التفتيش في نظم المعالجة الآلية للمعطيات

الأستاذة رابحي عزيزة
أستاذة مساعدة قسم أ
جامعة طاهري محمد بشار
كلية الحقوق و العلوم السياسية، قسم الحقوق

ملخص:

شاعت في السنوات الأخيرة طائفة جديدة من الجرائم التي تستهدف المعلومات وبرامج الحاسوب كالدخول غير المصرح به إلى أنظمة الحاسوب والشبكات، و باعتبار هذه الأخيرة تقع في بيئة رقمية قد تتعدى حدود الدول و حتى القارات، و هو الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة وبالذات فيما يخص إثبات هذه الجرائم، وآلية مباشرة إجراءات الاستدلال والتحقيق لتعقّب المجرمين وتقديمهم للعدالة، و من تلك الاجراءات إجراء تفتيش نظم المعالجة الآلية للمعطيات.

Résumé :

Étaler au cours des dernières années, une nouvelle gamme de crimes contre les systèmes d'information et des programmes informatiques tels que l'admission accès non autorisé aux systèmes et réseaux informatiques, et que celui-ci se trouve dans un environnement numérique peut aller au-delà des frontières des Etats et même des continents, et est quelque chose que Pat soulève des défis juridiques et pratiques à des dispositifs impliqués dans la lutte contre la criminalité, en particulier en matière d'établissement de ces crimes, et le mécanisme de raisonnement direct et d'enquête pour traquer les criminels et de les amener à des procédures de justice, et de ces actions systèmes de traitement de mener un mécanisme d'inspection pour les données.

مقدمة

نتج عن الزيادة المطردة في استخدام و تطور الحاسوب و شبكة الأنترنت ارتكاب العديد من الجرائم التي ترتكب بواسطة الحاسوب والأنترنت، واصطلح على تسميتها بالجرائم المعلوماتية، حيث أثارت هذه الأخيرة العديد من الإشكالات بالنسبة للقائمين على مكافحتها، و من أهمها التفتيش في النظام المعلوماتي، فالتفتيش في هذا النمط من الجرائم يتم عادة على نظم الحاسوب، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة به، وهذا هو الوضع الغالب في ظل شيوع التشبيك بين الحواسيب على مستوى الدول، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه يخلق تحديات كبيرة، إذ لا يعتبر بالأمر السهل حيث يتطلب التفتيش فيها استخدام تقنيات حديثة تتناسب و ارتكاب الجريمة، كما يتطلب أيضا خبرة فنية في المجال المعلوماتي بالنسبة للقائمين بعملية التفتيش.

إن التفتيش في قانون الإجراءات الجزائية هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة[1]، وقد احاط القانون هذا التفتيش بضمانات عديدة ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعية قد يكون متعلقا بالمتهم أو بغيره وهو في كل أحواله جائز مع الإختلاف في بعض الشروط.فالتفتيش بالمعنى التقليدي يهدف إلى حفظ اشياء مادية تتعلق بالجريمة و تفيد في كشف الحقيقة، بينما البيانات الالكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي، لذلك **هل يمكن أن يرد التفتيش على هذه البيانات غير المحسوسة ؟ أي ما مدى امكانية التفتيش في نظم المعالجة الآلية للمعطيات؟** و للإجابة على التساؤل المطروح سنقسم هذا الموضوع إلى مطلبين الأول يتعلق بمدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش (مطلب أول) و الثاني سيتم تخصيصه لضوابط إجراء تفتيش نظم الحاسب الآلي (مطلب ثان)

و يجدر بنا قبل ذلك بهدف التوضيح أن نشير إلى النقاط التالية:

1- أن التفتيش او البحث في الأنظمة المعلوماتية قد عرفه المجلس الأوروبي بانه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني[2]، و هو بذلك يسمح باستخدام الوسائل الالكترونية للبحث في اي مكان عن البيانات أو الأدلة المطلوبة[3].

2- يقال أن التفتيش في الأنظمة المعلوماتية يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط و أحكام.[4]

3- يمكن تعريف المصطلحات الواردة أدناه تطبيقا للمادة الثانية من القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها[5] كالتالي:

المنظومة المعلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، و يمكننا هنا الإشارة إلى أنه تم تعريف النظام المعلوماتي وفق للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 في الفصل الاول منها في المادة الثانية في تعريفها لبعض المصطلحات أنه" النظام المعلوماتي: مجموعة برامج وادوات معدة لمعالجة وادراة البيانات والمعلومات". ومهما كان اسلوب معالجتها للمعطيات فانها تشكل نظام معلوماتي.[1]

المعطيات المعلوماتية هي أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"، و نشير هنا أن المعطيات في اللغة تقابل "البيانات" و البيان في اللغة من مشتقات كلمة "بين" و من معانيه فيها ما يتبين به الشيئ من الدلالة و غيرها [6] و تقابلها في اللغة اللاتينية كلمة "datum" و تعني شيئ معطى أو مسلم به، أو شيئ ما معروف أو مسلم بصحته كحقيقة أو واقعة، وجمعها data و هي التي تستخدم كلاسيكيا في اللغة الانجليزية، بينما تستخدم اللغة الفرنسية مقابلا لها كلمة معطيات[7]، و هي الكلمة التي آثر على استعمالها المشرع الجزائري في مقابل كلمة البيانات، مع العلم أن كلا من القانونين يخلوان من دكر كلمة المعلومات رغم أن البعض فضلوا استخدام مصطلح المعلومات، لأنه من الضروري التـفرقة بين المعطيات ذلك أن المعطيات عندما تعالج آليا تأخد تسمية المعلومات.

