التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

Inspection as a traditional investigation procedure for the collection of crime evidence related to information and communication technologies

د. إلهام بن خليفة

أستاذة محاضرة "ب"

جامعة الشهيد حمة لخضر- الوادي

الملخص:

لمّا أجازت التشريعات الحديثة التفتيش كإجراء للتحقيق يصلح لجمع الأدلة الالكترونية الناتجة عن جرائم البيئة الالكترونية، فإنّ ذلك يقتضي أولاً البحث في مفهومه، خاصة إذا عرفنا أنه عبارة عن جمع للأدلة في العالم الافتراضي، وثانياً البحث في مدى إعمال هذه التشريعات للضوابط والشروط المقررة قانونا باعتباره ماسا للحرية الشخصية، خاصة إذا عرفنا أنّ هذا النوع من الأدلة سهل التعديل وسريع التبخر، إذ يتطلب الأمر نوع من السرية على التفتيش والإسراع في جمع الأدلة قبل امتداد يد العابثين إليها.

الكلمات المفتاحية: التفتيش- أدلة رقمية- تحقيق- إجراء مستحدث- حرية شخصية.

Abstract:

As modern legislation has authorized inspection as a procedure for investigating the collection of electronic evidence resulting from the crimes of the electronic environment, It requires first to research its concept, especially if we know that it is a collection of evidence in the virtual world. Secondly, to examine the extent to which this legislation is applied to the controls and conditions legally prescribed as a measure of personal freedom, Especially if we know that this type of evidence easy modification and rapid evaporation, It requires a kind of secrecy to inspect and expedite the collection of evidence before extending the hand of the abusers.

Keywords: *Inspection - Digital evidence - Investigation - An innovative procedure - Personal freedom.*

مقدمة

تُشير المذكرة التفسيرية لاتفاقية بودابست لمكافحة إجرام الفضاء المعلوماتي إلى أنّه يتطلب لمواجهة جرائم البيئة الالكترونية بنجاح أن تتم إجراءات جمع الأدلة بسرعة وسريّة وهو ما لا تحققه الإجراءات العادية التقليدية نظرًا لسهولة تدمير الأدلة الإلكترونية وسهولة تبخرها[1].

لهذا حرصت هذه الاتفاقية على وضع أسس وأساليب جديدة للتحقيق تكون متوافقة مع ما تتطلبه مثل هذه الأفعال على الشبكة الرقمية[2].

ولا تخرج الأساليب الجديدة للتحقيق على نوعين من الإجراءات تتمثل الأولى في إجراءات تقليدية مثل التفتيش والحجز في البيئة الالكترونية، وتتمثل الثانية في إجراءات جديدة غير تقليدية تتناسب والطبيعة التقنية لهذه الجرائم وأدلتها تُمكّن من الكشف عنها وعن مرتكبها، ويقصد بهذه الإجراءات الجديدة تكريس تقنية المعلومات لجمع الأدلة في الشكل الإلكتروني[3]؛ وبالرجوع إلى قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4] نجد أنّ المشرع الجزائري، قد نص إلى جانب هذه القواعد الإجرائية الجديدة، على قواعد إجرائية تقليدية خاصة بالتفتيش والحجز في مجال هذا النوع من الجرائم، ولقد جاء في عرض أسباب القانون أنّ هذه القواعد تكون وفقًا للمعايير العالمية المعمول بها ومع مراعاة ما تضمنّه قانون الإجراءات الجزائية من مبادئ عامة[5].

