جامعة 20 أوت 1955 – سكيكدة
كلية الحقوق والعلوم السياسية
قسم الحقوق

الجرائم الإلكترونية في التشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر تخصص : القانون الجنائي و العلوم الجنائية

من تقديم الطلبة:
* زرزار دنيا
* عبد النوري زينة
* زغيود صورية

تحت إشراف:
د. عبادة سيف الإسلام

لجنة المناقشة

الاسم و اللقب	الرتبة العلمية	الصفة
د/بن طالب أحسن	أستاذ محاضر	رئيسا
د/عبادة سيف الإسلام	أستاذ محاضر	مشرفا و مقررا
أ/ بوقرقور منال	أستاذ مساعد	مناقشا

2022/06/21

قال الله تعالى:

﴿وَلِيَعْلَمَ الَّذِينَ أُوتُوا الْعِلْمَ أَنَّهُ الْحَقُّ مِنْ رَبِّكَ فَيُؤْمِنُوا بِهِ﴾

[الحج الآية 54]

﴿ قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَاۖ إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ﴾

[البقرة الآية 32]

و عن أبي هريرة رضي الله عنه أن رسول الله صلى الله عليه وسلم قال:

﴿ إِذَا مَاتَ الإِنْسَانُ انْقَطَعَ عنْه عَمَلُهُ إِلَّا مِن ثَلَاثَةٍ: إِلَّا مِن صَدَقَةٍ جَارِيَةٍ، أَوْ عِلْمٍ يُنْتَفَعُ بِهِ، أَوْ وَلَدٍ صَالِحٍ يَدْعُو له﴾

رواه مسلم

الإهداء

كن عالما أو متعلما أو مستمعا ولا تكون الرابع فتهلك

ربي إذا أعطيتني نجاحا فلا تأخذ تواضعي، وإذا أعطيتني تواضعا فلا تأخذ اعتزازي بكرامتي

أهدي ثمرة جهدي المتواضع إلى

إلى من قدمت لي آيات الحب والحنان، إلى أعذب كلمة رددها لساني إلى من وضعت الجنة تحت أقدامها الجوهرة الثمينة صاحبة الصدر الدافئ والقلب العطوف رمز الصبر والتضحية **أمي حبيبتي** حفظها الله ورعاها وأطال في عمرها

إلى فرحتي في الحزن وقوتي في الضعف، إلى من تنحني هامتي له خجلا، إلى من زرع في قلبي حب العلم ووضع بين جنباتي القوة والعزيمة وأعطاني لأكون ما أنا عليه الآن، **أبي الغالي** حفظه الله سندا لي

إلى تيجان رأسي ومصدر همتي وفخري، إلى **إخوتي** أنار الله دربهم

إلى من كانت لي عونا ومصدر عطائي، إلى **أختي نهلة** من رعتني صغيرة وصاحبتني كبيرة حفظها الله هيا وجنينها

إلى من صادقتهم فصدقوا، **إلى صديقاتي** ا للاتي لا أعرف للحياة طعمنا بدونهم

إلى كل **من ذكرهم قلبي** ونسيهم قلمي

دنيا

الإهداء

إلى من كانت دعواها دوما تنير لي عقلي ودربي

إلى من أفاضت عليا برعايتها أمي حبيبتي التي أتاحت لي فرصة الدراسة إلى التي تعجز الكلمات عن وصفها مهما سال من سواد الحبر
على بياض الورق
إلى حبيبتي وغاليتي أمي
إلى أبي حبيبي ونور عيني
إلى إخوتي: **شهرزاد، شهيناز، سميرة، أمال** وأخواتي : **محمد، يوسف** سر سعادتي
إلى **زوج أختي أسامة** عبد النوري الذي كان له فضل كبير بما أنا عليه الآن أدعو الله عز وجل أن يحفظه
إلى الأزهار النرجسية التي تزين حقل العائلة **معتز، ميار، ديمة، نبال، عامر، فراس، عبيد، إياد**
إلى من خفق له قلبي **زوجي شمس الدين**
إلى كل صدقاتي **دنيا، عليا، ابتسام، رحمة، وسام، ايمان، نسرين، سميرة، هدى، إكرام**
إلى كل هؤلاء أهديهم ثمرة هذا الجهد الطيب المبارك الذي أحتسبه عند الله عز وجل في صحيفة حسناتي وأتمنى أن يكون من العلم الذي ينتفع به ونرجو من الله القبول

زينة

الإهداء

بسم الله والحمد لله الذي أنار طريقي
أهدي هذا العمل المتواضع إلى نبع الحنان، إلى ملاكي في الحياة إلى **أمي حبيبتي،** حفظها الله وأطال في عمرها وأمدها بالصحة والعافية
إلى **روح أبي** الطاهرة أسكنها الله فسيح جناته
وإلى أخي العزيز محفوظ الذي كان له عظيم الفضل فيما وصلت إليه من نجاح
إلى كل العائلة الكريمة، وإلى كل الأصدقاء

صوريــة

شكر و تقدير

قال تعالى: "لئن شكرتكم لأزيدنكم". (ابراهيم الآية 7)

الحمد لله الذي أعاننا على إنجاز هذا البحث

من فضل الله علينا ومنته وكرمه أن هدانا إلى سبيل الخير والرشاد

وأن يسر لنا طرق لاكتساب من العلم، فله الحمد والشكر.

أتقدم بخالص عبارات الشكر والتقدير وعظيم العرفان للأستاذ الفاضل **عبادة سيف الإسلام**، الذي تكرم وتفضل بالإشراف على عملنا هذا، ولما بدله معنا من جهد، فلقد كان معطاء بعلمه، ومصوبا

بإرشاده وتوجيهه وتعاليمه، كريما بوقته، لم يدخر جهدا ولا نصيحة.

كما يشرفني أن أتقدم بجزيل الشكر والتقدير إلى السادة **الأساتذة أعضاء اللجنة** على قبولهم مناقشة هذا العمل المتواضع، والذين منحوني من وقتهم الثمين، أدامهم الله للعلم ذخرا وللطلالة سندا.

كما أتقدم بشكر خاص إلى **كل أساتذتنا** من كلية الحقوق والعلوم السياسية على دعمهم وعلى كل ما قدموه لنا في مشوارنا الدراسي.

كما نشكر كل من ساعدنا في إنجاز هذه المذكرة من بعيد أو قريب ولو بكلمة طيبة، وبالأخص زميلنا **مراد تيفوتي** حفظه الله.

قائمة المختصرات

ق ع ج: قانون العقوبات الجزائري.
ق إ ج ج: قانون الإجراءات الجزائية.
م: المادة.
ط: طبعة.
د ط: دون طبعة.
د س ن: دون سنة النشر.
د د ن: دون دار النشر.
ج ر: جريدة رسمية.
ع: عدد.
م: مجلد.
ص: صفحة.
ص ص: من صفة إلى صفحة.
ق: قانون.

مقدمة

إن ظاهرة الجريمة من الظواهر التي تعاني منها جل المجتمعات البشرية منذ القدم، وخير مثال على ذلك ثمرة العداوة الأولى بين بني آدم عليه الصلاة والسلام، وذلك بقتل قابيل لأخيه هابيل، فالجريمة هي نتاج طبيعي للحياة الجماعية للإنسان في شتى مجالات الحياة، فبظهور ما يعرف بتكنولوجيا المعلومات التي تعتبر سمة العصر والمقياس الذي يحدد مدى تقدم الشعوب وتغير حياة المجتمعات المتقدمة منها والنامية، فقد أصبحت قطاعات مختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لما تتميز به من سرعة ودقة عالية في تجميع المعلومات وحفظها وتخزينها ومعالجتها وتبادلها بين الأفراد والمجتمعات وبين مختلف الدول أيضا، إلا أن الجانب المشرق والإيجابي لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها التقنية العالية لشبكة الأنترنت، وهذا نتيجة إساءة استخدام الأنظمة المعلوماتية على نحو غير مشروع، حيث أدى هذا التطور إلى ظهور جرائم مستحدثة والتي تم تسميتها بالجريمة الإلكترونية، فقد ظهرت لأول مرة في الدول المتقدمة ذات التكنولوجيا المتطورة ،ثم انتقلت إلى الدول الأخرى، فأصبحت لها خطورة تهدد المجتمع والعالم كونها لم تكن معروفة في القانون الجنائي ولم يشهد لها العالم مثيلا في الجرائم التقليدية .

فالجزائر تعرضت لمثل هذا النوع من التطور التكنولوجي إذن هي معنية بمكافحة هذا النوع من الجرائم بإيجاد إطار قانوني مناسب لسد الفراغ الإجرائي، فقد قام المشرع الجزائري بسن قوانين تتماشى مع التكنولوجيا المتنامية، وذلك بسبب تزايد معدلات هذه الجرائم في السنوات الأخيرة بصورة كبيرة.

فقد أفرزت الجرائم الإلكترونية تحديات واضحة للقوانين التي وضعت لمكافحتها، فقد تغيرت من صورتها المادية إلى المعنوية مما أدى إلى إفلات مرتكبي هذه الجرائم من العقاب، فهي جريمة مستقلة بذاتها، ولكن الصعوبة تكمن في كيفية ملاحقة المجرمين وتقفي آثارهم والوصول إليهم، فلإثبات قيام هذه الجريمة لابد من توافر الدليل بشأنها، ومن المرجح أن تصبح السيطرة على مصادر المعلومات ووسائل معالجتها أكثر أهمية من الموارد الأخرى، ويعد هذا الأمر أحد الأسباب التي تدفع الباحثين إلى إيجاد آليات لمكافحها .

وعلى ضوء ما سبق فقد قمنا باختيار هذا الموضوع لدراستنه في هذه المذكرة نظرا لأهميته البالغة كون أن استغلال التكنولوجيا في ارتكاب الجرائم يعتبر خطر يهدد المجتمعات والعالم أجمع مما يسبب خسائر على المستويات الاقتصادية والاجتماعية و الثقافية و الأمنية، فهي تمس حرمة الحياة الخاصة للأفراد، وتهدد الأمن الوطني وتؤدي إلى فقدان الثقة بالتقنية ، فلا يخفى على أحد مدى أهمية موضوع الجرائم الإلكترونية والحاجة الملحة لدراسته نظرا لأنها جرائم خطيرة، لتنبه المجتمعات لحجم المخاطر وكثرة الخسائر الناجمة عنها، لاسيما إن هذا الموضوع يتسم بالحداثة ويمتد أثره إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال.

كون هذه الجريمة هي جديدة يصعب على المحقق العادي التعامل معها، إذ نجد أن القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها ويرجع ذلك إلى التقنيات والوسائل المستعملة لارتكابها.

إن الغاية المرجوة من هذه الدراسة تتمحور أساسا حول دراسة الموضوع من شتى جوانبه، والتركيز على خصوصية الجرائم الإلكترونية، والوصول إلى أحدث القوانين التي تختص بها، و محاولة سد الفضول المعرفي الذي يلازمنا وإزالة الغموض عليها، والتعرف على أنواعها ، و كذا سمات وخصائص كل من الجريمة و مرتكبيها، و تحديد جهاز التحقيق فيها ، و كذلك طرق التحقيق فيها و استخلاص أدلة الإثبات الجنائي، ودراسة الظاهرة وتحليلها وبيان أساليب مكافحة هذه الجرائم من حيث الإجراءات والأساليب والهيئات مع أحدث التعديلات، ومحاولة إيجاد حلول قانونية لتحقيق التوازن بين مصلحة المجتمع في الاستفادة من المعلوماتية من جهة، وحق الفرد في حماية خصوصيته من جهة أخرى، وتوضيح بعض التشريعات السارية في الجزائر فيما يخص الجرائم الإلكترونية، ومعرفة كيفية التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

ترجع أسباب اختيار الموضوع إلى أسباب ذاتية بالدرجة الأولى والمتمثلة في الإهتمام الشخصي بالبحث في مجال الجرائم الإلكترونية ومكافحتها، وطموح ذاتي في الاطلاع على مجال الجرائم التي تحدث بسبب التكنولوجيا ومعرفة كيفية إثباتها ومحاربتها والقبض على مرتكبيها، وموضوع الجريمة الإلكترونية من أحدث المواضيع والأكثر انتشارا حاليا، وهي لها جانب من الغموض خصوصا في إطار مكافحتها، وهذا ما أعطانا دافع للبحث وحب التعرف عليها كونها متعلقة بالعالم الافتراضي، والتعرف على الدوافع التي تجعل المجرم يرتكبها.

وهناك أسباب علمية أو موضوعية تتمثل في الإهتمام بدراسة الجرائم الإلكترونية وتسليط الضوء على المكانة التي أصبحت تحتلها التكنولوجيا داخل المجتمع الجزائري ، و لأنه موضوع حديث يمس الواقع المعاش و كل القطاعات، وبسبب كثرة الجرائم الإلكترونية التي أصبح يتعرض لها المجتمع الجزائري والعالم ككل نتيجة التطور العلمي والتكنولوجي، والأهمية البالغة لها وما يشملها من إجراءات وآليات البحث والتحري والتحقيق، ومن المواضيع التي تثير جدل فقهي لدى فقهاء القانون الجنائي، وتعلق الموضوع بالوسائل الحديثة أي كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذه الجرائم، و حداثة الموضوع والتزايد المستمر لها، والرغبة في التعمق ومواجهة النشاط الإجرامي الإلكتروني.

وككل موضوع يعنى بالبحث والدراسة نجده لا يخلو من بعض الصعوبات ولعل أبرزها صعوبة الوصول إلى وضع خطة متوازنة ومعالجة وشاملة لموضوع البحث ذلك بالنظر إلى طبيعتها الافتراضية والمزدوجة كون أن لها جانب فني يعتمد على التقنية العالية وجانب قانوني، وكذا تشعب موضوعاتها كونها موضوع واسع يصعب حصره، بالإضافة إلى قلة المصادر التي تعالج الظاهرة من منظور التشريع الجزائري، كون أن أغلب المصادر التي تم العثور عليها تعود لدول عربية أخرى كالقانون المصري، القانون الأردني...إلخ.

إن الجريمة الإلكترونية ولدت نتيجة إساءة استخدام وسائل التكنولوجيا الحديثة التي ظهرت على الساحة في كل دول العالم، ومنها نتطرق إلى طرح الإشكالية التالية:

إلى أي مدى وفق المشرع الجزائري في الحد من ظاهرة الجريمة الإلكترونية؟

وسوف نتبع في دراستنا لهذا الموضوع منهجان الاول المنهج الوصفي و الذي يقوم على وصف الظاهرة وبيان المفاهيم القانونية الخاصة بها ولإبراز وتحديد أنواع الجرائم الإلكترونية وطنيا.

أما الثاني فهو المنهج التحليلي والذي يقوم على تحليل النصوص القانونية ذات الصلة بالموضوع وتبيان المبدأ القانوني التي تقوم عليه، وجمع الحقائق والبيانات ووضعها في البحث، بالإضافة إلى شرح وجهات النظر الفقهية والقانونية المختلفة، وتحليل المفاهيم وشرحها بالتفصيل.

ولمعالجة الإشكالية المطروحة في دراستنا من شتى الجوانب، فقد قسمنا خطة البحث إلى فصلين، في الفصل الأول تطرقنا إلى الأحكام العامة للجريمة الإلكترونية، حيث قسمنا هذا الفصل إلى مبحثين، في المبحث الأول عرضنا فيه الإطار المفاهيمي للجريمة الإلكترونية، بينما في المبحث الثاني عرضنا فيه الإطار الموضوعي للجريمة الإلكترونية، أما في الفصل الثاني فقد تطرقنا إلى آليات مكافحة الجريمة الإلكترونية ، وقد قسمناه أيضا إلى مبحثين، عرضنا في المبحث الأول المواجهة الموضوعية للجريمة الإلكترونية، أما في البحث الثاني فقد عرضنا المواجهة الإجرائية للجريمة الإلكترونية.

الفصل الأول: الأحكام العامة للجريمة الإلكترونية

تعد الجرائم الإلكترونية من أحدث الجرائم التي ظهرت في عصرنا الحديث نظرا لارتباطها بوسائل التقنيات الحديثة من شبكة الأنترنت وأجهزة الكمبيوتر والمواقع الإلكترونية، وذلك نتيجة التطور الهائل الذي شهده عصر العولمة، مما لا شك فيه أن الثورة المعلوماتية و نتيجة التقنيات العالية التي تقوم عليها، والتي تتمثل في استخدام شبكات الأنترنت والحواسيب التي ترتبط بينها لم يمر على العالم بسلام، لأنه بقدر ما أحدث من آثار إيجابية في تغيير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات لاسيما المعاملات الإلكترونية، إلا أنه لا ينفي الانعكاسات السلبية التي أفرزتها التقنية العالية لوسائل التكنولوجيا على حياة الناس ومصالح الدول، فهي تعتبر سلاح ذو حدين من جهة تسهل الحياة البشرية وتقدمها في جميع الميادين خصوصا مع ظهور الطريق السريع للمعلومات "الأنترنت" وما يقدمه من خدمات متميزة وكذلك عالميته، أي عدم الاعتراف بالحدود السياسية وتعديه للدول والأقاليم، ومن جهة أخرى أدت إلى ظهور جرائم لم يكن يعرفها الإنسان.

فقد أصبحت هذه الوسائل محل ارتكاب الجريمة بمفهومها الحديث لتكون عالما من عوالم الجريمة، وتبقى ظاهرة الجريمة المعلوماتية إلى يومنا هذا تشكل حالة من الغموض تجعلهم في كثير من الأحيان عاجزين عن مواجهتها وفهم طبيعتها نظرا لكونها سريعة التطور، ولأجل ذلك لابد من الإلمام بماهية الجريمة الإلكترونية والبحث والتحليل للتوصل إلى طبيعتها الفنية وبالتالي طبيعتها القانونية.

سنتطرق في هذا الفصل إلى دراسة الجريمة الإلكترونية من جانبيها، و على ضوء ذلك سنقسم هذا الفصل إلى مبحثين، في المبحث الأول تناولنا (الإطار المفاهيمي للجريمة الإلكترونية)، وفي المبحث الثاني تناولنا (الإطار الموضوعي للجريمة الإلكترونية)، وهذا ما سنقوم بتفصيل فيه.

المبحث الأول: الإطار المفاهيمي للجريمة الإلكترونية

بالرغم من أهمية الوسائل الإلكترونية إلا أن استخدامها غير المشروع أدى إلى ظهور نوع جديد من الجرائم، فقد انتقل بالجريمة من صورتها التقليدية إلى الإلكترونية قد يصعب التعامل معها، لهذا اعتبرت الجريمة الإلكترونية ما هي إلا امتداد للجرائم التقليدية.

سيتم تقسيم هذا المبحث إلى ثلاث مطالب، حيث سنستعرض في المطلب الأول (مفهوم الجريمة الإلكترونية)، ثم نستعرض في المطلب الثاني (خصائص هذه الجريمة)، وفي الأخير نستعرض (محل الجريمة الإلكترونية) في المطلب الثالث.

المطلب الأول: مفهوم الجريمة الإلكترونية

لقد كان الانتشار الهائل للجرائم المعلوماتية وتشعب موضوعاتها صدى واسع، بحيث مست جميع المجالات وكافة فروع القانون، وشتى المجالات الجنائية مما أدى إلى اختلاف تعريفاتها ومفاهيمها بحسب الزاوية التي تعالجها أو التي ينظر إليها من خلالها، فقد أثيرت العديد من التساؤلات حول تحديد مفهوم الجريمة الإلكترونية، يرجع ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم

فقد ظهرت العديد من الآراء الفقهية لفهم المقصود منها لكونها موضوعا واسعا، كما اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم التقليدية لهذا يتوجب علينا معرفة مفهومها وكذلك الطبيعة القانونية.

سنتناول في هذا المطلب (تعريف الجريمة الإلكترونية) في الفرع الأول، (وطبيعتها القانونية) في الفرع الثاني.

الفرع الأول: تعريف الجريمة الإلكترونية

سنقوم بتعريف الجريمة الإلكترونية لغة، واصطلاحا، وقانونا، مع بيان موقف المشرع الجزائري من الجريمة الإلكترونية.

أولا : تعريف الجريمة الإلكترونية لغة

يتكون مصطلح الجريمة الإلكترونية من شقين وهما الجريمة في شقها الأول والإلكترونية في شقها الثاني وهو ما سنتطرق له في هذا الفرع.

يستعمل مصطلح الجريمة في عدة مواضيع وله في كل موضوع مذ لول خاص به يختلف باختلاف وجهات النظر إليه، يرجع هذا الاختلاف إلى كون أن الجريمة محل الدراسة في مختلف العلوم ولكل علم غرضه في تحديد مضمون ما يعني هذا المصطلح، وما يهمنا هنا هو تعريف الجريمة في شقها القانوني فتعرف على أنها "كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية[1].

أما في ما يخص الشق الثاني والمتمثل في مصطلح الإلكترونية أو المعلوماتية فهناك تشابه بينهما، إلا أنه يعتبر مصطلح الجريمة الإلكترونية أدق وأوسع من الجريمة المعلوماتية لأنه يستخدم لوصف فكرة جزء من الحاسب أو عصر المعلومات، ومن خلال دراستنا وما سنتناوله في تعريفات الفقهاء والدارسين لهذا المصطلح سيتبين الفرق الجلي بينه وبين الجريمة التقليدية.

تعرف المعلوماتية لغة أنها: "المعالجة الآلية للمعلومات وهي ترجمة من اللغة الفرنسية لكلمة informatiqueو تعني تكنولوجيا ومعالجة وإرسال المعلومات بواسطة الكمبيوتر. و المعلوماتية يقصد بها ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بتحصيل معلومات وتجميلها وتنظيمها واختزانها واسترجاعها وتفسيرها وبثها وتحويلها واستخدامها[2].

كما يتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وبناء على ذلك تعرف الجريمة الإلكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال أي الجرائم التي ترتكب بأساليب ووسائل إلكترونية وآليات الاتصال عن بعد من التليفون والفاكس والحاسوب وغيرها[3].

قبل التوسع في تعريف الجريمة الإلكترونية لوجود مجموعة من المفاهيم المتقاربة يجب التطرق أولا إلى عدة تسميات تطلق على هذه الجرائم، فبداية

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 18،دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019 ، ص29.

[2] ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر "أساليب وثغرات"، د ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة،الجزائر،2010،ص 19.

[3] صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، العدد 01، المجلد 07، جامعة محمد بشير الإبراهيمي برج بوعريريج، 2021/06/28، ص2528.

بالاحتيال المعلوماتي ثم الجرائم التي يساعد على ارتكابها الحاسب الآلي ثم التعسف في استعماله أو إساءة استعمال الحاسب الآلي للدلالة على هذه الظاهرة باعتبارها أشمل و أوسع، كما أطلقوا عليها مصطلح الجريمة المعلوماتية لينتقلوا إلى مصطلحات أكثر حداثة و دقة و هي جرائم التقنية العالية ، جرائم الهاكرز أو جرائم ذوي الياقات البيضاء ثم جرائم الكمبيوتر والأنترنت[1].

ثانيا: تعريف الجريمة الإلكترونية اصطلاحا

نتيجة التطور المستمر واللامتناهي لتكنولوجيا المعلومات حتى الآن حال دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة الإلكترونية، فهي المشكلة الأولى والأساسية التي تعترض هذه الظاهرة، وذلك لغياب تعريف قانوني للجرائم المعلوماتية عند جل التشريعات، إلا أنه قد بدل الفقه من أجل ذلك جهود كثيرة لتعريف هذه الجريمة، قد انقسم الفقه إلى اتجاهين اتجاه ضيق ، أما الاتجاه الآخر فقد وسع في مفهومها.

1/الاتجاه الضيق لمفهوم الجريمة الإلكترونية

يذهب أنصار هذا الاتجاه إلى حصر الجريمة المعلوماتية في الحالات التي تتطلب أن يكون الجاني على قدر كبير من المعرفة لتقنية المعلومات وشبكة الأنترنت لأنه إذا قام شخص عادي بارتكاب هذا النوع من الجرائم تعتبر هذه الجريمة تدخل ضمن الجرائم التقليدية تتكفل بها نصوص قانون العقوبات العادية.

ومن التعريفات التي قدمت في هذا المجال أنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى"[2].

وعرفها الفقيه Trédeman"أن الجريمة المعلوماتية تشمل أي جريمة ضد المال باستخدام المعالجة الآلية للمعلومات"[3].

كما عرفها (بموازين) بأنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالع مكان مرتبط بتقنية المعلومات"[4].

كما نلاحظ من خلال هذه التعريفات أنها تضيق من مفهوم الجريمة المعلوماتية فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم، فقد تم نقد هذا الاتجاه لكونه يحصر الجريمة المعلوماتية في المجالات التي تتطلب قدر كبير من المعرفة التقنية في ارتكابها.

2/ الاتجاه الموسع من مفهوم الجريمة الإلكترونية

---

[1] معاشي سميرة، الجريمة المعلوماتية(دراسة تحليلية لمفهوم الجريمة المعلوماتية)،مجلة الفكر، جامعة محمد خيضر، بسكرة، الجزائر،العدد17، 2008،ص 400.

[2] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، د ط، الدار الجامعية للنشر،الإسكندرية،2008،ص 42.

[3] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني للحماية المعلوماتية "،د ط، دار الجامعة الجديدة للنشر،الإسكندرية،2009، ص154.

[4] فليح نور الدين، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق قانون جنائي و العلوم الجنائية، جامعة مولاي الطاهر سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2019/2018،ص10.

على عكس الاتجاه السابق فقد حاول هذا الاتجاه توسيع تعريف الجريمة المعلوماتية فعرفها البعض على أنها " عمل أو امتناع يأتيه الإنسان أضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، والتي يحميها قانون العقوبات ويفرض له عقابا"[1].

وعرفها الخبير الأمريكيParker على أنها "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عن خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[2].

وقد عبر خبراء المنظمة الأوروبية لتعاون الاقتصادي عن الجريمة المعلوماتية "بأنها كل سلوك غير مشروع أو منافي للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"[3].

وقد أقر المجلس الأوروبي في التقرير الخاص بالجرائم المتعلقة بالحاسوب بقيام المخالفة أي(الجريمة) في كل حالة يتم فيها "تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات ومعالجتها، وتبعا لذلك تسبب في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصاد غير مشروع له أو لشخص آخر"[4].

ثالثا: التعريف القانوني للجريمة الإلكترونية

المشرع الجزائري كغيره من التشريعات لم يعرف الجريمة الإلكترونية، فهو في الأصل لم يستعمل مصطلح الجريمة الإلكترونية أو المعلوماتية في القوانين التي سنها في مجال الجرائم، فقد كانت هذه الجريمة سنة 2004 أي قبل تعديل قانون العقوبات تدخل ضمن الجرائم التقليدية مثل خيانة الأمانة والسرقة وغيرها، رغم اختلافها عن الجريمة التقليدية إلا أنها كانت تفتقر إلى نصوص قانونية تنظمها فقد كانت تلبس ثوب العقوبات المقررة للجريمة التقليدية.