و الملاحظ على النص أن المشرع الجزائري أدرج البرنامج ضمن مفهوم المعطيات رغم - الفارق بينهما.[8]

4- المعالجة الآلية للمعطيات: يقصد بلمعالجة الالكترونية هي ليست معالجة يدوية او ميكانيكية او حرارية، بل هي وبكل بساطة عبارة عن معالجة بواسطة اجهزة الكترونية ومن هذه الاجهزة هي الحاسوب لانه مكون من عدة اجهزة تعمل كلها بواسطة شرائح

الكترونية وهذه الشرائح الالكترونية هي المتحكم في كل عمليات المعالجة وبالتالي فهي معالجة الكترونية.

و يقصد بالمعالجة الآلية للمعطيات وفق ما هو متعارف عليه في المجال التقني "مجموعة من العمليات المترابطة و المتسلسلة بدءا من جمع المعطيات و إدخالها إلى نظام المعالجة الآلية و معالجتها وفقا للبرامج التي تعمل به نظم المعالجة الآلية وصولا إلى تحليلها و إخراجها بصورة معلومات"،أماعن المقصود بمعالجة المعطيات فهي مجموعة العمليات التي تحوّل المعطيات إلى معلومات، حيث إن المعطيات أو البيانات هي مجموعة الحقائق الأولية والأشكال التي عادة ما تكون غير منظمة أو معالجة، في حين أن المعلومات هي البيانات المعالجة.[9]

و في اطار المادة الأولى من اتفاقية بودابست من الفصل الأول يقصد بمعالجة البيانات هي مجموعة عمليات تطبق على بيانات و يتم تسجيلها عن طريق تنفيد برنامج المعلوماتية.

المطلب الأول: مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

يتكون الحاسب الآلي من مكونات مادية و مكونات معنوية كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلي أو المستوى الدولي فهل تخضع هذه المكونات للتفتيش؟.

البند الأول: مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، للإجراءات القانونية الخاصة بالتفتيش وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أم مكان خاص، إذ ان لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونيا في التشريعات المختلفة[10]، كالقانون الجزائري حيث نصت المادة 64 من

قانون الاجراءات الجزائية و التي قيدت ممارسة هـذا الإجراء بالشروط التالية:
- الحصول على إذن للتفتيش من وكيل الجمهورية واستظهار هذه المذكرة قبل بدء العملية ، وتتضمن مذكرة التفتيش البيانات التالية:
- وصف الجريمة محل البحث والتحري، عنوان الأماكن التي سيتم تفتيشها، عدم ذكر هذه البيانات تؤدي إلى بطلان إجراء التفتيش.

- أن يجرى التفتيش بحضور صاحب المسكن وإن تعذر وجب تعيين ممثل له وإن تعذر الأمر كذ لك يقوم ضابط الشرطة القضائية بتعيين شاهدين لاعلاقة لهما (المادة 45من ق ا ج).

-أن يجري التفتيش بعد الساعة الخامسة 05 صباحا وقبل الساعة 08 مساءا غير أنه يجوز التفتيش في أي وقت إذا طلب صاحب المسكن ذلك أو إذا سمعت نداءات من داخل المسكن كما يجوز تفتيش الفنادق والمحلات والنوادي والمقاهي وأماكن المشاهدة العامة (المسرح، السينما) وكل مكان مفتوح للجمهور في أي ساعة ليلا ونهارا.

هدا و قد استثنى عن القاعدة العامة في المادة 64 السالفة الذكر بموجب الفقرة 3 من نفس المادة تطبيق هذه الضمانات على بعض الجرائم محيلا ذلك إلى المادة 47 في الفقرة 3 حيث أجازت أن يتم التفتيش و المعاينة في المساكن في كل ساعة ليلا ونهارا ودون التقيد لشرط حضور صاحب المسكن أو ممثيله اذا تعلق الأمر بالجرائم التالية:..... الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات.

و يجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم انها متصلة بحاسب أو بنهاية طرفية في مكان آخر كمسكن لا يخص مسكن المتهم، فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال[11] .

البند الثاني: مدى خضوع مكونات الحاسب المعنوية للتفتيش:

أثار تفتيش المكونات المنطقية للحاسب الآلي خلافا كبيرا في الفقه بشأن جواز تفتيشها من عدمه فصلاحية المكونات المعنوية للتفتيش هي محل جدل، كما يلي:

الرأي الأول:

فذهب رأي أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب، ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح ولذا لا يمكن ضبطه[12].

وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[13].

الراي الثاني:

وهناك على النقيض رأي آخر يرى على أنه يسمح بضبط بيانات الحاسب غير المحسوسة أي يجوز ضبط البيانات الالكترونية بمختلف اشكالها، ويستند هدا الرأي في دلك على القوانين الاجرائية عندما تنص على اصدار الادن بضبط (اي شيئ) فغد دلك يجب تفسيره بحيث يشمل بيانات الحاسب الآلي المحسوسة و غير المحسوسة، لأأن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها.[14]

وفي هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إليكترونيا،

ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق ان يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية، و وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة إرتكبت أو يشتبه في ارتكابها أو ان هناك نية في أن يستخدم في إرتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة[15].

