التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية

د. محمد جمال مطلق الذنيبات*

القاضي معن أحمد العناسوة

تاريخ تقديم البحث:٢٠٢٠/٢/٢٣م. تاريخ القبول: ٢٠٢١/٢/١٥م.

ملخص

تهدف هذه الدراسة إلى بيان مفهوم التفتيش في الجرائم الإلكترونية والقواعد القانونية التي تحكمه، وتحدد النصوص الناظمة للتفتيش في الجرائم الإلكترونية والخصائص التي تميزه عن غيره. والطبيعة القانونية للتفتيش بالإضافة إلى الضمانات التشريعية التي يتعين توافرها في التفتيش، فضلا عن الشروط الشكلية الواجب مراعاتها عند إجراء التفتيش في الجرائم الإلكترونية، وانتهت الدراسة إلى تحليل النصوص القانونية وبيان أوجه القصور فيها. وقدمت جملة من التوصيات والاستنتاجات للجهات ذات العلاقة.

الكلمات المفتاحية: جريمة إلكترونية، تفتيش إلكتروني، شروط شكلية.

* كلية الحقوق، جامعة عمان الأهلية، عمان– الأردن.

حقوق النشر محفوظة لجامعة مؤتة، الكرك، الأردن.

Inspection in Cybercrime: Its Nature and Formal Conditions

Dr. Mohmmad. J. Thneibat

Maen. A. Anaswa

Abstract

This study aims to clarify the concept of inspection in cybercrimes and its legal nature. It addresses the legal texts related to inspection; the characteristics associated with this type of crime, and the possible extent of inspection in electronic devices. This study is distinguished from other similes by tackling the conditions of inspection in cybercrimes and the guarantees in legislations, Furthermore, this research discusses formal conditions that must be taken into account when carrying out inspection. Eventually, the study provides conclusions along with significant recommendations to responsible authorities.

Keywords: Cybercrime, Cyber Evidence, Electronic Search, Cybercrime Scene, Cybercrime Commission

المقدمة:

شهد العالم العديد من التطورات خلال العقدين الماضيين وكان من أبرزها ثورة تكنولوجيا المعلومات وتطور شبكات الاتصال والإنترنت. الأمر الذي جعل التواصل بين الأشخاص حول بقاع الأرض أكثر سهولة وأسرع بكثير من أي وسيلة كانت معروفة مسبقاً. فكانت هنالك طائفة من الأشخاص الذين استفادوا من هذه الثورة بتطوير أعمالهم ومنهم من استفاد منها بالتواصل مع أصدقائه وأفراد أسرته، وغيرها الكثير من صور الاستفادة الإيجابية من هذا التطور. إلا أن هنالك فئة أخرى استخدمت هذا التطور بصورة سلبية فذهب أفرادها إلى الاتصال والتنسيق مع أقرانهم لارتكاب الجرائم باستخدام هذه التكنولوجيا وبالاستعانة بالأجهزة الإلكترونية التي تمكنه من الاستخدام الأمثل لها والاستفادة من ميزاتها. والدخول إلى خصوصيات الأشخاص والحكومات والمؤسسات المصرفية. واستغلال الأطفال والنساء والترويج للأعمال الإباحية وأعمال الدعارة عن طريق شبكة الإنترنت وغيرها من صور الجرائم الإلكترونية.

ولهذا أصبح شكل الدليل في الجريمة الإلكترونية مختلفاً عن شكله في الجريمة التقليدية كما أن له خصائص تختلف عن خصائص الدليل المادي الملموس. وبالتالي فإن إجراءات التفتيش عن هذا النوع من الأدلة يختلف عن التفتيش في الجريمة التقليدية. ولذا فإن هذا البحث سيقوم ومن خلال إتباع منهج البحث العلمي المقارن بتوضيح شروط التفتيش في الجرائم الالكترونية بحسب التشريعات الجزائية الأردنية والقوانين المقارنة. وبيان مدى إنتاجيتها وصلاحيتها عند القيام بتنفيذه في بيئة إلكترونية. وذلك من خلال تقسيمه إلى مبحثين الأول يبحث في ماهية التفتيش في الجرائم الالكترونية من حيث توضيح مفهومه والطبيعة القانونية لتفتيش نظم الحاسب الآلي وبيان النصوص الخاصة به وكذلك بيان مدى قابلية نظم الحاسب الآلي والإنترنت للتفتيش يتبعه المبحث الثاني الذي يبين خصائص التفتيش في الجريمة الإلكترونية والشروط الشكلية للتفتيش في مثل هذا النوع من الجرائم، منتهياً بخاتمته ومجموعة من النتائج والتوصيات التي وجد الباحثان بأنها تتعلق بموضوعه.

مشكلة الدراسة:

تكمن مشكلة الدراسة بتحديد الطبيعة القانونية للتفتيش في الجرائم الإلكترونية وتحديد الجهة المختصة للقيام به وبيان مدى إمكانية تطبيق النصوص القانونية الواردة في قانون أصول المحاكمات الجزائية الأردني والمتعلقة بالشروط الشكلية للتفتيش كإجراء من إجراءات التحقيق الابتدائي والضمانات المحددة لهالواردة على التفتيش في الجرائم الإلكترونية لعدم النص عليها ضمن قانون الجرائم الإلكترونية الأردني.

أهمية الدراسة (الإضافة العلمية الجديدة للدراسة):

يقوم هذا البحث بدراسة الطبيعة القانونية للتفتيش في الجرائم الالكترونية وخصائصه وبيان الشروط الشكلية للتفتيش في الجرائم الإلكترونية بحسب التشريعات الجزائية الأردنية، لذا سيتم التركيز على القواعد القانونية في تفتيش الأجهزة الإلكترونية التي تعود للمشتكى عليه؛ وما يتعلق به من شبهات؛ وبيان القصور التشريعي في قانون الجرائم الإلكترونية فيما يتعلق بتحديد الضمانات الخاصة بإجراءات التفتيش الإلكتروني؛ لتحقيق غايته وعدم التغول على خصوصية من يتعرضون له.

أهداف الدراسة:

يهدف هذا البحث إلى بيان الصورة الشاملة عن موضوع الطبيعة القانونية للتفتيش في الجرائم الالكترونية وخصائصه وبيان الشروط الشكلية للتفتيش في الجرائم الإلكترونية؛ لكي يكون منتجاً لآثاره القانونية المرجوة منه، وفي نهايته سيتم تحديد أوجه القصور التشريعي فيما يخص موضوعه وتوصيات الباحثين لمعالجتها.

فرضيات الدراسة و/ أو أسئلة الدراسة البحثية:

تدور الأسئلة البحثية في هذا البحث حول النقاط التالية:

١. ما هو التفتيش وما هي طبيعته القانونية في الجرائم الإلكترونية؟

٢. ما مدى قابلية البيئة الإلكترونية للتفتيش؟

٣. ما هي خصائص التفتيش في الجرائم الإلكترونية؟

٤. ما هي الشروط الشكلية للتفتيش في الجرائم الإلكترونية؟

محددات الدراسة (ما يدخل فيها وما يخرج عنها)

يقوم هذا البحث ومن خلال محتواه ومضمونه على دراسة الطبيعة القانونية للتفتيش في الجرائم الإلكترونية وخصائصه وشروطه الشكلية. ويخرج منه ما كان متعلقاً بخبرة فنيّة بحته في هذا المجال.

منهج الدراسة:

يرتكز البحث على المنهج الوصفي المقارن، حيث سيتم تحليل النصوص الناظمة لإجراءات التفتيش وبيان الجهة المختصة بذلك ومدى قابلية الأجهزة الالكترونية لإجراء التفتيش مع تحديد الشروط الشكلية والضمانات اللازمة لذلك تحت طائلة البطلان، كل ذلك سيتم بحثه مع إجراء مقارنة مع القانون الفرنسي والألماني والجزائري والفلسطيني ... كلما اقتضى البحث إجراء تلك المقارنة.

المبحث الأول: مفهوم التفتيش في الجرائم الإلكترونية

رافق التطور الكبير في استخدام أجهزة الحاسب الآلي والأجهزة الإلكترونية الأخرى، والتي تقبل الاتصال مع بعضها البعض من خلال شبكات الاتصال سواء المحلية أو العالمية ازديادا في أعداد الجرائم المرتكبة بواسطة هذه الأجهزة من خلال هذه الشبكات(١). وتثير الجرائم الإلكترونية العديد من الإشكاليات وذلك بسبب طبيعتها الفنية بالإضافة إلى القصور التشريعي في مكافحتها. ناهيك عن صعوبة اكتشافها وسهولة إتلاف أدلتها. وحيث أن أدلة الجريمة الإلكترونية تحتاج كغيرها من الجرائم إلى البحث والاستقصاء وجمع المعلومات والقيام بعمليات التفتيش لضبطها؛ فإن هذا يتطلب بالضرورة المعرفة التامة بكيفية تفتيش وسائل إرتكاب هذه الجريمة أو أدواتها وفقاً للنصوص التشريعية الخاصة بها بغية ضبط الأدلة المستساغة قانوناً لإدانة المشتكى عليهم.

إن الجريمة الإلكترونية لا تغدو أن تكون جريمة ذات طابع خاص؛ يتم ارتكابها باستخدام وسائل إلكترونية حديثة تضفي عليها هذه الخصوصية. ويوجد العديد من المفاهيم للجريمة الإلكترونية بسبب الطبيعة الخاصة لها وتختلف هذه التعريفات بحسب العناصر التي يتناولها المفهوم فالبعض منها اعتمد معياراً واحداً في التعريف مثل معيار موضوع الجريمة أو معيار السلوك الجرمي أو الوسيلة المستخدمة لإرتكاب الجريمة أو حتى معيار مرتكب الجريمة ومنها ما اعتمد أكثر من عنصر في تعريف الجريمة الإلكترونية، ولكن حقيقة القول بأن الجريمة الإلكترونية هي جريمة ذاتصفة خاصة لا تتوفر في غيرها من الجرائم وذلك لاعتمادها على وسائل إلكترونية لإرتكابها، تكون مرتبطة مع بعضها البعض بروابط مختلفة من الناحية الفنية متميزة ببرامج وتطبيقات موجودة داخل هذه الوسائل، تتضافر مع بعضها البعض من خلال سلوكها مجريات وخطوط معينة لتحقق النتيجة الجرمية المرجوة منها. وهذه الجرائم إما أن تكون داخل الإقليم الواحد أو أن تكون عابرة للحدود، بالإضافة إلى ما يمتاز به مرتكبو هذه

(١) وبلغ عدد الجرائم الإلكترونية في الأردن في عام ٢٠١٥ (٢٣١٣) قضية وفي عام ٢٠١٦ بلغ عدد القضايا الإلكترونية (٣٦٥٥) وفي عام ٢٠١٧ بلغ عدد القضايا الإلكترونية (٥٧٠٠) وفي عام ٢٠١٨ بلغ عدد القضايا الإلكترونية (٦٥٠٠) وفي عام ٢٠١٩ بلغ عدد القضايا الإلكترونية (٨٤٨٣) من مختلف صور الجرائم الإلكترونية، ونجد من خلال هذه الإحصائية الزيادة المستمرة في أعداد القضايا التي تم التعامل معها من وحدة الجرائم الإلكترونية في إدارة البحث الجنائي ويعود السبب في ذلك إلى ازدياد أعداد مستخدمي وسائل الإتصال والأجهزة الإلكترونية من مختلف الفئات العمرية ومن كلا الجنسين. المصدر وحدة الجرائم الإلكترونية التابعة لإدارة البحث الجنائي، وفي الهند مثلاً بلغ عدد الجرائم الإلكترونية في عام ٢٠١٣ (٧١٧٨٠) جريمة وفي عام ٢٠١٤ (١٤٩٢٥٤) أما في عام ٢٠١٥ فبلغ مجموعها (٣٠٠٠٠٠): وهنا نلاحظ الازدياد المطّرد في أعداد قضايا الجرائم الإلكترونية بمختلف صورها، المصدر

https://dazeinfo.com/6/1/2015/cyber-crimes-in-india-growth-2011-2015-study/

وتم الحصول عليها بتاريخ ٢٠٢٠/٨/٢٣ الساعة ١١:٤٥؛ للمزيد أيضاً أنظر

http://studies.aljazeera.net/ar/issues/2012229132228652960/02/2012/.html

الجرائم من صفات خاصة تؤهلهم للقيام بها، وعليه يأخذ الباحثان بتعريف الجريمة الإلكترونية بأنها: "كل فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبير احترازي يتم ارتكابه من خلال أي وسيلة إلكترونية"(١). وعليه فإن وقوع الجريمة وارتكابها بهذه الصورة الخاصة يضعنا أمام إجراءات التحقيق الإبتدائي ومنها إجراء التفتيش.