ويُثير الفقه عدة إشكاليات فيما يتعلق بمصطلح التفتيش كإجراء تحقيق تقليدي لجمع أدلة جرائم البيئة الالكترونية أولها مدى صحة اعتبار جمع الأدلة في العالم الافتراضي نوع من التفتيش، وثانيًها ما مدى مراعاة التشريعات للضمانات المقرّرة بمناسبة اتخاذ إجراء التفتيش في أنظمة الاعلام والاتصال؟ وهو ما نحاول الإجابة عليه في المباحث التالية:

المبحث الأول: مفهوم التفتيش في مجال البيئة الالكترونية

المبحث الثاني: شروط التفتيش في مجال البيئة الالكترونية

المبحث الأول

مفهوم التفتيش في مجال البيئة الالكترونية

نظرا للاختلاف بين القيام بإجراء التفتيش في المكان المادي للواقعة الإجرامية كإجراء تقليدي، وبين إجراءه في البيئة الالكترونية والمفترض أنّها مكان غير مادي لارتكاب الجريمة بل افتراضي معنوي، فإنّ الفقه أثيرت لديه اشكالية المصطلح الذي يناسبه غير مصطلح التفتيش الذي يتواءم فقط مع جمع الأدلة المادية في المسرح المادي للجريمة، وسوف نعرّج على رأي الفقه هذا بعد تناول

تعريف التفتيش التقليدي، ونتطرق كذلك للمصطلح الذي استعمله المشرع الفرنسي والجزائري.

المطلب الأول

تعريف التفتيش التقليدي

بعيدًا عن التفتيش في البيئة الالكترونية، يعرف الفقه[6] التفتيش التقليدي بأنّه إجراء من إجراءات التحقيق الابتدائي، فثمرته هي ضبط الأشياء المتعلقة بالجريمة، والتي تفيد في كشف الحقيقة وهذه الأشياء قد تُستمد منها أهم أدلة الجريمة إذ قد تكون أداة ارتكابها أو موضوعها أو متحصلاتها، فهدفه هو جمع الأدلة المادية على وقوع الجريمة ونسبتها إلى المتهم، وعلى خلاف إجراءات التحقيق الأخرى التي هدفها جمع الأدلة المادية كالخبرة والمعاينة فإنّ التفتيش يمسّ بحرمة الحياة الخاصة وحرمة المسكن لذلك نجد التشريعات تقرر إبطاله في حالة عدم مراعاة الضمانات والقيود المقررة لإجرائه.

المطلب الثاني

رأي الفقه حول مصطلح التفتيش في البيئة الالكترونية

يرى جانب من الفقه[7] في مجال مصطلح التفتيش في البيئة الالكترونية أنّه مصطلح غير صالح لعملية البحث عن أدلة الجريمة الإلكترونية، والمصطلح الأدّق في هذا المجال هو لفظ الولوج أو النفاذ لأنّ التفتيش يعني البحث والقراءة والتفحص والتدقيق في البيانات وهو مصطلح تقليدي.

إلاّ أنّ الملاحظ في المواثيق الدولية المهتمة بهذا الموضوع من بينها اتفاقية بودابست لجرائم الفضاء المعلوماتي أنّها تستخدم المصطلحين معًا بغرض التنسيق والتنظيم بين المفاهيم التقليدية والحديثة، أي أنّها تأخذ في الحسبان تطور المفاهيم في الوسط الإلكتروني مع تحديدها والاحتفاظ بجذورها التقليدية، بمعنى أنّ هذه المواثيق الدولية تضع للدول الأعضاء المصطلحين معًا للتخيير بين الأخذ بالمصطلح التقليدي وهو التفتيش أو المصطلح الحديث وهو الولوج أو النسخ[8]؛ إذ يُفهم من ذلك أنّ المصطلحين لهما معنى واحد.

كما يرى الفقه[9] أيضًا في مجال التفتيش في البيئة الالكترونية أنّ الأجدر إخضاعه لأحكام مستقلة تتلاءم والطبيعة الخاصة للجريمة الإلكترونية والأدلة الناتجة عنها لأنّ التفتيش التقليدي ما هو إلا وسيلة للإثبات المادي وأنّه يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وغايته دومًا الحصول على الدليل المادي وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي وكذا شبكة الانترنيت، فهي مجرد برامج وبيانات إلكترونية ليس لها أيّ مظهر مادي محسوس في العالم الخارجي.

ورغم ذلك فإنّ الفقه والتشريعات التي صدرت في هذا المجال أجازت بأن يرد التفتيش على هذه البيانات غير المحسوسة المتواجدة على مستوى أنظمة الحوسبة وشبكات الاتصال وفي الوسائط الإلكترونية كالاسطوانات والأقراص الممغنطة ومخرجات الحاسب الآلي، وعليه فهو يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام[10].

