التفتيش كآلية لإثبات جرائم نظم المعلوماتية

Inspection as a mechanism to prove information systems crimes

صغير يوسف [1]*،

[1]جامعة آكلي محند أولحاج –البويرة– (الجزائر)

تاريخ الاستلام: 2021/09/07 تاريخ القبول للنشر: 2021/10/24 تاريخ النشر: 2021/12/31

ملخص:

يهدف هذا المقال إلى دراسة موضوع التفتيش كآلية لإثبات الجرائم المعلوماتية، وذلك عن طريق تبيان مدى صلاحية الوسائل المادية والمعنوية وشبكات الحاسوب أن تكون محلا للتفتيش، بالإضافة إلى أهم الضمانات المقررة قانونا لإجراء التفتيش، فدراستنا للموضوع لم تأت من العدم بل كانت من منطلق أن التفتيش يعتبر من بين أهم وأخطر إجراءات التحقيق الجنائي نظرا لما يتميز به من ناحية أدلة الإثبات الناتجة عنه ومساسه بالحياة الخاصة للأفراد.

الكلمات المفتاحية: العالم الافتراضي، التفتيش، الجريمة المعلوماتية، ضمانات التفتيش، التفتيش عن بعد.

Abstract:

This article aims to study the subject of inspection as a mechanism to prove information crimes, by showing the validity of the physical and moral means and computer networks to be the subject of inspection, in addition to the most important legally established guarantees for conducting. It is among the most dangerous criminal investigation procedures due to what is distinguished in terms of the evidence resulting from it and its infringement of the private life of individuals.

Keywords: virtual world, inspection, cybercrime, inspection guarantees, remote inspection.

* صغير يوسف: y.sghir@univ-bouira.dz

مقدّمة:

أسفر التطور التكنولوجي في مجال التقنية الحديثة وشبكات الاتصال إلى ظهور العديد من الجرائم المستحدثة، ولعل خير دليل على ذلك ما يتبادر إلى أسماعنا عبر وسائل الإعلام المختلفة عن حجم الخسائر التي تنجر عن الجرائم المرتكبة عبر العالم الافتراضي وخاصة الشبكة العالمية للإنترنت.

واكبت التشريعات هذا التطور الكبير في الجريمة التي تستعمل وسائل التقنية الحديثة، وذلك عن طريق تحديث وتحيين ترسانتها القانونية الموضوعية منها و الإجرائية، ولقد نال الشق الإجرائي النصيب الأكبر من ناحية التعديل والتحيين، ولعل من بين الإجراءات التي حرصت التشريعات بما فيها المشرع الجزائري على تحيينها بما يتماشى مع إثبات جرائم المعلوماتية هو إجراء التفتيش، نظرا لأهميته والخطورة التي يتسم بها لما ينجر عنه من أدلة إثبات مادية تساعد في الكشف عن الجريمة، ولما فيه من مساس بحقوق وحريات الأفراد.

غير أن إجراء التفتيش كآلية أو كأسلوب تقليدي في الكشف عن الجريمة المرتكبة عبر العالم الافتراضي اعترته العديد من الإشكالات القانونية نظرا لاختلاف البيئة التي يتم فيها هذا الأخير المتمثلة في نظم المعلومات الافتراضي، الأمر الذي أدى بنا إلى التساؤل حول فعالية إجراء التفتيش في إثبات جرائم النظم المعلوماتية؟

المبحث الأول

التفتيش في الجرائم المعلوماتية بين الواقع المادي والطبيعة الافتراضية

يختلف محل التفتيش في العالم الافتراضي عن شبيهه في العالم المادي، فإذا كان هذا الأخير الغاية منه إثبات الجريمة عن طريق الادلة المادية المحسوسة، فإن التفتيش في العالم الافتراضي ينصب –بالإضافة إلى المكونات المادية للحاسب– على مكونات معنوية ومنطقية للحاسب متمثلة في نظم المعلوماتية المخزنة في ذاكرته، وينصب كذلك على الشبكات التي تربط هذه النظم بعضها البعض، الأمر الذي يؤدي بنا للتساؤل حول امكانية القيام بهذا الإجراء في العالم الافتراضي.

المطلب الأول: تفتيش المكونات المادية والمعنوية الحاسوب

إذا كان موضوع التفتيش المكونات المادية للحاسب (فرع أول) المتمثلة المكونات المحسوسة مثل الشاشة ولوحة التحكم والطابعات...الخ لا يطرح أي إشكال، فإن الإشكال يثور حول مدى امكانية تفتيش الوسائل المعنوية للحاسب والمتمثلة في نظم المعلومات المخزنة في ذاكرة هذا الأخير (فرع ثاني).

