مجـــلـة الحـــق للعلوم الشرعية والقانونية
Al-haq Journal for Sharia and Legal Sciences
تصدر عن كلية القانون – جامعة بني وليد – ليبيا
Website: https://www.al-haqjournal.ly/index.php/alhaq/index
المجلد الثاني عشر ــ العدد الثاني 2025 ــ الصفحات (326-339)
ISSN 3005 - 3919 معامل التأثير العربي 1.67 لسنة 2024 2.113 (ISI) لسنة 2025

Inspection in electronic media

Hind aldawy mosbah *
Department of Criminal Law, Faculty of Law, Al-Zaytouna University, Tarhuna, Libya
h.elmabryuk@azu.edu.ly

التفتيش في الأوساط الالكترونية

أ. هند الضاوي مصباح *
قسم القانون الجنائي، كلية القانون، جامعة الزيتونة، ترهونة ، ليبيا

تاريخ الاستلام: 27-06-2025 تاريخ القبول: 28-07-2025 تاريخ النشر: 04-08-2025

الملخص:
التفتيش في الأوساط الإلكترونية هو إجراء قضائي يهدف إلى جمع الأدلة من الأجهزة والأنظمة الرقمية لمكافحة الجرائم ويشمل هذا الإجراء فحص أجهزة الحاسوب والهواتف الذكية والخوادم، ووسائط التخزين الرقمية. يتطلب التفتيش الإلكتروني مهارات متخصصة ومعرفة فنية لضمان سلامة الأدلة الرقمية وعدم العبث بها، وذلك لتجنب إهدارها قانونيًا ويواجه هذا النوع من التفتيش تحديات تتعلق بحماية خصوصية الأفراد، حيث يجب أن يتم وفقًا لأوامر قضائية محددة النطاق والوقت وكما يتضمن التفتيش الإلكتروني استخدام أدوات وتقنيات متقدمة لتحليل البيانات واستخراج المعلومات المخفية، مما يجعله عنصرًا حيويًا في التحقيقات الجنائية الحديثة.

الكلمات الدالة: التفتيش الرقمي، الأدلة الإلكترونية، الجرائم السيبرانية، الخصوصية، التحقيق الجنائي.

Abstract:
Cyber forensics is a judicial procedure aimed at collecting evidence from digital devices and systems to combat crimes. This procedure includes examining computers, smartphones, servers, and digital storage media. Cyber forensics requires specialized skills and technical knowledge to ensure the integrity of digital evidence and prevent tampering, thus avoiding its legal loss. This type of forensics faces challenges related to protecting individual privacy, as it must be conducted pursuant to judicial orders with specific scope and timeframes. Cyber forensics also involve the use of advanced tools and techniques to analyze data and extract hidden information, making it a vital component of modern criminal investigations.

Keywords: Digital forensics, electronic evidence, cybercrime, privacy, criminal investigation.

المقدمة:

لقد شهد العالم تطوراً سريعاً في مجال الاتصالات والتكنولوجيا مما ترتب عليه ظهور وسائل وأوساط جديدة أصبحت مكمناً للسر، وازدادت هذه الوسائل انتشاراً وشيوعاً تحت أشكال وأنواع مختلفة ومثالها أجهزة الحاسب الآلي والهواتف الذكية والكاميرات وأجهزة التصوير ووسائط التخزين وشبكة الأنترنت بما تحويه من مواقع الكترونية، ولم يعد الانسان يحفظ أسراره في مكان سكنه أو معه بل أصبحت الوسائل الالكترونية الأكثر استخداماً انطلاقاً من سهولة استعمالها وسعتها التخزينية الكبيرة، وهذه الثورة المعرفية والتكنولوجية عادت بفوائد كثيرة علي المجتمع إلا أن البعض أساء استخدام التكنولوجيا في ارتكاب الجرائم، فكانت محلاً لارتكاب الجريمة وأداة لارتكابها، ولم يعد مسرح ارتكاب الجريمة عادياً، ولم تعد أدلة اثبات الجرائم مادية بل ظهرت الأدلة الرقمية كمخرج تكنولوجي والذي يمتاز بالحاجة إلي متخصصين للوصول إليه، ولقد تعددت طرق استخلاص الأدلة من تلك الوسائل ومنها المعاينة، والخبرة والتفتيش الذي هو موضوع هذا البحث.

أهمية البحث:

تبرز أهمية الموضوع في الحاجة المُلحة لدراسته، كون التفتيش في الوسط الالكتروني عملية معقدة ومتشابكة تختلف تماماً عن التفتيش في الجرائم التقليدية، كما تبرز أهمية البحث في دراسة أهم الإشكاليات المترتبة على تنفيذ التفتيش.

إشكالية البحث:

تتمحور إشكالية البحث الرئيسية في التساؤل الاتي: **ما مدي جواز التفتيش في الأوساط الالكترونية؟**

وتتفرع عن هذه الإشكالية عدة تساؤلات:

ما مدى قابلية تفتيش مكونات الحاسب الالي؟ وما مدى جواز امتداد إذن التفتيش في حالات التشابك بين أجهزة الحاسب الآلي؟ وماهي ضوابط التفتيش الالكتروني؟

منهج البحث:

تعتمد الباحثة على المنهج التحليلي، وذلك من خلال تحليل نصوص التشريع الليبي ذات الصلة بهذا الموضوع.

خطة البحث:

قسمت الدراسة الي مبحثين على

المبحث الأول: تفتيش الحاسب الآلي والأنظمة المتصلة به

المطلب الأول: مدي قابلية تفتيش مكونات الحاسب الآلي

المطلب الثاني: تفتيش الشبكات المتصلة بالحاسوب (التفتيش عن بعد)

المبحث الثاني: ضوابط التفتيش الالكتروني

المطلب الأول: الضوابط الشكلية

المطلب الثاني: الضوابط الموضوعية

المبحث الأول

تفتيش الحاسب الآلي والأنظمة المتصلة به

التفتيش وفقاً للقواعد العامة هو الاطلاع علي محل منحه القانون حرمة خاصة باعتباره مستودع سر صاحبه، فلا يجوز الاطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها في القانون أو برضا صاحبه، فيعرفه البعض بأنه**:** (إجراء من إجراءات التحقيق يُباشره موظف مختص بهدف البحث عن الأشياء المتعلقة بالجريمة في موضع له حرمة، والتي تفيد في الكشف عن الجريمة عند العثور على أدلتها المادية، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقاً للضمانات والضوابط المقررة قانونا).[1]

[1]ـ عبد الرحمن محمد أبوتوتة، شرح قانون الإجراءات الجنائية، الدعوى الجنائية والدعوى المدنية والاستدلات والتحقيق الابتدائي، دار الحكمة للنشر والتوزيع، ص 305

فالتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلي أدلة مادية تسهم في بيان الحقيقة وظهورها، ونتيجة لذلك يُعد تفتيش نظام الحاسوب والأنترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب جرائم تقنية المعلومات؛ لكون محل التفتيش هنا هو الحاسوب والشبكات، **وعليه فالتفتيش في الوسط الالكتروني**[1] هو: (إجراء من إجراءات التحقيق يهدف إلى البحث داخل نظام الحاسوب الآلي أو الأنترنت بإذن قضائي مسبق سواء أكان هذا النظام من حاسوب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياها القانون، والغرض منه استخراج أدلة معلوماتية متمثلة في المعلومات أو البيانات التي تساعد على كشف الحقيقة)،[2] وعرَّفه المجلس الأوربي بأنه: (إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني).[3]

فمحل التفتيش في البيئة الالكترونية هو جهاز الحاسوب والأجهزة المتصلة به والشبكة التي تشمل في مكوناته مزود الخدمة والمزود الآلي، والملحقات التقنية،[4] وهذا يعني أن التفتيش سوف ينصب على هذه المكونات، مما يدفعنا للتساؤل عن مدي خضوع مكونات الحاسب الآلي ونظمه للتفتيش؟

المطلب الأول

مدي قابلية مكونات الحاسب الالي للتفتيش

سنتطرق من خلال هذا المطلب إلى تفتيش مكونات الحاسب الآلي المادية (الفرع الأول)، ثم نتطرق إلى تفتيش المكونات المعنوية (الفرع الثاني).

