جامعة أكلي محند اولحاج-البويرة

كلية الحقوق والعلوم السياسية

قسم القانون العام

إنعكاسات خصوصية الجريمة المعلوماتية على إجراءات المتابعة في ظل قانون 14/25

مذكرة تخرج لنيل شهادة ماستر في الحقوق

تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبتين:

- حمادو إكرام
- يوس شهيرة

تحت إشراف الأستاذ:

- د.عتيق حنان

لجنة المناقشة

خليفي سمير _____رئيسا

عتيق حنان _____مشرفا و مقررا

زعادي محمد جلول _____ مناقشا

السنة الجامعية: 2025-2026

شكر وعرفان

في البداية نشكر الله عز وجل الذي اعطانا القوة للإتمام هذا العمل العلمي المتواضع.

ثم نتوجه بجزيل الشكر والامتنان الى الأستاذة الفاضلة عتيق حنان لقبولها الاشراف على هذه المذكرة اذ لم تبخل علينا بإرشاداتها وتوجهاتها القيمة لإثراء هذا العمل رغم التزاماتها الكثيرة.

كما اشكر أعضاء اللجنة الموقرة كل باسمه وصفته على قبولهم مناقشة هذه المذكرة.

ولا أنسى ان اشكر كل من قدم لي يد العون سواء من قريب او بعيد في انجار هذا العمل.

يوس شهيرة

حمادو إكرام

اهداء

اهدي تخرجي الى اليد الخفية والقلب الحنون صاحبة الدعاء الى من كانت سببا في وجودي

"امي الغالية"

الى من علمني القوة ومن اراه بعيني سندا لا يميل القائد الملهم

" ابي الغالي"

الى اخواتي واخوتي

أنتم القوة التي كانت خلفي دوما والدعم الذي لم يخذلني بحبكم وصبركم وتشجيعكم أكملت الطريق

الى رفيق الروح والدرب

لقد كنت دائما الضوء الذي يهديني والصوت الذي يدعمني على أنك قادرة على إتمام حلمك فالحقيقة هذا الإنجاز هو لك أيضا

الى ملاكي الصغيرة

اميرتي الحبيبة وجودك كان أكبر داعم لي شكرا على كل للحظة شكرا على كل كلمة شكرا اهديك هذا البحث العلمي ليكون بذرة في قلبك الصغير بان أمك تفخر بك وتطمح لتصنع مستقبلك بالعلم.

الى عائلتي الثانية اسرة زوجي

التي كانت اقوى سند وعون لي خلال مسيرتي العلمية اهديكم هذا العمل المتواضع كعربون تقدير وامتنان ***يوس شهيرة***

اهداء

هذه اللحظة ***لا تورث ولا تشترى، لقد دفعت ثمنها عمري خوفي، ودموعي، هي لهفة الوصول ودمعة الحزن فرحة العمر هذه هي النهاية السعيدة لبدايات*** أعظم ***وأصبح حلمي حقيقة.***

أهدي تخرجي إلى من هم كل ما أملك إلى العمود الثابت في عثرات أيامي إلى من هم في الحياة حياة إلى من بذلو جهد السنين من أجلي "أمي وأبي."

كما أهدي تخرجي إلى أختي، إلى من وقفت بجانبي في السراء والضراء ولكل روح عانقتني بالحب والدعوات.

شكراً لكل من كان في طريقي استندت عليه أو مر عابراً، شكراً لكل من علمني كلمة أو مهارة.

حمادو إكرام

قائمة المختصرات

ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري

ق.ع: قانون العقوبات

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الديمقراطية الشعبية

د.ذ.س.ن: دون ذكر سنة النشر

ص: صفحة

ص.ص: من صفحة إلى صفحة

ط: طبعة

ج: جزء

ع: عدد

مقدمة

يشهد العالم في المرحلة الراهنة تطورا فكريا ومعرفيا غير مسبوق نتيجة الثورة العلمية والتكنولوجية التي عرفها مجال الاتصالات والمعلومات، والتي أسهمت في إحداث نقلة نوعية شاملة مست مختلف مجالات الحياة الاقتصادية والاجتماعية والثقافية والعلمية وقد ترتب عن هذا التطور تراجع أثر الحدود السياسية والحواجز الجغرافية بين الدول والشعوب بفعل ما وفرته التكنولوجيا الحديثة من وسائل متطورة تعتمد على السرعة والدقة في جمع المعلومات ومعالجتها وتخزينها ثم نقلها وتبادلها عبر مختلف أنحاء العالم.

كما أدت هذه الثورة إلى تقليص المسافات واختزال الزمن، حتى أصبح العالم أشبه بقرية إلكترونية مترابطة في فضاء رقمي موحد ولهذا ذهب العديد من الباحثين والمفكرين إلى اعتبار الثورة المعلوماتية بمثابة الثورة الصناعية الثانية، مقارنة بالثورة الصناعية الأولى التي شهدها أواخر القرن التاسع عشر؛ إذ تمثل الهدف الأساسي للأولى في إحلال الآلة محل الجهد البدني للإنسان، في حين تهدف الثورة الثانية إلى إحلال التكنولوجيا والأنظمة الذكية محل جانب كبير من النشاط الذهني والمعرفي للإنسان.

ولا شك في أن الثورة المعلوماتية الحديثة قد تركت آثارا إيجابية بارزة على مختلف جوانب الحياة المعاصرة لما وفرته من وسائل تقنية أسهمت في اختصار الوقت وتقليل الجهد والتكلفة، وجعلت من أداء الأنشطة اليومية أكثر سهولة وفعالية وقد أدى ذلك إلى تزايد الإقبال على التقنيات المرتبطة بهذه الثورة وعلى رأسها الحواسيب الآلية والشبكات المعلوماتية مع اتساع نطاق استخدامها في مختلف المجالات والقطاعات.

كما تعزز الاعتماد على هذه التقنيات بصورة متزايدة داخل المؤسسات العامة والخاصة إلى درجة أصبحت فيها أداة أساسية لا غنى عنها في تسيير الأعمال وممارسة الأنشطة المختلفة الأمر الذي جعل الأداء الوظيفي والإداري والاقتصادي لهذه القطاعات مرتبطا ارتباطا وثيقا بمدى كفاءة واستمرارية الأنظمة المعلوماتية الحديثة.

وعلى الرغم من المزايا والفوائد العديدة التي أفرزتها تكنولوجيات المعلومات والاتصال وما حققته من تطور ملموس في مختلف مجالات الحياة، فإن التوسع المتزايد في استخدامها أفرز في المقابل جملة من الآثار السلبية التي باتت تشكل تهديدا حقيقيا لأمن المجتمع

واستقراره ويرجع ذلك إلى إساءة استعمال هذه التقنيات واستغلالها بطرق غير مشروعة تمس بمصالح الأفراد والجماعات وتلحق الضرر بحقوقهم وممتلكاتهم.

وقد ترتب عن هذا الوضع ظهور نمط جديد من الجرائم المستحدثة لم يكن معروفا بالصورة التي هو عليها اليوم أطلق عليه مصطلح جرائم تقنية المعلومات أو الجرائم الإلكترونية، وهي جرائم ترتكب باستخدام الوسائل الإلكترونية والأنظمة المعلوماتية مستفيدة من التطور التكنولوجي والانتشار الواسع لشبكات الاتصال الحديثة.

ولا خلاف في أن الجريمة الإلكترونية تعد من أخطر الجرائم وأكثرها تعقيدا في العصر الحديث إذ تتصدر صور الجريمة المنظمة المستحدثة لما تنطوي عليه من خصوصية وتميز في بنيتها القانونية والتقنية وتكمن خطورة هذا النوع من الجرائم في الطبيعة غير التقليدية لأركانها وحداثة الوسائل المستخدمة في ارتكابها فضلا عن البيئة الرقمية التي تقع فيها وما تتطلبه من أساليب خاصة للكشف والإثبات.

فالجريمة الإلكترونية هي جريمة ذات طابع تقني يسهل ارتكابها في بيئة افتراضية خفية قوامها إشارات وذبذبات إلكترونية تنتقل عبر أنظمة المعالجة الآلية للمعلومات وشبكات الاتصال دون أن تترك آثارا مادية محسوسة بالمعنى التقليدي كما أن مرتكبيها غالبا ما يتمتعون بقدر عال من الذكاء والخبرة التقنية والمعرفة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات بما يمكنهم من استغلال الوسائل التقنية الحديثة لتحقيق أغراض غير مشروعة.

وتزداد خطورة هذه الجرائم لكونها عابرة للحدود الوطنية إذ ترتكب عبر شبكة اتصالات عالمية غير مادية وغير مرئية، متاحة لمختلف الأشخاص في أنحاء العالم ولا تخضع لسيادة دولة بعينها الأمر الذي يجعل السلوك الإجرامي فيها متجاوزا للمفهوم التقليدي للمكان ويثير تحديات قانونية وإجرائية تتعلق بالاختصاص القضائي وآليات الملاحقة والإثبات.

أفضت الخصائص المميزة للجريمة الإلكترونية إلى تعقيد عملية مواجهة الأنشطة الإجرامية المستحدثة وإلى صعوبة إخضاعها لأحكام النصوص الجنائية التقليدية أو تكييفها وفق

القواعد القانونية القائمة لما قد يترتب على ذلك من مساس بمبدأ الشرعية الجنائية، وما يفرضه من ضرورة التفسير الضيق للنصوص الجزائية وحظر القياس في المجال الجنائي.

حمل هذا الواقع المشرع الجزائي مسؤولية جسيمة تقتضي التدخل التشريعي لمواكبة التطور التكنولوجي ومواجهة الجرائم الناشئة عن إساءة استخدام الأنظمة المعلوماتية. ويتحقق ذلك من خلال استحداث نصوص قانونية خاصة تتلائم مع طبيعة الجرائم الإلكترونية وخصوصيتها بما يضمن توفير الحماية الجنائية الفعالة للمصالح محل الاعتداء.

كما يهدف هذا التدخل التشريعي إلى تمكين أجهزة العدالة الجنائية من تطوير الآليات والإجراءات الكفيلة بالتصدي للجرائم التي أفرزتها تكنولوجيا الإعلام والاتصال والاستفادة من الوسائل التقنية الحديثة في كشف هذه الجرائم وإثباتها وتعقب مرتكبيها بما يضمن تقديمهم إلى العدالة وتحقيق فعالية السياسة الجنائية في البيئة الرقمية.

ومن هنا تتجلى أهمية هذا الموضوع **انعكاسات خصوصية الجريمة المعلوماتية على إجراءات المتابعة** وسبب اختيارنا لهذا الموضوع رغم ما يحيط به من صعوبات وإشكالات أساسا إلى حداثته وما يتسم به من طابع علمي وتقني دقيق كما أن أغلب الدراسات والأبحاث القانونية التي تناولت الجرائم الإلكترونية انصرفت إلى الجانب الموضوعي منها، في حين ظل الجانب الإجرائي يعاني من قلة وندرة المراجع والمؤلفات المتخصصة وقد كان لذلك أثر بالغ في إثارة اهتمامنا للبحث في هذا الموضوع وإثراء النقاش القانوني حوله، من خلال السعي إلى تحقيق مقصدين أساسيين؛ أولهما مقصد نظري يتمثل في دراسة الجرائم الإلكترونية أما المقصد الثاني ينبع من كون هذه الدراسة تأتي في مرحلة تتجه فيها العديد من الدول بما فيها الجزائر، إلى إعادة النظر في قوانين الإجراءات الجزائية وتحديثها بما يتلاءم مع المستجدات التقنية المعاصرة. كما تهدف الى ابراز خصوصية الجريمة المعلوماتية وكذا ابراز الإجراءات المتبعة في الكشف عن هذه الجريمة، كما تهدف أيضا هذه الدراسة الى تقديم اضافة علمية تثري الرصيد القانوني في مجال الجريمة الالكترونية ومحاولة وضع مرجع حديث في متناول الطلبة والباحثين بالإضافة الى سد ثغرة نقص المراجع المتخصصة المرتبطة بالقانون الجديد.

ومن بين دوافع اختيارنا لهذا الموضوع يكمن في شغفنا للاطلاع على كل ما يخص الجريمة المعلوماتية خاصة فيما يخص إجراءات المتابعة المستحدثة، بالإضافة الى السعي للإلمام بمختلف جوانب موضوع الدراسة كونه لم يسبق الإحالة اليه في الدراسات السابقة وكذا الرغبة في التطرق لموضوع معاصر يواكب التحولات الرقمية

اما بالنسبة للإشكالية التي يطرحها موضوع دراستنا في تنصب أساسا حول التطور السائد في المجال التكنولوجي والتزايد الهائل على استخدام البرامج المعلوماتية سواءا من قبل اشخاص طبيعية او اعتبارية كل هذا أدى الى بروز أنماط جديدة للإجرام المرتبطة بالتكنولوجيا في الآونة الأخيرة.

وبالتالي ارتئينا الى طرح الإشكالية الاتية

كيف تنعكس خصوصية الجريمة المعلوماتية على إجراءات المتابعة في ظل قانون إجراءات الجزائية ؟

وللاجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي التحليلي الذي يقوم على تسليط الضوء على خصوصية الجريمة المعلوماتية وتحليل إجراءات المتابعة الجزائية المرتبطة بها.

ونتبع في ذلك خطة تتضمن فصلين يتضمن الفصل الأول خصوصية الجريمة المعلوماتية وذلك من خلال التأكد في المبحث الأول من ماهية الجريمة المعلوماتية واهم أنواعها اما بالنسبة للمبحث الثاني خصصناه الى اهم خصائها وعرجنا في الفصل الثاني الى أبرز إجراءات المتابعة في الجريمة المعلوماتية من خلال ق.ا.ج.ج.

الفصل الأول:
خصوصية الجريمة المعلوماتية

لقد أفرز التطور التكنولوجي السريع في مختلف مجالات الحياة ظواهر إجرامية مستحدثة في مقدمتها الجريمة المعلوماتية التي باتت تشكل تهديدا حقيقيا لمصالح الأفراد والمؤسسات والدول على حد سواء وقد أصبحت هذه الجريمة محل اهتمام متزايد من قبل الفقهاء والمشرعين نظرا لما تطرحه من إشكالات قانونية وعملية خاصة فيما يتعلق بتحديد مفهومها وضبط نطاقها القانوني.

وقد ترتب عن هذا الاهتمام تعدد المصطلحات المستعملة للدلالة عليها منها: جرائم الحاسب الآلي، جرائم التقنية العالية، الجرائم المعلوماتية، جرائم الغش المعلوماتي وجرائم الإنترنت الأمر الذي يعكس غياب اتفاق موحد حول مفهوم دقيق لها ويعد هذا التباين من أبرز الإشكالات التي تواجه هذا المجال حيث اختلفت الاتجاهات الفقهية في تعريفها ولم يتم التوصل إلى إجماع شامل بشأنها وهو ما زاد من تعقيد معالجتها القانونية.

وتبرز أهمية الإحاطة بالجريمة المعلوماتية من خلال التطرق إلى إطارها المفاهيمي بالنظر إلى الطابع المستحدث الذي يميزها وما يفرضه ذلك من ضرورة تحديد معالمها الأساسية وتمييزها عن غيرها من الجرائم التقليدية إذ يقتضي الأمر الوقوف عند مختلف التعريفات الفقهية والتشريعية التي حاولت ضبط مفهومها مع إبراز خصائصها وأنواعها، بما يسمح بتكوين تصور واضح ودقيق حولها. وعليه سيتم في (المبحث الأول) دراسة ماهية الجريمة المعلوماتية من خلال تحديد مفهومها وبيان اهم أنواعها.

ولا تقتصر دراسة الجريمة المعلوماتية على الجانب المفاهيمي فحسب بل تمتد إلى إبراز خصوصيتها التي تجعلها تختلف عن الجرائم التقليدية سواء من حيث طبيعتها غير المادية أو الوسائل التقنية المعتمدة في ارتكابها أو طابعها العابر للحدود وهو ما يفرض تحديات حقيقية أمام القواعد القانونية التقليدية ويستدعي تكييفها لمواكبة هذه المستجدات وهذا ما سيتم دراسته في (المبحث الثاني) .

المبحث الأول:
الإطار المفاهيمي للجريمة المعلوماتية

يشهد العالم اليوم تطورا متسارعا في مجال التكنولوجيا الحديثة حيث أوجدت هذه القفزة وسائل جديدة تسهل على الفرد حياته اليومية في مختلف معاملاته الاقتصادية والتجارية والاجتماعية غير أن هذا التطور وما نتج عنه من انتشار الحاسب الآلي والأجهزة الإلكترونية قد ساهم أيضا في ظهور أنماط جديدة من الجرائم من أبرزها الجريمة المعلوماتية وتتميز هذه الجريمة بارتباطها الوثيق بالبيئة الرقمية مما يمنحها طابعا خاصا يميزها عن الجرائم التقليدية سواء من حيث الوسائل المستعملة أو طبيعة الأفعال المرتكبة كما أن انتشار شبكة الإنترنت ساهم في تسهيل ارتكابها وزاد من صعوبة اكتشافها وإثباته الأمر الذي يبرز خطورتها على الأفراد والمؤسسات.

وفي هذا المبحث سنتناول ماهية الجريمة المعلوماتية وذلك من خلال تخصيص

(المطلب الأول) لبيان مفهومها على أن يعالج (المطلب الثاني) أنواعها.

المطلب الأول:
مفهوم الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتقنية حديثة في تكنولوجيا المعلومات وقد احاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية الى تحديد تعريف جامع وموحد لها، فالفقه لم يتفق على تعريف بحجة أن هذا النوع من الجرائم ما هو الا جريمة ترتكب بأسلوب الكتروني وتختلف الجريمة المعلوماتية عن الجريمة التقليدية في الوسيلة المستعملة لارتكابها، وهو ما سنحاول تبيانه من تعريف الجريمة المعلوماتية قانونا (الفرع الأول) والتعريف الفقهي من خلال (الفرع الثاني).

الفرع الاول: التعريف القانوني للجريمة المعلوماتية

اشار المشرع الجزائري إلى الجريمة الإلكترونية من خلال المواد 335 الى 338 من ق.ا.ج.ج ويقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال أي جريمة ترتكب او يسهل ارتكابها استعمال منظومة معلوماتية او نظام للاتصالات الالكترونية او أي وسيلة أخرى او الية ذات صلة بتكنولوجيات الاعلام والاتصال.[1]

09-04 الذي وضع قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها.[2]

ويجدر التنويه إلى أن مصطلح "نظام المعالجة الآلية للمعطيات" يعد تعبيرا ذا طبيعة تقنية وفنية يصعب على القانوني إدراك مغزاه بشكل مباشر فضلا عن كونه مفهوما متطورا يخضع للتغيرات السريعة والمتلاحقة في مجال الحوسبة والأنظمة المعلوماتية. [3]

اشار المشرع الجزائري الى مختلف الجرائم المرتبطة بالمساس بأنظمة المعالجة الآلية للمعطيات في القانون رقم 24-06 المتضمن ق.ع.ج وذلك من خلال المواد من 394مكرر الى 394 مكرر7وتتمثل هذه الجرائم في أصلها في الدخول أو البقاء بالغش في أي جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك وكذا حذف أو تغيير معطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع تعطيل أو تخريب نظام اشتغالها. [4]

---

[1] انظر المواد 335-338 من قانون رقم 25-14 المتضمن ق.ا.ج.ج.

[2] القانون 09-04 المؤرخ في 14شعبان عام 1430 الموافق 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقابة من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر.ج.ج العدد 47 الصادرة بتاريخ 25 شعبان 1430 الموافق 16 غشت 2029.

[3] عبد الرؤوف بجاد بوديسة، اليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة برج بوعريرج، الجزائر، السنة 2021/2020، ص10.

[4] القانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق ل 28ابريل 2024 المعدل والمتمم للأمر رقم 66-155 المتضمن ق.ع، ج.ر.ج.ج العدد 30الصادرة بتاريخ 21شوال عام 1445 الموافق ل 30ابريل 2024.

وعليه من خلال هذه النصوص، يتضح أن المشرع الجزائري لم يضع تعريفا جامعا ومباشرا للجريمة المعلوماتية وإنما اكتفى بتحديد صور الأفعال المجرمة المرتبطة بالمساس بأنظمة الآلية للمعطيات وبالتالي يمكن القول إن الجريمة الإلكترونية وفق القانون رقم 15-04 هي:

كل فعل غير مشروع يتمثل في الدخول أو البقاء أو التلاعب أو الاتجار بالمعطيات داخل منظومة معلوماتية، بما يؤدي إلى المساس بسلامة وأمن أنظمة المعالجة الآلية للمعطيات.

ومن هذا المنطلق نستنتج بان ق.ع.ج المعدل والمتمم لم يتضمن تعريفا صريحا للجريمة المعلوماتية بل اقتصر على تجريم بعض الأفعال تحت عنوان الجرائم الماسة بأنظمة المعالجة الالية للمعطيات.

غير أنه في المادة الثانية من القانون رقم 04/09 قدم تعريفا لهذه الجرائم مستعملا مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث نص على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات، أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[1] ."

يستشف من التعريف الذي اعتمده المشرع الجزائري للجريمة المعلوماتية أنه تبنى جملة من المعايير القانونية والفنية غير أنه في المادة الثانية من القانون رقم 04/09 قدم تعريفا لهذه الجرائم مستعملا مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث نص على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات، أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."

ولم يقف المشرع الجزائري عند هذا الحد بل وسع من نطاق التجريم إذ اعتبر أن الجريمة المعلوماتية ترتكب داخل نظام معلوماتي أو يسهل ارتكابها من خلاله وبهذا التوسيع يكون

[1] انظر نص المادة 02 من القانون رقم 09-04 السالف الذكر.

المشرع الجزائري قد أرسى إطارا قانونيا شاملا يهدف إلى الإحاطة بمختلف صور الجرائم المرتبطة بالتكنولوجيات الحديثة. [1]

الفرع الثاني: التعريف الفقهي للجريمة للمعلوماتية

لقد تعددت آراء الفقهاء في محاولة وضع تعريف للجريمة المعلوماتية، حيث انقسمت اتجاهاتهم بين من ركز على الوسيلة التقنية المستعملة(أولا)، ومن اعتبر المعلومة محل الاعتداء(ثانيا)، ومن رأى أنها امتداد للجرائم التقليدية بوسائل حديثة(ثالثا)، بينما ركز آخرون على النتائج والأثر المترتب عنها كتعطيل الأنظمة أو الإضرار بالمصالح الاقتصادية والاجتماعية.[2]

أولا/ تعريف الجريمة المعلوماتية نسبة لوسيلة ارتكابها

تقوم بعض التعريفات الفقهية للجريمة الإلكترونية على أساس وسيلة ارتكابها حيث ينظر إلى الحاسوب أو شبكة الإنترنت باعتبارهما الأداة الرئيسة التي تميز هذا النوع من الجرائم فقد عرفها الأستاذ جون فورستر بأنها فعل إجرامي يرتكب باستخدام الكمبيوتر كأداة وهو ما ذهب إليه أيضا الفقيه تايد مان الذي أشار إلى أنها تشمل كل أشكال السلوك غير المشروع الذي يتم عبر الحاسوب، كما وصف مكتب تقييم التقنية في الولايات المتحدة هذه الجريمة بأنها تلك التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا، بينما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية ويكون ناتجا بصورة مباشرة عن تدخل التقنية المعلوماتية.[3]

---

[1] ريمة بن عميروش، عن خصوصية الجريمة المعلوماتية، المجلة الجزائرية للأبحاث والدراسات، المجلد 02، العدد 02، الجزائر، 2021، ص77.

[2] هبة الدزيري، جريمة الدخول الغير مشروع لنظام المعالجة الالية للمعطيات، مذكرة نهاية الدراسة لنيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الحميد ابن باديس مستغانم، الجزائر، 2020، ص15.

[3] رجاء اومدر، خصوصية الجريمة التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه ل.م.د، تخصص القانون الخاص، جامعة محمد البشير الابراهيمي برج بوعريج، الجزائر، سنة 2021/2020، ص17.

ثانيا/ تعريف الجريمة المعلوماتية من حيث موضوعها

تقوم بعض التعريفات الفقهية للجريمة المعلوماتية على أساس موضوعها بعيدا عن الوسيلة المستعملة أو هوية الفاعل، حيث ينظر إليها باعتبارها اعتداء موجها إلى المال المعلوماتي المعنوي ويشمل ذلك صورا متعددة مثل القرصنة، الاستعمال غير المشروع للأنظمة المعلوماتية أو الجرائم التي تستهدف الأنظمة الإلكترونية والشبكات ويعرف هذا الاتجاه الجريمة المعلوماتية بأنها كل فعل غير مشروع يهدف إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو أنها: " شكل من أشكال الغش المعلوماتي الذي ينصرف إلى البيانات والمعطيات الإلكترونية". ومن هنا فإن موضوع الجريمة هو المعلومة ذاتها باعتبارها قيمة معنوية محمية قانونا، وليست مجرد وسيلة أو أداة تقنية وقد ذهب بعض الفقهاء إلى أبعد من ذلك معتبرين أن هذه الجرائم تمثل اعتداء على حقوق أساسية مثل حق الملكية، الحق في سلامة الشرف والاعتبار، الحق في حماية الملكية الفكرية، والحق في الحفاظ على الحياة الخاصة. بل إن الأمر قد يمتد ليشمل المساس بسلامة الجسد ذاته كما في الحالات التي يستعمل فيها الخلل الإلكتروني لإحداث أضرار مادية مثل تعطيل أنظمة الحاسب الآلي التابعة لوسائل النقل الجوي أو البحري أو السكك الحديدية إذا كان الهدف منه الإضرار بسلامة الركاب أو إزهاق أرواحهم، وهكذا يتضح أن هذا الاتجاه يركز على جوهر الاعتداء المتمثل في المعلومات وما تمثله من حقوق ومصالح دون أن يعير اهتماما كبيرا للوسيلة التقنية المستعملة مما يجعله اتجاها يربط الجريمة المعلوماتية بمحلها وموضوعها أكثر من ارتباطها بالأداة أو الفاعل.[1]

ثالثا/ تعريف الجريمة من طرف خبير تقني

يعتمد بعض الفقهاء في تعريفهم للجريمة المعلوماتية على أساس الإلمام بالمعرفة التقنية حيث ينظر إلى هذه الجرائم باعتبارها أفعالا لا يمكن تصور وقوعها إلا من طرف أشخاص يمتلكون خبرة خاصة في مجال تقنية المعلومات، ويقوم هذا الاتجاه على معيار شخصي يتمثل في ضرورة توفر تقنية المعرفة لدى الفاعل وهو ما ذهب إليه الفقي David

[1] حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات، جامعة باتنة، الجزائر،2016، ص 22.

Thompsonالذي عرف الجريمة المعلوماتية بأنها جريمة يشترط لافتراضها أن يكون مرتكبها ملما بتقنية الحاسوب، كما عرفها جانب من الفقه بأنها الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها ومقاضاة فاعليها غير أن هذا الاتجاه تعرض لعدة انتقادات أبرزها أنه يضيق من نطاق الجريمة المعلوماتية بحصرها في دائرة الأشخاص ذوي الخبرة التقنية العالية متجاهلا أن الواقع العملي يشهد بارتكاب العديد من الجرائم المعلوماتية من طرف أشخاص عاديين لا يمتلكون معرفة متقدمة وذلك بفضل انتشار البرامج الجاهزة والأدوات المساعدة التي تسهل تنفيذ هذه الأفعال دون الحاجة إلى خبرة تقنية نادرة ومن ثم فإن الاقتصار على معيار الإلمام بالمعرفة التقنية يعد تصورا أقرب إلى الخيال منه إلى الواقع لأنه يستبعد صورا عديدة من الجرائم المعلوماتية التي يمكن أن تصدر عن مستخدمين عاديين وهو ما يبرز قصور هذا الاتجاه في الإحاطة الشاملة بمفهوم الجريمة الإلكترونية.[1]

رابعا/ تعريف الجريمة المعلوماتية حسب الاتجاه المختلط

يعتمد الاتجاه المختلط في تعريف الجريمة المعلوماتية على الجمع بين محل الجريمة ووسيلة ارتكابها، حيث يرى أن هذا النوع من الجرائم لا يمكن حصره في معيار واحد بل يجب أن يشمل جميع الأفعال غير المشروعة المرتبطة بالمعلوماتية سواء كانت المعلومات هي الهدف المباشر للاعتداء أو كان الحاسوب وتقنية المعلومات وسيلة لتنفيذه، وبذلك يعتبر جهاز الكمبيوتر في الوقت نفسه وسيلة ارتكاب الجريمة وضحية لها وهو ما يمنح هذا الاتجاه شمولية أكبر مقارنة بالاتجاهات الأخرى.[2]

وفي هذا الاتجاه قدم عدد من الفقهاء تعريفات مختلفة

– فالفقيه Loff Smebing عرف الجريمة المعلوماتية بأنها "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب".

---

[1] رجاء اومدر، مرجع سابق، ص20–21.

[2] نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة من اجل الحصول على شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر،2016، ص35.

-اما الفقيه Masse الذي أضاف عنصر الهدف من ارتكاب الجريمة، فعرفها بأنها "تلك الاعتداءات التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".

- كما ذهب اتجاه آخر إلى تعريفها بأنها كل عمل أو امتناع يأتيه الإنسان ويترتب عنه إضرار بمكونات الحاسب الآلي المادية أو المعنوية وشبكات الاتصال الخاصة به باعتبارها مصالح وقيم حديثة تستوجب الحماية الجنائية.[1]

ويظهر الاتجاه أن إعطاء تعريف موسع للجريمة المعلوماتية يدخل في نطاقه كل التصرفات غير المشروعة التي لها علاقة بالحاسب الآلي، أيا كانت طبيعة هذه العلاقة وأيا كان دور الحاسوب فيها سواء كان وسيلة مناسبة لارتكاب الفعل غير المشروع أو كان موضوعا للاعتداء أو مجرد مناسبة لوقوعه، ووفقا لتعريف منظمة التعاون الاقتصادي والتنمية OECDفي استبيان الغش المعلوماتي فإن الجرائم المعلوماتية هي "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات" ويعتبر هذا التعريف أكثر شمولا من غيره لأنه لم يقتصر على الفعل الإيجابي بل شمل أيضا السلوك السلبي المتمثل في الامتناع كما أنه لم يحصر الهدف في تحقيق الربح فقط، بل أشار إلى إمكانية أن يكون الدافع إثبات الذات أو الإضرار بالغير أو غيرها من الأسباب بهذا يتضح أن الاتجاه المختلط يعد من أكثر الاتجاهات قدرة على استيعاب التطورات التقنية وصور الجرائم المستحدثة لأنه يجمع بين محل الجريمة ووسيلة ارتكابها في إطار واحد شامل.[2]

المطلب الثاني

انواع الجريمة المعلوماتية

تعد الجرائم المرتكبة عبر شبكة الإنترنت من الجرائم المستحدثة التي ظهرت نتيجة التطور التكنولوجي الهائل وهي تستهدف قطاعات متعددة مما يجعل تحديدها وتصنيفها أكثر تعقيدا

[1] نورة طرشي، نفس المرجع، ص19.

[2] عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر، 2016، ص 25.

مقارنة بالجرائم التقليدية فبينما يسهل ضبط صور الجرائم التقليدية وفق معايير واضحة فإن الجرائم المعلوماتية تتسم بالتنوع والتطور المستمر الأمر الذي يخلق صعوبة في وضع تصنيف موحد لها.

ومع ذلك فقد استقر الفقه القانوني على اعتماد تصنيف عام لهذه الجرائم يقوم على التمييز بين الحالات التي تكون فيها المعلوماتية وسيلة لارتكاب الجريمة وبين الحالات التي تكون فيها المعلوماتية نفسها هدفا للاعتداء، وبناء على هذا التصنيف يمكن تقسيم الجرائم المعلوماتية إلى صور رئيسية سنتناولها بالتحليل في الفروع اللاحقة.

الفرع الاول: الاعتداءات على النظام المعلوماتي

تعتبر الجرائم المعلوماتية من أبرز صور الإجرام المستحدث حيث يشكل النظام المعلوماتي الوسيلة الأساسية لارتكابها ومن أهم صور هذه الجرائم:

اولا: جريمة الدخول أو البقاء غير المشروع في المنظومة المعلوماتية

يقصد بالدخول غير المشروع عملية الولوج إلى منظومة معلوماتية بطريقة غير شرعية وهو ما اعتبره المشرع الجزائري جريمة قائمة بذاتها، إذ يعد مجرد اختراق جهاز الحاسب الآلي أو الشبكة المعلوماتية انتهاكا للنظام المعلوماتي سواء كان الهدف الوصول إلى البيانات أو مجرد التسلية، وتتحقق هذه الجريمة بمجرد الدخول إلى النظام المعلوماتي بطريق الغش فهي جريمة عمدية يشترط فيها توافر القصد الجنائي العام أي أن يكون الجاني على علم بأنه يدخل إلى منظومة معلوماتية لا تخصه ويستخلص من نص المادة 394 مكرر من قانون العقوبات الجزائري أن الجريمة قائمة حتى لو لم يترتب عنها أي ضرر بالمعلومات.[1]

ويلاحظ من نص المادة 394 مكرر من قانون العقوبات الجزائري على انه تم تجريم كل من يقوم بالدخول أو البقاء في المنظومة المعلوماتية بطريقة غير مشروعة،اذ أن المشرع ميز بين فعل الدخول غير المشروع وفعل البقاء دون سند قانوني أو مصلحة مشروعة حيث

[1] تنص المادة 394 مكرر من ق.ع.ج. على انه" يعاقب بالحبس من 6اشهر الى سنتين وبغرامة من 60.000 دج الى 200.000 دج كل من يدخل او يبقى عن طريق الغش في كل او جزء من منظومة للمعالجة الالية للمعطيات او يحاول ذلك"

اعتبر أن الدخول إذا كان عن طريق الخطأ لا يشكل جريمة بينما البقاء عن قصد يعد جريمة قائمة بذاتها لأنه يعكس إرادة الجاني في الإضرار بالغير.[1]

ويستدل من ذلك على أن البقاء داخل النظام المعلوماتي يتطلب توافر الركن المعنوي للجريمة والمتمثل في القصد الجنائي، أي أن يكون الجاني مدركا أنه يستمر في التواجد داخل منظومة لا تخصه دون وجه حق ولم يحدد القانون المقارن بدقة اللحظة التي تنتهي فيها جريمة الدخول وتبدأ جريمة البقاء، غير أن بعض الفقه اعتبر أن بداية الجريمة تكون منذ اللحظة التي يبدأ فيها الجاني بالتجول داخل النظام المعلوماتي مستهدفا المعطيات أو المعدات المرتبطة به[2] وقد يترتب على هذا السلوك غير المشروع نتائج خطيرة مثل:

-حذف أو تغيير البيانات والمعطيات المخزنة.

- تخريب المعلومات أو العبث بها.

-تعطيل نظام تشغيل المنظومة أو إحداث خلل في عملها.

وبذلك تعد جريمة البقاء في المنظومة المعلوماتية من الجرائم التي تمس مباشرة سلامة وأمن النظام المعلوماتي وتكشف عن خطورة الاستعمال غير المشروع للتقنيات الحديثة.[3]

ثانيا: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الالية

تتمثل هذه الجريمة في قيام الجاني بإدخال معطيات أو برامج جديدة أو معلومات وهمية أو مزيفة إلى النظام المعلوماتي وهو ما يعد تدخلا في الكيان المنطقي للحاسوب الآلي ويكون

---

[1] خالد امين بن نعوم، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر تخصص قانون قضائي، جامعة عبد الحميد بن باديس مستغانم، الجزائر، السنة الجامعية 2019/2018، ص32.

[2] امال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، 2002، ص 19.

[3] نعيم سعيداني، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستير، تخصص القانون، جامعة الحاج لخضر باتنة، الجزائر،2013، ص 42-43.

الهدف من هذا السلوك الوصول إلى نتيجة معينة يسعى إليها الجاني سواء عبر التمويه أو التضليل أو تغيير الحقيقة.[1]

ويعتبر إدخال البيانات أو البرامج الجديدة المرحلة الأخطر في الجرائم المعلوماتية إذ انها تمهد لمرحلة لاحقة أكثر خطورة تتمثل في حذف او تغيير معطيات المنظومة، وهو ما نص عليه المشرع الجزائري في الفقرة الثانية من المادة 394 مكرر من القانون رقم 06/24 المتضمن ق.ع.ج حيث شدد العقوبة مقارنة بما ورد في الفقرة الأولى من المادة 394 مكرر وذلك إدراكا منه لخطورة هذا الفعل على سلامة النظام المعلوماتي والمعطيات المخزنة فيه.[2]

وتتجلى خطورة هذه الجريمة في أنها لا تقتصر على مجرد إدخال بيانات غير مشروعة بل قد تؤدي إلى:

-تضليل النظام المعلوماتي وإنتاج نتائج غير صحيحة.

- تغيير أو تحريف الحقائق المخزنة.

- تمهيد الطريق لعمليات احتيال أو استغلال لاحق للبيانات.

الفرع الثاني: الاعتداءات الواقعة بواسطة النظام المعلوماتي

ان النظام المعلوماتي في الوقت الحالي لا يقتصر فقط على كونه محلا للاعتداء بل أصبح كذلك وسيلة تستعمل في ارتكاب العديد من الجرائم وتختلف هذه الاعتداءات بحسب الهدف منها، وعليه سيتم التطرق في هذا الفرع إلى أهم صور الاعتداءات الواقعة بواسطة النظام المعلوماتي.

اولا: الجرائم التي تقع على الأشخاص

يقصد بهذا النوع من الجرائم تلك الأفعال التي تستهدف الحقوق ذات الطابع الشخصي أي الحقوق التي لها صلة بالإنسان والتي تعد من مقومات الحياة الخاصة، وهذه الحقوق تخرج

[1] هبة الدزيري، مرجع سابق ص 30.

[2] انظر المادة 394 مكرر من قانون رقم 06/24، السالف الذكر.

بطبيعتها عن دائرة التعامل الاقتصادي لذلك فإن الاعتداء عليها يعتبر من أخطر صور الجرائم المعلوماتية[1].

1 -جريمة القذف والسب عبر الإنترنت

تعد جرائم القذف والسب من الجرائم التي تترك آثارا سلبية بالغة على الأفراد وقد ازدادت شيوعا مع انتشار شبكة الإنترنت وما توفره من وسائل سهلة وسريعة للتواصل وتتمثل خطورتها في إساءة استخدام هذه الوسائل للنيل من شرف الغير أو كرامته أو اعتباره.

-القذف: هو إسناد واقعة محددة إلى شخص معين بشكل علني، بحيث لو كانت صحيحة لأوجبت العقاب على من نسبت إليه[2].

-السب: هو إسناد واقعة غير محددة إلى المجني علي على نحو يمس شرفه أو اعتباره ويُشعره بالاحتقار أمام الآخرين.

وتتحقق هذه الجرائم عبر الرسائل الإلكترونية أو ما ينشر على المواقع حيث يعتبر عنصر العلنية متوافرا بمجرد عرضها أو إرسالها عبر الوسائط الرقمية، وهو ما يجعلها أكثر خطورة من الجرائم التقليدية إذ إن انتشارها السريع عبر الإنترنت يؤدي إلى مضاعفة الأضرار التي تلحق بالضحايا سواء من حيث المساس بسمعتهم أو تعريضهم لبغض الناس واحتقارهم[3].

2 -جريمة انتحال الشخصية

تعد جريمة انتحال الشخصية من الجرائم القديمة التي كانت تُرتكب بالطرق التقليدية غير أن انتشار شبكة الإنترنت منحها أبعادا جديدة إذ أصبح من الممكن انتحال شخصية الأفراد عبر الفضاء الإلكتروني واستغلال بياناتهم الشخصية أسوء استغلال مثل العنوان، تاريخ الميلاد

---

[1] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح بورقلة، الجزائر، السنة الجامعية 2019، الصفحة 05.

[2] سهيلة بوزبرة، مذكرة لنيل شهادة الماجيستير في القانون الخاص، كلية الحقوق، جامعة جيجل، الجزائر،2008، ص 38.

[3] عائشة فلاح، خصوصية الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، الجزائر،2016، ص 45.

رقم الضمان الاجتماعي وغيرها بغرض الحصول على بطاقات ائتمانية أو مزايا مالية غير مشروعة[1].

ويستطيع الجاني من خلال هذه البيانات إخفاء هويته الحقيقية والتصرف بحرية تحت اسم مستعار، مما يصعب عملية كشفه وغالبا ما يتم الحصول على هذه المعلومات عبر الإعلانات المنتشرة على الشبكة أو من خلال وسائل أخرى تتيح الوصول إلى الكم الهائل من البيانات الشخصية المتاحة إلكترونيا.

3-*جريمة المضايقة والملاحقة الإلكترونية*

تعد المضايقة والملاحقة عبر الفضاء الإلكتروني من الجرائم المستحدثة التي أخذت في التزايد مع تطور برامج المحادثة والدردشة وتحديثها المستمر وتتمثل هذه الجريمة في استغلال المساحات التي توفرها الشبكة الإلكترونية للتواصل بين المستخدمين من أجل إرسال رسائل تتضمن تهديدا أو تخويفا أو مضايقة للضحية[2].

وقد شبه القضاء هذه الجريمة بما يعرف في الواقع التقليدي بجرائم التهديد العلني، غير أن ارتكابها عبر الإنترنت لا يتطلب أي اتصال مادي مباشر بين الجاني والضحية وهذا ما يجعلها ذات تأثير نفسي سلبي واضح، إذ تحدث اضطرابا وخوفا لدى الضحية دون أن تؤدي بالضرورة إلى أفعال عنف مادية[3].

4-جريمة التغرير والاستدراج عبر الإنترنت

تعد من أكثر الجرائم المعلوماتية انتشارا خاصة بين فئة صغار السن ومستخدمي الشبكة الإلكترونية، تقوم هذه الجريمة على عنصر الإيهام حيث يعمد الجاني إلى إقناع الضحية

---

[1] ياسمينة بونعارة، الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، الجزائر،2015، ص54.

[2] عبد القادر صنور، الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، الجزائر،2017، ص 38.

[3] إسماعيل ين يحيي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة ابى بكر بلقايد، تلمسان، الجزائر،2021، ص 158.

برغبته في تكوين علاقة صداقة أو زواج عبر الإنترنت، ثم يستغل هذه الثقة لتحقيق أهداف غير مشروعة وقد تتطور هذه الجريمة إلى لقاء مادي بين الطرفين مما يزيد من خطورتها

وتتميز جرائم التغرير والاستدراج بأنها لا تعرف حدودا جغرافية أو اجتماعية، إذ يمكن لأي شخص عبر الشبكة ارتكابها بسهولة كما يمكن أن يقع ضحيتها أي مستخدم حسن النية[1].

5-جريمة التشهير وتشويه السمعة الإلكترونية

مع انتشار الشائعات والأخبار الكاذبة عبر الإنترنت ظهرت جرائم تستهدف المساس بسمعة الأشخاص أو الرموز الفكرية والسياسية والدينية، وتتمثل هذه الجريمة في نشر معلومات أو صور غير صحيحة أو إنشاء مواقع إلكترونية مخصصة لترويج الشائعات والأخبار المغرضة وذلك بهدف تشويه السمعة أو ابتزاز الضحايا[2].

وترتكب هذه الجرائم بوسائل متعددة من أبرزها:

-إنشاء مواقع إلكترونية تحتوي على معلومات كاذبة أو مسيئة.

-نشر صور غير لائقة أو معلومات غير صحيحة عبر الشبكة.

-إرسال رسائل إلكترونية أو محتويات عبر منصات التواصل بهدف الإساءة أو الابتزاز[3].

وتعد هذه الجرائم من أخطر صور الاعتداءات على الأشخاص عبر الفضاء الإلكتروني لما لها من تأثير مباشر على السمعة والاعتبار الشخصي فضلا عن دورها في تسميم أفكار المجتمع ونشر الفوضى المعلوماتية.

---

[1] الطيبي بركة، الحماية الجنائية لنظام المعالجة الالية للمعطيات – دراسة مقارنة-، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة دارية، ادرار، الجزائر،2020، ص 150-154.

[2] خضرة شنتير، الاليات القانونية لمكافحة الجريمة الالكترونية-دراسة مقارنة-، أطروحة لنيل شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة داريه، ادرار، الجزائر،2021، ص 95-100.

[3] نسيمة جدي، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة لنيل شهاد الماجيستير، تخصص قانون جنائي، كلية الحقوق، جامعة وهران، الجزائر،2014، ص 35-45.

6-الجرائم المخلة بالأخلاق والآداب العامة عبر الإنترنت

تعد شبكة الإنترنت فضاءا عالميا مفتوحا لا تحده قيود جغرافية أو سياسية وهو ما يجعل المواد المعروضة عبرها تختلف في توصيفها القانوني من بلد إلى آخر، فالمحتوى الذي يعتبر مخالفا للأخلاق والآداب العامة في دولة معينة قد لا يجرم في دولة أخرى.

وتتجلى هذه الجرائم في صور متعددة أبرزها:

- تحريض القاصرين على ممارسة أنشطة جنسية غير مشروعة عبر الوسائل الإلكترونية.
- محاولة إغوائهم للقيام بأعمال فاحشة أو نشر بياناتهم الشخصية عبر الحاسب الآلي.
- تصوير القاصرين ضمن أنشطة جنسية أو استغلالهم في أعمال إباحية.

وتعتبر الأعمال الإباحية من أكثر الجرائم انتشارا ورواجا عبر الشبكة خاصة في الدول العربية والأوروبية والآسيوية، حيث تعرض بأشكال مختلفة مثل الصور، مقاطع الفيديو المحادثات الإلكترونية، أو حتى أرقام الهواتف وقد ساهمت سهولة الوصول إلى هذه المواد عبر الإنترنت في جعلها متاحة للجميع دون قيود أو حواجز مما يضاعف من خطورتها على المجتمع والقيم الأخلاقية.[1]

ثانيا: الجرائم التي تقع على الاموال

يقصد بهذا النوع من الجرائم تلك الأفعال التي تستهدف الأموال أو الحقوق ذات القيمة الاقتصادية فإذا كان الاعتداء موجها إلى الحاسب الآلي ذاته أو ما يرتبط به من أسلاك وملحقات فإن النصوص الجزائية التقليدية تكفي لحمايته باعتباره مالا منقولا عاديا غير أن الاعتداءات التي تستهدف البرمجيات والأنظمة المعلوماتية تعد أكثر تعقيدا، حيث إن

[1] حورية خليصة- حمزة فيروز، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، الجزائر،2024، ص 50-55.

النصوص التقليدية تكون قاصرة عن توفير الحماية اللازمة نظراً للطابع غير المادي وغير التقليدي لهذه الحقوق[1].

1 –جرائم صناعة ونشر الفيروسات

يعرف الفيروس المعلوماتي بأنه برنامج مصمم للتأثير على باقي البرامج الموجودة على جهاز الحاسب الآلي إما بتحويلها إلى نسخ منه أو بمسحها وتعطيلها عن العمل، ويختلف مبدأ عمل الفيروسات بحسب طريقة تصميمها فقد يبدأ نشاطها بمجرد فتح رسالة تحتويها أو عند تشغيل برنامج مصاب بها[2].

وتعتبر صناعة ونشر الفيروسات من أبرز الجرائم المعلوماتية وأكثرها انتشارا، حيث يعود الحديث عنها إلى أربعينيات القرن الماضي عندما تناولها العالم الرياضي فون نيومان في إطار الحاسب الآلي قبل ظهور الإنترنت ومن أشهر الأمثلة على هذه الفيروسات:

–فيروس رسائل الحب (Love Lettre Virus)

–فيروس الدودة الحمراء (Reed Worm Virus) الذي تسبب سنة 2001 في تعطيل أكثر من ربع مليون جهاز كمبيوتر خلال أقل من تسع ساعات.

وتبرز خطورة هذه الجرائم في قدرتها على إحداث خسائر مالية جسيمة وتعطيل الأنظمة المعلوماتية وتهديد الأمن المعلوماتي على نطاق واسع[3].

---

[1] دحمان عدلي، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ضمن متطلبات شهادة الماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2021، ص 60.

[2] عمار حشمان، المرجع السابق، الصفحة 08.

[3] عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجيستير، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر 2012، ص 45–48.

2 -جرائم الاختراقات

يعرف الاختراق بأنه عملية دخول غير مشروع إلى أجهزة الحاسب الآلي أو الشبكات الإلكترونية ويتم عادة باستخدام برامج متطورة من طرف أشخاص يمتلكون خبرة تقنية وقدرة على تجاوز أنظمة الحماية الموضوعة لتأمين تلك الأجهزة أو الشبكات[1].

وتتعدد دوافع الاختراق باختلاف أهداف القائمين به فقد يكون بدافع الفضول فقط أو بغرض سرقة البيانات والمعلومات، وهو السبب الأكثر شيوعا بين المخترقين حيث يسعون للحصول على معلومات حساسة قد تعرض للبيع أو تستغل لتحقيق مكسب مالي، كما قد يكون الهدف من الاختراق هو تبديل أو تحريف أو تعطيل المعلومات وهو ما يعتبر من أخطر صور الاختراقات نظرا لما يترتب عليه من آثار سلبية على الأفراد والمؤسسات[2].

ومن أبرز صور هذه الجرائم ما يعرف بتغيير وجه الموقع(Website D'effacement) حيث يقوم المخترقون بالاعتداء على مواقع الإنترنت وتغيير تصميمها أو محتواها مما يُلحق ضررا بسمعة الجهة المالكة للموقع ويفقدها ثقة المستخدمين[3].

3 -جريمة تعطيل الأجهزة والشبكات

يقصد بتعطيل الأجهزة والشبكات تلك الأفعال التي تستهدف الحواسيب أو الشبكات الإلكترونية بغرض منعها من أداء وظائفها الطبيعية، دون أن يتطلب ذلك بالضرورة عملية اختراق فعلية ويتم هذا التعطيل عادة عبر إرسال عدد هائل من الرسائل أو الطلبات بطرق تقنية معينة إلى الأجهزة أو الشبكات المستهدفة مما يؤدي إلى إعاقة عملها أو توقفها عن الاستجابة وقد يطال التعطيل البرامج والأنظمة وهو ما قد يترتب عليه أعطال فنية تؤثر حتى

---

[1] عبد اللطيف معتوق، مرجع سابق، ص 49-50.

[2] علي دحمان – سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ضمن متطلبات نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر،2012، ص 35.

[3] نسمة بطيحي، محاضرات في مقياس الوقاية من الجرائم الالكترونية، مطبوعة مقدمة لطلبة السنة الثانية ماستر، تخصص إدارة الكترونية وخدمات رقمية، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر،2022، ص 30-35.

على المكونات الإلكترونية للجهاز، وتعد هذه الجريمة من أخطر صور الاعتداءات المعلوماتية لما لها من آثار مباشرة على استمرارية عمل المؤسسات والأفراد[1].

4 -جريمة النصب والاحتيال عبر الإنترنت

أصبح التعاقد الإلكتروني عبر شبكة الإنترنت ضرورة ملحة نظرا لما يوفره من سرعة وسهولة في التعاملات، غير أن هذه الميزة رافقتها سلبيات عديدة تمثلت في ظهور جرائم النصب والاحتيال بصور جديدة وتشمل هذه الجرائم:

-ابتكار أساليب احتيالية جديدة لخرق التعاملات الإلكترونية.

-سرقة بيانات البطاقات الائتمانية واستخدامها للاستيلاء على الأموال الموجودة في حسابات الضحايا

ويعتبر الاحتيال عبر الإنترنت من أكثر الجرائم شيوعا حيث يسهل على مرتكبيه التخفي والهرب مما

يجعل ملاحقتهم والقبض عليهم أمرا بالغ الصعوبة وتبرز خطورة هذه الجريمة في أنها لا تقتصر على

خسائر مالية فحسب بل تهدد أيضا الثقة في المعاملات الإلكترونية وتعيق تطورها[2].

[1] هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2006، ص 55-65.

[2] نسيمة مرزوق، جرائم الانترنت، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2009، ص 48.

المبحث الثاني:
مظاهر خصوصية الجريمة المعلوماتية

إن الجرائم المعلوماتية تعد نتاجا مباشرا لتطور تقنيات المعلومات والاتصال إذ ترتبط بها ارتباطا وثيقا وتشكل انعكاسا لمظاهرها العملية وقد أضفى هذا الارتباط على تلك الجرائم طابعا قانونيا مميزا يميزها عن الجرائم التقليدية أو المستحدثة الأخرى حيث تجمع بين بعض السمات المشتركة مع غيرها من الجرائم لكنها في الوقت ذاته تنفرد بخصوصية استثنائية ناجمة عن طبيعة الأفعال الإجرامية التي تقوم عليها(المطلب الاول).

وتتجلى هذه الخصوصية في الصعوبات التي تواجه السلطات المختصة عند متابعة الجرائم المرتبطة بالحاسب الآلي والأنترنت والكشف عنها إذ غالبا ما تكون هذه الجرائم غير مرئية ولا تترك آثارا مادية ملموسة فهي لا تتعلق بسرقة أموال أو مجوهرات وإنما تتمثل في تغييرات رقمية داخل السجلات والأنظمة الإلكترونية، ومن ثم فإن اكتشافها غالبا ما يتم بمحض الصدفة وبعد مرور فترة زمنية طويلة على ارتكابها في حين أن نسبة الجرائم غير المكتشفة تفوق بكثير تلك التي تم الكشف عنها بالفعل (المطلب الثاني).

المطلب الأول:
الطبيعة الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تنفرد بها عن الجريمة التقليدية المعروفة منذ الأزل فالجريمة الالكترونية ترتكب بدون إنتقال الجاني من محله ودون اي تسبيب لضرر جسدي وهذا ماجعل جل الفقهاء والباحثين في هذا المجال يصفونها بالجريمة الهادئة أو الناعمة باعتبار انها لاتقع الا في بيئة معلوماتية (الفرع الاول) بالاضافة الى انها تمس بالحدود الجغرافية للدول ولكنها لاتلغيها بل تتعداها دون التقييد بمكان معين (الفرع الثاني).

الفرع الأول: وقوع الجريمة في بيئة معلوماتية

يشترط لقيام الجريمة المعلوماتية أن يكون التعامل مع بيانات معدة ومهيأة للدخول إلى النظام المعلوماتي بغرض معالجتها إلكترونيا، بحيث تتيح للمستخدم إمكانية تصحيحها أو

محوها أو تخزينها واسترجاعها أو طباعتها وتعد هذه العمليات ذات صلة وثيقة بارتكاب الجرائم المعلوماتية. [1]

وتجدر الإشارة إلى أن الجرائم المعلوماتية يمكن أن تقع في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي وهي: مرحلة الإدخال، مرحلة المعالجة ومرحلة الإخراج غير أن لكل مرحلة طبيعة خاصة من الجرائم لا يمكن ارتكابها إلا في سياقها المحدد.[2]

ففي مرحلة الإدخال قد يتم إدخال بيانات غير صحيحة أو إغفال إدخال وثائق أساسية أما في مرحلة المعالجة الآلية للبيانات فيمكن تحقيق الهدف الإجرامي عبر التلاعب ببرامج الحاسب الآلي أو تعديل البيانات أثناء معالجتها، وفي مرحلة الإخراج قد يقع التلاعب في النتائج التي ينتجها النظام رغم أن البيانات المدخلة والمعالجة كانت صحيحة [3].

وقد وسعت بعض التشريعات نطاق تعريف المعدات المستخدمة في مجال المعالجة الآلية ليشمل الأجهزة التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات ومن الشائع توصيف بيانات الحاسوب باعتبارها تمثيلا للحقائق والمعلومات القابلة للقراءة والمعالجة أو التخزين بواسطة الحاسوب وتذهب بعض الاتجاهات إلى اعتبار جهاز الحاسوب ذاته جزءا من هذا المفهوم. [4]

الفرع الثاني: الجريمة المعلوماتية متعدية الحدود

تعد خاصية تجاوز الحدود الجغرافية من أبرز السمات المميزة للجريمة المعلوماتية، إذ يطلق عليها البعض وصف "الجريمة العابرة للحدود" أو "الجريمة ذات الطبيعة الدولية" فمع ظهور شبكات المعلومات، لم تعد الحدود المادية أو المرئية عائقا أمام انتقال البيانات وتبادلها بين أنظمة تفصل بينها آلاف الأميال وقد أفضت هذه القدرة التقنية الهائلة للحواسيب إلى نتيجة مفادها أن جريمة معلوماتية واحدة قد تحدث أثرا متزامنا في دول متعددة، نظرا للسرعة الفائقة

[1] يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط 1، مطبعة الرمال، الجزائر، 2019، ص26
[2] يعيش تمام شوقي، نفس المرجع، ص27
[3] سهيل محمد العزام، الوجيز في جرائم الأنترنت، ط 1، دائرة مكتبة الجامعة الأردنية، الأردن، 2009، ص 79.
[4] سهيل ممد العزام، نفس المرجع، ص 79.

في تنفيذها وحجم المعلومات والأموال المستهدفة فضلا عن المسافة الكبيرة التي قد تفصل الجاني عن محل وقوع الجريمة أو عن الضحايا. [1]

إن هذا الطابع العابر للحدود يميز الجريمة المعلوماتية عن الجريمة التقليدية حيث لم يعد عنصر المكان محددا أو مقيدا كما هو الحال في الجرائم الجنائية الكلاسيكية، بل أصبحت الجريمة المعلوماتية ذات طبيعة دولية تتطلب تعاونا قانونيا وقضائيا عابرا للدول لمواجهتها بفعالية. [2]

إن الطبيعة العالمية للجريمة المعلوماتية ترجع أساسا إلى البيئة الإلكترونية التي ترتكب في إطارها هذه الجرائم، حيث تقوم على الربط الشبكي بين الحواسيب سواء داخل الدولة الواحدة أو عبر عدة دول من خلال شبكات دولية مثل الإنترنت، التي صممت في الأصل لتسهيل عملية نقل المعلومات والاتصالات لكنها أصبحت تستغل كوسيلة لارتكاب الجرائم، فقد ترتكب الجريمة بواسطة الحاسوب في دولة معينة، بينما تتحقق نتيجتها الإجرامية في دولة أخرى سواء عبر مزود خدمة أو قنوات اتصال تقع في إقليم دولة ثالثة. [3]

ويترتب على هذا البعد الدولي للجريمة المعلوماتية جملة من الإشكاليات المشابهة لتلك المرتبطة بالجرائم ذات الطابع العابر للحدود أهمها :

- ✓ صعوبة إصدار إجراءات التحقيق وضبط المتهمين وملاحقتهم في ظل مبدأ السيادة الوطنية للدول.
- ✓ تعقيد الإجراءات في الجرائم التي تستلزم اتخاذ تدابير تحقيق داخل إقليم دولة أجنبية.
- ✓ إشكالية تحديد الاختصاص القضائي بين الدول المعنية.

---

[1] شول بن شهرة، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، المركز الجامعي أفلو، غرادية ،المجلد الرابع، العدد الأول، الجزائر، جوان 2020، ص8

[2] شول بن شهرة، مراد مشوش، نفس المرجع، ص8

[3] اسمهان بن مالك، خصائص الجريمة المعلوماتية وأسباب ارتكابها، المجلة الجزائرية للأبحاث والدراسات، كلية الحقوق والعلوم السياسية بجامعة برج بوعريريج، المجلد الرابع، العدد الأول، 2019، ص 116

- ✓ إشكالية تحديد القانون الواجب التطبيق على الجريمة نظرا لتعدد الأنظمة القانونية التي قد تتداخل في مثل هذه الحالات[1].

المطلب الثاني:
صعوبة إكتشاف الجريمة المعلوماتية

تتسم الجرائم المعلوماتية بقدر كبير من التعقيد في عملية اكتشافها إذ غالبا ما تمر دون ملاحظة أو رصد مباشرويكون كشفها – إن حدث – نتيجة لظروف عرضية أو مصادفات غير مقصودة الأمر الذي يعكس طبيعتها الخفية وصعوبة تتبعها في البيئة التقليدية فيبدو جليا أن عدد الحالات التي يتم فيها اكتشاف الجرائم المعلوماتية يظل محدودا إذا ما تم مقارنته بما يكتشف من الجرائم التقليدية.

وتعود هذه الصعوبة في الكشف إلى عدة عوامل أبرزها أن هذا النوع من الجرائم لا يخلف عادة آثارا خارجية مرئية يمكن الاستدلال بها فضلا عن إمكانية ارتكابها عبر الحدود وفي دول وقارات مختلفة مما يجعلها جرائم ذات طبيعة دولية عابرة للحدود وهذا ماتم تناوله سابقا، كما أن قدرة الجاني على محو أو تدمير أدلة الإدانة في زمن قصير قد لا يتجاوز جزءا من الثانية يمثل عاملا إضافيا يعزز من تعقيد عملية اكتشافها ويضاعف من التحديات التي تواجه أجهزة العدالة الجنائية في التصدي لها.

وسيتم التعرض في هذا المطلب إلى صعوبة إثبات الجريمة المعلوماتية (الفرع الأول) ثم التعرض إلى صعوبة تحديد هوية الجاني المعلوماتي(الفرع الثاني).

الفرع الأول: صعوبة إثبات الجريمة المعلوماتية

إن إثبات الجريمة المعلوماتية يعد تحديا مضاعفا حتى بعد اكتشافها والإبلاغ عنها إذ يحيط به العديد من الصعوبات فهذه الجرائم تقع في بيئة غير تقليدية خارج إطار الواقع المادي الملموس حيث تتجسد عناصرها في فضاء الحاسوب وشبكات الإنترنت، هذا الطابع

[1] نفس المرجع، ص 116

الافتراضي يجعل مهمة سلطات الأمن وأجهزة التحقيق أكثر تعقيدا [1]إذ أن البيانات والمعلومات في هذا السياق لا تعدو كونها إشارات إلكترونية غير مرئية تتدفق عبر الأنظمة المعلوماتية مما يتيح للجاني إمكانية محو الأدلة أو طمسها بشكل كامل وبسهولة فائقة، وقد شهدت ألمانيا إحدى الحالات التي قام فيها الجاني بإدخال تعليمات أمنية داخل نظام الحاسوب لحماية البيانات المخزنة بحيث يؤدي أي اختراق خارجي إلى محوها بواسطة مجال كهربائي، وهو ما يعكس خطورة هذه الجرائم وصعوبة إثباتها وعلاوة على ذلك فإن الوسائل التقليدية للمعاينة الجنائية غالبا ما تفشل في التعامل مع هذا النوع من الجرائم نظرا لاختلاف طبيعتها عن الجرائم التقليدية التي تترك آثارا مادية ملموسة في مسرح الجريمة يمكن الاستناد إليها في التحقيق أما في الجرائم المعلوماتية فإن غياب المسرح المادي وندرة الأثار القابلة للتحفظ يجعل عملية الإثبات أكثر تعقيدا ويحد من قدرة سلطات الاستدلال والتحقيق على جمع الأدلة وفق الطرق التقليدية [2].

و تتجلى صعوبة الإثبات في الجرائم المعلوماتية بوضوح خاصة في ظل غياب الدليل المادي التقليدي الذي تعتمد عليه عادة في الجرائم الجنائية (كأثار الدم أو الشعر أو البصمات) ويزداد الأمر تعقيدا نتيجة ضعف الخبرة الفنية لدى أجهزة الشرطة في مجال الحاسب الألي سواء من حيث القدرة على تحديد الأدلة الرقمية المعتبرة أو من حيث استخراجها وحفظها بطريقة تضمن سلامتها القانونية ، كما أن القضاء حتى الأن لم يستوعب بصورة كاملة خصوصية هذه الجرائم إذ لا يزال يتردد في قبول كثير من صور الإثبات المستندة إلى الوسائل التقنية الحديثة ويستمر في التعامل معها وفق المفهوم التقليدي للجريمة العادية الأمر الذي يحد من فعالية الملاحقة القضائية ويؤكد الحاجة إلى تطوير منظومة الإثبات بما يتناسب مع طبيعة الجرائم المعلوماتية. [3]

---

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع ، الأردن، سنة 2010، ص53 – ص56.

[2] نهلا عبد المومني، مرجع سابق، ص56

[3] أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2014، ص9

الفرع الثاني: صعوبة تحديد هوية الجاني المعلوماتي

إن المجرم الإلكتروني الرقمي" هو الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا". [1]

كا يعرف أيضا بأنه: " هو كل شخص سواءا طفل أو رجل أو أنثى يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة ". [2]

و تتسم شخصية المجرم المعلوماتي بخصائص تتقاطع في كثير من الأحيان مع سمات المجرمين ذوي الياقات البيضاء إذ يشترك كلاهما في الانتماء إلى فئات اجتماعية ومهنية عليا ويشغلون مناصب مرموقة داخل مؤسساتهم، كما يتمتع هؤلاء الأفراد بمستويات عالية من التخصص والكفاءة إضافة إلى قدر ملحوظ من الذكاء والقدرة على التكيف الاجتماعي ضمن بيئاتهم المهنية والاجتماعية. [3]

استنادا إلى ماتم التطرق إليه أعلاه سيتم التركيز في هذا الفرع على السمات المرتبطة بالمجرم المعلوماتي (أولا) وأصنافه (ثانيا)، ثم الحديث عن الدوافع التي تحث المجرم المعلوماتي على إرتكاب الجريمة الإلكترونية (ثالثا)، بعدها الحديث عن المعيقات التي تعيق جهات التحقيق في تحديد هوية الجاني المعلوماتي (رابعا).

أولا: سمات المجرم المعلوماتي

يتحلى المجرم المعلومات بالمميزات الأتية:

---

[1] سهام خليلي، خصوصية المجرم المعلوماتي، مجلة المفكر، المجلد 12، العدد 15، الجزائر، 2017، ص 405.

[2] رضا عسال، عماد عبد الرزاق، الجريمة الإلكترونية والمجرم المعلوماتي: مقاربة مفاهمية، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد 05، الجزائر، 2020، ص 155.

[3] رضا عسال، نفس المرجع، ص 155.

-المجرم المعلوماتي ذو طبع إجتماعي: يتميز المجرم المعلوماتي عادة بكونه شخصا ذو طبيعة إجتماعية ويتميز أيضا بقدرته العالية على التكيف داخل بيئته المهنية، فالملاحظ أن هذا المجرم يتمتع بثقة زملائه في مجال عمله مما يبعد عنه دائرة الشبهات، فالمجرم المعلوماتي يسعى دائما كي لا يضع نفسه في موقع عداء مباشر مع المجتمع بل يسعى لإضفاء التوافق والتصالح مع هذا الأخير. [1]

-المجرم المعلوماتي يتمتع بالمهارة والكفاءة: يُلاحظ أن مجرمي المعلوماتية يتمتعون بقدر من المهارة والمعرفة في تقنيات الحاسوب والإنترنت حيث أن بعضهم يعدون من المتخصصين في مجال معالجة المعلومات آليا، فارتكاب الجريمة المعلوماتية يتطلب مستوى معين من الكفاءة التقنية التي غالبا ما تُكتسب من خلال الخبرة العملية في مجال تكنولوجيا المعلومات[2].

كما يتسم المجرم المعلوماتي بدرجة عالية من الذكاء وهو ما يُعد نتيجة طبيعية لخبرته واحترافه في هذا المجال إذ يوظف الحاسب الآلي كأداة رئيسية لتنفيذ مخططاته الإجرامية، هذا الذكاء يمنحه القدرة على تجاوز العقبات التقنية والقانونية التي قد تعترض سبيله أثناء ارتكاب الجريمة ومن أبرز صور هذا السلوك الإجرامي جريمة النصب المعلوماتي التي تتطلب مستوى مرتفع من الذكاء والقدرة على التلاعب بالأنظمة الإلكترونية[3]، وبالتالي يُطلق على هذا النمط من الجرائم وصف "إجرام الأذكياء" نظرا لاعتماده على المهارة الفكرية والقدرات التقنية بخلاف الإجرام التقليدي الذي يميل في الغالب إلى استخدام العنف المادي المباشر.

-العودة إلى الجريمة: يعتبر المجرم المعلوماتي من أكثر الفئات الإجرامية قابلية للعودة إلى ارتكاب جرائم جديدة في ذات المجال الإلكتروني فغالبا ما تدفعه الرغبة في سد الثغرات التي أدت إلى كشفه وتقديمه للمحاكمة في المرة السابقة إلى تطوير أساليبه والعودة إلى النشاط

---

[1] حسين ربيعي، مرجع سابق، ص 35-36.

[2] فاطيمة دهان، كلثوم دهان، إجراءات البحث والتحري في الجرائم المعلوماتية، مذكرة مقدمة ضمن متطابات نيل شهادة ماستر أكاديمي، تخصص: قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامهعة غرادية، الجزائر، 2021-2022، ص 25.

[3] نفس المرجع، ص 25.

الإجرامي وقد ينتهي به الأمر مجددا إلى المثول أمام القضاء نتيجة استمرار ممارساته غير المشروعة. [1]

يستثمر هذا النوع من المجرمين مهاراته التقنية في فهم كيفية عمل الحواسيب وآليات تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات بما يتيح له الدخول غير المصرح به إلى الأنظمة الإلكترونية ومن اللافت أن الدافع الأساسي وراء ارتكاب هذه الجرائم لا يكون بالضرورة الإيذاء المباشر وإنما ينبع من شعور المجرم بقدرته ومهارته في مجال الاختراق المعلوماتي وهو ما يعزز لديه الميل إلى التحدي والتمادي في السلوك الإجرامي [2].

ثانيا: أصناف المجرم المعلوماتي

يمكن تقسيم مرتكبي الجرائم المعلوماتية وفق طبيعة علاقتهم بالمنظومة المعلوماتية وأهدافهم الإجرامية إلى الفئات التالية:

الفئة الأولى: وهم الأفراد الذين يستخدمون الحاسب الآلي المنزلي وغالبا ما يكون دافعهم التسلية أو إزعاج الآخرين دون أهداف مادية أو استراتيجية واضحة هذه الفئة تمثل المستوى الأقل خطورة من حيث النتائج لكنها تظل محل مساءلة قانونية.

الفئة الثانية: تضم العاملين داخل المنظومة المعلوماتية نفسها ويتجلى خطر هذه الفئة في قدرتها على تخريب الأجهزة أو إتلافها أو سرقة البيانات وذلك بغرض الوصول إلى معلومات حساسة وخطيرة مما يجعل جرائمهم ذات أثر بالغ على الأمن المعلوماتي.

الفئة الثالثة: وهم ما يعرف بـ "الهاركز" الذين يسعون إلى المغامرة والتحدي وإثبات قدراتهم التقنية أمام أقرانهم ودوافعهم في الغالب ترفيهية أو استعراضية إلا أن بعضهم يتجاوز ذلك إلى العبث بمحتويات الأجهزة أو سرقتها لتحقيق مصالح شخصية أو لإيجاد حلول لمشاكلهم الخاصة.

---

[1] بشرى غريبي، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المجلد 02، العدد 02، الجزائر، 2021، ص 106.

[2] نفس المرجع، ص 106.

الفئة الرابعة: وتشمل المحترفين أو ما يطلق عليهم "الكراكز"، الذين يستهدفون المؤسسات التجارية والحكومية بغرض سرقة المعلومات وبيعها لجهات أخرى، هذه الفئة تمثل أخطر أنواع مرتكبي الجرائم المعلوماتية إذ غالبا ما تكون جرائمهم منظمة وذات أهداف اقتصادية أو استخباراتية. [1]

ثالثا: دوافع المجرم المعلوماتي لإرتكاب الجريمة المعلوماتية

إن الدوافع الباعثة لإرتكاب الجرائم الإلكترونية عديدة ومتنوعة ولا يمكن حصرها وعليه سيتم الحديث في هذا المقام على بعض الأمثلة التي تحدث عنها الخبراء والمتخصصين وهي:

01-الدوافع الشخصية

تتمثل الدوافع الشخصية في المحركات الذاتية التي تؤثر في سلوك الفرد سواء بدفعه إلى الإقدام على فعل معين أو الإحجام عنه وترتبط هذه الدوافع ارتباطا وثيقا بالبنية النفسية للفر[2]د وسيتم تفصيلها فيما يأتي:

-السعي لتحقيق ربح مادي: إن الدافع المادي يعد من أبرز الدوافع التي تقف خلف ارتكاب الجرائم الإلكترونية ففي دراسة أجراها الأستاذ باركر تبلغ نسبة حالات الغش المعلن عنها والتي ارتكبت بغرض الحصول على المال نسبة 43 %، فالقطاع الأكثر تضررا من هذه الجرائم هو القطاع المالي وذلك لاعتماد البنوك بشكل أساسي على أنظمة التحويل الإلكتروني[3].

-الرغبة في الحصول على معلومات جديدة: يعد حب الإطلاع والرغبة في اكتساب المعرفة من الدوافع الجوهرية التي تقود بعض الأفراد إلى ارتكاب الجرائم المعلوماتية إذ أن هناك فئة من مرتكبي هذه الأخيرة تسعى لإكتشاف الأنظمة المعلوماتية والتعمق في أليات عملها

[1] سهام خليلي، مرجع سابق، ص408.

[2] صابر بحري، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الإنحراف، المجلد 06، العدد 01، الجزائر، 2021، ص 48.

[3] عبد القادر درقاوي، المجرم المعلوماتي، مجلة الدراسات القانونية والسياسية، المجلد 11، العدد 02، الجزائر، 2025، ص 68.

وغالبا مايتم ذلك في إطار جماعي حيث يقومون بتعليم بعضهم البعض مع تبادل الخبرات فيما بينهم.[1]

-الرغبة في تحدي وقهر النظام المعلوماتي: من بين الدوافع التي قد تقود إلى ارتكاب الجرائم الإلكترونية يبرز دافع قهر النظام المعلوماتي وتجاوز حواجز الحماية التقنية فهنا لا يعكس السلوك الإجرامي بالضرورة خطورة إجرامية كامنة أو نزعة إجرامية متأصلة لدى الفاعل بل يتمثل غالبا في رغبة نفسية أو ذهنية في تحدي النظام التكنولوجي المعقد للحاسب الآلي ومحاولة إثبات القدرة على اختراقه والوصول إلى المعلومات المحمية، ومع تزايد الاهتمام بأمن المعلومات وتطوير تقنيات متقدمة للحماية مثل أنظمة التشفير المعقدة التي لا يفك رموزها سوى مستخدمها الشرعي تتضاعف رغبة بعض الأفراد في اختبار قدراتهم التقنية أمام هذه الأنظمة [2]. المعقدة

02-الدوافع الخارجية

و تتمثل هذه الدوافع في الأمور الخارجة عن شخصية ونفسية الجاني المعلوماتي وهي:

-إلحاق الضرر بالأخرين: يعد دافع إلحاق الضرر بالغير من بين أبرز الدوافع التي تقود لإرتكاب الجريمة المعلوماتية حيث قد يسعى الجاني إلى إلحاق خسائر مادية أو معنوية بالغير.

-التعاون والتواطؤ: غالبا ماتتوزع الأدوار والمهمات بين أكثر من شخص لتحقيق الفعل الإجرامي حيث يقوم أحد المتخصصين في الأنظمة المعلوماتية بالجانب الفني المتعلق بإختراق النظام أو التلاعب بالبيانات بينما يتولى شخص أخر من داخل المؤسسة أو خارجها مهمة تغطية العمليات غير المشروعة.

[1] صابر بحري، المرجع السابق، ص 49.

[2] عبد القادر درقاوي، مرجع سابق، ص 69.

-تهديد الأمن القومي والعسكري: إن أغلب الجرائم المعلوماتية غايتها المساس بالأمن القومي والعسكري للدول وهذا ما أدى لتطور بعض الجرائم من طبعها التقليدي إلى طبعها الإلكتروني منها التجسس الإلكتروني والإرهاب الإلكتروني. [1]

-دافع الإنتقام من رب العمل أو المؤسسة التابع لها: غالبا ما يصدر هذا الدافع عن موظف أو عامل سابق يمتلك معرفة واسعة بالبنية التقنية للمؤسسة أو الشركة التي يعمل بها ويظهر هذا السلوك الإجرامي عادةً عند الفصل من العمل أو الحرمان من الحوافز والترقيات، ومن أبرز الأمثلة على خطورة هذا الدافع حادثة شركة أوميغا التي وقعت في الولايات المتحدة حيث قام المبرمج والمصمم السابق للشبكاتTimothy Allen Lloyd بعد عشرين يوما من فصله من العمل بزرع "قنبلة إلكترونية" عام 1996 وقد أدى هذا الفعل التخريبي إلى إلغاء كافة التصاميم وبرامج الإنتاج الخاصة بأحد أكبر مصانع التقنية في نيوجرسي[2].

أسفرت هذه الجريمة عن خسائر مالية قدرت بحوالي عشرة ملايين دولار مما جعلها تصنف ضمن أخطر جرائم التخريب المعلوماتي منذ ظهور هذه الظاهرة[3].

رابعا: المعيقات التي تعيق جهات التحقيق في تحديد هوية الجاني المعلوماتي

يظهر الجاني المتمرس براعة في إخفاء مسارات الوصول إلى الأدلة الرقمية، حيث يواجه المحققون عقبة تتمثل في استخدامه لوسائل تقنية متقدمة تحول دون تعقب نشاطه أو كشف أوامره الإلكترونية. إذ يسعى إلى جعل أنشطته تبدو وكأنها بعيدة عن أعين السلطات المختصة بمكافحة الجريمة. ومن أبرز أساليبه في ذلك اللجوء إلى استخدام حواسيب لا تعود ملكيتها إليه، مثل الحواسيب المتوفرة في مقاهي الإنترنت التي لا تقوم عادة بتسجيل بيانات مرتاديها أو التحقق من هوياتهم، مما يجعل مهمة أجهزة الشرطة في تحديد هوية الجاني وعنوانه أكثر صعوبة وتعقيدا. [4]

---

[1] صابر بحري، المرجع السابق، ص 53-55.

[2] بشرى غريبي، المرجع السابق، ص 110.

[3] بشرى غريبي، المرجع السابق، ص 110.

[4] حيمي سيدي محمد، معوقات التحقيق الجنائي في الجرائم الإلكترونية، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، السنة 2022، ص1748

و تعد من بين أبرز العوامل التي تحول دون اكتشاف هوية الجاني المعلوماتي، امتناع المجني عليه عن الإفصاح عن الجرائم المعلوماتية وعدم قيامه بإبلاغ السلطات المختصة فور اكتشافها إذ غالبا ما تحرص المؤسسات والجهات التي تتعرض أنظمتها المعلوماتية للاختراق أو تتكبد خسائر جسيمة نتيجة لذلك، على التكتم وعدم الكشف حتى أمام موظفيها عما تعرضت له، مكتفية باتخاذ إجراءات إدارية داخلية لمعالجة الوضع، ويعزى هذا السلوك إلى رغبة تلك الجهات في تجنب الأضرار المحتملة التي قد تلحق بسمعتها أو مصالحها الاقتصادية في حال الإعلان عن الواقعة أو إشعار السلطات بها وهو ما يفضي عمليا إلى عرقلة جهود أجهزة العدالة الجنائية في تتبع الجناة وملاحقتهم. [1]

[1] حيمي سيدي محمد، المرجع نفسه، ص1747

الفصل الثاني:
أثر خصوصية الجريمة المعلوماتية على إجراءات المتابعة

لقد شهدت الجرائم السيبرانية في العصر الرقمي تزايدا ملحوظا الأمر الذي فرض تحديات جسيمة على الدول ومنها الجزائر، بحيث أصبح التصدي لهذا النمط المستحدث من الإجرام يتطلب توظيف مهارات وتقنيات متقدمة تتماشى مع التطورات التكنولوجية الحديثة فضلا عن ضرورة سن تشريعات قانونية خاصة تتلاءم مع طبيعة هذه الجرائم.

وتتميز الجرائم الإلكترونية عن الجرائم التقليدية بكونها تعتمد على القدرات الذهنية والمهارات التقنية للجاني بعيدا عن الجهد البدني مما يجعل عملية إثباتها أكثر تعقيدا ويضفي عليها خصوصية في مجالات البحث والتحري وأساليب التحقيق، هذا الطابع الفريد يفرض على المنظومة القانونية والأمنية تطوير أدواتها وآلياتها بما يضمن فعالية مواجهة هذا النوع من الجرائم.

ومن هذا المنطلق قد سعى المشرع الجزائري لإرساء منظومة قانونية متينة للحد من حدوث الجرائم الإلكترونية مع القدرة على إستنباط الأدلة المختلفة لإثبات هذه الأخيرة وذلك من خلال تبني إجراءات متابعة تعمل على كشف الجرائم السيبيرانية بمختلف أشكالها.

و بالتالي سيتم الحديث في هذا الفصل عن مدى فعالية وإمكانية تطبيق إجراءات المتابعة المستحدثة للكشف عن الجرائم المعلوماتية (مبحث أول) ثم إجراءات المتابعة العامة للكشف عن الجرائم المعلوماتية (مبحث ثاني).

المبحث الأول:

إجراءات المتابعة المستحدثة في الجرائم المعلوماتية

في ظل التطور التكنولوجي المتسارع شهدت منظومة الإثبات تحولا نوعيا حيث لم تعد الأدلة تقتصر على الوسائل التقليدية بل امتدت لتشمل الأدلة الرقمية بمختلف صورها كالمعطيات الإلكترونية، والصور الرقمية، ومقاطع الفيديو، وسجلات الاتصالات الناتجة عن استعمال تكنولوجيات الإعلام والاتصال، وقد أفرز هذا التحول تحديات جديدة أمام القواعد الإجرائية التقليدية لاسيما فيما يتعلق بطرق جمع الأدلة وحجيتها في الإثبات.

وأمام هذه المستجدات سارعت العديد من الدول ومن بينها الجزائر إلى تبني إطار قانوني خاص يهدف إلى مكافحة الجرائم الإلكترونية من خلال استحداث آليات إجرائية تتلائم مع طبيعة هذه الجرائم التي ترتكب في بيئة افتراضية، ويقتضي ذلك بالضرورة إقرار وسائل خاصة في البحث والتحري، وكذا اعتماد قواعد إثبات مرنة تعترف بالأدلة الرقمية وتحدد شروط مشروعيتها وحجيتها، فإن الإجراءات الخاصة بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال تتميز بخصوصية واضحة وهذا ما سنتطرق اليه من خلال اجراء التسرب في (المطلب الأول) وكذا اجراء اعتراض المراسلات والاتصالات الالكترونية (المطلب الثاني).

المطلب الأول:

التسرب الالكتروني

يعتبر التسرب من الوسائل الإجرائية المعتمدة في مجال التحري غير أنه لم يعد يقتصر على صورته التقليدية بل امتد ليشمل التسرب الإلكتروني الذي يعتمد عليه في مجال مكافحة الجرائم المرتبطة بالمنظومة المعلوماتية، وقد أقر المشرع الجزائري هذا الأسلوب ضمن الإطار القانوني المنظم لمكافحة الجرائم المعلوماتية، وعليه سنتناول من خلال هذا المطلب مفهوم التسرب (الفرع الأول) وكذا الشروط الخاصة بتنفيذ اجراء التسرب الالكتروني (الفرع الثاني).

الفرع الأول: مفهوم التسرب الالكتروني

يعد التسرب الالكتروني من اهم الإجراءات التي اثارت اهتمام المشرع الجزائري باعتباره اجراءا هاما في اثبات الجريمة المعلوماتية.

أولا: تعريف التسرب

نظرا لأهمية التسرب الالكتروني وما قد يترتب عنه من اضرار تمس سرية المعطيات كان لابد من التطرق الى المقصود به.

1- التعريف اللغوي للتسرب

يشتق لفظ التسرب في اللغة من الفعل "تسرب"، ويقال تسرب الشيء تسربا إذا انتقل خفية ومن دون ملاحظة كما يفيد معنى الولوج والدخول إلى مكان ما بطريقة غير ظاهرة أو دون علم الغير، وتسرب الشخص إلى جماعة معينة ويجعل أفرادها يعتقدون أنه ليس غريبا عنهم بل يوهمهم بأنه واحد منهم، مما يتيح له الاطلاع مسبقا على أهداف الجماعة الإجرامية وفهم توجهاتهم.[1]

2- التعريف الاصطلاحي للتسرب هي إحدى تقنيات التحري والتحقيق الخاصة، ولها عدة مرادفات اصطلاحية مثل التوغل والاختراق وتتمثل في السماح بالدخول إلى وسط مغلق كجماعة إجرامية مثلا أو إدخال عنصر أجنبي إلى شبكة تنشط في الاتجار بالمواد الممنوعة، وجميع هذه المصطلحات تؤكد فكرة الاندماج داخل الجماعة المستهدفة واختراقها، تتم هذه العملية في البداية بعد أن يختار ضابط الشرطة القضائية أحد العناصر الذين تتوفر فيهم بعض المواصفات الخاصة، مثل القدرة على التأقلم أو التكيف مع الوسط الذي يتبع له المستهدف.[2]

---

[1] الشيماء بن الداوي، التسرب ودوره في مكافحة الجريمة، مذكرة لاستكمال متطلبات نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، جامعة غرداية كلية الحقوق والعلوم السياسية قسم الحقوق، الجزائر، 2024، ص02.

[2] نبيلة قيشاح ،التسرب كالية للتحري والتحقيق في الجريمة المنظمة، مجلة المستقبل للدراسات القانونية والسياسية- المركز الجامعب بافلو،الجزائر،العدد03، 2018،ص 69-70.

3- التعريف القانوني

نص المشرع الجزائري في المادة 121 من القانون رقم 14/25 المتضمن ق. إ.ج على مصطلح التسرب المقابل لعبارةl'infiltration واعتبره من بين أساليب التحري الخاصة ويقصد به قيام ضابط أو عون من الشرطة القضائية تحت إشراف ومسؤولية جهة قضائية مختصة، بمهمة التغلغل داخل أوساط يُشتبه في نشاطها الإجرامي، ذلك من خلال إيهام المعنيين بأنه فاعل أو شريك في الجريمة، بغرض مراقبتهم وجمع المعلومات والاستدلالات والأدلة المتعلقة بها[1].

كما أن اللجوء إلى هذا الأسلوب لا يكون إلا لاعتبارات الضرورة الملحة خاصة في القضايا التي يصعب فيها الوصول إلى الحقيقة بالوسائل العادية مما يبرر اعتماده كإجراء استثنائي تحكمه ضوابط قانونية دقيقة.[2]

يعد التسرب عملية منظمة تحضر بعناية ودقة وتستهدف أوساطا معينة يشتبه في ضلوعها في نشاط إجرامي، ذلك بناء على دراسة مسبقة لهذه الأوساط ويهدف هذا الإجراء إلى مراقبة الأشخاص المشتبه فيهم وجمع المعلومات حول أنشطتهم، في إطار ما هو محدد قانونا وبعد استيفاء جميع الشروط الموضوعية والشكلية.[3]

ولا يلجأ إلى التسرب إلا تحت رقابة السلطة القضائية وفي حالات الضرورة الملحة التي تفرضها متطلبات التحري والتحقيق.

وعليه يقصد بالتسرب قيام الشخص المأذون له قانونا بالتحقيق في الجريمة بمراقبة المشتبه فيهم مع تمكين ضباط وأعوان الشرطة القضائية من استعمال هوية مستعارة، بل وقد يُرخص لهم عند الاقتضاء بارتكاب بعض الأفعال التي تعد في الأصل جرائم دون أن تترتب عن

---

[1] انظر نص المادة 121 من ق.إ.ج.ج، السالف الذكر.

[2] الشيماء بن الداوي، المرجع السابق، ص 04.

[3] زكرياء لدغم شيكوش، النظام القانون للتسرب في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية والإدارية، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر،2013، ص47-49.

ذلك مسؤوليتهم الجزائية، متى كان الهدف من ذلك كشف الأنشطة الإجرامية ومتابعة مرتكبيها، حيث توظف هذه التقنية لاختراق الأوساط الإجرامية ذات الطابع المنظم التي تتسم بالسرية والتعقيد ويصعب النفاذ إلى بنيتها أو الكشف عن أساليب نشاطها وتهدف هذه العملية إلى جمع المعلومات والأدلة المتعلقة بالنشاط الإجرامي وكشف المخططات المعدة في الخفاء، بما يتيح للسلطات المختصة اتخاذ الإجراءات القانونية الملائمة وفقا لما يقرره القانون وتحت إشراف القضاء عليها حصريا وهذا طبقا لما نصت عليه المادة 120 من القانون رقم14/25المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.[1]

3-1 التسرب الإلكتروني في القوانين الخاصة

أشار المشرع الجزائري للتسرب الإلكتروني في القوانين الخاصة كالقانون رقم 20-05

المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها والقانون 20-15 المتعلق بالوقاية من اختطاف الأشخاص ومكافحتها.

أ- التسرب الإلكتروني في القانون رقم05/20المتعلق بالوقاية من التمييز وخطابا الكراهية ومكافحتها:

حسب نص المادة 26 من القانون المذكور أعلاه، الذي جاء فيه: "يجوز لوكيل الجمهورية أو قاضي التحقيق، بعد استيفاء الإجراءات الإدارية والجنائية المقررة، أن يأذن تحت إشرافه ورقابته، لضابط الشرطة القضائية بالاطلاع على منظومة معلوماتية أو نظام اتصالات إلكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه في، ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون وذلك بإيهاميهم بانه فاعل معهم أو شريك لهم."[2]

[1] انظر نص المادة 120 من ق.إ.ج.ج، السالف لذكر.

[2] قانون 20-05، المؤرخ في 05 رمضان 1441 الموافق ل 28 افريل 2020 التعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج. ر.ج.ج. العدد 25 الصادرة بتاريخ 06 رمضان 1441 الموافق ل 29 ابريل 2020.

نفهم من خلال هذه المادة أن التسرب الإلكتروني يختلف نوعا ما عن التسرب المادي ويتمثل هذا الاختلاف على سبيل المثال في صور التسرب ففي التسرب المادي نجد أن الصور تحتوي على ثلاث صور رئيسية: صورة الفعل الأصلي، صورة الشريك، وصورة المتخفي[1].

أما الضابط في التسرب فيكون صلاحه إبراز الأشخاص أو الأمور الجوهرية، بينما التسرب الإلكتروني يمنع أي شخص مشبوه من الوصول إليها ويظهر فيها الشخص أحيانا كفاعل أصلي أو كأنه شريك، أو قد تخفى بعض التفاصيل، ويظهر هذا بوضوح في الصور حيث يكتفي التسرب المادي بالصور فقط بينما التسرب الإلكتروني يمكن أن يضم صورا إضافية أو يختفي فيها عناصر معينة مما يجعله أكثر مرونة وغموضا مقارنة بالتسرب المادي.[2]

ب- التسرب الإلكتروني في القانون رقم15/20المتعلق بالوقاية من اختطاف الأشخاص ومكافحتها:

تنص المادة 16 من القانون المذكور على أنه يجوز لوكيل الجمهورية أو قاضي التحقيق وفقا لاختصاصه أن يأذن لضابط الشرطة القضائية بالاطلاع على التسرب الإلكتروني للوصول إلى معلومات عن الأشخاص المشتبه بهم في أي وسيلة أو نظام للاتصالات الإلكترونية أو أي محتوى منصوص عليه في هذا القانون، ويتم ذلك بهدف إثبات ارتكاب أي جريمة سواء كان المشتبه به هو الفاعل الأصلي أو شريكا له.[3]

بناءا على القانون رقم 15/20 المذكور اعلاه، فإن التسرب الإلكتروني المشار إليه يختلف عن التسرب المادي فيما يتعلق بالآثار الجزائية وطبيعة البيئة الرقمية التي تُرتكب فيها الجريمة.

---

[1] كريمة تاجر، التسرب الالكتروني كألية لمكافحة الجريمة الالكترونية – دراسة مقارنة بين القانون الجزائري والفرنسي، المجلة النقدية للقانون والعلوم السياسية، المجلد 19، العدد 02، 2024، الجزائر، ص480

[2] كريمة تاجر، نفس المرجع، ص 481-484.

[3] قانون رقم 20 /15المؤرخ في 15 جمادة الأولى 1442 الموافق 30 ديسمبر 2020 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها، ج.ر.ج. ج عدد81، الصادرة بتاريخ 15 جمادة الأولى 1442 الموافق ل 30 ديسمبر2020.

ويتمثل هذا الاختلاف على وجه الخصوص في صور التسرب وطبيعة المعلومات المتاحة كما هو منصوص عليه في القانون رقم 15/20 والذي يخول للسلطات المختصة اتخاذ الإجراءات اللازمة لمراقبة واستخراج المعلومات المتعلقة بالأشخاص المشتبه بهم ضمن نظم أو وسائل الاتصالات الإلكترونية، وذلك لإثبات ارتكاب أي جريمة من قبل الفاعل الأصلي أو شركائه.[1]

كما نجد أن هناك اختلافا آخر من حيث مجال التطبيق حيث يقتصر التسرب المادي على تطبيق الأحكام الجزائية المنصوص عليها في قانون الإجراءات، بينما يستخدم التسرب الإلكتروني في الحالات الخطيرة التي تصف الجرائم ضمن مجال رقمي خاص يشتبه في استغلاله لارتكاب جريمة اختطاف أشخاص[2].

ويعني ذلك أن ضابط الشرطة القضائية من خلال الوصول إلى مسار التسرب الإلكتروني يمكنه متابعة الأشخاص المشتبه بهم بشكل محدد ودقيق، وذلك من أجل الكشف عن الجرائم المرتكبة ومنع المخاطر الناتجة عنها.[3]

يتبين من خلال ما ورد أن مجال تطبيق التسرب الإلكتروني مفتوح وغير مقصور على جرائم محددة حيث يمكن استخدام هذه الإجراءات في أي جريمة ترتكب عبر وسائل تكنولوجيا الإعلام والاتصال.[4]

---

[1] الدوادي مجراب، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة دكتوراه، تخصص الحقوق، جامعة بن يوسف بن خدة، الجزائر1، الجزائر،2016، 343.

[2] نفس المرجع، 344.

[3] سمير خلفي، التسرب الإلكتروني: اجراء لمكافحة المخدرات عبر الوسائط الإلكترونية في ظل انتشار جائحة كورونا، مجلة المحلل القانوني، جامعة البويرة، المجلد04، العدد 02، ديسمبر2022، ص 79.

[4] ليندة بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة لنيل درجة الدكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة ميلود معمري، جامعة تيزي وزو، الجزائر،2019، 285.

ثانيا: صور عملية التسرب

بالرجوع إلى نص المادة 121 يتبين أن المشرع قد حدد صور تنفيذ عملية التسرب والتي يمكن أن تتخذ ثلاث حالات: إما باعتبار الضابط أو العون المتسرب فاعلا أصليا، أو شريكا، أو من خلال تنفيذ عملية التسرب بصورة خفية.

1/ المتسرب كفاعل:

طبقا لنص المادة 41 من ق.ع.ج على انه" يعد فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكابها عن طريق الهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو من خلال التحايل أو التدليس الإجرامي" وبناءا على ذلك يجوز للعون أو الضابط المكلف بعملية التسرب عند مباشرته لها بأسلوب التمويه أن يتخذ صفة الفاعل الأصلي في الجريمة، من خلال القيام بالأفعال المنصوص عليها في المادة 114 من القانون 14/25 المتضمن ق.إ.ج وذلك بغرض كسب ثقة المشتبه فيهم وتمكينه من الحصول على أدلة مادية تفضي إلى ضبطهم دون أن يشكل ذلك تحريضا لهم على ارتكاب الجريمة[1].

وعليه أجاز القانون للعون المتسرب أن يكون فاعلا مع غيره بحيث يساهم شخصيا في ارتكاب الأفعال المادية المكونة للجريمة غير أنه لا ينفرد بذلك، بل يتم ذلك بمشاركة أشخاص آخرين فيعدون جميعا فاعلين أصليين في الجريمة ذاتها وعلى هذا الأساس يمكن للعون المتسرب أن يأتي أفعالا مادية تدخل ضمن عناصر الجريمة محل التغلغل بما يوحي بأنه يضطلع بدور مباشر في تنفيذ النشاط الإجرامي، دون أن تكيف هذه الأفعال على أنها تحريض غير أنه من الناحية القانونية لا يجوز للعون المتسرب بأي حال من الأحوال أن يعد فاعلا معنويا أو محرضا إذ لا يسمح له بخلق فكرة الجريمة لدى الغير إذا لم تكن قائمة في ذهنه مسبقا لأن دوره يقتصر على كشفها والتحقق من وجودها لا على إنشائها وفي هذا الإطار يعد المتسرب فاعلا ماديا يباشر الفعل الإجرامي بنفسه ولكن في إطار خفي وتحت

[1] مليسة حمري، حجية الدليل الإلكتروني في الإثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر،2020/2019، ص 56-58.

إشراف السلطات المختصة متظاهرا بالاندماج في النشاط الإجرامي وذلك بهدف جمع الأدلة الكافية لإثبات الجريمة.[1]

كمثال على ذلك في قضايا تهريب المخدرات يتم زرع عميل سري داخل شبكة إجرامية متخصصة في التهريب حيث يتولى هذا الأخير القيام بعملية شراء كمية من المخدرات من أفراد التنظيم الإجرامي، وذلك في إطار عملية تسرب محكمة وتوثق هذه العملية بوسائل تقنية كالتسجيل الصوتي والمرئي قصد تمكين السلطات المختصة من ضبط المتهمين في حالة تلبس وتثبيت الأدلة القانونية ضدهم[2].

وأيضا في قضايا الفساد قد يتظاهر عميل متسرب في إطار عملية التحري بأنه في حاجة إلى الحصول على ترخيص أو خدمة إدارية معينة ويعرض مبلغا ماليا على موظف يُشتبه في تورطه في أعمال الفساد فإذا ما قام الموظف بقبول الرشوة أو التفاعل معها يتم توثيق الواقعة وفق الأطر القانونية المعمول بها، ثم ضبطه متلبسًا بارتكاب الجريمة.[3]

وتأصيلا لما سبق فإنه إذا قام المتسرب بصفته فاعلا أصليا بتحريض الجناة على ارتكاب الجرائم فإن ذلك يعد باطلا وغير جائز قانونا ويترتب عنه مسؤوليته الجزائية ومتابعته قضائيا.

2/المتسرب كشريك

يعتبر شريكا في الجريمة وفقا لأحكام قانون العقوبات كل من ساعد الفاعل أو الفاعلين بأي طريقة كانت على ارتكاب الأفعال التحضيرية أو الميسرة أو المنفذة للجريمة شريطة علمه بذلك كما يعد في حكم الشريك كل من اعتاد توفير مسكن أو ملجأ أو مكان للاجتماع لشخص أو أكثر من ذوي السلوك الإجرامي الذين يمارسون أعمال اللصوصية أو العنف

---

[1] ويزة بلعسلي، *التسرب كآلية خاصة للبحث والتحري في الجرائم المستحدثة في قانون الإجراءات الجزائية*، المجلة النقدية للقانون والعلوم السياسية، ع05، 2015، الجزائر، ص145–ص149.

[2] نفس المرجع، ص 150.

[3] فراح حمادي – بوالزرد اسماء، التسرب في قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر، تخصص مهن قانونية وقضائية، جامعة جيجيل،الجزائر،2025، ص38.

الموجه ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال مع علمه بطبيعة نشاطهم غير المشروع[1].

وعملا بهذا بالشريك يعد عون أو ضابط الشرطة القضائية المأذون له بمباشرة عملية التسرب شريكا في الجريمة، بالنظر إلى ما قد يقدمه من مساهمات مادية، كإيواء المشتبه فيهم أو توفير مسكن أو ملجأ لهم، فضلا عن المساهمات المعنوية المتمثلة في مرافقتهم ومواكبة سلوكهم الإجرامي إلى غاية ضبطهم في حالة تلبس[2].

ومع ذلك، تجدر الإشارة إلى أن المتسرب في إطار هذه العملية لا يُسأل جزائيًا عن هذه الأفعال، لكونها تندرج ضمن الأفعال المبررة قانونًا والمأذون بها في إطار مهامه الخاصة بالتحري والتسرب[3].

3/ المتسرب كخفي

من بين صور تنفيذ عملية التسرب الإخفاء وهو ما تناوله المشرع في قانون العقوبات الجزائري حيث نص على أن كل من أخفى أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة، كلها أو جزء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر أو بغرامة من 100.000 إلى 500.000 دينار جزائري.[4]

كما وردت صورة الإخفاء أيضا في المادة 43 من القانون 01/06 المتعلق بالوقاية من الفساد ومكافحته إذ يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 200.000 إلى

---

[1] لمادتين 02 و03 من الامر رقم 156/66 لمتضمن ق.ع.ج ،السالف الذكر.

[2] عبد النور بشان، المتابعة الجزائية بين السرية والعلنية "دارسة مقارنة «، مذكرة لنيل شهادة الماجيستير كلية الحقوق والعلوم السياسية، جامعة الجزائر1، الجزائر، 2011، ص29.

[3] عبد النور بشان، نفس المرجع، ص 32.

[4] المادة 387من الأمر رقم 156/66 المتضمن ق.ع.ج، السالف الذكر.

1.000.000 دينار جزائري كل من أخفى كليا أو جزئيا العائدات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القانون.[1]

وعليه يتبين من خلال هاتين المادتين أن هذه الجريمة تقوم على ركنين أساسيين هما: علم الشخص الخافي بأن الأشياء محل الإخفاء متحصلة من جناية أو جنحة، بالإضافة إلى حيازتها وإخفائها عمدا وفي هذا الإطار جاءت المادة 121 من القانون 14/25 المتضمن ق.إ.ج لتجيز لعون أو ضابط الشرطة القضائية المأذون له والمسخر لتنفيذ العملية اللجوء إلى أسلوب إخفاء الأشياء المتحصلة من الجريمة بغرض إيهام الأشخاص المشتبه فيهم بأنه جزء من النشاط الإجرامي، وذلك دون أن يترتب عن هذه الأفعال قيام مسؤولية جزائية في حقه.[2]

وكمثال على ذلك، في قضايا اختراق الأنظمة الأمنية قد يباشر المتسرب مهامه كمبرمج داخل مؤسسة مستهدفة من طرف قراصنة إلكترونيين حيث يتولى رصد محاولات الاختراق ومتابعتها مع نقل المعلومات والمعطيات ذات الصلة إلى الجهات الأمنية المختصة بما يسمح بإحباط النشاط الإجرامي وضبط مرتكبيه.[3]

هنا لا يكون للمتسرب أي دور مباشر في ارتكاب الجريمة إذ يقتصر عمله أساسا على جمع المعلومات ورصد النشاط الإجرامي.

الفرع الثاني: الشروط الخاصة بتنفيذ اجراء التسرب الالكتروني

اقّ المشرع الجزائري لعملية التسرب جملة من الشروط الشكلية والموضوعية وألزم باحترامها والتقيد بها وإلا كانت هذه العملية باطلة ولا يعتد بها قانونا وهي كالتالي:

---

[1] قانون رقم 01/06 المؤرخ في 21 محرم 1427، الموافق ل 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، ج.ر.ج.ج، عدد14، الصادرة بتاريخ 08 مارس 2006.

[2] الداودي مجراب، مرجع سابق، ص365.

[3] فوزي عمارة، اعتراض المراسلات تسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية ،مجلة العلوم الانسانية، ع 33، 2010، ص236.

1/ الشروط الشكلية:

باستقراء نص المادة 120 وما يليها من القانون 14/25 المتضمن قانون الإجراءات الجزائية يتبين أن الشروط الشكلية لمباشرة عملية التسرب تتمثل في:

أ-تحرير التقرير:

طبقًا لنص المادة 122 يحرر ضابط الشرطة القضائية المكلف بعملية التسرب تقريرا مسبقا يتضمن العناصر الضرورية المتعلقة بمعاينة الجرائم، باستثناء تلك التي من شأنها أن تعرض أمن الضابط أو العون المتسرب للخطر وبناءا عليه، فإن ضابط الشرطة القضائية ملزم بإعداد تقرير مفصل حول عملية التسرب على أن يتضمن هذا التقرير ما يلي:[1]

*العناصر الجوهرية لمعاينة الجريمة محل العملية في ظروف تضمن حماية وتأمين عدم تعرض ضابط أو عون الشرطة القضائية المتسرب لأي خطر.

