القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري

The procedural rules established for inspecting the information system in Algerian law

ط/د: حمداش شمس الدين، جامعة المنار تونس،

maitre.hamadache4@gmail.com

تاريخ الإرسال: 2021/05/19 *تاريخ القبول: 2022/03/13* *تاريخ النشر: 2023/05/31*

ملخص:

تهدف هذه الورقة البحثية الى تسليط الضوء على اجراء تفتيش المنظومة المعلوماتية كصورة من صور اجراءات البحث والتحري في الجريمة الالكترونية، حيث نجد ان تفتيش المنظومة المعلوماتية بغرض استنباط الدليل اثبات الجريمة الالكترونية يجب ان يحترم فيه ضوابط وشروط معينة، وذلك نظرا لكونه يرد على جهاز الكومبيوتر وملحقاته، فهذا التفتيش له خصوصيات معينة، لكونه يدخل في إطار مكافحة الجريمة الالكترونية المستحدثة التي تملك ميزات تختلف عن الجرائم التقليدية.

كلمات مفتاحية: الجريمة الالكترونية-التفتيش-الجرائم المستحدثة-البحث والتحري

Abstract:

This research paper aims to highlight the conduct of inspection of the information system as a picture of the procedures for research and investigation of cybercrime, where we find that the inspection of the information system in order to devise evidence to prove electronic crime must respect certain controls and conditions, because it responds to the computer and its accessories, this inspection has certain

peculiarities, because it falls within the framework of the fight against new electronic crime, which has features different from traditional crimes.

Key words: cybercrime- new crimes -search and investigation

المؤلف المرسل: حمداش شمس الدين، maitre.hamadache4@gmail.com

مقدمة

شهد العالم ثورة مذهلة في مجال التكنولوجيا والاتصالات وتقنية المعلومات، وهذه الثورة التقنية كان من أهم أوجه انتفاضتها، التقدم المذهل في مجال الحواسيب الآلية، والبرامج التي تلحق بها، كما بات الاعتماد على هذه التكنولوجيا واضحا جليا في كل الجهات الرسمية وغير الرسمية، حتى بات العنصر البشري يشكو من إحلال الأجهزة الذكية من حواسيب وبرامج محل الجهد البشري، حتى حل الذكاء الاصطناعي محل الذكاء البشري.

وعلى الرغم من أن هذه التكنولوجيا هي صناعة بشرية في الأساس، ومن خلالها أصبحت الدول تقاس مدى تقدمها بقدرتها على امتلاك والتعامل مع التكنولوجيا الحديثة في شتى مناحي الحياة، إلا أن هذه النعمة صاحبتها نقمة، تمثلت في الاستخدام الغير قانوني لها، إذ أضحت تستخدم كمعول هدم لا للبناء في الكثير من الأحيان.

وتكمن خطورة هذه الجرائم، في كونها جرائم عابرة للحدود، لذا فسلوك الاجرامي الذي يستخدم شبكات المعلومات والتكنولوجيا الحديثة، يسهل التهرب من العقاب، حيث ترتكب كثير من هذه الجرائم من على بُعد دولي.

وما يلاحظ أن هذه الجرائم انتشرت في الآونة الأخيرة وشكلت ظاهرة إجرامية اطلق عليها مصطلح "الاجرام المستحدث"، الذي يتم عن طريق التكنولوجيا، فهي الجريمة الإلكترونية، أو الجريمة التي ترتكب بواسطة تقنية المعلومات، وقد بذلت الدول العديد من الجهود لإقرار تشريعات تجرم سلوكا اجراميا يرتكب بواسطة شبكات المعلومات والأجهزة الحديثة، وباتت تعرف بالجرائم الإلكترونية، فهي الوجه الآخر للإجرام التقليدي، الذي يرتكب في وسط مادي، ومسرح جريمة تقليدي، حتى بات الوسط الذي ترتكب فيه الجريمة الإلكترونية هو ومضات كهربائية ومغناطيسية، ورموز، وشفرات، ولم يعد مسرح الجريمة إلا مسرحا افتراضياً.

وللحد من ظاهرة الجريمة الالكترونية سطر المشرع الجزائري على غرار سائر التشريعات المقارنة، سياسة جنائية اتسمت بالصرامة والحزم، فمن جانب البحث والتحري في هذا النوع من الجرائم أعطى لها المشرع خصوصية معينة تختلف عن البحث والتحري في الجرائم التقليدية، ولعل أبرز اجراء يثير النقاش في موضوع التحري في الجرائم المعلوماتية هو اجراء تفتيش المنظومة المعلوماتية.