الفرع الأول/ تفتيش المكونات المادية للحاسوب:

نقصد هنا أن ينصب التفتيش علي المكونات المادية لجهاز الحاسوب وملحقاته كالشاشات، والذاكرات، والطابعات من خلال الولوج بداخلها بحثاً عن أدلة متصلة بالجريمة، حيث يخضع التفتيش في هذه الحالة للقواعد العامة التي تحكم تفتيش الأماكن والأشخاص، بمعني 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 قانوناً، وهذا ما أخذت به أغلب التشريعات؛ لأن الهدف من وراء التفتيش هو استخلاص دليل مادي على قيام المتهم بارتكاب الجريمة كاستخدامه الحاسب الآلي والطابعة الملونة في تزوير الأوراق النقدية مثلاً،[5] وإذا ما وُجد الشخص حاملاً لمكونات الحاسوب أو مسيطراً عليها فتفتيشها يكون بنفس الضمانات والقيود المقررة لتفتيش الأشخاص.

الفرع الثاني/ تفتيش المكونات المعنوية للحاسب الآلي:

وإذا كان الفقه قد أجمع على إمكانية تفتيش المكونات المادية للحاسوب فإن الأمر يختلف بشأن إمكانية تفتيش المكونات المعنوية المتمثلة بالبيانات بمختلف أشكالها المستخرجة من جهاز الحاسوب من خلال تقنيات فنية معقدة، والتي يثار بشأنها التساؤل حول صلاحيتها لأن تكون محلاً للتفتيش لضبط الدليل، وقد ثار جدل بين الفقهاء حول إمكانية تطبيق إجراءات التفتيش التقليدية عليها باعتبارها كيانات غير محسوسة، وانقسم الفقه في ذلك إلى فريقين، وهما:

---

[1]- الوسط الالكتروني او الوسط الافتراضي هو تعريب لمصطلح cyberوقد عرف قاموس أكسفورد كلمة سيبراني بأنها: (صفة لأي شخص مرتبط بثقافة الحواسيب او تقنية المعلومات او الوسط الافتراضي)، وقد عرف أيضاً بأنه عبارة عن فضاء رقمي يربط منظومات المعالجة الالكترونية للمعطيات بشبكات المعلومات والاتصال، ويشمل عناصر مادية ولا مادية من حواسيب وخوادم وأنظمة تشغيل وبرمجيات وشبكات اتصال ومحتوى رقمي والمستخدمين، سواء أكانوا مشغلين ام مستعملين وجميع العمليات التي تجري باستعمال هذه العناصر.

[2]- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، سنة 2011م، ص 55

[3]- مشار اليه لدي محمد جمال الذنيبات، القاضي معن احمد العناسوة، التفتيش في الجرائم الالكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، المجلد 13 العدد 3، سنة 2021م، ص83

[4] - عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، سنة2011م، ص26

[5]- حطاب كمال، خصوصية التفتيش في البيئة الالكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 09، ا لعدد 01 السنة 2023م، ص594

الراي الأول: ذهب إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق علي بيانات الحاسب الآلي غير المحسوسة أو الملموسة، ويقترح هذا الرأي لمعالجة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي".[1]

وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي، ولقد استجابت بعض التشريعات لهذه التغيرات ومنها المشرع الفرنسي الذي قام بتعديل نصوص التفتيش التقليدية لتواكب التكنولوجيا الحديثة، إذ أضاف بموجب المادة 42 من القانون رقم 545-2004 المتعلق بالثقة في الاقتصاد الرقمي عبارة "المعطيات المعلوماتية" مشيراً إلى المادة 94 من قانون الإجراءات الجنائية لتصبح هذه المادة على النحو التالي: يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيداً لإظهار الحقيقة.[2]

أما الرأي الثاني: ذهب إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على اصدار الأذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة.[3]

وفي إطار التشريعات العربية نجد أن القانون الأردني قد نص في المادة 12/أ من القانون رقم 30 سنة 2010م من قانون الجرائم الإلكترونية على أنه: (مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكي عليه الشخصية، يجوز لموظفي الضابطة العدلية بعد الحصول علي إذن من المدعي العام المختص أو المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم ....)،[4] أما المشرع المصري فقد صرح بجواز تفتيش قواعد البيانات والنظم المعلوماتية في المادة 2/6 من قانون مكافحة جرائم تقنية المعلومات رقم 175لسنة 2018م،[5] بقوله أنه: (لجهة التحقيق المختصة بحسب الأحوال ـ أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين... بواحد أو أكثر مما يلي: ...2ـ البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب الآلي وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط).[6]

وبالاطلاع على القانون الليبي نجد أن المشرع الليبي في القانون رقم 5 لسنة 2022م بشأن مكافحة الجرائم الإلكترونية لم ينص صراحة على جواز ضبط وتفتيش الدليل الرقمي، لذا يتم الرجوع إلى الأحكام العامة للتفتيش، وهنا نجد نص المادة 75 /2 من قانون الإجراءات الجنائية الليبي التي تنص على أنه: (للمحقق أن يفتش في أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل أنه يستعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليها وكل ما يفيد في كشف الحقيقة)، ونلاحظ أن هذا النص يجيز للمحقق أن يباشر التفتيش في أي مكان، ولو كان هذا المكان متمثلاً في الوسط الافتراضي للدليل وليس الوسط التقليدي أخذاً بالمعني الواسع للفظ المكان الوارد بالنص، ويجيز له ضبط كل ما يفيد في كشف الحقيقة، ولو تمثل محل

---

[1] ـ محمد مرزوق الظهورى، مأمون محمد سعيد ابوزيتون، لثر، إجراءات التفتيش التقليدية على حجية الدليل الالكتروني "دراسة مقارنة" مجلة جامعة الشارقة للعلوم القانونية، المجلد 21، العدد 3، سبتمبر 2024م، ص 153

[2] ـ أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الالكتروني (دراسة مقارنة)، مجلة الدراسات القانونية والاقتصادية، المجلد 8، العدد 2، سنة 2022م، ص 14

[3] ـ عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي مركز بحوث الشرطة ـالقيادة العامة لشرطة الشارقة، الامارات، مجلد 22 العدد86، سنة 2013م، ص261

[4] ـ ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الأردني، دراسات، علوم الشريعة والقانون، المجلد 45، عدد 4، ملحق2 لسنة 2018م، ص63

[5] ـ منشور في الجريدة الرسمية، العدد 32مكرر(ج) في 14 أغسطس سنة 2018م.

