التفتيش عن الدليل في الجرائم المعلوماتية

د. أسامة بن غانم العبيدي(*)

المقدمـــــــة

التطـور الكبير في وسـائل الاتصال الحديثـة والزيادة المطّردة في اسـتخدام **صاحب** شبكة الإنترنت زيادة كبيرة في الجرائم التي ترتكب باستخدام هذه الشبكة.

وقد أثارت الجرائم المعلوماتية العديد من الإشكالات بالنسبة للقائمين على مكافحتهـا ، ويرجـع ذلك إلى أن القوانين العقابية وقوانين الإجراءات الجنائية التقليدية تبسـط حمايتها على الأشـياء المادية الملموسـة، أما بالنسـبة للمعلومات والأشياء المعنوية الأخرى المرتبطة بها فلم تمتد إليها الحماية إلا حديثاً . كما أن كشف هذا النوع من الجرائم وإثباتهـا ليـس بالشيء السـهل وإنما يتطلـب اسـتخدام تقنيات حديثة لغـرض التحري والتفتيش وضبط الأدلة .

ويناقش هذا البحث موضوع التفتيش عن الدليل المعلوماتي في الجرائم المعلوماتية.

هدف البحث وأهميته :

يهـدف هذا البحث إلى دراسـة موضوع التفتيش عن الدليـل المعلوماتي في الجرائم المعلوماتيـة مـن حيـث ماهيـة التفتيـش وغايته ومـدى قابليـة مكونات الحاسـب الآلي والشـبكات المرتبطـة بـه للتفتيش ، وشروط التفتيـش، وبطلانه ، والسـلطات المختصة بإجرائه ، وإجراءات ضبط الأدلة المعلوماتية ، والأساليب المستخدمة في ارتكاب الجرائم المعلوماتية ، ووسائل التفتيش في هذه الجرائم، وصعوبات التفتيش عن الدليل المعلوماتي. وتكمـن أهميـة هذا البحث في مـدى اختلاف طبيعة التفتيش عـن الدليل المعلوماتي عن التفتيش عن الدليل التقليدي المادي.

(*) أستاذ القانون المشارك – معهد الإدارة العامة – الرياض.

خطة البحث

يشتمل هذا البحث على أربعة مباحث :

أولاً: ماهية التفتيش والغاية منه ومدى قابلية مكونات الحاسب الآلي والشبكات المرتبطة به للتفتيش .

ثانياً: شروط تفتيش النظام المعلوماتي وبطلانه والسلطات المختصة بالتفتيش .

ثالثاً: إجراءات ضبط أدلة الجرائم المعلوماتية وأساليب تنفيذ التفتيش.

رابعاً: وسائل التفتيش في الجرائم المعلوماتية وصعوبات التفتيش عن الدليل المعلوماتي .

منهج البحث

يعتمد هذا البحث على منهج الدراسة التحليلية لنصوص الأنظمة والقوانين المقارنة مع الاعتماد على المراجع العلمية القانونية ذات العلاقة .

أولاً: ماهية التفتيش والغاية منه ومدى قابلية مكونات الحاسب الآلي والشبكات المرتبطة به للتفتيش

نظـراً لأهميـة تحديد ماهية التفتيش والغاية منه سـنتناول في المطلب الأول من هذا المبحث ماهية التفتيش ، وفي الثاني نبين الغاية منه ، ثم سنتطرق إلى مدى قابلية مكونات الحاسب الآلي والشبكات المرتبطة به للتفتيش في المطلب الثالث .

١ ـ ماهية التفتيش

يعرف جانب من الفقه التفتيش (Search) بأنه : «البحث عن شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها . وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة»[1]، وقد أحاطت القوانين المقارنة هذا التفتيش بضمانات عديدة.

(١) أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، ١٩٨٠م . ص ٤٤٩ .

ومحل التفتيش إما أن يكون مسكناً أو شخصاً ، وهو بنوعيه قد يكون متعلقاً بالمتهم أو بغيره، وهو في كل أحواله جائز مع اختلاف في بعض الشروط . ويعرف جانب آخر من الفقه التفتيش بأنه «إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون ، يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة. ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه»[١] . وعرفه الفقه الفرنسي بأنه « بحث بوليسي أو قضائي عن عناصر الدليل في جريمة ما ، ويمكن وفقاً لقواعد قانونية خاصة أن ينفذ في المسكن الخاص بأي شخص أو في أي مكان آخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيداً في إظهار الحقيقة»[٢] . والتفتيش في مدلوله القانوني بالنسبة لجرائم الحاسب الآلي لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية ، فيقصد به أنه التنقيب في وعاء السر بقصد ضبط ما يفيد في كشف الحقيقة ، فهدف التفتيش في جرائم الحاسب الآلي هو الوصول إلى ما تحويه نظم الحاسب الآلي من أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إلى المتهم . أو هو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه ، يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو نظمه أو شبكة الإنترنت[٣].

ويتضح لنا من التعريفات السابقة أن التفتيش ما هو إلا وسيلة للإثبات المادي، وذلك لأنه يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، والهدف منه دائماً هو الحصول على الدليل المادي ، وهو ما يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، وكذلك شبكة الإنترنت ، فهي مجرد بيانات وبرامج إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[٤].

---

(١) فوزية عبدالستار ، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦م . ص٢٧٨.

(٢) انظر : Lexique de termes Juridique au Code de Dalloz Penale, 101 e ed. 2004

(٣) محمود محمد مصطفى ، الإثبات في المواد الجنائية في القانون المقارن ، التفتيش والضبط ، جامعة القاهرة ، القاهرة ، ١٩٨٧م . ص ٢١٤ . انظر أيضاً علي حسن الطوالبة ، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة ، إربد ، ٢٠٠٤م . ص ١١ .

(٤) أحمد فتحي سرور ، المرجع السابق . ص ٥٤٤ . انظر أيضاً نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٧م . ص ٢٢١ . وما بعدها .

٢ ـ الغاية من التفتيش

الغايـة مـن التفتيش هـي البحث عن الأشـياء المتعلقة بالجريمة أو تفيد في كشـف الحقيقـة، فالتفتيش باعتبـاره إجراء من إجراءات التحقيق يجب أن يكون قد تم القيام به لغاية معينة وهي الكشـف عن أشـياء تتعلق بالجريمة أو تفيد في كشف الحقيقة. ولذلك يقـع باطـلاً التفتيـش الـذي يقع لغاية أخرى خـلاف ما حدده المـشرع ، لأن كل تفتيش يتـم بغـير أن يتبين وجـه المصلحة منه يكون إجـراءً تحكمياً وباطلاً . ويعـد التفتيش من الإجـراءات التـي لا غنـى عنها للمحقـق في تقوية أواصر الأدلة أو في إسـناد الواقعة في مواجهة المتهم ، فالعثور على أدلة الجريمة من شأنه تقوية الاتهام ضد المتهم وبالتالي عدم إفلاته من العقاب ((١)).

٣ ـ مدى قابلية مكونات الحاسب الآلي والشبكات المرتبطة به للتفتيش

يوجد للحاسب الآلي مكونات مادية (Hardware) ، وأخرى معنوية أو برامجية (Software)،كما أن له شبكات اتصال (Network Telecommunications) سلكية ولاسلكية محلية ودولية . ويقصد بالتفتيش هنا التفتيش عن معطيات الحاسب الآلي غير المادية والمخزنة في جهاز الحاسـب الآلي ، أو المخزنة في الأقراص ، كما يقصد بالتفتيش، البحث في النظم المعلوماتية محل التحقيق(٢).

ويثور الجدل الفقهي حول قابلية مكونات الحاسب الآلي المادية والمعنوية والشبكات المرتبطة به للتفتيش(٣).

(١) عـادل عـزام سـقف الحيط ، جرائم الـذم والقدح والتحقـير المرتكبة عبر الوسـائط ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠١١م . ص ٢٣٠ وما بعدها . انظر أيضاً عبدالفتاح حجازي ، مبادئ الإجـراءات الجنائيـة في جرائم الكمبيوتر والإنترنـت ، دار الكتب القانونية ، القاهرة ، ٢٠٠٧م . ص ٢٥٧ وما بعدها. انظر أيضاً خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية، ٢٠٠٩م . ص ١٨٣ .

(٢) هـلالي عبدالله أحمد، تفتيش نظم الحاسـب الآلي وضمانات المتهـم المعلوماتي، دار النهضة العربية، القاهرة ، ٢٠٠٦م . ص ٦٩ وما بعدها .

(٣) حسين سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٩م ، ص ٤٧٠ وما بعدها .

وسوف نتطرق فيما يلي إلى مدى خضوع هذه المكونات للتفتيش على النحو التالي :

أ ـ مدى خضوع مكونات الحاسب الآلي المادية للتفتيش

تحكم الإجراءات القانونية الخاصة بالتفتيش فحص المكونات المادية للحاسب الآلي بحثاً عن أي دليل يتصل بجريمة معلوماتية حدثت ، ويفيد التفتيش في الكشف عن مرتكبها . ويخضع تفتيش الحاسب الآلي إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز . فإذا كان الحاسب الآلي مودعاً في مكان خاص، كمسكن المتهم أو أحد ملحقاته ، فتأخذ حكم المسكن (Home) ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم، وبذات الضمانات المقررة قانوناً في التشريعات المختلفة . فإذا كانت مكونات الحاسب الآلي المراد تفتيشه في المسكن غير متصلة بنهايات طرفية موجودة في مكان آخر، فلا يثور خلاف بشأن تفتيشها ، أما إذا كانت تلك النهايات مرتبطة في مكان آخر، وتطلبت دواعي التفتيش الوصول إليها وتفتيشها، فيجب مراعاة الضمانات والاشتراطات التي يتطلبها المشرع لتفتيش تلك الأماكن . أما بالنسبة للأماكن العامة ، (Public Places)، فإذا وجد شخص وهو يحمل مكونات الحاسب المادية، أو كان حائزاً لها أو مسيطراً عليها (In Possession or Control of the Computer) فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص ، وبنفس الضمانات والقيود المنصوص عليها قانوناً[(١)].

ب ـ مدى خضوع مكونات الحاسب الآلي المعنوية للتفتيش

أثار تفتيش المكونات المعنوية للحاسب الآلي خلافاً كبيراً في الفقه بشأن جواز تفتيشها من عدمه، فذهب رأي إلى جواز تفتيش البيانات الإلكترونية (Electronic Date) بمختلف أشكالها .

وفي هذا المعنى نجد أن المادة (٢٥١) من قانون الإجراءات الجنائية اليوناني ، تعطي سلطات التحقيق إمكانية القيام : «بأي شيء يكون ضرورياً لجمع الدليل وحمايته». ويفسر الفقه اليوناني عبارة» أي شيء «بأنها تشمل البيانات المخزنة أو المعالجة إلكترونياً، وبالتالي فإن ضبط المعطيات الإلكترونية بمختلف صورها المخزنة في الذاكرة الداخلية

(١) علي حسن الطوالبة ، المرجع السابق . ص٩ وما بعدها . انظر أيضاً عادل عزام سقف الحيط ، المرجع السابق ، ص ٢٣٠ وما بعدها .

للحاسب الآلي لا تثير أي خلاف في اليونان ، وهناك يطلب المحقق من الخبير المختص أن يقوم بجمع أي أدلة مقبولة دليلاً في المحاكمة الجزائية . كما أن قانون أصول المحاكمات الجزائية الأردني أباح لسلطة التحقيق وفقاً للمادة (٨٧) منه أن تقوم بضبط «جميع الأشياء التي تراها ضرورية لإظهار الحقيقة». ويفسر الفقه الأردني عبارة «الأشياء» بأنه يمتد ليشمل الكيانات المعنوية للحاسب الآلي[١].

وعلى النقيض من الرأي السابق ، يذهب رأي آخر إلى أن المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة ، ويقترح أصحاب هذا الرأي مواجهة هذا القصور التشريعي إضافة عبارة إلى القوانين ذات العلاقة وإلى مذكرات التفتيش ، مثل : «المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي»[٢].

وفي الولايات المتحدة الأمريكية تم إقرار نصوص تعالج تفتيش الكيانات المعنوية والتعامل مع الأدلة الرقمية .

ونرى بان البيانات والمعلومات المخزنة في الحاسب الآلي تصلح لأن تكون محلاً للتفتيش ، ويمكن ضبطها واستنساخها على الورق أو على الأقراص، أو على أي دعامة أخرى ، كالفلاش ميموري(Flash Memory) ؛ بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم للجريمة في مرحلة المحاكمة . لذلك ينبغي الإشارة في قوانين الإجراءات الجنائية على حرية تفتيش المكونات المادية والمعنوية لأجهزة الحاسب الآلي [٣].

ج ـ مدى خضوع شبكات الحاسب الآلي للتفتيش

شبكات الحاسب هي عبارة عن مجموعة مكونة من جهازين أو أكثر من أجهزة الحاسب الآلي والمتصلة ببعضها اتصالاً سلكياً أو لاسلكياً، وتوجد شبكات واسعة في أماكن متفرقة مرتبطة ببعضها البعض بواسطة الهاتف .

إن إجراءات تفتيش الحاسب الآلي تتضمن وجود وسائل فنية حديثة لتفتيش

(١) علي حسن الطوالبة ، المرجع السابق . ص ١٤١ .