من هنا نطرح الاشكالية التالية: ما المقصود بتفتيش المنظومة المعلوماتية؟ وما هي الشروط القانونية المقررة قانونا في ذلك؟ وكيف يتم تنفيذ التفتيش على المنظومة المعلوماتية؟

1. مفهوم تفتيش المنظومة المعلوماتية.

لأجل الوقوف على مفهوم تفتيش المنظومة المعلوماتية، لابد من الوقوف على تعريف تفتيش المنظومة المعلوماتية، وكذا نطاق تفتيش المنظومة المعلوماتية واخيرا الى دوافع ومبررات اللجوء الى هذا التفتيش.

1. 1: تعريف تفتيش المنظومة المعلوماتية.

التفتيش بصورة عامة هو البحث عن عناصر الحقيقة في مستودع السر[1]، وهذا التعريف يشمل تفتيش المساكن أو تفتيش الأشخاص، أو تفتيش متاعه.

لذا يعرف التفتيش على أنه: البحث عن أشياء تفيد الكشف عن جريمة وقعت ونسبتها إلى المتهم، كما يعرف بأنه: " البحث في مستودع سر شخص عن أشياء تفيد الكشف عن الجريمة ونسبتها إلى المتهم" [2].

والتفتيش وفقا للقواعد قانون الإجراءات الجزائية التقليدية ينقسم من حيث محله الى قسمين: الأول تفتيش ينصب على المنازل، وتفتيش يقع على الأشخاص، وتفتيش المنازل هو إجراء من إجراءات التحقيق بمقتضاه يقوم المحقق أو من يأذن له من رجال الشرطة القضائية بالبحث في منزل شخص معين على أشياء تتعلق بجناية أو جنحة قامت قرائن قوية على حيازته لها، والثاني هو إجراء من إجراءات التحقيق أيضا يقصد به ضبط ما يحوزه الشخص من أشياء تفيد كشف الحقيقة.

وبالرجوع الى التفتيش الخاص بالمنظومة المعلوماتية، فإنّ التفتيش في هذه الحالة ينصب على جهاز الحاسب الآلي الذي يعمل طبقا لتعليمات محددة سلفا يستقبل البيانات ويخزنها ويقوم بمعالجة واستخراج النتائج المطلوبة، وهو متصل بالشبكة للحصول على المعلومات وتبادلها عبر الشبكات والبريد الإلكتروني، ولهذا فإن التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة عن التفتيش التقليدي للأشخاص والمنازل، إلا أنه يخضع في إجراءاته للضوابط التي حددها قانون الإجراءات الجزائية، وما يستلزمه من وقوع الجريمة واتهام شخص أو أشخاص معينين بارتكاب جريمة، وأن تكون هناك دلائل أو قرائن على ما يفيد في كشف الحقيقة في أجهزة الحاسب الآلي والإنترنت خاصة بالمتهم أو غيره من الأشخاص، وإذا ما توافرت تلك الشروط، فإنه يجوز لسلطة التحقيق تفتيش جهاز الحاسب الآلي وملحقاته المكونة له المادية والمعنوية، وذلك من أجل ضبط أدلة

الجريمة، وما يحتمل أن يكون قد استعمل في ارتكابها أو نتج عنها أو وقعت عليه، وكل ما من شأنه أن يكشف عن الجريمة[3].

وما يمكن استنتاجه هنا هو أن معنى التفتيش في الجريمة التقليدية هو تقريبا ذاته في الجريمة المعلوماتية، وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم المنسوب إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتوي من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكيات المرتكبة وغير المشروعة والتي تشكل جناية أو جنحة[4].

2.1: حالات تفتيش المنظومة المعلوماتية.

ان تفتيش المنظومات المعلوماتية عالجها المشرع الجزائري في أحكام القانون :09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث وبالرجوع الى أحكام نص المادة :**05** من هذا القانون فإنها تنص صراحة على جواز الدخول ولو عن بعد للمنظومة المعلوماتية بغرض تفتيشها كليا أو جزء منها وتفتيش المعطيات المخزنة فيها وكذا تفتيش منظومة تخزين المعلوماتية، لذا فان هذا التفتيش مقيد، ولا يمكن اللجوء إليه إلا في جرائم محددة على سبيل الحصر، ويرد على الجهاز الذي ارتكبت بواسطته الجريمة.

1.2.1: من حيث نوع الجريمة.

