وزارة التعليم العالـي والبحث العلمي
جـامعة عباس لغرور – خنشلة "
كلية الحقـوق والعلوم السياسية

قسم الحقوق
نيابة العمادة للدراسات وشؤون الطلبة

التحقيق في الجريمة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر في الحقوق

تخصص: **قانون جنائي وعلوم جنائية**

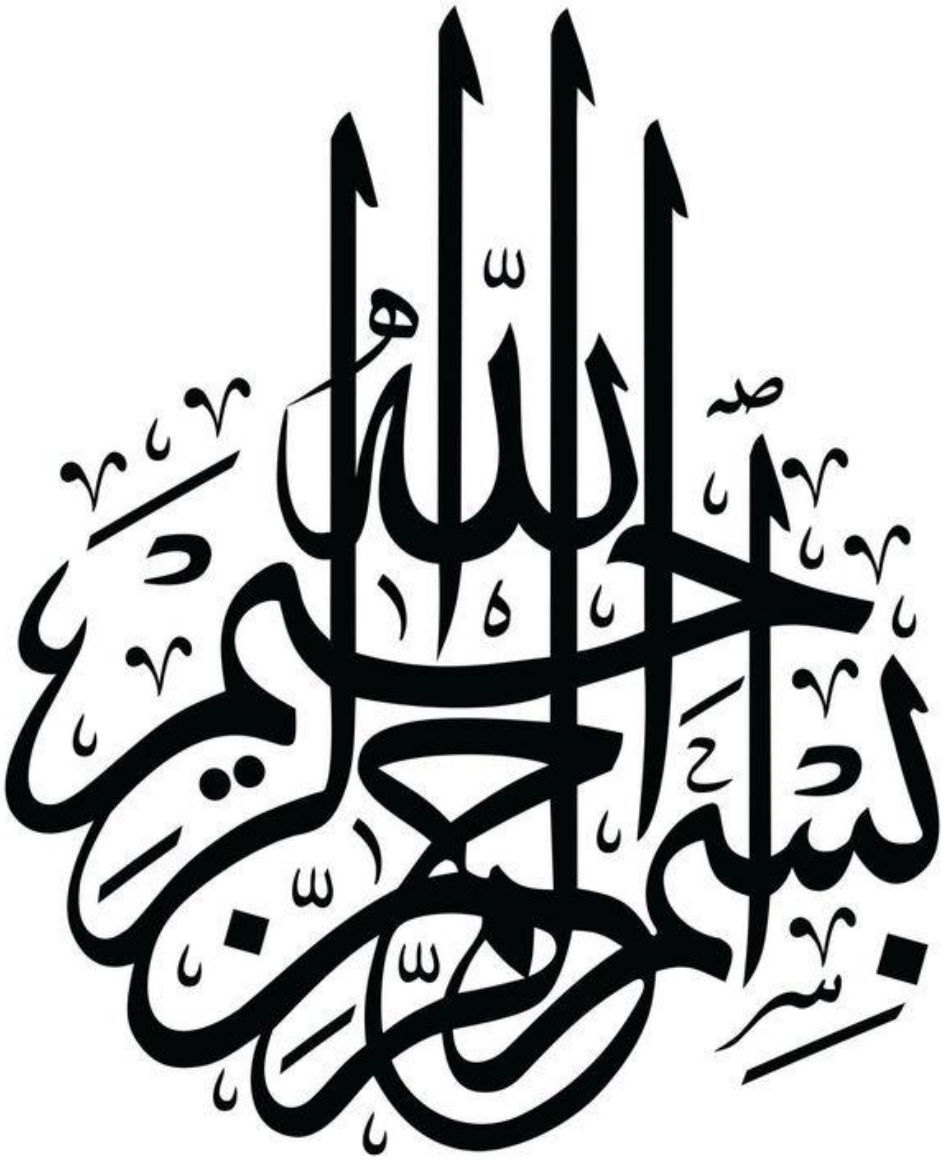
إعداد الطالبة:
✓ **ماجدة مخنان**

إشراف الدكتور:
*** د/ ياسين قوتال**

لجنة المناقشة:

اللقب والإسم	الرتبة العلمية	الجامعة الأصلية	الصفة
د/ محمد عبابسة	أستاذ محاضر أ	جامعة عباس لغرور –خنشلة	رئيسا
د/ قوتال ياسين	أستاذ التعليم العالي	جامعة عباس لغرور – خنشلة	مشرفا ومقررا
د/ كواشي نجوى	أستاذ مساعد أ	جامعة عباس لغرور – خنشلة	عضوا ممتحنا

السنة الجامعية: 2024/2023


بسم الله الرحمن الرحيم

شكر وتقدير

من أين تكون البداية؟ وماذا نقول؟

لمن لولا تفانيهم ما استطعنا أن نضع بين أيديكم هذا العمل المتواضع الذي كان بالأمس القريب مجرد فكرة ليصبح اليوم حقيقة، وواقع ملموسا على أيدي أساتذة ما كنا لنصل لولا جهودهم أبدا.

من الإشراف الحازم والجدية في العمل بفضلهم تعلمنا معنى البحث والاعتماد على النفس إيجاد الحلول لما أن يوجهنا فأينما وجد اشكال فالمؤكد أن الحل بين طياته.

إلى أستاذنا المشرف" قوتال ياسين" الذي لم يختلف يوما عن البساطة والتواضع في كل ما قدمه لي من أول حرف لآخر نقطة، ادونها لتكون بذلك مثالا للفكر الراقي في صورة ولا أروع منها.

إهداء

الحمد لله عند البدء وعند الختام، فما تناهى درب، ولا ختم جهد، ولا تم سعي إلا بفضله.

لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون، لم يكن الحلم قريبا لكنني نلتها .....

أهدي وبكل حب بحث تخرجي:

إلى التي كانت لي نورا في عتمتي وكان دعائها سر نجاحها أمي

إلى روح والدي الغالي رحمه الله الذي دعمني بلا حدود وأعطاني بلا مقابل

إلى تلك المرأة العظيمة التي شجعتني للوصول إلى طموحاتي إلى إخوتي وأخواتي

الطالبة ماجدة

قائمة المختصرات

المصطلح	الإختصار
قانون العقوبات	ق ع
قانون الاجراءات الجزائية	ق ا ج
الجريدة الرسمية	ج.ر
السنة	س
العدد	ع
الجزء	ج
الطبعة	ط
دون سنة نشر	د ن
دون طبعة	د ط
الصفحة	ص

مقدمة

نعيش اليوم في عصر الثورة المعلوماتية التي أحدثت تغييرات جذرية في طريقة تعاملنا مع المعلومات وتسهيل العمليات اليومية في مختلف المجالات، بفضل الإنترنت التي حولت العالم إلى قرية صغيرة بسرعتها الفائقة في تبادل البيانات.

هذه التطورات هي نتاج التكامل المذهل بين قطاعي تكنولوجيا المعلومات والاتصالات، وقد أسهمت في نشأة ما يُعرف اليوم بالثورة المعلوماتية، التي تمثل نقلة علمية وتكنولوجية هامة، حتى أصبح هذا الزمان يُعرف بعصر المعلومات، حيث كانت هذه الأخيرة دومًا من أثمن ما يمتلكه الإنسان، حيث سعى لجمعها وتوثيقها بدءًا من جدران المعابد والمقابر وصولًا إلى الأقراص الممغنطة الحديثة.

ورغم الفوائد الكبيرة التي جلبتها هذه التقنيات، مثل تحسين المستوى المعرفي والاقتصادي لشعوب العالم، إلا أنها جاءت مع عيوب جوهرية استفاق العالم على خطورتها وأصبح تأثيرها ملموسًا ومحسوسًا، ومن هذه العيوب إساءة استخدام الإنترنت والحواسيب، مما فتح الباب للمجرمين ذوي النوايا الخبيثة لاستغلال هذه التقنيات لتحقيق أغراضهم الإجرامية.

من هذا المنطلق، نشأت أنواع جديدة من الجرائم تختلف عن الجرائم التقليدية بخطورتها الكبيرة، نظرًا لطبيعتها الخاصة التي تتميز بصعوبة إثباتها سواء من حيث طرق ارتكابها أو هوية مرتكبيها قبل ذلك، و تبرز مشكلة أمن المعلومات كمهمة صعبة في عالم الجرائم المعلوماتية التي لا تعترف بالحدود الجغرافية أو الوطنية، ويتحرك مرتكبوها في عالم افتراضي.

لذا، أصبح تطوير أمن المعلومات ضروريًا ومحور قلق دائم للخبراء القانونيين، إن التصدي لأولى بوادر هذه المشاكل يعد أمرًا ضروريًا لمنع تفاقمها، خاصة مع النمو المتسارع في استخدام التكنولوجيا الذي تشهده الدول العربية، بما في ذلك الجزائر.

تتسارع الحاجة لمواجهة التحديات التي تجلبها العولمة والاعتماد التكنولوجي، مما يخلق بيئة مواتية لاختراق البيانات الشخصية والتأثير على الأمن القومي والسيادة الوطنية لهذه الدول.

أهمية الموضوع:

أصبحت الجرائم الإلكترونية من أكثر التحديات التي تواجه المجتمعات الحديثة نظرا لانتشار استخدام التقنيات الرقمية في جميع جوانب الحياة، ويكتسب التحقيق في هذا النوع من الجرائم أهمية كبيرة سيتم تقسيمها على النحو التالي:

الأهمية العلمية:

تتجلى الأهمية العلمية فيما يلي:

- ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق ونحن لا نزال في في بداية عصر الانفجار المعلوماتي، يعني توقع ظهور المزيد والمزيد من هذه الأنماط الجديدة التي يستوجب معها تحديث الأنظمة والتعليمات والجهات الامنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو مادعى إلى تطوير أسلوب التحقيق والتفتيش فيها.
- وأيضا في أن الجرائم الإلكترونية تتميز بصفات تجعلها صعبة الإثبات لعدم وجود الآثار المادية التقليدية مثل بقع الدم والبصمات، مما يؤدي إلى ضرورة البحث عن أدلة أخرى لإثباتها، ودون أدنى شك فإن مسألة الحصول على هذه الأدلة يتطلب منظومة قانونية وقضائية فعالة تتولى مسألة التحقيق في هذا النوع من الجزائم.

الأهمية العملية:

تكمن الأهمية العملية فيما يلي:

- تتضح الأهمية في كيفية تعامل جهات التحقيق مع هذه الجريمة لاستخلاص الدليل الرقمي.
- وأيضا أن التحقيق في الجرائم الرقمية يتم في وقت معاصر لوقوع الجريمة أو إثر ذلك مباشرة ما يتيح فرصة التنقيب وجمع أدلتها ذات الطابع الخاص في الوقت الملائم وأي تأخير قد يؤدي إلى العبث بها وإفسادها مما يفقدها قيمتها في الإثبات.
- كما أن هناك من الإجراءات العامة أو الخاصة ما تفرض طبيعته ضرورة مباشرته في أقرب وقت من وقوع الجريمة على اعتبار أن هذا النوع من الجرائم يقوم في بيئة إفتراضية
- تقييم مدى كفاءة النصوص القانونية الحالية في مكافحة الجرائم الإلكترونية والتقليل من حدوثها.
- عتبر تطوير مقترحات قانونية وعلمية لملء الفجوات التي يستغلها المجرمون بسبب عدم شمولية القوانين الراهنة لكافة أفعالهم.
- كما يجب الأخذ بعين الاعتبار استراتيجيات وحلول تشريعية ضمن إطار القانون الجزائري لمواجهة هذه الظاهرة بفعالية وقانونية.

أهداف الموضوع:

إن موضوع التحقيق الجنائي في الجرائم الالكترونية بات من المواضيع المستحدثة التي شكلت العديد من الإطلاعات للمشرع الجزائري من اجل مواكبة تطور الجريمة الالكترونية، وذلك من خلال سن نصوص قانوني تتماشى وتطور هذا النوع من الجرائم ومن أجل دراسة هذا الموضوع وجب علينا تسطير جملة من الأهداف العامة وكذا الأهداف الخاصة والتي تتمثل فيما يلي:

أهداف عامة:

- تطوير أساليب وآليات لكشف وجمع الأدلة الرقمية المتعلقة بالجرائم الإلكترونية بطريقة قانونية وموثوقة.
- تحليل الأدلة الرقمية بشكل علمي وفقا لمعايير مقبولة لاستخراج المعلومات ذات الصلة لغرض الإدانة أو البراءة.
- تطوير إطار تشريعي وقانوني شامل لمعالجة الجرائم الإلكترونية بما يضمن حماية الحقوق الأساسية للأفراد والمؤسسات.

أهداف خاصة:

- بيان ماهية الجريمة الالكترونية والكشف عن أهم خصائصها وكذا تسليط الضوء على مدى نجاعة النصوص القانونية في التعامل مع الجرائم الإلكترونية ومدى تجاوب المواجهة الأمنية معها.
- تجسيد واقع هذه الجرائم وملاحقتها والتعرف على التشريعات التي تنظم تجريم ومتابعة الجرائم الإلكترونية
- إبراز طرق التحقيق في الجرائم الإلكترونية، ذلك لأن اجراءات التحقيق فيها تختلف عن الجرائم التقليدية، وكذا جهود المشرع الجزائري في التصدي للانتهاكات والاختراقات الواقعة في مجال الأنظمة المعلوماتية.

إشكالية الموضوع:

يعد التحقيق في الجرائم الإلكترونية أحد الأنشطة القانونية المتعلقة بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الإستدلالات التي يتطلبها التحقيق، حيث أن الجرائم الإلكترونية عكس العادية من حيث عدم تركها لدليل خارجي فهي تتميز بالسرعة الفائقة في

ارتكابها، فتحدث عبر نبضات إلكترونية، مما يصعب التخطيط لمواجهاتها، ليبقي الإشكال الرئيس حول:

ما مدى كفاية وفعالية النصوص القانونية الحالية في مواجهة الجريمة الإلكترونية وردع مرتكبيها؟

وتندرج ضمن هذه الإشكالية مجموعة من الأسئلة الفرعية يمكن حصرها كالتالي:

- ما المقصود بالجريمة الإلكترونية؟ وفيما تتمثل الآليات المتخذة لمواجهة الجريمة الإلكترونية؟
- فيما تتمثل الآليات والإجراءات المستحدثة للتحقيق ومكافحة الجريمة الالكترونية ؟
- هل وفق المشرع الجزائري في تفعيل آليات التحقيق في الجرائم الالكترونية وكيف تم تطبيقها؟

أسباب اختيار الموضوع:

تبرز من وراء اختيارنا لهذا الموضوع جملة من الأسباب، منها ماهو ذاتي ومنها ما هو موضوعي:

1-الأسباب الذاتية:

- الرغبة القوية في فهم الجرائم الإلكترونية بعمق، والاهتمام بتقنيات الإنترنت.
- الرغبة في تعزيز المهارات القانونية والتقنية من خلال دراسة مفصلة للجرائم الإلكترونية وكيفية التحقيق فيها.

2-الأسباب الموضوعية:

- الجريمة الإلكترونية أصبحت مشكلة عالمية تؤثر على ملايين الأفراد والشركات عبر العالم، مما يجعل فهم آليات التحقيق فيها ضروريًا.

- تحديث المعرفة ذلك كون الجريمة الإلكترونية مجال ديناميكي ومتطور بسرعة، ودراسته يضمن مواكبة التطورات التكنولوجية والقانونية الحديثة.

