التفتيش في جرائم تكنولوجيات الإعلام والاتصال .

أة: مولاي ملياني دلال
أستاذة مساعدة صنف أ
جامعة الدكتور مولاي الطاهر سعيدة

ملخص

يعتبر التفتيش عن بعد في البيئة الافتراضية، مسرح جرائم تكنولوجيات الإعلام والاتصال،من بين الإجراءات التي تمنها المشرع الجزائري بسنه القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،ولما كان هذا الإجراء يمس بالحياة الخاصة للفرد وضعت له عدة شروط لمباشرته سواء في الدستور الجزائري أو قانون الإجراءات الجزائية،هذه الشروط ترفع ويحد منها إذا تعلق الأمر بالجرائم الخاصة ،وهو الحال بالنسبة لجرائم تكنولوجيات الإعلام والاتصال باعتبارها جرائم مستحدثة ذات طابع خاص.

Resume

The distance inspection in the virtual environment (the scene of information and communication technologies crimes) is among procedures that have been valuable by the Algerian legislature through enacting the 09-04 law, which contains special regulation for the prevention of crimes related to information and communication technologies. Since this procedure touches the private life of individual, several conditions were established to execute it, whether in the Algerian Constitution or the Code of Criminal procedures, those conditions can be removed or limited in the case of special crimes, which is the case with information and communication technologies crimes, as they are considered as an innovative crimes with special character.

المقدمة

"تشمل تقنية المعلومات فرعين الحوسبة والاتصال، أما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق،أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدراجة(الرسائل والأخبار والبيانات والمعرفة والوثائق والأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية)"[1]

ومع التطور الحاصل في تقنية المعلومات ،واجه المشرع الجزائري السلوكيات غير المشروعة الدائرة في مجالها بالقانون رقم 04-15[2] ثم القانون الخاص رقم 09-04[3]، بإدراج جرائم المعالجة الآلية للمعطيات ضمن جرائم تكنولوجيات الإعلام والاتصال ،هي"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[4]، كما ثمن بعض الإجراءات التي تتناسب مع هذا النوع من الجرائم على رأسها التفتيش، واقر صلاحية المنظومة المعلوماتية وبالتالي المعطيات المعالجة أليا للتفتيش، باعتبار مسرح الجرائم هو البيئة الافتراضية اللامادية،وباعتبار التفتيش من الإجراءات القسرية التي تمس الشخص سواء التفتيش الجسماني أو كل ما تعلق بالشخص وحياته الخاصة كالمسكن، تدخل معظم المشرعين لحماية الحياة الخاصة من كل انتهاك ،لان الفكرة الأساسية في التفتيش تكمن في إباحة انتهاك الحق في الخصوصية طالما هناك مبرر في القانون لهذا الانتهاك[5]، التفتيش هو البحث في مستودع السر عن اشياء تفيد في الكشف عن جريمة وقعت ونسبتها الى مرتكبيها [6]، هو " إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة " وعرفه البعض الآخر بأنه " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون " [7].

فمن خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة

المادية الملموسة، من هنا ذهب جانب من الفقه إلى القول بأنه إذا كانت الجريمة واقعة على المكونات المادية للنظام المعلوماتي[8] فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة على البرمجيات والتطبيقات وبيانات النظام المعلوماتي وشبكاته، فإن الصعوبات تبرز، والتي تستلزم أن يقع التفتيش على المكونات المادية والمعنوية للنظام المعلوماتي والشبكات، لضبط أدلتها وبالتالي إدانة مرتكبها، فإن المشرع الجزائري قد ساير تطور هذه الجريمة المستحدثة وذلك عندما نص على إجراءات التفتيش التي تتناسب وطبيعتها وذلك في القانون رقم 09 -04 السالف الذكر [9]، من كل ما سبق ما هي شروط التفتيش في جرائم تكنولوجيات الاعلام والاتصال، وهل أحيط الإجراء بضمانات كافية للحفاظ على حرمة الحياة الخاصة، اشكالية حاولنا الاجابة عليها من خلال مطلبين

المطلب الاول: نطاق تفتيش مكونات النظام ألمعلوماتي في جرائم تكنولوجيات الاعلام والاتصال

يتكون النظام ألمعلوماتي من مكونات مادية وغير مادية أي معنوية ،بالإضافة إلى الشبكات المحلية والإقليمية والدولية التي تكون محل للتفتيش من اجل الحصول عل الدليل الجنائي الالكتروني[10] وهو المعلومات المخزنة في الأجهزة الحاسوب ولواحقها وغيرها من الوسائل التقنية الأخرى وكذا شبكات الاتصال والتي يتم تجميعها باستخدام برامج وتطبيقات وتكنولوجيات خاصة بهدف إثبات وقوع الجريمة ونسبتها الى مرتكبها[11].

