تفتيش المنظومات المعلوماتية في القانون الجزائري

بقلم

د/ رضا هميسي

كلية الحقوق والعلوم السياسية
جامعة ورقلة

الملخص

يعتبر التفتيش عن الجريمة المعلوماتية في البيئة الرقمية من أصعب أنواع التفتيش، ويرجع ذلك إلى التطور المذهل في تكنولوجيا الإعلام والاتصال، وإن كان ذلك يخضع للقواعد المتعارف عليها في التفتيش طبقا لقانون الإجراءات الجزائية، إلا أنه يتميز بخصوصية معينة نظرا لطبيعة الجريمة المستهدفة وطبيعة مرتكبيها، فضلا عن مسرح الجريمة الذي هو عبارة عن بيئة افتراضية.

فأدلة الجريمة المبحوث عنها هي أدلة معلوماتية وهي عبارة عن بيانات مخزنة في حواسيب وأجهزة إلكترونية قد تتواجد في أماكن عدة سواء في الداخل أو في الخارج، ومن ثم فإن البحث عنها واكتشافها عملية بالغة التعقيد والصعوبة وتتطلب مهارة فنية وكفاءة عاليتين من لدن الجهات المباشرة لها.

ويبحث هذا المقال في مفهوم التفتيش في الأنظمة المعلوماتية من خلال إبراز خصائصه وشروطه الموضوعية والشكلية وكذلك متطلبات تنفيذه وآثاره من حيث الحجز على المعطيات المعلوماتية ومنع الوصول إليها.

Résumé:

La perquisition de la cybercriminalité dans l'environnement numérique est une recherche difficile à mener et cela revient au développement étonnant des technologies de l'information et de communication et ce, malgré la soumission de ce domaine aux même règles de perquisition en conformité avec le Code de Procédure Pénale et malgré sa particularité quant à la nature et du crime, et de son auteur et de l'environnement, généralement virtuel.

Par ailleurs, les preuves, qui attestent du crime, ce sont que des données prises à des ordinateurs aussi bien à l'intérieur qu'à l'extérieur du pays. D'ou la complexité des processus de la recherche et de la perquisition qui exigent des compétences certains et de haute efficacité de ceux qui doivent mener la perquisition.

Enfin, cet article vise à la clarification de la notion de perquisition liée à l'environnement informatique à travers la mise en évidence de ces caractéristiques, de ses moyens matériels et formels ainsi que sa mise en œuvre, et ces effets et ce, sans omettre les questions liées à la saisie de données informatiques et à et l'interdiction d'accès aux données.

مقدمة:

التفتيش هو إجراء من الإجراءات التي تهدف إلى البحث عن ملابسات الجريمة وهو إجراء يمس حقوق الإنسان كونه يتعلق بخصوصيته وبسره وبحرمة مسكنه، والتفتيش هو الوسيلة التي يتم بموجبها كشف الحقيقة وضبط الأدلة الجنائية على الجريمة وصحة إسنادها إلى الجاني؛ لذلك فقد أحاطه المشرع بعدة إجراءات وضمانات.

ومع تطور تكنولوجيا الإعلام والاتصال ظهر نوع جديد من الإجرام المستحدث؛ و نعني به الجرائم التي ترتكب عن طريق تقنية المعلومات وهو ما سمي بالجرائم المعلوماتية أو الإلكترونية.[1] وتختلف هذه الجرائم اختلافاً كبيراً عن غيرها من الجرائم التقليدية في وسائل ارتكابها وفي طبيعة الأشخاص الذين يقومون بها وكذلك تختلف عنها في مسرح الجريمة.

وبالتالي فإن مشكلة البحث عن الجريمة في البيئة الالكترونية تنبع من

طبيعة هذا النوع المستحدث من الإجرام فهي جريمة تتعلق ببيانات معالجة الكترونيا وكيانات غير مادية يصعب الكشف عنها، ويصعب في غالب الأحيان جمع الأدلة بشأنها والتفتيش عنها بالطرق المألوفة في الجريمة التقليدية. وتزداد المهمة صعوبة عندما يتعلق الأمر بتفتيش بيانات وأنظمة معلوماتية موجودة خارج النطاق الوطني، لأن الأمر قد يصطدم بسيادة دولة أخرى؛ في الحالة التي يلجأ فيها بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج. كما يُثير التفتيش في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد وبين تحقيق الفاعلية أثناء عملية التحقيق في كشف الجريمة وضبط فاعليها وتقديمهم للمحاكمة.

وبالتالي فإن هذه المقال سيتعرض إلى مفهوم التفتيش في المنظومات المعلوماتية، وإلى شروط إجرائه وكيفية تنفيذه وبحث الآثار المترتبة عنه بحسب التشريع الجزائري.

وسيتم نتناول كل ذلك وفقا للنصوص التي جاء بها القانون رقم 09- 04 المتضمن القواعد العامة الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فضلا عن أحكام قانون الإجراءات الجزائية.

المبحث الأول

مفهوم التفتيش

المطلب الأول: تعريفه

التفتيش بمعناه القانوني هو إجراء من إجراءات التحقيق، ووظيفته البحث عن أدلة الجريمة. فهو ليس دليلا بذاته وإنما هو وسيلة للحصول على دليل،

ولم تتضمن مختلف التشريعات تعريفاً للتفتيش مما يترك المجال للفقه والقضاء للتطرق إلى هذه المسألة. وقد وضع الفقه عدة تعريفات لعملية التفتيش؛ فقد عرفه البعض بأنه إجراء من إجراءات التحقيق، تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه.[2]

كما عرفه البعض الآخر بأنه: " إجراء من إجراءات التحقيق فهو ليس عملا إداريا من أعمال الضبط الإداري وإنما هو عمل من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين ".[3]

وهناك من يعرفه:" التفتيش هو البحث عن مكنون سر الأفراد على دليل للجريمة المرتكبة أو البحث عن الدليل وهو إجراء من إجراءات التحقيق الابتدائي الذي يخوله القانون لقاضي التحقيق أصلا واستثناء لضباط الشرطة القضائية" [4]

ومنهم من عرفه بأنه البحث والتحري داخل سر الأفراد عن أدلة تقيد لإثبات جريمة معنية ارتكبت فعلا وهو الإجراء من الإجراءات التحقيق.[5]

أما تفتيش الأنظمة المعلوماتية، فقد عرفه بعض الفقهاء بأنه البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو هو البحث الدقيق والإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكناً أو جهاز حاسوب أو أنظمة أو الانترنت"[6]. وتفتيش النظم المعلوماتية هو إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، ويستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب، والمعطيات المعلوماتية

والاتصالات الإلكترونية.