*وجوب أن تكون الجريمة من بين الجرائم المحددة في المادة 114 من القانون 14/25.

* تحديد هوية وصفة ضابط أو عون الشرطة القضائية المكلف بتنفيذ العملية مع تدوين كافة المعلومات المتعلقة بالأشخاص المسخرين للعملية.[2]

وهنا تجدر الإشارة إلى أن الفئة الأولى المخول لها قانونا القيام بعملية التسرب تتمثل في ضباط وأعوان الشرطة القضائية وذلك تحت إشراف ومسؤولية ضابط الشرطة القضائية. وبالرجوع إلى قانون الإجراءات الجزائية يتضح أنه قد حدد الأشخاص الذين يتمتعون بصفة ضابط الشرطة القضائية[3] وهم:

[1] انظر المادة 120من ق.إ.ج.ج، السالف الذكر.

[2] فراح حمادي، مرجع سابق، ص 22-24.

[3] المادة 23 من القانون 25 /14المتعلق بقانون الاجراءات الجزائية، السالف الذكر.

رؤساء المجالس الشعبية البلدية، ضباط الدرك الوطني، الموظفون المنتمون إلى الأسلاك الخاصة للمراقبين، إضافة إلى محافظي وضباط الشرطة التابعة للأمن الوطني....[1]

والملاحظ أن المشرع قد وسع من نطاق الأشخاص الذين يتمتعون بصفة الضبطية القضائية مقارنة بما كان معمولا به في القانون الملغى، كما خول لهم الإذن بمباشرة إجراء التسرب، غير أنه من الناحية العملية يتبين أنه لا يمكن لرؤساء المجالس الشعبية البلدية تطبيق هذا الإجراء لكونهم أشخاصا معروفين لدى عامة الناس فضلا عن أن مباشرة هذا الإجراء تتطلب قدرا عاليا من الدقة والخبرة لضمان تنفيذه على الوجه الأمثل، إضافة إلى ضرورة توفر تكوين خاص ومؤهلات مهنية دقيقة.

أما الفئة الثانية والمتمثلة في أعوان الضبط القضائي فهم موظفو مصالح الشرطة وذوو الرتب في الدرك الوطني، والدركيون، ومستخدمو المصالح العسكرية للأمن، ومفتشو الملاحة والعمل البحري، وكذا أعوان حرس السواحل التابعون للمصلحة الوطنية لحرس السواحل الذين لا يتمتعون بصفة ضابط الشرطة القضائية.[2]

أما الفئة الثالثة فتتمثل في الأشخاص المسخرين وقد ورد ذكرهم في نص المادتين 122 و123 من القانون 14/25المتضمن ق.إ.ج.ج وهم كل شخص ذكرا كان أو أنثى يتم الاستعانة به في عملية التسرب بناءا على تعيين من ضابط الشرطة القضائية المكلف

[1] ضباط الصف المنتمون إلى سلك الدرك الوطني الذين قضوا ثلاث (3) سنوات على الأقل في الخدمة، والموظفون التابعون للأسلاك الخاصة بالمفتشين والمحققين وحفاظ وأعوان الشرطة التابعة للأمن الوطني الذين أمضوا ثلاث (3) سنوات على الأقل، وضباط وضباط الصف العاملون بالمصالح العسكرية للأمن، إضافة إلى المتصرفين الإداريين في الشؤون البحرية وقادة الوحدات العائمة التابعين للمصلحة الوطنية لحرس السواحل، وكذا مفتشي الملاحة والعمل البحري وأعوان حرس السواحل المنتمين لنفس المصلحة، شريطة أن يكونوا قد قضوا في الخدمة بهذه الصفة مدة لا تقل عن ثلاث (3) سنوات.

[2] راوية مطماطي، عملية التسرب على ضوء قانون الإجراءات الجزائية14/25، مجلة حقوق الانسان والحريات العامة، المجلد10، العدد02، الجزائر، سنة 2025، ص411-412.

بتنسيق العملية، غير أن النصوص القانونية لم تحدد طبيعة هؤلاء الأشخاص أو مهامهم أو وضعيتهم القانونية كما لم تبين مستوى تكوينهم أو مؤهلاتهم.[1]

الجدير بالذكر في هذا السياق أنه عند مباشرة البحث والتحري في الجرائم التي حددها المشرع في نص المادة 114 من القانون 14/25 المتضمن ق.إ.ج.ج لا يلتزم ضباط الشرطة القضائية بالاختصاص الإقليمي، بل يمتد اختصاصهم ليشمل كامل الإقليم الوطني وذلك بهدف ضمان سرعة وفعالية إجراءات التحقيق وتفادي تجزئة العملية على عدة دوائر إقليمية.[2]

ب/الإذن بمباشرة عملية التسرب:

طبقًا لنص المادة 120 من القانون 14/25 المتضمن ق.إ.ج.ج يتطلب تنفيذ عملية التسرب الحصول على إذن مسبق من وكيل الجمهورية المختص إقليميا أو من قاضي التحقيق بعد إخطار وكيل الجمهورية وعليه، يجب أن يكون هذا الإذن قانونيا، مكتسبا لصفة الوثيقة الرسمية وأن يكون مكتوبا مما يستبعد الإذن الشفوي كما يشترط أن يكون الإذن مسببا من خلال بيان الدوافع والمبررات التي استندت إليها النيابة العامة في إصدار رهو يعد تسبيب الإذن ميزة إيجابية إذ يتيح للجهات القضائية إمكانية تقييم مدى صحته والتأكد من مشروعيته والحكم ببطلانه في حال صدوره دون استيفاء الشروط القانونية.[3]

كما يشترط أن يتضمن الإذن بيان الجريمة التي تبرر اللجوء إلى هذه التقنية على ألا تخرج هذه الجريمة عن نطاق الجرائم المحددة على سبيل الحصر في المادة 114 من القانون 14/25 المتضمن ق.إ.ج.ج كما يجب أن يشتمل الإذن أيضا على هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته والملاحظ أن المشرع لم يرتب جزاء البطلان على إغفال بعض البيانات، مثل عدم ذكر الجريمة أو هوية ضابط الشرطة القضائية بخلاف ما

---

[1] أمينة معزيز، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، المجلد6، العدد 11، الجزائر، سنة 2014، ص260.

[2] المادة 24 الفقرة07 من القانون 14/25 المتعلق ق.ا.ج.ج، السالف الذكر.

[3] فوزي عمارة، مرجع سابق، ص248.

يتعلق بعنصري الكتابة والتسبيب إذ يتبين من استقراء نص المادة 124 أنه يشترط أن يكون الإذن مكتوبا ومسببا تحت طائلة البطلان.[1]

ج/ مدة عملية التسرب:

تنص المادة 124 من القانون رقم 14/25 المتضمن ق.إ.ج.ج على أن مدة عملية التسرب تحدد بأربعة (04) أشهر قابلة للتجديد وفق نفس الشروط المذكورة أعلاه أي بإذن من وكيل الجمهورية أو من قاضي التحقيق بعد إخطار وكيل الجمهورية، يمكن للقاضي الذي رخص بإجراء عملية التسرب أن يأمر بوقفها في أي وقت قبل انقضاء مدتها وقد عالج المشرع في هذا الإطار مسألة بالغة الأهمية تتمثل في حالة صدور أمر بوقف العملية بينما يتعذر على العضو المتسرب الانسحاب الفوري أو التوقف المفاجئ عن نشاطه داخل الجماعة الإجرامية دون مبرر لما قد يشكله ذلك من خطر على حياته وحياة من يعولهم[2].

ولذلك أجاز له المشرع مواصلة نشاطه لمدة كافية تمكنه من إنهاء العملية في ظروف تضمن سلامته دون أن يتحمل مسؤولية جزائية على ألا تتجاوز هذه المدة أربعة (04) أشهر وإذا تعذر عليه التوقف خلال هذه الفترة يمكن للقاضي الترخيص بتمديدها لمدة إضافية لا تتجاوز أربعة (04) أشهر أخرى[3].

تجدر الإشارة إلى أن مدة عملية التسرب في التشريع الجزائري المحددة بأربعة أشهر تتوافق مع المدة المعتمدة في قانون الإجراءات الفرنسي في المادة83-706.[4]

02/الضوابط الموضوعية:

بالإضافة إلى الشروط الشكلية المشار إليها أعلاه، يقتضي اللجوء إلى إجراء التسرب توافر مجموعة من الضوابط الموضوعية والتي نص عليها المشرع في قانون الإجراءات الجزائية

---

[1]- عز الدين دواعي، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية المقارن، المجلة الأكاديمية للبحث القانوني، مجلد 16، عدد 02 ،2017، ص 277.

[2] راوية مطماطي، المرجع السابق، ص 420.

[3] المادة 126 الفقرة 2 من القانون 14/25 المتضمن ق.إ.ج.ج، السالف الذكر.

[4] أمينة معزيز، مرجع سابق، ص 242-252.

حيث اشترط أن تفرض ضرورات التحري أو التحقيق اتخاذ هذا الإجراء، وفي المقابل إذا توافرت أدلة كافية تدعم حالة الاشتباه أو تعزز قيام الاتهام فإن مبدأ الضرورة لاتباع إجراء التسرب ينتفي ويصبح هذا الإجراء غير مبرر من الناحية القانونية والإجرائية وعليه لا يصار إلى تطبيق هذه التقنية إلا في الحالات التي تثبت فيها الضرورة القصوى.[1]

يشترط اللجوء إلى إجراء التسرب في الحالات التي تتسم بندرة الأدلة أو بصعوبة الحصول عليها بالقدر الكافي لتحريك الدعوى العمومية واتخاذ ما يلزم من إجراءات قضائية بشأنها

كما قيد المشرع استخدام هذا الأسلوب بضرورة تلقه بجرائم محددة تتسم بالخطورة والتعقيد بحيث لا يعد الأمر بإجراء عمليات التسرب متاحًا على إطلاقه لكافة الجرائم، وإنما يقتصر على فئة محددة وردت على سبيل الحصر في المادة 114 من قانون رقم 14/25 المتضمن ق.إ.ج.ج وتشمل هذه الجرائم: القتل العمد، والجرائم المتعلقة بالمخدرات والمؤثرات العقلية، والجريمة المنظمة العابرة للحدود الوطنية، والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المرتبطة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، والتهريب، والاتجار بالبشر، والاتجار بالأعضاء وتهريب المهاجرين، واختطاف الأشخاص.[2]

يشترط اللجوء إلى إجراء التسرب في الحالات التي تتسم بندرة الأدلة أو بصعوبة الحصول عليها بالقدر الكافي لتحريك الدعوى العمومية واتخاذ ما يلزم من إجراءات قضائية بشأنها

وعليه فإن استخدام هذا الأسلوب خارج نطاق هذه الجرائم المحددة قانونا يعد مخالفا للقانون ويترتب عليه بطلان الإجراء.[3]

---

[1] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، ط04، دار هومة للطباعة والنشر والتوزيع، الجزائر،2025، ص 134.

[2] انظر المادة 114 من ق.إ.ج.ج، السالف الذكر.

[3] شمس الدين مهدي، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي ،جامعة محمد خضير، بسكرة، الجزائر،2014 ،

المطلب الثاني:
اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

استنادا إلى أحكام المادة 303 مكرر من قانون العقوبات فإن المساس بحرمة الحياة الخاصة للأشخاص يعد جريمة يعاقب عليها القانون ويشكل ذلك أصلا عاما يكرس حماية الخصوصية غير أنه وكما هو الشأن بالنسبة لكل مبدأ ترد عليه استثناءات تفرضها ضرورات البحث والتحري في بعض الجرائم

وفي هذا الإطار أجاز المشرع اللجوء إلى بعض إجراءات المراقبة شريطة إخضاعها لجملة من الضوابط والشروط التي تحول دون التعسف في المساس بالحياة الخاصة وعليه سنتناول هذا الموضوع من خلال التطرق إلى مفهوم المراقبة في (الفرع الأول) على أن نخصص (الفرع الثاني) لبيان الضوابط القانونية المنظمة لهذا النوع من المراقبة.

الفرع الأول: مفهوم اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تمهيدا لدراسة نظام المراقبة باعتباره من الإجراءات الاستثنائية التي تمس بالحياة الخاصة للأفراد، يقتضي الأمر تحديد مفهومه وضبط إطاره القانوني وعليه سيتم التطرق في هذا الفرع إلى تعريف المراقبة وبيان خصائصها الأساسية، ثم الانتقال إلى عرض الضوابط القانونية التي تحكم ممارستها في الفرع الموالي.

اولا: تعريف اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

نظرا لأهمية البالغة لإجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وما قد يترتب عنها من اضرار تمس حرمة الحياة الخاصة للإنسان كامن لا من التطرق الى المقصود لكل اجراء على حدا.

1- اعتراض المراسلات:

يعد هذا الإجراء من إجراءات التحقيق التي تباشر خفية دون علم الشخص المشتبه فيه ويقوم على تتبع المراسلات أو الاتصالات التي يجريها، وذلك بأمر صادر عن السلطة القضائية المختصة ووفق الشكل المحدد قانونا بهدف الحصول على دليل غير مادي

يتعلق بالجريمة وتتولى الضبطية القضائية تنفيذ هذا الإجراء سواء عبر الاتصالات السلكية أو اللاسلكية[1].

وهو ما نص عليه المشرع من خلال نص المادة 114الفقرة الثانية (02) من القانون 25/ 14 المتضمن ق.إ.ج.ج.[2]

2-تسجيل الأصوات

يقصد بالتسجيل الصوتي العملية التي يتم من خلالها تحويل الموجات الصوتية المؤقتة الصادرة عن الكلام إلى إشارات أو موجات ذات طبيعة أخرى قد تكون رقمية أو ممغنطة قابلة للحفظ والاسترجاع ويتم ذلك بواسطة جهاز مخصص يقوم بترجمة هذه الموجات الصوتية إلى إشارات قابلة للتخزين.[3]

يقصد بالتسجيل الصوتي تسجيل أحاديث المشتبه فيه وشركائه المتعلقة بوقائع معيشية أو وقائع منصوص عليها في المادة 114 الفقرة الثالثة (03) من القانون 14/25 المتضمن ق.إ.ج.ج ويتم هذا التسجيل خفية ودون علم المعني ودون رضاه وفقا لما يجيزه القانون وفي الحدود التي يحددها.[4]

كما يعرف بانه التنصت على المحادثات الخاصة المتعلقة بشخص أو أكثر مشتبه فيهم أو الاستماع إليها أو تسجيلها، إلا في الحالات التي يجيزها القانون وبموجب أمر قضائي صادر عن الجهة المختصة.[5]

---

[1] يوسف بلخضر، إجراءات البحث والتحري الخاصة في التشريع الجزائري، مذكرة لنيل شهادة ماستر أكاديمي في الحقوق تخصص قانون اعمال، كلية الحقوق والعلوم السياسية برج بوعريريج، الجزائر،2021/2020ص 24-26.

[2] أنظر نص المادة 114 من ق.إ.ج، السابق الذكر.

[3] خالد ضو، مبدأ اليقين القضائي في الأحكام الجنائية، مجلة الفكر القانوني السياسي، المجلد 06، العدد1، الجزائر،2022، ص 522.

[4] أنظر نص المادة 114 الفقرة 03 من ق.إ.ج.، السابق الذكر.

[5] يوسف بلخضر، مرجع السابق، ص27.

من خلال التعاريف السابقة يعد اللجوء إلى أسلوب التسجيل الصوتي أو التنصت على المكالمات الهاتفية من إجراءات التحري الخاصة في المادة الجزائية، والتي تمس بالحق في الحياة الخاصة للأفراد ولا يجوز اتخاذ هذا الإجراء إلا بموجب إذن مسبق صادر عن وكيل الجمهورية أو قاضي التحقيق[1]، كل حسب اختصاصه وتحت رقابتهما المباشرة وذلك وفقا لأحكام المادة 114 الفقرة الأخيرة من قانون الإجراءات الجزائية[2]

3-التقاط الصور

يقصد بها بمحاكاة أو استنساخ الشخص كل عملية تهدف إلى تقليد أو تمثيل مظهره أو هويته، وذلك باستعمال الوسائل التقنية الحديثة بما في ذلك الصور الفوتوغرافية والصور الإلكترونية.[3]

كما عرفها المشرّع الجزائري في الفقرة الثالثة من المادة 114 ب "التقاط" أو "تثبيت" الصور أو الأصوات على وسائط أو أجهزة حساسة، باعتباره إجراءا تقنيا يهدف إلى تسجيل صوت أو صورة أو وضعية أشخاص مشتبه فيهم أو غيرهم، على الحالة التي كانوا عليها وقت التصوير بغرض استعمال محتوى التسجيل كدليل مادي أمام القضاء ويعد هذا الإجراء وسيلة لإثبات العلاقة بين الأشخاص من حيث الزمان والمكان والظروف.[4]

ومع التطور العلمي والتكنولوجي أصبح من الممكن استعمال وسائل حديثة ذات تقنيات متقدمة تسمح بالتقاط صور ذات دقة عالية، خاصة خلال الفترة الليلية أو في ظروف خفية من خلال أجهزة تعتمد على الأشعة تحت الحمراء أو غيرها من التقنيات البصرية الدقيقة والتي تتيح تسجيل صور واضحة ودقيقة كما تتميز بعض هذه الأجهزة بصغر حجمها وسهولة إخفائها داخل أماكن خاصة بهدف إجراء عمليات التصوير السري وتعد الصور من

---

[1] أنظر نص المادة 114الفقرة 04 من ق.إ.ج.ج، السابق الذكر.

[2] يوسف بلخضر، مرجع السابق، ص27.

[3] امين بحري، دور التكنولوجيا في الاثبات الجنائي، مذكرة لنيل شهادة الماستر ،تخصص القانون الجنائي والعلوم الجنائية ،جامعة مولود معمري، تيزي وزو، الجزائر ،2025، ص 35.

[4] رشيد شميشم، الحق في الصورة، مجلة العلوم الإنسانية والاجتماعية، جامعة المدية، المجلد8، العدد3، الجزائر، 2008، ص165-169.

أفضل وسائل الإثبات في كشف الوقائع وتحديد الحالة محل النزاع، وقد اعتمدها المشرع كوسيلة من وسائل الإثبات التي لا يمكن إغفالها في العمل القضائي، لما لها من دور في إظهار الحقيقة ويتم استعمال الكاميرات في الأماكن العامة والخاصة في إطار ما يسمح به القانون بهدف توثيق الوقائع وجمع الأدلة.[1]

وهناك من عرفه بانه عملية قانونية استثنائية أقرها المشرع تهدف إلى حفظ وتسجيل الأصوات باستعمال أجهزة إلكترونية متطورة قصد إعادة استخدامها عند الاقتضاء أو الضرورة، لا سيما في مجال الإثبات الجنائي ويعد الصوت من الخصائص المميزة التي يمكن الاعتماد عليها في تحديد هوية الشخص وتثبيت نسبته إليه.[2]

ثانيا/التكييف القانوني لتسجيل الأصوات

تباينت الآراء الفقهية بخصوص التكييف القانوني لتسجيل الأصوات حيث انقسم الفقه إلى ثلاثة اتجاهات رئيسية وذلك على النحو الآتي:

الاتجاه الأول: يرى أن تسجيل الأصوات يعد من أعمال التفتيش وبالتالي فإنه يخضع للقيود المنظمة للتفتيش ويستند هذا الاتجاه إلى أن عملية التسجيل تتفق مع فكرة التفتيش من حيث الكشف عن السرية والبحث في مكنونها، إذ يتم من خلاله الاطلاع على ما هو مستتر داخل نطاق السر مما يؤدي إلى انتهاك الخصوصية بهدف الوصول إلى الحقيقة.[3]

وقد تم انتقاد هذا الاتجاه على أساس أن التفتيش يهدف إلى ضبط الأدلة المادية المتعلقة بالجريمة، في حين أن الحديث الهاتفي لا يعد شيئا ماديا ملموسا كما أن القواعد الإجرائية المنظمة لتسجيل الصوت في التشريع تختلف بصفة عامة عن القواعد المقررة للتفتيش.[4]

---

[1] خديجة هلال– حيرش خديجة، مشروعية الصوت والصورة في الاثبات الجنائي في الإجراءات الجزائية الجزائري، مذكرة مكملة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة سعيدة، الجزائر، 2021، ص 52.

[2] منيرة عبيزة، التسجيل الصوتي كدليل للإثبات، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد06، العدد1، الجزائر، 2023، ص 1602.

[3] ياسر الامير فاروق، مراقبة الأحاديث الخاصة في قانون الإجراءات الجزائية، دار المطبوعات الجامعية، القاهرة، مصر، 2009، ص 182.

[4] ابتسام بغو، مرجع سابق، ص 52.

الاتجاه الثاني: يرى أن عملية تسجيل الأصوات تعد نوعا من الاطلاع على الرسائل باعتبار أن الرسالة قد تتضمن بعض أسرار الحياة الخاصة للمرسل وغيره، وأن تسجيل الأصوات يهدف إلى ضبط محتوى مماثل لما تتضمنه الرسائل المكتوبة في حين أن التسجيلات الصوتية تتعلق بأحاديث شفوية ،وقد انتقد هذا الاتجاه لافتقاره إلى أساس قانوني سليم إذ لا يمكن اعتبار التسجيل الهاتفي رسالة بالمعنى القانوني شأنه شأن الخطابات لاختلافهما من حيث الطبيعة المادية والشكل.[1]

الاتجاه الثالث: يرى أن عملية تسجيل الأصوات تعد إجراءا ذا طبيعة خاصة يشبه التفتيش من حيث الغاية غير أنه لا يعتبر تفتيشا بالمعنى القانوني، بل هو إجراء مستقل بذاته منفصل عن إجراءات التفتيش وكذا عن إجراءات ضبط المراسلات وقد أخذ المشرع الجزائري بهذا الاتجاه ضمن قانون الإجراءات الجزائية.[2]

الفرع الثاني: ضوابط اتخاذ اجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يقصد بضوابط المراقبة تلك القيود القانونية التي تفرض على الجهة المختصة بإصدار الأمر بالمراقبة وكلما كانت هذه الضوابط واضحة ومحددة وكافية، كانت ممارسة المراقبة مقيدة ومحصورة في إطار الهدف الذي شرعت من أجله وعلى العكس فإن غموض هذه الضوابط أو قصورها يفتح المجال أمام سلطة تقديرية واسعة في اللجوء إلى المراقبة وهو ما يؤدي إلى تفاوت في تطبيقها من جهة إلى أخرى، ويشكل خطرا حقيقيا على حرمة الحياة الخاص

وتكمن الغاية من إقرار هذه الضوابط في تحقيق توازن دقيق بين حق الفرد في الخصوصية وحق المجتمع في ملاحقة الجرائم ومعاقبة مرتكبيها، بحيث لا تنتهك الحريات ولا تستباح الحرمات وفي الوقت نفسه لا تقيد يد المجتمع عن أداء دوره في مكافحة الجريمة وإنزال العقاب بالجناة.[3]

---

[1] ياسر الامير فاروق، مرجع سابق، ص 183.

[2] ابراهيم يامة، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد11، عدد02، الجزائر، 2019، ص148-152.

[3] أسماء عنتر، أطروحة مقدمة لنيل شهادة الدكتوراه، إجراءات التحقيق القضائي الخاصة، دراسة مقارنة، جامعة عبد الحميد بن باديس مستعانم، الجزائر،2021، ص 45.

يمكن تصنيف ضوابط المراقبة إلى نوعين رئيسيين: ضوابط موضوعية وأخرى شكلية حيث ترتبط الضوابط الموضوعية بشروط نشوء الحق في اللجوء إلى المراقبة، بينما تتعلق الضوابط الشكلية والإجرائية بسلامة إجراءات المراقبة وكيفية تنفيذها بما يضمن صحة النتائج المتحصل عليها منها ومشروعية الأدلة المستمدة منها.[1]

وعليه سنتطرق في هذا الفرع الى توضيح هذه الضوابط المفروضة على المراقبة الإلكترونية بهدف التحقق من سلامة الدليل الإلكتروني ومشروعيته، وضمان عدم المساس بالحقوق الشخصية وحرمة الحياة الخاصة وبناءا على ذلك سيتم تقسيم هذا الفرع كالتالي:

أولا/الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

كأصل عام لا يجوز اعتراض المراسلات أو استراق السمع إلى المحادثات وتسجيلها أو التقاط الصور خفية دون علم وموافقة مسبقة من الشخص المعني بها غير أن مقتضيات التحقيق وما تفرضه من ضرورات قد تبرر اللجوء إلى مثل هذه الإجراءات، خاصة في الجرائم المنصوص عليها في الفقرة الأولى من المادة 114من قانون 14/25 المتضمن ق.إ.ج.ج حيث تقدم مصلحة التحقيق في هذه الحالات على مصلحة الحفاظ على سرية الحياة الخاصة.

أ/ السلطة المختصة بإجراء هذه العمليات:

رغم أن قاضي التحقيق لا يتولى بنفسه عملية اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، إلا أنها تتم تحت إشرافه ورقابته المباشرة فهذه الإجراءات غالبا ما تتطلب استخدام تقنيات متخصصة قد لا يكون القاضي ملما بها بشكل مباشر، مما يستدعي الاستعانة بخبراء مختصين في هذا المجال ويقتصر دور قاضي التحقيق على ضمان تنفيذ هذه العمليات في إطارها القانوني، مع التقيد بالأحكام والإجراءات التي يفرضها القانون.[2]

---

[1] احمد عبد الله حاج، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي في التشريع الجزائري، مجلة الاجتهاد في الدراسات القانونية والاقتصادية، المجلد08، العدد05، الجزائر، 2019، ص 225-320.

[2] فوزي عمارة، مرجع سابق، ص 238.