وبعدما أفرزته الثورة المعلوماتية من أشكال جديدة من الجرائم التي لم تشهدها البشرية من قبل، تطرق المشرع الجزائري على غرار الدول الأخرى بتعديل قانون العقوبات الجزائري بموجب القانون رقم 04- 15[5] المعدل والمتمم للأمر رقم 66-156، فقد عمل المشرع الجزائري على تجريم الجرائم الإلكترونية التي أصبحت تنتشر و بسرعة فائقة في المجتمع الجزائري، لهذا استحدث بذلك قسما خاصا بالعقوبات المطبقة على هذا النوع من الجرائم وذلك في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المواد من 394 مكرر إلى 394 مكرر7. وبعد ازدياد الوعي بخطورة هذا النوع المستحدث من الجرائم وأصبح يؤثر على الاقتصاد الوطني بالدرجة الأولى، بعدها تم تشديد العقوبة

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق،ص158.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية،ط01،دار الثقافة للنشر والتوزيع،الأردن،1429ه-2008م،ص49.

[3] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت(الجرائم الإلكترونية)"دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة الى جهود مكافحتها محليا وعربيا ودوليا،ط01،منشورات الحلبي الحقوقية،2007،ص 16.

[4] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شهادة ماجستير قانون عام، جامعة ابو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2012/2011،ص40.

[5] القانون04-15 المؤرخ في10نوفمبر2004، المعدل والمتمم للأمر 66-156،المؤرخ في08جون1966، المتضمن قانون العقوبات، ج ر، العدد71، بتاريخ2004/11/10.

المقررة لهذه الأفعال سنة 2006 بموجب القانون 16- 02 [1] المعدل والمتمم لقانون العقوبات في المادة 394 مكرر 8 من نفس القسم وذلك دون المساس بالنصوص المجرمة الواردة في هذا القسم من قانون 04- 15.

تبنى المشرع الجزائري للدلالة على الجريمة الإلكترونية، مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، حيث يمثل هذا النظام المسألة الأولية أو الشرط الأولي الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام ، فإذا تخلف هذا الشرط لا يكون هناك مجال لهذا البحث[2].

إن نظام المعالجة الآلية للمعطيات تعبير تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال الحاسبات الآلية، لذلك فالمشرع الجزائري على غرار المشرع الفرنسي لم يقم بتعريف هذا النظام بل أوكل هذه المهمة لكل من الفقه والقضاء[3].

ومع انتقال الجزائر نحو إنتهاج إستراتيجية الجزائر الإلكترونية وظهور بوادر التحول الإلكتروني لجميع المؤسسات والهيئات والإدارات العمومية وجد المشرع الجزائري واقعا يفرض استحداث قانون جديد أكثر عمقا لمعالجة الجرائم الإلكترونية وما يتعلق بها من تجاوزات تمس الأفراد والمؤسسات فاصدر بذلك سنة 2009 أول نص قانوني يتعلق بالجرائم الإلكترونية ومكافحتها والذي وضع من خلاله المشرع الجزائري تعريفا للجرائم الإلكترونية التي اصطلح عليها بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك لاستبعاد الغموض والمرونة التي تتميز بها التعاريف الفقهية لهذا النوع من الجرائم[4]. بموجب أحكام المادة 2 من قانون 09-04 [5]عرف هذا المصطلح على أنه "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة اخرى ترتكب أو يسهل ارتكبها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

يلاحظ من هذا التعريف أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية. أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات. كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية، كونه أقر أن هذه

---

[1] القانون16-02 المؤرخ في2016/06/19،المعدل والمتمم للأمر66-156،المؤرخ في 08جوان1966،المتضمن قانون العقوبات.

[2] يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر أكاديمي، تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2017/2016،ص12.

[3] زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة مولود معمري، تيزي وزو، العدد 03،المجلد 04، 2019،ص132.

[4] دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، الجزائر، العدد 13، 2020/01/05،ص141.

[5] القانون09-04المؤرخ في2009/08/05،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر العدد07،لسنة2009.

الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، هذا ما يوسع نطاق مجال الجرائم المعلوماتية في القانون الجزائري[1].

وحسب المشرع الجزائري فإنه قد تتحقق هذه الجريمة بمجرد أن ترتكب، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[2].

مثال على الجرائم الإلكترونية في الجزائر تسريب أوراق امتحان البكالوريا لعام 2016. وبالمثل، اخترق المخترق الجزائري حمزة بن دلاج، في عالم القرصنة، حسابات بنكية عالمية اعتقلته الشرطة الفيدرالية الأمريكية، فهو أحد أشهر القراصنة في تاريخ الجزائر، وربما في العالم، لكن الحقائق التي أبلغ عنها مكتب التحقيقات الفيدرالي كافية لجعله أسطورة حية.

وفي الأخير يمكننا القول أنه و بالرغم من كون الجريمة الإلكترونية ذات بعد دولي، و بالغة الخطورة، وبسبب زيادة انتشارها بسرعة فائقة في كل أنحاء العالم، إلا أن الجزائر ليست طرف في جل الاتفاقيات الدولية التي تحارب ظاهرة الإجرام الإلكتروني، كاتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية سنة 2001 واتفاقية بودابست، ولكن نتيجة لتأثر الجزائر بما أفرزته تقنية المعلومات من أشكال جديدة للجرائم المستحدثة قد صادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1/15 /1432هـ الموافق 21/ 12/ 2010م، والتي صادقت عليها الجمهورية الجزائرية بتاريخ 2010/12/21، وأصبحت سارية المفعول بعد مضي ثلاثين يوماً من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية بموجب الفقرة (3) من الأحكام الخاتمة للاتفاقية. وقد قامت الجزائر بالتوقيع على هذه الاتفاقية رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، ففي المادة الأولى من هذه الاتفاقية تضمنت الهدف والغاية من ورائها[3].

---

[1] زيوش عبد الرؤوف، المرجع السابق،ص132.

[2] سوير سفيان ، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2011/2010، ص ص 14 إلى 16.

[3] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، القاهرة، مصر، 2010، والتي وقعت عليها الجزائر في 2010/12/21.

الفرع الثاني: الطبيعة القانونية للجريمة الإلكترونية

إن دراسة الجريمة الإلكترونية بشكل خاص تدخل ضمن قسم خاص من أقسام قانون العقوبات وهو ذلك الفرع الذي يدرس كل جريمة على حدى متناولا كل عناصرها الأساسية والعقوبة المقررة لها، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة، هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم إدخالها إلى الحاسب المرتبط بشبكة المعلومات لغرض الحصول على معلومات معينة ، كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص[1].

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام الخدمات البريدية أم التخابر الخاص أم يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم الإلكترونية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر الواقع والمعلومات فيها؟،ومن هذا النظام القانوني تتحدد المسؤولية التي يفترض تطبيقها على الأشخاص المسؤولين عند هذا النشر، ومن خلال المجال التي ترتكب فيها الجريمة الإلكترونية و محل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة[2].

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى ارتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات، لهذا صعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة[3]. فتطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات و صعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأنه من السهل محو أدلة الإدانة في وقت قصير[4].

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بمجموعة من الخصائص التي تنفرد بها وتميزها عن الجريمة التقليدية في أسلوبها وطريقة ارتكابها والتي ترتكب يوميا في كافة دول العالم، ولهدا سنقسم هذا المطلب الى الفرعين المواليين:

الفرع الأول: الخصائص المشتركة مع الجرائم الاخرى

أولا: جريمة عابرة للحدود

يمكن القول أن من أهم الخصائص التي تتميز بها الجريمة الإلكترونية هو كونها ذات بعد دولي، أي أنها تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه،

---

[1] مسيكة محمد الصغير و بوعيدلي جمال، مفهوم الجريمة المستحدثة وطبيعتها القانونية، كتاب أعمال الملتقى الوطني "الجريمة المستحدثة وآليات مكافحتها"، مخبر بحث نظام الحالة المدنية، جامعة الجيلالي بونعامة خميس مليانة، 05-06 /05/ 2019، ص ص13-14.

[2] مرابطن حياة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام،2019/2018،ص11.

[3] بوضياف اسمهان، الجريمة الإلكترونية وإجراءات تشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف مسيلة،العدد11، 2018، ص 358.

[4] مرابطن حياة، المرجع السابق، ص ص 11-12.

أي التباعد بين أداة الجريمة ومحلها، فيمكن أن ترتكب الجريمة من مجرم في دولة ما على مجني عليه في دولة أخرى في وقت قصير جدا، ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، والقانون الواجب التطبيق عليها[1].

ومن القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية نظرا لأهميتها كونها ولأول مرة تم تسليم المتهم في جريمة معلوماتية وقدم للمحاكمة بتهمة إعداد برنامج خبيث، وهي القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز)[2].

ثانيا: تتم عادة بالتعاون أكثر من شخص

تتسم الجرائم المتعلقة بشبكة الأنترنت بخطورة بالغة، فهي ترتكب من طرف فئات متعددة مما يصعب معرفة من هو مرتكب الجريمة، هذا ما جعل مكتب التحقيقات الفيدرالي الأمريكي يطلق عليها وصف الوباء[3]، و يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج مؤسسة المجني عليه لتغطية عملية التلاعب وتحويل المكسب إليه[4].

الفرع الثاني: الخصائص التي تنفرد بها الجريمة الإلكترونية عن الجرائم الأخرى

أولا: جريمة صعبة الاكتشاف

الجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها وهي خطيرة، وصعبة في تحديد مكان وقوعها، أو مكان التعامل معها بسبب اتساع نطاقها المكاني، وضخامة البيانات، فمعظم جرائم الأنترنت يتم اكتشافها بالمصادفة بل وبعد وقت طويل من ارتكابها زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه رقم خطير[5]، وهذا ما يعني وجود فجوة كبيرة أي أنه من الواضح أن الحالات التي يتم اكتشافها في هذه الجرائم قليلة جدا مقارنة بما يتم اكتشافها عادة في الجرائم التقليدية. ترجع معظم الأسباب إلى وسيلة تنفيذها وعدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، وقدرة الجاني على تدمير دليل الإدانة في أقل من ثانية يكون عاملا إضافيا في صعوبة الاكتشاف.

ثانيا: صعبة الإثبات

ترجع صعوبة إثبات الجريمة الإلكترونية إلى عدة صور منها:

---

[1] رضية بركايل، التنظيم القانوني الجزائي للجريمة المعلوماتية في التشريع الجزائري، الملتقى الوطني "الأمن المعلوماتي: مهدداته وسبل الحماية"، مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري03-20015/11/04، ص221.

[2] لاحظ نهلا عبد القادر المومني، المرجع السابق، ص 52.

[3] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجريمة الإلكترونية "دراسة مقارنة"، مذكرة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط،2014،ص24.

[4] نهلا عبد القادر المومني، المرجع السابق، ص58.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص ص 45 الى51.

- الجريمة لا تترك أي آثار مادية لها بعد ارتكابها فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير مرئية ولا توجد مستندات ورقية، كونها تتصف بالخفاء، وصعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، وذلك لسهولة محوه وتدميره في زمن قياسي[1].

-نتيجة لنقص الخبرة والتدريب كثيرا ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبدل لكشف غموضها وضبط مرتكبها جهودا تتناسب وهذه الأهمية، كما أن رجال الشرطة و ضباط الشرطة القضائية قد لا يتعاملون بمهارة واحتراف مع الدليل الإلكتروني المستند من الجريمة المعلوماتية[2].

ثالثا: المتطلبات الرئيسية لارتكاب الجريمة الإلكترونية

الجريمة الإلكترونية يرتبط وجودها بجهاز الحاسوب وشبكة الإنترنت وهو ما يضفي عليها الطابع الخاص الذي يميزها عن غيرها من الجرائم كونها تتطلب علم كافي بالجوانب الفنية، إن العلاقة بين مدى الخبرة بالجوانب التقنية والفنية للحاسوب وبين الجريمة الإلكترونية تعتبر علاقة طردية، أي أنه كلما زاد العلم لدى الأفراد بتقنية الحاسوب والأنترنت، زاد احتمال ارتكاب هذا النوع من الجرائم واستخدام خبراتهم بشكل غير مشروع.

كما أثبت الواقع العلمي أنها قد ترتكب من خلال الهواتف المحمولة خاصة بعد ظهور أجهزة الهواتف الذكية والتي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت ويسهل تخزين ونقل المعلومات من خلالها[3].

رابعا: جريمة ناعمة ومريحة للمجرمين

الجريمة الإلكترونية جريمة هادئة فهي لا تحتاج إلى مجهود عضلي لقيام المجرم بارتكابها مثل جرائم القتل والسرقة في الجريمة التقليدية، بل هي تحتاج إلى مجهود ذهني والتفكير المدروس، كذلك لا تحتاج إلى التقارب أو التلامس بين الجاني والضحية إذ أنه يمكن أن ترتكب مهما كان البعد بينهما كونها لا يحدها مكان وزمان معين.

تمتاز جرائم تكنولوجيا المعلومات بكونها أقل عنفا، وتمم بطريقة سهلة و آلية سريعة وبكبسة زر فقط، بمعنى أخر ركنها المادي قد لا يتجاوز لمسة بسيطة لمفاتيح التشغيل.

خامسا: ذكاء مرتكب الجريمة

إن مرتكب الجريمة يتميز فاعلها بقدر من الذكاء والدراية بالتكنولوجيا فهو يستخدم علمه لا قوته العضلية في ارتكاب الجريمة ويمتاز أيضا بميله للإجرام كونه إنسان متوافق مع المجتمع و قادر على التكيف معه[4]،على عكس الجريمة التقليدية

---

[1] خالد ممدوح إبراهيم، المرجع نفسه ،ص 45-46

[2] نهلا عبد القادر المومني، المرجع السابق،ص57.

[3] بن شهرة شول ومراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، المركز الجامعي آفلو، العدد 01،المجلد 04، 2020، ص7.

[4] وسيم حسام الدين الأحمد، مكافحة الجريمة الإلكترونية في التشريعات والاتفاقيات الدولية،ط01،دار غيداء للنشر والتوزيع، عمان، 2020، ص97

التي قد يكون مرتكبها شخص أمي بسيط متوسط التعليم، و ذلك أن الإجرام المعلوماتي هو إجرام الأذكياء.

فمرتكبي هذه الجرائم لهم صفات متميزة من حيث الثقافة والعلم التكنولوجي، فالمجرم في هذا النوع من الجرائم ليس عاديا فهو يرتكب جريمة متخصصة خاصة إذا ما تمثلت هذه الجريمة بسرقة مشفرة مما يستلزم معه خبرة تقنية عالية في هذا المجال[1].

سادسا: جريمة مستحدثة

تعتبر الجريمة الإلكترونية من الجرائم الجديدة التي تشكل خطرا كبيرا في العالم كونها عابرة للقارات، حيث أن التقدم السريع لتكنولوجيا المعلومات خلال السنوات الأخيرة جعل العالم عبارة عن قرية صغيرة. يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية بل أنه أضعف من قدراتها على تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها[2]،فيقال أن الجريمة الإلكترونية هي الابن الغير الشرعي الذي جاء نتيجة للتزاوج بين تكنولوجيا المعلومات مع العولمة، أو هي المارد الذي خرج من القمم، ولا تستطيع العولمة أن تصرفه، بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات[3].

المطلب الثالث: أنواع الجرائم الإلكترونية

قد اختلف الفقهاء في تسمية الجريمة الإلكترونية لهذا تم تصنيفها الى عدة مسميات، وبسبب ذلك عرفت اختلاف في تقسيماتها وذلك راجع إلى ظهور جرائم جديدة من حين إلى آخر، فلا يوجد لها حصر، ولا يمكن تشغيلها بكل أصنافها وأشكالها، فهي متغيرة ومتجددة، كلما ظهرت وسيلة جديدة لاستخدام الحاسب الآلي وشبكات الأنترنت ظهرت معها جريمة مستحدثة، حيث استند كل اتجاه على معيار معين، فمنهم من صنفها بالرجوع إلى وسيلة ارتكابها، أو على أساس محلها، والبعض يصنفها حسب الأسلوب المتبع فيها، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحقل المعتدي عليه[4].

أما بالنسبة للمشرع الجزائري فقسمها إلى الجرائم الواقعة بواسطة نظام المعلوماتي، والجرائم الواقعة على النظام المعلوماتي، بالنسبة للنوع الأول فقد نص عليه ولكن لم يحدده، أما بالنسبة للنوع الثاني فقد نص عليه وحدده بموجب قانون العقوبات الجزائري، وهذا ما سنتطرق له في الفرعين المواليين.

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

يشتمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي في هذه الطائفة وسيلة لتسهيل النتيجة الإجرامية و مضاعفا لجسامتها[5]. يستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة، فصور

---

[1] عبد الله عبد الكريم عبد الله، المرجع السابق،ص32.
[2] خالد ممدوح إبراهيم، المرجع السابق، ص51.
[3] رصاع فتيحة، المرجع السابق، ص36.
[4] رصاع فتيحة، المرجع السابق،ص69.
[5] سوير سفيان، المرجع السابق، ص33.

هذه الجرائم متعددة، بعضها قد ذكرها المشرع الجزائري، و البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها.

أولا: الجرائم الواقعة على الأشخاص

المقصود بها تلك الجرائم التي تهدد بالخطر الحقوق ذات الطابع الشخصي، سنحاول أن نستعرض بعض أنواع الجرائم التي تقع على الأشخاص بواسطة تكنولوجيا المعلومات، والتي قسمت إلى ثلاثة طوائف بحسب نوع الحق المتعدي عليه، ودور النظام المعلوماتي في اقترافها.

1/ جرائم الاعتداء على حرمة الحياة الخاصة

تعتبر فكرة الحياة الخاصة من الأفكار التي يصعب تعريفها فقد عانى كل من الفقه والقضاء في محاولة منهم لإيجاد مدلول واضح لها، فهي تتمتع بحماية دستورية وقانونية وكذلك دولية، في مختلف دول العالم، فهي تصنف ضمن الحقوق الشخصية، التي تثبت لكل شخص لمجرد كونه إنسانا، فالشخص الذي كان يستفرد بأسراره دون أن يقوم بإظهارها للغير إلا برضاه أصبحت الآن مكشوفة وواضحة أمام التقنية الحديثة و التي تعد خطرا حقيقيا يهدد الحياة الخاصة للفرد، فقد أصبح الدخول إلى خصوصيات وأسرار الفرد والاعتداء عليها سهلا. قد كفلت جل الدول الحياة الخاصة لمواطنيها بالحماية[1] وقد حدى الدستور الجزائري حدو الدساتير الدولية بحرصه على حماية الحياة الخاصة للمواطنين وهذا ما جاء في نصوص المواد 35 و38 و 39 من الدستور الجزائري.

و تجدر الإشارة إلى أنه لا يوجد تصنيف محدد أو دقيق يحدد كيفية انتهاك حرمة الحياة الخاصة بواسطة شبكة الأنترنت، ولكن رغم ذلك يمكن أن نذكر بعض من الجرائم التي تعتبر شائعة وتمس حرمة الحياة الخاصة على سبيل المثال جرائم القذف، السب، وتشويه السمعة.

تعد جرائم القذف والسب من أكثر الجرائم شيوعا في نطاق التكنولوجيا، فتوجد مواقع متخصصة تستعمل للمساس بشرف الغير، فهي تعمل على إبراز كافة سلبيات الشخص المستهدف وإفشاء أسراره، بالإضافة إلى أنه يتم السب والقذف مباشرة عبر خطوط الاتصال أو كتابيا أو بواسطة المطبوعات والرسائل، وذلك لاحتقار الناس وتشويه سمعتهم والنيل من كرامتهم واعتبارهم.

عرفت المادة 297 من ق ع ج السب بقولها:" يعد سباً كل تعبير مشين أو عبارة تتضمن تحقيراً أو قدحاً لا ينطوي على إسناد أية واقعة".

ويعرف القذف بأنه: إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسناداً علناً عموديا يفيد نسبة الأمر إلى الشخص على سبب التوكيد[2].نصت عليه المادة 296 ق ع ج.

يستعمل الجاني حسب القواعد العامة في جرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه، مهما كانت الوسيلة المعتمدة، مع علمه أن ما

[1] سوير سفيان، المرجع نفسه، ص 35.

[2] حسين فريجة، الجريمة الإلكترونية والأنترنت، مجلة المعلوماتية،العدد36،أكتوبر 2011، ص06.

يقوم به يعد مساسا بسمعة الغير[1]، في الغالب ما يقوم الجاني باستعمال البرامج التي تساعده في إخفاء هويته لكي لا يتعرض للمسائلة القانونية.

2/ جرائم الاستغلال الجنسي للأطفال عبر الأنترنت:

تعتبر الأنترنت سلاح فتاك، فبالرغم من كونها تنشر العلم، ومن خلالها يتم تبادل الثقافات وغيرها، إلا أنها وسيلة للفساد والانحراف نتيجة لظهور الإباحية من صور ماجنة ومقالات فاضحة و أفلام خليعة على الأنترنت عبر المواقع المخصصة لذلك.

قد فرض المشرع الجزائري حماية جنائية خاصة لطفل لتجنب الاعتداء عليه وذلك من خلال الأمر 66 /156[2] المعدل المتمم وذلك تحت عنوان تحريض القصر على الفسق والدعارة من المادة 342 إلى غاية المادة 349، أما في ما يخص جريمة الاستغلال الجنسي فقط صمت المشرع الجزائري ولم ينص صراحة على عقوبة هذه الجريمة رغم خطورتها والتي يكون الأطفال ضحاياها فهو لم يضمن الحماية الكاملة للطفل.

ومن أمثلة هذه الجرائم أنه في الولايات المتحدة الأمريكية قامت المباحث الفيدرالية عام 1997 بالقبض على 1500 شخص مشتبه فيهم بالتعامل في دعارة الأطفال عبر شبكة الإنترنت وبث صور ماجنة للقصر في قضيةOperations Ripa lord [3] .

3/ جرائم الاعتداء على الملكية الفكرية :

أحد أهم الأسباب التي تعود إليها ظاهرة "قرصنة برامج الحاسوب" هي ضعف وسائل الحماية القانونية لبرامج في معظم دول العالم الناتج عن الخلاف الفقهي التشريعي حول الطبيعة القانونية لبرامج الحاسوب، بسبب الطابع التقني الذي يميز هذه البرامج عن المؤلفات والمصنفات التقليدية، هذا فضلا عن تباين مستوى الحماية لهذه البرامج من دولة إلى أخرى، ما يسبب لمنتجها مشكلات متعددة[4].وقد نص المشرع الجزائري على حقوق الملكية الفكرية في الدستور الجزائري، و كذا الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر 03-07 المتعلق ببراءات الاختراع.

ثانيا: الجرائم الواقعة على الأموال

لم تقتصر الجريمة الإلكترونية على إلحاق الضرر بالأشخاص، بل تعدتها لتطال الذمة المالية للغير، فبعد تطور شبكة الأنترنت و أصبحت معظم المعاملات التجارية مثل البيع والشراء تتم بها، انتهز بعض المجرمين الفرصة للسطو عليهم، حيث تم ابتكار عدة طرق لذلك.

---

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية"، 2013،ص53.

[2] الأمر رقم 66-156، المتضمن قانون العقوبات، سالف الذكر.

[3] هروال هبة نبيلة، جرائم الأنترنت "دراسة مقارنة" ،مذكرة لنيل شهادة الدكتوراه، جامعة ابو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2011/2010، ص 172.

[4] علي جبار الحسناوي، جرائم الحاسوب والأنترنت، د ط، دار اليازوري العلمية للنشر والتوزيع، الأردن، عمان، 2009، ص ص 57-58.

جرائم الأموال بشكل عام هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات القيمة المالية[1]. من الجرائم التي تمس الذمة المالية للغير ونذكر منها ما يلي:

1/ جريمة السرقة الإلكترونية:

عرفت المادة350 ق ع السرقة كما يلي: "كل من اختلس شيئا غير مملوك له يعد سارقا"[2].

وتتجسد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الآلي للدخول إلى شبكة الأنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية[3].

2/ التحويل الإلكتروني غير المشروع للأموال:

قد ظهر العديد من المتسللين السطو عليها كونها نقود إلكترونية، بالاستيلاء على بطاقة الائتمان ليس بالأمر الصعب، مثلا يستطيعون سرقة الآلاف من أرقام البطاقات فقط في يوم واحد باستخدام شبكة الأنترنت ثم بيع هذه المعلومات.

إن البطاقة الائتمانية تعد نقودا إلكترونية والاستيلاء عليها يعد استيلاء على مال الغير، ونظرا لسهولة الاستيلاء على تلك الأرقام فقد تزايدت حوادث الاستيلاء عليها، كما تزايدت عمليات الابتزاز المصاحبة لارتكاب مثل تلك الجرائم، وعمليات الابتزاز تكون إما لإعادة تلك الأرقام أو لعدم نشرها أو استخدامها من قبل من استولى عليها[4].

3/ جريمة غسيل الأموال عبر الأنترنت:

تعرف جريمة غسيل الأموال بأنها": مجموعة عمليات معينة ذات طبيعة اقتصادية أو مالية تؤدي إلى إدخال الأموال دائرة الاقتصاد الشرعي رؤوس أموال ناتجة من أنشطة غير مشروعة تقليديا متعلقة بالمتاجرة بالمخدرات واليوم أصبحت نواتج كل جريمة جنائية ذات جسامة أو خطورة[5]. وتعتبر من الجرائم المعاصرة فهي صورة من صور الجريمة المنظمة، وغالبا ما تتم عن طريق تسلل الأموال إلى المشروعات الاقتصادية والتأثير فيها وبعد ذلك يعاد استغلالها على أنها مصدر ربح مشروع، ونتيجة التطور فقد استفاد مجرمو غسيل الأموال من التقنية ،مميزاتها أغراضها الإجرامية[6].

ثالثا: الجريمة الواقعة على أمن الدولة

---

[1] لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية "دراسة مقارنة"،ط1،دار الحامد للنشر والتوزيع،الأردن،عمان،2015م/1436ه،ص48.

[2] القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات الجزائري.

[3] سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2014/2013، ص29.

[4]Manacorda (SC)lareglementation du blanchiment de capitaux en droitInternational du systéme .rev SC criminelle . 2Avr il 1999 P251.

[5] أسامة غربي، جرائم الانترنت بين الجانب التقني وأساليب المكافحة، مجلة الحقوق والحريات، العدد 02، جامعة المدية، 2015،ص47.

[6] لينا محمد الاسدي، المرجع السابق،ص51.

بالنظر إلى خطورة الجرائم التي تقع على أمن الدولة ومكانتها فهي تحتل الدرجة الأولى مقارنة بباقي الجرائم، فقد استغلت الكثير من الجماعات المتطرفة الطبعة الاتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعدا الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الأنترنت، التي سمحت لهم في ارتكاب جرائم غاية الشك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الأنترنت لكثير من الدول ممارسة التجسس على دول أخرى[1].

1/ جريمة الإرهاب:

أصبح الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجيا أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث، فقد شهدت العقود الأخيرة من القرن العشرين بروز العديد من التنظيمات المسلحة والعمليات الإرهابية في مختلف أنحاء العالم[2].

لقد عرفت اتفاقية جنيف لقمع ومعاقبة الإرهاب لعام 1937م، في مادتها الأولى على أن الأعمال الإرهابية هي "الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف، أو يقصد بها، خلق حالة من الرعب في أذهان أشخاص معينين، أو مجموعة من الأشخاص، أو عامة الجمهور"[3]. أما جريمة الإرهاب الإلكتروني فتعرف على أنها هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الإنتقام أو الابتزاز أو الإجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة[4]. للجماعات الإرهابية القدرة على استخدام وسائل الاتصال المستحدثة لارتكاب جرائم معلوماتية من الدرجة الثالثة في سبيل إحداث أضرار جسيمة في دولة أو خلق جو من عدم الاستقرار و الرعب و الفوضى أو في سبيل الضغط على أي دولة لتلبية طلباتهم غيرا لمشروعة[5].