المطلب الثالث

مصطلح التفتيش في البيئة الالكترونية في التشريعات

بداية عرّف المجلس الأوروبي هذا النوع من التفتيش بأنّه إجراء يسمح بجمع الأدلة المخزّنة أو المسجّلة بشكل إلكتروني[11].

كما أنّ المشرع الفرنسي يُطلق على جمع الأدلة في الشكل الإلكتروني المصطلح التقليدي وهو التفتيش، ويستشف ذلك من خلال التعديل الذي أدخله على قانون الإجراءات العقابية[12] والتي جاء فيها: (يباشر التفتيش في الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدًا لإظهار الحقيقة).

كما أنّ المشرع الجزائري استخدم في المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها مصطلح الدخول إلى منظومة معلوماتية أو بمنظومة تخزين معلوماتية بغرض التفتيش في إطار قانون الإجراءات الجزائية، بمعنى أنّ الدخول هو التفتيش طبقًا لأحكام قانون الإجراءات الجزائية، ولكنّه يكون على نظام المعالجة الآلية للمعطيات أو مستخرجاتها والمحمولة على وسائط إلكترونية، وإذا كان قانون الإجراءات الجزائية يضع شروطًا يراعي فيها ضمانات الأفراد عند تفتيشهم شخصيًا أو تفتيش الأماكن، فما مدى انطباق هذه الشروط على تفتيش أنظمة المعالجة الآلية للمعطيات ومخرجاتها.

المبحث الثاني

شروط التفتيش في مجال البيئة الالكترونية

يُعتبر التفتيش من أخطر إجراءات التحقيق، لأنّها ينطوي على المساس بالحريه الشخصية، غير أنّه لغاية الكشف عن الحقيقة يسمح المشرع في مختلف دول العالم بالقيام بهذا الإجراء ويحرص في نفس الوقت على إحاطته بضوابط وشروط حيث توجد هذه الضوابط أو الشروط على قسمان، شروط موضوعية تتصل بنشوء السلطة في التفتيش، وشروط شكلية تتعلق بالأوضاع والبيانات التي يجب أن يستوفيها الأمر بالتفتيش أو حضور بعض الأشخاص في تنفيذ التفتيش[13].

المطلب الأول

الشروط الموضوعية

يمكن حصرها في ثلاث شروط أساسية وهي السبب والمحل والسلطة المختصة به[14]، نتناولها كما يلي:

الفرع الأول

سبب التفتيش في البيئة الإلكترونية

الأصل في القانون أنّ الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلاّ لسبب ضبط جريمة بوصف جناية أو جنحة ارتكبت بالفعل وترجحت نسبتها إلى متهم معين، وأنّ هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية، وهو ما أقرته محكمة النقض المصرية في حكم لها[15].

وبتطبيق ذلك على جرائم البيئة الالكترونية فإنّه لكي يكون التفتيش صحيحًا فإنّه يجب:

أولا: وجوب وقوع جريمة البيئة الالكترونية بالفعل

فإذا كان الهدف من إجراء التفتيش هو الحصول على أدلة تساهم في كشف حقيقة الواقعة الإجرامية ونسبتها إلى مرتكبها، فإنّ المنطق القانوني والعقلي يقتضي للقيام به ضرورة وقوع الجريمة بصورة قطعية سواء أكانت جناية أو جنحة[16] وتستبعد المخالفات لضآلة خطورتها[17]، ومن ثمّ لا يجوز إجراءه لضبط جريمة مستقبلاً أو لمجرد ورود معلومات تشير إلى إمكانية وقوع الجريمة مستقبلاً حتى ولو كانت الدلائل كافية على أنّها ستقع بالفعل[18].

وبناءًا عليه فلإمكانية إصدار أمر بالتفتيش لابد أن تكون جريمة البيئة الالكترونية قد تجسدت في الواقع بكل عناصرها المادية والمعنوية.