[6] ـ مصطفي علي خلف، التفتيش وفقا لأحكام القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، المجلة الجنائية القومية، المجلد 63، العدد 3، نوفمبر 2020م، ص 6

الضبط في المخرجات الرقمية أخذاً بعموم عبارة: (ضبط كل ما يفيد في كشف الحقيقية)، [1] ويري البعض وهو ما تؤيده الباحثة- بأن الوسط الافتراضي من الممكن أن يكون محلاً للتفتيش كما يمكن أن تكون محتوياته محلاً للضبط والتفتيش، ولا يعترض على ذلك بأن القانون يوجب تحريز المضبوطات،[2] وهو ما لا يتفق وطبيعة المخرجات الرقمية، فهذا ليس صحيحاً، ومن وجهة نظره يري أن هذه المخرجات يمكن تحريزها بطريقة تتفق وطبيعتها في حالة فصلها عن مصدرها في قرص (CD) وتحريز هذا القرص بالطريقة المنصوص عليها قانوناً، كما يمكن تحريزها إذا كانت في نصوص بعد طباعتها وتحويلها للشكل المادي الملموس.[3]

المطلب الثاني

تفتيش الشبكات المتصلة بالحاسوب (التفتيش عن بعد)

قد يكون جهاز المتهم في بعض الحالات متصلاً بغيره من الأجهزة داخل حدود الدولة أو خارجها، الأمر الذي يترتب عليه المساس بحقوق غير المتهم في المحافظة على الخصوصية في حالة إذا ما امتد التفتيش إلى جهاز هذا الغير داخل حدود الدولة، ومساس بسيادة الدول في الحالة التي يمتد فيها التفتيش إلى أجهزة موجودة خارج نطاق حدود دولة المتهم، فهل بالإمكان إجراء التفتيش أم لا؟

الإجابة عن هذا السؤال تختلف باختلاف الحالتين المشار إليهما على النحو الآتي:

الفرع الأول/ اتصال حاسوب المتهم بجهاز آخر موجود داخل إقليم الدولة:

تتحقق هذه الفرضية حينما يقوم المتهم بتحويل البيانات أو معلومات عبر الأنترنت متعلقة بجريمة ما من حاسب إلى حاسب مملوك للغير، في هذه الحالة تواجه سلطة التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية، والاعتداء على حرمة خصوصية الغير من ناحية أخرى.[4]

وبالرجوع إلى القواعد العامة للتفتيش في قانون الإجراءات الجنائية الليبي نجدها تقضي بأن تفتيش غير المتهمين أو تفتيش منازل غير المتهمين طبقاً لنص المادة 180 إجراءات جنائية لا يجوز إجراؤه من النيابة العامة إلا بعد الحصول على إذن من القاضي الجزئي، هذا إذا كان التحقيق تباشره النيابة العامة، أما إذا كان الذي يباشره قاضي التحقيق نفسه فلا يستلزم حصول هذا الإذن، وبناءً على ذلك فإذا كان الحاسوب موجوداً بمنزل غير المتهم فلا يجوز تفتيشه من قبل النيابة العامة إلا بعد استصدار اذن من القاضي الجزئي قبل ولوجه، وإلا كان الإجراء باطلاً وغير مثمر، غير أن صدور الإذن قد يستغرق بعض الوقت ما قد يؤدي إلى تلاشي الدليل واندثاره بالمحو والاتلاف، وهذا ربما يعيق الوصول إلى الدليل وتحصيله، فالجاني قد يحاول العبث بالدليل كي لا ينكشف أمره قبل صدور الإذن، ولاسيما أنه يستلزم تحديد محل الإذن بدقة حتي يتسنى تنفيذه،[5] لهذا رُئي ضرورة معالجة هذه المشكلة بنص خاص يقضي بتوسيع سلطات الجهة المعنية بإجراء التفتيش ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة إذا كان من شأن انتظار الإذن أن يفوت فرصة الحصول على الدليل.

وقد تبنت بعض التشريعات هذا الاتجاه - حيث نصت صراحة على جواز امتداد الحق في التفتيش عند الضرورة ليشمل أي أجهزة إلكترونية أو أجهزة الحاسب أو أية منظومة معلوماتية مرتبطة بجهاز الحاسب الآلي المأذون بتفتيشه، وضبط البيانات الضرورية التي تفيد في كشف الحقيقة دون التقيد بالحصول على إذن

---

[1] - مصطفي ابراهيم العربي، دور الدليل الرقمي في الاثبات الجنائي، مجلة البحوث القانونية، كلية القانون، جامعة مصراته، السنة الرابعة، العدد الأول، سنة 2016م، ص95

[2] - بينت المادة 44 من قانون الإجراءات الجنائية الكيفية التي يتم بها تحريز المضبوطات وذلك بقولها " توضع الأشياء واوراق التي تضبط في حرز مغلق وتربط كلما أمكن، ويختم عليها، ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء

[3] - طارق الجملي، الدليل الرقمي في مجال الاثبات الجنائي، مجلة الحقوق، جامعة البحرين، كلية الحقوق، المجلد 12، العدد 1، سنة 2015م، ص 62

[4] - جميلة سعيد شوران، اذن التفتيش في الأوساط الالكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، مجلد 15 العدد 1، مارس 2023م، ص 120

1- موسي مسعود ارحومة،الإشكاليات الإجرائية التي تثيرها الجرائم المعلوماتية عبر الوطنية ، بحث مقدم الي المؤتمر المغاربي الأول حول : المعلوماتية والقانون ،الذي نظمته اكاديمية الدراسات العليا، طرابلس، ليبيا خلال الفترة 28/10/29/2009م

مسبق آخر من السلطات المختصة بشأن الامتداد،[1] ومنها المشرع المصري حيث نصت المادة 1/6من القانون رقم 175 لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات بأن: (لجهة التحقيق المختصة بحسب الأحوال أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين... بواحد أو أكثر مما يلي: 1ـ ضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر).[2]

ولكن ماذا لو كان جهاز المتهم أو التطبيق الموجود على الجهاز لتخزين البيانات أو المعلومات المراد التفتيش عنها أو ضبطها محمياً بكلمات سر تمنع من الولوج إليها، **<u>فهل يمكن اجبار صاحب كلمة السر على الإفصاح عنها، حتى يتم الولوج إلى تلك البيانات؟</u>**

لقد تباينت الآراء بصدد هذه المسالة، فثمة رأي يرفض اجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي، والحجة التي يستند عليها هذا الرأي تتجسد في قاعدة معروفة ومستقرة أن المتهم لا يجوز اجباره على الإجابة عن الأسئلة التي من شأنها أن تقضي بإدانته إذا من حقه الاعتصام بالصمت دون أن يفسر ذلك الصمت ضد مصلحته، **وفي المقابل ذهب رأي آخر** إلى القول بأنه إذا كان لا يجوز اجبار الشخص علي الإدلاء بأقواله ضد نفسه، فلا ينبغي أن يكون ذلك حائلاً دون اجباره علي تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة متي كانت هذه المعلومات بحوزته قياسا علي اجبار الشخص علي تسليم مفتاح الخزنة الذي بحوزته، ولكن هذا الرأي الأخير أياً كانت المبررات التي يقوم عليها لا يمكن القبول به، فقياس المعلومة التي بحوزة المتهم على مفتاح الخزنة، وما في حكمه قياس مع الفارق ذلك أن المعلومة المتمثلة في كلمة السر وما في حكمها هي أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم هذا من ناحية، ومن ناحية أخرى فإن هذه الرأي يتنافى مع مقتضيات حق الدفاع أمام القضاء الجنائي.

