخصصة تقوم بمساعدة الدولة وتنتهج المنهج الوقائي، وقد لجأ المشرع إلى فكرة السلطات الإدارية [1]،حيث نص في المادة 13 من القانون رقم 04/09 على أنه: **"تنشأ هيئة وطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم "** ، وقد صدر التنظيم في 2019 حيث نص على أنه "تنشأ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجات الإعلام والاتصال 5 ، ونص كذلك على أن: **" الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي توضع تحت سلطة وزارة الدفاع الوطني"**، وقد خول المشرع لهذه الهيئة اختصاصا بمهمة المراقبة الوقائية للاتصالات في إطار الوقاية من الجرائم الموصوفة بالأعمال الإرهابية والاعتداء على أمن الدولة و يلاحظ أن المشرع خصّ الهيئة بالتحري في الجرائم التي تمس أمن الدولة عموما كالجرائم الإرهابية والتجسس والخيانة العظمى باستعمال وسائط إلكترونية بمعنى كل جريمة متعلقة بالأمن الوطني ومقومات الدولة الجزائرية. [2]

–تنظيم الهيئة : لكي تقوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بدورها على أكمل وجه وتحقق الفعالية المطلوبة، لابد أن تتكون من جهاز إداري تنفيذي من أجل نجاعة و فعالية الهيئة الوطنية في أداء الاختصاصات المنوطة بها، حيث منحها القانون مجموعة من الوسائل القانونية التي تضمن تأدية مهامها حيث نص المشرع بأن الهيئة تتكون من مجلس توجيه و مديرية عامة حيث يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله وتتشكل من الوزارات الآتية :

- وزارة الدفاع الوطني. وزارة العدل.
- الوزارة المكلفة بالداخلية.

[1] عمار حشمان ، المرجع السابق ، ص32 .

[2] سهيلة بوزبرة ،" *الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال*" ، المجلة النقدية للقانون والعلوم السياسية ،كلية الحقوق و العلوم السياسية ، جامعة تيزي وزو ، المجلد 17 ، العدد 2 ، 2022 ، ص ص 569-570 .

– الوزارة المكلفة بالمواصلات السلكية واللاسلكية.[1]

غير أنه وما يجب التأكيد عليه أن مثل هذه الهيئات لا تعمل بمعزل عن الأهداف الحكومية الكبرى أو خارج السياسة العامة للدولة ، لأن الهدف من إنشائها هو تحقيق سياسة الدولة في المجالات المعنية لذلك، ومن أجل إنجاح هذه المهمة تعمد الدولة إلى منح هذه الهيئات نوعا من الاستقلالية كقوة دفع لها، بغية إتاحة الفرصة لها للعمل بنجاعة كما تزود الهيئة بأمانة عامة توضع تحت سلطة وزارة الدفاع الوطني ، ويكلف مجلس التوجيه على الخصوص بما يأتي:

– التداول حول استراتيجية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– الموافقة على عمل الهيئة.

– دراسة التقرير السنوي للهيئة.

–إبداء رأيه في كل مسألة تتصل بمهام الهيئة

– المساهمة في ضبط المعايير القانونية في مجال اختصاصه.

– دراسة مشروع الهيئة.

وقد نص المشرع على أن سير مجلس التوجيه تحدد بموجب قرار من وزير الدفاع.

[1] مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

–مهام الهيئة: من خلال إسمها فإن للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها:

1/ الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الاعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات[1] .

2/ مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ِ المتصلة بتكنولوجيات الإعلام والاتصال.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتحديد مكان تواجدهم.[2]

ثانيا : المعهد الوطني للأدلة الجنائية على الاجرام: يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم املساعدات التقنية، ودائرة الاعلام الالي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[3] .