بالرجوع الى نص المادة: **05** من القانون :**04-09** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها:" ...يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة: **04** أعلاه..."، حيث باستقراء نص هذه المادة نجدها تنص صراحة على جواز تفتيش المنظومات المعلوماتية في حالات معينة، مذكورة في أحكام المادة: 04 القانون

:04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ويمكن حصر تلك الحالات فيما يلي :

-01- للوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

-02- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

-03- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية.

-04- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[5].

2.2.2: من حيث مكان وجود جهاز الذي ارتكبت به الجريمة

ان عملية تفتيش المنظومة المعلوماتية، تنصب على المكونات المادية بأوعيتها المختلفة، بغرض البحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، ويدخل هذا الامر في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

-الحالة الأولى : في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية :إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن[6].

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات [7].

3: مبررات تفتيش المنظومة المعلوماتية.

ترتب على إجراء التفتيش خلاف فقهي حول مدى مشروعية التفتيش في الجرائم المعلوماتية بين الذين يرون قابلية النصوص التقليدية لتطبيق هذا الإجراء في الجرائم المعلوماتية، مع الذين يتجهون إلى وجوب استحداث نصوص تشريعية جديدة تجرم الأفعال، وأثناء غياب تشريعات جديدة فلا مجال للحديث عن سبب تفتيش الحاسب الآلي، غير أن هذه المشكلة لا يمكن أن تثير سبب التفتيش في الجرائم المعلوماتية في الدول التي تضمنت نصوص قانونية للتجريم والعقاب على مثل هذه الجرائم إلاَ أن المشكلة تكمن في الدول التي لم تجرم الأفعال غير المشروعة الناشئة عن أنظمة الحاسب الآلي أين قد يكون التفتيش فيها باطل[8].

وبالتالي فقد تناول المشرع الجزائري سبب التفتيش في أكثر من نص منها المادة:**44** من قانون الإجراءات الجزائية والتي نصت على ما يلي: "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلاَ بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش".

كما نص على دواعي تفتيش المنظومة المعلوماتية في أحكام نص المادة: **03** من القانون :**04-09** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات التي تنص على أنه:" مع مراعاة الاحكام القانونية التي تضمن

سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الاجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع و تسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية ".

اذن فان مبررات اللجوء الى تفتيش المنظومة المعلوماتية يكون إما لحماية النظام العام أو لمستلزمات التحريات أو لأجل التحقيقات القضائية الجارية.

2: الشروط والاجراءات القانونية لتفتيش المنظومة المعلوماتية.

إن تفتيش المنظومة المعلوماتية أحاطها المشرع الجزائري بمجموعة من الضوابط القانونية، إذ لا يكون مطلقا نظرا لما فيه من مساس بحقوق وحريات الافراد، كما ان اخضاع المنظومة المعلوماتية للتفتيش يكون وفق لإجراءات معينة، وفيما يلي سنتناول الشروط والاجراءات الخاصة بتفتيش المنظومة المعلوماتية.

1.2: الشروط القانونية لتفتيش المنظومة الالكترونية.

بالرجوع الى أحكام قانون الاجراءات الجزائية فان المشرع وضع جملة من الشروط الشكلية والاخرى موضوعية التي يجب على القائم بالتفتيش أن يلتزم بها، تحت طائلة بطلان إجراءات التفتيش.

1.1.2: الشروط الموضوعية.

يشترط أن يتوافر في التفتيش سببا له، وأن يكون محله الحاسوب بكل مكوناته المادية والمنطقية والشبكة الإلكترونية، بالإضافة إلى وجود سلطة مختصة للقيام به، وعلى ضوء ما سبق فإن القواعد الموضوعية لتفتيش نظم المعلوماتية تتمثل فيما يلي:

1.1.2: سبب التفتيش.

إن سبب تفتيش المنظومة المعلوماتية كما سبق ذكره، يكون إما لحماية النظام العام أو لمستلزمات التحريات أو لأجل التحقيقات القضائية الجارية اليه في احكام نص المادة 44 من قانون الاجراءات الجزائية، غير أنه وخلافا لذلك فان المشرع الجزائري خرج عن هذه القواعد العامة بخصوص الجريمة المعلوماتية وجعل من التفتيش المنصب على المنظومة المعلوماتية إجراء وقائي في مواجهة ما قد يقدم عليه المجرم المعلوماتي واستعمال الرقابة التقنية لوسائل الاتصالات الالكترونية قد تكون سابقة لارتكاب أي جرم ودون توجيه الاتهام لأي شخص وقد أوضحت ذلك المادة:05 من القانون :**09-04** حين أشارت بالقول بان تفتيش المنظومة المعلوماتية جائز في اطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها في المادة :05 من القانون :**09-04** [9].