الفرع الأول : تفتيش مكونات النظام المعلوماتي المادية والمعنوية

يتكون النظام المعلوماتي من مكونات مادية وغير مادية أي معنوية، فبالنسبة للنوع الأول من هذه المكونات يمكن القول بأنها جميع المكونات المادية الملموسة، اللازمة لعمله وإشتغاله بوجه يحقق وظيفته ويؤدي الغرض المطلوب منه، ومن حيث الأصل يؤدي نظام المعالجة الآلية ثلاثة عمليات رئيسية هي الإدخال، المعالجة والتخزين، والإخراج، وتبعا لهذه العمليات تنقسم أجزاء نظام المعالجة الآلية إلى ثلاث أقسام رئيسية[12]، أما بالنسبة للنوع الثاني من مكونات النظام المعلوماتي أو نظام المعالجة الآلية، فهي تلك

المكونات الغير المادية أو كما يصطلح على تسميتها بالبرامج أو البرمجيات أو الكيان المنطقي والتي تعرف على أنها مجموعة البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات وبهذا يشمل الكيان المنطقي على جميع العناصر الغير المادية اللازمة لتشغيل الكيان المادي[13]، والواقع ان تفتيش النوع الأول من المكونات المادية لنظام المعلوماتي لا يثير أي مشكلات تعيق القيام به، مثلها مثل أي مكونات مادية أخرى يتم تفتيشها بالطرق العادية وبموجب النصوص الإجرائية العادية، بخلاف النوع الثاني الذي يثير تفتيشه مشكلات نظرا لطبيعتها المنطقية وكذلك طبيعة إجراءات التفتيش التي هي من نفس الطبيعة المعنوية [14].

<u>اولا : تفتيش مكونات النظام المعلوماتي المادية:</u> ليس هناك خلاف حول تفتيش المكونات المادية للنظام المعلوماتي بحثا عن شيء يتصل بجريمة وقعت، يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش،بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، هل هو من الأماكن العامة أو من الأماكن الخاصة؟ حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم وأحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا،أما لو وجد شخص يحمل مكونات الكمبيوتر المادية أو كان مسيطرا عليها أو حائز لها في مكان ما من الأماكن العامة سواء كانت بطبيعتها أو كانت عامة بالتخصيص فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال [15].

فالتشريع الإجرائي الجزائري، يتضمن نصوص قانونية تنطبق من حيث الأصل على تفتيش المكونات المادية للنظام المعلوماتي بهدف كشف الجريمة وتجميع الأدلة، وبناءً على ما سبق فإن تفتيش االمكونات المادية للمنظومة المعلوماتية مثل لوحة المفاتيح أو الفأرة أو الشاشة وغيرها من الأشياء المادية الملموسة وكذلك البصمات الموجودة عليها لا تدخل ضمن المشاكل الإجرائية التي تعيق إجراء التفتيش إذ بالإمكان تطبيق النصوص العادية وبهذا فإن أجهزة الكمبيوتر التي يراد تفتيشها تخضع للقواعد التي تخضع لها الأدوات المادية الأخرى، فإن كانت في مسكن فإنه ينطبق عليها ما ينطبق على تفتيش المساكن

والتي من بينها مراعاة وقت التفتيش والإذن بالتفتيش والأشخاص القائمين على التفتيش والأشخاص المطلوب حضورهم ومراعاة الإختصاص المكاني[16]، ومن النصوص القانونية التي يمكن تطبيقها في هذا المجال نص المادة 64 ق إ ج والمواد 37و40 و42 ومن المواد44 إلى 47ق إ ج[17].