الفرع الأول: تفتيش الوسائل المادية للحاسوب

تحكم الإجراءات القانونية الخاصة بالتفتيش فحص المكونات المادية للحاسب الآلي بحثا عن أي دليل يتصل بجريمة معلوماتية حدثت، ويفيد التفتيش في الكشف عن مرتكبها.

ويخضع تفتيش الحاسب الآلي إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز[1].

تكتسي صفة المكان وطبيعته أهمية قصوى 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 والإجراءات المقررة قانونا في التشريعات المختلفة.

يجب مراعاة التمييز في هذا الصدد بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلا، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما لو وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطريق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[2].

الفرع الثاني: مدى صلاحية المكونات المعنوية للحاسب أن تكون محلا للتفتيش

بعد أن اتفقت أغلب التشريعات على جواز امتداد التفتيش إلى الوسائل المادية للحاسوب، ظهر الجدل حول إمكانية خضوع الوسائل المعنوية أو المنطقية للحاسوب بأن تكون محلا للتفتيش، وفي هذا الصدد ظهر اتجاهين بين مؤيد ومعارض.

أيد أصحاب الاتجاه الأول جواز تفتيش المكونات المعنوية للحاسوب بمختلف أشكالها، وذلك بالرجوع إلى القوانين الإجرائية التي تجيز تفتيش "أي شيء"، حيث قاموا بتفسير كلمة الشيء تفسيرا موسعا وبالتالي في نظرهم يجوز تفتيش مكونات الحاسب المحسوسة وغير المحسوسة.

يستند كذلك أصحاب الاتجاه المؤيد 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.

---

[1] – **أسامة بن غانم العبيدي**، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، د.س.ن، ص 89.

[2] – **حسين بن سعيد الغافري**، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت"، ص 11-12، مقال متوفر عبر الموقع التالي: http://www.eastlaws.com

بناء على ذلك أن الكيان المنطقي للحاسوب –الذاكرة– تشغل حيزا ماديا يمكن قياس سعتها وحجمها بالحروف التي يمكن خزنها فيها[3].

بينما ذهب رأي آخر –الاتجاه الرافض– إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب[4].

أجاز المشرع الجزائري تفتيش المنظومة المعلوماتية بمقتضى موقف واضح من خلال المادة 05 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[5].

المطلب الثاني: مدى قابلية شبكات الحاسب الآلي للتفتيش

إن ارتباط الحاسبات الآلية فيما بعضها عبر الشبكات الافتراضية خاصة شبكة الإنترنت طرح عدة اشكالات قانونية فيما يخص إجراء التفتيش عبر هذه الأخيرة، فإذا كان التفتيش عبر الشبكات الافتراضية الموجودة داخل الإقليم الوطني لا يطرح هذا الإشكال بحدة (فرع أول)، فإن امتداد التفتيش عبر هذه الشبكات خارج الحدود الوطنية يطرح عدة اشكالات قانونية وإجرائية (فرع ثاني).

الفرع الأول: حالة ارتباط حاسب المتهم بمنظومة معلوماتية داخل الإقليم الوطني

يثير هذا الفرض تساؤل هام يتعلق بمدى إمكانية امتداد الحق في التفتيش، إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم؟[6]

يرى الفقه أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر في حالة اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر داخل إقليم الدولة[7]، حيث من بين الآراء الفقهية

---

3 – **ليندا بن طالب**، "التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 16، جوان 2017، ص 490.

4 – **حسين بن سعيد الغافري**، مرجع سابق، ص 12.

5 – أنظر في ذلك المادة 05 من قانون رقم 09-04، المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر عدد 47، صادر في 16 غشت 2009.

6 – **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 386.

7 – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 381.

التي أخذت بهذا المنحى نجد الفقه الألماني الذي يرى إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني[8].

أجاز المشرع الجزائري بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التفتيش، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك[9].

نص المشرع الجزائري على ذلك بمقتضى المادة 5 الفقرة 2 من القانون رقم 09-04 على النحو التالي: "...**في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، اذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك...**".

الفرع الثاني: حالة ارتباط حاسب المتهم بمنظومة معلوماتية خارج الإقليم الوطني

يظهر أحيانا في أثناء التحقيقات أنه من الضروري تفتيش جهاز كمبيوتر متواجد في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج حيث ترتبط أجهزة الشركة بعضها البعض وأحيانا ترتبط بعض الأجهزة بقاعدة بيانات متواجدة في الخارج[10].

يكتسي امتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على الدليل 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 يؤكد أهمية التعاون الدولي في مجال الجرائم الإلكترونية[11].

أجاز المشرع الجزائري تفتيش المنظومات المعلوماتية المتواجدة خارج الإقليم الوطني وفق ضمانات معينة نص عليها في المادة 5 فقرة 3 من قانون رقم 09-04، حيث جاءت على النحو التالي: "...**إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة**

---

[8] – **حسين بن سعيد الغافري**، مرجع سابق، ص 12.

[9] – **بوعناد فاطة الزهرة**، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، كلية، مجلة إلكترونية خاصة تعنى بنشر الدراسات القانونية، العدد الأول، 2013، ص 69.

[10] – **نزيهة مكاري**، "إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري، (دراسة مقارنة)"، مجلة العلوم الاقتصادية وعلوم التسيير، كلية العلوم الاقتصادية، جامعة فرحات عباس، سطيف، العدد 09، سنة 2009، ص 129.

[11] – **بن طالب ليندا**، التفتيش في الجريمة المعلوماتية، مرجع سابق، ص 491.

معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

نستشف مما سبق أن التفتيش يعتبر من وسائل الإثبات المادية التي تهدف إلى ضبط الأدلة المادية للجريمة فقط، الأمر الذي أدى إلى تصادمه مع الطبيعة غير المادية لبرامج الحاسوب من جهة، والمظهر غير المحسوس لبيانات شبكة الإنترنت من جهة أخرى، مما حدَ من فعاليته في إثبات هذا النوع المستحدث من الجرائم.

المبحث الثاني

مدى ضرورة توفر ضمانات لتفتيش النظم المعلوماتية

يستلزم إجراء التفتيش توفر ضمانات معينة من أجل القيام به، وذلك أن هذا الأخير يمس بحرية الأشخاص، لهذا نجد أغلب تشريعات الدول تسعى إلى تكريس هذه الضمانات من أجل إحداث الموازنة بين حقها في الدفاع عن المجتمع من جهة وبين ضمان حقوق المتهم من جهة أخرى.

تتمثل هذه الضمانات في الشروط الشكلية للتفتيش (مطلب أول)، وشروط موضوعية (مطلب ثاني).

المطلب الأول: الضمانات الشكلية

تتمثل الضمانات الشكلية للتفتيش الإلكتروني والتي إذا تخلفت يعتبر هذا الأخير باطلا في الزامية توفر الإذن بالتفتيش مع احترام التوقيت القانوني لهذا الأخير (فرع أول)، بالإضافة إلى ضرورة حضور أشخاص معينين قانونا لإجراءات التفتيش، وكذلك ضرورة تحرير محضر بعد نهاية التفتيش (فرع ثاني).

الفرع الأول: ضرورة توفر الإذن واحترام ميعاد التفتيش

يجب أثناء مباشرة إجراء التفتيش أن يتوفر إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق يتم استظهاره قبل دخول المنزل المراد تفتيشه، ويجب أن يحتوي هذا الأخير على بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش[12].

يلاحظ ان الأمر يختلف من حيث صدور الإذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى، لأن الإذن قد يصدر في حق شخص قد ارتكب جناية أو جنحة وقامت قرائن قوية على ارتكابه للجريمة وعند القيام بتنفيذ إذن التفتيش فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو أن للمتهم أكثر من جهاز في أماكن مختلفة، كأن يكون المتهم مالكا لجهاز في منزله وجهاز آخر في عمله، أو أن يكون الشخص له شريك في ارتكاب الجريمة ويخشى عند

---

12 – **رابح وهيبة**، "الجريمة المعلوماتية في التشريع الإجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخظر، باتنة 1، العدد الرابع، ديسمبر 2014، ص 327.

اكتشاف ذلك من محاولة المتهم محو تلك الأدلة في الأجهزة الأخرى مما يتطلب الحصول على إذن آخر من النيابة العامة[13].

نرى لحل هذا الإشكال أن يتصف الإذن الممنوح لضباط الشرطة القضائية من أجل إجراء التفتيش بالمرونة شرط توفر ضوابط لعدم انحراف هذا الأخير عن الغاية المرجوة منه، وذلك عن طريق تبيان مجال التفتيش ويتبعه من خلال تفتيش شبكات الحاسب الآلي.

اشترط المشرع الجزائري كقاعدة عامة في التفتيش، أن الأخذ بهذا الإجراء يجب أن يتم في نطاق زمني معين طبقا لنص المادة 47 من قانون الإجراءات الجزائية، وذلك من الخامسة صباحا إلى الثامنة مساءا ما عدا في الحالات الاستثنائية.