وعلى فرض التسليم بجواز اكراه المتهم أو المشتبه به على تقديم مفاتيح الشفرة أو الإفصاح عن كلمة السر التي تُمكن من الولوج إلى النظام المعلوماتي، فإن الأمر يكتنفه صعوبات عملية لا يمكن التغلب عليها لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة أو عدم امكان تذكرها.[3]

ويري جانب آخر من الفقه بأنه بالإمكان اجبار غير المتهم على الإفصاح عن كلمة السر لتيسير الدخول إلى المصدر الإلكتروني للمعلومة محل التفتيش،[4] شريطة أن يحترم الغير (مزود الخدمة) ما يفرضه مبدأ المحافظة على سرية المعلومات من قيود أهمها عدم الإفصاح عن أية معلومة متعلقة بالمستخدمين إلا بإذن من الجهات القضائية المختصة.

الفرع الثاني/ اتصال حاسب المتهم بجهاز آخر موجود خارج إقليم الدولة:

من المشاكل التي تواجه سلطة التحقيق في جمع الأدلة قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة، مستخدمين في ذلك شركة الاتصالات المعلوماتية مستهدفين عرقلة الادعاء في جمع الأدلة والتحقيقات،[5] وقد تباينت الاتجاهات حول مدى امتداد التفتيش للحواسيب الأخرى الموجودة خارج إقليم الدولة، فذهب رأي إلى رفض امتداد التفتيش للحواسيب الأخرى المتصلة بحاسوب المتهم خارج الدولة، بدعوى أن ذلك ينطوي على انتهاك لسيادة دولة أخرى، وبالأحرى يشكل اعتداء على ولاية الدولة التي يجري التفتيش في نطاق اقليمها، ومن ثم فالأمر يتطلب لجوء سلطات التحقيق إلى سلوك الإجراءات المعتادة في طلب المساعدة القضائية من السلطات الموازية في الدولة الأخرى، بعبارة أخرى مباشرة هذا الاجراء يستلزم وجود اتفاقية ثنائية أو متعددة الأطراف وإلا يفقد مشروعيته.[6]

---

[1] ـ محمد مرزق الظهورى، مأمون محمد سعيد أبو زيتون، اثر إجراءات التفتيش التقليدية علي حجية الدليل الالكتروني، مرجع سابق، ص 156

[2] ـ أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الالكتروني (دراسة مقارنة) مرجع سبق ذكره، ص15

[3] ـ موسي مسعود ارحومة، الإشكاليات التي تثيرها الجريمة المعلوماتية عبر الوطنية مرجع سابق، ص 9

[4] ـ مصطفي إبراهيم العربي، دور الدليل الرقمي في الاثبات الجنائي، مرجع سابق، ص95

[5] ـ شيماء حمدان، الإطار القانوني للتفتيش في الجرائم الالكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة محمد الصديق بن يحي، جيجل/الجزائر، 2023/2022م، ص22

[6] ـ موسي مسعود ارحومة، الإشكاليات التي تثيرها الجريمة المعلوماتية عبر الوطنية، مرجع سابق ص 9

وبالتالي لا يجوز القيام بذلك التفتيش العابر للحدود في ظل عدم وجود مثل تلك الاتفاقيات، أو كحد أدنى الحصول على موافقة الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المعلوماتية،[1] ومن أبرز صور المساعدة القضائية التي يمكن الاستفادة منها في هذه الحالات نقل الإجراءات، ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية، وهي بصدد التحقيق في جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة أبرزها التجريم المزدوج، بمعني أن يكون الفعل مجرماً في كلتا الدولتين، بالإضافة إلى شرعية الإجراءات المطلوب اتخادها، وأن يكون الإجراء مهماً لكشف الحقيقة، وقد أقرت العديد من الاتفاقيات الدولية هذه الإجراء.[2]

وفي المقابل يؤيد جانب آخر من الفقه جواز امتداد التفتيش الإلكتروني خارج حدود إقليم الدولة دون حاجة إلى استئذان الدولة التي امتد التفتيش عبر شبكة الاتصال فيها والحواسيب المرتبطة بها، منطلقاً بذلك من الواقع الذي تفرضه الجريمة المعلوماتية وما تثيره من معوقات أمام التفتيش، إذ أن انتظار الحصول على الإذن من الدولة التي امتد إليها التفتيش قد يؤدي إلى افراغ التفتيش من مضمونه نظراً لتمكن الجناة من محو الأدلة واخفاء معالم جريمتهم، ومن التشريعات التي أخذت بهذا الرأي التشريع الفرنسي الذي أجاز لقاضي التحقيق أخذ نسخة من البيانات التي يحتاجها للكشف عن جريمة معلوماتية دون انتظار الحصول على الاذن، ونلاحظ أن هذا الاتجاه يحاول أن يؤسس لقواعد جديدة في ظل المتغيرات الحاصلة في مسرح الجريمة والطبيعة الافتراضية الرقمية التي يتسم بها، إلا أنه لايزال يصطدم بمبدأ السيادة الذي يعد مثل هذا الأمر انتهاكاً صريحاً له.[3]

وفي نفس الاتجاه صدرت عن المجلس الأوربي توصية تجيز هذا، حيث أقرت التوصية 18 لسنة 1995م على أنه: (من الضروري ادخال إجراءات تتسم بالاستعجال تخول سلطات البحث والتحقيق أن تطلب من سلطات أجنبية أن تقوم بجمع الأدلة بشكل عاجل، لذا يجب تخويل السلطات المطلوب إليها أن تقوم بتزويد الجهة الطالبة بالمعلومات المتعلقة بحركة المراسلات التقنية، وأن تقوم باعتراض اتصالات معينة أو تقوم بتحديد مصادرها، ولتحقيق هذا الغرض يتعين إيجاد الوسائل التي تسمح بالمساعدة القضائية في هذا الخصوص).[4]

أما اتفاقية بودابست لسنة 2001م فقد نصت في المادة 32 من الاتفاقية الأوربية بشأن جرائم الأنترنت على أنه: (يمكن لأي طرف دون تصريح من الطرف الآخر:

1- أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور، بغض النظر عن موقعها الجغرافي.
2- أن يصل أو يتلقى عبر نظام معلوماتي يقع على اقليمه بيانات معلوماتية مخزنة في دولة أخرى، إذا حصل هذا الطرف على موافقة قانونية وإدارية من شخص لديه سلطة قانونية للكشف عن هذه البيانات .....).[5]

ولقد أكد المشرع المصري على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية في المادة 4 من القانون 175 لسنة 2018 م بشأن مكافحة جرائم تقنية المعلومات التي أقرت على تعاون السلطات المصرية مع نظيراتها في الدول الأجنبية ضمن اطار الاتفاقيات الثنائية أو الجماعية، أو تطبيق مبدأ المعاملة بالمثل.[6]

كما صدر عن الجامعة العربية الاتفاقية العربية لمكافحة جرائم التقنية الحديثة، والتي وافق عليها مجلس وزراء العرب بتاريخ 21-12-2010م، وتعد نقطة تحول في التعاون العربي لمكافحة هذه الجرائم، حيث

---

[1]- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص 93

[2]- جميلة سعيد مصباح شوران، اذن التفتيش في الأوساط الالكترونية، مرجع سابق، ص 120

[3]- صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، سنة 2016م، ص 271

[4]-مشار اليه لدي مصطفي علي خلف، التفتيش وفقا لأحكام القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، مرجع سابق، ص20

[5]- اتفاقية بودابست تعرف باسم اتفاقية مجلس أوروبا بشأن الجرائم الالكترونية، وقد فتح باب التوقيع عليها في عام 2001 ودخلت حيز التنفيذ في عام 2004م، وكانت اول معاهدة دولية تركز على الجرائم الالكترونية.

[6]- محمد مرزوق الظهوري، مأمون محمد سعيد، أثر إجراءات التفتيش التقليدية على حجية الدليل الالكتروني، مرجع سابق، ص 156

نصت الاتفاقية علي التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها التعاون القضائي وتبادل المعلومات وتبادل الخبرات، وباعتبار ليبيا من الدول الموقعة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فذلك يعني تمتعها بما تكفله هذه الاتفاقية من إمكانية التعاون بين الدول الأطراف في البحث عن الدليل الرقمي.[1]

المبحث الثاني

ضوابط التفتيش الالكتروني

من خلال هذا المبحث سنتطرق إلى أهم الضوابط الشكلية للتفتيش الإلكتروني (المطلب الأول)، ثم نتطرق إلى الضوابط الموضوعية (مطلب ثاني).

المطلب الأول

الضوابط الشكلية للتفتيش الإلكتروني

المقصود بالضوابط الشكلية تلك الإجراءات التي أوجب المشرع مراعاتها عند اجراء عملية التفتيش والهدف من وضع هذه الضوابط من قبل المشرع هو إحاطة عملية التفتيش بإجراءات وشكليات تتضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش، وإحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية، فالشكلية في الإجراءات الجنائية هي ضمانة لعدم تعسف الجهات القائمة بالتفتيش،[2] وتتمثل هذه الضوابط في:

الفرع الأول/ صدور إذن بالتفتيش:

يُقصد بإذن التفتيش ذلك التفويض الموجه من سلطة التفتيش المختصة إلى أحد مأموري الضبط القضائي متضمناً تخويله إياه إجراء التفتيش الذي تختص به تلك السلطة.[3]

كما ينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ويجب أن يحدد إذن التفتيش المكان المراد تفتيشه والشخص، أو الأشياء المراد تفتيشها وضبطها، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون له 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 أسماء هذه الملفات لا تدل بالضرورة علي ما تحتويها،[4] وبالتالي فهل يعتبر كل ملف "صندوقاً مغلقاً يحتاج إلى إذن قضائي مستقل عن الاخر؟

يري جانب من الفقه المصري أنه لا ينبغي تفتيش كل الملفات التي بجهاز الحاسوب بموجب إذن واحد فقط؛ ذلك لأن الإذن الذي صدر يكون بشأن جريمة محددة (جريمة قرصنة برامج مثلاً)، وبإمكان المأذون أن يصادف أثناء تنفيذ الإذن جريمة عرضية أخرى مثل حيازة صور مخلة، واستند هذا الرأي أيضاً أنه لا يتصور امتداد إذن التفتيش إلى كل ملفات الحاسوب؛ لأن التفتيش ليس إذناً باستباحة حرمة الشخص أو حرمة مسكنه بغير قيد، ولكنه مقيد بالغرض منه.[5]

كما نصت المادة 39 من قانون الإجراءات الجنائية الليبي على أنه: (لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها ...)، فهي تشترط أن ينصب التفتيش على مكان محدد أو قابل للتحديد بشكل نافٍ للجهالة، فيكون الإذن بغرض البحث عن جريمة ما، فهو محدد بهذه الجريمة لا يجوز أن يمتد لغيرها إلا عرضاً، حينها يحق لمأمور الضبط القضائي ضبط وتحريز الدليل

---

[1]- جميلة سعيد شوران، اذن التفتيش في الأوساط الالكترونية، مرجع سابق، ص 221

[2]- عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، سنة 2018م، ص 56

[3] - نص المشرع الأردني علي هذا الشرط في المادة 12/أ من القانون رقم 30 لسنة 2010 بشان الجرائم الالكترونية التي تنص علي انه "مع مراعاة حقوق المشتكي عليه الشخصية يجوز لموظفي الضابطة العدلية بعد الحصول علي اذن من المدعي العام المختص او من المحكمة المختصة الدخول الي أي مكان تشير الدلائل الي استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم وفي جميع الأحوال علي الموظف الذي قام بالتفتيش ان ينظم محضرا بذلك ويقدمه الي المدعي المختص "

[4]- ليندا طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، عدد16، سنة 2017م، ص 493

[5]- مصطفي علي خلف، التفتيش وفقا للأحكام القانون 175لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات، مرجع سابق، ص43

الذي تم العثور عليه عرضاً، فمثلاً إذا صدرت مذكرة التفتيش عن أدلة جريمة نشر فيروسات وأثناء التفتيش في كمبيوتر المتهم وجد مأمور الضبط صدفة ما يثبت قيامه بالترويج للمخدرات والمؤثرات العقلية عبر شبكة الأنترنت، فإن ضبط مأمور الضبط يعتبر صحيحاً؛ وذلك كون الدليل قد عُثر عليه بطريق الصدفة.[1]

الفرع الثاني/ الحضور الضروري للأشخاص المعنين بالتفتيش:

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان على سلامة الإجراء، وغني عن البيان أن التفتيش فيه اطلاع على أسرار الغير، فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الجنائية لصحته حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن ينص القانون على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه، أو المتهم عندما يتم تفتيش مسكنه، وإذا تعذر ذلك بامتناعه عن حضور التفتيش يتم هذا الإجراء بحضور شاهدين.[2]

إن قاعدة حضور المتهم لا تثير أي إشكاليات في مجال تفتيش الجرائم التقليدية بعكس التفتيش في الجرائم الإلكترونية، لما تفتضيه من السرعة في استخلاص الأدلة الإلكترونية وضبطها قبل حدوث أي تغير أو تلاعب فيها، مما قد يحول دون الوصول إلى الحقيقة المرجوة، لأن اغلب التشريعات القانونية لم تضمن نصوصاً خاصة بوضع حراسة إلكترونية على مسرح الجريمة الإلكتروني لتأمينه من أي عبث بالأدلة الإلكترونية، كوضع أجهزة لتشويش الاتصال وتعطيل أو فصل الشبكة الخلوية عن مسرح الجريمة؛ لذلك لابد من التنبه إلى مدى خطورة حضور المتهم عند التفتيش بحثاً عن الأدلة الالكترونية، بالأخص إذا كان المتهم ذو معرفة تقنية عالية، فيكفي أحياناً مجرد كبسة زر على لوحة المفاتيح أو حتي عن بعد باستخدام جهاز إلكتروني آخر لمحو الأدلة والبيانات المتعلقة بالجريمة أو التلاعب بالبرامج المراد تفتيشها، لذلك متى كان حضور المتهم إجراء التفتيش قد يتسبب بعرقلة سير التحقيق أو الإضرار به، فالأولي عدم حضوره كما قد يضطر المحقق إلى نقل أجهزة الحاسب الآلي وما في حكمها من الأجهزة الذكية إلى المختبر الجنائي عند تعذر الحصول على كلمة المرور لملفات معينة، مما قد يضطر إلى استخدام برمجيات وأدوات تقنية عالية لا تتوافر إلا في المختبر الجنائي، وقد يحتاج الخبير التقني وقتاً ليس بالقصير لفك الشفرة، فليس من المعقول احضار المتهم إلى المختبر الجنائي ليشهد تفتيش الملفات الإلكترونية بعد فك شفرتها.[3]

المطلب الثاني

الضوابط الموضوعية للتفتيش الالكتروني

ويقصد بهذه الضوابط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ومن هذه الضوابط:

الفرع الأول/ وجود سبب للتفتيش الإلكتروني:

إذا كان الهدف من إجراء التفتيش هو الحصول على أدلة تساهم في كشف حقيقة الواقعة الإجرامية ونسبتها إلى مرتكبها، فإن هذا الأمر يقتضي للقيام به ضرورة وقوع الجريمة بصورة قطعية، وتشترط بعض التشريعات (كالتشريع الليبي) أن تكون الجريمة ذات خطورة معينة، ففي التفتيش المنزلي اشترط المشرع الليبي أن يكون الشخص متهماً بارتكاب جناية أو جنحة، ومن ثم لا يجوز الإجراء لضبط جريمة مستقبلاً أو لمجرد ورود معلومات تشير إلى إمكانية وقوع الجريمة مستقبلاً، وحتى لو كانت الدلائل كافية على أنها ستقع بالفعل.[4]

الفرع الثاني/ توافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة معلوماتية تساعد في كشف الحقيقة:

---

[1]- جميلة سعيد شوران، اذن التفتيش في الأوساط الالكترونية، مرجع سابق، ص 118

[2] - طبقا للمادة 40 من قانون الإجراءات الجنائية يجب ان يتم تنفيذ التفتيش بحضور صاحب المنزل او القاطن فيه او من ينيبه متي أمكن ذلك، فضلا عن حضور شاهدين بالغين يكون قد الإمكان من اقاربه او القاطنين معه بالمنزل او الجيران، راجع بالخصوص الدكتور موسي مسعود ارحومة، الوسيط في شرح قانون الاحكام العامة لقانون الإجراءات الجنائية، الجزء الأول، الطبعة الاولي ،2020، ص 290

[3]- محمد مرزوق الضهورى، مأمون محمد سعيد، أثر إجراءات التفتيش التقليدية على حجية الدليل الالكتروني، مرجع سابق، ص160

[4]- الهام بن خليفة، التفتيش كأجراء تقليدي لجمع ادلة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 2، العدد 1، سنة 2018م، ص32

بالنسبة للتفتيش الشخصي فالمتفق عليه أنه كلما جاز القبض جاز التفتيش حسب المادة 35 من قانون الإجراءات الجنائية،[1] والمقصود بتفتيش شخص المتهم هنا هو كل ما يحمله بشخصه، لذلك تدخل في محيط هذا التفتيش الحقائب والأوراق التي يحملها سواء أكانت مختومة أم مغلقة، ولصحة هذا الإجراء تشترط التشريعات فيما عدا شرط الإذن الشروط المطلوبة في التفتيش المنزلي، وذلك من حيث خطورة الجريمة، وكذلك جدية التحريات بأن تتوافر لدى المحقق أسباب كافية بأن لدي الشخص المراد تفتيشه أدوات استعملت في ارتكاب جريمة الأنترنت أو ناتجة عنها، أو ما يدعو في الاعتقاد بأنه ساهم في ارتكابها بوصفه فاعلاً أو شريكاً مما يستوجب اتهامه،[2] ويقصد بالدلائل الكافية بصفة عامة شبهات مستمدة من الواقع وقرائن تنبئ عن ارتكاب شخص لجريمة من الجرائم، أما في جرائم الأنترنت فهي مجموعة من المظاهر أو الأمارات المعينة التي تنهض على السياق العقلي والمنطقي لملابسات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة جريمة الأنترنت إلى شخص معين سواء بوصفه فاعلاً أو شريكاً، كما يجب أن تتوافر لدى المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المطلوب تفتيشه أدوات استخدمت في الجريمة المعلوماتية، أو أشياء متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره، وذلك حتى يأذن بالتفتيش بقدر يبرر تعرض التفتيش لحرمة الشخص في حريته ومسكنه في سبيل كشف اتصاله بالجريمة المعلوماتية، فلا مجال للتفتيش أن لم تتوافر لدى المحقق أسباب كافية على أنه يوجد في مكان، أو لدى الشخص المطلوب تفتيشه أدوات استخدمت في الجريمة أو أشياء متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره، وذلك حتى يأذن له بالتفتيش بقدر يبرر تعرض التفتيش لحرمة الشخص في حريته ومسكنه في سبيل كشف الحقيقة[3] ، ولكن بسبب الاستخدام المتزايد للحاسوب المحمول وأجهزة التخزين الإلكترونية والهواتف المحمولة، فإن رجال الضبط القضائي قد يجدون تلك الهواتف المحمولة عند القيام بالتفتيش، فهل يجوز لمأمور الضبط القضائي الاطلاع على ذاكرة هذه الهواتف المحمولة أم أن ذلك يتطلب إذناً من السلطة المختصة؟

أجاب القضاء الأمريكي على ذلك وانقسم الي اتجاهين :الاتجاه الأول رافض لتفتيش الهاتف المحمول حوزة المقبوض عليه بدون اذن ويقيم هذا الاتجاه حجته على قاعدة مؤداها ان من حق الافراد ان يكونوا امنين على انفسهم وممتلكاتهم ومستنداتهم ضد عمليات التفتيش والمصادرة غير المعقولة ،وعليه فلا يجوز اصدار أي أوامر تفتيش قضائية الا بناء على أسباب محتملة ، وتطبيقا لذلك أصدرت المحكمة حكمها في قضية Ohi v.smil باستبعاد الدليل الناتج عن تفتيش الهاتف المحمول المضبوط حوزة المقبوض عليه متي تم دون امر قضائي ،وقررت المحكمة ان الهواتف المحمولة لها القدرة علي تخزين الكم الهائل من معلومات الرقمية ،وبالتالي فإنها تختلف عن أي شيء مادي اخر موجود داخل حقيبة مغلقة تحتوى أشياء مادية ورفضت المحكمة أي قياس يساوى بين الهاتف المحمول والحاوية المغلقة.

بينما الاتجاه الثاني يؤيد تفتيش الهاتف المحمول حوزة المقبوض عليه بدون اذن ويري هذا الاتجاه انه متي تم القبض فانه يجوز تفتيش الهاتف المحمول الذي يحوزه دون ان يسبق ذلك صدور اذن قضائي بالتفتيش، وانه ليس في ذلك أي مخالفة للتعديل الرابع من الدستور الأمريكي وذلك تطبيقا لقواعد التفتيش العامة ،فبيانات الهاتف قد تتضمن سلامة الضابط بطريقة غير مباشرة من خلال تنبيه ان شركاء المتهم في طريقهم الي مكان الحادث وانه حتي ولو تم تامين الهاتف المحمول فان معلومات الهاتف قد تكون عرضة للتدمير كأحد

[1]- يجري نص المادة 35 من قانون الإجراءات الجنائية على أنه " في الأحوال التي يجوز فيها القبض قانونا علي المتهم يجوز لمأمور الضبط القضائي ان يفتشه".