ثانيا : تفتيش مكونات النظام المعلوماتي المعنوية: قد يرد التفتيش على المكونات النظام المعلوماتي المتمثل في المعلومات المعالجة اليا، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات الذي يعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الإعتداء على نظم المعالجة الآلية[18]، مثل الدخول الغير المشروع إلى نظم الغير، فوجود برمجيات غير مصنفة تعمل في بيئة الإختراق أو تساعد عليه كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة يمكن أن يشكل منطقة إستفهام ودلالة كافية أيضا على إرتكاب الشخص لجريمة الدخول الغير المشروع لنظام المعالجة الآلية إذا إستتبع ذلك إعترافا[19] شفويا بإرتكاب الجريمة ،ومن هنا فإن التفتيش في مكونات النظام المعلوماتي المعنوية، يشكل إحدى أهم المشاكل التي تعيق إجراءات التحقيق، حيث أثارت هذه الصورة خلافا كبيرا في الفقه المقارن لأن هذا النوع من التفتيش ينصب على بيانات وبرامج النظام المعلوماتي التي تغيب فيها الطبيعة المادية فليس لها أي أثر مادي محسوس في العالم الخارجي [20].

فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء"،[21] فإن ذلك يجب تفسيره بحيث يشمل بيانات المعالجة اليا.

بينما ذهب رأي آخر إلى عدم إنطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير ملموسة ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أحكام خاصة تكون أكثر ملائمة لهذه المعلومات اللامحسوسة [22].

وهذا ما تبناه المشرع الجزائري حيث أنه وإستجابة لهذه التغيرات أجاز تفتيش المعطيات المعلوماتية وذلك بموجب المادة 05 من القانون رقم 09 -04 السالف الذكر، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من نفس القانون،

التي من بينها توافر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الإقتصاد الوطني وللوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية [23].

الفرع الثاني : تفتيش المنظومة المعلوماتية عن بعد في جرائم تكنولوجيات الاعلام والاتصال.

بالإضافة إلى كون تفتيش النظام المعلوماتي تعد من الإشكاليات التي تعيق سير التحقيق فإن تفتيش شبكات النظام المعلوماتي تثير مشكلة قد تكون أشد خطورة من تفتيش النظام المعلوماتي ذاته حينما يكون مرتبط بشبكة إتصال، وتثار هذه المشكلة عندما يتعلق الأمر بنهاية طرفية موجودة في منزل المتهم ومتصلة بجهاز يقع خارج منزل المتهم في نفس الدولة ومملوك لغير المتهم، كما تثار الإشكالية بصورة أكبر عندما يكون النظام المراد تفتيشه واقعا خارج الدولة وتعد شبكة الإنترنت هي الشبكة الأهم التي تشكل عائقا في مجال التفتيش الجنائي من بين الشبكات المختلفة بسبب الانتشار الواسع لها والعدد الهائل من البشر الذين يستخدمونها والخدمات التي تقدمها في مجال الحياة المختلفة والكم الهائل من البيانات والمواقع التي تتضمنها[24]، لذلك فان التفتيش في نطاق جرائم تكنولوجيات الاعلام والاتصال لا يخرج عن احدى الفرضيتن

اولا : <u>حالة جهاز متصل بجهاز المتهم داخل الدولة</u> : تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم ويقع داخل الدولة وتكمن المشكلة في تجاوز الإختصاص المكاني لسلطة التحقيق من ناحية والإعتداء على خصوصيات الغير من ناحية أخرى .

وقد عالجت بعض التشريعات هذه المسألة حيث نصت على إمكانية إمتداد تفتيش المسكن إلى تفتيش نظام آلي موجود في مكان آخر ، بغرض التوصل إلى بيانات تفيد في كشف الحقيقة وبالتالي يجوز للقائم بالتفتيش أن يسجل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق من قاضي التحقيق ،وبالنسبة للتشريع الجزائري فقد تضمن نصوص قانونية إجرائية ضمن

قانون الإجراءات الجزائية وسعت بعض الصلاحيات التي يمكن القيام بها من قبل سلطة التحقيق[25]، ومن ذلك إمكانية قيام قاضي التحقيق بالتفتيش أو الحجز في أي وقت وفي أي مكان على إمتداد كامل التراب الوطني أو يأمر ضابط الشرطة القضائية المختص للقيام بذلك وبالتالي القيام بإجراءات التحقيق في مجال الجرائم المعلوماتية التي تعتبر من جرائم تكنولوجيات الاعلام والاتصال في أي مكان داخل الإقليم الوطني للدولة .

ونظرا لوجود قصور في نصوص قانون الإجراءات الجزائية في تعديله الأخير لسنة 2006، حيث لم يتضمن التفتيش عن بعد للكيانات المنطقية في نظام المعالجة الآلية للبيانات[26]، فقد تلافى ذلك القصور بأن سمح للسلطات القضائية المختصة لمقتضيات التحريات والتحقيقات القضائية تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني وهذا ما نصت عليه الفقرة الثانية من المادة 05 من القانون رقم 09 – 04 السالف الذكر،وما يدخل ضمن نطاق حالة الاستعجال في تمديد الاختصاص خوفا من العبث بالأدلة الرقمية، والمنصوص عليه في المادة 19 من الاتفاقية الأوروبية للإجرام السيبيري المستقى منها القانون 09-04.