ثانيا: محل تفتيش النظم المعلوماتية.

لكي يكون التفتيش صحيحا يجب أن يرد على المحل الذي قد يكون الشخص فيه وبحوزته الحاسب الالكتروني، وهذا المحل يجب أن يكون محددا أو قابل لتحديد وجائزا قانونا، وبالتالي فالشخص الذي يقوم بتفتيش نظم المعلوماتية، قد يكون من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، أو من مشغلي، أو مستخدمي الحاسب، أو مقدمي الخدمة، أو من مهندسي الصيانة والاتصالات، أو من مديري نظم المعلوماتية، أما الأشخاص الذين يقوم عليهم التفتيش هم أي أشخاص آخرين يكون بحوزتهم معدات أو أجهزة معلوماتية أو أجهزة حاسب آلي محمول أو تلفونات متصلة بجهاز المودم أو مستندات، وفي كل الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به.

وتشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته[10]، والتي تتمثل في شكل وحدات كوحدة الذاكرة، لوحة المفاتيح والشاشة ووحدة التحكم، وكل واحدة لها مهمة محددة، فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية[11]، والتي يمكن إيجادها في مسكن المتهم أو

مسكن غير المتهم، والتي قد تتواجد أيضا في مكان عام، فهي بذلك تخضع للقواعد التي تحكم ذلك المكان، كما قد تتواجد هذه المكونات في حيازة شخص خارج مسكنه، فهي بذلك تخضع لقواعد تفتيش الأشخاص بوصف المكونات المادية للحاسوب أحد ملحقاته، وسواء كان الشخص الحائز المالك أو الغير، أما بالنسبة لمكونات الحاسوب المعنوية والمتمثلة في المعلومات والبيانات المعالجة آليا، فهي محل خلاف باعتبارها غير مادية.

الفرع الثاني: الشروط الشكلية لتفتيش النظم المعلوماتية.

يستخلص من نص المادة 05 من القانون :**04-09** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات، بان التفتيش في مجال جرائم المعلوماتية يدرجه المشرع في إطار أحكام قانون الاجراءات الجزائية.

والاختلاف الوحيد الموجود عن التفتيش العادي يكمن على طبيعة المكان الذي يوجد به الكومبيوتر ومكوناته وفيما إذا كان خاصا أو عاما، هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أم أجنبيا.

ففي الحالة الاصلية يكون التفتيش يكون بالانتقال الى مسكن المتهم أو المكان الذي تتواجد فيه الاجهزة المقصودة أو في الاماكن العامة حال حيازة شخص لجهاز الحاسوب الالي أو أحد مكوناته المادية كوسائط التخزين مثل الاقراص المرنة والاقراص الصلبة والاقراص المضغوطة والاشرطة الممغنطة فواضح بان القانون أحال هذه الاجراءات الى القواعد العامة في قانون الاجراءات الجزائية [12].

أولا: شروط تفتيش المنظومة المعلوماتية بالانتقال الى منزل المتهم.

ان تفتيش المنظومة المعلوماتية بالانتقال الى مسكن المتهم يأخذ ثلاث حالات، إما في حالة التلبس بالجريمة، أو في حالة التحريات الاولية واخيرا في حالة تنفيذ الانابات القضائية.

01- تفتيش المساكن في حالة الجرائم المتلبس بها.

بالرجوع الى الشروط العامة للتفتيش نجد أن المادة: **44** من قانون الإجراءات الجزائية تنص على أنه: **"**لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش**"** [13].

ومن خلال المادة: **44** قانون الإجراءات الجزائية نلاحظ أن المشرع الجزائري قد حرص على وضع قيود وضوابط، يجب أن يلتزم بها ضابط الشرطة القضائية عند تفتيشه لمنزل المشتبه فيه وتتمثل هذه القيود في:

- أن يكون قد ارتكب جناية، أو جنحة في حالة تلبس.

- أن يكون صاحب المسكن محل التفتيش ممن ارتكبوا، أو ساهموا في ارتكاب الجريمة، أو ممن تظهر عليهم أمارات تدل على أنه يحوزون أشياء، أو أوراق لها علاقة بالجناية.

