التفتيش في الجريمة المعلوماتية

الأستاذة/ ليندا بن طالب
أستاذة بجامعة مولود معمري تيزي وزو الجزائر

❖❖❖❖❖❖❖

ملخص:

إن التفتيش في الجريمة المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه والذي يسهل إخفاءه وتدميره، وقد يتصل بدول أخرى مما يزيد صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها. كما أن التفتيش في الأنظمة الإلكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة.

كما يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعين توفر شروط تفتيش المساكن، أما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنه يكفي توفر شروط تفتيش الشخص. عند صدور إذن بتفتيش نظام معين لمعالجة المعلومات آليا للحصول على دليل يفيد في كشف الحقيقة عن جريمة معلوماتية معينة، يجوز تفتيش كل الملفات المتواجدة في النظام.

إذا أسفر التفتيش عن ضبط البيانات المتواجدة في نظام المعالجة الآلية، فيمكن ضبطها دون ضبط النظام كله، وذلك بأخذ نسخة من البيانات الموجودة، ويلتزم المحقق بالتحفظ عليها بشكل يمنع العبث بها.

Abstract:

Inspection of cybercrime is difficult because of the nature of the obtained evidence, which is easy to hide and to destroy, it may also be related to other countries, making it more difficult to obtain because each country has its own sovereignty. Inspection of electronic systems also requires scientific and technical knowledge that may not be available to police officers, investigators and judges.

An inspection permit may be issued only for computer inspection. If the latter is present in a dwelling, the conditions for house inspection must be met, whether the computer is in the possession of a person outside his home or in his car outside the dwelling.

When an order is issued for the inspection of a particular system to process the information automatically in order to obtain evidence to reveal the truth about a particular information crime, all files in the system may be searched.

If the inspection results in the control of the data contained in the automated processing system, it can be set without controlling the whole system, by taking a copy of the existing data, and the investigator is obliged to reserve on it in a way that prevents tampering.

مقدمة:

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يقوم به موظف مختص، طبقا للإجراءات المقررة قانونا، في محل يتمتع بحرمته، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها، لإثبات ارتكابها ونسبها إلى المتهم، وقد أحاط المشرع إجراء التفتيش –نظرا لمساسه بالحريات الخاصة للأفراد– بضمانات عديدة(1).

محل التفتيش في الجرائم التقليدية قد يكون مسكنا أو شخصا، وقد يتعلق التفتيش بالمتهم سواء انصب على مسكنه أو شخصه، وقد ينصب على مسكن غير المتهم أو شخص غير المتهم، وهو في كل الأحوال تفتيش جائز بالشروط القانونية المقررة(2).

مع التطور التكنولوجي للاتصالات الذي يشهده العالم الحالي والذي استفاد منه عالم الإجرام، وجدت جرائم حديثة يطلق عليها مصطلح الجرائم المعلوماتية والتي أثارت العديد من المشكلات في نطاق قانون الإجراءات الجنائي، حيث وضعت نصوص هذا القانون لتحكم الإجراءات المتعلقة بالجرائم التقليدية، التي لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الإقناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم، أما في الجرائم المعلوماتية فيتسم إجراء التفتيش –من أهم إجراءات التحقيق– فيها بالعديد من المعوقات والصعوبات، فنظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم والشبكات بمختلف أنواعها.

وفي إطار هذه الدراسة نطرح التساؤل التالي: هل الإجراءات التي تحكم التفتيش في صوره السابقة هي نفسها تحكم تفتيش نظام الحاسب الآلي؟ وسنحاول الإجابة عن هذا التساؤل فيما يلي:

المبحث الأول

مدى قابلية نظام الحاسوب للتفتيش

يتكون الحاسب الآلي من مكونات مادية Hard ware ومكونات منطقية Soft ware، كما أن له شبكات اتصال بصرية سلكية ولاسلكية، سواء كان ذلك على المستوى المحلي أو على المستوى الدولي.

المطلب الأول: خضوع مكونات الحاسوب المادية للتفتيش

يرى جانب من الفقه الجنائي أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فبالتالي فإن تفتيش المكونات المادية للحاسب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عنها

وعن مرتكبيها، يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة[3]، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها.

إلا أن حكم هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء في الأماكن العامة أو الأماكن الخاصة، إذ للمكان أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه.