ثانيا : <u>حالة جهاز متصل بجهاز المتهم خارج الدولة</u>: في هذه الحالة فإن الإشكالية تثار بصورة أكبر، في حالة أن يكون الجهاز المطلوب تفتيشه والمتصل بجهاز المتهم بنهاية طرفية يقع خارج الدولة، ففي الغالب يعّمد مرتكبي جرائم تكنولوجيات الإعلام والاتصال إلى تخزين البيانات الخاصة بهم والتي تعد أدلة لإدانتهم في جرائم تم ارتكابها من قبلهم خارج الدولة اي قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة ،عن طريق شبكة الاتصالات البعدية بهدف عرقلة التحقيقات[27]

والتفتيش عن بعد أصبح مشكلة تواجه النظام الإجرائي ككل، حيث يتم إجراؤه من خلال الحاسوب ذاته وتزداد خطورة الأمر حينما يتم استخدام برامج تمتلكها دول معينة متقدمة في مجال التكنولوجيا الرقمية، للتفتيش على أنظمة دول أخرى، لكونه لا يستند إلى مبرر قانوني ويشكل اعتداء على الخصوصية، فضلا عن كونه يجعل الدولة عرضة للاعتداء في إطار جريمة التجسس عليها أي المساس بأمن الدولة.

وبالنسبة للقانون الجزائري فقد تلافى مشكلة التفتيش عن بعد خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة 5 من القانون رقم 09 – 04 السالف الذكر التي نصت

على أنه " إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل"، فبخصوص هذه الفقرة قيل بأنه لا يمكن تفتيش تلك المنظومة وإنما يجب الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ، فبالرغم من إمكانية تفتيشها من الناحية التقنية داخل النطاق الإقليمي إلا أن ذلك لا يتم إلا بعد موافقة الطرف الأجنبي لانه أمر متعلق بسيادة الدول على أراضيها وهذا يؤكد على أهمية التعاون الدولي في نطاق مكافحة جرائم تكنولوجيات الإعلام والاتصال والذي جسدة المشرع الجزائري من خلال المادة 21 من القانون 09-04، وبالعودة إلى الاتفاقية الأوربية الموقعة في بودابست وبالضبط في المادة 32 منها اجازت الولوج بغرض التفتيش والضبط في أجهزة موجودة خارج الحدود الإقليمية لدولة أخرى بدون إذن في حالة ان تكون البيانات متاحة للجمهور، اوحالة الرضا بالتفتيش من حائز البيانات ايا كان سواء المستخدم العادي أو مقدمي الخدمة.[28]وهو أمر فيه نظر ونسجل في صدده تحفظ شديد لما فيه من اعتداء على سيادة الدولة قبل الاعتداء على خصوصيات الأفراد.

وحتى لا يصبح اجراء التفتيش تحت طائلة البطلان،لابد من أن يستوفي مجموعة من الشروط الموضوعية والشكلية التي تعتبر ضمانات حماية الحق في الحياة الخاصة[29].

المطلب الثاني: شروط التفتيش في جرائم تكنولوجيات الاعلام والاتصال.

يتضح مما سبق ان جرائم تكنولوجيات الاعلام والاتصال يمكن أن تخضع لإجراء التفتيش طبقا للقواعد العادية أو المستحدثة، هذا الإجراء الذي وجد أثناء مباشرته أنه يتضمن تقييد للحرية الفردية وإعتداء على حرمة الحياة الخاصة[30]، لهذا نجد أن القوانين الإجرائية قد حرصت على إحاطة إجراء التفتيش بشروط وضمانات أساسية وهدف ذلك تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم، ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي .

الفرع الاول: الشروط الموضوعية للتفتيش في جرائم تكنولوجيات الاعلام والاتصال

تتمثل الشروط الموضوعية التي يلزم تحققها لإجراء التفتيش في سبب التفتيش الذي يتمثل في وقوع الجريمة، ونسبة إرتكابها إلى متهم إضافة إلى ضرورة أن ينصب التفتيش على محل يحتمل العثور فيه على أدلة الجريمة وأخيرا يفترض لكي يكون التفتيش صحيحا أن يكون له غاية تتمثل في أن يكون التفتيش بغرض العثور على الآثار والأشياء التي يمكن أن تفيد في كشف الجريمة .