ويقصد بالمنظومة المعلوماتية في التشريع الجزائري" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ برنامج معين ".[7]

وإجمالا فإن التفتيش، سواء أكان في شكله التقليدي أو الحديث، هو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة، وعن أشياء تفيد في معرفتها ونسبتها إلى المتهم.

المطلب الثاني: خصائصه

من خلال التعريف الذي وضعه الفقه للتفتيش على نظم المعلوماتية يتبين أنه يتميز عن غيره من الإجراءات التي تهدف إلى إثبات الجريمة كالشهود والخبرة والمعاينة بعدة خصائص أهمها:

- إن التفتيش في المنظومات المعلوماتية شأنه في ذلك شأن التفتيش بشكل عام؛ فيه تعرض قانوني لحرية المتهم الشخصية أو لحرمة مسكنة بغير إرادته ورغما عنه. وفيه اعتداء على أسراره وعلى حياته.

- يعتبر التفتيش وسيلة من وسائل التحري عن مختلف الأدلة المعنوية والمادية للجريمة؛ يهدف إلى جمع الأدلة التي تؤدي إلى كشف الحقيقة وضبطها والوصول إلى دليل حاسم، والوصول إلى الدليل في التحقيق الجنائي، إذ لا يدان شخص ولا يجازى دون دليل. [8]

- كما يعتبر التفتيش قيدا على حرمة وحصانة الشخص وفيه مساس بحق الشخص في السر، فهو اعتداء على أسراره سواء الموجودة على مستوى

نظامه المعلوماتي أو جهاز حاسوبه أو حتى بريده الالكتروني وفيه مساس بقاعدة حرمة الشخص في ذاته أو في رسائله، ويترتب على كون التفتيش يتضمن مساسا بحق السر أنه يخرج عن نطاقه كل إجراء لا يمس سرا لأحد فلا يعد تفتيشاً الإجراء الذي يمس شيئا مكشوفا ظاهرا للعيان.

- يسمح التفتيش أو البحث في الشبكات الإلكترونية عن الجرائم المعلوماتية؛ باستخدام قواعد وأساليب التحقيق الجنائي الفني المعروفة، بتقنيات خاصة، فريدة أو غير مسبوقة. فهو بعكس التفتيش في معناه التقليدي (الكلاسيكي) لا يتطلب - في كثير من الأحيان - الانتقال إلى مساكن الأشخاص الذين يشتبه في أنهم ساهموا في الجريمة، وإنما قد يتم عن بعد أو ما يعرف بالتفتيش على الخط perquisition en ligne كما تتطلب فيمن يباشر تحقيقها أن يكون متخصصا في التحقيق الجنائي ومعالجة البيانات والمراجعة والحسابات.[9]

- يتميز تفتيش المنظومات المعلوماتية أن المحتوى المعلوماتي يتميز بطابعه اللامادي وتجاوزه الحدود الوطنية والفورية وسهولة إتلافه أو مسحه أو تغييره في أوقات قياسية. فهو تفتيش للفضاء الافتراضي وأوعية التخزين وتفتيش للبيانات التي يحفظها جهاز الحاسوب.[10]

-كما يتميز التفتيش في الفضاء الرقمي بأنه عملية معقدة ومتشابكة؛ تقتضي من القائمين عليها أن يكون على دراية واسعة وكفاءة عالية في البحث عن المعلومة، وفي معالجة المعطيات وتحليلها وفك طلاسمها، ويزداد الأمر صعوبة في ظل التزايد المتسارع في حجم القرص الصلب للحواسيب، وما ينجم عنه من وجود كم هائل من الملفات المراد فك رموزها و تحليلها.[11]

- إن تفتيش الأنظمة المعلوماتية فيه مساس خطير بالحياة الخاصة، كونه

يتضمن وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وفيه تسجيل وتجميع آني وفوري لهذه الاتصالات، وكذا القيام بعمليات التفتيش والحجز داخل المنظومات المعلوماتية. ولعل المثال الواضح الآثار التي يتركها متصفح الإنترنت، والتي من خلالها يمكن تجميع كم هائل عن حياته الخاصة[12]، من قبيل صفحات الويب التي اطلع عليها، ووقت دخوله إلى الشبكة، ومدة بقائه فيها، والأشخاص الذين تواصل معهم، والملفات التي تبادلها، فضلا عن معرفة محتوى صندوق بريده الإلكتروني. ذلك أن كثيرا من المعطيات السلوكية التي يدونها مستعمل الشبكة العنكبوتية تترك آثار عليها[13]، وفي حالة إساءة استعمال هذه البيانات والمعلومات، أو توجيهها إلى العنوان الخطأ؛ فإنه يمكن استغلالها من قبل الجهات والهيئات المهتمة بالبحث عن سلوك المستخدمين، خاصة إذا علمنا أن جمعها والبحث عنها يتم دون علم أو رضا ذلك المستخدم.[14]

المبحث الثاني
شروط إجراء التفتيش وتنفيذه

يقتضي التفتيش أو الضبط أو المصادرة في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد، وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية، وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليها والتحقيق معهم وتقديمهم للمحاكمة.

والسؤال الذي يطرح نفسه هو: هل يمكن تطبيق القواعد الإجرائية في التفتيش وفقا للإجراءات المألوفة ؟ أم أن هناك إجراءات خاصة بالتفتيش في البيئة الرقمية؟ كما أن مسألة تنفيذ التفتيش تتطلب جملة من الترتيبات ينبغي

مراعاتها، سواء من حيث القائم به أو من حيث الإجراءات المتبعة. وسنتولى توضيح شروط التفتيش الموضوعية والشكلية فضلا عن بيان كيفيه تنفيذه.