ثالثا : الهيئات القضائية الجزائية المتخصصة: إن السلطة القضائية تخوض في قضايا الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، لاسيما بعد اللجوء الواسع والمتزايد الى الشبكات الرقمية في

---

[1] أحمد مسعود مريم ،" *آليات مكافحة جرائم تكنولوجيات الإعلام و الاتصال في ضوء القانون رقم 04/09* " ، رسالة ماجستير ، جامعة قاصدي مرباح ، ورقلة ، 2013 ، ص45 .

[2] المرجع نفسه ، ص 46 .

[3] هواري عياش، *" مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية* "،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق ، 2016 ، ص 3 .

حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى مطلوبة لمعالجة فعالة في هذه المواد التي تحتاج المجال العقابي.

ومنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية من أجل هذا تم دمج مادة " الجريمة المعلوماتية " في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء ، العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الاعلام والاتصال منظمة بالخارج لصالح القضاة واطارات وزارة العدل في إطار التعاون الثنائي، ومنها: التعاون الجزائري الفرنسي، الجزائري البلجيكي، والجزائري الأمريكي ولا شك أن تخصص القضاة هو من السمات الحديثة البارزة للتنظيم القضائي الجزائري[1] ، ونظرا لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها: مؤتمر روما سنة 1958، مؤتمر نيس سنة 1972 ،مؤتمر ريو دي جانيرو لسنة 1978، وقد أكدت هذه المؤتمرات أن التخصص في مجال القضاءّ له أهمية كبيرة و دور فعال في رفع مستوى العمل القضائي، ولنظام التخصص جانبين هما : تخصص القضاة، وتخصيص جهات القضاء

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص [2]، وما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية (ق.إ.ج) على أنَّه يجوز تمديد دائرة الإختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، كما نصت المادة 40 مكرر من ق إج على أنَّه " تُطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق

[1] سالم عبد الرزاق ، "*ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية*" ، بمحكمة سيدي محمد ، ص ص 12-14 .

[2] المرجع نفسه ، ص ص 15-18.

والمحاكمة أمام الجهات القضائية التي يتم توسيع إختصاصها المحلي طبقا للمواد 40 ، 37، 329 . من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه" .

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنَّه جعل المشرع الجزائري يختار أسلوب الأقطاب القضائية، فيتجنب إنشاء هيئات قضائية جديدة لكنّه يوسع من دائرة الإختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها إختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن إختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أنَّ التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية , هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسوم التنفيذي رقم 06/ 348 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق (جريدة رسمية رقم: 63) في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم ربع الخاص بالصرف، ولأنَّ الجريمة المنظمة متنوعة و تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة وتُرتكب من طرف عدة أفراد يتصرفون بطريقة منظمة، تعدُّ الجرائم الإلكترونية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الإختصاص القضائي في إطار الإهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة.

خلاصة الفصل الثاني:

نظرا للخصوصيات التي تتميز بها جرائم المساس بالأنظمة المعلوماتية او المعالجة الالية للمعطيات او الجريمة الإلكترونية وتطورها السريع والمستمر، جعل من الدول ومنها الجزائر تعمل على وضع الية قانونية جديدة للحد من خطورة هذه الجريمة على المجتمع ككل من خلال تمديد الاختصاص المحلي لبعض المحاكم لقضاة التحقيق ووكلاء الجمهورية وإنشاء هيكل قضائي جديد يعرف بالقطب الجزائي المتخصص ، تم استعراض كيفية سير وتنظيم هذا الهيكل بالإضافة الى قواعد اختصاص الأقطاب الجزئية المتخصصة النوعي فهي تختص في نوع معين من الجرائم محددة على سبيل الحصر متمثلة في الجريمة الإلكترونية من خلال نص المادة 37 ق.إ.ج.ج . وكذا توسيع اختصاصها المحلي ليشمل بعض المجالس القضائية وحددها في أربعة اقطاب فقط. وهران، قسنطينة، الجزائر، ورقلة. بالإضافة الى عرض القواعد الإجرائية لتسييرها والدور الأساسي الذي يلعبه النائب العام هذا فيما يخص بالجهود الداخلية، اما بالنسبة للجهود الدولية فقد عمدت جميع الدول والهيئات الى الحد او التقليص من خطورة الاجرام المعلوماتي وتأثيره على العام للدول والمؤسسات، وكذا الأشخاص مما دفعها الى محاولة وضع أطراف قانونية من اجل مجابهة الجريمة الإلكترونية ومكافحتها سواء على المستوى الدولي المتمثل في الاتفاقيات الدولية خاصة اتفاقية بودابست 2001 وكذا الاتفاقية المتعلقة بحماية الملكية الفكرية بيرس، بيرن، الويبو.