أولا : وجود سبب لتفتيش النظام المعلوماتي: الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة واقعة بالفعل، وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية[31]، وذلك عملا بقاعدة المشروعية" لا جريمة إلا بنص" وبالتالي لا يجوز التفتيش من أجل فعل لا يشكل جريمة وفي حالة عدم توافر الدلائل الكافية بإقترافها ونسبتها إلى شخص أو أشخاص، فسبب التفتيش بحثا عن أدلة الجريمة يعد ضمانة بالنسبة للجرائم المنصوص عليها في القوانين إذ بدون السّبب المتمثل في الجريمة،سواء كانت جناية او جنحة دون المخالفة، وبدون توجيه الإتهام لشخص أو أشخاص محددين فإن القيام بالتفتيش يعد إجراءً باطلا، ولا يكفي لقيام سبب التفتيش، وقوع جريمة منصوص عليها في القانون كجرائم تكنولوجيات الاعلام والاتصال التي تناولها المشرع الجزائري بنصوص قانونية تضفي وصف التجريم على الأفعال المكونة لها، بل لا بد من توافر أمارات قوية على وجود أشياء تفيد في كشف هذه الجريمة، عند وجود اجهزة ومعدات معلوماتية ويمكن ان تعد قرائن وإمارات قوية تدل على أنها استعملت في ارتكاب الجريمة المعلوماتية[32]، وبالتالي توجيه الاتهام الى شخص معين او عدة اشخاص بارتكاب جريمة من جرائم تكنولوجيات الاعلام والاتصال او الاشتراك فيها.

ثانيا : المحل و الغاية من التفتيش: يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سّره والسّر الذي يحميه القانون هو ذلك الذي

يستودع في محل له حرمة [33] ، ومحل التفتيش قد يكون منزلا وقد يكون شخصا وقد يكون محله رسائل[34].

هذا ومحل التفتيش في إطار جرائم تكنولوجيات الاعلام والاتصال هو نظام المعالجة بكل مكوناته المادية والمعنوية، وشبكات الإتصال كما سبق بيانه وفي هذا المجال لا داعي لتكرار مدى قابلية هذه المكونات المادية والمعنوية فضلا عن شبكات الإتصال للتفتيش،كما انه ونظرا لخطورة إجراء التفتيش على الحياة الخاصة للأفراد بإعتباره إجراء من إجراءات التحقيق فلا بد أن يكون له غاية إذ بدونها، وكذلك في حالة تجاوزها فإن الإجراء سيكون باطلا وبهذا الخصوص نصت المادة 81 ق إ ج على أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، وفي تكنولوجيات الاعلام والاتصال بصفة عامة نجد أن المشرع الجزائري وبخصوص الغرض من التفتيش قد أحال تفصيل ذلك إلى قواعد قانون الإجراءات الجزائية حيث نص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة الرابعة أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية. " [35].

وبالتالي فإنه إذا تحققت الغاية من التفتيش وفقا لنصوص قانون الإجراءات الجزائية فيحق للسلطات المختصة بالتحقيق الدخول إلى النظام المعلوماتي أو جزء منه سواء تعلق الامر بالمستخدم او مزود خدمة الانترنت سواء لتوصيل الخدمة او تقديم خدة الايواء، بغرض التفتيش على ذلك النظام أو المعطيات المخزنة به، كما يجوز الدخول إلى نظام معلوماتي آخر داخل الإقليم الوطني أيضا بغرض التفتيش إذا ما تحققت الغاية منه وذلك في حالة وجود أسباب تدعو للإعتقاد بأن المعطيات محل البحث مخزنة في ذلك النظام [36].

ثالثا: السلطات المختصة في التفتيش في جرائم تكنولوجيات الاعلام والاتصال: هذا وقد كلفت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

حصريا بالقيام بإجراءات التفتيش داخل منظومة معلوماتية تحت سلطة قاضي مختص وهذا وفق المادة 21 من المرسوم الرئاسي رقم 15-261[37]، على أن هذا الإجراء أي التفتيش وإجراء مراقبة الاتصالات الالكترونية هي مهام منوطة بهذه الهيئة لاغير،وهذا في إطار الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة،تحت طائلة العقوبات بالنسبة للمساس بالحياة الخاصة للغير،وهو مانصت عليه المادة 04 من القانون 09-04 سالف الذكر،كما يمكن القضاة وضباط الشرطة القضائية التابعون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز واو يستعمل وسائل وتجهيزات موجة لمراقبة الاتصالات الالكترونية وهذا وفق المادة 30 من المرسوم السالف الذكر

الفرع الثاني : الشروط الشكلية للتفتيش في جرائم تكنولوجيات الاعلام والاتصال .