المنهج المعتمد في الموضوع:

اعتمدنا على إحدى أدوات المنهج منها المنهج الوصفي الذي انتهجناه في توضيح وتبييت تعريف شامل الجرائم الإلكترونية وخصائصها الجوهرية التي تميزها عن بقية الجرائم لكونها من السلوكات الإجرامية الحديثة والمعاصرة ، إضافة إلى ذلك استخدمنا أداة التحليل وذلك من خلالا من خلال تحليل وإستقراء مختلف النصوص التشريعية والمواد القانونية التي تناولت الجرائم الالكترونية، وكذا تحليل بعض المفاهيم لتحديد هذا النوع من الجرائم، وإجراءات التحقيق فيها.

الدراسات السابقة:

في إطار اطلاعنا على الدراسات القانونية أو الأكاديمية أو المقالات التي تعرضت للموضوع بشكل دقيق، نذكر منها:

رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، 2012/2011، حيث جاءت هذه الدراسة الأكاديمية تحت إشكاليات مختلفة تتمثل في:* هل الأنماط الإجرائية المستحدثة تختلف عن نماط الجريمة التقليدية؟، وهل للمجرم الالكتروني خصائص تميزه عن باقي المجرمين التقليديين؟، وعلى أي أساس تحظى المعلومة بالحماية؟ وهل نصوص قانون العقوبات السارية كافية لمواجهة هذه الأفعال الإجرامية وهل توفر الحماية القانونية لها؟.

حيث توصلت فيها الطالبة إلى مجموعة من النتائج وهي: غياب مفهم عام متفق عليه بين الدول حول التعريف القانوني للنشاط الإجرامي المتعلق بالجريمة الالكترونية، والأنماط

المكونة لها، وعدم كفاءة وملائمة النصوص التقليدية مع جرائم اختراق نظم الكومبيوتر لأنها عادة ما تكون متعلقة بوقائع مادية خاصة بالجرائم الالكترونية وبالنتيجة فهي لا تتلاءم مع الوقائع التي تتميز بها الجريمة المعلوماتية.

إضافة إلى إنها ذكرت مجموعة من المقترحات وهي: إلقاء الضوء على موقف المشرع الجزائري الذي اتخذ لمواجهة هذا الشكل الجديد من الإجرام الحديث فالملاحظ أن مشرعنا قد استدرك مؤخرا الفراغ القانوني الملحوظ في الجرائم المعلوماتية وقد اعتمد في ذلك حلا يضمن حماية مزدوجة للحاسب الآلي من خلال نصوص حق المؤلف ومن خلال نصوص خاصة ادمجها من خلال قانون العقوبات، وكذا استحداث نص خاص بالاعتداء على سير نظام المعالجة الآلية للمعطيات، و حماية البرامج والمعلومات المعالجة بصفة مستقلة عن طريق معالجة الاستيلاء عليها دون المساس بسلامتها أو أصالتها.

صعوبات الدراسة:

كأي بحث وكأي دراسة لا بد من أن تعرقلها مجموعة من الصعوبات حيث تعرضنا من خلال بحثنا إلى بعض الصعوبات لكنها لم تحد من عزيمتنا ولعل من بين هذه هي الصعوبات، هي حداثة موضوع الجرائم الإلكترونية الذي لا يزال في أولى مراحله وعدم كفاية النصوص القانونية المعالجة له، كذلك قلة المراجع المتخصصة وكذا الأبحاث في هذا الموضوع خاصة في الجزائر.

خطة الموضوع:

على ضوء الإشكالية المطروحة يمكن دراسة هذا الموضوع وفق خطة ثنائية يتم من خلالها تقسيم الموضوع إلى فصلين، بحيث خصصنا الفصل الأول إلى: ماهية الجريمة الإلكترونيةوالذي قسم بدوره إلى مبحثين: يتناول المبحث الأول: مفهوم الجريمة الإلكترونية، بينما المبحث الثاني تحت عنوان:التكييف القانوني للجريمة الإلكترونية وأركانها،أما بالنسبة

للفصل الثاني تم تخصيصه مبحثين، المبحث الأول ماهية التحقيق الالكتروني الجنائي، أما المبحث الثاني بعنوان الآليات المستحدثة للتحقيق في الجرائم الالكترونية.

ونختتم هذه الدراسة بخاتمة تحتوي على مجموعة من النتائج التي تم التوصل إليها بالإضافة إلى مجموعة من التوصيات.

الفصل الأول

الفصل الأول: ماهية الجريمة الإلكترونية

تنوعت أشكال السلوك السلبي بشكل ملحوظ وتطورت بشكل مستمر، مأخوذة على أشكال لا حصر لها بناءً على التكنولوجيا والأدوات المتاحة للفرد، مما يمكنه من تنفيذ أفعاله بكل سهولة وفعالية في العالم الواقعي.

مع ظهور تقنيات نظم المعلومات والاتصالات، تبلورت أشكال جديدة من السلوكيات السلبية الخطيرة، حيث وفرت هذه التقنيات للمختلسين وسائل جديدة ومتطورة لارتكاب جرائمهم بكل يسر وسهولة، هذه السلوكيات الحديثة تسببت في ثورة كبيرة في الفهم العام للجريمة وتفاوت مستوياتها.

وتعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية التي تختلف كثيرا عن الجريمة التقليدية في طبيعتها وأنواعها وأدواتها ولذلك لابد من توضيح ماهيتها من خلال:

المبحث الأول: مفهوم الجريمة الإلكترونية

المبحث الثاني: التكييف القانوني للجريمة الإلكترونية وأركانها

المبحث الأول: مفهوم الجريمة الإلكترونية

تعد الجريمة الإلكترونية، آفة العصر، والأخطبوط الذي أنتجته الحضارة التقنية والثورة التكنولوجية، الذي تمتد أذرعه في جميع أنحاء العالم، ولم تفلت من قبضته لا الدولة الضعيفة ولا المتطورة.

وعليه من خلال هذا المبحث سوف نحاول تحديد التعاريف المختلفة للجريمة الالكترونية، وكذا الخصائص التي تمتاز بها عن غيرها، وذلك من خلال: تعريف الجريمة الإلكترونية في **المطلب الأول**، ثم خصائص والتطور التاريخي للجريمة الالكترونية في **المطلب الثاني**.

المطلب الأول: تعريف الجريمة الإلكترونية

نتيجة للتطور المذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الأنترنت فالانتشار الواسع والسريع هلا أدى إلى ظهور أشكال وأنماط جديدة من الجرائم لاسيما المتعلقة منها بشبكة الأنترنت، والتي باتت تشكل خطر ليس على سرية النظم الحاسوبية أو سلامته فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة،[1] كما لم يتم الإجماع على تعريف عام وموحد للجريمة الإلكترونية كما تجنب غالبية المشرعين الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات وأوكلوا مهمة ذلك إلى الفقه والقضاء.

قد تعددت واختلفت التعاريف بشأن الجريمة الإلكترونية باعتبارها ظاهرة جديدة مازالت قيد البحث والدراسة من طرف القانونين كالعديد من الفقهاء، وبالمثل لا يوجد تعريف متفق عليه لهذا النوع من الجرائم.[2]

1 عادل عبد العالي إبراهيم خراشي: إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلبِ عليها، دار الجامعة الجديدة، الإسكندرية، س 2015، ص 07.

[2] غنية بالطي: الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، س 2015، ص 15-16.

للوقوف على مفهوم الجريمة الإلكترونية قسمنا هذا المطلب إلى فرعين، ففي الفرع الأول سنتطرق لدراسة التعريف اللغوي للجريمة الإلكترونية، ثم تعريفها الاصطلاحي في الفرع الثاني.

الفرع الأول: تعريف الجريمة الإلكترونية لغة

الجريمة لغة كلمة مشتقة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقا للمفهوم الاجتماعي كل سلوك إرادي غير مشروع يصدر عن شخص مسؤول جنائيا في غير حالات الإباحة عدوانا على مال أو مصلحة أو حق محمي بجزاء جنائي.[1]

الإلكترونية: نسبة لكلمة "إلكترون" وهي جسيم متناهي الصغر موجود في الذرة، ويقصد بها هنا ما يتعلق بالتقنيات والأجهزة الكهربائية والرقمية الحديثة.

لذلك فإن مصطلح "الجريمة الإلكترونية" يشير لغويا إلى الأفعال أو الأنشطة غير المشروعة أو المحرمة قانونا والتي ترتكب باستخدام الوسائل والتقنيات الإلكترونية والرقمية الحديثة، كالحواسيب والشبكات والبرامج وأجهزة الاتصالات وغيرها، فهي تجمع بين "الجريمة" بوصفها فعلا محظورا ومخالفا للقانون، ومفهوم "الإلكترونية" الذي يشير إلى استخدام التقنيات الرقمية الحديثة في ارتكاب هذه الجريمة أو تسهيليها.[2]

لذلك، فإن التعريف اللغوي للجريمة الإلكترونية ينصب على كونها جريمة أو فعلا إجراميا يتم ارتكابه باستغلال التقنيات الإلكترونية والرقمية المتطورة.

---

1 هبة نبيلة هروال: جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013 ، ص 12.

[2]ذياب موسي، الجرائم الإلكترونية: المفهوم والأسباب، الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتجية، عمان، المملكة الأردنية الهاشمية، 2014، ص 3.

تعتبر الجريمة الالكترونية بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة، يقرر له القانون عقوبة أو تدبَيرا احًترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غَير المشروع لشبكة الأنترنت على المعلومة بشكل رئيسي،[1] وهذا الذي أدى إلى اطلاق مصطلح الجريمة الإلكترونية على هذا النوع من الجرائم.

الفرع الثاني: تعريف الجريمة الإلكترونية إصطلاحا

أولا: التعريف الفقهي للجريمة الالكترونية

هناك اتجاهان من الفقه في تعريف الجريمة الالكترونية اتجاه ضيق واتجاه واسع وعليه سوف نتطرق لكل منهما على النحو التالي:

أ: الاتجاه الضيق لتعريف الجريمة الالكترونية

عرف الفقيه André Lucas الجريمة الإلكترونية بأنها: " أي سلوك غير مشروع يرتكب عن طريق استخدام تقنيات المعلومات والاتصالات، سواء كان ذلك الهدف الرئيسي أو الوسيلة المستخدمة في ارتكاب الجريمة".

يغطي التعريف جميع أنواع الجرائم التي يمكن أن ترتكب باستخدام التكنولوجيا، سواء كانت الجريمة ذاتها تحدث عبر الإنترنت، أو تستخدم التكنولوجيا كوسيلة لتنفيذ جريمة تقليدية (مثل استخدام الإنترنت لتنسيق نشاط إجرامي).

كما انتقد هذا التعريف بأنه يفتقر إلى أمثلة محددة لأنواع الجرائم الإلكترونية، مما يمكن أن يحدث لبسا في فهمه وتطبيقه.

---

1 **يوسف صغير: الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، س 2013 ، ص 7.**

كما تم تعريفها من قبل الفقيه Yvonne Hassler بأنها: أي نشاط إجرامي يستخدم فيه الجاني التقنيات الرقمية لارتكاب جريمة تقليدية أو جريمة جديدة ناتجة عن استخدام هذه التقنيات".[1]

وتم نقد هذا التعريف بأنه لم يقدم ولم يحدد أنواع الجرائم التقليدية التي يمكن أن تتحول إلى جرائم إلكترونية، مما قد يؤدي إلى غموض في الفهم والتطبيق.

ب: التعريف الواسع للجريمة الالكترونية

يرى الخبير الأمريكي Parker مفهوما واسعا للجريمة المعلوماتية والمتمثل في كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، وينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.[2]

كما يعرف الأستاذ Vivant و Hestonc الجريمة الإلكترونية بأنها مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب.[3]

وعرفها الفقيه Ball .D. Leslie بأنها فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية.[4]

جرائم الكمبيوتر هو مصطلح شامل يتضمن جميع الجرائم التي يُستخدم فيها الكمبيوتر، سواء كأداة للجريمة أو كهدف لها، إذ يشمل هذا المصطلح الجرائم المعلوماتية وجرائم

---

[1] سامي على حامد عياد :الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، س 2008، ص ص 38،40.

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

[3] محمد العريان: الجرائم المعلوماتية، كلية الحقوق، جامعة الإسكندرية، دار الجامعة الجديدة للنشر، الإسكندرية، س2004 ، ص43.

4 عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، س 2006، ص 02.

الإنترنت، بالإضافة إلى الاعتداءات على الشبكات المحلية الخاصة بالهيئات والمنشآت الخاصة والعامة.

وجاء في تعريف آخر أن الجريمة الإلكترونية هي ببساطة استخدام التقنيات الرقمية لإخافة الآخرين.[1]

ثانيا: التعريف التشريعي للجريمة الالكترونية

بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، وعرفها بموجب أحكام المادة 02 من القانون 04/09 على أنها " جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية". [2]

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الألية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 07، وترك المجال واسع لأي جريمة اخرى ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية.[3]

---

[1] شهرزاد بولحية: تحديات الجريمة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدارسات القانونية والسياسية – المجلد 04 – العدد 02 – السنة 2019 ، ص 1979.

[2] القانون رقم 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج ر ، ع47.

[3] القانون رقم 04 – 15 ، الصادر في 10 نوفمبر 2004 ، معدل و متمم للأمر رقم 156/66 ، الصادر في جوان 1966 ، المتضمن ق. ع، ج ر العدد 71.

و حسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية مما يجعل هذا التعريف يشمل عدد كبير من الجرائم كما أن التعريف تضمن تكرار[1]، كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية.

ثالثا: التعريف القضائي للجريمة الإلكترونية

لا يوجد تعريف موحد ومتفق عليع من قبل القضاة لمفهوم "الجريمة الإلكترونية"، حيث يختلف التعريف من دولة إلى لأخرى وفقا للتشريعات والقوانين الوطنية المعمول بها، وكذلك بالنسبة للجزائر فإنها لم تضع تعريف محددا للجريمة الإلكترونية أو المعلوماتية من قبل القضاة بشكل مباشر، ولكن يتم الاعتماد على التعريف الوارد في القانون رقم 09-04 المذكور أعلاه، وبناء على التعريف الموجود في نص المادة الثانية، يستند القضاة في الجزائر على عدة عناصر لتكييف الجريمة على أنها جريمة إلكترونية، منها.[2]

- استخدام وسائل تكنولوجيا المعلومات والاتصال.
- استهداف أنظمة معالجة البيانات الآلية أو المعطيات الإلكترونية.
- أن يكون الفعل المرتكب يشكل جناية أو جنحة وفقا للقوانين الجزائرية.

المطلب الثاني: خصائص وتطور الجريمة الإلكترونية

إن تحديد مسار الحياة وصنع القرارات الصحيحة يمثلان جزءًا أساسيًا من رحلة الإنسان نحو تحقيق أهدافه وتحقيق رغباته، وهناك حاجة دائمة للمعرفة والمعلومات لاتخاذ قرارات مدروسة ومناسبة في عالمنا المعاصر، حيث تزداد التكنولوجيا تطورًا، يصبح تجميع

[1] سفيان سوير: جرائم المعلوماتية ، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية و علم الإجرام ، جامعة أبو بكر بلقايد، تلمسان ، س 2010- 2011 ، ص 14-16

[2] ابراهيم بلبالي، الجريمة الإلكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، مجلة الأستاذ الباحث، جامعة أدرار، المجلد 16، 2020، ص 135.

المعلومات وتحليلها أمرًا أكثر أهمية من أي وقت مضى وعليه فالجريمة الإلكترونية تمثل تطورًا تاريخيًا في مفهوم الجريمة، حيث تتميز بعدة خصائص تميزها عن الجرائم التقليدية.