خاتمـــــــــــة

خاتمة :

في ختام هذه الدراسة المتعلقة بالجريمة الإلكترونية يمكن إستخلاص أن هذه الجريمة تتميز بإختلاف تعاريفها بين مضيق و موسع لمفهومها و بين ماهو تقني و فني وكذا تطورها وإرهاقها للمجتمعات الحديثة ولذلك تصدت الأنظمة بتشريعاتها لبيان ماهيتها وطبيعتها ونطاقها .

تتشكل هذه الجريمة من الأركان الثلاثة المعروفة للجرائم التقليدية لكن هذه الأركان تتميز بخصوصيات تميزها عن الجريمة التقليدية .

جرم هذا النوع من السلوكات في مختلف قوانين العقوبات وفي القوانين الخاصة ، كما تم بيان اجراءات مكافحتها ومتابعتها في قوانين الإجراءات الجزائية .

النتائج :

ومن خلال هذا البحث توصلنا إلى جملة من النتائج :

– حداثة هذا السلوك الإجرامي والذي يتجسد في الجريمة الإلكترونية ، حيث لم يوجد لحد الآن إجماع فقهي موحد على تعريفها مما أدى بالقول أن جريمة الإلكترونية تقاوم التعريف.

– رغم تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الإعتداءات الواردة على منتوجات الإعلام الآلي إلا أنه لم يستحدث نصا خاصا بالتزوير المعلوماتي .

ـــ تم إنشاء أقطاب خاصة للجريمة الإلكترونية في حين لم يخصص قانون خاص لها من طرف المشرع الجزائري .

– يكون التفتيش على المكونات المادية للحاسب الألي.

– المعاينة في الجريمة الإلكترونية تتم على مسرحين : المسرح التقليدي و المسرح الإفتراضي .

– مراقبة الاتصالات الالكترونية وكذا حفظ المعطيات وهي اجراءات جاء بها قانون 04-09.

– متابعة المجرم المعلوماتي أمام الأقطاب الجزائية المتخصصة .

وقد لاحظنا في نهاية عرضنا هذا الموضوع أنه من الموضوعات الصعبة والمتشعبة خاصة فيما يتعلق بالجانب الإجرائي ولعل أهم المشكلات التي واجهتنا في إعداد بحثنا هذا . وبالرغم من وجود نصوص قانونية لمكافحة الجريمة الإلكترونية حبيسة العوائق الإجرائية في مجال المتابعة و أول إشكال أو عائق هو غياب القدرات التأهيلية والوسائل الفنية التي تنتج سرعة إدراك ما حصل و غياب التأهيل قد يؤدي إلى إتلاف الدليل وإفلات مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة الإلكترونية عابرة للحدود .