كذلك الشأن بالنسبة للمشرع الفرنسي حيث قام بتعديل نصوص التفتيش بالقانون رقم 2004/545 المؤرخ في جوان 2004 حيث قام بإضافة عبارة "المعطيات المعلوماتية" في المادة 94 من قانون الإجراءات الجزائية لتصبح المادة على النحو التالي:" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".

أما عن المشرع الجزائري فانه استجاب للرأي القائل –أي الثاني- بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة و على هذا الاساس أجاز تفتيش المعطيات و لكن بموجب نص جديد و هو المادة 5 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، حيث سمح لضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 من هدا القانون و من بين هذه الحالات توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، و للوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتيبة أو جزء منها و كذا المعطيات المخزنة فيها و كذا منظومة تخزين معلوماتية.[16]

و بالنسبة للتشريع الفرنسي فإنه أرسى القواعد التي تسمح بالتفتيش في البيئة الإلكترونية حيث نصت المادة 56 على أنه " في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير ، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير لإجراء تفتيش و تحرير محضر في الموضوع "، كما نصت الفقرتين الخامسة و السادسة من المادة 56 أيضا على أنه " يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية

المتضمنة لهذه المعلومات رهن إشارة العدالة أو بأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش ".

البند الثالث: مدى خضوع مكونات الحاسب المعنوية للتفتيش عن بعد

التفتيش عن بعد هو نتيجة لطبيعة للتكنولوجيا الرقمية، و هنا نميز بين ثلاث إحتمالات:

<u>الإحتمال الأول:</u>

إتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر داخل الدولة

هناك من الدول من وجدت حلا للاشكالية المتعلقة بمدى جواز امتداد التفتيش إلى الاجهزة الاخرى المتصلة بجهاز المتهم أو المشتبه فيه، ام يقتصر على جهازه فقط؟، و منها المشرع الجزائري حيث نصت المادة 05 في الفقرة 2 من القانون رقم 04/09 بأنه " في الحالة المنصوص عليها في الفقرة(أ) من هذه المادة، اذا كانت هناك أسباب تدعوا للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقابذلك ..."، و كدلك المشرع الفرنسي حيث أضاف المادة 1/57 من قانون الاجراءات الجزائية. ويرى الفقه الألماني أيضا بشان مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، انه يمكن ان يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع اخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني.

كما نص مشروع قانون جرائم الحاسب الآلي في هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود.[17]

كما نصت المادة 17 فقرة (أ) من القانون الفرنسي رقم 2003/239 بشأن الأمن الداخلي المؤرخ في مارس 2003 بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهم عملية البحث و التحري، فتنص المادة 17 نه على أنه :" يجوز لرجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن

التي يتم فيها التفتيش على البيانات التي تهم التحقيق و المخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتداءا من النظام الرئيسي"[18]

و تسمح الاتفاقية الأروبية لجرائم تقنية المعلومات لعام 2001 للدول الأعضاء أن تمد نطاق التفتيش الدي كان محله جهاز حاسب آلي معين إلى غيره، من الأجهزة المرتبطة به في حالة الاستعجال إدا كان يتواجد به معلومات يتم الدخول إليها في هدا الجهاز من خلال الجهاز محل التفتيش، فتنص الفقرة الثانية من المادة 19 من القسم الرابع على أنه من حق السلطة القائمة بتفتيش الحاسوب المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد التفتيش إلى جهاز آخر إدا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الآلي محل التفتيش.[19]

الإحتمال الثاني:

إتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة

من المتصور طبقا لهذا الإحتمال أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الإتصال البعيدة بهدف عرقلة سلطات الإدعاء في جميع الأدلة.[20]

ووفقا لما جاء بتقرير المجلس الأوروبي فإن الإختراق المباشر يعتبر انتهاكا لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشان ويؤيد الفقه الألماني ما جاء بتقرير المجلس الأوروبي حيث ان السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى وخرقا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية[21]، وقد أيد القضاء الألماني هذا الاتجاه حيث اسفر البحث في إحدى جرائم الغش المعلوماتي عن وجود طرفية حاسب في المانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة، وقد ساور الإعتقاد الشرطة اليابانية بأن مجموعة من المخربين قد أستخدمت أجهزة كمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن

بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى تتمكن من الوصول إلى جذور هذه العملية الإرهابية[22].