وهنا اشارة لأهمية تحديد مسار الحياة واتخاذ قرارات مدروسة لتحقيق الأهداف الشخصية، خصوصًا في زمن يشهد تسارعًا في التطور التكنولوجي، الأمر الذي يجعل الوصول إلى المعلومات ضروريًا لاتخاذ قرارات مستنيرة، كما تلقي الفقرة الضوء على كيفية تأثير التكنولوجيا في تطوير أشكال الجريمة، مما أدى إلى ظهور الجريمة الإلكترونية التي تتميز بأساليب وتأثيرات مختلفة عن الجرائم التقليدية.

وعليه في هذا المطلب سنقوم بدراسة الخصائص المميزة للجريمة الالكترونية في الفرع الأول، ثم مراحل تطورها في الفرع الثاني.

الفرع الأول: خصائص الجريمة الإلكترونية

تتسم الجريمة الإلكترونية بجملة من الصفات أو الخصائص نبينها على النحو الآتي:

اولا/ جريمة عابرة للحدود

إحدى أبرز سمات الجريمة الإلكترونية هي تجاوزها للحدود الجغرافية نتيجة ارتباطها بعالم الإنترنت وتقنية المعلومات، يمكن أن تتأثر العديد من الدول بهذه الجريمة في نفس الوقت نظراً للسرعة الفائقة في تنفيذها، فقد تُرتكب الجريمة في دولة واحدة من قبل الجاني بينما يكون الضحية في دولة أخرى، وكل ذلك يحدث في وقت قصير جداً.[1]

هذا النوع من الجرائم يتجاهل الحدود الجغرافية بين الدول والقارات، بفضل انتشار شبكة الاتصالات العالمية، أصبحت أعداد هائلة من أجهزة الكمبيوتر مرتبطة ببعضها عبر مختلف دول العالم، يمكن أن يكون الجاني في بلد والضحية في بلد آخر، مما يمنح الجريمة

[1] نهلا عبد القادر المومني: المرجع السابق، ص 50.

الإلكترونية طابعاً دولياً، الطبيعة العالمية للإنترنت تعني أن معظم دول العالم متصلة بشكل دائم، مما يسهل ارتكاب الجرائم عبر الحدود، لذلك تعتبر الجرائم الإلكترونية شكلاً جديداً من الجرائم العابرة للحدود الإقليمية.[1]

ثانيا/ صعوبة اكتشاف وإثبات الجرائم الإلكترونية

تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف والإثبات وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز و الأرقام، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة وغالبا ما يتم معاقبة مجرمين وذلك لعدم وجود أدلة قائمة في حقه.[2]

وصعوبة اكتشاف وإثبات الجرائم المعلوماتية راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات.[3]

كما تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي من بصمات، تخريب، شواهد مادية وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة.[4]

---

[1] خالد ممدوح ابراهيم: الجرائم المعلوماتية، ط2 ، دار الفكر الجامعي الإسكندرية، مصر، س2019 ، ص 77.

[2] عبد اللطيف معتوق: الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير، س 2011- 2012، ص 24.

[3] شهرزاد بولحية: المرجع السابق، ص 1988.

4 إسمهان بوضياف: الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 11، جامعة محمد بوضياف، المسيلة، س 2018، ص 356.

وعليه في جرائم المعلوماتية، يكون من الصعب العثور على أدلة مادية للجريمة بسبب استخدام الجاني وسائل تقنية وفنية معقدة في كثير من الأحيان، هذا السلوك الرقمي في ارتكاب الجريمة لا يستغرق سوى ثوانٍ معدودة، يتم خلالها محو الأدلة والتلاعب بها.

ثالثا/ جريمة مستحدثة

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطار جسيمة في ظل العولمة، فال غرابة أن تعتبر الجرائم الإلكترونية من الجرائم المستحدثة حيث أن التقدم التكنولوجي الذي تحقق خال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته و إمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها.[1]

الفرع الثاني: تطور الجريمة الإلكترونية

مرت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ولهذا مرت بمراحل سوف نوجزها على النحو التالي:

أولا/ مرحلة الخمسينيات والستنيات: تعد بداية صناعة الحواسيب وانطلاق ثورة تكنولوجيا المعلومات الإلكترونية مستقلة عن وسائل الاتصال التي وقعت بأربعينيات القرن الماضي وعليه يعد تاريخ ظهور الجرائم الإلكترونية حديثا نسبيا، حيث ارتبط ظهورها التاريخي مع ظهور الكمبيوتر وانتشار استعماله والذي كان عام 1954 في الولايات المتحدة الأمريكية، حيث بدأ طرح أول جهاز كمبيوتر للشراء وبدأ الاستخدام التجاري للحواسيب في الخمسينيات ومنذ ذلك الوقت بدأت ظاهرة جرائم الحاسوب في الظهور، ولكن كانت بدايتها تقتصر على

[1] **ابتسام بوبعابية: التحقيق في الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون الاعلام الآلي والأنترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر س 2022/2021، ص 18**

إساءة استخدام الحاسوب على البعد الأخلاقي، حيث تم تسجيل أول جرمية إلكترونية في الولايات المتحدة الأمريكية عام 1957، [1]وبعدها صدرت عدة تقارير تبني نسب ورصد حالات إساءة استخدام الحاسوب وصنفت هذه الجرمية إلى جرائم العبث والتخريب وسرقة المعلومات أو الاحتلال والاستخدام غير المصرح به، وفي هذا الوقت كان هناك عدم التمييز بين الجرائم التي تستهدف مادية الحاسوب أو التي تستهدف معطيات الحاسوب بسبب أن الأنشطة الإجرامية المتعلقة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني، أما من حيث التكييف القانوني للجرمية الإلكترونية كانت تتعامل معها بذات الدلالة التي تتعامل معها مع الجرائم التقليدية، من شيوع استخدام الحواسيب في الستينات على السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر ام ظاهرة إجرامية مستحدثة،[2] وان الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة[3].

ثانيا/ مرحلة الثمانينات ومرحلة التسعينيات: في هذه المرحلة ظهر مفهوم جديد لجرائم الكمبيوتر والأنترنت يرتبط بعمليات اقتحام نظم الكمبيوتر عن بعد كما ظهرت أنشطة الفيروسات الإلكترونية التي تقوم بتدمير الملفات والبرامج، وشاع مصطلح الهاكرز المعبر

---

[1] عفاف بعون ، نسيمة أولاد سالم: الجريمة الإلكترونية – قراءة سوسيوتارخية في النشأة والآثار، مجلة القبس للدراسات النفسية والاجتماعية، المجلد05 ، جامعة قاصدي مرباح، ع 20، س 2023، ص72.

2 عبد الفتاح مراد: دور الكمبيوتر في مجال ارتكاب الجرائم الإلكترونية ، شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية ، ص42-43

[3] المرجع نفسه، ص43.

عن مقتحمي نظام الكمبيوتر، كما شهدت التسعينات تنامياً هائلاً في حقل الجرائم الإلكترونية، وتغيّراً في نطاقها ومفهومهاً، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة، واقتحام شبكة المعلومات، وظهرت أنماط جديدة،[1] تقوم على فكرة تعطيل نظام تقني، ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامّة، التي يتسبّب انقطاعها عن الخدمة لساعات، في خسائر مالية بالملايين.. ونشطت جرائم نشر (الفيروسات) عبر المواقع الالكترونية، لما تسهّله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت الرسائل المنشورة على الانترنت، أو المراسلة بالبريد الإلكتروني، المنطوية على إثارة الأحقاد، أو المروّجة للمواد غير القانونية، أو غير المشروعة.[2]

ورغم تزايد الأبحاث، ومحاولات ابتكار أنظمة تكفل لأيّ كمبيوتر الحماية اللازمة، إلاّ أنه في المقابل يتمّ تطوير الإجراءات المضادة لهذه الحصون الأمنية، ومعنى ذلك أن خطر انتهاك أمن وسلامة الكمبيوتر، والجرائم المرتبطة به، سيظل قائماً ومستمراً مدى استمرارية التطور التكنولوجي.[3]

المبحث الثاني: التكييف القانوني للجريمة الإلكترونية وأركانها

تناول الجريمة الإلكترونية، في سياق التكييف القانوني، مجموعة من الأفعال غير القانونية التي تُرتكب باستخدام تقنيات الحاسوب والإنترنت، يهدف التكييف القانوني للجريمة الإلكترونية إلى تعريف الأفعال غير المشروعة في العالم الرقمي وتحديد العقوبات المناسبة لها.

[1] عبد الفتاح مراد، المرجع السابق، ص 43.

[2] المرجع نفسه، ص 43-44.

[3] المرجع نفسه، ص 43-44.

بمعنى أن التكييف القانوني للجريمة الإلكترونية يتعامل مع تحديد وتصنيف الأفعال غير القانونية التي تُرتكب باستخدام التكنولوجيا مثل الحواسيب والإنترنت، ويهدف إلى توضيح العقوبات المناسبة لهذه الأفعال في السياق الرقمي.

وعليه سوف نتطرق في هذا المبحث لدراسة التكييف القانوني للجرائم الالكترونية في المطلب الأول، ثم أركان الجريمة الالكترونية في المطلب الثاني.

المطلب الأول: التكييف القانوني للجريمة الإلكترونية

تصنف الجريمة بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية،[1] على خلاف هذه الجريمة، فإن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، و آخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه،[2] أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها ، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات.

تبنى المشرع الجزائري جهوداً مبادرة في مكافحة الجرائم الإلكترونية اعتبارًا من عام 2004، حيث أدرج في قانون العقوبات، بالفصل الثالث القسم السابع المتعلق بالجرائم الجنائية والمخالفات، قسمًا خاصًا بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وذلك

[1] أحسن بوسقيعة: الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، 2002 ، ط01 ، ص 24.

[2] رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، س2011 -2012، ص 69 .

ضمن القانون رقم 04-05 الصادر في 10 نوفمبر 2004، ومن خلال هذه التشريعات، تناول المشرع الجزائري مجموعة من الجرائم الإلكترونية في مختلف النصوص القانونية.

الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص لجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار وسوف نتطرق لكل منها على النحو التالي:

أولا/ الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية

تقع هذه الجرائم على الأشخاص و تنقسم بدورها إلى طائفتين بحسب نوع الحقوق المعتدى عليها و دور النظام المعلوماتي في اقترافها.

1- الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية

يمكن أن يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية، فعلى سبيل المثال، يمكن أن يتم السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، مما يعد اعتداءً على الحق المعنوي لصاحب المعلومة، بالإضافة إلى ذلك يعتبر هذا انتهاكاً لقيمتها المالية، حيث أن للمعلومات قيمة أدبية ومادية معاً، وتشمل حقوق الملكية الفكرية أيضاً براءات الاختراع ،[1] إذ تمثل براءات الاختراع أفكاراً للمخترعين تحمل حقوقاً معنوية ومالية، وقد نص المشرع الجزائري على حماية حقوق الملكية الفكرية من خلال

1 **سفيان سوير: جرائم المعلوماتية، المرجع السابق، ص 34.**

قوانين محددة، وهي الأمر رقم 05-03 لعام 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 لعام 2003 المتعلق ببراءات الاختراع.[1]

ومن أمثلتها: قرصنة البرامج والتطبيقات، وتشمل نسخ وتوزيع البرامج الحاسوبية أو تطبيقات الهواتف الذكية بشكل غير قانوني، دون الحصول على تصريح من مالكي حقوق الملكية الفكرية، وكذلك انتهاك براءات الاختراع، وتشمل استغلال واستخدام اختراعات أو اكتشافات علمية محمية ببراءة اختراع دون الحصول على ترخيص من مالكيها.

2- الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة

تأكد الدستور الجزائري من حماية حياة المواطنين الخاصة وعدم التدخل في هذه الحرمة. وبالنظر إلى دور الحاسوب الشخصي كمخزن للمعلومات الحساسة المتعلقة بالأفراد، فإن له القدرة على تخزين كميات هائلة من المعلومات، مما يجعله معرضاً لخطر الوصول غير المشروع لتلك المعلومات، يمكن أن يشمل ذلك إعداد ملفات تحتوي على معلومات شخصية لشخص آخر بدون إذنه، أو جمع المعلومات بالتعاون مع الشخص المعني ولكن بدون موافقته على حفظها بشكل غير مسموح به للآخرين، أو حتى الاختراق السري لمعلومات تعتبر سرية وخاصة، مثل المراسلات الشخصية والسير الذاتية، وكذلك الملاحقة الإلكترونية وتشمل استخدام وسائل التواصل الإلكتروني لمضايقة أو تهديد أو مراقبة الضحايا بشكل مستمر ومزعج، ونشر صور أو فيديوهات أو معلومات خاصة عن الأفراد على مواقع الانترنت دون موافقتهم، التنصت على المكالمات الهاتفية.[2]

[1] سفيان سوير: جرائم المعلوماتية، المرجع السابق، ص 34- 35.

2 عائشة نايري: الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، س 2016- 2017، ص 25- 26.

ثانيا/ الجرائم المعلوماتية الواقعة على الأسرار

هذه الجرائم تتمثل في استخدام أنظمة المعلومات لكشف الأسرار، سواء كانت هذه الأسرار تتعلق بمصالح الدولة وأنظمتها الدفاعية، أو بالأفراد والمصالح الاقتصادية للمؤسسات، بما في ذلك الأسرار المهنية، ويمكن تقسيم هذه الجرائم إلى صنفين، الأولى تتعلق بالجرائم التي ترتكب ضد أسرار الدولة، والثانية تتعلق بالجرائم التي ترتكب ضد الأسرار المهنية.

و تقع هذه الجريمة لسرقة معلومات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل.[1]

وهذه الجرائم تسبب أضرار لأصحابها أدبية و مادية معتبرة، لذا حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات و الجنح ضد الشيء العمومي من المادة 61 إلى 96 من قانون العقوبات،[2] بالإضافة إلى المادة 394 مكرر 03 التي تنص على: " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد".[3]

ومن أمثلتها اختراق أنظمة الحكومات والوزارات والمؤسسات العسكرية والأمنية للحصول على معلومات سرية تتعلق بالأمن القومي أو العلاقات الخارجية أو الاستراتجيات العسكرية.

---

[1] سفيان سوير: المرجع السابق، ص 38.

[2] الامر رقم 155/66 المؤرخ في 08 يونيو 1996، المتضمن ق. ع، المصدر السابق.

[3] أنظر المادة 394 مكرر 03 المصدر السابق.

وأيضا التجسس على أسرار العمل مثل قيام الموظفين المتعاقدين بتسريب معلومات سرية تتعلق بشركاتهم أو عملائهم، أو بيانات خاصة بالزبائن، انتهاكا لالتزاماتهم القانونية والأخلاقية.

ثالثا/ الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية، مثلا الاحتيال باستخدام بطاقات ائتمانية مسروقة حيث يقوم المجرومون باستخدام البيانات المسروقة لإجراء عمليات شراء أو سحب نقدي غير مشروعة.[1]

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الاستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة، أو استخدام شاشة النظام، أو الاطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة صلاحيتها أو تم إلغاؤها، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات.[2]

[1] عائشة نايري: المرجع السابق، ص 26.

[2] سفيان سوير: المرجع السابق ص 38.

الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي

تعتبر هذه الصورة بدون شك أكثر الصور خطورة وانتشارا حيث يتم بواسطة الاحتيال إدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها أو تغيير المعطيات المدرجة فيها.[1]

أولا/ جريمة الدخول أو البقاء في منظومة معلوماتية

إن قانون العقوبات الجزائري من القوانين العربية السباقة إلى دراسة هذا الموضوع، خطى المشرع الجزائري هذه الخطوة بتعديل قانون العقوبات، وذلك بإضافة القسم السابع مكرر، بمحتوى المواد 394 مكرر إلى 394 مكرر 7، وقد نصت المادة 394 مكرر منه على ما يلي: "يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك"[2].