- يجب أن يتم التفتيش بموجب إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق وذلك لاعتبارين اثنين أولهما أن التفتيش من اختصاص السلطة القضائية وهو أصلا من أعمال التحقيق القضائي وخوله المشرع استثناء لضابط الشرطة القضائية لمقتضيات القيام بالتحريات الأولية، وثانيها أن حماية الحقوق والحريات العامة للأفراد من اختصاص السلطة القضائية فيجب أن يتم التفتيش تحت رقابتها.

-إلزامية الاستظهار بالإذن المكتوب قبل الدخول إلى المسكن ومباشرة التفتيش.

- احترام ميعاد التفتيش، فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات الاستثنائية التي أقرها القانون، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل

ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كاستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة [14].

بالإضافة الى شرط تواجد الاجهزة المقصود، أي جهاز الحاسوب الالي أو أحد مكوناته المادية كوسائط التخزين مثل الاقراص المرنة والاقراص الصلبة والاقراص المضغوطة والاشرطة الممغنطة.

ثانيا: تفتيش مسكن شخص غير متهم.

بالرجوع إلى نص المادة: **63** من قانون الإجراءات الجزائية نجدها تنص على قيام ضباط الشرطة القضائية بالتحقيقات الابتدائية للجريمة بمجرد علمهم بوقوعها، إما بناء على تعليمات وكيل الجمهورية، وإما من تلقاء أنفسهم، ونصت المادة: 64 منه على أنه لا يجوز تفتيش المساكن في هذه الحالة ومعاينتها وضبط الأشياء المثبتة، إلا برضاء صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضاء بتصريح مكتوب بخط صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه وتطبق فضلا عن ذلك أحكام المواد من 44 إلى 47 من نفس القانون.

ثالثا: الحالات الاخرى لتفتيش المساكن.

هناك حالات أخرى لتفتيش المساكن خارج إطار التحريات الأولية يمكن لضابط الشرطة القضائية تنفيذها، وهي حالات نص عليها قانون الإجراءات الجزائية ونلخصها فيما يلي:

- تفتيش المنازل بموجب إنابة قضائية فضابط الشرطة القضائية الذي يكون مفوضا من طرف قاضي التحقيق المختص يمكن أن يباشر التفتيش في جميع الأماكن.

- التفتيش في إطار مكافحة جرائم الإرهاب والتخريب ما عدا ما يتعلق منها بالمحافظة على السر المهني.

أولا: شروط تفتيش المنظومة المعلوماتية في الاماكن العامة.

القاعدة العامة أنه ليس هناك من إجراءات أو قيود محددة بالنسبة للتفتيش خارج المساكن بل تطبق الإجراءات الخاصة بالمعاينات كما هو الحال في تفتيش المحلات العامة مادام الجمهور فيها، إلا أنه واستثناء للقاعدة العامة فإنه تلحق الحماية القانونية المقررة بالنسبة للمنزل، بمكاتب المحامين والأطباء وإليها من مكاتب الخبراء والمحاسبين، كونها تعتبر مستودع السر ولا يباح لأي فرد الاطلاع على ما بداخله[15]، حيث تنص المادة 45 ق.إ.ج:**"...غير انه يجب أن يراعى في التفتيش أماكن يشغلها شخص ملزم بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان السر المهني"**، وهذا الأمر مؤكد في المادة 80 من القانون المنظم لمهنة المحاماة **04/91**، فلا يجوز بموجب هذا المادة تفتيش أو حجز الوثائق المودعة في مكتب المحامي إلا بحضور النقيب أو ممثله وبعد إخطارهما شخصيا وبصفة قانونية وأي إجراء أو تصرف يكون مخالف لأحكام هذه المادة يكون باطلا بطلانا مطلقا.

المطلب الثالث: تنفيذ تفتيش المنظومة المعلوماتية.

حتى يكون تفتيش المنظومة المعلوماتية منتجا لأثاره القانونية وحتى نتوصل الى الغاية من وراء اللجوء اليه، فانه يجب ان يجرى من طرف الاهل الاختصاص المخول لهم قانونا ذلك ويجب ان يتبع في ذلك اجراءات محددة ويجب ان يكون في وقت محدد له قانونا

الفرع الاول: صفة القائم بالتفتيش المنظومة المعلوماتية.

الأصل أن تقوم بإجراء تفتيش المنظومة المعلوماتية سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق أو النيابة العامة باعتبارها سلطة قضائية، الا أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهو الامر الذي أكدته المادة 05 من القانون :04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات، وحددت الاشخاص المؤهل لهم قانونا بتفتيش المنظومة المعلوماتية، وحصرتهم فيما يلي:

أولا: السلطات القضائية.