فضلاً عن ذلك فإن الجريمة قد ترتكب في إقليم دولة ما وتمتد آثارها إلى إقليم دولة أخرى، فإذا كانت هذه الدولة مختصة بالتحقيق في هذه الجريمة لأن قانون عقوباتها واجب التطبيق، فإن التساؤل يثور حول مدى إمكانية تفتيش تلك الآلة الموجودة خارج الإقليم بواسطة السلطات التابعة لهذه الدولة ؟

إن اختصاص الدولة بالتحقيق في جريمة ما وإن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة مادامت خاضعة لقانون العقوبات الخاص بها، إلا أن ذلك لا يعني أن تباشر الدولة هذه الإجراءات خارج إقليمها، إذ يتعذر على الدولة مباشرة اختصاصاتها بالتحقيق خارج إقليمها، لأن ذلك من مظاهر سيادتها فلا يسمح لها بممارسته على إقليم دولة أخرى ولذا فمن المتعذر قانوناً مباشرة الدولة المختصة بالتحقيق لأي إجراء خارج إقليمها بشأن الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، ولذا تبدو مشكلة الحصول على دليل بشأن بعض الجرائم إذا كان الدليل المراد الحصول عليه يوجد في جهاز موجود في دولة أخرى في إطار الإشكالية المعروضة، إذ لن تتمكن سلطات التحقيق من الحصول عليه، ولذا تبدو اتفاقيات الإنابة القضائية هي السبيل لتحصيل هذا الدليل، بحيث تُقوَّض الدولة الأخرى في جمع هذا الدليل وإرساله لدولة التحقيق، وقد نصت المادة 25 /أ من قانون الحاسوب الهولندي على الاعتداد بالدليل المتحصل عليه في إقليم دولة أخرى إذا تم ذلك تنفيذاً لاتفاقيات التعاون الأمني والقضائي، وأحياناً تكون تلك الدولة مختصة هي الأخرى بالتحقيق في هذه الجريمة ، ولذا فإن هي لم ترغب في مباشرة التحقيق بشأنها قد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقاً لما يعرف بنظام تبادل المعلومات أو المساعدات

وقد نصت اتفاقية بودابست على هذا النظام في المادة 1/25 بقولها " تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلى أقصى حد ممكن، و ذلك للإغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التي لها علاقة بنظم وبيانات الكومبيوتر، أو بالنسبة لتجميع الأدلة الخاصة بالجريمة في شكل الكتروني"، كما نصت في المادة 32 على إمكانية الدخول بغرض التفتيش و الضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حاتين:الأولى إذا تعلق التفتيش

بمعلومات أو بيانات مباحة للجمهور، و الثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

أيضا المشرع الفرنسي في المادة 57-1من قانون الاجراءات الجزائية و التي سمحت صراحة بمباشرة بعض إجراءات البحث عن الجريمة الإلكترونية خارج الحدود الإقليمية كإمكانية تفتيش الأنظمة المعلوماتية المتصلة حتى ولو كانت متواجدة خارج إقليم الدولية ، حيث سمحت المادة المذكورة لضباط الشرطة القضائية بأن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية.

و كدلك المشرع الجزائري قام باجازة تفتيش الانظمة حتى و لو كانت خارج اقليم الدولة و دلك بموجب المادة 5 في الفقرة 3 منها من القانون 04/09 حيث أجاز النص الحصول على المعطيات المبحوث عنها و المخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني و التي يمكن الدخول إليها انطلاقا من المنظومة الاولى و دلك بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية دات الصلة و فقا لمبدا المعاملة بالمثل. و كدلك أكد بموجب نص المادة 16 من دات القانون على أنه و في اطار التحقيقات و التحريات القضائية التي تمت مباشرتها، وتتبع الجرائم المنصوص عليها في دات القانون و الكشف عن مرتكبيها، فإن السلكات المختصة بإنكانها تبادل المساعدات القضائية على المستوى الدولي.

و نصت المادة 2/16 أيضا من ذات القانون أنه من واجب سلطات التحقيق الجزائرية أن تقدم جميع التسهيلات لمراقبة الاتصالات و تفتيش المنظومات المعلوماتية الموجودة على التراب الوطني ، متى طلب منها دلك مع مراعاة مبدأ المعاملة بالمثل و الاتفاقيات الدولية.

و في نص المادة 18 من نفس القانون – اي القانون 04/09 – أورد المشرع استثناءات على طلب المساعدة القضائية، و هي الحالة التي يمكن أن تؤدي إلى المساس بالسيدة الوطنية أو النظام العام، كما اشترط المشرع الجزائري قبول المساعدة القضائية بضرورة الالتزام بالمحافظة على سرية المعلومات المبلغة و بشرط عدم استعمالها في غير الاغراض التي أدت إلى تجميعها.

كدلك الشان بالنسبة للمشرع الفرنسي حيث أجاز بموجب الفقرة 2 من المادة 57-1 من قانون الاجراءات الجزائية المضاف بموجب المادة 17 الفقرة 2 من قانون الأمن الداخلي رقم 239- 2003، حيث أجازت لمأمور الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى و لو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في العاهدات الدولية.

الاحتمال الثالث:

التصنت و المراقبة الإلكترونية لشبكات الحاسب اتلآلي

التصنت و الاشكال الأخرى للمراقبة الالكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا، مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة 04 في الفقرة "ج" من القانون 04/09 أجاز النص استثناء المراقبة الالكترونية للوصول إلى الحقيقة و اشترط أن تكون هي الحل الوحيد للوصول إلى الحقيقة.

