خصوصية التفتيش في البيئة الالكترونية

Electronic Environment Search Specifications

حطاب كمال ♦

جامعة جيلالي ليابس- سيدي بلعباس / الجزائر

Kamalhat5@gmail.com

تاريخ الإرسال: 2022/09/28	تاريخ القبول: 2023/05/31	تاريخ النشر: 2023/07/03

الملخص:

التفتيش هو الاطلاع على مستودع سر الشخص بهدف ضبط أدلة مادية تساعد على ظهور الحقيقة، وهو بهذا يقدم خدمة للعدالة، ولكنه في الوقت نفسه يمس حرمة الحياة الخاصة للأفراد، لذلك أحاطته التشريعات المختلفة بمجموعة من الضمانات، لكن الوضع يدق عندما يتعلق الأمر بالتفتيش في البيئة الالكترونية لما تتميز به من خصائص ومميزات، تفرض في سبيل استخلاص الدليل، الخروج عن القواعد العامة للتفتيش، ولكن دون التضحية بحرمة الحياة الخاصة.

الكلمات المفتاحية: تفتيش، قبض، جرائم معلوماتية، الحق في الخصوصية.

Abstract:

Search is the access to a secret place of a person for seizing physical evidence that helps to reveal the truth, and in this way, it does a service to justice, but at the same time it affects the sanctity of the privacy of individuals, therefore various legislations have surrounded it with a set of guarantees. The situation becomes delicate when it concerns the inspection in the electronic environment, which is distinguished by its characteristics, which impose to extract evidence, deviate from the general rules of inspection, but without sacrificing the sanctity of privacy.

Keywords: Search ; Arrest warrant ; Computer fraud ; Right to privacy.

♦ المؤلف المرسل

خصوصية التفتيش في البيئة الإلكترونية

مقدمة:

مع التطورات العلمية والتقنية المتلاحقة، ظهرت أنواع جديدة من الجرائم لم تكن معروفة من قبل، كما أخذت كثير من الجرائم التقليدية أبعادا مختلفة لاستغلالها الكبير للعلوم والتقنيات الحديثة، قصد تحقيق أهداف إجرامية بأكثر سرعة وأقل عناء، وأضخم حجما، حتى باتت تهدد الدول في اقتصادياتها وسياساتها الإنمائية، ومن هذه الجرائم ما يعرف بالجرائم المعلوماتية (أو الجرائم الالكترونية أو السيبرانية أو جرائم تقنية المعلومات..).ويمكن ردها إجمالا إلى نوعين: جرائم ترتكب بواسطة أنظمة المعالجة الآلية للمعطيات كالقرصنة والاحتيال الالكترونيين، والابتزاز عبر الانترنت، والنصب والاحتيال عبر شبكات التواصل الاجتماعي وغيرها، والجرائم الواقعة على نظام المعالجة الآلية للمعطيات نفسه، كالدخول غير المسموح به لنظام المعالجة الآلية للمعطيات، وزرع الفيروسات داخل هذه الأنظمة.

هذه الجرائم المعلوماتية لها خصوصيات، تجعل من الصعب على القائمين على جمع الأدلة اكتشاف مرتكبيها باتباع الطرق التقليدية في البحث والتحري عن الجرائم، لذا عمدت التشريعات المقارنة ومنها التشريع الجزائري إلى استحداث آليات جديدة تعتمد على العلوم والتقنيات العالية لمواجهة هذه الجرائم.

من الآليات التي يعتمد عليها المحققون لضبط الأدلة وكشف الحقيقة إجراء التفتيش، وهو إجراء مفيد جدا للوصول لفك لغز القضية، ولكنه في الوقت نفسه يمس حرمة الحياة الخاصة للأفراد، لذا وضعت التشريعات المختلفة جملة من الضمانات على شكل شروط موضوعية وأخرى شكلية، لتحقيق الموازنة بين مصلحة الأفراد ومصلحة المجتمع، بيد أن التشريعات وجدت نفسها تخرج عن القواعد العامة للتفتيش التي ألفها الناس وفسرها الفقه وكرسها مبادئها القضاء، حتى يمكن لهذا الإجراء من تحقيق أهدافه ولكن دون التفريط في الضمانات الممنوحة للأفراد، وصونا لمبدأ الشرعية الإجرائية.

مما تقدم يمكن طرح الإشكال التالي: كيف يتم إجراء التفتيش في البيئة الإلكترونية؟ وإلى أي مدى وفق المشرع الجزائري من خلال التعديلات التي جاء بها في قانون الإجراءات الجزائية وفي القانون 09-04 في تحقيق الموازنة المطلوبة: مواجهة الجريمة المستحدثة بفعالية وعدم المساس بحقوق الأفراد المكرسة في الدستور والمواثيق الدولية؟

تم الاعتماد على المنهج التحليلي المقارن، لمعالجة هذا الموضوع، من خلال تقسيمه إلى فكرتين رئيسيتين، عالجت الأولى موضوع خصائص التفتيش في البيئة الإلكترونية من خلال الحديث عن مدى خضوع مكونات الحاسب الآلي للتفتيش، ومدى قابلية شبكات الإعلام الآلي للتفتيش، أما الفكرة الثانية فتناولت شروط التفتيش عن في البيئة الإلكترونية، سواء أكانت هذه الشروط موضوعية، أم شكلية أم فنية.

1- خصائص التفتيش في البيئة الإلكترونية:

لقد ثار جدل فقهي حول مدى صلاحية مكونات الحاسب الآلي المعنوية للتفتيش، والضوابط التي يجب مراعاتها أثناء عمليات التفتيش في البيئة الرقمية، ذلك أن التفتيش بالمعنى التقليدي ينصب على الأشياء المادية الملموسة فقط، أما التفتيش في البيئة الرقمية فنطاقه أوسع وطبيعته مختلفة.

1.1- مفهوم التفتيش في البيئة الرقمية:

لم يعرف المشرع الجزائري التفتيش، سواء في قانون الإجراءات الجزائية[1]، أو في القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، واكتفى بتنظيم أحكامه في بعض مواد قانون الإجراءات الجزائية[3]، وكذا بعض مواد القانون 09-04 سالف الذكر، وخاصة المادة 5.

يعتبر كثير من الفقهاء التفتيش عملا من أعمال التحقيق[4]، يستهدف كشف الحقيقة بشأن الجرم الواقع، ومدى ثبوته في مواجهة المتهم، وهو البحث في مستودع أسرار المتهم[5]، ولقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، وإما أن يأذن بذلك لأحد ضباط الشرطة القضائية من خلال الإنابة القضائية، ويشمل التفتيش الأشخاص والمنازل، وهو من الإجراءات الخطيرة التي تمس بحريات الأشخاص وحرمة منازلهم، لذا أحاطته الدساتير والمواثيق الدولية، والتشريعات المقارنة بعدد من القيود كضمانات لحريات الأفراد وصونا لمبدأ المشروعية الإجرائية[6].

والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة، لضبط أشياء تتعلق بالجريمة، أو تفيد في الحصول على أدلة مادية تسهم في ظهور الحقيقة، وعليه فإن كل تفتيش تكون غايته خلاف ذلك يكون باطلا[7]، بطلانا مطلقا لتعلقه بالنظام العام[8].

---

[1] الأمر 56-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[2] القانون رقم 09-04 لمؤرخ في 14 شعبان 1430هـ الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 الصادر في 16 غشت 2009.

[3] في المواد من 44 إلى 48 تحت عنوان "الجناية أو الجنحة المتلبس بها"، والمادة 64 تحت عنوان "في التحقيق الابتدائي" والمواد من 79 إلى 86 تحت عنوان "في الانتقال والتفتيش والقبض" وكذا المادة 122 تحت عنوان "في أوامر القضاء وتنفيذها".

[4] محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر 2008، ص535، فقرة 282.

[5] عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر- 2012، ص125.

[6] جلال ثروت، سليمان عبد المنعم، أصول الإجراءات الجنائية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر2006، ص546.

[7] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر 2009، ص631.

[8] المرجع نفسه، ص640.

التفتيش في البيئة الإلكترونية أو الرقمية يعد من أخطر المراحل وأدقها نظرا لما تتسم به الجرائم المعلوماتية من خصوصية، تتعلق أساسا بمرتكبيها، وطبيعتها الفنية، وحجم ضررها، واتساع نطاقها[1].

2.1- مدى خضوع مكونات الحاسب الآلي للتفتيش:

يتألف الحاسب الآلي من مكونات مادية(hardware) وأخرى منطقية أو معنوية(software)، فهل كل هذه المكونات يجوز تفتيشها؟ وكيف يتم ذلك؟

1.2.1- تفتيش المكونات المادية للحاسب الآلي:

إن المكونات المادية للحاسب الآلي ولواحقه، كالذاكرة المركزية والطابعة والأقراص المضغوطة، والماسح الضوئي وغيرها، لا تثير أية مشكلة بخصوص جواز انطباق قواعد التفتيش التقليدية عليها، بالشروط ذاتها المطبقة بخصوص التفتيش في الجرائم التقليدية، بمعنى أن حكم تلك المكونات يتوقف على طبيعة الأماكن الموجودة فيها، سواء الأماكن العامة أو الخاصة، فإذا كانت موجودة في مكان خاص كمنزل المتهم أو مكتبه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المسكن، وبالضمانات المقررة قانونا، وفي الأوقات المقررة للتفتيش، وهذا ما أخذت به بعض التشريعات[2]، والهدف من وراء هذا التفتيش هو استخلاص دليل مادي على قيام المتهم بارتكاب الجريمة كاستخدامه للحاسب الآلي والطابعة الملونة في تزوير الأوراق النقدية[3].

أورد المشرع الجزائري في نص م1/64 من ق إ ج شروط تفتيش المساكن، ولكنه أورد عليها استثناءات بموجب القانون رقم 22/06 المعدل للأمر 66-155 المتضمن قانون الإجراءات الجزائية، إذ استثنى تطبيق هذه الضمانات على بعض الجرائم المستحدثة (م2/64 ق إ ج)، نظرا لخطورتها وطابعها الخاص، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وأجاز المشرع بذلك إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص (م3/47 ق إ ج)، كما يجوز في هذه الحالة لقاضي التحقيق القيام بالتفتيش، أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك (م4/47 ق ا ج)، والسؤال المطروح هنا: هل هذا الاستثناء يخص تفتيش المكونات المادية والمكونات المعنوية للحاسب الآلي على حد سواء؟ أم أنه متعلق فقط بتفتيش المكونات المعنوية؟ لم يبين المشرع الجزائري ذلك، وعليه وجب الأخذ بعموم النص، وإن كان من الأحسن إذا تعلق الأمر بتفتيش

---

[1] يراجع كل من:
نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان الأردن 2008، ص ص 45-94.
خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، شارع سوتير، الإسكندرية، مصر 2008، ص ص 69-88.

[2] ومنها التشريع المصري. يراجع:
عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي، في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، مصر، ص89.

[3] حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر 2017، ص43.

المكونات المادية للحاسب الآلي الموجودة داخل المسكن الأخذ بالقواعد العامة (م1/47 ق ا ج) بدل الاستثناء (م2/64 ق ا ج).

2.2.1- تفتيش المكونات المعنوية للحاسب الآلي:

لقد ثار خلاف تشريعي وفقهي بشأن المكونات المنطقية أو المعنوية للحاسب الآلي، بين مجيز لتفتيشها نظرا لعموم النص الوارد في كثير من النصوص الإجرائية المقارنة "ضبط أي شيء" ليشمل مكونات الحاسب الآلي المادية والمعنوية، وبين رافض لذلك باعتبار أن مفهوم التفتيش مفهوم مادي، وهو لا ينطبق على مكونات الحاسب الآلي المعنوية، وكان هذا الرأي الأخير سائدا عند بعض الفقه الفرنسي- إلى أن قام المشرع الفرنسي- بتعديل نصوص التفتيش بموجب القانون رقم 245-2004 المؤرخ في 2004/06/21، وقام بإضافة عبارة "المعطيات المعلوماتية" في م94 ق إ ج ف[1]، فأصبح الرأي الأول هو الراجح.

ومن الآراء الفقهية الأخرى حول المكونات المنطقية أو المعنوية للحاسب الآلي نجد فريقا فقهيا يذهب إلى القول بضرورة النظر إلى الواقع العملي، الذي يقتضي أن يقع الضبط على بيانات الحاسب إذا اتخذت شكلا ماديا، ومعنى ذلك أن البيانات المنفردة عن الدعامات لا تعد من قبيل الأشياء، وبالتالي لا يمكن ضبطها، غير أنه إذا تم طبع هذه البيانات، فإن مطبوعاتها تعد من الأشياء الملموسة المحسوسة التي يجوز ضبطها[2].

هناك اتجاه فقهي آخر يرى أن الأساس في تحديد مدلول الشيء فيما يخص مكونات الحاسب الآلي هو تحديد مدلول مصطلح المادة في العلوم الطبيعية، وكذا معرفة خصائص وكنه مكونات الحاسب المعنوية أو المنطقية؛ وبناء عليه يرى هذا الاتجاه أن البيانات والمكونات المنطقية للحاسب الآلي ليست من قبيل الشيء المعنوي كالآراء والأفكار والحقوق، بل يجوز اعتبارها أشياء لها وجود في العالم الخارجي الملموس، وهي شبيهة بالتيار الكهربائي، لذا يجوز أن يرد عليها الضبط والتفتيش، وهذا ما ذهبت إليه محكمة باريس الابتدائية في حكم لها، حينما قضت بأنه لا يوجد اختلاف في الطبيعة بين مخرجات البرامج وبين البرامج المستغلة، وكذلك وصفت محكمة جنح بروكسل هذه البيانات أو المكونات المنطقية بأنها تعد من قبيل الأشياء المحسوسة التي لها وجود مادي حقيقي[3].

---

[1] Voir l'article 94 du code de procédure pénal français, dernière modification le 15 avril 2022, document pdf, téléchargé à partir du site : www.légifrance.gouv.fr, vu le : 18/04/2022 à 22h.

[2] سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة الإسكندرية، مصر- 2010، ص253.

[3] سامح أحمد، المرجع السابق، ص ص254-255.

ولكن في حقيقة الأمر، هذه المكونات ليست شيئا محسوسا، ولكنها عبارة عن بيانات ونبضات إلكترونية، وقد قضت محكمة النقض الفرنسية في حكم لها، صادر سنة 1994 بأنه من غير المستساغ مقارنة الحصول على خدمات عن بعد بواسطة الانترنت بسرقة الكهرباء، فالمعلومات إبداع فكري محمي بقوانين حماية المؤلف[1].

أما الاتفاقية الأوربية حول الجرائم المعلوماتية، فقد نصت في م19 من القسم الرابع على أن لكل دولة طرف أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به، وكذا إلى الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها.

كما أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21، والتي صادقت عليها الجزائر[2]، نصت في م1/26 منها بأن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات أو جزء منها، والمعلومات المخزنة فيها أو المخزنة عليها، وكذا الوصول إلى بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

تطرق المشرع الجزائري إلى تفتيش المنظومات المعلوماتية في م5 من القانون 09-04، والتي نصت: "يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية...الدخول بغرض التفتيش ولو عن بعد إلى:

أ) منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها،

ب) منظومة تخزين معلوماتية...."

بنص المشرع الجزائري الصريح على تفتيش المنظومة المعلوماتية في م05 من القانون 09-04 يكون قد الخلاف الفقهي في الجزائر حول جواز تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما أنه أجاز في الفقرة الأخيرة من المادة نفسها أن تستعين السلطات المكلفة بالتفتيش بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

وقد حذا المشرع المصري حذو المشرع الجزائري في القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات، بحيث أجازت م2/6 من هذا القانون لجهات التحقيق المختصة حسب الأحوال البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها تحقيقا لغرض الضبط[3].

---

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر 2011، ص136.

[2] المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج رعدد 57، صادر في 28 سبتمبر 2014.

[3] الجريدة الرسمية لجمهورية مصر العربية، العدد 32 مكرر(ج) الصادر في 14 أغسطس 2018. اطلع عليها من موقع محكمة النقض المصرية: cc.gov.eg تاريخ الولوج: 2022/04/18 على الساعة 21.

أثار الفقه أيضا مسألة مدى شرعية إرغام صاحب نظام المعالجة الآلية للمعطيات، في حالة تمتع الجهاز بنظام حماية، على الإفصاح عن كلمة المرور وما في حكمها، ليتسنى للمكلفين بالتفتيش الولوج إلى نظام المعالجة والقيام بعملية التفتيش، وانقسم إلى فريقين: فريق مؤيد وحجته تغليب المصلحة العامة، وأن إجبار الشخص على ذلك ليس بدعة وإنما مثيله في القانون إجبار المتهم على تسليم مفتاح الخزانة التي بحوزته لفتحها والقيام بتفتيشها، وفريق يرفض ذلك وحجتهم القاعدة القانونية التي ترفض إجبار الشخص على الإدلاء بأقوال تدينه، ولعل هذا الرأي الثاني هو الأرجح خاصة وأنه يتوافق مع ما جاء في نص م100 ق ا ج[1].

3.1- مدى قابلية شبكات الحاسب الآلي للتفتيش:

ترتبط أجهزة الحاسب الآلي أحيانا ببعضها بعضا عن طريق شبكات، قد تكون داخل الشركة أو المؤسسة أو فروعها، داخل الحدود السياسية لدولة واحدة أو خارجها، كأن يرتبط جهاز في فرع الشركة الأم، ببلد معين مع أجهزة أخرى في فروع تابعة لهذه الشركة في بلدان أخرى.

هذا الأمر يعقد من التحديات التي تقف أمام التفتيش والضبط. والسؤال المطروح: هل يمتد تفتيش حاسب معين إلى الأجهزة المرتبطة به سواء كانت موجودة داخل البلاد أم خارجها؟

1.3.1- وجود الحاسب المراد تفتيشه في مكان آخر داخل الدولة:

الفرض هنا أن يتصل حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة نفسها.

أجازت التشريعات المقارنة امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر من الدولة، منها القانون الألماني، والقانون البلجيكي، والقانون الأسترالي[2]، وأجاز المشرع الأمريكي أن يمتد التفتيش الصادر بتفتيش مقر شركة معينة إلى فروع تلك الشركة الكائنة في العقار نفسه[3]، كما أجازه المشرع الجزائري في م05 من القانون 09-04 "... ولو عن بعد".

أما م1/17 من القانون الفرنسي رقم 239 لسنة 2003 بشأن الأمن الداخلي الصادر في 2003/03/18، فقد أجازت لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي تحت مسؤولية الضباط، أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق

[1] مليابي عبد الوهاب، أمن المعلومات في بيئة الأعمال الإلكترونية، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر 2017/2016، ص300.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة 2009، ص482.

[3] سامح أحمد، المرجع السابق، ص256.

والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيس، أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيس[1].

وكانت اتفاقية بودابست لعام 2001 قد نصت في م19 من القسم الرابع على: "من حق السلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة اختصاصاتها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر، إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش".

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر فقد نصت في م2/26 على أن "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها...فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

وبخصوص تفتيش الحاسبات الآلية التي تقع في أماكن عامة كالحاسبات الشخصية التي يحملها الشخص خارج منزله، أو الهواتف الذكية، فإن تفتيش أنظمتها لا يكون جائزا إلا في الأحوال التي يجيز فيها القانون تفتيش شخصه[2]، باعتبار أن تفتيش الشخص يشمل ذاته وكل ما في حوزته وقت هذا التفتيش، سواء أكان ملكا له أم لغيره، وفي الحالة التي يكون فيها الجهاز المراد تفتيشه داخل منزل أحد الأشخاص، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش مسكن المتهم أو تفتيش منزل غير المتهم[3].

2.3.1- وجود الحاسب أو الجهاز المراد تفتيشه متصلا بنهاية طرفية أو جهاز آخر خارج حدود الدولة:

من المشاكل التي تواجه القائمين على جمع الدليل الإلكتروني، قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة، مستخدمين في ذلك شبكة الاتصالات البعدية، بهدف عرقلة سير التحقيق ومن ثم الإفلات من العقاب، نتيجة تمسك كل دولة بسيادتها[4]، لذا ينبغي أن يتم التفتيش الإلكتروني في إطار اتفاقيات ثنائية تبرم بين الدول المعنية، وهذا يدخل ضمن إطار التعاون الدولي في مجال مكافحة ومجابهة الجرائم المعلوماتية، وهذا ما تطرقت له م05 من القانون 09-04 في إحدى فقراتها: «إذا تبين مسبقا بأن المعطيات المبحوث عنها ... فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل".

---

[1] عائشة بن قارة، المرجع السابق، ص94.

[2] لم ينظم القانون الجزائري مسألة التفتيش القضائي للأشخاص، ولكن الفقه يرى أن تفتيش بيت الشخص يجيز تفتيش شخصه، بل وتفتيش أفراد عائلته الذين يقطنون بالمسكن معه، وكل شخص متواجد بالمسكن محل التفتيش، كما يجيز الفقه لقاضي التحقيق الأمر بتفتيش الشخص إذا وجهت له النيابة العامة اتهاما في طلبها الافتتاحي أو في طلب إضافي إعمالا لنص م67 ق ا ج. يراجع:
عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار هومة، الجزائر 2018، ص488.

[3] الغافري، المرجع السابق، ص ص485-486.

[4] الغافري، المرجع السابق، ص484.

وقد أكد المجلس الأوربي في التوجيه رقم 17 لسنة 1995 على جواز امتداد نطاق تفتيش الحاسب إلى النظام المتواجد في الخارج، إذا كانت هناك ضرورة لاتخاذ إجراءات عاجلة في هذا الصدد، ويتوجب حينها الحصول على موافقة الدولة التي يمتد التفتيش إلى الأجهزة أو النظام المتواجد في إقليمها، كي يكون هذا التفتيش ذا أساس قانوني، ولا يمثل انتهاكا لسيادة تلك الدولة[1].

غير أن م32 من الاتفاقية الأوربية بشأن الجرائم المعلوماتية سالفة الذكر، أجازت الولوج بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى دون أخذ الإذن منها في حالتين: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، أو إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش، أي إذا رضي من يملك السلطة القانونية للكشف عن تلك البيانات، ويقصد به هنا مزود الخدمة، فإن كان للشخص بيانات مخزنة في دولة ما في بريده الإلكتروني مثلا، فإنه يجوز تفتيشها إذا قبل مزود الخدمة في هذه الدولة ذلك[2].

وقد أجازت م17-2/1 من قانون الأمن الداخلي الفرنسي سالف الذكر لمأموري الضبط القضائي القيام بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم الفرنسي، مع مراعاة الالتزامات الدولية.

2- شروط التفتيش في البيئة الإلكترونية:

حتى يقوم التفتيش صحيحا منتجا لآثاره، لا بد من توافر شروط موضوعية وأخرى شكلية.

1.2- الشروط الموضوعية للتفتيش في البيئة الرقمية:

الشروط الموضوعية لتفتيش جهاز الحاسب الآلي ومن هو في حكمه، فيقصد بها الضوابط المطلوبة لإجراء تفتيش صحيح، ويمكن حصرها في ثلاثة شروط رئيسة هي السبب، المحل، والسلطة المختصة للقيام بالتفتيش.

1.1.2- سبب التفتيش في البيئة الإلكترونية والسلطة المختصة به:

سبب التفتيش في البيئة المعلوماتية هو السعي نحو الحصول على دليل من أجل الوصول إلى اكتشاف الحقيقة، ويقتضي ذلك أن تقع جريمة من الجرائم المعلوماتية كالمساس بأنظمة المعالجة الآلية للمعطيات، أو الاستعمال غير المشروع لبطاقات الائتمان، أو التعدي على البيانات الشخصية، أو تبييض الأموال عبر الانترنت، وغيرها من الجرائم الواقعة على نظام المعالجة الآلية للمعطيات، أو الجرائم الواقعة باستعماله، ويشترط أن تشكل هذه الجرائم جنحا أو جنايات، فالمخالفات البسيطة تستبعد من نطاق التفتيش لتفاهتها، وعلى ذلك

[1] سامح أحمد، المرجع السابق، ص258.
[2] المرجع نفسه، ص259.

لا يجوز كأصل عام التفتيش أو الإذن به لضبط جريمة مستقبلية ولو ترجح وقوعها بالفعل، ذلك أن التفتيش ليس وسيلة لاكتشاف الجرائم بل إجراء من إجراءات التحقيق[1].

لكن المشرع الجزائري خرج عن هذا الأصل في نص م3 من القانون 09-04 التي أجازت وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية والقيام بإجراءات التفتيش والحجز (الضبط) داخل منظومة معلوماتية إذا تعلق الأمر بحماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية.

ويخشى من هذه المادة أن تمس بحرمة الحياة الخاصة للأشخاص دون مسوغ معقول، لأن استعمال المشرع لمصطلحين واسعي الدلالة (النظام العام ومستلزمات التحريات والتحقيقات) قد يفتح الباب للتوسع في اللجوء إلى مقتضيات نص م3 من القانون 09-04 لعدم وجود ضابط دقيق ومعيار واضح للمصطلحين المستعملين.

كما ينبغي أن تتوافر في حق من يراد تفتيش شخصه أو مسكنه دلائل قوية[2]، تدعو للاعتقاد أنه مساهم في الجريمة المعلوماتية، سواء أكانت المساهمة أصلية أم تبعية، أو توافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة لدى المشتبه فيه أو غيره[3]، وقد حددت المادة الرابعة من القانون 09-04 سالف الذكر الحالات التي تجيز تفتيش المنظومة المعلوماتية، ومنها مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى التفتيش، وكذا في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

أما فيما يخص السلطة المختصة بالتفتيش فإن الأصل أن يقوم قاضي التحقيق بالتفتيش (الجزائر)، أو النيابة العامة (مصر)، إلا أنه يجوز لضابط الشرطة القضائية القيام بذلك استثناء في حالة التلبس، وكذا في حالة الانتداب حسب القواعد العامة.

وكذا يجوز إجراء التفتيش باعتباره إجراء من إجراءات الاستدلال لا التحقيق، من قبل ضابط أو عون الشرطة القضائية في الأحوال العادية شريطة الرضا الصريح ممن يراد تفتيشه أو تفتيش جهازه[4]، كأن يقبل

---

[1] محمد زكي أبو عامر، المرجع السابق، ص538، فقرة283.

[2] لم تتطرق القوانين إلى تعريف المراد بالدلائل القوية، إلا أن الفقه حاول إجلاء الغموض عنها، ومن ذلك تعريفها بأنها: مجموعة من الوقائع الظاهرة والملموسة التي يستنتج منها أن شخصا معينا هو مرتكب الجريمة. وفي مجال الجرائم الإلكترونية فيقصد بالدلائل القوية أو الكافية مجموعة المظاهر أو الأمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للقائم بالتفتيش، والتي تؤيد نسبة ارتكاب الجريمة الالكترونية إلى شخص معين، سواء أكان فاعلا أم شريكا، ومن أمثلتها ارتباط عنوان انترنت بروتوكول الخاص بجهاز الحاسب الذ يحوي صورا فاضحة مثلا مع رقم حساب المتهم لدى مزود الخدمات، ووجود رقمين للهاتف لديه يستخدمان لذلك. ينظر:
شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر 2007، ص282.

[3] عائشة بن قارة، المرجع نفسه، ص103.

[4] إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، بن عكنون، الجزائر 1993، ص96.

الشخص صراحة لدحض الاشتباه عنه، أن يتأكد ضابط أو عون الشرطة القضائية من أن الهاتف المحمول للشخص ليس به صور فاضحة ملتقطة لأشخاص في أماكن خاصة.

بخصوص الاختصاص المحلي، سواء لوكيل الجمهورية أو قاضي التحقيق، فإن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1]، هو المختص حصريا لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وفق ما جاء في نص م211 مكرر26 ق ا ج، وهذا إذا تعلق الأمر بالجرائم المذكورة في نص م211 مكرر24 ق ا ج[2]، وكذا الجرائم المذكورة في نص م211 مكرر25 ق ا ج[3]، ويكون له اختصاص مشترك مع الاختصاص الناتج عن تطبيق المواد 37، 40، و329 من ق ا ج إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها (م211 مكرر1/27 ق ا ج)، أما إذا تزامن اختصاصه مع اختصاص القطب الاقتصادي والمالي[4]، فإن الاختصاص يؤول وجوبا لهذا الأخير (م211 مكرر28 ق ا ج)، وكذلك الأمر إذا تزامن اختصاصه مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقا للأحكام الواردة في المواد 211 مكرر 16 إلى 211 مكرر21 ق ا ج، فإن الاختصاص يؤول وجوبا لهذه الأخيرة.

يمارس وكيل الجمهورية وقاضي التحقيق لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال صلاحياتهم في كامل التراب الوطني (م211 مكرر23 ق ا ج).

2.1.2- محل التفتيش في البيئة الإلكترونية:

محل التفتيش في الجرائم المعلوماتية هو الحاسب الآلي أو أي جهاز آخر يقوم مقامه، وكذا الشبكة بكل ملحقاتها، ويجب أن يحدد في إذن الانتداب بالتفتيش المكانُ المراد تفتيشه، والشخص والأشياء المراد تفتيشها، فلا بد من التحديد لتجنب التفتيش الاستكشافي، بحيث لا يكون للضابط المنتدب أية سلطة تقديرية في ذلك، إلا أن هناك صعوبة في احترام هذا الشرط عمليا، نظرا للطبيعة الخاصة لأجهزة الحاسب الآلي التي تحوي عددا كبيرا من الملفات، كما أن أسماء هذه الملفات لا تدل بالضرورة على مسمياتها، فمن الوارد جدا أن يعمد المتهم إلى وضع أسماء مستعارة لملفات تحوي مواد غير مشروعة.

---

[1] استحدث هذا القطب بموجب الأمر 21-11 المؤرخ في 25 غشت 2021، المتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر، العدد 65 الصادر في 26 غشت 2021.

[2] وهي الجرائم التي تمس بأمن الدولة، جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع، جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العمومين ذات الطابع المنظم أو العابر للحدود الوطنية، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، جرائم الاتجار بالأشخاص أو بالأعضاء البشرية، أو تهريب المهاجرين، جرائم التمييز وخطاب الكراهية. وكل الجرائم المرتبطة بهذه الجرائم.

[3] وهي الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها.

[4] الذي تم استحداثه بموجب الأمر 20-04 المؤرخ في 30 غشت 2020 المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر، العدد 51، الصادر في 31 غشت 2020.

وقد أثيرت بعض الأسئلة بخصوص تفتيش أجهزة الحاسب الآلي منها: هل يعتبر كل ملف من ملفات الحاسب الآلي المراد تفتيشه صندوقا مغلقا يحتاج كل واحد منها إلى إذن قضائي خاص؟ أم أن إذنا واحدا يكفي لتفتيشها كلها؟

تضاربت أحكام القضاء الأمريكي بشأن هذه المسألة، حيث اعتبرت بعضها أن القرص الصلب بما يحويه من ملفات وجهاز الحاسب الآلي بما يحويه من ملفات صندوقا مغلقا واحدا، مما يجيز تفتيش الجهاز كله بما فيه من ملفات مختلفة، بناء على إذن تفتيش واحد، وعلى خلاف ذلك اعتبرت أحكام أخرى في القضاء الأمريكي أن كل ملف في جهاز الحاسب الآلي يتطلب إذنا خاصا لتفتيشه، وبناء عليه اعتبرت كل ملف صندوقا مغلقا؛ وأحكام هذا الاتجاه تعتبر أن جهاز الحاسب الآلي يحوي الكثير من المعلومات المتعلقة بالحياة الخاصة لصاحبه، التي يجب أن تصان من الاعتداء عليها[1].

غير أن اعتبار كل ملف من ملفات الحاسب الآلي صندوقا مغلقا يستوجب تفتيشه إذنا خاصا، أمر في غاية الصعوبة من الناحية العملية، خاصة مع التطور السريع لتقنيات الحاسب الآلي وخاصة من حيث السعة التي يمكن أن يحويها القرص الصلب، إذ بإمكانه أن يحوي عددا كبيرا جدا من الملفات، وكل ملف يحوي ملفات عديدة بداخله مما يجعل عدد الملفات قد يصل إلى مئات الآلاف، بل الملايين، فهل يعقل أن تستصدر مائة ألف أو أكثر من الأذونات لتفتيش جهاز حاسب آلي واحد؟ ولكن من ناحية أخرى لا يستساغ أن يمتد إذن التفتيش ليطال كل ملفات الحاسب، فتستباح بذلك حياة الشخص الفردية دونما مسوغ، وعليه يجب أن يقيد التفتيش للغرض الذي صدر الإذن لأجله، وهو الحصول على أدلة تفيد القضية محل التحقيق، فمجرد الحصول على هذه الأدلة يتوقف التفتيش، إذ لا داعي للاستمرار فيه حتى وإن كان ذلك سيكشف عن جرائم أخرى، طالما أن الإذن بالتفتيش محدد[2].

غير أنه وتطبيقا للقواعد العامة، إذا صادف المفتش أثناء بحثه عن الدليل بصدد الجريمة المحقق فيها جريمة أو أكثر عرضية مثل حيازة صور فاضحة فإن أدلة الإدانة بهذه الجريمة صحيحة ولا يشوبها البطلان[3].

2.2- الشروط الشكلية والفنية للتفتيش في البيئة الإلكترونية:

التفتيش بصفة عامة لابد له من شروط شكلية بالإضافة إلى الشروط الموضوعية، حتى يتم صحيحا ولا يعتريه البطلان، وللمحافظة على الحريات الشخصية من التعسف في استخدام السلطة، ولا بد أيضا من توافر قدر من المعرفة الفنية للتعامل الجيد مع نظام المعالجة الآلية للمعطيات.

---

[1] إسحاق إبراهيم منصور، المرجع السابق، ص106.

[2] شيماء عبد الغني، المرجع السابق، ص297.

[3] أسامة عبد الله قايد، الوسيط في شرح قانون الإجراءات الجزائية المصري، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر-2007، ص454، الفقرة 470.

1.2.2- الشروط الشكلية للتفتيش في البيئة الإلكترونية:

من الإجراءات الشكلية ضرورة حضور بعض الأشخاص أثناء إجراء تفتيش المساكن ومن في حكمها[1]، ويعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون لإجراء التفتيش، لذا ينص كل من المشرع الجزائري والمشرع الفرنسي على ضرورة حضور شاهدين، سواء أتم التفتيش بمعرفة قاضي التحقيق أم ضابط الشرطة القضائية، إذ وحسب نص م45 ق إ ج التي تقابلها م56 ق إ ج ف فلا بد من حصول التفتيش بحضور المتهم، فإذا لم يستطع الحضور وقت إجراء التفتيش كان عليه تعيين ممثل له، فإن امتنع أو كان هاربا، أجرى ضابط الشرطة القضائية التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته.

غير أن الفقرة الأخيرة من م45 ق إ ج سالفة الذكر[2]، استبعدت بصريح العبارة ضمانة حضور الأشخاص المذكورين آنفا إذا تعلق الأمر بجريمة المساس بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى[3]، وعليه يجوز التفتيش في هذه الجرائم دونما حاجة لحضور الأشخاص المذكورين أعلاه، ولعل ذلك مرده إلى الطبيعة الخاصة لهذه الجرائم التي تحتاج من أجل الكشف عن الأدلة المتعلقة بها إلى السرعة في التنفيذ، والسرية حتى لا يقوم المجرمون بمحو أو طمس أدلة الإدانة؛ كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بإجراء التفتيش عن بعد[4]، ومنها الجزائر، بحيث أجاز القانون 09-04 في م5 منه الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، والمعطيات المعلوماتية المخزنة فيها، وكذا إلى منظومة التخزين المعلوماتية.

من الشروط الشكلية للتفتيش أيضا إجراؤه في ميقات زمني محدد، حرصا على الحريات الشخصية للأفراد وحرمة مساكنهم، لذلك حظر المشرع الجزائري تفتيش المنازل ومن في حكمها في أوقات معينة حيث أجازه فقط من الساعة الخامسة صباحا إلى الساعة الثامنة مساء (م1/47 ق إ ج)، وكذا فعل المشرع الفرنسي- الذي أجاز التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساء (م59 ق إ ج ف)، أما المشرع المصري فقد ترك تحديد الوقت للقائم بالتفتيش، ومن ثم يجوز له القيام به في كل الأوقات وعلى مدار 24 ساعة في اليوم، وهو مسلك خطير فيه خشية مساس بحقوق الأفراد الشخصية.

وهناك حالات استثنائية نص عليها المشرع الجزائري يجوز فيها إجراء التفتيش ليلا ونهارا[5]، وحسب نص م3/47 ق إ ج[6]، فإنه يجوز لقاضي التحقيق القيام بأية عملية تفتيش أو حجز ليلا ونهارا..إذا تعلق الأمر ببعض الجرائم المستحدثة، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولعل الأمر راجع إلى خصوصية هذه

---

[1] كالأفنية والسيارات المتواجدة داخل المنازل، ومكاتب المحامين والموثقين وغيرها.

[2] عدلت م45 ق إ ج بالقانون 06-22 المؤرخ في 2006/12/20، ج ر 84، ص6.

[3] هي جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، وجرائم تبييض الأموال وتمويل الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

[4] عائشة بن قارة، المرجع السابق، ص109.

[5] م2/47 ق إ ج.

[6] المعدلة بالقانون 06-22 المؤرخ في 2006/12/20، ج ر84، ص6.

الجرائم التي لا تحتمل تأخير التفتيش بصددها، أما التشريعات التي لم تنص صراحة على مواعيد خاصة لإجراء التفتيش، فلا مناص من التقيد بالقواعد العامة التي تحدد المواقيت الزمنية لإجراء التفتيش في الجرائم الأخرى.

يجب تحرير محضر لإثبات ما تم من إجراءات، وما أسفرت عنه عملية التفتيش من نتائج، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبخصوص الجرائم الإلكترونية فمن المحبذ أن يكون رفقة القائم بالتفتيش شخص متخصص في تقنية المعلومات ليساعده على صياغة مسودة محضر التفتيش[1]، بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش، بالإضافة إلى المحافظة على الأدلة المتحصل عليها، وحمايتها من كل تلف أو مسح أو تحريف[2].

ويثور التساؤل حول شبكة الانترنت، هل يجوز تفتيشها دون إذن؟

الانترنت شبكة عالمية مفتوحة ومتاحة للجميع، لذا يجوز الدخول إليها والاطلاع على البيانات المتاحة للجمهور دون حاجة للحصول على إذن بالتفتيش، أما إذا كانت هذه البيانات مخزنة لدى مزودي خدمات متواجدين في إقليم دولة أخرى، فإنه واحتراما لسيادة هذه الدولة يجب اللجوء إلى طلب المساعدة القضائية من الدولة المتواجد بها مزودو الخدمات المخزنة لديهم البيانات المراد تفتيشها[3].

ووفقا للقواعد العامة، فإن تفتيش مواقع الانترنت لا تسري عليها قواعد وأحكام تفتيش المساكن، وبالتالي لا تتوافر لها الحماية المقررة في التشريعات المختلفة للمساكن ومن ضمنها الحصول على إذن التفتيش[4].

كما يثور تساؤل آخر مفاده: هل يجوز تفتيش الهاتف المحمول للشخص أو لوحته الالكترونية أو حاسبه المحمول... إذا تم القبض عليه؟

انقسم الفقه حول هذه النقطة إلى فريقين: فريق يجيز ذلك وفريق يرفض.

من حجج المؤيدين للتفتيش بعد القبض الصحيح، أن القبض أشد إهدارا لحقوق الشخص من تفتيشه، فإذا جاز القبض، جاز التفتيش بالتبعية، وقد نصت على ذلك بعض القوانين الإجرائية صراحة، من ذلك م46 من قانون الإجراءات الجزائية المصري، وهذه القاعدة عامة تسري على كل أنواع الجرائم، بما في ذلك الجرائم المعلوماتية، فالتفتيش في حالة التلبس لا يشمل الشخص وحده، بل يمتد إلى ما يحمله من متاع، والأجهزة الرقمية تندرج تحت مسمى المتاع، وهذا ما ذهب إليه القضاء المصري[5]، وبعض أحكام القضاء الأمريكي[1].

---

[1] عائشة بن قارة، المرجع السابق، ص113.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، شارع سوتير، الاسكندرية، مصر 2010، ص225.

[3] سامح أحمد، المرجع السابق، ص262.

[4] المرجع نفسه، الصفحة نفسها.

[5] محكمة النقض المصرية، الطعن رقم 5534 لسنة 1987، الصادر بجلسة 2017/10/10.

ينظر أيضا: أشرف توفيق شمس الدين، مدى دستورية تفتيش الهاتف المحمول كأثر للقبض، دراسة مقارنة، مقال موجود على الانترنت، على الرابط التالي: https://manshurat.org/node/71097 تاريخ الولوج: 2022/5/06 على الساعة 17.

أما الرافضون لتفتيش الأجهزة الرقمية بعد القبض الصحيح، فإنهم يعتبرون هذه الأجهزة مستودعا للحياة الخاصة، وتفتيشها انتهاك صارخ لمبدأ الحق في الخصوصية، دون مسوغ معقول، ويعتبرون أن ما جاء في بعض القوانين الإجرائية قد يصلح تطبيقه على الجرائم التقليدية، ولكن لا يمكن بحال تطبيقه على الأجهزة الرقمية، ولأدل على ذلك أن المشرع الفرنسي- يتطلب الحصول على إذن من القاضي الإداري الاستعجالي للقيام بالتفتيش حتى في حالة القبض والظروف الاستثنائية، وأكد على ذلك المجلس الدستوري الفرنسي- في أحد قراراته[2]، كما أن القضاء الأمريكي بدأ يميل إلى موقف الرافضين، خاصة بعد قرار المحكمة العليا الفدرالية في قضية "ريلي. ف كاليفورنيا"[3].

2.2.2- أسلوب تفتيش نظم الحاسب الآلي[4]:

جرائم تقنية المعلومات لها طبيعة خاصة، لذا يتوجب التعامل معها أثناء التفتيش بطرق خاصة تتلاءم وطبيعتها، بأن تكون هناك مرونة ولياقة لا تتعارض مع الطبيعة الخاصة لهذه الجرائم وتخدم روح العدالة.

التفتيش عن الملفات الموجودة في جهاز الحاسب الآلي من الأمور المعقدة، فالملفات يمكن تخزينها في قرص لين أو بطاقة ذاكرة أو غيرها أو عناوين مخبأة في الحاسب المتنقل الخاص بالمشتبه فيه، أو على خادم بعيد جدا وخارج حدود الدولة، كما يمكن تشفير الملفات، مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية، أو أن يتم خلطها مع آلاف بل ملايين الملفات التي ليس لها علاقة بالموضوع، أو ملفات غير سيئة أو غير ضارة وتكون محمية، لذا فإن تفتيش نظم الحاسب الآلي إجراءات هي للفن أقرب منها للعلم.

يمكن للقائمين بالتفتيش توسيع احتمالية نجاح العملية باتباع الخطوات التالية:

- تجميع فريق عمل، يكون من ضمنه الخبير الفني قبل القيام بالتفتيش.

- التعرف قدر المستطاع على نظم الحاسب الآلي المراد تفتيشها قبل وضع خطة التفتيش أو طلب الإذن.

- وضع خطة لتنفيذ التفتيش (الخطة أ) ووضع خطة بديلة (الخطة ب)، مبنية على المعلومات التي جمعت عن النظام المراد تفتيشه.

- إعطاء مسودة إذن التفتيش عناية خاصة من حيث اشتمالها على وصف لمحل التفتيش، والأشياء المراد ضبطها بدقة وواقعية، مع شرح استراتيجية التفتيش الممكنة.

---

[1] شيماء عبد الغني، المرجع السابق، ص382.

[2] La décision n^0 2016-536, QPC du 19/02/2016. Voir : www.conseil.constitutionnel.fr.

[3] مشار لها عند: لهوى رابح، الشرعية الإجرائية للأدلة المستمدة من التفتيش، أطروحة دكتوراه في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، السنة الجامعية 2021/2020، هامش ص202.

[4] خالد ممدوح إبراهيم، المرجع السابق، ص ص225-227.

كمثال عن العملية الفنية للتفتيش فإن المرشد الفدرالي الأمريكي أعطى أربع طرق للتفتيش وهي:

- تفتيش الحاسب الآلي وطبع نسخة ورقية لملفات معينة في الوقت نفسه.

- تفتيش الحاسب الآلي، وأخذ نسخة إلكترونية في الوقت نفسه.

- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين، وبعدها يتم إعادة عمل النسخة كي تعمل من جهاز التخزين خارج الموقع للمراجعة.

- ضبط (حجز) الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

خاتمة:

إذا كان التفتيش إجراء مهما من أجل حل لغز القضايا والمساعدة على إظهار الحقيقة، كونه يعني البحث في مستودع الأسرار، فهو أيضا إجراء خطير لأنه يمس حرمة الحياة الخاصة للأفراد، لذا وجب إحاطته بمجموعة من الشروط تكفل تطبيقه السليم فيما شرع له، وتزداد أهمية هذا الإجراء إذا تعلق الأمر بالجرائم المستحدثة، لأنها جرائم بالغة الخطورة لاستخدام مرتكبيها للتقنيات الحديثة المتطورة، كما أن مرتكبيها ذوو خبرة ومهارة، لذا عمد المشرع الجزائري إلى إصلاح قوانينه الإجرائية بما يتماشى والوضع الجديد، وإصدار قوانين جديدة، فنجده قد رفع القيود المتعلقة بالمواقيت الزمنية وبحضور المتهم أو من ينوب عنه إذا تعلق الأمر بالجرائم المستحدثة، كما أنه أجاز بنص صريح تفتيش المكونات المعنوية للحاسب الآلي مثلها مثل مكوناته المادية، بل وأجاز التفتيش عن بعد، وأجاز أيضا في حالة خشية المساس بالنظام العام، أو لمقتضيات حسن سير العدالة، أن يكون التفتيش وقائيا أي قبل وقوع الجريمة خروجا عن القواعد العامة، وقام باستحداث كل من القطب الجزائي الاقتصادي والمالي، والقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

لقد أحسن المشرع الجزائري عموما باتخاذه لهذه الإجراءات المتميزة، ولكن ورغم ذلك يورد الباحث التوصيات التالية:

- النص صراحة في قانون الإجراءات الجزائية على شروط وكيفية إجراء التفتيش إذا تعلق الأمر بالأشخاص والمركبات الخاصة، وشروط تفتيش شخص غير المتهم مثلما فعلت بعض التشريعات المقارنة.

- النص صراحة على شروط وكيفية تنفيذ تفتيش الهاتف المحمول أو الحاسب المحمول أو اللوحة الذكية التي توجد بحوزة المتهم عند القبض عليه أو عند الاشتباه فيه، سواء أكانت معه في مكان خاص أو عام، أو كانت بمنزله.

- تعديل نص م4 من القانون 09-04 التي تجيز التفتيش الوقائي إذا تعلق الأمر بالنظام العام ومقتضيات حسن سير العدالة، باستعمال مصطلحات أكثر دقة كي لا تتخذ هذه المادة ذريعة للنيل من حرمة الحياة الخاصة للأفراد.

- إعطاء دور أكبر للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في مجال المساعدة على التفتيش في البيئة الرقمية.
- القيام بدورات تكوينية وتدريبية رفيعة المستوى للقائمين على عملية التفتيش في البيئة الرقمية.

قائمة المراجع:

الكتب:

- أحسن بوسقيعة، قانون الإجراءات الجزائية في ضوء الممارسة القضائية، برتي للنشر، الجزائر 2017.
- أسامة عبد الله قايد، الوسيط في شرح قانون الإجراءات الجزائية المصري، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر2007.
- إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، بن عكنون، الجزائر 1993.
- جلال ثروت، سليمان عبد المنعم، أصول الإجراءات الجنائية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر2006.
- حازم مُحَمَّد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر 2017.
- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة 2009.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، شارع سوتير، الإسكندرية، مصر 2008.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، شارع سوتير، الاسكندرية، مصر 2010.
- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر 2011.
- شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر 2007.
- عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي، في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، مصر 2010.
- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر 2009.
- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار هومة، الجزائر 2018.
- عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، شارع عبد الخالق ثروت، القاهرة، مصر 2012.
- مُحَمَّد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر 2008.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان الأردن 2008.

الرسائل والأطروحات الجامعية:

- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة الإسكندرية، مصر 2010.

- لهوى رابح، الشرعية الإجرائية للأدلة المستمدة من التفتيش، أطروحة دكتوراه في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، السنة الجامعية 2021/2020.

- ملياني عبد الوهاب، أمن المعلومات في بيئة الأعمال الإلكترونية، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر 2017/2016.

المقالات:

- أشرف توفيق شمس الدين، مدى دستورية تفتيش الهاتف المحمول كأثر للقبض، دراسة مقارنة، مقال موجود على الانترنت، على الرابط التالي: https://manshurat.org/node/71097 تاريخ الولوج: 2022/5/06 على الساعة 17.

- بن عيمور أمينة، بوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، جامعة الإخوة منتوري، قسنطينة 1، الجزائر 2022، المجلد 07، العدد 01، ص ص 67-83.

- رحال بومدين، سعداني نورة، محل التفتيش في مجال جرائم التجارة الالكترونية وفق القانون الجزائري، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحيى الونشريسي، تيسمسيلت، الجزائر ديسمبر 2018، العدد 06، ص ص 165-179.

- شنة زواوي، أحكام تفتيش المساكن والأشخاص والمركبات في القانون بين النظرية والتطبيق، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي أمين العقال، تمنراست، الجزائر 2018، المجلد 7، العدد 02، ص ص 142-168.

- محمودي سماح، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، الجزائر، جوان 2017، المجلد 01، العدد 08، ص ص 326-339.

- مرنيز فاطمة، التفتيش الافتراضي كإجراء استدلالي في ضوء القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي أمين العقال، تمنراست، الجزائر 2021، المجلد 10، العدد 02، ص ص 237-254.

الوثائق القانونية:

- القانون رقم 09-04 لمؤرخ في 14 شعبان 1430هـ الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 الصادر في 16 غشت 2009.

- الأمر 20-04 المؤرخ في 30 غشت 2020 المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر، العدد 51، الصادر في 31 غشت 2020.

- الأمر 21-11 المؤرخ في 25 غشت 2021، المتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر، العدد 65 الصادر في 26 غشت 2021.

- المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج رعدد 57، صادر في 28 سبتمبر 2014.

- الاتفاقية المتعلقة بالجريمة الالكترونية بودابست 2001/11/23 (واردة كملحق في كتاب بيومي حجازي، الجوانب الإجرائية...ص ص 879-923).

المواقع الإلكترونية:

- www.cc.gov.eg
- www.conseil.constitutionnel.fr.
- www.joradp.dz
- www.légifrance.gouv.fr