بالإضافة إلى الشروط الموضوعية للتفتيش، توجد شروط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء وذلك صونا للحريات الفردية من التعسف أو الإنحراف في إستخدام السلطة[38]،

أولا : ميقات التفتيش: تذهب أغلب التشريعات الجزائية إلى تحديد وقت معين يتم فيه إجراء التفتيش، وذلك حرصا منها على تضيق نطاق الإعتداء على الحرية الفردية وحرمة المسكن، حيث ذهب المشرع الجزائري، إلى حظر تفتيش المنازل وما في حكمها في وقت معين فنجد ميقات التفتيش في التشريع الجزائري قد حدد من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وذلك من خلال المادة 47 ق إ ج، وبذلك نجد أن هذه النصوص قد هدفت إلى حماية حرمة الأفراد ليلا، حيث يعد المسكن ملجأ حصين لهم، لا يجوز إنتهاكه ليلا حفاظا على خصوصياتهم .

ومع أن إشتراط تفتيش المنازل بوقت معين يعد ضمانة للمحافظة على خصوصيات الآخرين، فإن ذلك الشرط لا يؤخذ به على إطلاقه، حيث ورد العديد من الإستثناءات على تلك القاعدة تضمنت الخروج على الميقات الزمني في التفتيش بالنسبة لبعض الجرائم وكذلك في بعض الحالات مثل حالة الضرورة، من ذلك وفي نطاق التفتيش المتعلق بجرائم تكنولوجيات الاعلام والاتصال، فإن الإستثناء الوارد بالمادة 47 / 3 ق إ ج

والمتعلق بجواز إجراء ضابط الشرطة القضائية التفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم، والتي شملت الجرائم المعلوماتية، ذلك أن تطبيق القيد السابق على هذا النوع من الجرائم، قد يكون سببا في إخفاء الأدلة ومن ثمت عرقلة سير التحقيق لكون أدلة هذه الجرائم هي عبارة عن كيانات غير مادية يمكن إخفاء أدلتها بسرعة غير متوقعة،إذا علم الجاني مسبقا بالوقت الذي سيتم تفتيش أنظمته فيه [39].

ثانيا : الأشخاص المطلوب حضورهم للتفتيش: يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم العادية وذلك لضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط [40]، حيث ذهب أغلب الفقهاء إلى ضرورة حضور المتهم التفتيش معتبرين ذلك من القواعد الأساسية التي يترتب على مخالفتها البطلان وقد نص المشرع الجزائري على هذا الضمان في المادة 45 و 83 ق إ ج.

وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى عدم التعسف في استخدامها، إلا أنها قد تتحول إلى مشكلات تحول دون الوصول إلى النتائج المتوقعة من إجراء التفتيش في حالة أن يكون التفتيش يخص إحدى جرائم تكنولوجيات الإعلام والاتصال، بسبب أن إشعار الأشخاص المطلوب حضورهم قد يتيح لهم التلاعب بالمعطيات والبرامج والتطبيقات المراد تفتيشها، وبالتالي إخفاء أدلة الجرائم أو التلاعب بها ومن ثم صعوبة التوصل إلى مرتكبها، فقد يتم التلاعب بالأدلة وإخفاءها عن بعد في الوقت ما بين إجراءات إصدار الإذن بالتفتيش وموافقة المتهم بأن يتم التفتيش بحضوره، وعليه فقد تنبه المشرع الجزائري لمثل هذا الإجراء فلم يشترط في تفتيش عدد من الجرائم حضور المتهم أو صاحب المنزل المراد تفتيشه أو الشهود ومن تلك الجرائم، الجرائم الماسة بأنظمة المعالجة الآلية، وجرائم المرتبطة بتكنولوجيات الاعلام والاتصال [41].