المطلب الثاني: خضوع مكونات الحاسوب المعنوية للتفتيش

إذا كان الأمر قد انتهى بنا إلى صلاحية المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش، فإن امتداد ذلك إلى مكوناته غير المادية، هو محل جدل كبير، حول مدى صلاحيتها كي تكون موضوعا للتفتيش.

وقد ذهب الفقه في هذا الشأن إلى مسارين رئيسيين:

المسار الأول: يلخص أصحاب هذا المسار في تفسيره إلى الاستناد على الربط بين النصوص الإجرائية والعلوم الطبيعية ومفهومها في البيانات المنطقية أو البرامج، حيث أن كلمة الشيء هو المادة بمعنى كل ما يشغل فراغ معين يمكن قياسه والتحكم فيه، بناء على ذلك أن الكيان المنطقي للحاسوب –الذاكرة – تشغل حيزا ماديا يمكن قياس سعتها وحجمها بالحروف التي يمكن خزنها فيها[4].

ويتضح موقف المشرع الجزائري من خلال المادة 5 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، حيث أجاز صراحة تفتيش المنظومة المعلوماتية.

المسار الثاني: يذهب إلى عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته[5].

ولذلك يقترح هذا الجانب الفقهي، إزاء النقص التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش إمكانية البحث والضبط للمواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، لتصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هو البحث عن الأدلة المادية وأية مادة معالجة بواسطة الحاسب الآلي[6].

المطلب الثالث: مدى خضوع شبكات الحاسوب للتفتيش " التفتيش عن بعد "

مع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الاتصالات محدودا في إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم وذلك بعد ظهور شبكة الإنترنت وهي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسب الموزعة عبر مختلف دول العالم.

إن طبيعة التكنولوجيا الرقمية عقدت التحدي أمام أعمال التفتيش والضبط، بسبب امتداد الأدلة الإلكترونية عبر شبكات الحاسوب[7] في أماكن بعيدة عن الموقع المادي للتفتيش، وإن كان من الممكن الوصول إليها من خلال الحاسوب بعد أخذ إذن تفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، وهو ما يزيد المسألة تعقيدا باعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم تقريبا. وبالتالي فإن الحاسوب الذي يمكن أن ترتكب عليه أو بواسطته الجريمة المعلوماتية يخضع للقانون الإجرائي الخاص بتلك المنطقة[8].

فالسؤال المطروح: هل يمكن تفتيش الأنظمة المتصلة بالنظام المسموح بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة أو حتى خارج البلاد؟ وللإجابة عن هذا التساؤل يجب التفرقة بين الفرضيتين التاليتين:

الفرضية الأولى: اتصال حاسب المشتبه فيه أو المتهم بحاسب آخر موجود في مكان آخر داخل الدولة:

نجد المشرع الجزائري أجاز تمديد التفتيش وذلك في نص المادة 05 الفقرة الثانية من القانون 04/09[9] بأنه في حالة التفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وانطلاقا مما سبق ذكره، نلاحظ أن ذاتية تفتيش الحاسوب وقصور القواعد الإجرائية التقليدية تظهر بصورة جلية أثناء امتداد التفتيش إلى الأجهزة المرتبطة به، فالانتقال غير مهم إلى مكان الجهاز الثاني، بل إن ذلك يتم باستعمال وسائل تقنية حديثة " برامج الدخول "، وهنا يبقى السؤال مطروحا ألا يعد استعمال هذه البرامج اعتداء على حرمة الحياة الخاصة للأفراد، خاصة وأن الأجهزة الأخرى تنتمي إلى أشخاص غير المتهم؟

الفرضية الثانية: اتصال حاسب المشتبه فيه أو المتهم بحاسب موجود في مكان آخر خارج الدولة:

إنّ لامتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على دليل عن بعد وفي بضع ثوان، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاك لسيادة الدولة الأجنبية، وإذا اقتضت ضرورة التحقيق القيام بذلك ينبغي مراعاة العديد من الضمانات يكون متفقا عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية[10].

إنّ المشرع الجزائري أخذ نفس مسار المشرع الفرنسي حيث أجاز هو ذلك تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، وهذا ما نصت عليه المادة 05 فقرة 3 من القانون رقم 04/09 « ... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ».

