جامعة أكلي محند أولحاج – البويرة

كلية الحقوق والعلوم السياسية

قسم القانون العام

الخصوصية الإجرائية للتحقيق في الجريمة المعلوماتية

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم القانونية

تخصص القانون الجنائي و العلوم الجنائية

إعداد الطالب:

- جومي الأمين

إشراف الأستاذ:

- د/ خليفي سمير

لجنة المناقشة

الأستاذ:.....رئيسا

الأستاذ: د/ خليفي سمير.....مشرفا ومقررا

الأستاذ:.....ممتحنا

السنة الجامعية: 2021/2020.

شكر وتقدير

بعد شكر الله سبحانه وتعالى وحسن توفيقه على إنجاز هذا البحث، يشرفني أن أتقدم بجزيل الشكر والتقدير لأستاذ القدير"خليفي سمير"الذي أشرف على هذا البحث وعلى كل المساعدات والتوجيهات والتوضيحات والنصائح التي أسدها لي في كل خطوة من خطوات إنجاز هذه المذكرة دون ملل أو ضجر.

فلكل أستاذي الفاضل أسمى معاني الشكر والتقدير.

كما لا يفوتني أن أشكر لجنة المناقشة على تفضلها وقبولها مناقشة هذا العمل من أجل إثراء محتواه وإبداء ملاحظاتها التي ترفع من قيمة هذه المذكرة مضافةإلى البحوث العلمية التي سيعتمد عليها الطلبة والباحثين من بعدنا ،

فلكم ألف شكر وتحية.

الإهداء

أهدي ثمرة عملي وجهدي المتواضع هذا إلى من أعطتني الحياة مصدر الحب والحنان إلى أسمى عاطفة وأحلى ما ينطق به اللسان أمي الغالية حفظها الله لي

كما أهدي ثمرة جهدي و سهري إلى زوجتي وولداي أسيل و إياد حفظهم الله و أدام عليهم نعمة الصحة و العافية.

وإلى كل عائلتي.

إلى من شاركوني هذا العمل والحياة ومن أخشى ألا أنصفهم حقهم، أصدقائي وأحبائي ورفقاء الدراسة.

إلى كل من وسعته ذاكرتي ولم تصبه مذكرتي وكل من سيتصفح هذه المذكرة.

أهدي لكم هذا العمل المتواضع.

الأميـــــن

مقدمة

مقدمة:

دخلت البشرية مرحلة جديدة من خلال النقلة العلمية والتكنولوجية التي طغت على كافة مجلات الحياة، وأضحت إحدى سمات العصر الحديث، بحيث أصبحت تكنولوجيا المعلومات من متطلبات الحياة اليومية إن لم نقل من ضرورياتها التي لا يكاد يستغني عنها أحد فقد ساهمت إلى حد كبير في تهاوي كل الحدود الجغرافية والزمنية وأصبح العالم بالمفهوم التكنولوجي عبارة عن قرية صغيرة تترابط فيها الدول بشبكة اتصالات معقدة ومتشبعة وقد كان لهذه النقلة بلا شك انعكاسا إيجابيا على مختلف مناخي الحياة جسدته الحاسبات الآلية التي تعتبر واجهة هذا التطور بعد ظهور شبكة الانترنت.

وأصبحت إحدى الدعائم الأساسية التي يعتمد عليها في تسيير شؤون الإنسان العامة منها والخاصة لما تتميز به من قدرة هائلة على تخزين المعلومات والسرعة في معالجة البيانات وإجراء العمليات الحسابية. كما لعبت دورا كبيرا في تقليص الزمن والمسافات والجهد البدني والعقلي، لكن الدور الإيجابي للتكنولوجيا لا يجعلنا نغفل عن سلبياتها المتمثلة كارتكاب أفعال غير مشروعة ما يجعل منها بيئة خصبة لإرتكاب مختلف الجرائم أو وسيلة مسهلة لإرتكابها ما يجعلها في الكثير من الأحيان تشكل تهديدا على قيم المجتمعات وأمن واستقرار الدول.

وقد أدى سوء استغلال التكنولوجيا إلى ظهور نوع جديد من الجرائم تختلف طبيعتها والبيئة التي ترتكب فيها عن ما هو مألوف في الجرائم التقليدية، وهو ما أصبح يعرف بجرائم الوسط الرقمي أو الجرائم المعلوماتية، ومن الصعوبات التي واجهت مختلف الأنظمة القانونية في مواجهة الإجرام المعلوماتي الطبيعية الخاصة التي تتميز بها هذه الجرائم حيث أنها لا تخضع لضابط الحدود الجغرافية. كما تتميز بصعوبة اكتشافها حيث يطلق عليها البعض تسمية الجرائم الناعمة كونها لا تنطوي على عنف، ولا تخلف أثار مادية بالمفهوم التقليدي في الجرائم العادية كما يتميز مرتكبوها بصفاة تختلف عن ما هو مألوف في المجرم العادي كالإلمام بتقنيات التعامل مع الحاسبات الآلية والتكنولوجيا

الحديثة ونسبة ذكاء مرتفع ما جعل الأنظمة القانونية عاجزة على مواجهة هذا الإجرام بالترسانة القانونية التقليدية التي قد يؤدي تطبيقها على هذه الجرائم إلى إهدار العديد من المبادئ القانونية الراسخة في المجال الجنائي كشرعية التجريم والعقاب والتفسير الضيق للنص الجنائي وحضر القياس وهو ما أخذ به المشرع الجنائي إلى أخذ خطوات لمواجهتها وذلك بوضع نصوص قانونية تتلاءم وطبيعة نظرا لقصر النصوص التقليدية في مكافحتها وكذا إدخال تعديلات على قوانين سارية المفعول محاولا مسايرة التطور الحاصل في هذا المجال، ولم يكن المشرع الجزائري بمنأى عن هذا ولم يقتصر الأمر على الشق الموضوعي وحسب بل تعداه إلى الجانب الإجرائي خاصة ما تعلق منه بآلية إجراء الاستدلالات والتحقيقات عبر البيئة الرقمية وتكييفها بطريقة تتلاءم وخص وصية هذا النوع من الجرائم حتى تتحقق النجاعة المطلوبة في الكشف عنها وملاحقة مرتكبيها وتقديمهم للعدالة، ومن هنا تظهر أهمية البث كونه يلقي الضوء على الجرائم المعلوماتية والتي تعتبر من الجرائم الحديثة التي تتميز عن غيرها من الجرائم المألوفة بخصائص تجعل الإجراءات التقليدية قاصرة في مواجهتها بالإضافة إلى خطورة هذه الجرائم وجسامة الخسائر التي تخلفها خاصة وأن التكنولوجيا الحديثة أصبحت تغزو جميع المجالات الحياتية ولم يعد أحد بمنأى عن مخاطرها كما أن دراسة الشق الإجرامي المتعلق بالجريمة المعلوماتية يعتبر من الموضوعات التي لم تستوفي حقها من الدراسة والبحث.

ومن الدراسات السابقة التي تناولت هذا الموضوع كتاب مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت للدكتور عبد الفتاح بيومي حجازي الطبعة الأولى لسنة 2006 والذي تناول من خلاله الجانب الإجرائي للجرائم المعلوماتية.

ومما سبق فإن الذي دفعني لاختيار هذا الموضوع تتفرع إلى أسباب شخصية وأخرى موضوعية، **الأسباب الشخصية**: من الأسباب الشخصية التي دفعتني إلى خوض

غمار البحث في هذا الموضوع هو الرغبة في كشف النقاب عن آلية التحقيق في هذا النوع من الجرائم من أجل توسيع مداركي العلمية في هذا الجانب على اعتبار أن هذا الموضوع من الموضوعات التي تثير الاهتمام لكونه من الموضوعات الحديثة.

_ **الأسباب الموضوعية**: تكمن في الإشكالات التي يثيرها هذا الموضوع من ناحية مدى فعالية الإجراءات المستحدثة في مكافحة هذه الجرائم بطريقة تتلاءم والطبيعة الخاصة التي يميزها عن الجرائم التقليدية ومدى مسايرتها للتطور الذي تعرفه الجريمة المعلوماتية

حيث نجد أن التطور السريع للجريمة والذي لم يعد يقتصر فقط على تطور أساليب ارتكاب الجرائم كما عهدناه سابقا بل أصبح هناك نوع جديد من الجرائم يستفيد من وسائل التطور التكنولوجي والعلمي وأصبح البيئة الرقمية حاضنتا لشتى أنواع الجرائم في ظل قصور النصوص الإجرائية التقليدية على مواجهتها، وهو ما دفع بالمشرع الجزائري إلى أن يحذو حذو العديد من التشريعات الأخرى باستحداث نصوص قانونية قادرة على مواجهة هذا النوع من الإجرام الخطير لاسيما ما تعلق منها بمساعدة جهات التحقيق في الكشف عن هذه الجرائم وملاحقة مرتكبيها ومنع إفلاتهم من العقاب.

ومن هنا يمكننا طرح الإشكالية التالية: **ما هي الخصوصية الإجرامية التي تميز التحقيق في الجريمة المعلوماتية والآلية التي اعتمدها المشرع للتحقيق في الجريمة المعلوماتية؟**

ولإجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي، لأنه أكثر منهج قدر على وصف إجراءات التي يتم بها التحقيق في الجريمة المعلوماتية والمنهج التحليلي الذي يمكنني من التطرق لكل إجراء بشيء من التدقيق.

ومن ذلك تقسيم البحث إلى فصلين يتضمنان فكرتين رئيستين تمثلان إشكالية البحث فصلين فصل الأول بعنوان إجراءات التحقيق العادية في الجرائم المعلوماتية والذي من خلاله تطرقت إلى التفتيش كإجراء مألوف للتحقيق ومدى قابليته للتطبيق على الجرائم المعلوماتية، حيث عالجنا في المطلب الأول موضوع التفتيش في البيئة الرقمية من خلال التطرق إلى مفهومه ومدى قابلية مكونات الحاسب الآلي للمعاينة بالإضافة إلى الضوابط التي تحكمه، ومن خلال المطلب الثاني تطرقنا إلى الآثار المترتبة عن التفتيش في البيئة الرقمية من خلال إظهار محل الحجز في البيئة الرقمية، أما المبحث الثاني فقد تطرقنا من خلاله إلى ضوابط التحقيق الأخرى كالمعاينة التي تطرقنا إليها في المطلب الأول من خلال مفهومها ومدى قابلية مسرح الجريمة المعلوماتي للمعاينة، بالإضافة إلى الخبرة الفنية في المطلب الثاني من حيث ماهيتها ومتطلبات أعمالها لإثبات الجرائم المعلوماتية.

أما في الفصل الثاني فقد تطرقت من خلاله إلى الإجراءات المستحدثة التي اعتمدها المشرع للتحقيق في الجرائم المعلوماتية كإجراء التسرب والذي تطرقت إليه في المبحث الأول من خلال توضيح مفهومه في المطلب الأول والضوابط التي تحكم هذا الإجراء، أما المبحث الثاني فقد خصصته للحديث عن الإجراءات الأخرى المستحدثة للتحقيق في الجرائم المعلوماتية من خلال التطرق إلى اعتراض المرسلات والمراقبة الالكترونية للتحقيق في الجريمة المعلوماتية من خلال توضيح مفهومها والضمانات الواردة عليها، أما في المطلب الثاني فقد بينت من خلاله الإجراءات الأخرى المتصلة بعملية التحقيق في الجريمة المعلوماتية ويتعلق الأمر بإجراء الحفظ والإفشاء العاجلان للمعطيات الالكترونية من خلال توضيح المقصود به وضمانات المشتبه فيه أثناء هذا الإجراء.

الفصل الأول:

إجراءات التحقيق العادية في الجرائم المعلوماتية

إن الاستخدام غير المشروع للتقنيات المعلوماتية الحديثة، وما أصابه من إشكالات قانونية تتعلق أساسا بتطبيق النصوص الجنائية التقليدية على هذا النوع من الجرائم المستحدثة.

قد ساهم إلى حد كبير في قلب المفاهيم القانونية السائدة إلا أنه ومن جهة أخرى قد خلق مشكلات قانونية تتعلق بالشق الإجرائي للقانون الجزائي، من حيث مدى قدرة القواعد الإجرائية المألوفة في البحث و التحقيق على ضبط الجريمة و منع إفلات مرتكبيها من العقاب.

حيث أن هذه الجرائم ونظرا للخصوصية الفنية التي تميزها قد خلقت تحسديات قانونية أمام سلطات البحث و التحقيق، ما فرض وضع مجموعة من الإجراءات منها ما يعد مألوفا كإجراء تحقيق في الجرائم التقليدية،ومنهما يقتصر تطبيقه على الجرائم المعلوماتية.

ومما لاشك فيه أن المشرع حينما أراد توسيع تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الإلكترونية، فإنه يقصد بها تلك الإجراءات التي تثير إشكالات عملية تعود إلى خصوصية هذه الجرائم ،والوسط الذي ترتكب فيه كالتفتيش و المعاينة و الخبرة الفنية.

حيث إن إعمال هذه الإجراءات في الجرائم المعلوماتية يختلف عن ما هو عليه في الجرائم التقليدية كوننا نتعامل مع عالم إفتراضي غالبا ما لا تخلف جرائمه أثار مادية ملموسة بمفهوم الجرائم التقليدية و التي سيغت هذه الإجراءات في ظلها.

لذالك فإن إجراءات التحقيق التقليدية وإن أجاز التشريعات الحديثة تطبيقها على الجرائم المعلوماتية، فإنها تكون بنوع من الخصوصية تتلائم و طبيعة هذه الجرائم.

لذالك قمنا بتقسيم الفصل الأول إلى مبحثين المبحث الأول سنطرق من خلاله إلى التفتيش كإجراء مألوف في الجرائم المعلوماتية،أما في المبحث الثاني فسوف نتطرق إلى المعاينة كضابط للتحقيق في الجريمة المعلوماتية و الخبرة الفنية كأحد متطلبات التحقيق في الجريمة المعلوماتية.

المبحث الأول:

التفتيش كإجراء تحقيق مألوف في الجرائم المعلوماتية

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق المألوفة في الجرائم التقليدية يهدف إلى ضبط أدلة مادية تتعلق بجناية أو جنحة تحقق وجودها.

وعادة ما يكون في أماكن تتمتع بالحرمة لذلك فإن المشرع الجزائري نص عليه بموجب مواد دستورية تضمن عدم المساس بحرمة المساكن والأشخاص وكذا حرياتهم الأساسية الفردية لما لهذا الإجراء من خطورة على هذه الحقوق الجوهرية.

ولقد أجازت التشريعات الحديثة اللجوء إليه لجمع الأدلة الناتجة عن الجرائم التي تقع في البيئة الرقمية والتي يختلف مدلولها على ما هو مألوف في البيئة المادية.

ومن هذا المنطلق ينبغي علينا التطرق إلى موضوع التفتيش في البيئة الرقمية من حيث مفهومه ومدى قابلية أعمال هذا الإجراء في الوسط الرقمي كمطلب أول، وإلى الآثار المترتبة عنه كمطلب ثاني.

المطلب الأول:

موضوع التفتيش في البيئة الرقمية

الفرع الأول: مفهوم التفتيش في البيئة الرقمية ومدى قابلية مكونات الحاسب الآلي للتفتيش

أولا: مفهوم التفتيش في البيئة الرقمية

1_ التعريف التقليدي للتفتيش

نظرا للخصوصية الفنية للجريمة المعلوماتية كونها تقع في بيئة لا مادية أو افتراضية فإن القيام بإجراء التفتيش في هذه البيئة يختلف عنه في البيئة المادية الملموسة.

ويعرف الفقه التفتيش بأنه إجراء من إجراءات التحقيق الابتدائي، فثمرتهي ضبط الأشياء المتعلقة بالجريمة والتي تفيد في كشف الحقيقة وهذه الأشياء قد تستمد منها أدلة

الجريمة إذ قد تمثل أداة الجريمة أو موضوعها أو متحصلاتها[1]، كما يميل الفقه الفرنسي إلى اعتباره بحثا بوليسي أو قضائي وفقا لقواعد قانونية خاصة، أن ينفذ في المسكن الخاص بأي شخص أو في أي مكان أخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة.[2]

2_ رأي الفقه في مدى تلائم مصطلح التفتيش مع البيئة الرقمية

بإستقراء التعاريف السابقة يتبين لنا بأن التفتيش بالمفهوم التقليدي يختلف عنه في البيئة الرقمية حيث أن التفتيش ما هو إلا وسيلة للإثبات المادي غايته ضبط أدلة مادية ما يجعله يتنافى مع الطبيعة الغير مادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت التي ليس لها أي مظهر مادي ملموس.[3]

حيث يرى جانب من الفقه أن مصطلح التفتيش لا يتلائم مع البيئة الرقمية كمحل لهذا الأخير.[4]

وقد تنازع الفقه المقارن حول مدى إمكانية اعتبار الولوج أو النفاذ في الأنظمة المعلوماتية تفتيشا فظهر اتجاهان:

_ الاتجاه الأول:

يرى أصحابه ضرورة تعديل النصوص والقواعد التقليدية للتفتيش على نحو يمكن معه استيعاب النفاذ أو الولوج بإضافة مادة معالجة بالحاسوب إلى جانب الأشياء المادية

---

[1]_ إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 2، العدد 1، 2018، ص 30.

[2]_ أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، ص 87.

[3]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون جنائي، جامعة مولود معمري، تيزي وزو، 2018، ص 14.

[4]_ حيث يرى هذا الجانب ضرورة تعديل المصطلح في العالم الافتراضي واستخدام مصطلح الولوج أو النفاذ بدلا من التفتيش لأنه سيكون أكثر دقة كونه ينص على الصفحات الالكترونية وأنظمة وبرامج.

التي ترد عليها التفتيش، و قد استجاب لهذا الاتجاه بعض التشريعات الجزائية الإجرائية كالولايات المتحدة الأمريكية، حيث نظمت إجراء البحث والضبط والتفتيش في بيئة الحاسوب في القسم 2000 رقم USC 42

وكذا التشريع الفرنسي، أما على المستوى الهرمي فنجد تشريع المملكة العربية المتحدة في قانون إساءة استخدام الحاسب الآلي لسنة 1990 التي تنص على إجراء التفتيش لنظم الحاسوب في جرائم الولوج غير المصرح به للأنظمة وتعديلها، أما إذا كان الولوج غير مقترن بنية إجرامية فلا بد للتفتيش من إذن قضائي.[1]

_ الاتجاه الثاني:

يرى أصحاب هذا الاتجاه عدم ضرورة وجدوى التعديل في نصوص التفتيش التقليدية عامة حيث يمكن تفسيرها على نحو يستوعب البيانات المعالجة الكترونيا، حيث يخضع التفتيش في العالم افتراضي لنفس المبادئ والأحكام العامة والشروط التقليدية لأنها عبارة عن ومضات ونبضات مهنية قابلة للتخزين على وسائط مادية بحيث يمكن نقلها واستغلالها. فهي شيء يمكن ترجمته في العالم المادي الملموس لتكون محلا للتفتيش والضبط.[2]

إلا أن الملاحظ في المواثيق الدولية المهتمة بهذا الموضوع من بينها اتفاقية يودابيست لجرائم الفضاء المعلوماتي أنها اعتمدت المصطلحين معا أي أخذت في الحسبان تطور المفاهيم في الوسط الالكتروني مع تحديدها والاحتفاظ بجذورها التقليدية بمعنى أن هذه المواثيق الدولية تضع للدول الأعضاء المصلحين معا للتخير بين الأخذ

---

[1]_ مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية، المجلد 11، العدد 1، 2011، ص229.

[2]_ المرجع نفسه، ص ص 229-230.

بالمصطلح التقليدي وهو التفتيش أو المصطلح الحديث وهو الولوج أو النسخ إذ يفهم من ذلك أن المصطلحين لهما نفس المعنى.[1]

ثانيا: مدى قابلية مكونات الحاسب الآلي للتفتيش

يتكون النظام المعلوماتي من مكونات مادية ومكونات غير مادية أو معنوية كما أن له شبكة سلكية ولاسلكية فهل يمكن أن تخضع هذه المكونات لإجراء التفتيش من أجل الحصول على الدليل الجنائي الالكتروني؟.

1_ مدى قابلية مكونات الحاسب العادية للتفتيش HARDWARE

تحكم الإجراءات القانونية الخاصة بالتفتيش فحص المكونات المادية للحاسب الآلي بحثا عن أي دليل يتصل بجريمة معلوماتية حدثت، ويفيد التفتيش في الكشف عن مرتكبيها ويخضع تفتيش الحاسب الآلي لأحكام تفتيش المكان الذي يوجد به ذلك الجهاز.[2]

إذ أن التفتيش الواقع على المكونات المادية للنظام المعلوماتي لا إشكال فيه، حيث نصت 44 من ق إ ج ج بأن التفتيش يقع على المكونات المادية مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها ويخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بالجريمة المعلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها للإجراءات القانونية الخاصة بالتفتيش أن يتوقف جواز التفتيش تلك المكونات على ضبطه المكان الذي تتواجد فيه وهل هو عام أو خاص، أن لصفة المكان أهمية خاصة في مجال التفتيش.[3]

---

[1]_ إلهام بن خليفة، المرجع السابق، ص ص 230-231.

[2]_ أسامة بن غانم العبيدي، المرجع السابق، ص 79.

[3]_ تشوار الجلالي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2018/2017، ص 279.