و بالنسبة للمشرع الفرنسي نجد حالتين أجاز فيهما امكانية مراقبة الاتصالات و هما الحالة المنصوص عليها في قانون الاجراءات الجزائية في المادة 100 و هي الحالة المتعلقة بالمراقبة بغرض تحقيق قضائي، و كان التحقيق في الجرائم التي هي على درجة من الخطورة[23]، و الحالة الثانية هي الحالة الواردة في نص المادة 03 من القانون رقم 669/2004 المعدل للقانون 646/91 الخاص بحماية المراسلات التي تتم عن طريق وسائل الاتصال عن بعد، حيث أجازت المادة بصفة استثنائية على النحو المنصوص عليه في المادة الرابعة من دات القانون التي تنص على حماية الاتصالات الالكترونية أنيتم الترخيص باعتراض المراسلات الاكترونية بالوسائل الفنية، لأغراض البحث عن المعلومات التي تمس الأمن القومي و المحافظة على العناصر الأساسية للمكنون العلمي والاقتصادي للبلاد، و الوقاية من الارهاب و منع الجريمة المنظمة.

و أما عن السلطة المختصة بالتفتيش فيختص قاضي التحقيق أصلا بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم و اتخاذ الإجراءات الملائمة بصددها ثم يخطر قاضي التحقيق الذي يتولى مباشرة التحقيق، فالنيابة توجه الاتهام والتحقيق يباشر إجراءات التحقيق.

ولقد نصت المادتين 81 و82 ق.إ.ج على أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء يفيد اكتشافها في إظهار الحقيقة.

ولقد أجازت المادة 83 ق.إ.ج لقاضي التحقيق القيام بنفسه بالتفتيش في أي مكان آخر وبالتالي أي مسكن آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها، وكل شيء آخر يفيد في كشف الحقيقة، كما منحته المادة84 ق ا ج حق إنابة احد ضباط الشرطة القضائية للقيام بهذا التفتيش إذا استحال على قاضي التحقيق تنفيذ هذا التفتيش بنفسه وطبقا للشروط التي نصت عليها المواد 138 إلى 142 ق ا ج. إذ أن المشرع الجزائري قيد سلطة قاضي التحقيق في منح الإنابة بشرط استحالة قيامه بالإجراء بنفسه نظرا لخطورة السلطات التي يملكها قاضي التحقيق ومنها التفتيش.

و بالنسبة لضباط الشرطة القضائية فإن من الممكن أيضا أن يقوم بعملية التفتيش حيث يتم التفتيش بمعرفة ضباط الشرطة القضائية في الجرائم المتلبس بها ولقد نصت المادة 15 ق.إ.ج على أعضاء الضبطية القضائية الذين لهم صفة ضابط الشرطة القضائية، إذ نص القانون على ضرورة إجراء التفتيش من طرف ضابط يساعده أعوان ولكن يتم الإجراء بحضوره وتحت إشرافه وإلا وقع باطلا.

المطلب الثاني: ضوابط إجراء تفتيش نظم الحاسب الآلي

يمكننا أن نحصر ضوابط تفتيش نظم الحاسب الآلي في بعض الضوابط أو الشروط الموضوعية و الشكلية و التي سنعرضها على النحو التالي:

الفرع الأول: الضوابط الموضوعية لإجراء التفتيش

يقصد بالضوابط الموضوعية الشروط اللازمة لإجراء تفتيش صحيح و هي في الغالب تكون سابقة له،و يمكن حصرها في ثلاثة شروط أساية هي: السبب و المحل و السلطة المختصة بالقيام بالتفتيش و ستتم التفصيل فيها كالتالي:

أولا: سبب التفتيش

سبب التفتيش في الحلات التقليدية يعني السعي نحو الحصول على الدليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث [24]، و يمكن إجماله في الآتي:

أ- وقوع جريمة من جرائم الاعتداء على نظام المعالجة الآلية للمعطيات:
يقتضي المنطق العقلي و القانوني للقيام بإجراء التفتيش وقوع جريمة جناية أو جنحة و

تستبعد المخالفة لضآلة خطورتها، و الملاحظ أنه لا محل لإصدار إذن بتفتيش نظم المعالجة الآلية للمعطيات إلا إذا كان المشرع قد نص على الجرائم التي تشكل إعتداءا عليها في شكل نصوص التجريم و العقاب تطبيقا لمبدأ شرعية الجرائم و العقوبات، و ذلك ما قامت به الكثير التشريعات المقارنة و قام به المشرع الجزائري ن خلال القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 حيث أدرج فصلا خاصا بجرئم الاعتداء على نظم المعالجة الآلية للمعطيات(الفصل السابع) و عزز هذه الحماية بموجب القانون رقم 04/09 المؤرخ في 5 أوت في 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته.

ب - اتهام شخص أو أشخاص معينين بالجريمة أو المشاركة أو الشروع فيها: ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعوا إلى الاعتقاد المعقول بأنه قد ساهم في ارتكاب الجريمة المعلوماتية بوصفه فاعلا أصليا أو شريكا فيها مما يستوجب اتهامه بها، و حيث أن قوانين الاجراءات الجزائية لم تعرف الدلائل بينما عرفها الفقه بالنسبة لجرائم الاعتداء على المعالجة الآلية للمعطيات أنها مجموعة من المظاهر أو الأمرات التي تكفي وفق السياق العقلي و المنطقي أن ترجح جريمة من جرائم نظم المعالجة الآلية إلى شخص معين سواء بوصفه فاعلا أو شريكا.[25]

ج - توافر امارات قوية أو قرائنأو أشياء أو أجهزة أو معدات تفيد في كشف الحقيقة، لدى المتهم المعلوماتي و غيره: يجب أن تتوافر لدى سلطات التحقيق أسباب كافية أنه يوجد في المكان أو لدى الشخص المراد تفتيشه هو أو غيره أدوات أستخدمت في جريمة من جرائم الاعتداء على نظم المعالجة الآلية أو أشياء متحصلة منها.