إن التفتيش لا يغدو أن يكون وسيلة من وسائل الإثبات المادي في الجرائم بغية اكتشاف مرتكبيها وملاحقتهم واقتصاص حق المجتمع منهم لإرتكابهم هذه الجرائم عند التثبت من ذلك. وهذا التفتيش وسيلة لتحقيق غاية معينة، ولا يكون هذا الإجراء مطلقا على مجمله، فالغاية لا تبرر الوسيلة، وذلك لأن بعض الغايات يمكن الوصول إليها بطرق مختلفة. فالتفتيش في الجرائم الإلكترونية يجب أن يكون مقيداً لما فيه من اطلاع على خصوصيات الغير، فإذا كان هنالك وسائل أخرى تؤدي إلى إثبات وقوع الجريمة، فلا لزوم لإجراء التفتيش، ولذلك سيتم تحديد مفهوم التفتيش في الجرائم الإلكترونية وطبيعته والنصوص الخاصة به والسلطة المختصة بالقيام به في المطلب الأول وفي المطلب الثاني سيتم الحديث عن خصائص التفتيش في الجرائم الالكترونية.

المطلب الأول: تعريف التفتيش في الجرائم الإلكترونية وطبيعته والنصوص الخاصة به والسلطة المختصة بالقيام به

إن التفتيش بوجه عام هو أحد إجراءات التحقيق الابتدائي والذي يهدف إلى معرفة الحقيقة وضبط أدلة الجريمة. ويكون التفتيش إما بشخص المشتبه به أو مسكنه أو مراسلاته المادية أو أغراضه. ومع التطور الذي رافق الحياة فقد أصبحت هذه الصور مختلفة فيما يتعلق بموجودات المسكن أو طريقة إرسال الرسائل وحفظها. والتفتيش بوجه عام يتم جبراً دون الحاجة إلى موافقة صاحب الشأن.

أولاً: تعريف التفتيش في الجرائم الإلكترونية

إن الجريمة الإلكترونية في بعض صورها لا تغدو أن تكون جريمة تقليدية، ولكن تم ارتكابها بوسائل إلكترونية حديثة. حيث يتوجب لإثبات الجريمة وربطها بفاعلها وجود الأدلة المادية على ارتكابها من قبله، وإن مثل هذه الأدلة قد لا تتوافر في الجرائم الإلكترونية، وذلك بسبب عدم وجودها مادياً كما هو الحال في أدلة الجرائم التقليدية. لكنه من المتصور وجود الأدلة المعنوية مثل البيانات والمعلومات الأمر الذي يتطلب معه تحويل هذه الأدلة إن أمكن إلى أدلة مادية من خلال استخراج هذه البيانات أو المعلومات أو استرجاعها.

(١) العناسوة، معن احمد محمد، (٢٠١٨). التفتيش في الجرائم الإلكترونية–دراسة مقارنة، رسالة ماجستير، جامعة عمان الأهلية، عمان، ص ٤٩.

والتفتيش هو: "البحث في مستودع للسر عن أشياء تتعلق بجريمة وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبها"[١]. وخصائصه هي الجبر والإكراه والمساس بحق السر وأخيراً البحث عن الأدلة المادية للجريمة. وهنا يثور التساؤل حول اعتبار تطبيقات الحاسب الآلي والهواتف النقالة والإنترنت والأدلة المستخرجة منها أدلة مادية أم أنها غير مادية. حيث إنه لا يمكن ضبط الأدلة الموجودة داخل هذه الأجهزة أو شبكات الاتصال بالصورة المادية للأشياء والأدوات التي يتم ضبطها في الجرائم العادية[٢].

لم يورد المشرع الأردني في قانون الجرائم الإلكترونية كغيره من المشرعين[٣] تعريفاً خاصاً بالتفتيش في الجرائم الإلكترونية، ولم يتم تحديد مفهومه أيضاً على وجه الخصوص في محكمة التمييز الأردنية بسبب حداثة قانون الجرائم الإلكترونية، ولا يوجد مثل هذا التحديد لدى محكمة النقض المصرية؛ لعدم وجود قانون خاص لديهم يتعلق بالجرائم الإلكترونية.

عرف التفتيش في الجرائم الإلكترونية بأنه: "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه" أو "الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[٤]، وعرفه المجلس الأوروبي بأنه: "إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني"[٥]، وعرف بأنه: "إجراء من إجراءات التحقيق، تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير

(١) د. القهوجي، علي عبد القادر، شرح قانون أصول المحاكمات الجزائية، الكتاب الثاني، منشورات الحلبي الحقوقية، بيروت، ص٢٧٢.

(٢) الحلبي، خالد عياد، (٢٠١١). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، ص ١٥٢.

(٣) ومنهم المشرع العُماني في المرسوم السلطاني الخاص بقانون جرائم تقنية المعلومات؛ المشرع الكويتي في قانون مكافحة جرائم تقنية المعلومات؛ المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ المشرع الفلسطيني في قانون الجرائم الإلكترونية الفلسطيني.

(٤) كما ورد في مؤلف د. الطوالبة، على حسن محمد، (٢٠٠٤). التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث للنشر والتوزيع، إربد، ص١٢-١٣، ويجد الباحثان بأن هذين المفهومين هما مفهومين للتفتيش تم إضافة عبارة "أشياء مادية أو معنوية" لأحدهما، والآخر إضافة عبارة "جهاز الحاسوب أو نظمه أو الانترنت" وهما لكل من د. أحمد فتحي السرور و د. حسن الجوخدار كما ورد في ذات المؤلف ص١١ هامش ٣.

(٥) كما ورد في بحث، الفيل، علي عدنان، (٢٠١٠). إجراءات التحقيق الابتدائي في الجريمة المعلوماتية: دراسة مقارنة، مجلة البحوث والدراسات العربية، العدد (٥٣)، القاهرة، ص٢٦.

مشروعة تكون مرتكبة وتشكل جناية أو جنحه والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها"[١].

ويجد الباحثان بأن التفتيش في الجرائم الإلكترونية هو: "البحث في الأجهزة الإلكترونية والشبكات التي اتصلت بها لارتكاب الجريمة، لضبط الأدلة المعنوية والمادية بداخلها، والتي تثبت وقوع الجريمة، وتوثيق الأدلة المعنوية وإن كانت هذه الأجهزة خاصة وموطن سر أو كانت تابعة لأي جهة أخرى".

ثانياً: الطبيعة القانونية لتفتيش نظم الحاسب الآلي والأجهزة الإلكترونية

تتحدد الطبيعة القانونية للتفتيش بأنه إجراء من إجراءات التحقيق الابتدائي، وليس من إجراءات البحث والإستدلال. ونجد أن الفقهاء انقسموا إلى أربعة اتجاهات حول تحديد الطبيعة القانونية للتفتيش، حيث اعتمد الاتجاه الأول معيار الغاية من التفتيش وهو جمع أدلة الجريمة لتحديد طبيعة التفتيش، في حين ذهب الاتجاه الثاني إلى اعتماد المرحلة التي يجري بها التفتيش لتحديد طبيعته فإن تم بعد تحريك الدعوى فهو إجراء تحقيق ابتدائي إن تم قبلها لا يعتبر كذلك، ويرى الاتجاه الثالث بأن طبيعة التفتيش يحددها من يقوم به فلا يعتبر تفتيش بالمعنى القانوني إلا إذا تولته النيابة العامة، أما الاتجاه الرابع فيجمع بين المعايير الثلاثة في الاتجاهات السابقة، حيث اعتبر التفتيش بأنه إجراء من إجراءات التحقيق، تقوم به السلطة المختصة بالتحقيق الابتدائي، بعد تحريك الدعوى الجزائية، بقصد الكشف عن الحقيقة. وهذاالإتجاه هو ما أخذت به محكمة النقض المصرية[٢].

ثالثاً: النصوص الخاصة بالتفتيش في الجرائم الإلكترونية والسلطة المختصة بالقيام به

أورد المشرع الأردني نصاً خاصاً فيما يتعلق بالتفتيش في الجرائم الإلكترونية حيث جاء بنص المادة (١٣) من قانون الجرائم الإلكترونية على إنه: "أ. مع مراعاة الشروط والأحكام المقررة في

(١) تعريف د. هلالي عبداللاه أحمد كما ورد في العدواني، محمد نافع رشدان، (٢٠١٥).حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي والأردني)، رسالة ماجستير، جامعة الشرق الأوسط، ص٧٥؛ فرغلي، عبدالناصر محمد محمود، د. المسماري، محمد عبيد سيف سعيد، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ١٢-٢٠٠٧/١١/١٤، ص ١٩؛ وذهب البعض إلى تسميته بالتفتيش التقني، وعرفه بأنه: "الدخول التقني المعنوي إلى محتويات جهاز حاسب آلي أو شبكة إتصالات معلوماتية مغلقة أو مفتوحة والبحث فيها فنياً عن أدلة أو معلومات تقنية معينة والخروج بذات الطريقة"؛ المطيري، فيصل عايش، (٢٠١٣). مدى مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، رسالة ماجستير، جامعة عمان العربية، ص ٥.

(٢) د. هلالي أحمد عبداللاه، مرجع سابق، ص٥٢؛ د. علي حسن الطوالبة، مرجع سابق، ص ١٦؛ الشهاوي، قدري عبدالفتاح، (٢٠٠٥). ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، ص١٧، د. سامي الحسيني، مرجع سابق ص٥٥-٥٦.

التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من 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، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص...)، أما المشرع العُماني فلم يورد ضمن نصوص قانون مكافحة جرائم تقنية المعلومات ما يتعلق بإجراءات التفتيش أو السلطة المختصة بها وإنما أورد نصاً يتعلق بصلاحيات المحكمة المتعلقة بالمصادرة والإغلاق في المادة (٣٢) منه، وهو ما ذهب إليه المشرع الكويتي في قانون مكافحة جرائم تقنية المعلومات في المادة (١٣) منه، أما المشرع الفلسطيني في قانون الجرائم الإلكترونية فقد نص في المادة (٣٢) منه على إجراءات التفتيش في الجرائم الإلكترونية والسلطة المختصة بها، حيث نصت: "١. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة...". ومن خلال هذا النص نجد أن المشرع الفلسطيني حدد السلطة المختصة بإجراء التفتيش بالنيابة العامة أصولاً وإنتداباً لمأموري الضبط القضائي ولم يجعل هذا الإجراء من ضمن صلاحيات المحكمة. أما المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الفصل الثالث القواعد الإجرائية تفتيش المنظومات المعلوماتية في المادة (٥) منه حيث حددت هذه المادة حالات الدخول _ولو عن بعد_ والتفتيش التي يجوز القيام بها بموافقة السلطة القضائية المختصة وإمكانية تفتيش نظم داخل البلاد والتعاون في إجراءات التفتيش إذا كانت النظم خارج البلاد وإمكانية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية. ويجد الباحث بأن المشرع الفلسطيني قد أبلى بلاءً حسناً في تحديد السلطة المختصة وإجراءات التفتيش وضماناته[١]. وهنا يثور السؤال حول مدى إمكانية قيام المحكمة بإجراء التفتيش؟ وهل هذا التفتيش هو ذات التفتيش الذي يتم في مرحلة التحقيق الابتدائي؟ مع ملاحظة أن التفتيش إذا تم عن طريقة المحكمة هل يعتبر وسيلة لجمع الأدلة لجريمة ارتكبت؟ وهل يعتبر هذا الدور من الأدوار التي تقوم بها المحكمة بشكل عام؟ كما أنه لم يتم تحديد المحكمة المختصة بالنظر في الجرائم الإلكترونية وفق أحكام قانون الجرائم الإلكترونية.

(١) المرسوم السلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات العُماني المنشور في عدد الجريدة الرسمية رقم (٩٢٩) تاريخ ٢٠١١/٢/٦، قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنه ٢٠١٥، قانون الجرائم الالكترونية الفلسطيني، رقم (١٠) لسنه ٢٠١٨.

وهنا نجيب عن بعض هذه التساؤلات، ابتداءً من تحديد المحكمة المختصة بالنظر في الجرائم المرتكبة وفقاً لنصوص قانون الجرائم الإلكترونية. حيث لم يتم النص على تحديدها بصورة خاصة وبالرجوع إلى قانون محاكم الصلح و قانون تشكيل المحاكم النظامية الأردنيين نجد بأن محاكم الصلح ومحاكم البداية هي المختصة بالنظر في الجرائم الإلكترونية وذلك تبعاً للعقوبة المفروضة على هذه الجرائم[1]. وبحسب نص المادة (١٣) من قانون الجرائم الإلكترونية الأردني فإن التفتيش إما أن يتم بناءً على إذن من المدعي العام المختص أو من المحكمة المختصة. وهنا يثور التساؤل حول إمكانية الإذن بالتفتيش من قبل المحكمة؟ على الرغم من أن التفتيش هو إجراء من إجراءات التحقيق الإبتدائي وليس من إجراءات التحقيق النهائي.