فالتشريع الإجرائي الجزائري يتضمن نصوص قانونية تنطبق من حيث الأجل على تفتيش المكونات المادية للمنظومة المعلوماتية وبناءا على ما سبق فإن تفتيش المكونات المادية للمنظومة المعلوماتية مثل لوحة المفاتيح والفأرة أو الشاشة وغيرها من الأشياء المادية الملموسة وكذا البصمات الموجودة عليها لا تدخل ضمن المشاكل الإجرائية التي تعيق إجراءات التفتيش إذ بإمكان تطبيق النصوص العادية عليها فإذا كانت في مسكن فإنه يطبق عليها ما يطبق على تفتيش المساكن من حيث مراعاة الإذن بالتفتيش، ووقت التفتيش والأشخاص القائمين على التفتيش وكذا المطلوب حضورهم وقت التفتيش مع مراعاة قواعد الاختصاص المكاني.[1]

2_ مدى قابلية مكونات الحاسب المعنوية للتفتيش SOFTWARE

يطلق أيضا على المكونات المعنوية للحاسوب اسم البرمجيات فهي بمثابة عصب عمل الكمبيوتر إذ توفر إمكانية وسرعة فائقة في إنجاز المهام المطلوبة كما يعرف الكيان المنطقي للحاسوب لغة بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كأنظم التشغيل وبرامج التطبيقات.[2]

حيث أن البيانات الالكترونية ليس لها مظهر مادي ملموسا، ومع ذلك قد يمكن أن يرد التفتيش عليها عن طريق الوسائط الالكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة ومخرجات الحاسب لهذا فقد أجاز الفقه والتشريعات إمكانية أن يكون محل التفتيش البيانات المعالجة آليا والمخزنة بالحاسب الآلي ثم ضبطها والتحفظ عليها

---

[1]_ مولاي ملياني، التفتيش في جرائم تكنولوجيا الإعلام والاتصال، مجلة القانون والعلوم السياسية، المجلد 2، العدد1، 2016، ص 295.

[2]_ يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل للعلوم الإنسانية والاجتماعية، جامعة باجي مختار، المجلد 22، العدد 2، 2016، ص 85.

أو ضبط الوسائط الالكترونية التي سجلت عليها هذه البيانات وعلى ضوء هذا تخضع لما يخضع إليه التفتيش بمعناه التقليدي من ضوابط وأحكام.[1].

وذهب رأي إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها ويستند هذا الرأي إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط " أي شيء " فإن ذلك يجب تفسيره بحيث يشمل البيانات المعالجة آليا.[2]

ومن بين هذه التشريعات القانون الجنائي الإجرائي اليوناني في المادة 251 منه والتي تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع الدليل وحمايته ويفسر الفقه اليوناني عبارة " أي شيء " بأنها تشمل البيانات المخزنة والمعالجة الكترونيا.[3]

وعلى النقيض من الرأي الأول نجد رأي ثاني يرى بعدم انطباق المفهوم المادي على بيانات الحاسبة الغير مرئية لذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسبة الالكترونية يجب أن يشمل المواد المعالجة عن طريق الحاسبة الالكترونية أو بيانات الحاسبة الالكترونية.[4]

وهذا ما تبناه المشرع الجزائري حيث أنه استجاب لهذه التغيرات وأجاز تفتيش المعطيات المعلوماتية بموجب نص المادة 05 من القانون رقم 09-04 حيث أجازت هذه المادة للسلطات القضائية في إطار ق إ ج ج وفي الحالات المنصوص عليها في المادة 04 من نفس القانون التي من بينها توفر احتمالية اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من الجرائم الماسة بأمن الدولة،

---

[1]_ رحل بومدين، محل التفتيش في مجال جرائم التجارة الالكترونية وفق القانون الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 3، العدد 2، 2018، ص 170.

[2]_ مولاي ملياني دلال، المرجع السابق، ص 295.

[3]_ أسامة بن غانم العبيدي، المرجع السابق، ص 79.

[4]_ علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، بغداد، 2012، ص ص 42-43.

الدخول بغرض التفتيشولو عن بعد منظومة معلوماتية أو جزء منها وكذا منظومة تخزين المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلومات.[1]

3_ مدى قابلية شبكات الحاسب الآلي للتفتيش

تعتبرشبكات الحاسب عبارة عن مجموعة مكونة من جهازين أو أكثر مرتبطة ببعضها سلكيا أو لاسلكيا ومن هنا يثور التساؤل حول مدى إمكانية امتداد التفتيش إلى منظومة معلوماتية أخرى انطلاقا من المنظومة التي يجري بها التفتيش ؟.

ويثير تفتيش شبكات النظام المعلوماتي مشكلة خاصة عندما يكون مرتبط بشبكة اتصال فالبيانات التي تحوي أدلة قد تتوزع عبر شبكات الحاسب الآلي وهنا نميز بين حالتين.

أ _ اتصال حاسب المتهم بحاسب أخر أو نهايةطرفية في مكان أخر داخل الدولة

يرى الفقه الألماني في هذه الحالة انه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع أخر استنادا إلى مقتضيات المادة 105 من قانون الإجراءات الجنائية الألماني وذلك عندما يكون مكان التخزين الفعلي خارج المكان الذي يتم فيه ذلك الإجراء، كذالك بالنسبة لمشروع قانون جريمة الحاسب في هولندا أن نجده بنص على إمكانية امتداد التفتيش إلى الأجهزة المعلوماتية الموجودة في موقع أخر شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة.[2]

أما بالنسبة للتشريع الجزائري وبالرجوع إلى نصوص قانون الإجراءات الجزائية نجده قد وسع بعض صلاحيات جهات التحقيق حيث سمح بإمكانية قيام قاضي التحقيق بالتفتيش والحجز في أي وقت ليلا أو نهارا على امتداد التراب الوطني أو بأمر ضباط الشرطة القضائية المختصين بذلك ومن بين الحالات التي تسمح سلطة قاضي التحقيق

---

[1] _مولاي ملياني دلال، المرجع السابق، ص ص 295- 296.

[2] _ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص 239.

بإجراء التفتيش والحجز وفق الصورة السابقة، عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

غير أن القصور الذي شاب نصوص قانون الإجراءات الجزائية هو عدم تضمنه التفتيش عن بعد في الكيانات المنطقية وأنظمة المعالجة الآلية للمعطيات فنلاحظ أن المشرع الجزائري قد تدارك هذا القصور بالسماح للسلطات القضائية المختصة لمقتضيات التحقيق تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني.[2]

وهو ما نصت عليه كذلك الاتفاقية الأوربية للإجرام السيراني في المادة 19 منها : "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة عن البحث أو النفاذ:

أ_ إلى أي نظام كمبيوتر أو أي جزء منه والبيانات المخزنة فيه.

ب _ أي دعامة تخزين بيانات الكمبيوتر مخزنة داخلها على أراضي تلك الدولة.[3]

ب_ اتصال حاسب المتهم بحاسب أخر نهايته الطرفية موجودة في مكان أخر خارج إقليم الدولة

وفقا لهذا الاحتمال يقوم مرتكبو الجريمة المعلوماتية بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكة الاتصال الرابطة بينهم.

---

[1]_ راجع المادة 47 فقرة 3 و 4 من قانون رقم 06-22 المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 156/66 يتضمن قانون الإجراءات الجزائية، ج ر ج ج، العدد 71، الصادرة بتاريخ 2004/11/10 معدل ومتمم.

[2]_ راجع المادة 5 فقرة 02 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 05 غشت سنة 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج ر ج ج، رقم 47 الصادرة بتاريخ 16 أوت 2009.

[3]_ الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية رقم 185 لعام 2001 متاحة على الموقع

Rm. Coe.Ine/Budapest- convention- Arabic/1680739173.

ومن التشريعات التي تصدت لهذه الإشكالية قانون جريمة الحاسب في هولندا والذي نص في مادته 125 فقرة الأولى على إمكانيةإجراء التفتيش داخل الأماكن بما يتضمن تفتيش نظم الحاسب الآلي المرتبطة حتى إن كانت موجودة في دولة أخرى وهذا بشرط أن يكون هذا التدخل مؤقتا وأن تكون البيانات محل التفتيش لازمة لإظهار الحقيقة.[1]

كما أجازت المادة 32 من الاتفاقية الأوربية بشأن مكافحة الجرائم المعلوماتية لعام 2001 إمكانية الدخول بغرض التفتيش والضبط في أجهزة الحاسب أو الشبكات تابعة لدولة أخرى دون إذنها في حالتين، إذ تعلق التفتيش بمعلومات وبيانات متاحة للعامة وفي حالة رضى المالك أو حائز هذه البيانات بهذا التفتيش.[2]

إلا أنه بالرغم من ذالك فإن الفقه يتحفظ على مثل هكذا أجزاء لأنه ينطوي على انتهاك سيادة الدولة التي يمتد إليها التفتيش.

أما بالنسبة للمشرع الجزائري فقد تلافى هذه المشكلة حيث نصت المادة 3/05 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بالنص على : " إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة المعلوماتية الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل".[3]

وبهذا فإن المشرع الجزائري قد وسع من نطاق التفتيش عن بعد إلى خارج الإقليم الوطني، إذا كان هناك أسباب تدعو إلى الاعتقاد بوجود المعطيات محل البحث والتي يمكن الدخول إليها انطلاقا من منظومة معلوماتية أو جزء منها أو انطلاقا من المعطيات

---

[1]_ نبيلة هبة هروال، المرجع السابق، ص 240.

[2]_ علي عدنان الفيل، إجراءات التحقيق وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع سابق، ص47.

[3]_ راجع الفقرة الثالثة من المادة 05 من القانون رقم 09-04، مرجع سابق.

المعلوماتية المخزنة فيها خارج الإقليم الوطني فإن السلطات القضائية المختصة وكذا ضباط الشرطة القضائية يمكنهم الحصول على المعطيات المبحوث عنها في إطار مساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.[1]

الفرع الثاني: ضوابط التفتيش في نظم الحاسب الآلي

باعتبار التفتيش هو الإجراء الذي تقوم به السلطات القضائية بغرض البحث عن الأدلة اللازمة للتحقيق والذي ينطوي في أغلب الأحيان على الإطلاع على محل يتمتع بالحرمة، فقد حرص جل التشريعات الإجرائية على إحاطة بجملة من الشروط التي تضمن عدم المساس بها، ومن بين هذه الشروط نجد شروطا شكلية وأخرى موضوعية.

أولا: الشروط الشكلية

هي شروط تهدف في أغلبها إلى ضمان صحة إجراءات التفتيش بالإضافة إلى أنها تمثل الضامن الذي يرمي إلى حماية الحريات الفردية.

ومن أهم هذه الشروط نجد:

أ_ الميقات الزمني لإجراء التفتيش

تحرص أغلب التشريعات على حضر القيام بالتفتيش في أوقات معينة حيث يذهب أغلبها إلى تحديد وقت معين يتم فيه هذا الإجراء وذلك لغرض تضيق نطاق الاعتداء على الحريات الفردية.

في حين ترك تشريعات أخرى تحديد الوقت الذي يجوز فيه التفتيش إلى القائم بالتفتيش ومن بين هذه التشريعات نجد قانون الإجراءات الجنائية المصري، حيث لم يحدد وقت معين يتم فيه هذا الإجراء أي يجوز في كل وقت سواء ليلا أو نهارا بغض النظر عن الاعتبارات المرتبطة بالمحل المراد تفتيشه.[2]

---

[1]_ أومدوار رجاء، فرسة كمال، التفتيش الجزائي في البيئة الافتراضية، مجلة صوت القانون، المجلد 07، العدد 1، 2020، ص ص 983-984.

[2]_ نبيلة هبة هروال، مرجع سابق، ص 258.

وذلك عكس التشريع الجزائري والفرنسي اللذين حظرا تفتيش المساكن في وقت معين، حيث نجد المشرع الجزائري حدد ميقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا.[1]

أما المشرع الفرنسي فقد حصره بين الساعة السادسة صباحا إلى الساعة التاسعة مساءا من خلال نص المادة 59 من قانون الإجراءات الجنائية الفرنسي[2]، وبالعودة إلى المشرع الجزائري نجده قد أجاز الخروج عن الميقات المحدد في حالات معينة ويصبح التفتيش في أي ساعة من ساعات الليل أو النهار فنجده قد استثنى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من تطبيق هذا القيد في الفقرة الأولى من المادة 47 ق إ ج ج حيث تنص الفقرة الثالثة على أنه" ... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من النهار أو الليل..."[3] ولعل هذا الاستثناء له ما يبرره إذ أن تعليب المشرع لمصلحة المجتمع على مصلحة الأفراد في حرمة حياتهم الخاصة يرجع إلى الطبيعة المميزة لهذه الجرائم التي لا يحكمها ميقات زمني إذ يمكن ارتكابها في أي وقت كما أن الدليل لإثباتها قابل للمحو والتعديل في وقت قصير.

---

[1]_ راجع المادة 47 من ق إ ج ج، مرجع سابق.

[2]_ بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012، ص 258.

[3]_ الفقرة الثالثة من المادة 47 من ق إ ج ج، مرجع سابق

ب_ في الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش

الأصل أن الشخص الذي يستوجب القانون حضورهوقت إجراء التفتيش هو المتهم إلا أن هذا الشرط يكون قائما حتما في تفتيش الأشخاص طالما التفتيش يقع عليه، غير أنه من المتصور إجراء التفتيش في غياب المتهم عندما يتعلق الأمر بتفتيش المساكن.[1]

لذلك فإن معظم التشريعات تشترط للقيام عملية التفتيش حضور أشخاص معينين كالتشريع الإجرائي المصري الذي يشترط في تفتيش المنازل وما في حكمها من قبل مأمور الضبط القضائي أن يتم في حضور المتهم أو من ينوبه وفي حالة غيابه ينبغي أن يكون الإجراء بحضور شاهدين يكونان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران.[2]

إلى جانب التشريع المصري يوجد التشريع الإجرائي الجزائري الذي اشترط أيضا أن يتم تفتيش المنازل بحضور صاحب المسكن فإن تعذر عليه الحضور فإن ضابط الشرطة القضائية المكلف بإجراء التفتيش بكلفه بتعين ممثل له وفي حالة امتنع أو كان هاربا استدعى ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته لحضور عملية التفتيش.[3]

كذلك الأمر إذا تم التفتيش من طرف قاضي التحقيق[4] ونظرا لخصوصية الجريمة محل الدراسة فإن التعديل الذي أدخله المشرع على المادة 45 ق إ ج ج يتماشى وخصوصيتها كون هذه الضمانات في ظل هذه الجرائم تتحول إلى مشكلات تحول دون الوصول إلى نتائج من التفتيش كون إشعار الأشخاص المطلوب حضورهم قد يتيح لهم

---

[1]_ رابحي عزيزة، التفتيش في نظم المعالجة الآلية للمعطيات، مجلة القانون والعلوم السياسية، المجلد 2، العدد 1، 2016، ص 406

[2]_ نبيلة هبة هروال، مرجع سابق، ص 235.

[3]_ انظر المادة 1/145 من ق إ ج ج، مرجع سابق.

[4]_ راجع المادة 82 من نفس القانون.

التلاعب بالمعطيات والبرامج والتطبيقات المراد تفتيشها وبالتالي إخفاء أدلة الجرائم والتلاعب بها كما قد يتم التلاعب بالأدلة عن بعد.[1]

ثانيا: الضوابط الموضوعية

يقصد بها الأحوال التي يجوز فيها اللجوء للتفتيش حيث تمثل الدافع للجهات المختصة بإصدار إذن التفتيش وتمثل في العناصر التالية:

أ_ سبب التفتيش في نظم المعلومات

التفتيش بوصفة إجراء من إجراءات التحقيق يكون عادة عند وقوع جريمة من الجرائم وإسنادها إلى شخص معين سواء بصفته مرتكبا مباشرا أو مساهما فيها.

بناءا على قرائن قوية تفيد تورطهم في هذه الجريمة عملا بمبدأ الشرعية الجنائية.

إذ يجب أن يستند إلى مبررات توضح سبب اللجوء إليه والهدف منه والمتمثلة في:

أ_ وقوع جريمة معلوماتية

يتعين لإجراء عملية تفتيش المنظومات المعلوماتية أن تكون قد وقعت فعلا جريمة معلوماتية، فإن كان الهدف هو الحصول على أدلة تساهم في كشف حقيقة الواقعة الجرمية ونسبها إلى مرتكبها فإن المنطق القانوني والعقلي يقتضي للقيام به ضرورة وقوع الجريمة بصورة قطعية سواء كانت جناية أو جنحة وتستبعد المخالفة لضآلة خطورتها.[2]

والملاحظ أن المشرع الجزائري قد خرج عن هذه القاعدة عند صياغة المادة 05 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث أجاز اللجوء إلى إجراء التفتيش في النظم المعلوماتية للوقاية من جرائم

---

[1]_ مولاي ملياني جلال، مرجع سابق، ص 302.

[2]_ إلهام بن خليفة، مرجع سابق، ص 32.

أو في حالة توفر معلومات عن احتمال وقوع معينة حددتها المادة 04 من نفس القانون.[1]

2_ نسبة الجريمة لشخص أو الأشخاص معينين

الأصل أن مجرد وقوع جريمة سواء كانت جناية أو جنحة لا يكفي لقيام بسبب التفتيش بل يجب توافر دلائل كافية تدعو للاعتقاد بأن ذالك المشتبه قد ساهم في ارتكابها مساهمة أصلية أو تبعية.[2]

وفي حالة عدم توفرها وعدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى أصدر أمرا بألا وجه للمتابعة وكان هذا سبب لحفظ ملف الدعوى.[3]

ويقصد بالدلائل الكافية بصفة عامة " شبهات مستمدة من الواقع والقرائن تنبأ عن ارتكاب شخص لجريمة من الجرائم أما في جريمة الانترنت فهي مجموعة من المظاهر والإمارات المعينة تنهض على السياق العقلي والمنطقي لملابسات الواقعة وكذا على خبرة وحرفية القائم بالتفتيش والتي تؤدي إلى نسب الجريمة إلى شخص معين بوصفه فاعلا أو شريكا.[4]

3_ وجود إمارات قوية أو قرائن على وجود معطيات أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره

لا مجال لإجراء التفتيش إن لم تتوفر لدى المحقق أسباب كافية على أنه يوجد في المكان المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة أو أشياء متحصلة عنها[5] كما

---

[1]_ انظر المادة (4) و(5) من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق

[2]_ الهام بن خليفة، مرجع سابق، ص 32.

[3]_ حيث تنص المادة 163 ق إ ج ج " إذ رأى قاضي التحقيق ... أنه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة لا يزال مجهولا أصدر أمرا بألا وجه لمتابعة المتهم".

[4]_ نبيلة هبة هروال، مرجع سابق، ص 233.

[5]_ إلهام بن خليفة، مرجع سابق، ص 32.

لا يكفي اتهام شخص معين بارتكابها أو المشاركة فيها بل يجب أن تتوفر إلى جانب ذلك إمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية، تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره.[1]

وهذا ما يفهم من نص المادة 44 من قانون الإجراءات الجزائية[2]

ويتم الحصول عادة على هذه القرائن والأمارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال بعد إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش والتي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى هذا الإجراء كما أنه وبخلاف ما هو عليه في الجرائم التقليدية فإن التوصل إلى قرائن وإمارات قوية لسبب للقيام بالتفتيش في الجرائم المعلوماتية ليس بالأمر الهين نظرا للصعوبات التي تواجه سلطات التحري والاستعدال[3] تتعلق أساسابنقص الخبرة وكذا خصوصية الدليل المعلوماتي.[4]

كما أن المشرع الجزائري وطبقا للمادة 5 الفقرة 01 والمادة 4 فقرة ج من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. أجاز التفتيش في النظم المعلوماتية ونظم التخزين لمقتضيات التحقيقات أو التحريات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم

---

[1] _ نبيلة هبة هروال، مرجع سابق، ص 233.

[2] _ حيث تنص المادة 44 من ق إ ج ج على أنه " لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في جناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش...".

[3] _ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 35.

[4] _ إذ يتميز الدليل المعلوماتي بطابعه اللامادي وتجاوزه الحدود الوطنية وسهولة مسحه أو إتلافه أو تغييره في أوقات قياسية كما يتميز التفتيش في القضاء الرقمي بأنه عملية معقدة ومتشابكة تقتضي من القائمين عليها أن يكونوا على دراية واسعة وكفاءة عالية في البحث عن المعلومات ..." انظر رضى هميسي، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 05، جوان 2012، ص 162.

الأبحاث الجارية، ويفهم من ذلك أنه لا يشترط المشرع للتفتيش في الأنظمة المعلوماتية توفر الدلائل للولوج بغرض التفتيش بل أنه يمكن ذلك هنا أجل الحصول على الدليل.[1]

ب_ محل التفتيش:

والمحل يقصد به المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره والسر الذي يحميه القانون هو الذي يستودع في محل له حرمة وفي النظام المعلوماتي هو الحاسب بكل مكوناته المادية والمعنويةوشبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب محل التفتيش.[2]

ج _ السلطة المختصة بالتفتيش

باعتبار التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس بالحريات الشخصية وحرمة الحياة الخاصة فقد حرص المشرع الجزائي على إسنادها لجهة قضائية تكفل تلك الحقوق والحريات إلا أنه وبالنظر إلى الضروريات العملية، أجيز تفويض هذا الاختصاص على أحد أعضاء الضبطية.

1_ النسب أو صدور إذن بالتفتيش

يقصد بالإذن ذلك التفويض الموجه من سلطة التفتيش إلى أحد مأموري الضبط القضائي يتضمن تحويلهم إجراء التفتيش الذي تختص به تلك السلطة.[3]

وإذا كان الإذن بالتفتيش لا يثير أي مشاكل في الجرائم العادية فإنه في الجرائم العادية فإنه في الجرائم المعلوماتية يواجه بعض الصعوبات التي مردها الطبيعة الخاصة

---

[1]_ إلهام بن خليفة، مرجع سابق، ص 33.

[2]_ تشوار الجلالي، الأسرار المعلوماتية وحمايتها الجزائية، مرجع سابق، ص 288.

[3]_ نبيلة هبة هروال، مرجع سابق، ص 493.