ثانيا: محل التفتيش:

يقصد بالمحل المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة[26]، ومحل التفتيش في النظام المعلوماتي هو الحاسوب بكل مكوناته المادية و المعنوية و شبكات الاتصال الخاصة به بالإضافة إلى الاشخاص الذين يستخدمون الحاسوب محل التفتيش.[27]

ثالثا: السلطة المختصة بالتفتيش:

باعتبار أن إجراء التفتيش من إجراءات التحقيق الإبتدائي و التي تمس بالحرية الشخصية و انتهاك حرمة الحياة الخاصة للأفراد، حرص المشرع الجزائي على العموم

على أسناد مهمة التفتيش لجهة قضائية تكفل تلك الحقوق و الحريات و تضمنها، و حدد الجهة المختصة بالتفتيش في قاضي التحقيق حيث يختص بإجراء التفتيش و تساعده النيابة العامة بتوليها تتبع الجرائم و اتخاذ الإجراءات الملائمة بصددها.

الفرع الثاني:الضوابط الشكلية لإجراء التفتيش

سنحاول أن نسرد بعض التفصيل في الضوابط الشكلية لعملية التفتيش وسنقصرها على المشرع الجزائري، مع العلم أننا نخص بالذكر التفتيش داخل منظومة معلوماتية وهي كالتالي:

أولا:الحضور الضروري لبعض الأشخاص

يستوجب إجراء التفتيش عند مباشرته سواء تم بمعرفة سلطة التحقيق أم بمعرفة الشرطة القضائية وجوب حضور أشخاص عند مباشرته، وأول من يتعين حضوره هو المتهم، ويعتبر هذا شرطا مفترضا إذا ما تعلق الأمر بتفتيش شخصه، وذلك على خلاف تفتيش المساكن إذ من المتصور إجراء التفتيش بغير حضور المشتبه فيه متى كان حضوره غير ممكن، وبخلاف المتهم الذي يتعين حضوره قد يتطلب الأمر حضور بعض الشهود لأجراء التفتيش.

فلقد نصت المادة 45 من قانون الإجراءات الجزائية في فقرتها الأولى على ضرورة حضور صاحب المسكن عملية التفتيش، فادا تعذر عليه الحضور لسبب ما مثل السفر فإنه يتعين عليه تعيين ممثل له بناءا على أمر مكتوب من ضابط الشرطة القضائية المكلف بالتفتيش وينوه عن ذلك في محضر التفتيش، فإذا أمتنع صاحب المسكن أو كان هاربا فان ضابط الشرطة القضائية المكلف بإجراء التفتيش يستدعى شاهدين شريطة أن لا يكونا من الموظفين الخاضعين لسلطته، ويجب أن يتضمن محضر التفتيش اسمهما ولقبهما وكل البيانات المتعلقة بالتفتيش، ويتم تسخير الشاهدين بواسطة محضر يوقعه الشاهدين مع ضابط الشرطة القضائية. هذا إذا كان القائم بالتفتيش هو ضابط الشرطة القضائية بناءا على أمر من قاضي التحقيق (ندب) أما إذا حصل التفتيش بمعرفة قاضي التحقيق فلقد نص المشرع على نفس الأحكام، إذا أحال في نص المادة 82 من قانون الإجراءات الجزائية على نص المواد من 45 إلى 47.

أما إذا حصل التفتيش أثناء التحقيق الابتدائي فلقد نصت المادة 64 من قانون الإجراءات الجزائية على انه لا يجوز تفتيش المسكن إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، وحددت المادة شكل الرضا الذي يكون مكتوبا بخط يد صاحب الشأن فإذا كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه وينوه عن ذلك في المحضر كما أحالت نفس المادة على المواد 44إلى 47 من نفس القانون.

تضبط الأشياء والأوراق التي يعثر عليها جراء عملية التفتيش والتي تكون مفيدة لإظهار الحقيقة أو التي يمكن أن تشكل دلائل أو أدلة مادية في القضية كما يقوم ضابط الشرطة القضائية بجرد كل المضبوطات ويرقمها ويصنفها في أحراز مختومة بعد تقديمها للمشتبه فيه أو الشهود للتعرف عليها.[28]

إذن يشترط حضور صاحب المسكن[29] في عملية التفتيش أو شخصين عدا أعضاء التابعين للمحقق و هدا يعتبر كضمانة شكلية للتفتيش مما يحقق الاطمئنان على سلامة الاجراءات وصحة الضبط ، و هدا فيما يتعلق بالتفتيش في الجرائم التقليدية، في حين بالنسبة للجرائم المعلوماتية أو المستحدثة بما فيها جرائم الدراسة فانه يختلف عنه في أن عملية التفتيش فيها تكون إما بالنتقال إلى مسكن المتهم أو إلى المكان الموجودة به الأجهزة المراد تفتيشها أو أن يتم دلك عن بعد.فالنسبة للطريقة الأولى أحالها المشرع إلى القواعد العامة في التفتيش الواردة في قانون الاجراءات الجزائية كغيرها من الجرائم التقليدية، وفي هدا تطبق اجراءات التفتيش المنصوص عليها في المادة 44 من قانون الاجراءات الجزائية.