(٢) هلالي عبداللاه أحمد ، المرجع السابق. ص ٧١ وما بعدها . انظر أيضاً سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) ، دار النهضة العربية ، القاهرة ، ٢٠٠٨م . ص ٣٠٠ وما بعدها .

(٣) هلالي عبداللاه أحمد ، المرجع السابق . ص ١٤٢ وما بعدها.

الشبكات المرتبطة به، والمراقبة الإلكترونية لنظم المعلومات (Information Systems) والشبكات المعلوماتية، رغم أن ذلك يتعرض لحقوق الأشخاص وحرياتهم، إلا أن ذلك لا ينبغي أن يحدث دون الحصول على موافقة القضاء وأن يكون محدد المدة والنطاق[1].

فلا شك أن طبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش والضبط في الجرائم المعلوماتية. فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش. كما قد يكون الموقع الفعلي للبيانات والمعلومات يدخل ضمن الاختصاص القضائي لدولة أخرى ما قد يعقد الصعوبات التي تواجه مكافحة الجرائم المعلوماتية، ويزيد من أهمية وجود تعاون دولي في مكافحة مثل هذا النوع[2]. وتوجد ثلاثة احتمالات تتعلق بشبكات الحاسب الآلي نوردها على النحو التالي:

الاحتمال الأول: اتصال الحاسب الآلي العائد للمتهم بحاسب آلي آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة

يثور التساؤل بمدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية (Terminal) في مسكن المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم.

ويرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في مكان آخر، استناداً إلى ما نص عليه في القسم (١٠٣) من قانون الإجراءات الجنائية الألماني، وذلك عندما يكون مكان التخزين الفعلي (Storage) خارج المكان الذي يتم فيه التفتيش[3].

(١) علي حسن الطوالبة، المرجع. ص٧١ وما بعدها. انظر أيضاً خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١م. ص ١٦١ وما بعدها.

(٢) خالد ممدوح إبراهيم، المرجع السابق. ص ٢٠٠ وما بعدها.

(٣) خالد ممدوح إبراهيم، المرجع السابق. ص ٢٠٠ وما بعدها. انظر أيضاً:

Manfred Mohrenschlager, Computer Crime and Other Crime Against Information Technology in Germany , R.I.D.P. 1993 , at 351.

انظر أيضاً هلالي عبداللاه أحمد، المرجع السابق. ص٧٤ وما بعدها.

كـما نـص قانون الإجراءات الجنائية البلجيكي في المـادة (٨٨) منه على أنه «إذا أمر قـاضي التحقيـق بالتفتيش في نظام معلوماتي، أو في جزء منـه فإن هذا البحث يمكن أن يمتـد إلى نظـام معلوماتي آخـر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين :

أ ـ إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث .

ب ـ إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث[١].

وذات الشيء نجده في القانون الاتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة المعلوماتية تقتصر على مواقع محددة، فقد أخذ القانون الاتحادي الأسترالي بمكافحـة الجرائـم المعلوماتيـة بإمكانيـة أن تتوزع بيانات الأدلة على حسـب شـبكات الحاسـب الآلي . ويسـمح هذا القانون أيضاً بعمليات تفتيش بيانات خارج المواقع التي يمكن اختراقها من خلال أجهزة حاسب آلي موجودة في الأماكن التي يجري تفتيشها .

ويشير مصطلح البيانات المحتجزة في حاسب آلي ما إلى أي بيانات محتجزة في جهاز تخزين على شبكة حاسبات آلية يشكل الحاسب الآلي جزءاً منها، فلا توجد حدود جغرافية محددة، ولا أي اشتراط بالحصول على موافقة طرف ثالث[٢].

وبالإضافـة إلى ذلـك فإن قانون مكافحة جرائم الحاسـب الآلي في هولندا قد نص عـلى جواز امتـداد التفتيش إلى نظم المعلومات الموجـودة في موقع آخر شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة[٣].

الاحتمال الثاني: اتصالات الحاسـب الآلي العائد للمتهم بحاسـب آلي آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة :

ووفقـاً لهـذا الاحتمال يقوم مرتكبـو الجريمة المعلوماتية بتخزيـن بياناتهم في أنظمة

(١) بكري يوسـف بكري، التفتيش عن المعلومات في وسـائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، ٢٠١١م . ص ٨١ وما بعدها .

(٢) حسين سعيد الغافري، المرجع السابق . ص ٤٨٢ وما بعدها .

(٣) المادة (١٢٥)، قانون مكافحة جرائم الحاسب الآلي الهولندي .

المعلومات خارج الدولة عن طريق شبكات الاتصالات بهدف عرقلة سلطات التحقيق في جمع الأدلة .

وللتعامل مع هذا الاحتمال نص قانون مكافحة جرائم الحاسب الآلي الهولندي على أنه يجوز لجهات التحقيق القيام بالتفتيش داخل الأماكن، وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة به حتى لو كانت موجودة في دول أخرى ، وبشرط أن يكون هذا التدخل مؤقتاً ، وأن تكون البيانات التي يتم التفتيش عنها ضرورية لإظهار الحقيقة [1]. ويرى جانب من الفقه أن التفتيش الإلكتروني العابر للحدود لا بد وأن يتم في إطار اتفاقيات تعاون خاصة ثنائية (Bi – Lateral) أو دولية تسمح بهذا الامتداد يتم إبرامها بين الدول المعنية ، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في ظل عدم وجود مثل تلك الاتفاقيات ، أو كحدٍ أدنى الحصول على موافقة الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المعلوماتية[2].

وقد أجازت المادة (٣٢) من الاتفاقية الأوروبية بشأن مكافحة الجرائم المعلوماتية والتي أعدها المجلس الأوروبي (The Council of Europe) وتم التوقيع عليها في بودابست في عام ٢٠٠١م إمكانية الدخول بغرض التفتيش والضبط في أجهزة حاسب أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين :

الأولى إذا تعلق التفتيش بمعلومات أو بيانات متاحة للعامة ، والثانية إذا رضي المالك أو حائز هذه البيانات بهذا التفتيش.

ويؤيد الفقه الألماني ما جاء في الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية في هذا الخصوص، ذلك أن السماح باسترجاع البيانات (Retrieval of Data) التي تم تخزينها في الخارج يعد انتهاكاً لسيادة دولة أخرى وخرقاً للقوانين الوطنية والاتفاقيات الدولية المتعلقة

(١) المادة (١٢٥) ، قانون مكافحة جرائم الحاسب الآلي الهولندي .

(٢) هشام محمد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني ، مؤتمر القانون والكمبيوتر والإنترنت ، جامعة الإمارات العربية المتحدة ٢٠٠٠م ، ص ٧١ وما بعدها. انظر أيضاً خالد ممدوح إبراهيم، المرجع السابق . ص ٢٠٣ وما بعدها .

بإمكانية التعاون في مجال مكافحة الجرائم بشكل عام والجرائم المعلوماتية بشكل خاص[١].

وفي إحدى جرائم الغش المعلوماتي (Information Fraud) أيد القضاء الألماني هـذا الاتجـاه ، حيث أسـفر البحث في إحدى جرائم الغش المعلومـاتي عن وجود طرفية حاسب آلي في ألمانيا متصلة بشبكة اتصالات موجودة في سويسرا. حيث كان يتم تخزين بيانـات المشروعات فيها، وعندما رغبت سـلطات التحقيـق في ألمانيا الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة[٢].

ووفقاً للإجراءات المعقدة للتعاون الدولي القضائي ، فإن الدول تبدو غير مستعدة في وقتنـا الراهـن لقبول طلبات إجراء التفتيش الإلكـتروني العابر للحدود التي تعتبرها بمثابة مساس بسيادتها .

أما عن تفتيش أجهزة الحاسـب الآلي الواقعة في أماكن عامة كالحاسـبات الشخصية (Personal Computers) التـي يحملهـا الشـخص خارج منزله، فـإن تفتيش أنظمتها لا يكـون جائـزاً إلا في الأحوال التي يبيح فيها القانون تفتيش شـخصه على اعتبار أن تفتيش الشخص يشمل ذاته وكل ما بحوزته عند إجراء هذا التفتيش وسواء أكان مملوكاً له أم لغيره .

أمـا في الحالـة التي يكون فيها جهاز الحاسـب الآلي المراد تفتيش نظمه داخل منزل أحد الأشخاص ، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش منازل الأشخاص[٣].

(١) عدنان الفيل ، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعـي الحديـث ، عـمان ، ٢٠١١م . ص ٤٦ . انظـر أيضاً عبدالفتاح بيومـي حجازي ، المرجع السابق. ص ٣٨٠ وما بعدها .

(٢) وفي إحدى الحالات قامت مجموعة إجرامية من المخربين باسـتخدام أجهزة حاسـب آلي موجودة في الولايـات المتحـدة والصين بمهاجمة واختراق العديد من المواقع الإلكترونية الخاصة بالحكومة اليابانية على شبكة الإنترنت . وقد طلبت الشرطة اليابانية من الولايات المتحدة الأمريكية والصين تسليمها بيانات الدخول المسجلة على أجهزة الحاسب الآلي في كل من هاتين الدولتين حتى يتمكنوا من الوصول إلى الجناة ومعاقبتهم على جرائمهم . انظر عبدالفتاح حجازي، المرجع السابق . ص ٣٨١ وما بعدها .

(٣) هلالي عبداللاه أحمد ، المرجع السابق . ص ٧٧ وما بعدها . انظر أيضاً خالد ممدوح إبراهيم، المرجع السابق . ص ٢٠٥ وما بعدها . انظر أيضاً هشام رستم ، المرجع السابق . ص ٧٣ .

الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي

التنصت (Wiretapping) والأشكال الأخرى للمراقبة الإلكترونية (Electronic Monitoring) رغم كونها وسائل مثيرة للجدل القانوني (Legal Debate) حول مدى مشروعيتها، إلا أنه يسمح بها وفق ظروف معينة في جميع دول العالم تقريباً.

فالقانون الفرنسي لعام ١٩٩١ يجيز اعتراض الاتصالات الهاتفية بما في ذلك شبكات تبادل المعلومات.

وفي هولندا أجاز القانون الهولندي لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات (Telecommunication Networks) في حالة وجود جرائم جسيمة ارتكبها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات[١].

أما في الولايات المتحدة الأمريكية فيجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسب الآلي شريطة الحصول على إذن تفتيش صادر من القاضي.

أما في اليابان حيث لا توجد نصوص تشريعية، فقد أقرت المحاكم اليابانية شرعية التنصت على شبكات الحاسب الآلي للبحث عن أدلة[٢].

ثانياً: شروط تفتيش النظام المعلوماتي وبطلانه والسلطات المختصة بالتفتيش

سنبين في المطلب الأول من هذا المبحث شروط تفتيش النظام المعلوماتي، ثم نتناول في المطلب الثاني بطلان تفتيش النظام المعلوماتي، أما في المطلب الثالث فسنتطرق إلى السلطات المختصة بالتفتيش.

١ ـ شروط تفتيش النظام المعلوماتي

يمكن تقسيم شروط تفتيش النظم المعلوماتية للحاسب الآلي إلى نوعين، شروط موضوعية وأخرى شكلية:

(١) حسين الغافري، المرجع السابق. ص ٤٨٤ وما بعدها. انظر أيضاً عبدالفتاح حجازي، المرجع السابق. ص ٣٨٢ وما بعدها.

(٢) هلالي عبداللاه أحمد، المرجع السابق، ص ٧٧ وما بعدها. انظر أيضاً عبدالفتاح حجازي، المرجع السابق ص٣٨٢ وما بعدها.

أ ـ الشروط الموضوعية لتفتيش نظم الحاسب الآلي

تتضمن الشروط الموضوعية لتفتيش نظم الحاسب الآلي الشروط التالية :

ـ سبب التفتيش

الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يجوز إصداره إلا بعد وقوع جناية أو جنحة وترجحت نسبتها إلى متهم معين ، وتوافر إمارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره . وهو ما أقرته محكمة النقض المصرية في حكم لها ذكرت فيه أن : « الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة ـ جناية أو جنحة ـ واقعة بالفعل وترجحت نسبتها إلى متهم معين ، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية»[١].

وبناء على ذلك وتطبيقاً على الجرائم المعلوماتية فإنه لا بد ليكون التفتيش مشروعاً أن نكون :

ـ بصدد جريمة معلوماتية حدثت بالفعل سواء أكانت جنحة أم جناية .

ـ لا بد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة المعلوماتية أو المشاركة في ارتكابها .

ـ لا بد من توافر إمارات قوية أو قرائن على وجود أجهزة أو أدلة معلوماتية تفيد في كشف الحقيقة وإدانة المتهم .

وسنتطرق فيما يلي لتفصيل ذلك :

١ ـ أن نكون بصدد جريمة معلوماتية سواء جنحة أم جناية : وتعرف الجريمة المعلوماتية بأنها أي سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة[٢].

(١) انظر حكم محكمة النقض المصرية لعام ١٩٦٧م . مجموعة أحكام النقض س ١٨ رقم (١٩٥) . ص٩٦٥ . نقض ١٦ أكتوبر لعام ١٩٦٧م . انظر أيضاً هلالي عبداللاه أحمد ، المرجع السابق . ص ١٠٢ وما بعدها .

(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٣٨٥ وما بعدها .

أو هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي[١]. أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات[٢]. وهناك العديد من التشريعات التي حرصت على استحداث نصوص قانونية خاصة للجرائم المعلوماتية، من ذلك القانون الإنجليزي في شأن إساءة استخدام الحاسب الآلي (Computer Misuse Act) لعام ١٩٩٠م. وكذلك فقد صدر في الولايات المتحدة الأمريكية القانون الفيدرالي لعام ١٩٨٦م لمواجهة الاحتيال وإساءة استخدام الإنترنت، وكذلك فقد أصدرت العديد من الولايات الأمريكية مثل نيويورك وكاليفورنيا وواشنطن وغيرها قوانين لمكافحة الجرائم المعلوماتية[٣]. كما أصدرت المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية في عام ١٤٢٨هـ. ويهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي :

أ ـ المساعدة على تحقيق الأمن المعلوماتي.

ب ـ حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .

ج ـ حماية المصلحة العامة، والأخلاق، والآداب العامة .

د ـ حماية الاقتصاد الوطني[٤].

والإذن بالتفتيش غير جائز إلا إذا كانت الجريمة جناية (Felony) أو جنحة (Misdemeanor) ومن ثم تم استبعاد المخالفات (Violations) لأنها قليلة الأهمية ولا تستحق التعرض لحريات الأشخاص أو انتهاك خصوصياتهم[٥].

---

(١) هشام فريد، المرجع السابق . ص ٣٠ .

(٢)هشام فريد، المرجع السابق . ص ٣٠ .

(٣) عبدالفتاح حجازي، المرجع السابق . ص ٣٨٥ وما بعدها .

(٤) المادة (٢)، نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بقرار مجلس الوزراء رقم (٧٩) وتاريخ ٧/ ٣/ ١٤٢٨هـ، والمرسوم الملكي رقم (م / ١٧) وتاريخ ٨/ ٣/ ١٤٢٨هـ الصادر بالمصادقة عليه.

(٥) خالد الحلبي، المرجع السابق . ص ١٥٣ . انظر أيضاً خالد ممدوح إبراهيم، المرجع السابق. ص٢١١ وما بعدها .

٢ ـ تورط شخص أو أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيها: يجب أن تتوافر في حق الشخص المطلوب تفتيشه أو تفتيش مسكنه أو حاسبه الآلي، دلائل كافية تؤدي إلى الاعتقاد بأنه قد أسهم في ارتكاب جريمة معلوماتية بصفته فاعلاً (Principal) أو شريكاً (Accomplice) في هذه الجريمة[١].

٣ ـ توافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تساعد في كشف الحقيقة لدى المتهم بارتكاب جرائم معلوماتية : يجب عدم إجراء التفتيش إلا إذا توافرت للمحقق دلائل كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة المعلوماتية أو أشياء متحصلة منها أو أي مستندات أو محررات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى الشخص المتهم بارتكاب جريمة معلوماتية. وهذا الشرط ذاته متطلب في حال التفتيش بصدد جريمة تقليدية، ذلك أنه لا يمكن تفتيش شخص أو تفتيش مسكنه ما لم تكن هناك دلائل كافية على ارتكاب الشخص إحدى الجرائم بوصفه فاعلاً أو شريكاً ، وقد نص نظام الإجراءات الجزائية السعودي على أن « للمحقق أن يفتش المتهم ، وله تفتيش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة، ويراعى في التفتيش حكم المادة الثانية والأربعين من هذا النظام كما نص نظام الإجراءات الجزائية السعودي أيضاً على أنه « يراعى في ضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات والمحادثات الهاتفية وغيرها من وسائل الاتصال أحكام المواد من الخامسة والخمسين إلى الحادية والستين من هذا النظام»[٢].

---

(١) والدلائل تعني علامات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها بأن جريمة ما قد وقعت ، وأن شخصاً معيناً هو مرتكبها ومن ثم هي مجرد افتراضات قد لا تصلح وحدها سبباً للإدانة. أو هي ذلك القدر الضئيل المبني على احتمال معقول تؤديه الظروف والاستنتاجات التي تكفي للاعتقاد بارتكاب جريمة وتبرر اتخاذ بعض الإجراءات الماسة بالحرية الفردية ضماناً لحسن سير العدالة (Proper Conduct of Justice) . انظر خالد إبراهيم ، المرجع السابق . ص ٢١١ وما بعدها .

(٢) المادة (٨١) و (٨٢) من نظام الإجراءات الجزائية السعودي ، وفيما يتعلق بالجرائم المعلوماتية والتي يصدر الإذن بالتفتيش لضبط وقوعها فإنه يقصد بالدلائل الكافية بالنسبة لها مجموعة الأمارات والمظاهر التي تكفي وفقاً للسياق العقلي والمنطقي ترجيح ارتكابها ونسبتها إلى المتهم .

٤ ـ تحديد محل التفتيش: يجب تحديد محل التفتيش وهو الشيء الذي يقع عليه التفتيش للحصـول على أدلة في الجرائـم المعلوماتية وخاصة الجرائم المتعلقة بالإنترنت وهو جهاز الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الاتصال الخاصة به . بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش ، والأماكن التي توجد بها تلك الأشياء[١].

وتشـمل المكونـات الماديـة للحاسـب الآلي وحـدة الإدخـال (Input Unit) أو وحدة الذاكرة الرئيسـة (Main Memory) ووحدة الحسـاب والمنطق (Arithmetic and Logic Unit) ووحدات الإخراج (Output unit) ووحدات التخزين الثانوية (Secondary Storage Unit) . أما المكونات المعنوية للحاسـب الآلي فإنها تنقسـم إلى الكيانـات المنطقيـة الأساسـية أو برامج التطبيقات سـابقة التجهيـز وبرامج التطبيقات المستخدمة من قبل مستخدم الحاسب الآلي . كما يستلزم الحاسب الآلي بمكوناته السابقة مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسب الآلي (Computer Operators) ومبرمجـو الحاسـب الآلي (Programmers) ، وقـد يكونون من المحللين أو مهندسي الصيانة والاتصالات، أو من مديري النظم المعلوماتية (Information Systems). أو مـن أي أشـخاص آخريـن يكـون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة (Laptops)[٢].

أما المنازل (Homes) وما في حكمها لتفتيش نظم الحاسب الآلي فيقصد بها كافة محال الإقامة (Residences) أو المأوى والملحقات المخصصة لمنافعها والتي يشغلها الشخص سـواء بصفة دائمة أو مؤقتة وسـواء كانت ثابتة أم متنقلة، متى ما وجدت فيها مكونات الحاسب الآلي ، سواء أكانت مكونات مادية أم منطقية أم شبكات اتصال خاص، وتخضع عملية التفتيش هنا لذات شروط وقواعد إجراءات تفتيش المساكن .

---

(١) عـلي عدنـان الفيل ، المرجع السـابق . ص ٤٩ وما بعدها . انظر أيضاً سـليمان أحمد فضل، المرجع السابق . ص ٣٠١ وما بعدها .

(٢) حسـين الغافري ، المرجع السـابق . ص ٤٩٠ وما بعدها . انظر أيضاً عبدالفتاح حجازي، المرجع السابق . ص ٣٨٧ وما بعدها .

ب ـ الشروط الشكلية لتفتيش نظم الحاسب الآلي

بالإضافة إلى الشروط الموضوعية لتفتيش نظم الحاسب الآلي والتي سبق تناولها توجد شروط أخرى ذات طابع شكلي يجب الالتزام بها عند القيام بالتفتيش وذلك حماية للحريات الفردية من التعسف أو الانحراف أو استغلال السلطة ، وهذه الشروط تتمثل فيما يلي :

ـ أن يكون الأمر بالتفتيش مسبباً

يعد من الضمانات المقررة في قوانين الإجراءات الجنائية تسبيب أمر التفتيش (Search Warrant) ، ويقصد بالتسبيب أن الأمر الصادر بالتفتيش يجب أن يكون مبنياً على عدد من القرائن والدلائل التي تدل على أن في المكان أو الشخص المراد تفتيشه ما يفيد في كشف الحقيقة. وقد نص نظام الإجراءات الجزائية السعودي على أنه «تفتيش المساكن عمل من أعمال التحقيق ولا يجوز الالتجاء إليه بناء على اتهام موجه إلى شخص يقيم في المسكن المراد تفتيشه بارتكاب جريمة، أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة . وللمحقق أن يفتش أي مكان ويضبط كل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها، وكل ما يفيد في كشف الحقيقة بما في ذلك الأوراق والأسلحة ، وفي جميع الأحوال يجب أن يُعدّ محضراً عن واقعة التفتيش يتضمن الأسباب التي بُني عليها ونتائجه، مع مراعاة أنه لا يجوز دخول المساكن أو تفتيشها إلا في الأحوال المنصوص عليها نظاماً وبأمر مسبب من هيئة التحقيق والإدعاء العام»[1] .

فالتفتيش باعتباره إجراء من إجراءات التحقيق ، يلزم أن يكون قد تم اتخاذه لغاية محددة وهي الكشف عن أشياء تتعلق بالجريمة أو تفيد في إظهار الحقيقة، كأن يكون قائماً بقصد التوصل إلى ما يفيد ارتكاب جريمة احتيال معلوماتي أو سرقة مال معلوماتي أو غيرها من الجرائم المعلوماتية[2].

وفي الحقيقة فإن صياغة وتنفيذ أوامر التفتيش في الجرائم المعلوماتية يشكلان تحدياً

(١) المادة (٨٠)، نظام الإجراءات الجزائية السعودي . انظر أيضاً هلالي عبداللاه أحمد ، المرجع السابق. ص ١٦٣ وما بعدها .

(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٣٥٥ وما بعدها .

كبيراً . إذ إن الأدلة المطلوب الحصول عليها قد تختلط بكميات هائلة من البيانات الأخرى التي قد لا يكون لها علاقة بالتحقيق ، إضافة إلى أن الوسيلة التي تخزن بها قد تكون جزءاً مكملاً من نظام تشغيل معلوماتي عائد لمؤسسة أخرى لا علاقة لها بهذا التحقيق . وما لم يشكل النظام ذاته أداة للجريمة المدعى ارتكابها فإن ضبط النظام وتعطيله برمته قد يسبب خسارة غير مبررة لأصحاب المؤسسة أو لعملائها[1]. ومثال ذلك قضية اندرو جونسون ضد مكتب التحقيقات الفيدرالية الأمريكية (FBI) ، والتي ضبط فيها مكتب التحقيقات الفيدرالية المكونات الحاسوبية وملفات البيانات لإحدى شركات البرامج الحاسوبية، الأمر الذي أوقف نشاط الشركة بشكل كامل . ما ترتب عليه خسائر مادية كبيرة لها ولعملائها . ولم يتم مقاضاة الشركة ولا رئيسها، فقد اعتقد مكتب التحقيقات الفيدرالية أن المادة التي تم ضبطها تحتوي على أدلة لجريمة ارتكبها أحد عملاء الشركة[2].

ـ الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش

ويعد هذا الشرط من أهم الشروط الشكلية التي قررها القانون، والغاية من تقرير هذا الشرط تتمثل في اطمئنان الخاضع لهذا التفتيش إلى سيره وفقاً للقانون والحيلولة دون تعسف الجهة التي تقوم بالتفتيش[3]. وقد نص نظام الإجراءات الجزائية السعودي على أنه « يتم تفتيش المسكن بحضور صاحبه أو من ينيبه أو أحد أفراد أسرته البالغين المقيمين معه ، وإذا تعذر حضور أحد هؤلاء وجب أن يكون التفتيش بحضور عمدة الحي أو من في حكمه أو شاهدين، ويُمكّن صاحب المسكن أو من ينوب عنه من الاطلاع على إذن التفتيش ويثبت ذلك في المحضر »[4].

أما القانون المصري فيستلزم إذا كان التفتيش قد تم من النيابة العامة لمنزل المتهم ، أن يتم هنا التفتيش في حضور المتهم ، فإذا لم يتيسر ذلك لغياب المتهم أو لرفضه الحضور يتم التفتيش بحضور من ينيبه كلما كان ذلك ممكناً.

(١) عبدالفتاح حجازي ، المرجع السابق . ص ٣٥٧ وما بعدها .
(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٣٥٨ . انظر أيضاً حسين الغافري ، المرجع السابق. ص ٤٩٣ وما بعدها .
(٣) عبدالفتاح حجازي ، المرجع السابق . ص ٣٥٩ وما بعدها .
(٤) المادة (٤٦) ، نظام الإجراءات الجزائية السعودي .

فـإن تعذرت هـذه الإنابة كذلك سـواء لرفض المتهم أو لعدم إمـكان الاتصال به مقدماً قبل التفتيش حتى لا يضيع عنصر المفاجأة كان للنيابة العامة إجراء التفتيش بدون حضور أحد[١].

ـ تحرير محضر التفتيش

حيث إن التفتيش يعد حسب الأصل عملاً من أعمال التحقيق فإنه يجب تحرير محضر يثبـت فيـه كل ما تـم من إجراءات ، وما نتج عن التفتيش من أدلـة . ولم يتطلب القانون شـكلاً خاصاً لهذا المحضر، ما يعني أنه لا يشـترط لصحته سـوى ما تسـتوجبه القواعد العامة في المحاضر بشكل عام . كأن يكون مكتوباً باللغة الرسمية وهي في المملكة اللغة العربيـة، وأن يحمل تاريخ تحريره وتوقيع الشـخص الـذي قام بتحريره . وقد نص نظام الإجراءات الجزائية السعودي على أنه يجب أن يتضمن محضر التفتيش ما يأتي :

١ ـ اسم من قام بإجراء التفتيش ووظيفته وتاريخ التفتيش وساعته .
٢ ـ نـص الإذن الصـادر بإجـراء التفتيـش ، أو بيان الضرورة الملحـة التي اقتضت التفتيش بغير إذن .
٣ ـ أسماء الأشخاص الذين حضروا التفتيش ، وتوقيعاتهم على المحضر .
٤ ـ وصف الأشياء التي ضبطت وصفاً دقيقاً .
٥ ـ إثبات جميع الإجراءات التي اتخذت أثناء التفتيش والإجراءات المتخذة بالنسبة للأشياء المضبوطة[٢] .

د ـ أسلوب تنفيذ التفتيش

لإجراءات تنفيذ التفتيش على نظم الحاسب الآلي والإنترنت خصوصية تميزها عن الإجراءات المتبعة في التفتيش الواقع على الأشخاص أو المساكن ، لذا يجب على المحقق أن يتخذ إجراءات وتحريات شاملة ودقيقة قبل القيام بإجراء التفتيش وهي كالتالي :

١ ـ تحديـد نوع النظام المعلوماتي المراد تفتيشـه . فيجـب على المحقق أن يحصل على

(١) المادة (٩٢)، قانون الإجراءات الجنائية المصري .
(٢) المـادة (٤٧) ، نظـام الإجـراءات الجزائيـة السـعودي ، انظـر أيضاً عـلي الفيل ، المرجع السـابق ، ص ٥٢ وما بعدها . انظر أيضاً علي الطوالبة ، المرجع السابق . ص٥٥ وما بعدها .

المواصفات الشكلية للنظام المعلوماتي المراد تفتيشه .

٢ ـ تجميع فريق عمل يتكون من المحقق إضافة إلى الخبراء الفنيين ورجال الضبط الجنائي المكلفين بالمهمة قبل القيام بالتفتيش ((١)).

٣ ـ وضع خطة لتنفيذ التفتيش بناء على المعلومات التي تم الحصول عليها عن النظام المعلوماتي المراد تفتيشه .

٤ ـ يجب إعطاء مسودة إذن التفتيش عناية خاصة من حيث تضمنها على وصف لمحل التفتيش ، والملكية المراد ضبطها بشكل محدد ودقيق مع تقديم شرح للاستراتيجية التي سيتم اتباعها عند إجراء التفتيش. وتفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة ، فمثلاً يذكر المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسب الآلي أربع طرق أساسية ممكنة للتفتيش في النظام المعلوماتي هي :

أ ـ تفتيش الحاسب الآلي وطبع نسخة ورقية (Paper Copies) من ملفات معينة في ذات الوقت .

ب ـ تفتيش الحاسب الآلي وعمل نسخة إلكترونية (Electronic Copy) من ملفات معينة في ذات الوقت .

ج ـ عمل نسخة إلكترونية طبق الأصل (Electronic Exact Copy) من جهاز التخزين بالكامل في الموقع ، ثم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة .

د ـ ضبط جهاز الحاسب الآلي وملحقاته ومراجعة محتوياته خارج الموقع[٢].

---

(١) علي الطوالبة ، المرجع السابق . ص ٥٥ .

(٢) تم وضع هذا المرشد (U.S Guidelines For Search and Seizure of Computers) عام ١٩٩٤م . وصدر له ملحقان (Annexes) في عامي ١٩٩٧م و ١٩٩٩م ، وقام بإعداده مجموعة عمل (Working Group) في قسم جرائم الحاسب الآلي والملكية الفكرية (Intellectual Property) بإشراف أستاذ القانون الجنائي الأمريكي (Orin Kerr) ، ولقد صدرت له عدة تعديلات كان آخرها في عام ٢٠٠٢م. انظر أيضاً هلالي عبداللاه أحمد ، المرجع السابق ص ١٦٤ . انظر أيضاً حسين الغافري، المرجع السابق . ص ٤٩٤ وما بعدها .

هـ ـ تحديد مدة الإذن بالتفتيش

يجب أن يكون إذن التفتيش محدد المدة ويكون المحقق ملتزماً بالقيام به خلال هذه المدة ، ويراعي المحقق عند إصداره لهذا الإذن ألا تكون مدته تتجاوز المدة المعقولة، أي أن لا تكـون مدتـه طويلة، حتى لا يبقى الصادر في حقه الإذن بالتفتيش مهدداً في حريته وحرمة مسكنه مدة طويلة [١] .

٢ ـ بطلان تفتيش النظام المعلوماتي

يكـون الدليـل الإلكـتروني باطلاً إذا تم الحصول عليه بشـكل مخالف للقانون ، ولهذا الأمر أهمية بالغة لما يترتب على بطلان الدليل من آثار ، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد إليه في إدانة الجاني ، فإذا ما شاب التفتيش الواقع على النظـام المعلومـاتي عيب فإنـه يبطله، والتفتيش الذي يقوم بـه المحقق بغير الشروط التي نص عليها القانون يعد باطلاً بطلاناً مطلقاً ولا يجوز التمسك بما ورد في محضر التفتيش كما لا يجوز للمحكمة أن تعتمد عليه في حكمها[٢] .

٣ ـ السلطات المختصة بالتفتيش

الأصل أن يتم التفتيش سواء للمساكن أو للأشخاص بمعرفة سلطات التحقيق الأصليـة باعتبارهـا صاحبـة الاختصاص الأصيـل في القيام بأي إجـراء يمس حريات الأفـراد. وسـلطات التحقيـق الأصليـة هي النيابة العامـة بصفة أصليـة . وينص قانون الإجـراءات الجنائيـة المصري على أن « تفتيش المنازل عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا بناء على تهمة موجهة إلى شـخص يقيم في المنزل المراد تفتيشـه بارتكاب جناية أو جنحة أو بإشتراكه في ارتكابها ، أو إذا وجدت قرائن على أنه حائز لأشياء تتعلق بالجريمـة . ولقـاضي التحقيق أن يفتش أي مكان ويضبط فيه الأوراق والأسـلحة وكل

(١) خالد الحلبي ، المرجع السـابق . ص ١٥٥ وما بعدها . انظر أيضاً خالد إبراهيم ، المرجع السـابق. ص ٢٢٢ وما بعدها .

(٢) هـلالي عبداللـاه أحمـد ، المرجع السـابق . ص ٢٢٧ وما بعدها . انظر أيضاً عـلي الطوالبة، المرجع السابق . ص ١٧٧ وما بعدها .

ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه ، وكل ما يفيد في كشف الحقيقة . وفي جميع الأحوال يجب أن يكون أمر التفتيش مسبباً[١].

وهذا النص يسري على النيابة العامة وعلى قاضي التحقيق إذ نص قانون الإجراءات الجنائية المصري على أنه « فيما عدا الجرائم التي يختص قاضي التحقيق بتحقيقها وفقاً لأحكام المادة (٦٤) تباشر النيابة العامة التحقيق في مواد الجنايات والجنح طبقاً للأحكام المقررة لقاضي التحقيق»[٢].

إلا أن قانون الإجراءات الجنائية المصري أجاز لرجال الضبط القضائي من غير أعضاء النيابة العامة القبض على المتهمين في بعض الجرائم في حالة التلبس بها ثم تفتيشهم وتفتيش مساكنهم[٣].

وسلطة التحقيق غير ملزمة بإجراء التحقيق بنفسها فقد لا يسمح وقت المحقق بذلك خصوصاً إذا تعددت الأمكنة المراد تفتيشها أو الأشخاص المراد تفتيشهم . لذلك يجوز للمحقق أن يقوم بندب أحد رجال الضبط القضائي للقيام به بناء على ما يسمى «إذن أو أمر التفتيش»[٤].

أما نظام الإجراءات الجزائية السعودي فقد نص على أنه «لا يجوز لرجال الضبط الجنائي الدخول في أي محل مسكون أو تفتيشه إلا في الأحوال المنصوص عليها نظاماً ، بأمر مسبب من هيئة التحقيق والادعاء العام، وما عدا المساكن فيكتفى في تفتيشها بإذن مسبب من المحقق»[٥].

كما نص نظام الإجراءات الجزائية السعودي على أنه « لا يجوز تفتيش غير المتهم أو مسكن غير مسكنه إلا إذا اتضح من أمارات قوية أن هذا التفتيش سيفيد في التحقيق»[٦]

(١) المادة (٩١/ ١) ، قانون الإجراءات الجنائية المصري .
(٢) المادة (١٩٩) ، قانون الإجراءات الجنائية المصري .
(٣) المواد (٣٤ – ٤٧) ، قانون الإجراءات الجنائية المصري .
(٤) رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري ، دار الجيل للطباعة، القاهرة، ١٩٨٩م. ص ٤٠٥ وما بعدها . انظر أيضاً بكري يوسف بكري ، المرجع السابق . ص ١١٣ وما بعدها.
(٥) المادة (٤١) ، نظام الإجراءات الجزائية السعودي .
(٦) المادة (٥٤) ، نظام الإجراءات الجزائية السعودي .

. وبناء على ذلك ، يشترط لصحة إصدار الأمر بالتفتيش وفقاً لنظام الإجراءات الجزائية السعودي أن تتوافر لدى سلطة التحقيق قرائن على اتهام شخص بارتكاب جريمة إما بصفته فاعلاً أصلياً أو شريكاً فيها، أو أن تتوافر دلائل أو قرائن على حيازته (Possession) لأشياء تتعلق بالجريمة .

ثالثاً: إجراءات ضبط أدلة الجرائم المعلوماتية وأساليب تنفيذ التفتيش

سنبين في المطلب الأول من هذا المبحث إجراءات ضبط أدلة الجرائم المعلوماتية ، ثم سنتناول في المطلب الثاني أساليب تنفيذ التفتيش .

١ ـ إجراءات ضبط أدلة الجرائم المعلوماتية

الغاية من التفتيش هي ضبط شيء يتعلق بالجريمة ويفيد في التحقيق القائم بشأنها ، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أم شيئاً نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة . ويقصد بالضبط وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة والوصول إلى مرتكب الجريمة . وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق بحسب الجهة التي قامت به . فإذا كانت جهة تحقيق عد إجراءً تحقيقياً، أما إذا كانت جهة استدلال فيعد إجراءً استدلالياً .

فإذا تم الضبط نتيجة لتفتيش المتهم أو مسكنه ، ففي هذه الحالة يعد الضبط من إجراءات التحقيق وليس من إجراءات الاستدلال ، فتفتيش المساكن يعد من اختصاص سلطة التحقيق[١] .

وقد نص قانون الإجراءات الجزائية الاتحادي الإماراتي على أنه «لمأموري الضبط القضائي أن يضبطوا الأشياء التي يحتمل أن تكون قد استعملت في ارتكاب الجريمة أو نتجت عن ارتكابها أو يحتمل أن تكون قد وقعت عليها الجريمة وكذلك كل ما يفيد في كشف الحقيقة»[٢] .

(١) خالد الحلبي ، المرجع السابق . ص ١٦٨ وما بعدها .

(٢) المادة (٦١) ، قانون الإجراءات الجزائية الاتحادي الإماراتي . وهذا النص يقابله نص المادة (٥٥) من قانون الإجراءات الجنائية المصري .

كـما نـص قانون الإجراءات الجزائية الاتحادي على أنه « لمأمور الضبط القضائي أن يفضها ، وعليه إثباتها في محضر التفتيش وعرضها على النيابة العامة»[١].

كـما نـص نظام الإجـراءات الجزائية السـعودي بأن على المحقـق أن «يضبط كل ما يحتمل أنه اسـتعمل في ارتكاب الجريمة أو نتج عنها ، وكل ما يفيد في كشـف الحقيقة بما في ذلك الأوراق والأسلحة[٢].

وبحسب النصوص القانونية السابقة فإن هدف التفتيش هو ضبط الأشياء التي تفيد في كشف الحقيقة ، أي الأشياء التي تعد في ذاتها دليلاً على الجريمة ، أو يمكن استخراج هذا الدليل منها .

وهذه الأشياء قد تكون هي ما استعمل في ارتكاب الجريمة، وقد تكون ما نتج عن ارتكابها ، وقد تكون الموضوع الذي وقعت عليه الجريمة[٣].

ولا يفـرق القانـون في مجال الضبط بـين المنقـول (Personal Property) والعقار (Real Property) فكلاهمـا يمكـن ضبطه ، كذلك يسـتوي أن يكـون الشيء المضبوط مملوكاً لمتهم أو لغيره ، والقاعدة أن الضبط لا يرد إلا على شيء مادي. أما الأشياء المعنوية فلا تصلح بطبيعتها محلاً للضبط[٤].

وقد نص قانون الإجراءات الجنائية المصري على أن توضع هذه الأشياء والأوراق في حـرز مغلـق يختم ويكتب عليه تاريخ المحضر المحرر لضبط تلك الأشـياء ، ولا يجوز فض هذه الأحكام إلا بحضور المتهم أو وكيله أو من ضبط لديه[٥].

---

(١) المـادة (٥٨) ، قانـون الإجراءات الجزائية الاتحادي الإماراتي . وهذا النص تقابله المادة (٥٢) من قانون الإجراءات الجنائية المصري .

(٢) المادة (٨٠) ، نظام الإجراءات الجزائية السعودي .

(٣) هلالي عبداللاه أحمد ، المرجع السابق . ص ٨١ وما بعدها . انظر أيضاً عبدالفتاح حجازي، المرجع السابق . ص ٢٠٧ وما بعدها .

(٤) مصطفى موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، بدون ناشر ، ٢٠٠٩م . ص ٢٠٨ وما بعدها . انظر أيضاً علي الفيل ، المرجع السابق . ص ٥٢ وما بعدها .

(٥) المادة (٦٢) ، قانون الإجراءات الجنائية المصري .

والهدف من ذلك هو المحافظة على هذه الأشياء والأوراق فلا يرد عليها تغيير أو تبديل.

مدى صلاحية ضبط أدلة الجرائم المعلوماتية :

ونفرق في هذا الشأن بين حالتين :

الحالة الأولى : الجرائم الواقعة على المكونات المادية للحاسب الآلي:

لا يثير ضبط المكونات المادية للحاسب الآلي أي مشاكل في الفقه المقارن، إذ يمكن ضبط الأدلة بموجب القواعد التقليدية للتفتيش المنصوص عليها في قانون الإجراءات الجنائية . وبالتالي لا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات وهي :

١ ـ وحدة الإدخال (Input Unit) : بما تشمله من مفردات كلوحة المفاتيح (Keyboard) ، وشاشات اللمس (Touch Screen) ، ونظام الفأرة (Mouse System) ، ونظام القلم الضوئي (Light Pen System)، ونظام القراءة الضوئية للحروف (Optical Character Recognition System)، ونظام قراءة الحروف المغناطيسية (Magnetic Character Recognition System)، ونظام إدخال الأشكال والرسومات .

٢ ـ وحدة الذاكرة الرئيسة (Main Memory): سواء كانت ذاكرة القراءة فقط (Read Only Memory) أم كانت ذاكرة للقراءة والكتابة معاً (Random Access Memory) .

٣ ـ وحدة الحساب والمنطق (Arithmetic and Logic Unit) : وتشمل مجموعة من الدوائر الإلكترونية (Electric Circuits) والمسجلات .

٤ ـ وحدة التحكم (Control Unit): وما تستعين به من مسجلات وسماعات منطقية .

٥ ـ وحدة المخرجات (Output Unit) : وما تشمله من وسائط كالشاشة (Monitor)، والطابعة (Printer)، والرسم (Plotter)، والمصغرات الفلمية (Micro Filmed Prints).

٦ ـ وحدات التخزين الثانوية (Secondary Storage Units) : بما تشمله من أقراص مغناطيسية (Magnetic Discs) بنوعيها المرن (Floppy Disk) والصلب (Hard Disk) والأشرطة المغناطيسية (Magnetic Tape) والفلاش ميموري (Flash Memory) والسي دي (CD)[١].

الحالة الثانية : الجرائم الواقعة على المكونات غير المادية للحاسب الآلي

نظراً لكون الضبط محله في مجال الجرائم المعلوماتية البيانات المعالجة إلكترونياً ، فقد ثار التساؤل : هل يصلح هذا النوع من البيانات الإلكترونية (Electronic Data) لأن يكون محلاً للضبط الذي يعني وضع اليد على شيء مادي ملموس ؟ (Tangible Thing).

وقد انقسم الفقه القانوني حول مدى إمكانية ضبط الدليل في الجرائم المعلوماتية خصوصاً فيما يتعلق بالبيانات الإلكترونية المجردة عن الدعامة المادية المخزنة عليها . وكذلك ما إذا كانت تقبل التعامل معها وفق النصوص القانونية التقليدية المعمول بها في ضبط الأدلة الجنائية[٢].

فيرى جانب من الفقه أن البيانات الإلكترونية للحاسب الآلي لا تصلح لأن تكون محلاً للضبط (Subject to Seizure) ،وأنه لا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، ويستند هذا الرأي إلى أن النصوص القانونية التقليدية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة (Tangible Things) ، فقانون الإجراءات الجنائية الألماني ، جعل الضبط (Seizure) يقع على الأشياء المادية المحسوسة ، وأن البيانات المعالجة إلكترونياً لا يمكن ضبطها مجردة إلا إذا تم تحويلها إلى كيان مادي مطبوعة على الورق، أو عن طريق التصوير الفوتوغرافي [٣] .

---

(١) هلالي عبداللاه أحمد ، المرجع السابق . ص ١٩٧ وما بعدها . انظر أيضاً عبدالفتاح حجازي، المرجع السابق . ص ٢٠٩ وما بعدها .

(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٢١٠ وما بعدها . انظر أيضاً خالد الحلبي ، المرجع السابق . ص ١٧٠ وما بعدها .

(٣) المواد (٩٤) ، (١٦١) ، قانون الإجراءات الجنائية الألماني .

ويـرى الاتجـاه الآخـر أن البيانـات الإلكترونية ما هـي إلا ذبذبـات إلكترونية أو موجات كهرومغناطيسية تقبل التخزين والحفظ والتسجيل على وسائط مادية ، ويمكن نقلهـا وبثهـا واسـتقبالها وإعادة إنتاجها، وبالتـالي فإن وجودها المـادي لا يمكن تجاهله وإنكاره[١].

فقانـون الإجـراءات الجنائيـة الكندي ، يجيز ضبـط الأشـياء ذات الطبيعة المادية، وضبـط المكونات المعنوية من المعطيات المخزنة في الأقراص والدعامات المادية، فضبط الأشياء المخزنة في الحاسب الآلي يشمل ضبط كياناته المادية والمعنوية[٢].

كـما ينـص قانـون الإثبـات الكنـدي (Code of Evidence) على أنه «مـا لم يرد ما يخالف ذلك في أمر التفتيش وضبط الدفاتر والسـجلات الخاصة بمؤسسـة مالية يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخ من المواد المكتوبة ، وينطبق هذا النص سواء كانت السجلات مكتوبة أم كانت على شكل إلكتروني ، أما إذا كان التفتيش في مكان غير تابع لمؤسسـة مالية ، فإن أخذ السـجلات الأصلية أو الحصول على نسخ منها فحسب ، أمر يخضع بشكل عام للسلطة التقديرية للشرطة»[٣].

ونـرى ضرورة تطوير النصوص القانونية التقليديـة المتعلقة بالتفتيش والضبط في جرائـم المعلوماتية ، لتشـمل البيانات الإلكترونية ، فيجـب أن يدخل في نطاق التفتيش والضبـط ، التفتيـش عـن المكونـات المعنويـة للحاسـب الآلي ، كالبيانـات الإلكترونية والمراسلات والاتصالات الإلكترونية ، وإلا أدى ذلك إلى إيجاد العديد من الصعوبات أمـام جهـات التحقيق فيـما يتعلق بجمع الأدلـة التي تفيد في كشـف الحقيقة في الجريمة المعلوماتية ، وقد يؤدي عدم اعتبار المكونات المعنوية للحاسـب الآلي من الأشـياء التي تخضع للتفتيش إلى عدم قيام الجريمة المعلوماتية وذلك متى كانت هذه المكونات المعنوية هي السبيل الوحيد للوصول إلى حقيقة الجريمة المعلوماتية .

(١) عبدالفتـاح حجـازي ، المرجع السـابق . ص ٢١٠ وما بعدها . انظر أيضاً بكري يوسـف بكري، المرجع السابق . ص ١٣٥ وما بعدها .
(٢) المادة (٤٢١) ، قانون الإجراءات الجنائية الكندي .
(٣) المادة (٢٩) ، قانون الإثبات الكندي .

وإذا كان الأمر قد انتهى بنا إلى ضرورة أن يشمل التفتيش المكونات المعنوية للحاسب الآلي فإنه من الضروري أن يترتب على ذلك إباحة ضبطها.

ويجب على المشرعين أن يمنحوا المحققين سلطة التحفظ على البيانات الإلكترونية والمعطيات المخزنة في الحاسب الآلي محل الجريمة، وكذلك على الأدوات التي تم استخدامها في ارتكابها وكذلك الآثار التي من الممكن أن تفيد في كشف الجريمة وإدانة الجاني .

وتوجد عدة صعوبات تواجه عملية ضبط البيانات الإلكترونية منها :

١ ـ وجود هذه البيانات الإلكترونية في شبكات أو أنظمة معلوماتية تابعة لدولة أخرى ، ما يستدعي تعاون تلك الدولة مع أجهزة الشرطة والتحقيق في عملية التفتيش والضبط[١] .

٢ ـ الحجم الكبير للشبكة المحتوية للبيانات الإلكترونية وبالتالي ضرورة البحث المضني في تلك الشبكة للوصول إلى الأدلة . كما قد يؤدي الضبط إلى عزل النظام المعلوماتي عن مشغليه ومستخدميه لفترة زمنية قد تطول ما قد ينتج عنه أضرار بهؤلاء المشغلين والمستخدمين .

٣ ـ قد يمثل التفتيش والضبط اعتداء على حقوق الغير (Third Parties) ويجب اتخاذ الضمانات الكافية لحماية حقوق الغير من الانتهاك .

٤ ـ كذلك فإن الجاني يستطيع محو أو إتلاف البيانات المطلوب ضبطها لتعلقها بإرتكاب جريمة ما خلال مدة زمنية قصيرة لا تتعدى ثواني معدودة، كما يستطيع الجاني تفسير وجود هذه البيانات في حالة ضبطها بوجود خطأ في النظام المعلوماتي وبالتالي يحاول نفي المسؤولية عنه[٢].

٥ ـ إحجام المجني عليه في هذا النوع من الجرائم عن إبلاغ السلطات، وذلك تحاشياً للأضرار المترتبة على الإبلاغ ، خوفاً على سمعة الجهة المجني عليها من أن تهتز أمام عملائها .

(١) هلالي عبداللاه أحمد ، المرجع السابق . ص ١٩٨ وما بعدها .
(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٢١٠ وما بعدها .

٦ ـ عـدم وجود محققين مؤهلين، لديهم القدرة على كيفية التعامل مع هذه البيانات وضبطها ، الأمر الذي يؤدي إما إلى إهمال الدليل أو إتلافه في أحيان كثيرة[١] .

٢ ـ أسلوب تنفيذ تفتيش النظام المعلوماتي

إن معرفة جهة التحقيق بالأسـاليب المسـتخدمة في ارتكاب الجرائم المعلوماتية هي من الأمور المهمة التي تفيدها في كشف الجناة وتحديد مكان ارتكاب الجريمة، ومن أي جهـاز حاسـب أو طرفيـة إلكترونية نتج الفعل الإجرامي، كما تفيد أيضاً في مناقشـة الشهود واستجواب المتهمين ومواجهتهم بكيفية ارتكاب الجريمة ووسائل ارتكابها .

ولأن الجرائـم المعلوماتيـة كثيرة ومتعددة ، ويسـتخدم مرتكبوها أسـاليب حديثة ومتجـددة فـلا بـد للمحققين في مثل هـذا النوع مـن الجرائم أن يواكبوا هـذه التغيرات والتطـورات ولا بـد لهـم أيضـاً أن يلموا بتقنيـات الأمـن المعلوماتية والحاسـوبية لأنها تساعدهم في معرفة مجريات التحقيق .

وتوجـد العديـد من التقنيات التي تسـتخدم في الأمن المعلوماتي وأمن الشـبكات (Network Security) والتي تكون وثيقة الصلة بالتحقيق، ويكون فهم المحقق لوظائفها وأسـلوب اسـتخدامها عاملاً مسـاعداً له في فهم تقارير خبراء الحاسب الآلي والتي يتم إرفاقها مع محاضر التحقيق ويعتمد عليها عند توجيه الاتهام للمتهم .

ومـن أهـم هذه التقنيـات الجـدار النـاري (Firewall) وأنظمة كشـف الاختراق وأدوات تتبـع مصدر الاتصال الشـبكي (Source of Network Communication) وأدوات مراجعـة العمليـات الحاسـوبية . ولا شـك أنه يعد ضرورياً ـ رغم أن المحقق يسـتعين بخبـير الحاسـب الآلي في التحقيق الذي يجريـه إلا أنه يجب أن يكـون لديه فهم جيد لهذه الوسائل والتقنيات حتى يستطيع التواصل مع الخبير فيما يتعلق بهذه التقنيات والوسائل[٢].

---

(١) عـلي الفيـل ، المرجـع السـابق . ص ٥٨ ومـا بعدهـا . انظر أيضاً خالـد الحلبي ، المرجع السـابق، ص ١٧٤ وما بعدها .

(٢) محمد نصير السرحاني ، مهارات التحقيق الجنائي الفني في جرائم الحاسـوب والإنترنت، رسـالة ماجسـتير ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٤م . ص ٩٨ وما بعدها . انظر أيضاً خالد الحلبي ، المرجع السابق . ص ١٨٦ وما بعدها .

يعـد التفتيـش عن الملفات المخزنة في جهاز الحاسـب الآلي من المهـام المعقدة التي يحتـاج المحقـق إلى القيام بها . حيث إن هذه الملفات يمكـن للجاني تخزينها ونقلها حول العـالم بضغطـة زر . وقـد لا يكـون المحقـق على معرفة بمـكان تخزين الملفـات أو في أي شكل تم تخزينها، فالملفات يمكن تخزينها على قرص مرن أو في عناوين مخبأة في الحاسب الآلي المتنقل (Laptop) الخاص بالجاني أو على خادم (Server) قد يكون على بعد آلاف الكيلومترات ، كما يستطيع الجاني تشفير الملفات أو وضع عناوين مضللة لها . كما يستطيع أيضـاً خلطهـا مع ملفات أخرى لا علاقة لها بالجريمـة . ونتيجة لعدم التحقق من مكان الملفات أو وجودها فإن المحقق سيواجه صعوبات عديدة في تحديد هذه الملفات وبالتالي فإن قيامه بتفتيش أنظمة الحاسب الآلي سيواجه العديد من العقبات[1].

ويمكـن لرجال الضبط الجنائي والمحققين زيادة فرص نجاح تفتيش وضبط نظام الحاسب الآلي باتباع الخطوات الآتية :

١ ـ إصدار إذن من النيابة العامة يجيز تفتيش أنظمة الحاسب الآلي ، على أن يتضمن هذا الإذن تحديد النظام المعلوماتي محل التفتيش بشكل دقيق وعنوان الشخص المراد تفتيش منزله واسمه وصفته ، وتحديد وسائل التفتيش والجهاز الذي سيقوم به، والأشياء التي يتم البحث عنها ومنح فريق التفتيش الصلاحية (Authority) لدخـول النظام المعلوماتي وتفتيشـه وضبط ما يحتويـه من بيانات ومعلومات . ويجب على الفريق الذي يقوم بالتفتيش والضبط معرفة كيفية التعامل مع الأدلة بطريقة فنية صحيحة لتلافي إتلافها أو محوها والمحافظة عليها[2].

٢ ـ تشـكيل فريـق عمل (Task Force) يتكـون من رجل الضبط الجنائي المكلف بالمهمة أو المحقق والمدعي العام وخبير فني متخصص في مجال الحاسب الآلي قبل القيام بالتفتيش .

٣ـ التعرف قدر الإمكان على النظم المعلوماتية المراد تفتيشها قبل وضع خطة التفتيش أو طلب الإذن بالتفتيش .

(١) خالد ممدوح إبراهيم ، المرجع السابق . ص ٢٢٤ وما بعدها .
(٢) خالد الحلبي ، المرجع السابق ، ص ١٨٦ وما بعدها .

٤ ـ وضع خطة لتنفيذ التفتيش تكون مبنية على المعلومات التي تم الحصول عليها عن النظام المعلوماتي المراد تفتيشه ((١)).

٥ ـ المحافظة على مسرح الجريمة (Secure the Scene) بحيث تتم حماية أي بصمات (Fingerprints) قد تكون عائدة للمتهم في مسرح الجريمة ومنع دخول وخروج أي شخص إلى مسرح الجريمة ومنع أي استخدام لأجهزة الحاسب الآلي الموجودة في مسرح الجريمة .

٦ ـ قطع الاتصال الهاتفي (Phone Lines) عن أجهزة الحاسب الآلي الموجودة في مسرح الجريمة . لأن البيانات المخزنة في تلك الأجهزة يمكن أن يتم الدخول إليها من قبل الجاني أو غيره من بعيد (Remotely)((٢)).

٧ ـ عدم تشغيل الحاسب الآلي في حالة ما إذا كان على وضعية « OFF» أما في حالة ما إذا كان الحاسب الآلي في وضعية التشغيل «ON» فهنا يجب استشارة خبير في الحاسب الآلي . فمجرد تشغيل وإطفاء جهاز الحاسب الآلي قد يتسبب في محو وإتلاف الدليل ، كما يجب أخذ صور فوتوغرافية لمسرح الجريمة ثم القيام بقطع الكهرباء عن تلك الأجهزة .

٨ ـ عند نقل مكونات الحاسب الآلي يجب بذل العناية اللازمة لعدم إتلافها بأي شكل من الأشكال وتخزينها في مكان ملائم(٣). حيث إن الأدلة الإلكترونية حساسة تجاه الظروف البيئية كالحرارة والرطوبة والدخان والمجالات الإلكترومغناطيسية (Elector Magnetic Fields) . فهذه المؤثرات البيئية ممكن أن تؤثر وتغير في الدليل الإلكتروني .

٩ ـ يجب عمل نسخة إلكترونية طبق الأصل (Exact Copy) من جهاز التخزين

(١) خالد ممدوح إبراهيم ، المرجع السابق . ص ٢٢٤ . انظر أيضاً حسين الغافري ، المرجع السابق. ص ٤٩٥ وما بعدها .

(2) Michael R. Overly, Best Practices For Seizing Electronic Evidence, Expert Series , 2011 at 5-7.
Thomas A. Mauet and Warren D. Wolfson, Aspen Publishers, Inc. A Wolters KluwerBusiness, 2009 . at 1-9.

(3) Michael Overly, supra , at 2.

(Hard Disk) قبل تشغيل جهاز الحاسب الآلي المراد تفتيشه، لضمان عدم المساس بالدليل الأصلي والتعامل مع النظام من قبل أشخاص مختصين بعلوم الحاسب الآلي .

١٠ ـ ضبط جهاز الحاسب الآلي وإزالة ملحقاته ومراجعة محتوياته خارج الموقع. كما يجب عدم تنفيذ البرامج المخزنة على الحاسب الآلي المضبوطة خشية إتلاف الأدلة الموجودة عليه أو محو الذاكرة (Memory) أو الملفات (Files) ، كما يجب عدم السماح للمشتبه به بالتعامل مع الحاسب الآلي المضبوط .

١١ ـ إعداد نسخة احتياطية عن وسائل تخزين المعلومات الموجودة في مسرح الجريمة[١].

١٢ ـ توثيق جميع نشاطات التحقيق في محاضر التحقيق على أن تتضمن كل ما قام به المحقق من إجراءات ووقت وتاريخ القيام بها، ومعرفة ماهية المعلومات والبيانات المحفوظة وعمل نسخة احتياطية للأدلة المعلوماتية[٢].

رابعاً: وسائل التفتيش في الجرائم المعلوماتية وصعوبات التفتيش عن الدليل المعلوماتي

سنبين في المطلب الأول من هذا المبحث وسائل التفتيش في الجرائم المعلوماتية، ثم نتناول في المطلب الثاني صعوبات التفتيش عن الدليل المعلوماتي.

١ ـ وسائل التفتيش في الجرائم المعلوماتية

يحتاج المحقق في الجرائم المعلوماتية إلى معاينة وفحص الأدلة المعلوماتية ، ويجب أن يكون ملماً بجرائم الحاسب الآلي والإنترنت حتى يتمكن من مواجهة هذه الجرائم .

(١) حسين الغافري ، المرجع السابق . ص ٤٩٧ وما بعدها . انظر أيضاً خالد ممدوح إبراهيم، المرجع لسابق . ص ٢٢٦ وما بعدها .

(٢) حسين الغافري ، المرجع السابق . ص ٤٩٨ وما بعدها . انظر أيضاً خالد الحلبي، المرجع السابق. ص ١٧٧ وما بعدها.

وحيث إن الجرائم المعلوماتية لها طابعها الخاص المميز لها ، فإن التفتيش فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة وبالتالي حل غموضها والوصول إلى الجاني. وتوجد عدة وسائل تساعد على ذلك وهي كالتالي :

أ ـ الوسائل المادية

وهي الأدلة الفنية (Technical Tools) التي عادة ما تستخدم في بنية نظم المعلومات (Information Systems) والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتحديد شخصية الجاني ومن أهمها :

ـ عناوين الإنترنت ، والبريد الإلكتروني ، وبرامج المحادثة

عنوان الإنترنت (Internet Protocol Address) هو المسؤول عن تراسل حزم البيانات عبر الإنترنت وتوجيهها إلى أهدافها ، ويعد هذا البروتوكول الطابع المميز لاستخدام شبكة الإنترنت ، فأي شخص يحصل على بروتوكول الإنترنت (IP) يمكنه الدخول إلى المواقع الافتراضية ، فيستطيع تصفح المواقع والانتفاع بخدماتها. وعملية البحث في قواعد البيانات (Data Bases) لدى مسجلي بروتوكول الإنترنت عملية سهلة ، تمكن سلطة التحقيق من تحديد حائز هذا البروتوكول، عن طريق البحث في قاعدة البيانات (Who Is) الخاصة بالمسجلين (Registrars)[1].

وعنوان الإنترنت يوجد بكل جهاز مرتبط بشبكة الإنترنت، ويتكون من أربعة أجزاء ، كل جزء يتكون من أربع خانات (Four Digits) ، فيكون المجموع اثنتي عشرة خانة كحد أقصى ، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة ، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه .

وفي حالة ارتكاب جريمة باستخدام شبكة الإنترنت فإن المحقق يستطيع البحث عن رقم الجهاز وتحديد موقعه للتوصل إلى الجاني . كما توجد أكثر من طريقة يمكن من

(١) هلالي عبداللاه أحمد ، المرجع السابق . ص ٢١٢ وما بعدها . انظر أيضاً عادل عزام سقف الحيط، المرجع السابق . ص ٢٤٧ وما بعدها .

خلالها معرفة هذا العنوان الخاص بجهاز الحاسب الآلي في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل Windows حيث يتم كتابة Winpcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان IP ، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت[١].

ـ البروكسي (Proxy)

يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة ، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (Cache Memory)[٢].

وتقوم فكرة البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيقوم البروكسي بالتحقق عما إذا كانت هذه الصفحة قد جرى تنزيلها (Downloaded) من قبل ، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية (World Wide Web) أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية.

وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP . ولعل من أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها ما يجعل دوره قوياً في الإثبات (Evidence) عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عن مزود الخدمة (Service Provider)[٣].

ـ برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الاختراق (Hacking Attempts)

(١) عبدالفتاح حجازي ، المرجع السابق . ص ٣٩٤ وما بعدها . انظر أيضاً حسين الغافري، المرجع السابق . ص ٥١٠ وما بعدها .
(٢) حسين الغافري، المرجع السابق . ص ٥١١ وما بعدها .
(٣) عادل سقف الحيط ، المرجع السابق . ص ٢٤٨ وما بعدها . انظر أيضاً حسين الغافري ، المرجع السابق . ص ٥١١ وما بعدها .

التي تتم وتقدم بياناً شاملاً بها إلى المستخدم الذي تم اختراق جهازه ، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق أو محاولة الاختراق ، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق ، وأرقام مداخلها ومخارجها على شبكة الإنترنت ، إضافة إلى معلومات أخرى[١].

ـ نظام كشف الاختراق (Intrusion Detection System)

وهذه الفئة من البرامج تقوم بمراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو شبكة الإنترنت وتقوم بتحليلها بحثاً عن أي إشارة تدل على وجود مشكلة تهدد أمن الحاسب الآلي أو شبكة الإنترنت .

ويحدث ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر شبكة الإنترنت ومراقبة ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور حدوثها في جهاز الحاسب الآلي أو شبكة الإنترنت، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة (Common Characteristics) للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها مصطلح التوقيع، وفي حال كشف النظام وجود أحد هذه التواقيع يقوم بتنبيه مدير النظام بشكل فوري ويقوم بتسجيل البيانات الخاصة بهذا الاعتداء في سجلات خاصة والتي يمكن أن تقدم معلومات قيمة للمحقق تساعده في التعرف على طريقة ارتكاب الجريمة وأسلوبها ومصدرها[٢].

ـ فحص الخادم (Server)

الخادم هو حاسوب ضخم مهمته تحقيق حركة الاتصال بالمواقع والصفحات، وكذلك تحديد مسارات الاتصال المعقدة،على هيئة بيانات رقمية (Digital Data) على شبكة الإنترنت . ومن الخوادم ما لا تكون مهمته تحقيق اتصال مع المواقع والصفحات، وإنما القيام بتحقيق التواصل مع حلقات النقاش والأحاديث المباشرة أو تخزين البريد الإلكتروني.

(١) عادل سقف الحيط ، المرجع السابق . ص ٢٤٩ . انظر أيضاً حسين الغافري ، المرجع السابق. ص ٥١١ وما بعدها .

(٢) علي الطوالبة ، المرجع السابق . ص ١٤٨ وما بعدها . انظر أيضاً خالد الحلبي، المرجع السابق. ص ٢٠٧ وما بعدها .

ـ نظام جرة العسل (Honey Pot)

وهو نظام حاسوبي مصمم خصيصاً لكي يتعرض لأنواع مختلفة من الهجمات عبر شبكة الإنترنت دون أن يكون عليه أي بيانات ذات أهمية ، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعاً خاطئاً بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة ، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء وتحليلها . وهذه المعلومات التي يتم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها وتساعد المحقق في توضيح معالم الجريمة[1].

ـ أدوات تدقيق ومراجعة العمليات الحاسوبية

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجرى على ملفات ونظام تشغيل حاسب آلي معين وتسجيلها في ملفات خاصة يطلق عليها Logs ، وتقوم هذه الأدوات بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة[2].

ـ أدوات الضبط

وهي أدوات تساعد على ضبط الجريمة المعلوماتية، ومنها على سبيل المثال برامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة ، وبرامج التنصت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات ، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي والتسجيل .

ـ الوسائل المساعدة للتحقيق

الوسائل المساعدة للتحقيق هي الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة ، وبرامج كسر كلمات المرور (Passwords) ، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب، وبرامج نسخ البيانات ، وبرامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة، وهناك أيضاً البرامج التي

(١) عبدالفتاح حجازي، المرجع السابق . ص ٣٩٥ . انظر أيضاً خالد الحلبي، المرجع السابق. ص٢٠٧ وما بعدها .

(٢) علي الفيل ، المرجع السابق . ص ٦٨ وما بعدها .