لكن الإشكال الذي يطرح في هذا السياق هو: إذا كان بإمكان قاضي التحقيق انتداب من يقوم بهذه الإجراءات نيابة عنه، فما حدود هذه الإنابة؟ وما مدى خضوع من ينتدب لرقابة القاضي والتقيد بالضوابط القانونية أثناء تنفيذها؟ وهل تبقى المسؤولية القانونية قائمة على عاتق قاضي التحقيق رغم عدم مباشرته لهذه العمليات بنفسه.[1]

نظرا لحداثة هذه الإجراءات في قانون الإجراءات الجزائية الجزائري يمكن القول انه استنادا إلى الفقرة الرابعة من المادة من 114قانون 14/25فإن الإشراف المباشر على هذه العمليات ينبغي أن يظل حكرا على قاضي التحقيق لما تنطوي عليه من خطورة وارتباطها الوثيق بالحريات الأساسية والحق في الخصوصية الذي كفله الدستور.[32]

وعليه لا ينبغي ترك تنفيذ هذه الإجراءات والإشراف عليها لضباط الشرطة القضائية لما قد ينطوي عليه ذلك من مخاطر، إذ إن توجه رجل الشرطة غالبا ما يكون منصبا على البحث عن أدلة الإثبات أكثر من أدلة النفي وهو ما قد يفضي إلى تجاوزات تمس في المقام الأول الحريات الفردية وحرمة الحياة الخاصة.[4]

وإذا كان المشرع قد أسند لقاضي التحقيق مهمة الإشراف المباشر على هذه العمليات فإنه في المقابل أجاز له، فيما يتعلق بتنفيذها أن ينيب أحد ضباط الشرطة القضائية للقيام بها تحت إشرافه (المادتين 114 و115 من ق.ا.ج.ج). [5]

ب/ ميقات ومكان إجراء هذه العمليات:

يضع قانون الإجراءات الجزائية الجزائري قيودا زمنية ومكانية حسب المادة 116 الفقرة الثانية من القانون 14/25 المتضمن ق. إ.ج. ج على إجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، حيث أجاز تنفيذ هذه العمليات في جميع ساعات النهار والليل

[1] فوزي عمارة، نفس المرجع، ص238-239.

[2]

[3] انظر نص المادة 114 الفقرة 04، ق.إ.ج.ج السالف الذكر.

[4]صالح براهيمي، الإثبات بشهادة الشهود في القانون الجزائري، أطروحة دكتوراه في الحقوق، جامعة مولود معمري، تيزي وزو الجزائر، 2016، ص 285.

[5] صالح براهيمي، نفس المرجع، ص 286.

وفي مختلف الأماكن العامة والخاصة واستثناءا من ذلك يتمثل القيد الوحيد الذي نص عليه المشرع صراحة في ضرورة اتخاذ الإجراءات الكفيلة بضمان احترام سر المهنة، وهو ما يترتب عنه صون سرية المراسلات والمحادثات الهاتفية، لاسيما تلك التي تتم بين المحامي وموكله.[1]

ومتى تجاوز الملزم بكتمان السر المهني حدود وظيفته ورسالته المهنية وأصبح طرفا فاعلا مع المتهم في الجرائم المنصوص عليها في المادة 114 الفقرة الأولى من القانون 14/25 المتضمن ق. إ. ج. ج أو شريكا له فيها، فإنه لا يجوز له التذرع بحماية السر المهني باعتبار أن هذه الحماية تقررت للسر المهني ذاته وليس للشخص القائم به وإلى جانب هذا القيد الصريح، يمكن استنتاج قيد آخر رغم عدم النص عليه من طرف المشرع، يتمثل في استبعاد مقار السفارات والقنصليات الأجنبية من نطاق الأماكن القابلة لمباشرة هذه الإجراءات.[2]

ت/عدم مسؤولية القائم والمشرف على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

ان الأفعال المتمثلة في الاعتداء على الحياة الخاصة للأفراد، كالتقاط صورهم أو تسجيل أصواتهم خلسة أو دخول مساكنهم دون رضاهم وموافقتهم، في أي وقت من ساعات النهار أو الليل بما في ذلك الكسر أو تسلق الجدران أو فتح الأقفال، وكذا استعمال أساليب الخداع أو إفشاء السر المهني، تعد في الأصل جرائم يعاقب عليها القانون، غير أنه لا تقوم المسؤولية الجنائية بشأنها في حق القائمين بها إذا ارتكبت أثناء تنفيذ عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بموجب إذن صادر عن قاضي التحقيق وفي

إطار تحقيق قضائي يتعلق بالجرائم المنصوص عليها في 114 الفقرة الأولى من المادة من قانون الإجراءات الجزائية.[3]

---

[1] انظر نص المادة 116 الفقرة 02، ق.ا.ج.ج السالف الذكر.

[2] فوزي عمارة، مرجع سابق، ص 240.

[3] انظر المادة 114 الفقرة الأولى من ق.إ.ج.ج، السالف الذكر.

ث/ضرورة لجوء قاضي التحقيق إليها:

ان مجرد وقوع إحدى الجرائم المنصوص عليها في الفقرة الأولى من المادة 114من قانون الإجراءات الجزائية الجزائري لا يعد سببا كافيا وحده للجوء قاضي التحقيق إلى إجراء اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور بحق الشخص محل المتابعة، بل يتعين فضلا عن ذلك أن تقتضي مصلحة التحقيق اللجوء إلى هذه التدابير بحيث يكون الإذن بها ذا فائدة في كشف الحقيقة[1].

كما يشترط كذلك أن تقوم دلائل قوية على وقوع الجريمة ونسبتها إلى المتهم على نحو تشير فيه القرائن الجدية والكافية إلى شخص أو أشخاص يشتبه في ارتكابهم للجريمة أو حيازتهم لمعلومات تفيد في إظهار الحقيقة أو امتلاكهم أشياء ذات صلة بها، وفي جميع الأحوال فإن تقدير مدى ضرورة اللجوء إلى هذه الإجراءات من عدمه يبقى من السلطة التقديرية المخولة لقاضي التحقيق وفقا لأحكام المادة114 من قانون الإجراءات الجزائية الجزائري.[2]

ثانيا/الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يعد الاستثناء عن القاعدة العامة هو مشروعية اعتراض مراسلات الأشخاص وتسجيل أصواتهم والتقاط صورهم، حيث يهدف إقرار هذا النوع من الإجراءات إلى تحقيق توازن بين حق الفرد في الحياة الخاصة وسرية مراسلاته، وبين حق المجتمع في مكافحة أخطر الجرائم بوسائل فعالة تتناسب مع خطورتها.[3]

بالنظر إلى طبيعة الجرائم التي تكون محلا لهذه العمليات فقد خصها المشرع بجملة من الشروط الشكلية يمكن إجمالها فيما يلي:

أ/ شكل الإذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور

---

[1] نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، المجلد 4 العدد 11، الجزائر، 2017، ص 908-910.

[2] هدى زوزو، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسية والقانون، العدد 11، الجزائر، 2014، ص117-120.

[3] منيرة عبيزة، مرجع سابق، ص 1602.

عندما اشترط المشرع في الفقرة الرابعة من المادة من القانون 14/25 المتضمن 114 ق.ا.ج.ج انه لإجراء هذه العمليات في إطار تحقيق قضائي وبموجب إذن صادر عن قاضي التحقيق، فإن ذلك يفيد منع ضباط الشرطة القضائية حتى في حالة الندب من مباشرة هذه الإجراءات ما لم يكونوا حائزين على ذلك الإذن ويهدف ذلك إلى كون اعتراض المراسلات وتسجيل الأصوات والتقاط الصور تعد من إجراءات التحقيق التي تستلزم ضمانات قانونية خاصة.[1]

ومن الناحية القانونية، لا يجوز لقاضي التحقيق إصدار إذن بإجراء عمليات اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور في حال تعلق الأمر بوجود دلائل على ارتكاب الجرائم المنصوص عليها في المادة 114 الفقرة الاولى من القانون 14/25 المتضمن ق. إ. ج. في المستقبل ما دام أنه لم يخطر بعد بملف الدعوى ولم تعرض عليه وقائعها بصورة رسمية.[2]

لم يشترط المشرع الجزائري شكلا معينا للإذن الصادر عن قاضي التحقيق بشأن إجراء هذه العمليات، غير أنه ألزم بأن يكون هذا الإذن مكتوبا وأن يتضمن كافة العناصر التي تسمح بتحديد الاتصالات المراد اعتراضها والأماكن المعنية سواء كانت سكنية أو غير سكنية إضافة إلى بيان الجريمة التي تبرر اللجوء إلى هذه التدابير، كما يجب أن يحدد مدة تنفيذ هذه العمليات على ألا تتجاوز أربعة أشهر قابلة للتجديد ضمن نفس الشروط وذلك وفقا لنص المادة المادة 116 الفقرة الثانية من القانون 14/25 المتضمن ق.ا.ج.ج.[3]

يلاحظ على المادة محل الدراسة جملة من الملاحظات من أهمها

أنها قد قصرت الإذن على تدبير اعتراض المراسلات دون أن تمتد صراحة إلى عمليتي التسجيل الصوتي أو السمعي البصري، كما يؤخذ على المشرع الجزائري أنه لم يراع العامل

---

[1] عبد القادر رويسي، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة مستغانم، العدد03، الجزائر،2017، ص41.

[2] فوزي عمارة، مرجع سابق، ص 241.

[3] جميلة ملحق، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 15، العدد 42، الجزائر، 2015، ص 178.

الزمني، إذ لم يحدد عدد مرات تجديد هذا الإذن، ولم ينص كذلك على إمكانية قيام قاضي التحقيق الذي أصدره بتوقيفه قبل انتهاء المدة المحددة فيه.

ومن جهة أخرى، لم يلزم المشرع بتسبيب هذا الإذن من طرف قاضي التحقيق، الأمر الذي يضعف من ضمانات الدفاع في مواجهة هذا الإجراء كما أنه لم يشترط صدور الإذن بناءا على طلبات النيابة العامة ولم يشر إلى وجوب إخطار وكيل الجمهورية به[1].

وإضافة إلى ذلك لم يرتب المشرع أي جزاء على مخالفة أحكام هذه المادة 116 رغم أنه استعمل في صدرها عبارة "يجب" الدالة على الإلزام مما يثير التساؤل حول جدوى الإلزام في غياب الجزاء المترتب عن مخالفته[2].

ولعل أبرز ملاحظة تثير الانتباه هي استعمال المشرع لمصطلح الإذن (autorisation) بدلا من مصطلح الأمر(ordonnance)الذي يستخدمه عادة في أوامر قاضي التحقيق وهو ما يطرح تساؤلا حول ما إذا كان هذا الاختيار يحمل دلالة قانونية مقصودة أم أنه مجرد تنوع في الصياغة الاصطلاحية، وإذا سلمنا بفرضية التنويع في المصطلحات يثور تساؤل آخر حول مدى إمكانية الطعن بالاستئناف في مثل هذا الإذن من طرف النيابة العامة خاصة وأنها تعد طرفا في الخصومة الجزائية.[3]

اما في حالة التسليم بالفرضية الأولى أي القول بأن المشرع تعمد استعمال مصطلح الإذن بدل الأمر لاعتبار خاص، فيمكن القول إن هدفه المحتمل من ذلك هو استبعاد إمكانية الطعن بالاستئناف في هذا الإجراء، باعتبار أنه يتعلق بإذن وليس بأمر كما أن طبيعة هذا الإذن ترتبط بإجراءات تتسم بقدر كبير من السرية والخفاء والحذر حتى لا تكشف وتفقد الغاية المرجوة من اللجوء إليها[4].

---

[1] عبد القادر الرويسي، مرجع سابق، ص 52.

[2] فوزي عمارة، مرجع سابق، ص 242.

[3] إسماعيل بن يحي، مرجع سابق، ص85.

[4] إسماعيل بن يحيى، مرجع سابق، ص 86

ب/ اجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

ان الإذن الممنوح لضابط الشرطة القضائية المنتدب من طرف قاضي التحقيق للقيام بتدابير اعتراض المراسلات وتسجيل الأصوات والتقاط الصور يخول له الاستعانة بأهل الخبرة حيث يجوز له تسخير كل عون مؤهل تابع لمصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، وذلك قصد التكفل بالجوانب التقنية المرتبطة بتنفيذ هذه العمليات وفقا لنص المادة 117 من القانون 14/25 المتضمن الإجراءات الجزائية الجزائري.[1]

غير أن النصوص المنظمة لهذه التدابير لم تبين صراحة نطاق الاطلاع على التسجيلات المتحصل عليها من خلال هذه الإجراءات مما يثير إشكالا قانونيا حول مدى جواز اطلاع الفنيين المسخرين من طرف ضابط الشرطة القضائية المنتدب على مضمون التسجيلات الصوتية أو السمعية البصرية أو المراسلات المعترضة[2].

ويطرح هذا السكوت تساؤلا حول ما إذا كان الاطلاع يقتصر على قاضي التحقيق وضابط الشرطة القضائية المنتدب فقط، في حين يقتصر دور الفنيين على الجانب التقني المحض المتعلق بإنجاح العملية وضبطها دون الاطلاع على محتواها، أم أن نطاق هذا الاطلاع يمكن أن يمتد إليهم بحكم الضرورة التقنية التي تقتضيها طبيعة التنفيذ ويخول الإذن كذلك لضابط الشرطة القضائية المنتدب لإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، صلاحية اتخاذ الترتيبات التقنية اللازمة دون اشتراط الحصول على موافقة الشخص الذي يكون محل هذه التدابير وذلك وفقا لأحكام المادة 117من القانون 14/25 المتضمن قانون الإجراءات الجزائية الجزائري[3].

---

[1] انظر نص المادة 117 من ق.ا.ج.ج. السالف الذكر.

[2] صالح جزول، ضمانات مشروعية التصنت التلفوني واعتراض المراسلات في القانون الاجرائي الجزائري، مجلة نوميروس الأكاديمية، المجلد01 ، العدد02، الجزائر،2020، ص155-165.

[3] مختار خداوي، اجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر،2016/2015، ص 65.

كما أن المشرع الجزائري لم يضع قيودا على قاضي التحقيق أو الضابط المنتدب عند مباشرة هذه العمليات، سوى الالتزام باتخاذ الإجراءات الكفيلة بضمان عدم المساس بالسر المهني وفقا لما نصت عليه المادة 115 من القانون 14/25 المتضمن قانون الإجراءات الجزائية الجزائري وفيما يتعلق بعمليات تسجيل الأصوات والتقاط الصور، فإنه باستثناء القيد الوارد في المادة115 المشار إليها أعلاه، تصبح مختلف الوسائل الإجرائية مباحة من أجل بلوغ الهدف المنشود وفي هذا الإطار، قد تبدو بعض المبادئ الدستورية كالحريات الفردية وحرمة المساكن وسرية الاتصالات وحرمة الحياة الخاصة، وكأنها تتراجع أمام سلطة هذا الإذن خاصة إذا اكتفى بتسبيبه بعبارات عامة من قبيل ضرورة مقتضيات التحقيق[1].

ومن ثم يثور التساؤل حول ما إذا كان الإذن الصادر لقاضي التحقيق أو للضابط المنتدب في إطار هذه العمليات يشكل غطاءا قانونيا كافيا لرفع المسؤولية الجنائية عنهما بما قد يفتح المجال لاحتمال التعسف في استعمال السلطة[2].

كان الأجدر بالمشرع تفاديا لأي تعسف محتمل في استعمال السلطة أن يقرن هذه الأحكام بجزاءات صريحة عند مخالفة القواعد المنظمة لهذه العمليات، خاصة وأن الواقع العملي يثبت أن قاضي التحقيق رغم صفته، يظل بشرا معرضا للخطأ وعليه فإن من الضروري وضع ضوابط قانونية دقيقة تحد من سلطته التقديرية، بدل تركها دون رقابة فعالة أو آليات ردع واضحة. [3]

ت/محضر اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

ان النظر إلى طبيعة عمليات الاعتراض والتسجيل والتقاط الصور، فإنه لا يشترط انتظار بلوغها مرحلتها النهائية لتحرير محضر بشأنها بل يقتضي الأمر بالنظر إلى خضوعها لمراقبة مباشرة من قاضي التحقيق وتنفيذها من طرف ضابط الشرطة القضائية المنتدب

[1] ياسمين باينين، دور وسائل التكنولوجيا في الإثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر،2022 /2023، ص 72.

[2] يوسف بالخضر، مرجع سابق، ص 65.

[3] عمر شهياني، التسرب في قانون الإجراءات الجزائية الجزائري، أطروحة لنيل درجة الدكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر،2023، ص 220.

تحرير محاضر بشكل منفصل عن كل مرحلة من مراحل التنفيذ، وعليه يتم تحرير محضر خاص بالترتيبات التقنية، ومحضر للدخول إلى المساكن عند الاقتضاء، ومحضر لعملية الالتقاط، ومحضر للتثبيت، ومحضر للتسجيل الصوتي أو السمعي البصري، إضافة إلى محضر مستقل لعملية الاعتراض، وكذا محضر يتعلق بتسجيل المراسلات، وذلك وفق تسلسل الإجراءات المتخذة أثناء التنفيذ.[1]

يشار في هذا الإطار إلى أن محاضر عمليات الاعتراض تستكمل ببيان تاريخ وساعة الانتهاء منها، وفقا لما نصت عليه المادة 118 من القانون 14/25 المتضمن قانون الإجراءات الجزائية الجزائري كما يرفق بملف الدعوى محضر يتضمن وصفا أو نسخة من المراسلات أو الصور أو المحادثات التي من شأنها الإسهام في إظهار الحقيقة، وذلك طبقا لأحكام المادة 119 من نفس القانون14/25 المتضمن ق.إ.ج.ج وعند الاقتضاء إذا كانت المكالمات أو التسجيلات محل الاعتراض بلغة أجنبية، فإنه يتم ترجمتها بمساعدة مترجم يتم تسخيره لهذا الغرض.[2]

غير أنه يلاحظ بخصوص إعداد هذه المحاضر أن المشرع لم يحل سواء في المادة 114 على المواد المنظمة للشروط الشكلية الواجب توافرها في المحضر، ولا سيما تلك المتعلقة بضوابط تحريره كما أنه عند تنظيمه للاستعانة بالمترجم، لم يحل إلى الأحكام الخاصة بكيفيات تعيينه واستدعائه، خاصة المواد المتعلقة باستدعاء المترجم وأداء اليمين رغم أهمية ذلك لضمان حجية الترجمة، لم تنص صراحة على وجوب تحليف المترجم اليمين إذا لم يكن قد سبق له أداؤها.[3]

---

[1] شريفة طاهري، تأثير أدلة الإثبات على الاقتناع الشخصي للقضاء الجنائي، رسالة لنيل شهادة الماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2003، ص 65.

[2] أنيس الحسيب السيد المحلاوي، مدى مشروعية الوسائل التي تستخدم بشكل خفي كدليل في الإثبات الجنائي، مجلة كلية الشريعة والقانون، كلية الشريعة والقانون، جامعة الأزهر القاهرة، المجلد20 ، العدد04، مصر، 2018، ص 2760-2770.

[3] عبد القادر فلاح، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، جامعة الجيلالي بونعامة خميس مليانة، المجلد08 ، العدد 01، الجزائر، 2021، ص172-175.

وهذا لم يوضحه المشرع الجزائري في النصوص المنظمة لهذه التدابير هو كيفية حفظ التسجيلات والنسخ والصور المرفقة بملف الدعوى، إذ يثور التساؤل حول ما إذا كان يتم إيداعها في أحراز مغلقة ومختومة بختم قاضي التحقيق، على غرار ما هو معمول به في حالات الحجز العادية، أم أنها تحفظ دون إجراءات حماية كافية بما قد يفتح المجال لاحتمال التلاعب بها أو المساس بسلامتها، وعليه كان الأجدر بالمشرع في تقديرنا وبالنظر إلى خطورة المعطيات المتحصل عليها من هذه العمليات، أن يحيطها بنظام حماية خاص أو على الأقل مماثل للنظام المطبق على إجراءات الحجز في الحالات العادية[1].

فضلا عن ذلك لم يحدد المشرع المصير النهائي لهذه التسجيلات والنسخ والصور بعد إرفاقها بالمحاضر وما إذا كان يتم الاحتفاظ بها أو إتلافها عند انتهاء الغرض الذي أعدت من أجله، ويظل هذا الإشكال مطروحًا إلى حين تدخل المشرّع بالتعديل، أو صدور اجتهاد قضائي يضع حدا للغموض القائم في هذا الشأن.[2]

[1] عبد القادر فلاح، نفس المرجع، ص 185-194.

[2] إسماعيل بن يحي، مرجع سابق، ص85.

المبحث الثاني:
إجراءات المتابعة العامة للكشف عن الجريمة المعلوماتية

أقرّ المشرع الجزائري شأنه شأن العديد من التشريعات المقارنة مجموعة من القواعد والضوابط التي تهدف إلى متابعة مرتكبي الجرائم المعلوماتية وضمان حماية معطيات أنظمة الحاسب الآلي لاسيما في مرحلة جمع الاستدلالات، وتضطلع أجهزة الشرطة بدور محوري في هذه المرحلة، إذ تتولى المعاينة مكان وقوع الجريمة وضبط الأدلة المرتبطة بها والقبض على المشتبه فيهم، إضافة إلى القيام بكافة الإجراءات التي من شأنها الإسهام في كشف الحقيقة ويأتي ذلك في إطار التنسيق مع سلطات التحقيق قصد الوصول إلى حقيقة الواقعة وتحديد هوية مرتكبيها بدقة بما يحقق الفعالية المرجوة في مكافحة هذا النوع المستحدث من الجرائم.

في هذا المقام سيتم النظر في إجراء المعاينة الإلكترونية (مطلب أول) ثم بعد ذلك سيتم النظر في إجراء التفتيش الإلكتروني (مطلب ثاني).

المطلب الأول:
المعاينة الإلكترونية

تعد المعاينة من أهم وسائل الإثبات الجنائي في المسائل ذات الطابع المادي سواء من الناحية الإجرائية أو القانونية إذ تعتبر من أبرز الأعمال التي تضطلع بها الجهات المكلفة بالتحقيق الجنائي الأولي فهي تمكن من الوقوف على الأدلة التي يمكن من خلالها الوصول إلى الحقيقة وتكوين قناعة قضائية دقيقة بشأن وصف الأفعال المرتكبة، كما تتيح تصويرا واقعيا لمجمل مكونات مسرح الجريمة بما يسهم في كشف غموضها وفك أسرارها.

الفرع الأول: مفهوم المعاينة الإلكترونية

تعد المعاينة إحدى أهم إجراءات المتابعة في الجرائم المعلوماتية وقد خضعت لتنظيم دقيق بموجب مجموعة من النصوص القانونية وذلك انسجاما مع مبدأ الشرعية الإجرائية [1]، وعليه سيتم التطرق في هذا الفرع إلى تعريف إجراء المعاينة (أولا) ثم تحديد شروط صحتها (ثانيا)

أولا: تعريف المعاينة

لقد تبيانت التعريفات الفقهية لمفهوم المعاينة إذ لم يتدخل المشرع لوضع تعريف محدد لها واكتفى بتنظيم الإجراءات المتعلقة بكيفية القيام بها وهي:

تعرف المعاينة على أنها: " الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها وبالتالي يجب على السلطات المختصة الانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة الآثار المادية للجريمة التي تساعد في التنقيب عن الحقيقة [2]".

كما يقصد بأنها: " إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة ". [3]

و تعرف أيضا على أنها: " إثبات مباشر ومادي لحالة الشيء أو الشخص معين ويكون ذلك من خلال الرؤية أو الفحص المباشر للشيء بواسطة باقي الإجراءات ". [4]

---

[1] سومية قلات، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد الحادي عشر، العدد الأول، 2023، ص522

[2] نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية (القانون الخاص)، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، الجزائر، 2021 / 2022، ص350

[3] سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية ، مصر، 2013، ص286

يتضح من خلال التعاريف السابقة أن جوهر المعاينة في مجال التحقيق الجنائي يتمثل في القيام بملاحظة دقيقة وفحص حسي مباشر لمكان أو شخص أو شيء له صلة بالجريمة، ذلك بغرض إثبات حالته الراهنة والكشف عن الأدلة المحتملة والتحفظ عليها بما يساهم في الوصول إلى الحقيقة وإظهارها. [1]

ومن هذا المنطلق فإن المعاينة في الجريمة الالكترونية يقصد بها: " معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الأنترنيت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية ". [2]

مما لا شك فيه أن المعاينة تحتل مكانة محورية في التحقيقات الجنائية التقليدية إذ تعد من أبرز إجراءات البحث لما تؤديه من دور أساسي في تصور وقوع الجريمة وفهم ظروف وملابسات ارتكابها، فضلا عن كونها وسيلة رئيسة لجمع الأدلة المادية وتحليلها وتقييم الأدلة الأخرى في ضوء ما تكشفه من معطيات بما يتيح التخطيط السليم لعمليات البحث والتحقيق وتطويرها، فالمعاينة في مسرح الجريمة التقليدية تمكن المحقق الجنائي من الوقوف على الآثار المادية التي خلفها الفعل الإجرامي والتحفظ على الأشياء التي قد تكون ذات صلة بالتحقيق[3]. وبطبيعة الحال إن الأمر يختلف في مجال الجرائم الإلكترونية إذ لا يوجد عادة مسرح مادي مماثل لمسرح الجريمة التقليدية فالأقرب إلى ذلك هو موقع الأجهزة والأنظمة الإلكترونية التي شكلت محل الجريمة أو أداتها. [4]

ومن الجدير بالملاحظة أن مسرح الجريمة في الجرائم الإلكترونية يختلف جذريا عن نظيره في الجرائم التقليدية، إذ يقلل هذا المسرح الافتراضي من فرص الكشف عن الحقائق المرجوة من المعاينة لسببين رئيسيين :

---

[4] حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية ، مصر، 2017، ص54

[1] نصيرة بوحزمة، مرجع سابق، ص351

[2] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دار الفكر الجامعي ، مصر، 2009، ص153

[3] حازم محمد حنفي، مرجع سابق، ص57

[4] حازم محمد حنفي، المرجع السابق، ص58

1. الجرائم التي ترتكب بواسطة الأنظمة الإلكترونية نادرا ما تخلف آثارا مادية ملموسة يمكن ضبطها أو الاستناد إليها في التحقيق، بخلاف الجرائم التقليدية التي تترك عادة بصمات أو أدوات أو آثارا مادية واضحة.
2. غالبا ما تمر فترة زمنية طويلة نسبيا بين ارتكاب الجريمة الإلكترونية واكتشافها وخلال هذه الفترة قد يتردد عدد كبير من الأشخاص على المكان الذي توجد فيه الأجهزة أو الأنظمة محل الجريمة، مما يفتح المجال لحدوث تغييرات أو تلف أو عبث بالآثار الرقمية أو حتى زوال بعضها. [1]

ثانيا: شروط صحة المعاينة الإلكترونية

حتى تكون المعاينة في مجال الجرائم الإلكترونية أداة فعالة لكشف ملابسات الواقعة وتحديد هوية الفاعل، فإنها تخضع لجملة من الشروط الجوهرية التي تضمن سلامة الإجراءات وموثوقية النتائج. [2]ومن أبرز هذه الشروط ما يلي :

- سرعة الإنتقال إلى مكان وقوع الجريمة السيبيرانية: يشترط لصحة المعاينة في الجرائم الإلكترونية أن تتم بسرعة ودقة بحيث تبادر السلطة المختصة بالتحقيق إلى الانتقال فور علمها بوقوع الجريمة إلى مكان الواقعة، ويعد عنصر السرعة هنا أساسيا إذ يضمن الحفاظ على مسرح الجريمة في حالته الأصلية التي تركها الجاني ويحول دون أي تغيير أو عبث قد يؤثر في سلامة الأدلة الرقمية أو المادية المرتبطة بها. [3]
- التسلسل في المعاينة: وذلك بأن تجرى وفق تسلسل منهجي يضمن دقة الإجراءات وفعالية النتائج، فالسلطة المختصة بالتحقيق مطالبة بمراعاة نقطتين أساسيتين: أولهما تحديد نقطة البدء في المعاينة بشكل واضح ومنظم بما يسمح بتتبع الأدلة وفق ترتيب منطقي يسهل عملية الفحص والتحليل، وثانيهما الالتزام بعدم الانتقال من مكان إلى

---

[1] عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الألي، الطبعة الثانية، دار النهضة العربية ، مصر، 2001، ص365 – ص366

[2] نصيرة بوحزمة، المرجع السابق، ص353

[3] ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص: قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، الجزائر، سنة 2015-2016، ص65

آخر إلا بعد التأكد من استكمال معاينته بصورة شاملة، وعدم ترك أي عنصر أو أثر دون فحص أو توثيق[1].