المطلب الأول: الشروط الموضوعية لتفتيش نظم المعلوماتية

ينبغي أن يجرى التفتيش وفقاً لشروط موضوعية معينة، وعلى الجهة القائمة به أن تراعيها؛ وإلا كان عملها خالياً من أي أثر قانوني وتتمثل هذه الشروط في سبب التفتيش والمحل المراد تفتيشه، وسنتولى بيان ذلك فيما يأتي:

الفرع الأول: سبب تفتيش نظم المعلوماتية

إن التفتيش بوصفه إجراء من إجراءات التحقيق يكون عادة عند وقوع جريمة من الجرائم وإسنادها إلى شخص معين سواء بصفته مرتكباً مباشراً أو مساهماً فيها أو توافر أدلة أو قرائن على وجود أشياء تفيد في إثبات الجريمة أو الكشف عنها. ويقصد بالسبب من التفتيش هو الحصول على الدليل في تحقيق قائم بقصد كشف الحقيقة .

ويفترض أن التفتيش يجب أن يستند عند إجرائه إلى مبررات توضح السبب والهدف منه، وتتمثل هذه المبررات فيما يأتي:

1 ـ وقوع جريمة معلوماتية: يتعين لإجراء عملية تفتيش المنظومات المعلوماتية أن تكون الجرائم قد وقعت فعلاً يتعين أن تكون قد وقعت فعلا جريمة معلوماتية معينة، فلا يمكن إجراء التفتيش من أجل جريمة محتملة الوقوع حتى ولو كانت هناك مؤشرات على جدية احتمال وقوعها[15] وهو شرط مستقى من طبيعة التفتيش باعتباره عملاً من أعمال التحقيق الابتدائي.[16]

وفي مفهوم القانون الجزائري فإننا نكون بصدد جريمة معلوماتية[17] أو إحدى الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؛ جرائم المساس بأنظمة المعالجة الآلية للمعطيات[18] وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية[19] أو نظام للاتصالات الإلكترونية، أو أي جريمة ترتكب عن طريق وسائل الإعلام الإلكترونية[20] أو أية وسيلة اتصال أخرى كالهاتف النقال، أو آلة تصوير رقمية، أو جهاز تسجيل.

2 ـ توجيه التهمة إلى شخص وإسنادها إليه: يتعين للقيام بإجراء التفتيش بالإضافة إلى وقوع الجريمة أن يكون هناك اتهام موجهه إلى شخص أو عدة أشخاص سواء بصفته فاعلاً أو شريكاً أو حائزاً لأشياء تتعلق بالجريمة من جرائم تكنولوجيا الإعلام والاتصال. معنى ذلك أن تتوافر في حق المراد تفتيشه دلائل قوية وكافية تدعو إلى الاعتقاد بأنه ساهم في ارتكاب الجريمة المعلوماتية، ولا يقتصر الأمر على مجرد تجميع القرائن والأدلة التي تفيد وقوع الجريمة ونسبتها إلى فاعلها، بل يجب أن تتضمن كذلك المعلومات والقرائن التي تعزز موقف المشتبه فيه وتنفي عنه ارتكابه للجريمة.[21]

كما يجب أن يكون الاتهام جدياً ومبنياً على أدلة وقرائن قانونية وعليه يتعين على الجهة التي تمنح الإذن بالتفتيش أن تراقب هذه الإجراءات.فالتفتيش لا يجوز إجراؤه إلا إذا كان هناك احتمال للعثور على دليل من ورائه[22]؛ فالاشتباه مبناه الظن، فلا يكفي مجرد الظن أو الاشتباه بل ينبغي توفر بعض الأدلة والقرائن المعقولة و الجدية التي تحمل على الاعتقاد بوقوع جريمة معلوماتية ونسبتها إلى المتهم المراد تفتيش منظومته المعلوماتية أو نظام اتصالاته الإلكترونية.

الفرع الثاني: محل تفتيش نظم المعلوماتية

يقع التفتيش دائما على مستودع السر الذي يحتفظ به المرء بالأشياء المادية واللامادية التي تتضمن سره، وينصب محل تفتيش نظم المعلوماتية على كل ماله صلة بهذه النظم من برامج وآلات وأجهزة الحاسوب وغيرها من الأجهزة الإلكترونية؛ ويكون التفتيش إما للأشخاص وإما للمساكن التي توجد فيها تلك الأجهزة أو الشبكات المعلوماتية.

وقد يرد التفتيش على المكونات المادية للحاسب الآلي(Hardware) وملحقاته، وهذه لا خلاف يُذكر حول خضوعها للتفتيش والضبط طبقاً لقواعد قانون الإجراءات الجزائية، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية ، وذلك تبعاً للمكان أو الحيز الموجودة فيه[23] ومن ثُم ، إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن ؛ إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً ، والعكس صحيح . وفي حال وجودها في مكان عام فيحكمها ما يحكم هذا المكان من أحكام ، وهلم جرا. [24] أما إذا كانت في حوزة شخص خارج مسكنه، فإن تفتيشه عندئذٍ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته، ويستوي أن يكون الحائز هو مالك الجهاز أم سواه .

ومن ناحية أخرى، وهو موضوع هذا المقال، إن التفتيش وما في حكمه قد يرد على الجانب المنطقي للحاسوب(Software)، المتمثل في المعلومات والبيانات المعالجة والمخزنة إلكترونياً، وهي محل جدل كبير حول صلاحيتها لأن تكون موضوعاً للتفتيش والضبط من عدمها[25]؛ ومكمن هذا الجدل هو صعوبة تطبيق القواعد العامة التقليدية للقانون. فالجرائم

التقليدية ضد الأموال يقصد بها حماية الأفعال المادية في حين أن استعمال المعلوماتية يشكل أموالاً غير مادية.[26] لذلك فإنه يسهل اكتشاف أمر الجرائم التي ترتكب على الكيانات المادية للحاسوب وضبطها، إما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية.[27]

وهكذا فإن محل التفتيش يشمل المكونات المادية والمعنوية للنظم المعلوماتية؛ وهو يمتد إلى البيانات والمعلومات والبرمجيات المخزنة في الحواسيب فضلا عن الأقراص والأشرطة، وغيره من وسائل الاتصال الحديثة كالهواتف الخلوية، والهواتف الذكية، وشرائح الهاتف (carte SIM)، وبطاقات الذكراة، وآلالات التصوير الرقمية.كما قد يرد التفتيش أيضا على بطاقات فك التفشير الخاصة بالتلفزيون الرقمي.[28]

ويميز المشرع الجزائري في تفتيش المنظومات المعلوماتية بين ما إذا كانت المنظومة متصلة بنظام آخر داخل التراب الجزائري، أو كانت المنظومة متصلة بمنظومة معلوماتية تقع خارج الإقليم الوطني.[29]