2/ الجريمة المنظمة:

الهدف الأساسي للجريمة المنظمة في الأساس هو السعي للإفادة المادية، أو تحقيق الأرباح، من خلال مواصلة العمل بوسائل إجرامية، ولذا كما تستعين الشركات العادية بشبكة الأنترنت بحثاً عن فرص جديدة لتحقيق الأرباح، كذلك تفعل المنظمات الإجرامية[6].

إن أعضاء الجريمة المنظمة يستفيدون من التطور التكنولوجي في مجال المعلومات الإلكترونية، وذلك من خلال استغلال الإمكانات المتاحة إلكترونيا في

---

[1] بوضياف اسمهان، المرجع السابق، ص 358.
[2] سمية مزغيش، المرجع السابق، ص34.
[3] هروال هبة نبيلة، المرجع السابق ، ص 316.
[4] هروال هبة نبيلة، المرجع نفسه، ص 333.
[5] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، جامعة منتوري قسنطينة، كلية الحقوق،2014/2013، ص157.
[6] رصاع فتيحة، المرجع سابق، ص82.

التخطيط والتوجيه وتنفيذ المخططات الإجرامية بسهولة مخترقة حدود الدول بأقل تكلفة ممكنة ودون مخاطرة[1].

3/ جريمة التجسس:

ينتج عن الاستخدام المتزايد للحاسبات الآلية في العديد من المجلات، تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريها[2].

ويقصد بالتجسس هنا "الحصول وتجميع المعلومات السرية المخزنة والمحفوظة داخل الحواسيب المرتبطة بالأنترنت و الخاصة بسياسة الدولة وبدفاعها و نظامها الاقتصادي والصناعي وكذا أبحاثها العلمية خاصة تلك المتعلقة بأبحاث الطاقة النووية وتسليمها إلى حكومة أجنبية أخرى"[3].سهلت شبكة الأنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية، وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي[4].

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

إضافة إلى ما تم ذكره سابقا على الجريمة الإلكترونية الواقعة باستخدام النظام المعلوماتي، فهناك نوع آخر وذلك بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية، ويتمثل في الجريمة الواقعة على النظام المعلوماتي وهما: جريمة الدخول والبقاء غير المشروع لأنظمة المعالجة الآلية للمعطيات، و جريمة المساس بالأنظمة الآلية لمعالجة المعطيات، والتي سبقا وتطرقنا لهم، كما تضمن صور أخرى.

أولا: جريمة الدخول والبقاء غير المشروع لأنظمة المعالجة الآلية للمعطيات

لعل جريمة الدخول والبقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات هي من أهم جرائم المعطيات والجرائم المعلوماتية عموما، ذلك أن أغلب جرائم المعطيات لا يمكن ارتكابها إلا بعد الدخول للنظام، ولهذا كانت جريمة الدخول في الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرى، لذلك أولت لها التشريعات اهتماما كبيرا وهناك من التشريعات من يجعلها الجريمة الأساسية وما بقي من الجرائم إلا نتائج لها[5] .

---

[1] رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية أدرار، العدد 41، 2018، ص449.

[2] صغير يوسف، المرجع السابق، ص57.

[3] هروال هبة نبيلة، المرجع السابق، ص 372.

[4] صغير يوسف، المرجع السابق، ص57.

[5] ابتسام موهوب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2014/2013، ص9.

ثانيا: جريمة المساس بالأنظمة الآلية لمعالجة المعطيات

يأخذ السلوك الإجرامي لهذه الجريمة إما الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات أو الاعتداء العمدي على المعطيات ، فكما سبقا وذكرنا أن المشرع الجزائري لم ينص على الاعتداء العمدي على سير نظام للمعالجة الآلية للمعطيات واكتفى بالنص على الاعتداء على المعطيات الموجودة داخل النظام[1].

الفرع الثالث: أفعال إجرامية أخرى

أولا: جريمة الاعتداء على المكونات المادية

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في التشغيل مثل الأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن يكون محل السرقة وخيانة الأمانة أو الإتلاف العمدي أو الاختراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة[2].

ثانيا: جريمة الاعتداء على المكونات المنطقية(البرامج)

تأخذ شكلين قد تقع على البرامج التطبيقية وإما على برامج التشغيل، ويقصد بالأولى البرامج المكتوبة بإحدى لغات الكمبيوتر عالية المستوى وهي يمكن استعمالها من قبل كافة العملاء بصرف النظر عن نوع الحساب الذي يملكونه. أما الثانية فيقصد بها تلك البرامج التي عن طريقها يتم القيام بوظائفها المحددة لها، فهذه البرامج تعتبر المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط التعليمات الخاصة بالنظام[3].

[1] مراد مشوش، ، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجريمة المتصلة بتكنولوجيا الإعلام والاتصال، مخبر البحث في السياحة، الإقليم والمؤسسات، العدد 01،المجلد 09، 2020 ، ص115.

[2] بوضياف اسمهان، المرجع السابق، ص 359.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص67.

المبحث الثاني: الإطار الموضوعي للجريمة الإلكترونية

سبقا وقد تطرقنا إلى مفهوم الجريمة الإلكترونية والجذل الواقع في تسميتها، لا تختلف عن الجريمة التقليدية في كثير من الأشكال، ومن خلال هذا المبحث سنقوم ببيان الملامح التي توضح لنا الإطار الموضوعي الجريمة الإلكترونية، وهذا ما يتطلب لبيان أركانها، وأنواعها، وخصوصية مرتكب هذه الجريمة وضحاياها ، لهذا قسمنا المبحث إلى ثلاث مطالب.

المطلب الأول: أركان الجريمة الإلكترونية

أركان الجريمة الإلكترونية لا يختلف عن ما هو متعارف عليه في الجرائم التقليدية، فلا بد أن تكون لكل جريمة أركان تقوم عليها تتحقق بتوفرها وتزول بزوالها كغيرها من الجرائم، حسب ما تطرق له المشرع الجزائري في نصوص القانون سنحاول أن نستخلص أركان الجريمة الإلكترونية والتي تقوم بشكل عام على ثلاثة أركان وهي الشرعي المتمثل في النصوص القانونية التي تدين الفعل، المادي المتمثل في السلوكيات المادية المجرمة، المعنوي المتمثل في القصد الجنائي للجريمة الإلكترونية.

الفرع الأول: الركن الشرعي

انطلاقا من المبدأ الذي استقر عليه المشرع الجزائري في المادة الأولى من قانون العقوبات الجزائري أنه "لا جريمة ولا عقوبة إلا بنص"[1]. القاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية القانون الجنائي، لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون، يتميز هذا المبدأ أن القاضي الجنائي عند تفسير نصوص القانون أن يفسرها تفسيرا ضيقا، بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل لم يرد تجريمه على فعل ورد تجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني لتشابه الفعلين[2].

فقد أحداث المشرع الجزائري بموجب القانون رقم04-15[3] قسم خاص للمساس بأنظمة المعالجة الآلية للمعطيات يتضمن المواد من 394 مكرر إلى 394مكرر7.

والمشرع الجزائري لم يغفل عن عقوبة الشروع والتي نص عليها في المادة 394 مكرر7 والتي نصت على "يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، من خلال هذا النص يتضح لنا أن الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات تلبس وصف جنحة ولا عقاب على الشروع في الجنح إلا بنص. أما الاشتراك نصت عليه المادة 394مكرر5 قانون العقوبات الجزائري بقولها "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا

---

[1] الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق ل 08 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم، ج ر عدد 84، بتاريخ 24-12-2006.

[2] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري "دراسة مقارنة"، مذكرة مكملة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015-2016، ص44.

[3] القانون رقم 04-15، سالف الذكر.

القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

الفرع الثاني: الركن المادي

أولا: الاعتداء على أنظمة المعالجة الآلية للمعطيات

الدخول أو البقاء غير مشروع في نظام المعالجة الآلية للمعطيات قد نصت عليه المادة 394مكرر ق ع ج على أنه "يعاقب بالحبس من (03) أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من (06) أشهر إلى سنتين و الغرامة من 50000 دج إلى150000 دج.

هذا في ما يخص العقوبات الأصلية، أما في ما يخص العقوبات التكميلية فقد نصت عليهم المادة 394مكرر6، وتتمثل في المصادرة والغلق.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب نظام أشغال المنظومة[1].

ونستخلص من نص المادة 394 مكرر ق ع لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات الصورة الأولى تتمثل في الصورة البسيطة وهي مجرد الدخول أو البقاء غير المشروعين في النظام، والصورة الثانية هي الصورة المشددة تتحقق بتوفر الظروف المشددة وهي: حذف أو تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروعين، تخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين[2].

1/ الصورة البسيطة: يشمل النشاط الإجرامي في هذه الصورة الأفعال التالية:

أ/ فعل الدخول: يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبها، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات[3].

لم يقم المشرع الجزائري بتحديد الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام، أي أنها تقع بأي وسيلة أو طريقة كانت سواء مباشرة أو غير مباشرة.

إن جريمة الدخول الغير مصرح إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة،

---

[1] داود وسيلة، الجريمة الإلكترونية على ضوء قانون العقوبات الجزائري، مذكرة لنيل شهادة ماستر، جامعة عبد الحميد بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم قانون خاص،2019/2018،ص 37.

[2] بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة عبد الرحمان بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم قانون خاص،2019، ص25.

[3] بعرة سعيدة، المرجع السابق، ص51.

يكفي الوصول إلى المعلومات المخزنة بداخل النظام، فبمجرد الوصول إليها تقوم الجريمة[1].

ب/ فعل البقاء: هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام، وكما قد يجتمعان[2].

وللعلم يتحقق البقاء المعاقب عليه داخل النظام المعلوماتي مستقبلا عن الدخول للنظام أو قد يجتمع معا، ويكون البقاء معاقبا عليه مستقلا عندما يكون الدخول إلى النظام مصرحا به[3].

نظرا لاختلاف الطبيعة القانونية بين فعل الدخول غير المصرح والبقاء غير المشروع كذا يمكن وضعها في نص قانوني واحد حيث يعد فعل الدخول غير مصرح والبقاء غير المشروع جريمة شكلية[4].

2/ الصورة المشددة: كما نصت المادة394مكرر/02 سالفة الذكر على تضاعف عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عنهما إما محو أو تغيير للمعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء الوظائف نتيجة التخريب أو التعديل. إن ظرف التشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية لكي نقول أن الشرط متوفر. أما في الفقرة الثالثة من نفس المادة فقد شدد المشرع عقوبة المحو وتعديل المعطيات كل واحد على حدى تخريب نظام اشتغال المنظومة من جهة أخرى، وعقوبة هذه الأخيرة أشد لأن عقوبة المحو أو التغيير هي ضعف عقوبة الدخول والبقاء غير المشروعين[5].

ثانيا: الاعتداء العمدي على نظام المعالجة الآلية للمعطيات

بالنسبة للمشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام، واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة داخل النظام، وهذا راجع إلى تفسير أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه[6].

تشمل صورة هذا الاعتداء فعلين يتمثلان في:

1/ التعطيل(العرقلة): تفترض وجود عمل إيجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة سواء مادية أو معنوية وسواء إقترنت بالعنف أم لا[7].

2/ الإفساد: هو كل فعل و إن كان لا يؤدي إلى التعطيل، يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للإستعمال السليم وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[1].

---

[1] بن نعوم خالد أمين، المرجع السابق، ص26

[2] فتيحة مهري، جريمة الدخول والبقاء في أنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2016/2015، ص21.

[3] أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة الجلفة، الجزائر، العدد01، المجلد10، 2017،ص 485.

[4] بن نعوم خالد أمين، المرجع السابق، ص27.

[5] بن نعوم خالد أمين، المرجع نفسه، ص27.

[6] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط02، دار هومة لطباعة النشر والتوزيع، الجزائر، 2007، ص114.

[7] مراد مشوش، المرجع السابق، ص 116.

ثالثا: الاعتداءات العمدية على المعطيات

المشرع الجزائري نص عليه في المادة 394 مكرر2 من ق ع التي تنص على أنه "يعاقب بالحبس من شهرين(02) إلى ثلاثة (03) سنوات وبغرامة من1000000 إلى 5000000دج كل من يقوم عمدا وعن طريق الغش بما يلي:

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

2-حيازة أو إفشاء أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

ومن هنا نستخلص أن النشاط الإجرامي لجريمة الاعتداء العمدي للمعطيات يتجسد في صورتين:

1/ الاعتداءات العمدية على المعطيات الموجودة داخل النظام:تتجسد في ثلاث أفعال هي:

أ/ فعل الإدخال: يقصد بذلك إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، ولا على اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال، حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب[2].

ب/ فعل التعديل: يقصد به تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برامج الفيروسات بصفة عامة[3].

ج/ فعل المحو: هو إزالة جزء من المعطيات المسجلة على دعامة، والموجود داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[4].

وفي الأخير يمكن القول أن هذه الأفعال الثلاثة قد وردت على سبيل الحصر أي لا تقع تحت طائلة تجريم أي فعل آخر غير هذه الأفعال، وكذلك لم يشترط المشرع اجتماع هذه الصور، بل يكتفي أن يصدر عن الجاني فعل واحد من هذه الأفعال المجرمة لقيام الركن المادي.

2/ المساس العمدي بالمعطيات خارج النظام:

نص المشرع الجزائري على صورتين للمساس العمدي بالمعطيات خارج النظام، الصورة الأولى تتعلق بحماية المعطيات من استعمالها في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، والثانية تتعلق بحماية المعطيات

---

[1] أمال قارة، المرجع السابق، ص 119.

[2] ختير مسعود، المرجع السابق، ص124.

[3] أمال قارة، المرجع السابق، ص122.

[4] ختير مسعود، المرجع السابق، ص124.

المتحصل عليها من هذه الاعتداءات وذلك في نص المادة394 مكرر02 ق ع المشار إليها سابقا[1].

الفرع الثالث: الركن المعنوي

الركن المعنوي للجريمة الإلكترونية يختلف باختلاف أشكالها وعليه يجب التعرض للركن المعنوي لكل جريمة على حده.

أولا: جريمة الدخول والبقاء غير المشروع داخل النظام

إن جريمة الدخول والبقاء غير المشروع هي جرائم تتطلب قصدا جنائيا وذلك بنص المادة 394مكرر ق ع ج التي عبرت عن القصد الجنائي بنصها" كل من يدخل أو يبقى عن طريق الغش"[2].فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في هذا النظام غير مشروع.

يتطلب القصد الجنائي أن تتجه إرادة الجاني إلى فعل الدخول والبقاء وأن يكون على علم بأن ليس له الحق في ذلك أي لا يتوفر القصد الجنائي إن كان الجاني يعتقد أن فعله مشروع أو كان الجاني يجهل بوجود حظر الدخول أو البقاء ينتفي فيه القصد الجنائي.

ويتطلّب أيضا أن يتوقّع الجاني النّتيجة الإجرامية التي ستترتّب عن القيام بفعله، فتوقّع النتيجة هو أساس النّفي الذي تقوم عليه إرادتها، فحيث لا يكون التّوقّع لا نتصور الإرادة، والسلوك الذي يجب أن يتّجه إليها توقّع الفاعل هي النّتيجة التي يحددها القانون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات[3].

ولا يشترط توفر القصد الجنائي الخاص، فيكتفي توفر القصد العام بعنصريه العلم والارادة، ولا عبرة بالباعث أو الغاية. إذا أثبت الجاني انتفاء العلاقة السببية بين السلوك والنتيجة التي هي ذات الظرف المشدد في الجريمة، كأن يثبت أن تعديل أو محو المعطيات، أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة، أو الحادث المفاجئ، انتفى السلوك الإجرامي، وانتفى بذلك معه القصد الجنائي[4].

ثانيا: الاعتداءات العمدية على سير نظام المعالجة الالية للمعطيات

إن هذه الجريمة هي جريمة عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء غير المشروع داخل النظام، وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[5].

وهذه الاعتداءات تتطلّب القصد الجنائي العام من علم وإرادة ، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنّه يقوم بإحدى هذه الأعمال التي أوردها النّص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه

---

[1] بعرة سعيدة، المرجع السابق، ص57.

[2] بن نعوم خالد أمين، المرجع السابق، ص32.

[3] لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، جامعة أكلي محند أولحاج البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام،2015/2014، ص39.

[4] فتيحة مهري، المرجع السابق، ص43.

[5] أمال قارة، المرجع السابق، ص125.

يقوم بفعل الإدخال أو المحو أو التّعديل، ويعلم خطورة النّشاط الإجرامي الذي يقوم به وما يترتّب عنه من عقاب[1].

ثالثا: الاعتداءات العمدية على المعطيات

فيجب لقيام الركن المعنوي أن يتوافر القصد الجنائي العام، وهو ما عبرت عنه المادة 394 مكرر 02 بعبارة " كل من يقوم عمداً وعن طريق الغش".

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل توافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة[2].

المطلب الثاني: محل الجريمة الإلكترونية

محل الجريمة الإلكترونية هو الموضوع الذي تنطوي عليه الجريمة، وهو النظام المعلوماتي ففي هذه الحالة إما أن يكون محل الاعتداء هو المكونات المعنوية للنظام المعلوماتي كالبيانات والبرامج[3]، أو يكون محل الاعتداء على المكونات المادية للنظام المعلوماتي ولكنها تعتبر ضمن نطاق الجرائم التقليدية لأنها تستهدف المال كالسرقة لشاشة الحاسب. ولعل جرائم المعلوماتية والإنترنت تستهدف أحد أو كل العناصر التالية:

الفرع الأول: المعلومات

تشمل الجرائم المعلوماتية في هذه الحالة سرقة أو تغيير أو حذف المعلومات فمثلا في حالة النشاط الإجرامي الذي يستهدف اختراق بريد إلكتروني والعبث بمحتوياته أو سرقة المعلومات المخزنة في موقع ما، ما هو إلا للاستفادة منها بما يحمل في طياته بعض من انتهاك للخصوصية وحقوق الملكية الفكرية وأنماط الجرائم الاخرى[4].ففي هذه الحالة يجب أن تكون المعلومات بمفهومها الواسع هي وحدها محلا للجريمة المعلوماتية، ومن ثم فقد اعتبرت الجريمة المعلوماتية من طائفة الجرائم التي تنصب على المعلومات بكل أنواعها، سواء المداخلة أو المعالجة أو المخزنة داخل الجهاز وتستهدف هذه الجرائم الحق في المعلومات، ويمتد الحق في المعلومات ليشمل الحق في انسيابها وتدفقها[5].ومن أمثلتها سرقة المعلومات المخزنة في موقع ما و الاستفادة منها بما يحمل في طياته بعض من انتهاك الخصوصية[6].

---

[1] العاقل فريال، المرجع السابق، ص40.

[2] أمال قارة، المرجع السابق، ص ص 125- 126.

[3] وسيم حسام الدين الأحمد، المرجع السابق،ص99.

[4] عبد الله عبد الكريم عبد الله، المرجع السابق، ص18.

[5] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2012، ص37.

[6] شنتير خضرة، الآليات القانونية لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية ،قسم الحقوق، 2012/2011،ص21.

الفرع الثاني: الأجهزة (أجهزة الحاسوب وملحقاتها)

الأجهزة هي المستهدف الأول وقد يكون الأوحد وذلك بقصد تعطيل أجهزة الكمبيوتر أو تخريبها عبر إرسال الفيروسات والبرامج التي تحتوي أنظمة هجومية مما يسبب تلفا في أنظمة الكمبيوتر يؤدي لشلل كل الأنشطة المرتبطة بهذا الجهاز أو الأنظمة المرتبطة به. ولنتصور مدى الدمار والخسائر التي ستلحق بشبكة مصارف مرتبطة بأنظمة عبر الكمبيوتر المركزي يحوي حسابات عملاء فمن الذي سيحصل لو تم تعطيل الكمبيوتر المركزي أو إتلاف أنظمته[1]. فالجهاز هو الأداة الأساسية للولوج إلى الشبكة، بدونه لا تستطيع إدراج أي معلومة لذلك يجب حماية الأجهزة من أي تعطيل وتخريب[2].

الفرع الثالث: الأشخاص أو الجهات

الجريمة إما أن تستهدف شخص محددا أو جهة معينة وتقع بصورة مباشرة أو غير مباشرة ومثالها جرائم التهديد أو الحض على الفجور[3]، تهدف فئة كبيرة من الجرائم على شبكة الأنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الإبتزاز أو السرقة أو ممارسة الفاحشة، فمثلا سرقة المال عبر الأنترنت باستخدام أرقام لبطاقات مصرفية تعود للغير، أو الحض على الفجور وممارسة الفاحشة مع قاصر عبر الأنترنت أو الإرشادات التي تحمل في طياتها تعليمات إرهابية كلها موجهة ضد أشخاص أو جهات بعينها[4].

المطلب الثالث: خصوصية مرتكب الجريمة وضحاياها

إن الجريمة الإلكترونية كغيرها من الجرائم تتطلب وجود فاعلين في الدعوى العمومية من مرتكب الجريمة والضحية، غير أنه يعتبر أن أطراف الجريمة الإلكترونية يختلف نوعا ما عن أطراف الجريمة العادية، المجرم في جرائم الأنترنت ليس مجرما عاديا فهو من الخبراء في هذه التقنية أو النابغين فيها سواء كان من الأحداث أو البالغين، ولذلك قيل أن الجريمة المعلوماتية جريمة متخصصة، بمعنى لا يقترفها سوى مجرم له طبيعة خاصة.

الفرع الأول: من حيث مرتكب الجريمة الإلكترونية

أولا: تعريف مرتكب الجريمة الإلكترونية

يطلق فقهاء القانون الجنائي عليه مصطلح المجرم المعلوماتي وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السرى لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه[5]. فالجرم المعلوماتي هو شخص سواء طفل أو رجل ذكر أو أنثى يأتي أفعالا لا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلومات لإحداث فعل إجرامي بالاعتداء على حق أو مصلحة وهم يتمتعون بالذكاء والفطنة والقدرة على

---

[1] عبد الله عبد الكريم عبد الله، المرجع السابق، ص ص18-19.

[2] شنتير خضرة، المرجع السابق، ص 24.

[3] وسم حسام الدين الأحمد، المرجع السابق، ص100.

[4] عبد الله عبد الكريم عبد الله، المرجع السابق، ص19

[5] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية،ط01،دار النشر،1430ه-2009م، ص143.

التحكم في تقنية الحاسوب والمعلومات والإنترنت[1]. يمكن القول بأن المجرم المعلوماتي تعبير ينطوي على قدر من التجاوز في القول، فالصحيح أنه لا يوجد نموذج محدد للمجرم المعلوماتي، بل هناك عدة نماذج للمجرمين قد يستخدمون الكمبيوتر في جرائمهم قد يقومون بأفعال إجرامية ضد نظام الكمبيوتر نفسه[2].
وسبب الرئيسي لظهور ما يعرف بالإجرام المعلوماتي والاستخدام المطرد للمعلوماتية سواء كان في شكل أموال معلوماتية أو أساليب مستخدمة وهذه هي الخلاصة والنتيجة القطعية تقدم علمي أو تقني مستحدث[3].
وتقترب سمات المجرم المعلوماتي في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء، حيث أن كلا من هؤلاء المجرمين قد يكون من ذوي المناصب رفيعة المستوى ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء والقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه[4].

ثانيا: سمات مرتكب الجريمة الإلكترونية

يتميز مرتكب الجريمة الإلكترونية بجملة من الخصائص تميزه عن غيره من المجرمين، فهو يتصف بسمات خاصة جعلت منه محلا لكثير من الأبحاث والدراسات، ومنها ما يلي:

1/ يتمتع بالمهارة والمعرفة والذكاء:

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والأنترنت، بل أن بعض مرتكب هذه الجرائم هم من متخصصين في مجال معالجة المعلومات آليا[5].
تعد المهارة المطلوبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، ويجب التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها و احتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم[6].

2/ إنسان متكيف اجتماعيا بطبعه:

المجرم الإلكتروني شخص اجتماعي قادر على التكيف في بيئته الاجتماعية والتصالح معها، شعور المجرم أنه محل ثقة من مجتمعه، وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدي رجال القضاء[7].

3/ مجرم متخصص:

---

[1] يوسفي عبد الهادي، علم الإجرام المعلوماتي، محاضرات مقدمة لسنة ثانية ماستر حقوق، قانون جنائي وعلوم جنائية،2021/2020، ص03.
[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي "دراسة قانونية متعمقة في القانون المعلوماتي، د ط، دار الكتب القانونية للنشر،مصر،2007، ص 81.
[3] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، د ط، دار الفكر الجامعي للنشر،الإسكندرية،2007، ص 46.
[4] نهلا عبد القادر المومني، المرجع السابق، ص76.
[5] نهلا عبد القادر المومني، المرجع السابق، ص77.
[6] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص176.
[7] نهلا عبد القادر المومني، المرجع السابق، ص 79.

المجرم المعلوماتي مجرم متخصص له القدرة الفائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل شيء غالي وثمين من البيانات والمعلومات الموجودة على أجهزة الحاسوب ومن خلال الشبكات[1].

4/ يتمتع بالسلطة تجاه النظام المعلوماتي:

ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتية التي تمكنه من ارتكاب جريمته، كثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة فتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها[2].

5/ مجرم عائد الإجرام:

غالبا ما يعود مرتكب الجرائم المعلوماتية إلى ارتكاب جريمة أخرى في مجال المعلوماتية وذلك لسد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحكمة في المرة السابقة، وقد ينتهي بهم الأمر كذلك في المرة الثانية إلى كشفهم وتقديمهم إلى المحاكمة[3].

ثالثا: فئات مرتكبي الجريمة الإلكترونية

الجريمة المعلوماتية جريمة مستحدثة بلغ منها التطور الحد الذي يجعل لمسة زر فقط كافية لإسقاط أنظمة الحماية والحواجز الأقوى تشفير عن المعلومات الأكثر سرية، رغم ذلك يمكننا أن نبين بعض من فئات و طوائف لهؤلاء المجرمين، تجدر بنا الاشارة إلى أن ليس كل مجرم يندرج تحت فئة معينة فقط دون غيرها من الفئات التي سنذكرها بل يمكن أن يكون المجرم الواحد يندرج تحت أكثر من فئة في آن واحد.

1/ فئة القراصنة:

قراصنة المعلومات هم عادة مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة[4]. ويمكن تصنيف القراصنة الى صنفين هما:

أ/ القراصنة الهواة العابثون(الهاكرز):

الهاكرز وهم المتطفلون الذين يتحدون أمن النظم المعلوماتية والشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنما ينطلقون من هدف اكتساب الخبرة أو بدافع الفضول أو لمجرد التحدي وإثبات الذات[5].

---

[1] الشافعي مالكية، تكنولوجيا المعلومات الحديثة وأثارها في تسريب أسئلة البكالوريا وأسئلة التعليم المتوسط بالجزائر2015 ،الملتقى الوطني" الأمن المعلوماتي :مهدداته وسبل الحماية"، الممارسات اللغوية في الجزائر، جامعة مولود معمري،03-2015/11/04،ص ص 100-101.