الأصل أن التفتيش يتم مباشرة تجاه جريمة ارتكبت، ويكون القصد منه جمع الأدلة التي تثبت وقوع الجريمة وربطها بشخص مرتكبها، بالإضافة إلى أن التفتيش هو أحد إجراءات التحقيق الابتدائي والأصل أن يتم القيام به قبل تحويل ملف النيابة العامة إلى المحكمة المختصة للسير بإجراءات التحقيق النهائي. فهل يجوز أخذ الإذن من المحكمة للقيام به؟ لا سيما أن إجراءات التحقيق الابتدائي تتوقف منذ لحظة إحالة الملف التحقيقي إلى المحكمة المختصة سواء بقرار الظن أو لائحة اتهام أو ضبط المخالفة.

لم يورد المشرع الجزائي الأردني نصاً محدداً يمنع المحكمة من منح الإذن في إجراء التفتيش، ولكن وبحسب القاعدة العامة بأن التفتيش إجراء من إجراءات التحقيق الابتدائي ويهدف إلى جمع الأدلة في جريمة ارتكبت، وهو من اختصاص النيابة العامة المكلفة في كشف الجرائم وملاحقة مرتكبيها. وكما أنه لا يجوز القياس في النصوص الجزائية. فذهب رأيٌ من الفقه بعدم جواز المحكمة من القيام به. ومن مبررات هذه الطائفة بأن التفتيش شرع في سبيل تحقيق المصلحة العامة، وتغليب مصلحة المجتمع على مصلحة الفرد، وإنه بهذه الصورة يعتبر استثناءً، والاستثناء لا يجوز التوسع في تفسيره، كما أن النصوص الخاصة بالتفتيش وردت بقانون أصول المحاكمات الجزائية في القسم

(١) حيث نصت المادة (٣) من قانون محاكم الصلح على إنه: "تختص محكمة الصلح بالنظر في المخالفات والجنح جميعها والتي لم يعين القانون محاكم أخرى للنظر فيها" قانون محاكم الصلح رقم (٢٣) لسنة ٢٠١٧. وبحسب قانون تشكيل المحاكم النظامية رقم (١٧) لسنه ٢٠٠١، فإن اختصاص المحاكم البدائية وبحسب نص المادة (٥/ب) يكون اختصاصها في الجنح التي تخرج عن صلاحيات محاكم الصلح وكذلك تنظر في الجرائم الجنائية. وكما هو معلوم فان تقسيم الجنايات والجنح والمخالفات يعتمد على العقوبة المفروضة عل كل فعل كما ورد في قانون العقوبات وفقا لأحكام المواد (١٦-١٤). وبتطبيق هذه النصوص على الجرائم الإلكترونية فإن المحاكم النظامية هي المحاكم المختصة في النظر فيها وفقا للعقوبة المقررة لكل صورة من صور الجرائم الإلكترونية إن كانت مخالفة أو جنحة أو جناية.

الخاص بمعاملات التحقيق. وكذلك أضافوا بأن التفتيش لا يحقق الغرض منه إلا إذا تم القيام به في وقت قريب من ارتكاب الجريمة(١).

أما الطائفة الأخرى من الفقه فذهبت إلى القول بجواز إجراء التفتيش من قبل المحكمة أو من قبل أحد أعضائها أو من تنتدبه لهذه الغاية. وحجتهم في ذلك أن المحكمة لها أن تتخذ ما تراه ضرورياً أو مناسباً لكشف الحقيقة(٢). كما أن إجراءات المحاكمة ما هي إلا إجراءات تحقيق نهائي ويصدق عليها وصف التحقيق، ولا عبرة بمكان وجود النصوص ضمن قانون أصول المحاكمات الجزائية، وأنه إذا لم تقم المحكمة بهذا الإجراء فإنها تكون قد حرمت من جمع عناصر الدعوة وفهمها إن استلزم الأمر القيام بالتفتيش(٣).

ويجد الباحثان بأن التفتيش هو إجراء من إجراءات التحقيق الابتدائي وأن المدعي العام هو السلطة المختصة للقيام به بوصفه محققاً أو من ينتدبه لهذه الغاية. واستثناءً فإنه من صلاحيات مساعدي الضابطة العدلية في حالات الجرم المشهود بصفتهم محققين. كما أن الغاية من التفتيش هي جمع الأدلة لجريمة ارتكبت سواء كانت هذه الأدلة أدلة إدانة أم أدلة براءة والتي تقع مسؤولية جمعها وضبطها على المدعي العام الذي يقوم بإجراءات التحقيق الابتدائي قبل إحالة الملف والشخص إلى المحكمة المختصة. كذلك فإن المشرع أحاط التفتيش بمجموعة من الضمانات لما فيه انتهاك لحرمة الشخص الذي يتعرض له ولأسرار حياته الخاصة. وشُرع التفتيش لحماية المجتمع وتغليب مصلحته على مصلحة الأفراد ورفع عنها الحماية القانونية المقررة لها دستورياً وقانونياً. فهل يعقل أن تباح مرة أخرى لضبط دليل جديد؟. ذلك لأن الدليل الذي سيتم البحث عنه إن كان دليل دفاع فإنه بإمكان الشخص المشتكى عليه تقديمه للمحكمة دون الحاجة إلى تفتيش منزله. والثابت وفق نصوص القانون في أصول المحاكمات الجزائية الأردني أن المحكمة مختصة بالسير في إجراءات التحقيق النهائي وأن

(١) د. قدري الشهاوي، مرجع سابق، ص ٢٢؛ د. سامي الحسيني، مرجع سابق، ص ٦٨؛ د. السعيد، كامل، (٢٠٠٨). شرح قانون أصول المحاكمات الجزائية، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر والتوزيع، عمان، ص٤٥٧.

(٢) م (٢/١٦٢) من قانون أصول المحاكمات الجزائية الأردني نصت على: "للمحكمة أنت أمر ولو من تلقاء نفسها أثناء نظر الدعوى وفي أي دور من أدوار المحاكمة فيها بتقديم أي دليل وبدعوة أي شاهدت راه لازماً لظهور الحقيقة"؛ ويقابلها نص المادة (٢٩١) من قانون الإجراءات المصري الجنائية: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى تقديم أي دليل تراه لازما لظهور الحقيقة"؛ يقابلها نص المادة (١٧٩) من قانون الإجراءات الجزائية لدولة الإمارات العربية؛ وأيضا ما جاء بنص المادة (٢٣٥) من قانون الإجراءات الجزائية الجزائري؛ وجاء نص المادة مادة (٢٠٨) من قانون الإجراءات الجزائية الفلسطيني على انه: "للمحكمة بناء على طلب الخصوم، أو من تلقاء نفسها أثناء سير الدعوى أن تأمر بتقديم أي دليل تراه لازماً لظهور الحقيقة، ولها أن تسمع شهادة من يحضر من تلقاء نفسه لإبداء معلوماته في الدعوى".

(٣) د. كامل السعيد، مرجع سابق، ص ٤٥٧؛ د. قدري الشهاوي، مرجع سابق، ص ٢٢-٢٣؛ د. سامي الحسيني، مرجع سابق، ص٦٨-٦٩.

واجبها الحكم في القضية المنظورة أمامها وفقاً لما قدمه الخصوم وتم مناقشته أمامها وما تقتنع به. وليس من واجبها خلق دليل جديد للإدانة. وهذا ثابت ومستقر عليه في قضاء محكمة التمييز الأردنية بصفتها الجزائية(١).

وعليه فإن الباحثين يأخذان برأي من ذهبوا إلى عدم جواز قيام المحكمة_ القاضي الجزائي_ ابالتفتيش في مرحلة التحقيق النهائي. وأن نص المادة (٢/١٦٢) من قانون أصول المحاكمات الجزائية الأردني جاءت في سبيل الاستيضاح من الشهود لإظهار الحقيقة، وذلك بدلالة ذات الإجراء في إجراءات المحاكمة في القضايا الجنائية حسب نص المادة (١/٢٢٦) من ذات القانون(٢). وعليه تكون السلطة المختصة بإجراء التفتيش في الجرائم الإلكترونية هي سلطة التحقيق الإبتدائي. مع إمكانية الإستعانة بالخبراء وأصحاب الخبرة الفنية في إجراءات التفتيش نظراً إلى خصوصية هذه الجريمة(٣).

الفرع الثاني: خصائص التفتيش في الجرائم الإلكترونية

يتميز التفتيش القانوني بمجموعة من الخصائص التي تفرده عن غيره من الأعمال التي قد تشتبه معه في بعض إجراءاتها وتسميتها، وهذه الخصائص مستمدة من النصوص القانونية المتعلقة بالتفتيش وإجراءاته، والتفتيش في الجرائم الإلكترونية لا يغدو أن يكون تفتيشاً قانونياً وفقاً لطبيعته. وسيتم بحث خصائص التفتيش على النحو التاليأولا الجبر والإكراه؛ ثانيا المساس بحق السر وثالثاً البحث عن الأدلة المادية للجريمة (غايته).

(١) حيث جاء بقرارها رقم (٤٩٠) لسنة ٢٠٠٤، هيئة خماسية بتاريخ ٢٠٠٤/٦/٦ انه: "إذا لم تقم النيابة بإجراء الخبرة أو إستكتاب المتهم لبيان فيما إذا كان التوقيع المنسوب للمشتكية على المحضر التنفيذي قد ثبت بخط يد المتهم أم لا، وإنما إكتفت بإجراء الخبرة بإستكتاب المشتكية فقط حيث ثبت أن التوقيع لا يعود للمشتكية ولم يكتب بخط يدها، فإن النيابة تكون قد قصرت في التحقيق والتحري عن الدليل ولا يرد القول أنه كان على المحكمة أن تتدارك ذلك النقص باستعمال صلاحياتها المنصوص عليها في المادة (٢٢٦) من قانون أصول المحاكمات الجزائية باستكتاب المتهم لبيان فيما لو كان التوقيع على المحضر التنفيذي بخط يده أم لا، لأن ذلك فيه خلق بينة ضد المتهم وليس للمحكمة أن تخلق دليلاً وأن ذلك يخرج المحكمة عن حيادها"، للمزيد أيضاً أنظر قراراتها ذوات الأرقام (٢٠١٠/٢٦١ هيئة خماسية، تاريخ ٢٠١٠/٣/٢، وقرارها ٢٠٠٩/١٨٤٦ تاريخ ٢٠١٠/٣/٢٢، وقرارها رقم ٢٠٠٩/١٨٢٣ هيئة خماسية تاريخ ٢٠١٠/١/١٤، وكذلك قرارها رقم ٢٠٠٧/١٠٠٢، هيئة خماسية تاريخ ٢٠٠٧/٩/٤.

(٢) حيث نصت المادة (١/٢٢٦) على انه: "للمحكمة أثناء النظر في الدعوى أن تستدعي من تلقاء نفسها أي شخص لاستماع أقواله كشاهد إذا رأت أن ذلك يساعد على إظهار الحقيقة ... ".

(٣) خالد عياد الحلبي، مرجع سابق، ص ١٥٥-١٥٦؛ د. العقيدة، محمد أبو العلا، ورقة عمل مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، تاريخ ٢٦/٤-٢٠٠٣/٤/٢٨، الإمارات العربية المتحدة، عبر الرابط:

http://www.th3 professional.com/2010/11/blog-post_5845.html

أولاً: الجبر والإكراه

إن إجراءات التحقيق الابتدائي[١] التي يقوم بها المدعي العام وفقاً لصلاحياته المنصوص عليها تشريعياً في قانون أصول المحاكمات الجزائية لم يجعل فيها المشرع خياراً لصاحب الشأن بالرضا أم عدمه، وعليه فإن إجراءات التحقيق الابتدائي التي يقوم بها المدعي العام تمتاز بصفة الجبر والإكراه والتعرض القانوني لحرية الشخص–المشتكى عليه– ومسكنه، وهذه الخصيصة تتوافر عند إجراء التفتيش في الجرائم الإلكترونية فلا يشترط موافقة المشتكى عليه عند تنفيذه.

ثانياً: المساس بحق السر

يمتاز التفتيش أيضاً بأنه يمس حق المشتكى عليه بالاحتفاظ بأسراره الخاصة، وتعتبر الأجهزة الإلكترونية وما يرتبط بها من أدوات أو وسائل وما تحتويه من بيانات ومعلومات أو صور في داخلها موطن سر لمالكين هذه الأجهزة أو الأدوات أو الوسائل وبغض النظر عن طبيعتها أو أماكن حفظها وعليه يكون تفتيش هذه الأجهزة أو الأدوات أو الوسائل فيه مساس بحق السر لشخص المشتكى عليه.

ثالثاً: البحث عن الأدلة المادية للجريمة

إن الغاية من إجراءات التحقيق الإبتدائي هي إثبات وقوع الجريمة وضبط مرتكبيها وإحالتهم إلى الجهات القضائية المختصة؛ لإيقاع العقوبات بحق من يثبت ارتكابه لها.

ويتوجب أن تكون الغاية من تفتيش الأجهزة الالكترونية أو الأدوات أو الوسائل المستخدمة بارتكاب الجريمة الالكترونية ضبط الأدلة الموجودة داخلها أو في أماكن تخزينها وذلك بعد ضبطها بصورتها المادية التي تمكن المحكمة من الاطلاع عليها وتقدير مدى نجاعتها في إصدار حكمها.

المبحث الثاني: مدى قابلية نظم الحاسب الآلي والانترنت للتفتيش والشروط الشكلية للتفتيش في الجرائم الإلكترونية

وحيث أنالجريمة الإلكترونية يتم إرتكابها باستخدام جهاز الحاسب الآلي أو الأجهزة الإلكترونية الأخرى من خلال شبكات الاتصال المختلفة وتكون الأدلة موجودة بداخلها، أو أن تستهدف هذه الجريمة الأجهزة الإلكترونية ذاتها[٢]. فإنه يتوجب علينا معرفة مدى قابلية نظم الحاسب الآلي

(١) نص قانون أصول المحاكمات الجزائية الأردني في الكتاب الأول على تحديد الضابطة العدلية ووظائفها ومنها: تلقي الإخبارات والشكاوى، الاستجواب، التفتيش، التوقيف،....

(٢) وزارة العدل الأمريكية، مكتب برامج العدالة، المعهد الوطني للعدالة، ص١، ٢٠٠١.
Electronic Crime Scene Investigation: A Guide for First Responders

والإنترنت للتفتيش في المطلب الأول. وفي المطلب الثاني سيتم بحث الشروط الشكلية للتفتيش في الجرائم الإلكترونية.

المطلب الأول: مدى قابلية نظم الحاسب الآلي والإنترنت للتفتيش

أولاً: مدى قابلية نظم الحاسب الآلي والأجهزة الإلكترونية للتفتيش

لا بد في البداية من تحديد مفهوم جهاز الحاسب الآلي ومكوناته وأدواته، لنتمكن من تحديد قابليته للتفتيش وعرف بأنه: "جهاز إلكتروني بإمكانه ترجمة أوامر لإدخال البيانات أو إخراج معلومات وإجراء عمليات حسابية ومنطقية، ويقوم بالكتابة على أجهزة الإخراج أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل لوحة المفاتيح أو استرجاعها من خلال المعالجة المركزية التي تقوم بإجراء العمليات الحسابية والعمليات المنطقية، وبعد معالجة البيانات تكتب على أجهزة الإخراج كالطابعات أو شرائط التخزين"[1]. ونجد بأن هذا التعريف اشتمل على جميع العمليات التي يقوم بها الحاسب الآلي بالإضافة إلى مكوناته وأجزائه الرئيسية. وعليه فإن جهاز الحاسب الآلي يتكون من مكونات مادية (Hardware) ومكونات معنوية (Software) وإمكانية ارتباطه بشبكة الإنترنت. وفي الحقيقة إن تكوين الحاسب الآلي والأجهزة الإلكترونية التي تشابهه من هذه المكونات يجعلها محلاً قابلاً للتفتيش وضبط الأدلة التي تفيد في اكتشاف الجريمة. وتعتبر الأجهزة الإلكترونية بوجه عام موطن سر للأشخاص والشركات فهم يستخدمون الأوعية الخاصة بهذه الأجهزة لتخزين البيانات الخاصة بهم عليها وذلك بغية المحافظة عليها والاحتفاظ بها وعدم تركها عرضة للتداول بين أيدي الآخرين.

إن التفتيش في هذه المكونات يكون بقصد البحث عن الأدلة غير المادية المخزنة داخل الجهاز الإلكتروني، أو المخزنة في وسائل التخزين الخارجية أو الأقراص المدمجة (CD) أو أي وحدة يمكن استخراج الدليل الإلكتروني منها بالإضافة إلى البحث في النظم المعلوماتية. وهذا التفتيش يكون على جهاز الحاسب الآلي وحده أو على عدة أجهزة أخرى متصلة به من خلال شبكة الإتصال. وهنا تثور التساؤلات حول قانونية ضبط المعلومات والبيانات الموجودة داخل هذه الأجهزة أو الأدوات أو الشبكات؟ وهل يعتبر مثل هذا الإجراء تفتيشاً بالمعنى المقصود قانونا؟ وهل تنطبق عليه قواعد التفتيش وشروطه؟ ونجد هنا بأن هذا التفتيش يمتاز بخصوصية تتطلب الاستعانة بالخبرة الفنية عند إجرائه. وبالتالي فإن التفتيش في الجرائم الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان

(١) د عزت، فتحي محمد أنور، (٢٠١٠). الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، ص ٢٨.

عن البيانات والأدلة المطلوبة. كما أن الأدلة التي يتم ضبطها من الممكن أن تكون مخزنة في الجهاز الإلكتروني وملحقاته أو أن تكون على شكل مدخلات أو مخرجات منه[١].

أ- مدى قابلية مكونات الأجهزة الإلكترونية المادية للتفتيش

إن الدخول إلى الأجهزة الإلكترونية التي تحتوي معالج بيانات (Processor) والذي يقوم بتحويل البيانات إلى أرقام داخل الحاسب الآلي، الأجهزة الشخصية، (Laptop, ipad)، كاميرا الفيديو، والكاميرا الرقمية (Digital Camera)، الهواتف الذكية وغيرها بقصد البحث داخل هذه الأجهزة وأجزائها المختلفة عن أدلة مرتبطة بجريمة إلكترونية وقعت بقصد اكتشاف هذه الجريمة وربطها بمرتكبها أو مرتكبيها؛ فلا خلاف بأنه تفتيش بالمعنى المقصود قانوناً وفقاً للتشريعات الجزائية.

لذلك نجد بأن تطبيق القواعد العامة في التفتيش بشكل عام على التفتيش في الجرائم الإلكترونية هو أحد ضمانات التزام الجهات المختصة بالقيام به بالمحافظة على تطبيق القواعد القانونية الخاصة بالتفتيش تحت طائلة البطلان في حال عدم تقيدها بها.

ويثور التساؤل في حالة تفتيش المساكن والأماكن الخاصة فيما إذا كانت أجهزة الحاسب الآلي أو الأجهزة الإلكترونية مرتبطة بأجهزة أخرى أم لا؟ أو أنها موجودة داخل هذا المسكن أو المكان الخاص وحدة؟ وفي الحقيقة إن الصورة الثانية لا تثير جدلا حيث يجب ضبط جميع الأجهزة الإلكترونية المستخدمة في ارتكاب الجريمة الإلكترونية الموجودة داخل هذا المكان المحدد. وأما في الصورة الأولى فإنها تمثل تعدد الأماكن والمساكن المراد تفتيشها وذلك بسبب ارتباط هذه الأجهزة بنهايات طرفية موجودة في مكان آخر وإمكانية وجود أدلة داخلها[٢].

(١) محمد نافع فالح العدواني، مرجع سابق، ص ٧٥- ٧٦؛ الكبيجي، بهاء فهمي، (٢٠١٣).مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير، جامعة الشرق الأوسط، ص ١١٤؛ د. هلالي عبداللاه احمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص ٧١-٧٣؛ د العبيدي، أسامة بن غانم، التفتيش عن الدليل في الجرائم المعلوماتية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، ٢٠١٣/١١، المجلد (٢٩)، العدد (٥٨)، ص٨٨.

(٢) منها صوره ارتباط الأجهزة الإلكترونية مع بعضها البعض عن طريق الربط من خلال الشبكة المحليةسواء باستخدام الكيبلات المعدّة لهذه الغاية أو من خلال ربط هذه الأجهزة لاسلكيا. وهذه الأجهزة ترتبط مع بعضها البعض في صورة (العميل/ الخادم) بحيث يستطيع الجهاز العميل طلب المعلومات من الجهاز الخادم ويتم تبادل المعلومات فيما بينها، والحاسب أو جهاز الخادم يكون هو المزود بهذه المعلومات أو الوثائق أو يكون وسيلةً لتوزيعها بين باقي الأجهزة المتصلة به. أو أن يكون الربط أكثر انتشاراً من خلال الشبكة واسعة النطاق أو الشبكة الممتدة، للمزيد راجع أيضاً د. موسى، مصطفى محمد، (٢٠٠٨). التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، ص ٥٤-٥٥؛ د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص ٣٧-٣٨؛ د. علي حسن الطوالبة، مرجع سابق، ص ٣٤؛ المناعسة، أسامة، الزعبي، جلال، (٢٠١٧). جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، ٣٨؛ د. فتحي محمد أنور عزت، مرجع سابق، ص ٤٠؛ د. هلالي عبداللاه أحمد، جرائم الحاسب والانترنت، مرجع سابق، ص ١٠٥-١١٠؛ علي عدنان الفيل، مرجع سابق، ص ٢٧-٢٨؛ بهاء فهمي الكبيجي، مرجع سابق، ص ١١٦-١١٧؛ د. حازم محمد حنفي، مرجع سابق، ص ٤٢-٤٣؛ خالد عياد الحلبي، مرجع سابق، ص ١٥٨-١٥٩؛ د. سقف الحيط، عادل عزام، (٢٠١٥). جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ص ٢٤٣-٢٤٤.

ب. مدى قابلية مكونات الأجهزة الإلكترونية المعنوية للتفتيش

إن تفتيش الأماكن أو المساكن أو الأشخاص أو المراسلات المكتوبة أو الأمتعة والأشياء. بشكل عام وتقليدي لا يثير أي خلافات جدلية بين الفقهاء كالتي يثيرها موضوع تفتيش المكونات المعنوية (Soft ware) لجهاز الحاسب الآلي أو الأجهزة الإلكترونية حيث ذهب رأي إلى جواز تفتيش المكونات المعنوية والبيانات الإلكترونية بمختلف أشكالها. وذهبت بعض التشريعات إلى النص صراحة على تفتيش مكونات الحاسب الآلي[١]. وذهب اتجاه آخر إلى أن المفهوم الخاص بالمكونات المعنوية والبيانات الإلكترونية لا ينطبق عليه المفهوم المادي الملموس في إجراء التفتيش التقليدي وذلك لأن هذه المكونات والبيانات ليست بشيء ملموس. ويرى الفقهاء في هذا الإتجاه إلى ضرورة معالجة القصور التشريعي بالنص صراحة على أن التفتيش في الأجهزة الإلكترونية يشمل المواد المعالجة عن طريق هذه الأجهزة أو بيانات الحاسب الآلي[٢].

أما موقف المشرع الأردني فقد نصت المادة (١٣) من قانون الجرائم الإلكترونية على أنه: "... يجوز لموظف الضابطة العدلية بعد الحصول على موافقة المدعي العام أو المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه في إرتكاب 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 لإرتكاب أي من تلك الجرائم...". وهو أمر محمود يوقف الإجتهادات الفقهية المتعلقة بمدى خضوع المكونات المعنوية للأجهزة الإلكترونية للتفتيش حيث نص المشرع الجزائي الأردني على جواز مثل هذا التفتيش[٣]. وهو ما ذهب إليه المشرع الجزائري في قانون

---

(١) حيث تعطي المادة (٢٥١) من قانون الإجراءات الجنائية اليوناني لسلطات التحقيق أمكانية القيام به: "بأي شيءيكون ضرورياً لجمع الدليل وحمايته". ويفسر الفقه اليوناني عبارة"أي شيء" بأنها تشمل البيانات المخزنة أو المعالجة الكترونياً كما ورد في بحث د. أسامة بن غانم العبيدي، مرجع سابق، ص ٨٩؛ د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب، مرجع سابق، ص٧٤ و٨٢-٨٣، تم الإشارة إلى ذات رقم المادة لدى محمد نافع فالح العدواني، مرجع سابق، ص ٧٨؛ علي عدنان الفيل، مرجع سابق، ص ٢٩.

(٢) للمزيد انظر د. هلالي عبداللاه احمد، تفتيش نظم الحاسب، مرجع سابق، ص٧٥-٧٦؛ بهاء فهمي الكبيجي، مرجع سابق، ص ١١٧؛ علي عدنان الفيل، مرجع سابق، ص ٢٩؛ د. حازم محمد حنفي، مرجع سابق، ص ٤٣-٤٨.

(٣) مع العلم بأن التعديل المطروح في مسودة قانون الجرائم الإلكترونية إضافة عبارة "والتفتيش" بعد كلمة الدخول في المادة (١٣) منه وبذلك تصبح: "...الدخول والتفتيش إلى أي مكان تشير الدلائل...". كذلك فقد نصت المادة (١٢) من قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (٣٠) لسنة ٢٠١٠ الذي حل محله قانون الجرائم الإلكترونية حيث جاء فيها: "كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم..."وفي حقيقة الأمر فإن تفتيش المكونات المعنوية للأجهزة الإلكترونية وقبل إصدار أي من هذين القانونين كان متصوراً بموجب نصوص قانون أصول المحاكمات الجزائية حيث أوردت المادة (٨٧) منه ونصت على انه: "... ويضبط أو يأمر بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة ...". ونجد في هذا النص أن المشرع أورد عبارة الأشياء (Things)، والأشياء جمع شيء والشيء هو الموجود، والشيء ما يتصور ويخبر عنه كما ورد في المعجم الوسيط، الجزء الأول، صفحه ٥٢١. والشيء هو: "اسم لأي موجود ثابت متحقق يصبح أن يتصور ويخبر عنه سواء كان حسياً أم معنويا" كما ورد في تطبيق معجم المعاني، وموجود أيضا على الرابط التالي على شبكة الانترنت: www.almaany.com/ar/dict/ar-arشيء/

الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لسنه ٢٠٠٩، حيث نصت على ذلك المادة (٥) منه، وكان هذا أيضاً موقف المشرع الفلسطيني حيث نصت المادة (٣٣) من قانون الجرائم الإلكترونية لسنة ٢٠١٧.

ثانياً: مدى قابلية شبكات الإنترنت للتفتيش

تلعب شبكات الإتصال المختلفة ومنها شبكة الإنترنت الدور الأكثر أهمية في جعل الجريمة الإلكترونية جريمة عابرة للحدود، كما أنها وسيلة الربط بين الأجهزة الإلكترونية المتواجدة في أماكن مختلفة سواء كانت داخل النطاق الإقليمي للدولة أو كانت خارج هذا النطاق وشبكات الإتصال إما أن تكون شبكة انترانت (Intranet) أو أن تكون شبكة اكسترانت (Extranet) أو تكون شبكة الإنترنت (Internet). وهذه الشبكات تربط جهازين أو أكثر بعضهما ببعض، وهذا الإتصال إما أن يكون سلكياً أو لاسلكياً أو عن طريق الهاتف.

إن تفتيش شبكات الإتصال المرتبطة بالأجهزة الإلكترونية والمراقبة الإلكترونية لأنظمة المعلومات، يجب أن يتم وفقاً للقواعد القانونية المنصوص عليها لإجراء التفتيش، لما فيه من تعرض لحرية وخصوصية الأشخاص أو الأشخاص الاعتباريين الذين تتصل بهم هذه المعلومات، وذلك لأن استخدام شبكات الإتصال تمثل وسيلة توزيع للعديد من البيانات بين المستخدمين. وهذه البيانات يتم توزيعها على أكثر من مستوى سواء أكان وطنياً أمْ دولياً. الأمر الذي يترتب عليه زيادة الصعوبات في إجراءات التحقيق والتفتيش والضبط المتعلق بالجرائم الإلكترونية.

وهذه البيانات المراد ضبطها لإثبات وقوع الجريمة الإلكترونية من المتصور عدم وجودها في المكان الذي يتم تفتيشه بسبب انتقالها إلى مكان آخر من خلال شبكة الإتصالات. ومما يزيد صعوبة الأمر هو وجود هذه البيانات خارج الحدود الجغرافية للدولة. الأمر الذي يتطلب تعاوناً دولياً في هذا المجال[١].

بناءً على ما سبق، فإن هنالك ثلاثة احتمالات تتعلق بشبكات الحاسب الآلي وهي:

أولاً: اتصال الجهاز الإلكتروني للمشتبه به مع جهاز إلكتروني آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

(١) د. علي حسن الطوالبة، مرجع سابق، ص٤٢-٤٣؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص٩٠-٩١؛ د. حازم حنفي، مرجع سابق، ص٤٨؛ خالد عياد الحلبي، مرجع سابق، ص١٦٣؛ علي عدنان الفيل، مرجع سابق، ص٣٠-٣١.

نجد في هذه الصورة بأن هنالك طرفين في هذا الارتباط أحدهما يعود لشخص المشتبه به والآخر لا يعود له ومن المتصور أن يعود لنفس الشخص أيضاًفي مكانين مختلفين[١]. والأصل في التفتيش أنه لا يتم إلا بموجب مذكرة من السلطة المختصة به ويكون هذا الأذن بالتفتيش محدداً ولغاية محددة ومكان محدد، إن صورة إجراء التفتيش لنفس شخص المشتبه به ومكان سكنه وما يحتويه من شبكة اتصال داخلية وأجهزة إلكترونية متعددة لا تثير أي مسائل خلافية. وهنا يثور التساؤل حول إمكانية إمتداد الحق في التفتيش ليشمل الطرف الآخر _جهاز إلكتروني أو نهاية طرفية (Terminal)_ المملوك لغير شخص المشتبه به؟

وحيال هذا التساؤل نجد بأن المشرع الألماني في قانون الإجراءات الجنائية نص في المادة (١٠٣) منه على التفتيش في مواجهة الأشخاص الآخرين–حيث نصت المادة (١٠٢) منه على التفتيش في مواجهة المشتبه به_. حيث جاء في مضمونها بأن تفتيش أشخاص غير شخص المشتبه به يكون مسموحاً به لضبط المشتبه به أو لمتابعة الأدلة الخاصة بالجريمة أو لضبط أشياء محددة. وذهب الفقه الألماني إلى القول بجواز امتداد التفتيش إلى السجلات والبيانات الموجودة في موقع آخر[٢]. وذهبت تشريعات أخرى للنص على جواز إمتداد التفتيش في الجرائم الإلكترونية إلى أنظمة وأجهزة أخرى ومنها منها قانون الإجراءات الجنائية البلجيكي حيث نصت المادة (٨٨) منه على أنه: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين: أ. إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث. ب. إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث"[٣]،أما المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد نص في المادة (٥) منه على أنه: "... إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها، انطلاقاً من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة

(١) كأن يستخدم شخص المشتبه به هاتفه الخلوي الذكي لإرسال مادة أو بيانات معينة من خلال بريده الالكتروني أو أي تطبيق آخر إلى جهاز الحاسب الآلي العائد له والذي يتم استخدامه من داخل منزله من قبل أشخاص آخرين.

(٢) نص قانون الإجراءات الجنائية الألماني باللغة الألمانية واللغة الانجليزية موجود عبر الرابط
www.gesetze-im-internet.de/english-stpo/english-stpo.html

(٣) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب، ص٧٧؛ د. حازم حنفي، مرجع سابق، ص٤٨؛ د. عادل عزام سقف الحيط، مرجع سابق، ص٢٤٠ و ٢٤٥؛ خالد عياد الحلبي، مرجع سابق، ص١٦٤–١٦٥؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص٩١–٩٢؛ علي عدنان الفيل، مرجع سابق، ص٣١–٣٢؛ بهاء فهمي الكبيجي، مرجع سابق، ص١١٨؛ د. علي حسن الطوالبة، مرجع سابق، ص٤٣؛ صفاء حسن نصيف، مرجع سابق، ص ٢٧٠.

القضائية المختصة مسبقاً بذلك... إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل ..."[١].

ثانياً: اتصال الجهاز الإلكتروني للمشتبه به مع جهاز إلكتروني آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

في هذا الاحتمال نجد صعوبة في إجراء التفتيش المتعلق بشبكة الاتصال التي جمعت بين جهاز المشتبه به وجهاز آخر أو نهاية طرفية خارج البلاد. وذلك لصعوبة القيام بهذا التفتيش من الناحية المادية، وكذلك من الناحية القانونية وسيادة الدول وعدم جواز إجراء التفتيش لديها لعدم قانونية هذا الإجراء، كما أن الدليل الذي يتم ضبطه يفقد الصفة الشرعية في ضبطه وبالتالي فقدانه لحجية الإثبات أمام المحاكم الوطنية؛ لأن وسيلة الحصول عليه لم تكن مشروعة قانوناً.

يقوم مرتكبو الجريمة الإلكترونية بتخزين البيانات المتعلقة بجرائمهم في أنظمة ووسائل معلومات خارج حدود الدولة عن طريق شبكات الإتصالات ويكون هذا الإجراء فيه تعطيل لكشف غموض هذه الجريمة وعرقلة سلطات التحقيق من جمع وضبط هذه الأدلة.

وللقيام بهذا الولوج أو الدخول إلى نظام معلومات خارج حدود الدولة فإن القيام به لا يكون بموجب إذن من المحقق _المدعي العام_لأنه غير مختص بإعطاء إذنالتفتيش لمكان يقع خارج منطقة إختصاصه وولايته، كما أن الشروط الخاصة بالتفتيش تختلف من دولة إلى أخرى وكذلك قواعد الاختصاص. ويتوجب أن يتم تنظيم هذا الإجراء تشريعياً وفقاً لاتفاقيات دولية يتم الاتفاق فيها على جواز هذا الولوج. وهذه الاتفاقيات من الممكن أن تكون دولية على مستوى دول العالم أو أن تكون على مستوى إقليم أو منطقة معينة أو اتحاد دول معينة[٢].

ونتيجة لهذه الحاجة تم تنظيم عدد من الاتفاقيات الدولية المتعلقة بمكافحة الجريمة الإلكترونية ومنها الاتفاقية الأوروبية بشأن الجرائم المعلوماتية (اتفاقية بودابست) حيث نصت المادة (٣٢) منها على أنه: "الدخول عبر الحدود على بيانات مخزنة، عن طريق الموافقة أو حيثما تكون متاحة علناً يجوز لأي طرف دون تفويض من أي طرف آخر: أ. الدخول على بيانات حاسوب مخزنة علناً

(١) قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجزائري، رقم (٠٩-٠٤) لسنة ٢٠٠٩.

(٢) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص٧٨؛ د. عادل عزام سقف الحيط، مرجع سابق، ص٢٤٦؛ د. حازم محمد حنفي، مرجع سابق، ص٥٠؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص٩٢-٩٣؛ علي عدنان الفيل، مرجع سابق، ص٣٢-٣٣؛ بهاء فهمي الكبيجي، مرجع سابق، ص١١٩-١٢٠؛ صفاء حسن نصيف، مرجع سابق، ص ٢٧١.

(مصدر مفتوح)، بغض النظر عن مكان تواجد البيانات جغرافياً. ب. الدخول على بيانات حاسوب مخزنة، موجودة في طرف آخر، أو أن يتلقاها عن طريق نظام حاسوب في إقليمه، وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية، من الشخص الذي له السلطة القانونية في الكشف عن البيانات لذلك الطرف، من خلال نظام الحاسوب المذكور"، ونصت المادة (٢٣) من الاتفاقية الأوروبية في القسم الثالث منها على المبادئ العامة المتعلقة بالتعاون الدولي على أنه: "يتعاون الأطراف، بعضهم مع بعض، .... من خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية، ومن خلال الترتيبات المتفق عليها بمقتضى التشريعات الموحدة والمتبادلة بالمثل، والقوانين الوطنية، لأقصى درجة ممكنة، لأغراض إجراءات التحقيقات التي تتعلق بجرائم نظم الحاسوب وبياناته، أو من أجل تجميع أدلة الجريمة الجنائية بشكل إلكتروني"[١].

وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٢ والتي نصت المادة (٢٦) منها على: "١. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: أ. تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. ب. بيئة أو وسيط تخزين معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. ٢. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (١/أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى"[٢].

كما نصت ذات الاتفاقية في المادة (٣٢) منها على المساعدة بين الدول الأطراف حيث جاء فيها: "١. على جميع الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيق أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم ..."[٣]، ونجد بأن المادة (٢٦) منها وضحت الإجراءات التي يجب على الدول الموقعة عليها الالتزام بها وضرورة إجراء التعديلات التشريعية على قوانينها الداخلية بما يضمن تطبيقها. وفي نص هذه المادة

(١) سميت بهذا الاسم لأنه تم التوقيع عليها في مدينة بودابست بتاريخ ٢٠٠١/١١/٢٣. ووقعت عليها ست وعشرون دولة من مجلس أوروبا بالإضافة إلى الولايات المتحدة وكندا واليابان وجنوب إفريقيا؛ د. عادل عزام سقف الحيط، مرجع سابق، ص٣٨٢و ص٥٣٠-٥٣٢؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص٩٣؛ علي عدنان الفيل، مرجع سابق، ص٣٣؛ د. حازم محمد حنفي، مرجع سابق، ص٥٠.

(٢) وقعت هذه الاتفاقية في القاهرة بتاريخ ٢٠١٠/١٢/٢١.

(٣) من الجدير بالذكر أن المملكة الأردنية الهاشمية صادقت على هذه الاتفاقية بموجب قانون التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (١٩) لسنة ٢٠١٢ والمنشور في عدد الجريمة الرسمية رقم (٥١٦٢) ص (٢٥٨٠) تاريخ ٢٠١٢/٦/١٧، وبلغ عدد الدول العربية الموقعة على هذه الاتفاقية (١٨) دولة وهي: الأردن، الإمارات العربية المتحدة، البحرين، تونس، الجزائر، المملكة العربية السعودية، السودان، سوريا، العراق، سلطنة عُمان، فلسطين، قطر، الكويت، ليبيا، مصر، المغرب، موريتانيا واليمن.

نجد أن الفقرة الأولى نصت على التفتيش في الجريمة الإلكترونية سواء في تقنية المعلومات أم أجزاء منها أم في بيئة أم في وسيط تخزين، وفي فقرتها الثانية نصت صراحة على توسيع نطاق التفتيش متى كان ذلك ممكناً من الناحية الفنية والقيام بإجراءات التفتيش لضبط الأدلة الخاصة بالجريمة الإلكترونية.

واختلفت التشريعات من حيث النص على امتداد التفتيش في الجرائم الإلكترونية إذا كان الجهاز مرتبطاً بجهاز آخر خارج الحدود الإقليمية للدولة، حيث ذهب المشرع الهولندي في مشروع قانون جريمة الحاسب إلى التصريح لجهات التحقيق بإجراء التفتيش داخل الأماكن بما يتضمن تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دول أخرى بشرط أن يكون هذا التدخل والتفتيش مؤقتاً وأن تكون البيانات التي يتم التفتيش عنها لازمةً لإظهار الحقيقة(١).

أما المشرع الفرنسي فذهب إلى تعديل قانون الإجراءات الجنائية بهدف إجراء التفتيش بالسرعة الممكنة لضبط الأدلة الإلكترونية في الجرائم الإلكترونية حيث نصت المادة (٢/١٧) من قانون الأمن الداخلي رقم (٢٣٩) لسنة (٢٠٠٣) على أنه: "لمأمور الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى لو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية"(٢). ونص المشرع الجزائري على جواز امتداد التفتيش داخل الحدود الوطنية وعدم جوازه خارجها، وإن الحصول على المعلومات والبيانات المخزنة خارج الإقليم يتم من خلال طلب المساعدة من السلطات الأجنبية المختصة طبقاً للمعاهدات الدولية فيما يتعلق بالجرائم الإلكترونية(٣). أما المشرع الأردني فلم يتطرق لمثل هذه الفرضية في قانون مكافحة الجرائم الإلكترونية ولا في قانون أصول المحاكمات الجزائية(٤).

ويجد الباحثان أن السماح بامتداد التفتيش إلى نظم خارج حدود الإقليم أو إلى شبكات اتصال خارجه يشكل خرقاً لسيادة الدول وانتهاكاً لحريات الأفراد فيها. كما أن مدى قانونية هذا الإجراء موضع نظر لأنه صدر من شخص لا يملك الصلاحية في إصداره وذلك لعدم امتداد اختصاص المدعيين العامين المحليين خارج حدود الدولة، ومن الثابت قانوناً وفقهاً وقضاءً شرط الاختصاص المكاني وهو

(١) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص٧٨؛ د. علي حسن الطوالبة، مرجع سابق، ص٤٣، حيث أورد نص المادة (١٢٥) (J) من ذات القانون:"تفتيش المسكن يمكن أن يمتد 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 تسجيلها"؛ د. عادل عزام سقف الحيط، مرجع سابق، ص٢٤٦؛ خالد عياد الحلبي، مرجع سابق، ص١٦٥؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص٩٣؛ بهاء فهمي الكبيجي، مرجع سابق، ص١٢٠.

(٢) كما ورد في مؤلف د. حازم محمد حنفي، مرجع سابق، ص٥١.

(٣) كما ورد في المادة (٥) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجزائري.

(٤) وكان هذا أيضاً شأن المشرع الجزائي الفلسطيني والكويتي والعُماني والسعودي.

أحد الشروط الموضوعية لإجراء التفتيش سواء أكان من يقوم به المدعي العام بصفته محققاً أو من يقوم به من ينتدبه لهذه الغاية ضمن منطقة اختصاصه [١].

وبالتالي فإن ما ينتج عن هذا الإجراء الباطل من نتائج تتمثل بضبط أدلة مخزنة على شبكة الاتصال أو في جهاز آخر خارج حدود ولاية المدعي العام وخارج حدود إختصاصه، يعتبر إجراءً باطلاً ولا يعول عليه في قضاء الحكم.

ثالثاً: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي

إن التنصت وأشكال المراقبة الإلكترونية يوجد بها تعرض وانتهاك لحرية الحياة الخاصة بالأفراد، إذا تمت دون ضوابط قانونية. وهذا الإجراء يثير جدلاً قانونياً حول جوازه أو عدمه. إلا أن معظم التشريعات أجازته وفق ضوابط قانونية معينة. حيث يزيل المشرع الحماية الجزائية عن هذا الحق ويجعله مبرراً إذا ما تم سنداً لأحكام القانون كما هو الحال في فكرة التفتيش. ففي فرنسا أجاز قانون ١٩٩١ اعتراض الاتصالات الهاتفية بما في ذلك شبكات تبادل المعلومات. وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات (Telecommunication Networks) إذا كان هنالك جرائم خطيرة.

وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسب الآلي بعد الحصول على إذن تفتيش من القاضي المختص. وتم رفع الكثير من القيود على عمليات التصنت والرقابة الهاتفية ورقابة الإنترنت والبريد الإلكتروني خصوصاً بعد أحداث مركز التجارة العالمي والبنتاغون [٢].

---

(١) نصت المادة (١٤) من قانون أصول المحاكمات الجزائية الأردني على أنه:"يعين لدى كل محكمة بدائية قاضٍ يدعى (المدعي العام)، يمارس وظيفة المدعي العام لديها، ولدى المحاكم الصلحية ضمن دائرة اختصاصه"، وكذلك المادة (١٥) من ذات القانون:"المدعي العام هو رئيس الضابطة العدلية في منطقته ... "، وبهذا نجد جزماً بأن المدعي العام له منطقة اختصاص يباشر فيها صلاحيته، فهل يمكن أن يكون له اختصاص خارج حدود دولته لإعطاء إذن تفتيش شبكة اتصالات خارج إقليم دولته؟!! وهل فاقد الشيء يعطيه؟!، وجاء في قانون تشكيل المحاكم النظامية في المادتين (٣) و (٤) منه على تشكيل محاكم الصلح والبداية، وأورد نظام تشكيل محاكم الصلح والبداية وتحديد الصلاحية المكانية لمحاكم الصلح والبداية والاستئناف رقم (٤٢) لسنة ٢٠٠٥ والمنشور في عدد الجريدة الرسمية رقم (٤٧١١) صفحة (٢٤٦٢) تاريخ ٢٠٠٥/٦/١٦ في المادة الثانية منه اختصاص محاكم الصلح وفي المادة الثالثة منه اختصاص محاكم البداية المكاني لكل منهما.

(٢) د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص٧٩-٨٠؛ أسامة بن غانم العبيدي، مرجع سابق، ص٩٥؛ علي عدنان الفيل، مرجع سابق، ص٣٤؛ خالد عياد الحلبي، مرجع سابق، ص١٦٦-١٦٧؛ د. عادل عزام سقف الحيط، مرجع سابق، ص٢٤٦-٢٤٧؛ صفاء حسن نصيف، مرجع سابق، ص ٢٧٢؛

Jarrett, H. Marshall, and Others, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Published by Office of Legal Education Executive Office for United States Attorneys, P1.

أما المشرع الأردني أجاز للمدعي العام مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة[١]، أما المشرع الجزائري فقد نص في المادة (٣) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: "مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات. يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون. وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"[٢]. وهنا يجد الباحثان بأن المشرع الجزائري نظم جميع الإجراءات المتعلقة بالجريمة الإلكترونية وآلية ضبط أدلتها وفقاً لنصوص القانون، متجنباً أي اجتهادات قد تثار بهذه المسائل، كما أن هذا الأمر فيه تحديد الأطر القانونية التي يجب التقيد بها لتحقيق الغاية من التفتيش والضبط أو المراقبة وهي تحقيق العدالة سواء بإثبات التهمة أو نفيها عن المشتبه به.

المطلب الثاني: الشروط الشكلية للتفتيش في الجرائم الالكترونية

أولا: تسبيب أمر التفتيش في الجرائم الإلكترونية

نصت المادة ٣/٨٧ من قانون أصول المحاكمات الجزائية على وجوب أن يتم تسبيب ار التفتيش، أما بخصوص الجرائم الالكترونية فلم ينص المشرع الأردني في قانون الجرائم الإلكترونية على تسبيب أمر التفتيش صراحةً، إنما ذكر في المادة (١٣) منه: "... الدخول إلى أي مكان تشير الدلائل إلى استخدامه لإرتكاب أي من هذه الجرائم ... كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لإرتكاب أي من تلك الجرائم

(١) نص المادة (٨٨) من قانون أصول المحاكمات الجزائية الأردني.

(٢) كما نصت المادة (٤) من ذات القانون على الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية، كما بينت الضمانات والشروط الواجب مراعاتها، ومن هذه الحالات: ".... ج. لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية. د. في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ... ". كما نص المشرع الجزائري في الباب الثاني (في التحقيقات) من قانون الإجراءات الجزائية في الفصل الرابع منه، تحت عنوان في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المواد ٦٥ مكرر ٥– ٦٥ مكرر ١٠، حيث نصت المادة (٦٥ مكرر ٥) على انه: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي: ١. اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية. ٢. وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية ... يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ...".

... "[1]، ولم يتعرض هذا القانون من خلال نصوصه إلى موضوع تفتيش الأشخاص إذا توافرت إمارات قوية أو دلائل بحقهم. وعليه يتم الرجوع هنا للنصوص العامة في قانون أصول المحاكمات الجزائية. وفي جميع هذه الأحوال يتوجب أن تكون غاية التفتيش في هذه الجريمة الإلكترونية هي التوصل إلى كشف الحقيقة من خلال ضبط الأشياء المتعلقة بالجريمة الإلكترونية[2].

وفي حقيقة الأمر إن إجراء التفتيش في الجرائم الإلكترونية مختلف عن غيره من صور التفتيش؛ وذلك لأن التفتيش في الجريمة الإلكترونية قد يكون في أكثر من مكان، وقد يكون داخل البلد الواحد أو في أكثر من بلد، ومن الممكن أن يكون في أكثر من جهاز أو وسيلة، ومن الممكن أن يكون بحوزة شخص أو عدة أشخاص، لذلك فإنه يكون لزاماً وضماناً لعدم تغول سلطات التحقيق أن يكون أمر التفتيش مسبباً وأن يكون محدداً فيه أماكن التفتيش والأدوات التي يراد تفتيشها والوسائل والشبكات التي سوف تخضع له مع تحديد أسباب هذا الإجراء لكل منها[3]. وهو ما يرى الباحثان ضرورة النص عليه في قانون الجرائم الإلكترونية والذي يحتاج إلى أشخاص ذوي علم ودراية في مجال البيئة الإلكترونية لتحديده بالشكل المطلوب، وهو ما يمكن تحقيقه من خلال تشكيل هيئة حكومية للتحقيق في الجرائم الإلكترونية.

وقد تنبه المشرع الفلسطيني في قانون الجرائم الإلكترونية لسنة ٢٠١٨ النص إلى تسبيب أمر التفتيش في هذه الجرائم حيث جاء في المادة (٣٢) منه.

ويجد الباحثان بأن المشرع الفلسطيني كان موفقاً بالنص على أن يكون أمر التفتيش في الجرائم الإلكترونية مسبباً ومحدداً وقابلاً للتجديد، وهو تطبيق قانوني سليم فيه ضمانات للحرية الشخصية كما أن فيه مرونة للتطبيق العملي لضبط الأدلة المتعلقة بالجريمة الإلكترونية.

ثانياً: قواعد الحضور عند التفتيش في الجرائم الإلكترونية

إن حضور الأشخاص عند إجراء التفتيش يعتبر ضماناً لحرية الأشخاص وذلك من خلال مراقبة سلامة إجراءات التفتيش الأمر الذي يأتي متطابقاً مع قاعدة علانية التحقيق بالنسبة للخصوم، وهذا الشرط يتيح للأشخاص الحاضرين لإجراءات التفتيش من الاطلاع على ما يتم ضبطه أثناء تنفيذه وهو

(١) في مشروع تعديل هذا القانون الموجود على موقع ديوان التشريع والرأي، أضافت كلمة والتفتيش بعد كلمة الدخول لتصبح: "... الدخول والتفتيش إلى أي مكان .... ".

(٢) د. أسامة بن غانم العبيدي، مرجع سابق، ص١٠٠.

(٣) د. محمد أبو العلا عقيدة، مرجع سابق. ص ٨ وما بعدها.

يساهم أيضاً عند الطعن في إجراءات التفتيش وعند الطعن فيما تم ضبطه، وبالتالي فإن عدم حضور الشخص أو الأشخاص للتفتيش يفقدهم الحق في مراقبة إجراءات التفتيش وقانونيته(١).

إذا كانت قواعد الحضور عند إجراء التفتيش بهذه الأهمية، فكيف يمكن تطبيقها عند التفتيش في الجرائم الإلكترونية، إذا ما علمنا بأن التفتيش في الجرائم الإلكترونية من الممكن أن يتم في نفس المكان الذي يتم ضبط الأجهزة الإلكترونية أو الأدوات أو المعدات وهي الصورة الأقل حدوثاً وبين أن يتم في مختبر خاص مزود بمجموعة من أجهزة الحاسب الآلي القادرة على استرجاع البيانات المحذوفة من هذه الأجهزة أو الأدوات أو المعدات، مع وجود أشخاص مختصين للقيام بهذا الإجراء.