لهذه الأخيرة إذ أنه في الغالب يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يحتويه هذا الأخير.[1]

فهل يجوز لضابط الشرطة القضائية إجراء التفتيش في البيئة الرقمية للبحث عن دليل إثبات بموجب الإذن الصادر بتفتيش المسكن؟

يرى أغلب الفقه في هذه الحالة أنه يجب تحديد إذن التفتيش لتجنب التفتيش الإستكشافي و لا شك أن احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الكمبيوتر يثير صعوبات إذن هذا الأخير يحوى عدد كبير من الملفات بالإضافة إلى أن أسماء هذه الملفات قد لا تدل بالضرورة على محتواها.[2]

وما يثير التساؤل حول ما إذا كان ملف يلزم التعامل معه كما حاوية مغلقة تحتاج إلى إذن قضائي مستقل؟.[3]

والمشرع الجزائري في القواعد الخاصة بإجراء التفتيش في البيئة المعلوماتية في القانون رقم 09-09 لا نجده يتحدث عن هذا الشرط وكل ما في الأمر أنه تحدث عن إعلام حلمات التحقيق المختصة في حال تمديد التفتيش إلى منظومة معلوماتية.

---

[1]_ ليندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد 8، العدد 2، 2017، ص 493.

[2]_ ليندة بن طالب، مرجع سابق، ص 493.

[3]_ فالإحكام القضائية في مختلف الدول قليلة وتوصلت إلى نتائج متضاربة قاضي الولايات المتحدة الأمريكية تضاربت الأحكام القضائية، فمن جهة اعتبرت الديسك بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات يعتبر حاويه مغلقة واحدة، وعلى خلاف ذلك اتجهت أحكام أخرى للقضاء الأمريكي إلى اعتبار كل ملف في الكمبيوتر يتطلب إذن خاصا لتفتيشه، حيث يرجع أساس هذا الحكم إلى اعتبار الكمبيوتر يحوي الكثير من الملفات التي تتعلق بالحياة الخاصة لصاحبه ما يرجع احتمالية التعدي عليها واختلاف أحكام القضاء الأمريكي له أساس من المنطق العقلي والقانوني، فمن جهة فإن القدرة التخزينية الكثيرة للحاسب يجعل صدور إذن بالتفتيش حسب عدد الملفات أمر غير معقول، ومن جهة أخرى لا يتضرر امتداد الإذن بالتفتيش على كل الملفات المخزنة بنظم المعالجة الآلية للمعطيات حفاظا على الحياة الخاصة".

انظر بوكر رشيدة، جرائم الاعتداد على النظم المعالجة الآلية للمعطيات، مرجع سابق، ص 412.

2_ حالة القبض على المتهم بناءا على دلائل كافية

من الآثار المترتبة على القبض الصحيح تفتيش شخص المتهم عموما والمجرم المعلوماتي بصفة خاصة.

ويقصد بشخص المتهم المعلوماتي كمحل للتفتيش تحسس جسمه وملابسه وفحصه بدقة وإخراج ما يخفيه فيها من متحصلات جريمة الانترنت وإذا كان معه أمتعة جاز تفتيشها بحثا عن جزئيات تتعلق بالوحدات المعلوماتية محل البحث سواء كانت بين يديه أو يضعها في سيارته.[1]

والمشرع الجزائري لم يفرد قواعد خاصة بشأن تفتيش الأشخاص وفي ظل هذا الفراغ حاول القضاء في البلاد الأجنبية تنظيم هذا الموضوع، حيث يشترط في تفتيش الأشخاص وجود اتهام موجه للشخص بارتكاب جريمة معينة أو الاشتراك فيها، وجود دلائل كافية على حيازته لأشياء تتعلق بالجريمة.[2]

3_ التفتيش بناءا على حالة التلبس

تعتبر حالة التلبس أو الجرم المشهود من الحالات التي تتسع فيها سلطات الضبطية القضائية بحيث تصبح تمارس اختصاصات هي أصلا من اختصاصات سلطات التحقيق.[3]

وتجدر الإشارة إلى أن بعض القوانين لا تسمح لأعضاء الضبط القضائي بتفتيش منزل المتهم بناءا على حالة التلبس مثل قانون الإجراءات المصري بعد حكم بعدم دستورية المادة 47 منه في حين تميز قوانين أخرى لإعطاء الضبط القضائي القيام به في حالة التلبس كما هو الحال في فرنسا وذلك طبقا لنص الفقرة الأولى من المادة 56 والتي

---

[1]_ نبيلة هبة هروال، مرجع سابق، ص 246.

[2]_شنة زواوي، أحكام تفتيش المساكن والأشخاص والمركبات في القانون بين النظرية والتطبيق، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07، العدد 02، 2018، ص ص 152-153.

[3]_نبيلة هبة هروال، مرجع سابق، ص 246.

جاء في مضمونها: " أنه إذا كانت الجناية من النوع الذي يمكن إثباته بواسطة ضبط أوراق ومستندات وغيرها من الأشياء الموجودة في حوزة أشخاص تضمن مشاركتهم في الجناية أو تكون بيدهم مستندات أو أشياء تتعلق بالأفعال الإجرامية المرتكبة فإن ضابط الشرطة القضائية ينتقل حالا إلى منزل أو لا شك الأشخاص لإجراء التفتيش.[1]

وكذلك الشأن بالنسبة للمشرع الجزائري الذي سمح لأعضاء الضبط القضائي بتفتيش منزل المتهمفي حالة التلبس.[2]

4_ التفتيش بناءا على رضى المتهم

وجد حالات خارج التلبس يمكن أجراء بتفتيش فيها طالما تم هذا التفتيش بناءا على رضى وموافقة ذي الشأن فقد نصت المادة 76 من قانون الإجراءات الجنائية الفرنسي على أن تفتيش المساكن وضبط الأشياء المتعلقة بالجريمة لا يمكن أن يتم دون موافقة صريحة من الشخص المزمع إجراء التفتيش عنده كما تقرر المادة 127 من المرسوم الصادر في 20 ماي 1903 أن تفتيش المسكن وضبط الأشياء المتعلقة بالجريمة لا يجب أن يتم دون موافقة صريحة من ذي الشأن وتعطي بحرية وعن معرفة للسبب كما يجب أن تكون مكتوبة وأن تصدر هذه الموافقة من لدن الشخص ذي الشأن لا غيره.[3]

إلا أنه بالنظر إلى القضاء الأمريكي فنجده لا يشترط صدور الموافقة من ذي الشأن فقط بل يكتفي في حال غيابه أن يحل محله أشخاص آخرون في حال ما إذا كان شخصان أو أكثر يشتركان في امتلاك جهاز الحاسب إذا كانت الملفات غير محمية لكلمة السر خاصة بمالكه وهنا يمكن لرجال الضبط القضائي الاعتماد على إرادة أحدهما

---

[1]_ طارق إبراهيم الدسوقي عطية، النظام القانوني لحماية المعلومات، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 436.

[2]_ راجع المادة 44 و45 ق إ ج ج، مرجع سابق.

[3]_ طارق إبراهيم عطية الدسوقي، مرجع سابق، ص 438.

طالما كان لذلك الأخير سلطة على الحاسوب[1] وهو ما قضى به القضاء الأمريكي في قضية STAIESV SMITHE.[2]

المطلب الثاني:

الآثار المترتبة على التفتيش في الجرائم المعلوماتية

إن الغاية من التفتيش هي ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها سواء أكان هذا الشيء أدوات استعملت في ارتكابها أو شيء ينتج عنها أو غير ذلك من الأشياء التي تفيد في كشف الحقيقة عن الجريمة أو مرتكبها ومن المألوف في الجرائم العادية أن يقع الضبط على الأشياء المادية أما في الجريمة المعلوماتية فقد يرد على المكونات المادية للحاسب كما قد يرد على المكونات المعنوية كما أن طرق ضبط الدليل المعلوماتي يتخذ طابعا خاصا يتلاءم وطبيعته، وسنتطرق في هذا المطلب إلى محل الحجز في الجريمة المعلوماتية (فرع أول) والطرق التي يتم بها حجز الدليل المعلوماتي (فرع ثاني).

---

[1] _ نبيلة هبة هروال، مرجع سابق، ص ص 249-250.

[2] _ وتتخلص وقائع القضية في:

كان المدعو "SMITHE " يعيش مع سيدة تدعى "USHMAN" وابنها وعندما أثير إدعاء التحرش الجنسي بالأطفال ضد "SMITHE " وافقت " USHMAN " على تفتيش حاسوبه الخاص الموجود داخل المنزل في تجويف مرتبط بحجرة النوم الرئيسية بالرغم من أن هذه الأخيرة استخدمت الحاسوب الخاص بالمتهم مرات قليلة فقط فقررت محكمة المقاطعة بأنها يمكنها إيداء الموافقة على تفتيش الحاسوب الخاص بالمتهم لأن "USHMAN " لم تكن ممنوعة من دخول المكان الذي به الحاسوب كما أن المتهم ليس لديه كلمة السر يحمي حاسوبه. فقررت المحكمة أن المرأة المذكورة لديها السلطة على الموافقة على التفتيش حتى إن كانت تنقصها السلطة الفعلية على الموافقة. أنظر نبيلة هبة هروال، مرجع نفسه، ص 251.

الفرع الأول: محل الحجز في الجريمة المعلوماتية

القاعدة في حجز أنه لا يقع إلا على الشيء المادي أما الأشياء المعنوية فإنها لا تصلح بطبيعتها لتكون محل للحجز أما في الجريمة محل الدراسة فقد يرد الحجز بالإضافة إلى الأشياء المادية على البيانات المعالجة الكترونيا أو الكيانات المنطقية للحاسب.[1]

أولا: الأشياء المادية كمحل للحجز في الجريمة المعلوماتية

لا يثير ضبط المكونات المادية للحاسب الآلي أي مشاكل في الفقه المقارن إذ يمكن ضبط هذه الأخيرة بموجب القوانين التقليدية للتفتيش وبالتالي لا يوجد خلاف بين الفقهاء في إمكانية ضبطها.[2]

ومن المكونات المادية في الجريمة المعلوماتية التي يجوز ضبطها والتي لها قيمة خاصة في إثبات جرائم الحاسبة الآلية.

1_ وحدة الإدخال (inputunit).

2_ شاشة اللمس (touchscreen).

3_ نظام الفأرة ونظام القلم الضوئي (pen systemlight).

4_ نظام القراءة الضوئية للحروف (opticalcharacterreading system).

5_نظام قراءة الحروف المغناطسية(magneticcharacterreading system).

6_ نظام إدخال الأشكال والرسومات.[3]

---

[1]_ أسامة بن غانم العبيدي، مرجع سابق، ص 109.

[2]_ ما يلاحظ بالنسبة لضبط الأدلة الرقمية في القانون رقم 09-04 هو استعمال المشرع لمصطلح الحجز على غير ما هو مألوف في ق إ ج ج حيث كان يستعمل مصطلح الضبط .

كون مصطلح الحجز لا يتعارض مع مصطلح الضبط إلا أنه أنسب من ناحية تماشية مع الطبيعة اللامادية للأدلة الرقمية.

[3]_ طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 449.

7_ وحدة الذاكرة الرئيسية سواءا كانت ذاكرة القراءة فقط أم كانت ذاكرة للقراءة والكتابة معا.

8_ وحدة الحساب والمنطق وتشمل مجموعة من الدوائر الالكترونية والمسجلات.

9_ وحدة التحكم وما تستعين به من مسجلات وسماعات منطقية.

10_ وحدة المخرجات وما تشمله من وسائط كالشاشة والطابعة.

11_ وحدة التخزين الثانوية وما تشمله من أقراص مغناطيسية بنوعيها المرن والصلب والفلاش ميموري والسي دي.[1]

ثانيا: المكونات اللامادية كمحل للحجز في الجريمة المعلوماتية

نظرا للان الضبط في مجال الجرائم المعلوماتية محله البيانات المعالجة الكترونيا فقد ثار التساؤل حول مدى صلاحية هذه الأخيرة لأن تكون محلا للضبط وقد انقسم الفقه القانوني حول مدى إمكانية ضبط الدليل في الجرائم المعلوماتية خصوصا فيما يتعلق بالبيانات الالكترونية المجردة من الدعامة المادية المخزنة عليها وكذلك ما إذا كانت تقبل التعامل معها وفق النصوص القانونية التقليدية المعمول بها في ضبط الأدلة الجنائية.[2]

أ_ الرأي الأول:

يرى بأن بيانات الحاسبة الالكترونية لا تصلح لأن تكون محلا للضبط لإنتفاء الكيان المادي عنها ولا سبيل لضبطها إلا بعد نقلها إلى كيان مادي ملموس عن طريق التصوير الفوتوغرافي أو بنقلها على دعامة أو غيرها من الوسائل المادية ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء الملموسة.[3]

ففي ألمانيا حسب القسم 94 من قانون الإجراءات الجنائية الألماني فإن الأدلة المضبوطة يحب أن تكون الأشياء مادية ملموسة وذلك يشمل ليس فقط نظم الحاسب بل أيضا حاملات البيانات وهذه البيانات تنقصها بالضرورة الخاصة المادية وبالتالي لا تشكل

---

[1]_ أسامة بن غانم العبيدي، مرجع سابق، ص 109.

[2]_ أسامة بن غانم العبيدي، مرجع سابق، ص 109.

[3]_ علي عدنان الفيل، مرجع سابق، ص 57.

الأشياء التي يمكن ضبطها لكن إذا تم طبع هذه البيانات فإن المطبوعات يمكن ضبطها.[1]

ب_ الرأي الثاني

يرى أصحاب هذا الرأي لا يوجد ما يمنع من حجر هذه البيانات والمعطيات المعالجة بنظام المعلومات أو ما يعرف بالبيانات الالكترونية على أساس تمديد مفهوم ضبط الأدلة المادية لتشمل البيانات الالكترونية والتي تتكون من المعلومات وهي لا يمكن حجزها لأنها أشياء معنوية، بينما البيانات المعالجة آليا فهي ذات طابع مادي على أساس أنها ذبذبات أو موجات كهرومعناطيسية يمكن أن تسجل وتخزن على وسائط معينة ويمكن قياسها.[2]

ويستند هذا الرأي على بعض النصوص التشريعية كالمادة 7/29 من قانون الإثبات الكندي والتي تنص: " أن التفتيش وضبط الدفاتر والتسجيلات الخاصة بمؤسسة مالية يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة وتستوي في ذلك أن تكون السجلات مكتوبة أو في شكل إلكتروني".[3]

وفي اليونان نجد المادة 251 من قانون الإجراءات الحالي تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل.

ويفسر الفقه اليوناني عبارة أي " شيء " بأنها تشمل ضبط البيانات المخزنة والمعالجة إلكترونيا".[4]

---

[1]_ طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 454.

[2]_ رضا هميسي، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل، المجلد 22، العدد 2، 2016، ص 175.

[3]_ علي عدنان الفيل، مرجع سابق، ص 58.

[4]_ طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 452.

وبستقراء موقف المشرع الجزائري نجده قد ذهب إلى تأكيد الاتجاه القائل بإمكانية تفتيش البيانات المعالجة آليا وضبطها.

حيث نصت المادة 06 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على حجز المعطيات الآلية حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية وعلى البيانات المعالجة إلكترونيا.[1]

حيث تدخل المشرع الجزائري لاستكمال ما تبقى من فراغ تشريعي في المنظومة التشريعية بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وكان المشرع قد أضفى حماية للمعطيات بموجب الأمر رقم 05/03 المؤرخ في 2003/07/19 والمتعلق بحقوق المؤلف والحقوق المجاورة والتي اعتبرت قواعد البيانات من المصنفات المحمية سواءا كانت مست نسخة أو على دعامة قابلة للاستغلال.

وأجازت المادة 146 من الأمر ذاته لضابط الشرطة القضائية والأعوان التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة حجز نسخ دعائم المصنفات ووضعها تحت حراسة الديوان.[2]

إلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي قام هو الآخر بإدخال تعديل على قانون الإجراءات الجزائية الفرنسي لسد هذا الفراغ التشريعي بموجب قانون الأمن الداخلي رقم 239 لسنة 2003، حيث نص في فقرته الثالثة من المادة 57-1 على أن المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين

---

[1]_ تاني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية الفنية، دون طبعة، تلمسان ، الجزائر، 2018، ص 120.

[2]_ انظر المادة 05 و 146 من القانون رقم 05/03 المؤرخ في 19 جمادى الأولى عام 1424 هـ الموافق لـ 19 جويلية 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ج ج، رقم 44 الصادرة بتاريخ 2003/07/19.

نسخها على دعامات تخزين و دعامات تخزين المعلومات هذه يتعين تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون.[1]

كما نصت الاتفاقية الأوربية لجرائم المعلوماتية لعام 2001 على صلاحية المكونات المنطقة والوسائل الالكترونية لأن تكون محلا للضبط حيث نص في الفقرة 3 من المادة 19: " يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئات المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين (1) و(2)".[2]

الفرع الثاني: طرق حجز الدليل المعلوماتي

إن طريقة ضبط المعلومات المعالجة آليا تختلف عما هي عليه عن ضبط المكونات المحسوسة كالأقراص المرنة والمودم والخادم ونتيجة لذلك يفضل البعض استخدام مصطلح الحصول بطريقة مشابهة عوض مصطلح الضبط (SAISIN) وذلك من أجل الأخذ في الاعتبار الطرق الأخرى لرفع المعلومات الغير المادية وهو ما يستفاد بوضوح من الفقرة 03 من المادة 19 من الاتفاقية الأوربية لجرائم المعلوماتية.[3]

أولا: طريقة النسخ

بالرجوع إلى نص الفقرة 03 من المادة 19 السالفة الذكر فإن هذه الأخيرة تخول سلطات البحث والتحري طريقتين لضبط البيانات المعلوماتية.

تتلخص الطريقة الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية (كالأقراص المغنطة، بطاقات الذاكرة، فلاش ديسك) وتكون

---

[1] _ بركر رشيدة، مرجع سابق، ص 420.

[2] _ براهيمي جمال، مرجع سابق، ص 47.

[3] _ بوبكر رشيدة، مرجع سابق، ص 421.

هذه الأخيرة قابلة للضبط والوضع في إحراز مختومة حسب ما هو مقرر في قواعد حجز الدليل المنصوص عليها في قوانين الإجراءات الجزئية.[1]

ويتم هذه العملية باستخدام برامج متخصصة في النسخ مثل برنامج " Laplink"، حيث تؤخذ نسخه من تلك البيانات ويتم لصقها وخزنها باسم معين على أحد منظومات التخزين (Flashmemory. DVD. CD) الخاصة بالجهة القائمة بالحجز وعادة ما يؤخذ بهذه الطريقة الأحراز المعلوماتية المشفرة بغية فك شفرتها فيما بعد[2] كما يتم اللجوء إليها عندما يتخوف من أن يكون النظام المعلوماتي مبرمجا ببرامج القنبلة الذهنية.[3]

وطبقا للمادة 06 من القانون رقم 09-04 فتتم طريقة نسخ المعطيات محل البحث والمعطيات الضرورية لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز ثم توضع في احراز طبقا لأحكام قانون الإجراءات الجزئية وهذه الطريقة يتم اللجوء إليها حسب نفس المادة عندما يكون من غير الضروري حجز كل المنظومة المعلوماتية.[4]

وعليه فإن حجز المعطيات ذات المحتوى المجرم أو التي تستخدم كدليل يكون غير كاف إذا لم يقترن بحجز المعطيات اللازمة لفهمها ومثاله حالة متابعة بسبب نشر صور ومقالات ذات محتوى مجرم على مواقع التواصل الاجتماعي كالفايسبوك، فإنه لا يكفي

---

[1]_ براهيمي جمال، مرجع سابق، ص 48.

[2]_ قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق جامعة محند أكلي أولحاج، البويرة، 2015، ص ص 76-77.

[3]_ القنابل الذهبية: هي التي تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة كإنفجار القنبلة الالكترونية التي استهدفت نظام البريد الالكتروني في الجامعة التي ترتبط به أعمال على درجة من الأهمية كالتسجيل وتبادل الأبحاث حيث تمكن فريق تحقيق من تحديد الساعة والعنوان الخاص بالكمبيوتر المستخدم في الجريمة.

انظر سجتوت نادية، التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية، المجلة العربية للأبحاث في العلوم الإنسانية والاجتماعية، المجلد 1، العدد 1، الجلفة، 2009، ص 44.

[4]_ انظر المادة 06 من القانون رقم 09-04، مرجع سابق.

نسخ المحتوى المجرم لوحدة بل يجب نسخ الصفحة كاملة وبصفة تفاعلية.[1] ومثال ذلك نسخ الصفحة كاملة بصيغة HTML.[2]

ثانيا: طريقة المنع من الوصول إلى المعلومات

وهي المعبر عنها في المادة 19 الفقرة 03 من اتفاقية بودابست وتكون باستعمال تقنيات وتدابير الحماية الفنية كتقنيات التشفير والترميز، منع الكتابة واستخدام الخوارزميات للملفات المشفرة من أجل منع الأشخاص المرخص لهم باستخدام المنظومة المعلوماتية والوصول إلى المعطيات والبيانات الأصلية التي تحتويها هذه المنظومة أو القيام بنسخها فهذه الطريقة تتضمن تدابير مستحدثة خصصا لضبط الأدلة الجنائية الرقمية وهي المعبر عنها في هذه المادة بمصطلح " الحصول بطريقة مشابهة على البيانات المعلوماتية وتكون في حالة ما إذ استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى.[3]

ووفق المذكرة التفسيرية للاتفاقية فإنه يتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت المعطيات تتضمن حظرا أو ضررا بالمجتمع بالبرامج التي تحتوي على فيروسات أو تقدم نموذج لعمل الفيروسات أو القنابل.[4]

وقد نص المشرع الجزائري على هذا الإجراء في المادة 07 من القانون رقم 09-04 والتي تنص على أنه:"إذ استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 لأسباب تقنية يتعين على السلطة التيتقوم بالتفتيش استعمال التقنيات المناسبة لمنع

---

[1]_ نلني لحسن، مرجع سابق، ص 122.