[2] نهلا عبد القادر المومني، المرجع السابق، ص80.

[3] عبد الفتاح بيومي حجازي، المرجع السابق، ص83.

[4] نهلا عبد القادر المومني، المرجع السابق، ص 83.

[5] سعيداني نعيم، المرجع السابق، ص54.

ب/ القراصنة المحترفين (الكراكرز):

هذا الصنف هو الأكثر خطورة من الصنف الأول وقد يحدثون أضرارا كبيرة، وقد يؤلفون أندية لتبادل المعلومات فيما بينهم. فيفضل القراصنة العمل عادة في جماعات عن العمل الفردي، فقد أثبت الواقع العملي أن الهاكرز يستعين بالكراكرز إذا ما صادفه أي نوع من أنواع الحماية، وغالبا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة[1].

وفي الأخير يمكننا القول انه هناك تباينا جوهريا بين المصطلحين ،الهاكرز متطفلين يتخذون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الكراكرز فإن اعتداءاتهم تعكس ميولا جريمة خطرة تنبئ عنها رغباتهم في إحداث التخريب[2].يطلق خبراء أمن المعلومات الإلكترونية مصطلح "هاكر" على من يخترق الحاسب الآلي، ومصطلح كراكرز على الفئة التي لديها قدرة على الاختراق[3].

2/ فئة صغار ونوابغ المعلوماتية:

وهم الشباب البالغ المفتون بالمعلوماتية وتتمثل أفعالهم في الانتهاك غير المسموح به في ذاكرات الحاسبات الآلية وإن كانت وسائل الاعلام المرئية تحاول التضخم من هذه الظاهرة التسويق وسائلهم لأن هؤلاء الشباب مفتونين بهذه الأنشطة الإجرامية المبتكرة والمستحدثة [4].

ومن الأمثلة على الجرائم التي ترتكب من هذه الفئة، العصابة الشهيرة التي أطلق عليها (عصابة 414)، والتي نسب إليها ارتكاب ستون فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحواسيب[5].

3/ فئة مجرمو المعلوماتية أصحاب الآراء المتطرفة:

يعرف التطرف في هذا المجال بأنه عبارة عن أنشطة توظف شبكة الأنترنت في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري[6]. وتتكون هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات أو أفكار اجتماعية أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامي[7].

4/ فئة الموظفون العاملون في مجال الأنظمة المعلوماتية:

---

[1] سعيداني نعيم، المرجع نفسه، ص54.

[2] وسيم حسام الدين الأحمد، المرجع السابق، ص74.

[3] مصطفى محمد موسى، المرجع السابق، ص 143.

[4] سامي علي حامد عياد، المرجع السابق، ص52.

[5] لاحظ عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات،ط01، دار المستقبل للنشر والتوزيع،عمان،1430ه-2019م ، ص164.

[6] صغير يوسف، المرجع السابق، ص29.

[7] عبد السلام محمد المايل "وأخرون" ،الجريمة الإلكترونية في الفضاء الإلكتروني "المفهوم -الأسباب-سبل المكافحة مع التعرض لحالة ليبيا" ،مجلة أفاق للبحوث والدراسات سداسية دولية محكمة، المركز الجامعي إليزي، العدد 04، 2019،ص248.

بحكم طبيعة عمل هؤلاء الموظفين ونظراً لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظراً للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها[1].

5/ فئة مجرمي المعلوماتية في إطار الجريمة المنظمة:

تتخذ الجريمة المنظمة مفهوما أكثر اتساعا من عصابات المافيا، حيث تشمل كل منظمة ذات هيكل محدد، وتوزع عائد أنشطتها الإجرامية على أعضائها، إلا أن الجريمة المنظمة بالمعنى الدقيق تطلق على عصابات المافيا، ورغم عدم دخول الجريمة المنظمة عالم الإجرام المعلوماتي بشكل كبير حتى الآن، إلا أنه من المتوقع دخولها هذا المجال على نحو واسع، وذلك لارتفاع عائد للجريمة المعلوماتية[2].

6/ فئة المتجسسين:

لقد تغيرت وسائل التجسس من طرق التقليدية وتطورت إلى طرق حديثة لاستخدامها تقنية الأنترنت، وهذا بسبب ضعف الوسائل الأمنية التي تستخدمها الدول أو المؤسسات في حماية شبكاتهم. وذلك من خلال اختراق هذه الشبكات من قبل القراصنة و إتلاف أو سرقة المعلومات المخزنة.

فالخطر الحقيقي على تلك المواقع يكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها إلى دول أخرى معادية أو استغلالها لما يضر المصلحة الوطنية لتلك الدولة. هذه الطائفة غير مرتبطة بغرض محدد، إذ أن أغلب من يقومون بهذا العمل هم موظفون لدى الدول أو الشركات والمؤسسات التي يعملون بها، فليس لهذه الطائفة أهداف شخصية[3].

7/ فئة الحاقدون:

هذه الطائفة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم يحركون أنشطتهم رغبتا في الإنتقام ، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم[4]، تعتبر هذه الفئة مقارنة بالفئات السابقة أقل خطورة منهم ومن السهل كشف الأنشطة التي يقومون بها وذلك لتوفر ظروف وعوامل تساعد على ذلك[5].

تختلف الجريمة الإلكترونية عن الجريمة التقليدية أيضا من خلال الدوافع، وهذا ما سنحاول التطرق له.

---

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

[2] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2012/2011، ص43.

[3] صغير يوسف، المرجع السابق، ص ص 30-31.

[4] عبد الحكيم رشيد توبة، المرجع السابق، ص163.

[5] هروال هبة نبيلة، المرجع السابق، ص ص 54-55.

رابعا: دوافع ارتكاب الجريمة الإلكترونية

حسب ما تتطلب طبيعة المجرم و مدى ثقافته وعلمه في مجال التكنولوجيا، تختلف الدوافع المؤدية لارتكاب الجريمة الإلكترونية، هذا هو السبب في تنوع الدوافع في منها شخصية، وأخرى خارجية.

1/ الدوافع الشخصية:

هي عوامل لصيقة بالشخص ذاته، وتصنف هذه الدوافع إلى دوافع مادية، ودافع الرغبة في التعلم، ودوافع ذهنية أو نمطية و هذا ما سنفصل فيه :

أ/ الدوافع المادية: من أجل تحقيق المكاسب المالية يتم اللجوء إلى ارتكاب الجريمة المعلوماتية إما عن طريق المساومة على البرامج أو المعلومات المتحصلة بطريقة الاختلاس من جهاز الحاسوب، أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية وغير ذلك الكثير[1].

فهي من أهم الدوافع والأكثر انتشارا، ففي الغالب يكون الباعث وراء ارتكاب الجريمة هو وقوع الجاني في ضيق مادي فيعجز مثلا عن سداد ديونه، ففي حالة نجاح العملية التي خطط لها سيحقق أرباح هائلة في زمن القياسي.

ب/ الرغبة في التعلم: يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع إلى ارتكاب مثل هذه الجرائم لأن المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب أن لا تبقى المعلومات حكرا على أي أحد[2].

ج/ دوافع ذهنية أو نمطية: غالبا ما يكون الدافع وراء ارتكاب الجريمة الإلكترونية هو المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات، في اختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعه كبيرة لمرتكبها وتسلية تغطي أوقات فراغه[3].

يتزايد شيوع هذا الدافع لدى فئة صغار السن الذين يقضون وقتا طويلا أمام حواسبهم الشخصية في محاولة إظهار تفوقهم على وسائل التقنية[4]. فهو من أكثر الدوافع التي يتم استغلالها من قبل المنظمات الإجرامية.

بالإضافة لهذه الدوافع الشخصية فهناك دوافع أخرى خارجة عن نطاق مرتكب الجريمة الإلكترونية تدفعه لارتكابها وهذا ما سنتطرق له في العنصر الموالي.

2/ الدوافع الخارجية:

قد يتأثر مرتكب الجريمة ببعض المواقف تدفعه إلى اقترافه للفعل المجرم ولا تكون بدوافع أخرى غير تلك التي تم ذكرها سابقا وهذا ما سنتطرق له.

أ/ دافع الإنتقام وإلحاق الضرر برب العمل: نزعة الإنتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ومنها التي يقوم بها موظف تم فصله من العمل أو تخطيه في الحواجز أو الترقية[5].

---

[1] نهلا عبد القادر المومني، المرجع السابق، ص90.

[2] داود وسيلة، المرجع السابق، ص24.

[3] رمزي حوحو، منيرة بلوزغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، العدد 02، 2014، ص51.

[4] سوير سفيان، المرجع السابق، ص ص 27-28.

[5] شنتير خضرة، المرجع السابق، ص36.

ب/ دافع التعاون والتواطؤ: هذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[1].

3/ دوافع أخرى:

الدوافع السابقة ليست هي الوحيدة بل هناك دوافع أخرى تدفع لارتكاب الجريمة الإلكترونية ومن أبرزها: دوافع سياسية، التنافس السياسي والاقتصادي، مناهضة العولمة .

التسابق العسكري بين الدول، الدعوة للإلحاد، المنافسة التجارية أو التجسس العسكري أو الصناعي، عمليات غسيل الأموال[2]، ضعف انفاذ القانون وتطبيقه في الجريمة الإلكترونية فهناك الكثير من الدول التي لم تطور شرعيتها وأجهزة العدالة فيها[3].

هذه هي أبرز الدوافع التي تدفع مرتكب الجريمة للاعتداء على أنشطة نظام المعالجة الآلية، إلا أنها غير ثابتة ومتعددة لدى كل من الفقهاء والباحثين لأنها قد تتغير تتحول بسرعة في حالة العبث والتحدي وغيرها، لا تتوقف عند هذا الحد، لأنه في كل جريمة جديدة تتكون دوافع جديدة.

خامسا: أساليب ارتكاب الجريمة الإلكترونية

وتتنوع كذلك أساليب ارتكاب الجريمة الإلكترونية من قبل مجرمي المعلوماتية، وذلك لوجود تقنيات مختلفة لتنفيذ مخططاتهم، حتى وإن أمكن حصر هذه الأساليب في الوضع الراهن إلا أنه لا يمكن التنبؤ بالتقنية التي قد تستحدث وتتطور، وهذا ما سنحاول شرحه في ما يلي:

1/ الفيروسات(الفيروس المعلوماتي):

هو برنامج خادع يخفي ظاهرة غرضها غير مشروع ويظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدميه بينما يكون بداخله وبطريقة خفية بعض الأوامر أو التعليمات التي تؤدي عند تشغليه مهاما ضارة غير متوقعة تمثل أغراضه الحقيقة المضرة[4].

الفيروس المعلوماتي يقترب في خصائصه من المجرم أثناء ارتكابه الجريمة، فهو يختفي كخطوة أولى ثم يبدأ في الظهور كخطوة ثانية ليدمر في الخطوة الثالثة، وهو كالمجرم الذي يضع خطته لارتكاب الجريمة. كما أنه قد يتخذ لنفسه طريقة مستقلة[5].

---

[1] سعيداني نعيم، المرجع السابق، ص62.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 94.

[3] دياب موسى البادية، الجرائم الإلكترونية "مفهوم والأسباب"، الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية،عمان،7-9/ 11/ 1435ه الموافق ل 2-4/ 09/ 2014م، ص15.

[4]زبيخة نور الهدى، الإثبات الجنائي في الجرائم الالكترونية، مذكرة لنيل شهادة الماستر، جامعة العربي بن مهيدي ،أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015،،ص19.

[5] سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الانترنت،ط01،منشورات الحلبي الحقوقية،لبنان،بيروت،2011، ص ص 326-327.

هناك صعوبة في حصر أنواع الفيروسات بسبب تعددها وتزايدها المستمر في التطور، و يمكن ذكر بعض من أنواع الفيروسات مثل فيروسات الجزء التشغيلي للأسطوانة، الفيروسات المتطفلة، فيروسات قطاع الإقلاع، فيروسات الماكرو، حصان طروادة[1].

2/ برنامج الدودة:

هو عبارة عن برمجية تقوم بالإنتقال من حاسوب إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها، وخاصة التنشيط الذاتي، وبهذا تختلف الدودة عن حصان طروادة إلا أنها لا تلتصق بنظام التشغيل في الحاسوب الذي تصيبه وتتسبب حركة الدودة في تعطيل الحاسوب بتجميد لوحة المفاتيح والشاشة وتعبئة الذاكرة وتبطئة الحاسوب[2].

3/القنبلة الموقوتة: وهي نوعين

أ/ القنبلة المنطقية: هي تعمل عند حدوث ظروف معينة وتصمم من قبل أحد المبرمجين المخربين في المنظمة ،بحيث تبرمج لتعمل عند حذف اسم الخرب(واضع القنبلة) من كشوف الرواتب مثلا، فتؤدي إلى تخريب بعض النظم ومسح بعض البيانات[3].

ب/ القنبلة الزمنية أو المؤقتة: هي عبارة عن برامج يتم إدخالها بطرق مشروعه متخفية في برامج أخرى، تهدف إلى تدمير برامج ومعلومات النظام وتغييرها وتعمل على مبدأ التوقيت حيث تنفجر في وقت معين[4].

4/ قرصنة البيانات والمعلومات: ويشمل اعتراض البيانات خطفها بقصد الإستفادة منها وخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر[5].

5/ قرصنة البرامج: وهي حيازة أو استخدام برامج الحاسب بدون ترخيص من المالك أو إعادة إنتاج برامج محمية دون تصريح[6].

6/ التلاعب بالمعلومات: من الممكن أن يلجأ الجاني إلى التلاعب بالمعلومات، كأسلوب يبتغي من ورائه تحويل كل أو جزء من أرصدة الغير أو فوائدها إلى حسابه أو حساب أشخاص آخرين يتم الإتفاق معهم مقابل مادي[7].

وهناك أساليب متعددة ومتنوعة منها أسلوب تقريب الأرقام، أسلوب السجق، أسلوب الباب السحري، أسلوب البرامج المعدلة لأغراض محددة، غش البيانات،

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2006، ص ص 51 الى 54.

[2] حسين فريجه، الجريمة الإلكترونية والأنترنت، مجلة المعلوماتية، العدد36، أكتوبر 2011، ص06.

[3] خديجة حامي، الأنظمة المعلوماتية في مواجهة القرصنة والتخريب "المخاطر المحدقة والحلول الناجعة"، الملتقى الوطني"الأمن المعلوماتي: مهدداته وسبل الحماية"، مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري،03-2015/11/04،ص46.

[4] نهلا عبد القادر المومني، المرجع السابق، ص 133.

[5] دياب موسى البادية، المرجع السابق، ص23.

[6] وسيم حسام الدين الأحمد، المرجع السابق،ص155.

[7] سليم عبد الله الجبوري، المرجع السابق، ص329.

التزوير، تسريب البيانات، التنصت على الاتصالات السلكية و اللاسلكية، الهواية، الخداع الإلكتروني[1].

الفرع الثاني: من حيث الضحية

قد تم تعريف الضحايا وفق الإعلان العالمي الذي يتضمن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها رقم 401434 الصادر في 1985/11/29 في فقراتها(1*2*3)[2].

يبنى على ذلك أن الضحية في الجريمة بصفة عامة كل شخص طبيعي أو معنوي أصيب بخسارة أو ضرر أو بعدوان نتيجة ارتكاب جريمة سواء بفعل أو بالامتناع عن فعل أما المقصود بالضحية في الجريمة المعلوماتية هو كل شخص أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع لتقنية المعلومات، وقد يكون شخصا عاما ممثلا في مؤسسات الدولة وهيأتها وقد يكون خاصا ممثلا في الأشخاص الطبيعية أو المعنوية وبحسب ذلك فإن الضحايا في الجريمة المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية[3].

إن الغالبية العظمى من هذه الجرائم تقع على شخص معنوي، إلا أن المعلومات المجردة تعد في الوقت الحاضر من أهم المصالح المستهدفة بعد الأموال وخصوصا إذا كانت هذه المعلومات ذات أهمية بالغة[4].نظرا لطبيعة استخدام تقنية المعلومات في جميع المعاملات الاقتصادية والمالية الوطنية والدولية والاعتماد عليها في تسيير شؤون الحياة اليومية بالنسبة للأفراد والشؤون العامة بالنسبة للحكومات كان من شأن ذلك أن يضفي أبعادا غير مسبوقة في توسع دائرة المتضررين من الجرائم المعلوماتية وتعدد فئاتهم[5]. فمن الصعب تقدير حجم الجريمة المعلوماتية عن طريق تحديد الضحايا في هذه الجرائم، وربما سبب ذلك يعود إلى عدة عوامل منها ما يتعلق بالجريمة ذاتها ومنها ما يتعلق بالضحايا أنفسهم.

برغم من انعدام الدقة في الإحصائيات التي تخص حجم جرائم العالم الافتراضي إلا أن ذلك يساعد في إعطاء مؤشر واضح عن مدى كثرة المتضررين منه.

لقد تعددت الجرائم المعلوماتية حدود المعلومات المالية والتجارية والصناعية وكذلك الشخصية لتمس المعلومات العسكرية التي تتمثل في أسرار الدولة والتي تشكل خطرا كبيرا نظرا لأهمية المعلومات التي تحتويها فقد يتسبب بظهور حرب من نوع جديد وهي الحرب المعلوماتية.

لا يقتصر تصنيف الضحايا فقط على قطاعات المالية والجهات الحكومية، بل يتعدى إلى الأشخاص الطبيعيين، وأيضا فإن من ضحايا الجريمة الإلكترونية فئة

---

[1] عبد الحكيم رشيد توبة، المرجع السابق، ص ص 171-172.

[2] لاحظ مصطفى محمد موسى، المرجع السابق، ص158.

[3] رمزي حوحو و منيرة بلوزغي، المرجع السابق، ص49.

[4] لامية طالة، الجريمة الإلكترونية "بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي"، مجلة الرواق للدراسات القانونية والسياسية، جامعة الجزائر، العدد2، المجلد6، 2020، ص74.

[5] رمزي حوحو و منيرة بلوزغي، المرجع السابق، ص49.

مقدمي الخدمات الوسطية في نطاق شبكة الإنترنت وهم الأشخاص الدين يقومون بالمساعدة للوصول إلى شبكة الإنترنت، فيمكن أن يكون هو الوسيط بين الزبون(العميل) و الضحية، وهؤلاء الأشخاص هم متعهد الوصول، متعهد الإيواء، متعهد الخدمات[1].

[1]سعيداني نعيم، المرجع السابق، ص 66.

في نهاية هذا الفصل يتضح لنا أن الجريمة الإلكترونية هي جريمة مستحدثة ناتجة عن الممارسة السيئة لتكنولوجيا المعلومات والتي تستهدف الاعتداء على المعطيات أو الاستعانة بها لارتكاب مختلف الجرائم، فقد حاولنا في هذا الفصل تحديد مفهوم هذه الجريمة من خلال استعراض المقصود منها، وتحديد طبيعتها الخاصة، ثم تبيان خصائصها والتي من أهمها كونها متعدية الحدود و كذا طابعها التقني الذي جعل مسألة إثباتها صعبة ومعقدة، وكذلك خصائص مرتكبيها التي يتميز بها عن باقي الجرائم الأخرى، وهذا ما جعل من دوافعهم تختلف عن المجرمين العاديين ، كذلك كونها تتطلب قدرا كبيرا من الذكاء والتقنية العالية، بالإضافة إلى استيضاح موقف المشرع الجزائري من هذه الجريمة والذي اصطلح على تسميتها بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون15-04، وهذه الجريمة كغيرها من الجرائم الأخرى لها أركان تقوم بقيامها وتزول بزوال أحدها.

وتوصلنا أيضا إلى كون الضرر الناجم عن الجريمة قد يكون كبير جدا ويمتد إلى عدد كبير من الضحايا، فبسبب خطورتها جعلت منها عائقا يواجه مختلف مظاهر الحياة الأمنية والمالية و الاقتصادية و الاجتماعية.

الفصل الثاني: آليات مكافحة الجريمة الإلكترونية

بعد التطرق إلى الأحكام العامة للجريمة الإلكترونية، من خلال تعريفها وطبيعتها وبيان أنواعها وتحديد أركانها ومعرفة دوافع ارتكابها و أساليبها. نتعرض في هذا الفصل إلى بيان آليات مكافحتها أي كيفية التصدي لها من طرف المشرع الجزائري و توفير الحماية الموضوعية عن طريق استحداث قانون جديد 09-04 سالف الذكر، وكذا تعديل قانون العقوبات وقانون الإجراءات الجزائية، و كذلك توفير حماية إجرائية لنظام المعلوماتي من خلال وسائل مستحدثة للكشف عن هذه الجرائم التي تعتبر بالغة الخطورة وصعبة الإثبات وملاحقة مرتكبها، وهذا ما سيتم توضيحه في المبحثين التاليين.

فلم يكن لدى المشرع الجزائري خيار أخر للتصدي لظاهرة الإجرام الإلكتروني في بداية ظهوره إلا باعتماده على النصوص الجزائية القائمة بمختلف فروعها الموضوعية والإجرائية، وهذا لتفادي إفلات مرتكبي هذه الجريمة من العقاب هذا من جهة، ومن جهة أخرى عدم وجود قواعد قانونية تتلاءم مع طبيعة هذه الجرائم المستحدثة، ولكن بعد التطور السريع الحاصل في مجال تكنولوجيا المعلومات وما صاحبه من انعكاسات على الجرائم، جعل من هذه القوانين غير نافعة وغير مواكبة لها قام بتوفير حماية قانونية وحماية إجرائية.

ومن خلال هذا الموقف ارتأينا أن تكون نقطة الانطلاق من عنوان هذا الفصل الذي تم تقسيمه الى مبحثين، فنستعرض في المبحث الأول (المواجهة الموضوعية للجرائم الإلكترونية)، و (المواجهة الإجرائية لها) في البحث الثاني.

المبحث الأول: المواجهة الموضوعية للجريمة الإلكترونية

لابد من الاعتراف بأن المحاولة في اقتراح حلول المشكلة التي يطرحها موضوع الحماية الموضوعية للمعلوماتية مهمة صعبة سبب ذلك راجع إلى اتساعها وتشعب موضوعاتها والجوانب التي تتعلق بها، كون أن المعلومة التي يحتفظ بها جهاز الحاسب الآلي في حد ذاتها تمثل قيمة مالية كبرى أو ثروة اقتصادية أو سر من أسرار الدولة كما تم ذكرهم سابقا، هذا ما جعل منها جريمة خطيرة في المجتمع بل في العالم أجمع، لهذا استوجب على المشرع الجزائري توفير حماية جنائية خاصة بها كونها تختلف عن الجرائم التقليدية التي أصبحت نصوصها غير كافية لتطبيقها على الجرائم المستحدثة، فبات من الضروري استحداث قواعد قانونية جديدة لمواجهتها.

نعرض المواجهة الموضوعية للجريمة الإلكترونية من خلال تقسيمنا لهذا المبحث إلى مطلبين، في المطلب الأول تناولنا (الحماية القانونية في النصوص العامة)، و في المطلب الثاني(الحماية القانونية في النصوص الخاصة).

المطلب الأول: الحماية القانونية في النصوص العامة

لقد تدارك المشرع الجزائري مؤخرا الفراغ القانوني في مجال الإجرام الإلكتروني ذلك عن طريق استحداث نصوص تجريمية لمحاربة الاعتداءات الحاصلة على المعلوماتية ذلك بوجب القانون 04-15 المعدل لقانون العقوبات، وكذلك فقد عدل من قانون الإجراءات الجزائية لمواكبة التطور الحاصل، لهذا سنتطرق في هذا المطلب إلى (الحماية في الدستور الجزائري) في الفرع الأول، (الحماية في قانون العقوبات) في الفرع الثاني، و(الحماية في قانون الإجراءات الجزائية) في الفرع الثالث.

الفرع الأول: الحماية في الدستور الجزائري

لقد كفل المشرع الجزائري الحقوق والحريات الفردية حماية، وقد تم تكريس المبادئ الدستورية بواسطة تطبيق نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية و قوانين خاصة أخرى ، فقد سعى المشرع إلى حماية الحقوق من جميع الانتهاكات بمختلف أشكالها.

الفرع الثاني: الحماية في قانون العقوبات الجزائري

كما سبق وقد أشرنا في بداية بحثنا أن المشرع الجزائري قام بتعديل قانون العقوبات الجزائري بموجب القانون 04-15 وذلك للحد من الاعتداءات الصادرة ضد الأنظمة المعلوماتية، لهذا تجدر الإشارة أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية أو ما يعرف بالغش المعلوماتي، و أغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي المتمثلة في التزوير المعلوماتي[1].وقد تطرقنا سابقا إلى أهم الأحكام الخاصة بالجرائم الماسة بالأنظمة المعلوماتية مع تحديد كل من الركن المادي والمعنوي وكذا الجزاءات المقررة لها من خلال جرائم:

-الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

-الاعتداءات العمدية على سلامة المعطيات الموجودة داخل وخارج النظام.

- الاعتداء العمدي على نظام المعالجة الآلية للمعطيات.

أولا: جرائم المساس بالأنظمة المعالجة الالية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي، وهو الفعل المنصوص والمعاقب عليه في المواد من 394 مكرر إلى المادة 394مكرر7، ونجد أن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي، وكذلك الفقه الفرنسي[2]. إذ أنه لابد من التعرض أولا إلى مفهوم نظام المعالجة الالية للمعطيات.

1/ تعريف نظام المعالجة الآلية للمعطيات:

يعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الاعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، إذ أن هذا الشرط يعتبر عنصرا لازما لكل منها[3].

وهو تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[4].

وقد عرف مجلس الشيوخ الفرنسي هذا النظام بأنه كل مجموعة متألفة من وحدة أو عدة وحدات لمعالجة المعلومات أو اختزانها أو إعداد البرامج أو المعطيات وكل ما يؤدي إلى إدخال واسترجاع المعلومات[5].

---

[1] فليح نور الدين، المرجع السابق، ص 77.

[2] العاقل فريال، المرجع السابق، ص 45.

[3] خثير مسعود، المرجع السابق، ص 108.

[4] أمال قارة، المرجع السابق، ص 101.

[5] Bologna Jack, RobertK G, Lindquist : Fraud Audttng. And forensic accounting, New tools and

فقد تبنى المشرع تعريفها في المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي سماها بالمنظومة المعلوماتية[1].

وبناء على هذه التعريفات نتوصل أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين، العنصر الأول مركب يتكون من عناصر مادية ومعنوية مختلفة تربط بينها نتيجة علاقات توحدها نحو تحقيق هدف محدد، أما الثاني فهو ضرورة خضوع النظام لحماية فنية[2].

2/ مكونات النظام:

العناصر المادية والمعنوية التي يتكون منها المركب جاءت على سبيل المثال لا الحصر، لفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال. ومثال على ذلك البرامج، المعطيات، أجهزة الرد[3].

وهذا يفتح المجال أمام عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال، أي أنه لا تقع أي جريمة من جرائم الاعتداء المنصوص عليها إذ وقع على عنصر بمفرده كما إذ وقع هذا الاعتداء على برامج معروضة للبيع أو على جهاز حاسب لم يدخل الخدمة....إلخ .ولكن على عكس ذلك تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره أو النظام كله في حالة عطل تام، وكان يمكن إصلاحه، فتقع الجريمة أيضا اذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة[4] .