من المتفق عليه أن الجريمة تقوم على ركنين مادي ومعنوي، ومن المبادئ المستقرة في القانون الجنائي أن كل جريمة يستلزم لقيامها تحقق ركن مادي يتمثل بواقعة ترتب ضررا, أو تشكل خطرا على المصالح المحمية قانونا.[3]

الملاحظ على هذا النوع من الجرائم، أنها ليست من الجرائم التي يطلق عليها جرائم ذو الصفة، مثل الرشوة أو الاختلاس أو الزنا، بل تقع وترتكب عن كل شخص أي كانت صفته

---

[1] سمية عكور: الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانون والأمني، الملتقى العلمي "حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الاستراتيجية، الأردن، 02-04-09- س 2016 ص 12.

[2] زبيدة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، س 2011 ، ص 46.

[3] أحسن بوسقيعة: الوجيز في القانون الجنائي العام ،الديوان الوطني للأشغال التربوية ،الجزائر، س 2002، ص47

سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا طريقة تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أم لا.[1]

و بالرجوع إلى نص المادة 394 مكرر الفقرة الثانية يلاحظ أن المشرع الجزائري قد شدد في العقاب بالنسبة لجريمتي الدخول و البقاء في النظام المعلوماتي، حيث ضاعف من العقوبة إذا ترتب عن الدخول و البقاء حذف أو تغيير لمعطيات المنظومة الآلية، و كذلك في الحالة التي يتم فيها تخريب نظام اشتغال المنظومة فإن العقوبة تشدد أيضا.

تضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام و هذا حسب المادة 394 مكرر3 من قانون العقوبات الجزائري حيث تنص على أنه: " و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 150000 دج".[2]

ثانيا/ جريمة المساس بمنظومة معلوماتية

تنص المادة 394 مكرر 1 من قانون العقوبات على أنه: " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".[3]

هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل سوف نشرح كل منها على النحو التالي:

---

[1] قورة نائلة: جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، س 2004 ، ص 343.

[2] أنظر المادة 394 مكرر 3 من ق.ع، المصدر السابق.

[3] أنظر المادة 394 مكرر 1 من ق.ع، المصدر السابق.

أ/ فعل الادخال: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بالمعلومات المعالجة آليا سواء كانت خيالية أم كان يوجد عليها معطيات من قبل بقصد التشويش على صحة البيانات القائمة.[1]

ب/ فعل المحو: يقصد به إفناء أو شطب المعلومات الموجودة داخل النظام كليا أو جزئيا، أو إزالة جزء من المعطيات المسجلة على الدعامة أو الموجودة بداخل النظام أو تحطيمها، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[2]

وعملية المحو هي عملية لاحقة على إدخال المعطيات فالمحو يفترض الوجود السابق لعملية الادخال.[3]

ج/ فعل التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، أو عن طريق التلاعب في البرامج، و ذلك بإمداده بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها.[4]

ويتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرامج الممحاة أو برامج الفيروسات بصفة عامة، و من الفيروسات التي تساهم في تعديل

---

[1] آمنة امجدي بوزينة: خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببلوفيليا لدراسة المكتبات و المعلومات، جامعة العربي التبسي، تبسة، الجزائر، المجلد 02 ج ر ،العدد 05، مارس 2020، ص 80- 81.

[2] نسيمة جدي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير في القانون، كلية الحقوق، جامعة وهران، الجزائر، س 2014، ص 66

[3] عبد الفتاح بيومي حجازي: مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي، دار النهضة العربية، مصر، س 2009، ص 384.

[4] المرجع نفسه ، ص 386.

أو إتلاف النظام فيروس "حصان طروادة" و منها كذلك فيروس الدودة و هو عبارة عن برنامج يتميز بقدرته العالية على تعطيل و إيقاف نظام الحاسب الآلي كاملا.[1]

المطلب الثاني: أركان الجريمة الإلكترونية

الجريمة الإلكترونية تمتلك طبيعة خاصة تميزها عن بقية الجرائم لارتباطها بالحاسبة وأنظمة المعلومات، وما تتمتع به من أمور فنية في اغلب جوانب هذه الطبيعة ميزت هذه الجريمة بعدة خصائص انعكست على مرتكب الجريمة الذي يطلق عليه المجرم المعلوماتي، لتمييزه عن المجرم العادي نتيجة لذلك اكتسبت هذه الجرائم شكلا جديدا،[2] ومن اجل اعتبار أي سلوك جريمة بمعناها القانوني لابد من توفر أركان وهذه الأركان هي الركن المادي والركن المعنوي، هذا ما يخص الجريمة العادية، أما ما يتعلق بالجريمة الإلكترونية فلابد من توافر الركن المادي والركن المعنوي إضافة إلى القصد الخاص في بعض الجرائم.

وعليه تقوم الجريمة الإلكترونية على ثلاثة أركان تتمثل في الركن المادي، الركن المعنوي، الركن الشرعي، سنتناول كل ركن على حدى:

الفرع الأول: الركن المادي

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر :

أولا– السلوك الإجرامي.

ثانيا– النتيجة الإجرامية.

---

[1] عبد الفتاح بيومي حجازي: المرجع السابق، ص 388.

[2] رعد فجر فتح، ياسر عواد: اثبات الجريمة الإلكترونية بالدليل العلمي، مجلة تكريت للحقوق، المجلد 1، ج ر، ع2، الجزء 4، ص 479.

ثالثا – العلاقة السببية بين الفعل والنتيجة.

أولا/ السلوك الإجرامي

هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة المعلوماتية يمكن أن نجده بنوعيه السلوك الإيجابي او السلبي، كما لا ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بالشك صعوبات كثيرة.[1]

ثانيا/ النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.[2]

ثالثا/ العلاقة السببية بين الفعل والنتيجة

إذا ما كان القانون يشترط حصول نتيجة جرمية لقيام الجريمة فلابد من قيام علاقة سببية ما بين الفعل والنتيجة حتى يستكمل الركن المادي عناصره وبذلك فإن علاقة السببية تلعب دورا هاما في رسم حدود المسؤولية الجنائية، فتتوافر هذه المسؤولية عندما يمكن إسناد

---

[1] أسامة أحمد المناعسة، جلال محمد الزعبي: جرائم تقنية نظم المعلومات الإلكترونية، ط 3، دار النشر والتوزيع، عمان، س 2014 ، ص 51- 52.

[2] بلعلبات إبراهيم: أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط الأولى، دار الخلدونية، الجزائر، س 2007، ص 18.

النتيجة التي وقعت إلى مرتكب السلوك الذي أدى إليها، وهو ما يؤدي على استبعادها حيث لا ترتبط النتيجة بالفعل ارتباطا سببيا.

وهذه هي عناصر الركن المادي البد من توافرها مجتمعة حتى يستكمل عناصره، وتختلف عن الجريمة التقليدية في السلوك الإجرامي حيث يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير.[1]

الفرع الثاني: الركن المعنوي

الركن المعنوي هو الحالة النفسية للجاني، والعالقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة، بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العالمات التجارية في القانون الفيدرالي الأمريكي وأحيانا أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.[2]

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين أساسيين هما العلم والإرادة:

العلم يعني إدراك الفاعل بأن ما يقوم به هو فعل مجرم قانونًا أما الإرادة تعني أن الفاعل يتعمد القيام بالسلوك الإجرامي بهدف تحقيق نتيجة معينة.

1 سبع زيان، سلمى المفتي: صور وأركان الجريمة المنظمة، دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد13، ع 3 ، س 2020 ص 233.

2 عبد الرؤوف بوديسة بجاد: آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة ماستر مهني في الحقوق تخصص قانون الاعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، س 2021، 2022، ص 20

وفقًا للمبادئ العامة في قانون العقوبات الجزائري، يمكن أن يكون القصد الجنائي إما عامًا أو خاصًا، وعليه القصد الجنائي العام هو الهدف المباشر من السلوك الإجرامي، ويقتصر على مجرد ارتكاب الفعل المجرم.[1]

أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة بل يذهب إلى التأكد من تحقيق النتيجة مثال في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه.

أما فيما يتعلق بالجريمة الإلكترونية، يُفترض أن الفاعل يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به، مع علمه وقصده لذلك، وبغض النظر عن الظروف، لا يمكن أن ينتفي عنصر العلم كركن أساسي للقصد الجنائي العام.[2]

وعليه، فإن القصد الجنائي العام متوفر في جميع الجرائم الإلكترونية دون استثناء، ومع ذلك، قد يتوفر القصد الجنائي الخاص في بعض الجرائم الإلكترونية، مثل جرائم تشويه السمعة عبر الإنترنت، ويبقى تقدير ذلك للسلطة التقديرية للقاضي.[3]

فيما يتعلق بجريمة الاحتيال الإلكتروني التي تُعد جريمة عمدية، يتطلب المشرع توفر القصد الجنائي لتحقيق مسؤولية الجاني، القصد الجنائي المطلوب هو بنوعيه العام والخاص، حيث يكون المجرم على علم بأنه يخالف القانون بسلوكه، ونيته تتجه إلى تحقيق ربح غير مشروع له أو للغير، أو تجريد شخص آخر من ممتلكاته بطريقة غير مشروعة.[4]

---

[1] بوضياف اسمهان: المرجع السابق، ص 354.

[2] سفيان سوير: المرجع السابق، ص 12 .

[3] محمود نجيب حسني: شرح قانون العقوبات، دار النهضة العربية، القاهرة، س 1992 ، ص 4.

[4] احمد خليفة الملط: الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية س 2006 ، ص 112-113.

الفرع الثالث: الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص و الالتزام بمضامينه.[1]

يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري وال مجال لإهمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم.[2]

إن الركن الشرعي للجريمة، الذي يتمثل في الصفة غير المشروعة للفعل الذي يقوم به الجاني، يتضمن عنصرين أساسيين:

1. مطابقة الفعل لنص التجريم.
2. ألا يكون الفعل المرتكب مشمولاً بأحد أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد

---

[1] أسامة احمد المناعسة، جلال محمد الزعبي: المرجع السابق، ص45.

[2] حنان ريحان مبارك المضحاكي: الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، س 2014 ص57.

ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة.[1]

[1] بلعليات إبراهيم: المرجع السابق، ص94-95

خلاصة الفصل الأول

في هذا الفصل من الدراسة، قمنا بمناقشة مفهوم الجرائم الإلكترونية واستعرضنا العديد من التعاريف المتعلقة بها، مع الإشارة إلى المعايير الأساسية التي تم الاعتماد عليها في صياغة هذه المفاهيم، حيث لوحظ أن المشرع الجزائري لم يقدم تعريفًا محددًا للجريمة الإلكترونية، بل اكتفى بالإشارة إليها من خلال تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

كما تطرقنا لمراحل تطور هذه الجرائم اضافة إلى الخصائص الفريدة التي تميز الجرائم الإلكترونية، مما يجعلها قضية معقدة ومتفردة في نطاق القانون، أما الأركان القانونية المرتبطة بها، فهي تشمل كل من الركن المادي والشرعي والمعنوي، الأمر الذي يؤكد على الحاجة لفهم دقيق ومفصل لهذه الجرائم، هذا النقاش يهدف إلى تعميق الفهم لطبيعة الجريمة الإلكترونية وكيفية تعامل القانون معها، مع التركيز على الحاجة إلى توفير تعريفات واضحة ومحددة للتصدي لهذه الجرائم بكفاءة في الإطار القانوني الجزائري.

الفصل الثاني

الفصل الثاني: النظام القانوني للتحقيق الجنائي الالكتروني

إن ظهور الجريمة الالكترونية فرض على جهات التحقيق تحديثات عظيمة لم يسبق لها مثيل نظرا للطابع الذي تتميز به هذه الأخيرة، مما أدى إلى إعادة النظر في وسائل المكافحة التقليدية للجريمة الالكترونية وأساليبها، وطرق الوقاية منها، وأصبح من الضروري وضع الخطط والبرامج الإستراتيجية لتحديد أجهزة العدالة الجنائية من حيث بنيتها المؤسساتية، وكوادرها البشرية، لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة، فرجال التحقيق يواجهون صعوبات شديدة في ضبط وتوصيف الجرائم الالكترونية وتعقب مرتكبيها، ويعود ذلك إلى كونها جرائم ترتكب في فضاء الكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود، وتعتبر التحقيق واثبات الجرائم الالكترونية من أهم المواضيع القانونية ذلك بالنظر إلى المشكلات الإجرائية التي أثارتها هذه الجرائم المستحدثة والمتمثلة في سرعة ودقة التنفيذ وإمكانية إزالة أثارها، هذا ما أوقع أجهزة التحقيق أمام تحدي كبير ظهر فيه تفوق واضح لمرتكبي هذا النوع من الجرائم من حيث قدرتهم على التعامل مع هذه التقنيات الحديثة، والولوج إلى مكوناتها المعقدة، وهذا ما سيتم التطرق إليه من خلال هذا الفصل حيث سنقوم بتقسيمه إلى مبحثين كالتالي:

المبحث الأول: ماهية التحقيق الالكتروني الجنائي

المبحث الثاني: الآليات المستحدثة للتحقيق في الجرائم الالكترونية

المبحث الأول: ماهية التحقيق الجنائي الالكتروني

يعتبر التحقيق الجنائي صراع بين المحقق والمجرم، الأول ينشد الحقيقة والثاني يحاول التضليل وطمس الحقائق حتى يفلت من العقاب، ولكن بقدر ما يكون المحقق الجنائي من خبرة وإلمام بالعلوم الجنائية وبقدر ما يتمتع به من كفاءة ومقدرة وسيطرة على المواقف التي يواجهها بقدر ما تكون النتيجة في صالح التحقيق ارساءا لقواعد الحق، فالتحقيق في الجرائم الالكترونية يمتاز بخصوصية تجعله يفترق عن التحقيق في الجرائم التقليدية نظرا لتميز هذه الجرائم عن غيرها من الجرائم التقليدية الأخرى خاصة فيما يتعلق بطبيعة مسرح الجريمة، الأمر الذي يقتضي ضرورة تطوير أساليب التحقيق الجنائي الالكتروني بصورة تجعله يتلاءم مع هذا التميز، بحيث تكن سلطة التحقيق من كشف غموض هذه الجرائم وتحديد شخص المتهم واثبات التهمة عليه، كما أن التحقيق الجنائي الالكتروني ليس مقتصرا فقط على الأجهزة الالكترونية أو أدلة ملموسة، بل من الممكن أن تكون أيضا عملية تتبع الأدلة والأمور التي تم إجراءها إثناء وبعد عملية الاختراق من خلال تحليل ملفات النظام وتتبع اثره والحركات التي قام بها كل هذا سيتم تناوله من خلال هذا المبحث حيث ستناول في المطلب الأول تعريف التحقيق الالكتروني الجنائي ثم في المطلب الثاني عناصر ووسائل التحقيق الالكتروني.

المطب الأول: تعريف التحقيق الجنائي الالكتروني

لعل من أكثر الأمور صعوبة في الأبحاث الشرطية هو التوفيق بين مقتضيات كشف الحقيقة عند وقوع الجريمة، وبين حرية المتهم التي تصونها نظم قانونية اعتباره بريء إلى أن تثبت إدانته، مع الأخذ بعين الاعتبار ضرورة التحرك لجمع الأدلة دون إبطاء أو تأخير، فوسائل التحقيق الجنائي غي عصر المعلوماتية تطورت تطورا ملموسا يواكب حركة الجريمة وتور أساليب ارتكابها، بعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية واستخدام الانترنيت هي الصفة المميزة والغالبة.