الحالة الأولى: إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، ويمكن الولوج إليها انطلاقا من المنظومة الأولى، فإنه يجوز تفتيش هذه المنظومة بسرعة دون استصدار إذن قضائي، وإنما يكفي إعلام السلطة القضائية المختصة بذلك (المادة 5 ف 2 من قانون 04/09)، ولعل انتظار صدور الإذن من السلطات المختصة قد يأخذ بعض الوقت ما قد يؤدي إلى تلاشي الدليل واندثاره في وقت قياسي كأن يقوم المشتبه فيه بمحوه وإتلافه[30] إذ يكفي الضغط على مكان معين لإنهاء وجود المعلومة، ومن ثم تتبخر عناصر الإثبات ما يشكل صعوبة في إيجاد دليل حاسم. لذلك

فإن استصدار إذن قضائي في مثل هذه الحالات لا طائل منه.

الحالة الثانية: وهي الحالة التي تكون فيها المعطيات المراد تفتيشها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني الجزائري، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، فإنه يجوز للسلطات المختصة وكذا ضباط الشرطة القضائية تفتيش هذه المنظومة، ولا يعد ذلك أبدا انتهاكاً لسيادة دولة أخرى، طالما أن مقتضيات التعاون الدولي تستدعي محاصرة هذه الجرائم؛ وطلب مساعدة سلطات الدول الأجنبية، طالما أن ذلك يتم في إطار الاتفاقات الدولية الثنائية والمتعددة الأطراف التي أبرمتها الجزائر، وطبقا لمبادئ القانون الدولي والعلاقات الودية بين الدول التي تنص على مبدأ المعاملة بالمثل. (المادة 5 ف 3 من قانون 04/09)

المطلب الثاني: الشروط الشكلية لتفتيش النظم المعلوماتية

يتطلب القانون شروطا شكلية معينة ينبغي مراعاتها عند مباشرة التفتيش، والغرض من تلك الإجراءات إحاطة المتهم بضمانات لحماية حريته، ومن المتعارف عليه أن الإجراءات الشكلية لأي إجراء ومنها التفتيش لا ترمي إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لتجميع الأدلة بل تهدف إلى حماية الحريات الفردية والحقوق الخاصة للأفراد وضمان صيانتها[31].

الفرع الأول: أن يجري التفتيش بحضور أشخاص يحددهم القانون

تشترط معظم التشريعات للقيام بعملية التفتيش حضور أشخاص معينين يحددهم المشرع، وتختلف هذه الأشخاص حسب كل تشريع فهناك من يشترط ضرورة حضور المتهم أومن ينوبه أو صاحب المسكن أو شاهدين

يحددهم القائم بالتفتيش أو من يأمر به ولحضور هؤلاء الأشخاص أهمية مزدوجة؛ فهو من جهة يعد بمثابة رقابة على القائم به، ومن جهة ثانية يوفر جواً من الطمأنينة والثقة لدى من يجرى تفتيش مسكنة.

وبالنسبة للمشرع الجزائري فقد اشترط لإجراء عملية التفتيش في المعطيات المخزنة في المنظومة المعلوماتية، إعمال قاعدة الحضور تطبيقا لأحكام المادة 05 من القانون 04/09 التي تحيل إلى الأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية؛ ومن ثم فإنه يشترط ضرورة حضور صاحب مسكن المشتبه في ارتكابه الجريمة أو صاحب مسكن شخص من الغير يحوز أوراقاً أو أشياء تتعلق بالجريمة لعملية التفتيش أو من ينوبهما أو حضور شاهدين إذا تعذر حضورهما بحسب ما نصت عليه أحكام المادة 45 من ق.إ.ج.

ومما سبق ذكره، يمكننا القول أنه في حال ارتكاب أحد الجرائم المتصلة بتكنولوجيا الإعلام والاتصال يسمح إذن التفتيش للشخص المكلف بتنفيذه سلطة تفتيش المكان للبحث عن الأشياء، وأيضاً البحث في داخل النظام المعلوماتي الموجود في المكان المحدد للحصول على معلومات يمكن أن تستخدم كدليل على ارتكاب الجريمة وضبط هذه المعلومات وحفظها.

الفرع الثاني: أن يتم تحرير محضر خاص بعملية التفتيش

لما كان التفتيش عملا من أعمال التحقيق فإنه يتوجب تدوينه، ويكون ذلك بإعداد محضر يُثبت فيه ما تم من إجراءات بشأنه وما أسفر عنه من أدلة، ويجب أن يتضمن المحضر المحرر عن عملية التفتيش وصف العملية من بدايتها إلى نهايتها، مع تبيان وقت بداية العملية ونهايتها وكذا جرد

الأشياء وضبطها التي يتم حجزها أثناء عملية التفتيش. ويجب أن يمضى هذا المحضر من طرف القائم بالتفتيش ومن الأشخاص الذين يحدد القانون ضرورة إمضائهم لذلك المحضر.

ويشترط القانون الجزائري حضور كاتب أثناء أجراء التفتيش طبقا لنص المادة 79 من ق.إ.ج على قاضي التحقيق أثناء قيامه بعملية التفتيش أن يصطحب معه كاتب ويتعين عليه تحرير محضر يمضى من طرفه ومن طرف الكاتب.

ولا تشترط التشريعات عادة شكلا معينا لمحاضر التفتيش وإنما تشترط فيها أن تتضمن بيانات معينة تختلف من تشريع إلى أخر كضرورة إمضائها من طرف القائم بالتفتيش والكاتب أحيانا.

وفيما يخص شكل المحضر فإن المشرع الجزائري لم يشترط شكلا خاصا في محضر التفتيش، وبالتالي فهو لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر بشكل عام أي يجب أن يتضمن كافة البيانات المتعلقة بعملية التفتيش و بيان صفة القائم بالتفتيش ومن حضر التفتيش.

ويختلف الأمر عما إذا كان التفتيش تم من طرف ضابط الشرطة القضائية الذي يخضع للقواعد العامة التي يجب أن تتضمنها المحاضر المحررة من طرف الضبطية القضائية؛ عنه إذا كان قد أجرى من طرف قاضي التحقيق الذي يشترط أن يكون مصحوبا بكاتب وأن يمضي المحضر من الكاتب وإلا كان باطلا.