ثانيا: نسبة جريمة البيئة الالكترونية لشخص أو أشخاص معيّنين إمّا بصفتهم فاعلين أصليين أو شركاء في ارتكابها

فلا يكفي مجرد وقوع جريمة البيئة الالكترونية بالفعل، بل يجب توافر دلائل كافية تدعو للاعتقاد بأنّ ذلك المشتبه فيه قد ساهم في ارتكابها مساهمة مباشرة أصلية أو مساهمة غير مباشرة تبعية، فإن لم تتوافر هذه الدلائل فالإجراء الذي يُفترض اتخاذه هو أمر بألاّ وجه للمتابعة، غير أنّ هذه الدلائل التي تدعو للاتهام لم تتناولها قوانين الإجراءات الجزائية بالتعريف، واكتفت بضرورة توافر الدلائل القوية والمتوافقة مع الاتهام، حيث عرّفها الفقه[19] بأنّها مجموعة من المظاهر أو الأمارات التي تكفي وفق السياق العقلي والمنطقي أن تُرجح نسبة الجريمة إلى شخص معين سواء بوصفه فاعلاً أو شريكًا.

ثالثا: وجود أمارات قوية أو قرائن على وجود معطيات أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره

لا مجال لإجراء التفتيش إن لم تتوافر لدى المحقق أسباب كافية على أنّه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة أو

أشياء متحصلة عنها[20]، إذ لا يكفي وقوع الجريمة واتهام شخص معين باقترافها، وحسب المشرع الجزائري فإنّه يجوز التفتيش في النظم المعلوماتية ونظم التخزين لمقتضيات التحقيقات أو التحريات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية، وهذا طبقًا للمادة الخامسة الفقرة الأولى والمادة الرابعة/ج من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ويُفهم من ذلك أنّه لا يشترط المشرع للتفتيش في الأنظمة المعلوماتية توافر الدلائل للولوج بغرض التفتيش، بل إنّه يمكن ذلك من أجل الحصول على الدليل.

الفرع الثاني

محل التفتيش في البيئة الإلكترونية

محل التفتيش في جرائم البيئة الإلكترونية هو نظام الحاسب الآلي بكل مكوناته المادية أو المعنوية أو شبكات الاتصال التي تشمل في مكونات الخادم والمزود الآلي والمضيف والملحقات التقنية أو الوسائط الالكترونية بمختلف أنواعها.

ولا يختلف اثنان في أنّ الولوج للمكونات المادية للحاسب الآلي بحثًا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للقواعد الإجرائية الخاصة بالتفتيش[21]، وذلك تبعًا لطبيعة المحل الموجودة فيه والذي قد يكون ماديًا أو شخصيًا، إذ يكون شخصي إذا كان الحاسب الآلي بحيازة شخص ما قد يكون مالكه أو غيره، إذ يخضع التفتيش في هذه الحالة للقواعد التي يخضع لها تفتيش الأشخاص بنفس القيود والضمانات في هذا المجال[22]، ويكون ماديًا إذا كان الحاسب الآلي في مكان ما قد يكون عامًا أو خاصًا، إذ لصفة المكان أهمية خاصة في التفتيش، فإذا كان خاصًا كمسكن المتهم، فتنطبق على تفتيشه نفس القواعد التي يخضع لها تفتيش المسكن والتي تقررها أغلب التشريعات الإجرائية، إذ نص عليها المشرع الجزائري في المواد من 44 إلى 47 والمادة 64 من قانون الإجراءات الجزائية.

والجدير بالذكر في هذا الخصوص أنّ المشرع استثنى بعض الجرائم من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجرائم المنظمة والعابرة للحدود الوطنية من أن تُطبق عليها القواعد المنصوص عليها في المواد السابقة، إذ جاء في الفقرة الثالثة من المادة 47 أنّه يجوز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النّهار أو اللّيل، وذلك بناءًا على إذن مسبق من وكيل الجمهورية المختص، ويرجع ذلك إلى اعتبارين[23]:

- ذاتية الجرائم الالكترونية القابلة للاختفاء في أقل من ثانية.