ثالثاً: تحرير محضر التفتيش في الجرائم الإلكترونية

الأصل هو توثيق بيانات التفتيش في ضبط وتوقيع جميع الحضور، وفي محضر التفتيش في الجريمة الإلكترونية نرى أنه إذا كان في مكان سكن أو مكان خاص يمكن أن تدون فيه جميع هذه الإجراءات، وكذلك إذا حدث تفتيش لشخص موجود في المكان واشتبه فيه فتذكر في المحضر هذه التفصيلات، ولكنها غير متصورة جميعها عند القيام بتفتيش الجهاز الإلكتروني أو المعدات أو الأدوات داخل المختبرات الخاصة باسترجاع البيانات أو استخراجها من داخل هذه الأجهزة (٢).

ونص المشرع الجزائي الأردني في قانون الجرائم الإلكترونية على ضرورة تنظيم محضر بإجراءات التفتيش وتقديمه إلى المدعي العام المختص سواء أأسفر تفتيش أي جهاز إلكتروني عن ضبط أدلة مرتبطة بالجريمة أوبغيرها أم لم يسفر عن ذلك(٣).

---

(١) د. حسن الجوخدار، (٢٠١١). التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص١٦٣؛ د. سامي الحسيني، مرجع سابق، ص٢٦٣؛ د. قدري عبد الفتاح الشهاوي، مرجع سابق، ص١٥٥-١٥٦؛ د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص١٦٤-١٦٦؛ د. علي حسن الطوالبة، مرجع سابق، ص٢١٢-٢١٧؛ نص المشرع الجزائي الأردني على قواعد حضور التفتيش في المواد (٣٦، ٨٣، ٨٥، ٩٤) من قانون أصول المحاكمات الجزائية فيما يتعلق بتفتيش المنازل، وفي المادة (٨٦) فيما يتعلق بتفتيش الأشخاص؛ ويقابلها المادة (٤٦) من نظام الإجراءات الجزائية السعودي؛ وكذلك المادة (٤٥) معدلة من قانون الإجراءات الجزائية الجزائري، إلا أن المشرع الجزائري أخرج تطبيق هذه القواعد _قواعد الحضور في التفتيش_ عند تعلق التفتيش بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف؛ ويقابلها المادة (٩٢) من قانون الإجراءات الجنائية المصري؛ وكذلك المادة (٦٠) من قانون المسطرة الجنائية المغربي؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص١٠١-١٠٢؛ محمد نافع فالح العدواني، مرجع سابق، ص٧٩.

(٢) د. أسامة بن غانم العبيدي، مرجع سابق، ص١٠٢؛ د. أحمد أبو العلا عقيدة، مرجع سابق؛ ونصت المادة (٥٧) من نظام الإجراءات الجزائية السعودي على أنه:"يجب أن يتضمن محضر التفتيش: ١. اسم من قام بالتفتيش ووظيفته وتاريخ التفتيش وساعته. ٢. نص الإذن الصادر بإجراء التفتيش، أو بيان الضرورة الملحة التي اقتضت التفتيش بغير إذن. ٣.أسماء الأشخاص الذين حضروا التفتيش وتوقيعهم على المحضر. ٤. وصف الأشياء التي ضبطت وصفاً دقيقاً. ٥.إثبات جميع الإجراءات التي اتخذت أثناء التفتيش والإجراءات المتخذة بالنسبة للأشياء المضبوطة".

(٣) حيث جاء في المادة (١٣) منه:"... وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص...".

أما المشرع الفلسطيني فذهب للنص في قانون الجرائم الإلكترونية في المادة (٣٢) منه على أنه: "... ٣. إذا أسفر التفتيش المحدد في الفقرة (٢) من هذه المادة على ضبط أجهزة، أو أدوات، أو وسائل ذات صلة بالجريمة؛ يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها ...". ويجد الباحثان بأن ضرورة تدوين محضر التفتيش مكتوباً هو الأصل دون النظر إلى النتيجة التي تحققت منه سواء أكانت بضبط الأدلة أم لا، كما أن تدوين المحضر فيه ضمانة لسلامة الإجراءات حفاظاً على من قام به وفي ذات الوقت حفاظاً لحقوق من تعرض له.

رابعاً: وقت إجراء التفتيش في الجرائم الإلكترونية

لم يورد المشرع الجزائي الأردني ضمن قانون أصول المحاكمات الجزائية أو قانون الجرائم الإلكترونية وقتاً لتنفيذ التفتيش، فتركه مطلقاً والمطلق يؤخذ على إطلاقه. لكن يتوجب ذكر توقيت إجراء التفتيش وتحديد وقت بدايته وانتهائه إلا أن بعض التشريعات الجزائية العربية حددت فترة زمنية لإجراء التفتيش خلالها، وعدم جوازه إذا تم خارجها وإلى ذلك ذهب المشرع المغربي في قانون المسطرة الجزائية حيث نص في المادة (٦٢) منه، كذلك نص المشرع الجزائي الكويتي في قانون الإجراءات والمحاكمات الجزائية الكويتي في المادة (٨٥) منه ؛ ونص المشرع الجزائري في قانون الإجراءات الجزائية في المادة (٤٧) المعدلة؛ وكذلك المشرع الفلسطيني في قانون الإجراءات الجزائية رقم (٣) لسنة ٢٠٠١ حيث نص على ذلك في المادة (٤١) منه، ونجد في هذه الدراسة بان معظم التشريعات التي نصت على تحديد موعد إجراء التفتيش أوردت في عجز المادة حالات استثنائية لتجاوز فترة التفتيش، وأحسن المشرع الجزائي الجزائري عندما وضع استثناءً لذلك في الجرائم الإلكترونية وذلك بسبب الطبيعة الخاصة للجريمة الإلكترونية وخصائص الأدلة المراد ضبطها وسهولة إتلافها أو إخفائها. وكان المشرع الجزائري هو المشرع الوحيد الذي أورد مثل هذا النص ضمن القوانين العربية المقارنة حيث حدد المشرع الجزائري الميعاد القانوني الذي يجوز فيه دخول المساكن وتفتيشها وذلك بموجب المادة ١/٤٧ من قانون الإجراءات الجزائية التي نصت على أنه "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحا[٥٠]، ولا بعد الساعة الثامنة مساءً"، وهذا يعني أنه لا يجوز كقاعدة عامة تفتيش ومعاينة المساكن بعد الساعة الثامنة ليلا، وقبل الساعة الخامسة صباحا، وقد حرص المشرع من وراء هذا النص إلى صون الحرية الفردية وحرية المسكن.[51]

غير أن هذه القاعدة أورد عليها المشرع استثناء بحيث أجاز إجراء التفتيش في كل ساعة من ساعات الليل أو النهار وذلك عندما يتعلق التحقيق بنوع معين من الجرائم، وتشكل الجرائم المعلوماتية إحدى هذه الجرائم التي شملها الاستثناء[٥٢] الوارد في الفقرة ٠٣ من نفس المادة المذكورة أعلاه وبذلك

يكون المشرع الجزائري قد غلب مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن

ويجد الباحثان بأنه وضماناً للحرية الشخصية للأشخاص ومأمنهم في مسكنهم فإنه يتوجب تحديد توقيت لإجراء التفتيش وأن يضاف إليه الاستثناء الوارد لدى المشرع الجزائري عندما يتعلق التفتيش بالجرائم الإلكترونية. وبهذا النص نخرج من جدل تحديد زمن التفتيش فيها.

خامسا: بطلان التفتيش في الجرائم الإلكترونية

ما يترتب على التفتيش الباطل في الجرائم العادية يسري على الجرائم الالكترونية، فإذا ما تم إجراء التفتيش بصورة باطلة فإن الدليل الإلكتروني المتحصل عليه نتيجة لهذا الإجراء يقع باطلاً ولا يجوز الركون إليه عند إصدار الحكم. واختلفت التشريعات حول طبيعة البطلان فيما إذا كان ذاتياً أو كان بطلاناً قانونياً أم كان يجمع بينهما، ولن يتم الحديث بصور موسعة هنا عنها(١). والبطلان بصورة عامة إما أن يكون بطلاناً مطلقاً أو نسبياً فإذا كان متعلقاً بالنظام العام كان مطلقاً وهو ما يتمثل بمخالفة الشروط الموضوعية للتفتيش. وقد يكون نسبياً أي متعلقاً بحقوق الخصوم وهنا يتوجب إثارته من قبل الخصوم أما المحكمة المختصة وأن يكون مقدم الطلب صاحب شأن في تقديمه.

يقسم التفتيش في الجريمة الإلكترونية إلى قسمين أولهما التفتيش الذي يجري على الشخص أو منزله بقصد ضبط الأجهزة الإلكترونية أو الوسائل أو المعدات المستخدمة في ارتكابها. والقسم الثاني الذي يتم على هذه الأجهزة أو الوسائل أو المعدات وهذه الصورة من الممكن أن تتم في نفس موقع التفتيش أو أن تتم في مكان مخصص لهذه الغاية وبوجود أجهزة إلكترونية ومعدات مخصصة للقيام به. ففي القسم الأول–إجراء التفتيش على جسد الشخص أو منزله– فإنه يتوجب توافر الشروط الموضوعية للتفتيش وتطبيق الشروط الشكلية عند القيام به فإذا تخلف أحد الشروط الموضوعية فإن التفتيش بقع باطلاً بطلاناً مطلقاً متعلقاً بالنظام العام ويترتب عليه عدم الركون إلى ما نتج عنه. وأما في القسم الثاني فإن تفتيش الأجهزة الإلكترونية أو الوسائل أو المعدات إن تم تفتيشها في نفس موقع التفتيش فيرى الباحثان ضرورة التقيد بالشروط الموضوعية والشكلية الواجب توفرها لتفتيش الأشخاص والمنازل، مع مراعاة الشروط التي لا تتعارض مع ضرورة الاستعانة بالمعدات الالكترونية في حالة حالة فحص تفتيش الاوعية الالكترونية في مختبر منفصل.

(١) للمزيد انظر د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق ص٢٢٧–٢٣٤؛ د. علي حسن الطوالبة، مرجع سابق، ص١٦٧–١٨٠؛ د. أسامة بن غانم العبيدي، مرجع سابق، ص١٠٤؛ د. مصطفى محمد موسى، مرجع سابق، ص٢٠١–٢٠٣.

ويترتب على بطلان التفتيش في الجرائم الإلكترونية مجموعة من الآثار منها عدم ترتب الأثر القانوني الذي نصت عليه القاعدة الإجرائية لأن العمل الإجرائي المتخذ لم يستكمل شروط صحته أو شكله أو صيغته أو الكيفية المنصوص عليها في القانون فيصبح الإجراء وما يترتب عليه من إجراءات لا قيمة لها قانوناً[١]. ومن هنا نجد بأن البطلان يطال الإجراء الباطل وما ترتب عليه من إجراءات. وهذا ما جاء بنص المادة (٧) من قانون أصول المحاكمات الجزائية الأردني حيث جاء فيها: "... ٤. لا يترتب على بطلان الإجراء بطلان الإجراءات السابقة له، أما الإجراءات اللاحقة به فلا تكون باطلة إلا إذا كانت مبنية على الإجراء الباطل"[٢].

والبطلان بحسب التشريع الجزائي الأردني يأخذ صورة البطلان القانوني وصورة البطلان الذاتي – البطلان بنص القانون والبطلان في حال وجود العيب الجوهري_. وفي حال بطلان التفتيش في الجريمة الإلكترونية فإنه يترتب عليه بطلان ما تم ضبطه وتحصل عنه. ولهذا يتوجب على القائمين بمكافحة الجريمة الإلكترونية التنبه إلى صحة الإجراءات التي يقومون بها؛ إذ إن الدليل المتحصل عن التفتيش في أغلب الأحيان هو الدليل الذي تنهض عليه الجريمة الإلكترونية لإدانة المشتكي عليه.

من الممكن أن يكون تفتيش أحد الأجهزة الإلكترونية باطلاً وتفتيش باقي الأجهزة صحيحاً؛ فإن ما ينتج عن التفتيش الباطل يقع باطلاً ولا يمتد إلى باقي التفتيشات التي تمت لأجهزة أو وسائل أو أدوات أخرى. وفي هذه الحالة فإن المحكمة تستطيع الركون إلى الإجراءات الصحيحة عند إعداد مسودة الحكم لحين النطق به. وشرع البطلان لمن له مصلحة فيه. وهو في الجريمة الإلكترونية صاحب الجهاز الإلكتروني أو الأداة أو الوسيلة الإلكترونية، ولا يقبل الدفع بالبطلان لغير من شرع له، إلا إذا كان متعلقاً بالنظام العام فالمحكمة تحكم به مِنْ تلقاء نفسها[٣].

النتائج والتوصيات:

بعد هذه الدراسة وصل الباحثان إلى مجموعة من النتائج ومنها:

١. التفتيش في الجرائم الإلكترونية وفي مسرحها إجراء مختلف عنه في الجريمة التقليدية ومسرحها، من حيث طبيعة الدليل وطريقة الحصول عليه واجراءات التفتيش.

(١) كما ورد في مؤلف د. علي حسن الطوالبة، مرجع سابق، ص١٦٨.