3/ ضرورة خضوع النظام للحماية الفنية:

يقصد بمصطلح الحماية الفنية للنظام أنه ذلك الإجراء الوقائي الذي يتخذه صاحب النظام أو صانع البرنامج أثناء وضعه له للحد من الاعتداءات الخارجية التي قد تقع عليه، وفي هذا الصدد هناك طريقتان من الحماية هما أسلوب التشفير، والتحقق من شخصية المتعاقدين[5].

حيث يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات، وبالأخص حاليا شبكة الأنترنت فهم يسعون لتأمين سرية الرسائل الإلكترونية وسرية البيانات المتناقلة وخاصة بأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الإلكترونية[6]. كما أن هناك شكلين أساسيين لتشفير هما acrptologiesymétrique الذي أساسه أن نفس المفتاح التشفير يستعمل للتشفير وفك الشفرة في آن واحد، أما الشكل

techniques, 1995, p55.

[1]Droit pénal de l'informatique les systémes de traitements automatique des données, Commentaire de la loi n°88/18 du 03/01/1988 relative à la fraude informatique, 1988, doct, p95.

[2] أمال قارة، المرجع السابق، ص 102.

[3]خثير مسعود، المرجع السابق، ص 109.

[4] أمال قارة، المرجع السابق، ص ص 102-103.

[5]خثير مسعود، المرجع السابق، ص 111.

[6] أمال قارة، المرجع السابق، ص 103.

الثاني فهو la cryptologie asymétrique وأساسه أنه ليس نفس المفتاح هو الذي يشفر ويفك الشيفرة فهو يملك مفتاح خاص ومفتاح عاما[1].

وبهذا فقد أثير تساؤل حول ضرورة وجود أو عدم وجود الحماية الفنية كشرط لتتمتع بالحماية الجنائية. وللإجابة على هذا التساؤل فقد قسمت أنظمة المعالجة إلى ثلاثة أنواع: أنظمة مفتوحة للجمهور، وأنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية، وأنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية. وبمقتضى تطبيق هذا العنصر(الحماية الفنية) أن النوع الثالث فقط منها هو الذي يتمتع فقط بالحماية الجنائية، دون النوع الأول والثاني[2].

وبالرجوع إلى النصوص المتعلقة بهذا النوع من الجرائم فإنها لا تتضمن شرط الحماية، ولا يجوز تقييد النص المطلق أو تخصيص النص العام إلا بوجود نص يجيز ذلك، وتطبيقا لذلك فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيد بوجود الحماية الفنية. إذ أنه في الواقع نلاحظ أن غالبية النظام تتمتع بنظام الحماية التي تساعد على إثبات أركان الجريمة وبالخصوص الركن المعنوي[3].

ثانيا: أشكال الاعتداء على نظام المعالجة الآلية للمعطيات

قد تضمنتها المواد من 394 مكرر الى 394 مكرر7 ق ع ج، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والتي يمكن تلخيصها في ما يلي:

-الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو في جزء منها.

-إتلاف أو حذف أو تغيير لمعطيات المنظومة أو تخريب اشتغال المنظومة.

-إدخال بطريق الغش معطيات في نظم المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

-كل من يقوم عمدا بطريق الغش.

وقد تم التطرق لهم بالتفصيل في المطلب الأول بعنوان أركان الجريمة الإلكترونية ، في المبحث الثاني تحت عنوان الإطار الموضوعي للجريمة الإلكترونية.

الفرع الثالث: الحماية في قانون الإجراءات الجزائية

قد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بالجريمة المعلوماتية، محاولة منه تطويقها و القضاء عليها أو على الأقل الحد من انتشارها، حيث وضع قواعد و أحكام خاصة لسلطة التحري و المتابعة ،الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون الإجراءات الجزائية، متابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة والضبط ...إلخ. كما قام باستحداث أساليب

[1] أمال قارة، المرجع نفسه، ص 104.

[2] خثير مسعود، المرجع السابق، ص ص 111-112.

[3] أمال قارة، المرجع السابق، ص ص 105-106.

أخرى خاصة كاعتراض المراسلات، المراقبة الإلكترونية، التسرب، تسجيل الأصوات والتقاط الصور[1].

نجد أن المشرع الجزائري أيضا نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في نص المادة 37 من قانون الإجراءات الجزائية. ونص على التفتيش في المادة 45 الفقرة 7، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 06، ونص على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر5 إلى65 مكرر 10 أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية[2]، وهذا ما سنتطرق له بالتفصيل في المبحث الثاني من هذا الفصل.

المطلب الثاني: الحماية القانونية في النصوص الخاصة

الحماية في النصوص الخاصة تشمل الحماية من خلال (قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال) في الفرع الأول، والحماية من خلال (قانون البريد والمواصلات السلكية و اللاسلكية) في الفرع الثاني، (والحماية من خلال قانون التأمينات) في الفرع الثالث، و(الحماية في نصوص الملكية الفكرية) في الفرع الرابع.

الفرع الأول: قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

دفع القصور الذي عرفه قانون 04-15 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، مما أدى المشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه هذا المجال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، وذلك بوضع قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من أجل تعزيز القواعد السابقة[3].

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها، كما أخذ المشرع في عين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك ثم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حتى يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا[4].

---

[1] بوشعرة أمينة، مساوي سهام، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر، جامعة عبد الرحمان ميرة، بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2018/2017، ص ص 69-70.

[2] الأمر 66-156، المؤرخ في 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، ج ر، عدد07، المؤرخة في 10 يونيو سنة 1966.

[3] مراد مشوش، المرجع السابق، ص 121.

[4] مراد مشوش، المرجع نفسه، ص 121.

-نصت المادة 02 من القانون 09-04 على مفهوم كل من المصطلحات التالية: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، منظومة معلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة السير والاتصالات الإلكترونية.

-نصت المادة 04 منه على مراقبة الاتصالات الإلكترونية في الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية.

- نصت المادة 05 منه على القواعد الإجرائية لتفتيش المنظومة المعلوماتية.
- نصت المادة06 منه على حجز المعطيات المعلوماتية.
- نصت المادة07 منه على الحجز عن طريق منع الوصول إلى المعطيات.
- نصت المادة 08 منه على المعطيات المحجوزة ذات المحتوى المجرم.
- نصت المادة 09 منه على حدود استعمال المعطيات المتحصل عليها.
- نصت المادة 10 منه على التزامات مقدمي الخدمات مساعدة السلطات.
- نصت المادة 11 منه على حفظ المعطيات المتعلقة بحركة السير.
- نصت المادة 12 على الالتزامات الخاصة بمقدمي خدمة الأنترنت.
- نصت المادة 13و 14 منه على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: قانون البريد والمواصلات السلكية واللاسلكية

تسارع قانون رقم 2000-03[1] المؤرخ في 05 أوث 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية ولاسلكية الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الإلكترونيات ذلك ما نصت عليه المادة 87 من هذا القانون بالقول " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني.

وقد سعى قانون البريد والمواصلات لمواجهة هذه الظاهرة الإجرامية، من خلال المواد التي تضمنها لهذا الغرض، بات من السهولة إجراء التحويلات المالية عن الطريق الإلكتروني نظرا لتطور تكنولوجيا الإعلام والاتصال و كذلك قد نص على استخدام حوالات الدفع الإلكترونية أو البرقية[2].

الفرع الثالث: قانون التأمينات

نصت المادة 06 مكرر من قانون 08-01[3] المؤرخ في 23 جانفي 2008 المتمم لقانون رقم83-11 المتعلق بالتأمينات على " تثبت صفة المؤمن له اجتماعيا ببطاقة إلكترونية.

---

[1]قانون رقم 2000-03 مؤرخ في 05 جمادى الأول عام 1421 الموافق 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

[2]بوشعرة أمينة، مساوي سهام، المرجع السابق، ص 70.

[3]القانون رقم 08-01 المؤرخ في 2008/01/23 المتعلق بالتأمينات الاجتماعية، ج ر، عدد 04، الصادرة في 27 يناير 2008، المعدل والمتمم للقانون 83-11 المتعلق لتأمينات الاجتماعية.

تتحدد تسمية البطاقة الإلكترونية ومضمونها وشروط تسليمها و استعمالها وحالات تجديدها وتحيينها وتعويضها في حالة السرقة أو ضياع عن طريق التنظيم".

نصت المادة 93 مكرر 02[1] من نفس القانون على عقوبة كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو مفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة.

تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية، التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني[2].

الفرع الرابع: الحماية في نصوص الملكية الفكرية

باعتبار المعلوماتية نتاج فكر وإبداع، جعل من المشرع الجزائري يوفر لها الحماية الموضوعية كونها من أهم المسائل التي رافقت تطور النظام الاقتصادي الحديث، وذلك تصديا لتعديات التي تمس حقوق الغير والمجتمع والتي ترتبط بشكل وثيق بحقوق الملكية الفكرية.

وتعتبر أبرز التقسيمات الشائعة لحقوق الملكية الفكرية هو تقسيمها إلى ملكية صناعية و أخرى أدبية، وهذا ما اعتمدناه في تقسيمنا لهذا المطلب.

أولا: مدى خضوع المعلوماتية لنصوص الملكية الصناعية

1/تعرف الملكية الصناعية:

تعرف الملكية الصناعية بأنها الحق الذي يرد على براءات الاختراع والرسوم والنماذج الصناعية والعلامات التجارية والأسماء وكذلك ملكية المحل التجاري[3].

ومن هذا التعريف نجد أن الملكية الصناعية تحتوي على كل من الرسوم والنماذج الصناعية وامتيازات الاختراعات والرسوم وبراءات الاختراع. وبالتالي فإن دراستنا للملكية الصناعية سيكون من خلال اختيار أهم مفرداتها وهي براءة الاختراع وبيان أهم الأحكام الخاصة بها وبيان إمكانية حماية برامج الحاسب الآلي من خلالها[4].

أولت كل التشريعات اهتمامها بالمبتكرات والاختراعات الجديدة بشتى أنواعها، حيث بسط المشرع الجزائري حمايته على هذه الابتكارات و الاختراعات والتي تكون نتيجتها منتوج جديد وطريقة جديدة ذات تطبيق صناعي، وذلك بواسطة قانون براءة الاختراع والمتمثل في المرسوم التشريعي رقم 93-17المؤرخ في 07 ديسمبر 1993، وكذا الأمر 03-07 المؤرخ في 19 جويلية 2003 فيما يخص براءات الاختراع[5].

أ/ مفهوم براءة الاختراع:

---

[1] القانون 08-01، سالف الذكر.

[2]بوشعرة أمينة، مساوي سهام، المرجع السابق، ص 72.

[3]خثير مسعود، المرجع السابق، ص 67.

[4] عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الألي ومشكلة قرصنة البرامج، ط01، دار وائل للنشر، 2005، ص 71.

[5]خثير مسعود، المرجع السابق، ص 68.

عرفت المادة 02 من الامر 03-07[1] الاختراع "بأنه فكرة لمخترع يسمح عمليا بإجاد حل لمشكل محدد في مجال التقنية".

أما براءة الاختراع فهي وثيقة تمنحها الدولة للمخترع فتخول له حق استغلاله ماليا والتمتع بالحماية القانونية المقررة لهذا الغرض، وذلك لمدة محدودة وبشروط معينة[2].

ب/ الشروط الواجب توافرها في الاختراع:

نصت المادة الثالثة من الامر 03-07[3] على ما يلي:" يمكن أن تقع تحت حماية براءة الاختراعات الجديدة الناتجة عن نشاط اختراعي والقابلة للتطبيق صناعيا".

ونستخلص أن قانون الملكية الصناعية يضفي حمايته عن طريق براءة الاختراع حيث لابد من توفر هذه الشروط في الاختراع وهي: شرط الابتكار، شرط الجدة، القابلية لتطبيق الصناعي، المشروعية[4].

في حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية[5].

2/ مدى انطباق الشروط الخاصة بالاختراع على برامج الحاسب الآلي

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

- إما تجرد البرامج من أي طابع صناعي.

- إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه[6].

حسب ما يراه المختصون في الميدان فإنه من الصعب توفير حماية ناجعة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، ويتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة:

- شرط الجدة.
- القابلية للاستغلال الصناعي.

---

[1] الأمر 03-07، المؤرخ في 2003/07/19 يتعلق ببراءات الاختراع ، ج ر عدد 44، الصادرة في 2003/07/23.

[2] خثير مسعود، المرجع السابق، ص ص 68-69.

[3] الأمر 03-07، سالف الذكر.

[4] أمار قارة، المرجع السابق، ص 64.

[5] فليح نور الدين، المرجع السابق، ص ص 98-99.

[6] فبيح نور الدين، المرجع نفسه، ص 99.

هذان الشرطان تتفق حولهما التشريعات المقارنة مع التشريع الجزائري فيما يضيف هذا الأخير شرطا آخر هو أن يكون الاختراع نشاطا خلاقا[1].

أ/ شرط الجدة:

طبقا للمادة 09 من الأمر 03-07[2]:" يعتبر الاختراع ناتجا عن نشاط اختراعي إذا لم يكن ناجما بداهة عن الحالة التقنية".

وهذا مالا يكون من الهين تحققه في البرمجيات ولا من الهين إثباته، إذ يجب لتقرير بتوافر هذا الشرط أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لكي تقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم، وأن صعوبة تقييم طابع الجدة بالنسبة للكيانات غير المادية ليس مرده لاعتبارات قانونية، بل مرجع ذلك عدم توفر الكفاءات اللازمة التي يمكنها بحث وفحص الكيان المنطقي والنظر في مدى توافر شرط الجدة من عدمه[3].

والجهة المكلفة بتقرير توافر شرط الجدة في الجزائر هي المعهد الجزائري لحماية الملكية الصناعية إذ يأخذ المشرع الجزائري بمبدأ الجدة المطلقة الذي يتنافى مع وجود أية سابقة دون تحديد زماني أو مكاني، إنما يشرط أن تتوافر علانية هذه السابقة[4].

ب/ صعوبة قابلية الكيان المنطقي للاستغلال الصناعي:

يجب أن يكون الاختراع قابلا للإستغلال الصناعي لكي يتمتع بنصوص الحماية الخاصة ببراءة الاختراع، هذا الشرط يفترض أن يكون الاختراع ذا صفة مادية، ويجب أن يؤدي استغلاله إلى منتج صناعي، أو يمكن من الوصول إلى نتيجة صناعية، وكل هذه الأمور تتناقض مع الكيان المنطقي ذو الطابع الذهني أو المعنوي[5].

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه يمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة[6].

تجدر الإشارة الى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 03-07 المتضمن براءة الاختراع "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"[7].

ثانيا: مدى خضوع المعلوماتية لنصوص الملكية الادبية والفنية

---

[1] أمال قارة، المرجع السابق، ص 66.
[2] الأمر 03-07، سالف الذكر.
[3] أمال قارة، المرجع السابق، ص ص 66-67.
[4] فليح نور الدين، المرجع السابق، ص 99.
[5] أمال قارة، المرجع السابق، ص 67.
[6] فليح نور الدين، المرجع السابق، ص 100.
[7] أمال قارة، المرجع السابق، ص 69.

تعرف الملكية الأدبية والفنية على أنها ما للمؤلف من حق على مصنفاته المبتكرة في الآداب والعلوم والفنون[1].

1/ مدى اعتبار البرامج كموضوع من موضوعات حق المؤلف

موضوع حق المؤلف هو المصنف الادبي والفني وقد عرف المشرع الجزائري المصنف في المادة الأولى من الأمر 73- 14[2] .

فنصت المادة02 من الأمر 73-14[3]، على المصنفات التي تشملها حماية حق المؤلف، فالمشرع الجزائري لم يدرج برامج الكمبيوتر صراحة ضمن المصنفات الخاضعة لحماية حق المؤلف، فإن هذا التعدد قد ورد على سبيل المثال لا الحصر في الأمر 73-14 المتعلق بحقوق المؤلف.

أ/ الحماية في النصوص التقليدية لحقوق المؤلف:

تنص المادة 02 من الأمر 73-14 وإن كان لم يذكر صراحة برامج الحاسوب ضمن المصنفات المحمية لحماية حق المؤلف إلا أن صياغتها قد جاءت ضمن المصنفات المحمية لحماية حق المؤلف إلا أن صياغتها قد جاءت في صورة عامة، هذا التعداد ورد على سبيل المثال لا الحصر[4].

ومنعا لأي لبس كان من الأفضل النص على البرامج صراحة ضمن قائمة المصنفات المحمية، وهذا ما فعله المشرع الجزائري في تعديل قانون حق المؤلف بمقتضى الأمرين 10-97 و 03-05 حيث أدمج برامج الإعلام الآلي ضمن المصنفات الأصلية[5].

وما يؤكد ذلك أن المادة 07 من الامر 96-16 تخضع للإيداع القانوني الوثائق المطبوعة والصوتية والسمعية البصرية أو التصويرية وبرامج الحاسوب بكل أنواعها أو قواعد المعطيات وذلك مهما لدعامة التي تحملها تقنية الإنتاج والنشر والتوزيع (الأمر 96-16 في 1996/07/02)[6].

ب/ الحماية بالنصوص المعدلة لحقوق المؤلف:

من استقراء الأمرين97-10-03-05 المعدل والمتمم للأمر 14/73نستخلص ما يلي:

- مجموعة المصنفات والأساليب والقواعد، كما يمكن أن يشمل الوثائق المتعلقة بسير ومعالجة المعطيات.
- إن مدة الحماية تحدد من 25سنة إلى 50سنة بعد وفاة المبدع تماشيا مع اتفاقية "بارن" التي حددت كمدة للحماية 50 سنة[7].

تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية (المادة 153 الأمر 03-05 تقابل المادة 151 الأمر 97-10)، إذ في السابق تجريم الاعتداءات على الملكية الفكرية تناولته المواد 390إلى394 من ق ع

---

[1] خثير مسعود، المرجع السابق، ص67.
[2] الأمر 73-14، المؤرخ في 03 أفريل 1973 المتعلق بحقوق المؤلف و الحقوق المجاورة له.
[3] الأمر 73-14، سالف الذكر.
[4] أمال قارة، المرجع السابق، ص76.
[5] فليح نور الدين، المرجع السابق، ص 102.
[6] أمال قارة، المرجع السابق، ص 76.
[7] فليح نور الدين، المرجع السابق، ص 102.

ج، لكنها أخرجت بموجب الأمر 97-10 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة على حق المؤلف، بينما الأمر 97-10 وكذا الأمر 03-05 يقرران عقوبتي الحبس والغرامة[1].

تجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين97-10/03-05 تعود لأسباب أهمها الانضمام إلى المنظمة العالمية للتجارة هو المصادقة على اتفاقية بارن وهو ما فعلته الجزائر بموجب المرسوم الرئاسي[2] .

إضافة إلى تبني أحكام اتفاق جوانب الملكية الفكرية المتعلق بالتجارة ومن أهم ما ورد في هذا الاتفاق هو ما جاء في نص المادة 10 أن برامج الإعلام الآلي سواء كانت في صورة برامج مصدر أو الصورة المنقوشة فهي محمية على أساس أنها المصنفات الأدبية[3].

2/ مدى خضوع برامج الحاسب الآلي لنشاط الاجرامي لجرائم التقليد في التشريع الجزائري

قانون حق المؤلف يوفر الحماية الجزائية لمصنفات الإعلام الآلي بعد إدماجها صراحة ضمن المصنفات المحمية. في السابق كانت أفعال التعدي على حقوق الملكية الأدبية والفنية معاقب عليها في قانون العقوبات المواد من390 إلى 394 غير أن هذه المواد ألغيت بمقتضى المادة 165 من الأمر97-10[4].

وقد عرفت جريمة التقليد بأنها القيام بعمل لا يقوم به سوى المؤلف أو يرخص به[5].

والملاحظ أن الاعتداءات على حقوق المؤلف أخرجت بموجب الأمر97-10من تحت مظلة قانون العقوبات، حيث كان منصوصا عليها في القسم التاسع المعنون بجنح التعدي على الملكية الأدبية والفنية من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال. لكن حاليا أخرجت من نطاق قانون العقوبات وأصبح لها تجريم خاص في إطار قانون حق المؤلف[6].

تجدر الإشارة إلى الأمر 97-10 فقد شدد في العقوبات المقررة للاعتداءات على حقوق المؤلف مقارنة بالعقوبات المنصوص عليها في قانون العقوبات المادة 75الأمر73-14 تحيل إلى المادة 390من ق ع تقرر الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر97-10 يقرر عقوبتي الحبس والغرامة[7].

رغم اعتراف المشرع الجزائري لبرامج الإعلام الآلي وقواعد البيانات بصفة المصنف المحمي إلا أنه لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنصب بصفة أساسية على شكل البرامج أو مضمونه الابتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرامج، ولهذا السبب كان البحث عن نوع آخر

[1] أمال قارة، المرجع السابق، ص ص 78-79.
[2] فليح نور الدين، المرجع السابق، ص103.
[3] أمال قارة، المرجع السابق، ص ص 79-80.
[4] فليح نور الدين، المرجع السابق، ص 104.
[5] خثير مسعود، المرجع السابق، ص 88.
[6] فليح نور الدين، المرجع السابق، ص 104.
[7] فبيح نور الدين، المرجع نفسه، ص 104.

من الحماية يضم إلى الحماية السابقة من الحماية الجزائية لهذه البرامج في مثل هذه الحالات، ولذلك فلا مفر من ضرورة اللجوء إلى استحداث نصوص تجريمية خاصة بالمعلوماتية[1].

[1] أمال قارة، المرجع السابق، ص 95.

المبحث الثاني: المواجهة الإجرائية للجريمة الإلكترونية

إن طبيعة الجرائم الإلكترونية بكل عناصرها ووسائل ارتكابها دفعت المشرع الجزائري إلى إعادة النظر في كثير من المسائل الإجرائية، كون أن القواعد التقليدية غير قادرة على كشف هذا النوع من الجرائم، مما يستوجب تدخل من المشرع لتكريس هذه القواعد لتمكن الجهات المكلفة بعملية البحث والتحري الاعتماد عليها للوصول إلى الحقيقة.

التحقيق أهم إجراء من الإجراءات التي تتخذ بعد وقوع الجريمة، فإجراءات التحقيق المتبعة في الجريمة الإلكترونية تأخذ بجميع عناصر و مراحل التحقيق في الجرائم العادية، فالنتيجة النهائية من هذا التحقيق هو العثور على أدلة واضحة يمكن أن يبنى عليها الإدعاء لتصدر العقوبة في المحكمة على أساسه. فبسبب تنوع الأنشطة الإجرامية فيها أصبح هناك تنوع في ملاحقتها ومتابعتها وذلك إبتداءا من تجريمها وبيان إجراءات ملاحقتها و كذا الأجهزة المختصة في الوقاية منها.

ولهذا سنتطرق (للأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية) في المطلب الأول، وسنتطرق إلى (البحث الأولي) في المطلب الثاني، أما في المطلب الثالث فقد تناولنا فيه (التحقيق الإبتدائي)، وفي المطلب الرابع (التحقيق النهائي)

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية

لم يخص المشرع الجزائري الجريمة المعلوماتية بأحكام إجرائية خاصة ومفردة في قانون الإجراءات الجزائية تتعلق بكيفيات سير إجراءات التحقيق والمتابعة، لكنه في المقابل حدد بعض التدابير التي تهدف إلى اقتفاء أثر الجريمة المعلوماتية، واستخلاص الأدلة الرقمية[1]، ومن ضمنها بعض الأجهزة المكلفة بعملية البحث والتحري والتي سنتطرق لبعض منها في الفروع الموالية.

[1] يعيش تمام شوقي، الجريمة المعلوماتية "دراسة تأصيلية مقارنة"، سلسلة مطبوعات المخبر، مخبر أثر الإجتهاد القضائي على حركة التشريع، الجزائر، بسكرة، جانفي 2019، ص 63.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

كما سبق وقد أشرنا من خلال بحثنا عن الق 09-04[1] المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي عرفتها المادة 02 على أنها" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام لاتصالات الإلكترونية.

وبموجب المرسوم الرئاسي رقم 15-261[2] الذي يحدد تنظيم وتشكيل الهيئة وكفيات سيرها، وقد نص المشرع على إنشاء هذه الهيئة والتي كانت محط أنظار العديد من وسائل الإعلام، وعلى غير العادة قام المشرع الجزائري بعدها بأربع سنوات تقريبا بإصدار مرسوم 19-172[3]، والخاص بتشكيلة الهيئة والتي نصت عليه المادة الثالثة منه. وقد نصت المادة 13 من ق 09-04[4] على إنشاء هذه الهيئة، والمادة 14 منه تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم أمام الهيئة.

الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني

أولا: الأمن الوطني

لقد سجلت مصالح المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خلال الـ 08 أشهر الأولى من السنة الجارية،567 قضية تتعلق بجرائم الأنترنت، تورّط فيها 543 شخصا.حيث تمكنت من خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر، من معالجة 385 جريمة إلكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها، وهذا وفق ما توضحه المعطيات الواردة في الجدول التالي[5]:

[1] القانون 09-04، سالف الذكر.

[2] المرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق ل08 أكتوبر سنة 2015، يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] مرسوم رئاسي رقم 19-172 مؤرخ في 03 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.

[4] القانون 09-04، سالف الذكر.

[5] https://www.algeriepolice.dz.2022/06/05 ساعة الاطلاع 22:15، تاريخ الاطلاع

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الأنترنت	430	289	365	%68
جرائم الإعتداء على سلامة الأنظمة المعلوماتية	57	31	39	%55
جرائم الإحتيال عبر الأنترنت	25	17	32	%68
جرائم التحريض والتطرف عبر الأنترنت	14	14	31	%100
الجرائم المخلة بالحياء	12	08	22	%67
جرائم بيع السلع المحظورة عبر الأنترنت	06	05	15	%84
جرائم مختلفة (نسخ البرامج دون حق، القرصنة)	23	21	39	%92
المجموع	**567**	**385**	**543**	**%68**

عالجت المديرية العامة للأمن الوطني، 5200 قضية خاصة بالجرائم الإلكترونية سنة 2020، مقارنة بأقل من 500 جريمة سنة 2015.

وأفاد الملازم الأول مطمط أمين، في تصريح للإذاعة الجزائرية، أنه تم إنشاء فرق خاصة لمكافحة الجرائم الإلكترونية. وقال أنها تتزايد نتيجة تطور التكنولوجيا[1].

ثانيا: الدرك الوطني

صرح رئيس مركز مكافحة الجرائم الإلكترونية و مكافحتها بالدرك الوطني جمال بن رجم للإذاعة أنه: 95 بالمائة من قضايا الجرائم الإلكترونية التي تصل إلى المركز تم حلها بنجاح ، مشيرا إلى معالجة 100 قضية تتعلق بالطفولة والمراهقين و 20 جريمة مالية خلال 2017 ، وشدد على أن حماية المواطن الجزائري في الفضاء السيبرياني جزء لا يتجزأ من مهام الدرك الوطني[2].

المطلب الثاني: مرحلة البحث الأولي

قبل عرض الدعوى العمومية على القضاء لابد أولا من المرور بمرحلة تمهيدية والتي تتم فيها البحث والتحري على الجريمة وجمع كل الأدلة المتعلقة بها للوصول إلى مرتكب الفعل الإجرامي سواء كان شخص أو عدة أشخاص، ويتولى عملية البحث الأولي جهاز الضبطية القضائية والذي أصبح يعرف الآن بتسمية الشرطة القضائية، وهذا ما سنتطرق له في الفروع الموالية.

الفرع الأول: مفهوم الضبطية القضائية

يعتبر أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية وخولهم بموجبها حقوق وفرض عليهم واجبات في إطار البحث عن

[1] بقلم فطومة حيدر ، الأمن الوطني يسجل 5200 جريمة إلكترونية سنة 2020،ساعة الاطلاع 22:27، تاريخ الاطلاع 2022/06/05، https://www.ennaharonline.com.

[2] https://radioalgerie.dz/news/ar/tags، ساعة الاطلاع 22:32، تاريخ الاطلاع 2022/06/05.

الجريمة ومرتكبيها وجمع الاستدلالات عنها، فيبدأ دورهم بعد وقوع الجريمة وينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم[1].

فحسب ما جاء في نص المادة 12 ق إ ج ج أنه "يقوم بمهمة الشرطة القضائية، القضاة والضباط والأعوان والموظفون..."، وتنص المادة 14 من نفس القانون أيضا على أصناف الضبطية القضائية بقول "يشمل الضبط القضائي:

1- ضباط الشرطة القضائية.

2- أعوان الضبط القضائي.

3- الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي.

اهتمت المواد 15، 19، 20، 21، 22، 23، 27، 28 ق إ ج ج، بتحديد الموظفين والأعوان الذين تثبت لهم صفة من صفات الضبطية القضائية المحددة بالمادة 14 ق إ ج ج، أو الذين يمكن إضفاؤها عليهم وفقا لقواعد محددة سلفا، فجاءت المادة15 ق إ ج ج محددة من تثبت لهم صفة "ضباط شرطة قضائية"، والمادتان19، 20 تحدد طائفة الأعوان، وتحدد المواد 21، 28 طوائف الموظفين الموكول لهم بعض مهام الضبط القضائي، وأحالت المادة 27 على القوانين الخاصة لإمكان إضفاء صفة الضبطية القضائية على الموظفين والأعوان[2].

الفرع الثاني: اختصاص الضبطية القضائية

يناط بالضبط القضائي أو الشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات والقوانين المكملة له، وجمع الأدلة عنها والبحث عن مرتكبيها، وتمارس الشرطة القضائية في حدود اختصاصها كافة الإجراءات التي يقررها القانون[3].

أولا: الاختصاص النوعي

يقصد به اختصاص عضو الضبطية القضائية بنوع معين من الجرائم دون غيرها من الجرائم. وقد ميز المشرع بين الاختصاص العام، لبعض فئات أعضاء الضبطية القضائية أي اختصاصهم بشأن جميع الجرائم. وهي الفئات المنصوص عليها في ق إ ج، فلهم الاختصاص العام بالبحث والتحري في جميع الجرائم أما الفئات الأخرى من الضباط المحددين في الفقرة 7من المادة15وكذلك المواد 27 و 21 و 28 ق إ ج فإنهم ذو اختصاص خاص وليس عام يتحدد بنطاق جرائم معينة[4].

ثانيا: الاختصاص المحلي

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة، ويتحدد بنطاق الحدود الذي يباشر فيها وظائفه

---

[1] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد 04، جانفي 2018، ص 53.

[2] عبد الله وهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)،د ط، دار هومة للطباعة والنشر والتوزيع، 2004، ص ص 191-192.

[3] عبد الله وهايبية، المرجع نفسه، ص 206.

[4] ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2016/2015، ص ص 5-6.

المعتادة ولذلك يتعين أن يكون مكان وقوع الجريمة أو محل إقامة المتهم أو محل القبض عليه[1]. وقد نصت عليه المادة16 ق إ ج ج.
يجوز القانون تمديد الاختصاص المحلي لضباط الشرطة القضائية في حالات التي نصت عليها المادة 16 في فقرتها 3/2 ق إ ج ج.

الفرع الثالث: صلاحيات الضبطية القضائية

أسند قانون الإجراءات الجزائية لضبطية القضائية صلاحيات واسعة، سواء في الحالات العادية أو الاستثنائية، فالضبط القضائي مرحلة شبه قضائية تهدف إلى البحث والتحري، واستثناء يخولون بناءا على القانون مباشرة بعض الإجراءات التي تعتبر أصلا من اختصاص جهات التحقيق بنص قانوني صريح أو بناء على إنابة قضائية من طرف قاضي التحقيق.

أولا: اختصاصات الضبطية القضائية في الحالات العادية

تنص المادة 17 ق إ ج ج على أنه" يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية".

بينما نصت المادة 18 ق إ ج ج على أنه" يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم.....بمحرريها".

وعليه يتبين من النصوص السابقة أن الاختصاصات العادية لضباط الشرطة القضائية تتمثل في:

1/ تلقي الشكاوى والبلاغات:

في جميع الأحوال عند تلقي بلاغ عن وقوع الجريمة الإلكترونية، وبعد التأكد من البيانات الضرورية في البلاغ يتم الإنتقال إلى مسرح الجريمة لمعاينته، و مسرح الجريمة الإلكترونية يختلف طبعا عن الجريمة التقليدية ودون الخوض في أوجه الخلاف فإن البعض يرى أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية، وذلك لندرة تخلف آثار مادية عقب ارتكاب هذه الجريمة، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو محو أو تلف تلك الآثار[2].

فالمهمة الأساسية للضبطية القضائية هي ملاحقة ومتابعة الجريمة بعد ارتكابها بالإضافة إلى قبولها الشكاوى والبلاغات التي ترد إليها بشأن الجرائم، وأن تبلغ عنها مباشرة السيد وكيل الجمهورية[3].

2/ جمع الاستدلالات:

وهي قيام ضباط الشرطة القضائية بإجراء تحقيق أولي إما بناء على بلاغ أو شكوى أو بناء على تعليمات وكيل الجمهورية، حيث يقوم ضباط الشرطة القضائية

---

[1] عبد الله وهايبية، المرجع السابق، ص 209.

[2] مليكة أبوديار، الإثبات الجنائي في الجرائم الإلكترونية، المجلة الإلكترونية للأبحاث القانونية، العدد 02، 2018، ص ص 104-105

[3] بغانة عبد السلام، مقياس قانون الإجراءات الجزائية، مطبوعة موجهة لطلبة نظام ل م د شريعة وقانون وحقوق الانسان، جامعة الأمير عبد القادر للعلوم الإسلامية، كلية الشريعة والاقتصاد، قسم الشريعة والقانون، 2015/2014، ص36.

بجمع الاستدلالات عن الجريمة من خلال سماع الأشخاص، والانتقال إلى مكان وقوع الجريمة للقيام بالمعاينات اللازمة والبحث عن آثارها والتحفظ على كل الأدوات التي استعملت فيها وضبط الأشياء المتعلقة بها و إقامة حراسة عليها وسماع الشهود وكل من له علاقة أو مساكن الأشخاص الذين قد يكونوا ساهموا في الجناية أو الجنحة أو إذا كانوا يحوزون أشياء أو أوراق متعلقة بها للقيام بإجراء التفتيش وفقا للأوضاع التي يقررها القانون وهذا بموجب المادة 64، والمادتين44 إلى47 ق إ ج ج[1].

3/ تحرير محاضر:

يشترط المشرع من ضباط الشرطة القضائية أن يحرر محضر بأعماله طبقا لنص المادة 18 ق إ ج ج، بالإضافة إلى توقيع المشتبه فيه والضحية والشهود والخبراء إن وجدو، وترسل هذه المحاضر إلى النيابة العامة مع الأوراق والأشياء المحجوزة، وذلك بغرض إمدادها بالمعلومات اللازمة[2].

4/ توقيف الشخص المشتبه فيه: نصت عليه المادة 01/65 ق إ ج ج[3].

ثانيا: اختصاصات الضبطية القضائية في الحالات الاستثنائية

1/ في حالة التلبس:

إذا توافرت إحدى حالات التلبس التي وردت في نص المادة 41 ق إ ج ج، فإنه يجوز لضباط الشرطة القضائية اتخاذ إجراءات فورية للكشف عن مرتكب هذه الجريمة وجمع الاستدلالات قبل زوال آثارها وقد نصت عليها المادة 42 ق إ ج ج، على أنه" يجب على ضباط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل .....للتعرف عليها".

ويجوز لضباط الشرطة القضائية في حالة التلبس ممارسة الصلاحيات الآتية:

أ/ تعيين الخبراء: يمكن لضباط الشرطة القضائية الاستعانة بالخبراء في حالة التلبس لإجراء المعاينات اللازمة والتي لا يمكن تأخيرها وينبغي على الخبراء أداء اليمين كتابة على أن يبدوا آراءهم بما تمليه عليهم ضمائرهم وشرفهم المادة 49 ق إ ج ج[4].

ب/ سماع الشهود: نصت عليه المادة 50 ق إ ج ج ، خولت لضباط الشرطة القضائية منع أي شخص من مغادرة مكان الجريمة لحين انتهاءه من تحرياته، كما أجازت له التعرف على هوية أي شخص والتحقيق من شخصيته إذا ما تراءى له ذلك ضروريا لإجراء التحقيقات، أو أوجبت على ذلك الشخص الالتزام والامتثال له[5].

ج/ التوقيف للنظر: نصت على هذا الإجراء المادة 51 ق إ ج ج، فقد أجاز المشرع الجزائري لضباط الشرطة القضائية توقيف لنظر شخصا أو أكثر لمدة 48 ساعة،

---

[1] محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، ط02، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019، ص ص 179-180.

[2] عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط03، د دار النشر، الجزائر، بجاية، 2017، ص 104.

[3] القانون رقم 06-22، المؤرخ في 2006/12/20، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[4] بغانة عبد السلام، المرجع السابق، ص 41.

[5] محمد حزيط ، المرجع السابق، ص 195.

ويجوز تمديد مدة التوقيف للنظر حسب نص المادة 51 ق إ ج ج، وبالنسبة لجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات فيجوز التمديد لمرة واحدة فقط[1].

د/ التفتيش: نصت عليه المادة 44 ق إ ج ج، ويخضع ضباط الشرطة القضائية لشروط معينة نص عليهم قانون الإجراءات الجزائية. ويجوز إجراء التفتيش والمعاينة والحجز في كل وقت إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وعدم احترام شروط إجراء التفتيش المنصوص عليها في المواد تؤدي إلى بطلان التفتيش[2].

و/ ضبط الأشياء: نصت عليه المادة 42 ق إ ج ج.

ه/ اعتراض المراسلات وتسجيل الأصوات: نصت عليه المادة 65 مكرر5 ق إ ج ج، وفي حالة الجريمة المتلبس بها بالإذن بالكشف واعتراض المراسلات التي تتم عن طريق الوسائل السلكية واللاسلكية، وكذا التقاط الصور لهم وتسجيل الأصوات سواء كان ذلك في أماكن عامة أو خاصة[3].

2/ في حالة الإنابة القضائية:

التحقيق أصلا من اختصاص قاضي التحقيق، فلا يجوز لضابط الشرطة القضائية كقاعدة القيام به، ولكن خول لجهة التحقيق إنابة غيرها في القيام ببعض إجراءات التحقيق وهذا ما جاء في نص المادة 6/68 ق إ ج ج، فقد خولت المواد من 138إلى 142 لقاضي التحقيق أن يندب أو يفوض بعض صلاحياته لجهات أخرى[4]. فقد نصت المادتين 139/138ق إ ج ج على الشروط الإنابة القضائية.

إذا توافرت الشروط الخاصة بالندب القضائية فإنها تنتج آثارها صحيحة وخاصة منها منح سلطة لضباط الشرطة القضائية بإجراءات التحقيق المطلوبة، ويعتبر المحضر الذي يحرره محضر التحقيق وليس الاستدلال، وللضباط في هذه الحالة سلطة سماع الشهود مع تحليف اليمين للشاهد م140ق إ ج ج، كما يجوز له حجز الشخص تحت النظر م141 ق إ ج ج ، ويجب عليهم الالتزام بحدود الإنابة والتقييد بالمدة المحددة له م141 ق إ ج ج، وتجدر الإشارة إلى أن الإنابة هي شخصية فلا يجوز ندب الغير للقيام بها[5].

المطلب الثالث: التحقيق الابتدائي

يعد التحقيق الابتدائي نشاط إجرائي تباشره سلطة قضائية مختصة بالتحقيق للبحث في مدى صحة الاتهام بشأن واقعة جنائية معروضة عليها، وللبحث عن الأدلة المثبتة للتهمة والمجرمين المتهمين بها، والتحقيق الابتدائي مرحلة لاحقة لإجراءات جمع الاستدلالات والبحث الأولي والذي تباشره الضبطية القضائية والتي سبق وقد تطرقنا لها، وتسبق مرحلة المحاكمة التي تقوم بها جهات الحكم والتي سنتطرق لها لاحقا، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.

---

[1] عبد الرحمان خلفي، المرجع السابق، ص 129.
[2] الأمر 66-155، المتضمن قانون الإجراءات الجزائية، سالف الذكر.
[3] بغانة عبد السلام، المرجع السابق، ص 43.
[4] عبد الله وهايبية، المرجع السابق، ص 273.
[5] بغانة عبد السلام، المرجع السابق، ص 44.

الفرع الأول: قاضي الحقيق

أولا: مفهوم قاضي الحقيق

إن الصراع بين المحقق الذي هدفه الوصول إلى الحقيقة، والمجرم الذي يحاول تضليل العدالة لكي يفلت من العقاب، يطلق عليه التحقيق الجنائي، فالتحقيق الإبتدائي يتميز عن غيره من إجراءات الدعوى عبر مراحلها المختلفة بموضوعه والقائم به هو قاضي التحقيق والذي لا يختلف عن ما هو متعارف عليه في الجريمة التقليدية لكن الفرق يكمن في نوعية الجريمة.

يتم تعيين قاضي التحقيق بموجب مرسوم رئاسي بناء على اقتراح من وزير العدل، وبعد مداولة المجلس الأعلى وهذا ما نصت عليه المادة 03 من القانون 04-11، ولم يقرن المشرع الجزائري هذا التعيين بمدة زمنية محددة، وما يميز وظيفة التحقيق التي يمارسها قاضي التحقيق هي كونها من الوظائف القضائية النوعية[1]، وتنتهي مهامها بنفس الإشكال. فهو يجمع بين أعمال ضباط الشرطة القضائية من تحقيق وتحري بحثا عن الحقيقة، وبين أعماله كقاضي تحقيق يصدر مجموعة أوامر لها طبيعة قضائية، ويتم الاستعانة به أيضا ليقوم بوظائف قاضي حكم، ويترأس جلسات المحكمة، ويصدر أحكام مختلفة ماعدا في الحالات التي نصت عليها المادة 38 فقرة01 ق إ ج ج[2].

يتم اختيار قاضي التحقيق من طرف وكيل الجمهورية لتحقيق في قضية معينة، وفي حالة خطورتها جاز أن يلحق بالقاضي المكلف قاضي تحقيق آخر أو عدة قضاة سواء في بداية التحقيق أو أثناء سير الإجراءات[3].

فقاضي التحقيق الذي يقوم بالتحقيق في جرائم تتعلق بتكنولوجيا المعلومات يجب أن يتصف بخصائص تميزه عن غيره من المحققين، إذ يجب أن يكون على معرفة جيدة بالجوانب الفنية والتقنية لأجهزة الحاسوب والتي تتعلق بالجريمة المرتكبة، إضافة إلى إتباع الإجراءات الصحيحة والمشروعة للمحافظة على الدليل الإلكتروني، وكذلك تشكيل فريق تحقيق فني دو خبرة[4]، وغيرها من السمات التي يجب أن تتوفر في كل قاضي مكلف بمثل هذا النوع من الإجرام.

بعد وقوع الجريمة وقيام ضباط الشرطة القضائية بجميع إجراءات البحث وجمع الاستدلالات عن الجريمة الإلكترونية بأنها وقعت، يخطر وكيل الجمهورية قاضي التحقيق بضرورة التحقيق في الجريمة عن طريق النائب العام، وفور انتقال

---

[1] عماري فوزي، التحقيق الجنائي، محاضرات ألقيت على طلبة الماستر سنة أولى، تخصص قانون العقوبات والعلوم الجنائية، ص ص 2-3.

[2] حمداش كاهنة، مداني وفاء، التحقيق القضائي في ظل قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2017/11/30، ص 20.

[3] حمداش كاهنة، مداني وفاء، التحقيق القضائي في ظل قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2017/11/30، ص 22.

[4] يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر أكاديمي، تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2017/2016، ص 24.

الاختصاص لقاضي التحقيق على مستوى القطب الجزائي المختص ويتلقى ضباط الشرطة القضائية العاملين بدائرة اختصاص القطب التعليمات الخاصة[1].

ثانيا: اختصاص قاضي التحقيق

1/ الاختصاص الإقليمي:

يقصد به المجال المكاني الذي يباشر فيه قاضي التحقيق عمله في التحقيق باتخاذ إجراءاته، ويضيق هذا المجال المكاني بحسب ما يقرره القانون من دوائر اختصاص مكانية، فقد يكون اختصاص محليا يمكن تمديده لدوائر اختصاص أخرى، وقد يكون وطنيا يشمل كل تراب الجمهورية[2].

2/ الاختصاص النوعي:

يقصد به المجال الجرمي الذي يباشر فيه قاضي التحقيق مهامه، فيحقق كأصل عام في كل جريمة معاقب عليها طبقا لقانون العقوبات أو القوانين المكملة له هذا من جهة، إلا أنه لا يجوز له التحقيق في الجرائم العسكرية كونها تخرج من دائرة اختصاصه[3].

نصت المادة 66 ق إ ج ج على أنه "التحقيق الابتدائي وجوبي في مواد الجنايات أما في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة. كما يجوز إجراؤه في مواد المخالفات إذا طالبه وكيل الجمهورية"[4].

3/ الاختصاص المحلي:

نصت المادة 40 ق إ ج ج فقرة1 على أنه " يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر"[5].

وقد تم تمديد الاختصاص المحلي نظرا لخطورة وخصوصية بعض الجرائم ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد نصت عليه المادة 40 سالفة الذكر في فقرتها الثانية على أنه " يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجرائم المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف". وقد تم تنظيم تمديد الاختصاص بموجب المرسوم التنفيذي 06-348[6].

ثالثا: صلاحيات قاضي التحقيق

---

[1] إبتسام بغو، المرجع السابق، ص 54.

[2] عبد الله وهايبية المرجع السابق، ص ص 322-323.

[3] عبد الله وهايبية، المرجع نفسه، ص 326.

[4] الأمر 66-155، المتضمن قانون الإجراءات الجزائية، سالف الذكر.

[5] القانون 04-14 من الأمر 69-73، المؤرخ في 2004/11/10، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري .

[6] المرسوم التنفيذي 06-348 المؤرخ في 12 رمضان عام 1427 الموافق ل05 اكتوبر سنة 2006، والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد 63.

قد خص المشرع الجزائري قاضي التحقيق بسلطات وصلاحيات واسعة في سبيل تحقيق الهدف من إسناد مهمة التحقيق إلى قاضي تحقيق مستقل عن جهة المتابعة وجهة الحكم، وقد خولته المادة68 ق إ ج ج سلطة اتخاذ أي إجراء يراه ضروريا للكشف عن الحقيقة، وقد اتجهت إرادة المشرع إلى منحه سلطات جديدة لم يكن يتمتع بها في سبيل مواجهة الأنواع الجديدة من الجريمة الإلكترونية[1].وسنقوم بذكر أعمال التحقيق كما ورد في القانون.

1/ الانتقال والمعاينة:

الانتقال هو حركة مادية يقصد بها أن يباشر المحقق إجراءات التحقيق في غير المقر العادي له، وليس الهدف منه إجراء معاينة فقط، فالانتقال إلى مكان الواقعة ييسر له مباشرة جميع الإجراءات إذ دعوة الشهود للإدلاء بمعلوماتهم فور وقوع الحادث، وكلما بادرا المحقق بالانتقال إلى مكان وقوع الجريمة كلما ساعد ذلك على الوصول إلى الحقيقة[2]. وقد نص عليه المشرع في المواد 79و 80 ق إ ج ج.

وتعتبر المعاينة إجراء من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها. كما يمكن للمحكمة أن تقوم بإجراءات معاينة إذا رأت ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناء على طلب من الشخص المعني بعد موافقة القاضي المختص بناء على طلب عريضة[3].

والمعاينة هي إجراء ينتقل بمقتضاه المحقق أو القاضي لمكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بها، ويعرف كيف وقعت، ويقوم بجمع الأشياء التي تفيد في كشف الحقيقة. ويعد مسرح الجريمة بمثابة الشاهد الصامت، الذي إذا أحسن المحقق استنطاقه حصل على معلومات مؤكدة[4]. لهذا ينبغي التعامل معه على أنه مسرحان هما:

- المسرح التقليدي: هو الذي يقع خارج البيئة المعلوماتية ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى المسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه[5].
- المسرح الافتراضي: هو الذي يقع داخل البيئة المعلوماتية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله[6].

---

[1] إبتسام بغو، المرجع السابق، ص 62.

[2] حمداش كاهنة، مداني وفاء، المرجع السابق، ص 63.

[3] بن زرت أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019/2018، ص 20.

[4] شنتير خضرة، المرجع السابق، ص 64.

[5] الصغير يوسف، المرجع السابق، ص84.

[6] بن زرت أسيا، المرجع السابق، ص 20.

ونظرا لاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم العادية لذلك ينبغي تعامل خاص مع هذه الجريمة وذلك بإتباع عدة ضوابط في مسرح الجريمة ومن بينها:

-تصوير الحاسب الإلكتروني والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته[1].

-العناية بملاحظة الطريقة التي يتم بها إعداد النظام وكذلك ملاحظة إثبات حالة التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة[2].

-عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطسية[3].

-التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة و أوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع عليها البصمات ذات الصلة بالجريمة. وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لفرع ومضاهاة ما قد يوجد عليها من البصمات[4].

-قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسبات والشبكات واسترجاع المعلومات و أن يكون قد تلقوا تدريبا جيدا على ذلك[5].

وهناك نطاق للمعاينة وهي نوعين الأول يتمثل في معاينة مكونات الحاسوب، ولكون أن الحواسيب أهم مصدر يستسقى منه الأدلة ، لدى يجب معاينة كل من الجرائم الواقعة على المكونات المادية للحاسوب (hardware)كشاشة العرض ومفاتيح التشغيل و الأقراص وغيرها ، فهي لا تثير أي مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة، وكذلك معاينة الجرائم الواقعة على المكونات غير المادية (software)، كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته[6].أما الثاني يتمثل في معاينة أنظمة الاتصال بشبكة الأنترنت فلأولى لا تكون كافية لاستخلاص الدليل الإلكتروني، فعلى المحقق فحص أنظمة الاتصال بشبكة الأنترنت، والمقصود من

---

[1] زبيخة نور الهدى، المرجع السابق، ص 40.
[2] الصغير يوسف، المرجع السابق، ص 85.
[3] زبيخة نور الهدى، المرجع السابق، ص 40.
[4] صغير يوسف ، المرجع السابق، ص 86.
[5] زبيخة نور الهدى، المرجع السابق ، ص 41.
[6] محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، كتاب أعمال الملتقى الوطني: أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، جامعة حسيبة بن بوعلي، الشلف، 29 مارس 2017، ص 61.

هذا الفحص مجموع الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالأنترنت[1].

2/ التفتيش وضبط الأدلة:

أ/ التفتيش:

التفتيش في ق إ ج هو البحث عن شيء يتصل بجريمة وقعت وتفيد في كشف الجريمة عنها وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون هذا التفتيش بضمانات عديدة، ومحل التفتيش إما أن يكون مسكنا أو شخصا.

فقد نص المشرع الجزائري بمقتضى قواعد دستورية، حيث تضمن الدولة عدم انتهاك حرمة منزل (مسكن) فلا تفتيش إلا بمقتضى القانون. وفي إطار احترامه فلا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة. هذا بالإضافة إلى نصوص ق إ ج ج وأيضا القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

تنقسم شروط التفتيش إلى نوعين هما:

الشروط الشكلية: والتي نصت عليها كل من المواد 47،45،44 ق إ ج[2] كالآتي:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق، مع وجوب الاستظهار بهذا الأمر قبل الدخول المنزل والشروع في التفتيش.
- يجب أن يتضمن الإذن بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها وذلك تحت طائلة البطلان.
- تنجز هذه العمليات تحت الاشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان.
- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.
- في حال امتناعه عن الحضور أو كان هاربا استدعي ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.
- حدد المشرع وقت لإجراء التفتيش وهو قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا .

غير أنه يجوز التفتيش في كل ساعة من ساعات الليل أو النهار في الحالات الاستثنائية كحالة الطوارئ أو إذا تعلق الأمر بالجرائم الستة المنصوص عليها في المادة 47 ق إ ج، ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

يتم تحرير محضر التفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لكي يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة ولم يتطلب القانون شكل خاص لمحضر التفتيش وبالتالي لا يشترط لصحته سوء ما تستجوبه القواعد العامة في المحاضر عموما[3].

---

[1] بن يوسف هشام، بولعبايز أشرف الدين، التحقيق القضائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، جامعة20 أوت، سكيكدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019، ص ص 66-67.

[2] قانون06-22، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون الإجراءات الجزائية.

[3] بعرة سعيدة، المرجع السابق، ص 79.

أما الشروط الموضوعية فيقصد بها بصفة عامة في الجرائم التقليدية وبصفة خاصة في الجرائم الماسة بالمعطيات الرقمية الشروط اللازمة لإجراء تفتيش صحيح، ويمكن حصرها في الشروط الأساسية وهي سبب التفتيش، محل التفتيش، السلطة المختصة بالقيام بالتفتيش[1].

-سبب التفتيش و الهدف منه هو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث ويتمثل في وقوع الجريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين في كشف الحقيقة لدى المتهم أو في مسكنه أو بشخص غيره أو مسكنه[2].

-محل التفتيش وهو المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة[3].

فإجراء التفتيش في الجريمة الإلكترونية تحتاج إلى تقنيات خاصة تختلف عن التفتيش في الجريمة التقليدية، لأن تفتيش نظم المعلومات ليس سهلة وتتطلب معرفة بتقنية الحاسب الآلي لأنه يسهل إتلافها كليا أو جزئيا، كما يصعب تحديد مكان الدليل. وبالتالي يقع التفتيش على موضوعين الأول هو تفتيش المكونات الحاسب الآلي المادية والمعنوية والتي نص عليها القانون09-04 سالف الذكر في مادة الخامسة منه. فبالنسبة للجريمة الواقعة على المكونات المادية لا تثار إشكالية أو صعوبة إذ كان محل الجريمة أشياء مادية محسوسة، حيث ينطبق عليها ذات القواعد التقليدية للتفتيش دون أدنى عائق يحول دون هذا الإجراء، أما الجرائم الواقعة على المكونات المعنوية فيما يتعلق بالبرامج الإلكترونية لا يحتاج الأمر إلى قواعد جديدة للتفتيش عن أدلة الجريمة التي يكون محلها سرقة أو إتلاف أو استعمال هذه البرامج للتزوير أو التلاعب بالبيانات المخزنة، وفيما يتعلق بالبيانات الإلكترونية فإن في الأمر صعوبات عملية وإجرائية نظرا لتجردها من الكيان المادي المحسوس في المحيط الخارجي، وهو ما يعيق عملية إخضاعها لقواعد التفتيش التقليدية[4].