- افتراض كون الدليل في هذه الجرائم هو الدليل الوحيد لإثباتها.

ويجب أن يراعى في تفتيش المساكن التمييز بين ما إذا كانت المكونات المادية للحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أم أنّها متصلة بحاسب آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلاً، فإذا كان كذلك وكانت هناك بيانات مخزنة في الأوعية المادية لهذا النّظام الأخير من شأنها كشف الحقيقة[24] فإنّه يتوجب تفتيشها.

أمّا إذا كان المكان عامًا فسواء أكانت الأماكن عامةً بطبيعتها كالطرق العامة والميادين والشوارع أو كانت عامةً بالتخصيص كالمقاهي أو المطاعم أو قاعات السينما أو الملاعب أو غيرها فإنّ إجراءات التفتيش تكون وفقًا للأصول الخاصة بتلك الأماكن، إذ أنّ تفتيشها لا يكون إلاّ في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص في هذا المجال[25].

ويخضع التفتيش في المكونات المعنوية للحاسب الآلي لما تخضع له التفتيش في المكونات المادية للحاسب الآلي[26]، طالما أنّ التشريعات المختلفة تنص على جواز التفتيش في الأنظمة ومخرجاتها بكافة مكوناتها.

وفيما يتعلق بالتفتيش في الشبكات أو ما يسمى بالتفتيش عن بعد فإنّ طبيعة التقنية الرقمية قد عقدت من التحدي أمام أعمال التفتيش، ذلك أنّ البيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تمامًا عن الموقع المادي للتفتيش، وإن كان من الممكن الوصول إليها من خلال حواسيب إلكترونية تقع في الأمكنة الجاري تفتيشها، إلاّ أنّه قد تكون هذه البيانات البعيدة داخل اختصاص قضائي آخر أو قد تكون في دولة أخرى وبالتالي فهل يمكن تمديد التفتيش؟

بالرجوع إلى المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإنّها تنص على أنّه يجوز تمديد التفتيش في الحالة الأولى، وعلى أنّ الحصول على المعلومات في الحالة الثانية يكون عن طريق المساعدة القضائية الدولية طبقًا للاتفاقيات الدولية ومبدأ المعاملة بالمثل، ويكون ذلك كما يلي:

الحالة الأولى: اتصال نظام المتهم بنظام آخر موجود في مكان آخر داخل الدولة، إذ أنّه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزّنة فيها، وإذا كانت هناك أسباب تدعو إلى الاعتقاد بأنّ المعطيات المبحوث عنها مخزّنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها

انطلاقًا من المنظومة أو جزء منها، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك، وهو الأمر نفسه الذي حثّت به الاتفاقية العربية لمكافحة تقنية المعلومات[27] الدول الأعضاء فيها على تبنيه، وذلك من خلال الفقرة رقم 02 من المادة 26.

وكذلك نص المشرع الفرنسي في قانون الإجراءات العقابية في المادة 1/57[28] الفقرة الأولى على أنّه (يمكن لضباط الشرطة القضائية، ومن هم تحت مسؤولياتهم أعوان الشرطة القضائية أثناء التفتيش الجاري والمحدد بالشروط المنصوص عليها في هذا القانون الدخول عن طريق نظام معلوماتي موجود في المكان أين يجرى فيه التفتيش على معطيات تهم التحقيق الجاري والمخزنة في النظام المذكور أو في نظام معلوماتي آخر عندما تكون هذه المعطيات متاحة أو يمكن الدخول إليها انطلاقًا من النظام الرئيسي) وهو أيضًا ما أوصت به اتفاقية بودابست الدول الأعضاء فيها بمقتضى المادة 19 الفقرة 02.