وهذا ما يدفعنا إلى إثارة عنصر الماهية أو الإطار المفاهيمي لموضوع دراستنا المتمثل في التحقيق الجنائي الالكتروني والذي يتطلب بالضرورة تعريفه (الفرع الأول)، ثم شروط التحقيق في الجريمة الالكترونية (الفرع الثاني) وخصائص التحقيق الالكتروني (الفرع الثالث).

الفرع الأول: تعريف التحقيق الجنائي الالكتروني

التحقيق الجنائي في الجرائم الالكترونية عبارة عن فحص جهاز الجاني أو المشتبه فيه من قبل المحققين فمثلا إذا تمت جريمة عن طريق الحاسوب أو الأجهزة الذكية، يأتي المحقق المتخصص ليفحص ما به وذلك باستخدام أدوات خاصة ودراسات سابقة وكل ماهو ممكن والهدف منها جمع الأدلة المطلوبة.

ويعرف أيضا بأنه:" عمل قانوني يقوم به مأمور اضبط القضائي المختص لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل"[1].

يتضح من خلال هذا التعريف الإجراءات المعقدة والمحددة اللازمة لضبط الجرائم الإلكترونية وتقديم الجناة إلى العدالة، مع التأكيد على أهمية التخصص والخبرة في التعامل مع هذا النوع من الجرائم.

كما يعرف أيضا بانه:" استخدام الطرق المثبتة علميا، لحفظ، جمع، عرض، تحديد، تحليل، ترجمة، توثيق والتحقيق من صحة الأدلة الرقمية المستخرجة من المصادر الرقمية،

[1] **مصطفى محمد موسى: المراقبة الالكترونية عبر شبكة الانترنيت، دراسة مقارنة بين المراقبة الأمنية والتقليدية والالكترونية، كتاب 05، دار الكتب والوثائق القومية، مصر، القاهرة، 2003.، ص 166.**

بهدف تسهيل أو تعزيز بناء الأحداث الجنائية أو المساعدة في إحباط العمليات غير الشرعية المرتقبة"[1].

تعريف عام للتحقيق الجنائي الإلكتروني: "هو العملية المنهجية لجمع وتحليل واستخراج المعلومات والأدلة الرقمية من الأجهزة الإلكترونية أو أنظمة الحاسب الآلي، بهدف استخدامها في التحقيقات الجنائية والإجراءات القانونية"[2]

ولقد تم نقد التحقيق الجنائي الإلكتروني على أنه قد تنتهك عملية التحقيق الجنائي الإلكتروني خصوصية الأفراد إذا لم تتم بطريقة قانونية وأخلاقية، مما قد يؤدي إلى انتهاكات لحقوق الإنسان، كما أن التحقيق الجنائي الإلكتروني يتطلب استثمارات كبيرة في البنية التحتية والموارد البشرية المتخصصة، مما قد يشكل عبئا ماليا على الوكالات القانونية والحكومية، وكذا صعوبة تدريب المحققين، وسرعة التقادم، حيث أن التقنيات الرقمية تتطور بسرعة كبيرة، مما يجعل من الصعب على المحققين مواكبة التغيرات وتحديث معارفهم ومهاراتهم باستمرار.

رغم هذا النقد، فإن التحقيق الجنائي الإلكتروني يظل أداة قيمة للكشف عن الجرائم الإلكترونية والحصول على الأدلة الرقمية اللازمة للمحاكمات ومع ذلك، يجب التعامل معه بحرص وفقا للقوانين واللوائح المعمول بها لضمان حماية حقوق الإنسان والخصوصية والعدالة.

[1] محمد معسكر: مقال بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته، متوفر على الموقع التالي: htt//www.isecurity.org.، تم الاطلاع عليه يوم 2024/05/03 على الساعة 17:15.

[2] كاهنة آيت حمودة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي، جامعة الشلف، المجلد 07 العدد 01، 2023، ص 187.

الفرع الثاني: شروط التحقيق في الجريمة الالكترونية

من المقرر والمعروف أن التحقيق في الجرائم الالكترونية يتطلب توافر عدة شروط أساسية تنحصر فيما يلي:

أولا: أن يكون التحقيق بصدد جريمة (جناية أو جنحة)

يقصد بذلك أن تكون جريمة معاقب عليها في القانون، فلا شان للمحقق بعمل لا يشكل جريمة ويجري التحقيق واقعة توصف بأنها جناية أو جنحة فبمجرد وقوع الجريمة تبدأ عمليات التحقيق وبذلك يتم تكييفها تكيفا قانونيا، فالمبدأ العام في القضايا الجنائية أن التحقيق فيا وجوبيا وهذا ما نصت عليه المادة 66 من قانون الإجراءات الجزائية فلا يجوز إحالة المتهم بجناية إلى جهات الحكم دون المرور على التحقيق وذلك لخطورة هذا النوع من الجرائم والعقوبات المترتبة عليه آما التحقيق في مواد الجنح يكون مطلوبا وضروريا كلما كانت القضية معقدة، وخطيرة وكلما تطلب الأمر اتخاذ إجراء من إجراءات التحقيق يدخل طبيعيا في اختصاص قاضي التحقيق كاقتضاء وضع الشخص رهن الحبس المؤقت أو اجراء خبرة أو انابة قضائية ..الخ، آما فيما يخص مواد المخالفات التي تعد اقل الجرائم خطورة فان التحقيق فيها يكون دائما جوازيا بمعنى بإمكان وكيل الجمهورية طلبه إذا رأى ضرورة ذلك[1].

ثانيا: أن تكون الجريمة قد وقعت فعلا أو ترجح وقوعها

العبرة في اتخاذ الإجراءات في شان الجرائم الالكترونية أن تكون الجريمة محل التحقيق قد وقعت فعلا أو ترجح وقوعها، فلا يجري التحقيق بشان جريمة محتملة، وإلا كان الإجراء باطلان ومما لا شك فيه أن لمأمور الضبط القضائي أن يباشر إجراءات الاستدلال وجمع التحريات بشان وجود أدلة كافية على وجود جريمة قامت الدلائل الكافية على وقوعها، كان

[1] **عمارة فوزي: قاضي التحقيق، أطروحة دكتوراه في العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2010/2009، ص 39.**

يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على ارتكابه جريمة في الجنايات أو الجنح عموما[1].

الفرع الثالث: الفرق بين التحقيق الالكتروني والعادي التقليدي

يتميز التحقيق الجنائي في الجرائم الالكترونية بسمات ذاتية تميزه عن التحقيق التقليدي وترجع هذه الذاتية إلى الأسباب التالية:

- أن مرتكبي الجرائم الالكترونية لديهم قدرة الكترونية قادرة على سرعة إتلاف وتشويه واضاعة الدليل الالكتروني في وقت قصير.
- هذه النوعية من الجرائم الالكترونية لا تترك أثرا ماديا في كثير منها على مسرح الجريمة.
- أن التحقيق في الجريمة الالكترونية ذات البنية الرقمية يحتاج لإمكانيات مادية وقواعد وإجراءات تختلف عن التحقيق في الجرائم التقليدية سواء من حيث طبيعة السلوك الإجرامي الالكتروني أو من حيث طبيعة الدليل الالكتروني أو وسائل واليات كشف الجريمة والوصول إلى الدليل الالكتروني[2].

المطلب الثاني: عناصر التحقيق في الجريمة الالكترونية

لا تختلف الجريمة المعلوماتية عن الجريمة الكلاسيكية في الأركان المتعارف عليها، إلا أن الأولى لها خصوصية تختلف عن الجريمة الثانية، لذلك يجب على المحقق أن يستظهر اركن المادي **(الفرع الأول)**، والركن المعنوي للجريمة محل التحقيق **(الفرع الثاني)**،

---

[1] سرحان حسن المعيني: التحقيق في الجرائم تقنية المعلومات، الفكر الشرطي، المجلد 20، العدد 04، رقم 79 الشارقة، الإمارات العربية المتحدة، س 2011، ص 48.

[2] مصطفى محمد موسى: المرجع السابق، ص 166-167.

الفرع الأول: إظهار الركن المادي للجرائم الالكترونية

إن النشاط أو السلوك المادي في جرائم الانترنيت يتطلب وجود بيئة رقمية واتصالات بالانترنيت[1]، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته فمثلا يقوم مرتكب الجريمة بتجهيز الحاسبة الالكترونية لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسبة الالكترونية ببرامج اختراق أو أن يقوم بتعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف كما يكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها[2].

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الالكترونية حتى ولو كان القانون لا يعاقب على

الأعمال التحضيرية، إلا انه في مجال تقنية المعلومات الأمر يختلف بعض الشيء فشراء برامج اختراق وبرامج فيروسات ومعدات لفك الشفرات وكلمات المرور، فمثل هذه الأشياء تشكل جريمة في حد ذاتها[3].

الفرع الثاني: إظهار الركن المعنوي للجرائم الالكترونية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم فهو

---

[1] عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الفكر الجامعي، الإسكندرية، س 2006، ص 80-81.

[2] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 52.

[3] علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة الالكترونية، المكتب الجامعي، الإسكندرية، س 2012، ص 66.

تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانوني التجاري وتارة أخرى إثبات العلم أي علم الجاني بأنه ارتكب فعلا مجرما.[1]

القصد الجنائي، يتحقق القصد الجنائي في الجرائم الإلكترونية عندما يتوافر لدى الجاني إرادة حرة ومدركة لارتكاب الفعل المجرم، مع علمه بالظروف والنتائج المترتبة على فعله، وينقسم القصد الجنائي إلى قصد عام وأخر خاص:

القصد العام: هو توافر نية الجاني في ارتكاب الفعل المكون للجريمة، دون اشتراط قصد نتيجة معينة.

مثال: قيام شخص باختراق موقع الكتروني لمجرد إثبات قدراته.

القصد الخاص: وهو توافر نية الجاني في ارتكاب الفعل المكون للجريمة، مع توافر قصد نتيجة معينة.

مثال: قيام شخص باختراق موقع بنك بهدف سرقة البيانات المالية للعملاء.[2]

المطلب الثالث: الأجهزة المكلفة بالتحقيق في الجرائم الالكترونية

منح القانون 09-04 دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم الماسة بأنظمة الاتصال والمعلوماتية وكشف مرتكبيها حيث تنص المادة 08 منه على وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية

[1] خالد ممدوح ابراهيم: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، الاسكندرية، س 2010 ص 36-37.

[2] إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة آفاق للبحوث والدراسات السياسية، المركز الجامعي إيليزي، العدد 04، 2019، ص 187.

اللجوء إلى مساعدة السلطات الأجنبية المختصة من اجل الحصول على المعطيات المبحوث عنها وقد أناط مهمة التحقيق الجنائي إلى أجهزة سوف نقم بالتطرق إليها بالتفصيل من خلال هذا المطلب.

الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الالكترونية

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة على ضمن حدود اختصاصها الفني أو التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من اجل ضمان تحقيق اكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها[1].

تعتبر الضبطية القضائي صاحبة الاختصاص الأصيل في كل الجرائم بما فيحجا الجرائم الالكترونية وقد منحها القانون أساليب تحري جديدة نبينها فيما يلي:[2]

أولا: على مستوى جهاز الشرطة

انشات المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الانترنيت[3]، بالإضافة

---

[1] عز الدين عثماني: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دار البحوث والدراسات القانونية والسياسية، العدد 04، تبسة، جانفي 2018، ص 51.

[2] أمهدي بوزينة أمنة: إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مداخلة مشارك به في ملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 2007، ص 57.

[3] سعيد نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في العلم القانونية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 115.

لإنشائها ثلاثة مخابر على مستوى بشار وورقلة وتمنراست قيد الانجاز من اجل تعميم هذا النشاط على كافة ربوع الوطن[1]، كما يضم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الالكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية والتي تضم 03 أقسام وهي:

- قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الالكترونية[2].

ثانيا: على مستوى جهاز الدرك الوطني

تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الالكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره ببوشاوي التابع لقيادة الدرك العامة قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الالكترونية[3]، وأيضا بواسطة الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الالكترونية[4].

الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية عن طريق المرسوم الرئاسي رقم 15-261 ومقره بئر مراد رايس، وهو تابع لمديرية الأمن للدرك الوطني، وقد حددت المادة 01 منه تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة

[1] ربيعي حسين: آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، جامعة باتنة، س 2016-2017، ص 176.

[2] ربيعي حسين: نفس المرجع، 177.

[3] سعيداني نعيم: المرجع السابق، ص 116.

[4] ربيعي حسين: المرجع السابق، ص 182.

بتكنولوجيات الإعلام والاتصال[1]، وتمارس هذه الهيئة العديد من المهام في مجال التصدي للجريمة الالكترونية ورد النص عليها في المادة 14 من القانون 09-04 السالف الذكر وهي:

- ضمان المراقبة المستمرة لشبكة الانترنيت.
- القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني.
- المشاركة في عمليات البحث والتحري عن الجرائم الالكترونية.

[1] **راجع المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة 1436 الموافق ل 08 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة في 18 اكتوبر 2015.**

المبحث الثاني: الإجراءات المستحدثة الخاصة بالتحقيق الالكتروني

إذا كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها بظهور أنماط مستحدثة من الجرائم عرفت بجرائم المعلوماتية، فإنها في المقابل أثرت على وسائل التحقيق في هذه الجرائم، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الإجرامي المستجد الذي يحتاج إلى طرق وتقنيات جديدة تتناسب مع طبيعته، يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لان تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة، واعتبارا للطبيعة الخاصة للجرائم الالكترونية في عناصرها ووسائل وتقنيات ارتكابها، اضطر المشرع الجزائري إلى أعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسالة التحقيق والإثبات، باعتبارها أهم موضوعات هذا القانون، لان الدليل الذي يقوي على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية والفنية وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية للتحقيق واستخلاص الدليل قادرة على القيام به مما قد يؤدي في الغالب إلى إفلات العديد من المجرمين من العقاب.

وعلى ضوء ما تقدم، كان لازما على المشرع التدخل بقواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها ففي الكشف عن المجرم ألمعلوماتي والوصول إلى دليل إثبات فيها بسرعة وسهولة، وهي الإجراءات التي سوف نتناولها بشيء من التفصيل ففي هذا المبحث من خلال مطلبين:

المطلب الأول: التسرب الالكتروني

المطلب الثاني: التسليم المراقب

المطلب الأول: التسرب الالكتروني

يعد التسرب إجراء من إجراءات البحث والتحقيق المستحدثة والتي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الالكترونية ومن بينها المشرع الجزائري الذي تبنى بدوره هذا الإجراء مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة لمكافحة جرائم الحاسوب بموجب المرسوم الرئاسي رقم 02-05 المؤرخ في 2002/02/02، واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19.

الفرع الأول: تعريف التسرب الالكتروني

لقد تطرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية على انه:" قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك معهم أو خاف".

وعليه يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وان يرتكب عن الضرورة الأفعال الآتي بيانها:

- حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات يتحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها.
- استعمال أو وع تحت تصرف مرتكبي هذه الجرائم كافة الوسائل[1].

آما في مجال الجريمة الالكترونية فتتم بدخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك ب:

- اختراقه لمواقع معينة وفتح ثغرات الكترونية فيها.

[1] أحسن بوسقيعة: التحقيق القضائي، ط7، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2008، ص 114.

- اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان مثلهم، مستخدما أسماء أو صفة هيئات مستعارة ووهمية وذلك سعيا منه للاستفادة منهم حول كيفية اقتحام الهكر لموقع ما مثلا.