ثالثا :محضر التفتيش: وباعتبار التفتيش عمل من أعمال التحقيق، فإنه ينبغي تحرير محضر يدرج فيه كل ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة اثبات، بحيث يتطلب القانون شكلا خاصا لهذا المحضر، وتنطبق عليه شروط صحة ما تستوجبه القواعد العامة في المحاضر وفق قانون الإجراءات الجزائية، كأن يكون مكتوبا باللغة

الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره، وأن يحوي في طياته كافة الإجراءات التي أتخذها بشأن الوقائع التي احتواها، حيث نصت المادة 68 / 2 ق إ ج ج " وتحرر نسخة من هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل " ، كما نصت المادة 79 ق إ ج ج على أنه "... ويستعين قاضي التحقيق دائما بكاتب ويحرر محضرا بما يقوم به من إجراءات "

بالإضافة إلى ما سبق ذكره من إحاطة قاضي التحقيق أو عضو النيابة العامة بتقنية المعلومات، ومن جهة أخرى لا بد أن يرافقه عون متخصص في المعلوماتية والشبكات للاستعانة به في المشاكل التقنية التي تواجهه، فوجود خبير سوف يساعد السلطات المختصة في تحرير محضر التحقيق بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش [42] الرقمي.

الخاتمة

إن الحديث عن التفتيش في جرائم تكنولوجيات الإعلام والاتصال، لا يكتمل إلا بالتعرض لإجراء الضبط أو حجز المعطيات المعلوماتية أي اثر التفتيش، باعتباره الوسيلة التي من خلالها يتم الوصول إلى الأدلة التي تثبت الحقيقة التي تبحث عنها الدعوى الجزائية، وهذا ما سيتم التطرق له في المقالات اللاحقة إن شاء الله،ونحن لا ننكر التطور الحاصل في المنظومة التشريعية خصوصا ماتعلق بالتكنولوجيات الحديثة من تمديد في الاختصاص الإقليمي وإدراج المعطيات المعلوماتية ضمن الاشياء التي هي قابلة للحجز، ولكن لابد علينا من إبداء بعض الملاحظات وإدراج بالمقابل توصيات، بذلك أن المشرع الجزائري لم يفصل في الجرائم الخاصة بتكنولوجيات الإعلام والاتصال مما يتناقض ومبدأ التفسير الضيق للنص الجنائي، فاقتصر على ذكر الجرائم العادية التي تقع عبر الانترنت كجرائم الإرهاب دون باقي الجرائم الأخرى، كما انه لم يدرج أهم إجراء خول للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 04 من المرسوم سالف الذكر الا وهو التفتيش، بالمقابل لم يدرج المشرع ضمانات كافية لحماية الحق في الحياة الخاصة أثناء التفتيش خصوصا في باقي جرائم المتعلقة بتكنولوجيات الإعلام والاتصال ماعدا ماتعلق منها بالجرائم الإرهابية وامن الدولة، وبالتالي فالباحثة توصي بضرورة وضع آلية تشريعية لتحديد ماهية جرائم تكنولوجيات

الإعلام والاتصال باعتماد النشاط التقني ركنا مفترضا في هذا النوع من الجرائم، وإدراج إجراء التفتيش ضمن المادة الرابعة من المرسوم سالف الذكر، وإيجاد ضمانات مناسبة للتفتيش في البيئة الافتراضية باعتبارها تختلف عن البيئة العادية، وبالتالي إقامة نوع من الموازنة بين الإجراءات وحقوق وحريات الإنسان.

الهوامش

1. فهد عبد الله العبيد العازمي،الإجراءات الجنائية المعلوماتية ،دكتوراه في الحقوق،كلية الحقوق ،جامعة عين شمس،القاهرة،2012،ص 35.
2. القانون 04-15 المؤرخ في 10نوفمبر 2004 ،يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 جويلية 1966،المتضمن قانون العقوبات،ج ر 71يوم 10 نوفمبر 2004.
3. القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 14 غشت عام 1430 الموافق 05غشت سنة 2009– الجريدة الرسمية عدد 47 ل 16غشت 2009 ص 05.
4. المادة الثانية من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ص05
5. سامح احمد البلتاجي موسى،الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت،رسالة دكتوراه ،جامعة الإسكندرية، مصر 2010،ص 239.
6. مأمون سلامة ،قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام القضاء ،مكتبة رجال القضاء ،1980،ص 244.
7. خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، 2009 ، ص. 182 .
8. المنظومة المعلوماتية: أي نظام منفصل او مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرامج معينة