بينما حالة التفتيش عن بعد فقد تكون المنظومة داخل الجزائر أو خارجها، و في الحالة الأخيرة فإن دلك مرهون بمساعدة السلطات الأجنبية المختصة التي توجد بها المنظومة، و يتم دلك في نطاق الاتفاقيات التي تم ابرامها في مجال ملاحقة الجرائم المعلوماتية و طبقا لمبدأ المعاملة بالمثل.[30]

و طبقا لنص المادتين 04 و05 من القانون 04/09 فلا يجوز إجراء عملية التفتيش إلا بإدن مكتوب من السلطة القضائية المختصة.

ثانيا: طريقة التعامل مع الادلة التقنية المضبوطة

حدد المشرع الجزائري من خلال القانون 04/09 في المواد السادسة والسابعة و الثامنة، حيث تنص الثامنة على المحافظة على سرية المعلومات التي تم ضبطها، و هو

إلتزام يقع السلطة التي تباشر التحقيق حيث لابد لها من اتخاد كل الاجراءات اللازمة التي من شأنها منع الاشخاص غير المسموح لهم قانونا بالاطلاع عليها، و تكليف شخص مؤهل للقيام بدلك.

كما يعاقب كل من يستعمل تلك المعلومات المتحصل عليها من التفتيش في غير الأغراض التي ضبطت من أجلها و هدا تطبيقا للمادة 09 من القانون 04/09 و دلك لما قد تتضمنه من أسرار خاصة بأشخاص آخرين.

ثالثا: محضر التفتيش

القاعدة المسلم بها أن أعمال التحقيق جميعا ينبغي كتابتها، والكتابة تشمل جميع إجراءات التحقيق سواء كانت معاينة، سماع شهود أو إجراءات التفتيش وتنص المادة 68 فقرة 2 من ق إ ج "وتحرر نسخة عن هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل".

وبقصد حماية الحريات الفردية والمنع من التعسف، ألزم المشرع الجزائري ضباط الشرطة القضائية المنتدبين للتحقيق تحرير المحاضر المثبتة لما قاموا به من إجراءات مبينين فيها الإجراءات، والمحضر بشكل عام له مجموعة من البيانات الواجب توافرها إضافة إلى الأشخاص المؤهلين لتحريره[31].

رابعا:وقت أو ميعاد إجراء التفتيش

حرصا على تضييق نطاق ناق الإعتداء على الحرية الفردية و حرمة المسكن، تحرص التشريعات الإجرائية على تحديد وقت معين يتم فيه إجراء التفتيش في حين تترك بعض التشريعات الإجرائية أمر تحديد دلك الوقت للقائم بالتفتيش.[32]

المقصود به هو الوقت من الزمن الذي يسمح فيه بتنفيذ التفتيش فلقد حظر المشرع الجزائري القيام بتفتيش المساكن في أوقات معينة، إذ نصت المادة47 فقرة 01 ق إ ج "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحا ولا بعد الثامنة مساءا" ، ويستفاد من هذا النص أن المشرع الجزائري اعتبر وقت الليل الفترة الواقعة قبل الساعة الخامسة صباحا أو بعد الساعة الثامنة مساءا وهذا يعني أن المشرع حظر التفتيش ليلا، وتبعا لذاك فإن الأصل في النظام الإجرائي الجزائري هو عدم دخول المساكن وتفتيشها أثناء الليل، ولا يجوز الخروج عن هدا الأصل مبدئيا، فإن كان من الضروري عدم الانتظار إلى وقت النهار خشية هروب المتهم أو تهريب الأدلة الجريمة

المطلوب ضبطها وجب الاكتفاء بمحاصرة المسكن ومراقبته من الخارج حتى وصول الوقت الجائز قانونا مباشرة التفتيش فيه، وهذا ما أكدت عليه المادة 122 في فقرتها الأولى والثانية من قانون الإجراءات الجزائية على انه: "لا يجوز للمكلف بتنفيذ أمر القبض أن يدخل مسكن أي مواطن قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا وله أن يصطحب معه قوة كافية لكي لا يتمكن المتهم من الإفلات من سلطة القانون".

إذن القاعدة انه لا يجوز مباشرة التفتيش خارج الأوقات المسموح بها قانونا ، لكن استثناءا حدد المشرع الجزائري بعض الحالات على سبيل الحصر، أجاز فيها لضابط الشرطة القضائية الخروج عن القاعدة و منه يجوز لهم التفتيش في أي وقت حتى ليلا وتتمثل في عد حالات منها الجرائم المستحدثة حيث نصت المادة 47 بعد تعديلها بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006على" :عندما يتعلق الأمر بجرائم المخدرات أو جريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال أو الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص."[33]

الخـــاتمة:

وبناءً على ما تقدم و باعتبار أن التفتيش من أهم إجراءات جمع الأدلة في مجال البيئة الرقمية و فضلاً عما يثيره هذا الأخير من من عقبات تواجه الأجهزة القضائية والأمنية ذلك لسبب هام جدا و هو ارتكاب الجريمة بطرق تقنية معلوماتية في تطور متجدد، جعل بمن هم قائمون على مكافحة هذا النوع من الجريمة في تحدي كبير لهؤلاء المجرمين. و في هذا السياق يجدر بنا أن نشير إلى أنه هناك العديد من الآليات و الاستراتيجيات المتبعة لتأهيل رجال التحقيق في البيئة الإلكترونية على الصعيدين الداخلي و الدولي ليكونوا أكثر كفاءة ليتمكنوا من أداء مهامهم على أكمل وجه و ذلك عن طريق تدريبهم على كل ما هو جديد في المجال المعلوماتي، إضافة إلى أنه يشترط في المحقق الجنائي في الجريمة المعلوماتية المرتكبة في البيئة الرقمية مجموعة من المؤهلات الفنية و تتعلق عموما

بكيفية التعامل مع هده الأخيرة، و ليتمكن من ذلك لابد له من الالمام بعلم الكمبيوتر و الأدلة الرقمية أي الاستخدام الأمثل للحاسب الآلي و نظمه و برامجه و

وسائل الاتصال الالكترونية الرقمية، و يجب أن يتحقق لديه التوازن الفكري الالكتروني

باستمرار القراءة في مجال التقنية الالكترونية الرقمية و شبكة الأنترنت و التعليم و التدريب والخبرة، لأنها تحقق لصاحبها التفوق.

الهوامش:

1. الشحات ابراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية و القوانين الوضعية، دار الفكر الجامعي، الأسكندرية، الطبعة الاولى، 2011، ص 196.
2. علي عدنان الفيل، ، اجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، الناشر المكتب الجامعي الحديث، 2012 بدون طبعة،ص 39، عن conseil de l eurpe , problemes de procedure penale lies a la technogie de l information , recommendation n .r(95) 13 et expose des motif . ed. conceil de l europe 1996 , p 28.
3. علي عدنان الفيل، المرجع نفسه ص 39.
4. علي عدنان الفيل، مرجع سابق، ص 39.
5. القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها المؤرخ في 5 أوت 2009 الصادر في الجريدة الرسمية العدد 47. Hollande alain, de bellefonds l'inantxavier, op. cit, page 250.
6. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الالي ، دار الجامعة الجديدة للنشر الاسكندرية، بدون طبعة، سنة النشر 2007 ، ص 86.
7. محمد خليفة، مرجع سابق، ص 86- 87 .
8. المعلومات هي المعنى المستخلص من المعطيات بعد معالجتها آليا و البرنامج هو المستودع الذي يتم فيه معالجة هذه المعطيات.

9. http://www.startimes.com/ بتاريخ 2014/10/23.
10. علي عدنان الفيل، مرجع سابق، ص 41.
11. علي عدنان الفيل، مرجع سابق،ص 41.
12. عبد الفتاح بيومي حجازي، المرجع السابق، ص 653.
13. عبد الفتاح بيومي حجازي، المرجع نفسه، ص 657.
14. علي عدنان الفيل، المرجع السابق،ص 42.
15. علي عدنان الفيل، المرجع نفسه، ص 42.
16. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية بيروت، لبنان، الطبعة الأولى، 2012ص 398.
17. هلالي عبد الله، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1998، ص 375.
18. عاشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الأزاريطة، بدون طبعة، سنة النشر 2010، ص 93 و 94.
19. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، بدون طبعة، سنة النشر 2007، ص 300.
20. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار النهضة العربية الاسكندرية، الطبعة الاولى، 2009، ، ص 655.
21. عبد الفتاح بيومي حجازي، المرجع نفسه، ص 656.
22. عبد الفتاح بيومي حجازي، المرجع السابق، ص 656 و 657 .
23. حد تلك الخطورة بأن تكون العقوبة المقررة لهاالحبس من سنتين أو أكثر على أن لا تزيد المراقبة على أربعة أشهر في جميع الأحوال.
24. قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري و المقارن، منشأة المعارف الأسكندرية، بدون طبعة، سنة النشر 2005، ص 53.

25. هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، ص 121.

26. قدري عبد الفتاح الشهاوي، مرجع سابق، ص 110.

27. خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت، دار الثاقة للنشر و التوزيع، عمان الاردن، الطبعة الأولى، 2011، ص 154، عن صالح البريري، دور الشرطة في مكافحة جرائم الأنترنت، مؤتمر الجوانب القانونية و الأمنية، للعمليات الالكترونية، دبي 2003، ص 392.

28. http://www.djelfa.info يوم 2015/06/21.

29. أورد المشرع الجزائري تعريف المسكن في نص المادة 355 من قانون العقوبات: "يعد منزلا مسكونا كل مبنى أو دار أو غرفة أو خيمة أو كشك ولو متنقل متى كان معدا للسكن وإن لم يكن مسكونا ووقتذاك وكافة توابعه مثل الأحواش وحظائر الدواجن ومخازن الغلال والإسطبلات والمباني التي توجد بداخلها مهما كان استعمالها حتى لو كانت محاطة بسياج خاص داخل السياج أو السور."

30. المسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي و التكنولوجي –دراسة مقارنة رسالة دكتوراه جامعة سيدي بلعباس، ، ص 309.

31. http://www.djelfa.info يوم 2015/06/26.

32. رشيدة بوكر، مرجع سابق، ص 415.

33. http://www.djelfa.info يوم 2015/06/26.