يلاحظ مما سبق أن عملية التسرب عملية معقدة حيث تتطلب أن يدخل العون المكلف بالعملية ف اتصال بالأشخاص المشتبه فيهم ويربط علاقات من اجل تحقيق الهدف النهائي من العملية.

كما تستلزم هذه العملية ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه، وكذلك معرفة عناصر الجماعة وكيفية نشأتها واختصاصات كل فرد منها بالإضافة إلى الوسائل التي تعمل بها، وبعد أن يتم دراسة الوسط المستهدف يتم اختيار الأشخاص المناسبين للقيام بمهمة التسرب[1].

الفرع الثاني: شروط صحة التسرب

باعتبار عملية التسرب إجراء غير عادي لجمع البيانات والمعطيات الخاصة لتي تشير إلى كافة الأعمال الإجرائية، وتمكين المصالح الأمنية من معرفة الإمكانيات والأساليب المستعملة لارتكاب الأفعال المجرمة، فقد تمت إحاطته بجملة من الشروط التي يجب مراعاتها عندما تقتضي ضرورات التحري أو التحقيق اللجوء اليه، وعليه فتتمثل هذه الشروط في:

[1] **هدى زوزو: التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد 11، جوان 2014، ص 118.**

أولا: الشروط الموضوعية

يشترط للقيام بعملية التسرب مراعاة مجموعة من الشروط الموضوعية من قبل السلطة المختصة بإجراء التسرب، خاصة وقت ومكان إجراء عملية التسرب، نوع الجريمة، التسبب، أن يكون المتسرب فاعلا أو شريكا.

1. السلطة المختصة بمنح اذن لإجراء التسرب

تتمثل الجهة المختصة بإصدار أو منح الإذن بالتسرب آما وكيل الجمهورية أو قاضي التحقيق.

- ففي مرحلة التحري فان وكيل الجمهورية هو من يقوم بمتابعة والرقابة على تلك العملية، أي انه هو من يأذن بالعملية وهو من يتولى عملية سيره من خلال ما له من مكانة في إدارة نشاط ضابط وأعوان الشرطة القضائية.
- آما في مرحلة التحقيق فان قاضي التحقيق بعد إخطار كيل الجمهورية هو الذي يأذن بالتسرب وهو من يقوم بمراقبته[1]، حيث يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.

2. وقت ومكان إجراء عملية التسرب

باعتبار التسرب إجراء مكن إجراءات التحقيق يجعل من المتسرب غير مقيد بحيز زمني يتحرك فيه، فضرورة التحقيق تبرر عملياته طول ساعات الليل والنهار، وله أن يدخل كل الأماكن التي يمكن أن يكشف فيها الحقيقة دون قيد أو شرط لأنه لا يتحرك بصفة ضابط أو عون الشرطة القضائية بل هوية مستعارة.

[1] **زيدان زبيخة: الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، ط1، ص 169.**

3. التسبيب

يعتبر التسبيب أساس العمل القضائي فمن خلاله تثبت العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن، وكذا الحجج والمبررات التي أقنعتها لمنح الإذن بإجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية ليلجا إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكوون ضمن موضوع طلب الإذن[1].

ثانيا: الشروط الشكلية

1. تحرير تقرير من طرف ضابط الشرطة القضائية

طبقا للمادة **65** مكرر **13** يكلف ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقرير يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقا للمادة **65** مكرر **14**، وعليه فلا بد على ضابط الشرطة القضائية المكلف بتنسيق العملية وقبل مباشرتها أن يقوم بتحرير تقرير مفصل عن العملية.

2. الإذن بمباشرة عملية التسرب .

قبل البدء في عملية التسرب لابد من الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية طبقا للمادة 65 مكرر15 من ق ا ج ويجب أن يكون الإذن مكتوبا ومسبقا طبقا لنفس المادة السالفة الذكر وذلك تحت طائلة البطلان ولابد أن يتضمن إذن التسرب وراء منح الإذن ويتعلق التسرب غالب بضرورة البحث والتحري في الجرائم الواردة في المادة 65 مكرر.[2]

---

[1] هوام علاوة: التسرب كإلية للكشف عن جرائم في القانون الجزائري، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص 03.

[2] – فوزي عمارة ،المرجع السابق ، ص 248 .

3. مدة المعاينة

حدد قانون الإجراءات الجزائية في المادة 65 مكرر15 مدة العملية بأربعة 04 أشهر قابلة للتجديد ضمن نفس الشروط أي بناء على إذن مكتوب من قبل وكيل الجمهورية أو قاض التحقيق بعد إخطار وكيل الجمهورية وهي تتضمن المدة التي اخذ بها قانون الإجراءات الجزائية الفرنسي في المادة 706/ 8 .

ويمكن لوكيل الجمهورية أو قاض التحقيق الذي أصدر الرخصة بان يأمر بإيقاف العملية في أي وقت قبل انقضاء المدة المحددة طبقا للفقرة 4 من المادة 65 مكرر 15 في هذه الحالة فان العضو المتسرب قد لا تمكن من إيقاف نشاطه مع الجماعة الإجرامية فجأة ودون سبب مما قد يعرضه لأن يكون عرضة للانتقام خوف من انكشاف أمره .

وهو ما يجعل حياته وحياة أسرته عرضة للخطر، لذلك نظم المشرع الجزائري هذه المسألة في المادة 65 مكرر 17 بمواصلة نشاطاته الوقت الكافي لتوقيف عمليات المراقبة في ظروف تضمن سلامته ودون أن دون أن يكون مسئولا جزائيا على أن لا تتجاوز هذه المدة 04 أشهر أخرى طبقا للمادة 65 مكرر فقرة 2 من قانون الإجراءات الجزائية .

ولا يودع الإذن المتعلق في بالتسرب في ملف الإجراءات إلا بعد انتهاء العملية والحكمة من إيداعها بعد نهاية العملية وليس قبلها أو أثناء العملية كون عملية التسرب سرية لا يعلم بها إلا القاضي الذي رخص بها والضابط المشرف عليها والعون المسرب .[1]

4. الاختصاص الإقليمي

يقصد بالاختصاص الإقليمي النطاق الجغرافي الذي يمارس فيه هؤلاء صلاحياتهم وتحدد بالدائرة الإقليمية التي يباشرون فيها أعمالهم حسب المادة **1/16** من قانون الإجراءات الجزائية (يمارس ضابط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون

[1]– لوجاني نور الدين: أساليب التحري الخاصة و إجراءاتها ، ورقة بحثية مقدمة في اليوم الدراسي حول : علاقة النيابة العامة بالشرطة القضائية ، اليزي ، 2008/12/12، ص 14.

منها وظائفهم المعتادة) وجعل هذا الاختصاص وطنيا بالنسبة لفئة معينة وهم ضباط الشرطة القضائية التابعين لمصالح الأمن العسكري طبقا للمادة 6/16 من قانون الإجراءات الجزائية .

ولم يضع المشرع الجزائري ضوابط تحدد افتقاد ضباط الشرطة القضائية الاختصاص المحلي إلا انه يمكن تحديده بالرجوع إلى المواد37 و40 من ق ا ج التي تحدد الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق بمكان وقوع الجريمة أو محل إقامة المشتبه فيه أو المكان الذي تم في دائرة القبض على المشتبه فيه .[1]

إلا أنه وفيما يتعلق بجرائم محددة على سبيل الحصر في المادة 6/16 من قانون الإجراءات الجزائية اقر المشرع الجزائري إمكانية تمديد الاختصاص المحلي لضباط الشرطة القضائية ليشمل كافة إقليم الوطني وتتعلق هذه الجرائم في :

- جرائم المخدرات.
- الجريمة المنظمة عبر الحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- جرائم تبييض الأموال.
- جرائم الإرهاب.
- الجرائم المتعلقة بالتشريع الخاص بالصرف .

وعليه عند البحث في جريمة من هذه الجرائم لا يتقيد ضابط باختصاص إقليمي معين وإنما يشمل كافة أراضي الجمهورية والهدف من ذلك هو ضمان السرعة والفعالية وكما تركز التحقيق وعدم تجزئته على عدة دوائر إقليمية.

والملاحظ أن هذه الجرائم هي الجرائم نفسها المذكورة في المادة 65 مكرر 5 والخاصة بأساليب التحري الخاصة باستثناء جرائم الفساد التي لم يرد ذكرها في المادة 6/16 من ق ا

[1] – **ركاب أمينة: المرجع السابق ، ص15.**

ج إلى انه بالرجوع إلى قانون مكافحة الفساد نجده ينص في المادة 24 مكرر على إنشاء الديوان المركزي لقمع الفساد يكلف بمهمة البحث والتحري عن جرائم الفساد وقد صدر المرسوم 11-426 في 13 محرم 1433 الموافق لـ 8 ديسمبر 2011[1]، الذي يحدد تشكيلة الديوان المركزي للفساد وتنظيمه وكيفية سيره ويشكل من :

- ضباط وأعوان الشرطة القضائية التابعين لوزارة الدفاع الوطني.
- ضباط وأعوان الشرطة التابعين لوزارة الداخلية والجماعات المحلية.
- أعوان عموميون ذوي كفاءات أكيدة في مجال مكافحة الفساد .

وطبقا للمادة 05 من المرسوم الرئاسي السالف الذكر والمادة 24 مكرر 1 من قانون مكافحة الفساد يمارس ضباط الشرطة القضائية التابعون للديوان مهامهم وفقا لقانون الإجراءات الجزائية، أما فيما يتعلق بنطاق اختصاصهم المحلي في هذه فيمتد ليشمل كافة الإقليم الوطني.

وعليه فالتسرب في هذه الجرائم يتم في كامل الإقليم الوطني، غير انه وبعد الحصول على إذن والبدء في عملية التسرب قد يصطدم القائم بعقبة أخرى وهي أن الجماعة الإجرامية لها نشاطات أخرى خارجا لإقليم الوطني، وان اغلب هذه الجرائم تشكل صورة من صور الجريمة المنظمة عبر الوطن التي تتم في إطار عصابات لها نشاطات خار الإقليم الوطني، وهي الحالة التي لم يتطرق لها المشرع الجزائري فكان بإمكانية النص في هذه الحالة على إمكانية إنشاء هيئات تحقيق مشتركة وذلك عن طريق إتمام اتفاقيات أو ترتيبات ثنائية وقد نصت على هذا الشكل عن إشكال التعاون المادة 19 من اتفاقية مكافحة الجريمة المنظمة (يتعين على الدول الأطراف أن تنظر في إبرام اتفاقيات أو ترتيبات ثنائية أو متعددة الأطراف تجيز للسلطات المعنية أن تنشئ هيئات تحقيق مشتركة، فيما يتعلق بالمسائل التي هي موضع تحقيقات أو ملاحظات أو إجراءات قضائية في دولة

[1]- المرسوم رقم 11- 426 المؤرخ في 13 محرم 1493 الموافق لـ 08 ديسمبر 2011 يحدد تشكيلة الديوان المركزي للفساد وتنظيمه وكيفيات سيره .

أو أكثر، وفي حال عدم وجود اتفاقيات أو ترتيبات كهذه يجوز القيام بالتحقيقات المشتركة بالاتفاق في كل حالة على حدا ويتعين على الدول الأطراف المعنية أن تكفل الاحترام التام لسيادة الدولة الطرف التي سيجري دلك التحقيق داخل إقليمها) [1].

الفرع الثالث: صور التسرب وآثاره

أولا : صور تنفيذ عملية التسرب

لم يكتف المشرع الجزائري بتعيين الأساليب أو الأموال التي يمكن للتسرب القيام بها بل قام بتعيين صور تنفيذ العملية في المادة 65 مكرر 12[2] كما يلي :

1. **المتسرب كفاعل** : ورد تعريف الفاعل في المادة 41 من ق ا ج (يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي) وطبقا للمادة 65 مكرر 12 يمكن للشخص الذي يتولى القيام بعملية التسرب عن طريق التمويه أن يتخذ صورة فاعل أساسي في الجريمة ويقوم بالأفعال المنصوص عليها في المادة 65 مكرر 14 في هذا الصدد لا بد من التفريق بين إيهام الغير على انه فاعل وبين التحريض على ارتكاب الجريمة [3].

فالتحريض الشرطي هو دفع الخ إلى ارتكاب الجريمة والذي لم يكن ليرتكبها لولا تدخل عون الشرطة، وعليه في هذه الحالة لابد من معرفة فيما إذا كان لدى الشخص مرتكب الجريمة ميول أو استعداد لارتكاب الجريمة، وقد عرفت محكمة النقض الأمريكية التحريض على انه (هو مشروع إجرامي نجد مصوره في تصرفات أعوان الحكومة الذين يقومون بغرس فكرة ارتكاب الأفعال المجرمة في ذهن الشخص من اجل متابعة بهذه الأفعال).

---

[1] – المادة 19 من اتفاقية مكافحة الجريمة المنظمة

[2] – راجع المادة 65 مكرر 12 من قانون الإجراءات الجزائية.

[3] – عبد العالي خواشي: ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي ، دار الجامعة للنشر، الإسكندرية، مصر 2006 ص 212 .

ولمعرفة فيما إذا هناك تحريض أم لا يجب النظر إلى العلاقة السببية بين فعل عون الشرطة والجريمة المرتكبة فذا كان قول عون الشرطة القضائية هو الذي دفع الشخص إلى ارتكاب الجريمة نكون بصدد التحريض وعليه فان إيهام الغير بان المتسرب فاعل إنما هو من اجل الحصول على دليل وليس من اجل التحريض على الجريمة وهو ما أخذ به المشرع الجزائري في المادة 65 مكرر 12 حيث نص إن هذه الأفعال لا يجوز أن تشكل تحريض على ارتكاب الجرائم.[1]

2. **المتسرب كشريك** : ورد تعريف الشريك في المادتين 42 و 43 ق ع فحسب المادة 42 فالشريك هو كل من ساعد بكل الطرق او عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك ويدخل في حكم الشريك طبقا للمادة 43 من اعتياد تقديم مسكن أو ملجأ أو مكان للاجتماع لواحد أو أكثر من الأشرار اللذين يمارسون اللصوصية أو عنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال مع علمه بسلوكه الإجرامي .[2]

3. **المتسرب كخاف** : يقصد بذلك أن يقوم المتسرب بإيهام أعضاء الجماعة الإجرامية بأنه واحد منهم من خلال قيامه بإخفاء أشياء قد تكون أدلة ارتكابهم للجريمة أو العائدات التي تم تحصيلها من خلال ارتكاب الجرائم وقد ورد على مفهوم إخفاء الأشياء في المواد 387 ق ع (كل من اخفي أشياء مختلفة أو مبددة أو متحصله من جناية أو جنحة أو مجموعها أو جزء منها يعاقب بالحبس من سنة على الأقل إلى خمسة سنوات على الأكثر وبغرامة من 500 إلى 20.000 د ج) والمادة 43 من قانون مكافحة الفساد (يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 2000.0000 دج إلى 10000000 دج كل شخص اخفي كلا أو جزءا من

---

[1] – عبد الله سليمان: المرجع السابق، ص 60.

[2] – حليمة بن بنونة: سلطات الضبط القضائي في قانون الإجراءات الجزائية ، مذكرة لنيل شهادة الماستر، جامعة المجيد بن باديس ، مستغانم، 2014–2015، ص 63.

العائدات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القانون) ، ومن خلال هاتين المادتين فان الجريمة تقوم على عنصرين:

- العلم بان هاته الأشياء مختلسة أو مبددة أو متحصله من جناية أو جنحة.
- حيازة وإخفاء هاته الأشياء .