[2]_ هي اختصار للمصطلح " HydertextMarkupLanguage" وتسمى بلغة كل ميز النصوص، لغة خاصة ايتكرت لأجل إنشاء وتصميم صفحات الويب، فهي توضع شرحا مفضلا حول الشكل الذي عليه آلية عرض محتويات الموقع الالكتروني. أطلع عليه في 2019/09/08، الساعة 23:08 متاح على الموقع: Http// :mut tamil. com

[3]_ براهيمي جمال، مرجع سابق، ص 48.

[4]_ بوكر رشيدة، مرجع سابق، ص 123.

الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".[1]

إلا أن الملاحظ في هذه المسألة هو عدم تحديد المشرع للأسباب التقنية المانعة للحجز سواء ما تعلق منها بالمنظومة المعلوماتية نفسها كاستجابة الدخول لوجود كلمة السر أو نظام الحماية يصعب اختراقه.[2]

إلا أننا نؤيد رأي المشرع في عدم تحديد الأسباب المانعة للحجز كونها أسباب تقنية بحتة يرجع تقديرها للتفتيش أصحاب الاختصاص تبعا لما يرونه من استحالة في الحجز المعطيات.

ثالثا: طريقة التجميد

أسلوب تجميد التعامل بنظام المعالجة الآلية للمعطيات أو أحد القطع المكونة له والتي استخدمت في ارتكاب الجريمة ويتخذ هذا الأسلوب عدة مظاهر من أبرزها نظام ضبط محتويات القرص الصلب وكذلك نقل المحتويات إلى أقراص صلبة متعددة أو ممغنطة ومثل هذا الإجراء يصلح في مواجهة الحاسبات الخادة التي تحتوي مواقع الهاكرز أو ملفات فيروسية.[3]

---

[1]_ أنظر المادة 07 من القانون رقم 09-04، مرجع سابق.

[2]_ يزيد بوحليط، تفتيش المنظومة المعلوماتية و حجز المعطيات في التشريع الجزائري، مرجع سابق، ص 91.

[3]_ بوبكر رشيدة، مرجع سابق، ص 421.

المبحث الثاني: الضوابط الإجرائية الأخرى المتصلة بعملية التحقيق في الجريمة المعلوماتية

تعتبر المعاينة والخبرة من المتطلبات الضرورية في الجرائم المعلوماتية والتي يمكن من خلالها الوصول إلى دليل جنائي يخدم التحقيق كما يقدم هذان الإجراءات عونا كبيرا لجهات التحقيق في كشف غموض الجريمة خاصة ما تعلق منها بالجانب الفني تمهيدا للوصول إلى رأي بشأن المسائل الفنية التي تمثل المظهر الخاص لهذه الجرائم والتي من خلالها يمكن إظهار الحقيقة من خلال دراسة هذين الإجراءين اللذين يمثلان العمود الفقري لعملية التحقيق حيث سنتطرق في المطلب الأول إلى المعاينة ودورها كضابط للتحقيق في الجريمة المعلوماتية أما في المطلب الثاني فسنحاول التطرق إلى الخبرة الفنية على اعتبارها من متطلبات التحقيق في هذه الجرائم.

المطلب الأول:

المعاينة كضابط التحقيق في الجريمة المعلوماتية

تعتبر معاينة مسرح الجريمة عملية رئيسية في كشف الحقيقة والبحث عن آثار الجريمة ومرتكبها حيث يعتبر مسرح الجريمة شاهدا شكليا وموضوعيا في التحقيق لما يوفره من أدلة إثبات، غير أنه في الجرائم المعلوماتية يتخذ مظهرا خاصا يتماشى وطبيعة الجريمة غير أن البعض يرى بأن المعاينة في هذه الجرائم ليست بنفس درجة أهميتها في الجرائم التقليدية غير أن هذا لا يمنع من التسليم بأهميتها في كشف غموض بعض الجرائم.

وسنتطرق في هذا المطلب إلى مفهوم المعاينة ومدى صلاحية مسرح الجريمة المعلوماتي للمعاينة (فرع أول)، وإلى القواعد الواجب إتباعها في معاينة الجرائم المعلوماتية (فرع ثاني).

الفرع الأول: مفهوم المعاينة ومدى صلاحية مسرح الجريمة المعلوماتي للمعاينة

أولا: مفهوم المعاينة

لم يحدد المشرع المقصود بالمعاينة لذلك فقد عرفت من قبل الفقه الجنائي بأنها رؤية بالعين لمكان أو شخص لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة وعرفت كذلك بأنها إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة.[1]

كما تعرف بأنها الملاحظة والكشف الحسي المباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالة والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة.[2]

كما تتصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بها من آثار وعرفها جانب من الفقه بأنها مشاهدة وإثبات الحالة في مكان الجريمة.[3]

والمعاينة من إجراءات التحقيق الابتدائي ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق[4] والأصل أن تجرى المعاينة بحضور طرف الدعوى الجزائية غير أنه يجوز للمحقق إجراءها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة.[5]

وللمعاينة أهمية كبيرة في الجرائم التقليدية حيث يوجد مسرح فعلي يحتوي على آثار مادية فعلية يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها

---

[1]_ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 179.

[2]_ نبيلة هبة هروال، مرجع سابق، ص 212.

[3]_ الصغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 83.

[4]_ تنص المادة 79 من ق إ ج ج على أنه: " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة...".

[5]_ علي عدنان الفيل، مرجع سابق، ص32.

في الإثبات غير أن الحال ليست كذلك عندما يتعلق الأمر بالجرائم المعلوماتية حيث يندر أن تخلف آثار مادية.[1]

سيما إذا تعلق الأمر بالجرائم الواقعة على المكونات غير المادية أو بواسطتها كما أجاز القانون الأمريكي 18USCODE SEC2703 لعضو نيابة المعلومات CTC إذ يعجل بإجراء المعاينة خشية ضياع الأدلة وذلك بإرسال رسالة إلى مزود الانترنت يلزمه فيها بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذها لذلك الإجراء أو غيره، ولكن تأتي المعاينة بثمارها وتفي بأغراضها المنشودة نجد أن بعض التشريعات قد قررت جزاءات جنائية على كل من يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة.[2]

وغرار ذلك نجد أن المشرع الجزائري أخذ نفس التوجه حيث يحضر على كل شخص لاصقة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة، أو بنزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي وإلا عوقب من 200 إلى 1000 دج.[3]

ثانيا: مدى صلاحية مسرح الجريمة المعلوماتي للمعاينة وهنا يجب التفريق بين حالتين:

أ_ الجرائم الواقعة على المكونات المادية للحاسب

أن مسرح الجريمة المعلوماتي يتكون بحسب طبيعة إلى مسرحين، الأول تقليدي ويقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح الجريمة التقليدية، وقد يترك به

---

[1]_ علي عدنان الفيل، مرجع سابق، ص 32.

[2]_ نبيلة هبة هروال، مرجع سابق، ص 215.

[3]_ انظر المادة 43 من ق إ ج ج، مرجع سابق.

الجاني آثار عدة كالبصمات وغيرها وربما ترك متعلقاته الشخصية أو وسائط تخزين رقمية.[1]

أي أن الجرائم تكون واقعة على المكونات المادية للحاسب ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب والكابلات الخاصة به وشاشات العرض ومفاتيح التشغيل وليس هناك صعوبة مادية لتقرير صلاحية هذه المكونات للمعاينة من قبل مأموري الضبط القضائي والتحفظ على الأشياء التي تعد أدلة ارتكاب الجريمة ونسبها إلى شخص معين.[2]

ب_ الجرائم الواقعة على المكونات الغير المادية للحاسبوبواسطتها

وفي مقدمتها الجرائم الواقعة على برامج الحاسب الآلي وبياناته أو التي تتم بواسطتها وكذلك الجرائم التي بطرق الانترنت وجرائم التزوير المعلوماتي والتخريب الذي يتم بطريق الفيروس المعلوماتي.[3]

ويلاحظ أن معاينة مسرح الجريمة المعلوماتية الواقعة على المكونات غير المادية يثير صعوبات كون مسرح الجريمة هنا يختلف عنه في الجرائم التقليدية، حيث أن المعاينة بصورتها التقليدية تنحصر في البحث عن الأدلة المادية الملموسة في حين أن الأثر الذي يتركه المجرم المعلوماتي غالبا ما يكون ذا طبيعة معنوية غير محسوسة يصعب التعامل معه عبر الوسائل التقليدية.[4]

كما أن هناك صعوبات تحول دون فعالية المعاينة في الجرائم المعلوماتية يمكن تلخيصها في النقاط التالية:

---

[1]_ الصغير يوسف، مرجع سابق، ص 84.

[2]_ عبد الفتاح بيومي حجازي، مرجع سابق، ص 182.

[3]_ مرجع نفسه، ص 185.

[4]_ راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، دراسة تطبيقية على إمارة أبو ظبي، مركز الإمارات للدراسات والبحوث الإستراتيجية، مجلة دراسات الإستراتيجية، الإمارات العربية المتحدة، الطبعة الأولى، العدد131، 2008، ص 50.

_ ندرة وتخلف الآثار المادية عند ارتكاب الجريمة المعلوماتية كما أن طول الفترة بين وقوع الجريمة ومن اكتشافها يكون له أثر سلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار.[1]

_ العدد الكبير من الأشخاص الذين قد يترددون على مسرح الجريمة خلال فترة زمنية التي تتوسط ارتكاب الجريمة واكتشافها، مما يهيء الفرصة لحدوث تغيير أو إتلاف أو عبث بآثار الجريمة أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة.[2]

_ إمكانية التلاعب في البيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل الجاني ولذلك يرى جانب من الفقه الجنائي ضرورة إتباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجريمة المعلوماتي.[3]

الفرع الثاني: القواعد الواجب إتباعها في معاينة الجرائم المعلوماتية

نظرا للخصوصية والحساسية التي تتمتع بها مسرح الجريمة المعلوماتي ينبغي قبل إجراء المعاينة مراعاة بعض القواعد التي من شأنها العمل على عدم ضياع الأدلة أو فسادها ولاسيما عندما يتعلق الأمر بالمعاينة المكونات اللامادية للبيئة الرقمية.

أولا: كيفية الانتقال إلى العالم الافتراضي للمعاينة

لقد بين فيما سبق أن مسرح الجريمة المعلوماتي يتكون بحسب طبيعة من مسرح تقليدي وأخر افتراضي حيث لا يثير المسرح التقليدي إشكالا كما سبق وأن وضعنا فهو

---

[1]_ بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ميلة، 2014/2013، ص 86.

[2]_ محمد محمد الالفي، الدليل الرقمي وحجيته في الإثبات، بحث متوفر على الموقع:

http// : repository. Nauss.edu. sa

[3]_نبيلة هبة هروال، مرجع سابق، ص 218.

يعامل معاملة مسرح الجريمة التقليدية باستثناء بعض الخصوصية الفنية المرتبطة بطبيعة هذه الجرائم.

وبما أن المعاينة في جرائم الانترنت تتم كأي جريمة أخرى أن يجب على المحقق الانتقال المادي إلى مسرح الجريمة غير أنه في الجرائم المعلوماتية قد لا يكون الانتقال إلى مسرح الجريمة ماديا، إذ يمكن للمحقق اللجوء إلى مقهى الانترنت أو إلى بيت الخبرة القضائية أو الخبرة الاستشارية إذ توفر له في التشريع ما يبح له ذلك كما يمكن أيضا اللجوء إلى مقر مزود الانترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.[1]

ويمكن المعاينة عن طريق تصوير شاشة الحاسوب سواء باستخدام آلة تصوير تقليدية أو عن طريق تجميد مخرجات الشاشة أو عن طريق حفظ الموقع باستخدام خاصية الحفظ الموجودة في نظام التشغيل كما يمكن إجراء المعاينة بالنسبة لشبكة الانترنت عن طريق إنزال نسخة من المصنف محل الاعتداء في حالة الاعتداء على الملكية الفكرية أو التحفظ على نسخة في حالة الصور والعلامات بطباعتها على ورقة مثلا.[2]

ثانيا: الخطوات الواجب مراعاتها قبل البدأ في معاينة الجرائم المعلوماتية

يجب على المحقق وقبل شروعه في معاينة مسرح الجريمة المعلوماتي الأخذ بعين الاعتبار خصوصية هذا الأخير إذ ينبغي التعامل معه بحذر واحترافية من أجل تحقيق أقصى النتائج المرجوة إذ ينبغي عليه مراعاة الخطوات التالية:

1_ تحديد فريق المعاينة من المحققين والخبراء الذين تتوفر فيهم الكفاءة العلمية والخبرة الفنية في المجال المعلوماتي.

---

[1]_ نبيلة هبة هروال، مرجع سابق، ص 215.

[2]_ جميل عبد الباقي، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الانترنت، ورقة عمل مقدمة في الحلقة العلمية بعنوان (الانترنت والإرهاب) المنظمة من طرف جامعة نايف الأمنية، ص 19.

2_ توفر معلومات مسبقة عن مكان الجريمة والمالك لهذا المكان ونوع وعدد الأجهزة الكمبيوتر والشبكات المرتبطة بها فنيا.

3_ تحديد الأدوات والاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في معاينة الجرائم المعلوماتية.

4_ اتخاذ الإجراءات والاحتياجات المسبقة قبل بدا المعاينة كقطع التيار الكهربائي عن مكان المعاينة لمنع الجاني من القيام بأي فعل من شأنه التأثير على أداة الجريمة أو محو آثارها.[1]

5_ عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبار للتأكد من خلو الموقع الخارجي من أي مجال لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.[2]

6_ وضع حراسة على المكان وعدم السماح لأي شخص من الاقتراب من الأجهزة لحين الانتهاء من فحصها ونقلها إلى الجهة المختصة أن تطلب الأمر ذلك.[3]

المطلب الثاني:

الخبرة الفنية من متطلبات التحقيق في الجريمة المعلوماتية

تعتبر الخبرة الفنية إحدى المتطلبات الضرورية للتحقيق في الجرائم المعلوماتية لما تقتضيه هذه الأخيرة من معرفة واضطلاع في الجانب الفني ففي كثير من الأحيان يؤدي نقص الخبرة لدى سلطات التحقيق والاستدلال إلى تدمير الدليل المعلوماتي، ولذلك فإنه لا يمكن تصور عدم اللجوء إليها في مثل هذه الجرائم وسنتطرق في هذا المطلب إلى مفهوم

---

[1]_ نديم محمد حسن الشيراوي، سلطات النيابة العامة في الجريمة المعلوماتية، مجلة الأندلس للعلوم الإنسانية، العدد 13، المجلد م 1، 2007، ص 318.

[2]_محمد محمد الالفي، الدليل الرقمي وحجيته في الإثبات، بحث متوفر على الموقع:

http// : repository. Nouss.edu. sa

[3]_ راشد بشير إبراهيم، مرجع سابق، ص 53.

الخبرة الفنية وأهميتها ودورها في استخلاص الدليل المعلوماتي (فرع أول)، وإلى القواعد التي تحكم الخبرة الفنية (فرع ثاني).

الفرع الأول: ماهية الخبرة الفنيةو متطلبات أعمالها لإثبات الجرائم المعلوماتية

أولا: ماهية الخبرة الفنية

تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوفر لدى جهات التحقيق والقضاء من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن واقعة أو نسبها للمتهم.[1]

فهي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكانية استخلاص الدليل منه أو هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية لا تتوفر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته.[2]

حيث أنه ومنذ ظهور الجرائم التكنولوجيا الحديثة و الضبطية القضائية وسلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسوب الآلي والمنظمات المعلوماتية بغرض كشف الغموض عن الجريمة وتجميع أدلتها، ولقد أشار المشرع الجزائري في الفقرة الأخيرة من المادة الخامسة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إلى إمكانية لجوء السلطات المكلفة بتفتيش المنظومة المعلوماتية إلى تسخير كل شخص له

---

[1] _ براهيمي جمال، مرجع سابق، ص 68.

[2] _ عبد الناصر محمد محمود فرغلي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الجنائية والطب الشرعي المنظم بارياني للفترة الممتدة بين 12 و14 نوفمبر 2008، ص24.

دراية بعمل المنظومة محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها.[1]

وتكمن أهمية الاستعانة بالخبرة الفنية في أنها تبين الطريق لجهات التحقيق والقضاء وسائل السلطات المختصة بالدعوى الجزائية.

لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد من 143 إلى 156 من قانون الإجراءات الجزائية واعتبرها من إجراءات البحث عن الدليل حيث تنص المادة 143 على أنه : " لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمربندب خبير إما من تلقاء نفسها أو بناءا على طلب من النيابة العامة وإما بطلب من الخصوم".[2]

وأهمية الاستعانة بالخبرة الفنية أو الخبير الفني في الجرائم المعلوماتية تظهر عند غياب هذا الأخير فقد تعجز جهات الاستدلال عن كشف غموض الجريمة كما قد تفشل جهات التحقيق عن جمع الأدلة حول الجريمة وقد تدمر الدليل المعلوماتي أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.[3]

ولعل الأهمية التي تكتسبها الخبرة في مجال الجرائم المعلوماتية جعلت بعض التشريعات لا تكتفي بالنصوص التقليدية التي تنظم الخبرة وعمدت إلى إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال.

ومن التشريعات الحديثة التي نظمت عمل الخبرة في مجال الجرائم المعلوماتية القانون البلجيكي الصادر في 2000/11/23 فقد نصت المادة 88 منه على أنه يجوز

---

[1]_ راجع الفقرة الأخيرة من المادة 05 من القانون رقم 09-04، مرجع سابق.

[2]_ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص 166.

[3]_ علي عدنان الفيل، مرجع سابق، ص 28

لقاضي التحقيق وللشرطة القضائية أن يستعين بالخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول لبيانات المخزونة أو المعالجة أو المنقولة بواسطته.[1]

وفي هذا نجد المشرع الجزائري لم يختلف عن باقي التشريعات وذلك بموجب المادة 05 الفقرة الأخيرة من القانون رقم 09-04 والتي أعطت الحق للسلطات المكلفة بتفتيش المنظومة المعلوماتية بتسجيل كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها في أداء مهامها وتزويدها بكل المعلومات اللازمة لانجاز مهمتها.[2]

كما أنه وبموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26 تم إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني.

أما على المستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية ومن الفروع التي تتضمنها خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية.[3]

ثانيا: متطلبات أعمال الخبرة الفنية لإثبات الجرائم المعلوماتية

تتنوع الوسائل الالكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية كما تتنوع شبكات الاتصال بينها وتتمايز خصائصها الفنية فتتدرج تحت تخصصات فنية وعلمية دقيقة مما يستوجب والحال كذلك أن تدفق جهات التحقيق والمحاكمة عند اختيارها للخبير

---

[1]_ علي عدنان الفيل، مرجع سابق، ص 30.

[2]_ راجع المادة 05 الفقرة الأخيرة من القانون رقم 09-04، مرجع سابق.

[3]_ أمال فكري، إشكالية الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابر للحدود، مجلة العلوم القانونية والسياسة، المجلد 9، العدد 1، 2018، ص 635.

فيجب أن تثيق أنه تتوفر لديه الإمكانيات والقدرة العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه.[1]

إذ يجب أن تتوفر لديه الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية، وبالنظر إلى الطبيعة العلمية والفنية للخبرة في مجال الجرائم المعلوماتية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية:

1_ الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشكيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر وأكواد التشفير.

2_ طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.[2]

_ قدرة الخبير على إتقان مأمورية دون أن يترتب عن ذلك أي مشكل أو تدمير للأدلة المتحصلة من الوسائل الالكترونية.[3]

3_ أن تتوفر لديه القدرة على تحويل أدلة الإثبات من الكيانات غير المحسوسة إلى كيانات مقروءة أو مرئية وعزل النظام المعلوماتي دون إلحاق هدر بالأدلة المستهدفة.

4_ القدرة على تتبع مصادر الاعتداء وتحركات مستخدمي الحاسب الآلي من حيث المعلومات التي يقدمونها والمواقع التي يزورونها ومشاركتهم في المنتديات وعرف الدردشة والرسائل والصور التي يبثونها.[4]

---

[1]_ ثنيان ناصر إل ثنيان، إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص سياسة جنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 112.

[2]_ عبد الناصر محمد محمود فرعلي، مرجع سابق، ص 33.

[3]_ثنيان ناصر إل ثنيان، مرجع سابق، ص 112.

[4]_ راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، دراسة تطبيقية على إمارة أبو ظبي، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الأولى، العدد 131 ، الإمارات العربية المتحدة، 2008، ص 69.

علاوة على ذلك يرى البعض أن الخبير المعلوماتي يجب أن يكون لديه العلم والخبرة والمهارة التي تمكنه من أداء مهمته على أكمل وجه لذلك يجب أن يكون ملم بمايلي:

1_ نظم الحاسب الآلي بمكوناته المادية والبرمجية.

2_ وسائل وبرامج وطرق فحص نظم الحاسب الآلي كبرامج كشف وإزالة الفيروسات وبرامج استرجاع البيانات والمعلومات وإصلاح التالف منها وإظهار المخفي وبرامج فك الشفرات وكلمة السر.

3_ وسائل وبرامج نسخ البرامج والملفات وعمل نسخة من القرص الصلب طبقا للأصل.

4_ كيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث.

5_ كيفية تفسير الملاحظات والربط بين الأشياء واستخلاص النتائج ذات دلالة علمية، فنية، قضائية.[1]

الفرع الثاني: القواعد التي تحكم الخبرة الفنية في الجريمة المعلوماتية

مما لاشك فيه أن الخبرة الفنية في مجال المعلوماتية قواعد وضوابط تحكمها فمنها ما هو قانوني ومنها ما هو فني.