التوصيات: انطلاقا مما توصلنا إليه من دراسة هذا الموضوع، وكذا النتائج المتوصل إليها يمكن اقتراح جملة من التوصيات :

- على المشرع استحداث تعريف قانوني خاص لهذا النوع المستجد من الجرائم، نظرا لازدياد خطورته، الأمر الذي يستوجب إضفاء تعريف يبين نوعية الجريمة لعدم الوقوع في الخطأ خاصة من ناحية التكييف.
- على المشرع أن يقوم بتطوير بنيته التشريعية تماشيا مع التطور السريع والملحوظ لهذه الجريمة .
- ضرورة تكوين قضاة التحقيق في مجال الجرائم الإلكترونية في معاهد متخصصة.
- انشاء أقسام متخصصة على مستوى كل المجالس القضائية .
- الإسراع في سن قواعد إجرائية خاصة تتلائم مع طبيعة الجريمة الإلكترونية حتى تكون أكثر فاعليه .
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم وذلك بعقد دورات تكوينية بشكل دائم .
- تدريس الأنظمة المعلوماتية والجرائم التي تقع عليها في كليات الحقوق و المعاهد وتفعيل دور الأسرة في متابعة أبنائهم لوقايتهم من الأثار السلبية للإستخدام السيئ لشبكة الأنترنت.

قائمة المصادر و المراجع

قائمة المصادر و المراجع :

قائمة المصادر :

النصوص القانونية :

1- القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية (الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004).

2- القانون رقم 04 - 15 المؤرخ في 10 نوفمبر ،2004(ج.ر71 ص11. و12)،القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن المواد من 394 مكرر إلى المادة 394 مكرر 7 .

3- قانون رقم 08 - 01 مؤرّخ في 15 محرّم عام 1429 الموافق 23 يناير سنة 2008 يتمّم القانون رقم 83 - 11 المؤرخ في23 رمضان عام 1403 الموافق 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية ، ج.ر ، عدد 04 ، 27 جانفي 2008 .

4- القانون 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

5- قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 15 ماي سنة 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية .

6- الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية .

7- مرسوم رئاسي رقم 261-15 مؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

8- مرسوم تنفيذي رقم 06 - 348 مؤرّخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006،الجريدة الرسمية عدد 63، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق .

قائمة المراجع :

المؤلفات (الكتب) :

1- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط18 ، 2019

2- احمد شوقي الشلقاني .مبادئ الاجراءات الجزائة الجزائري الجزء الثاني.ط 05. ديوان المطبوعات الجامعية الجزائر.

3- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2008 .

4- خالد حسن أحمد لطفي , الدليل الرقمي و دوره في اثبات الجريمة المعلوماتية , دار الفكر الجامعي , الاسكندرية , 2019 .

5- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية ، الإسكندرية ، 2008.

6- خثير مسعود ، الحماية الجنائية لبرامج الكمبيوتر ، دار الهدى ، عين مليلة ، الجزائر ، 2010 .

7- شوقي يعيش تمام , الجريمة المعلوماتية دراسة تأصيلية مقارنة , مخبر أثر الاجتهاد القضائي على حركة التشريع , جامعة محمد خيضر , بسكرة , جانفي 2019 .

8- عادل عزام سقف الحيط ، جرائم الذم و القدح و التحقير المرتكبة عبر الوسائط الالكترونية ، دار الثقافة للنشر و التوزيع ، الطبعة الثانية ، 2015 .

9- عبد العال الديربي و محمد صادق اسماعيل، الجرائم الالكترونية-دراسة قانونية قضائية مقارنة، المركز القومي للاصدارات القانونية القاهرة، مصر، ط1 ،2012 .

10- عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر و الأنترنت ، دار الكتب القانونية ، مصر ، 2007 .

11- علي جبار الحسيناوي , جرائم الحاسوب و الانترنت , دار اليازوري العلمية للنشر والتوزيع , 2018 .

12- عمرو عيسى الفقي ، الجرائم المعلوماتية ، المكتب الجامعي الحديث ، الإسكندرية ، مصر ، 2006 .

13- محمد هماج مرهج الهيتي ,جرائم الحاسوب , ط 1, دار المناهج للنشر والتوزيع , الاسكندرية , 2012 .

14- مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، 2008 .