المبحث الثاني

ضوابط التفتيش في البيئة الإلكترونية

نجد ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات التي تمس حريتهم كالتفتيش وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم. وتنقسم الضوابط العامة للتفتيش إلى نوعين، ضوابط موضوعية وشكلية:

المطلب الأول: الضوابط الموضوعية لتفتيش نظم الحاسوب

يقصد بهذه الضوابط بصفة عامة، الشروط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاثة ضوابط أساسية: السبب، المحل والسلطة المختصة للقيام به.

الفرع الأول: وجود سبب للتفتيش في البيئة الإلكترونية

سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث، ويتمثل في وقوع جريمة ما جناية أو جنحة، اتهام شخص أو أشخاص معنيين بارتكابها أو المشاركة فيها، وتوافر قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو المتهم أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما ينطبق على الجريمة الإلكترونية(11).

الفرع الثاني: محل التفتيش

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره في الجريمة التقليدية فإن التفتيش ينصب على شخص المتهم أو غير المتهم، وكذلك على مسكن المتهم وما في حكمه وملحقاته، أو على مسكن غير المتهم وما في حكمه وملحقاته(12). لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به ، كما سبق شرحه وبيانه.

ولكي يتم التفتيش على هذه الحال، ينبغي الإشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال الذكي.سبق وأن أشرنا إلى مدى قابلية المكونات المادية والمعنوية للحاسوب وشبكات الاتصال الخاصة به للتفتيش.

الفرع الثالث: السلطة المختصة بالتفتيش

إن لتفتيش إجراء من إجراءات التحقيق التي تمس بالحرية الشخصية للأفراد، حرصت التشريعات الجنائية على إسنادها لجهة قضائية تكمل تلك الحريات والحقوق وتضمنها، إلا أن هذه التشريعات لم تسر على نسق واحد فيما يخص تحديد الجهة التي يعهد لها بالتحقيق الإبتدائي لتكون صاحبة الاختصاص الأصيل بإجراء التفتيش، فقد ذهبت بعض القوانين كالتشريع المصري إلى منح هذه السلطة للنيابة العامة، حيث لما صدر قانون الإجراءات الجنائية بموجب قانون رقم 150 لسنة 1950 عاد مرة أخرى على نظام الجمع بين سلطتي التحقيق والاتهام بيد النيابة العامة باستثناء جرائم معينة. رأى أن يختص بها قاضي التحقيق(13) بخلاف الحال عند كل من الجزائر وفرنسا حيث أخذا بنظام الفصل بين سلطتي الاتهام والتحقيق، حيث عهدت هذه الأخيرة لقاضي التحقيق أما الأولى فعهدت للنيابة العامة

الفرع الرابع: الإذن بالتفتيش

غالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن ثم هل يجوز بمقتضى هذا الإذن لضباط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن أدلة إثبات التي يمكن أن تكون محل الضبط؟

وفي هذه الحالة يرى أغلب الفقهاء أنه يجب أن يحدد إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (أجهزة الحاسوب، صور جنسية إلكترونية خاصة بالأطفال، مصنفات إلكترونية مقلدة...)، والهدف من هذا التحديد في إذن التفتيش لا هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك، إلا أن هناك صعوبة في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الكمبيوتر، ويرجع ذلك إلى الطبيعة

الخاصة لهذه الأخيرة، فالكمبيوتر يحتوي على عدد كبير من الملفات، بالإضافة إلى أن أسماء هذه الملفات لا تدل بالضرورة على ما تحتويها، بالتالي هنا تثار الصعوبات فهل يعتبر كل ملف " صندوقا مغلقا " يحتاج إلى إذن قضائي مستقل عن الآخر؟ خاصة وقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة[14].

أما المشرع الجزائري في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في قانون رقم 04/09، لا نجده يتحدث عن هذا الشرط، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

المطلب الثاني: الضوابط الشكلية لتفتيش نظم الحاسوب الآلي

إن هذه الضوابط أو الشروط الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، بل تقيم – بالإضافة إلى مقتضيات الإجراء – سياجا يحمي حقوق والحريات الفردية.وتتمثل هذه الضوابط الشكلية في:

الفرع الأول: إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الإطمئنان على سلامة الإجراء غني عن البيان أن التفتيش فيه اطلاع على أسرار الغير.

فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن، ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه – سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية – وإذا تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا، يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش[15].