ونرى أن تحرير محضر عن عملية التفتيش هي لازمة وذلك لتمكين الجهات القضائية المختصة بنظر مدى احترام الإجراءات المتطلبة في عملية

التفتيش ومن ثم بسط رقابتها على شرعية الإجراء، لذلك ففي حالة عدم إتباع هذه المتطلبات فقد رتب المشرع الجزائري البطلان على عدم احترام الإجراءات المنصوص عليها في المواد 48 من ق.ا.ج وأنه من المعلوم أن بطلان إجراءات التفتيش يؤدي إلى بطلان واستبعاد الدليل المحصل من هذه العملية .

المطلب الثالث: إجراءات تنفيذ تفتيش نظم المعلوماتية

حتى يكون التفتيش صحيحا ومنتجا لأثره، يجب أن يجرى من طرف ذي صفة، وإتباع إجراءات محددة حتى لا يخرج عن إطاره المحدد له وغايته وكذا يجب أن يتم في الوقت المحدد له قانونا .

الفرع الأول: صفة القائم بالتفتيش ومساعديه

لا يتم التفتيش من طرف أي شخص كان بل يتعين أن يتم من قبل الأشخاص الذين يحددهم القانون ويعطيهم صلاحيات القيام بإجرائه. ويختلف هذا الأمر من دولة إلى أخرى باختلاف النصوص الإجرائية المنظمة لعملية التفتيش؛ فهناك من يشترط أن يقوم به المدعى العام أو قاضي التحقيق أو ضابط الشرطة القضائية، و هناك من التشريعات من تعطى هذه الصلاحية لجميع هؤلاء. أما بالنسبة للمشرع الجزائري فقد أعطى صلاحية إجراء التفتيش إلى السلطات القضائية: النيابة أو التحقيق وكذا ضباط الشرطة القضائية طبقا لنص المادة 5 من قانون 09/ 04.

ونظرا لخصوصيات جرائم نظم المعلومات، وتعقدها وتشابكها، فضلا عن صعوبة البحث عن الدليل، وصعوبة القبض على مرتكبيها؛ فإن هذا يؤدي إلى مراعاة هذه الخصوصيات عند القيام بإجراء التفتيش على نظم

المعلومات، ويتعين مراعاة الدقة في التعامل مع الأجهزة والبرامج الموجودة عليها وأخذ الاحتياطات اللازمة[32].ولأجل ذلك فإن الاستعانة بأهل الاختصاص هي ضرورة ملحة تقتضيها ظروف الحال.

وبحسب التشريع الجزائري فإنه يمكن للسلطات المكلفة بالتفتيش أن تأمر كل شخص يفترض أن له دراية خاصة بالأنظمة المعلوماتية موضوع التفتيش أو بالتدابير المتخذة لحماية المعطيات المعلومات المخزنة فيها، بغرض مساعدتها وتزويدها بكافة المعلومات الضرورية لإنجاز مهمتها (المادة 5 الفقرة 4 من قانون 09/ 04)، وتتمثل مهمة الشخص - الخبير- في تقديم التوضيحات الكافية حول كيفية تشغيل هذه الأنظمة وطريقة النفاذ إليها أو إلى المعطيات المخزنة أو المعالجة أو المنقولة في شكل يمكن فهمه وإدراكه.[33]

كما أن أمر التسخير المنصوص عليه في الفقرة 4 من المادة 5، يمتد ليشمل أيضا مقدمي الخدمات[34] الذين يشترط عليهم القانون الالتزام بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية. ومناط هذا الالتزام هو المسؤولية التي يتحملها مقدم خدمات "انترنت" عن محتوى الصفحات والمعطيات التي يستخرجها ويأويها.[35]

وتتمثل المساعدة المطلوبة في جمع المعطيات وتسجيلها التي لها علاقة بمضمون الاتصالات في حينها ووضعها تحت تصرف السلطات المختصة بالتحقيق (المادة 10 فقرة 2)، وهو ما يعبر عنه بـ" الجمع الحيني للمعطيات الالكترونية".[36] كما يتعين على مقدمي الخدمات القيام بحفظ هذه المعطيات[37] لفترة لا تزيد عن سنة ابتداء من تاريخ التسجيل[38].

كما أن هناك جهة أخرى تضطلع بمهمة مساعدة السلطات القضائية

ومصالح الشرطة القضائية في التحريات التي تجريها؛ ونعني بها " الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال "[39]، وذلك عن طريق تجميع المعلومات وإنجاز الخبرات.

الفرع الثاني: ميعاد تنفيذ التفتيش

لقد اختلفت التشريعات في تحديد الوقت الذي يتم فيه إجراء التفتيش فهناك من التشريع ما يسمح بالتفتيش في أي وقت من الأوقات نهارا أو ليلا وهناك من يسمح به نهار فقط، وهناك من يسمح به نهارا وليلا استثناء، أما المشرع الجزائري قد أباح إجراء التفتيش من الخامسة صباحا إلى الثامنة ليلا كقاعدة عامة ما عدا في الحالات الاستثنائية طبق للمادة 47 ق.إ.ج .

ونظرا لطبيعة المعطيات المعلوماتية وسرعة إتلافها وفسخها أو تعديلها بكل سهولة،كما قدمنا، خاصة إذا تناهى إلى علم المشتبه به بوجود تفتيش، فيقوم بكل سهولة بمسح الدليل أو تحويله؛ لذلك فإن أغلب الفقهاء يرون بأنه يستلزم في ما يخص التفتيش على نظام المعلوماتية ترك إجرائه في أي وقت من أوقات النهار أو الليل وذلك حسب ما تقدره الجهة القائمة بالتحقيق. وقد أخذ بهذا الرأي المشرع الجزائري حيث أباح فيما يتعلق بجرائم المعلوماتية إجراء التفتيش ليلا أو نهارا وفي جميع الأوقات ويشترط الحصول على أذن من الجهة القضائية المختصة (المادة 47 /3 ق.ا.ج) .

