التفتيش وفقاً لأحكام القانون رقم ١٧٥ لسنة ٢٠١٨
فى شأن مكافحة جرائم تقنية المعلومات*

مصطفى على خلف

تتناول هذه الدراسة جانب هام من الجوانب الإجرائية الحديثة التى تتعلق بالبحث والتنقيب عن الدليل فى جرائم تقنية المعلومات، يتمثل فى تفتيش أجهزة الحاسوب فى ضوء القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات، وفى هذا السياق ناقشت الورقة قضية تفتيش الحاسب الآلى والأنظمة المتصلة به من الداخل، وفى الخارج، وناقشت أيضًا قضية التفتيش التقنى بناء على إذن من سلطة التحقيق، وكيفية تعيين محل التفتيش وتنفيذ الإذن.

مقدمة

اكتسبت ثورة المعلومات فى العصر الحاضر أبعادًا جديدة وأهمية خاصة نتيجة تطور وسائل الاتصال بين الدول، وأصبحت المعلومات ثروة يجب المحافظة عليها وصيانتها(١).

ولا شك أن هذه الثورة المعلوماتية تركت آثارا إيجابية وشكلت قفزة حضارية ونوعية فى حياة الأفراد والدول(٢)، حيث تعتمد القطاعات المختلفة فى الوقت الحالى فى أداء عملها بشكل أساسى على استخدام الأنظمة المعلوماتية؛ نظرا لما تتميز به من عنصرى السرعة والدقة فى تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والجهات والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول(٣). كما أصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية، ومستودعا لأسرار الدول الحربية والصناعية والاقتصادية التى هى على جانب كبير من الأهمية والسرية(٤).

إلا أن هذا الجانب الإيجابى لعصر المعلوماتية لا ينفى الانعكاسات السلبية

---

* رئيس محكمة الاستئناف.

التى أفرزتها هذه التقنية والمتمثلة فى إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة تضر بمصالح الأفراد والجماعات وبالتالى مصلحة المجتمع، حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم[٥] اصطلح على تسميتها بجرائم التقنية الحديثة، سواء كانت هذه الجرائم من الجرائم التقليدية التى ترتكب عن طريق وسائل الاتصال الحديثة مثل جرائم القتل[٦]، أو جرائم مستحدثة فى مجال المعلوماتية: مثل اختراق شبكات المعلومات، والاستيلاء على هذه المعلومات، والدخول أو البقاء فى الأنظمة المعلوماتية بطريق غير مشروع[٧][٨].

فضلًا عن ذلك؛ فإن جرائم التقنية الحديثة عادة ما تخرج من نطاقها الافتراضى داخل شبكة المعلومات إلى العالم الخارجى الملموس[٩].

وإذا كان الهدف المنشود لرجال الضبط القضائى هو سرعة ضبط الجريمة والوصول إلى معرفة مرتكبها وتجميع الأدلة التى تفيد التحقيق بشأنها. فكيف يمكن البحث والتنقيب عن الأدلة فى جرائم التقنية الحديثة بما لها من طبيعتها الخاصة؟ كما أن هذه الجرائم لا تَخْلف أثرًا ماديًا يمكن تَتَبعه، فضلًا عن قدرة الجناة على محو أدلة الإدانة أو تدميرها فى وقت قصير للغاية تجعل من الصعب جدا إثبات هذه الجرائم. وأيضًا من الصعب اكتشافها فى حالة ارتكابها عن بعد من داخل دولة أجنبية، علاوة على ذلك فإن استخدام الجناة للبريد الإلكترونى فى إصدار تعليماتهم لمنفذى تلك الجرائم يجعل من الصعب مراقبتهم مثل مراقبة المحادثات السلكية واللاسلكية التقليدية. وكثير ما يستخدم (الهكرة) نظام الحاسب الآلى فى تخزين البيانات الشخصية المسروقة.

وأمام كل هذه الصعوبات قد لا يجد رجال الضبط القضائى مفرًا من اللجوء إلى بعض الإجراءات التى تحاط بها الشكوك حول شرعيتها مثل مراقبة المحادثات التى تتم عبر مواقع التواصل الاجتماعى المختلفة الفيسبوك والتويتر والياهو

ماسنجر... أو يتم اللجوء إلى مزود خدمة الإنترنت للإطلاع على ما يحتفظ به من معلومات تخص العملاء لديه سواء كانت هذه المعلومات معلومات أساسية عن المشترك أو تتعلق بمضمون ما يجرونه أو يتلقونه من اتصالات، أو أن يتم اللجوء إلى صاحب العمل لأخذ موافقته على تفتيش أجهزة الحاسب الآلى الخاصة بالموظفين لديه باعتبارها إحدى أدوات العمل المملوكة له، أو أن يقوم رجال الضبط بتفتيش أجهزة الحاسوب التى وجدت فى حوزة المتهم المطلوب ضبطه أو وجدت فى المسكن المراد تفتيشه، أو تفتيش جميع ملفات جهاز الحاسوب. فما مدى شرعية تلك الإجراءات وخاصة أنها تتعارض مع حق الفرد فى الخصوصية؟

وقد أثار ذلك مشكلات كثيرة تتعلق بكيفية تفتيش هذه الأنظمة الإلكترونية وضبط ما يتم الحصول عليه من بيانات وكذلك مدى حجية الأدلة الناتجة عن الحاسبات الآلية ومدى صلاحيتها لأن تكون دليلا فى الإثبات الجنائى(١٠).

وقد أدى ذلك كله إلى وجوب وضع أطر قانونية إجرائية تتواءم مع الطبيعة الخاصة لهذه الجرائم، فوقعت المعاهدات الدولية منها على سبيل المثال معاهدة بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فحددت كل منهما القواعد الإجرائية التى يتعين أن تسير على منهجها التشريعات الوطنية لكل من الدول الأعضاء. وقد استجاب كثير من الدول لذلك الأمر وأدخلت على تشريعاتها الإجرائية عددا ليس بقليل من النصوص الخاصة بالجرائم التقنية الحديثة لا سيما ما يتعلق بإجراءات التفتيش والضبط. ومنها المشرع المصرى؛ فأصدر القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات ليتواءم مع هذه المتغيرات(١١).

موضوع الدراسة

رأينا أن نخصص موضوع هذا البحث لما يتعلق بإجراءات التفتيش كأحد إجراءات جمع الدليل بشأن جرائم التقنية الحديثة. باعتباره من أهم الإجراءات التى تحمى حقوق الإنسان لأنه يتعرض لأهم حق له، ألا وهو حقه فى الخصوصية.

أهمية الدراسة

تسليط الضوء على النقاط التى أغفلها المشرع المصرى فى القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات، بهدف مساعدته فى معالجتها من خلال تعديل بعض مواده.

منهج الدراسة

وتناولنا لهذا البحث سوف يكون من خلال دراسة تحليلية تطبيقية مقارنة، حيث نقوم بتحليل قواعد القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات، غير مكتفين بالجانب النظرى فقط بل سنجمع بينه وبين الجانب التطبيقى لبيان مدى كفاية هذه النصوص الإجرائية على حل المشكلات العملية التى قد تظهر عند إعمال نصوص هذا القانون، مستعينين فى ذلك بالكثير من التطبيقات القضائية المتعلقة بهذه النوعية من الجرائم، كما نوضح ما انتهت إليه النظم القانونية الأخرى مقارنة بالوضع فى التشريع المصرى.

المقصود بالتفتيش التقنى

التفتيش: هو البحث فى مستودع أسرار فرد معين عن أدلة تفيد التحقيق بشأن جريمة– معينة جناية أو جنحة– وقعت وتقوم الدلائل الجدية ضد هذا الشخص على ارتكابها. وقد يكون مستودع الأسرار– محل التفتيش– شخص هذا الفرد كما قد يكون أمكنة خاصة به لها حرمتها. وهو لذلك إجراء من إجراءات التحقيق[١٢]. ولا يعتبر

التفتيش من إجراءات كشف الجريمة قبل وقوعها، بل إنه من إجراءات تحقيقها بعد ارتكابها. وقد يكون التفتيش من إجراءات جمع الاستدلالات كما لو عثر رجل الضبط القضائى على جهاز حاسوب ملقى بالطريق العام، وبفحصه تبين قيام صاحبه بترويج الأفلام الجنسية الخاصة بدعارة الأطفال، ومن ثم فإن التقاط جهاز الحاسوب وفحصه هو إجراء من إجراءات الاستدلال. ويعتبر التفتيش كذلك من إجراءات جمع الاستدلالات إذا سُلم جهاز الحاسوب إلى رجل الضبط اختيارًا من حائزه أو ممن عثر عليه(١٣).

ويتمثل مجال السرية الذى يتعرض له التفتيش هنا إما فى شخص المتهم وإما فى المكان الذى يعمل به أو يقيم فيه. فالأصل أنه لا يجوز أن يترتب على حق الدولة فى العقاب المساس بالحق فى السرية من أجل جمع أدلة إثبات الجريمة ونسبتها إلى المتهم، لما فى ذلك من انتهاك للحق فى الحياة الخاصة. ولكن للتوفيق بين حق الدولة فى العقاب وحق المتهم فى الحياة الخاصة أجاز القانون المساس بهذا الحق الأخير عن طريق التفتيش، بعد أن أخضعه لضمانات معينة تتمثل إما فى شخص القائم به وإما فى شروطه الموضوعية والشكلية التى يتعين توافرها فى هذا الإجراء(١٤). وتكمن الفكرة الأساسية للتفتيش فى إباحة انتهاك الحق فى الخصوصية طالما أن هناك مبررًا فى القانون لهذا الانتهاك، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الأساسية التى أسهمت التشريعات الكبرى فى المحافظة عليه.

أما التفتيش فى جرائم التقنية الحديثة فيعرف بأنه: الولوج فى نظم المعالجة الآلية للبيانات وذلك للبحث والتنقيب فى البرامج المستخدمة وملفات البيانات المخزنة عما يتصل بجريمة وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبها(١٥).

وتفتيش نظام الحاسوب والإنترنت يعد من أخطر الإجراءات الجنائية التى تتخذ ضد مرتكب جريمة التقنية الحديثة لكون محل التفتيش هنا هو الحاسوب

أو الشبكات بما يتضمنه من معلومات سواء كانت متعلقة بالجريمة التى يتم البحث عن الدليل فيها أو بعيدة تمام البعد عنها.

ونظرًا للطبيعة الخاصة لهذه الجرائم- على النحو سالف البيان- اتجهت معظم التشريعات المقارنة إلى استحداث قواعد إجرائية جديدة تطبق عليها.

وقد سار المشرع المصرى على النهج ذاته الذى سلكته الكثير من التشريعات المقارنة، فأصدر القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرام تقنية المعلومات[١٦]. فقد نصت المادة السادسة على أنه: لجهة التحقيق المختصة بحسب الأحوال، أن تصدر أمرا مسببا لمأمورى الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد مرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحدة أو أكثر مما يأتى: ١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه. ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتض. ٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط. ٣- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى موجود تحت سيطرته أو مخزن لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو النظام التقنى.