15- نائلة عادل محمد فؤاد قورة ، " *جرائم الحاسب الآلي الاقتصادية* " ، ط1 ، سوريا ، منشورات الحلبي الحقوقية ، 2005م .

16- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة ، عمان ، الأردن ، 2008 .

17- يزيد بوحليط , الجرائم الالكترونية و الوقاية منها في القانون الجزائري , دار الجامعة الجديدة , الاسكندرية , 2019 .

المقالات والمجلات:

1- أسامة حسين محي الدين عبد العال , جرائم الحاسب الألي دراسة تحليلية , مجلة العلوم القانونية و الاقتصادية(JELC), المجلد 55، العدد 2، جويلية 2013 .

2- إسمهان بوضياف , الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر, مجلة الاستاذ الباحث للدراسات القانونية والسياسية, العدد 11 ، سبتمبر 2018 .

3- اسمهان عون , اركان جريمة الاتلاف المعلوماتي وعقوباتها دراسةمقارنة, مجلة الدراسات الافريقية وحوض النيل, المجلد 04 ، العدد 13 ، أكتوبر2021م .

4- حسن بن احمد الشهري , قانون دولي موحد لمكافحة الجرائم الالكترونية , المجلة العربية للدراسات الامنية والتدريب ، المجلد 27 ، العدد 53 ، 2011 .

5- راضية عيمور , الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري , المجلة الاكاديمية للبحوث القانونية والسياسية , المجلد 06 ، العدد 01 ، 2022 .

6- سفيان حديدان ،الدخول أو البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات ،مجلة الاستاذ الباحث للدراسات القانونية والسياسية ،مجلد 02 ، العدد 08 ،قالمة،الجزائر، ديسمبر2017 .

7- عادل يوسف عبد النبي الشكري ، الجريمة المعلوماتية وأزمة الشرعية الجزائية , مجلة مركز دراسات الكوفة , العراق, المجلد 05 ، العدد 07 ، 2008 .

8- عطاءالله فشار , مواجهة الجريمة المعلوماتية في التشريع الجزائري , جامع الكتب الإسلامية ، المجلد 1 ، 2009 .

9- محمد خليفة , خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها , مجلة دراسات و ابحاث , كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009 .

10- مولاي براهيم عبد الحكيم , الجرائم الالكترونية , مجلة الحقوق والعلوم الانسانية, العدد 23 ، 2015 .

المداخلات و الملتقيات :

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

2- فضيلة عاقلي ,الجريمة الالكترونية و اجراءات مواجهتها من خلال التشريع الجزائري ، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية , مركز جيل البحث العلمي ,طرابلس ، 2017 .

3- محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية ، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة، 29 مارس ،2017 .

4- مختارية بوزيدي ،ماهية الجريمة الالكترونية , الملتقى الوطني اليات مكافحة الجرائم الالكترونية في التشريع الجزائري , مركز جيل البحث العلمي , 2017 .

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

6- يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل .2006 .

الرسائل العلمية :

2- برا هيمي جمال , التحقيق الجنائي في الجرائم الالكترونية , أطروحة دكتوراه , جامعة مولود معمري تيزي وزو , 2018 .

8- عزيزة رباحي ، الأسرار المعلوماتية ،وحمايتها الجزائية ، أطروحة دكتوراه ،كلية الحقوق والعلوم السياسية ،جامعة أبوبكر بلقايد ،تلمسان ،الجزائر ، -2017 2018 .

1- إيمان مكري , الجريمة الالكترونية في التشريع الجزائري , ماجستير , كلية علوم الاعلام و الاتصال , جامعة الجزائر 3 , 2015 .

3- بوخبزة عائشة , الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري , مذكرة ماجستير في القانون الجنائي , كلية الحقوق , جامعة وهران , الجزائر .

4- سفيان سوير ، "*جرائم المعلوماتية* " ، رسالة ماجستير ،كلية الحقوق و العلوم السياسية ، جامعة أبو بكر بلقايد، تلمسان ،2011/2010 .

5- صغير يوسف , الجريمة المرتكبة عبر الانترنت , ماجستير , جامعة مولود معمري , تيزي وزو , 2013 .

6- طرشي نورة , مكافحة الجريمة المعلوماتية , ماجيستير , كلية الحقوق , جامعة الجزائر 1 ، 2012

7- عائشة بن قارة , حجية الدليل الالكتروني في مجال الاثبات الجنائي , رسالة ماجستير , جامعة الاسكندرية , مصر ,2009 .

9- فتيحة رصاع , الحماية الجنائية للمعلومات على شبكة الأنترنت , ماجيستير, جامعة أبي بكر بلقايد , تلمسان , 2012.

10- محمد بن أحمد بن محمد آل مكدي , السرقة المعلوماتية عقوبتها وطرق الوقاية منها , رسالة ماجستير , جامعة الملك خالد , المملكة العربية السعودية , 2009-2010 .

11- ياسين بوعروة , جريمة التزوير المعلوماتي , مذكرة ماستر , كلية الحقوق و العلوم السياسية , جامعة العربي بن امهيدي , ام البواقي , 2013-2014 .

الاتفاقيات الدولية:

1- اتفاقية بودابست المؤرخة في 23 نوفمبر 2001.

2- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ، وافق عليها مجلسا وزراء الداخلية و العدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21-12-2010 .

فهرس المحتويات

العنوان	الصفحة
مقدمة	1
الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية	
المبحث الأول: ماهية الجريمة الإلكترونية	6
المطلب الاول: مفهوم الجريمة الإلكترونية	6
الفرع الأول : تعريف الفقه للجريمة الإلكترونية	7
الفرع الثاني: موقف المشرع الجزائري	11
المطلب الثاني: خصائص و أركان الجريمة الإلكترونية	14
الفرع الأول: خصائص الجريمة الإلكترونية	14
الفرع الثاني: أركان الجريمة الإلكترونية	22
المبحث الثاني: أنواع الجرائم الالكترونية و صورها	25
المطلب الأول : أنواع الجرائم الالكترونية في التشريع الجزائري	25
الفرع الأول: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي	26
الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي	28
المطلب الثاني : صور الجرائم الالكترونية	31
الفرع الأول : الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	32
الفرع الثاني:جرائم الاعتداء على الحياة الخاصة للاشخاص	37
الفرع الثالث : جرائم الاعتداء على بالأموال	42
الفرع الرابع : الجرائم الماسة بأمن الدولة	46
الفصل الثاني : إجراءات المتابعة و أساليب المكافحة	
المبحث الأول : إجراءات متابعة الجريمة الإلكترونية و العقوبات المقررة لها	53
المطلب الأول : اجراءات البحث و التحري في سبيل متابعة الجرائم الالكترونية	53
الفرع الأول: الاجراءات العامة لمتابعة الجريمة الإلكترونية	53

الفرع الثاني : الاجراءات الخاصة لمتابعة الجريمة الإلكترونية	67
المطلب الثاني : مباشرة التحقيق و المحاكمة	75
الفرع الأول : مرحلة التحقيق	76
الفرع الثاني : مـرحلـة المحـاكمـة	81
المبحث الثاني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري	86
المطلب الاول: مكافحة الجريمة الالكترونية وفقا للقوانين العامة	86
الفرع الاول: مكافحة الجريمة الالكترونية بموجب قانون العقوبات الجزائري	87
الفرع الثاني : مكافحة الجريمة الالكترونية بموجب قانون الاجراءات الجزائية	88
المطلب الثاني : مكافحة الجريمة الالكترونية بموجب القوانين والهياكل الخاصة	89
الفرع الاول : مكافحة الجرائم الالكترونية بموجب القوانين الخاصة	89
الفرع الثاني : مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة	92
خـــــــــــــــاتمة	100

الملاحق

ملحق 1 : إذن بالتسرب .