(٢) مما تجدر الإشارة إليه بان النظرية العامة للبطلان لم يكن منصوصاً عليها قبل التعديل الذي جرى على قانون أصول المحاكمات الجزائية الأردني بموجب القانون المعدل رقم (١٦) لسنة ٢٠٠١ حيث تم إضافة هذه المادة.

(٣) للمزيد انظر د. حسن الجوخدار، (٢٠١١). التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص١٨٣-١٨٤؛ د. محمد سعيد نمور، مرجع سابق، ص٣٨٩؛ د. سامي الحسيني، مرجع سابق، ص٤٦٥-٤٩٥؛ د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق ص٢٢٧-٢٣٤؛ د. علي حسن الطوالبة، مرجع سابق، ص١٧٠-١٧٧.

٢. التفتيش الإلكتروني قد يحتاج إلى فترات زمنية طويلة لإتمامه وذلك لأنه يمثل بحثاً في كم هائل جداً من المعلومات والبيانات الموجودة داخل الجهاز أو الوسائل التخزينية أو وسائل وشبكات الإتصال للحصول على دليل جريمة معينة.
٣. التفتيش الإلكتروني يحتاج إلى وسائل وبرامج ومعدات مساعدة لتنفيذه.
٤. التفتيش في الجريمة الإلكترونية يحتاج إلى تعاون دولي في حال وجود الأدلة خارج إقليم الدولة.
٥. يتطلب التفتيش في الجريمة الإلكترونية إعداد وتأهيل العاملين في مجال مكافحتها سواء من أفراد الضابطة العدلية أو السلطة القضائية بما يحقق الغاية من إجراء التفتيش الإلكتروني بالصورة القانونية السلمية واستخلاص الأدلة بطريقة مشروعة وقبولها لدى السلطة القضائية.

التوصيات:

١. النص في قانون الجرائم الإلكترونية الأردني على تشكيل هيئة وطنية متخصصة للوقاية من الجرائم الإلكترونية والتحقيق فيها وضبط أدلتها، تتكون من قانونيين وفنيين تتمتع باستقلال إداري ومالي ويخول موظفيها سلطة الضابطة العدلية.
٢. إسناد جميع إجراءات التحقيق الابتدائي في الجرائم الإلكترونية إلى النيابة العامة دون النظر إلى ماهية الجرم _جناية أم جنحة_ وأن تتم مباشرتها من أمامه ويكون ذلك بالنص صراحة على اختصاص النيابة العامة بتحريك دعوى الحق العام ومباشرتها واستقبال الشكاوي في الجرائم المنصوص عليها في قانون الجرائم الإلكترونية، وإلغاء كلمة المحكمة المختصة الواردة في هذه المادة.
٣. إيجاد نص في قانون الجرائم الإلكترونية يتعلق بتسبيب إجراء التفتيش الإلكتروني تحت طائلة البطلان.
٤. النص في قانون الجرائم الإلكترونية على ضرورة المحافظة على الأدلة المستخرجة من الأجهزة الإلكترونية وإخراجها من طبيعتها المعنوية إلى طبيعة مادية عن طريق الطباعة أو النسخ على وسيلة تخزين خارجية
٥. الاشتراك في اتفاقيات دولية وإقليمية بخصوص الجرائم الإلكترونية لتيسير المساعدة القضائية في الحصول على الأدلة الإلكترونية.
٦. إدراج مادة في قانون الجرائم الإلكترونية تتيح لسلطة التحقيق إمكانية امتداد اجراءات التفتيش في الجرائم الإلكترونية خوفاً من ضياع الأدلة أو فقدانها كلياً أو جزئياً إلى أماكن أخرى داخل حدود الدولة غير المنصوص عليها في مذكرة التفتيش.

المراجع

الجوخدار، حسن، (٢٠٠٨)، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان.

الجوخدار، حسن، (٢٠١١)، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان.

الحسيني، سامي حسني، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية للنشر، القاهرة، ١٩٧٢.

سرور، أحمد فتحي، (١٩٨٥)، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة.

السعيد، كامل، شرح قانون أصول المحاكمات الجزائية، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨.

شمس الدين، أشرف توفيق، شرح قانون الإجراءات الجنائية، ٢٠١٢.

الشهاوي، قدري عبدالفتاح، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، ٢٠٠٥.

عبدالستار، فوزية، شرح قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهرة، ١٩٧٧.

العكايلة، عبدالله ماجد، الاختصاصات القانونية لمأموري الضبط القضائي في الأحوال العادية والاستثنائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠.

القهوجي، علي عبد القادر، شرح قانون أصول المحاكمات الجزائية، الكتاب الثاني، منشورات الحلبي الحقوقية، بيروت، ص٢٧٢.

المطيري، غانم محمد الحجي، شرح إجراءات التحقيق الابتدائي في قانون الإجراءات والمحاكمات الجزائية الكويتي، الطبعة الأولى، ١٩٩٧.

نمور، محمد سعيد، أصول الإجـــراءات الجزائية، الطبعة الرابعة، دار الثقافة للنشـــر والتوزيع، عمان، ٢٠١٦.

أحمد، هلالي عبداللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٨.

أحمد، هلالي عبداللاه، جرائم الحاسب والانترنت بين التجريم وآليات المواجهة، دار النهضة العربية، القاهرة، ٢٠١٥-٢٠١٦.

الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١.

حنفي، حازم محمد، الدليل الالكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٧.

سقف الحيط، عادل عزام، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٥.

الطوالبة، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث للنشر والتوزيع، اربد، ٢٠٠٤.

عزت، فتحي محمد أنور، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠١٠.

فرغلي، عبدالناصر محمد محمود، د. المسماري، محمد عبيد سيف سعيد، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ١٢-٢٠٠٧/١١/١٤.

المساعدة، أنور "محمد صدقي"، قضايا أمنية معاصرة، كلية العلوم الشرطية-جامعة مؤته، الطبعة الأولى، الكرك، ٢٠٠٧.

المناعسة، أسامة أحمد، ومشاركوه، جرائم الحاسب الآلي والإنترنت، الطبعة الأولى، دار وائل للنشر، عمان، ٢٠٠١.

المناعسة، أسامة، الزعبي، جلال، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٧.

موسى، مصطفى محمد، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، ٢٠٠٨.

البحوث وأوراق العمل

الطوالبة، علي حسن، إجراءات ضبط المكونات المعنوية والانترنت، بحث منشور على الموقع الرسمي للمركز الإعلامي الأمني التابع لوزارة الداخلية البحرينية.

العبيدي، أسامة بن غانم، التفتيش عن الدليل في الجرائم المعلوماتية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، ٢٠١٣/١١، المجلد (٢٩)، العدد (٥٨).

العدوان، ممدوح حسن مانع، السلامات، نادر عبدالحليم، مشروعية وحجية الدليل المستخلص من التفتيش الإلكتروني في التشريع الجزائي الأردني، بحث منشور في مجلة دراسات الشريعة والقانون، المجلد (٤٥)، العدد (٤)، الملحق (٢)، الجامعة الأردنية، ٢٠١٨.

العقيدة، محمد أبو العلا، ورقة عمل مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، تاريخ ٢٦/٤-٢٠٠٣/٤/٢٨، الإمارات العربية المتحدة.

الفيل، علي عدنان، إجراءات التحقيق الابتدائي في الجريمة المعلوماتية: دراسة مقارنة، مجلة البحوث والدراسات العربية، العدد (٥٣)، القاهرة، ٢٠١٠.

نصيف، صفاء حسن، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، بحث منشور في مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، جامعة ديالى، العراق، ٢٠١٦.

References

General references

Al-Jokhadar, Hassan, (2008), the preliminary investigation into the Code of Criminal Procedure, first edition, House of Culture for Publishing and Distribution, Amman.

Al-Jokhdar, Hassan, (2011), The Primary Investigation of the Code of Criminal Procedure, second edition, House of Culture for Publishing and Distribution, Amman.

Al-Husseini, Sami Hosni, The General Theory of Inspection in Egyptian and Comparative Law, Dar Al-Nahda Al-Arabiya Publishing, Cairo, 1972.

Sorour, Ahmed Fathi, (1985), Mediator in the Criminal Procedure Law, Dar Al-Nahda Al-Arabiya, Cairo.

Al-Saeed, Kamel, Explanation of the Code of Criminal Procedure, First Edition, Second Edition, House of Culture for Publishing and Distribution, Amman, 2008

Shams El-Din, Ashraf Tawfiq, Explanation of the Criminal Procedure Code, 2012.

El-Shahawi, Qadri Abdel-Fattah, Inspection Controls in Egyptian and Comparative Legislation, Mansha'at al-Maaref, Alexandria, 2005.

Abdel-Sattar, Fawzia, Explanation of the Criminal Procedure Law, Part One, Dar Al-Nahda Al-Arabiya, Cairo, 1977.

Al-Akaileh, Abdullah Majid, The Legal Competencies of Judicial Enforcement Officers in Ordinary and Exceptional Cases, First Edition, House of Culture for Publishing and Distribution, Amman, 2010.

Al-Qahwaji, Ali Abdel-Qader, Explanation of the Code of Criminal Procedure, Book Two, Al-Halabi Human Rights Publications, Beirut, p. 272.

Al-Mutairi, Ghanem Muhammad Al-Hajji, Explanation of the Procedures for the Primary Investigation in the Kuwaiti Criminal Procedures and Trials Law, first edition, 1997.

Nammour, Muhammad Saeed, The Origins of Criminal Procedures, Fourth Edition, House of Culture for Publishing and Distribution, Amman, 2016.

Special references

Ahmed, Hilali Abdallah, Inspection of computer systems and information security, a comparative study, second edition, Dar Al-Nahda Al-Arabiya, Cairo, 2008.

Ahmed, Hilali Abdallah, Computer and Internet crimes between criminalization and confrontation mechanisms, Arab Renaissance House, Cairo, 2015-2016.

Al-Halabi, Khaled Ayyad, Investigation and Investigation Procedures in Computer and Internet Crimes, House of Culture for Publishing and Distribution, Amman, 2011.

Hanafi, Hazem Muhammad, Electronic evidence and its role in the criminal field, first edition, Dar Al-Nahda Al-Arabiya, Cairo, 2017.

Saqf Al-Hait, Adel Azzam, Crimes of Defamation, Defamation and Humiliation Committed Through Electronic Media, Second Edition, House of Culture for Publishing and Distribution, Amman, 2015.

Tawalbeh, Ali Hassan Muhammad, Criminal Inspection of Computer and Internet Systems, Modern World of Books for Publishing and Distribution, Irbid, 2004.

Ezzat, Fathi Muhammad Anwar, Electronic evidence in criminal matters and civil and commercial transactions for the information society, second edition, Arab Renaissance House, Cairo, 2010.

Farghali, Abdel Nasser Mohamed Mahmoud, d. Al-Mismari, Muhammad Obaid Saif Saeed, Criminal Proof of Digital Evidence from the Legal and Technical Perspectives, A Comparative Applied Study, the First Arab Conference on Forensic Science and Forensic Medicine, Naif Arab University for Security Sciences, Riyadh, 12-14/11/2007.

The Help, Anwar "Muhammad Sidqi", Contemporary Security Issues, College of Police Sciences - Mutah University, first edition, Karak, 2007.

Al-Manaasah, Osama Ahmed and Associates, Computer and Internet Crimes, first edition, Wael Publishing House, Amman, 2001.

Al-Manasah, Osama, Al-Zoubi, Jalal, Electronic Information Systems Technology Crimes, third edition, House of Culture for Publishing and Distribution, Amman, 2017.

Mousa, Mustafa Mohamed, Criminal Investigation of Electronic Crimes, first edition, Police Press, Cairo, 2008.

Research and working papers

Tawalbeh, Ali Hassan, Procedures for Controlling Moral Components and the Internet, research published on the official website of the Security Media Center of the Bahraini Ministry of Interior.

Al-Obaidi, Osama bin Ghanem, Searching for Evidence in Information Crimes, research published in the ArabJournal for Security Studies and Training, 11/2013, Volume (29), Issue (58).

Al-Adwan, Mamdouh Hassan Manea, Salamat, Nader Abdel Halim, Legality and Authenticity of Evidence Extracted from Electronic Inspection in Jordanian Penal Legislation, research published in the Journal of Sharia and Law Studies, Volume (45), Issue (4), Supplement (2), University of Jordan, 2018.

Creed, Muhammad Abu Al-Ela, working paper presented at the first scientific conference on the legal and security aspects of electronic operations, Dubai Police Academy, dated 04/26-28/4/2003, United Arab Emirates.

El-Fil, Ali Adnan, Procedures for the Primary Investigation of Information Crime: A Comparative Study, Journal of Arab Research and Studies, Issue (53), Cairo, 2010.

Nassif, Safa Hassan, Procedural Challenges Related to Information Crimes, Research published in the Journal of Legal and Political Sciences, Volume Five, Number Two, University of Diyala, Iraq, 2016.

Foreign references

Electronic Crime Scene Investigation: A Guide for First Responders, 2001.

Jarrett, H. Marshall, and Others, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Published by Office of Legal Education Executive Office for United States Attorneys, P1.