وفى كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسببًا. ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة، فى المواعيد ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية.

ونقول أن المشرع المصرى أقر حق سلطة التحقيق فى تفتيش نظم الحاسب للوصول إلى البيانات المخزنة فيه وضبطها. وبالتالى حُسم الجدل القائم حول مدى قابلية مكونات الحاسب الآلى والشبكات للتفتيش والضبط(١٧).

أولاً: تفتيش الحاسب الآلى والأنظمة المتصلة به

يختلف التفتيش التقنى- تفتيش الحاسوب- عن التفتيش التقليدى وبصفة خاصة موضوع (محل) التفتيش والغاية منه، إذ يكونان أكثر تحديدًا فى التفتيش التقليدى. فإذا صدر إذن بشأن ضبط مواد مخدرة، فيكون موضوع التفتيش هو المنزل الخاص بالمتهم- مثلًا- وتكون الغاية من التفتيش هى ضبط المخدر نفسه؛ الذى قد يكون مخبأ فى ملابس المتهم أو فى حقيبته أو داخل دولاب غرفته. غير أن الوضع ليس بهذا الوضوح فيما يتعلق بالتفتيش التقنى، ذلك أن غايته ضبط المعلومات التقنية أو الملفات التى تحوى على أدلة الجريمة كرسائل البريد الإلكترونى أو صور الأطفال الجنسية أو الملفات التى يحتفظ بها المتهم والخاصة بأماكن وجود الأموال التى قام بغسلها... وهذه الملفات تأخذ صورة نبضات إلكترونية، يمكن تخزينها فى عناوين مخبأة فى جهاز الحاسوب الخاص بالمتهم سواء كان بحيازته الشخصية أو داخل المسكن الخاص به، وقد يتم حفظ هذه الملفات داخل أجهزة حاسوب أخرى- موجودة فى مكان آخر بخلاف مسكن المتهم- متصلة بجهاز حاسوب المتهم أو حفظها على خادم Server بعيد جدا سواء كان داخل حدود الدولة أو خارجها. وفى أغلب الأحوال تكون تلك الملفات مشفرة وعليها عناوين مضللة ويتم خلطها مع الملايين من الملفات بحيث يصعب الوصول إليها.

وإذا كان من المعتاد عليه أن أجهزة الحاسوب فى بعض الأحيان قد يرتبط بعضها ببعض عن طريق دائرة داخلية تنتمى إلى ذات الشركة أو البنك أو المدرسة وذلك عن طريق شبكة محلية- Local area network- أو عن طريق الإنترنت إذا

تعددت فروعها سواء كانت هذه الفروع تقع داخل النطاق الإقليمى أو خارجه وذلك عن طريق شبكة واسعة النطاق– wide area network– كما أن تفتيش جهاز معين قد يستتبع بالضرورة الدخول إلى جهاز آخر ينتمى إلى شخص آخر فى مكان مختلف، فيقوم رجال الضبط باستخدام برنامج معين والدخول به ابتداء من الجهاز محل التفتيش إلى جهاز ثان وربما جهاز ثالث.

فإذا تم ضبط رسالة أو ملف ما؛ فى الجهاز الثانى الذى تم دخوله عن طريق الجهاز محل الإذن. فهل هذا الضبط صحيح أم أن مأمور الضبط القضائى يكون قد تجاوز حدود ذلك الإذن؟

أو بمعنى أدق هل يمتد إذن التفتيش الصادر لمأمور الضبط القضائى إلى أجهزة الحاسوب المرتبطة بجهاز الحاسوب محل الإذن؟ وهل يتساوى الأمر إذا كانت تلك الأجهزة المرتبطة موجودة داخل حدود الدولة أو خارجها؟ أم أنه يتعين عليه الحصول على إذن تفتيش مستقل لهذه الأجهزة؟ وهل يؤثر فى ذلك خصائص الدليل التقنى من حيث سهولة تدميرها أو حتى إمكانية قطع الاتصال مع هذه الأجهزة المرتبطة بسهولة إذا ما عرف أمر التفتيش؟

وعلى ذلك، فإن تفتيش أجهزة الحاسوب وما له من طبيعته الخاصة يضعنا أمام عدة تساؤلات تتعلق بمشروعية تفتيش الملفات الموجودة على الأجهزة المرتبطة بالجهاز الصادر بشأنه إذن التفتيش إذا كان يعتقد أنه يحوى ملفات تفيد فى كشف الحقيقة.

١- تفتيش الحاسب الآلى والأنظمة المتصلة به فى الداخل:

سمحت اتفاقية بودابست وبعض التشريعات المقارنة لرجال الضبط القضائى بتفتيش الأجهزة المرتبطة بجهاز الحاسوب محل الإذن. ورفضت التشريعات الأخرى امتداد

ذلك التفتيش. وسوف نوضح هذه التشريعات ثم نبين موقف التشريع المصرى وذلك على النحو التالى:

اتفاقية بودابست: نصت المادة ١٩ من القسم الرابع للاتفاقية الأوروبية لجرائم السايبر- بودابست- على أنه (من حق السلطة القائمة بتفتيش الكمبيوتر الموجود فى دائرة اختصاصها أن تقوم- فى حالة الاستعجال- بمد نطاق التفتيش إلى أى جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلى محل التفتيش)[١٨].

وبذلك سمحت الاتفاقية للدول الأعضاء بامتداد التفتيش الذى يجرى، إلى نظام حاسوب آخر أو جزء منه إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المتطلبة تم تخزينها فى ذلك النظام، بشرط أن يكون فى النطاق الاقليمى، كما يجب أن يكون الدخول على البيانات المراد التفتيش عنها قانونيًا من نظم الحاسوب الأولى. وذلك على النحو الذى بينته المذكرة الإيضاحية لتلك الاتفاقية[١٩].

وذات الأمر قررته **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، حيث نص البند الثانى من المادة السادسة والعشرين على أنه (تلتزم كل دولة طرف بتبنى 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 فى تقنية معلومات أخرى أو جزء منها فى إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة فى التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى)[٢٠].

وأجاز المشرع الفرنسى ذلك الإجراء بموجب ما نصت عليه المادة ١٧ فقرة أ من قانون الأمن الداخلى رقم ٢٣٩ لسنة ٢٠٠٣ والتى نصت على أنه (يجوز لرجال الضبط القضائى من درجة ضابط وغيرهم من رجال الضبط القضائى أن

يدخلوا عن طريق الأنظمة المعلوماتية المثبتة فى الأماكن التى تم التفتيش فيها على البيانات التى تهم التحقيق والمخزنة فى النظام المذكور أو فى نظام معلوماتى آخر ما دامت هذه البيانات متصلة فى شبكة واحدة مع النظام الرئيسى أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسى)[٢١].

وفى التشريع الهولندى سمحت المادة ١٢٥ فقرة (j) من قانون الإجراءات الجنائية الهولندى بإمكانية امتداد التفتيش إلى الأجهزة التقنية الموجودة فى مكان آخر ما دامت مرتبطة بهذا الجهاز بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة وإذا ما وجدت هذه البيانات يجب تسجيلها كوسيلة لضبطها[٢٢].

وفى ألمانيا: يرى الفقه؛ متى تبين أن الحاسب أو النهاية الطرفية فى منزل المتهم– محل الإذن– متصلة بجهاز أو نهاية طرفية فى مكان آخر مملوك لشخص غير المتهم، فإنه يمكن أن يمتد التفتيش إلى سجلات البيانات التى تكون فى موقع آخر[٢٣]. وقد استندوا فى ذلك إلى مقتضيات توسيع تفسير نص المادة ١٠٣ من قانون الإجراءات الجنائية متى كان مكان التخزين الفعلى فى خارج المكان الذى يتم فيه التفتيش[٢٤].

وفى القانون الكندى وضع المشرع قواعد خاصة بالتفتيش التقنى للحاسوب، وذلك فى المادة ٤٨٧ (١/٢) (a) من قانون الإجراءات الكندى، والتى نصت على أنه (للقائم بتفتيش النظام وفقا لأحكام هذا الفصل أن يقوم بتفتيش أجهزة الكمبيوتر الأخرى الموجودة فى ذات المكان أو فى ذات المبنى الذى صدر بخصوصه إذن بتفتيش كمبيوتر وذلك للبحث عن أى بيانات متاحة لنظام جهاز الكمبيوتر)[٢٥]. وكذلك أعطت المادة ١٦ من قانون المنافسة الكندى الحق للقائم بالتفتيش فى ضبط المعلومات التى توجد فى أنظمة الحاسوب للشركة محل التفتيش وكذلك الأجهزة المتصلة بها[٢٦].

وفى القانون البلجيكى: أكدت المادة ٨٨ من قانون الإجراءات الجنائية جواز امتداد إذن التفتيش الصادر من القاضى إلى أنظمة الكمبيوتر المختلفة المرتبطة بالحاسب محل الإذن وفق ضوابط معينة، حيث نصت على أنه (إذا أمر قاضى التحقيق بالتفتيش فى نظام معلوماتى أو فى جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتى آخر يوجد فى مكان غير مكان البحث الأصلى، وذلك وفق ضابطين ١- إذا كان ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث ٢- إذا وجدت مخاطر تؤدى إلى فقد الأدلة إذا لم يمتد التفتيش)[٢٧].

وفى أستراليا لم يقصر القانون الاتحادى صلاحية التفتيش فيما يتعلق بالأدلة التقنية على مواقع محددة، فقد أشار قانون الجرائم السايبرانية لعام ٢٠٠١ إلى أن البيانات التقنية يمكن أن تتوزع على شبكة الحواسيب، وبالتالى سمح هذا القانون بامتداد عمليات تفتيش البيانات إلى خارج المواقع محل الإذن والتى يمكن اختراقها من خلال حواسيب توجد فى البنية الجارى تفتيشها. ويشير مصطلح (البيانات المحتجزة فى حاسوب ما) إلى أية بيانات محتجزة فى جهاز تخزين على شبكة حواسيب يشكل الحاسوب محل الإذن جزء منها، فلا توجد حدود جغرافية محددة ولا أى اشتراط بالحصول على موافقة طرف ثالث[٢٨].

وفى الولايات المتحدة الأمريكية: أجازت التوجيهات الداخلية الخاصة بإجراءات التفتيش امتداد إذن التفتيش لمقر شركة معينة إلى فروعها الكائنة فى نفس العقار[٢٩].

ومن ناحية أخرى: بين المرشد الفيدرالى الأمريكى لتفتيش وضبط الحاسوب تفتيش الشبكات بطريقة أكثر وضوحًا. حيث أشار إلى أن القاعدة العامة وفق القراءة الصارمة للمادة ٤١ من قانون الإجراءات الجنائية الفيدرالى (أنه يجب على رجال الضبط القضائى الحصول على العديد من الأذون إذا كان لديهم سبب يدعو إلى

الاعتقاد بأن تفتيش الشبكة سوف يؤدى إلى استرداد بيانات مخزنة فى مناطق عديدة)[٣٠].

ومع ذلك جاءت المادة سالفة الذكر فى فقرتها (a) وقررت أنه (إذا أصدر قاضى التحقيق فى نطاق اختصاصه المكانى إذنا لتفتيش ملكية داخل المنطقة... أو تفتيش ملكية خارج المنطقة إذا كانت الملكية داخل المنطقة عند طلب الإذن، ولكن ربما تتحرك لخارج المنطقة قبل تنفيذ الإذن)[٣١]. وتوضيحًا لذلك فقد يصدر قاضى التحقيق إذنا بتفتيش سيارة معينه وذلك فى نطاق اختصاصه المكانى، إلا أنه عند تنفيذ ذلك الإذن قد تتحرك تلك السيارة لمكان آخر خارج الاختصاص المكانى لقاضى التحقيق. وعليه فإن ضبط السيارة فى الحالة الأخيرة عمل لا يشوبه البطلان.

وإذا كان الأمر على هذا النحو، فقد وسعت المحكمة العليا الأمريكية من نطاق تفسير المادة ٤١ من قانون الإجراءات الجنائية الفيدرالى فى وصفها لمعنى (الملكية) حيث لم تقصرها على الملكية المادية فقط بل جعلتها تشمل الملكية غير المادية مثل بيانات الحاسوب[٣٢].

وتطبيقًا لذلك ففى ظل القانون الأمريكى: فإنه يتم التفرقة بين أمرين: الأول: أن يكون رجال الضبط القضائى قادرين على معرفة الأماكن المخزن فيها الملفات المطلوبة، فإذا كانت أماكن التخزين فى مكانين مختلفين أو أكثر داخل الولايات المتحدة الأمريكية، فإنه على رجال الضبط القضائى الحصول على أذون إضافية لكل مكان توجد فيه البيانات، وذلك تطبيقًا لنص المادة ٤١.

الثانى: إذا كان رجال الضبط القضائى لا يعرفون أو لا يستطيعون أن يعرفوا أماكن وجود البيانات المراد تفتيشها، وعما إذا كانت هذه البيانات موجودة فى منطقة واحدة أو أكثر، فإن الدليل الذى يتم ضبطه بعيدًا عن منطقة الاختصاص لا يشوبه البطلان، ذلك أنه يمكن أن تتوصل المحاكم إلى أن رجال الضبط القائمين

على تفتيش الحاسوب تسببوا بدون قصد فى إرسال- تحريك- المعلومة من منطقة إلى أخرى، وبالتالى يكون ذلك متفقا مع المادة ٤١ سالفة الذكر[٣٣].

وعلى العكس من ذلك: فإن هناك من التشريعات المقارنة ما تجعل إذن التفتيش مقصورًا على الأجهزة الموجودة فى مكان محدد دون امتدادها إلى الأجهزة المرتبطة مثل التشريع السويسرى[٣٤].

موقف التشريع المصرى:

سمحت المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات بتتبع البيانات والمعلومات فى أى مكان أو نظام أو حاسب تكون موجودة فيه. فقد نصت المادة سالفة البيان فى البند رقم (١) من الفقرة الأولى على أنه (لجهة التحقيق المختصة بحسب الأحوال... ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه).

وإذا كان النص على النحو سالف البيان لم يبين صراحة عما إذا كان هذا التتبع يتضمن إمكانية الدخول إلى الأجهزة التقنية الموجودة فى مكان آخر والمرتبطة بالجهاز التقنى محل الإذن بالضبط أم لا؟ فضلا عن ذلك فإنه نظرًا لحداثة الموضوع فلم تتعرض له محكمة النقض المصرية حتى الآن. فكان لزامًا علينا بيان المحاولات الفقهية التى تعرضت لهذا الأمر حتى وإن ظهرت قبل صدور القانون رقم ١٧٥ لسنة ٢٠١٨.

فقد انقسم رأى الفقه إلى ثلاثة آراء: الأول- أقر بامتداد التفتيش للنظام التقنى المتصل بالنظام محل الإذن، والثانى- رفض امتداد التفتيش، بل واشترط صدور قرار مسبب من قاضى التحقيق. وظهر رأى ثالث اتخذ موقفًا وسطًا. وسوف نبين هذه الآراء ثم نتبعها برأينا، وذلك على النحو التالى:

الرأى الأول: استقر أنصار هذا الرأى على أن التفتيش يمتد إلى أى نظام معلوماتى متصل بالنظام المعلوماتى الصادر بشأنه إذن التفتيش، واستندوا فى ذلك إلى طبيعة الأدلة التقنية التى يتم التفتيش بحثا عنها، إذ إنه يمكن العثور عليها مخبأة داخل نظام معلوماتى آخر لم يتم الحصول على إذن بتفتيشه. فقد توجد استحالة فى الوصول بالفحص الفنى لمكان وجود الدليل تحديدًا داخل النظام المعلوماتى المراد تفتيشه، وإنما يتم التحديد من خلال النظام المعلوماتى محل الجريمة[٣٥]، وإذا كان التشريع المصرى لم يواجه الجرائم المستحدثة بما فيها من نقاط فنية يعجز القانون التقليدى عن ملاحقتها وإيقافها، الأمر الذى يؤدى إلى استخدام الجناة تلك الثغرات القانونية، فيقوم المجرم المعلوماتى بوضع المعلومات المسروقة على نظام معلوماتى آخر غير النظام محل الإذن ولكنه متصل به، معتمدًا على أن التشريع المصرى لم يتناول مسألة امتداد التفتيش، وطالما لم يجرم المشرع أو يرتب البطلان على الدخول والتفتيش داخل نظام معلوماتى متصل بالنظام محل التفتيش بغير إذن فإنه يمكن للسلطة المختصة القيام بذلك وصولًا إلى ضبط الجناة[٣٦].

الرأى الثانى: رفض انصار هذا الرأى[٣٧] امتداد التفتيش ليشمل الحاسوب المرتبط بالجهاز المأذون بتفتيشه والموجود داخل الدولة، واستند البعض منهم إلى حكم نسب لمحكمة النقض المصرية خلص إلى أن إلقاء صاحب المنزل المأذون بتفتيشه للفافة فى أحد المنازل المجاورة لا يخول لمأمور الضبط القضائى تعقب ما ألقى فى المنزل المجاور[٣٨].

بل واشترط هذا الرأى صدور أمر مسبب من القاضى الجزئى متى كان الحاسب الموجود فى مسكن المتهم متصلًا بأجهزة معلوماتية موجودة فى أماكن أخرى داخل الدولة، كمسكن غير مسكنه أو خاصة بشخص آخر غير المتهم، وذلك استنادًا إلى الفقرة الثالثة من المادة ٢٠٦ من قانون الإجراءات الجنائية المصرى[٣٩].

ورد أنصار هذا الرأى على ما يراه البعض من إعمال حكم الفقرة الثانية من المادة ٧١ من قانون الإجراءات الجنائية والتى نصت أن (للمندوب أن يجرى أى عمل آخر من أعمال التحقيق أو أن يستجوب المتهم فى الأحوال التى يخشى فيها فوات الوقت متى كان متصلًا بالعمل المندوب له ولازمًا فى كشف الحقيقة) من أن تلك رؤية غير صائبة لأن تفتيش المنازل بغير رضا أصحابها محظور بنص الدستور– ولو فى حالة الضرورة– إلا بناء على أمر قضائى مسبب– م ٤٤ من الدستور والتى تقابلها المادة ٥٨ من الدستور الحالى ٢٠١٤– وفى مقابل ذلك يستطيع مأمور الضبط القضائى اتخاذ الإجراءات التحفظية اللازمة حتى يتم استصدار إذن التفتيش المطلوب من الجهة المختصة. ورغم ذلك اعتبر أنصار هذا الرأى الإجراءات التحفظية التى– نادوا بها– أنها تتعارض مع خصائص الدليل التقنى الذى قد يطمس عمدًا من قبل المتهم أثناء تحضير إذن التفتيش الجديد(٤٠).

وبين هذين الرأيين ظهر رأى ثالث: لم ينكر تفتيش الأجهزة المرتبطة بصفة مطلقة، وقصره فقط على حالة التلبس وأرجع ذلك إلى أن قواعد تفتيش أجهزة الكمبيوتر لها ذاتية تميزها عن قواعد التفتيش التقليدية، ذلك أن تفتيش أجهزة الكمبيوتر المرتبطة غير الخاصة بالمتهم لا تحتاج إلى الانتقال لمكان وجودها، بل يتم ذلك عن بعد بواسطة وسائل تقنية حديثة (برامج دخول). أما فى غير ذلك فإن قواعد التفتيش تقتضى أن يقوم مأمور الضبط القضائى عند تنفيذ إذن تفتيش المكان باصطحاب اثنين من الشهود، سواء من أصحاب المنزل محل التفتيش أو غيرهم (م ٩٢ إجراءات جنائية). وإذا تعلق الأمر بجهاز كمبيوتر فيمكن له أن يصطحب اثنين من الخبراء فى مجال الكمبيوتر(٤١).

وعاب أنصار هذا الرأى على ما جاء بنص المادة التاسعة عشرة من القسم الرابع لاتفاقية بودابست والتى أتاحت تفتيش أجهزة الكمبيوتر المرتبطة متى كانت

متاحة للجهاز محل التفتيش، ذلك أن أجهزة الكمبيوتر قد تتصل ببعضها البعض فى انحاء العالم، فلا يعقل أن تكون سلطة التفتيش من الاتساع بحيث تمتد إلى أجهزة كثيرة ومتعددة، لذا فإذا صح القول بأن هذا النص يؤدى إلى جواز التفتيش بدون إذن لتلك الأجهزة، فإن ذلك يتعارض مع ميثاق الحقوق والحريات الكندى- الفصل الثامن- الذى يؤكد حماية حق الفرد من التفتيش والضبط غير المعقولين[٤٢].

ونرى أن الرأى الأول هو الرأى الأولى بالتأييد، فمتى كان جهاز الحاسوب محل الإذن مرتبطًا بجهاز آخر، فإن إذن التفتيش والضبط يمتد ليشمل ذلك الجهاز. وذلك بشرطين: الأول- أن يكون الدخول للمعلومات الموجودة بداخل الجهاز قد تم عن طريق الجهاز محل الإذن. والشرط الثانى- أن يحوى هذا الجهاز على بيانات أو معلومات تكون لها فائدة فى إظهار الحقيقة، وذلك حتى نتجنب التعسف فى تنفيذ الإذن.

وسندنا فى ذلك أن المشرع أورد فى نص البند (١) من الفقرة الأولى من المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ (ضبط أو سحب... البيانات والمعلومات... أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه) وكلمة التتبع اصطلاحًا تعنى سار فى أثره، أى أن لجهة التحقيق أن تصدر قرارها لمأمور الضبط القضائى بتتبع البيانات والمعلومات- أى السير فى أثرها- فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه.

فضلًا عن ذلك فقد أناط المشرع لجهة التحقيق المختصة إصدار الأمر بتتبع البيانات والمعلومات فى أى مكان أو نظام تكون موجودة فيه والبحث والتفتيش فى برامج الحاسب وقواعد البيانات والنظم المعلوماتية (م ١/٦ من قانون مكافحة جرائم تقنية المعلومات)، وجهة التحقيق المختصة وفق عموم النص إما أن تكون

النيابة العامة وإما قاضى التحقيق بحسب الأحوال، وعلى ذلك فيجوز لعضو النيابة أن يصدر الإذن بتفتيش وضبط أجهزة الحاسوب والنظم المعلوماتية حتى ولو كانت فى حيازة غير المتهم أو موجودة فى منزل غير منزله[٤٣]، وإذا كان الأمر على هذا النحو؛ فلا يجوز القول بأنه ليس من سلطة عضو النيابة أن يصدر أمره بتتبع البيانات والمعلومات حتى ولو كانت موجودة فى جهاز حاسوبى آخر يمكن الولوج إليه من خلال الجهاز الخاص بالمتهم.

كما أن هذا التفسير يتفق مع ما ورد بالبند الثانى من المادة السادسة والعشرين من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التى وقعت عليها مصر وأصدر المشرع المصرى القانون رقم ١٧٥ لسنة ٢٠١٨ إعمالًا لهذه الاتفاقية. فقد نصت المادة المشار إليها على أنه (تلتزم كل دولة طرف بتبنى الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينه أو جزء منها بما يتوافق مع الفقرة (١- أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة فى تقنية معلومات أخرى أو جزء منها فى إقليمها وكانت هذه المعلومات قابلة للوصول قانونًا أو متوفرة فى التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول إلى التقنية الأخرى).

ويجب أن نوضح أن الارتباط (الاتصال) بين أجهزة الحاسوب فى هذا الموضع- كما سبق وأن بينا- يقصد به: وجود جهاز حاسوب أو أكثر متصل بالجهاز محل التفتيش سواء كان ذلك عن طريق شبكة سلكية أو لاسلكية، ومن خلال ذلك الاتصال الوصول إلى المعلومات الموجودة فى الجهاز الثانى بواسطة الجهاز محل التفتيش. ومن ثم فيخرج من هذا النطاق الأجهزة التى تتصل ببعضها بعضا عن طريق جهاز راوتر واحد، وتأخذ هذه الصورة قيام أحد الأشخاص بالاشتراك مع إحدى الشركات التى تقدم خدمة الإنترنت، ويتم توصيل الخدمة من خلال جهاز راوتر

معين، وقد يستفاد أكثر من جهاز حاسوب من خدمة الإنترنت إذا اتصل سلكيًا بجهاز الراوتر. فلا تعد أجهزة الحاسوب سالفة الذكر مرتبطة ذلك أنه لا يمكن الوصول إلى المعلومات الموجودة بتلك الأجهزة من خلال الجهاز محل التفتيش.

فالواقع العملى كشف عن عدم فهم البعض من رجال الضبط القضائى وسلطة التحقيق للمقصود بامتداد إذن التفتيش للأجهزة المرتبطة بالجهاز محل الإذن، فاعتبروا أن مجرد وجود اتصال بين جهازى حاسوب سلكيًا عن طريق جهاز راوتر واحد يتحقق به معنى الارتباط، إذ تم ضبط وتفتيش جهاز الحاسوب الخاص بالمتهم لارتباطه بجهاز الحاسوب محل الإذن سلكيًا عن طريق جهاز راوتر واحد. وذلك فى قضية تتلخص فى أن إحدى الصفحات على موقع التواصل الاجتماعى- فيسبوك- تقوم بنشر أسئلة الامتحان الخاصة بالثانوية العامة، ومن خلال العنوان التعريفى تم التوصل إلى شخص وعنوان المتحرى عنه، وبعد إجراء التحريات صدر إذن من النيابة العامة بضبط وتفتيش شخص ومسكن الأخير وضبط كل الأجهزة التقنية المستخدمة فى ارتكاب الجريمة، وحال تنفيذ الإذن تبين أن المتهم يشارك المتحرى عنه فى خدمة الإنترنت عبر كابل ممتد من جهاز الراوتر الخاص بالمتحرى عنه، وبناء على ذلك الإذن أيضًا تم ضبط الجهاز الخاص بالمتهم حيث أقر بالجريمة وبتفتيش جهاز الحاسوب الخاص به عثر على ملفات خاصة بالجريمة محل الإذن[٤٤]. وفى واقعة أخرى أسفرت التحريات عن قيام المتهم بإنشاء صفحة على موقع التواصل الاجتماعى تسمى (داهف) هدفها التحريض على ارتكاب أعمال تخريبية داخل الدولة، وأصدرت النيابة العامة- وكيل النيابة- إذنًا بضبط وتفتيش شخص ومسكن المتهم وضبط الأجهزة التقنية المستخدمة فى ارتكاب تلك الجريمة وكذا تتبع خطوط ووصلات الشبكة الخاصة بجهاز ADSL إن وجدت[٤٥].

٢- تفتيش الحاسب الآلى والأنظمة المتصلة به فى الخارج:

يظهر أحيانًا فى أثناء التحقيقات أنه من الضرورى تفتيش جهاز حاسوب موجودة فى الخارج، كما لو تعلق الأمر بشركة رئيسية وفروعها فى الخارج، حيث ترتبط أجهزة الشركة بعضها ببعض، أو أن ترتبط تلك الأجهزة بقاعدة بيانات موجودة فى الخارج. وهنا يثار التساؤل: هل يمتد إذن التفتيش ليشمل جهاز حاسب آخر موجودا خارج الدولة ولكنه متصل بجهاز الحاسب محل الإذن؟

نقول إن هذه المشكلة من المشكلات التى تواجه سلطات التحقيق وجمع الأدلة وخاصة أن الكثير من مرتكبى الجرائم يتعمدون تخزين بياناتهم فى أنظمة تقنية خارج الدولة عن طريق شبكة الإنترنت وذلك بهدف عرقلة التحقيقات[٤٦].

وسوف نبين فى هذا المطلب ما استقرت عليه الاتفاقيات الدولية والتشريعات المقارنة ثم نعقبه برأينا، وذلك على النحو التالى:

أ- الاتفاقيات الدولية:

المجلس الأوروبى: أطلق المجلس الأوروبى على تفتيش النظام إذا كان موجودا فى دولة أخرى اسم الاختراق المباشر أو التفتيش عبر الحدود[٤٧] وقد أصدر المجلس توصيات فى هذا الشأن؛ أجازت أن يمتد التفتيش التقنى لأجهزة الحاسوب إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة. فنصت التوصية رقم ١٣ لسنة ١٩٩٥ المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات فى مادتها الثالثة على أنه (لسلطة التحقيق عند تفتيش المعلومات- وفقًا لضوابط معينة- أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل فى دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات الموجودة فيها ما دام أنه من الضرورى التدخل الفورى للقيام بذلك)[٤٨].

كما نصت المادة السابعة عشرة منها على أنه (يمكن أن يمتد نطاق تفتيش الكمبيوتر إلى النظام الموجود فى الخارج، إذا كان من الضرورى اتخاذ إجراءات عاجلة فى هذا الشأن. ويتعين أن يوجد أساس قانونى لامتداد مجال هذا النوع من التفتيش حتى لا يشكل ذلك الإجراء مخالفة لسيادة دولة أجنبية. لذلك فإنه من الضرورى الحصول على موافقة الدولة التى يمتد التفتيش إلى نظام يوجد على إقليمها)[٤٩].

وكذلك نصت المادة الثامنة عشرة منها على أنه (من الضرورى إدخال إجراءات تتسم بالاستعجال تخول سلطات البحث والتحقيق أن تطلب من سلطات أجنبية أن تقوم بجمع الأدلة بشكل عاجل. لذا يجب تخويل السلطات المطلوب إليها أن تقوم بتزويد الجهة الطالبة بالمعلومات المتعلقة بحركة المراسلات التقنية وأن تقوم باعتراض اتصالات معينة أو تقوم بتحديد مصادرها. ولتحقيق هذا الغرض يتعين إيجاد الوسائل التى تسمح بالمساعدة القضائية فى هذا الخصوص)[٥٠].

اتفاقية بودابست: نصت المادة ٣٢ من الاتفاقية الأوروبية بشأن جرائم الإنترنت– بودابست– على أنه يمكن لأى طرف دون تصريح من الطرف الآخر:

١– أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور (مصدر مفتوح) بغض النظر عن موقعها الجغرافى.

٢– أن يصل أو يتلقى عبر نظام معلوماتى يقع على إقليمه، بيانات معلوماتية مخزنة فى دولة أخرى، إذا حصل هذا الطرف على موافقة قانونية وإدارية من شخص لديه سلطة قانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال النظام المعلوماتى[٥١][٥٢].

وبذلك فقد أجازت اتفاقية بودابست إمكانية الدخول بغرض التفتيش والضبط فى أجهزة أو شبكات تابعة لدولة أخرى بدون إذن منها فى حالتين: الأولى– إذا تعلق

التفتيش بمعلومات أو بيانات متاحة للجمهور كما لو تم الدخول على الرسائل والندوات التى تجرى عبر الإنترنت والتى يتاح لكل الناس الاشتراك فيها أو متابعتها، فإن ذلك ليس عملا من أعمال التفتيش ولا تحتاج موافقة من دولة أخرى للقيام به. والثانية- إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش(٥٣).

كما انتهت اللجنة الأوروبية للمشكلات الجنائية التابعة للمجلس الأوروبى إلى القول بأن التفتيش والضبط والإجراءات القسرية الأخرى التى تقع على إقليم دولة أخرى تعتبر غير مشروعة، إلا إذا كان قانون الدولة يجيزها(٥٤). ويلاحظ أنه فى هذا الخصوص يُعَرف خبراء المجلس الأوروبى التفتيش بقولهم إنه يتوافر التفتيش فى إقليم دولة أجنبية إذا توافرت علاقة سببية بين أفعال سلطات التحقيق قى بلد معين وبين عمل جهاز كمبيوتر يوجد فى بلد آخر(٥٥).

وعلى ذلك، فإذا كان التفتيش التقنى عبر الحدود له أهميته فى إمكانية الوصول إلى الدليل فى ثوان معدودة، إلا أن ذلك يصطدم بقاعدة سيادة الدول الأجنبية. فتطبيق قواعد الضبط والتفتيش الصادرة من السلطات الأجنبية على إقليم دولة أخرى يعتبر من الوسائل القسرية التى لا يسمح أن تمارسها دولة على إقليم دولة أخرى حتى ولو كان ذلك بهدف البحث عن دليل على أن دولة صدر منها مخالفة للقانون(٥٦).

ب- الاتفاقية العربية لمكافحة جرائم التقنية الحديثة:

نصت المادة ١/٣٢ على أنه (على جميع الدول الأطراف تبادل المساعدات فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية فى الجرائم). كما نصت المادة ١/٣٩ على أنه (يجوز لأى دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضى

الدولة الطرف المطلوب منها بما فى ذلك المعلومات التى تم حفظها بحسب المادة السابعة والثلاثين). ونصت المادة ٤٠ على أنه (يجوز لأى دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى: ١- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة- مصدر مفتوح- بغض النظر عن الموقع الجغرافى للمعلومات. ٢- أن تصل أو تستقبل- خلال تقنية المعلومات فى إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذى يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة).

وبذلك اتفقت الاتفاقية العربية لمكافحة جرائم التقنية الحديثة مع ما انتهت إليه اتفاقية بودابست فى هذا الشأن من إمكانية الدخول بغرض التفتيش والضبط فى أجهزة أو شبكات تابعة لدولة أخرى بدون إذن منها فى حالتين: الأولى- إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور، فإن ذلك ليس عملًا من أعمال التفتيش ولا تحتاج موافقة من دولة أخرى للقيام به. والثانية- إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش.

جـ- التشريعات المقارنة:

حاولت بعض الدول التصدى لمشكلة امتداد التفتيش التقنى عن بعد عبر الحدود وذلك بإقرارها تشريعات تسمح بتفتيش الأنظمة المتصلة حتى ولو كانت موجودة خارج إقليم الدولة وذلك فى إطار التعاون الدولى وذلك على النحو التالى:

التشريع الفرنسى: أجازت المادة ١٧ فقرة ٢ من قانون الأمن الداخلى رقم ٢٣٩ لسنة ٢٠٠٣ لمأمورى الضبط القضائى أن يفتشوا الأنظمة المتصلة حتى ولو وجدت فى خارج الإقليم مع مراعاة الشروط المنصوص عليها فى المعاهدات الدولية، حيث نصت تلك المادة على أنه (إذا كانت البيانات مخزنة فى نظام معلوماتى يقع

خارج إقليم الدولة، فإنه يجوز لرجال الضبط الدخول على هذه البيانات مع مراعاة الشروط المنصوص عليها فى المعاهدات الدولية)[٥٧].

وفى المجر: يرى الفقه أن لجوء الجناة إلى تخزين بيانات بالخارج بهدف عرقلة التحقيقات لا يثير لغطا، وذلك فى إطار اشتراك الشرطة المجرية فى شبكة اتصالات الإنتربول[٥٨].

وعلى العكس من ذلك: فى **ألمانيا**– رفض بعض الفقهاء فكر امتداد التفتيش لأنظمة تقنية المعلومات الأجنبية لضبط البيانات المخزنة فيها، وذلك فى ظل غياب اتفاق خاص بين الدول المعنية، إذ قد يعتبر ذلك خرقًا لحقوق السيادة لدولة أخرى وتحايلًا على النصوص القائمة المتعلقة بقبول المساعدة القضائية[٥٩]. بل يمكن أن يعرض القائم به للعقاب على مخالفة النصوص الداخلية التى تحظر الولوج غير المصرح به لنظم الحاسبات[٦٠].

ويؤيد هذا الرأى التطبيق القضائى الألمانى– ذلك أنه فى إحدى قضايا الغش المعلوماتى ثبت اتصال جهاز حاسوب فى ألمانيا بشبكة اتصالات فى سويسرا يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطة التحقيق الألمانية الحصول على هذه المعلومات، لم يتحقق لها ذلك إلا من خلال التماس المساعدات المتبادلة[٦١].

وفى الولايات المتحدة الأمريكية: إذا ثبت لرجال الضبط القضائى قبل القيام بالتفتيش أن بعض أو جميع البيانات مخزنة بعيدًا خارج الأراضى الأمريكية فإنه يتعين القيام بأعمال تتراوح ما بين الملاحظة غير الرسمية إلى طلب رسمى للمساعدة موجه إلى الدولة المعنية. وأكثر من ذلك فإن بعض الدول قد تعترض على محاولات السلطات الأمريكية للإطلاع على حواسيب موجودة داخل حدود تلك الدول. وذلك على الرغم من أن التفتيش ربما يبدو محليًا بالنسبة لرجل الضبط الأمريكى الذى يقوم

بتنفيذ تفتيش داخل الولايات المتحدة وفقًا لإذن، إلا أن الدول الأخرى ربما تراه بشكل آخر، ومن ثم يجب طلب المساعدة القضائية قبل القيام بهذا التفتيش[٦٢].

التشريع المصرى: نصت المادة (٤) من القانون رقم ١٧٥ لسنة ٢٠١٨ على أنه (تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيرتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقًا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها).

وعلى ذلك فإن المشرع المصرى جعل امتداد التفتيش داخل نظام معلوماتى يوجد فى مكان آخر خارج الدولة مسألة تخضع للاتفاقيات الدولية والمعاهدات ونظام المعاملة بالمثل ما بين المنح والمنع. ويجب أن نضع فى الاعتبار أن الولوج داخل النظم المعلوماتية بغير إذن قضائى يعد فعلًا مجرمًا، وبالتالى يعد التفتيش داخل هذا النظام من قبيل انتهاك حرمة قوانين هذه الدول الأجنبية، بل قد تصل إلى أبعد من ذلك باعتبار هذا الفعل من قبيل أعمال الجاسوسية التى تمس الأمن القومى لأى دولة[٦٣].

ثانياً: التفتيش التقنى بناء على إذن

نصت المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أنه: (لجهة التحقيق المختصة بحسب الأحوال، أن تصدر أمرًا مسببًا لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد مرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحدة أو أكثر مما يأتى: البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط).

وبذلك فقد أجاز المشرع المصرى لجهة التحقيق أن تصدر أمرها لرجال الضبط القضائى بتفتيش أجهزة الحاسوب والنظم المعلوماتية (الشبكات) للوصول إلى البيانات والمعلومات التى تكون لها فائدة فى ظهور الحقيقة.

ويثار التساؤل هل يخضع التفتيش التقنى لذات القواعد والشروط المتطلبة فى الجرائم التقليدية أم أن له قواعده التى تخصه باعتبار أن محله هو جهاز الحاسوب والنظم المعلوماتية؟ وهل يعتبر الحاسوب جزءًا من المكان الذى يتم تفتيشه أم يتعين تخصيص محل الإذن ليسطر فيه الأجهزة التقنية وعددها بشكل ناف للجهالة؟ وهل يعتبر الحاسوب صندوقًا مغلقًا واحدًا؟ أم أن كل ملف داخل الحاسوب مستقل بذاته، بحيث يجب صدور إذن خاص لكل ملف على حدة؟ وإذا صدر إذن بضبط أحد ملفات الحاسوب فهل يعنى ذلك ضبط الجهاز بالكامل أو الشبكة بكاملها؟ وهل الإذن الصادر بتفتيش الحاسوب يسمح بضبط وتفتيش ملحقات هذا الجهاز من الطباعة والأقراص الممغنطة؟ وهل يحق لرجال الضبط الإفراط فى تنفيذ الإذن عن طريق عزل النظام بكامله؟ وهل لتجنب ذلك لهم الحق فى إجبار المتهم أو الشاهد على الإدلاء بالأرقام السرية اللازمة للدخول إلى النظام المعلوماتى؟

ونظرًا لحداثة قانون مكافحة جرائم تقنية المعلومات المصرى وعدم وجود تطبيقات قضائية فى شأنه كان لزامًا علينا الاستعانة بالقضاء والفقه المقارن حتى يتسنى لنا الإجابة على التساؤلات السابقة، والتى سوف نجيب عليها من خلال النقاط التالية:

١- الشروط الشكلية لأمر التفتيش التقنى.

٢- الشروط الموضوعية لأمر التفتيش التقنى.

٣- تعيين محل التفتيش التقنى.

٤- تنفيذ الإذن بالتفتيش والضبط التقنى.

٥- مدى جواز إلزام المتهم أو الشاهد بكشف شفرة الدخول إلى المعلومات المجرمة.

١- الشروط الشكلية لأمر التفتيش التقنى:

يشترط المشرع بعض الشروط التى يتعين أن تتوافر فى شكل الأمر الصادر بالتفتيش وإلا فَقَدَ الأمر أحد مقومات وجوده. فينبغى أن يكون الأمر ثابتًا بالكتابة، ومحددًا فيه موضوعه، وأن يكون مسببًا. ويثير تحديد موضوع الأمر فى جرائم التقنية الحديثة صعوبة كبيرة وخاصة أنه قد يصعب تحديد المطلوب تفتيشه على نحو دقيق، وذلك فى ظل وجود عدد كبير جدًا من الملفات وقد يتعمد الجانى إخفاء الملف الذى يحوى على المعلومات محل الضبط داخل ملفات أخرى أو يضع لهذه الملفات عناوين مضللة، وقد يثار التساؤل: إذا لم يتم تخصيص أمر التفتيش بالنص فيه على تفتيش الحاسوب؟ فهل يكفى لصحة الأمر أن يكون عامًا لضبط كل ما يفيد فى كشف الحقيقة؟

وسوف نتناول هذه الشروط وذلك على النحو التالى:

أ- أن يكون الأمر ثابتًا بالكتابة وأن يكون موقعًا ومؤرخًا:

فيتعين أن يكون أمر التفتيش ثابتًا بالكتابة كما هو الشأن فى جميع إجراءات التحقيق، فلا يكون منتجا أثره؛ إذن التفتيش الصادر شفويًا ولو أقر به وكيل النيابة بالجلسة[٦٤]. ولا إذن تليفونى ثابت فى دفتر الإشارات التليفونية ما دام ليس له أصل موقع عليه ممن أصدره[٦٥]. ولا يلزم وجود ورقة الإذن بيد مأمور الضبط القضائى المنتدب، لأن فى ذلك عرقلة لإجراءات التحقيق وهى بطبيعتها تقتضى السرعة، وإنما الذى يشترط هو أن يكون للتبليغ بفحوى الإذن أصل ثابت فى الأوراق[٦٦]، وإذا فُقد أمر الندب فإن هذا لا يمنع المحكمة من التعويل على الدليل الذى أسفرت عنه الإجراءات ما دامت المحكمة قد أوردت الأدلة السائغة على سبق صدور هذا الأمر[٦٧]. ويجب أن يتضمن

الأمر بيانات معينه من أهمها اسم من أصدره ووظيفته واسم المتهم والتهمة المنسوبة إليه وتوقيع مصدره، ولا يغنى عن التوقيع أن يكون الأمر محررًا بخط الآمر أو معنونا باسمه(٦٨).

ب- تحديد موضوع الضبط:

من أهم الشروط الشكلية اللازم توافرها فى إذن التفتيش تحديد الأعمال المطلوب إجراؤها، فكما سبق وأن بينا أن التفتيش عن ملفات الحاسوب أكثر تعقيدًا لأن تلك الملفات يمكن تخزينها فى أى شىء تقنى مثل القرص المرن أو فى عناوين مخبأة فى الحاسوب النقال الخاص بالمتهم أو غيره، أو على جهاز خادم يبعد آلاف الأميال عن المتهم، بل ويمكن تشفير تلك الملفات ووضع عناوين مضللة لها وتخزينها فى شكل ملفات غير تقليدية أو يتم خلطها بملايين الملفات التى ليس لها علاقة بالموضوع أو ملفات ضارة أو محمية. ونتيجة لعدم التأكد؛ فلا يمكن لرجال الضبط تقديم وصف دقيق للملفات التى يحتاجون إليها والقيام باستردادها، كما أن ذلك يتطلب ثقافة فنية متخصصة قد تتجاوز ثقافتهم بشأن الأشياء التى ينبغى ضبطها(٦٩).

ولا يقبل- تطبيقا للقواعد العامة- أن يكون إذن التفتيش شاملًا، وإنما ينبغى أن يكون أكثر تخصصا لكى يكون مبررا القيام به(٧٠)، وقد قضت بذلك المحكمة الفيدرالية الأمريكية فى هذا الصدد بأن إذن التفتيش الذى لا يبين ماهية الأشياء المراد ضبطها يعد كما لو كان يرمى إلى تخويل تفتيش عام بقصد اكتشاف الجرائم(٧١).

ويشير أكثر الفقه- الأمريكى- إلى أن أمر التفتيش الذى استخدم فى قضية وورد ضد المحكمة العليا- Ward v. Superior Court- يعد مثالًا نموذجيًا على التحديد الفنى المتطلب فى إذن التفتيش، والذى حدد المطلوب تفتيشه بأنه بنك ذاكرة الحاسب والأدوات الأخرى لتخزين البيانات والمزودة مغناطيسيًا حسب تصميم نظم المعلومات ببرامج حاسب طباعة عن بعد(٧٢). ومع أن تلك الصياغة كانت نموذجًا

لأمد طويل إلا أن جانبًا من الفقه رأى أنها قد فقدت صلاحيتها لأن التقدم التقنى قد تجاوزها[٧٣].

وحسبما تفيد الخبرة المستخلصة من الإدارة الأمنية لمركز المعلوماتية التابع للشرطة الملكية الكندية، فإنه يتعين أن يتضمن الإذن البحث عن وضبط: البرنامج أو الكيان المنطقى بما فى ذلك البرامج التطبيقية ونظام التشغيل والنظم الفرعية والبرامج والخدمات المساعدة أيا كان شكلها أو دعامتها المادية، بالإضافة إلى المستندات المتعلقة بهذا البرنامج أو الكيان المنطقى. وكذا البيانات (المعطيات) التى يجرى استخدامها عن طريق البرنامج سالف الذكر بما فى ذلك البيانات المعدة للتسجيل أو المسجلة فى ذاكرة الحاسب أو فى مخرجاته أيا كان شكلها أو دعامتها ووعاؤها وكذلك أية وثيقة تتعلق بها. وأيضًا: السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات بما فى ذلك سجل أو دفتر يومية التشغيل وسجل المعاملات وسجل الفواتير أيا كان شكل هذه السجلات أو الدعامة المادية التى تجسدها، بالإضافة إلى أى وثيقة تتعلق بها. بالإضافة إلى السجلات الخاصة بعمليات ولوج نظام المعالجة الآلية للبيانات واستخدام إمكاناته بما فى ذلك سجلات كلمات السر ومفتاح الدخول ومفاتيح فك الشفرات وذلك أيا كان شكلها أو دعامتها ووعاؤها وكذا أى وثيقة تتعلق بها[٧٤].

ومع ذلك يرى جانب من الفقه- وبحق- أنه لا يعتبر الإذن مخلًا بشرط التحديد إن نص على ضبط وتفتيش جهاز الحاسوب والأقراص الممغنطة والمدمجة وكل البرامج التى يمكن أن تحتوى على أدلة تفيد فى كشف الجريمة. بل ويكفى أيضًا لصحة الإذن أن يقتصر على ذكر ضبط جهاز الحاسوب الخاص بالمتهم دون تحديد أكثر من ذلك[٧٥].

بل إن أحكام القضاء الأمريكى اطردت على جواز ضبط الحاسوب مع أن الإذن جاء بصيغة عامة مشيرًا إلى المستندات بوجه عام دون الإشارة إلى المستندات المدمجة(٧٦).

جـ- تسبيب الأمر بالتفتيش:

اشترطت المادة السادسة من قانون مكافحة جرائم تقنية المعلومات أن يكون أمر التفتيش مسببًا، ويقصد بالتسبيب فى هذا المقام بيان العناصر التى تقنع بتوافر الدلائل والقرائن والإمارات الكافية المبررة لإصدار أمر التفتيش(٧٧). ولم يرسم القانون للتسبيب شكلًا ولا قدرًا معينًا، وجرى قضاء النقض على أنه يجوز لمصدر الأمر أن يتخذ من الدلائل الواردة فى محضر تحريات الشرطة إذا رأى جديتها أسبابًا لأمره بالتفتيش، وأن تأشير وكيل النيابة على محضر التحريات بالإذن بالتفتيش تفيد أنه اتخذ من الدلائل الواردة فى هذا المحضر أسبابًا لأمره(٧٨).

٢- الشروط الموضوعية لأمر التفتيش التقنى:

نصت المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات على أنه (لجهة التحقيق المختصة بحسب الأحوال، أن تصدر أمرًا مسببًا لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد مرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحدة أو أكثر مما يأتى: البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط) ويستبين من النصوص السابقة أن هناك عدة شروط موضوعية يتعين توافرها لصدور الأمر بالتفتيش:

أ- أن نكون بصدد جريمة معاقب عليها بمقتضى أحكام قانون مكافحة جرائم تقنية المعلومات:

وهذه الجرائم أوردها المشرع فى الباب الثالث من القانون وهى: جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها (م ١٣)، جريمة الدخول غير المشروع (م ١٤)، وجريمة تجاوز حدود الحق فى الدخول (م ١٥)، وجريمة الاعتراض غير المشروع (م ١٦)، جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية (م ١٧)، وجريمة الاعتداء على البريد الإلكترونى أو المواقع أو الحسابات الخاصة (م ١٨)، وجريمة الاعتداء على تصميم موقع (م ١٩)، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة (م ٢٠)، وجريمة الاعتداء على سلامة الشبكات المعلوماتية (م ٢١) وجريمة حيازة البرامج والأجهزة والمعدات المستخدمة فى ارتكاب جرائم تقنية المعلومات (م ٢٢)، وجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكترونى (م ٢٣)، وجرائم اصطناع المواقع والحسابات الخاصة والبريد الإلكترونى (م ٢٤) وجرائم الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع (م ٢٥- ٢٦)، والجرائم التى ترتكب من مدير الموقع مثل إنشاء مواقع بهدف ارتكاب جريمة (م ٢٧) والعبث بالأدلة أو إخفائها (م ٢٨).

ومع أن نص المادة السادسة من قانون مكافحة جرائم تقنية المعلومات- سالف البيان- قد حدد نطاق الإذن البحث والتفتيش على هذه النوعية من الجرائم المستحدثة، فإنه يثار التساؤل: إذا ارتكبت جريمة تقليدية وكان الجانى يحتفظ ببعض المخاطبات الإلكترونية مع شركائه فى تلك الجريمة، فهل يعنى ذلك عدم جواز صدور الإذن بتفتيش جهاز الحاسوب أو النظام المعلوماتى الذى يحوى على هذه المخاطبات

الإلكترونية؟ نقول إنه فى هذا الشأن يتم اللجوء للقواعد العامة التى تتعلق بالتفتيش بحثًا عن الدليل.

ب- صدور الأمر بعد وقوع الجريمة:

يشترط أن يصدر الأمر بالتفتيش بعد وقوع جريمة من الجرائم المبينة سلفًا، لأن الأمر بالتفتيش إجراء تحقيق. والتحقيق لا يبدأ إلا من بعد وقوع الجريمة، والغرض منه هو جمع الأدلة على الجريمة التى وقعت. فإذا لم تكن هناك جريمة قد وقعت لم يكن هناك محل لإجراء تحقيق وبالتالى لإجراء التفتيش[٧٩]. ولا يعنى وقوع الجريمة وجوب تمامها، إذ يصح التفتيش ولو وقفت الجريمة عند حد الشروع، لأن الشروع لا يغير من وصف الجريمة وإنما يخفف من عقوبتها فحسب[٨٠].

وجرت أحكام القضاء فى مصر على أن العبرة فى القول بوقوع الجريمة كشرط لإصدار الأمر هى بظاهر الحال بصرف النظر عما يسفر عنه إجراء التفتيش، فلا يخل بسلامة الأمر عدم ضبط شىء أو يسفر التفتيش على أن الجريمة الصادر بشأنها الأمر لم تقع أصلًا[٨١]، كما لو ادعى شخص كذبًا على المتهم بأنه أرسل عبارات السب والقذف عبر رسائل البريد التقنى أو مواقع التواصل الاجتماعى المختلفة. وكذلك لو ثبت بعد التفتيش أن مرتكب الجريمة شخص آخر بخلاف المتهم.

وإذا كانت الجريمة لم تقع بعد فإن التفتيش لا يجوز، ولو كانت على وشك الوقوع. فلا يجوز إصدار أمر التفتيش عن جريمة مستقبلة[٨٢]، كما لو أثبتت التحريات أن المتهم يتواصل مع أحد القراصنة لتعلم كيفية اختراق المواقع الحكومية والبنوك وأنه ينوى اختراق هذه المواقع، أو أنه دخل على أحد المواقع التقنية التى تتيح المعلومات حول تصنيع القنابل البدائية فى الوقت الذى أكدت فيه التحريات ميوله الإرهابية. وبصفة عامة لا يجوز التفتيش لاكتشاف جريمة[٨٣]، ومن قبيل ذلك طلب

مأمور الضبط القضائى من المحقق إصدار إذن التفتيش بشأن شخص معين تثار بشأنه الشبهات بأنه يتواصل مع الأطفال القصر لتحريضهم على الفجور.

جـ- وجود دلائل كافية ضد شخص معين[٨٤]:

من الشروط الموضوعية لصحة أمر التفتيش أن توجد دلائل وأمارات جدية سابقة على إصداره تكفى لتوجيه الاتهام إلى الشخص المراد تفتيشه أو تفتيش منزله بارتكاب الجريمة موضوع التحقيق[٨٥]، أو أنه يحوز أشياء متعلقة بالجريمة التى يجرى التحقيق بشأنها[٨٦].

ويقصد بالدلائل الكافية بصفة عامة أنها شبهات مستمدة من الواقع والقرائن تنبئ عن ارتكاب شخص لجريمة من الجرائم[٨٧].

ويقصد بالدلائل الكافية فى الجرائم التقنية: مجموعة من المظاهر أو الأمارات المعينة التى تعتمد على خبرة ومهارة القائم بالتفتيش والتى تؤيد للوصول لمرتكب الجريمة سواء بوصفه فاعلًا أو شريكًا[٨٨]، أو أن نظام المعلومات المطلوب تفتيشه يحوى على بيانات ومعلومات لها فائدة فى ظهور الحقيقة. ولا يشترط أن تكون هذه الدلائل قد جاءت نتيجة إجراء سابق من إجراءات التحقيق، بل يصح أن تكون وليدة تحريات قام بها مأمور الضبط القضائى أو معاونوه طالما كانت هذه التحريات مثبتة فى المحاضر التى تحرر بمعرفتهم[٨٩].

وبذلك فإن الدلائل ليست مجرد ظن يراود المحقق وينبع من ذاته ولكنها أمارة ظاهرة لها وجود فى العالم الخارجى وتؤدى عقلًا إلى الاعتقاد بوجود ما يفيد فى كشف الحقيقة، ومعيار الكفاية فيها أن يراها الشخص المعتاد كذلك[٩٠]، ولا يعتبر البلاغ مجرد قرينة كافية على وقوع الجريمة، ولذلك يبطل التفتيش الذى يأمر به المحقق استنادًا إلى مجرد بلاغ تلقاه بوقوع الجريمة[٩١].

وتقدير كفاية الدلائل على الاتهام أو وجود المعلومات المتعلقة بالجريمة موكول إلى سلطة التحقيق تحت رقابة محكمة الموضوع التى لها- إن تبينت أن التفتيش تم بصفة مخالفة للقانون- أن لا تأخذ فى حكمها بالدليل المستمد منه[٩٢].

على أنه ينبغى ملاحظة أنه إذا قامت لدى المحقق أسباب جدية دعته إلى اتهام شخص معين واقتضى الأمر تفتيش جهاز الحاسوب الخاص به، فإنه لا ينال من صحة هذا التفتيش ما قد يسفر عنه التحقيق أو المحاكمة مستقبلًا من براءة هذا الشخص من الجريمة التى تم التفتيش بسببها، وينبنى على ذلك أنه إذا أسفر التفتيش عن اكتشاف جريمة أخرى فإن ما تم اكتشافه يصح الاعتداد به قانونًا، لأنه تفتيش صحيح، ذلك أن الأحكام فى قانون الإجراءات تجرى على حسب الظاهر. وتطبيقًا لذلك إذا أثبتت التحريات أن المتهم قد أرسل عبارات السب والقذف إلى المجنى عليها مستخدمًا فى ذلك جهاز الحاسوب الخاص به المرتبط بشبكة الإنترنت من خلال هاتف أرضى معين وبناء على إذن المحقق تم تفتيش الحاسوب الخاص بالمتهم وتبين أنه يحوي على صور جنسية خاصة بالأطفال- وهى الجريمة المؤثمة بموجب المادة ١١٦/أ من قانون الطفل رقم ١٢ لسنة ١٩٩٦- فإن اكتشاف الجريمة الأخيرة قد صادف صحيح القانون، ولا يؤثر فى ذلك ما تسفر عنه التحقيقات بشأن الجريمة الأصلية من أن نجل المتهم هو من أرسل تلك العبارات بواسطة جهاز الحاسوب المحمول الخاص به.

ويجدر التنبيه إلى أنه لا يشترط لصحة تفتيش أنظمة المعلومات أن يكون هناك شخص معين أسندت إليه الجريمة، بل يصح التفتيش ما دامت هناك دلائل كافية على وجود ما يفيد في كشف الحقيقة، سواء كان المحقق قد وجه الاتهام إلى شخص بعينه أو لم يكن قد اتهم أحدًا بعد.

ومن قبيل الدلائل الكافية فى جرائم التقنية: الربط بين نقل الصور الفاضحة وعنوان إنترنت بروتوكول مع رقم حساب المتهم لدى مزود الخدمة ووجود رقمين للتليفون لديه يُستخدمان فى ذلك، وكذلك الربط بين وسائل التحريض على الفسق والتهديد بنشر الصور الفاضحة المرسلة إلى المجنى عليها بعد عدة عناوين بريدية مرتبطة مع عنوان بروتوكول المتهم فى منزله وعنوان بروتوكول آخر فى محل عمله حال وجود خلافات عائلية سابقة بينه وبين المجنى عليها.

د- وجود فائدة من التفتيش:

حدد الشارع الفائدة أو الغاية من التفتيش بأنها (ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات) المادة ١/٦ بند ١ من قانون مكافحة جرائم تقنية المعلومات- وعلى ذلك فيجب أن يتوافر لدى المحقق أسباب كافية على أنه يوجد نظام الحاسوب أو النظام المعلوماتى بيانات أو معلومات لها فائدة فى ظهور الحقيقة على ارتكاب جريمة من الجرائم المؤثمة بموجب هذا القانون.

فإن لم يكن للتفتيش غاية يستهدفها، أو كان يستهدف غاية غير ما حدده الشارع فهو مشوب بعيب التعسف فى استعمال السلطة[٩٣]، ومثال الحالة الأولى أن تكون الواقعة هى اطلاع غير مصرح به على ملفات بيانات مخزنة داخل نظام حاسب إحدى الجهات من قبل أحد القائمين على تشغيله فإنه واضح منذ البداية أن التفتيش عقيم ولا طائل من ورائه[٩٤]، ومثال الحالة الثانية: أن تكون الجريمة المرتكبة سبًا وقذفًا عن طريق الإنترنت وأن تكون الغاية المرجوة من التفتيش هى معرفة حسابات المتهم لدى البنوك.

وتتطلب هذه الفائدة المرجوة أن يسبق التفتيش تحريات جدية تسوغ الأمر به بحيث إذا تم التفتيش دون أن تسبقه تحريات جدية تنبئ عن وجود دلائل قوية على

حيازة من تم تفتيشه لأشياء أو أجهزة معلوماتية تفيد فى كشف الحقيقة وأسفر هذا التفتيش عن كشف جريمة. فإنه لا يعتد بهذا التفتيش ولا بنتائجه[٩٥].

وعلى ذلك يقع باطلًا إذن التفتيش المبنى على مجرد أقوال من المرشد السرى؛ مفادها أن المتهم يدير صفحة على مواقع التواصل الاجتماعى لتبادل الزوجات مع آخرين وأن التحريات التى أجراها مأمور الضبط مصدرها ذلك المرشد السرى وأنه لم يقم بالدخول على ذلك الموقع للتأكد من صحة تلك الجرائم وتتبع مرتكبيها ومحاولة التواصل معهم. ذلك أن تلك التحريات تصبح مجرد إبلاغ تلقاه من المرشد السرى.

وإذا كان المشرع قد حدد الغاية من التفتيش بأنه يحصل (متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى هذا القانون) فهل يفهم من ذلك أنه يحصل فقط للبحث عن أدلة الاتهام أو تأييد الإدانة بخلاف التفتيش فى الجرائم التقليدية الذى يكون للبحث عن كل ما يفيد فى كشف الحقيقة طبقًا لنص المادة (٩١) من قانون الإجراءات الجنائية؟ نقول فى هذا الشأن أن مبدأ الحياد هو الذى ينبغى أن يسود التحقيق الابتدائى[٩٦] لذلك فإن ظهور الحقيقة على ارتكاب الجريمة لا يعنى البحث عن أدلة الإدانة فقط بل وأدلة البراءة أيضًا؛ فهى تظهر الحقيقة فى أن المشتبه فيه ليس متهمًا. وتطبيقًا لذلك إذا أقر المتهم بأنه سطر عبارات التحريض على الفسق للمجنى عليها من خلال بريده التقنى إلا أنها هى التى بادرت بإغوائه وأن الرسائل الخاصة بها قد طمسها، فإذا تم تفتيش جهاز الحاسوب الخاص بالمتهم وعثر على أثر لهذه الرسائل كان على القائم بالتفتيش ضبط تلك الرسائل المرسلة من المجنى عليها.

هـ- السلطة المختصة بإصدار الإذن:

تختلف التشريعات المقارنة فيما بينها بشأن الجهة صاحبة السلطة فى إصدار إذن التفتيش ما بين قاضى التحقيق والنيابة العامة والشرطة وذلك على النحو التالى:

التشريع الفرنسى: جعل المشرع الفرنسى قاضى التحقيق هو صاحب الاختصاص الأصيل فى إصدار إذن التفتيش، أما النيابة العامة فلا تختص بالتفتيش إلا فى حالات معينة كالتلبس. ومتى اختص قاضى التحقيق بالدعوى أصبح من حقه إجراء التفتيش على النحو الذى يراه مفيدًا فى كشف الحقيقة سواء كان ذلك لدى المتهم أو غيره دون قيد على سلطانه إلا ما تعلق بحقوق الدفاع[٩٧].

وفى إنجلترا: معظم الإجراءات الجنائية منوطة بالشرطة ما عدا بعض الجرائم التى تناط بالمدعى العام أو النائب العام[٩٨].

وفى الولايات المتحدة الأمريكية: فإنها تأخذ بنظام النيابة العامة، وهى التى يقع عليها عبء القيام بأغلبية الإجراءات الجنائية[٩٩].

أما فى مصر: فإن جهة التحقيق المختصة هى التى تصدر الإذن بالتفتيش، وهى إما أن تكون النيابة العامة وإما قاضى التحقيق بحسب الأحوال (م ١/٦ من قانون مكافحة جرائم تقنية المعلومات). ووفق عموم هذا النص فإنه يجوز لعضو النيابة المحقق أن يصدر الإذن بتفتيش وضبط أجهزة الحاسوب والنظم المعلوماتية حتى ولو كانت فى حيازة شخص آخر غير المتهم أو موجودة فى منزل غير منزله. ويجب أن نوضح أن الضبط والتفتيش هنا يقتصر فقط على ضبط أجهزة الحاسوب أو النظم المعلوماتية دون أن يتعداها لتفتيش شخص غير المتهم أو غير منزله، إذ أنه يتعين لصحة هذا التفتيش الحصول مقدمًا على أمر مسبب من القاضى الجزئى (م ٢٠٦ من قانون الإجراءات الجنائية) أو صدوره من قاضى التحقيق (م ٩١، ٩٤ من قانون الإجراءات الجنائية).

ولكن يثار التساؤل: هل يجوز أن للمحكمة أن تأمر بتفتيش الأجهزة والنظم المعلوماتية؟ ويثار هذا التساؤل بشكل كبير فيما يتعلق بالجرائم التقنية لا سيما أن هناك سمات معينة يتصف بها المجرم التقنى وهو أحد أصحاب الياقات البيضاء ومنها شغفه لإثبات مدى إتقانه المجال التقنى- فقد يبادر بعد تسليط الضوء عليه من خلال وسائل الإعلام إلى الاعتراف بمزيد من الأدلة التقنية، وذلك حال محاكمته، وأنه يحتفظ بتلك الأدلة فى بعض الحوافظ التقنية بمسكنه أو لدى الغير، فهل يجوز للمحكمة فى هذه الحالة أن تأمر بتفتيش تلك الأجهزة؟

استخلص بعض الفقهاء من وصف الشارع التفتيش بأنه عمل تحقيق أن مجاله مقتصر فقط على سلطة التحقيق الابتدائى فإذا دخلت الدعوى فى حوزة المحكمة، فقد انقضى هذا التحقيق بما يتضمنه من إجراءات(١٠٠).