المبحث الثالث
آثار التفتيش

يهدف إجراء التفتيش إلى الحصول على الدليل لإثبات الجريمة محل التحقيق وإسنادها إلى شخص معين فإذا كانت نتائج التفتيش إيجابية وتم العثور على المعطيات المبحوث عنها فإنه يجب ضبطها وحجزها إذا كانت

قابلة للحجز، وفي حالة استحالة ذلك، فإنه يجوز للسلطات المختصة اللجوء إلى منع الوصول إليها. وسنتطرق إلى ذلك وفقا لما يأتي:

المطلب الأول: حجز المعطيات المعلوماتية

إذا كان من المعروف في التفتيش في الجرائم العادية بأنه يتم ضبط الأشياء وحجزها التي تفيد في إثبات الجريمة وهي أشياء مادية إذ يتم جرد المنقولات ووضعها في أحراز ونقلها بينما يتم التحفظ على العقارات وتشميعها للمحافظة على أثار الجريمة فإن الأمر يختلف عنه في الجريمة المعلوماتية لأنها تتضمن أشياء مادية تتمثل في أجهزة الحاسوب ولواحقها، والأقراص الصلبة والمرنة، وأشرطة التخزين، وأجهزة الإرسال[40]، وأشياء معنوية غير محسوسة تتمثل في البيانات والنظم والبرامج الموجودة التي تكون محل التفتيش.

فبالنسبة للأشياء المادية، فلا جدال في إمكانية ضبط وحجز جميع الأشياء المفيدة في إظهار الحقيقة والناتجة عن عملية التفتيش وإذا كانت هذه الأشياء مادية والتي يمكن أن يكون من بينها أجهزة الحاسوب أو إحدى مكوناته المادية فإنه يجوز حجزها إذا كانت تفيد في إظهار الحقيقة ويتعين جرد هذه الأشياء وتحرير محضر عنها وإرفاقه بملف الإجراءات ويتعين على القائم بالتفتيش والحجز أن يحافظ على هذه الأجهزة بالحالة التي كانت عليها (المادة 84 ق.إ. ج).

أما فيما يتعلق بالأشياء اللامادية أو المعنوية فقد اختلف الفقهاء فيما يتعلق بحجز وضبط البيانات المعالجة والمعطيات المخزنة في الحاسوب أو النظم المعلوماتية. وظهر هناك اتجاهان[41]:

الاتجاه الأول: ويرى أنصاره أنه لا يمكن تصور إجراء الحجز وضبط الكيانات المنطقية لانتفاء الكيان المادي لها. إلاّ أن هذه النظرية عفا عنها الزمن ولم تعد تساير متطلبات التفتيش عن الجريمة في المجتمع الرقمي، ما أدى إلى هجرها من قبل الفقه.[42]

الاتجاه الثاني: ويرى أصحاب هذا الاتجاه أنه لا يوجد ما يمنع من حجز هذه البيانات والمعطيات المعالجة بنظام المعلوماتية أو ما يعرف بالبيانات الالكترونية على أساس تمديد مفهوم ضبط الأدلة المادية ليشمل البيانات الالكترونية، والتي تتكون من المعلومات وهي لا يمكن حجزها لأنها أشياء معنوية بينما البيانات المعالجة آلياً فهي ذات طابع مادي على أساس أنها ذبذبات الكترونية وإشارات أو موجات كهرومغناطيسية يمكن أن تُسجل وتُخزن على وسائط معينة ويمكن قياسها.

ومهما يكن من أمر، فإن القواعد الخاصة بالتفتيش بمفهومه التقليدي لم تعد تلبي متطلبات التحقيق في الجرائم المستحدثة التي ينبغي أن تحكمها قواعد تراعي الجوانب التقنية للمعلوماتية وتتماشى مع البيئة الرقمية التي ترتكب فيها مثل هذه الجرائم.

وباستقراء موقف المشرع الجزائري نجده قد ذهب إلى تأكيد الاتجاه القائل بإمكانية تفتيش البيانات المعالجة آليا وضبطها، فقد أجاز حجز المعطيات المخزنة داخل النظم المعلوماتية إذا كانت تفيد في كشف الجرائم أو مرتكبيها (المادة6 فقرة1 من قانون 04/09).

أما عن طريقة حجز المعطيات المعلوماتية، طبقا للمادة 6، فتتم عن طريق نسخ المعطيات محل البحث والمعطيات الضرورية لفهمها، على دعامة تخزين الكترونية تكون قابلة للحجز ثم توضع في أحراز طبقا لأحكام

قانون الإجراءات الجزائية. ويتم اللجوء إلى عملية النسخ عندما يكون من غير الضروري حجز كل المنظومة المعلوماتية، حيث أن المعلومة ستكون بالضرورة بالقرص الصلب للحاسوب التابع لمقدم الخدمة، وبالتالي فإن نسخها يتطلب حفظها على دعامات تخزين إلكترونية مثل الأقراص المضغوطة أو المتحركة أو الأقراص الصلبة الخارجية، كما تمتد عملية النسخ إلى المعطيات اللازمة لفهم المعطيات محل التفتيش؛ حيث أنه من الممكن أن هذه الأخيرة لا تقرأ مباشرة إلا بتدخل وسائل معينة ومعطيات أخرى.[43]

وبعد القيام بعملية التفتيش والحجز وَجب على السلطة التي قامت بذلك المحافظة على سلامة المعطيات في المنظومة المعلوماتية محل التفتيش[44]، وذلك باتخاذ الوسائل الفنية المطلوبة لضمان سلامة المعطيات المعلوماتية المحجوزة، حيث أن الحجز في مثل هذه الحالات لا يعني محو المعطيات المخالفة أو إتلافها، بل هو إجراء يهدف إلى جمع أدلة الإثبات.وإذا حجزت مع المعطيات أجهزة لها علاقة بالنظم المعلوماتية؛ فينبغي أن تعامل بنفس الكيفية من حيث السلامة.

غير أنه - ولأغراض التحقيق- يجوز للسلطة التي تقوم بالتفتيش والحجز أن تقوم بتشكيل المعطيات المحجوزة أو إعادة تشكيلها [45]بهدف جعلها قابلة للاستغلال وذلك باستعمال الوسائل التقنية اللازمة لذلك، على شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات المعلوماتية؛ كأن يؤدي ذلك إلى تعديل مضمونها أو محو جزء منها، أو تعطيل جزء آخر.

المطلب الثاني: منع الوصول إلى المعطيات المعلوماتية

في بعض الأحيان يستحيل نسخ المعطيات لأسباب تقنية، كما لو كانت

المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها، فيتعين حينئذ على السلطة المكلفة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (المادة7 من قانون 04/09) والهدف من هذا الإجراء الاحترازي هو الحفاظ على الأدلة في محيطها الإلكتروني، ومنع أي محاولة لطمسها أو إخفاء معالمها، وهو ما سيكون له دون شك الأثر الإيجابي في نجاح إجراءات التفتيش والحجز.

الخاتمة:

نخلص إلى القول أن تفتيش المنظومات المعلوماتية هو من أصعب إجراءات البحث والتحري عن الجريمة ومرتكبيها، ولعل ذلك يعزى إلى طبيعة الإجرام المعلوماتي في حد ذاته، الأمر الذي يتطلب خبرة واسعة وكفاءة عالية من لدن القائمين به، كما يتطلب في الوقت نفسه تعاوناً دولياً فعالاً لمحاصرة هذه الجرائم وملاحقة مرتكبيها وإنزال العقاب بهم.كما أن التفتيش في البيئة الافتراضية يختلف كثيرا عن التفتيش بمفهومه التقليدي، وإن كانت تحكمه في بعض جوانبه القواعد المألوفة في قانون الإجراءات الجزائية؛ مثل تفتيش المساكن والمحال التي توجد فيها أجهزة الإعلام الآلي.

وما يمكن ملاحظته هو مشاركة عدّة أطراف في عمليتي التفتيش والحجز عن المعطيات المعلوماتية؛ فهناك السلطات القضائية؛ النيابة والتحقيق وكذا الضبطية القضائية، ومقدمو الخدمات، والهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال ومكافحتها، فضلاً عن الأشخاص الذين لهم دراية واسعة بعمل الشبكات المعلوماتية محل البحث والتحري. ويعكس كثرة المتدخلين في تفتيش النظم المعلومات إلى خطورة هذه

الجرائم وجسامة الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها)، هذا من جهة؛ وإلى خصوصيتها وتعقد أساليب البحث عنها وتشابكها، من جهة ثانية، وقد يزداد الأمر تعقيدا عندما تكون البيانات المراد البحث مخزنة في منظومة معلوماتية تقع في الخارج، وإن كان يخضع في هذه الحالة - بحسب التشريع الجزائري - إلى الاتفاقيات الدولية التي تبرمها الجزائر في إطار التعاون القضائي الدولي. إلا أن السؤال المطروح: ما مصير التفتيش في حالة عدم وجود اتفاقية دولية ؟

كما يمكننا أخيراً أن نقدم بعض التوصيات:

ضرورة توحيد القواعد المتعلقة بالإجراءات المتبعة في مكافحة جرائم تكنولوجيا الإعلام والاتصال في مدونة واحدة تبعا لخصوصيات هذه الجرائم وخصوصية مرتكبيها، أو بدلا من ذلك؛ إدماجها في قانون الإجراءات الجزائية.

ضرورة تقنين كل الجرائم المعلوماتية أو التي ترتكب أو يَسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، في قانون واحد، يضم كافة جرائم الحاسوب والإنترنت والوسائط المتعددة؛ سواء تعلق منها بجرائم الأشخاص أو الأموال، أو الجرائم الماسة بالنظام العام والآداب العامة، أو كانت جرائم تمس حقوق الملكية الفكرية، أو تتضمن انتهاكا لحماية خاصة أولتها القوانين لبعض الفئات الخاصة؛ كالأطفال والنساء.

إيلاء أهمية قصوى للخصوصية أثناء تفتيش المنظومات المعلوماتية، والالتزام بمبادئ حماية الحياة الخاصة، من حيث عدم نشر وتوزيع المعلومة

والمتاجرة فيها، وعدم استعمالها و تجميعها في غير ضرورة البحث والتحقيق. وفي هذا الشأن يتعين على مزودي خدمات الانترنت وعلى القائمين بإدارة قواعد المعلومات الحفاظ على المعطيات المتعلقة بالخصوصية، وعدم إفشاء أسرارها.

الهوامش:

1- يطلق المشرع الجزائري على الجرائم المعلوماتية مصطلح: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. انظر: القانون 09ـ04 المؤرخ في 5 غشت 2009 الجريدة الرسمية، العدد47.

2 - سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة 1972، ص 36.

3 - عبد الواحد إمام مرسي، الموسوعة الذهبية في التحريات، دار المعارف والمكتبات الكبرى، الإسكندرية 1996، ص370.

4- عبد الله أوهابية، شرح قانون الإجراءات الجزائية، الجزء الأول، مطبعة الكاهنة، الجزائر 1998، ص164.

5 - انظر: فضيل العيش، شرح قانون الإجراءات الجزائية بين النظري والعملي، طبعة منقحة، دار البدر، الجزائر 2008، ص 113 .

6 - علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت - دراسة مقارنة، عالم الكتاب الحديث، اربد الطبعة الأولى 2004،ص 12-13 .

7- المادة 2 (ب) من القانون 04/09. ونشير أنه نفس التعريف الوارد في المادة الأولى (أ) من اتفاقية بودابست حول الجريمة المعلوماتية العام 2001 .

8 - عمر الحاج الحضيري، إجراءات التفتيش وتطبيقاته في الإدارة الأمنية، رسالة ماجستير في العلوم الأمنية، المركز العربي للدراسات الأمنية والتدريب، الرياض 1986 -1987، ص 19.

9 - هشام محمد رستم، الجرائم المعلوماتية: أصول التحقيق الجنائي الفني، بحث مقدم لمؤتمر "القانون والكومبيوتر والإنترنت"،كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 1- 3 مايو 2000 ، المجلد الثاني، الطبعة الثالثة، دبي 2004، ص442 .

10- عبد الله بن عبد العزيزبن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية- دراسة تطبيقية- رسالة ماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 1432 هـ - 2011 م ، ص 35.

11- انظر

Freyssinet Eric , « La preuve numérique » Un défi pour l'enquête criminelle du 21e siècle, Les Cahiers du numérique, 2003/3 Vol. 4, p. 212 et S.

12 - انظر:

Valérie–Laure BENABOU, Vie privée sur interne : le traçage électronique, in Les libertés individuelles à l'épreuve de NTIC, Eudes réunies sous la direction de Marie-Christine Piatti ,PUL 2001,PP.89-91.

13 - يمكن استعمال هذه الآثار(le traçage) في الإشهار التجاري، حيث تقوم شبكات التواصل الاجتماعي(SRS) بجني الكثير من الأرباح من خلال بيع المعلومات الخاصة بالسلوك الاستهلاكي للمستخدمين إلى الشركات التجارية؛ ما يشكل تهديداً خطيراً للخصوصية. في هذا الشأن، انظر:

Laurent COLLÉE, Sécurité et vie privée sur les réseaux sociaux, Mémoire pour l'obtention du diplôme de Master en Gestion de la sécurité des systèmes d'information, Faculté de Droit, d'Economie et de Finance, Université du Luxembourg Année académique 2009, p.40.

14 - عبد العزيز نويري، المخاطر القانونية لإنترنت على حرية التعبير والحياة الخاصة، مجلة "التواصل"، جامعة عنابة، عدد: 26، جوان 2010، ص70.

15- انظر على حسن محمد الطوالبة، المرجع نفسه، ص 62 ومايليها.

16 - عثمان جبر محمد عاصي، ضمانات المشتكي عليه في التحقيق الجزائي الابتدائي في الأردن، رسالة ماجستير، كلية الدراسات الفقهية والقانونية، جامعة آل البيت الأردن 1998، ص 149 .

17- انظر المادة 2 (أ) من القانون رقم 09 / 04 .

18 - وهي الجرائم التي وردت تحت عنوان: " المساس بأنظمة المعالجة الآلية للمعطيات "، انظر: المواد من 394 مكرر إلى المادة 394 مكرر7 قانون العقوبات الجزائري.

19 - قد ترتكب بعض الجرائم الماسة بحقوق الملكية الفكرية، والمحمية بموجب قانون المؤلف والحقوق المجاورة؛ عن طريق استعمال منظومة معالجة معلوماتية، كجريمة تقليد ونسخ المصنفات؛ أو ما يعرف بجرائم القرصنة. انظر: المادتين 151 و152 من القانون رقم 03 - 05 والمؤرخ في 19 يوليو 2003 والمتضمن حقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد: 44 . كما قد ترتكب الجريمة الماسة بتكنولوجيا المعلومات

والاتصال؛ عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا؛ والمعروفة ببطاقة " الشفاء "، أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة، أو من خلال النسخ أو التعديل الغير مشروع للبرمجيات التي تسمح بالوصول إلى استعمال هذه البطاقة أو المفتاح الإلكتروني، أو عن طريق نسخ أو حيازة أو توزيع بوسيلة غير مشروعة البطاقة الإلكترونية أو المفتاح الإلكتروني. راجع: المادتين 93 مكرر3 المادة 93 مكرر4 من القانون رقم 08-01 المؤرخ في 23 يناير 2008 والمتضمن بالتأمينات الاجتماعية، المعدّل والمتمّم، الجريدة الرسمية، العدد 04.

20- انظر المواد 119 - 123 وكذلك المادة 125 من القانون العضوي رقم 12-05 المؤرخ في 12 يناير 2012، والمتعلق بالإعلام، الجريدة الرسمية، العدد:02.

21- عبد الله بن عبد العزيزبن عبد الله الخثعمي، المرجع نفسه، ص 54 .

22- سامي حسني الحسيني، المرجع نفسه، ص 98.

23- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية - دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط 1994، ص 64 وما بعدها.

24 - موسى مسعود ارحومة الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا 28- 29 /10/ 2009، ص7 .

25 - أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر عمان 2000، ص278 وما بعدها.

26- عبد الكريم غالي، الحماية الجنائية للمعلومات على ضوء القانون المغربي، بحث مقدم لمؤتمر " الوقاية من الجريمة في عصر العولمة "، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة بالتعاون مع أكاديمية نايف للعلوم الأمنية، دبي من 6 - 8 مايو 2000، ص 653.

27- عبد الله بن عبد العزيزبن عبد الله الخثعمي، المرجع نفسه، ص 37 .

28- carte de décodage de télévision numérique

29 - انظر المادة 5 الفقرة 2 و 3 من القانون رقم 04/09 .

30 - موسى مسعود ارحومة، المرجع نفسه، ص9.

31 – انظر : أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر الإسكندرية 2007، ص671.

32 – علي حسن الطوالبة، المرجع نفسه، ص 55 وما بعدها .

33– على كحلون، الجرائم المتعلقة بالمحتوى المعلوماتي، مجلة " القضاء والتشريع"، مركز الدراسات القانونية والقضائية، تونس، العدد 9، السنة 45، نوفمبر 2003، ص87.

34 – تعرف المادة 2/د من القانون 04/09 مقدمي الخدمات.

35 – المادة 14 من المرسوم التفيذي رقم 89–257 المؤرخ في 25 غشت 1998 الذي يضبط شروط وكيفيات إقامة خدمات " أنترنات " واستغلالها. كذلك من بين الالتزمات الخاصة بمقدمي خدمة " الإنترنت " ما ورد في نص المادة 12 من القانون 04/09.

36 – collecte en temps réel de données informatiques ويقصد به التدخل السريع خلال الوقت الفعلي للمبادلات الالكترونية بهدف تسجيل المعطيات المتبادلة في حينها. للمزيد حول هذا المصطلح، راجع: علي كحلون، المرجع نفسه، ص98 وما يليها. وكذلك:

WARUSFEL B., « Procédure pénale et technologie de l'information : de la Convention sur la cybercriminalité à la Loi sur la sécurité quotidienne, pp.4 et SS . http://www.droit.univ-paris5.fr/warusfel/articles/procpenale-ntic_warusfel02.pdf.

37– تنص المادة 11 من القانون 04/09 على المعطيات التي يلتزم مقدمو الخدمات بحفظها.

38– انظر: المادة 11 الفقرة 3.

39 – انظر: المادة 14 من القانون 04/09. مع الإشارة إلى أنه لم يتم بعد تنصيب هذ الهيئة.

40 – راجع: حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض 1420 هـ 2000 م، ص 226.

41 – راجع علي حسن محمد الطوالبة، المرجع نفسه، ص 145–147.

42– انظر:

M. Chawky, Le vol d'informations : quel cadre juridique aujourd'hui ?, Droit-Tic, juill. 2006, note.10, p.4.

http://www.droit-ntic.com/trav/info.php?id_trav=92

43– انظر: علي كحلون، المرجع نفسه، ص 96.

44– راجع: المادة 6 الفقرة 2 من القانون 04/09.

45– راجع: المادة 6 الفقرة 3 من القانون 04/09.