أولا:القواعد القانونية التي تحكم الخبرة الفنيةفي الجريمة المعلوماتية

أ_ اختيار الخبراء

يختار الخبير من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة دون الالتزام بترتيب معين تبعا لثقة المحقق أو القاضي وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل.[2]

---

[1]_ عبد الناصر محمد محمود فرعلي، مرجع سابق، ص 33.

[2]_ بوكر رشيدة، مرجع سابق، ص 426.

غير أنه كاستثناء يجوز اختيار الخبراء وخارج الجدول ويستوجب تحت طائلة البطلان أن يستند هذا إلى تسبيب خاص كحالة الاستعجال، وغياب الخبير المتخصص المسجل في الجدول أو التخصص الدقيق للخبير في فرع من الفروع العلمية ذات الصلة بمسألة البحث.[1]

وقد تركت حرية اختيار خبير واحد أو عدة خبراء لجهات التحقيق، فمفهوم نص المادة 147 من ق إ ج ج فإنه للقاضي أن يندب خبيرا واحدا أو خبراء متعددين حسب الحاجة ولا يهم أن كان شخصا طبيعيا أو معنويا كمؤسسة متخصصة تعمل في مجال الخبرة الفنية.[2]

ب_ واجبات الخبير الفني

1_ حلف اليمين

قد واجب المشرع الجزائري الخبير قبل أداء مهامه أن يحلف اليمين القانونية حيث تنص المادة 145 من ق إ ج ج على أنه: " يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية: أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبإخلاص وأن أبدي رأيي بكل نزاهة واستقلال".

ولا يجدد هذا القسم مادام الخبير مقيدا في الجدول ويؤدي الخبير الذي يختار من خارج الجدول قبل مباشرة مهامه اليمين السابق بيانها أمام قاضي التحقيق أو القاضي المعين من الجهة القضائية.

---

[1]_ نجمي جمال، قانون الإجراءات الجزائية على ضوء الاجتهاد القضائي، الطبعة الثالثة، دار هومة، الجزائر، 2017، ص 251.

[2]_ براهيمي جمال، مرجع سابق، ص 74.

إذ يجب لصحة عمل الخبير أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الاطمئنان في أرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو الثقة بقية أطراف الدعوى.[1]

2_ ممارسة مهامه تحت الرقابة القضائية

على الخبير أن يتولى مهمته تحت رقابة القاضي الذي أمر بإجراء الخبرة ولا يستلزم ذلك حضوره فعلا أثناء قيامه بأعماله بل يكفي أن يبقى على اتصال معه بهدف إحاطته علما بكل المستجدات التي تطرأ عليه في مجال عمله على اعتبار أن الخبير هومساعد فني للقاضي.[2]

حيث تنص المادة 143 من ق إ ج ج في فقرتها الأخيرة على أنه: " يقوم الخبراء بأداء مهمتهم تحت رقابة قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية التي أمرت بإجراء الخبرة.[3]

3_ إيداع تقرير الخبرة

يتعين على الخبير تفرغه منأبحاثه وفحوصاته إعداد تقرير مفصل حول المسألة محل البحث يبين فيه خلاصة ما توصل إليه من نتائج وعلى الخبير إيداع تقرير خبرته لدى كتابة الجهة القضائية التي أمرت بالخبرة خلال الآجال المجددة في أمر التعين والإنجاز استبداله بغيره.[4]

وتقارير الخبرة تصبح حتمية في الجرائم المعلوماتية نظرا للجانب التقني الطاعن عليها والذي يفرض الاستعانة بخبير لفك رموزها.

---

[1]_ راجع الفقرة الأولى والثانية من المادة 145 ق إ ج ج، مرجع سابق.

[2]_ بوكر رشيدة، مرجع سابق، ص 428.

[3]_ انظر الفقرة الأخيرة من المادة 143 من ق إ ج ج، مرجع سابق.

[4]_ براهيمي جمال، مرجع سابق، ص 75.

ثانيا:القواعد الفنية التي تحكم الخبرة الفنيةفي الجريمة المعلوماتية

تعتبر هذه القواعد الوسائل الفنية التي يستعين بها الخبير المعلوماتي من أجل إظهار الحقيقة لغرض جمع الدليل الرقمي الذي يثبت الجريمة المرتكبة ونسبها لفاعلها.

أ_ الوسائل التي يستعين بها الخبير في اكتشاف الدليل الرقمي

1_ الوسائل المادية

والتي يمكن إجمالها فيما يلي:

عنوان بروتوكول الانترنت (makip)،البريد الالكتروني، برامج المحادثة، حيث يعتبر عنوان الانترانت المسؤول عن تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها على أهدافها وهو يتواجد بكل جهاز مرتبط بالانترنت ويتكون من أربعة أجزاء حيث أن الجزء الرابع يحدد جهاز الحاسوب الذي يتم الاتصال منه، وعليه فإنه في حالة اقتراف إحدى الجرائم المعلوماتية يكون من السهل التعرف على رقم الجهاز الذي تم من خلاله ارتكاب العملية وبالتالي تحديد الجاني.[1]

_ نظام البروكسي proxy

يعمل هذا النظام كوسيط بين الشبكة ومستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهزة، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما من ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تنزيلها من قبلفيما تم إرسال الطلب إلى الشبكة العالمية، وهنا يستخدم البروكسي أحد عناوين TP ومن أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تحتفظ بتلك العلميات التي تمت عليها مما يجعل دوره قويا في الإثبات عن طريق فحص تلك العمليات المحفوظة.[2]

---

[1]_ بن فوزية محمد، الدليل الجنائي الرقمي و حجيته أمام القضاء، دراسة تطبيقية، المجلة الأكاديمية للبحث القانوني، المجلد 5، العدد 1، 2014، ص 279.

[2]_ سعيداني نعيم، مرجع سابق، ص 173.

برنامج التتبع:

تقوم هذه البرامج بالتعرف على محاولات الاختراق وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ومثاله برنامج Hack Laracev وهو مصمم للعمل في الأجهزة المكتبية وعندما يرصد محاولة للاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتناء أثر مرتكب العملية، حتى يصل إلى الجهاز الذي حدثت منه العملية.

_ أنظمة كشف الاختراق

يكمن دور هذه الفئة من البرامج في مراقبة العمليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة ومن بين هذه الأنظمة برنامج (Hack Tracer V1.2) الذي يتكون من شاشة رئيسية تقدم للمستخدم بيانا شاملا لعملية الاختراق كاسم وتاريخ الواقعة وعنوان (TP) الذي تمت من خلاله عملية الاختراق واسم مزود الخدمة والمستضيف ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي يتبعها مزود الخدمة للمخترق بما فيها أرقام هواتفها.[1]

ب_ الوسائل الإجرائية

من بين الوسائل الإجرائية التي يلجأ إليها الخبير والتي تساعده في عمله.

1_ اقتفاء الأثر

تتم عملية تبع المجرم المعلوماتي في حالة إذا لم يقم بمحو أثاره وهذا عن طريق اقتفاء هذه الآثار باستخدام مجموعة من البرامج المساعدة وصولا إلى الحاسب الذي تمت منه العملية.[2]

---

[1]_ بن فوزية محمد، مرجع سابق، ص 280.

[2]_ براهيمي جمال، مرجع سابق، ص ص 79-80.

2_ الاستعانة بالذكاء الاصطناعي

نقصد الذكاء الاصطناعي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها عن طريق عمليات حسابية يتم حلها بواسطة برامج الحاسب الآلي صممت خصيصا لهذا الغرض كبرنامجXtreeProgocdلذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة والمرنة المضغوطة وقراءة محتوياتها في صورتها الأصلية من أجل التحليل والتقويم.[1]

ثالثا: أساليب عمل الخبير

يجب على الخبير لجمع الأدلة المتعلقة بالجرائم محل الدراسة أن يتبع الخطوات التالية:

أ_ مرحلة ما قبل التشغيل والفحص

وهذه المرحلة تضم عدة خطوات يتعين على الخبير مراعاتها وتتمثل في:

1_ التأكد من مطابقة محتويات احراز المضبوطات لما هم مدون عليها.

2_ التأكد من صلاحية وحدات النظام للتشغيل.

3_ تسجيل معطيات وحدات المكونات المضبوطة كالنوع والطرازوالرقم التسلسلي.[2]

ب_ مرحلة التشغيل والفحص

وتظم هذه المرحلة عدة إجراءات تكمل المرحلة الأولى وهي:

1_ استكمال تسجيل باقي معطيات الوحدات من خلال الجهاز.

2_ وضع نسخة لكل دعامة لحماية الأصل من أي فقد أو تلف أو تدمير سببه سوء الاستخدام أو برامج القراءة المدمرة.

---

[1]_ بن فوزية محمد، مرجع سابق، ص 280.

[2]_ بوكر رشيدة، مرجع سابق، ص 480.

3_ تحديد أسماء وأنواع المجموعات البرمجية ذات دلالة بالجريمة، كبرنامج النظام وبرنامج التطبيقات وبرنامج الاتصال.

4_ إظهار الملفات المخبأة والنصوص المخفية داخل الصور.

5_ استرجاع الملفات التي تم محوها وإصلاح المعطلة أو التالفة.

6_ تخزين هذه الملفات أو البيانات وعمل نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها من أجلفحصها.

7_ إعداد قائمة يجرد فيها الخبير كل الأدلة المتحصل عليها مع إجراء مراجعة لكل نسخة أو صورة محذوفة بها في جهاز أخر للتأكد من سلامتها.

8_ تحديد الخصائص المميزة بكل جزء من الأدلة الرقمية مثل المستندات، البرامج، التطبيقات النصوص، الأصوات وتحويلها إلى هيئة مادية كل حسب طبيعته.[1]

ج_ مرحلة تحديد مدى الترابط بين الدليل المادي والدليل الرقمي

في هذهالمرحلة يتم فحص كل من الدليل المادي المضبوط والدليل المادي المستخرج من جهاز الحاسب الآلي (الذي أصله هو الدليل الرقمي)) الموجود بالملفات النظام المضبوط، كصور النصوص، أصوات ... الخ.

وبذلك يكون تم الربط بين الدليل الرقمي والدليل المادي، مما يكسب الدليل الموضوعية واليقينية التي تؤدي إلىقبوله لدى جهات التحقيق وجهات الحكم....[2]

د_ مرحلة تدوين النتائج وإعداد التقارير

حيث يتمفي هذه المرحلة إعداد تقرير بجميع خطوات وإجراءات البحث يرفق به في الغالب الملاحق الإيضاحية المصورة أو المسجلة وغيرها لاعتمادها ويتم تصديرها إلى جهات التحقيق أو جهات الحكم.

---

[1]_ براهيمي جمال، مرجع سابق، ص ص 77-78.

[2]_ عبد الناصر محمد محمود فرعلي، مرجع سابق، ص 36.

الفصل الثاني:
إجراءات التحقيق المستحدثة
في الجرائم الالكترونية

إن التطور السريع في المجال المعلوماتي و ما صاحبه من تطور في طرق و أساليب ارتكاب الجرائم في هذا المجال طرح العديد من المشاكل الإجرائية ومدى قدرة الإجراءات التقليدية للتحقيق على مسايرة هذا التطور ففي بعض الحالات يصعب على المحققين إجراء التحقيق و جمع الأدلة الرقمية بإتباعالأساليب التقليدية للتحقيق لذا فقد أجاز المشرع الجزائري اللجوء لبعض الأساليب الحديثة و الخاصة أثناء مرحلتي التحري والتحقيق الابتدائي رغبتا منه في مكافحة فعالة لبعض الجرائم الخطيرة و التي من بينها الجرائم المعلوماتية على اعتبار إن هذه الأساليب لها دور هام في جمع أدلةالإثبات الجزائية و إظهار الحقيقة قصد التوصل إلى ضبط الفاعلين الأصليين والمساهمين في ارتكاب الجريمة

وعند فشل الإجراءات التقليدية في الوصول إلى نتيجة تهم التحقيق في الجريمة وقد تبنى المشرع الجزائري أساليب جديدة و مستحدثة للتحري و التحقيق من خلال التعديلات التي المؤرخ في 22-06 ادخلها بموجب القانون20ديسمبر2006 بالإضافة إلى القانون09-04المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و الذي خلق من خلاله آليات جديدة للتحري لمكافحة الجريمة المعلوماتية ورغم ما تثيره هذه الإجراءات من مشكلات تتعلق أساسات بالمساس بالحياة الخاصة للأفراد إلا أن المشرع حرص على عدم المساس بحرمة هذا الحق من خلال الضمانات و القواعد التي أحاطها بها.

لذا ومن خلال ما سبق فقد قسمنا هذا الفصل إلى مبحثين حيث سنتطرق في المبحث الأول إلى التسرب كإجراء مستحدث للتحقيق في الجريمة المعلوماتية من خلال تبيان مفهومه كمطلب أول والضوابط التي تحكم عملية التسرب كمطلب ثان أما المبحث الثاني فسنتطرق من خلاله إلىالإجراءاتالأخرى المستحدثة للتحقيق في الجريمة المعلوماتية حيث سنتطرق في المطلب الأول لاعتراض المراسلات و المراقبة الالكترونية أما في المطلب الثاني لإجراء الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بحركة السير.

المبحث الأول:

التسرب كإجراء تحقيق جديد في الجريمة المعلوماتية

يعتبر التسرب من إجراءات البحث والتحقيق الجديدة التي سعى المشرع الجزائري وعلى غرار معظم التشريعات إلى إرسائها لمسايرة التطور الحاصل في ميدان الإجرام والتفعيل البحث والتحري وجمع الأدلة عن الجرائم ولقد نص المشرع الجزائري على هذا الإجراء لأول مرة في المادة (56) من قانون مكافحة الفساد[1]، حيث استعمل مصطلح الاحتراف للدلالة عليه إلا أن المقصد من هذا المصطلح وكيفيات اللجوء إليه بقي مبهما إلى غاية تعديل قانون الإجراءات الجزائية بموجب القانون رقم 22/06 المؤرخ في 2006/12/20 أين تم تحديد كل الإجراءات المتعلقة به في المواد من 5 مكرر 11 إلى 65 مكرر 18.

المطلب الأول:

مفهوم التسرب

يعتبر التسرب من التقنيات الجديدة والخاصة للبحث والتحري في أخطر الجرائم والتي حددتها المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي من ضمنها الجرائم المعلوماتية وسنحاول في هذا المطلب تحديد مفهوم إجراء التسرب من خلال التطرق إلى تعريفه (فرع أول) وبيان خصائصه وصوره (فرع ثاني).

[1]_ المادة 65 من القانون رقم 01/06 المؤرخ في 21 محرم عام 1427 الموافق لـ 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج، العدد 14 الصادرة بتاريخ 03/08/ 2006 على أنه: " من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في القانون يمكن اللجوء إلى التسليم المراقب أو إتباع أساليب تحري خاصة كالرصد والاختراق ...".

الفرع الأول: تعريف التسرب

التسرب تقنية جديدةبالغة الخطورة على أمن الضبطية القضائية وتتطلب الجرأة والكفاءة ودقة العمل.

أولا: التعريف التسرب لغتا

التسرب كلمة مأخوذة من الفعل تسرب تسربا أي دخل وانتقل خفية وهو الولوج بطريقة سرية إلى مكان أو جماعة وجعلهم يعتقدون بأن التسرب ليس غريبا عنهم.[1]

ثانيا: التعريف الاصطلاحيللتسرب

يقصد بالتسرب تلك العملية المحضر لها والمراد منها التوغل من أجل معرفة حقيقة النشاط البارز وكشف النشاط الخفي والعمل من أجل الاستعلام عنه ومعرفة كل التفاصيل والخصوصيات والأسرار حسب تطلعات الجهات الأمنية والقضائية.[2]

ثالثا: التعريف القانوني للتسرب:

عرف قانون الإجراءات الجزائية التسرب في المادة 65 مكرر 12 بقولها: " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهمانه فاعل معهم أو شريك أو خاف.[3]

وتعريف قانون الإجراءات الجزائية أكثر دقة من بعض ما تعارف عليه الفقه من تعريفات ومن ذلك ما ذهب إليه البعض من أن التسرب هو تلك العملية المحضر لها المراد منها التوغل داخل مكان، أو هدف أو تنظيم إجرامي يصعب الدخول إليه ويسمى بالمكان المغلق لمعرفة حقيقته معرفة جيدة من خلال نشاطه البارز وكشف نشاطه

---

[1]_ صحراوي الرزاق، التسرب ودوره في التصدي لمكافحة الجريمة المنظمة العابرة للأوطان-الجزائر نموذجا- ، مجلة البحوث القانونية والاقتصادية، المجلد 2، العدد 2، 2020، ص179.

[2]_ المرجع نفسه، ص 180.

[3]_ بوكر رشيدة، مرجع سابق، ص 434.

الخفي، والراجح فقها هو أن الأصح في تسميه العملية بالغة العربية هو الاحتراق وليس التسرب وهو المصطلح الذي استعمله المشرع الجزائري في المادة 56 من قانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته المعدل والمتمم.[1]

ومن خلال التعاريف السابقة يمكن تصور عملية التسرب في نطاق جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وإشراكه في محادثة في غرف الدردشة أو حلقات النقاش والاتصال المباشر في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات، متدخلا في ذلك هوية مستعارة أو باستخدام أسماء أو صفات هيئات وهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعلا مثلهم سعيا منه إلى الكشف والإطاحة بالمجرمين.[2]

الفرع الثاني: خصائص التسرب وصوره

أولا: خصائص التسرب

إن إجراء التسرب له خصائص تتلائم وضعية الجرائم المقصودة به حيث تلعب هذه الخصائص دورا هاما في ضمان فعالية ونجاعة إجراء التسرب ومن بين هذه الخصائص يمكن حصر أهم أربع خصائص يتميز بها.

1_ السرية

والمقصود بها هو كتمان السر فيما يتعلق بالعملية، وتكون السرية عاملا يضمن عدم الترصد بالنسبة للمتسرب ومن جهة يضمن إبقاء النشاط الإجرامي للشبكة في سريان

---

[1]_ بامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانون الجزائري والفرنسي، مجلة دفاتر السياسية والقانون، المجلد 11، العدد 2، 2019، ص 150.

[2]_ براهيمي جمال، مكافحة الجرائم المستحدثة في التشريع الجزائري، التسرب نموذجا، مرجع سابق، ص ص142_143.

عادي دون أن يمسك المجرم بأنه تحت المراقبة كما أن لها دور فعال في ضمان أمن وسلامة المتسرب وحسن سير العملية.[1]

ولقد أجاز المشرع الجزائري لضابط الشرطة القضائية أو عون الشرطة القضائية المتسرب إخفاء هويته وصفته الحقيقية أثناء القيام بالمهمة وفق ما نصت عليه المادة 65 مكرر 1/16 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية والتي نصت: " لا يجوز إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات".[2]

وتتمثل صورة السرية في:

أ_ الهوية المستعارة

جاء في الفقرة 65 مكرر 12 من قانون الإجراءات الجزائية على أنه : " يسمح لضابط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة...

فيقوم ضابط الشرطة القضائية تحت علم وكيل الجمهورية بمنح العون المتسرب أوراق هوية يتم استعمالها أثناء القيام بعملية التسرب لأن هذا الأمر يساعد على اكتشاف الكثير من الحقائق التي قد يتعذر اكتشافها في حال إفصاح المندمج أو المتسرب عن صفته.[3]

ب_ عدم إيداع رخصة الإذن:

هذا الإجراء شكلي من شانه المحافظة على السرية في العملية خاصة أثناء القيام وبعد الانتهاء من العملية خاصة أثناء القيام بها وبعد الانتهاء من العملية تودع الرخصة

---

[1]_ أسماء عنتر، مرجع سابق، ص 79.

[2]_ داعي عز الدين، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحوث القانونية، مجلد 8، العدد 3، 2017، ص 205.

[3]_ لدغم سيكو زكريا، النظام القانوني للتسرب، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية والإدارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص 78.

بشكل عادي في ملف إجراء التسرب وهذا حسب نص المادة 65 مكرر 15 من قانون الإجراءات الجزائية.[1]

2_ الحيلة

تعتبر الحيلة من أهم خصائص التسرب والتي نجدها في نص المادة 65 مكرر 12 .... بإيهام .... فعلى القائم بإجراء التسرب مراعاة هذا الأمر وذلك بالقضاء على كل الشكوك التي تبادر إلى ذهن المشتبه فيه[2] وذلك لنجاح هذه العملية وما على ضباط وأعوان الشرطة القضائية إلا استعمال الحيلة والخديعة، وافتعال سيناريوهات وهمية لكسب ثقة المجرم لجمع المعلومات المتعلقة بالجريمة.[3]

3_ الخطورة

يعتبر إجراء التسرب من أخطر الإجراءات التحقيق القضائي ويعود ذلك إلى عدة عوامل:

1_ منها ما يتعلق بالإجرام فهي كل الأعمال التي يؤديها المتسرب المتعلقة بالتغطية على صفة القضائية وعليه تعد من الأعمال الإجرامية المرتبة لخطورة كونها تعد اعتداء على حقوق الآخرين ما قد يعرض المتسرب إلى الدفاع الشرعي من الصحي.[4]

2_ ما يتعلق بمكان تواجد المتسرب فواجبه المهني يحتم عليه التواجد بأماكن أكثر أمنا للمجرمين والأخطر على حياته مثل التسرب في الشبكات الإرهابية التي تعتمد على الأوكار والمخابئ[5]، كما تظهر صعوبة وتعقيد هذا الإجراء بكونه يتطلب تنفيذه ربط علاقات مع الأشخاص المشتبه فيهم والاتصال بهم بشتى الطرق سواء المباشرة أو غير

---

(1)_لدغم سيكو زكريا، مرجع سابق، ص 78.

(2)_ أسماء عنتر، مرجع سابق، ص 79.

(3)_ وداعي عز الدين، مرجع سابق، ص 205.

(4)_ أسماء عنتر، مرجع سابق، ص 79.

(5)_ مرجع نفسه، ص 80.