غير أنه ونظرا لطبيعة المعطيات المعلوماتية محل التفتيش التي يسهل إتلافها وفسخها وتعديلها، بمجرد تناهى إلى علم المشتبه به بوجود تفتيش، فإن أغلب الفقهاء يرون بعدم إخضاع التفتيش على نظم المعلوماتية لشرط الميقات الزمني، إنما ينبغي ترك إجرائه في أي وقت من الليل والنهار وذلك حسب مل تقدره الجهة القائمة بالتحقيق، وقد أخذ المشرع الجزائري بهذا الرأي بمقتضى المادة 3/47 من قانون الإجراءات الجزائية، حيث أباح فيما يتعلق بجرائم المعلوماتية إجراء التفتيش ليلا أو نهارا وفي جميع الأوقات بشرط الحصول على الإذن من الجهة القضائية المختصة[14].

الفرع الثاني: حضور أشخاص معينين وضرورة تحرير محضر التفتيش

حرصا على تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، تسهر معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يقوم مقامه معتبرين ذلك من القواعد الأساسية التي يترتب عن مخالفتها البطلان[15].

نص المشرع الجزائري على هذا الشرط بمقتضى نص المادة 1/45 من قانون الإجراءات الجزائية على النحو التالي: "**إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته**".

---

13 – **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د.ن، د.ب.ن، 2005، ص 178.

14 – **رضا هميسي**، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 05، جوان 2012، ص 173.

15 – **براهيمي جمال**، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 43

يجب بعد إجراء التفتيش على القائم به أن يحرر محضر يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي أثبتت، وأن يحمل تاريخ تحريره وتوقيع محرره[16]، ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية بالإضافة إلى ما تم ذكره سالفا.

غير أنه يشترط في محضر التفتيش وجوب الاستعانة بكاتب الذي يصطحبه المفتش من أجل تحرير المحضر وتدوين كل الإجراءات والتأشير عليها، وطبقا لنص المادة 68 فقرة 2 من قانون الإجراءات الجزائية التي تنص على: "**وتحرر نسخة من هذه الإجراءات وجميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل**".

المطلب الثاني: الضمانات الموضوعية

تتمثل الضمانات الموضوعية التي أقرها القانون من أجل إجراء التفتيش في الجرائم التقليدية والجرائم المعلوماتية على حد سواء في ضرورة تبيان محل التفتيش وماهية السلطة المختصة بذلك (فرع أول)، بالإضافة غلى ذلك توضيح السبب الذي من خلاله يتم اللجوء إلى هذا الإجراء (فرع ثاني).

الفرع الأول: محل التفتيش والسلطة المختصة

يجيب أن يكون للتفتيش محلا والمتمثل إما في الشخص أو المكان ويشترط موضوع التفتيش المحل أن يكون محددا أو قابلا للتحديد وأن يكون مشروعا، اي يرد على محل جائز قانونا[17]، ويقصد به ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال به[18].

لكي يكون التفتيش في جرائم نظم المعلومات أو غيرها صحيحا ومنتجا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية باختلاف تشريعات الدول، مع مراعاة الاختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة، وإما بمكان إقامة المتهم أو مكان القبض عليه.

---

16 – **صالح شنين**، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2013/2012، ص 237.

17 – **عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري**، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة مقارنة"، مداخلة موجهة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد بتاريخ 12-14 نوفمبر 2008، بجامعة نايف العربية للعلوم الأمنية، الرياض، ص 19.

18 – **بن طالب ليندا**، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، ص 59.

إلا أنه استثناء، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وذلك وفقا للشروط والإجراءات المنصوص عليها في القانون، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناء على إذن بالتفتيش صحيح صادر من هيئة مختصة، وفي غياب هذا الإذن، أو صحته يصبح عدم مشروعية التفتيش أمرا مؤكدا[19].

الفرع الثاني: ضرورة توفر سبب التفتيش

أ-وقوع جريمة معلوماتية

إن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، إلا أنه بالرجوع إلى نص المادتان 04 و05 من القانون رقم 09-04 يتبين أن المشرع الجزائري قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة[20].

ب-توجيه التهمة لشخص معين

ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب جريمة معلوماتية بوصفه فاعلا لها أو شريكا فيها، مما يستوجب اتهامه فيه، وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش التي تؤيد نسبة تلك الجريمة المعلوماتية إلى ذلك الشخص بوصفه فاعلا أو شريكا[21].

ج-توفر أدلة مادية تكشف الجريمة

لا يكفي وقوع جريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الإلكترونية، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية وقرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو أية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة[22].

---

19 – **برهيمي جمال**، مرجع سابق، ص 38.

20 – **بن طالب ليندا**، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، مرجع سابق ص 59.

21 – **نزيهة مكاري**، مرجع سابق، ص 131.

22 – **براهيمي جمال**، مرجع سابق، ص 34.

نستخلص مما سبق أن أغلب التشريعات ومنها المشرع الجزائري أحاط إجراء التفتيش بعدة ضمانات وذلك سعيا منه إلى حماية خصوصية الأفراد من الاعتداء، غير أن الملاحظ بالنسبة لهذه الضمانات أصبحت تشكل عقبة أدت إلى الحد من فعالية هذا الإجراء، وذلك راجع إلى عدم مواكبته للسرعة التي تعرفها جرائم نظم المعلوماتية سواء من ناحية السرعة في ارتكاب هذه الجريمة أو من حيث السرعة في إخفاء ومحو الدليل المنجر عنها.

الخاتمة:

نستنتج مما سبق أن التفتيش كإجراء من إجراءات التحقيق في العالم الافتراضي أثبت فعاليته في مكافحة الجريمة المرتكبة عبر النظم المعلوماتية، سواء من الناحية القانونية أو الفعلية، غير أن هذه الفعالية غير مطلقة نظرا لما يتميز به من خصوصيات سواء من ناحية القيام بالتفتيش، حيث يتميز عن التفتيش في العالم التقليدي بأنه يتم في عالم افتراضي غير محسوس وما ينجر عنه من عراقيل قانونية خاصة في حالة التفتيش عن بعد، أو من ناحية الضمانات المكرسة من أجل إجراء التفتيش، خاصة وأن هذا الأخير دائما ما يصطدم بضرورة حماية الحياة الخاصة للأفراد، والملاحظ أن هذه الضمانات غير كافية لحمايتها، وذلك أن الحياة الخاصة تطورت بتطور عالم التقنية، فالنظرة التقليدية للحياة الخاصة انتهت مع ظهور ما يسمى الحياة الخاصة التقنية والفنية، والتي لا تخضع إجراءات البحث والتحري فيها إلى رقابة القاضي كما هو الحال في العالم التقليدي، بل تخض لرأي الخبراء بما أنها إجراءات فنية، الأمر الذي يدعو المشرع إلى ضرورة:

- إعادة النظر في الترسانة القانونية الإجرائية.
- تكوين قضاة متخصصين في مجال التقنية العالية لفرض الرقابة القانونية اللازمة الخاصة بالإجراءات المستحدثة بما فيها التفتيش.
- ضرورة وضع أطر قانونية مستحدثة تكرس التعاون الدولي في مجال إجراء التفتيش عبر شبكة الإنترنت
- ضرورة إنشاء وحدات أمنية متخصصة في مجال المعلوماتية ومكافحة الجرائم المرتكبة في هذا المجال
- ضرورة تحسيس المواطنين بالتبليغ عن جرائم نظم المعلوماتية من أجل السماح للضبطية القضائية القيام بمهامها بصفة أكثر فعالية.

قائمة المراجع

الكتب

1. **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د.ن، د.ب.ن، 2005.
2. **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

3. **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

المقالات

1. **أسامة بن غانم العبيدي**، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، د.س.ن.
2. **بوعناد فاطة الزهرة**، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، كلية، مجلة إلكترونية خاصة تعنى بنشر الدراسات القانونية، العدد الأول، 2013.
3. **حسين بن سعيد الغافري**، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت"، ص 11-12، مقال متوفر عبر الموقع التالي: http://www.eastlaws.com
4. **نزيهة مكاري**، "إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري، (دراسة مقارنة)"، مجلة العلوم الاقتصادية وعلوم التسيير، كلية العلوم الاقتصادية، جامعة فرحات عباس، سطيف، العدد 09، سنة 2009.
5. **رابح وهيبة**، "الجريمة المعلوماتية في التشريع الإجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخظر، باتنة 1، العدد الرابع، ديسمبر 2014.
6. **رضا هميسي**، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 05، جوان 2012.
7. **عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري**، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة مقارنة"، مداخلة موجهة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد بتاريخ 12-14 نوفمبر 2008، بجامعة نايف العربية للعلوم الأمنية، الرياض.
8. **ليندا بن طالب**، "التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، عدد 16، جوان 2017.

الرسائل الجامعية

1. **براهيمي جمال**، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.
2. **بن طالب ليندا**، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو.

3. **صالح شنين**، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2013/2012.

النصوص القانونية

1. قانون رقم 09-04، المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر عدد 47، صادر في 16 غشت 2009.