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 من المادة 45 منه، حيث استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد. كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بنظام التفتيش عن بعد، أو ما يطلق عليه الفقه الفرنسي " التفتيش على المباشر perquisition en ligne "[16].

الفرع الثاني: الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية

يقصد بشرط الميعاد الزمني في التفتيش، أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن. إنّ القانون الجزائري يحظر تفتيش المنازل وما في حكمهما في وقت معين، وهو محدد في القانون الإجراءات الجزائية من خلال المادة 47 من الساعة الخامسة صباحا على الساعة الثامنة مساء. وهناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد ويصح إجراء التفتيش في أي ساعة من ساعات الليل والنهار،

وأن المشرع الجزائري قد أورد في قانون الإجراءات الجنائية المادة 3/64 « أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 3/47 من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر حيث أجاز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص » وجاء في نص المادة 3/47 من قانون الإجراءات الجزائية[17]، حيث استثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في هذه المادة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. والملاحظ أن المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتباره مستودع أسرارهم، إلا أن ما يبرره ويقل من خطورته الطبيعة الخاصة لهذه الجرائم خاصة الجريمة الإلكترونية وطبيعة الدليل لإثباتها فهو قابل للمحو والتعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية، وما يزيد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوة الجنائية. أما بالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل معه مكونات الحاسوب سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

الفرع الثالث: محضر التفتيش في الجرائم المعلوماتية

باعتبار أن التفتيش من أعمال التحقيق، لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة، والقانون لم يتطلب شكلا خاصا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكونا مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية.

خاتمة:

إنّ موضوع هذا البحث قد تناول مشكلة من المشكلات التي أفرزتها ثورة المعلومات والاتصالات عن بعد، حيث أنه لا شك في أن التفتيش المتعلق بالجرائم المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه، والذي يسهل إخفاءه وتدميره، وقد يتصل بدول أخرى مما يزيد صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها. كما أن التفتيش في الأنظمة الإلكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة.

ومن أهم النتائج التي يمكن أن نخلص إليها:

- إن قانون الإجراءات الجزائية الجزائري يجيز التفتيش في البيئة المعلوماتية—الرقمية– لضبط المعلومات على الرغم من طبيعتها المعنوية.
- كما أنه يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعين توفر شروط تفتيش المساكن، إما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنه يكفي توافر شروط تفتيش الشخص.
- عند صدور إذن بتفتيش نظام معين لمعالجة المعلومات آليا للحصول على دليل يفيد في كشف الحقيقة عن جريمة معلوماتية معينة، يجوز تفتيش كل الملفات المتواجدة في النظام.

– إذا أسفر التفتيش عن ضبط البيانات المتواجدة في نظام المعالجة الآلية، فيمكن ضبطها دون ضبط النظام كله، وذلك بأخذ نسخة من البيانات الموجودة، ويلتزم المحقق بالتحفظ عليها بشكل يمنع العبث بها.

التهميش:

(1) عوض محمد عوض، قانون الإجراءات الجنائية، الجزء الأول، مؤسسة الثقافة الجامعية، 1989، ص 475.

(2) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 3.

(3) عبد الفتاح بيومي حجازي، المرجع السابق، ص 78.

(4) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 54.

(5) علي حسن طوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الطبعة الأولى، 2004، ص 31.

(6) هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 76.

(7) هلالي عبد الله احمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم ألمعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 76.

(8) علي حسن محمد الطوالبة، مرجع سابق، ص 42.

(9) قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها.

(10) Vergucht Pascal, La répression des délits informatiques dans une perspective internationale, thèse, Montpelier, 1996, p 336.

(11) Roger Merle et Andre Vitu, traite de droit criminel, Tome2, quatrième édition, édition Cujas, Paris, 1989, p 757.

(12) قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشاة المعارف، الإسكندرية، 2005، ص 111.

(13) عائشة بن قارة مصطفى، مرجع سابق، ص 63 وما بعدها.

(14) عائشة بن قارة مصطفى، المرجع السابق، ص 63.

(15) المادة 45 من القانون الإجراءات الجزائية الجزائري سالف الذكر.

(16) Yann Padova, Un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénale, n° 4, Dalloz, 2002, p770.

(17) المادة 3/47 المعدلة بموجب المادة 10 من قانون رقم 06-22 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية.