التفتيش فى الجريمة الإلكترونية

سعود على اللوغانى

التفتيش فى الجريمة الإلكترونية

سعود على اللوغانى

بسم الله الرحمن الرحيم

المقدمة

يعرف التفتيش بأنه " عبارة عن اجراء من اجراءات التحقيق التي تهدف الى البحث عن أدلة مادية لجناية او جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف اثبات ارتكابها أو نسبتها الى المتهم وفقاً لاجراءات قانونية محددة[1].

ولم تحدد بعض التشريعات المقصود بالتفتيش ومنها المشرع المصري على الرغم أنه ذكره كاحد اجراءات التحقيق الأصلية ونص عليه بذلك ، بينما تناول المشرع الاماراتي التفتيش وعرفه بشكل غير مباشر في المادة ٥١ من قانون الإجراءات الجزائية بأنه " البحث عن آثار أو اشياء تتعلق بالجريمة أو لازمة للتحقيق فيها" .

كما عرفتها ايضا المادة ١٢٢ من التعليمات القضائية للنيابة العامة الاتحادية بأنه " اجراء من اجراءات التحقيق التي تهدف الى ضبط أدلة الجريمة موضوع التحقيق وكل مايفيد في كشف الحقيقة ، من أجل اثبات ارتكاب الجريمة أو نسبتها الى المتهم ، وينصب على المتهم والمكان الذي يقيم فيه ، ويجوز أن يمتد الى أشخاص غير المتهمين ومساكنهم وذلك بالشروط والأوضاع المحددة في القانون" .

واذا ما امعنا النظر في أساس التفتيش بشكل عام نجد أن فيه انتهاكاً للحق في الخصوصية التي حماها الدستور وبالتالي يستباح هذا الحق طالما

---

(١) هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٤٧ .

أن هنالك مبرراً نص عليه القانون لهذا الانتهاك ، لذا فهو يعد من بين أقسى الصلاحيات التي يمارسها القانون ضد المواطن ، ويعد أحد مظاهر تقييد الحريات الانسانية التي ساهمت التشريعات الكبرى الاساسية وبشكل مباشر في دعم المحافظة عليها[1].

واذا ما كان التفتيش يهدف الى ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة فان وقوعه على الدعائم المادية لوسائل التقنية الحديثة لا يثير جدلا فقهيا، الا أن الامر يختلف تماما بالنسبة للكيان المعنوي لهذه الوسائل التقنية والمتمثل في البيانات والمعلومات الالكترونية غير المحسوسة، حيث يثير وقوع التفتيش على هذه المكونات جدلا كبيرا لما لها من طبيعة خاصة تخرجها من دائرة المكونات المادية لوسائل التقنية الحديثة، وعلى ذلك يعد تفتيش انظمة الحاسب الآلي والشبكة المعلوماتية من اخطر المراحل حال اتخاذ الإجراءات الجزائية ضد المجرم المعلوماتي، لكون محل التفتيش هنا يرد على نظام تقني رقمي، الامر الذي يثير جدلا فقهيا متزايدا يوما بعد يوم فيما يخص الجانب غير المادي له ، فهو لا يعدو ان يكون الا معلومات الكترونية ليس لها اي مظهر مادي محسوس في العالم الخارجي.

وحال أنه تقتضي مصلحة وظروف التحقيق في هذه النوعية من الجرائم المستحدثة الدخول الى انظمة الحاسب الالي والشبكة المعلوماتية، للبحث والتنقيب في البرامج المستخدمة وملفات البيانات المخزنة، عما يتعلق بجريمة وقعت باستخدام الانظمة الالكترونية، فما مدى صلاحيتها كمحل يرد عليه التفتيش، وما هي الضمانات المقررة لذلك في ضوء القوانين الجزائية المقارنة، وهذا ما سنقوم بالتطرق له من خلال المطالب الآتية:

---

(١) عمر محمد ابوبكر بن يونس : الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، ٢٠٠٤، ص ٨٥٢

المطلب الأول: تفتيش أنظمة المعلومات الالكترونية

المطلب الثاني: الحدود المكانية لتفتيش شبكات الحاسب الآلي

المطلب الثالث: ضوابط التفتيش في الجرائم الالكترونية

المطلب الأول
تفتيش أنظمة المعلومات الإلكترونية

لا يختلف التفتيش في مدلوله القانوني بالنسبة للجرائم المعلوماتية عن مدلوله السائد في فقه الإجراءات الجنائية ، فالمقصود منه هو أنه " اجراء من اجراءات التحقيق تقوم به سلطة مختصة ، لأجل الدخول الى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات ، وذلك لأجل البحث فيها عن افعال غير مشروعة تكون مرتكبة من قبل شخص ما ، وتشكل جناية او جنحة ، والتوصل من خلال ذلك الى أدلة وآثار تفيد في اثبات الجريمة الواقعة ونسبتها الى المتهم بارتكابها"[1] .

وعلى الرغم من الصلاحيات التي منحها القانون للقائمين بالتفتيش، فان هنالك بعض الإجراءات التي تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية ، ومنها تعدد الأماكن التي يوجد بها النظام المعلوماتي داخل أو خارج الدولة ، كما أن هنالك صعوبة في تحديد الأشياء التي تهدف من عملية التفتيش القائمة ، وغيرها من الصعوبات مثل عدم اكتمال المعرفة المعلوماتية والتقنية للقيام بعملية التفتيش بالصورة المطلوبة[2] .

---

(١) هشام محمد رستم : الجوانب الاجرائية للجرائم المعلوماتية، – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤ ، ص٦٢.
. انظر ايضا : هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص ٧٣ .

(٢) انظر : .عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣، ص ٣٤٤ .

وفي سياق موضوعنا لا بد أن نشير الى ان المادة ٥١ من اتفاقية بودابست[1] قد نصت على أن لكل طرف اتخاذ الإجراءات التشريعية لكي يمنح السلطات المختصة اذناً بالتفتيش أو الدخول بطريقة مشابهة[2] :-

١- لأية شبكة معلومات أو لجزء منها، وكذلك البيانات المعلوماتية المخزنة بها.

٢- أي جهاز تخزين معلومات يسمح بتخزين البيانات المعلوماتية في داخل النطاق المحلي.

٣- لكل طرف أن يتخذ الإجراءات التشريعية اللازمة أو غيرها مما يراها ضرورية للسماح للسلطات بالتفتيش، أو الدخول بطريقة مشابهة داخل شبكة معلومات أو في جزء منها، وفقاً للفقرة الأولى (أ) بعد أن يتوافر لديهم الأسباب الكافية للاعتقاد بأن المعلومات المطلوب البحث عنها وجدت مخزنة في شبكة معلومات أخرى، أو في جزء آخر من تلك الشبكة الموجودة في إطار النطاق المحلي، وأنه يمكن

---

(١) بتاريخ ٢٠ نيسان تقدمت اللجنة الاوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية CYPER CRIME بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الاراء خلال الفترة من اصدار مشروعها الأول وحتى اعداد مسودتها النهائية التي اقرت لاحقا في بودابست ٢٠٠١ وتعرف بهذا الاسم بودابست ٢٠٠١، وكان قد تم طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات واطلق ضمن مواقع عديدة اوروبية وامريكية على شبكة الانترنت للتباحث وابداء الراي بشأنها. وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الاوروبي ومجلس اوروبا ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر واغراضها منذ اكثر من ١٠ اعوام.

(٢) صالح أحمد البربري، دور الشرطة في مكافحة جرائم الانترنت، في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٣-١١-٢٠٠١م، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية الذي عقد في أكاديمية شرطة دبي بدولة الإمارات العربية المتحدة، بتاريخ ٢٦- ٢٨ ابريل ٢٠٠٣م، ص٣٩٩.

الوصول إلى هذه المعلومات بطريقة مشروعة عن طريق شبكة رئيسة أخرى، أو لدى تلك الشبكة، وأنه يحق لتلك السلطات المختصة أن تمد التفتيش إليها بسرعة.

٤- أن يمنح كل طرف السلطات المختصة صلاحية ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية والتي تم الدخول على الشبكة من أجل الحصول عليها تطبيقاً للفقرة ١، ٢.

- وهذه الإجراءات تشمل الصلاحيات الآتية

١. ضبط أو الحصول بطريقة مشابهة على شبكة المعلومات أو جزء منها أو أي جهاز لتخزين هذه المعلومات.
٢. نقل وحفظ صورة من تلك البيانات المعلوماتية.
٣. المحافظة على كامل البيانات المعلوماتية المخزونة.
٤. العمل على منع أي أحد من الدخول أو أخذ هذه البيانات المعلوماتية من شبكة المعلومات المعنية.
٥. على كل طرف أن يرخص للسلطات المختصة بأن تصدر أوامرها لأي شخص على علم بنظام تشغيل نظام المعلومات، أو الإجراءات المطبقة لحماية البيانات المعلوماتية التي تحتويها، وأن يمدها بالمعلومات المعقولة واللازمة التي تمكن من تطبيق الإجراءات المنصوص عليها في الفقرة "أ".[١]

وبناءً على ما سبق فاننا نلاحظ أن التفتيش قد يرد على الحاسب الآلي ذاته ومكوناته المادية مثل الشاشة وأجهزة الإدخال والإخراج، والطابعات وأجهزة الماسحات الضوئية والفارة والكابلات والاسطوانات ولوحة المفاتيح وجهاز الكمبيوتر نفسه ووحدات المعالجة المركزية cpu،

(١) د.هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٧، الطبعة الأولى، ص٢٥٠ وما بعدها.

وقد يرد ايضاً على المكونات المعنوية للحاسب الآلي كالأنظمة التقنية والبرمجيات .

والسؤال الذي يستوجب الاجابة عنه ، ما مدى قابلية كل من المكونات المادية وشبكات الحاسب الآلي للتفتيش والمكونات المعنوية ، وماهي الضوابط الموضوعة والتي يجب اتباعها في ذلك ، وهذا ما سنبينه في الفرعين الآتيين : -

الفرع الأول : مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

الفرع الثاني : مدى قابلية المكونات المنطقية "المعنوية" للحاسب الآلي للتفتيش

الفرع الأول
مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

ان خضوع المكونات المادية للحاسب الآلي بمختلف اشكالها وانواعها للتفتيش في مسرح الجريمة الالكترونية لا تثير أية مشكلة ، بمعنى أن صلاحية تفتيش هذه المكونات المادية تتوقف على طبيعة الأماكن الموجودة فيه ، حيث ان لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش ، فاذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها نفس حكمه ، فلا يجوز تفتيشها الا في نفس الحالات التي يجوز بها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة في اغلب التشريعات المختلفة[1] كالمشرع الاماراتي والمصري.

والحقيقة هي ان ظاهرة التفتيش قابلة للعديد من الاحتمالات ، وليس هناك احتمال وحيد يرتبط بوجود او عدم وجود دليل يرتب الادانة امام القضاء ، ومثل هذا الأمر يجعل الحاسب الآلي يتخذ شكلا موسعاً في هذا الشأن ، وهذا الأمر يدفعنا لشمول الحاسب الآلي بالحرز الخاص

(١) د. هشام محمد رستم ، الجوانب الاجرائية للجرائم المعلوماتية ، مرجع سابق ، ص ٦٩ .

الذي يستلزم الاعتراف له بالخصوصية التي يكفلها له القانون وعدم اخضاعه للمكان الموجود فيه أي تجريده منه.

علماً بأن هنالك بعض الأنظمة التي تمنح الحق في ضبط جهاز الحاسب الآلي نفسه، كما هو الحال في المادة "٤١" من قانون الإجراءات الجنائية الفيدرالي[1].

ولم ينص المشرع الاماراتي على ذلك صراحة ولكن نستقي ذلك من نص المادة "٥١" من قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة على أنه: "لمأمور الضبط القضائي أن يفتش المتهم في الأحوال التي يجوز فيها قانوناً القبض عليه ويجري تفتيش المتهم بالبحث عما يكون بجسمه أو ملابسه أو أمتعته من آثار أو أشياء تتعلق بالجريمة أو تكون لازمة للتحقيق فيها".

في حين أنالمادة "١٦" من قانون المنافسة الكندية قد أتاحت لمأموري الضبط القضائي "أن يستخدم أو يعمل على استخدام نظام الحاسب الآلي في المكان محل التفتيش، وذلك للتفتيش عن أية بيانات مخزنة فيه، أو صالحة لاستخدام نظام الحاسب الآلي، كما يمكنه أن يستخرج أو يعمل على استخراج بيانات في شكل مطبوعات أو أية مخرجات غير ملموسة، كما يستطيع أن يضبط المطبوعات، أو المخرجات الأخرى لفحصها أو أخذ صورة عنها[2].

كذلك يجب مراعاة التمييز بين ماذا كانت مكونات الحاسب الآلي – محل التفتيش- منعزلة عن الحاسبات الأخرى ام انها متصلة بحاسب آلي

---

(١) عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفيدرالي لتفتيش وضبط الحواسيب وصولا الى الدليل الالكتروني في التحقيقات الجنائية، بدون دار النشر، ٢٠٠٦. ص ١٧٣.

(٢) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص ١٥٣.

بمنزل شخص أخر غير المتهم على سبيل المثال ، لأنه في هذه الحالة يجب مراعاة القيود والإجراءات التي حددها المشرع لتفتيش ذلك المكان . على خلاف ذلك بالنسبة للاماكن العامة ، فاذا وجد الشخص فيها حاملا مكونات الحاسب المادية أو مسيطرا عليها او حائزا لها فان تفتيشها لا يكون الا في الحالات التي يجوز فيها تفتيش الاشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال ، باعتبار أن تفتيش الشخص يشمل بشكل عام تفتيش ذاته وكل مافي حوزته وقت تفتيشه ، وسواء كان مملوكا له او لغيره فالامر سيان[1] .

الفرع الثاني

مدى قابلية المكونات المنطقية "المعنوية" للحاسب الآلي للتفتيش

لقد أثار موضوع المكونات المنطقية للحاسب الآلي خلافا كبيرا بين الفقه بشأن مدى خضوع هذه المكونات ذات الطبيعة المعنوية (Software) للتفتيش والمتمثلة في الشبكات والبرامج والأنظمة والمعلومات ، فثمة اتجاه يرى أن هذه المكونات المنطقية لا تصلح بطبيعتها لأن تكون كذلك ، على اعتبار أن التفتيش يهدف في المقام الأول الى ضبط الأدلة المادية التي يمكن مشاهدتها ، وبالتالي فانه يصعب خضوع هذه المكونات المعنوية وغير المرئية للتفتيش طبقا لقواعد التفتيش المنصوص عليها في قوانين الإجراءات الجنائية في معظم تشريعات الدول.

ولذلك فقد اقترح البعض لمواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لابد أن يشمل " المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي ، بحيث تصبح الغاية من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات

---

(١) عبدالله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الثانية، ٢٠٠٢، ص ٣٧٠.

والتكنولوجيا تتركز في البحث عن الأدلة المادية او أي مادة معالجة بواسطة الحاسب الالي[1].

وفي المقابل هناك اتجاه آخر يرى أن المكونات المعنوية لا تختلف عن الكيان المادي للحاسب الآلي من حيث خضوعها لأحكام التفتيش ومافي حكمه ، بدعوى أن البيانات التي هي عبارة عن نبضات الكترونية قابلة للتخزين على أوعية ووسائط مادية كالاشرطة المغنطة والاقراص والاسطوانات ، كذلك يمكن تقديرها وقياسها بوحدات قياس خاصة معروفة ، وعلى هذا الأساس تكون صالحة كموضوع للضبط والتفتيش شأنها في ذلك شأن الوسائط المادية ذاتها[2] ، ويستند أصحاب هذا الرأي الى أن القوانين الاجرائية عندما تنص على اصدار الاذن بضبط " أي شيء " فان ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة[3] .

وعليه فان التشكيك في الطبيعة المادية للبيانات الالكترونية قد لا يكون له مسوغ قانوني ، لأن هذه البيانات ولأسباب قانونية وتقنية يجب النظر اليها على أساس أن البيانات و المعلومات هي عبارة عن " أشياء" كما وصفها القانون الفرنسي ، وبذلك تعتبر البيانات والمعلومات نبضات أو ذبذبات الكترونية أو موجات كهورمغناطيسية يمكن تخزينها على وسائط متعددة ، ويمكن نقلها من مكان لآخر ، كما يمكن تقييمها وقياسها ، أي

1- Piragoff (Donald K) Computer crimes and other crimes against information technology in Canada :Rev. Intern. De. Dr.pen 1993. P 241

(٢) موسى مسعود ارحومة ، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، بحث مقدم الى المؤتمر المغاربي الاول حول : المعلوماتية والقانون ، الذي تنظمه اكاديمية الدراسات العليا- طرابلس ، خلال الفترة ٢٨- ٢٠٠٩/١٠/٢٩ ، ص ٧ .

(٣) خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الاولى ، ٢٠١٠ ، ص ١٩٧ .

انها كما وصفتها محكمة بروكسل أشياء محسوسة ومادية يمكن أن ترد عليها عملية التفتيش عند الاعتداء عليها[1] .

ونلاحظ أن الاختلاف بين الأشياء المادية والمعنوية (المعلومات) تكمن في نوع الوعاء الخاص بحفظ كل منهما ، ففي النوع الأول فالوعاء هو الأوراق المادية ، وفي النوع الثاني فيكون الوعاء في ذاكرة الحاسب الآلي او خادم Server أو شبكة الكمبيوتر أو الانترنت ، وهذا الاختلاف مجرد اختلاف شكلي ليس له تاثير على مضمون الوعاء من المعلومات والبيانات[2] ، ويرجع الأساس في هذا الاختلاف الى أن جرائم المعلومات ذات طبيعة تقنية الكترونية وبالتالي فان بياناتها في الغالب ستكون ايضا من طبيعة الكترونية ، وهذا لا يعني أن اثباتها ببيانات أخرى من غير هذه الطبيعة أمر غير متيسر[3].

فالوقوف على مصطلح " الاشياء" عند الاشياء المادية قد يصطدم مع المذهب السائد في تفسير النصوص الجنائية ، والذي لا يعتمد على التفسير الحرفي للفظ فقط ، وانما يعتمد وبشكل أوسع على مذهب التفسير المنطقي ، والذي يطبق اذا كان النص محل التفسير غامضا في المعنى المقصود منه[4].

---

(١) هشام محمد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مرجع سابق، ص ٦٨ .

(٢) عارف محمد عبدالرحيم، دور ومهام أعضاء الضبط القضائي في مرحلتي التحري والتحقيق الابتدائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٠٧، ص٢٥٤.

(٣) اسامة أحمد المناعسة، جلال صايل الهواوشة، جلال الزعبي، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، الاردن، عمان، ٢٠٠١، ص٢٦٦ .

(٤) علي محمود علي حمودة، أدلة اثبات الجرائم الالكترونية وتقديرها في اطار نظرية الاثبات الجنائي، بحث منشور في مجلة الامن والقانون، مجلة تصدر عن أكاديمية شرطة دبي، ص ٣٨ .

فما عناه المشرع من إجازة التفتيش هو إتاحة الفرصة للبحث عن الدليل الذي يساعد في كشف الحقيقة بشأن جريمة وقعت، ولا شك أن المشرع حينما استعمل لفظ (شيء) لم يكن يقصد بذلك الكلمة بمفهومها الحرفي، إذ ما قصده هو البحث عن الدليل في موضعه ، بصرف النظر عما إذا كان موضع البحث شيئا مادياً أو معنوياً، وما إذا كانت الأشياء المراد ضبطها مادية أو معنوية، الأمر الذي يعني أن المشرع وقت وضع النص لم تكن في ذهنه مسألة الوسط الافتراضي لعدم شيوعه آن ذاك ، ولذا فسكوته عن التصريح بإمكانية تفتيشه والحالة هذه لا يحول دون شموله بالنص تطبيقاً لفكرة التفسير الغائي.

وعلى الرغم من أن المشرع الاماراتي لم يعبر بصريح العبارة عن مدى خضوع المكونات المنطقية للحاسب الآلي للتفتيش ، الا أنه قد أكد ذلك في قانون الإجراءات الجزائية الاتحادي ، حيث أشارت نصوص المواد (٥١ ، ٥٣ ، ٥٥ ، ٥٧) من هذا القانون إلى أن التفتيش يقع على الأشياء المتعلقة بالجريمة أو التي تكون لازمة للتحقيق فيها، وقد كرر المشرع كلمة أشياء في جميع هذه المواد دون أن يحدد ماهية هذه الأشياء، وهل هي أشياء مادية أو معنوية.

وعلى هذا النهج نجد أن المادة ٤٨٧ من القانون الجنائي الكندي تعطي للسلطة المختصة الحق في اصدار الاذن بضبط " أي شيء " طالما تتوافر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها باستخدامه ، أو أن هناك نية في أن يستخدم في ارتكاب الجريمة ، أو انه سوف ينتج دليلا على وقوع الجريمة ، ويفسر الفقه عبارة أي شيء بأنها تشمل المكونات المادية والمعنوية في الحاسب الآلي[1] .

---

(١) انظر : هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ص ٨٢ .

كما أن المادة ٢٥١ من قانون الإجراءات الجنائية اليوناني تمنح سلطة التحقيق الحق في القيام باي عمل ضروري لجمع الدليل من مسرح الجريمة وحمايته ، وفي ذلك يفسر الفقه اليوناني عبارة " أي شيء" بأنها تشمل ضبط البيانات المخزنة أو المعالجة الكترونياً ، وبذلك فان تفتيش البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أي مشكلة في القانون اليوناني ، اذ يمكن للمحقق أن يعطي تعليماته للخبير لجمع البيانات التي تكون مقبولة كدليل أمام هيئة المحكمة[1] .

وقد اعتبرت بعض التشريعات مثل فرنسا[2] الى أن الكيان المعنوي المتمثل في البرامج والتي تشغل حيزاً في ذاكرة الحاسب الآلي وتشكل نبضات الكترونية ، أنه كيان مادي ويتشابه مع التيار الكهربائي ويعد من قبيل الأشياء المادية التي يرد عليها الضبط والتفتيش .

ومن خلال استقراء موقف التشريعات الحديثة نجدها قد ذهبت صراحة الى أن التفتيش يمكن أن يقع على جميع انظمة وبرامج الحاسب الآلي . ومثال ذلك التشريع الانجليزي بشأن اساءة استخدام الحاسب الآلي

---

(١) نفس المرجع ص ٨٤ .

(٢) جرم قانون العقوبات الفرنسي الجديد الاستيلاء غير المشروع على التيار الكهربائي في فروضه المختلفة ، فنص في المادة ٣١١- ٢ منه على " اختلاس الطاقة عمداً اضرارا بالغير ياخذ حكم السرقة " . حيث ان المشرع الفرنسي قد اعتبر سرقة التيار الكهربائي من قبيل الاشياء عندما وسع في مفهوم السرقة بحيث يمكن ان تقع على الشيء أو منفعة الشيء ، وهي على هذا النحو لا يمكن أن تتمخض عنها جريمة سرقة الا بوقوع الفعل المادي للسرقة المتمثل في اختلاس التيار الكهربائي بتمريره خارج العداد الذي يحصي كمية التيار الكهربائي المستهلكة ، فلو لا هذا السلوك لما أمكن اكتشاف هذه الجريمة والعقاب عليها تحت وصف السرقة . انظر : حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٩ ، ، ص ٤٧٩ .

الصادر في سنة ١٩٩٠ الذي نص على أن اجراءات التفتيش تشمل أنظمة الحاسب الآلي[١] .

وكذلك أخذ القانون الفرنسي في المادة ١/٥٧ من قانون الإجراءات الجنائية الفرنسي ، المضافة بالقانون ٢٠٠٣- ٢٣٩ الصادر في ١٨ مارس لسنة ٢٠٠٣ اذ تجيز لمأموري الضبط القضائي التفتيش عن المعلومات في الأماكن التي يجري فيها التحقيق سواء أكانت معلومات مخزنة في النظام المعلوماتي للمتهم أم كانت مخزنة في نظام معلوماتي آخر طالما أن هذه المعلومات تم الوصول اليها من النظام الاساسي أو متاح الوصول اليها بواسطة هذا النظام الأساسي[٢] .

وكذلك الحال في التشريع الامريكي حيث بينت المادة ٣٤ من القواعد الفديرالية الخاصة بالإجراءات الجنائية الصادرة سنة ١٩٧٠ بعد تعديلها الى مد نطاق التفتيش ليشمل ضمن ما يشمل من أجهزة الحاسب الآلي وأوعية التخزين والبريد الالكتروني والصوتي والمنقول عن طريق الفاكس[٣] .

فضلاً عن أن (اتفاقية بودابست) تقضي في المادة (١٩ من القسم الرابع) بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في اطار الإجراءات الجنائية ، حيث نصت على أن " لكل دولة طرف حق أن تسن من القوانين ماهو ضروري لتمكين السلطات المختصة بالتفتيش او الدخول الى :

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.

---

(١) د. علي محمود علي حمودة ، أدلة اثبات الجرائم الالكترونية ، مرجع سابق ، ص ٣٧ .

(٢) بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، دار الفكر الجامعي ، الطبعة الاولى ، ٢٠١١ ، ص ٧٣ .

(٣) انظر في ذلك : هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص ٨٤ .

- الوسائط التي يتم تخزين معلومات الكمبيوتر بها مادامت مخزنة في اقليمها."

وتأسيساً على ما سبق يتبين لنا أنه يجوز ان يتم تفتيش أنظمة جهاز الحاسب الآلي والمعلومات الالكترونية المحتواه نفسها ، لما لها من أهمية اقتصادية كبيرة جدا اذا ما تم الاعتداء عليها بالاتلاف أو التخريب أو التشويه ، بل ان المعلومات الالكترونية تعتبر هي عصب الحياة الاقتصادية ، وبذلك فان القانون لم يكتفي بأن كفل لها الحماية القانونية اللازمة بل اضافة الى ذلك فقد نص على أن اجراء التفتيش على نظم المعلومات الالكترونية وأوعية حفظها وتخزينها والوسائط المتعددة التابعة لها هو اجراء يندرج ضمن اجراءات التفتيش القانوني[1] .

وتفادياً للقصور الذي يعتري بعض التشريعات الجنائية ، وحتى لايتم تفسير بعض ألفاظ النصوص القانونية تفسيراً ضمنيا قد ينطوي على احتمالين يسبب تضاربا وجدلا لدى فقهاء القانون فانه يجب مراعاة اضافة عبارة (المعلومات والأنظمة الالكترونية أو البيانات المخزنة في الحاسب الآلي والمعالجة بواسطته) ضمن تلك التشريعات ، وذلك حتى يمتد ضبط الأدلة المادية للحاسب الآلي ليشمل ايضا البيانات المعلوماتية بمختلف أشكالها .

المطلب الثاني
الحدود المكانية لتفتيش شبكات الحاسب الآلي

ان الطبيعة التي تتميز بها أجهزة الحاسب الآلي هي كونها متصلة مع بعضها عن طريق الشبكة المحلية في اقليم الدولة ، أو انها قد تتصل مع بعضها بحواسب تقع خارج اقليم الدولة وذلك عن طريق الشبكة المعلوماتية العالمية " الانترنت " . ومن شأن ذلك أن يفضي الى بعد الأدلة

---

(١) انظر : يونس عرب، حجية الاثبات بالمستخرجات الالكترونية في القضايا المصرفية بحث منشور على الرابط الالكتروني :
http://www.arab-elaw.com/show_similar.aspx?id=78

الالكترونية الموجودة عبر شبكات الحاسب الآلي عن الموقع المادي للتفتيش ، وان كان يمكن الوصول اليها عن طريق نفس الحاسب الآلي الذي صدر له اذن التفتيش ، فقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر او ربما في بلد آخر ، والسؤال الذي يطرح هنا : هل يمتد تفتيش حاسوب معين الى الأجهزة الاخرى المرتبطة به سواء أكان داخل اقليم الدولة أم خارجها ؟

وللاجابة على هذا السؤال لابد من بيان ثلاثة احتمالات :-

الاحتمال الأول :- اتصال حاسوب المتهم بحاسوب آخر موجود في مكان آخر داخل الدولة

ويثير هذا الاحتمال سؤالين ، الأول هل يقتصر التفتيش على الحاسب الآلي الخاص بالمتهم والموجود في منزله ؟ والثاني : هل يمتد التفتيش ليشمل الأجهزة الاخرى المتصلة بجهاز المتهم والمملوكة لشخص آخر خلاف المتهم ؟

بالرجوع الى القواعد العامة للتفتيش في قانون الإجراءات الجزائية الاماراتي ، نجد أنها تقضي بأنه لا يجوز تفتيش غير المتهمين أو تفتيش منازل غير المتهمين طبقا للمادة (٥٣) الا بعد الحصول على اذن خطي من النيابة العامة ، وبناءً على ذلك فانه لايجوز تفتيش الحاسب الآلي الموجود بمنزل غير المتهم الا بعد استصدار الاذن والا كان الاجراء باطلاً .

غير أن الإجراءات قد تستغرق وقتاً لصدور الاذن من النيابة العامة ، الأمر الذي قد يفضي الى تلاشي الدليل أو صعوبة الوصول اليه ، فضلاً عن أن الجاني نفسه قد يجدها فرصة مواتية حتى يقوم بالعبث بالدليل أو محاولة طمسه حتى لا يكتشف أمره ، وهذا بحد ذاته يشكل تهديداً حقيقياً للسلطات المختصة وعرقلة لسير اجراءاتها ، لأنه وكما اسلفنا بأن سرعة الانتقال الى مسرح الجريمة لمعاينته وضبط الآثار وأدلة الجريمة هي من

الأمور التي تساهم في الحفاظ على الأدلة وتحصيلها و سرعة اكتشاف الجريمة .

وعليه فاننا نرى ضرورة معالجة هذه المشكلة بنص خاص يشمل توسيع دائرة اختصاص السلطات المعنية بالتفتيش لاجراء تفتيشها ، ولو استلزم الأمر الدخول الى النظام المعلوماتي دون الحصول على اذن بذلك ولكن ضمن قيود وشروط محددة .

وقد تبنت بعض التشريعات الجنائية الحديثة ومنها القانون الألماني هذا الاتجاه حيث يرى امكانية تفتيش سجلات البيانات التي تكون في موقع آخر استنادا الى مقتضيات القسم ١٠٣ من قانون الإجراءات الالمانية، وكذلك الحال بالنسبة للقانون الاتحادي الاسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة فقط ، وانما تتوزع لتشمل بيانات الأدلة على شبكة الحواسيب ، فلا توجد حدود جغرافية محددة ، ولا يحتاج الأمر الى الحصول على موافقة الطرف الثالث للقيام بعملية التفتيش[1] .

كما وتسمح اتفاقية بودابست ٢٠٠١ للدول الاعضاء أن تمد نطاق التفتيش الذي يكون محله جهاز كمبيوتر معين الى غيره من الأجهزة المرتبطة به في حالة الاستعجال اذا كان يتواجد به معلومات يتم الدخول اليها من خلال جهاز الحاسب الآلي الاصلي محل التفتيش وذلك وفقاً للمادة ١٩ من القسم الرابع[2] .

---

(١) انظر : هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص ٨٣ .

(٢) ان بعض فقه الجنائي ينتقد مثل هذا النص بحجة أنه يعطي للجهات القائمة بالتفتيش سلطة واسعة المدى، وبما أن أجهزة الكمبيوتر تتصل ببعضها البعض على مستوى العالم، فان سلطتها تلك ستمتد الى تفتيش اجهزة كثيرة ومتعددة، من دون الحصول على اذن لتفتيشها، وهذا ما يتعارض مع ما تضمنه ميثاق الحقوق والحريات الكندي في الفصل الثامن منه والذي ينص=

واخيرا فان المشرع الهولندي قد أجاز من خلال قانون جريمة الحاسوب الهولندي في المادة (٢٥/أ) منه ، إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلي موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها ، ومن ثم أجاز المشرع للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من المحقق المختص ، وعلى الرغم مما تقدم فان هذه السلطة غير مطلقة بل هي مقيدة بقيود ثلاثة[1] :-

١- ألا تكون النهاية الطرفية المتصل بها الحاسوب موجودة ضمن إقليم دولة أخرى حتى لا يفضي الاتصال بها إلى انتهاك سيادة الدولة الإقليمية.

٢- أن تحتوي النهاية الطرفية المتصل بها الحاسوب على بيانات ضرورية بصورة كافية لظهور الحقيقة.

٣- أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.

الاحتمال الثاني :- اتصال حاسوب المتهم بحاسوب آخر موجود في مكان آخر خارج الدولة

قد يلجأ بعض الجناة بتخزين بياناتهم في أنظمة حاسب آلي يقع خارج اقليم الدولة التي يقيمون فيها عن طريق شبكة الاتصالات البعدية، مستغلين عدم امكانية الوصول اليها ، وعليه فان تفتيش هذه الأجهزة

=على حق الفرد في الحماية من التفتيش والضبط غير المعقولين . انظر في ذلك : شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، ٢٠٠٧، ص ٣٠٠.

(١) د.عفيفي كامل عفيفي، مرجع سابق، - ص ٣٤٧.

التي تقع خارج حدود الدولة تتعلق بجريمة ما قد يتعذر القيام به دون الحصول على موافقة تلك الدولة نظرا لتمسك كل دولة بسيادتها[1] .

وهذا الأمر قد يزيد من تعقيد مشاكل الجريمة الالكترونية ، اذ ان انعقاد اختصاص التفتيش الالكتروني العابر للحدود لابد ان يتم في اطار اتفاقيات ثنائية او دولية تجيزه ، ومن ثم فانه لايجوز القيام به في ظل غياب هذه الاتفاقية ، او على الاقل الحصول على اذن الدولة الاخرى التي يجري التفتيش في اقليمها ، ومن هنا تبرز أهمية الحاجة الملحة الى التعاون الدولي بين الدول لما فيه من مصلحة مشتركة تصب في التصدي لهذه الجرائم المستحدثة وردع مرتكبيها[2] .

وقد عرضت على القضاء الالماني واقعة تتعلق بالغش المعلوماتي ، وتبين وجود اتصال بين الحاسب الآلي المتواجد في المانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها ، الا أنها لم تتمكن من ذلك الا عن طريق التماس المساعدة بالتبادل بين الدولتين[3] .

وفي المقابل يؤيد جانب من الفقه أمر امتداد التفتيش الى أجهزة الحاسب الآلي الموجودة خارج اقليم الدولة ، حيث يقوم هذا الراي على اساس واقعي، اذ ان معتنقيه يحاولون التعامل بواقعية مع ما يعترض سلطات التحقيق من مشكلات . وهذا الاتجاه أخذ به المشرع الفرنسي حيث أجازت المادة ١٧ من الفقرة الثانية من قانون الامن الداخلي رقم ٢٣٩ لسنة ٢٠٠٣ لمأمور الضبط القضائي أن يقوم بتفتيش الأنظمة المتصلة

---

(١) هشام محمد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مرجع سابق، ص ٧١ .

(٢) انظر : محمد ابو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية الذي عقد بأكاديمية شرطة دبي من ٢٦- ٢٨ أبريل ٢٠٠٣م، الجزء الأول، محور القانون الجنائي، ص ٣٥ .

(٣) حسين بن سعيد الغافري، مرجع سابق، ص ٤٨٥ .

حتى ولو كانت خارج الاقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية. كما يسمح قانون التحقيق البلجيكي مادة ٨٨ لقاضي التحقيق الحصول على نسخة من البيانات التي هو في حاجة اليها دون انتظار اذن من سلطات الدول الاخرى[١] .

كما أجازت المادة "٣٢" من الاتفاقية الأوروبية التي أعدها المجلس الأوروبي في صيغتها النهائية في ٢٥ مايو من عام ٢٠٠١م إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها، وذلك في حالتين الأولى اذا تعلق الأمر بمعلومات او بيانات مباحة للجمهور، والثانية اذا رضي صاحب هذه البيانات أو حائزها بعملية التفتيش[٢] .

ونشير في هذا المقام الى أن القانون الاجرائي الاماراتي لم يتطرق الى مسألة تنظيم عمليات التفتيش عن بعد ، ومن أجل سد هذه الثغرات نرى ألا يكون الاذن بالتفتيش الالكتروني محددا في مكان معين ، بل يجب ان يمتد الى تفتيش اي نظام موجود في مكان آخر بغية التوصل الى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة ، شريطة عدم انتهاك سيادة الدول الاخرى ، حيث أنه في ضوء نصوص القانون الاماراتي الحالي نجد انه لايكمن العمل بها بشكل مطلق ، لأن هذا النوع من التفتيش ينطوي في الحقيقة على معنى تفتيش غير المتهم، ولذلك فإنه لا يجوز إعماله إلا في الأحوال التي يجوز فيها للقائم بالتفتيش تفتيش غير المتهم أو منزله .

وبناء على ماتقدم فان تفتيش نظم الحاسب الآلي يعتبر تفتيشاً للفضاء الافتراضي وأوعية التخزين ، وهو أمر يتعلق بالقدرة على تحديد

---

(١) د. موسى مسعود ارحومة، مرجع سابق، ص ١١ .

(٢) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص ٢٣٠، انظر أيضاً احمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، مرجع سابق، ص ٣٦.

المطلوب مسبقاً وليس مجرد سبر غور نظام الكتروني ، لأن التعامل وفق المسلك الأخير قد يكون له عواقب قانونية تتمثل في بطلان الإجراءات لانها خارج نطاق امر التفتيش ، او لربما قد تنطوي الإجراءات على كشف خصوصية البيانات المخزنة في النظام ، فالبيانات المخزنة في نظام الحاسب الآلي لا تتعلق جميعها بالجريمة المراد التفتيش على اثرها ، فمنها بيانات خاصة تتعلق بالمتهم ، لهذا اهتم الفقه بمخاطر الاعتداء على الخصوصية أو الحياة الخاصة في معرض الكشف عن الدليل[1] .

الاحتمال الثالث :- التنصت والمراقبة الالكترونية لشبكات الحاسب الآلي

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم سواء التامة أو غير التامة ، وسواء التقليدية أو المستحدثة كالجرائم الالكترونية ، فهي جزء لا يستغنى عنه في اعمال رجال البحث والتحري اذ تعتبر اسرع الطرق لكشف الجرائم.

ويقصد بالمراقبة الالكترونية هو العمل الذي يقوم به المراقب باستخدم التقنية الالكترونية لجمع معلومات وبيانات عن المشتبه به سواء كان شخصا او مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض امني او لاي غرض آخر[2] .

وان مسألة التنصت والمراقبة الالكترونية بالرغم من كونها مثيرة للجدل الا أن التشريعات المعاصرة تقرر أن " ضابط فائدة المراقبة يكمن في ظهور الحقيقة " ويعتبر السند الشرعي المبرر لهذه المراقبة ، وذلك بسبب أن

---

(١) انظر : د- يونس عرب، حجية الاثبات بالمستخرجات الالكترونية في القضايا المصرفية بحث منشور على الرابط الالكتروني :
http://www.arab-elaw.com/show_similar.aspx?id=78

(٢) مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، دار الكتب والوثائق القومية، الطبعة الاولى، ٢٠٠٣، ص ٣ .

هذا الاجراء يتضمن اعتداءا جسيما على حرمة الحياة الخاصة وسرية الاتصالات ، فيباح استثناءا وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق باظهار الحقيقة بكشف غموض الجريمة وضبط الجناة.

وقد اختلف الفقهاء في تحديد الطبيعة القانونية لمراقبة المحادثات الهاتفية والاتصالات الالكترونية ، فذهب بعض الفقهاء الى ان مراقبة المحادثات الهاتفية والاتصالات الالكترونية يعد نوعا من التفتيش وبالتالي تخضع لقيوده ، واستندوا في ذلك الى ان هذه المراقبة تتفق مع التفتيش في ان الهدف منها البحث في وعاء لسر توصلاً الى السر ذاته ، وازاحة ستار الكتمان عنه بغرض ضبط ما يفيد الوصول الى الحقيقة . ولا أهمية هنا لوجود الكيان المادي لوعاء السر ، فيصح ان يكون ماديا يمكن ضبطه بوضع اليد عليه استقلالا ، ويمكن ان يكون معنويا يتعذر ضبطه الا اذا اندمج في كيان مادي ، فالغاية من مراقبة المحادثات التليفونية هي البحث عن دليل معين وهي ذات الغاية من التفتيش[1].

في حين يرى البعض الآخران هذا التكييف لا يتماشى مع تعريف التفتيش بانه التنقيب عن الادلة المادية للجريمة ، فالمحادثات السلكية واللاسلكية ليس لها كيان مادى ملموس يمكن ضبطه ، ذلك ان التنصت عليها لا يضبط دليلا ماديا ، وانماهو دليل قولي ليس الا ، ولا يعد شريط التسجيل الذي افرغ فيه المحادثة هو الدليل بذاته ، بل هو الوسيلة التي ادت الى المحافظة على الدليل القولي. والقول بغير ذلك يفضي الى اعتبار الاعتراف الشفوي وشهادة الشهود دليلا غير قولي مادام قد تم تثبيتهافي محضر مكتوب ، فضلا عن أن القواعد الاجرائية لعمليتي التنصت والمراقبة تختلف عن القواعد الاجرائية لعملية التفتيش ذاتها[2] .

---

(١) احمد فتحي سرور، مراقبة المكالمات التليفونية، مشار اليه عند : د. علي محمود حمودة، ادلة اثبات الجرائم الالكترونية، مرجع سابق، ص ٧٢ .

(٢) تتلخص محاور الاختلاف بين كل من القواعد الاجرائية للمراقبة والتسجيل عن قواعد التفتيش كون المشرع المصري قد قام بوضع ضمانات تحول دون استخدام هذا التعسف حيث حدد المشرع مدة الاذن بالتسجيل والتنصت=

وطبقا للمادة (٧٥) من قانون الإجراءات الجزائية الاتحادي فانه يجوز للنيابة العامة مراقبة وتسجيل المحادثات السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك بعد الحصول على اذن من النائب العام[1]، ونجد أن هذا النص لم يشمل صراحة مراقبة وضبط الأجهزة الالكترونية بجميع اشكالها وصورها بما في ذلك الرسائل الالكترونية بمختلف انواعها على شبكة الانترنت.

ويمكن برأينا أن تشمل هذه المراقبة الوسائل الالكترونية والمحادثات الالكترونية لأن شبكات الحاسب الآلي تستخدم في اجراء الاتصالات الهاتفية والمراسلات الالكترونية وتصفح المواقع على شبكة الانترنت خطوط الهاتف من خلال جهاز يرتبط بها يسمى المودم ، وهو جهاز معدل للموجات[2] ، ولذلك فان المراقبة الالكترونية لهذه الاتصالات

=بثلاثين يوما تجدد لمدة اخرى مماثلة، خلافا لاذن التفتيش الذي لم يشترط مدة معينة لسريانه . الامر الثاني وهو الحصول على أمر مسبب من القاضي بعد اطلاعه على الاوراق من اجل اقرار عملية المراقبة، بخلاف التفتيش الذي يتولاه القائم بالتحقيق سواء كان قاضي التحقيق او احد اعضاء النيابة العامة . الامر الثالث هو ان عملية التفتيش تتم في حضور المتهم على خلاف مراقبة المحادثات التلفونية التي ينبغي اجراؤها بشكل سري دون علم المشتبه فيه . انظر في ذلك : محمد امين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١، ص٥٥ وما بعدها .

(١) حيث تطرقت المادة ١٥ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ بعقوبة التقاط أو اعتراض أي اتصال عن طريق شبكة معلوماتية عمدا وبدون تصريح بالحبس والغرامة التي لا تقل عن ١٥٠ الف درهم ولا تتجاوز ٥٠٠ الف درهم او باحدى هاتين العقوبتين، وهذا برأينا يمكن ان يشمل الاتصال السلكي او اللاسلكي للاتصالات والمكالمات على شبكة الانترنت.

(٢) هلالي عبد اللاه احمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص ٢٢١ .

يمكـن ان تـتم بمراقبـة خطـوط الهـاتف الـتي تـتم بواسـطته عمليـة الاتصال[1] .

ولذا يمكن ان تمتد سلطة النائب العام بمراقبة المحادثات الهاتفية الى هذه الاتصالات الالكترونية من محادثات وغيرها ، مما يتم استعراضه على جهاز الحاسب الآلي طالما أن هذا الاتصال يتم بواسطة خطوط الهاتف.

وباستعراض موقف التشريعات المختلفة في هذا المجال نجد أن القانون الفرنسي الصادر في ١٩٩١/٧/١٠ يجيز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات[2].كما واستقر قضاء محكمة النقض الفرنسية على مشروعية مراقبة المحادثات التلفونية ، الا أنها استلزمت العديد من الضمانات لتحقيق تلك المشروعية ، وبعد تحقق الشروط الثلاثة الآتية : الحصول على اذن بالمراقبة من قاضي التحقيق ، وثانيا : حتمية اشراف القاضي على عملية المراقبة ، وثالثا : عدم استخدام اساليب الغش والخداع في التنصت ومراعاة حقوق الدفاع[3] . وقد حدد المشرع الفرنسي

---

(١) في ديسمبر سنة ١٩٩٤ اكتشف أحد الباحثين في مركز الحاسبات الآلية الموجودة في San-Diego بجنوب كاليفورنيا أن تم اختراق الحاسب الآلي الشخصي الخاص به من جهاز يقع بمدينة شيكاغو، ولكن يتم التحكم فيه عن بعد . وبعد مضي شهر عثر على المعلومات المسروقة على موقع Well على الانترنت، فقام المجني عليه بمراقبة الشبكة الا أنه يبدو أن الجاني كان يعمل من عدة مدن . وبمراجعة المكالمات التلفونية المسجلة بمعرفة شركة التلفونات عن طريق الكمبيوتر وجد ان الجاني يقوم بالبث باستخدام Mpdem متصل بتلفون محمول. وباختراقه المدينة بمستقبل هوائي خاص متصل بجهاز كمبيوتر محمول امكن لفريق البحث أن يحدد المكان الذي تصدر منه النداءات والذبذبات وتم القبض على الجاني . انظر: جميل عبدالباقي الصغير، ادلة الاثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص ١٠٠ .

(٢) حسين بن سعيد الغافري، مرجع سابق، ص ٤٨٦ .

(٣) انظر : محمد أبو العلا عقيدة، مراقبة المحادثات التلفونية، مشار اليه عند : محمد امين الخرشة، مرجع سابق، ص ٨٢ .

مدة المراقبة بأربعة اشهر قابلة للتجديد وذلك حرصا منه من تعسف استخدام هذا الحق واساءة استعمال السلطة.

وفي هولندا أجاز المشرع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات اذا كانت هناك جرائم خطيرة مشترك فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات .

وفي الولايات المتحدة الامريكية[1] يمكن مصادرة محتوى الرسائل الرقمية بواسطة قانون التنصت ١٨ U.S.C. ٢٥١٠ ولكنه يشمل متطلبات صارمة للحصول على موافقة قضائية ، حيث يتطلب موافقة مسبقة من قاضي فدرالي وهو أكثر صرامة في المتطلبات اذا قورن بالمتطلبات اللازمة للحصول على اذن تفتيش الممتلكات ، حيث تصبح عمليات التنصت جزءا لا يتجزأ من التحقيق بعد استنفاذ اساليب التحقيق الأخرى . وقبل اصدار الأمر بالتنصت يجب على القاضي الفيدرالي أن يبحث في ما يلي : -

أ- سبب محتمل يجعله يعتقد بأن هذا الشخص يرتكب أو ارتكب جريمة من الجرائم في قائمة الجرائم المحددة.

ب- سبب محتمل أن تكون الاتصالات الخاصة بالجريمة سيتم الحصول عليها من خلال عمليات اعتراض الرسائل .

ج- أن اساليب التحقيق الطبيعية قد تم تجربتها وباءت بالفشل أو انها من غير الممكن أن تنجح أو انها بالغة الخطورة .

د- سبب محتمل أن الوسائل التي يتم اعتراض الاتصالات منها تستخدم فيما يتعلق بتنفيذ الجريمة.

---

(١) لين وينميل، الجريمة الالكترونية : القضايا والتحديات في الولايات المتحدة، من أوراق العمل المقدمة الى ورشة عمل الجريمة الالكترونية، وزارة العدل، أبوظبي، في الفترة من ٢ الى ٣ يونيو ٢٠١٠ .

أما في المانيا فقد تم تعديل القوانين الخاصة بها واصبح للقاضي الحق في اصدار أوامره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها الا أن القانون قد حددها مدة اقصاها ثلاثة أيام فقط، وكذلك اقرت محكمة مقاطعة KOFU في اليابان سنة ١٩٩١ شرعية التنصت على شبكات الحاسب الآلي لغرض البحث عن دليل يفيد الجريمة [١].

ومما يجدر الاشارة اليه بهذا الصدد أن هذا المنع لا يشمل الرقابة التي تمارسها المؤسسات الكبرى على عمل موظفيها، لأن تلك الرقابة تعتبر رقابة إدارية لمصلحة أرباب العمل للتأكد من أن الموظف لم يبدد وقت العمل لمصلحة شخصية، أو أنهم يعملون لحساب الغير، ويوجد في أمريكا جهاز يسمى penregisster and atrap and trace device وهو جهاز تسجيل التقصي trap@trace device يصور الموجات الإلكترونية، ويمكنه أن يقوم بتعريف وتحديد رقم الاتصال المطلوب، أو تحديد عنوان البريد الالكتروني، أو الموقع الالكتروني، ورقم التعريف الدولي IP [٢] للمتهم المتصل بشبكة الإنترنت، فيساعد الجهات الأمنية

---

(١) منير محمد الجنبيهي و ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ٢٠٠٥، ص ١٩٠.

(٢) يعرف ال (IP) وهو اختصار لكلمة Internet protacop انه وسيلة لنقل البيانات من مكان على الانترنت الى مكان آخر، اما IP address فهو عنوان مكون من أربعة أرقام ويستخدم لتحديد هوية كل جهاز يتصل بالانترنت، ذلك أنه عندما يتجول مستخدم الانترنت في حوار على شبكة الانترنت، فانه يترك اثاره في كل مكان يقوم بزيارته او الدخول عليه على الشبكة، ذلك ان الموقع الذي يمر به يفتح سجلا خاصا به يتضمن عوان الموقع الذي جاء منه، ونوع الكمبيوتر والمتصفح الذي يستخدمه، وعنوان رقم الدائم والمتغير للكمبيوتر الذي يتصل منه. وتتمثل عملية الاستفادة عما يكشف عنه الرقم IP في البحث والتحقيق الجنائي، ذلك أنه عندما يزور شخصا موقعا على الشبكة، يقوم الكمبيوتر بتسجيل ال IP العائد للكمبيوتر الذي اتصل منه، وعند ارسال بريد الكتروني كذلك، يمكن لمستلم الرسالة معرفة عنوان ال IP للكمبيوتر المرسل منه، وكذلك عند استخدام برنامج=

والقضائية في الوصول إلى الدليل الجنائي عند الحاجة وعند حدوث جريمة، ولدقة هذا الجهاز في التحري والمراقبة الالكترونية نقترح اعتماده كما هو مطبق في تسجيل المكالمات الهاتفية بعد صدور إذن بذلك من النيابة العامة.

كما ويمكن الاستعانة بشركات الاتصالات المزودة للخدمة في الحصول على معلومات العميل الذي يكون موضع شبهه، من خلال البحث على دليل يساعد في ثبوت التهمة أو نفيها من خلال معرفة المواقع الالكترونية التي قام بزيارتها، وما هي الرسائل التي أرسلها عبر مزود الخدمة، بعد مراعاة الخصوصية والضمانات الدستورية للمتهم المعلوماتي.

وتأسيساً على ما سبق نشير الى أن الطبيعة الخاصة التي يتمتع بها الدليل الالكتروني من حيث سرعة فقده وزواله ، قد تفرض علينا أن نقوم بالتخفيف من حدة شروط استئذان النيابة العامة أو القاضي المختص بالرغم من كونها تمس خصوصية الأفراد ، حتى تتمكن من مباشرة اعتراض الاتصالات الالكترونية في الحالة التي تتولى التحقيق بنفسها في جريمة الكترونية قائمة وتبين لها ضرورة القيام بالمراقبة وتسجيل هذه الاتصالات عبر شبكة الانترنت ، وذلك كسباً للوقت وضبط الدليل والتحفظ عليه .

المطلب الثالث
ضوابط التفتيش في الجرائم الالكترونية
الفرع الأول
الضوابط الموضوعية لتفتيش نظم الحاسب الآلي

يقصد بالشروط الموضوعية بصفة عامة الضوابط التي لابد من الأخذ بمقتضاها حتى يكون التفتيش صحيحا من الناحية القانونية كونه اجراء من

=الاوت لوك يمكن النقر على زر Option بعد ان يفتح الرسالة فيتم الاطلاع على عنوان المرسل. انظر في ذلك، د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت –دار الكتب القانونية، مصر، ٢٠٠٢، ٦٣، ٦٤.

اجراءات التحقيق ، ويترتب على عدم صحته او مشروعيته البطلان اذا ما دفع به المتهم ، وتكمن في سبب التفتيش ومحله والسلطة المختصة به .

أولا: سبب التفتيش:

ان الهدف الرئيسي من اجراء التفتيش هو البحث عن الدليل الجنائي في الجرائم المرتكبة بهدف الوصول الى الحقيقة ، واقتناع عدالة المحكمة به . ويشترط لمباشرة التفتيش باعتباره اجراءا من اجراءات التحقيق ان تكون هناك جريمة وقعت بالفعل سواء كانت جناية ام جنحة ، وان يكون هناك اتهام موجه للشخص المراد تفتيشه او تفتيش مسكنه ، أو توافر امارات قوية وقرائن ودلائل تفيد في الكشف عن الحقيقه سواء في مسكنه او شخص غيره أو مسكن غيره .

وهذا ما أخذت به محكمة النقض المصرية في حكم لها بقولها " الأصل في القانون أن الاذن بالتفتيش هو اجراء من اجراءات التحقيق لا يصح اصداره الا لضبط جريمة – جناية أو جنحة – واقعة بالفعل ترجحت نسبتها الى متهم معين ، وان هنالك من الدلائل ما يكفي للتصدي لحرمة مسكنه او لحرمته الشخصية"[1] ، وسنتطرق بايجاز لكل نقطة منها كما يأتي :-

أ- وقوع جريمة الكترونية تشكل جناية او جنحة

يعني انه يشترط لصحة اجراء التفتيش في النظم المعلوماتية أن نكون بصدد جريمة معلوماتية نص عليها القانون ويعتبرها القانون جناية أو جنحة ، ومن ثم فانه يستبعد من نطاق التفتيش أن تكون الجريمة المرتكبة من المخالفات نظراً لضآلتها بحيث لا يتوفر لها من الخطورة ما يبرر اهدار حرمة الشخص أو حرمة مسكنه عن طريق التفتيش.

وتطبيقاً لمبدأ شرعية الجرائم والعقوبات ، فانه لا محل لاصدار اذن تفتيش نظام حاسب آلي معين الا اذا نص المشرع صراحة على أن هذا

---

(١) نقض ١٦ اكتوبر ١٩٦٧ ، مجموعة احكام النقض س ١٨ رقم ١٩٥ ص ٩٦٥.

الفعل المرتكب من قبيل الأفعال غير المشروعة والتي تعتبر بنظر القانون من الجرائم وحدد لها عقوبة معينة ، كما اورد المشرع الاماراتي تلك الافعال ضمن قانون مكافحة جرائم تقنية المعلومات، كالاتلاف ، التعديل، التغيير، الافشاء، التعطيل، والايقاف، وعلى ذلك لايكفي القول بمجرد وقوع الجريمة للقول بجواز التفتيش .

ولذا فقد نصت العديد من التشريعات كما بينا على استحداث نص خاص للجريمة المعلوماتية . كما هو الحال بالنسبة لقانون اساءة استخدام الحاسب الالي الذي صدر في انجلترا سنة ١٩٩٠ ، وقانون الاحتيال واساءة استخدام الحاسب الآلي الأمريكي الصادر سنة ١٩٨٦ والذي طبق على المستوى الفيدرالي ، وفي فرنسا صدر قانون خاص بالغش المعلوماتي عام ١٩٨٨[1] .

ومع ذلك إن خلا تشريع دولة ما من النص على تجريم أنماط السلوك التي تمس بنظام المعلومات ، فإن ذلك لا يمنع من قيام وصف الجريمة للفعل المراد جمع الدليل بشأنه في حالات كثيرة كاستعمال الحاسوب في التزوير أو استعمال شبكة المعلومات العالمية في إرسال رسائل سب وتشهير ونحوه، إذ أن وصف الجريمة يثبت لهذه الأفعال وفقاً للتكييف التقليدي المقرر بموجب قانون العقوبات ، فالحاسوب في هذه الحالة وسيلة لارتكاب الجريمة ولا يغير من وصفها كجريمة تقليدية.

ب- اتهام شخص او اشخاص معينين بارتكاب الجريمة الالكترونية او المشاركة فيها:

ويعني ذلك وجوب أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية ، تعزز القناعة بانه قد ساهم في ارتكاب الجريمة الالكترونية سواء باعتباره فاعلا اصليا أو شريكاً فيها مما يستوجب اتهامه فيها، وعليه فاذا لم تتوافر هذه الدلائل الكافية فلا يجوز توجيه الاتهام له وبالتالي لايجوز تفتيشه .

---

(١) انظر : د.عبدالله حسين علي محمود، مرجع سابق، ص ٣٧٨ .

وعليه فانه بمجرد توافر الأدلة والقرائن يعد مسوغاً كافيا للحق في تفتيشه دون انتظار تحقق أي اعتبار آخر ، وعلى ذلك نصت المادة ٧٢ من قانون الإجراءات الجزائية الاتحادي على أن " لعضو النيابة العامة تفتيش منزل المتهم بناء على تهمة موجهة اليه بارتكاب جريمة او باشتراكه في ارتكابها ، وله ان يفتش أي مكان ويضبط فيه أية اوراق او اسلحة وكل ما يفيد في كشف الحقيقة " .

ت- توافر امارات قوية او قرائن او اجهزة او معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره:

لم تتعرض قوانين الإجراءات الجنائية لتعريف الدلائل وانما اكتفت بالنص الذي على وجوب توافر دلائل قوية متوافقة مع الاتهام الموجه للمتهم، الا ان الفقه تصدى لتحديد مفهومها حيث عرفها بعض الفقهاء بأنها " مجموعة الوقائع الظاهرة والملموسة التي يستنتج منها ان شخصاً معيناً هو مرتكب الجريمة"[1] ، وعرفها آخرون بأنها " امارات معينة تستند الى العقل وتبدأ من ظروف أو وقائع يستنتج منها الفعل توحي للوهلة الأولى بأن جريمة ما وقعت وأن شخصاً معينا هو مرتكبها " وهذه الامارات لا يكفي في تقديرها مجرد المنطق بل لابد في شأنها من تدخل الخبرة والتعقل"[2].

وقد اشترط المشرع الاماراتي وجود هذه الامارات والقرائن كشرط لاجراء التفتيش اذ نصت المادة ٧٥ اجراءات جزائية على أن " لعضو النيابة العامة ان يفتش المتهم ولا يجوز له تفتيش غير المتهم او منزل غير منزله الا اذا اتضح من أمارات قوية انه حائز لاشياء تتعلق بالجريمة ... " .

وبناءً على ما سبق فان المشرع الاماراتي لم يشترط وجود امارات او قرائن تدل على وجود ما يتعلق بالجريمة في المنزل المراد تفتيشه ، مما يفيد في

---

(١) محمد زكي ابو عامر، الاجراءات الجنائية، دار المطبوعات الجامعية، ١٩٨٤، ص ٧٧.

(٢) بكري يوسف بكري، مرجع سابق، ص ٩٤ .

كشف الحقيقة ، ولكن المشرع قد اشترط وجود هذه الامارات والقرائن بالنسبة لتفتيش شخص غير المتهم او مسكن غير المتهم .

أما قانون الإجراءات الجنائية الأمريكية فقد عبر عن الدلائل الكافية باصطلاح السبب المعقول أو المحتمل ، ونص على ذلك ايضاً التعديل الرابع للدستور الامريكي فذكر بأنه لايجب اصدار اوامر القبض أو التفتيش مالم تكن بناء على سبب معقول[1] .

وفي المبادىء الخاصة بضبط وتفتيش الدليل الالكتروني قرر القضاء الأمريكي بقوله " أن اذن التفتيش والضبط الذي يشير الى كافة البرمجيات والقطع الصلبة للحاسوب دون تحديد لا يعد أمراً غير دستوري أو امرا محظورا ، اذا كان هناك سبب ملائم يدعو الى الاعتقاد بان الحاسوب على سبيل المثال قد تم استخدامه لتخزين وارسال صور دعارة للاطفال- بمعنى انه يمكن الحصول من خلاله على دليل الكتروني يساهم في كشف الجريمة - فقبل عملية الضبط كان المتهم قد الغى اكثر من ١٤٠٠ صورة اباحية وقام رجال الضبط باسترداد بعضا منها باستخدام برنامج خاص. ومثل هذا لا يعد تجاوزا لصلاحية اذن التفتيش حيث كان مضمونه يرتبط بما يتم البحث عنه وليس كيف تتم عملية البحث والتفتيش[2].

وعموماً فان تقدير هذه الدلائل متروك للسلطة التي تصدر الاذن بالتفتيش شريطة ان يكون تقديرها منطقيا ومتفقاً مع الواقع ، بحيث تكشف هذه الدلائل بجدية عن وقوع الجريمة محل الاذن بالتفتيش وأن يكون هناك جاني تنسب اليه التهمة ، فالتقدير المجرد بذاته للدلائل التي تبرر المساس بحريات الاشخاص لا يمكن أن تكون محل مصداقية ، وانما

---

(١) هلالي عبداللاه احمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص١١٧.

(٢) عمر محمد بن يونس، مستشار موسوعة التشريعات العربية (سجل جينيس للأرقام القياسية ١٩٩٩)، الطبعة الأولى ٢٠٠٧- ٢٠٠٨، بدون دار نشر، ص ١٤٤ .

يجب ان تقترن هذه الدلائل مع ما درجت عليه قواعد الخبرة بما لا ينافي العقل والمنطق.

ويقصد بالدلائل الكافية للتفتيش في مجال الجريمة الالكترونية هي مجموعة المظاهر والامارات المعينة وفقاً للسياق العقلي والمنطقي والخبرة الفنية والحرفية للقائم بالتفتيش ، والتي ترجح نسبة الجريمة الالكترونية الى شخص ما بوصفه فاعلاً أو شريكاً[1] .

ومن أمثلتها : ارتباط عنوان انترنت بروتوكول الخاص بجهاز الحاسب الآلي الذي يحتوي على صور فاضحة مع رقم حساب المتهم لدى مزود الخدمات ، ووجود رقمين للهاتف لديه يستخدمهما في ذلك[2].

ث- ان يكون التفتيش بقصد ضبط اشياء تتعلق بالجريمة او تفيد في كشف الحقيقة.

أن يكون الاذن الصادر بالتفتيش موضوعه جريمة الكترونية اي يهدف للبحث عن أدلة في مسرح الجريمة ذات طبيعة الكترونية تتصل بالحاسب الآلي أو احد انظمته وبرمجياته ، ولذلك يبطل كل تفتيش يجري لغاية اخرى خلاف ما نص عليه المشرع.

وقد نصت المادة ١٢٨ من تعلميات النيابة العامة على أنه " يكون تفتيش مسكن المتهم للبحث عن الاشياء الخاصة بالجريمة التي يجري جمع الأدلة أو التحقيق بشأنها ، ومع ذلك اذا ظهرت عرضاً اثناء التفتيش اشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى وجب ضبطها شريطة الا يكون ذلك نتيجة سعي يستهدف البحث عنها ، أو تعسفا في تنفيذ التفتيش".

---

(١) د. هلالي عبداللاه احمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص١٢١ .

(٢) د. شيماء عبد الغني، مرجع سابق، ص ٢٨٢ .

وفي هذا السياق ذكر الملحق الخاص بمبادىء التفتيش وضبط الدليل الالكتروني في القضاء الأمريكي أنه اثناء التفتيش عن دليل رقمي له علاقة بجرائم المخدرات اكتشف مأمور الضبط القضائي صور اباحية للاطفال (جريمة عرضية) ، فاستمر في التفتيش عن أدلة اخرى تخص هذه الجريمة العرضية ، فان هذا الاستمرار في التفتيش عن الجريمة العرضية يعد باطلاً وبالتالي يعد الدليل المستمد منه باطلا ولو تم برضا المتهم .

وعليه يمكن القول ان اذن التفتيش الصادر بتفتيش عقار يوجد به حاسب آلي يستلزم فيه توضيح الصفة القانونية للحاسب الآلي بشكل مستقل ، وبما يوحي بضرورة وجود ما يدل على امكانية التحفظ على الحاسب الآلي بشكل مستقل للكشف عن الأدلة المرتبطة به من قبل المختصين بذلك ، فاذن التفتيش ينبغي ان يحتوي على كشف بما يجب ان تكون عليه المواد المراد ضبطها ، فمسألة التفتيش في ذاتها ليست عشوائية وانما قيدها المشرع ضمن اطار وحدود معينة حتى لا يحول عن الهدف الخاص الذي يرنو للوصول اليه .

ثانيا: محل التفتيش

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالاشياء المادية التي تضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة . ولاشك في ان تحديد محل التفتيش تحديداً دقيقا بالنسبة للجرائم الالكترونية قد تكتنفه بعض الصعوبة ، ذلك أن تحديد كل او بعض مكونات الوسائل الالكترونية وايرادها في اذن التفتيش وتحديدها تحديداً دقيقاً قد يستلزم ثقافة فنية عالية في تقنية الحاسب الآلي ، وقد لا تتوافر للمحقق أو مأمور الضبط القضائي[1] .

---

(١) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص ١٥١ .

ومحل التفتيش في موضوع بحثنا يمكن أن يشمل الحاسب الآلي والأنظمة التقنية والشبكة المرتبطة به والملحقات الفنية وكل مكوناته المادية والمعنوية وكل ما قد يتصل به اتصالاً مباشرا او غير مباشر، وقد يكون موضوع الجريمة محل التفتيش شخصا معينا أو مكان معين يتمتع بالخصوصية.

فالشخص باعتباره محلا قائما لاجراء التفتيش[1] عليه، قد يكون من مستغلي أو مستخدمي الحاسب الآلي أو من خبراء البرامج سواء أكانت برامج النظام أم برامج تطبيقية ، وقد يكون من المحللين أو من مهندسي الصيانة والاتصالات ، أو من مديري النظم المعلوماتية ، او أي اشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو اجهزة حاسب آلي محمولة أو هواتف متصلو بجهاز المودم أو مستندات او اكواد او غير ذلك مما يتعلق بالجريمة محل البحث[2].

---

(١) اذا كان محل التفتيش انثى فيشترط تفتيشها بمعرفة انثى مثلها، وذلك بهدف الحفاظ على حياء المرأة وصيانة لعرضها وشرفها وهذا المبدأ يتعلق بالنظام العام، ويرتب البطلان في حال عدم التقيد به . وهذا ما نصت عليه المادة (٥٢) من قانون الاجراءات الجزائية الاتحادي بقولها " اذا كان المتهم انثى، يجب ان يكون التفتيش بمعرفة انثى يندبها لذلك مأمور الضبط القضائي بعد تحليفها يمينا بأن تؤدي اعمالها بالأمانة والصدق ويتعين كذلك أن يكون شهود التفتيش من النساء " وذات المبدأ جرى العمل عليه في فرنسا لتعلقه بالاداب العامة، بالرغم من عدم وجود نص في قانون الاجراءات الجنائية الفرنسي يوجب ان يتم تفتيش الانثى بمعرفة أنثى، الا أن هذا المبدأ يجد اساسه في بعض النصوص القانونية الأخرى غير قانون الاجراءات الجنائية مثل المرسوم الصادر في نوفمبر سنة ١٨٨٥ والخاص بنظام العمل في السجون حيث تقضي المادة ٣٤ من هذا المرسوم بضرورة تفتيش الانثى بمعرفة الانثى، وهو ذات المبدأ الذي تضمنته الفقرة الثانية من المادة ٢٧٥ من المرسوم الصادر في ٢٣ فبراير ١٩٥٩ والذي حل محل المرسوم الأول . انظر: د . بكري يوسف بكري، مرجع سابق، ص ٩٩ ومابعدها .

(٢) ويستبعد من نطاق تفتيش الأشخاص من يتمتعون بحصانات معينة، انظر في ذلك : د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص ١٢٦ .

ومما يجدر التنويه اليه في هذا الصدد أنه لا يشترط في هذه الاشياء ان تكون مملوكة للمتهم وانما يكفي ان يكون حائزا لها ، كما لا يشترط أن تكون في يد المتهم وقت التفتيش وانما يصح تفتيشها حتى لو كان يضعها امامه في طريق عام طالما أن ظاهر الحال لا يوحي بأنه تخلى عنها.

أما بالنسبة للمنازل ومافي حكمها ، كمحل يرد عليه تفتيش الحاسب الالي فقد نصت المادة ١٢٤ من تعليمات النيابة العامة على انه " ينصرف تفتيش المسكن الى كل مكان خاص يقيم فيه المتهم بصفة دائمة او مؤقتة كما ينصرف الى ملحقات هذا المكان كالحديقة او المخزن او المرآب أو حظائر الحيوانات والطيور ، كما يمتد الى مافي حكمه من الأماكن الخاصة التي يقيم فيها الشخص ولو لفترة محدودة من اليوم كعيادة الطبيب ومكتب المحامي والمتجر.

أما إذا انتفت صفة الخصوصية والسر المهني عن المحل بأن كان من المحلات العامة كالمقاهي، ودور السينما، وقاعة الانتظار بالعيادة الطبية وجميع المحلات التي يمكن ارتيادها من قبل أي شخص، فإنه لا يخضع لقيود التفتيش الخاصة بالمساكن .

ثالثا: السلطة المختصة بالتفتيش

لقد خول القانون الحق في التفتيش لجهات معينة نص عليها قانوناً كون التفتيش اجراء من اجراءات التحقيق وفيه مساس بالحرية الشخصية للأفراد وانتهاكا للحرمة الخاصة لهم وتلك الجهات هي النيابة العامة وقاضي التحقيق باعتبارهما السلطات الأصلية للتحقيق.

كما أن القانون خول للنيابة العامة أن تنتدب مأموري الضبط القضائي أو من الموظفين الذين يتم منحهم صفة مأموري الضبط

القضائيوأجاز لهم التفتيش ولكن ضمن شروط وضوابط معينة لا يجوز الخروج عنها ، ونفرق هنا بين حالتي التلبس[1] وحالة غير التلبس.

١- في حالة التلبس :

ان الجرائم الالكترونية كغيرها من الجرائم التقليدية يمكن أن تتوافر فيها شروط الجريمة المتلبس بها وفي هذه الحالة نفرق بين تفتيش الأشخاص وتفتيش المنازل :

بالنسبة لتفتيش الأشخاص فان اغلب التشريعات الجنائية تجيز تفتيش الأشخاص في حالة التلبس دون الحصول على اذن بذلك من النيابة العامة ، تطبيقا للقاعدة السائدة اذا جاز القبض على الشخص جاز تفتيشه ، وذلك حتى يتم تدارك عرقلة الإجراءات المتخذة في موقع الحادثة من قبض على المتهم وجمع أدلة وسؤال الشهود ، ولانه كما اسلفنا القول بأنه كلما كان عنصر السرعة والانتقال الفوري من أهم العناصر التي تؤدي الى عدم ضياع الأدلة وسرعة اكتشاف الجاني ، وهذا ما يتحقق في حالة التلبس بالجريمة[2] والتي يضبطها مأمور الضبط القضائي .

---

(١) عرفت المحكمة الاتحادية العليا التلبس بأنه " صفة تلازم الجريمة لا شخص المجرم، وأن وجود مظاهر خارجية تنبىء بذاتها عن وقوع الجريمة كاف لقيام حالة التلبس ، وتقدير حالة التلبس أو عدم توافرها أمر موضوعي يترك لرجل الضبط القضائي ، ويخضع في ذلك لرقابة سلطة التحقيق تحت اشراف محكمة الموضوع ." الطعن رقم ٢٠٢ ، جلسة ١٩٩٢/٥/١٣ لسنة ١٣ قضائية ، المحكمة الاتحادية العليا بأبوظبي.

(٢) تنص المادة ٤٢ من قانون الاجراءات الجزائية الاتحادي على أنه : تكون الجريمة متلبس بها حال ارتكابها أو بعد ارتكابها ببرهة يسيرة . وتعتبر الجريمة متلبسا بها اذا تبع المجني عليه مرتكبها ، او تبعته العامة مع الصياح اثر وقوعها او اذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا الات أو اسلحة او متاع او اشياء يستدل منها على أنه فاعل او شريك فيها او اذا وجدت به في هذا الوقت آثار او علامات تفيد ذلك.

ففي قانون الإجراءات الجزائية الاماراتي نصت المادة ٥١ منه على انه يجوز لمأمور الضبط القضائي أن يفتش المتهم في الأحوال التي يجوز فيها قانونا القبض عليه ، وتقابله في ذلك المادة ١/٤٦ من قانون الإجراءات الجنائية المصري.

واباحة تفتيش المتهم المقبوض عليه مقصورة على شخصه بالبحث عما يكون في جسمه او ملابسه او الامتعة التي يحملها من اثار أو ادلة تتعلق بالجريمة الواقعة ، وعليه فلا يملك مأمور الضبط القضائي تفتيش منزله لمجرد أن القبض عليه وقع صحيحا .

وتحدد المادة ٤٥ من قانون الإجراءات الجزائية الاتحادي الحالات التي يجوز فيها القبض استناداً لحالة التلبس اذ نصت على أنه " لمأمور الضبط القضائي أن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على ارتكابه جريمة في احوال التلبس بالجنايات أو الجنح المتلبس بها والمعاقب عليها بغير الغرامة أو الجنح المعاقب عليها بغير الغرامة اذا كان المتهم موضوعاً تحت المراقبة أو يخشى هروبه أو في جنح السرقة والاحتيال وخيانة الامانة والتعدي الشديد ومقاومة أفراد السلطة العامة بالقوة وانتهاك حرمة الآداب العامة والجنح المتعلقة بالاسلحة والذخائر والمسكرات والعقاقير الخطرة "[1] . بل ان المشرع توسع في مسألة القبض في حالة التلبس فأعطى لكل شخص من غير مأموري الضبط القضائي في حال مشاهدته للجاني يرتكب جنحة او جناية أن يقوم بالقبض عليه وتسليمه لافراد السلطة العامة أو مركز الشرطة ، حيث نص على ذلك في المادة ٤٨ من ذات

---

(١) ويقابلها في ذلك المادة ٣٤ من قانون الاجراءات الجنائية المصري التي تنص بقولها " لمأمور الضبط القضائي في احوال التلبس بالجنايات أو الجنح التي يعاقب عليها بالحبس لمدة لاتزيد على ثلاثة أشهر أن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه".

القانون " لكل من شاهد الجاني متلبساً بجناية أو جنحة ، أن يسلمه الى أقرب أفراد السلطة العامة دون احتياج الى أمر بضبطه" .

ثم اضافت المادة ٤٦ أنه : اذا لم يكن المتهم حاضراً في الاحوال المبينة في المادة السابقة جاز لمأمور الضبط القضائي أن يصدر أمراً بضبطه واحضاره ، ويذكر ذلك في المحضر.

والجدير بالذكر أن التلبس يتحقق بمشاهدة الجريمة لا بمشاهدة شخص الجاني ، فطبيعة التلبس عينية وليست شخصية كونها حالة تلازم الفعل لا الفاعل ، فلذا تكون لمأمور الضبط الاختصاصات الواسعة التي تمنحها له حالة التلبس ولو لم يكن قد شاهد الجاني أو عرفه ، بل شاهد الجريمة فحسب ، كما لو شاهد المجني عليه يصاب بعيار ناري في حضوره دون أن يشاهد مطلق هذا العيار[1].

اما بالنسبة لتفتيش المنازل فقد فرق قانون الإجراءات الجزائية بينه وبين تفتيش الأشخاص حيث أوجب الحصول على اذن بالتفتيش من النيابة العامة وذلك وفقا لما نصت عليه المادة ٥٣ من ذات القانون بقولها " لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير اذن كتابي من النيابة العامة ما لم تكن الجريمة متلبسا بها وتتوافر امارات قوية على أن المتهم يخفي اشياء أو اوراقا تفيد كشف الحقيقة" . كما يتم البحث عن الاشياء والاوراق المطلوب ضبطها في جميع انحاء المنزل وملحقاته ومحتوياته.

وتنسحب قواعد التفتيش السابقة على ما يخص التفتيش عن الأدلة الالكترونية والمعلومات في وسائل التقنية الحديثة ، وفي كل الاحوال فان ممارسة مأمور الضبط القضائي للتفتيش المصرح به قانونا بناء على حالة التلبس دون توفر حالة من الحالات التي تم ذكرها تعرض هذا الاجراء

---

(١) محمد عيد الغريب، الاختصاص القضائي لمأمور الضبط القضائي في الاحوال العادية والاستثنائية، بدون دار نشر، ٢٠٠٣، ص ٦٤ .

للبطلان ، ومع ذلك فان تقدير ما اذا كانت الجريمة في حالة تلبس ام لا يتم في لحظة التدخل من مأمور الضبط القضائي ، وطالما قدر مأمور الضبط القضائي أن الجريمة في حالة تلبس وتستدعي التدخل من قبله ، وكان تقديره مبنيا على أسباب معقولة ، فان تدخله يظل مشروعاً ولو اتضح بعد ذلك أن الجريمة ليست في حالة تلبس ، ذلك أن تقديره للمسألة كانت متعلقة بالفعل المرتكب لا الفاعل .

٢- في حالة غير التلبس

اذا لم تتوافر حالة من حالات التلبس المنصوص عليها في القانون فانه لايجوز القبض على أي شخص أو تفتيشه أو حبسه أو تقييد حريته الا بأمر من القاضي المختص أو النيابة العامة وذلك لحماية الحريات التي كفلها الدستور للافراد وبالتالي فهي حماية شاملة لأفراد المجتمع بأسره ، وفي هذه الحالة أجاز القانون ان تقوم السلطة المختصة بانتداب أحد مأموري الضبط القضائي لتفتيش شخص متهم أو تفتيشه منزله[1] . فالندب يعتبر اجراء من اجراءات التحقيق ولما كان التحقيق اساسا من اختصاص النيابة العامة فقد خولها المشرع باصدار القرار دون غيرها ، ويمكننا استخلاص ذلك من المواد ٦٨ ، ٦٩ من قانون الإجراءات الجزائية الاتحادي ، والمادتين "٧٠- ٢٠٠" من قانون الإجراءات الجنائية المصري، كما يستلزم أن يستوفي أمر الندب لشروطه الشكلية والموضوعية التي حددها القانون.

ويتضح لنا مما سبق أن الاصل في التفتيش هو عمل تحقيقي تختص به النيابة العامة أساسا ، الا وانه على سبيل الاستثناء وفي احوال معينة

---

(١) يعرف الانتداب للتفتيش بانه " تصرف اجرائي يصدر عن سلطة التحقيق بمقتضاه تمنح أحد مأموري الضبط القضائي اذنا بتفتيش شخص ومسكن متهم في جناية او جنحة تحقق وقوعها اذا توافرت دلائل جدية على حيازته لأشياء تتعلق بالجريمة المرتكبة تفيد في كشف الحقيقة عنها. انظر: د. خالد ممدوح ابراهيم، فن التحقيق في الجرائم الالكترونية، مرجع سابق، ص ١٩١ .

وبشروط خاصة ، يجوز لمأموري الضبط القضائي القيام به ، بمعنى أخر ان التفتيش الذي يقوم به مأمور الضبط القضائي يعد من الصلاحيات الاستثنائية الممنوحة له بنص القانون طالما قامت مسبباته ، وبالتالي فان كل تفتيش يقوم به مأمور الضبط القضائي لا يكون صحيحاً في القانون ما لم يكن قد قامت حالة استثنائية قررها القانون[1].

وعليه فان القواعد السابقة تسري على التفتيش في البيئة الالكترونية بحثا عن الدليل الالكتروني ، نظرا لعدم وجود النصوص الخاصة بالتفتيش في هذه الوسائل في التشريع الاماراتي ، لذلك فان تم التفتيش بمعرفة النيابة العامة فانها تتقيد بذات القيود التي يتقيد بها مأمور الضبط القضائي عند القيام بالتفتيش ، وتتمتع بنفس سلطاته فلها تفتيش المكان ومن كان موجودا وقامت ضده دلائل قوية توحي انه يخفي معه اشياء تفيد كشف الحقيقة ، كما أنها مقيدة بعدم التعسف في التفتيش والبحث والتنقيب في اشياء اخرى لا تمت للجريمة بصلة.

وبما ان محل التفتيش الذي بيناه بالتفصيل يقع على الوسائل الالكترونية سواء تم ضبطها مع الشخص نفسه أو بداخل منزله ، وقد يقع التفتيش على الحاسب المحمول الخاص بالمتهم والذي قد يكون مزوداً بنظام حماية يمنع من دخوله دون تدخل المتهم ومساعدته ، فهل يجوز اجبار المتهم على تزويد السلطات المختصة بكلمة المرور Password ؟ أو بالأحرى هل يمكن اكراهه على الافصاح عن كلمة السر ومافي حكمها من أجل تسهيل الوصول الى البيئة المعلوماتية محل التفتيش ؟[2]

---

(١) حسين بن سعيد الغافري، مرجع سابق، ص ٣٦٨.

(٢) ظهرت في الآونة الاخيرة العديد من البرمجيات التي تساعد على كسر كلمات سر الملفات المحمية، أو تكشف كلمة سر حافظ الشاشة، بل وحتى كلمة مدير الشبكة مثل برنامج Recovery Modules Password وبرنامج Crak Software وبرنامج Revelation وهذا الأمر يفيد مأموري الضبط القضائي حيث يمكنهم فك كلمات السر والشفرات الخاصة بالانظمة=

لقد تباينت الأراء الفقهية في ذلك ، فثمة راي يرفض اجبار المتهم على تقديم المعلومات اللازمة لتسهيل عملية الدخول للنظام الالكتروني ، وحجتهم في ذلك قاعدة معروفة وهي عدم جواز اجبار المتهم على تقديم دليل ضد نفسه ، بل له الحق في الصمت دون أن يفسر ذلك اقراراً منه على صحة الاتهام الموجه اليه . ويترتب على ذلك أنه لا يجوز اجبار المتهم بالادلاء عن المعلومات أو كلمة المرور الخاصة به أو اجباره على طباعة ملفات موجودة داخل النظام . حيث أن في اجباره على ذلك يجعل من الدليل الذي تم الحصول عليه دليلا غير مشروع لا يعتد به في الاثبات[1].

كما تضمنت أيضا توصيات المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما عام ١٩٥٣ أنه " لا يجبر المتهم على الاجابة ، ومن باب أولى لا يكره عليها ، فهو حر في اختيار الطريق الذي يسلكه ويراه محققا لمصلحته".

=الالكترونية للبحث عن أدلة الجريمة والتحقيق فيها . انظر في ذلك : د. ممدوح عبدالحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، الجريمة عبر الانترنت، البحث والتحقيق في جرائم الكمبيوتر، مكتبة دار الحقوق، الشارقة، الامارات العربية المتحدة، الطبعة الاولى، ٢٠٠١، ص ١٢٢ وما بعدها .

كما أن هناك برامج عشوائية لاستخراج كلمة المرور، ويتم ذلك بمحاولة توليد كلمات مرور متوالية أو كلمات مأخوذه من قاموس اللغة (وهو موجود على أقراص مضغوطة ويمكن البحث فيه بسهولة كبيرة) حتى يمكن الحصول على النتيجة المطلوبة . ولكن هذه البرامج تحتاج الى حاسبات سريعة لأنها قد تجرب ملايين أو آلاف الملايين من كلمات المرور حتى تصل الى الكلمة المنشودة، وبعض المجرمين يستخدمون كلمات مرور مكونة من مزيج من الحروف الكبيرة والصغيرة لجعل الأمر أكثر صعوبة أمام هذه البرامج العشوائية . انظر : حسن طاهر محمود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٠، ص ٢٣٩ .

(١) هشام فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مرجع سابق، ص ٨٢ .

اضف الى ذلك ان الحاسب الآلي الخاص بالمتهم يحتمل ان يحتوي على العديد من المستندات والمعلومات الخاصة به وباشخاص آخرين ، وفي اطلاع الجهات القائمة بالتحقيق على هذه المستندات والمعلومات انتهاكا لخصوصية الغير.

وهذا الاتجاه اعتنقته بعض التشريعات الحديثة ، ومنها القانون الياباني الذي يحظر على الأجهزة المختصة اكراه المتهم على الافصاح عن كلمة المرور ، وكذلك تبنى الشيء نفسه مشروع قانون الإجراءات الجنائية البولندي.

وفي المقابل ذهب راي آخر الى القول بأنه وان كان لايجوز اجبار الشخص على الادلاء بأقواله ضد نفسه ، بيد أن ذلك لا ينبغي ان يكون حائلاً دون اجباره على تقديم معلومات يقتضيها دخول السلطات المختصة للنظام المعلوماتي ، متى كانت هذه المعلومات بحوزته قياساً على اجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته[1].

ويرى البعض أن الرأي الأخير لايمكن القبول به ايًا كانت مبرراته ، فقياس المعلومة التي بحوزة المتهم على مفتاح الخزنة ومافي 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 فان هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الاثبات الجنائي ، كما ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجنائي. ومن ناحية ثالثة وحتى لو سلمنا بفرضية بجواز اكراه المتهم على اعطاء كلمة المرور التي تمكن من الدخول للنظام المعلوماتي ، فان الأمر يتخلله صعوبات حقيقة موجودة لا يمكن التغلب عليها وهي

---

(١) جميل عبدالباقي الصغير، أدلة الاثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ٢٠٠٢، ص ١٠٥ .

تذرع المتهم بنسيان كلمة المرور أو عدم حفظها أو شيء من هذا القبيل[1].

والذي نراه أنه في سبيل الحصول على كلمة المرور الخاصة بالنظام المعلوماتي للمتهم بطريقة مشروعة وقانونية لا يترتب على اثرها بطلان الإجراءات ، فانه يمكن اجبار غير المتهم للحصول على المعلومة التي من شأنها تيسير الدخول الى النظام المعلوماتي كمزود الخدمة في البلد نفسه في سبيل الحصول على معلومات العميل الذي يكون موضع شبهة من خلال معرفة المواقع الإلكترونية التي قام بزيارتها، وما هي الرسائل التي أرسلها عبر مزود الخدمة. ، ذلك لأن الاكراه الذي يقع على غير المتهم في تحقيق مصلحة عامة لا يمس حقوق الدفاع ، فعنصر الاكراه أو الاجبار هنا لا يشكل ضرراً بالنسبة له خلافاً للوضع بالنسبة للمتهم .

حيث أنه يمكن لمزود الخدمة تحديد وقت دخوله تلك المواقع ووقت خروجه منها من خلال الاحتفاظ بسجل الدخول والخروج Log files ورقم التعريف الدولي (IP Address) وهو ما يعرف باسم Dynamic IP Address ، حيث تعرف الأولى بأنها العناوين المحددة لكل مستخدم، ويتم استخدامها في كل مرة يتم فيها الدخول إلى الشبكة العالمية (الإنترنت)، وكذلك معرفة الأجهزة التي تتصل معها من خلال التعريف الدولي، مع ملاحظة أن مزودي الخدمة لا يطلعون عادة على السجلات ما لم يطلب منهم ذلك بشكل رسمي وبعد الحصول على إذن تفتيش من النيابة العامة، ومراعاة عدم التعسف في البحث عن الدليل الرقمي المحدد للإدانة[2].

---

(١) انظر : موسى مسعود ارحومة، مرجع سابق، ص ٨ ومابعدها .

(٢) ممدوح عبدالحميد عبد المطلب جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة، الامارات العربية المتحدة، الطبعة الاولى، ٢٠٠٠، ص ١١٤ .

ويثور تساؤل في هذا المقام عن المسؤولية الجنائية لمزود الخدمة ذاته فهل تتحقق مسؤولية عن تقصيره في عدم التقيد بلوائح وقيود تقديم الخدمة وتقييدها ضمن اطار معين يمنع القيام بالعبث من خلالها أو بواسطتها ، او من جانب آخر ما يتم بثه وتداوله من عناصر هي تشكل في حقيقتها جريمة كارسال المواد الاباحية عن شبكة الانترنت ، حيث يرى البعض عدم قيام المسؤولية الجنائية في أي حال من الاحوال ، بينما يرى رأي اخرون قيام المسؤولية الجنائية ضد مزود الخدمة ..

وعليه فقد قامت بعض الدول الى وضع ما يسمى بالبروكسي (Proxy)[1] عن طريق الشركة القائمة بتزويد خدمة الانترنت في تلك الدول وذلك حتى تتم عملية المراقبة على تلك المواقع .

وبالنظر للقوانين المقارنة نجد أن الولايات المتحدة الامريكية واجهت مثل هذه المشكلة ، الى حين اصدر المشرع الأمريكي في ٨ فبراير ١٩٩٦ قانون اداب الاتصالات بقصد مواجهة تفشي تداول المواد الاباحية في وسائل الاتصال العامة ومن بينها شبكة الانترنت ، وقد تضمن هذا القانون احكاما مختلفة بث مشاهدة المواد الاباحية .

---

(١) البروكسي يعمل كوسيط بين الشبكة ومستخدميها من أجل التحكم والسيطرة على شبكة الانترنت ، وتسهيل الوصول ، وفلترة المواقع ، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة ، فيتحقق البروكسي فيما اذا كانت هذه الصفحة قد جرى تنزيلها من قبل ، فيقوم باعادة ارسالها الى المستخدم بدون الحاجة الى ارسال الطلب الى الشبكة العالمية . ان انه لم يتم تزيلها من قبل فيتم ارسال الطلب الى الشبكة العالمية ، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP . ومن اهم مزايا البروكسي ان ذاكرة Cache المتوفرة لديه يمكن ان تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره اقوى في الاثبات عن طريق فحص تلك العمليات المحفوظة بها ، والتي تخص المتهم والموجودة عند مزود الخدمة . انظر : د. حسين بن سعيد الغافري ، مرجع سابق ، ص ٥١٢ .

ولكن ورود هذه العبارات في القانون اثار حالة من الارتياب ونقاشا شديداً في اوساط من المحاكم الامريكية التي اعتبرت احداها أن عبارتي فاحشة (Indecent) وفاضحة (Monifestementchoquants) غير دستورية وذلك بعد أن استفاضت في اجراء تحليل مسهب لخصوصيات الاتصال بواسطة شبكة الانترنت[1].

وفي فرنسا تم الاستعانة بتجربة (التيليماتيك) أو شبكة المينتيل والتي سبقت استخدام الانترنت في هذه الدول بسنوات عديدة ، واعتبرت ان شبكة الانترنت خدمة من بين الخدمات المقدمة وانها تخضع لقانون الاتصال عن بعد الصادر في ٣٠ سبتمبر ١٩٨٦ على اعتبار انها توفر خدمات سمعية وبصرية وفقا للمعنى المبين في هذا القانون[2].

وقد نص هذا القانون على أنه يقع على عاتق مزود الخدمة الالتزام بحسن تنفيذ الخدمة المعلوماتية بحيث يتم تنفيذها بما يتفق مع اعراف المهنة ويلتزم ايضا بالاعلام عن وسائل الدخول الى الخدمة مثل شفرة تحقيق هوية المستخدم ، والذي يقوم بمراقبة محتوى الرسائل التي تصل اليه[3]، وهذا ما قد يفيد في التحقيقات الجنائية وصولاً الى الدليل الالكتروني في الجريمة الالكترونية المرتكبة .

وخلاصة القول ان الدول قد شعرت بما قد يسفر عن الانترنت من جرائم تمس المجتمع والأفراد ، فقامت بدورها بسن تشريعات معينة بهدف مواجهة هذا الخطر القادم ، وتحميل مزود الخدمة أو مقدمها في بعض الأحيان المسؤولية الجنائية ، في حال اخلاله بالالتزامات المفروضة عليه ، والتي تعد بمثابة ثغرة جنائية تمكن للمجرم الالكتروني العبور من خلالها

---

(١) طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، صادر لبنان، ٢٠٠١، ص ١٧٠ .

(٢) المرجع السابق، ص ١٧٢ .

(٣) جميل عبدالباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، ٢٠٠٢، ص ١٦٢ .

وارتكاب جريمته ، في حين أنه ربما لم يتمكن من ارتكاب جريمته في حال التزام مزود الخدمة بما يفترض عليه .

لذلك نرى ضرورة إضافة مادة في قانون مكافحة جرائم تقنية المعلومات تلزم الشركات المزودة لخدمات الاتصالات بالاحتفاظ بسجلات الدخول والخروج (Log files) لمدة مناسبة إذا لم يكن مطبقاً وذلك لسهولة تتبع مجرمي الإنترنت كما هو الحال في بعض الجهات، مثل شركة Googleجوجل التي تحتفظ بسجلات تصفح المستخدمين لفترة تمتد بين ١٨ إلى ٢٤ شهراً[1] ، وجدير بالذكر بأنه لا يحق لمزودي الخدمة الاطلاع على هذه المعلومات من تلقاء انفسهم، ما لم يتم تزويدهم بطلب رسمي من الجهات المسؤولة عن تطبيق القانون، لكي يمكن لمأموري الضبط القضائي من مراقبة تحركات مستخدمي شبكة المعلومات المشتبه بهم، وما إذا كانت تحركاتهم تشكل جريمة أم لا[2].

الفرع الثاني
الضوابط الشكلية لتفتيش نظم الحاسب الآلي

بجانب الضوابط والشروط الموضوعية التي تستوجب مراعاتها لصحة اجراء تفتيش نظم الحاسب الآلي ، فان هنالك ضوابط وشروط شكلية نص عليها القانون تستلزم التقيد والأخذ بها وذلك صوناً للحريات الفردية من التعسف أو الانحراف عند قيامها باجراء التفتيش ومن أهمها ما يأتي :

اولا: تسبيب الأمر بالتفتيش :

والمقصود بالتسبيب هو وجود دلائل وقرائن تدل على وجود أدلة معينة من شأنها ان تكشف عن الغموض الذي يعتري الجريمة المرتكبة.

---

(١) انظر التقرير منشور عبر الموقع الإلكتروني الخاص بهيئة الإذاعة البريطانية. http://news.bbc.co.uk/hi/arabic/sci_tech/newsid_6457000/6457527.stm

2 -sheetz, Michael, computer crime investigation, jhonwileg & sons , incorporated , new jersey , usa, 2007, p: 102

ويعتبر من الضمانات القانونية المقررة في التشريعات الاجرائية للكثير من الدول[1] .

وهذا التسبيب ضمان لتوافر العناصر الواقعية التي يجب ان يحتويها سبب التفتيش بالمعنى الدقيق وحتى يكون ذلك التسبيب تحت رقابة هيئة الحكم وكذلك الدفاع حتى يمكن مراقبة ما اذا تم اصدار اذن التفتيش وفقاً للشروط القانونية من عدمه ، وحتى يمكن تقدير جدية صدوره وهو أمر تقديري لسلطة التحقيق تحت رقابة محكمة الموضوع .

وعليه فان امر التفتيش في الجريمة الالكترونية يهدف للتوصل الى ما يفيد ارتكاب جريمة تشكل عدوانا وانتهاكا على الأنظمة التقنية ، وبالتالي فان التفتيش لا يكون شاملاً وانما محددا ومخصصا في الاشياء التي يمكن ان يستمد منها الدليل الاكتروني لكي يكون مبرراً للقيام به .

ثانيا : الحضور الضروري لبعض الاشخاص عند القيام بعملية التفتيش :

ويعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون وذلك لضمان الاطمئنان الى سلامة الاجراء وفقا للقواعد التي قررها القانون دون ان تشكل انتهاكاً لأحد .

وتفاديا لأي دفع بعدم حيازة الأشياء المضبوطة ، وضمانا لحرمة مسكن المشبوه فيه أوجب المشرع حضوره أو من ينوب عنه كضمانة لصحة التفتيش. أما إذا كان المشتبه به قد امتنع عن الحضور أو كان فارا، يكون في هذه الحالة مأمور الضبط القضائي ملزما بالقيام بالتفتيش وذلك بحضور شاهدين لا يكونان موظفين تحت سلطة ضابط الشرطة القضائية ، والمشرع الاماراتي لم يشترط هذا الاجراء الا بالنسبة لتفتيش المسكن حيث نص في المادة ٥٩ اجراءات بأنه " يجري التفتيش بحضور المتهم أو من ينيبه كلما امكن ذلك ، والا تم بحضور شاهدين ويكون هذان الشاهدان بقدر الامكان من اقاربه الراشدين او القاطنين معه بالمنزل او من جيرانه ويثبت

(١) انظر المواد ٥١ – ٥٣ من قانون الاجراءات الجزائية الاتحادي .

ذلك بالمحضر "، ويقابله ذات المعنى في التشريع المصري . أما بالنسبة لتفتيش الأشخاص فان المشرع لم يشترط حضور شهود اثناء عملية التفتيش وفقا لما نصت عليه المادة ٥١ اجراءات جزائية.

اما اذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة فيصح اتخاذ هذا الاجراء دون حاجة لاستدعاء شهود (المادة ٢٩) اجراءات جزائية مصرية ولم يرد مثل هذا النص في قانون الإجراءات الجزائية الاماراتي ، ويستوي الأمر عند قيام مأمور الضبط القضائي بمباشرة التفتيش بناء على ذلك من سلطة التحقيق ، فلا يلتزم باستدعاء شهود لأن المندوب يحل محل النائب تماما[1].

ثالثا : وقت التفتيش

تركت بعض التشريعات الاجرائية أمر تحديد وقت التفتيش متروكاً للقائم بعملية التفتيش، ومن ثم فانه يجوز له القيام بالتفتيش في الوقت الذي يراه مناسبا ليلا او نهارا ، حسب ملابسات الواقعة وظروفها وطبيعتها ، حيث نصت المادة ١٣٩ من التعليمات القضائية للنيابة العامة على " ..... ويجوز اجراء التفتيش في أي وقت ليلا او نهارا وان يجري بالكيفية التي تحقق الغرض منه وبالطريقة التي يراها "، وبنفس الرأي قد اخذ قانون الإجراءات الجنائية المصري.

على خلاف ذلك فنجد أن هناك بعض التشريعات الاجرائية تحظر تفتيش المنازل ومافي حكمها الا في اوقات محدد نص عليها القانون .

ويستخلص من مقتضيات المادة٦٢ من قانون الإجراءات الجنائية المغربي على أنه لا يمكن الشروع في تفتيش المنازل أو معاينتها قبل الساعة السادسة صباحا وبعد الساعة التاسعة ليلا ، إلا إذا طلب رب المنزل أو وجهت استغاثة من داخله ، أو في الحالات الاستثنائية التي نص عليها القانون[2] ، غير أن العمليات التي ابتدأت في ساعة قانونية يمكن مواصلتها

---

(١) هلالي عبداللاه احمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ١٦٥ .

(٢) كما اوردنا اعلاه فان هناك حالات استثنائية يصح من خلالها القيام بعملية التفتيش ليلا او نهارا دون التقيد بالوقت الذي حدده المشرع ومنها :=

دون توقف. وهكذا لا يمكن لمأمور الضبط القضائي أن يقوم بتفتيش المنزل في أي وقت شاء وإنما عليه أن يراعي الوقت القانوني المسموح به[1] ، ومثل ذلك نجده في المادة ٥٩ من قانون الإجراءات الجنائية الفرنسي فقد حدد وقت التفتيش من الساعة السادسة صباحا الى الساعة التاسعة مساءا[2].

ولأهمية هذا الموضوع ولأن الناس غالباً ما يكونون في حالة استرخاء في الفترة الممتدة بين غروب الشمس وشروقها ، لذا نرى وضع نص يمنع فيه اجراء التفتيش في هذه الفترة الا في جرائم معينة وفي حالات الضرورة القصوى ، وحسنا فعل المشرع الاماراتي اذ لم يحدد وقتا معينا للقيام بالتفتيش وانما ترك أمر تقدير مدى جديته وضرورته الى تقدير النيابة العامة ، ذلك أن الجريمة الالكترونية جريمة لا تتقيد بوقت معين لأن الجاني يمكنه القيام بجريمته وهو في منزله سواء في اقليم الدولة أو خارجها ، وكما بينا سلفا فان الدليل الالكتروني يصعب الحصول عليه أو قد يتعرض للحذف والتغيير ، لذا تستلزم بعض الجرائم نظرا لخطورتها وصعوبة اثباتها لاحقا الى ضبط الجاني مع جهاز الحاسب الآلي متلبسا بجريمته .

وعليه نستخلص مما سبق أنه يسري على الجرائم الالكترونية القواعد العامة لاجراء التفتيش فان كان التشريع يتضمن وقتا معينا يتم خلاله القيام بعملية التفتيش فان الجريمة الالكترونية تندرج تحت هذه القواعد العامة وضعها في ذلك وضع الجريمة التقليدية ، وعلى العكس من ذلك

= - حالة رضا صاحب المنزل رضاءا حرا صريحا وعن علمه بالسبب.

- حالة الضرورة وتتثمل في حالة الاستغاثة من داخل المنزل وحالتي الحريق والغرق وما شابه ذلك.

انظر : محمود نجيب حسني، شرح قانون الاجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٨٨، ص ٥٨٠ .

(١) انظر الرابط الالكتروني :
http://www.blog.saeeed.com/2009/11/perquisition-domiciliaire-garanties-droits-crime-terrorisme/

(٢) نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، الاسكندرية، دار الفكر الجامعي، ٢٠٠٧، ص ٢٥٩ .

فان كان المشرع لم يحدد وقتا ولا زمنا معينا للقيام بعملية التفتيش فانه يجوز اجراء التفتيش في أي وقت وفقا لما تراه السلطات المختصة بذلك بناء على تقديرها لوقائع وظروف وملابسات الجريمة .

رابعا : تحرير محضر بتفتيش نظم الحاسب الآلي :

باعتبار أن التفتيش عمل من أعمال التحقيق ، فينبغي تحرير محضر يثبت فيه ما تم من اجراءات ، وما أسفر عنه التفتيش من أدلة ، ولم يتطلب القانون شكلاً معينا في محضر التفتيش ، وبالتالي فانه لايشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقضي بأن يكون مكتوباً باللغة العربية اللغة الرسمية للدولة وأن يحمل تاريخ تحرير وتوقيع محرره وان يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي بينها .

ولا يختلف الأمر بالنسبة لمحضر تفتيش النظم المعلوماتية ، فيما عدا أن يستلزم بالاضافة الى الشكليات السابقة ضرورة احاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات ، ومن جهة اخرى ان يكون هناك شخص متخصص في الحاسوب والانظمة التقنية للاستعانة به في المسائل الفنية الضرورية ، والمحافظة على الأدلة المتحصل عليها من التلف أو الازالة .

الفرع الثالث
الإجراءات التي يجب اتباعها عند التفتيش في مجال نظم المعلومات الإلكترونية[1]

أولاً- عدم العبث بالأجهزة التقنية ونقلها من مكان إلى آخر إلا من قبل مختصين:

عندما يتم تفتيش الأجهزة التقنية ، فإنه يجب أن يتم ذلك من قبل مختصين أو محققين مدربين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات ، حتى لا يتم تغيير حالة الأجهزة والبرامج ، لأن ذلك قد

---

(١) كمال أحمد الكركي ، التحقيق في جرائم الحاسوب ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر: أكاديمية شرطة دبي– مركز البحوث والدراسات خلال الفترة : ٢٦- ٢٨ /٤/ ٢٠٠٣م : دبي– الإمارات العربية المتحدة ، ص ٤٨٦.

يفضي إلى ضياع الدليل الجنائي بسهولة إذا ما تم التعامل مع الآثار الموجودة في مسرح الجريمة من قبل غير المختصين.

ثانياً ـ عدم فتح جهاز الحاسب الآلي محل التفتيش في مسرح الجريمة :

يفضل أن يتم تصوير جهاز الحاسب الآلي والأجهزة التقنية الأخرى ذات العلاقة بالجريمة قبل أن يتم نقلها إلى المختبر في مسرح الجريمة، وأن يتم ذكر وقت وتاريخ ومكان التقاط كل صورة، وأن لا يتم تشغيلها[1] ، وأن يكون التفتيش بشكل ظاهري في مسرح الجريمة لاحتمال إتلاف الدليل الجنائي الموجودة عليها، أو على الأقل قد يغير حالة الذاكرة أو الملفات، وإذا كان هناك حاجة إلى تشغيل جهاز الحاسب الآلي في مسرح الجريمة، فيجب أن يتم من قبل مختصين، وأن يتم تدوين جميع الخطوات التي تمت.

ثالثاً ـ أن لا يتم السماح للمشتبه به التعامل مع جهاز الحساب الآلي موضوع الجريمة في مسرح الجريمة:

إن الأدلة الإلكترونية من السهل محوها أو إتلافها عند العمل على جهاز الحاسب الآلي، لذلك يجب عدم السماح للمشتبه به من التقرب أو لمس أوالعمل على هذه الأجهزة تحت أي سبب ، حتى وان أبدى رغبته في الولوج الى النظام المعلوماتي بادخال كلمة السر ، لانه لربما قد يقوم متعمدا بمسح الأدلة المخزنة على جهاز الحاسب الآلي ، لذا يفضل ان يقوم باعطاء كلمة المرور لمأموري الضبط القضائي أو ان يقوم بالدخول الى النظام أمام ناظريهم وتحت اشرافهم المباشر ، وأن يتم منعه من الاقتراب من مصدر الطاقة في مسرح الحادث.

رابعاً ـ أن يتم إعداد نسخة احتياطية عن وسائط تخزين المعلومات الموجودة في مسرح الجريمة[2]

---

(١) د. هلالي عبد اللاه احمد، تفتيش نظم الحاسب الآلي؛ مرجع سابق، ص ١٧٥.

(٢) تعليمات طرق تفتيش الأجهزة الإلكترونية في دورة (جرائم الكمبيوتر)، التي عقدت بمعهد العلوم الأمنية والإدارية بأكاديمية شرطة دبي بالتعاون مع مكتب التحقيقات الفيدرالي FBI، بتاريخ ٢٠٠٨/٠٥/٠٩م.

يجب أن يتم أخذ نسخة احتياطية عندما يتم تفتيش الأجهزة الإلكترونية إذا وجدت في حالة تشغيل قبل أن يتم إطفاؤها ونقلها إلى المختبر الجنائي للفحص، وذلك خشية أن يتم إتلاف الدليل الجنائي وقت إغلاقها أو وقت نقلها.

خامساً ـ توثيق جميع خطوات التحقيق[1]

من المتعارف عليه أنه لا بد من تدوين جميع إجراءات التحقيق بشكل عام، وتوثيق جميع إجراءات التفتيش في مجال تفتيش أجهزة الكمبيوتر وأجهزة نظم المعلومات الإلكترونية بشكل خاص، من حيث تحديد الوقت والتاريخ وذكر الخطوات بالتفصيل.

سادساً ـ أن يتم التعامل مع الدليل الجنائي الرقمي بعناية فائقة:

يجب التعامل بعناية فائقة مع الأدلة الرقمية، لأنها حساسة، ويمكن أن تتلف بسهولة، ويجب أن يتم الاحتفاظ بها في أماكن لا تحتوي على أي مجال من المجالات الكهرومغناطيسية أو الكهربائية[2].

النتائج

- يجب أن يخضع التفتيش في الجرائم الالكترونية لمجموعة من الضمانات التي توضح حدوده المكانية والزمانية والموضوعية والاجرائية ، نظرا لخطورته ومساسه بالحريات الشخصية للافراد وحياتهم الخاصة وحرمة منازلهم، ومن أهم هذه الضمانات، ان يتم مباشرة من قبل السلطة المختصة وفقا للاجراءات المقررة قانونا، وان يراعى وقت التفتيش بناءً على تقديرهم لخطورة الجريمة من عدمه.
- ينبغي أن يتضمن اذن التفتيش في الجرائم الالكترونية أمرا خاصا بتفتيش وضبط جهاز الحاسب الآلي وملحقاته وما يتبعها من أشرطة

---

(١) كمال أحمد الكركي، مرجع سابق، ص٤٨٨.

(٢) د. هشام فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مرجع سابق، ص١٢٧.

ممغنطة واقراص ضوئية وكل ما من شأنه ان يكون دليلا على ارتكاب الجريمة الالكترونية، وان لايتم الا للبحث عن الاشياء الخاصة بالجريمة التي يجري جمع الاستدلالات بشأنها.

- صعوبة الحصول على الدليل الالكتروني بسبب امتداد النطاق المكاني في عملية التفتيش الى أنظمة وحواسيب أخرى ذات صلة بالجريمة واتساع الرقعة الجغرافية مما يفضي الى صعوبة الوصول الى هذا الدليل، الأمر الذي يقضي بتفعيل دور التعاون الدولي اطار اتفاقيات ثنائية او دولية تجيزه ، ومن ثم فانه لايجوز القيام به في ظل غياب هذه الاتفاقية ، او على الاقل الحصول على اذن الدولة الاخرى التي يجري التفتيش في اقليمها.
- عدم جدوى الإجراءات التقليدية في التفتيش عن الادلة الالكترونية اذ لابد من اتباع بعض الإجراءات التقنية المتخصصة التي تتفق مع طبيعة وتقنية الدليل بحيث تساند وتدعم تلك الإجراءات في سبيل استخراج الدليل من البيئة الرقمية .

التوصيات

- دعوة الدول العربية للانضمام للاتفاقيات الدولية التي تعنى بشؤون الجرائم الالكترونية ولاسيما اتفاقية بودابست لمكافحة جرائم المعلوماتية، من خلال تبني واعتماد منهجية الإجراءات العملية الحديثة المتعلقة بالتفتيش في سبيل مواجهة ومكافحة الجرائم الالكترونية أو الحد منها أو من تفاقمها قدر الامكان.
- ضرورة استحداث قواعد خاصة بالإجراءات الجنائية في مرحلة التحقيق في الجرائم الالكترونية ، تتضمن كيفية اجراء التفتيش على المكونات المكونات المادية والمعنوية للحاسب الآلي وملحقاته وما يتعلق به من انظمة تقنية وبيانات الكترونية والتحفظ على الأدلة

المتحصلة من الجريمة، وعدم الاكتفاء باخضاع التفتيش التقني لقواعد التفتيش التقليدي.

- ضرورة التخفيف من الشروط الشكلية في الحصول على اذن النيابة العامة أو القاضي المختص للتفتيش في الجرائم الالكترونية نظرا للطبيعة الخاصة التي يتمتع بها الدليل الالكتروني من حيث سرعة تغييره وزواله ، كسباً للوقت وضبطاً للدليل الالكتروني والتحفظ عليه.
- ضرورة قيام الجهات المختصة بعقد دورات تدريبية محلية واقليمية ودولية لأموري الضبط القضائي فيما يتعلق بالطرق الفنية الحديثة للتفتيش على الادلة الالكترونية في الكيان الرقمي، وكذلك بالنسبةلاعضاء النيابة العامة والقضاة ، ليكونوا أكثر قدرة على فهم وقائع الجريمة المرتكبة حين الخوض في المسائل الفنية، كاستجواب المتهمين وسماع تقرير الخبير التقني .
- ضرورة إضافة مادة في قانون مكافحة جرائم تقنية المعلومات تلزم الشركات المزودة لخدمات الاتصالات بالاحتفاظ بسجلات الدخول والخروج (Log files) لمدة مناسبة وذلك لسهولة تتبع مجرمي الإنترنت.

المراجع

المؤلفات العربية

- اسامة أحمد المناعسة ، جلال صايل الهواوشة ، جلال الزعبي ، جرائم الحاسب الآلي والانترنت ، دراسة تحليلة مقارنة ، الاردن ، عمان ، ٢٠٠١
- بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، دار الفكر الجامعي ، الطبعة الاولى ٢٠١١.

- جميل عبدالباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠٢.
- جميل عبدالباقي الصغير ، أدلة الاثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية، القاهرة ، ٢٠٠٢.
- حسن طاهر محمود ، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، الطبعة الأولى ، الرياض ، ٢٠٠٠
- حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٩
- خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الاولى، ٢٠١٠
- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، ٢٠٠٧.
- طوني ميشال عيسى ، التنظيم القانوني لشبكة الانترنت ، صادر لبنان ، ٢٠٠١
- عارف محمد عبدالرحيم ، دور ومهام أعضاء الضبط القضائي في مرحلتي التحري والتحقيق الابتدائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة المنصورة ، ٢٠٠٧
- عبدالله حسين محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، دار النهضة العربية ، القاهرة ، الطبعة الثانية ، ٢٠٠٢
- علي محمود علي حمودة ، أدلة اثبات الجرائم الالكترونية وتقديرها في اطار نظرية الاثبات الجنائي ، بحث منشور في مجلة الامن والقانون ، مجلة تصدر عن أكاديمية شرطة دبي

- عمرمحمد ابوبكر بن يونس : الجرائم الناشئة عن استخدام الانترنت ، رسالة دكتوراه ، جامعة عين شمس ، ٢٠٠٤.
- عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣
- عمر محمد بن يونس ، مستشار موسوعة التشريعات العربية (سجل جينيس للأرقام القياسية ١٩٩٩) ، الطبعة الأولى ٢٠٠٧- ٢٠٠٨ ، بدون دار نشر.
- عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، المرشد الفيدرالي لتفتيش وضبط الحواسيب وصولا الى الدليل الالكتروني في التحقيقات الجنائية ، بدون دار النشر ، ٢٠٠٦
- موسى مسعود ارحومة ، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، بحث مقدم الى المؤتمر المغاربي الاول حول : المعلوماتية والقانون ، الذي تنظمه اكاديمية الدراسات العليا- طرابلس ، خلال الفترة ٢٨- ٢٠٠٩/١٠/٢٩
- مصطفى محمد موسى ، المراقبة الالكترونية عبر شبكة الانترنت ، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية ، دار الكتب والوثائق القومية ، الطبعة الاولى ، ٢٠٠٣
- محمد امين الخرشة ، مشروعية الصوت والصورة في الاثبات الجنائي ، دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠١١ .
- منير محمد الجنبيهي و ممدوح محمد الجنبيهي ، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الاسكندرية ، ٢٠٠٥ .

- محمد زكي ابو عامر ، الإجراءات الجنائية ، دار المطبوعات الجامعية ، ١٩٨٤.
- محمد عيد الغريب ، الاختصاص القضائي لمأمور الضبط القضائي في الاحوال العادية والاستثنائية ، بدون دار نشر ، ٢٠٠٣ .
- ممدوح عبدالحميد عبد المطلب جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية ، مكتبة دار الحقوق ، الشارقة ، الامارات العربية المتحدة ، الطبعة الاولى ، ٢٠٠٠.
- محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٨٨ .
- نبيلة هبة هروال ، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، الاسكندرية ، دار الفكر الجامعي ، ٢٠٠٧.
- هشام محمد رستم : الجوانب الاجرائية للجرائم المعلوماتية ، — دراسة مقارنة — مكتبة الآلات الحديثة — أسيوط — ١٩٩٤.
- هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٦ .
- هلاليعبداللاهأحمد، اتفاقيةبودابست لمكافحة جرائم المعلوماتية، دارالنهضةالعربية، القاهرة، ٢٠٠٧، الطبعة الأولى.
- البحوث والندوات
- صالح أحمد البربري، دور الشرطة في مكافحة جرائم الانترنت، في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٣-١١-٢٠٠١م، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية الذي عقد في أكاديمية شرطة دبي بدولة الإمارات العربية المتحدة، بتاريخ ٢٦- ٢٨ ابريل ٢٠٠٣

- كمال أحمد الكركي، التحقيق في جرائم الحاسوب، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر: أكاديمية شرطة دبي– مركز البحوث والدراسات خلال الفترة : ٢٦- ٢٨ /٤/٢٠٠٣م : دبي– الإمارات العربية المتحدة.
- لين وينميل ، الجريمة الالكترونية : القضايا والتحديات في الولايات المتحدة ، من أوراق العمل المقدمة الى ورشة عمل الجريمة الالكترونية ، وزارة العدل ، أبوظبي ، في الفترة من ٢ الى ٣ يونيو ٢٠١٠ .
- محمد ابو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية الذي عقد بأكاديمية شرطة دبي من ٢٦- ٢٨ أبريل ٢٠٠٣م، الجزء الأول، محور القانون الجنائي.

المواقع الالكترونية

- http://www.arab-elaw.com/show_similar.aspx?id=78
- http://www.blog.saeeed.com/2009/11/perquisition-domiciliaire-garanties-droits-crime-terrorisme
- http://news.bbc.co.uk/hi/arabic/sci_tech/newsid_6457000/6457527.stm

المراجع الاجنبية

- sheetz, Michael, computer crime investigation, jhonwileg & sons, incorporated, new jersey, usa, 2007
- Piragoff (Donald K) Computer crimes and other crimes against information technology in Canada :Rev. Intern.De.Dr.pen1993.P241.