أما الثاني فهو تفتيش الشبكات المعلوماتية المتصلة بالحاسوب التفتيش عن بعد، امتداد عملية التفتيش إلى خارج الحدود الإقليمية الوطنية لابد منها في هذه الجريمة ، إلا أن ذلك يجب أن يتم وفق المعايير القانونية المنصوص عليها في القوانين الداخلية أو في الاتفاقيات الدولية، أو حتى بموجب المعاملة بالمثل، رغم أن مثل هذا الإجراء قد يستغرق وقتا طويلاً وغير مضمون النجاح بسبب التنوع التشريعي الخاص بالجريمة الإلكترونية بين مختلف الدول، ولهذا فإن الدول

---

[1] عز الدين عثماني، المرجع السابق، ص 58.

[2] بن زرت أسيا، المرجع السابق، ص 24.

[3] بن نعوم خالد أمين، المرجع السابق، ص 51.

[4] ثيتان ناصر ثيتان، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة مكملة لدرجة الماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 1433ه/2012م، ص64.

تسعى دائماً إلى إيجاد حلول قانونية للعراقيل التي تواجهها في هذا المجال، لذا نجدها تبرم العديد من الاتفاقيات الثنائية التي تتمكن من خلالها تسهيل عملية التفتيش عن الجرائم ومرتكبيها[1]. ولأجل تسهيل عملية البحث والتفتيش عن الجرائم ومرتكبيها فقد نصت عليه المادة 26من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر.

يجب أن يتم مراعاة مجموعة من الضوابط عن القيام بهذا الاجراء، لكي تتسم العملية بالشرعية وتجنب التعدي على خصوصيات الأفراد ومن أهمها وقوع جريمة إلكترونية، ونكون بصدد الجريمة الإلكترونية إذا وقعت الأفعال الإجرامية المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر8 ق.ع.ج. وكذلك إتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها[2].

ب/ ضبط الأدلة:

المقصود به هو وضع اليد على شيء يتصل بجريمة وقعت لكشف الحقيقة عنها وعن مرتكبيها. فالضبط في الجريمة الإلكترونية يختلف عن ضبط الجرائم الأخرى من حيث المحل[3]، وهي المكونات المادية والمعنوية للحاسوب التي سبق وذكرناهم.

تتمثل أشياء محل الضبط في الأشياء التي لا قيمة لها في الإثبات وهي: ضبط جهاز الحاسوب وملحقاته، وضبط المعدات المستعملة في شبكة الأنترنت، وضبط وسائط التخزين المتحركة ، وضبط وسائط التخزين المتحركة ، وضبط البرمجيات، وكذلك ضبط البريد الإلكتروني والذي قد يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية[4].

3/ الشهادة و الاستجواب:

أ/ الشهادة:

الشهادة في الجريمة الإلكترونية لا تختلف من حيث ماهيتها عن الجريمة التقليدية، وأمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية وله أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه[5].

الشهادة هي الأقوال التي يد لي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها، لذلك فالشهود ينقسمون إلى شهود نفي و شهود الإثبات[6].

أما الشاهد في الجريمة التقليدية يختلف عن الشاهد في الجريمة المعلوماتية، وهو ما اصطلح عليه بالشاهد المعلوماتي، كون أن هذا الأخير ينبغي أن يكون ذو خبرة وكفاءة وتأهيل في مجال معين متعلق ببرمجيات وتقنيات بمجال الحاسوب،

---

[1] شنتير خضرة، المرجع السابق، ص 100.

[2] بن يوسف هشام، بولعبابز أشرف الدين، المرجع السابق، ص ص 69-70.

[3] مرابطن حياة، المرجع السابق، ص ص 40-41.

[4] يوسف جفال، المرجع السابق، ص ص 32-33.

[5] غرباوي نادية، أساليب البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2017/2016، ص 74.

[6] زبيخة نور الهدى، المرجع السابق، ص 41.

حيث تمكنه خبرته من استخراج الأدلة والكشف عنها، لذلك نجد أن الشاهد المعلوماتي ينحصر في عدة طوائف تتمثل في: مشغلو الحاسب الآلي، خبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات، مديرو النظام[1].

فلشاهد التزامات لابد التقيد بها مثل : طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق والإفصاح عن كلمات المرور السرية و الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة[2].

وعموما هناك شروط يجب توافرها من أجل إلزام الشاهد المعلوماتي بالإعلام في الجرائم الإلكترونية وهي وقوع الجريمة، وعلم الشاهد الإلكتروني بالمعلومات الجوهرية المتصلة بالواقعة، أن تقتضي مصلحة التحقيق الإدلاء بهذه الشهادة.

إن إجراءات الإدلاء بالشهادة في الجريمة الإلكترونية هي نفسها في الجريمة التقليدية، وهي ما نصت عليهم المواد من 88 إلى 97 ق إ ج ج.

ب/ الاستجواب:

لم يعرف المشرع الجزائري الاستجواب فقد ترك المهمة للفقه والقضاء لأنه قد نظم هذا الاجراء في المواد من 100 إلى 108 ق إ ج ج. و الاستجواب ما هو إلا مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تفنيذا أو تسليما وذلك قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية[3].

أحاطت التشريعات استجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الاستعانة بمحام أثناء الاستجواب وتمكينه من الاطلاع على الملف والاتصال به[4].

هناك قواعد مشتركة تحكم كل الاستجوابات التي تباشر خلال مرحلة التحقيق كما أن هناك قواعد خاصة تتعلق بكل من الاستجواب الأول والاستجوابات اللاحقة له، وتنطوي هذه القواعد المشتركة باعتبارها قواعد عامة على الإجراءات الواجب إتباعها من جهة وعدد الاستجوابات من جهة أخرى[5].

3/ الخبرة:

الخبرة القضائية هي وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل أو تعزيز أدلة قائمة، كما أنها تعتبر استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية، التي يحتاج تقديرها إلى دراية علمية لا تتوفر لدى عضو السلطة القضائية المختصة بحكم عملها وثقافتها[6].

---

[1] رابح وهيبة، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد4، ديسمبر 2014، ص329.

[2] بعرة سعيدة ، المرجع السابق، ص 82.

[3] مرابطن حياة، المرجع السابق، ص 43.

[4] بعرة سعيدة، المرجع السابق، ص 82.

[5] بن يوسف هشام، بولعبايز أشرف الدين، المرجع السابق، ص 85.

[6] عبد الحليم بن بادة، إجراءات البحث والتحري عن الجرائم المعلوماتية " الخصوصية والإشكالات"، مجلة الحقوق والعلوم الإنسانية، مجلة فصلية دولية محكمة، جامعة زيان عاشور، العدد 23، مجلد2، جوان 2015 ، ص ص 82-83.

يعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاة أو سلطات الاستدلال على حد سواء، وذلك كل ما استعصى عليهم فهم موضوع معين يتميز بالتقنية، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة المرتكبة عبر الأنترنت، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الشبكات[1].

تكمن أهمية الخبرة في البحث عن الدليل الرقمي في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة من المواد 143 إلى 156 ق إ ج ج واعتبرها من إجراءات البحث عن الدليل[2].

وأنواع الخبراء يتمثلون في الخبراء الإلكترونيون في المبرمجون، المحلل مهندس الصيانة والاتصالات، مشغل الحاسب الآلي وشبكاته، مدير النظام المعلوماتي[3].

هناك شروط وضوابط للخبرة منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة، في ما يخص الأول فإنه يشترط اختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا هذا ما نصت عليه المادة 144 ق إ ج ج، و يحلف الخبير اليمين القانونية أماما المجلس حسب ما جاء في نص المادة 145 ق إ ج الج.

وأما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه وفحوصاته يعد تقريرا يتضمن خلاصة لما توصل إليه من نتائج، بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث. وإن كان المشرع لم يوجب إتباع شكل معين في تقرير الخبرة فقد يكون شفويا وقد يكون كتابيا وفقا لما تحدده طبيعة الضبطية[4].

أما فيما يخص متطلبات أعمال الخبرة في الجريمة الإلكترونية فتتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية كما تتنوع شبكات الاتصال بينها، مما أن تدقق جهات التحقيق والمحاكمة عند اختيارها للخبير[5].

4/ التسرب:

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل ق إ ج ج سنة2006 ولكون أن الجريمة الإلكترونية من الجرائم التي يمكن اللجوء فيها إلى إجراء التسرب أذا اقتضت ضرورة البحث والتحري، لذلك فقد أصبح لوكيل الجمهورية ولقاضي التحقيق بعد إخطار وكيل الجمهورية بصلاحية منح الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص والتسرب بينهم على أنه فاعل أو شريك معهم في الجريمة وقد نظمتهم المواد من 65مكرر 11 الى 65 مكرر 18 ق إ ج ج.

عرفته المادة 65 مكرر12 " يقصد بالتسرب قيام ضابط 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".

---

[1] صغير يوسف، المرجع السابق، ص 87.
[2] زبيخة نور الهدى، المرجع السابق، ص 45.
[3] يوسف جفال، المرجع السابق، ص 34.
[4] سعيداني نعيم، المرجع السابق، ص ص 168-169.
[5] غرباوي نادية، المرجع السابق، ص 73.

لقد أحاط المشرع الجزائري هذا الإجراء بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية، كون أن التسرب يخضع لعدة شروط شكلية وموضوعية و في حالة مخالفتها يحكم على العملية بالبطلان وهو ما تناولته المواد 65 مكرر11 و 65مكرر15.

يمكن تصور عملية التسرب في نطاق هذه الجرائم في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو اشتراكه في محادثات في غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم، والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام المخترق للمواقع، أو كيفية ارتكاب الجرائم وحتى المشاركة معهم في ارتكابها لتجميع كل ما يمكن جمعه من الأدلة[1].

5/ اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

قد نظم المشرع الجزائري هذه الإجراءات للكشف عن الجرائم والمتورطين فيها في المواد من 65 مكرر 05 إلى 65 مكرر 10 ق 06-22 المعدل والمتمم لقانون الإجراءات الجزائية. ولصحة هذه الإجراءات يشترط على أنه لا يمكن اللجوء إلى هذه الوسائل إلا في الجرائم المتلبس بها أو في التحقيق الأولي المتعلق بالجرائم الستة المنصوص عليهم في المادة37 ق إ ج، كذلك الحصول على إذن من وكيل الجمهورية المختص أو قاضي التحقيق، ويجب أن يقوم ضباط الشرطة القضائية بتحرير محضر عن كل عملية اعتراض أو تصوير قام بها مع ذكر تاريخ وساعة بداية العملية ونهايتها[2].

تعرف على أنها اعتراض كل المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية التي يقصد بها التنصت التليفوني و هي تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء إلى تسجيل المكالمات في أشرطة ممغنطة[3].

تتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات، والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض، وذلك باستعمال وسائل اتصال سلكية و لاسلكية ، ويشمل اعتراض المراسلات نوعان الأول يتمثل في المراسلات الإلكترونية، والأخرى المراسلات البريدية[4].

وتضمنت المواد من 65 مكرر5 إلى 65 مكرر7 شروط هذا الإجراء.

والتقاط الصور هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص وهذه الإجراءات بالسرية التامة، وهي إجراءات فيها مساس بحرمة الحياة الخاصة للأشخاص المكفولة

---

[1] يوسف جفال، المرجع السابق، ص 37.

[2] فريدة بن يونس، الإطار الناظم لاختصاص الشرطة القضائية في مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة الاجتهاد القضائي، المجلد 12، عدد22، خبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، 2020، ص ص 131-132.

[3] غرباوي نادية، المرجع السابق، ص ص 78-79.

[4] فريدة بن يونس، المرجع السابق، ص ص 131-132.

دستوريا، غير أن المشروع كفلها بضمانات وضوابط أساسية سيتم التطرق إليها فيما بعد[1].

أما تسجيل الأصوات يقصد به النقل المباشر و الآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل يحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي، بحيث يمكن لإعادة سماع الصوت والتعرف على مضمونه، وهو ما أشار إليه المشرع الجزائري في المادة 65 مكرر05 ق إ ج ج. ويتم استخدام هذه الوسائل في المحلات السكنية و الأماكن الخاصة والأماكن العامة، ويتم تسجيل الأصوات باستعمال أجهزة التسجيل المستخدمة في تسجيل الصوت على أشرطة يمكن سماعها فيما بعد وفي أي وقت، وتتمثل أجهزة تعمل بواسطة الاتصال السلكي الخارجي و اللاسلكي، وأجهزة التسجيل الصوتي من داخل المكان ومن خارج المكان، ميكروفونات الليزر والتوجيه والتلامس[2] .

6/المراقبة الإلكترونية:

هذا الإجراء تم استحداثه بموجب المادة 03 من القانون 09-04 المتضمن القواعد الخاصة من الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحتهما، فقد أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواه[3].

لم يتطرق المشرع الجزائري لتعريف المراقبة الإلكترونية واكتفى بتحديد مفهوم الاتصالات الإلكترونية في المادة 01 من القانون 09-04، إلا أن الفقه تصدى لذلك وعرفه على أنه مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات أو معلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[4].

من الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الإلكتروني فقط بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب القيام بإجراءات مراقبة الاتصالات الإلكترونية فإنه يمكن كذلك تطوير هذه التقنية، لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة[5].

أحاط المشرع هذا الإجراء باعتباره وسيلة إجرائية للحصول على الدليل الرقمي في مجال هذه الجريمة بمجموعة من الشروط وكذلك هناك حالات يسمح

---

[1] إبتسام بغو، المرجع السابق، ص ص 35-36.

[2] فريدة بن يوسف، المرجع السابق، ص 132.

[3] عبد الحليم بن بادة ، المرجع السابق، ص 86.

[4] إلهام بن خليفة، القواعد الإجرائية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مداخلة، جامعة الشهيد حمة لخضر، الوادي، كلية الحقوق والعلوم السياسية، ص 06.

[5] يوسف جفال، المرجع السابق، ص ص 40-41.

فيه باللجوء إلى المراقبة الإلكترونية وقد تضمنتهم المادة 04 من ق 09-04 سالف الذكر.

يجب الاعتراف للمشرع الجزائري أنه قد خطى خطوة جريئة من خلال نصه على إجراء الرقابة الإلكترونية للاتصالات، على اعتبار أنه من أخطر الإجراءات في النظام الإجرائي عبر العالم الافتراضي كونه يمس بخصوصية وحرمة حياته[1].

7/ حفظ المعطيات:

بعد مباشرة عملية التفتيش من طرف السلطات المختصة واكتشاف معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[2].

وقد ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف، ووضعها في ترتيب معين، في حين اتخاد إجراءات قانونية محتملة أخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير (معطيات المرور)[3]، والتي عرفتها المادة 02 من القانون 09-04 سالف الذكر، و يلتزم مقدمو الخدمات بحفظ المعطيات المتعلقة بحركة السير والتي حصرها المشرع الجزائري في المادة 11 من القانون 09-04[4].

في إطار تطبيق قانون 09-04 وبموجب المادة 11 منه، يتعين على مقدمي الخدمات تقديم المساعدة لسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة وذلك لتمكن سلطات التحقيق من التعرف على مستعملي الخدمة. ويتعين عليهم أيضا كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، وقد حدد المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل[5].

---

[1] عبد الحليم بن بادة ، المرجع السابق، ص 86.

[2] يعيش تمام شوقي، المرجع السابق، ص 69.

[3] نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة أحمد دراية ، أدرار، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017/2016، ص 52.

[4] لاحظ المادة 11 من القانون 09-04، سالف الذكر، التي تنص على أنه" مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ: .....المطلع عليها"

[5] أمحمدي بوزينة أمنة، المرجع السابق، ص 78.

وحسب نص المادة 12 من نفس القانون فقد نصت على الالتزامات الخاصة لمقدمي الخدمة.

الفرع الثاني: غرفة الاتهام

نظم المشرع الجزائري غرفة الاتهام في إ ج ج في المواد من 176 إلى 211، فقد خول لها سلطات واسعة وهامة في مجال التحقيق القضائي خصوصا فيما يتعلق باستئناف أحد أطراف الدعوى لأوامر قاضي التحقيق أو إذا كان الأمر يتعلق بجناية بحيث أن تدخلها إلزامي و وجوبي بقوة القانون باعتبارها درجة ثانية للتحقيق في مواد الجنايات، وبعد ذلك تقوم بإصدار مجموعة من القرارات الخاصة بالتحقيق[1]. وما يهمنا هنا هو اختصاص غرفة الاتهام كجهة استئناف هي تلك الصادرة عن قاضي التحقيق.

وغرفة الاتهام هي إحدى غرف المجلس القضائي، تختص بالنظر في القضايا المطروحة عليها من النائب العام لتقرر بشأنها ألا وجه للمتابعة، أو بإحالة حسب الأحوال، كما تختص كما سبق وأن ذكرنا باستئناف قرارات قاضي التحقيق وطلب الاسترداد و كذلك بمراقبة أعمال الضبطية القضائية[2].

لقد أقر المشرع حق الاستئناف لأوامر قاضي التحقيق لكل الخصوم في الدعوى العمومية، أي كما يجوز للنيابة العامة أن تستأنف أوامر قاضي التحقيق يجوز كذلك للمتهم ومحاميه وللمدعي المدني أو محاميه أن يستأنف هذه الأوامر، فالمشرع حدد لكل طرف الأوامر التي يطعن فيها بالاستئناف وقد جاءت على سبيل الحصر[3].

فالاستئناف طريق من طرق الطعن، قرره القانون لنعي على أوامر قاضي التحقيق لدى جهة عليا وهي غرفة الاتهام، والطعن بهذا المفهوم يعتبر إعادة للتحقيق وتجديدا له. ويحكم استئناف أوامر قاضي التحقيق ضوابط مختلفة، حددتها الأحكام الواردة في المواد 170ألى. 174 ق إ ج ج، وهذه الضوابط منها ما يتعلق بالخصوم، ومنها ما يتعلق بالأوامر التي يجوز استئنافها[4].

لنيابة العامة الحق في استئناف جميع و أوامر قاضي التحقيق وهذا ما نصت عليه المادة 1/170 ق إ ج ج، وقد نصت المادة 2/170 ق إ ج ج على أنه استئناف وكيل الجمهورية يكون بتقرير لدى كاتب ضبط التحقيق ويجب أن يرفع في ظرف 3 أيام من تاريخ صدور الأمر موضوع الاستئناف[5].وهذا ما أكدته المحكمة العليا في إحدى قراراتها أيضا بالقول" يجوز لوكيل الجمهورية ، استئناف أوامر قاضي التحقيق، بما فيها تلك المطابقة لطلباته"[6].

وللمتهم ومحاميه أيضا حق الاستئناف أمام غرفة الاتهام كما سبق وذكرنا وهذا ما نصت عليه المادة 172 ق إ ج ج.

---

[1] مفتاح بلال، اختصاصات غرفة الاتهام في قانون الاجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015، ص 16.

[2] طواهري اسماعيل، محاضرات شرح قانون الاجراءات الجزائية الجزائري، محضرات ألقيت لطلبة السنة الثانية حقوق، جامعة الوادي، كلية الحقوق والعلوم السياسية، 2015/2014، ص 65.

[3] مفتاح بلال، المرجع السابق، ص 18.

[4] عبد الله وهايبية، المرجع السابق، ص ص 425-426.

[5] مفتاح بلال، المرجع السابق، ص 25.

[6] القرار رقم 385600، الصادر بتاريخ 2005/09/21/، المجلة القضائية رقم 2 الصادرة سنة 2005، ص455.

وللمدعي المدني ومحاميه أيضا الحق باستئناف أوامر قاضي التحقيق أمام غرفة الاتهام وذلك حسب ما جاءت به المادة 173 ق إ ج ج، وما أكده قرار المحكمة العليا بقولها" من المقرر قانونا يجوز للمدعي المدني أو وكيله أن يطعن بطريق الاستئناف.....حقوقه المدنية"[1].

المطلب الثالث: التحقيق النهائي

تعتبر مرحلة المحاكمة الحلقة الأخيرة في سبيل الإجراءات التي تمر بها الدعوى وذلك عن طريق صدور حكم قضائي فيها، وتسمى هذه المرحلة عادة بالتحقيق النهائي وهذا ما اصطلحت على تسميته، فسنتطرق من خلال هذا المطلب إلى تبيان اختصاص المحكمة وكذا تشكيلتها وإجراءات سيرها، وفي الأخير القواعد العامة للمتابعة.

الفرع الأول: الاختصاص

أولا: الاختصاص النوعي

يتحدد الاختصاص النوعي للمحكمة الفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من ق إ ج ج، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في القوانين الخاصة حسب المادة 328 ق إ ج ج[2].

ولان الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء أن يخضعوا لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع الجزائري مع بعض أنواع الجرائم، إذ جعل الاختصاص ينعقد إلى دائرة اختصاص محاكم أخرى وهذا ما نصت عليه المواد 37، 40، والمادة 329 من ق إ ج ج أثر التعديل الذي جاء به القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة، وهران، ورقلة[3].

ثانيا: الاختصاص المحلي

طبقا لنص المادة 37 ق إ ج يتحدد الاختصاص المحلي للجريمة في ثلاثة ضوابط مكان وقوع الجريمة، محل اقامة أحد الأشخاص المشتبه فيهم، مكان الضبط أو القبض، ويجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخري[4].

وفي نطاق الجرائم الإلكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في

---

[1] القرار رقم 195889، الصادر بتاريخ 1998/07/14، المجلة القضائية رقم02، الصادرة سنة 1998.

[2] بن زرت أسيا، المرجع السابق، ص 39.

[3] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنسل شهادة الماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012/2011، ص 106.

[4] القانون 04-14،سالف الذكر.

مكان آخر، فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، وتعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الأنترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة اليها[1].

كما نصت أحكام المرسوم التنفيذي رقم 06-348[2] على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة إلى دائرة اختصاص محاكم أخرى، ويجيز كذلك القانون تمديد الاختصاص المحلي لضباط الشرطة القضائية في الحالات المنصوص عليها في المادة 16 ق إ ج الج .

وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني ، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الاستراتيجية للدولة وذلك في إطار التعاون الدولي[3].

الفرع الثاني: تشكيلة المحكمة

تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع الجنح الخاصة بالجريمة الإلكترونية على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه. أما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فيها ثلاثية أي تتشكل من رئيس غرفة ومستشارين بالإضافة إلى كاتب ضبط وبحضور نائب عام أو أحد مساعديه أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها [4].

الفرع الثالث: إجراءات سير المحاكمة

تباشر المحكمة جلستها بالإعلان أولا عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها، وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة[5].

وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر 06 ق إ ج تتخذ المحكمة إحدى الاجراءات التالية:

"إذا قررت المحكمة تأجيل القضية يمكنها، بعد الاستماع إلى طلبات النيابة والمتهم ودفاعه، اتخاذ أحد التدابير التالية:

- ترك المتهم حرا.
- إخضاع المتهم لتدبير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر01 قانون الإجراءات الجزائية من هدا القانون.

---

[1] بعرة سعيدة، المرجع السابق، ص 93.

[2] المرسوم التنفيذي رقم 06-348، سالف الذكر.

[3] محمد بن عمرة، سيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في العلوم القانونية، جامعة أكلي محند الحاج، بويرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020/2019، ص 49.

[4] مرابطن حياة، المرجع السابق، ص 53.

[5] بن زرت أسيا، المرجع السابق، ص 40.

- وضع المتهم في الحبس المؤقت.

لا يجوز الاستئناف في الأوامر التي تصدرها المحكمة وفقا لهذه المادة".

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفوري فإنه يساق بواسطة القوة العمومية لحضور الجلسة و يخطره رئيس الجلسة بأن له الحق في اختيار محام الدفاع عنه فإن طلب ذلك أمهله القاضي مهلة لا تقل عن ثلاثة أيام لتحضير دفاعه .ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي وبعدها يقوم القاضي بسماع الشهود[1].

وبعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني فقط دون المطالعة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة و تقديم التماساها، ليقوم دفاع المتهم بتقديم مرافعته وتقديم التماساها، ويكون بعدها لنيابة العامة والمدعى حق الرد على موافقة محام المتهم وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحقا منطق بالحكم[2].

الفرع الرابع: القواعد العامة للمحاكمة

تقوم المحاكمة على مجموعة من المبادئ تنطبق على المحكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية وسنحاول شرحها كالآتي بيانه:

أولا/ علانية الجلسة:

جل التشريعات تقر بمبدأ علانية الجلسة، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الاطمئنان والشعور بالعدالة وهذا على البحث الأولي الذي يقوم به ضباط الشرطة القضائية وكذا التحقيق الإبتدائي الذي تقوم به الجهات التحقيق، فكلاهما يتم في سرية ، إلا أن العلانية ليست في جميع الجلسات فللقاضي سلطة تقديرية في إخراج القصر من الجلسة ، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على النظام العام والآداب العامة ، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية، وبحكم هذا المبدأ نص المادة 285من ق إ ج ج[3].

ثانيا: شفوية المرافعات:

لأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولا يتم الاكتفاء بالتحقيقات الأولية والابتدائية التي سبقت المحاكمة[4].

ثالثا: حضور أطراف الخصومة:

لا يجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة لنيابة فهي جزء من التشكيلة[5].

رابعا/ تدوين التحقيق النهائي:

---

[1] محمد بن عمرة، سيد علي بنينال، المرجع السابق، ص 51.

[2] مرابطن حياة، المرجع السابق،54-55.

[3] محمد بن عمرة، سيد علي بنينال، المرجع السابق، ص 51.

[4] بن زرت أسيا، المرجع السابق، ص 42.

[5] بعرة سعيدة، المرجع السابق، ص 97.

لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دوره يتجسد في تدوين كل ما يدور بالجلسة وفي الأخير نستنتج أن الجريمة الإلكترونية لم يخصص لها إجراءات متابعة خاصة بها وإنما تخضع لنفس إجراءات الجريمة لتقليدية[1].

في نهاية هذا الفصل تتضح لنا الرؤية على أن الجريمة الإلكترونية فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الإجرام الذي أصبح يهدد أمن و استقرار المجتمعات، والمشرع الجزائري حاول وضع مجموعة من الآليات الموضوعية والإجرائية لمواجهته بشكل فعال، وهذا ما تطرقنا له من خلال المبحثين، كون أنه سبق وأشرنا أن القواعد الإجرائية التقليدية المقررة لمتابعة الجريمة التقليدية لا تتلاءم مع الطبيعة التقنية الخاصة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال والأدلة الناتجة عنها والتي تكون في شكل إلكتروني والتي يصعب أيضا على المحقق العادي التعامل معها، كونها تحتاج إلى إلمام خاص بكافة جوانب تكنولوجيا المعلومات، ولهذا كان من اللازم خلق قواعد إجرائية مستحدثة وكذا نصوص قانونية جديدة لتواكب التطور السريع الحاصل في مجال المعلوماتية، وكذلك قام المشرع بتمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق بموجب المرسوم التنفيذي 06-348، وذلك نظرا لخطورة بعض الجرائم وخصوصيتها والتي تعتبر الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات من ضمن هذه الجرائم.