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء .....

محكمة .....

نيابة الجمهورية **إذن بالتـــــــــــسرب**

رقم:....

نحن وكيل الجمهورية لدى محكمة.....

-بعد الاطلاع على التقرير الإخباري رقم:..... المؤرخ في :.....

الصادرة عن :.....

المتعلقة بدخول لنظام المعالجة الآلية للمعطيات الخاص بـ:.....عن طريق الغش

-وبعد الاطلاع على المواد 65 مكرر 11 إلى65 مكرر 18 من ق إ ج .

- ونظرا ولخطورة هذه الوقائع، ولوقف أي اعتداء آخر على المنظومة، واستعمال المعطيات التي يمكن أن تكون قد أخذت بطريقة الغش.

نأذن للسيد:.....(ذكر هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته)

ضابط الشرطة القضائية بـ:.....

بتنسيق عملية التسرب التي تقوم بها احد أعوانه، وتحت مسؤوليته

مع الإذن باستعمال العون المتسرب لآي هوية مستعارة.

نأذن بهذا التسرب لمدة أقصاها 04 أشهر من تاريخ هذا الإذن، مالم نأمر بإيقافها قبل انقضاء هذه المدة .

وعلى ضابط الشرطة القضائية المنسق للعملية موافاتنا بتقرير حول سيرها.

حرر بمكتبنا بتاريخ:.....

وكيل الجمهورية

ملحق 2 : إذن بالتقاط الصور و تسجيل الأصوات .

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء .....

محكمة .....

نيابة الجمهورية **إذن بالتقاط الصور وتسجيل الاصوات**

رقم:...

نحن وكيل الجمهورية لدى محكمة.....

-بعد الاطلاع على التقرير الإخباري رقم:..... المؤرخ في :.....

الصادرة عن :.....

المتعلقة بتخريب اشتغال نظام المعالجة الآلية للمعطيات الخاص بـ:.....

والذي يشتبه أن تكون قد تمت انطلاقا من منزل المسمى .....الكائن بـ .....

-وبعد الاطلاع على المواد 65 مكرر 5 إلى65 مكرر 10 من ق إ ج .

- ونظرا ولخطورة هذه الوقائع، ولمقتضيات التحري في الجريمة والوصول إلى الفاعل.

نأذن للسيد:.....(ذكر هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته)

ضابط الشرطة القضائية بـ:.....

بالقيام بإجراء التقاط الصور وتسجيل الأصوات بمسكن المسمى .....الكائن بـ.....

وتسخير أي عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة لتكفل بالجوانب التقنية للعملية.

نأذن بهذا الإجراء لمدة أقصاها 04 أشهر من تاريخ هذا الإذن، ما لم نأمر بإيقافها قبل انقضاء هذه المدة .

وعلى ضابط الشرطة القضائية المنسق للعملية موافاتنا بتقرير حول سيرها.

حرر بمكتبنا بـتاريخ:.....

وكيل الجمهورية

ملحق 3 : إذن بإعتراض المراسلات .

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء .....

محكمة .....

مكتب السيد:..... **<u>إذن بإعتراض المراسلات</u>**

قاضي التحقيق الغرفة رقم:....

رقم النيابة:.....

رقم التحقيق:......

نحن..... قاضي التحقيق الغرفة ..... لدى محكمة.....

-بعد الاطلاع على ملف القضية المتبعة ضد:.....

من اجل جنحة:الاشتراك في مجموعة تألفت بغرض تصميم معطيات موجهة لارتكاب جرم الدخول في نظام للمعالجة الآلية للمعطيات،طبقا للمادتين 394 مكرر1/2 و 394 مكرر 5 من قانون العقوبات.

-وبعد الاطلاع على المواد 65 مكرر 5 إلى65 مكرر 10 من ق إ ج .