باعتبار ان الامر بإجراء تفتيش هو مخول حصريا للسلطات القضائية دون سواها فان قاضي التحقيق باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته واستثناءا يجوز لوكيل الجمهورية أن يقوم ببعض إجراءات التحقيق، لأن الاختصاص الأصيل بمباشرته يعود لقاضي التحقيق وحده دون سواه ولا يكفي توافر صفة قاضي التحقيق لكي يقوم بإجراء التفتيش، بل لابد أن يكون مختصا سواء من ناحية الاختصاص المكاني أو النوعي، فيتحدد اختصاص قاضي التحقيق محليا إمَا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

ثانيا: إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية.

يتمتع قاضي التحقيق وحده بالاختصاص الأصيل لإجراء التحقيق، ونظرا لكثرة هذه الإجراءات وتنوعها أجاز له القانون أن يندب غيره - ضباط الشرطة القضائية -للقيام ببعضها وفقا لشروط يجب توافرها وتطبيقها بحذافيرها.

وبالتالي فإن ضابط الشرطة القضائية المنتدب الذي يختص في الجريمة التقليدية هو نفسه الذي يختص في الجريمة المعلوماتية، ويتحقق إجراء التفتيش نظم

المعلوماتية بمعرفة ضابط الشرطة القضائية في حالة التفتيش بناء على إذن قضائي بإجرائه، التفتيش بناء على حالة التلبس بالجريمة، التفتيش بناء على موافقة المتهم، كما سبق ذكره.

المطلب الثاني: اجراءات تنفيذ تفتيش للمنظومة المعلوماتية.

ان تفتيش المنظومة المعلوماتية يختلف حسب كل حالة ويمكن حصر هاته الحالات فيما يلي:

الفرع الاول: التفتيش عن بعد.

هو الذي نصت عليه الفقرة الثانية من المادة 05 والتي قضت بأنه: « في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك"، فقد صرحت المادة: 05 الفقرة: 02 بإمكانية الدخول إلى منظومة معلوماتية موجودة على جهاز آخر متصل بالجهاز الأول ولكن في مكان مختلف تماماً عنه داخل الدولة ومتصلان فيما بينهما بشبكة اتصالات أياً كانت، يمكن الدخول إلى هذه المنظومة سواء كان الجهاز الثاني ملك للمتهم أو لشخص آخر فلا فرق، ما دامت هناك دلائل على إمكانية وجود المعطيات المبحوث عنها في ذلك النظام، وعليه فإن التفتيش عن بعد في هذه الفرضية يشترط:

1- وجود دلائل أو أسباب تدعو للاعتقاد بأن الكشف عن المعطيات يكون بالبحث في المنظومة الثانية.

2 -إعلام السلطة القضائية: فلم يفرض المشرع طلب إذن ثان يسمح بهذا التفتيش وانما مجرد إعلام السلطة القضائية التي تولت أمر هذا التفتيش (وكيل الجمهورية، أو قاضي التحقيق بحسب الحالة).

الفرع الثاني: تفتيش المنظومة المعلوماتية على سبيل التفتيش الوقائي.

بالعودة الى المادة: 05 في فقرتها الأولى نصت «.. ولو عن بعد » قبل ذكر الأنظمة التي يمكن تفتيشها، ثم تناولت حالة اتصال الحاسوبين وإمكانية الدخول إلى النظام الثاني، فما كان على المشرع سوى أن يذكر هذا الأمر دون تناوله مسبقاً، فقد قدم المشرع في هذه الحالة إمكانية تفتيش المنظومة المعلوماتية عن بعد على سبيل التفتيش الوقائي أو التفتيش الافتراضي، وهو يختلف عن مراقبة الاتصالات الإلكترونية من حيث التقنية، فالمراقبة تعني اعتراض المراسلات (SMS, Mail-E)،غرف الدردشة وكشف محتواها بدون الدخول إلى النظام المعلوماتي للجهاز الذي يتم مراقبته، أما التفتيش عن بعد فهو يتم عن طريق برنامج تجسس (حصان طروادة) يسمح بالولوج للنظام المعلوماتي المستهدف ومعرفة كل ما يحصل فيه من عمليات، وهذا يعد تسجيل البيانات، الحفظ، تحويل...، وكأن المراقب يشاهد ما يشاهده الشخص المعني بالتفتيش على جهازه أمر خطير لأنه يمس مباشرة بالحياة الخاصة بالأشخاص بما تحويه تلك الأنظمة من بيانات شخصية قد لا تهم أبداً في التحقيقات والتحريات التي تتم.