[2]- جميلة سعيد شوران ، اذن التفتيش فبي الأوساط الالكترونية ، مرجع سابق ، ص118

[3]- الهام بن خليفة، التفتيش كأجراء تحقيق تقليدي لجمع ادلة الجرائم المتصلة بتكنولوجيا الاعلام ولاتصال، مرجع سابق، ص33

خصائص التي تنفرد بها البيانات الرقمية مثل المسح عن بعد او تشفير تلك التي تحدث عندما يلتقي الهاتف المتصل بشبكة اللاسلكية إشارة يرسلها طرف ثالث عن بعد من شأنها مسح البيانات المخزنة [1].
بالرجوع لنص المادة 35 من قانون الإجراءات الجنائية نجد أنها سمحت لمأمور الضبط القضائي بتفتيش الشخص وما يحمله في حالة القبض الصحيح، فيظهر تعارض هذا النص عند تطبيقه على تفتيش الهواتف المحمولة التي بحوزة الشخص والبحث في ما قد تحمله من بيانات ومعلومات شخصية، مع ما جاء في حكم للمحكمة العليا الليبية قضت فيه بأن: (القبض على المتهم، وتفتيشه دون توافر دلائل كافية هو قبض باطل، وأمر خطير لا يمكن اقراره أو التسليم به) [(2)] ، وهذه الدلائل الكافية غالباً ما تكون غير موجودة في حالات الاستيقاف التي يتم فيها تفتيش أجهزة الشخص، كما يتعارض هذا مع رغبة المشرع في حماية الحياة الخاصة وضمان سرية البيانات والرسائل وعدم جواز الاطلاع عليها، نظراً لما تحويه من أسرار تتعلق بالحياة الخاصة للفرد، كما تظهر رغبة المشرع في حماية الحياة الخاصة واضحة في النصوص الواردة في قانون الاتصالات رقم 22 لسنة 2010م في المادة 15 منه [(3)] ، فالهاتف المحمول أصبح يلعب دور مهم في حياة الإنسان، فهو ليس وسيلة لإجراء واستقبال المكالمات الهاتفية فقط، لأن الهواتف الذكية أصبحت تحتوى على تطبيقات إلكترونية تسمح بالاحتفاظ بسجل المكالمات والرسائل النصية ورسائل البريد الإلكتروني وغيرها من الاتصالات بالإضافة إلى الصور والعديد من البرامج والتطبيقات الموجودة بالهاتف، وبمعني آخر إن هذه الهواتف تحوى بيانات ومعلومات وأسرار خاصة بالفرد يمكن أن يكون أكثر مما يحويه منزله ومراسلاته، مما يعني ضرورة تدخل المشرع الليبي لإحاطتها بضمان الإذن عند التفتيش لتوفير الحماية لها بشكل أكبر.

الفرع الثالث/ صفة القائم بالتفتيش:

يقتصر القيام بالتفتيش كإجراء من إجراءات التحقيق على الجهات التي خصَّها المشرع بالصفة لممارسة هذا الإجراء، والواقع أنه في ضوء القانون الليبي يقتصر القيام به على جهات التحقيق ومأمور الضبط القضائي في أحوال استثنائية، وبالنظر إلى الطبيعة الفنية لتفتيش الوسط الافتراضي فإنه يقتضي أن يكون القائم به مؤهلاً من الناحية الفنية ليتمكن من مباشرته.

الفرع الرابع/ أن يكون الهدف من التفتيش جمع وضبط الأدلة التي تتعلق بالجريمة التي وقعت:

بالإضافة إلى الشروط السابقة فإنه يشترط أن يكون الغرض من التفتيش الإلكتروني من الناحية الموضوعية أن يكون الغرض منه ضبط أشياء تتعلق بالجريمة التي وقعت؛ لأن التفتيش إجراء من إجراءات التحقيق والهدف الرئيسي منه هو جمع الأدلة وكشف الحقيقة عن مرتكبها لهذا لابد أن يكون السبب هو تحقيق ذلك الغرض، وألا يقع التفتيش باطلاً إذا كان لأي غرض آخر.[(4)]

الخاتمة

نظراً للتطور العلمي وانتشار التقنية المعلوماتية في التعاملات اليومية، فقد أدى ذلك إلى استغلال الجناة هذه التقنية كوسيلة لارتكاب الجرائم، ولذلك اختلف الوسط الذي ترتكب فيه الجريمة من وسط مادي إلى وسط معنوي أو افتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة هذا الوسط الذي ترتكب فيه الجريمة، وهو ما يسمي بالأدلة الإلكترونية أو الرقمية.

ولقد خلص هذا البحث إلى مجموعة من النتائج والتوصيات نوردها على النحو الآتي

---

[1] ـ مشار اليه لدي مصطفي على خلف ، تفتيش الهاتف المحمول حوزة المقبوض عليه "دراسة تحليلية تطبيقية مقارنة" المجلة الدولية للفقه والقضاء والتشريع ،المجلد 5،العدد1 ، 2024،ص 156/153، انظر أيضا الي محمد زيد الهاجري، تفتيش المقتنيات الالكترونية للمتهم والتوقع المعقول للخصوصية دراسة مقارنة في النظامين الكويتي والامريكي، المجلة القانونية ،المجلد 7،العدد 5، 2020،ص31

[2] ـ طعن جنائي رقم 53/1162ق، مجموعة احكام المحكمة العليا.

[3] ـ جميلة سعيد شوران، اذن التفتيش في الأوساط الالكترونية، مرجع سابق، ص 119

[4] ـ سعاد راضي حسين، الإجراءات الجزائية في تفتيش محل الجرائم الالكترونية، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد 4، العدد 4 ، سنة 2024م ، ص135

أولاً/ النتائج:

1- أثناء التفتيش غالباً ما تستباح ملفات المتهم الإلكترونية من قبل مأمور الضبط القضائي، وغالباً ما يتم اكتشاف بيانات وأسرار شخصية تدخل ضمن الحياة الخاصة للأفراد والتي تحرص التشريعات على حمايتها وضمان سريتها، سواء كانت خاصة بالمتهم أو بغيره وجب ألا يتم التفتيش إلا بضمانات تحمي هذه الخصوصية.

2- في حالة تشابك الأجهزة لا يجوز التفتيش خارج حدود الدولة احتراماً لمبدأ السيادة، ومع ذلك يجوز الحصول على الأدلة الموجودة في الوسط الافتراضي خارج حدود الدولة، تطبيقاً لاتفاقيات الانابة القضائية.

3- الهواتف المحمولة تلعب دور مهم في حياة الإنسان، فهو ليس وسيلة لإجراء واستقبال المكالمات الهاتفية فقط، لأن الهواتف الذكية أصبحت تحتوي على تطبيقات إلكترونية تسمح بالاحتفاظ بسجل المكالمات والرسائل النصية ورسائل البريد الإلكتروني وغيرها من الاتصالات بالإضافة إلى الصور والعديد من البرامج والتطبيقات الموجودة بالهاتف.

4- قصور أغلب التشريعات من الناحية الإجرائية فيما يخص إجراءات الحصول على الدليل الرقمي، حيث تقتصر على القواعد العامة والإجراءات التقليدية.

ثانياً/ التوصيات:

1- اهيب بالمشرع الليبي النص صراحة على إجراءات الحصول على الدليل الرقمي وعلى وسائل التأكد من سلامته.

2- النص صراحة على جواز البحث في المكونات المعنوية للحاسب الآلي والأنظمة المعلوماتية وما في حكمها من التقنيات الحديثة، وكل ما يمت بصلة للجريمة ويساهم في اظهار الحقيقة والكشف عن الجريمة.

3- ضرورة وضع نصوص تضمن خصوصية الشخص المراد تفتيش منزله أو شخصه، وذلك من خلال وضع ضوابط تحد من سلطة مأمور الضبط القضائي من الاطلاع على الأجهزة المحمولة الخاصة بالشخص، كأن يتم قيدها بالحصول على إذن من القاضي المختص، إلا إذا وجد خطر يهدد حياة مأمور الضبط القضائي أو يهدد الدليل الرقمي بالتلف.

4- تدعو الباحثة المشرع الليبي الى ضرورة التوسع في عقد الاتفاقيات الدولية للاستفادة من نظام الانابة القضائية وتبادل المعلومات في المجال المعلوماتي لتفادي مشكلة البحث عن الدليل الرقمي خارج حدود الدولة.