-وحيث وأن التحقيق أسفر على أن المسمى ..... على علاقة مع المسمى .....، وإنهما يخططان لتخريب نظام المعالجة الآلية للمعطيات الخاصة بـ.....

ونظرا لمقتضيات التحقيق، ولخطورة الوقائع، ولإظهار الحقيقة، وتفادي أي نتائج خطيرة.

نأذن للسيد:.....ضابط الشرطة القضائية:.....

بالقيام باعتراض المراسلات السلكية واللاسلكية التي تتم بين.....و.....

وتسخير أي عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة لتكفل بالجوانب التقنية للعملية.

نأذن بهذا الإجراء لمدة أقصاها 04 أشهر من تاريخ هذا الإذن، ما لم نأمر بإيقافها قبل انقضاء هذه المدة .

وعلى ضابط الشرطة القضائية المنسق للعملية موافاتنا بتقرير حول سيرها.

حرر بمكتبنا بـتاريخ:.....

قاضي التحقيق

الملخص

ملخص :

صحيح أن الجريمة الإلكترونية قد مرت بتطورات تاريخية وطفرات تكنولوجية ، وهذا جعل من الصعب على التشريعات إيجاد تعريف موحد لها. وفعلاً تختلف تعريفاتها من التعريفات الواسعة إلى التعريفات الضيقة. ومع ذلك، فقد قامت التشريعات بتبني مفاهيم وتعاريف للجريمة الإلكترونية وتطوير آليات مكافحتها.

فيما يتعلق بالتشريع الجزائري، فقد تم التطرق إلى تعريف الجريمة الإلكترونية ووصفها بأنها جريمة المساس بأنظمة المعالجة الآلية للمعطيات. وتتشابه أركان هذه الجريمة مع أركان الجريمة التقليدية المعروفة، حيث يشمل الركن الشرعي وجود تثبت الجريمة، والركن المادي يتعلق بالسلوكات الإجرامية المحددة في القانون، والركن المعنوي يتعلق بالقصد الجنائي لارتكاب هذه الجريمة.

لم يقتصر الأمر على تجريم الأعمال الإلكترونية في التشريعات المقارنة والتشريع الجزائري فقط، بل تم إنشاء جهات خاصة لمتابعة ومكافحة هذه الجريمة. على سبيل المثال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. وتعمل هذه الجهات باستخدام أحدث الأساليب والتقنيات العلمية المتطورة لمكافحة الجريمة الإلكترونية .

وأخيرا نقول إن الجريمة الإلكترونية مهما تمت مكافحتها فهي تتطور بتطور وسائل التكنولوجيا.

الكلمات المفتاحية : 1/الجريمة الإلكترونية ، /2الحماية القانونية ، /3النظام المعلوماتي ، 4/تكنولوجيا الإعلام و الإتصال ، /5المعالجة الألية للمعطيات ، /6التشريع الجزائري .

Summary:

It is true that cybercrime has undergone historical developments and technological advancements, making it challenging for legislations to find a unified definition. Indeed, definitions of cybercrime vary from broad to narrow. However, legislations have adopted concepts and definitions for cybercrime and developed mechanisms to combat it.

Regarding Algerian legislation, the definition of cybercrime has been addressed as a crime that interferes with data processing systems. The elements of this crime resemble those of traditional known crimes, including the legal element of proving the crime, the material element concerning specific criminal acts defined by the law, and the moral element relating to the criminal intent to commit this crime.

The criminalization of electronic acts is not limited to comparative legislations and Algerian legislation alone, as specialized entities have been established to monitor and combat this crime. For example, the National Authority for the Prevention of Crimes Related to Information and Communication Technology. These entities work using the latest advanced scientific methods and techniques to combat cybercrime.

Finally, it should be noted that cybercrime continues to evolve with the advancement of technology.

Keywords: 1. Cybercrime, 2. Legal protection, 3. Information system, 4. Information and communication technology, 5. Data processing, 6. Algerian legislation.