الفرع الثالث: حالة وجود معطيات مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني.

وهي الحالة التي نصت عليها المادة: 05 فقرة 03 من قانون: 04/09 فإن كان الأمر كذلك فلا يمكن تفتيش تلك المنظومة وانما يجب الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل، فبالرغم من إمكانية تفتيشها من الناحية الفنية داخل النطاق الإقليمي، إلا أن ذلك لا يتم إلا بعد موافقة الطرف الأجنبي، وهو أمر متعلق بسيادة الدول على أراضيها وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني.

ويجدر التنبيه الى أنه يمكن بناءً على اتفاقيات دولية ثنائية أو متعددة الأطراف السماح بتفتيش نظم المعلوماتية خارج إقليم الدولة وبدون إذن الدولة المعنية الطرف في الاتفاقية، ولكن بالطبع في حدود معينة يسمح بها التعاون، من أجل معرفة المعطيات الموجودة في خادم موجود الدولي ووفقاً لمبدأ المعاملة بالمثل بين أطراف الاتفاقية الدولية بالخارج، فإن فتح تحقيق قضائي يسمح بتحرير إنابة قضائية دولية يمكن أن يتم اللجوء إليها، تمثل في غالب الأحيان عقبة وقتية للحصول عليها، وفي هذه الحال يمكن للمجرم المعلوماتي أن يستغل هذا الوقت لنقل أو إخفاء المعطيات[16].

الفرع الرابع: التسخير

من أجل جمع عناصر الدليل الرقمي، فإن القضاة (وكيل الجمهورية، قاضي التحقيق بحسب الحالة) يمكنهم اللجوء لمختلف التصرفات وأساليب التحقيق ومن ذلك التسخير، والتسخير عبارة عن إجراء من طرف قاضي أو ضابط شرطة قضائية يفوض فيه شخص لتقديم عمل لا يمكنه القيام به بنفسه لنقص الوسائل أو لانعدام الاختصاص التقني الضروري.

-1- في الجنايات والجنح المتلبس بها : لضابط الشرطة القضائية إن اقتضى الأمر ذلك أن يستعين بأشخاص مؤهلين لإجراء معاينات لا يمكن تأخيرها (المادة 49 ق إ ج) وهو حكم عام في قانون الإجراءات الجزائية، وهذا لمساعدته في الكشف عن الأدلة والمحافظة عليها ولا يتأتى ذلك إلا بالاستعانة بأهل الخبرة والمعرفة التقنية.

-2- التحريات الأولية والتحقيق القضائي: على نص المادة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو باتخاذ التدابير اللازمة لحماية المعطيات المعلوماتية التي تتضمنها، فالتسخير يتم من طرف السلطات المكلفة بالتفتيش: ضابط الشرطة القضائية بإذن من قاضي التحقيق أو

وكيل الجمهورية، لأشخاص سواء من القطاع العام أو الخاص لهم إطلاع كاف بتكنولوجيات الإعلام والاتصال، وقد حدد المشرع هذا الإطلاع على نحو :

- دراية المسخر بعمل المنظومة المعلوماتية.

- دراية المسخر بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها المنظومة المعلوماتية .وهدف التسخير مساعدة سلطات التفتيش في عملها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

خاتمة:

في نهاية هذه الورقة البحثية نخلص الا ان المشرع الجزائري لم يميز بين التفتيش بمفهومه التقليدي وتفتيش المنظومة المعلوماتية وذلك بصدد البحث والتحري في الجرائم المعلوماتية، اذ لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية، مع مراعاة بعض الاجراءات وذلك راجع للطابع الخاص للمنظومة المعلوماتية، كما نخلص الا ان هذا التفتيش قد يقع على الكومبيوتر أو أحد أجزائه كما قد يكون علة كامل المنظومة المعلوماتية أو جزء منه وذلك من خلال الولوج اليها و استخلاص الدليل الجنائي الالكتروني، كما قد يمتد هذا التفتيش الى خارج المنظومة الالكترونية الوطنية وذلك مع مراعاة الاتفاقيات الموقع بهذا الصدد، ويتم هذا التفتيش بإذن من السلطات القضائية، او عن طريق التسخيرة من السلطات القضائية، وفي الاخير نخلص الا ان المشرع الجزائري احاط موضوع تفتيش المنظومة المعلوماتية بمجموعة من الضمانات التي تصون الحريات الفردية ، وقرر بطلان كل تفتيش للمنظومة الالكترونية لا يحترم فيه الشروط الشكلية أو الموضوعية .