المباشرة، حتى لو تطلب الأمر المشاركة في نشاط الخلية الإجرامية[1] حيث قد يأخذ المتسرب عدة صور للاندماج في نشاط الخلية الإجرامية وهذا ما سنتطرق إليه في النقطة الموالية.

ثانيا: صور التسرب

يعتبر القائم بإجراء التسرب كعميل سري حيث قد يأخذ عمله عدة صور ليتمكن من الحصول على المعلومات واختراق الجماعة الإجرامية فقد بأخذ صورة الفاعل أو الشريك أو الخاف حيث نصت المادة 65 مكرر 12 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية:

على أنه: " يقصد بالتسرب قيام ضباط وأعوان الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة أو بإيهامهم أنه فاعل أو شريك لهم أو خاف .[2]

1_ المتسرب كفاعل

نص المشرع الجزائري في المادة 44 من قانون العقوبات على أنه: " يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي".[3]

إذ ولكي يتوصل ضباط وأعوان الشرطة القضائية المأذون له بعملية التسرب إلى الهدف المنشود لابد أن يتصرفوا مع المشتبه فيهم كأنهم عناصر منهم وفاعلين ومساهمين

---

[1]_ رويس عبد القادر، أساليب البحث والتحري وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 2، العدد 1، 2017، ص 42.

[2]_ انظر المادة 65 مكرر 12 من قانون الإجراءات الجزائية.

[3]_ انظر المادة 41 من قانون رقم 04-05 المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات، ج ر ج ج، العدد 71 الصادرة بتاريخ 2004/10/10، معدل ومتمم.

في الجريمة لكسب ثقتهم وللحصول على دليل مادي للإيقاع المشتبه فيهم وليس للتحريض على ارتكاب الجريمة.[1]

2_ المتسرب كشريك

المقصود بالشريك في حسب نص المادة 42 من قانون العقوبات " يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك"[2]، ويندرج ضمن الأعمال المسهلة.

من يقف لمجرد مراقبة الطريق أثناء تنفيذ لجريمة ومن يقف إلى جوار الفاعل الأصلي لشد أزره ورفع روحه المعنوية دون أن يتدخل بأي عمل يعد بدا في التنفيذ وفق ضابط الشروع، أما الأعمال المنفذة أو المتممة فهي التي تعاصر المرحلة الختامية لتنفيذ الجريمة وهي لا تختلف عن الأعمال المسهلة باعتبارها تعاصر أيضا مرحلة تنفيذ الجريمة.[3]

كما حدد المشرع الجزائري الأشخاص الذين يدخلون في حكم الشريك حسب نص المادة 43 من قانون العقوبات " يأخذ حكم الشريك كل من اعتاد أن يقدم مسكنا أو ملجأ أو مكان للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو الأشخاص أو الأموال مع عمله بسلوك الإجرامي".[4]

وعملا بمحتوى هذه النصوص القانونية الخاصة بالشريك، فإنه يعتبر عون أو ضابط الشرطة القضائية المتسرب وكذا العون المسخر شركاء في الجريمة، بالنظر إلى

---

[1]_ وداعي عز الدين، مرجع سابق، ص 207.

[2]_ انظر المادة 42 من قانون العقوبات الجزائري، مرجع سابق.

[3]_ بامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانون الجزائري والفرنسي، مرجع سابق، ص 150.

[4]_ انظر المادة 43 من قانون العقوبات الجزائري، مرجع سابق.

المساعدة المادية والمعنوية التي يقدمونها للمشتبه فيهم لإنجاز مخططاتهم الإجرامية، لكن دون أن يكونوا مسؤولين جزائيا عن ذلك لأنها تدخل ضمن الأفعال المبررة.[1]

وهذا حسب نص المادة 65 مكرر 12 التي تنص في فقرتها الثانية على:" ... يسمح لضباط أو عون الشرطة القضائية لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر14 أدناه...".[2]

كما جعل المشرع الجزائري على غرار المشرعين الفرنسي وما جاء بمسودة مشروع قانون يقضي بتغير وبتميم قانون المسطرة الجنائية المغربيةمن بين الصور التي تتم بها عملية التسرب الإخفاء والذي تطرق إليه في نص المادة 387 من الأمر 66-156 المتضمن قانون العقوبات الجزائري.[3]

3_ المتسرب كخاف

تعني كلمة خاف لغة، الخافي من الأشياء هو ما لا يرى وتعني كلمة إخفاء، أي كتم وخبأ.

وفي الاصطلاح القانوني يأخذ الإخفاء حالتين حالة تعتبر فيها صورة من صور التدخل في الجناية أو الجنحة، شرط أن يكون مرتكب جرم الإخفاء على علم سابق بالجريمة المراد ارتكابها، وحالة يعتبر فيها الإخفاء جريمة مستقلة بحد ذاتها، يشرط أن يكون مرتكب الإخفاء قد علم بالجريمة بعد ارتكابها، وفي هذه الحالة تكون جريمة الفاعل مستقلة عن جريمة الفاعل الأصلي.[4]

---

[1]_ وداعي عز الدين، مرجع سابق، ص 207.

[2]_ انظر المادة 43 من قانون العقوبات الجزائري، مرجع سابق.

[3]_ وداعي عز الدين، مرجع سابق، ص 207.

[4]_ لدغم شيكو زكريا، مرجع سابق، ص 82.

ولقد عرف المشرع الجزائري الخافي في نص المادة 387 على أنه: " كل من أخفى أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة أو في جزء منها ... ".[1]

كما تطرق إليها كذلك في نص المادة 43 من القانون رقم 06-01 المؤرخ في 2006/02/20 والمتعلق بالوقاية من الفساد ومكافحته " ... كل شخص أخفى عمدا كل أو جزء من العائدات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القانون".

كما نصت المادة 65 مكرر 12 من قانون الإجراءات الجزائية على أن المتسرب يستطيع القيام بإخفاء الأشياء المتحصل عليها أثناء قيامه بمهامه وإذا استدعت الضرورة التحري والتحقيق ذلك دون أن تقوم المسؤولية الجزائية على ارتكابه لهذا الفعل.[2]

المطلب الثاني:

الضوابط التي تحكم عملية التسرب في الجرائم الالكترونية

نظرا لخطورة إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه قيد المشرع الجزائري اللجوء إلى هذا الإجراء بجملة من الضوابط والشروط التي يتعين مراعاتها قبل وأثناء مباشرته.

الفرع الأول: الشروط الشكلية لإجراء التسرب

لقد حرص المشرع الجزائري على إحاطة عملية التسرب بشروط شكلية لضمان حسن سير هذه العملية وذلك راجع لطبيعة هذا الإجراء كونه من الإجراءات التي يمنع اللجوء إليها في الحالات العادية ومن بين الشروط الشكلية.

---

[1]_ انظر المادة 387 من قانون العقوبات.

[2]_ لدغم شيكو زكريا، مرجع سابق، ص 83.

أولا: تحرير تقرير من طرف ضابط الشرطة القضائية

بحيث يقوم ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب بتحرير تقرير يتضمن العناصر الضرورية لمعاينة الجريمة وذلك ما نصت عليه المادة 65 مكرر 13 من قانون إ ج ج " يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقرير يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضباط أو العون المتسرب وكذا الأشخاص المسخرين طبقا للمادة 65 مكرر 14 أدناه".[1]

وعليه فالتقرير يجب أن يحتوي على العناصر التالية:

1_ طبيعة الجريمة

وقد حدد المشرع الجزائري هذه الجرائم وحصرها في 7 جرائم وطبقا لنص المادة 65 مكرر 5 والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بحيث يجب أن تتوافق طبيعة الجريمة مع ما هو محصور من جرائم في المادة 65 مكرر 5 .[2]

2_ السبب وراء العملية

على ضابط الشرطة القضائية أن يذكر مبررات ودواعي اللجوء إلى هذا الإجراء وهي غالبا مرتبطة بضرورة التعمق في البحث والتحري خاصة مع هذا النوع من الجرائم ذات الطابع المعقد وهذا من أجل إقناع وكيل الجمهورية بمنح الإذن لهذا الإجراء وهذا ما يدعو ضابط الشرطة القضائية إلى تأسيس طلبه على عدد من العناصر التي تبرر هذا الإجراء.[3]

---

[1]_ انظر المادة 65 مكرر 13 ق إ ج ج.

[2]_ راجع المادة 65 مكرر 5 من ق إ ج ج.

[3]_ لدغم شيكو زكريا، مرجع سابق، ص 73.

3_ هوية ضابط الشرطة القضائية

يجب أن يتضمن التقرير ذكر هوية ضابط الشرطة أو عون الشرطة القائم بالعملية وذلك بكتابة جامع المعلومات المتعلقة بهويته أو صفته.[1]

4_ تحديد عناصر الجريمة

وذلك بذكر جميع المعلومات المتعلقة بها والمكونة لهاكا:

_ ذكر هوية الأشخاص المشتبه فيهم كتحديد أسمائهم وألقابهم المستعارة والأفعال المجرة المنسوبة لكل واحد منهم وتاريخهم الإجرامي.

_ ذكر الوسائل المستعملة في الجريمة: تحديد المركبات المستعملة والأماكن والعناوين المرتادة من قبلهم وأماكن التخزين.[2]

ثانيا: الإذن بمباشرة عملية التسرب

قبل البدا في تنفيذ عملية التسرب لابد من الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية[3]. حيث نصت على هذا الشرط المادة 65 مكرر 11 ومفاده أنه لا يجوز لضابط الشرطة القضائية اللجوء إلى التسرب إلا بناءا على إذن مكتوب صادر من وكيل الجمهورية المختص أو قاضي التحقيق بعد إخطار وكيل الجمهورية.[4]

---

[1]_ معزيز أمينة، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة القانون والمجتمع، المجلد 3، العدد 1، 2015، ص 252.

[2]_ لدغم شيكو زكريا، مرجع سابق، ص 74.

[3]_ معزيز امينة، مرجع سابق، ص 252.

[4]_ براهيمي جمال، مرجع سابق، ص 144.

حيث تنص المادة 65 مكرر 11 على أنه : " ... يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة ومباشرة عملية التسرب ضمن الشروط المبينة في المراد أدناه".[1]

بحيث يكون الإذن بالتسرب حسب الشروط المبينة في المادة 65 مكرر 15 وهي:

1_ أن يكون الإذن مكتوبا ومسببا

من بين شروط التي اشتراطها المشرع في الإذن بالتسرب هي الكتابة والتسبيب ويكون هذا تحت طائلة البطلان وفقا للمادة 65 مكرر 15 من ق إ ج ج والتي تنص على أنه: " يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا تحت طائلة البطلان...".[2]

فالكتابة تعتبر ركنا شكليا لإصدار الإذن فإذا تخلفت يعتبر الإذن باطلا فأساس الإجراءات تبقى في الوثائق المكتوبة والمعروضة على القاضي وبالتالي لا يجوز لوكيل الجمهورية إصدار إذن بصفة شفوية.

أما التسبيب فيعتبر ضمانة هامة إذ توضح من خلاله الأسباب المبررة التي دفعت بوكيل الجمهورية الإصدار إذن بإجراء التسرب الذي تقتضيه الضرورة البحث والتعمق والتحري في الجرائم.[3]

2_ هوية ضابط الشرطة القضائية

يجب أن يتضمن الإذن الممنوح بالتسرب الهوية الكاملة لضابط الشرطة القضائية المسؤول عن عملية التسرب كالاسم واللقب والصفة والرتبة والمصلحة التابع لها.[4]

---

[1]_ انظر المادة 65 مكرر 11 من ق إ ج ج.

[2]_ راجع المادة 65 مكرر 15 من ق إ ج ج.

[3]_ أسماء عنتر، مرجع سابق، ص 81.

[4]_ لدغم شيكو زكريا، مرجع سابق، ص 57.

3_ مدة العملية التسرب

حدد قانون الإجراءات الجزائية في المادة 65 مكرر 15 مدة العملية بأربعة أشهر قابلة للتحديد ضمن نفس الشروط أي بناء على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.[1]

بحيث يجب على وكيل الجمهورية أو قاضي التحقيق الذي إذن بالقيام بعملية التسرب أن يحدد المدة الزمنية للعملية والتي لا يمكن أن تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق بنفس الشروط.[2]

ويجوز لقاضي الذي رخص بإجراء التسرب أن يأمر في أي وقت بوقفه قبل انقضاء المدة القانونية وفي هذه الحالة وتحسبا للظروف الأمنية للمتسرب أجازت المادة 65 مكرر 17 من نفس القانون لهذا الأخير مواصلة نشاطه لمدة لا تتجاوز أربعة أشهر دون أن يكون مسؤولا جزائيا على ذلك بشرط أن يخبر السلطة المصدرة للإذن بذلك في أقرب أجل.[3]

4_ الجهات المخول لها إصدار الإذن بإجراء عملية التسرب

تبعا لنص المادة 65 مكرر 11 من ق إ ج ج فإن الأشخاص المخول لهم منح الإذن بمباشرة عملية التسرب لهم وكيل الجمهورية باعتباره المسؤول الأول عن منح الإذن بصفته الممثل الأول للنيابة العامة، كما يستطيع قاضي التحقيق أن يمنح الإذن مباشرة العملية بعد إخطار النيابة العامة.[4]

---

[1]_ معزيز امينة، مرجع سابق، ص 253.

[2]_ راجع المادة 65 مكرر 15 من ق إ ج ج.

[3]_ براهيمي جمال، مرجع سابق، ص 144.

[4]_ راجع المادة 65 مكرر 11 من ق إ ج ج.

الفرع الثاني: الشروط الموضوعية لعملية التسرب

بالإضافة إلى المشرع والضوابط الإجرامية المذكورة أعلاه أحاط المشرع عملية التسرب بشروط موضوعية فالتسرب من الإجراءات التي لا يمكن اللجوء إليها إلا في حالة عدم قدرة أساليب التحقيق العادية على تحقيق نتيجة كما أنه يتم اللجوء إليه في جرائم حددها المشرع على سبيل الحصر.

لذلك ينبغي أن يتم التسرب تحت مسؤولية الجهات المختصة مع احترام السرية وتوفر حالة الضرورة التي تفرض اللجوء إليه.

أولا: وجود حالة الضرورة

لقد نصت المادة 65 مكرر 11 من القانون رقم 06-22[1]على هذه الحالة بعبارة"عندما تقتضي ضرورات التحري أو التحقيق في الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 05 أعلاه " وهو ما نجده يتطابق مع نص المادة 706-81 من قانون الإجراءات الجزائية الفرنسي حيث استعمل المشرع الفرنسي عبارة " nécessites" التي يقصد بها ضرورات البحث مما نستنتج أنه إذ كان بإمكان النيابة العامة استعمال الطرق الكلاسيكية في البحث والتحري عن الجرائم فإنه لا يجوز لها اللجوء إلى إجراء عملية التسرب إلا للضرورة فقط[2]، فضرورة التحقيق في معناها الضيق تعد من الشروط الأساسية للجوء إلى هذا الإجراء لأن التسرب أجيز لعلة معينة ولغرض خاص وبصفة

[1]_ تنص المادة 65 مكرر 11 من قانون ق إ ج ج على أنه: " عندما تقتضي ضرورات التحري أو التحقيق في الجرائم المذكورة على سبيل الحصر.

في المادة 65 مكرر 05 أعلاه يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه".

[2]_ وداعي عز الدين، مرجع سابق، ص 211.

استثنائية، فتخلف تلك العلة يمنح قاضي التحقيق من الإذن به وإلا عد متعسفا، أو بمعنى أخر أن التسرب الذي لا يلتمس من حصوله فائدة لإظهار الحقيقة يعد تسربا تحكميا.[1]

ثانيا: السرية

لقد حرص المشرع الجزائري على سرية عملية التسرب وحصر مجال العلم بها في الجهات القضائية المختصة المانحة للإذن (وكيل الجمهورية، قاضي التحقيق) وذلك وفقا للمادة 65 مكرر 16 من قانون الإجراءات الجزائية.

والسرية في قصد المشرع هي السرية المطلقة[2] ومن خلال ما جاء في نص هذه المادة فقد ذهب المشرع إلى أبعد من ذلك حيث رتب جزاء على كل من يكشف هوية ضابط الشرطة القضائية حيث تنص المادة على أنه: " ... يعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 50.00 دج إلى 200.000 دج".

وإذا تسبب هذا الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (05) سنوات إلى عشر (10) سنوات والغرامة من 200.000 دج إلى 500.000 دج.

وإذا تسبب هذا الكشف عن وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من 500.000 دج إلى 1000.000 دج دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات".[3]

---

[1]_ فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، المجلد 21، العدد 1، 2016، ص 247.

[2]_ أسماء عنتر، مرجع سابق، ص 83.

[3]_ انظر المادة 65 مكرر 16 من قانون إ ج ج.

كما رتب المشرع الجزائري حماية أخرى تمثل في عدم تقديم العون المتسرب للإدلاء بشهادته شخصيا حفاظا على حياته، حيث يقتصر الأمر على إدلاء ضابط الشرطة القضائية المكلف بتنسيق العملية وحده دون سواه[1] وهذا ما جاء بنص المادة 65 مكرر 18 من ق إ ج ج.[2]

وتتمثل صور السرية في:

1_ استعمال هوية مستعارة

جاء في الفقرة الثانية من المادة 65 مكرر 12 من قانون الإجراءات الجزائية على أنه: " يسمح لضابط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعاره..."

فيقوم ضابط الشرطة القضائية المسؤول عن العملية تحت علم وكيل الجمهورية بمنح العون المتسرب أوراق هوية مستعارة يتم استعمالها أثناء القيام بعملية التسرب لأن هذا الأمر يساعد على اكتشاف الكثير من الحقائق التي قد يتعذر اكتشافها في حالة إفصاح المندمج أو المتسرب عن صفته.[3]

2_ عدم إيداع رخصة الإذن بالعملية في ملف الإجراءات

وهذا الإجراء هو إجراء شكلي ولكن الهدف منه هو ضمان أكثر سرية عن عملية التسرب وهو ما نصت عليه المادة 65 مكرر 15 في فقرتها الأخيرة " ... توضع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب".[4]

---

[1]_ صحراوي عبد الرزاق، مرجع سابق، ص 182.

[2]_ تنص المادة 65 مكرر 18 من قانون إ ج ج على أنه: " يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهد على العملية.

[3]_ لدغم شيكو زكريا، مرجع سابق، ص 78.

[4]_ انظر المادة 65 مكرر 15 من ق إ ج ج.

ثالثا: الجهة المختصة بإجراء عملية التسرب

طبقا للمادة 65 مكرر 12 يتولى القيام بعملية التسرب ضباط وأعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية.

بالعودة إلى نص المادة 15 من ق إ ج ج نجدها قد حددت الأشخاص الذين يتمتعون بهذه الصفة.[1]

[1]_ معزيز أمينة، مرجع سابق، ص 259.

المبحث الثاني:

الإجراءات الأخرى المستحدثة للتحقيق في الجرائم المعلوماتية

في ظل إثبات الإجراءات القانونية التقليدية قصورها في مواجهة الإجرام المعلوماتي حيث أن هذه الأخيرة صيغت في أساسا لمواجهة جرائم تقليدية ، حيث رغم التعديلات التي ادخلها المشرع الجزائري عليها لجعلها ملائمة للتطبيق على الجرائم المعلوماتية إلا أن هذا لم يكن كافيا مادفع المشرع الجزائري يضع قواعد جديدة تتلائم وطبيعة هذا و لتي و ضعت الأساس لمجموعة من الوسائل الكفيلة لمواجهة هذا الإجرام المستحدث و لعل من ابرز هذه الإجراءات إعتراض المراسلات و المراقبة الالكترونية بالإضافة إلى هذا الإجراء نجد جرئين آخرين أشار إليهما المشرع الجزائري في المادة 10من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ويتعلق الأمر بإجرائي الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بحركة السيروالتي من خلالها نجد المشرع الجزائري قد خرج عن الأصل في حماية الحياة الخاصة للأفراد و عدم جواز المساس بها رغبة منه في تغليب المصلحة العامة للمجتمع وكذا خطورة هذه الجرائم ،حيث أحاطهما بجملة من القيود و التي تعتبر في نفس الوقت ضمانات من اجلو جعل اللجوء إليهيتم فقط تحت رقابة السلطات القضائية.

وسنحاول من خلال هذا المبحث التطرق إلى هذه الإجراءات على حدى حيث سنتطرق في المطلب الأول إلى بيان مفهوم اعتراض المرسلات والمراقبة الالكترونية للتحقيق في الجريمة المعلوماتية و الضمانات الواردة عليه،بينما سنخصص المطلب الثاني إلى مفهوم الحفظ العاجل للمعطيات المتعلقة بالسير و ضمانات المشتبه فيه أثناء عملية حفظ المعطيات المتعلقة بحركة السير

المطلب الأول:

اعتراض المرسلات والمراقبة الالكترونية للتحقيق في الجريمة المعلوماتية

إن الجزائر وعلى غرار باقي التشريعات المقارنة قد تبنت ما جاء في مضمون الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية لاسيما المادة 20[1]منها إذ نص المشرع الجزائري على مصطلح المراقبة في ق إ ج ج بعد تعديله سنة 2006 ليكرس مفهوم المراقبة الاستدلالية في نص المادة 16 مكرر.

وكذا في نص المواد من 65 مكرر إلى 65 مكرر 10 من ق إ ج ج والتي جاءت تحت تسمية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.[2]

وسنحاول في هذا المطلب التطرق إلى مفهوم الاعتراض والمراقبة الالكترونية (فرع أول)، وخصائص الاعتراض والمراقبة الالكترونية (فرع ثاني).