الحالة الثانية: اتصال نظام المتهم بنظام يقع خارج إقليم الدولة، فغالبًا ما يعمد مجرمي المعلوماتية المحترفين إلى تخزين المعطيات غير المشروعة أو التي تفيد في كشفهم في أنظمة معلوماتية خارج حدود الدولة بغية إعاقة الوصول إلى الدليل المُثبت للتهمة، ومن ثمّ عرقلة سير العدالة، وهو ما دفع بالمشرع الجزائري، وكذا الفرنسي لغاية عدم إفلات المجرم من العقاب إلى إمكانية تمديد التفتيش ولكن في إطار المساعدة القضائية الدولية.

إذ نصت الفقرة الثالثة من المادة السابقة الذكر من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على : (إذا تبيّن مسبقًا أنّ المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإنّ الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقًا للاتفاقيات الدولية ذات الصلة ووفقًا لمبدأ المعاملة بالمثل).

ونصت المادة 1/57 الفقرة الثالثة من قانون الإجراءات العقابية الفرنسي: (إذا تبين مسبقًا أنّ هذه المعطيات يمكن الدخول إليها أو متاحة عبر نظام معلوماتي رئيسي ومخزنة في نظام معلوماتي آخر موجود خارج الإقليم الوطني، فإنّه يمكن الحصول عليها من طرف ضابط الشرطة القضائية في إطار شروط الدخول المنصوص عليها في المعاهدات الدولية النافذة المفعول).

الفرع الثالث

السلطة المختصة بالتفتيش

يُعتبر التفتيش سواء أكان في الجرائم العادية أو في جرائم البيئة الالكترونية إجراء من إجراءات التحقيق التي تمسّ بحقوق وحريات الأفراد، ولهذا تخول التشريعات الإجرائية أمر القيام بها لسلطة التحقيق؛ إلاّ أنّه وبالنظر إلى ضرورات عملية مردّها كثرة القضايا والحرص على سرعة إنجاز أعمال التحقيق فيها، وتسهيله والاستفادة من قدرات رجال الضبطية القضائية أجيز لسلطة التحقيق تكليف هؤلاء بتنفيذ التفتيش[29].

ويُجيز المشرع الجزائري لسلطة التحقيق التي تباشر إجراء التفتيش بنفسها أو عن طريق الإذن أو الإنابة أن تستعين في ذلك بخبير له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، وهو ما جاء في الفقرة الأخيرة من المادة الخامسة السابقة الذكر.

ونفس الأمر الذي أجازه المشرع الفرنسي في الفقرة الخامسة من المادة 1/57 السابقة الذكر، والتي تنص على: (يمكن لضباط الشرطة القضائية بكل الطرق تسخير كل شخص:

1- له معرفة بالتدابير المطبقة من أجل حماية المعطيات التي تسمح بالدخول في إطار التفتيش.

2- ويزودها بالمعلومات التي تسمح بالدخول للمعطيات المحددة في الفقرة رقم 01).

المطلب الثاني

الشروط الشكلية

تتطلب بعض التشريعات الإجرائية شرطين شكليين لصحة إجراء التفتيش يتعلق أولها بالأمر أو الإذن به، فقد اشترطت تسبيبه، ويتعلق ثانيُها بتنفيذه فقد اشترطت أن يحضره أشخاص معينون[30].

الفرع الأول

الإذن بالتفتيش

ينص المشرع الجزائري في المادة 44 من قانون الإجراءات الجزائية أنّه لا يجوز القيام بإجراء التفتيش إلاّ بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق، ويشترط المشرع في هذا الإذن أولاً وجوب استظهاره قبل الدخول إلى المنزل والشروع في تفتيشه وثانيًا أن يتضمن الإذن بيان وصف الجُرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز عليها، بمعنى أن يكون مسببًا، وعلّة التسبيب هي بيان هدف التفتيش والتحقق من مشروعيته بثبوت أنّها الغاية التي حددها القانون، ذلك أنّ الإذن حسب المادة 44 السابقة الذكر، إذا لم يتضمن التسبيب يقع تحت طائلة البطلان، إذ أنّ اشتراط

المشرع للتسبيب يُتيح للقضاء تقدير صحة الأمر بالتفتيش وتقرير بطلانه إذا ثبت أنّه يستهدف غاية أخرى غير ما حدده القانون[31]، ولا يشترط المشرع في التسبيب أن يكون تفصيليًا، بل يكفي بيان الجرم بالاستناد إلى الدلائل التي استخلصتها الضبطية من تحرياتها.