تساعد على استرجاع الملفات (Retrieval of Files) التي قد يلجأ الجاني إلى حذفها نهائياً من الحاسب الآلي . وهناك برامج البحث عن المفردات النصية والتي تستخدم في البحث عبر البيانات عن تلك الملفات التي تحتوي على مفردات معينة عادة ما تكون لها علاقة بالقضية ، وهناك أيضاً برمجيات تحرير الملفات الست عشرية (Hexadecimal Editors) وهي برامج تمكن المحقق من الاطلاع على محتوى كل ملف حاسوبي بشكله الثنائي ، متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خاصة وأن بعض الأنظمة قد لا تتمكن من تحديد إلى أي فئة من الملفات ينتمي هذا الملف، وقد يتطلب الأمر استخدام هذا النوع من برامج التحرير التي تعتمد على أن العديد من الملفات تحتوي على مجموعة من الرموز (Symbols) ذات الدلالة توجد في بداية الملف ، ويستطيع الخبير المعلوماتي من خلالها تحديد نوع الملف بدقة ومن أشهر هذه البرمجيات برنامج (Gander)وبرنامج (Winhex)[1] .

ـ أدوات فحص ومراقبة الشبكات

ويتم استخدام هذه الأدوات في فحص بروتوكول TCP /IP لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي قد تتعرض لها ، ومن هذه الأدوات :

١ ـ أداة ARP : ووظيفتها تحديد مكان الحاسب الآلي وموقعه على الشبكة .

٢ ـ برنامج Visual Route 5.2a : وهو عبارة عن برنامج يلتقط أي عملية تم اتخاذها ضد الشبكة ، ويبين المناطق التي مر فيها الهجوم ، وبعد أن يتعرف هذا البرنامج على عنوان IP أو اسم الجهة يحدد هذا البرنامج مسار الهجوم بين مصدره والجهة التي استهدفها هذا الهجوم أو التعدي .

٣ ـ أداة TRACER : تقوم هذه الأداة بإظهار العناوين التي زارها الجاني والوقت والفترات التي قضاها فيها ، وهي تسمح برؤية المسار الذي اتخذه IP من

(١) كذلك توجد برامج استعراض الصور والتي تستخدم في عرض الصور الرقمية (Digital Images) على شاشة الجهاز وبالتالي فهي تمكن المحقق من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسب الآلي أو وسائط التخزين الخارجية ، وتبرز الحاجة لهذا النوع من البرامج في الجرائم الإباحية . انظر علي الفيل ، المرجع السابق . ص ٧١ وما بعدها . انظر أيضاً حسين الغافري ، المرجع السابق. ص ٥١٦ وما بعدها .

مضيف إلى آخر . ويمكن عن طريق هذه الأداة معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها[1].

٤ ـ أداة Net Stat : وهي أداة لفحص حالة الاتصال الحالي للبروتوكول TCP/ IP، ولها عدد من المهام من أهمها إظهار جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه .

أ ـ الوسائل الإجرائية

والمقصود بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق التي تثبت وقوع الجريمة وتحدد شخصية الجاني وهي كالتالي :

ـ اقتفاء الأثر

يحاول مرتكب الجريمة المعلوماتية دائماً إخفاء آثاره حتى لا يتم القبض عليه ومحاسبته على جريمته . ويمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه لارتكاب الجريمة المعلوماتية [2].

ـ الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

يجب على المحقق عند القيام بالتحقيق في إحدى الجرائم المعلوماتية أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات عملاء، كما ينبغي عليه الاطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة المستفيدين من النظام والمستخدمين والملفات والإجراءات ، ومدى تخصيص وقت معين من اليوم يسمح باستخدام كلمات السر (Passwords) ، ومدى توزيع الصلاحيات للمستخدمين ، وإجراءات أمن العاملين وأسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية، كمراقبة المستفيدين والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام (Failed Attempts to Access the System) .

(١) علي الفيل ، المرجع السابق . ص ٧٢ وما بعدها . انظر أيضاً حسين الغافري ، المرجع السابق. ص ٥١٧ .

(٢) عبدالفتاح حجازي ، المرجع السابق . ص ٣٩٦ ، انظر أيضاً حسين الغافري ، المرجع السابق. ص٥١٨ .

بالإضافة إلى التعرف على برامج الحماية وأسلوب عملها، والاستفادة من تقارير نظم أمن البيانات وتقارير جدران الحماية[١].

٢ ـ صعوبات التفتيش عن الدليل المعلوماتي

توجد العديد من الصعوبات التي تؤثر على عملية تفتيش النظام المعلوماتي نوردها كالآتي :

١ ـ صعوبات تتعلق بالجريمة

كإخفاء الجريمة وغياب الدليل المرئي ، وافتقاد الآثار التقليدية وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام الجاني كلمات السر (Passwords) بشكل يمنع وصول المحقق إلى الأدلة الإلكترونية أو تشفير المعلومات لإعاقة محاولات المحقق والخبير الوصول إليها .

سهولة محو الدليل أو تدميره (Destruction of Evidence) في وقت قصير جداً، بحيث تعجز سلطات التحقيق عن كشف الجريمة والوصول إلى مرتكبيها ، وبالتالي يتنصل الجاني من المسؤولية عن هذه الجريمة .

ضخامة كم البيانات والمعلومات المتعين فحصها ، وإمكانية وجودها خارج إقليم الدولة، ووجود الجاني والمجني عليه في دولتين مختلفتين[٢].

٢ ـ صعوبات تتعلق بالمجني عليه

إن عدم إدراك خطورة الجرائم المعلوماتية من قبل الجهات المجني عليها تعد إحدى معوقات التفتيش والتحقيق . وبالتالي تبقى الجريمة المعلوماتية خفية ما لم يتم

(١) عبدالفتاح حجازي ، المرجع السابق . ص ٣٩٦ وما بعدها . انظر أيضاً خالد الحلبي ، المرجع السابق . ص ٢٠٨ وما بعدها .

(٢) ومن الأمثلة على ذلك قيام أحد مرتكبي جرائم غسل الأموال (Money Laundering) في فرنسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسب محو وتدمير كل البيانات والمعلومات المخزنة فيه . انظر علي الفيل ، المرجع السابق . ص ٨٠ وما بعدها . انظر أيضاً حسين الغافري . المرجع السابق ، ص ٥٢١ وما بعدها .

الإبلاغ عن حدوثها. والصعوبة التي تواجه جهات التحقيق هي أن هذه الجرائم لا تصل إلى علمها بالطرق العادية ـ كما هو الحال في الجرائم التقليدية ـ وذلك لصعوبة اكتشافها من قبل الجهات المجني عليها ، أو لأن هذه الجهات تحاول تلافي النتائج السلبية للإبلاغ عما حدث لها وحرصاً على احتفاظها بثقة عملائها، وبالتالي تتجنب الإبلاغ عن الجرائم المعلوماتية التي وقعت ضحية لها[1].

كما أن هذه الجهات المجني عليها تدخل في اعتباراتها أن الإبلاغ عن الجرائم المعلوماتية التي وقعت ضحية لها قد يؤدي إلى إحاطة المجرمين علماً بنقاط الضعف في أنظمة الأمن والحماية لدى هذه الجهات ، خاصة البنوك والشركات الكبرى . كما قد تخشى تلك المؤسسات والشركات من أن تؤدي أعمال التحقيق إلى احتجاز أجهزة الحاسب الآلي العائدة لها أو تعطيل شبكاتها لمدة طويلة، ما قد يتسبب لها في خسائر مالية كبيرة[2].

ج ـ صعوبات تتعلق بنقص خبرة جهات التحقيق

وقد تعود هذه الصعوبات إلى عدم تمكن المحقق من تقنيات الحاسب الآلي والقدرة على استخدام شبكة الإنترنت ، إضافة إلى عدم متابعة المحقق للمستجدات في مجال الحاسب الآلي وجرائم المعلوماتية .

كما قد لا تتوافر المهارة الفنية لدى المحقق في مثل هذا النوع من الجرائم، وعدم توافر المعرفة لديه بأساليب ارتكاب الجرائم المعلوماتية، وقلة الخبرة في مجال التحقيق

---

(١) ووفقاً لبعض التغييرات فإن ما بين (٢٠ – ٢٥٪) من جرائم المعلوماتية في الولايات المتحدة لا يتم الإبلاغ عنه مطلقاً خشية الإساءة لسمعة المؤسسة أو الشركة المجني عليها ، إلا أن دراسة أخرى أجريت على خمسمائة شركة أظهرت نتائجها أن (٢٪) فقط من كل جرائم المعلوماتية يتم الإبلاغ عنها للشركة أو لمكتب التحقيقات الفيدرالي (FBI) . انظر :

- Gregory P. Joseph ,"Internet and Email Evidence", Practical Lawyer, February 2012 at 158 – 160 .
- Theodore J. Koerth, and Christopher E. Paetsch, "How to Admit E-Mail and Web Pages Into Evidence" , Illinois Bar Journal , December , 2006 . at 194 – 197.

(٢) علي الفيل ، المرجع السابق . ص ٧٩ وما بعدها . انظر أيضاً عبدالفتاح حجازي، المرجع السابق. ص ٦٧ وما بعدها . انظر أيضاً محمد الأمين البشرى ، التحقيق في الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية ، الرياض ٢٠٠٤م . ص ١٧ وما بعدها .

في جرائم المعلوماتية[١]، خاصة وأن للمتخصصين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم فيما بينهم، كما اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى (First Letters) لتكوين لغة خاصة بهم تعرف بالمختصرات (Acronyms) وهي لغة خاصة بمستخدمي الحاسب الآلي . ولذلك بدأت بعض الجهات الأمنية والقضائية في استقطاب المتخصصين في الحاسب الآلي ليكونوا ضمن كوادرها، كما جرى تدريب بعض رجال الشرطة على استخدام الحاسب الآلي وشبكة الإنترنت[٢].

د ـ صعوبات تتعلق بإجراءات الحصول على الدليل المعلوماتي

لا تقف صعوبة إثبات الجرائم المعلوماتية عند مسألة تعذر الوصول إلى الأدلة اللازمة لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، فإذا كان من السهل على جهات التحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم المعلوماتية .

كما أن المجرمين الذين يرتكبون الجرائم المعلوماتية عادة ما يتخذون كلمات سر (Passwords) تزيد من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة (Evidence) التي تدينهم .

فعن طريق استخدامهم كلمات السر لا يتمكن غيرهم من الوصول إلى البيانات

(١) عبدالفتاح حجازي، المرجع السابق . ص ٦٧ وما بعدها .

(٢) وقد أكدت ورشة العمل التي عقدتها وزارة العدل بدولة الإمارات العربية المتحدة والتي عقدت في ١٠ مايو ٢٠٠٩م على أهمية تدريب رجال الشرطة والمحققين على استخدام الحاسب الآلي وشبكة الإنترنت وكذلك التعامل مع هذه التقنية . كما أكدت على أهمية الاطلاع على أحدث التجارب في التعامل مع الأدلة الرقمية غير التقليدية . كما تناولت هذه الورشة معايير وحجية الأدلة الرقمية والدليل الإلكتروني . انظر صحيفة الاتحاد، تاريخ الاثنين ١١ مايو ٢٠٠٩م يتوافر على :
http: / /www.alittihad.ae /details.phpid.
انظر أيضاً حسين الغافري، المرجع السابق . ص ٥٢٧ وما بعدها .

المخزنة إلكترونياً أو المنقولة عبر شبكة الإنترنت . كما قد يلجأ هؤلاء المجرمون أيضاً إلى دس تعليمات خفية (Hidden Instructions) بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات الضبط والتحقيق الوصول إلى كشف أفعالهم غير المشروعة[1].

كذلك فإن هناك صعوبات عديدة قد تعترض الحصول على الأدلة بالنسبة للجرائم المعلوماتية، ومثال ذلك أنه قد يتعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلاً بحاسبات آلية أخرى تقع خارج إقليم الدولة، ويكون تفتيش هذه الحاسبات ضرورياً لكشف عما قد تشتمله من أفعال غير مشروعة .

فالجرائم التي ترتكب باستخدام شبكة الإنترنت كما أنها تقع على المستوى الوطني فإنها قد ترتكب أيضاً على المستوى الدولي أي خارج نطاق إقليم الدولة، وهذا قد يثير مشكلات عديدة مثل تتبع تلك الاتصالات الإلكترونية بواسطة سلطات التحقيق لأجل إقامة الدليل على الجرائم التي ترتكب باستخدام شبكة الإنترنت[2].

كما أن اختلاف تشريعات الدول فيما بينها فيما يتعلق بشروط ومتطلبات قبولها للأدلة والقيام ببعض الإجراءات مثل التفتيش عبر الحدود يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود .

فعلى الرغم من أن التطور التقني الهائل في مجال الاتصالات قد أفرز العديد من الجرائم ذات الطبيعة الخاصة ، فما زالت إجراءات البحث والتنقيب عن هذه الجرائم وضبطها في العديد من دول العالم تتم في إطار النصوص الإجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية ، الشيء الذي سيترتب عليه العديد من المشكلات بالنسبة لضبط هذا النوع من الجرائم المستحدثة ذات الطبيعة المعنوية والتي قد تتعدد أماكن ارتكابها داخل إقليم الدولة الواحدة، أو يمتد نطاقها ليشمل دولاً متعددة عبر

(١) علي الفيل ، المرجع السابق . ص ٨٢ وما بعدها . انظر أيضاً حسين الغافري ، المرجع السابق. ص٥٢٧ وما بعدها .

(٢) عبدالفتاح حجازي ، المرجع السابق . ص٦٨ وما بعدها . انظر أيضاً خالد ممدوح إبراهيم ، المرجع السابق . ص ٧٤ وما بعدها .

شبكة الإنترنت ، فيتعذر بناء على ذلك اتخاذ إجراءات جمع الأدلة ، أو قد تلحق عدم المشروعية بهذه الإجراءات [١] .

الخاتمـــــة

تعرضنا في هذا المبحث لموضوع التفتيش في النظام المعلوماتي لما لهذا الموضوع من أهمية متزايدة نظراً للزيادة الكبيرة في الجرائم المعلوماتية حول العالم . وتوصلنا في ختام هذا البحث إلى النتائج والتوصيات الآتية :

أولاً: النتائج:

١ ـ التفتيش في الجرائم المعلوماتية وإثباتها ليس بالأمر السهل ويستلزم استخدام تقنيات ووسائل حديثة في عمليات التحري والكشف عن الأدلة والتحقيق، ولذلك ينبغي استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة المعلوماتية والتحقيق فيها، إذ إن التفتيش في النظام المعلوماتي يتم في بيئة رقمية، من خلال التعامل مع الحاسبات والشبكات ووسائط التخزين ووسائل الاتصال .

٢ ـ إمكانية تلاعب الجاني بالبيانات عن بعد أو محوها من خلال وحدة طرفية.

٣ ـ يعد الدخول إلى النظام المعلوماتي إجراء يندرج ضمن التفتيش بمعناه القانوني، ويخضع لأحكامه.

٤ ـ تثور العديد من الصعوبات أمام تطبيق النصوص التجريمية التقليدية التي تتضمنها القوانين التقليدية على الجرائم المعلوماتية إذ إن تطبيق مثل هذه

(١) لذلك فإن بعض الفقه في عدد من الدول كبريطانيا وألمانيا يشكك في إمكانية الدخول إلى الأنظمة المعلوماتية لدى الحاسبات الأخرى التي توجد خارج إقليم الدولة بغرض ضبط البيانات المخزنة بها (Stored Data) لأنه بدون وجود اتفاق بين الدول المعنية ينظم هذه المسألة ، فإن اتخاذ مثل هذا الإجراء يعد خرقاً لسيادة (Sovereignty) كل دولة على إقليمها (Territory) ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية ومكافحة الجريمة . انظر خالد ممدوح إبراهيم . المرجع السابق. ص ٧٥ وما بعدها . انظر أيضاً حسين الغافري ، المرجع السابق . ص ٥٢٩ وما بعدها .

النصوص التقليدية قد لا يتوافق مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها البيانات أو المعلومات.

٥ ـ يوجد قصور واضح في كثير من التشريعات الجنائية في الدول العربية في مواجهة ظاهرة الإجرام المعلوماتي ، فما زال الكثير منها يخضع هذه الجرائم للنصوص التقليدية وهو ما قد يترتب عليه الاعتداء على مبدأ شرعية الجرائم والعقوبات من جهة ، وإفلات الكثير من الجناة من العقاب من جهة أخرى .

٦ ـ تعقب مرتكب الجريمة المعلوماتية وتفتيش حاسبه الآلي وملحقاته وتتبع آثاره وضبط الأدلة المعلوماتية الدالة على ارتكابه الجريمة قد لا يتقيد بإقليم الدولة التي تضررت من جريمته ، وإنما قد يمتد إلى خارج إقليم تلك الدولة، وهذا يعود إلى أن شبكة الإنترنت هي شبكة عالمية تربط جميع الدول ببعضها البعض وأصبح لا يحدها فاصل .

٧ ـ مكافحة الجرائم المعلوماتية تقتضي تأهيل وتدريب القائمين على هذه المكافحة .

٨ ـ إن الخطأ في إجراء التفتيش وضبط الأدلة قد يؤدي إلى ضياع فرصة كشف الجريمة أو عدم تحقق الإدانة حتى مع معرفة الجاني .

٩ ـ من خلال استعراض النصوص الإجرائية في نظام الإجراءات الجزائية السعودي المتعلقة بالضبط نجد أنها أجازت لسلطة التحقيق ضبط جميع الأشياء التي تفيد في كشف الحقيقة ، وبالتالي يمكن أن تنطبق على أجهزة الحاسب الآلي ونظم الحاسب الآلي والإنترنت .

١٠ ـ ما من دولة يمكنها النجاح في مواجهة هذا النوع من الجرائم بمفردها دون تعاون وتنسيق مع غيرها من الدول سواء في مجال المساعدات القضائية المتبادلة (Judicial Assistance) أو في مجال التدريب .

١١ ـ يترتب على التفتيش الذي يتم في إطار حدوده المكانية والزمانية والموضوعية والإجرائية نشوء حق في ضبط الأشياء التي تفيد في كشف حقيقة الجريمة المرتكبة بوضع اليد على الشيء المتصل بالجريمة والذي يفيد في كشف الحقيقة عنها وعن مرتكبها . وهذه الأشياء محل الضبط، قد تكون أشياء مادية كأجهزة

الحاسب الآلي وملحقاتها، كما يمكن أن تكون أشياء معنوية كالمراسلات والاتصالات الإلكترونية والمعلومات المعالجة إلكترونياً وكافة المكونات المعنوية لوسائل الاتصال الحديثة .

ثانياً: التوصيات :

١ ـ ضرورة تطوير قوانين العقوبات في الدول المختلفة ، وإصدار تشريعات جديدة لمواجهة الجرائم المعلوماتية بسن نصوص تشريعية في قوانين العقوبات تجرم هذه الأفعال ببيان كل جريمة ووضع العقوبة المقررة لها، وكذلك في قوانين الإجراءات الجنائية لتنظيم إجراءات التفتيش والتحقيق في هذه الجرائم .

٢ ـ ينبغي أن تسمح الإجراءات الجنائية للجهات القائمة على التفتيش بضبط برامج الحاسب الآلي والمعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بإجراءات التفتيش التقليدية .

٣ ـ لتسهيل مهمة هيئة التحقيق والإدعاء العام في ضبط نظم الحاسب الآلي والإنترنت نقترح تعديل نص المادة (٥٦) من نظام الإجراءات الجزائية السعودي لتشمل المراقبة عبر الإنترنت وشبكات الحاسب الآلي لتصبح كما يلي: «لرئيس هيئة ا لتحقيق والإدعاء العام أن يأمر بضبط الرسائل والخطابات والمطبوعات والطرود ، وله أن يأذن بمراقبة المحادثات الهاتفية وشبكات الحاسب الآلي والإنترنت وتسجيلها متى كان لذلك فائدة في ظهور الحقيقة في جريمة وقعت ، على أن يكون الإذن مسبباً ومحدداً بمدة لا تزيد على عشرة أيام قابلة للتجديد وفقاً لمقتضيات التحقيق».

٤ ـ يجب أن يخضع التفتيش لمجموعة من الضمانات (Guarantees) التي توضح حدوده المكانية والزمانية والموضوعية والإجرائية، نظراً لخطورته ومساسه بالحريات الشخصية (Personal Freedoms) للأشخاص وحياتهم الخاصة وحرمة منازلهم، ومن أهم هذه الضمانات مباشرته من قبل سلطة التحقيق وفقاً للإجراءات المقررة قانوناً .

٥ ـ ضرورة إعداد الكوادر الأمنية ، وسلطات الضبط والتحقيق من الناحية الفنية

للبحث والتفتيش والتحقيق وجمع الأدلة في مجال الجرائم المعلوماتية وتأهيل وتدريب القائمين على هذه المكافحة .

٦ ـ ضرورة إبرام اتفاقيات تنظم وقت امتداد إجراءات التفتيش خارج إقليم الدولة وكيفية اتخاذ مثل هذا الإجراء . كما ينبغي السماح أثناء تنفيذ التفتيش لجهات التحقيق بمد التفتيش إلى أنظمة الحاسب الآلي الأخرى ضمن دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات بشرط أن يكون هذا الإجراء ضرورياً وشريطة مراعاة الضمانات المقررة قانوناً .

٧ ـ ضرورة اتخاذ التدابير اللازمة لحل مشكلات الاختصاص القانوني والقضائي التي تثيرها الجرائم المتعلقة بشبكة الإنترنت .

٨ ـ ضرورة حضور المتهم عند تفتيش حاسبه الآلي أو نظمه وكذلك في حالة تفتيش حاسب أو نظم غيره إذا كان الأمر متعلقاً بضبط دليل ضده وذلك لإتاحة الفرصة أمام المتهم لمواجهته بالدليل المتحصل من التفتيش ، شريطة ألا يسبب حضوره إضراراً بسير التحقيق .

٩ ـ ضرورة التعاون بين الدول المختلفة، وبين تلك الدول ومنظمة الشرطة الدولية (الإنتربول) بتبادل المعلومات والخبرات والتعاون في المجال الأمني والقضائي بصوره المختلفة في مجال مكافحة الجرائم المعلوماتية وعقد اتفاقيات تعاون مشتركة لهذا الغرض .

١٠ ـ ضرورة اتباع القواعد الفنية اللازمة لحماية البيانات وتجنيبها خطر الإتلاف عند تفتيش النظم المعلوماتية .

١١ ـ على القائم بالتفتيش أن يلتزم واجب الحيطة والحذر أثناء التفتيش فلا يطلع إلا على الأشياء والأماكن التي يحتمل أن يجد فيها بيانات أو برامج أو أشياء أو أدلة لها علاقة بالجريمة المعلوماتية ، حيث إن قوانين الإجراءات الجنائية تحظر الاطلاع على الأشياء والأماكن التي لا يكون لها علاقة بالجريمة محل التفتيش .

١٢ـ ضرورة اتخاذ تدابير حماية للمعلومات والبيانات في النظام المعلوماتي الذي يتم تفتيشه لمنع الجاني من اختراقها وإتلافها .

المراجـــع

أولاً: الكتب والبحوث العربية:

أحمد ، هلالي عبداللاه ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، القاهرة ، ٢٠٠٦م .

إبراهيم ، خالد ممدوح ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الإسكندرية ، ٢٠٠٩م .

البشرى ، محمد الأمين ، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٤م .

بكري، بكري يوسف ، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي ، الإسكندرية ، ٢٠١١م .

حجازي ، عبدالفتاح ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، القاهرة ، ٢٠٠٧م .

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

رستم ، هشام محمد ، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مؤتمر القانون والكمبيوتر والإنترنت ، جامعة الإمارات العربية المتحدة، ٢٠٠٠م .

سرور ، أحمد فتحي ، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة، ١٩٨٠م .

سقف الحيط ، عادل عزام ، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠١١م .

الطوالبة، علي حسن ، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة ، إربد ، ٢٠٠٤م .

عبدالستار، فوزية ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة ، ١٩٨٦م .

الغافري ، حسين سعيد ، السياسة الجنائية في مواجهة جرائم الإنترنت، دارسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠٩م .

فضل ، سـليمان أحمد ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) ، دار النهضة العربية، القاهرة، ٢٠٠٨م .

الفيـل ، عـلي عدنان ، إجـراءات التحري وجمـع الأدلة والتحقيـق الابتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث ، عمان ، ٢٠١١م .

مصطفى ، محمود محمد ، الإثبات في المواد الجنائية في القانون المقارن، التفتيش والضبط، جامعة القاهرة ، القاهرة ، ١٩٨٧م .

هروال ، نبيلة هبة ، الجوانب الإجرائية لجرائم الإنترنت ، دار الفكر الجامعي ، الإسكندرية ٢٠٠٧م .

ثانياً: المراجع الأجنبية :

Joseph , Gregory P (20120), "Internet and Email Evidence" , Practical Lawyer, February.

Koerth,Theodore J. and Christopher E. Paetsch (2006), "How to Admit E-mail and Web Pages Into Evidence", Illinois Bar Journal , December.

Mauet ,Thomas A. and Warren D. Wolfson (2009), Aspen Publishers, Inc. , A Wolters Kluwer Business.

Mohrenschlager, Manfred (1993), Computer Crime and Other Crimes Against Information Technology in Germany, R.I.D.P.

Overly, Michael R. (2011) Best Practices For Seizing Electronic Evidence, Expert Series.

ثالثاً: القوانين والأنظمة :

نظـام مكافحة الجرائم المعلوماتية السـعودي ، الصادر بالمرسـوم الملكـي رقم (م/ ١٧) وتاريخ ٨/ ٣/ ١٤٢٨هـ .

نظـام الإجـراءات الجزائية السـعودي ، الصادر بالمرسـوم الملكي رقـم (م/ ٣٩) بتاريخ ٢٨/ ٧/ ١٤٢٢هـ .

قانون الإجراءات الجنائية المصري .

قانون الإجراءات الجزائية الاتحادي الإماراتي .

قانون الإجراءات الجنائية الألماني .

قانون الإثبات الكندي .

قانون الإجراءات الجنائية الكندي .

الدليل الأمريكي لتفتيش وضبط الحاسبات الآلية لعام ١٩٩٤م .

قانون مكافحة الجرائم المعلوماتية الهولندي .

رابعاً : الصحف العربية :

جريدة الاتحاد الإماراتية بتاريخ الاثنين ١١ مايو ٢٠٠٩م ، متوافر على

http: / /www.alittihad.ae.