قائمة المراجع

أولاً/ الكتب:

1- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر ، سنة 2011م.

2- عبد الرحمن محمد أبوتوتة، شرح قانون الإجراءات الجنائية، الدعوى الجنائية والدعوى المدنية والاستدلالات والتحقيق الابتدائي، دار الحكمة للنشر والتوزيع،

ثانياً/ الرسائل والأطروحات العلمية:

1- شيماء حمدان، الإطار القانوني للتفتيش في الجرائم الالكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة محمد الصديق بن يحي، جيجل/الجزائر، 2023/2022م

2- عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا ،2011 سنة

ثالثاً/ البحوث والمقالات المنشورة:

1- أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الالكتروني (دراسة مقارنة)، مجلة الدراسات القانونية والاقتصادية، المجلد 8،العدد 2، سنة 2022م.

2- إلهام بن خليفة، التفتيش كأجراء تقليدي لجمع ادلة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 2، العدد 1، سنة 2018م.
3- جميلة سعيد شوران، إذن التفتيش في الأوساط الالكترونية، مجلة أبحاث بكلية الآداب، جامعة سرت، مجلد 15 العدد 1، مارس 2023م.
4- حطاب كمال، خصوصية التفتيش في البيئة الالكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 09، ا لعدد 01 السنة 2023م.
5- سعاد راضي حسين، الإجراءات الجزائية في تفتيش محل الجرائم الالكترونية، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد 4، العدد 4، سنة 2024م.
6- صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، سنة 2016م.
7- طارق الجملي، الدليل الرقمي في مجال الاثبات الجنائي، مجلة الحقوق، جامعة البحرين، كلية الحقوق، المجلد 12، العدد 1، سنة 2015م.
8- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي مركز بحوث الشرطة بالقيادة العامة لشرطة الشارقة، الامارات، مجلد 22 العدد86، سنة 2013م.
9- عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، سنة 2018م.
10- محمد جمال الذنيبات، القاضي معن أحمد العناسوة، التفتيش في الجرائم الالكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، المجلد 13 العدد 3، سنة 2021م.
11- محمد مرزوق الظهورى، مأمون محمد سعيد أبو زيتون، لثر، إجراءات التفتيش التقليدية على حجية الدليل الالكتروني "دراسة مقارنة" مجلة جامعة الشارقة للعلوم القانونية، المجلد 21، العدد 3، سبتمبر 2024م.
12- مصطفي إبراهيم العربي، دور الدليل الرقمي في الاثبات الجنائي، مجلة البحوث القانونية، كلية القانون، جامعة مصراتة، السنة الرابعة، العدد الأول، سنة 2016م.
13- مصطفي علي خلف، التفتيش وفقا لأحكام القانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات، المجلة الجنائية القومية، المجلد 63، العدد 3، نوفمبر 2020م.
14- ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الأردني، دراسات، علوم الشريعة والقانون، المجلد 45، عدد 4، ملحق2 لسنة 2018م.
15- موسي مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجرائم المعلوماتية عبر الوطنية، بحث مقدم الي المؤتمر المغاربي الأول حول: المعلوماتية والقانون الذي نظمته أكاديمية الدراسات العليا، طرابلس، ليبيا خلال الفترة 28/29/10/2009م.

References

First: Books:

1- Sami Jalal Faqi Hussein, Investigation in Cybercrimes, An Analytical Study, Dar Al-Kotob Al-Qanuniyah, Egypt, 2011.

2- Abdul Rahman Muhammad Abu Tuta, Explanation of the Criminal Procedure Code, Criminal and Civil Suits, Evidence, and Preliminary Investigation, Dar Al-Hikma for Publishing and Distribution.

Second: Academic Theses:

1- Shaima Hamdan, The Legal Framework for Investigation in Cybercrimes, Master's Thesis, Faculty of Law and Political Science, University of Mohamed Seddik Ben Yahia, Jijel, Algeria, 2022/2023.

2-Abdullah bin Abdulaziz Al-Khathami, Investigation in Cybercrimes in the Saudi System, Master's Thesis, Naif Arab University for Security Sciences, College of Graduate Studies, 2011.

Third: Published Research and Articles:

1- Ahmed Lotfi Al-Sayed Marai, Digital Evidence Obtained from Electronic Criminal Investigation (A Comparative Study), Journal of Legal and Economic Studies, Volume 8, Issue 2, 2022.

2- Ilham Bin Khalifa, "Search as a Traditional Procedure for Collecting Evidence of ICT-Related Crimes," International Journal of Legal and Political Research, Volume 2, Issue 1, 2018.

3- Jamila Saeed Shuran, "Search Permits in Electronic Media," Journal of Research, Faculty of Arts, University of Sirte, Volume 15, Issue 1, March 2023.

4- Hattab Kamal, "The Privacy of Searches in the Electronic Environment," Journal of Research in Law and Political Science, Volume 9, Issue 1, 2023.

5- Suad Radhi Hussein, "Criminal Procedures in Searching Cybercrime Sites," Middle East Journal of Legal and Jurisprudential Studies, Volume 4, Issue 4, 2024.

6- Safaa Hassan Nassif, "Procedural Challenges Related to Cybercrimes," Journal of Legal and Political Science, Volume 5, Issue 2, 2016.

7- Tariq Al-Jamali, Digital Evidence in the Field of Criminal Evidence, Journal of Law, University of Bahrain, College of Law, Volume 12, Issue 1, 2015.

8- Adel Abdullah Khamis Al-Maamari, Investigation in Cybercrimes, Journal of Police Thought, Police Research Center, Sharjah Police General Command, UAE, Volume 22, Issue 86, 2013.

9- Ezzedine Othmani, Investigation and Inspection Procedures in Crimes Affecting Communications and Information Systems, Journal of the Department of Legal and Political Research and Studies, Laboratory of Constitutional Institutions and Political Systems, Issue 4, 2018.

10- Muhammad Jamal Al-Dhunaibat, Judge Maan Ahmad Al-Anaswa, Investigation in Cybercrimes: Its Nature and Formal Conditions, Jordanian Journal of Law and Political Science, Volume 13, Issue 3, 2021.

11- Muhammad Marzouq Al-Dhahouri, Mamoun Muhammad Saeed Abu Zaytoun, "Traditional Inspection Procedures for the Validity of Electronic Evidence: A Comparative Study," Sharjah University Journal of Legal Sciences, Volume 21, Issue 3, September 2024.

12- Mustafa Ibrahim Al-Arabi, "The Role of Digital Evidence in Criminal Proof," Legal Research Journal, Faculty of Law, Misurata University, Fourth Year, Issue 1, 2016.

13- Mustafa Ali Khalaf, "Inspection in Accordance with the Provisions of Law No. 175 of 2018 Concerning Combating Information Technology Crimes," National Criminal Journal, Volume 63, Issue 3, November 2020.

14- Mamdouh Hassan Mani' Al-Adwan, Nader Abdul Halim Al-Salamat, "The Legitimacy and Validity of Evidence Extracted from Electronic Inspection in Jordanian Legislation," Studies, Sharia and Legal Sciences, Volume 45, Issue 4, Supplement 2, 2018.

15- Musa Masoud Arhuma, Procedural Problems Raised by Transnational Cybercrimes, a paper presented to the First Maghreb Conference on: Information Technology and the Law, organized by the Academy of Graduate Studies, Tripoli, Libya, during the period 28/29/10/2009.