الفرع الثاني

حضور بعض الأشخاص أثناء إجراء التفتيش

يشترط المشرع الجزائري لإجراء التفتيش - مهمًا كان القائم به، طبقًا للمادة 45 في فقرتها الأولى - حضور صاحب المسكن الذي يشتبه في أنّه ساهم في ارتكاب الجريمة، وفي حالة تعذر حضوره فإنّ ضابط الشرطة القضائية ملزم بأن يكلّفه بتعيين ممثل له، وإن امتنع عن ذلك أو كان هاربًا، استدعى ضابط الشرطة القضائية لحضور التفتيش شاهدين من غير الموظفين الخاضعين لسلطته.

غير أنّه فيما يتعلق بالجرائم المتصلة بأنظمة المعالجة الآلية للمعطيات والجرائم المنظمة العابرة للحدود الوطنية وغيرها من الجرائم المحددة أورد المشرع استثناء في الفقرة الأخيرة من نفس المادة يقضي فيه بإجراء التفتيش بغير حضور كل من سبق ذكرهم، ولعلّ سبب المشرع في هذا الاستثناء يرجع إلى الخاصية التي تتطلبها أدلة الجريمة الإلكترونية المتمثلة في سهولة تعديلها وسهولة تبخرها، لذلك يتطلب الأمر نوع من السرية على التفتيش والإسراع في جمع الأدلة قبل امتداد يد العابثين إليها.

الخاتمة

توصلنا من خلال هذا البحث إلى:

- أنّه على الرغم من أنّ إجراء التفتيش كإجراء تقليدي للتحقيق سُنّ للتعاطي مع وضعيات مادية، يبدو قاصرا على استخلاص الدليل في الشكل الإلكتروني ومواجهة ظاهرة جرائم البيئة الالكترونية، مما يترتب عليه إفلات الكثير من الجناة من العقاب، غير أنّ المشرع في كثير من دول العالم عمد إلى إعادة تقييم منهجه على ضوء ما توصلت إليه التطورات التكنولوجية.

- أنّ التشريعات أجازت بأن يرد التفتيش على البيانات غير المحسوسة المحفوظة أو المخزنة في المكونات المادية والمعنوية للحاسب الآلي وفي شبكة الاتصالات وأيضا في الوسائط الإلكترونية كالاسطوانات والأقراص الممغنطة ومخرجات الحاسب الآلي، وهو يخضع لما يخضع له التفتيش بمعناه التقليدي.

- أنّ التفتيش على الرغم من اعتباره من أخطر إجراءات التحقيق لإنطوائه على المساس بالحريه الشخصية، نجد المشرع يسمح بالقيام به لغاية الكشف عن الحقيقة ويحرص في نفس الوقت على إحاطته بضوابط وشروط،

إلاّ أنّ الأمر عندما يتعلق بضرورة البحث عن أدلة جرائم البيئة الالكترونية، نجده يسمح باتخاذه من دون إعمال بعض هذه الضوابط والشروط لأن مثل هذه الجرائم تتطلب سرعة وسرية الكشف عنها لأنّ أدلتها تتمتع بخاصية غير متواجدة في الأدلة المادية ألا وهي سهولة التعديل وسرعة التبخر.

الهوامش:

(1) د/ هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية، القاهرة 2006، ص: 161.

(2) د/ نعيم مغبغب، مخاطر المعلوماتية والانترنيت، منشورات الحلبي الحقوقية، بيروت 2008، ص:227.

(3) رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2012، ص: 440.

(4) قانون رقم 04/09 مؤرخ في 14 شعبان عام 1430 الموافق 05 عشت سنة 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، منشور في الجريدة الرسمية، العدد 47، المؤرخة في 25 شعبان عام 1430هـ الموافق 16 غشت 2009.

(5) أنظر مشروع القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر عن وزارة العدل، الجمهورية الجزائرية الديمقراطية الشعبية، ص:02.