الفرع الأول: مفهوم الاعتراض والمراقبة الالكترونية

لم ينص المشرع الجزائري في قانون الإجراءات الجزائية على تعريف محدد لأسلوب اعتراض المراسلات واكتفى بوضع النصوص المنظمة له في المواد 65 مكرر 5 إلى 65 مكرر 10 من ذات القانون لكن يمكن تعريفه حسب ما عرفته بقية التشريعات المقارنة والتي عرفت الاعتراض يعني الاستيلاء بهذه على محتويات المراسلات والرسائل المنقولة عبر وسائل الاتصال السلكية ولاسلكية هذه الأخيرة التي تعتبر وسيلة تفيد في استقبال

---

[1]_ تنص المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية على أنه: " تقوم كل دولة طرف ضمن حدود إمكانياتها ووفقا للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب وكذا ما تراه مناسبا من استخدام أساليب تحري خاصة مثل المراقبة الالكترونية ...".

[2]_ بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق ، جامعة وهران، 2013، ص 125.

وإرسال الإشارات أو كتابة أو صورة أو صوت أو معلومة من أي نوع كانت عبر الأسلاك أو الألياف البصرية أو الكهرباء لاسلكية أو بمختلف الأنظمة الكهرومغناطيسية أو الأقمار الصناعية.[1]

كما عرفت لجنة الخبراء البرلمان الأوربي بمناسبة اجتماعها المنعقد بستراسبورغ في 2006/10/06 لدراسة أساليب التحري وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها " عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابها أو مشاركتهم في ارتكاب جريمة.[2]

أولا: بيان طبيعة الاتصالات الالكترونية المطلوب مراقبتها

ينص الإذن بإجراء مراقبة الاتصالات الالكترونية على محل معين يتمثل في اتصالات الشخص الالكترونية وتبعا لذلك فيجب أن يحدد الإذن كل العناصر التي تسمح بالتعرف على الاتصالات الالكترونية المطلوب تجميعها وتسجيلها والذي يجب أن يحدد بدقة طبيعة هذه الاتصالات هل هي مراسلات الالكترونية تتعلق برسائل تصل بريده الالكتروني أو أحاديث خاصة تتم عن طريق شبكة الانترنت[3] إلى جانب تحديد المدة اللازمة في عملية الاعتراض والمراقبة وقد حددها المشرع الجزائري بأربعة أشهر قابلة للتجديد ضمن الشروط نفسها حسب تقرير السلطة المصدرة للإذن[4] باستثناء إذا تعلق

---

[1]_ زوزو زليخة، ضوابط المراقبة الالكترونية في التشريع الجزائي، مجلة الفكر، العدد 18، 2019، ص 405.

[2]_ بوكر رشيدة، مرجع سابق، ص 442.

[3]_ ثابت دينازاد، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد 06، ص 218.

[4]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 95.

الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الماسة بأمن الدولة وحددت فيها مدة الإذن بـ 06 أشهر قابلة للتجديد طبقا لنص المادة 4 الفقرة 6 من القانون رقم 09-04.[1]

ولا يكفي الحصول على الإذن المتضمن العناصر السالفة بل ينبغي أن يتم الإجراء تحت الرقابة المباشرة للسلطات التي أذنت بها وهذا ما جاء بنص المادة 65 مكرر 09 من ق إ ج ج: " يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري.

بذكر بالمحضر تاريخ وساعة بداية هذه العملية والانتهاء منها".[2]

ثانيا: تسبيب الإذن باللجوء إلى اعتراض ومراقبة المراسلات

والمقصود بتسبيب الإذن بالمراقبة بأنه بيان الأسانيد الواقعية والقانونية التي أدت إلى إصداره ومن ثم يجب على السلطة القضائية المختصة ذكر الأسباب التي دفعت بها إلى إصداره[3]. فوقوع جريمة من الجرائم التي حددتها الفقرة الأولى من المادة 65 مكرر 5 من ق إ ج ج وحده لا يعد مبررا كافيا للجوء إلى هذا الإجراء بل يجب فضلا على ذلك أن تقتضي مصلحة التحقيق ذلك بأن يكون الإذن بها له فائدة في إظهار الحقيقة، فضلا عن وجود دلائل قوية على وقوع الجريمة ونسبتها إلى المتهم بأن تشير طابع الإتهام

---

[1]_ تنص الفقرة 06 من المادة 04 من القانون رقم 09-04 على أنه: " عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة " أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه لمدة 06 أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها".

[2]_ انظر المادة 65 مكرر 9 من ق إ ج ج

[3]_ ثابت دينازاد، مرجع سابق، ص ص 219-220.

بدلائها الجدية والكافية على شخص أو عدة أشخاص هم من ارتكبوا ولديهم معلومات بشأنها تفيد في إظهار الحقيقة أو بحوزتهم أشياء تعلق بها.[1]

كم أجاز المشرع إمكانية القيام بهذا الإجراء لغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما لو تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم إرهابية أو التخريب أو الجرائم الماسة بأمن الدولة.[2]

وفي جميع الأحوال فإن مسألة تقدير ضرورة اللجوء إلى هذا الإجراء من عدمه هي متروكة لتقدير السلطة القضائية.[3]

ثالثا: نوع الجريمة التي اقتضت ضرورة التحري والتحقيق القضائي

أيأن ينصب الاعتراض على إحدى الجرائم التي سمحت المادة 65 مكرر 5 من قانون الإجراءات الجزائية الاستعانة بهذا الإجراء وحددتها على سبيل الحصر.[4]

بالإضافة إلى الجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة 04 من القانون رقم 09-04 المتمثلة في الأفعال الموصوفة بجرائم إرهابية أو تخريب، الاعتداء على منظومة معلوماتية، الماسة بأمن الدولة بما فيها التي تهدد النظام العام أو الدفاع الوطني، كما تجدر الإشارة إلى أن المشرع لم يحدد نوع الجرائم التي تندرج ضمن الفقرة ج من المادة 04 والتي يصعب وصول التحريات والتحقيقات القضائية الجارية بشأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى المراقبة الالكترونية، وهو ما يفتح المجال أمام

---

[1]_ فوزي عمارة، اعتراض المرسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، المجلد 21، العدد 1، 2010، ص 240.

[2]_ انظر المادة 4 الفقرة 1 و 2 من القانون رقم 09-04.

[3]_ راجع المادة 65 مكرر 5 من ق إ ج ج.

[4]_ براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، مرجع سابق، ص 141

جميع جرائم القانون العام لكي تكون محلا للمراقبة الالكترونية كلما دعت ضرورة التحقيق لذلك.[1]

الفرع الثاني:الضمانات الواردة على عملية الاعتراض والمراقبة الالكترونية

أباح المشرع الجزائري إجراء الاعتراض والمراقبة الالكترونية لما لها من دور في كشف وإثبات الجرائم ومن جهة أخرى قيد اللجوء إلى هذا الإجراء بما يضمن قدرا من التوازن بين ضرورات التحقيق وحرية الحياة الخاصة للأفراد وسرية مراسلاتهم واتصالاتهم حيث تنص المادة 46 من الدستور على أنه:" لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".[2]

وسنورد في ما يلي أهم هذه الضمانات:

أولا: قيد اللجوء الإذن المسبق من السلطة القضائية المختصة

قيد القانون اللجوء إلى عملية المراقبة الالكترونية بشرط الحصول على الإذن مكتوب المسبق من الجهات القضائية المختصة، فاللجوء إلى الأحكام العامة المنصوص عليها في ق إ ج ج فإن الإذن يمنح لإجراء المراقبة الالكترونية من طرف وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي أو قاضي التحقيق في مرحلة التحقيق القضائي وإلا كان الإجراء باطلا وهو ما نصت عليه المادة 65 مكرر 5 من ق إ ج ج.[3]

وكاستثناء على القاعدة السابقة وبالرجوع إلى الفقرة 6 و 7 من المادة 4 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

---

[1]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 97.

[2]_ انظر المادة 46 من القانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق 06 مارس سنة 2016 المتضمن التعديل الدستوري، ج رج ج، العدد 14، ص 11.

[3]_ بن بادة عبد الحليم، المراقبة الالكترونية كإجراء لاستخلاص الدليل الالكتروني بين الحق في الخصوصية ومشروعية الدليل الالكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03، 2019، ص 397.

وعندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة يكون النائب العاملون مجلس قضاء الجزائر هو المختص بمنح الإذن بإجراء عملية المراقبة.[1]

ثانيا: العناصر الواجب توفرها في الإذن

أ_ أن يكون الإذن مكتوبا

لم ينص قانون الإجراءات الجزئية على هذا الشرط صراحة لكن بالرجوع إلى الفقرة 05 من المادة الرابعة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فقد نصت على أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه الإذن مكتوب من السلطات القضائية المختصة".[2]

واستقر الفقه في ذلك إن كتابة أمر بالإذن هو الدليل الوحيد على حصوله فلا يصح إثباته بوسيلة أخرى.

ب_ طبيعة الجريمة التي تبرر الإجراء

والتي ينبغي أن تكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية وإذا اكتشفت جرائم أخرى، غير تلك الواردة في الإذن فلا تبطل الإجراءات العارضة.[3]وهي الجرائم المحددة على سبيل الحصر في المادة 65 مكرر 5 من ق إ ج ج والمادة 4 من القانون رقم 09-04.[4]

---

[1]_ انظر الفقرة 6 و 7 من المادة 4 من القانون رقم 09-04.

[2]_ انظر المادة 4 من فقرة 05 القانون رقم 09-04.

[3]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 95.

[4]_ انظر المادة 65 مكرر من ق إ ج ج والمادة 4 من القانون رقم 09-04.

والراجح في التعاريف السابقة أنها أجمعت على أناعتراض المرسلات هي عملية أو أسلوب مراقبة سرية للمراسلات عن طريق وسائل الاتصال السلكية واللاسلكية[1] حيث في الغالب تنص على المراسلات الالكترونية مهما كان نوعها أو البرنامج الذي تمت بواسطته. حيث يهتم القائمون بعملية المراقبة بإخضاع كل المراسلات الالكترونية لعملية الاعتراض والمراقبة.[2]

ووفقا لنص القانون رقم 09-04 يقصد بالاتصالات الالكترونية في مفهوم هذا القانون ووفقا لما ذهبت إليه المادة 2 بند (و) " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.[3] أما بالرجوع إلى نص المادة 65 مكرر 05 نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصالات السلكية اللاسلكية دون أن يشير إلى طبيعة هذه المراسلات مما يفتح المجال لمختلف الرسائل المكتوبة بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو دعامات التي تصب عليها (ورقية أو رقمية) أو الوسيلة المستعملة لإرسالها (كالفاكس، تليغرام) أم لاسلكية (البريد الالكتروني، الهاتف النقال) باستثناء الكتب والمجالات والرسائل والحوليات التي تعد مراسلات خاصة.[4]

والملاحظ أن المشرع الجزائري لم يحدد التقنية التي يمكن اللجوء إليها في هذه العملية ما عدا ما ذكره في أنه يتوجب وضع الترتيبات التقنية الخاصة بالمراقبة والرجوع إلى الفقه المقارن فقد ذهب البعض إلى تحديد أشكال المراقبة الالكترونية في:

---

[1]_ زوزو زليخة، مرجع سابق، ص 406.

[2]_ بن بادة عبد الحليم، المراقبة الالكترونية كإجراء لاستخلاص الدليل الالكتروني بين الحق في الخصوصية ومشروعية الدليل الالكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03، 2019، ص

[3]_ ثابت دنيازاد، مرجع سابق، ص 220.

[4]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 89.

1_ استخدام بما يسمى بقلم التسجيل أو ما يسمى بالفخ و المتابعة في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الالكتروني أو مع من يقوم بالمحادثة الفورية معه.

2_ استخدام وسائل التنصت على محتوى الرسائل الالكترونية أو المحادثات الفورية الالكترونية بواسطة الاعتراض والتنصت.[1]

كما أن أغلب أنظمة التواصل الالكتروني حاليا والتي تكون محلا للمراقبة البريد الالكتروني والذي هو بمثابة نظام للتراسل باستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه إلا عن طريق كلمة المرور.[2]

وبموجب القانون رقم 09-04 المتضمن القواعد الخاصة المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والذي تضمن مجموعة من القواعد الوقائية التي تسمح بالترصد المبكر للاعتداءات المحتملة والتدخل السريع لمعرفة مصدرها ومرتكبيها فقد أباح المشرع الجزائري اللجوء إلى استعمال تقنية مراقبة الاتصالات الالكترونية بشأن الجرائم الماسة بتكنولوجيا الإعلام والاتصال، وذلك بعد الثورة التي عرفها العالم في مجال المعلوماتية وتطور وسائل الاتصال وظهور الانترنت وتطور صور الإجرام المعلوماتي الأمر الذي تطلب ضرورة وضع نصوص قانونية تتلاءم وخصوصيتها.[3]

وتجدر الإشارة بأن المشرع الجزائري طبقا لنص المادة 03 من القانون رقم 09-04 فقد وضع بين أيدي الجهات المختصة بمكافحة الجريمة المتصلة بتكنولوجيا المعلومات وسيلة قانونية جديدة من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع

---

[1]_ ثابت دينازاد، مرجع سابق، ص ص 207-208.

[2]_ زليخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، ص 159.

[3]_ ثابت دينازاد، مرجع سابق، ص207.

وتسجيل محتواها في حينها وهو ما أطلق عليه مصطلح مراقبة الاتصالات الالكترونية في عنوان الفصل الثاني من ذات القانون.[1]

كما حددت المادة 4 من ذات القانون حالات اللجوء إلى هذا الإجراء في حالة الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني.[2]

ومن بين الأدوات التي وضعها المشرع في يد السلطات المختصة بمكافحة الجريمة المتصلة بتكنولوجيا المعلوماتية إنشاء للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بموجب المرسوم الرئاسي رقم 15/261 والتي أوكل إليها بالإضافة إلى مهام أخرى مهمة تنشيط وتنسيق عمليات الوقائية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مع السلطات القضائية ومصالح الشرطة القضائية بما في ذلك جمع المعلومات والتزويد بها من خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريب والماسة بأمن الدولة تحت سلطة القاضي المختص وكذا تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.[3]

---

[1]_ ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية، دون طبعة، النشر الجامعي الجديد، تلمسان، الجزائر، 2018، ص 76.

[2]_ المادة 4 تنص على أنه: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

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

ب_ في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ....".

[3]_ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 93.

المطلب الثاني:

الحفظ والإفشاء العاجلان للمعطيات الالكترونية

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية من الإجراءات المستحدثة التي فرضت على مزودي خدمة الانترنت على غرار باقي التشريعات لمتابعة الالكترونية ومعاقبة مرتكبها حيث تضمن القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص المادة 10 منه على عددمن الالتزامات المفروضة على مقدمي الخدمات الانترنت فيما يتعلق بالعمليات التي تنجزها السلطات المكلفة بالبحث والاستدلال لأغراض التحقيق والتي من بينها: حفظ المعطيات المعلوماتية بالسير ووضعها تحت تصرفهم.[1]

وفي هذا المطلب سنحاول تفصيل هذين العنصرين.

الفرع الأول: مفهوم الحفظ العاجل للمعطيات بالسير

أولا: المقصود بالحفظ العاجل للمعطيات المتعلقة بالسير

استرشادا بما سبق ذكره يمكننا تحديد المقصود بحفظ المعطيات على أنه قيام مزودي الخدمات بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش وغيره.[2]

فعملية الحفظ هي من مهام مقدمي الخدمات[3] والغرض منها حماية المعطيات التي سبق وجودها في شكل مخزن من كل ما يمكن أن يتسبب في إتلافها أو تجريدها من

---

[1]_ انظر المادة 10 من القانون رقم 09-04.

[2]_ بوكر رشيدة، مرجع سابق، ص 448.

[3]_ حيث عرفت المادة 2 من القانون رقم 09-04 مقدم الخدمات على أنه:

" أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات".

صفتها أو حالتها الأصلية، و لا تهم الطريقة التي يتم من خلالها الحفظ على المعطيات الالكترونية ولا الوسيلة القانونية المقررة لذلك فالأمر متروك لكل دولة لتقدير النماذج التي تراها ملائمة لوضع عملية الحفظ موضع تنفيذ.[1]

وليست كل المعطيات المعلوماتية محل اعتبار بل المشرع الجزائري حدد المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمات وهي معطيات المرور أو كما أسماها حركة السير. والتي عرفها في الفقرة 5 من المادة 2 من القانون رقم 09-04 على أنها معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزاءا في حلقة اتصالات توضع مصدر الاتصال، والوجهة المرسل إليها والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوعه.[2]

وبالرجوع إلى المادة 10 من القانون رقم 09-04 نجد أن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشرط أن يكون هذا التسجيل في حينه.

ومن ضمن المعطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها نجد أن المشرع الجزائري حددها في المادة 11 من القانون رقم 09-04 وحصرها في:

_ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

_ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

_ الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

_ المعطيات المتعلقة بالخدمة التكميلية المطلوبة أو المستعملة ومقدميها.

_ المعطيات التي تسمح بالتعرف على المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

---

[1] _ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، ص 101.

[2] _ انظر الفقرة 5 من المادة 02 من القانون رقم 09-04.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة " أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.[1]

وإذا كان تحديد معطيات المرور أمرا سهلا عندما تكون تلك المعطيات مرتبطة بمقدم خدمة واحد، إلا أنه في الغالب يحدث أن يكون عدة مقدمي خدمات قد ساهموا في نقل الاتصال، وأن يكون بحوزة كل منهم بعض البيانات المرور المتعلقة بنقل اتصال معين والتي نتجت وتم الاحتفاظ بها بواسطة مقدم الخدمة بمناسبة مرور الاتصال عن طريق نظامه، أو عن طريق مقدمي خدمة آخرين، وقد يحدث أيضا أن تكون بيانات المرور أو بعض نماذج من بيانات المرور مشتركة بين مقدمي الخدمات الذين ساهموا في نقلالاتصال لأغراض تجارية أو أمنية أو تقنية وفي مثل هذه الحالة فإن أي من مقدمي الخدمات يمكن أن يكون بحوزته بيانات مرور جوهرية من أجل تحديد المصدر والحفظ النهائي للاتصال.

ومع ذلك ففي الغالب أن مقدم خدمة بمفرده لا يكون بحوزته من بيانات المرور ما يكفي للتحديد بإتقان لمصدر أو نهاية الاتصال إذ أن كل مقدم خدمة من هؤلاء يكون لديه بعض أجزاء اللغز وبالتالي فإنه من جميع هذه الأجزاء التي يجب اختيارها يمكن التعرف على مصدر ومنتهى هذه الاتصالات.[2]

ومن وسائل التحفظ العاجل على البيانات في مثل هذه الحالة تتمثل في قيام السلطات المختصة بإصدار أمر عاجل منفصل لكل مقدم من مقدمي لكن لوحظ أن الحصول على عدة أوامر منفصلة يمكن أن يستغرق وقتا طويلا للغاية ولذلك فإنه من بين أحد الحلول هو الحصول على أمر واحد ينطبق نطاقه على جميع مقدمي الخدمة الذين تم تحديد مشاركتهم في إرسال الاتصالات المحددة، والذي يمكن توجيهه بالتتابع إلى كل

---

[1]_انظر المادة 11 من القانون رقم 09-04.

[2]_ هلالي عبد الإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بوداباست، دار النهضة العربية، القاهرة، 2006، ص 207.

مزود خدمة محدد، كما يمكن أن تشمل البدائل الممكنة إشراك مقدمي الخدمة في هذه العملية ومطالبة مقدم الخدمة الذي تسلم الأمر بإخطار مقدم الخدمة الموالي في تسلسل لقائمة بوجود أمر الحفظ وشروطه.[1]

ثانيا: ضمانات المشتبه فيه أثناء عملية حفظ المعطيات

نظرا لتعارض عملية التحفظ على المعطيات الالكترونية مع الحق في الخصوصية فقد قيدها القانون بجملة من الشروط في شكل التزامات وضعت على عاتق مقدمي الخدمات أو أي كيان أخر يقع عليه عبئ الحفظ وتتمثل هذه الالتزامات فيما يلي:

1_ احترام المدة المقررة لعملية الحفظ

تعتبر عملية الحفظ تدبيرا مؤقتا يتم اللجوء إليه بموجب أمر توجهه السلطات المختصة إلى مقدم خدمات الاتصال تلزمه بحفظ البيانات الالكترونية فترة من الزمن، في حين حددتها الاتفاقية العربية بـ 09 يوما أو بما يحدده الاتحاد الأوربي وفق الأمر 95/46EC بالمدة الضرورية وهو الأجل الذي يسمح لضباط الشرطة القضائية بالرجوع إليها من أجل تحديد هوية وأماكن ارتكاب الجرائم المعلوماتية وذلك نظرا للاعتبارات التالية:

_ قابلية البيانات المعلوماتية للتلاشي والتلاعب والتغيير.

_ ارتكاب غالبية الجرائم عن طريق نظم الاتصالات وهو ما يساعد على تحديد هوية مرتكبي هذه الجرائم.

_ التحفظ على هوية البيانات تعتبر أحد أهم عناصر الإثبات التي يمكن أن تكشف عن هوية مرتكبي هذه الجرائم.[2]

---

[1]_ راجع المادة 16 من التقرير التفسيري لاتفاقية الجريمة الالكترونية في 23 نوفمبر 2001.

[2]_ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016، ص 232.

نجد المشرع الجزائري قد حددها بسنة واحدة منذ تاريخ تسجيلها وهو ما يستفاد جاء به نص المادة 11 من القانون رقم 09-04: " ... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداءا من تاريخ التسجيل...".[1]وهي مدة طويلة نسبيا مقارنتا بما حدده الاتحاد الأوربي وفق الأمر 95/46EC والاتفاقية العربية لمكافحة جرائم التقنية المعلوماتية والتي تنص الفقرة الثانية من المادة 23 منها على " ... تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته من أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد من أجل تمكين السلطات المختصة من البحث والتقصي".[2]

ومباشرة بعد انقضاء المدة المقررة يجب على مزود الخدمة التدخل فورا لسحب وإزالة كل المعطيات التي تم تخزينها حفاظا على سريتها وخصوصيتها، وإلا تعرض لعقوبات إدارية وأخرى جزائية، بل وعندما يؤدي إخلاله بالالتزامات المذكورة إلى عرقلة حسن سير التحريات فإن ذلك يعرضه للعقوبات المنصوص عليها في المادة 11 فقرة الأخيرة من القانون رقم 09-04.[3]

2_ الالتزام بكتمان سرية التحفظ والمعلومات المتصلة بها

أوجب المشرع الجزائري في نص المادة 10 من القانون رقم 09-04 في فقرتها الثالثة على ضرورة التزام مقدمو الخدمات في إطار تقديمهم المساعدة للسلطات المكلفة

---

[1]_ انظر المادة 11 من القانون رقم 09-04.