- الدقة والعناية الفائقة في معاينة مسرح الجرائم السيبيرانية: إذ يتعين على السلطة المختصة أن تقوم بوصف شامل ودقيق للمنطقة التي ارتكبت فيها الجريمة، فإذا كانت الواقعة داخل مبنى فإن المعاينة يجب أن تشمل جميع منافذ الدخول والخروج مع تسجيل تفاصيلها بدقة، كما ينبغي وصف المحتويات ذات الصلة المباشرة بالجريمة مثل أجهزة الحاسوب، الماسحات الضوئية، الطابعات، الأقراص المدمجة، وغيرها من الوسائل التقنية التي قد تكون استخدمت في ارتكاب الفعل الإجرامي. [2]
- تدوين المعاينة: يعتبر تدوين المعاينة من الشروط الجوهرية لضمان حجية هذا الإجراء في التحقيقات المتعلقة بالجرائم السيبيرانية ويجب أن يتم التدوين بصورة رسمية وموثقة سواء كتابيا أو تصويريا بحيث يشمل تصوير الأجهزة المضبوطة في مكان ارتكاب الجريمة وعلى رأسها أجهزة الحاسوب والأجهزة الطرفية المتصلة بها ويعطى اهتمام خاص لتوثيق الأجزاء الخلفية للحاسوب وملحقاته لما قد تحتويه من منافذ أو أدوات تخزين ذات صلة بالفعل الإجرامي كما يتعين تسجيل تاريخ ووقت ومكان التقاط كل صورة بشكل دقيق. [3]

الفرع الثاني: إجراءات المعاينة الإلكترونية

في هذا الفرع سيتم التطرق للهيئات المكلفة بإجراء المعاينة الرقمية والمحددة في قانون الإجراءات الجزائية الجزائري (أولا)، ثم بعد ذلك سيتم الحديث عن الشروط القانونية الخاصة بالمعاينة الرقمية (ثانيا).

---

[1] نصيرة بوحزمة، مرجع سابق، ص353

[2] عبد الهادي قادة، دور المعاينة الجنائية في الإثبات الجنائي، مذكرة مقدمة لنيل شهادة الماستر، تخصص: قانون جنائي وعلوم جنائية، قسم: قانون عام، ميدان الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2023- 2024، ص48

[3] نصيرة بوحزمة، المرجع السابق، ص354

أولا: الهيئات المكلفة بإجراء المعاينة الإلكترونية

تعد المعاينة من أهم الإجراءات الجنائية التي يباشرها ضباط الشرطة القضائية المنصوص عليهم في المادة 20 وما يليها من قانون الإجراءات الجزائية[1] وذلك تحت إشراف النيابة العامة باعتبارها صاحبة الاختصاص الأصيل في البحث والتحري، كما يمكن أن يضطلع بها قاضي التحقيق كل في حدود اختصاصه الإقليمي والنوعي بغية الوصول إلى الحقيقة وكشف ملابسات الوقائع محل البحث.

ولا ينبغي إغفال الدور الذي تضطلع به الهيئة الوطنية في هذا السياق بما يعزز من فعالية المعاينة كوسيلة إثبات أساسية في النظام الإجرائي الجزائي. [2]

يباشر ضباط الشرطة القضائية بمجرد علمهم بوقوع الجريمة الانتقال الفوري إلى مكانها قصد معاينتها في إطار التحقيقات الأولية وذلك بعد إخطار وكيل الجمهورية وفقا لما تقتضيه أحكام قانون الإجراءات الجزائية، وتنص المادة 96 من هذا القانون على أن ضباط الشرطة القضائية وتحت إشرافهم أعوان الشرطة القضائية يتولون مباشرة التحقيقات الابتدائية فور علمهم بوقوع الجريمة سواء بناء على تعليمات صادرة عن وكيل الجمهورية أو بمبادرة منهم. [3]

أما المادة 97 من ق.إ.ج فقد وضعت قيدا جوهريا يتعلق بحرمة المساكن، حيث نصت على أنه لا يجوز القيام بالتفتيش أو المعاينة أو ضبط الأشياء التي من شأنها إثبات التهمة إلا بناء على رضا صريح من الشخص المعني، ويعد هذا النص تكريسا لمبدأ حماية الحرية الفردية وضمانات الخصوصية في إطار التوازن بين متطلبات التحقيق الجنائي وحقوق الأفراد [4].

---

[1] قانون رقم 25-14 المؤرخ في 09 صفر عام 1447 الموافق ل 03 أوت سنة 2025 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 54 الصادرة بتاريخ 19 صفر 1447 الموافق ل 13 أوت سنة 2025

[2] قلات سومية، حاحة عبد العالي، مرجع سابق، ص525

[3] أنظر نص المادة 96 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر

[4] نص المادة 97 من القانون رقم 25-14

وتظهر المواد القانونية ذات الصلة بتنظيم أعمال الضبطية القضائية أن المشرع قد اعتمد صياغة عامة تسمح بإسقاطها على مختلف صور الجريمة سواء التقليدية أو المعلوماتية[1].

فالمادة 122 تنص على أن ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب يحرر تقريرا يتضمن العناصر الجوهرية لمعاينة الجرائم، وهو ما يضع إطارا عاما يمكن تطبيقه على الجرائم المستحدثة في المجال المعلوماتي. [2]

وبالرجوع إلى المادة 74 من قانون الإجراءات الجزائية نجد أنها رتبت جزاءا على كل من يتعمد تغيير حالة الأماكن التي ارتكبت فيها الجريمة أو نزع شيء منها[3] وهو ما ينطبق أيضا على الجرائم المعلوماتية.

أما المادة 78 من ق.إ.ج فقد خصت إجراء المعاينة في الجرائم المعلوماتية بوقت غير محدد شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص، في حين نصت المادة 81 من قانون رقم 25-14 على إمكانية الاستعانة بالخبراء أثناء إجراء المعاينة وذلك يكون الخبير المطلوب ذا دراية تقنية متقدمة في مجال المعلوماتية والتكنولوجيا الحديثة وقد يتطلب الأمر الاستعانة بمجموعة من الخبراء المتخصصين في فروع مختلفة من علوم الحاسوب والأمن السيبراني. [4]

وعلى صعيد الجريمة المتلبس بها قد نظمها قانون الإجراءات الجزائية الجزائري في المادتان 72 و73 بحيث أوجب على ضابط الشرطة القضائية القيام بجملة من الإجراءات الجوهرية عند وقوع الجريمة في حالة التلبس:

يتعين على الضابط إخطار وكيل الجمهورية فورا ثم الانتقال مباشرة إلى مكان ارتكاب الجريمة لمعاينة الوضع بنفسه، وعند وصوله يباشر التحريات اللازمة مع الحرص على المحافظة على الآثار المادية التي قد تختفي وضبط كل ما من شأنه أن يسهم في كشف

[1] قلات سومية، حاحة عبد العالي، مرجع سابق، ص526

[2] نص المادة 122 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر

[3] نص المادة 74 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر

[4] نص المادتان 78 و81 من القانون رقم 25- 14 المتضمن ق.إ.ج السالف الذكر

الحقيقة، [1]كما يلتزم ضابط الشرطة القضائية عند ضبط أشياء مرتبطة بالجريمة بعرضها على المشتبه فيهم للتعرف عليها.

لقد نص المشرع الجزائري على الدور الذي تتخذه الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في كشف الجرائم السيبيرانية في نص المادة 14 فقرة "ب" من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على أن من بين مهام الهيئة المختصة مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بالجرائم المعلوماتية وذلك من خلال تجميع المعلومات وإنجاز الخبرات القضائية اللازمة. [2]

يتضح من هذا النص أن للهيئة صلاحية مباشرة إجراءات المعاينة في إطار المساعدة القضائية الداخلية، باعتبار أن المعاينة تمثل وسيلة أساسية للكشف عن الجرائم المعلوماتية وتحديد الأدلة الرقمية المرتبطة بها، وتكتسي هذه الصلاحية أهمية بالغة إذ تمكن الهيئة من دعم التحقيقات الجنائية عبر تقديم خبرة تقنية متخصصة بما يضمن فعالية أكبر في مواجهة الجرائم المستحدثة التي تتسم بالتعقيد وسرعة التطور. [3]

وعليه فإن المشرع قد أرسى إطارا قانونيا يسمح بتكامل الأدوار بين السلطات القضائية والهيئات التقنية المختصة بما يعزز من قدرة المنظومة الجزائية على التصدي للجرائم المعلوماتية سواء من خلال الوقاية أو من خلال الملاحقة القضائية الفعالة.

ثانيا: الشروط القانونية الخاصة بالمعاينة الإلكترونية

تتجلى الشروط القانونية المتعلقة بالمعاينة الرقمية فيما يلي:

[1] نص المادة 73 من القانون رقم 25-14

[2] أنظر نص المادة 14 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[3] سومية قلات، حاحي عبد العالي، مرجع سابق، ص525

1. *الإذن بالمعاينة الرقمية*: إن أمر أو إذن المعاينة المعلوماتية لا يجوز تنفيذه إلا بناء على رضا صريح وواضح من الشخص الذي ستتخذ لديه هذه الإجراءات وذلك وفقا لما نصت عليه المادة 97 السالفة الذكر [1]
2. *وقت إجراء المعاينة الرقمية*: المعاينة المعلوماتية باعتبارها إجراء من إجراءات التحقيق في الجرائم ذات الطبيعة الإلكترونية يمكن القيام بها في أي وقت من ساعات النهار أو الليل شريطة أن تكون مستندة إلى إذن مسبق صادر عن وكيل الجمهورية وذلك وفقا لما نصت عليه المادة 78 من قانون الإجراءات الجزائية، ويميز هذا التنظيم المعاينة في الجرائم المعلوماتية عن نظيرتها في الجرائم التقليدية حيث يفرض القانون في هذه الأخيرة قيودا زمنية محددة لإجرائها . [2]
3. *محضر المعاينة الرقمية*: يعد محضر المعاينة المعلوماتية ثمرة الجهود المبذولة من قبل الهيئات المكلفة بإنجازها بحيث ألزم قانون الإجراءات الجزائية ضباط الشرطة القضائية بتحرير محاضر تتضمن كافة الأعمال والإجراءات التي قاموا بها وذلك وفقا لما نصت عليه المادة 27 من القانون ذاته، ويتضمن محضر المعاينة بيانات جوهرية تتعلق بالجريمة والمشتبه فيه إضافة إلى هوية محرر المحضر وصفته ورتبته وتوقيعه وختمه وتاريخ تحريره. [3]

المطلب الثاني:
التفتيش الإلكتروني

يعد التفتيش من أبرز إجراءات التحقيق الابتدائي إذ يهدف إلى ضبط الأدلة والأشياء المرتبطة بالجريمة سواء لدى المتهم شخصيا أو في مسكنه أو في أماكن أخرى ذات صلة ويعتبر هذا الإجراء في الأصل من اختصاص سلطة التحقيق المتمثلة في قاضي التحقيق أو النيابة العامة وذلك بحسب ما تقرره التشريعات الوطنية المختلفة غير أن المشرع قد خول استثناءا لرجال الضبطية القضائية مباشرة التفتيش في حالات محددة نص عليها القانون

[1] أنظر نص المادة 97 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر
[2] أنظر نص المادة 78 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر
[3] أنظر نص المادة 27 من قانون رقم 25-14 المتضمن ق.إ.ج السالف الذكر

25-14 على سبيل الحصر ضمانا لفعالية التحقيق وسرعة جمع الأدلة مع مراعاة الضوابط القانونية التي تكفل حماية الحقوق والحريات الفردية. [1]

الفرع الأول: مفهوم التفتيش الإلكتروني

لم يتطرق المشرع الجزائري لتعريف التفتيش بل ترك هذه المهمة للفقه القانوني، فعرفه البعض بأنه: "إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة، وهو ينطوي على مساس بحق المتهم في سرية حياته الخاصة " [2]

و كما تعرفه الأستاذة الدكتورة آمال عثمان بأنه:" وسيلة للإثبات المادي تهدف إلى اكتشاف أشياء خفية أو أشخاص هاربين من وجه العدالة فهو وسيلة لإثبات أدلة مادية وقد يكون موضوعه شخصا أو مكانا " [3].

و يعرف أيضا: " التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا ". [4]

وعلى صعيد الجريمة السيبيرانية يقصد بالتفتيش أنه: " الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه ويستوي في ذلك أن يكون هذا المحل جهاز الي أو أنظمة أو شبكة الأنترنيت ".[5]

---

[1] إسحاق ابراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، سنة 1995، ص105

[2] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، مصر، د.ذ.س.ن، ص449

[3] أمال عثمان، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، د.ذ.س.ن، ص305

[4] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، مصر، سنة 2006، ص192

[5] نصيرة بوحزمة، المرجع السابق، ص302

كما يعرف بأنه: "إجراء من إجراءات التحقيق يهدف إلى البحث في نظام حاسوبي معين بإذن قضائي مسبق سواءا كان هذا النظام مكونا من حاسب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياه القانون والغرض استخراج أدلة معلوماتية ممثلة بالمعلومات أو البيانات والتي تساعد في كشف الحقيقة في جريمة من نوع جناية أو جنحة وقعت وجار التحقيق فيها. [1]

يعرف التفتيش الإلكتروني أيضا بأنه :" إجراء من إجراءات التحقيق يستهدف الكشف عن أدلة تفيد في إظهار الحقيقة وإسنادها إلى المتهم إذ تباشر الجهة المختصة عملية الولوج أو الدخول إلى نظم المعالجة الألية للبيانات بما تتضمنه من مدخلات ومخرجات وبيانات مخزنة قصد البحث عن السلوكيات الإجرامية وغير المشروعة والتي تشكل جناية أو جنحة ."[2]

الفرع الثاني: الشروط الشكلية والموضوعية للتفتيش الإلكتروني

سيتم الحديث أولا على الشروط الشكلية للتفتيش الإلكتروني، بعدها الشروط الموضوعية للتفتيش الإلكتروني

أولا: الشروط الشكلية

يقصد بالشروط الشكلية تلك الإجراءات التي ألزم المشرع مراعاتها عند القيام بعملية التفتيش إذ تهدف هذه الشروط إلى إحاطة عملية التفتيش بضوابط قانونية دقيقة تضمن صحتها ودقة النتائج المتوصل إليها من قبل القائم بها مع توفير ضمانات كافية للمتهم للحفاظ على حريته الفردية [3]. وهي:

---

[1] نصيرة بوحزمة، المرجع السابق، ص302

[2] أنفال لمصارة، منال محلول، إجراءات التفتيش الإلكتروني في التشريع الجزائري، مذكرة مكملة لمقتضيات نيل شهادة الماستر، تخصص: قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2024-2025، ص14-15.

[3] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، مخبر المؤسسات الدستورية والنظم السياسية، مجلة دائرة البحوث والدراسات القانونية والسياسية، تبسة، الجزائر، العدد الرابع، سنة 2018، ص57

-وقت إجراء التفتيش: نص المشرع الجزائري في قانون الإجراءات الجزائية على أنه "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحا ولا بعد الساعة الثامنة مساء إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا وهذا هو الأصل، لكن إستثناءا فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مكتوب مسبق من وكيل الجمهورية . [1]

ويفهم من نص المادة أعلاه أن المشرع الجزائري لم يحدد وقت معين لإجراء التفتيش الرقمي بل أجازه في كل الأوقات إن كان صباحا أو مساءا، ليلا أو نهارا وذلك في جرائم معينة منها الجرائم السيبيرانية.

-حضور الأشخاص المعنيين أثناء التفتيش: يشترط المشرع الجزائري ضمانا لاحترام حقوق الأفراد أثناء إجراءات التفتيش أن يتم تفتيش المنازل بحضور الشخص المعني أي المتهم وفي حال تعذر حضوره في وقت الإجراء يلتزم ضابط الشرطة القضائية بتمكينه من تعيين ممثل عنه، أما إذا امتنع المتهم عن ذلك أو كان في حالة فرار فإن القانون يفرض أن يستعاض عن حضوره بشاهدين من غير الموظفين التابعين للضابط القائم بالتفتيش وذلك تعزيزا لمبدأ الحياد وضمانًا لمصداقية الإجراءات [2].

-محضر التفتيش: تعد محاضر الشرطة القضائية في مجال الجرائم المرتبطة بالمعطيات الرقمية من أهم أدوات الإثبات في مرحلة البحث الابتدائي إذ تكتسب قيمة قانونية خاصة باعتبارها وسيلة لإثبات وقوع الجريمة ونسبتها إلى مرتكبها، وتزداد أهميتها بالنظر إلى الصلاحيات الواسعة التي يمنحها القانون لضابط الشرطة القضائية أثناء مباشرة مهامه في هذا المجال وتعرف هذه المحاضر بأنها وثائق رسمية مكتوبة يحررها ضابط الشرطة القضائية أثناء أدائه لمهامه متضمنة ما عاينه بنفسه أو ما تلقاه من تصريحات أو ما قام به من إجراءات تدخل ضمن اختصاصه القانوني.[3]

---

[1] نص المادة 78 من القانون رقم 25- 14، المتضمن قانون الإجراءات الجزائية الجزائري، السالف الذكر

[2] عز الدين عثماني، مرجع سابق، ص58

[3] عز الدين عثماني، مرجع سابق، ص58

ثانيا: الشروط الموضوعية

يتعين على الجهات المكلفة بالتفتيش مراعاة جملة من الضوابط الموضوعية وإلا كان التفتيش عديم الأثر القانوني وتتمثل هذه الضوابط أساسا في: وجود سبب مشروع للتفتيش يبرر اللجوء إليه مع تحديد محل التفتيش بدقة منعا لأي تجاوز وبيان الغاية من التفتيش بما يضمن ارتباطه بالتحقيق في الجريمة [1] خاصة في مجال الجرائم الإلكترونية حيث تكتسي هذه الضوابط أهمية مضاعفة نظرا لطبيعة الفضاء المعلوماتي.

-سبب التفتيش: لا خلاف في أن التفتيش يعد وسيلة أساسية من وسائل التحقيق الجنائي إذ يهدف إلى الوصول إلى الدليل باعتباره الطريق الأمثل لكشف الحقيقة، ويتحقق سبب التفتيش عند وقوع جريمة معينة يشتبه في ارتكابها من طرف شخص أو مجموعة أشخاص سواء بصورة مباشرة أو باعتبارهم شركاء فيها متى وُجدت إمارات وقرائن قوية تدل على وقوع الجريمة وتشير إلى احتمال تورطهم فيها. [2]

-محل التفتيش: يعد تحديد محل التفتيش من الضوابط الجوهرية الواجب مراعاتها في مجال الجرائم الإلكترونية إذ يتعين أن يكون محل التفتيش محددا تحديدا نافيا للجهالة بما يضمن وضوح نطاق الإجراء ويحول دون أي تجاوز أو تعسف، ويأخذ هذا المحل صورا متعددة بحسب طبيعة الجريمة الإلكترونية فقد يكون جهازا معلوماتيا بعينه، أو حسابا إلكترونيا محددا، أو قاعدة بيانات، أو أي وسيط رقمي آخر يحتمل أن يحتوي على أدلة ذات صلة بالتحقيق [3].

-غاية التفتيش: بما أن التفتيش يعد وسيلة من وسائل البحث عن الحقيقة، فإن الغاية الأساسية منه تتمثل في البحث عن الدليل الذي يسهم في كشف ملابسات الجريمة وتوضيح

---

[1] ليندة بومحراث، ضوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار ، مجلد 28، العدد الأول، الجزائر، سنة 2024، ص393

[2] أنفال لمصارة، مرجع سابق، ص 19.

[3] شمس الدين حمداش، البشير بن مبروك، القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة صوت القانون، المجلد 09، العدد 02، الجزائر، 2023، ص 104.

عناصرها، ومن ثم فإن كل ما يساعد المحقق من أشياء أو بيانات ذات صلة بالجريمة يعتبر جزءا من أهداف التفتيش. [1]

ويقع باطلا كل تفتيش يجرى لتحقيق غاية أخرى مخالفة لما حدده القانون، إذ يشترط المشرع أن تعرض مسبقا على السلطة المختصة المصلحة المرجوة من التفتيش، وإلا أصبح الإجراء تعسفيا فاقدا للمشروعية. أما في الجرائم الإلكترونية، فإن الغاية من التفتيش تتمثل أساسا في الحصول على الأدلة الرقمية التي تساعد على كشف الحقيقة وإثبات الجريمة. [2]

المطلب الثالث:

الخبرة التقنية

تشهد الخبرة في المجال الجزائي أهمية فائقة كونها وسيلة جوهرية لإنارة طريق جهات التحقيق والقضاء إذ تعد من إجراءات البحث والتحري عن الدليل وقد أولى المشرع الجزائري عناية خاصة بتنظيم أعمال الخبرة من خلال سن المواد من 239 إلى 252 من القانون رقم 14/25 حيث نصت المادة 239 من ق.إ.ج على صلاحية جهات التحقيق أو الحكم عندما يتم عرض عليها مسألة ذات طابع فني أن تأمر بندب خبير تلقائيا أو بناءا على طلب من النيابة العامة أو من أحد الخصوم أو محاميهم. [3]

و منذ ظهور الجرائم المعلوماتية أصبحت الضبطية القضائية وسلطات التحقيق تعتمد بشكل كبير على الخبراء المتخصصين في مجال الحاسب الألي والأنظمة المعلوماتية بغرض الكشف عن أي غموض يشوب الجريمة مع جمع الأدلة والتحفظ عليها بالإضافة إلى مساعدة قاضي التحقيق في فهم العمليات الإلكترونية الدقيقة المرتبطة بالواقعة محل التحقيق.

---

[1] ليندة بومحراث، مرجع سابق، ص396.

[2] ليندة بومحراث، مرجع سابق، ص396

[3] تنص المادة 239 من ق.إ.ج على أنه: لجهات التحقيق أو الحكم، عندما تعرض عليها مسألة ذات طابع فني، أن تأمر بندب خبير تلقائيا أو بناءا على طلب النيابة العامة أو من الخصوم أو محاميهم.

و نظرا لطبيعة الجريمة المعلوماتية الخاصة جعلت أمر الإستعانة بالخبراء أمر ضروري وحتمي نظرا للتعقيدات التي تصاحب التقنيات المتطورة والحديثة في مجال المعلوماتية.

الفرع الأول: تعريف الخبرة

الخبرة القضائية هي :" إجراء يستهدف الإستعانة بالقدرات الفنية أو العلمية لشخص الخبير والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد معرفة الظروف التي وقعت فيها الجريمة أو نسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية ". [1]

أو هي تلك الإستشارة الفنية التي يستعيين بها القاضي أو المحقق لمساعدته في تكوين عقيدته في المسائل التي يحتاج تقديرها إلى معرفة ودراية علمية خاصة لا توجد لدى المحقق. [2]

مما تقدم يمكن القول بأن الخبير هو ذلك الشخص الذي تكون لديه دراية ومعرفة في مجال معين والتي تؤهله لإبداء رأيه بما يخص الواقعة المرتكبة فالخبير في مجال الجريمة المعلوماتية هو ذلك الشخص الذي تلقى تكوينا أكسبه كفاءة تتيح له إبداء رأيه بخصوص الجريمة الإلكترونية. [3]

الفرع الثاني: إجراءات الخبرة التقنية

تتجلى إجراءات الخبرة التقنية في الضوابط القانونية والفنية التي تضفي على تقارير الخبرة حجية قضائية وهي:

إختيار الخبير من جدول الخبراء: الأصل أن يختار الخبراء من الجدول الذي تعده المجالس القضائية وذلك بعد إستطلاع رأي النيابة العامة وهذا مثل ما نصت عليه الفقرة الأولى من

---

[1] أحمد شوقي شلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2، ديوان المطبوعات الجامعية، الجزائر، سنة 1999، ص 259

[2] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، ط1، منشورات الحلبي الحقوقية، لبنان، سنة 2015، ص 184

[3] إسماعيل بن يحي، مرجع سابق، ص 215

المادة 240 ق.إ.ج لكن إستثناءا نصت الفقرة الأخيرة من هذه الأخيرة على جوازية إختيار خبراء ليسوا مقيدين في الجداول المخصصة لذلك. [1]

أداء اليمين القانونية: أوجب المشرع الجزائري في نص المادة 241 من ق.إ.ج على الخبير في كل مرة يختار فيها وقبل أداء مهامه أن يحلف اليمين القانونية، غير أنه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى مادام قد أدى اليمين عند تقييده بالجدول أول مرة. [2]

تقرير الخبرة: يتعين على الخبراء بعد الإنتهاء من أداء أعمال الخبرة القيام بإعداد تقرير مشترك يشتمل على وصف ماقاموا به من أعمال والنتائج المتوصل لها، وعلى الخبراء أن يشهدوا بقيامهم شخصيا بمباشرة هذه الأعمال المنوطة بهم باتخاذها مع ضرورة التوقيع على تلك التقارير وإذا اختلف الخبراء في الرأي أو كانت لهم تحفظات في شأن النتائج المشتركة يبدي كل منهم رأيه أو تحفظاته على حدة مع ضرورة تعليل وجهة نظره. [3]

تجدر الإشارة إلى أنه إذا توافرت تقارير الخبرة على كل الشروط المذكورة أعلاه تكون لها حجية نسبية أمام القضاء، فالمبدأ الراسخ في الفكر القانوني هو الإقتناع الشخصي للقاضي وبذلك له الحق في الأخذ بها كليا أو جزئيا أو استبعادها إذا اقتنع بعدم صحتها بشرط تسبيب ذلك.