9. فايز محمد راجح غلاب فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني ، رسالة دكتوراه ، قسم الحقوق جامعة الجزائر ، 2009 – 2010 ، ص307 .
10. المادة من16 القانون 09-04
11. عائشة بن قارة مصطفى، حجية الدليل الجنائي الالكتروني في مجال الإثبات الجنائي،في القانون الجزائري والقانون المقارن،دار الجامعة الجديدة ،الإسكندرية، مصر 2010، ص61
12. وحدات الإدخال : وهي مجموعة الوحدات المسؤولة عن إيصال البيانات للحاسوب فتقوم باستقبال البيانات المدخلة إلى الحاسوب وتمريرها داخل الجهاز إلى وحدة الذاكرة للتخزين ، ومن أجهزة الإدخال لوحة المفاتيح ، الفأرة ، مشغل الأقراص .
وحدة المعالجة المركزية : وتعتبر بمثابة العقل المفكر والمسيطر على باقي الوحدات المكونة لنظام المعالجة الآلية بحيث تعمل هذه الوحدة على تنفيذ جميع العمليات الخاصة بالتشغيل وعمليات المقارنة المنطقية والعمليات الحسابية الموجودة في البرنامج تنفيذه من وإلى الوحدات المساعدة مع ضمان تحرك المعلومات من وإلى الذاكرة الرئيسية ، ومن أهم مكونات هذه الوحدة الذاكرة ووحدة الحساب والمنطق ووحدة التحكم .
وحدة الإخراج : وهي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات ومن أهم هذه الوسائل الشاشة والطابعة.انظر رشيدة بوكر ،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارنة، الطبعة الأولى ، منشورات حلبي الحقوقية، لبنان 2012 ، ص. 58
13. جبار الحسناوي ، جرائم الحاسوب علي والأنترنت ، الطبعة العربية ، دار اليازوري العلمية للنشر والتوزيع ، عمان ، 2009 ، ص. 25 .
14. فايز محمد راجح غلاب ، المرجع السابق ، ص. 307 .
15. خالد ممدوح إبراهيم ، ، المرجع السابق ، ص. 195 ، 196 .
16. فايز محمد راجح غلاب ، المرجع السابق ، ص. 309 .

17. المادة 64 والمواد من 44 إلى 47 من القانون رقم 06 – 22 ، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمور رقم 66 – 155 – ج ر ، العدد 84 ، الصادرة في 24 ديسمبر 2006، ص. 16.
18. رشيدة بوكر ، المرجع السابق ، ص. 397
19. الاعتراف وشهادة الشهود والخبرة هي من دعائم الاثبات الجنائي في جرائم تكنولوجيات الاعلام والاتصال.
20. فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 311 .
21. انظر في ذلك عائشة بن قارة مصطفى،المرجع السابق،ص.91
22. خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع السابق، ص. 197.
23. رشيدة بوكر، المرجع السابق، ص. 348، 349
24. فايز محمد راجح غلاب، المرجع السابق، ص. 312 .
25. يجوز تمديد الاختصاص الملي في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب المادة 40 من قانون الإجراءات الجزائية
26. فايز محمد راجح غلاب، المرجع السابق، ص. 314 .
27. فايز محمد راجح غلاب، المرجع السابق، ص. 314 .
28.
29. حيث يمكن تعريف الحق في الحياة الخاصة بأنه حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي ،انظر في ذلك عبد الله فكري،جرائم نظم المعلومات، دراسة مقارنة ،دار الجامعية للنشر ،مصر،2007،ص613
30. رشيدة بوكر، المرجع السابق، ص. 405 .
31. خالد ممدوح إبراهيم ،المرجع السابق ، ص. 209 .
32. فهد عبد الله عبيد العازمي، المرجع السابق ،ص.
33. رشيدة بوكر، المرجع السابق، ص. 408 .
34. فايز محمد راجح غلاب، المرجع السابق نفسه ، ص. 321 ..

35. المادة 05 من القانون 09 – 04 السالف الذكر
36. فايز محمد راجح غلاب ، المرجع السابق ، ص. 327 .
37. مرسوم الرئاسي رقم 15-261 مؤرخ في 24ذي الحجة عام 1436 الموافق 8 اكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ج ر 53 ص 21.
38. خالد ممدوح إبراهيم، المرجع السابق ، ص. 220 .
39. فايز محمد راجح غلاب ، المرجع السابق ، ص. 329 – 330 .
40. رشيدة بوكر، المرجع السابق، ص. 413
41. فايز محمد راجح غلاب، المرجع السابق، ص. 337 .
42. خالد ممدوح إبراهيم، المرجع السابق، ص. 225 عائشة بن قارة مصطفى، المرجع السابق،ص 113.