(6) أنظر ذلك في: د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقًا لأحدث التعديلات التشريعية، الجزء الأول، دار النهضة العربية، القاهرة 2013، ص: 592، ود/ أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر1998، ص، ص : 240- 241، ود/ مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، الطبعة الأولى، دار التجهيزات الفنية، القاهرة 2009، ص189، وعلي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية 2012، ص: 38.

(7) Convention sur la cybercriminalité, rapport explicative, disponible en ligne à l'adresse suivante: http://convention.coe.int

مشار إليه في: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية 2007، ص، ص : 223 – 224.

(8) أنظر ذلك في: د/ هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص: 164، ونبيلة هبة هروال، المرجع السابق، ص 224.

(9) نفس المرجع، ص: 223

(10) M.Moherenschlager: computer crimes and others crimes againts information technology in the Germany.Rev.int.pen.1993;p.319, spec.349

مشار إليه في: علي عدنان الفيل، المرجع السابق، ص:39، انظر أيضا: د/ مسعود موسى ارحومة، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة عمل مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس خلال الفترة 28-2009/10/29 متاح على الموقع: *http://iefpedia.com/ar.ab/wp-c* "تم الاطلاع عليه بتاريخ: 2015/11/28".

[11] علي عدنان الفيل، المرجع السابق، نفس الصفحة.

[12] أضيفت هذه المادة بموجب قانون رقم: 575/2004، المؤرخ في 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي وهو:

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique; disponible au site suivant: www.legifrance.gowv.fr/WAspad/UntextedeJorf?numjo=ECOXO200175L, "consulté le 21/12/2015".

[13] د/ محمود نجيب حسني، المرجع السابق، ص: 594.

[14] أنظر ذلك في: رشيدة بوكر، المرجع السابق، ص:405، ونبيلة هبة هروال، المرجع السابق، ص:229.

[15] طعن نقض جنائي، جلسة 1968/10/16، مجموعة أحكام النقض، ص18، رقم 195، ص: 965 انظر ذلك في: د/ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية 2010، ص:209.

[16] أنظر الفقرة 1 و 2 من المادة 44 من قانون الإجراءات الجزائية الجزائري.

[17] رشيدة بوكر، المرجع السابق، ص: 406.

[18] نقض 1973/02/16 مجموعة أحكام النقض، س24، رقم 49، ص223، انظر ذلك في: نبيلة هبة هروال، المرجع السابق، ص:231.

[19] د/ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 2006، ص: 121.

[20] علي عدنان الفيل، المرجع السابق، ص:50.

[21] د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنيت، بحث منشور على الموقع: *http.//www.eastlaws.com* ، ص: 11، " تاريخ الاطلاع: 2015/12/22 ".

[22] رشيدة بوكر، المرجع السابق، ص:396.

[23] نفس المرجع، نفس الصفحة.

[24] د/ حسين بن سعيد الغافري، المرجع السابق، ص: 12.

25 د/ خالد ممدوح إبراهيم، المرجع السابق، ص:196.

[26] د/ موسى مسعود ارحومة، المرجع السابق.

[27] صادقت الجزائر على هذه الاتفاقية بمقتضى المرسوم الرئاسي رقم 14-252 مؤرخ في13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، منشور في الجريدة الرسمية، العدد 57، المؤرخة في: 4 ذو الحجة عام 1435 الموافق 28 سبتمبر سنة 2014.

[28] أضيفت هذه المادة بموجب قانون الأمن الداخلي رقم 239/2003 الصادر في 18 مارس 2003، انظر ذلك في:

Emanuelle Matignon, la Cybercriminalité: un focus dans le monde des telecoms, Mémoire de Master Droit numérique Administrations, Université Paris 1 Panthéon – Sebtembre 2011/2012, p:43.

[29] رشيد بوكر، المرجع السابق، ص: 410.

[30] د/ محمود نجيب حسني، المرجع السابق، ص: 605.

[31] نفس المرجع، نفس الصفحة.