---

[1] أنظر نص المادة 240 من ق.إ.ج رقم 25-14 السالف الذكر

[2] تنص المادة 241 من ق.إ.ج رقم 25-14 على أنه: يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي أمام القاضي وبحضور أمين الضبط يمينا أمام ذلك المجلس بالصيغة الأتية بيانها: " أقسم بالله العظيم وأتعهد بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال ". ولا يجدد هذا القسم مادام الخبير مقيدا في الجدول.

[3] أنظر نص المادة 249 من ق.إ.ج السالف الذكر

الخاتمة

خاتمة

إن خصوصية الجريمة المعلوماتية تجعلها تختلف عن الجريمة التقليدية في مختلف الجوانب وهو ما يصعب في عملية الكشف عنها وتتبع مرتكبيها وهو ما يجعلها تؤثر بشكل فعال على إجراءات المتابعة، وعليه فإن هذه الخصوصيات تفرض على المشرع الجزائري إعتماد قواعد قانونية وإجرائية تتلائم مع طبيعة الجريمة المعلوماتية

ومن خلال دراستنا لموضوع إنعاكاسات خصوصية الجريمة المعلوماتية على إجراءات المتابعة توصلنا للنتائج الآتية:

-إنفراد الجريمة المعلوماتية عن باقي الجرائم الأخرى بسماتها المتميزة، منها أنها لا تقع إلا في بيئة معلوماتية أو بالأحرى لا تكون الجريمة جريمة معلوماتية إلا إذا تمت في نظام معلوماتي، دون ذلك فالجريمة المرتكبة تعد جريمة تقليدية.

-خصوصية الجريمة المعلوماتية من ناحية البعد الدولي الذي تتخذه أثناء وقوعها، فالجريمة المعلوماتية يمكن لها أن تشمل ثلاث دول أو أكثر على حسب طبيعة الجريمة المعلوماتية المرتكبة.

- إتسام الجريمة المعلوماتية بإجراءات خاصة بها تضمن مكافحتها والتصدي له.

-الرؤية الشاملة للجريمة المعلوماتية والتي إنفرد بها المشرع الجزائري على غرار التشريعات الأخرى، وذلك لسنه العديد من النصوص القانونية التي تمس هذا المقام

-إغفال المشرع الجزائري لموضوع القيمة الإثباتية للدليل الرقمي بين أدلة الإثبات الجنائية المتنوعة، فالدليل الرقمي هو الحلقة الجوهرية التي تقام من أجله التحقيقات وإجراءات المتابعة.

-الإجراءات الجنائية المستحدثة لعبت دورا هاما في الكشف عن الجرائم المعلوماتية بمختلف أنواعها

ومن هذا المنطلق نرى بضرورة تقديم بعض التوصيات منها:

-على المشرع الجزائري وضع قانون خاص بالجريمة المعلوماتية لتبيان النصوص

الموضوعية والإجرائية بدقة ووضوح.

-ضرورة تعزيز التعاون الإقليمي والدولي في مجال مكافحة الجرائم المعلوماتية بين الدول

-ضرورة التكوين المستمر والمتخصص لرجال الضبطية القضائية في مجال طرق مكافحة الجريمة الإلكترونية.

-ضرورة تشجيع الجامعات على تنظيم ندوات وملتقيات بخصوص الجريمة المعلوماتية ومدى خطورتها وضرورة التصدي لها

-ضرورة تشجيع الطلبة والباحثين على القيام بدراسات تطبيقية وميدانية وذلك لتطويق الأساليب الإجرامية والحد منها

-تنمية الوعي لدى الفئات المجتمعية حول مخاطر الجريمة المعلوماتية وطرق الوقاية منها

-تشجيع المواطنيين وتحسيسهم حول أهمية التبليغ عن الجرائم المعلوماتية من خلال تطوير آليات التبليغ عن هذه الأخيرة وذلك من خلال إنشاء منصات إلكترونية

-تدعيم أجهزة الضبطية القضائية بوسائل وآليات وتقنيات حديثة تضمن الكشف والمواجهة الفعالة للجرائم الإلكترونية

قائمة المصادر والمراجع

أولا: الكتب

1.أحمد شوقي شلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري،ج2، ديوان المطبوعات الجامعية،الجزائر، سنة 1999.

2.أحمد غاي، الوجيز في تنظيم مهام الشرطة القضائية، ط5، دار هومة للنشر والتوزيع، الجزائر، د.س.ن.

3.أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، مصر، د.س.ن

4.أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة، ط2، دار الثقافة للنشر والتوزيع، الأردن، سنة 2014.

5.إسحاق ابراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، د.ط، ديوان المطبوعات الجامعية، الجزائر، سنة 1995.

6.أمال عثمان، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، د.س.ن

7.أمين محمد خرشة، مشروعية الصوت والصورة في الإثبات الجنائي، ط1، دار الثقافة للنشر والتوزيع، الأردن، د.س.ن.

8.جمال نعيمي، قانون الإجراءات الجزائية على ضوء الإجتهاد القضائي، ج1، ط4، دار هومة للنشر والتوزيع، الجزائر، سنة 2018.

9.حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، مصر، سنة 2017.

10. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، د.ط، دار الفكر الجامعي، مصر، سنة 2009.

11. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، د.ط، دار النهضة العربية، مصر، سنة 2013.

12. سهيل محمد العزام، الوجيز في جرائم الأنترنت، ط 1، دائرة مكتبة الجامعة الأردنية، الأردن، 2009

13. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، د.ط، دار الفكر الجامعي، مصر، سنة 2006.

14. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الألي، ط2، دار النهضة العربية، مصر، سنة 2001.

15. عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، ط1، منشورات الحلبي الحقوقية، لبنان، سنة 2015.

16. محمد حزيط، مذكرات في قانون الإجراءات الجزائية، د.ط، دار هومة للنشر والتوزيع، الجزائر، سنة 2011.

17. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، الأردن، سنة 2010.

18. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في قانون الإجراءات الجزائية، د.ط، دار المطبوعات الجامعية، مصر، سنة 2009.

19. يعيش تمام شوقي، الجريمة المعلوماتية [دراسة تأصيلية ومقارنة]، ط1، مطبعة الرمال، الجزائر، سنة 2019.

ثانيا: المقالات

1.ابراهيم يامة، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد11، عدد02، الجزائر، 2019، ص148 – ص159.

2.أسماء عنترة، مكافحة الجرائم المستحدثة في التشريع الجزائري "التسرب نموذجا"، مجلة القانون العام الجزائري والمقارن، عدد06، الجزائر،2017، ص74 – ص89.

3.اسمهان بن مالك، خصائص الجريمة المعلوماتية وأسباب ارتكابها، المجلة الجزائرية للأبحاث والدراسات، كلية الحقوق والعلوم السياسية بجامعة برج بوعريريج، المجلد الرابع، العدد الأول، 2019، ص102 – ص124.

4.أمينة معزيز، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، االمجلد6، العدد 11، الجزائر، سنة 2014، ص242 – ص272.

5.أنيس الحسيب السيد المحلاوي، مدى مشروعية الوسائل التي تستخدم بشكل خفي كدليل في الإثبات الجنائي، مجلة كلية الشريعة والقانون، المجلد20 ، العدد04، مصر، 2018، ص2755 – ص2840.

6.بشرى غريبي، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المجلد 02، العدد 02، الجزائر، 2021، ص101 – ص115.

7.جميلة ملحق، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 15، العدد 42، الجزائر، 2015، ص174 – ص187.

8.حيمي سيدي محمد، معوقات التحقيق الجنائي في الجرائم الإلكترونية،المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول،2022، ص1734 – ص1752.

9.خالد ضو، مبدأ اليقين القضائي في الأحكام الجنائية، مجلة الفكر القانوني السياسي، المجلد 06، العدد1، الجزائر،2022، ص520 – ص534.

10. راوية مطماطي، عملية التسرب على ضوء قانون الإجراءات الجزائية14/25، مجلة حقوق الانسان والحريات العامة جامعة عبد الحمبد ابن باديس مستغانم، الجزائر، المجلد10، العدد02، سنة 2025، ص397 – ص427.

11. رشيد شميشم، الحق في الصورة، مجلة العلوم الإنسانية والاجتماعية، المجلد8، العدد3، الجزائر، 2008، ص158 – ص171.

12. رضا عسال، عماد عبد الرزاق، الجريمة الإلكترونية والمجرم المعلوماتي: مقاربة مفاهمية، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد 05، الجزائر، 2020، ص151 – ص158.

13. ريمة عميروش، عن خصوصية الجريمة المعلوماتية، المجلة الجزائرية للأبحاث والدراسات، المجلد 02، العدد 02، الجزائر، سنة 2021، ص73 – ص 88.

14. سمير خلفي، التسرب الإلكتروني: اجراء لمكافحة المخدرات عبر الوسائط الإلكترونية في ظل انتشار جائحة كورونا، مجلة المحلل القانوني، جامعة البويرة، المجلد04، العدد 02، ديسمبر2022، ص74 – ص90.

15. سهام خليلي، خصوصية المجرم المعلوماتي، مجلة المفكر، المجلد 12، العدد 15، الجزائر، 2017، ص401 – ص414.

16. سومية قلات، حاحة عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد الحادي عشر، العدد الأول، 2023، ص519 – ص551.

17. شمس الدين حمداش، البشير بن مبروك، القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة صوت القانون، المجلد 09، العدد 02، الجزائر، 2023، ص96 – ص116.

18. شول بن شهرة، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، المركز الجامعي أفلو، غرادية،المجلد الرابع، العدد الأول، جوان 2020، ص01 – ص21.

19. صابر بحري، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الإنحراف، المجلد 06، العدد 01، الجزائر، 2021، ص36 – ص59.

20. صالح جزول، ضمانات مشروعية التصنت التلفوني واعتراض المراسلات في القانون الاجرائي الجزائري، مجلة نوميروس الأكاديمية، المجلد01 ، العدد02، الجزائر،2020، ص155 – ص175.

21. عبد القادر درقاوي، المجرم المعلوماتي، مجلة الدراسات القانونية والسياسية، المجلد 11، العدد 02، الجزائر، 2025، ص 60 – ص73.

22. عبد القادر رويسي، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، العدد03، الجزائر،2017، ص38 – ص50.

23. عبد القادر فلاح، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، المجلد08 ، العدد 01، الجزائر، 2021، ص177 – ص194.

24. عبد الله حاج احمد، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي في التشريع الجزائري، مجلة الاجتهاد في الدراسات القانونية والاقتصادية، المجلد08، العدد05، الجزائر، 2019، ص337 – ص357.

25. عز الدين دواعي، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية المقارن، المجلة الأكاديمية للبحث القانوني، مجلد 16، العدد 02،2017 ص270 – ص285.

26. عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، مخبر المؤسسات الدستورية والنظم السياسية، مجلة دائرة البحوث والدراسات القانونية والسياسية، تبسة، الجزائر، العدد الرابع، سنة 2018، ص48 – ص66.

27. فوزي عمارة، اعتراض المراسلات تسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، ع 33، جوان 2010، ص235 – ص254.

28. كريمة تاجر، التسرب الالكتروني كألية لمكافحة الجريمة الالكترونية – دراسة مقارنة بين القانون الجزائري والفرنسي، المجلة النقدية للقانون والعلوم السياسية، المجلد 19، العدد 02، 2024، ص 477 – ص491.

29. ليندة بومحراث، ضوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، مجلد 28، العدد الأول، الجزائر، سنة 2024، ص389 – ص402.

30. منيرة عبيزة، التسجيل الصوتي كدليل للإثبات، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد06، العدد1، 2023، ص1599 – ص1625.

31. نبيلة قيشاح،التسرب كالية للتحري والتحقيق في الجريمة المنظمة، مجلة المستقبل للدراسات القانونية والسياسية– المركز الجامعب بافلو،الجزائر،العدد03، 2018، ص77 – ص88.

32. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، المجلد 4، العدد 11، الجزائر،2017، ص908 – ص926.

33. هدى زوزو، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسية والقانون، العدد 11، الجزائر، 2014، ص115 – ص124.

34. ويزة بلعسلي، التسرب كألية خاصة للبحث والتحري في الجرائم المستحدثة في قانون الإجراءات الجزائية، المجلة النقدية للقانون والعلوم السياسية، العدد 05، الجزائر، 2015، ص143 – ص157.

ثالثا: المذكرات والأطروحات الجامعية

أ/ أطروحات الدكتوراه

1. إسماعيل ين يحيي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة ابى بكر بلقايد، تلمسان، الجزائر،2021.

2. حسين ربيعي، أليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم، تخصص: قانون العقوبات والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2015-2016.

3. خضرة شنتير، الاليات القانونية لمكافحة الجريمة الالكترونية-دراسة مقارنة-، أطروحة لنيل شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة دارية، ادرار، الجزائر،2021.

4. الدوادي مجراب، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة دكتوراه، تخصص الحقوق، جامعة بن يوسف بن خدة، الجزائر1، الجزائر،2016

5. رجاء اومدر، خصوصية الجريمة التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه ل.م.د، تخصص القانون الخاص، جامعة محمد البشير الابراهيمي برج بوعريج، الجزائر، سنة 2021/2020

6. صالح براهيمي، الإثبات بشهادة الشهود في القانون الجزائري، أطروحة دكتوراه في الحقوق، جامعة مولود معمري، تيزي وزو الجزائر، 2016.

7. الطيبي بركة، الحماية الجنائية لنظام المعالجة الالية للمعطيات – دراسة مقارنة- ، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة دارية، ادرار، الجزائر،2020.

8. عمر شهياني، التسرب في قانون الإجراءات الجزائية الجزائري، أطروحة لنيل درجة الدكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر،2023.

9. عنتر أسماء، أطروحة مقدمة لنيل شهادة الدكتوراه، إجراءات التحقيق القضائي الخاصة، دراسة مقارنة، جامعة عبد الحميد بن باديس مستعانم، الجزائر،2021.

10. ليندة بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة لنيل درجة الدكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة ميلود معمري، جامعة تيزي وزو، الجزائر،2019

11. نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية (القانون الخاص)، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، الجزائر، 2021 / 2022

ب/ مذكرات الماجيستير والماستر

12. ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص: قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن المهيدي، ام البواقي، الجزائر، 2016.

13. امال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، 2002.

14. امين بحري، دور التكنولوجيا في الاثبات الجنائي مذكرة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية جامعة مولود معمري تيزي وزو، الجزائر،2025.

15. امين خالد بن نعوم، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر تخصص قانون قضائي، جامعة عبد الحميد بن باديس مستغانم، الجزائر، السنة الجامعية 2019/2018.

16. أنفال لمصارة، منال محلول، إجراءات التفتيش الإلكتروني في التشريع الجزائري، مذكرة مكملة لمقتضيات نيل شهادة الماستر، تخصص: قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2024-2025.

17. حورية خليصة- حمزة فيروز، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، الجزائر،2024.

18. خديجة هلال، حيرش خديجة، مشروعية الصوت والصورة في الاثبات الجنائي في الإجراءات الجزائية الجزائري، مذكرة مكملة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة سعيدة، الجزائر، 2021.

19. زكرياء لدغم شيكوش، النظام القانون للتسرب في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية والإدارية، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر،2013.

20. سهيلة بوزبرة، مذكرة لنيل شهادة الماجيستير في القانون الخاص، كلية الحقوق، جامعة جيجل، الجزائر،2008

21. شريفة طاهري، تأثير أدلة الإثبات على الاقتناع الشخصي للقضاء الجنائي، رسالة لنيل شهادة الماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2003

22. شمس الدين مهدي، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي جامعة محمد خضير، بسكرة، الجزائر،2014.

23. الشيماء بن الداوي، التسرب ودوره في مكافحة الجريمة، مذكرة لاستكمال متطلبات نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، جامعة غرداية كلية الحقوق والعلوم السياسية قسم الحقوق، الجزائر، 2024.

24. عبد الرؤوف بجاد بوديسة، اليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة برج بوعريرج، الجزائر، السنة 2021/2020.

25. عبد القادر صنور، الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، الجزائر،2017.

26. عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر، 2016.

27. عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجيستير، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر2012

28. عبد النور بشان، المتابعة الجزائية بين السرية والعلنية "دارسة مقارنة «، مذكرة لنيل شهادة الماجيستير كلية الحقوق والعلوم السياسية، جامعة الجزائر1، الجزائر، 2011.

29. عبد الهادي قادة، دور المعاينة الجنائية في الإثبات الجنائي، مذكرة مقدمة لنيل شهادة الماستر، تخصص: قانون جنائي وعلوم جنائية، قسم: قانون عام، ميدان الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2023-2024.

30. علي دحمان – سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ضمن متطلبات نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر،2012.

31. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، تخصص إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح بورقلة، الجزائر، السنة الجامعية 2019.

32. فاطيمة دهان، كلثوم دهان، إجراءات البحث والتحري في الجرائم المعلوماتية، مذكرة مقدمة ضمن متطابات نيل شهادة ماستر أكاديمي، تخصص: قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرادية، الجزائر، 2021-2022.

33. فراح حمادي، التسرب في قانون الإجراءات الجزائية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص مهن قانونية وقضائية، كلية الحقوق والعلوم السياسية، جامعة جيجل، الجزائر، 2025/2024.

34. فلاح عائشة، خصوصية الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، الجزائر،2016.

35. مختار خداوي، اجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر،2016/2015.

36. مليسة حمري، حجية الدليل الإلكتروني في الإثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر،2020/2019.

37. نسيمة بجدي، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة لنيل شهاد الماجيستير، تخصص قانون جنائي، كلية الحقوق، جامعة وهران، الجزائر،2014.

38. نعيم سعيداني، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستير، تخصص القانون، جامعة الحاج لخضر باتنة، الجزائر،2013،

39. نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة من اجل الحصول على شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر،2016.

40. هبة الدزيري، جريمة الدخول الغير مشروع لنظام المعالجة الالية للمعطيات، مذكرة نهاية الدراسة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم

جنائية، شعبة الحقوق، جامعة عبد الحميد ابن باديس، مستغانم، الجزائر، السنة الجامعية 2020/2019.

41. ياسمين باينين، دور وسائل التكنولوجيا في الإثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر،2022 /2023.

42. ياسمينة بونعارة، الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، الجزائر،2015.

43. يوسف بالخضر، إجراءات البحث والتحري الخاصة في التشريع الجزائري، مذكرة لنيل شهادة ماستر أكاديمي في الحقوق تخصص قانون اعمال، كلية الحقوق والعلوم السياسية برج بوعريريج، الجزائر،2021/2020.

ج/ مذكرات المدرسة العليا للقضاء

44.مرزوق نسيمة، جرائم الانترنت، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2009.

45.هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر،2006.

رابعا: المحاضرات الجامعية

1. نسمة بطيحي، محاضرات في مقياس الوقاية من الجرائم الالكترونية، مطبوعة مقدمة لطلبة السنة الثانية ماستر، تخصص إدارة الكترونية وخدمات رقمية، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر،2022.

خامسا: الأوامر والقوانين

1. قانون رقم 04-15 المؤرخ في 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 71 الصادر في 10 نوفمبر سنة 2004

2. قانون رقم 06-01 المؤرخ في 21 محرم عام 1427 الموافق ل 20 فبراير سنة 2006 المتعلق بالوقاية من الفساد ومكافحته المعدل والمتمم، الجريدة الرسمية للجمهورية

الجزائرية عدد 14 الصادر بتاريخ 08 صفر عام 1427 الموافق ل 08 مارس سنة 1427

3. قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية عدد 47 الصادرة بتاريخ 25 شعبان عام 1430 الموافق ل 16 أوت سنة 2009

4. قانون رقم 20-05 المؤرخ في 05 رمضان عام 1441 الموافق ل 28 أبريل سنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية عدد 25 الصادرة بتاريخ 06 رمضان عام 1441 الموافق ل 29 أبريل سنة 2020

5. قانون رقم 20-15 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020 المتعلق بالوقاية من جرائم إختطاف الأشخاص ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية عدد 81 الصادرة بتاريخ 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020.

6. قانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق ل 28 أبريل سنة 2024 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 30 الصادر بتاريخ 21 شوال عام 1445 الموافق ل 30 أبريل سنة

7. . قانون رقم 25-14 المؤرخ في 09 صفر عام 1447 الموافق ل 03 أوت سنة 2025 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 54 الصادر بتاريخ 19 صفر عام 1447 الموافق ل 13 أوت سنة 2025

فهرس المحتويات

فهرس المحتويات

مقدمة _____ 6

الفصل الأول: خصوصية الجريمة المعلوماتية _____ 11

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية _____ 13

المطلب الأول: مفهوم الجريمة المعلوماتية _____ 13

الفرع الاول: التعريف القانوني للجريمة المعلوماتية _____ 14

الفرع الثاني: التعريف الفقهي للجريمة للمعلوماتية _____ 16

أولا/ تعربف الجريمة المعلوماتية نسبة لوسيلة ارتكابها _____ 16

ثانيا/ تعربف الجريمة المعلوماتية من حيث موضوعها _____ 17

ثالثا/ تعريف الجريمة من طرف خبير تقني _____ 17

رابعا/ تعربف الجريمة المعلوماتية حسب الاتجاه المختلط _____ 18

المطلب الثاني انواع الجريمة المعلوماتية _____ 19

الفرع الاول: الاعتداءات على النظام المعلوماتي _____ 20

اولا: جريمة الدخول أو البقاء غير المشروع في المنظومة المعلوماتية _____ 20

ثانيا: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الالية _____ 21

الفرع الثاني: الاعتداءات الواقعة بواسطة النظام المعلوماتي _____ 22

اولا: الجرائم التي تقع على الأشخاص _____ 22

ثانيا: الجرائم التي تقع على الاموال _____ 26

المبحث الثاني: مظاهر خصوصية الجريمة المعلوماتية _____ 30

المطلب الأول: الطبيعة الخاصة بالجريمة المعلوماتية _____ 30

الفرع الأول: وقوع الجريمة في بيئة معلوماتية _____ 30

الفرع الثاني: الجريمة المعلوماتية متعدية الحدود _____ 31

المطلب الثاني: صعوبة إكتشاف الجريمة المعلوماتية _____ 33

الفرع الأول: صعوبة إثبات الجريمة المعلوماتية _____ 33

الفرع الثاني: صعوبة تحديد هوية الجاني المعلوماتي _____ 35

أولا: سمات المجرم المعلوماتي _____ 35

ثانيا: أصناف المجرم المعلوماتي _____ 37

ثالثا: دوافع المجرم المعلوماتي لإرتكاب الجريمة المعلوماتية _____ 38

رابعا: المعيقات التي تعيق جهات التحقيق في تحديد هوية الجاني المعلوماتي _____ 40

الفصل الثاني: أثر خصوصية الجريمة المعلوماتية على إجراءات المتابعة ____ 42

المبحث الأول: إجراءات المتابعة المستحدثة في الجرائم المعلوماتية _____ 44

المطلب الأول: التسرب الالكتروني _____ 44

الفرع الأول: مفهوم التسرب الالكتروني _____ 45

أولا: تعريف التسرب _____ 45

ثانيا: صور عملية التسرب _____ 50

الفرع الثاني: الشروط الخاصة بتنفيذ اجراء التسرب الالكتروني _____ 53

المطلب الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور _____ 59

الفرع الأول: مفهوم اعتراض المراسلات وتسجيل الأصوات والتقاط الصور _____ 59

اولا: تعريف اعتراض المراسلات وتسجيل الأصوات والتقاط الصور _____ 59

الفرع الثاني: ضوابط اتخاذ اجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور _____ 63

أولا/الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور: _____ 64

ثانيا/الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور _____ 67

المبحث الثاني: إجراءات المتابعة العامة للكشف عن الجريمة المعلوماتية _____ 74

المطلب الأول: المعاينة الإلكترونية 74

الفرع الأول: مفهوم المعاينة الإلكترونية 75

أولا: تعريف المعاينة 75

ثانيا: شروط صحة المعاينة الإلكترونية 77

الفرع الثاني: إجراءات المعاينة الإلكترونية 78

أولا: الهيئات المكلفة بإجراء المعاينة الإلكترونية 79

ثانيا: الشروط القانونية الخاصة بالمعاينة الإلكترونية 81

المطلب الثاني: التفتيش الإلكتروني 82

الفرع الأول: مفهوم التفتيش الإلكتروني 83

الفرع الثاني: الشروط الشكلية والموضوعية للتفتيش الإلكتروني 84

أولا: الشروط الشكلية 84

ثانيا: الشروط الموضوعية 86

المطلب الثالث: الخبرة التقنية 87

الفرع الأول: تعريف الخبرة 88

الفرع الثاني: إجراءات الخبرة التقنية 88

الخاتمة 90

قائمة المصادر والمراجع 93

فهرس المحتويات 106