وطبقا للمادة 65 مكرر 12 يستطيع المتسرب إخفاء الأشياء المتحصل عليها من الجريمة أثناء قيامه بمهامه دون أن تقوم مسؤوليته الجنائية .[1]

ثانيا: آثار التسرب

بعد صدور الأمر بالتسرب من طرف القاضي يباشر العون المسرب عملية حسب المقتضيات المطلوبة منه ومن هناك آثار مقترب عن ذلك منها:

1. تسخير الوسائل المادية والقانونية.

نصت على ذلك المادة 65 مكرر 14 من ق ا ج على انه يمكن اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها وكذا استعمال أو وضع تحت التصرف مرتكبي هذه الجرائم والوسائل ذات الطابع القانوني أو الحالي وكذا وسائل ذات طابع القانوني او الحالي وكذا وسائل النقل أو التخزين أو الإيواء أو الاتصال وبالتالي يمكن للعون المتسرب استعمال الأموال المتحصل عليها من ارتكاب المذكورة لنص المادة 65 مكرر 5 ق ا ج وعليه يمكن القول أن هناك استثناء في هذه الحالة طبقا لأحكام المادة 2 من القانون رقم 05/01 المتعلق من الوقاية من تبييض الأموال والإرهاب ومكافحتها.[2]

---

[1] – معزيز أمينة: التسرب في قانون الإجراءات الجزائية ، مجلة القانون والمجتمع ، جامعة مستغانم ، د س ، ص 266-267.

[2] – عمر خوري: شرح قانون الإجراءات الجزائية، دار هومة ، الجزائر، 2007، ص 155

2. **الإعفاء من المسؤولية** : سوف نتناول المسؤولية بنوعيها :

أ. **المسؤولية الجزائية** : نصت المادة 85 مكرر 14 من قانون ا ج على أن ضابط وأعوان الشرطة القضائية المسخرين في عملية التسرب لا يكونوا مسئولين جزائيا حسب الحالات المذكورة سابقا وهذه الحالة ماهي إلا تكريسا للمادة 39 ق ع والتي من خلالها يمكن إدخال نظام التسرب ضمن أسباب الإباحة باعتبار أن القانون إذن بذلك مما جعل المتسرب معفي من المسؤولية الجزائية هذا من جهة ومن جهة أخرى نصت المادة 65 مكرر 12 من ق ا ج على انه لا يجوز له تحت طائلة البطلان أن تشكل الأفعال المسموح له القيام بها تحريض على ارتكاب الجريمة.

ب. **المسؤولية المدنية** : يقصد بها كل التصرفات المدنية أو حتى التجارية التي تقوم بها كإبرام العقود أو حتى عقود تمس الحالة الشخصية للمتسرب نفسه كعقد الزواج ن تطلبت الضرورة لذلك وعليه يبقى السؤال مطروح فيما يخص مصير التصرفات في حالة انتهاء التسرب.

2. إحاطة العملية بالسرية التامة

تتطلب عملية التسرب أحاطتها السرية التامة وقد نص قانون الإجراءات الجزائية على إجراءات عقابية مشددة في حالة إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية في المادة 65 مكرر 16 ق ا ج وقد تعددت الحماية حتى للأفراد عائلة المتسرب وتتراوح هذه العقوبات من سنتين 02 إلى عشرين 20 سنة حبس وغرامة من خمسين ألف إلى مليون دينار حسب الحالات الثلاث المذكورة بالمادة كما أن قانون العقوبات منع سماع الضابط المشرف على العملية بوصفه شاهد كما ورد في المادة 85 مكرر 18 من ق ا ج.[1]

ولقد صادقت الجرائد على هذه الاتفاقية بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002، وتساعد هذه الوسيلة في كسب الوقت وتقديم نتائج أفضل كما تسمح بتجنب ازدواجية المتابعة وتجنب المشاكل الناتجة عن تنازع الاختصاصات.

[1] – انظر المادة 85 مكرر 18 من قانون الإجراءات الجزائية .

المطلب الثاني: التسليم المراقب

يعتبر التسليم المراقب من بين أهم إجراءات وأساليب التحري التي استحدثها المشرع الجزائري بموجب قانون الإجراءات الجزائية والغاية منه هو الكشف عن الجرائم الخطيرة ومن بينها الجرائم الالكتروني والجرائم الماسة بنظام المعالجة الإلية للمعطيات وهذا ما سنتناوله من خلال هذا المطلب.

الفرع الأول: تعريف التسليم المراقب

نص المشرع الجزائري على التسليم المراقب من خلال المادة 16 من ق ا ج لكنه لم يعرفه، عرف المشرع الجزائري التسليم المراقب في المادة 02 من قانون الوقاية من الفساد ومكافحته والتي تنص على (إجراء يسمح لشحنات غير مشروعة أو مشبوهة بالخروج من الإقليم الوطني أو المرور عبره أو دخوله بعلم من السلطات المختصة تحت مراقبتها بغية التحري عن الجرائم وكشف هوية الأشخاص المساهمين في ارتكابها) .[1]

وعرفت المادة 40 من قانون مكافحة التهريب [2] التسليم المراقب بأنه ترخيص السلطات المختصة بمكافحة التهريب بعلمها وتحت مراقبتها حركة البضائع غير المروعة أو المشبوهة للخروج أو المرور أو الدخول إلى الإقليم الوطني بغرض البحث عن أفعال التهريب ومحاربتها بناء على إذن من وكيل الجمهورية.[3]

كما عرف الفقه التسليم المراقب على أنه أسلوب تقفي حركات الأموال الغير معروفة مصدرها أو المشتبه بكونها عائدات أو متحصلات إجرامية في صورتها المادية وحتى لدى

---

[1] – قانون رقم 01/06 المؤرخ في 20 فبراير 2006 ، يتعلق بالوقاية من الفساد ومكافحته ح ، ر ، عدد 14 مؤرخ في 08 مارس 2006 ، معدل ومتمم إلى غاية سنة 2011 بالقانون رقم 15/11 مؤرخ في 02 غشت 2001 ج ر ، عدد 44 مؤرخ في 10 غشت 2011.

[2] – انظر المادة 40 من الأمر 06/05 المتعلق بمكافحة التهريب .

[3] – شنين صالح: التسليم المراقب في التشريع الجزائري واقع و تحديات، المجلة الالكترونية للبحث القانوني، المجلد12، العدد02، جامعة عبد الرحمان ميرة، بجاية، 2015 ، ص25.

نقل الأموال في صورتها الغير عادية ، مثل التحويلات البرقية أو الالكترونية وذلك بالتنسيق بين المؤسسات المالية في الدول المختلفة وبغض النظر ما إذا كانت الأموال غير مشروعة في صورتها المادية الأصلية (نقود سائلة) تحولت إلى صورة مادية أخرى كالذهب أو الأوراق المالية.[1]

الفرع الثاني: شروط التسليم المراقب

يخضع التسليم المراقب للضوابط التالية :

أولا: إذن وكيل الجمهورية

اشترط القانون للقيام بالتسليم المراقب إذن وكيل الجمهورية وذلك في المادة 16 مكرر التي تنص على (يمكن ضابط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية بعد إخباره أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة وجهة نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها)، ونصت على هذا الشرط أيضا المادة **56** من قانون الوقاية من الفساد ومكافحته التي نصت (من أجل تسهيل عملية جمع الأدلة المتعلقة بهذه الجرائم يمكن اللجوء التسليم المراقب ... إلا بعد إذن من السلطة القضائية المختصة)، ويتضح من هذه المادة أن القانون يشترط للقيام بالتسليم المراقب صور إذن من السلطة القضائية المختصة، والمتمثلة في وكيل الجمهورية باعتبار التسليم المراقب أسلوب تحري يلجأ إليه في مرحلة البحث والتحري.[2]

---

[1] – ركاب أمينة: المرجع السابق ، ص 15 .

[2] – شنين صالح: المرجع السابق، ص204.

ثانيا: ممارسته من طرف الضبطية القضائية

طبقا للمادة **16** مكرر من قانون الإجراءات الجزائية يمارس التسليم المراقب بعد إذن وكيل الجمهورية ضباط الشرطة القضائية المحددين في المادة **15** من قانون الإجراءات الجزائية.[1]

يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة إلا انه يجوز لهم في حالة الاستعجال أن يباشروا مهمتهم في كافة دائرة الاختصاص المجلس القضائي الملحقين به،[2] ويجوز لهم أيضا في حالة الاستعجال أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا ويجب أن يساعدهم ضباط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعينة ويتعين عليهم في الحالتين السابقتين أن يخبروا مسبقا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة اختصاصه.[3]

الفرع الثالث: مجال التسليم المراقب

أجاز المشرع الجزائري في المادة **16** مكرر من قانون الإجراءات الجزائية اللجوء إلى هذا الإجراء في بعض الجرائم الخطيرة المنصوص عليها في المادة **7/16** من قانون الاجرءات الجزائية.

ولقد حصرتها هذه المادة في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بالمعالجة الآلية والمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[4]

---

[1] – المادة 15 من قانون الإجراءات الجزائية .

[2] – عبد الرحمان خلفي: المرجع السابق ، ص 72 .

[3] – المادة 16 مكرر من قانون الإجراءات الجزائية .

[4] – المرجع نفسه، ص70 – 71.

وعليه لا يجوز اللجوء إلى التسليم في غير هذه الجرائم مهما كانت خطورتها لان المشرع حددها على سبيل الحصر.

خلاصة الفصل الثاني

نستخلص أن التحقيق الجنائي في الجرائم الالكترونية التي تعد من الأنماط الإجرامية الجديدة التي فجرتها ثورة تقنية المعلومات والاتصالات من العمليات الصعبة والمعقدة التي تتطلب الماما بالتكنولوجيا الإعلام والاتصال.

حيث أن التحقيق الجنائي الالكتروني يعتمد في طياته على تسخيرات مادية وأجهزة الكترونية من اجل الوقوف على مكافحة الجرائم الالكترونية بالإضافة إلى أن المشرع الجزائري استحدث العديد من الإجراءات والآليات التي من شانها مكافحة الجريمة الالكترونية والمتمثلة في التسرب والتسليم المراقب هذه الآليات التي جاءت في قانون الإجراءات الجزائية والتي تبنتها الجزائر على غرار دول العالم حيث استدعى تفاقم هذه الجرائم إلى ضرورة استحداث مثل هكذا آليات لتصدي لها.

خاتمة

الخاتمة

تبين لنا من خلال هذه الدراسة أن التحقيق في الجريمة الالكترونية يختلف تماما عن نظيره في الجرائم المعروفة في العالم التقليدي و تتجلى هذه الخصوصية في عدم إمكانية تطبيق أحكام الجرائم التقليدية على الجرائم المرتكبة في العالم الافتراضي بأصلها و إنما تأخذ طابع خاص و ذلك نظرا للطابع المستحدث لهذه الجريمة المتسمة بالتشعب، أيضا هذه الخصوصية للجرائم المرتكبة عبر الانترنت جعلت مختلف الدول و الهيئات والمنظمات الدولية والإقليمية تدرك مدى خطورتها ومدى التحديات التي تفرضها عليها مما أدى بها إلى المسارعة من أجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحتها.

وتمثلت الجهود الدولية في عقد المؤتمرات وإبرام معاهدات و اتفاقيات دولية وإقليمية مثل اتفاقية بودابست سنة 2001 التي وضعت الأسس السليمة لمكافحة الجريمة الالكترونية، وقد واكب المشرع الجزائري هذه الحركة التشريعية بعد الفراغ التشريعي الذي عانته الجزائر في هذا المجال بتعديل قانون العقوبات بالقانون رقم : 04-15 و بعدها إصدار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها وإدراج تعديلات على قانون الإجراءات الجزائية بما يتلاءم وخصوصية التحقيق في الجرائم الرقمية، والتي تستهدف إظهار أركان الجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية والوصول إلى دليل إدانة و تحقيق العدالة بين جميع أطراف الدعوى التي تستوجب العمل تحت ضمانات المحاكمة العادلة والتحقيق في قضايا نظم المعلومات كما رأينا عادة ما يكون أكبر من أن يتولاه شخص واحد بمفرده فمن الأفضل أن يتعاون عدة أشخاص في إنجاز هذه المهمة فهناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذو معرفة واسعة وغيرهم كل يعمل على شاكلته

وبإتباع آليات جاءت بها التعديلات الجديدة التي تتلاءم وطبيعة الجرائم الرقمية من أجل إثبات المسألة بدليلها .

وعلى ضوء الإشكالات التي ظهرت من خلال الدراسة خلصنا إلى جملة من النتائج تذكر منها ما يلي:

1-إن مفهوم الجرائم الالكترونية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات التي تستهدف البيئة الإلكترونية و عليه فان محل الجريمة التقليدية يختلف تماما عن محل الجريمة الرقمية الذي يكون في شكل افتراضي.

2-المحقق في الجريمة الالكترونية يجب أن يكون على معرفة ودراية بالجوانب الفنية و كذا التقنية للحاسب الآلي والانترنت.

3- توسيع دائرة اختصاص كل من قضاة التحقيق وضباط الشرطة القضائية في مجال متابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و البيانات.

4- تفتيش المنظومة المعلوماتية من أصعب إجراءات البحث والتحري عن الجريمة ومرتكبيها، الأمر الذي يتطلب خبرة واسعة و كفاءة عالية من قبل القائمين به، كما يتطلب في الوقت نفسه تعاونا دوليا فعالا لمحاصرة هذه الجرائم و ملاحقة مرتكبيها، لان التفتيش في البيئة الافتراضية يختلف كثيرا عن مفهومه التقليدي وإن كانت تحكمه في بعض جوانبه القواعد المألوفة في قانون الإجراءات الجزائية مثل تفتيش المساكن و المجال الذي توجد فيه أجهزة الإعلام الآلي.

5- وكما لاحظنا أيضا مشاركة عدة أطراف في عملية التفتيش والحجز عن المعطيات المعلوماتية مثل النيابة العامة، قاضي التحقيق وكذلك الضبطية القضائية و مقدمو الخدمات والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

6- المعاينة في الجريمة الالكترونية أقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الالكترونية وهذا ما تستدعيه طبيعة هذه الجريمة، كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.

7- نتيجة لخصوصية هذه الجريمة لجأ المشرع إلى استحداث قوانين تتلاءم مع الطبيعة الخاصة لهذه الجرائم من خلال إصدار القانون 09/04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى المرسوم الرئاسي رقم 15/261 المؤرخ في 08/10/2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال ومكافحتها.

8- تبين لنا أيضا أن الاتصالات الالكترونية والنظم المعلوماتية تعتبر أحد أوجه الحياة الخاصة للإنسان ومظهرا من مظاهر خصوصياته، وعليه فإن إجراءات استخلاص الدليل الرقمي من الممكن أن تؤدي إلى المساس بهذه الخصوصية والاطلاع على أسرار أشخاص قد لا تكون لهم أية صلة بالجريمة، لذلك اشترط المشرع اللجوء إلى هذه الآليات الخاصة في التحري إذا دعت الضرورة لذلك ولم تعد أساليب التحري التقليدية كافية لمحاربة هذا النوع من الجرائم المستحدثة.

9- كما أضاف المشرع في تعديله وسيلة جديدة والمتمثل في التسرب وهو إجراء خطير سبقته إليه بعض التشريعات منها التشريع الفرنسي وهو يهدف للكشف عن الجرائم الخطيرة والمتورطين فيها وتحديد هويتهم ومناطق نشاطهم و الوسائل التي يستعملونها و ضبط كل ماله علاقة بهذه الجرائم من أدلة أو قرائن.