التهميش والاحالات:

[1] - د. محمود محمود مصطفى، شرح قانون الإجراءات الجزائية، دار النهضة القاهرة، طبعة 12، ص 140.

[2]- د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، الجزء الأول، منشورات الجامعة الليبية كلية الحقوق، الطبعة الأولى، 1971، ص481.

[3] - راجع فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 2011 ، ص- 373 .

[4]- علي محمود علي حموده ، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، " المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع1 ،دبي - الإمارات العربية المتحدة-26-28 نيسان 2003 ،ص .24

[5]- راجع أحكام المادة 04 القانون :04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، جريدة رسمية عدد: 47 .

[6]- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر1، 2011-2012، ص.2015

[7]- طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009، ص 385.

-8 فايز محمد راجح غلاب، مرجع سابق، ص 317-.319

9- أ. زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، سنة : 2011، ص.139

10- علي حسن الطوالبه،" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة، بحث منشور على شبكة الانترنت : www.policeme.gouv.

11- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1 .، دار الثقافة للنشر والتوزيع، 2011 ، ص158 .

12- أ. زبيحة زيدان ،نفس المرجع السابق ، ص.133

13- الصياغة الجديدة التي وضعها المشرع بموجب القانون رقم 82-03 المؤرخ في 13 فبراير 1982 و قد كانت الصياغة القديمة لهذه المادة " يجوز لمأمور الضبط القضائي

لانتقال إلى مساكن الأشخاص الذين قد يكونوا ساهموا في الجناية أو يحوزون أوراق أو أشياء متعلقة بالأفعال الجناية و يجري تفتيشا و يحرر عنه محضرا، و بما أن هذه المادة غير دستورية لكونها تتناقض مع نص المادة 50 من دستور 1976 التي نصها**«تضمن الدولة حرمة المسكن لا يفتش إلا بمقتضى القانون و في حدوده، لا يفتش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة»**. فجاء التعديل لتدارك القصور والتناقض بين التشريع و أحكام الدستور.

14- الصياغة الجديدة التي وضعها المشرع بموجب القانون رقم 82-03 المؤرخ في 13 فبراير 1982 و قد كانت الصياغة القديمة لهذه المادة " يجوز لمأمور الضبط القضائي لانتقال إلى مساكن الأشخاص الذين قد يكونوا ساهموا في الجناية أو يحوزون أوراق أو أشياء متعلقة بالأفعال الجناية و يجري تفتيشا و يحرر عنه محضرا، و بما أن هذه المادة غير دستورية لكونها تتناقض مع نص المادة 50 من دستور 1976 التي نصها**«تضمن الدولة حرمة المسكن لا يفتش إلا بمقتضى القانون و في حدوده، لا يفتش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة»**. فجاء التعديل لتدارك القصور والتناقض بين التشريع وأحكام الدستور.

15- د. سليمان بارش، شرح قانون الإجراءات الجزائية، الطبعة الأولى، دار الشهاب، الجزائر، سنة 1987، ص.185.

16- خالد ممدوح إبراهم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص206.

قائمة المراجع

- القوانين:

-01-القانون : 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، جريدة رسمية عدد: 47 .

-02- الامر :66-155 المتضمن قانون الاجراءات الجزائية المعدل والمتمم بالقانون رقم:06-28 ، المؤرخ في :2006/12/20، الجريدة الرسمية رقم :84.

الكتب

-01- - د. محمود محمود مصطفى، شرح قانون الإجراءات الجزائية، دار النهضة القاهرة، طبعة 12،

-02- د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، الجزء الأول ، منشورات الجامعة الليبية كلية الحقوق ، الطبعة الأولى .

-03- طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009.
-04- د.سليمان بارش، شرح قانون الإجراءات الجزائية، الطبعة الأولى، دار الشهاب، الجزائر، سنة 1987.
-05- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1 .، دار الثقافة للنشر والتوزيع، 2011 .
-06- أ. زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، سنة : 2011.

مذكرات و رسائل التخرج:

-01- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 2011 .
-02- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر1، 2011-2012.

مقالات علمية :

-01- علي محمود علي حموده ، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، " المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع1 ،دبي - الإمارات العربية المتحدة،سنة: 2003 .

مواقع الانترنت:

-01- علي حسن الطوالبه،" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة، بحث منشور على شبكة الانترنت : www.policeme.gouv