[2]_ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 متاحة على الموقع:

Haqqi. Info/ar/haqqi/ legislation/ arab- convention- cyber.

[3]_ حيث تنص الفقرة الأخيرة من المادة 11 من القانون رقم 09-04 على أنه: " دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 إلى 500.000 دج".

بالتحريات القضائية كتمان السر المهني عند القيام بأي من العمليات التي ينجزونها بطلب من المحققين سواءا عند قيامهم بجمع أو تسجيل المعطيات أو عند قيامهم بحفظها[1] تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق وطبقا لنص المادة 3/2/11 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزئية التي تنص على أنه " تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، دون الإضرار بحقوق الدفاع.

كل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبنية في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه".[2]

الفرع الثاني: الإفشاء العاجل لمعطيات السير

بعد هذا الإجراء من الالتزامات المترتبة على مقدمي الخدمات الانترنت في إطار مساعدة السلطات المكلفة بالبحث والتحقيق في الجرائم الالكترونية، فهي عملية مكملة لإجراء الحفظ.

وقد جاء النص على هذا الإجراء في المادة 17 من اتفاقية بودابسيت المتعلقة بالجريمة الالكترونية لسنة 2001 على أنه : " تعتمد كل دولة طرف، فيما يتعلق ببيانات الحركة الواجب حفظها بموجب المادة 16، ما يلزم من تدابير تشريعية وغيرها بغية:

أ_ ضمان توفير إمكانية التعجيل في حفظ بيانات الحركة بصرف النظر عن مشاركة مزود خدمة واحدة أو أكثر في عملية نقل هذا الاتصال، و

---

[1]_ تنص المادة 2/10 من القانون رقم 09-04 على ما يلي: " ... ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

[2]_ انظر المادة 11 من الفقرة 2 و 3 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، مرجع سابق.

ب_ ضمان تعجيل الكشف للسلطة المختصة لدى الدولة الطرف، من تحديد مزود لخدمة والمسار الذي تم من خلاله نقل الاتصال...".[1]

كما أوضح المشرع الجزائري إجراء الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله التزاما على عاتق كل مقدمي الخدمات وذلك من خلال نصه في المادة (10) من القانون رقم 09-04 على أنه:" في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه تحت تصرف السلطات المذكورة...".[2]

[1]_ انظر نص المادة 17 من اتفاقية بودابسيت لعام 2001 متوفرة على الموقع:

http:// rm. Coe.Int/budapert- convention-in- arabic.

[2]_ انظر المادة 10 من القانون رقم 09-04، مرجع سابق.

خاتمة

خاتمة

حاولنا من خلال هذه الدراسة تسليط الضوء على الجانب الإجرائي المتعلق بالتحقيق في الجريمة المعلوماتية من خلال استعراض إجراءات التحقيق فيها حيث إتضح لنا من خلال ذالك مدى تأثير الجانب التقني لهذه الجرائم و التي يميزها عن غيرها من الجرائم التقليدية و يعتبر من أبرز خصائصها.

ولقد حاول المشرع الجزائري كغيره من التشريعات الأخرى مجارات هذا التطور التكنولوجي في مجال التقنية المعلوماتية و الذي بدوره يؤثر على على مدى تطور الجريمة في هذا المجال من خلال وضع قواعد و قانونية و تعديل أخرى محاولا بذالك تلافي النقص الذي عرفه التشريع في هذا المجال وتماشيا مع طبيعة الجريمة .

وقد تمورت نتائج البحث فيما يلي:

1- المشرع الجزائري بالإضافة إلى تعديل بعض المواد أضاف مواد جديدة تتلائم مع طبيعة هذه الجرائم، حيث نجده فيما يخص التفتيش قد أدخل تعديلات على المواد 44و 47 بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006 و أجازه في كل ساعة من ساعات الليل أو النهار دون إشتراط حضور أشخاص معينين و هنا نلاحظ أن المشرع الجزائري قد غلب مصلحة المجتمع على المصلحة الخاصة للأفراد في حرمة حياتهم الخاصة مراعيا بذالك الطبيعة المميزة لهذه الجرائم و درجة الخطورة التي تشكلها ن حيث يمكن أن ترتكب في أي وقت كما أن دليل إثباتها قابل للمحو و التعديل في وقت قصرولايشترط في ذالك أن يتم في مكان الجريمة بل قد يتم عن بعد إلا انه و رغم ذالك فقد أحاط هذا الإجراء ببعض الضمانات من خلال جعله يتم تحت رقابة السلطات القضائية لإعطائه المشروعية الأزمة.

كما نلاحظ أيضا أن المشرع الجزائري وفي ظل القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام و الإتصال ومكافحتها في المادة 05 منه قد و سع من نطاق التفتيش في الجرائم المعلوماتية ليمتد إلى منظومة معلوماتية أخرى سواءا

كانت داخل الإقليم أو خارجه وكما انه في الحالة الأولى قد راعى سرعة تداول المعلومات و أجاز تمديد بمجرد إعلام السلطات المختصة بذالك مسبقا، أما في الحالة الثانية فيكون بمساعدة السلطات الأجنبية حيث يمكن أن التمتد الجريمة إلى خارج الإقليم الوطني و قد تحدث في إحدى الدول الأجنبية و تتحقق نتيجتها داخل الوطن، إلا انه راعى سيادة الدول على إقليمها و إشترط أن يتم هذا الإجراء بمساعدة في إطار الإتفاقيات الدولية ذات الصلة و فق مبدأ المعاملة بالمثل .

02-كما نلاحظ انه راعى أيضا الطبيعة الامادية للدليل الإلكتروني و بين طريقة حجزه أخذا في عين الإعتبارأن الدليل الرقمي ماهو إلا نبضات إلكترونية قابلة للنسخ و التخزين على دعامات إلكترونية بحيث يمكن حجزها و تحريزها و إستغلالها كدليل إثبات

05-للمعاينة أهمية كبيرة في الجرائم التقليدية حيث يوجد مسرح فعلي يحتوي على آثار مادية فعلية يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات غير أن الحال ليست كذلك عندما يتعلق الأمر بالجرائم المعلوماتية حيث نادرا ما تخلف آثار ماديةسيما إذا تعلق الأمر بالجرائم الواقعة على المكونات غير المادية أو بواسطتها كما،وذالك نظرا للعدد الكبير من الأشخاص الذين قد يترددون على الموقع ما يزيد من إمكانية حدوث عبث بآثار الجريمة أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة.

06- أهمية الخبرو ودور الخبير في الجريمة المعلوماتيةذالك أن الطابع الفني الذي تتميزبه يجعل من المستحيل الاستغناء عن دور الخبير المعلوماتي، و الذي في الغالب يكون له الدور الأكبر في الوصول إلى إثبات الجرائم المعلوماتية.

04- وقد وسع المشرع في إطار الجريمة المعلوماتية من صلاحيات الضبطية القضائية و ذالك من خلال التعديلات التي أدخلها على قانون العقوبات بموجب القانون 06-22 عن طريق وإضافة أساليب خاصة للتحري كاعتراض المراسلات و تسجيل

الأصوات و التقاط الصور و التسرب مراعيا في ذالك صعوبة الوصول إلى دليل يهم التحقيق من خلال الإجراءات التقليدية وعلى الرغم من الإنتقادات الموجهة لهذه الإجراءات كونها تتم دون علم ورضا من تمت في حقهم مايجعل حياتهم الخاصة عرضة للإنتهاك إلا أننا نؤيد توجه المشرع وميله إلى تغليب المصلحة العامة و حق المجتمع في تطبيق العقاب على المصالح الفردية و حق الأشخاص في حرية حياتهم الخاصة خاصتا في ضل الضمانات التي أحاط بها المشرع اللجوء إلى هذه الإجراءات مما يجعلها لاتخرج عن إطار المشروعية.

وبناءا على ماسبق نقترح التوصيات التالية.

. الاهتمام بدور الخبرو وعمل الخبير المعلوماتي بشكل خاص و جعل اللجوء إلى الاستعانة به وجوبيا عندما يتعلق الأمر بجرائم من هذا النوع فقد يؤدي الجهل بالتعامل مع مسرح الجريمة المعلوماتي قد يؤدي إلى تدمير الدليل الرقمي أوإتلافه.

-إنشاء دورات تكوينية في المجال المعلوماتي لفائدة ضباط الشرطة و القضاة تكون ذات طبيعة مستمرة وذالك لغرض مواكبة التطور الحاصل في هذا المجل.

-فرض رقابة كافية على مسيري المقاهي الالكترونية من خلال وضع إجراءات من شأنها المساعدة على تحديد هوية مستخدم جهاز الحاسب و ساعة استخدامهإذأن الجريمة المعلوماتية قد ترتكب من أي مكان إذ أن تحديد عنوان البروتوكول ت (IP) للجهاز الذي تم من خلاله ارتكاب الجريمة عير كافي في اغلب الحالات

قائمة المراجع

قائمة المراجع

أولا :الكتب:

1. بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012.
2. تاني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية الفنية، دون طبعة، تلمسان ، الجزائر، 2018.
3. جميل عبد الباقي، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الانترنت، ورقة عمل مقدمة في الحلقة العلمية بعنوان (الانترنت والإرهاب) المنظمة من طرف جامعة نايف الأمنية.
4. زيدان زليخة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر.
5. طارق إبراهيم الدسوقي عطية، النظام القانوني لحماية المعلومات، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.
6. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
7. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، بغداد، 2012.
8. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013.
9. نجمي جمال، قانون الإجراءات الجزائية على ضوء الاجتهاد القضائي، الطبعة الثالثة، دار هومة، الجزائر، 2017.

10. هلالي عبد الإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بوداباست، دار النهضة العربية، القاهرة، 2006.

ثانيا: رسائل ومذكرات الجامعية:

1_ رسائل الدكتوراه:

1. براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون جنائي، جامعة مولود معمري، تيزي وزو، 2018.
2. تشوار الجلالي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2018/2017.
3. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016.

2_ مذكرات الماجستير:

1. بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق ، جامعة وهران، 2013.
2. ثنيان ناصر إل ثنيان، إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص سياسة جنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.
3. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

4. الصغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
5. لدغم سيكو زكريا، النظام القانوني للتسرب، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية والإدارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.

3_ **مذكرات الماستر**:

1. بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ميلة، 2014/2013.
2. قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق جامعة محند أكلي أولحاج، البويرة، 2015.

ثالثا: **المجالات**:

1. أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58.
2. إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 2، العدد 1، 2018، ص 28-40.
3. أمال فكري، إشكالية الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابر للحدود، مجلة العلوم القانونية والسياسة، المجلد 9، العدد 1، 2018، ص 630-651.

4. أومدوار رجاء، فرسة كمال، التفتيش الجزائي في البيئة الافتراضية، مجلة صوت القانون، المجلد 07، العدد 1، 2020، ص 973-999.
5. بن بادة عبد الحليم، المراقبة الالكترونية كإجراء لاستخلاص الدليل الالكتروني بين الحق في الخصوصية ومشروعية الدليل الالكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03، 2019.
6. بن بامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانون الجزائري والفرنسي، مجلة دفاتر السياسية والقانون، المجلد 11، العدد 2، 2019، ص 148-159
7. بن فوزية محمد، الدليل الجنائي الرقمي و حجيته أمام القضاء، دراسة تطبيقية، المجلة الأكاديمية للبحث القانوني، المجلد 5، العدد 1، 2014.
8. ثابت دينازاد، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد 06.
9. داعي عز الدين، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحوث القانونية، مجلد 8، العدد 3، 2017، ص 200-218.
10. رابحي عزيزة، التفتيش في نظم المعالجة الآلية للمعطيات، مجلة القانون والعلوم السياسية، المجلد 2، العدد 1، 2016، ص 392- 412.
11. راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، دراسة تطبيقية على إمارة أبو ظبي، مركز الإمارات للدراسات والبحوث الإستراتيجية، مجلة دراسات الإستراتيجية والبحوث الإستراتيجية، الإمارات العربية المتحدة، الطبعة الأولى، العدد131، 2008.

12. رحال بومدين، محل التفتيش في مجال جرائم التجارة الالكترونية وفق القانون الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 3، العدد 2، 2018، ص 165-179.

13. رضا هميسي، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، المجلد 3، العدد 2، 2012، ص 157-182

14. رويس عبد القادر، أساليب البحث والتحري وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 2، العدد 1، 2017، ص38-50.

15. زوزو زليخة، ضوابط المراقبة الالكترونية في التشريع الجزائي، مجلة الفكر، العدد 18، 2019.

16. شنة زواوي، أحكام تفتيش المساكن والأشخاص والمركبات في القانون بين النظرية والتطبيق، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07، العدد 02، 2018، ص 152-153.

17. صحراوي عبد الرزاق، التسرب ودوره في التصدي لمكافحة الجريمة المنظمة العابرة للأوطان _ الجزائر نموذجا _ ، مجلة البحوث القانونية والاقتصادية، المجلد 2، العدد 2، 2020، ص 175-184.

18. عبد الناصر محمد محمود فرغلي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الجنائية والطب الشرعي المنظم بارياني للفترة الممتدة بين 12 و14 نوفمبر 2008، ص01-45.

19. فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، المجلد 21، العدد 2، 2010، ص 238-254.

20. ليندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد 8، العدد 2، 2017، ص 488-495.
21. مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية، المجلد 11، العدد 1، 2011، ص 227-243.
22. معزيز أمينة، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة القانون والمجتمع، المجلد 3، العدد 1، 2015، ص 242-272.
23. مولاي ملياني، التفتيش في جرائم تكنولوجيا الإعلام والاتصال، مجلة القانون والعلوم السياسية، المجلد 2، العدد1، 2016، ص 291-307.
24. نديم محمد حسن الشيراوي، سلطات النيابة العامة في الجريمة المعلوماتية، مجلة الأندلس للعلوم الإنسانية، ، المجلد 15،العدد 13، 2017.
25. يزيد بوحليط، تفتيش المنظومة المعلوماتية و حجز المعطيات في التشريع الجزائري، مجلة التواصل للعلوم الإنسانية والاجتماعية، جامعة باجي مختار، المجلد 22، العدد 2، 2016، ص 82-94.

رابعا: النصوص القانونية:

1. قانون رقم 05/03 المؤرخ في 19 جمادى الأولى عام 1424 هـ الموافق لـ 19 جويلية 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ج ج، رقم 44 الصادرة بتاريخ 2003/07/19.
2. القانون رقم 04-05 المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات، ج ر ج ج، العدد 71 الصادرة بتاريخ 2004/10/10، معدل ومتمم.

3. قانون رقم 06-22 المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 156/66 يتضمن قانون الإجراءات الجزائية، ج ر ج ج، العدد 84، الصادرة بتاريخ 2006/12/24 معدل ومتمم.

4. القانون رقم 01/06 المؤرخ في 21 محرم عام 1427 الموافق لـ 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، ج ر ج ج، العدد 14 الصادرة بتاريخ 03/08/ 2006

5. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 05 غشت سنة 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج ر ج ج، رقم 47 الصادرة بتاريخ 16 أوت 2009.

6. القانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق 06 مارس سنة 2016 المتضمن التعديل الدستوري، ج ر ج ج، العدد 14، صادرة 2016.

خامسا: المواقع الالكترونية:

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 متاحة على الموقع:

Haqqi. Info/ar/haqqi/ legislation/ arab- convention- cyber.

2. اتفاقية بودابسيت لعام 2001 متوفرة على الموقع:

http:// rm. Coe.Int/budapert- convention-in- arabic

3. الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية رقم 185 لعام 2001 متاحة على الموقع

Rm. Coe.Ine/Budapest- convention- Arabic/1680739173.

4. محمد محمد الالفي، الدليل الرقمي وحجيته في الإثبات، بحث متوفر على الموقع:

http// : repository. Nauss.edu. sa

فهرس المحتويات

فهرس المحتويات:

العنوان	الصفحة
إهداء	
شكر وعرفان	
مقدمة	
الفصل الأول: إجراءات التحقيق العادية في الجرائم المعلوماتية	
المبحث الأول: التفتيش كإجراء مألوف في الجرائم المعلوماتية	08
المطلب الأول: موضوع التفتيش في البيئة الرقمية	08
الفرع الأول: مفهوم التفتيش في البيئة الرقمية ومدى قابلية مكونات الحاسب الآلي للتفتيش	08
أولا: مفهوم التفتيش في البيئة الرقمية	08
ثانيا: ومدى قابلية مكونات الحاسب الآلي للتفتيش	11
الفرع الثاني: ضوابط التفتيش في نظم الحاسب الآلي	17
أولا:الضوابط الشكلية	17
ثانيا:الضوابط الموضوعية	20
المطلب الثاني: الآثار المترتبة عن عملية التفتيش في الجرائم المعلوماتية	27
الفرع الاول: محل الحجز في الجريمة المعلوماتية	27
أولا: الاشياء المادية كمل للحجز في الجريمة المعلوماتية	28
ثانيا: المكونات المعنوية كمحل للحجز في الجريمة المعلوماتية	29
الفرع الثاني: طرق حجز الدليل المعلوماتي	32
أولا: طريقة النسخ	32
ثانيا: طريقة المنع من الوصول إلى المعلومات	34
ثالثا: طريقة التجميد	35
المبحث الثاني:الضوابط الإجرائية الأخرى المتصلة بعملية التحقيق في الجريمة	36

المعلوماتية	
المطلب الأول: المعاينة كضابط للتحقيق في الجريمة المعلوماتية	36
الفرع الأول: مفهوم المعاينة و مدى صلاحية مسرحى الجريمة المعلوماتية للمعاينة	37
أولا: مفهوم المعاينة	37
ثانيا:مدى صلاحية مسرحى الجريمة المعلوماتية للمعاينة	38
الفرع الثاني: القواعد الواجب إتباعها في معاينة الجرائم المعلوماتية	40
أولا: كيفية الانتقال إلى العالم الافتراضي للمعاينة	40
ثانيا: الخطوات الواجب مراعاتها قبل البدأ في معاينة الجرائم المعلوماتية	41
المطلب الثاني:الخبرة الفنية من متطلبات التحقيق في الجريمة المعلوماتية	42
الفرعالأول: ماهية الخبرة الفنية و متطلبات أعمالها لإثبات الجرائم المعلوماتية	43
أولا: ماهية الخبرة الفنية	43
ثانيا: متطلباتأعمالها الخبرة الفنية لإثبات الجرائم المعلوماتية	45
الفرع الثاني: القواعد التي تحكم الخبرة الفنية في الجرائم المعلوماتية	47
أولا: القواعد القانونية التي تحكم الخبرة في الجرائم المعلوماتية	47
ثانيا: القواعد الفنية التي تحكم الخبرة الفنية في الجرائم المعلوماتية	50
ثالثا: أساليب عمل الخبير	52
الفصل الثاني :الإجراءات المستحدثة للتحقيق في الجرائم المعلوماتية	
المبحث الأول:التسرب كإجراء تحقيق جديد في الجريمة المعلوماتية	56
المطلب الأول: مفهوم التسرب	56
الفرع الأول: تعريف التسرب	57
أولا: التعريف التسرب لغتا	57
ثانيا: التعريف الاصطلاحي للتسرب	57

ثالثا: التعريف القانوني للتسرب	57
الفرع الثاني: خصائص التسرب وصوره	58
أولا: خصائص التسرب	58
ثانيا: صور التسرب	61
المطلب الثاني :الضوابط التي تحكم عملية التسرب في الجرائم الالكترونية	64
الفرع الأول: الشروط الشكلية لإجراء التسرب	64
أولا: تحرير تقرير من طرف ضابط الشرطة القضائية	65
ثانيا: الإذن بمباشرة عملية التسرب	66
الفرع الثاني: الشروط الموضوعية لعملية التسرب	69
أولا: وجود حالة الضرورة	69
ثانيا: السرية	70
ثالثا: الجهة المختصة بإجراء عملية التسرب	72
المبحث الثاني :الإجراءات الأخرى المستحدثة للتحقيق في الجرائم المعلوماتية	73
المطلب الأول :اعتراض المرسلات والمراقبة الالكترونية للتحقيق في الجريمة المعلوماتية	74
الفرع الأول: مفهوم الاعتراض والمراقبة الالكترونية	74
أولا: بيان طبيعة الاتصالات الالكترونية المطلوب مراقبتها	75
ثانيا: تسبيب الإذن باللجوء إلى اعتراض ومراقبة المراسلات	76
ثالثا: نوع الجريمة التي اقتضت ضرورة التحري والتحقيق القضائي	77
الفرع الثاني: الضمانات الواردة على عملية الاعتراض والمراقبة الالكترونية	78
أولا: قيد اللجوء الإذن المسبق من السلطة القضائية المختصة	78
ثانيا: العناصر الواجب توفرها في الإذن	79
المطلب الثاني:الحفظ والإفشاء العاجلان للمعطيات الالكترونية	83

الفرع الأول: مفهوم الحفظ العاجل للمعطيات المتعلقة بالسير	83
أولا: المقصود بالحفظ العاجل للمعطيات المتعلقة بالسير	83
ثانيا: ضمانات المشتبه فيه أثناء عملية حفظ المعطيات	86
الفرع الثاني: الإفشاء العاجل لمعطيات السير	88
خاتمة	91
قائمة المراجع	95
فهرس المحتويات	103