و بناءا على هذه النتائج نستخلص مجموعة من الاقتراحات نذكر منها ما يلي:

1-إنشاء دورات تكوينية لتدريب وتأهيل قضاة التحقيق وضباط الشرطة القضائية في مجال نظم المعلوماتية والحواسيب لان دور القاضي مهم في توجيه مسار القضايا،

فإذا كان القاضي غير ملم بالجوانب التقنية الحديثة للحاسب الآلي و الانترنت، فانه لا يستطيع تقدير مدى خطورة المجرم المعلوماتي، وعليه يصدر أحكام غير متكافئة مع الجريمة المرتكبة.

2- نقترح إدراج المراسلات الالكترونية صراحة ضمن إجراء اعتراض المراسلات التي أضحت وسيلة فعالة في ارتكاب الجرائم الخطيرة في قانون الإجراءات الجزائية ليتماشى مع جاء في بها المشرع في القانون 09/04 السالف الذكر .

3-دعوة المشرع إلى تعديل المادة 56 مكرر 18 من القانون 06/22 المعدل و المتمم لقانون الإجراءات الجزائية وجعلها تسمح لضابط الشرطة القضائية المسئول عن عملية التسرب أو العون المتسرب الإدلاء بشهادته عن طريق الشاشة الالكترونية مع إمكانية تغيير الصوت والصورة.

4- استحداث جهاز على مستوى وزارة العدل لحفظ ومتابعة الهوية الحقيقة للعون المتسرب لأنه لا يكمن تصور ما يحدث له (العون المتسرب إذا توفي رئيسه المسؤول عن العملية أو تم فصله أو قام نزاع بينه وبين المتسرب، ولذلك يستحسن أن تكون هناك جهة ثانية على دراية بهويته و متابعتها.

5- يتعين إتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم الالكترونية، وذلك خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم. 6- التطرق إلى الضمانات المتعلقة بتنفيذ الإجراءات الخاصة، من هذه الضمانات تذكر مثلا إخطار الشخص بمراقبة أحاديثه بعد انتهاء عملية المراقبة تمكينه من الاطلاع عليها و مناقشتها و الاعتراض عليها خلال التحقيق الابتدائي خلو قانون إجراءات الجزائية من بيان مصير التسجيلات المتحصل عليها بعد إنهاء العملية.

وهكذا يكون البحث قد اكتمل بحمد الله وعونه ولا يسعنا سوى القول إن كان فيه من الحسن والصواب فهو من الله سبحانه وتعالى، وإن كان فيه نقص أو قصور فهو منا، ولما لا ونحن بشر نجتهد ونخطي ونصيب فإن أصبنا فأجرنا على الله وإن أخطانا فندعوه ألا

يحرمنا أجر المجتهدين، مصداقا لقول نبينا الكريم " إذا اجتهد العالم فأصاب فله أجران و إن اجتهد وأخطأ فله أجر .

تم بحمد الله

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا/ المصادر

القرآن الكريم

القرءان الكريم برواية ورش

أ: القواميس

1. ابن منظور أبو الفضل جمال الدين مكرم: لسان العرب، دار صادر، بيروت، ط 3، ج 12، س 1414هـ 1993م.
2. محي الدين الفيروزي الأبادي: القاموس المحيط، دار الكتب العلمية، بيروت، س 2007.

ب: القوانين

1. القانون رقم 04 – 15 ، الصادر في 10 نوفمبر 2004 ، معدل و متمم للأمر رقم 156/66 ، الصادر في جوان 1966 ، المتضمن قانون العقوبات، ج ر العدد 71.
2. قانون الإجراءات الجزائية المعدل والمتمم للأمر 66- 155 المؤرخ في08 جوان 1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم.
3. قانون رقم 01/06 المؤرخ في 20 فبراير 2006 ، يتعلق بالوقاية من الفساد ومكافحته ح ، ر ، عدد 14 مؤرخ في 08 مارس 2006 ، معدل ومتمم إلى غاية سنة 2011 بالقانون رقم 15/11 مؤرخ في 02 غشت 2001 ج ر ، عدد 44 مؤرخ في 10 غشت 2011.
4. القانون رقم 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، جريدة رسمية العدد 47.

ج: المراسيم الرئاسية

1-المرسوم رقم 11- 426 المؤرخ في 13 محرم 1493 الموافق لـ 08 ديسمبر 2011 يحدد تشكيلة الديوان المركزي للفساد وتنظيمه وكيفيات سيره.

2-المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة 1436 الموافق ل 08 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة في 18 أكتوبر 2015.

ثانيا/ المراجع

أ: الكتب

1-أحسن بوسقيعة: التحقيق القضائي، دار هومة للطباعة والنشر والتوزيع، ط7، الجزائر، 2008.

2-أحسن بوسقيعة: الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، ط 1، الجزائر، 2002.

3-أحسن بوسقيعة: الوجيز في القانون الجزائي العام، دار هومة، ط3 ، الجزائر، س 2006.

4-أسامة احمد المناعسة، جلال محمد الزعبي: جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان، س 2014.

5- إبراهيم بلعليات: أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط الأولى، دار الخلدونية، الجزائر، س 2007.

6-حنان ريحان مبارك المضحاكي: الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، س 2014.

7-خالد ممدوح إبراهيم: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، الإسكندرية، 2010.

8-خالد ممدوح ابراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، ط2 ، الإسكندرية، مصر، 2019.

9-خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

10- زبيدة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، س 2011 .

11- سامي على حامد عياد :الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، س 2008.

12- محمد العريان: الجرائم المعلوماتية، كلية الحقوق، جامعة الإسكندرية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004

13- عادل عبد العالي إبراهيم خراشي: إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلبِ عليها، دار الجامعة الجديدة، الإسكندرية، س 2015.

14- عبد العالي خواشي: ضوابط التحري والاستدلال عن الجرائم في الفقه الإسلامي والقانون الوضعي ، دار الجامعة للنشر ، الإسكندرية ، مصر 2006

15- عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الفكر الجامعي، الإسكندرية، 2006.

16- عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، س 2006.

17- عبد الفتاح بيومي حجازي: مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي، دار النهضة العربية، مصر، س 2009.

18- عبد الفتاح مراد: دور الكمبيوتر في مجال ارتكاب الجرائم الإلكترونية ، شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية .

19- عبد المجيد جباري: دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة ، دار هومة ، الجزائر ، 2012.

20- علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة الالكترونية، المكتب الجامعي، الإسكندرية.

21- عمر خوري: شرح قانون الإجراءات الجزائية، دار هومة ، الجزائر، 2007.

22- غنية بالطي: الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، س 2015.

23- فضيل العيش: شرح قانون الإجراءات الجزائية النظرية والعلمية، د ط، دار البدر، الجزائر، 2010.

24- قورة نائلة: جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، س 2004.

25- محمود نجيب حسني: شرح قانون العقوبات، دار النهضة العربية، القاهرة، س 1992.

26- مصطفى محمد موسى: المراقبة الالكترونية عبر شبكة الانترنيت، دراسة مقارنة بين المراقبة الأمنية والتقليدية والالكترونية، كتاب 05، دار الكتب والوثائق القومية، مصر، القاهرة، 2003.

ب: الرسائل الجامعية

1: الدكتوراه

1- حسين ربيعي: آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، جامعة باتنة، 2016-2017.

2- عمارة فوزي: قاضي التحقيق، أطروحة دكتوراه في العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2010/009.

3- هبة نبيلة هروال: جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013.

الماجستير

1- سعيد نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في العلم القانونية، جامعة الحاج لخضر، باتنة، 2012-2013.

2- سفيان سوير: جرائم المعلوماتية ، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية و علم الإجرام ، جامعة أبو بكر بلقايد، تلمسان ، س 2010- 2011 .

3- عبد اللطيف معتوق: الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير، س 2011-2012.

4- فتيحة رصاع: الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، س2011 -2012.

5- نسيمة جدي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير في القانون، كلية الحقوق، جامعة وهران، الجزائر، س 2014.

6- نهلا عبد القادر المومني: ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع، 1429هـ -2008، الطبعة الأولى، الاصدار الأول، س 2008.

7- يوسف صغير: الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013.

2: الماستر

1- ابتسام بوبعابية: التحقيق في الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون الاعلام الآلي والأنترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر س 2022/2021.

2- حليمة بن بنونة: سلطات الضبط القضائي في قانون الإجراءات الجزائية ، مذكرة لنيل شهادة الماستر ،جامعة المجيد بن باديس ، مستغانم، 2014-2015.

3- عائشة نايري: الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، س 2016- 2017.

4- عبد الرؤوف بوديسة بجاد: آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة ماستر مهني في الحقوق تخصص قانون الاعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، س 2021، 2022.

ج: المقالات العلمية

1-اسمهان بوضياف: الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، الجزائر، ج ر العدد 11، س 2018 .

2-أمنة أمحمدي بوزينة: إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مداخلة مشارك به في ملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 2007.

3-آمنة امحمدي بوزينة: خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببلوفيليا لدراسة المكتبات و

المعلومات، جامعة العربي التبسي، تبسة، الجزائر، المجلد 02 ج ر ،العدد 05، مارس 2020.

4-راضية عيمور: الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية، المجلد 6، العدد الأول، جامعة الأغواط ، 2022.

5-رعد فجر فتح، ياسر عواد: أثبات الجريمة الإلكترونية بالدليل العلمي، مجلة تكريت للحقوق، المجلد 1، ج ر العدد 2، الجزء 4.

6-سرحان حسن المعيني: التحقيق في الجرائم تقنية المعلومات، الفكر الشرطي، المجلد 20، العدد 04، رقم 79 الشارقة، الإمارات العربية المتحدة، 2011

7-سمية عكور: الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانون والأمني، الملتقى العلمي "حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الاستراتيجية، الأردن، 02-04-09- س 2016.

8- سبع زيان، سلمى المفتي: صور وأركان الجريمة المنظمة، دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد13، العدد 3 ،2020.

9-شهرزاد بولحية: تحديات الجريمة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدارسات القانونية والسياسية – المجلد 04 – العدد 02 – السنة 2019.

10- صالح شنين: التسليم المراقب في التشريع الجزائري واقع و تحديات، المجلة الالكترونية للبحث القانوني، المجلد12، العدد02، جامعة عبد الرحمان ميرة، بجاية، 2015.

11- عز الدين عثماني: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دار البحوث والدراسات القانونية والسياسية، العدد 04، تبسة، جانفي 2018.

12- عفاف بعون ، نسيمة أولاد سالم: الجريمة الإلكترونية – قراءة سوسيوتارخية في النشأة والآثار، مجلة القبس للدراسات النفسية والاجتماعية، المجلد05 ، جامعة قاصدي مرباح، العدد 20، سنة 2023.

13- علاوة هوام: التسرب كإلية للكشف عن جرائم في القانون الجزائري، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012

14- لوجاني نور الدين: أساليب التحري الخاصة و إجراءاتها ،ورقة بحثية مقدمة في اليوم الدراسي حول : علاقة النيابة العامة بالشرطة القضائية، اليزي، 2008/12/12.

15- محمد معسكر: مقال بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته، متوفر على الموقع التالي: .http//www.isecurity.org

16- معزيز أمينة: التسرب في قانون الإجراءات الجزائية ، مجلة القانون والمجتمع ، جامعة مستغانم ، د س .

17- هدى زوزو: التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد 11، جوان 2014.

فهرس الموضوعات

شكر	**–**
الإهداء	**–**
مقدمة.....	**07**
الفصل الأول: ماهية الجريمة الالكترونية	**16**
المبحث الأول: مفهوم الجريمة الإلكترونية.....	**17**
المطلب الأول: تعريف الجريمة الإلكترونية	**17**
الفرع الأول: تعريف الجريمة الإلكترونية لغة.....	**18**
الفرع الثاني: تعريف الجريمة الإلكترونية إصطلاحا.....	**19**
المطلب الثاني: خصائص وتطور الجريمة الإلكترونية	**22**
الفرع الأول: خصائص الجريمة الإلكترونية.....	**23**
الفرع الثاني: تطور الجريمة الإلكترونية.....	**25**
المبحث الثاني: التكييف القانوني للجريمة الإلكترونية وأركانها	**27**
المطلب الأول: التكييف القانوني للجريمة الإلكترونية.....	**28**
الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي	**29**
الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي.....	**33**
المطلب الثاني: أركان الجريمة الإلكترونية	**36**
الفرع الأول: الركن المادي.....	**36**
الفرع الثاني: الركن المعنوي.....	**38**
الفرع الثالث: الركن الشرعي.....	**40**
خلاصة الفصل الأول	**42**
الفصل الثاني: النظام القانوني للتحقيق الجنائي الالكتروني	**44**
المبحث الأول: ماهية التحقيق الجنائي الالكتروني.....	**45**
المطب الأول: تعريف التحقيق الجنائي الالكتروني.....	**45**
الفرع الأول: تعريف التحقيق الجنائي الالكتروني.....	**46**

الفرع الثاني: شروط التحقيق في الجريمة الالكترونية.....	**48**
الفرع الثالث: الفرق بين التحقيق الالكتروني والعادي التقليدي.....	**49**
المطلب الثاني: عناصر التحقيق في الجريمة الالكترونية.....	**49**
الفرع الأول: إظهار الركن المادي للجرائم الالكترونية.....	**50**
الفرع الثاني: إظهار الركن المعنوي للجرائم الالكترونية.....	**50**
المطلب الثالث: الأجهزة المكلفة بالتحقيق في الجرائم الالكترونية.....	**51**
الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الالكترونية.....	**52**
الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية	**53**
المبحث الثاني: الإجراءات المستحدثة الخاصة بالتحقيق الالكتروني.....	**55**
المطلب الأول: التسرب الالكتروني.....	**56**
الفرع الأول: تعريف التسرب الالكتروني.....	**56**
الفرع الثاني: شروط صحة التسرب.....	**57**
الفرع الثالث: صور التسرب وآثاره.....	**63**
المطلب الثاني: التسليم المراقب.....	**67**
الفرع الأول: تعريف التسليم المراقب.....	**67**
الفرع الثاني: شروط التسليم المراقب.....	**68**
الفرع الثالث: مجال التسليم المراقب.....	**69**
خلاصة الفصل الثاني.....	**71**
الخاتمة	**73**
قائمة المراجع	**79**
الفهرس.....	**–**
الملخص.....	**–**

ملخص

الجريمة الإلكترونية تشير إلى الأفعال الإجرامية التي تتم باستخدام الإنترنت أو الأجهزة الإلكترونية. تتنوع هذه الجرائم من الاحتيال الإلكتروني، وسرقة الهوية، إلى الهجمات التي تستهدف شبكات الكمبيوتر والبيانات الشخصية.

التحقيق في هذه الجرائم يتطلب مهارات تقنية متخصصة لجمع الأدلة الرقمية بشكل قانوني وفعال، وتحليلها لتعقب الجناة، يعتمد التحقيق على التعاون بين الأجهزة الأمنية المحلية والدولية للتعامل مع التحديات التي تفرضها طبيعة هذه الجرائم المعقدة والعابرة للحدود، الهدف هو ليس فقط معاقبة الجناة بل أيضًا فهم أساليبهم لتطوير طرق أفضل للوقاية من هذه الجرائم مستقبلاً

Abstract

Cybercrime refers to criminal activities carried out using the internet or electronic devices. These crimes range from online fraud and identity theft to attacks targeting computer networks and personal data.

Investigating these crimes requires specialized technical skills to legally and effectively collect digital evidence and analyze it to track down perpetrators. The investigation relies on collaboration between local and international law enforcement agencies to address the challenges posed by the complex and transnational nature of these crimes. The goal is not only to prosecute offenders but also to understand their methods to develop better ways to prevent such crimes in the future.