وبالإضافة إلى ما تثيره هذه الجريمة من عقبات تواجه الأجهزة القضائية والأمنية، ولهذا وجب منح أفراد الشرطة القضائية صلاحيات تمكنهم من اتخاد إجراءات أولية سريعة ضمن ضوابط قانونية، وفي ذات الحين منحت عدة صلاحيات لقاضي التحقيق لكشف مرتكب هذه الجرائم والمتسبب بالأضرار ضمن ضوابط قانونية حددتها نصوص قانون الإجراءات الجزائية، فقد سبقت الإشارة الى كل هذه النقاط من خلال هذا الفصل.

[1] محمد بن عمرة، سيد علي بنينال، المرجع السابق، ص 52.

خاتمة

بعد انتهائنا بفضل الله من كتابة هذا البحث والذي هو حصيلة جهد متواضع. الذي كان موضوعه الجرائم الإلكترونية في التشريع الجزائري، و التي تعتبر من الجرائم المستحدثة في المجتمع، ولارتباطها بالتكنولوجيا المتطورة أدى هذا إلى تمييزها عن الجرائم التقليدية بدءا من تسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها.

ونتيجة لهذا التطور الذي جاءت به الأنظمة المعلوماتية، والذي عاد على الدول بمخاطر عدة ناتجة عن إساءة استخدام شبكة الأنترنت و تطويعها لصالح مرتكب الجريمة لممارسة نشاطاته الجرمية، وبذلك أصبحنا أمام مشكلة من المشكلات التي أفرزتها ثورة الاتصالات، فقد غيرت هذه الجريمة النظرة التقليدية التي كان ينظر بها إلى الجريمة على العموم، فقد ظهر مع ظهور الجريمة مفهوم جديد لم يعرفه القانون من قبل، فهي لم تنل قدرا كبيرا من التقنين، كونها اتسمت بخصوصية ميزتها عن غيرها من الجرائم، فقد تعددت التعريفات واختلفت في وصف هذه الظاهرة الإجرامية المستحدثة، وكذلك تميزها بطابعها العابر للحدود، بالإضافة إلى ضعف القائمين على مكافحتها، نظرا إلى التطور المتسارع في ارتكابها، وكذلك السمات التي انفرد بها مرتكب الجريمة جعلت منها جريمة مميزة. فقد حاولوا خلق إطار قانوني كفيل بحصر الأفعال الإجرامية التي يقوم بها مرتكبوها، أولئك المجرمون الذين لهم صفات تمكنهم من القيام بجرائمهم بكل حرفية وسرعة وذكاء مما يجعلها صعبة ومعقدة، مما تستلزم آليات مكافحة خاصة، والاعتماد على جهات بحث وتحري متمكنة لصد مثل هذا النوع الخطير من الجرائم، وكذا جهات محاكمة متخصصة، فقد قام المشرع الجزائري بتعديل قانون العقوبات ليواكب التطور، وكذلك بإصداره قانون 09-04 ليتناسب مع الظاهرة المستحدثة.

ولا ننكر الصعوبة التي واجهتنا لإنجاز هذه الدراسة خاصة بالنسبة لضرورة إلمامنا بالجوانب التقنية حتى نتمكن من الإحاطة بالجوانب القانونية، إلا أن ذلك لا يمنع أننا توصلنا في ختام دراستنا لهذا الموضوع إلى أهم النتائج، ومجموعة من التوصيات، وذلك على النحو التالي:

النتائج المتوصل إليها:

-نظرا لحداثة هذا السلوك الإجرامي والذي يتجسد في الجريمة الإلكترونية، إلا أنه لا يوجد لحد الآن إجماع فقهي موحد على تعريف لها مما أدى بالقول أن هذه الجريمة تقاوم التعريف.

-إن الجريمة الإلكترونية ظاهرة جديدة وخطيرة وهي تمثل الوجه السلبي لثورة المعلوماتية والتطور التكنولوجي كونها تتخذ نظام الحاسوب كوسيلة لها.

-إن ارتباط الجرائم الإلكترونية بالتقنية المعلوماتية جعل منها جريمة ذات طبيعة خاصة، تتميز عن غيرها من الجرائم التقليدية، سواء من حيث ماهيتها، أو خصائصها، أو مرتكبيها، وحتى ضحاياها.

-الجرائم الإلكترونية من بين الجرائم التي لا يتطلب فيها عنف على الإطلاق كون أن مرتكب هذه الجريمة يتصف بالذكاء والمعرفة والسرعة، وكذلك مميزا بالدقة و التخصص في مجال التقنية المعلوماتية.
-هي من بين الجرائم التي تتوافق مع غيرها من الجرائم في مدى توفر القصد الجنائي العام.
-عدم كفاية النصوص القانونية المتوصل إليها من طرف المشرع الجزائري بمناسبة التجريم والعقوبة في مادة الجريمة الإلكترونية وذلك لتعدد الأوصاف والكيفيات التي تتخذها الجريمة المعلوماتية في ظل التطور المذهل والمتسارع مما يلزم المشرع على أن يتماشى وما يفرضه التقدم لوضع آليات لتصدي لمثل هذه الجرائم.
- -المشرع الجزائري لم يقم بتحديد الجرائم المرتكبة باستخدام النظام المعلوماتي وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراتها.
-وسائل التحقيق التقليدية لم تعد كافية لإثبات هدا النوع من الجرائم.

ومن خلال هذه النتائج نتوصل إلى التوصيات الآتية:

-ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل فيه كل السلوكات الجرمية.
-ضرورة انضمام الجزائر إلى الاتفاقيات الدولية والعربية لتعاون على التصدي للجريمة الإلكترونية، ومن بينها انضمامها إلى اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية.
-وضع إجراءات كالتحقيق والمكافحة للجريمة الإلكترونية تختلف عن الجريمة التقليدية.
-ضرورة تكريس مقياس الجريمة الإلكترونية من ضمن المنهج الدراسي لطلبة القانون الجنائي.
-ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الإجرام وتحقيق التعاون مع أصحاب الخبرة، وذلك بشكل دائم.
-ضرورة إعطاء صلاحيات واسعة للهيئة الوطنية للوقاية من الإجرام.
-ضرورة استحداث نصوص قانونية جديدة خاصة في قانون الإجراءات حتى تتلاءم في مجال الضبط والتحقيق.
-ضرورة وضع قانون جديد خاص بالجرائم الإلكترونية باختلاف أنواعها وطرق مكافحتها.
-تفعيل دور الأسرة في متابعة الأبناء لحمايتهم من الآثار السلبية والمخاطر المترتبة عن الاستخدام الغير آمن لشبكات الأنترنت.

قائمة المصادر والمراجع

I. النصوص الرسمية

أ-المعاهدات

1-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، القاهرة، مصر، 2010، والتي وقعت عليها الجزائر في 2010/12/21.

ب- النصوص التشريعية

1-الأمر 66-156، المؤرخ في 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، ج ر، عدد07، المؤرخة في 10 يونيو سنة 1966، المعدل والمتمم.
2-الأمر رقم 66-156المؤرخ في18 صفر1386الموافق ل08 يونيو1966، المتضمن قانون العقوبات المعدل والمتمم، ج ر عدد 84، بتاريخ24-12-2006 ، المعدل والمتمم.
3-الأمر 73-14، المؤرخ في 03 أفريل 1973 المتعلق بحقوق المؤلف و الحقوق المجاورة له.
4-قانون رقم 2000-03 مؤرخ في 05 جمادى الأول عام 1421 الموافق 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.
5-الأمر 03-07، المؤرخ في 2003/07/19 يتعلق ببراءات الاختراع ، ج ر عدد 44، الصادرة في 2003/07/23.
6-القانون رقم 08-01 المؤرخ في 2008/01/23 المتعلق بالتأمينات الاجتماعية، ج ر، عدد 04، الصادرة في 27 يناير 2008، المعدل والمتمم للقانون 83-11 المتعلق لتأمينات الاجتماعية.
7-القانون09-04المؤرخ في2009/08/05،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر العدد07،لسنة2009.

ج/المراسيم

1-المرسوم التنفيذي 06-348 المؤرخ في 12 رمضان عام 1427 الموافق ل05 اكتوبر سنة 2006، والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد 63.
2-المرسوم رئاسي رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق ل08 أكتوبر سنة 2015، يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3-المرسوم رئاسي رقم 19-172 المؤرخ في 03 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.

د/القرارات القضائية

1-القرار رقم 385600، الصادر بتاريخ 2005/09/21/، المجلة القضائيةرقم02، 2005.
2-القرار رقم 195889، الصادر بتاريخ 1998/07/14، المجلة القضائية رقم1998،02.

II. الكتب

1-أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 18، دار هومة للطباعة والنشر والتوزيع،الجزائر،2019.

2- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط02، دار هومة لطباعة النشر والتوزيع، الجزائر، 2007.
3- ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر "أساليب وثغرات"، د ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2010.
4- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، د ط، الدار الجامعية للنشر،الإسكندرية،2008.
5- سامي على حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، د ط، دار الفكر الجامعي للنشر،الإسكندرية،2007.
6- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، ط01، منشورات الحلبي الحقوقية، لبنان، بيروت،2011.
7- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني للحماية المعلوماتية "، د ط، دار الجامعة الجديدة للنشر،الإسكندرية،2009.
8- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت(الجرائم الإلكترونية)"دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة الى جهود مكافحتها محليا وعربيا ودوليا،ط01،منشورات الحلبي الحقوقية،2007.
9- عبد الله وهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، د ط، دار هومة للطباعة والنشر والتوزيع، 2004.
10- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، ط01، دار المستقبل للنشر والتوزيع،عمان،1430ه-2019م.
11- عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط03، د دار النشر، الجزائر، بجاية، 2017.
12- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي "دراسة قانونية متعمقة في القانون المعلوماتي، د ط، دار الكتب القانونية للنشر، مصر،2007.
13- عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الألي ومشكلة قرصنة البرامج، ط01، دار وائل للنشر، 2005.
14- علي جبار الحسناوي، جرائم الحاسوب والأنترنت، د ط، دار اليازوري العلمية للنشر والتوزيع، الاردن، عمان،2009.
15- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية "دراسة مقارنة"، ط1، دار الحامد للنشر والتوزيع،الاردن،عمان،2015م/1436ه.
16- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكثرونية،ط01،دار النشر،1430ه-2009م.
17- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2006.
18- محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، ط02، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019.

19- نهلا عبد القادر المومني، الجرائم المعلوماتية،ط01،دار الثقافة للنشر والتوزيع،الأردن،1429ه-2008م.
20- وسيم حسام الدين الأحمد، مكافحة الجريمة الإلكترونية في التشريعات والاتفاقيات الدولية،ط01،دار غيداء للنشر والتوزيع، عمان، 2020.
21- يعيش تمام شوقي، الجريمة المعلوماتية "دراسة تلأصيلية مقارنة"، ط 01، سلسلة مطبوعات المخبر، مخبر أثر الإجتهاد القضائي على حركة التشريع، الجزائر، بسكرة، جانفي 2019.

III. مذكرات ورسائل الجامعية

أ/ دكتوراه

1-هروال هبة نبيلة، جرائم الأنترنت "دراسة مقارنة" ،مذكرة لنيل شهادة الدكتوراه، جامعة ابو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2011/2010.

ب/ ماجستير

1-صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية"،2013.
2-ثيتان ناصر ثيتان، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة مكملة لدرجة الماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 1433ه/2012م.
3-حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2012/2011.
4-دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، جامعة منثوري قسنطينة، كلية الحقوق،2014/2013.
5-رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شهادة ماجستير قانون عام، جامعة ابو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2012/2011.
6-سوير سفيان ، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بالقايد تلمسان، كلية الحقوق والعلوم السياسية،2011/2010 .
7-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2012.
8-شنتير خضرة، الآليات القانونية لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية ،قسم الحقوق، 2012/2011.
9-عبد الله دغش العجمي، المشكلات العلمية والقانونية للجريمة الإلكترونية "دراسة مقارنة"، مذكرة لنيل درجة الماجستير في القانون العام، جامعة الشرق الأوسط،2014.

10-معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنسل شهادة الماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012/2011.

ت/ مذكرات ماستر

1-ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2016/2015.

2-ابتسام موهوب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2014/2013.

3-بن زرت أسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مدكرة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2019/2018.

4-بن يوسف هشام، بولعبايز أشرف الدين، التحقيق القضائي في الجرائم الإلكترونية، مدكرة لنيل شهادة الماستر، جامعة20 أوت، سكيكدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019.

5-بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري "دراسة مقارنة"، مذكرة مكملة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2015-2016.

6-بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة عبد الرحمان بن باديس، مستغانم، كلية الحقوق والعلوم السياسية، قسم قانون خاص،2019.

10-بوشعرة أمينة، مساوي سهام، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مدكرة لنيل شهادة الماستر، جامعة عبد الرحمان ميرة، بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص،2018/2017.

11-حمداش كاهنة، مداني وفاء، التحقيق القضائي في ظل قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2017/11/30.

12-زبيخة نور الهدى، الإثبات الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، جامعة العربي بن مهيدي ،أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015.

13-سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2014/2013.

14-غرباوي نادية، أساليب البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر، جامعة أكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، 2017/2016.

15-فتيحة مهري، جريمة الدخول والبقاء في أنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق،2016/2015.
16-فليح نور الدين، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق قانون جنائي و العلوم الجنائية، جامعة مولاي الطاهر سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2019/2018.
17-لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، جامعة أكلي محند أولحاج البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام،2015/2014.
18-مرابطن حياة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون الجنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، كلية الحقوق والعلوم السياسية، قسم القانون العام،2019/2018.
19-محمد بن عمرة، سيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مدكرة لنيل شهادة ماستر في العلوم القانونية، جامعة أكلي محند الحاج، بويرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020/2019.
20-مفتاح بلال، اختصاصات غرفة الاتهام في قانون الاجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2016/2015.
21-نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مدكرة لنيل شهادة الماستر، جامعة أحمد دراية ، أدرار، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017/2016.
22-يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر أكاديمي، تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2017/2016.

IV. المقالات والمجلات والملتقيات

1- أسامة غربي، جرائم الأنترنت بين الجانب التقني وأساليب المكافحة، مجلة الحقوق والحريات، العدد 02، جامعة المدية، 2015.
2-أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة الجلفة، العدد01، المجلد10، 2017.
3-بوضياف اسمهان، الجريمة الإلكترونية وإجراءات تشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف مسيلة،العدد11، 2018.
4-بن شهرة شول ومراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، المركز الجامعي آفلو، العدد 01،المجلد 04، 2020.
5-حسين فريجة، الجريمة الإلكترونية والأنترنت، مجلة المعلوماتية،العدد36،أكتوبر 2011.
6-رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية أدرار، العدد 41، 2018.

7-رابح وهيبة، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد4، ديسمبر 2014.
8-رمزي حوحو و منيرة بلوزغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، العدد 02، 2014.
9-زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة مولود معمري، العدد 03،المجلد 04، 2019.
10-صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، العدد 01، المجلد 07، 2021/06/28.
11-دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 13، 2020/01/05.
12-فريدة بن يونس، الإطار الناظم لاختصاص الشرطة القضائية في مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة الاجتهاد القضائي، المجلد 12، عدد22،خبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، 2020.
13-عبد الحليم بن بادة، إجراءات البحث والتحري عن الجرائم المعلوماتية " الخصوصية والإشكالات"، مجلة الحقوق والعلوم الإنسانية، مجلة فصلية دولية محكمة، جامعة زيان عاشور، العدد 23، مجلد2، جوان 2015.
14-عبد السلام محمد المايل "وأخرون" ،الجريمة الإلكترونية في الفضاء الإلكتروني "المفهوم -الأسباب-سبل المكافحة مع التعرض لحالة ليبيا" ،مجلة أفاق للبحوث والدراسات سداسية دولية محكمة، المركز الجامعي إليزي، العدد 04، 2019.
14-عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد 04، جانفي 2018.
15-لاميةطالة، الجريمة الإلكترونية "بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، جامعة الجزائر، العدد 02، المجلد 06، 2020.
16-مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجريمة المتصلة بتكنولوجيا الإعلام والاتصال، مخبر البحث في السياحة، الإقليم والمؤسسات، العدد 01،المجلد 09، 2020.
17-معاشي سميرة، الجريمة المعلوماتية(دراسة تحليلية لمفهوم الجريمة المعلوماتية)،مجلة الفكر، جامعة محمد خيضر،العدد17، 2008.
18-مليكة أبوديار، الإثبات الجنائي في الجرائم الإلكترونية، المجلة الإلكترونية للأبحاث القانونية، العدد 02، 2018.

V. الملتقيات والندوات

1-الشافعي مالكية، تكنولوجيا المعلومات الحديثة وأثارها في تسريب أسئلة البكالوريا وأسئلة التعليم المتوسط بالجزائر2015 ،الملتقى الوطني" الأمن المعلوماتي :مهدداته وسبل الحماية"، الممارسات اللغوية في الجزائر، جامعة مولود معمري،03-2015/11/04.
2-محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، كتاب أعمال الملتقى الوطني: أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، جامعة حسيبة بن بوعلي، الجزائر، 29 مارس 2017.
3-إلهام بن خليفة، القواعد الإجرائية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مداخلة، جامعة الشهيد حمة لخضر، الوادي، كلية الحقوق والعلوم السياسية.
4-خديجة حامي، الأنظمة المعلوماتية في مواجهة القرصنة والتخريب "المخاطر المحدقة والحلول الناجعة"، الملتقى الوطني "الأمن المعلوماتي: مهدداته وسبل الحماية"، مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري،03-2015/11/04.
5-دياب موسى البادية، الجرائم الإلكترونية "مفهوم والأسباب"، الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية،عمان،7-9/ 11/ 1435ه الموافق ل 2-4/ 09/ 2014م.
6-رضية بركايل، التنظيم القانوني الجزائي للجريمة المعلوماتية في التشريع الجزائري، الملتقى الوطني "الأمن المعلوماتي: مهدداته وسبل الحماية "مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري03-2015/11/04.
7-مسيكة محمد الصغير و بوعيدلي جمال، مفهوم الجريمة المستحدثة وطبيعتها القانونية، كتاب أعمال الملتقى الوطني "الجريمة المستحدثة وآليات مكافحتها "مخبر بحث نظام الحالة المدنية، جامعة الجيلالي بونعامة خميس مليانة، 05-06 /05/ 2019.

VI. التقارير والمحاضرات

1-بغانة عبد السلام، مقياس قانون الإجراءات الجزائية، مطبوعة موجهة لطلبة نظام ل م د شريعة وقانون وحقوق الإنسان، جامعة الأمير عبد القادر للعلوم الإنسانية، كلية الشريعة والاقتصاد، قسم الشريعة والقانون، 2015/2014.
2-طواهري اسماعيل، محاضرات شرح قانون الاجراءات الجزائية الجزائري، محضرات ألقيت لطلبة السنة الثانية حقوق، جامعة الوادي، كلية الحقوق والعلوم السياسية، 2015/2014.
3-عماري فوزي، التحقيق الجنائي، محاضرات ألقيت على طلبة الماستر سنة أولى، تخصص قانون العقوبات والعلوم الجنائية.
4-يوسفي عبد الهادي، علم الإجرام المعلوماتي، محاضرات مقدمة لسنة ثانية ماستر حقوق، قانون جنائي وعلوم جنائية،2021/2020.

VII. المواقع الإلكترونية

https://www.algeriepolice.dz ساعة الاطلاع 22:15، تاريخ الاطلاع 2022/06/05.

بقلم فطومة حيدر ، الأمن الوطني يسجل 5200 جريمة إلكترونية سنة 2020،ساعة الاطلاع 22:27، تاريخ الاطلاع 2022/06/05،https://www.ennaharonline.com.
https://radioalgerie.dz/news/ar/tags، ساعة الاطلاع 22:32، تاريخ الاطلاع 2022/06/05.

VIII. مراجع أجنبية

- Bologna Jack, RobertK G, Lindquist : Fraud Audttng. And forensic accounting, New tools andtechniques, 1995.
- Drouit pénal de l'informatique les systémes de traitements automatique des données, Commentaire de la loi n°88/18 du 03/01/1988 relative à la fraude informatique, 1988, doct.
- Manacorda (SC)la réglementation du blanchiment de capitaux en droit International du systéme .rev SC criminelle . 2Avr il 1999.

فهرس الموضوعات

الإهداء .....

شكر و تقدير .....

قائمة المختصرات .....

مقدمة *1*

الفصل الأول: الأحكام العامة للجريمة الإلكترونية *5*

المبحث الأول: الإطار المفاهيمي للجريمة الإلكترونية **5**

المطلب الأول: مفهوم الجريمة الإلكترونية 5

الفرع الأول: تعريف الجريمة الإلكترونية 6

الفرع الثاني: الطبيعة القانونية للجريمة الإلكترونية 11

المطلب الثاني: خصائص الجريمة الإلكترونية 11

الفرع الأول: الخصائص المشتركة مع الجرائم الاخرى 11

الفرع الثاني: الخصائص التي تنفرد بها الجريمة الإلكترونية عن الجرائم الأخرى 12

المطلب الثالث: أنواع الجرائم الإلكترونية 14

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي 14

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي 19

الفرع الثالث: أفعال إجرامية أخرى 20

المبحث الثاني: الإطار الموضوعي للجريمة الإلكترونية **21**

المطلب الأول: أركان الجريمة الإلكترونية 21

الفــرع الأول: الركن الشرعي 21

الفرع الثاني: الركن المادي 22

الفرع الثالث: الركن المعنوي 25

المطلب الثاني: محل الجريمة الإلكترونية 26

الفــرع الأول: المعلومات 26

الفرع الثاني: الأجهزة (أجهزة الحاسوب وملحقاتها) 27

الفــرع الثالث: الأشخاص أو الجهات 27

المطلب الثالث: خصوصية مرتكب الجريمة وضحاياها 27

الفرع الأول: من حيث مرتكب الجريمة الإلكترونية 27

الفرع الثاني: من حيث الضحية 35

الفصل الثاني: آليات مكافحة الجريمة الإلكترونية *52*

المبحث الأول: المواجهة الموضوعية للجريمة الإلكترونية **53**

المطلب الأول: الحماية القانونية في النصوص العامة 53

الفرع الأول: الحماية في الدستور الجزائري 54

الفرع الثاني: الحماية في قانون العقوبات الجزائري 54

الفرع الثالث: الحماية في قانون الإجراءات الجزائية 56

المطلب الثاني: الحماية القانونية في النصوص الخاصة 57

الفرع الأول: قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 57

الفرع الثاني: قانون البريد والمواصلات السلكية واللاسلكية 58

الفرع الثالث: قانون التأمينات 58
الفرع الرابع: الحماية في نصوص الملكية الفكرية 59
المبحث الثاني: المواجهة الإجرائية للجريمة الإلكترونية 65
المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية 65
الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 66
الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني 66
المطلب الثاني: مرحلة البحث الأولي 67
الفرع الأول: مفهوم الضبطية القضائية 67
الفرع الثاني: اختصاص الضبطية القضائية 68
الفرع الثالث: صلاحيات الضبطية القضائية 69
المطلب الثالث: التحقيق الابتدائي 71
الفرع الأول: قاضي الحقيق 72
الفرع الثاني: غرفة الاتهام 84
المطلب الثالث: التحـــقيـــق النهائي 85
الفرع الأول: الاختصاص 85
الفرع الثاني: تشكيلة المحكمة 86
الفرع الثالث: إجراءات سير المحاكمة 86
الفرع الرابع: القواعد العامة للمحاكمة 87
خاتمة 104
قائمة المصادر والمراجع 107
***ملخص المذكرة ..... ***

ملخص المذكرة

الجريمة الإلكترونية هي واحدة من معضلات العصر الحديث التي أصبحت واقعا مقلقا للدول والأفراد، فمع انتشار استخدام شبكات المعلوماتية في العالم لقدرة الأفراد على التعامل مع التقنيات المتطورة التي توفرها لتحقيق أهدافهم ومتطلباتهم، ظهرت لنا الجريمة المعلوماتية كرد فعل متوقع للتطور السريع الحاصل في مجال الثورة التكنولوجية والمعلوماتية التي عهدنا أنها تعمل لتغير نمط حياة الأفراد والمجتمعات للأفضل فقط، وقد توصلنا من هذه الدراسة إلى عدم وجود مصطلح قانوني موحد للدلالة على هذه الجريمة، وكذلك هناك اختلاف في تعريفاتها، لهذا كان من الضروري تدخل المشرع الجزائري لتصدي لهذا النوع الخطير من الجرائم، والتي عرفها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وهي تتصف بسمات تجعله مختلف عن المجرم التقليدي، وكذا بالنسبة لمحل الجريمة والذي يختلف كل الاختلاف عن ما هو موجود في الجرائم العادية، كما لها صور متعددة من الجرائم ، يرتكبها كل شخص طبيعي ومعنوي، ولكن رغم اختلاف هذه الجريمة عن الجريمة التقليدية إلا أنها تشترك معها من حيث الأركان التي تقوم بهم وإذا تخلف ركن لا نكون بصدد جريمة.

وبسبب طبيعتها الافتراضية نجد أن المشرع قام بسن نصوص قانونية جديدة تتماشى مع التطور الحاصل في تكنولوجيا المعلومات وذلك لقمع هذه الجريمة والتصدي للاعتداءات التي أصبحت تتزايد مع مرور الزمن على الأنظمة المعلوماتية، حيث أقر بعض الإجراءات والوسائل لمحاربة هذا السلوك المستحدث.

Résumé

La cybercriminalité est l'une des Les crimes les plus graves de ce siècle qui sont devenus Une réalité terrifiante pour les pays et les individus, avec la propagation de L'utilisation d'Internet dans le monde à la capacité de Des particuliers pour faire face aux technologies de pointe fournis pour atteindre leurs objectifs et leurs exigences, La criminalité informatique est apparue comme une réponse Evolution attendue du loyer dans le domaine de La révolution technologique et informationnelle qui Notre promesse est que cela fonctionne pour changer le mode de vie des individus Et les sociétés ne sont que pour le mieux, et nous sommes venus De cette étude à l'absence de terme preuves juridiques unifiées pour ce crime, Il y a aussi une différence dans leurs définitions, pour cette raison L'intervention du législateur était nécessaire algérien pour contrer ce dangereux type de Crimes, qu'il a définis comme le crime de préjugé des systèmes de traitement automatisé de données, qui sont Il a des caractéristiques qui le rendent différent du criminel traditionnel, ainsi que pour la scène du crime Ce qui est complètement différent de ce qui est Il est présent dans les crimes ordinaires, ainsi que ses images Plusieurs crimes commis par chacun La personne physique et morale, mais malgré La différence entre ce crime et le crime traditionnel, mais il partage avec lui en termes de Les piliers que vous faites, et si nous laissons un coin, non Nous sommes sur le point de commettre un crime.

En raison de sa nature hypothétique, nous constatons que Le législateur a édicté de nouveaux textes juridiques En phase avec l'évolution de la technologie.

informations afin de réprimer ce crime Et répondre aux attaques qui se multiplient temps sur les systèmes Informatique, où je procédures distingue certaines Et les moyens de lutter contre ce comportement se sont développés.