غير أن هذه الحجة غير حاسمة؛ فوصف التفتيش بأنه "عمل تحقيق" لا ينبغى أن يحول بين المحكمة والأمر به، إذ إن إجراءات المحاكمة هى بدورها "أعمال تحقيق"، وبالإضافة إلى ذلك فإن هذا الرأى يناقض المبدأ الذى يخول للمحكمة أن تتخذ كل إجراء تراه ضروريًا أو ملائمًا لكشف الحقيقة، وهو المبدأ الذى قننه الشارع فى المادة ٢٩١ من قانون الإجراءات الجنائية ذلك أنه لا يعقل أن يحظر على المحكمة طريق ميسور لكشف الحقيقة، خاصة أن دور القاضى الجنائى ايجابى فعليه أن يتحرى الحقيقة بنفسه ولا يجوز له أن يقتصر على الأدلة التى قدمها له أطراف الدعوى. وغنى عن البيان أنه إذا ندبت المحكمة أحد أعضائها أو قاضيًا آخر لتحقيق الدعوى- المادة ٢٩٤ من قانون الإجراءات الجنائية- فله- دون شك- سلطة الأمر بالتفتيش إذا قدر ضرورته أو ملاءمته(١٠١).

ولا يكفى توافر صفة قاضى التحقيق أو عضو النيابة لكى يقوم بهذا الإجراء، بل لا بد وأن يكون مختصًا أصلًا بالتحقيق فى الجريمة التى أُصْدر بشأنها

أمر التفتيش[١٠٢] ويتحدد الاختصاص بالتحقيق بمحل الواقعة أو المكان الذى ضبط فيه المتهم أو محل إقامته[١٠٣]، وبناء على ذلك إذا صدر الإذن بالتفتيش من محقق فى غير دائرة اختصاصه كان الإذن باطلًا[١٠٤].

ويجب أن يكون من صدر له الإذن بالتفتيش من مأمورى الضبط القضائى (م ١/٦ من قانون مكافحة جرائم تقنية المعلومات) فلا يجوز ندب أعوانهم أو مرؤوسيهم وإلا كان الندب باطلًا[١٠٥]، فإذا أصدرت النيابة العامة إذنًا لأحد الخبراء التقنيين من غير مأمورى الضبط القضائى لتنفيذ إذن تفتيش محله إحدى الشبكات كان هذا الإذن باطلًا. غير أنه لمأمور الضبط القضائى الصادر له الإذن أن يستعين بالخبراء ممن لا تتوافر فيهم صفة الضبطية القضائية طالما كان ذلك تحت الإشراف المباشر لمأمور الضبط القضائى المندوب[١٠٦]. ولا يعيب الإذن صدوره من غير تعيين المأذون له بإجراء التفتيش حيث يمكن أن يقوم به أى مأمور من مأمورى الضبط المختصين بالتفتيش ولو كان غير من طلب الإذن له[١٠٧] إلا أن المحقق إذا كان قد اختص مأمورًا معينًا فلا بد وأن يقوم هذا المأمور بإجراء التفتيش بنفسه[١٠٨].

٣- تعيين محل التفتيش التقنى:

من الشروط الموضوعية لسلامة إصدار أمر التفتيش أن يكون محل الأمر معينا التعيين النافى للجهالة. محل التفتيش هو المستودع الذى يحتفظ فيه المرء بالأشياء التى تضمن سره، والمحل الذى يقع عليه التفتيش فى جرائم التقنية الحديثة هو الحاسوب والشبكة التى تشمل مكوناتها الخادم والمزود الآلى والمضيف[١٠٩]، وهذا المحل لا يكون قائما بذاته وإنما يشمله مكان ما أو عقار أو أن يكون بصحبة مالكه أو حائزه.

ولا يشكل الأمر صعوبة إذا كان جهاز الحاسوب محل التفتيش بصحبة المتهم، أو في مكان عام يسهل على مأمور الضبط القضائى دخوله كمقر شركة

مثلًا. ولكن تثار الصعوبة ويدق الأمر إذا كان جهاز الحاسوب المراد ضبطه وتفتيشه موجودًا داخل مكان ما أو عقار لا يجوز دخوله وتفتيشه إلا بموجب أمر قضائى كمنزل المتهم أو منزل غير المتهم، فإذا رفض صاحب الشأن تسليم جهاز الحاسوب محل الإذن، فهل لمأمور الضبط القضائى الدخول لهذا المكان وتفتيشه بحثًا عن ذلك الحاسوب أم يجب أن يتضمن الإذن فضلًا عن ضبط جهاز الحاسوب وتفتيشه– تفتيش مكان وجود الحاسوب بحثا عنه؟ وهل يختلف الأمر لو كان الحاسوب موجودًا فى منزل غير منزل المتهم؟ وهل يعتبر الحاسوب جزءًا من المكان الذى يتم تفتيشه أم يتعين تخصيص محل الإذن ليسطر فيه الأجهزة التقنية وعددها بشكل ناف للجهالة؟ وأيضًا هل يعتبر الحاسوب صندوقًا مغلقًا واحدًا أم أن كل ملف داخل الحاسوب مستقل بذاته، بحيث يجب صدور إذن خاص لكل ملف على حدة؟ وماذا بشأن تفتيش الحاسوب الذى يتشارك فيه المتهم مع آخرين؟ وسوف نجيب عن هذه التساؤلات، وذلك على النحو التالى:

بداية نبين أنه وفقًا للقواعد العامة للتفتيش– من الشروط الموضوعية اللازمة لسلامة إصدار أمر التفتيش أن يكون محل الأمر معينا التعيين النافى للجهالة، فما المقصود بذلك؟ نقول فى هذا الشأن؛ إن محل التفتيش قد يكون مسكنًا أو شخصًا، فإذا كان مسكنًا يكون تعيينه بأن يذكر أنه منزل فلان الكائن بشارع كذا ويكفى ذكر عنوان المنزل ولو حدث خطأ فى اسم المتهم[١١٠]، وأن يتضمن كذلك تعيين الشخص المقيم فيه الذى يوجه إليه الاتهام بارتكاب الجريمة أو أن تقوم ضده الدلائل على أنه يخفى الأشياء المتعلقة بها[١١١]. ولا يجوز أن يصدر أمر بتفتيش عدد غير محدد من المنازل كأن يصدر أمر بتفتيش منازل مدينة معينة أو قرية معينة أو جميع غرف فندق معين وذلك للبحث عن أداة ارتكاب الجريمة فمثل هذا الأمر باطل لعدم تحديد المحل الوارد عليه، وأيضًا لأنه لم يقع على دلائل كافية، بل اعتمد

على الحدس أملًا فى العثور على ما يرجو فى هذا المنزل أو ذاك[١١٢]. وهذه القواعد العامة تطبق أيضًا على جرائم التقنية الحديثة وتطبيقا لذلك: إذا ثبت من خلال التحرى ووسائل التتبع التقنية أن جهاز الحاسوب الخاص أو الهاتف الجوال الخاص الذى تمكن من اختراق قاعدة معلومات عملاء أحد البنوك وسرقتها يوجد فى إطار مجموعة معينة من العقارات فلا يجوز للمحقق إصدار أمره بتفتيش تلك العقارات بحثًا عن ذلك الجهاز. وإذا كان محل التفتيش شخصًا فيجب أن يحدد فيه الشخص المعنى بالتفتيش، والأصل أن يحدد باسمه، ويكفى تحديده بأى بيانات كما لو كان اسم الشهرة[١١٣]. أما إذا كانت لا توجد أى بيانات لتحديده أو كانت البيانات غير كافية لهذا التحديد كان الأمر باطلًا حتى ولو وقع التفتيش على الشخص المعنىِّ فعلًا[١١٤].

- رفض الحائز تسليم جهاز الحاسوب محل الإذن:

وإذا كان جهاز الحاسوب المراد ضبطه وتفتيشه فى حيازة آخر غير المتهم أو منزل غير منزله ورفض الحائز تسليم ذلك جهاز الحاسوب، فهل لمأمور الضبط القضائى تفتيش ذلك الشخص أو تفتيش منزله لضبط جهاز الحاسوب. فنرى أنه لا يجوز لمأمور الضبط القضائى تفتيش غير المتهم أو غير منزله إلا وفقًا للضمانات المقررة التى أوردها قانون الإجراءات الجنائية، فيجب صدور أمر قضائى من قاضى التحقيق أو من النيابة العامة بعد موافقة القاضى الجزئى يتضمن تفتيش الشخص أو المكان بحثًا عن جهاز الحاسوب وذلك إعمالًا للقواعد العامة فى هذا الشأن (م ٩١، ٩٤، ٢٠٦ من قانون الإجراءات الجنائية).

- مدى اعتبار الحاسوب جزءًا من المكان الذى يتم تفتيشه:

إذا صدر أمر تفتيش لمكانٍ فهل يشمل بالضرورة تفتيش هذا الحاسوب؟ أم أنه لكى يقع التفتيش على الحاسوب لا بد من تضمينه فى إذن التفتيش تخصيصًا إلى جوار الصيغة العامة التى تضمنها إذن التفتيش لكون الحاسوب متميزًا عن المحتويات

الأخرى للمنزل المراد تفتيشه- مثلًا- وفى هذه الحالة يجب أن يحدد إذن التفتيش الحاسوب المراد تفتيشه وعدد الأجهزة المراد تفتيشها؟

نرى اعتبار الحاسوب ضمن متعلقات المكان أو ما يحوزه المتهم- سواء كان ذلك بناء على حالة التلبس أو أمر صادر من المحقق- فالحاسوب والأجهزة الملحقة به تعد جميعها عرضة للتفتيش متى صدر الأمر بذلك[١١٥]. فأجهزة الحاسوب لا تكون قائمة بذاتها، بل تكون إما موضوعة فى مكان ما كمسكن أو مكتب وإما أن تكون صحبة مالكها أو حائزها كما هو الشأن فى الحاسوب المحمول أو الهاتف النقال. فحكم تلك الأشياء يتوقف على طبيعة المكان الموجودة فيه؛ فإذا كانت فى مكان خاص أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا فى الحالات التى يجوز فيها تفتيش المسكن وبذات الضمانات المقررة فى القانون[١١٦]. وإذا كان الشخص يهيمن على أجهزة الحاسوب فى الطرق والمواصلات العامة باعتباره حافظا لها، فإن تفتيش تلك الأجهزة لا يكون جائزًا إلا فى الأحوال التى يجيز فيها القانون تفتيش الشخص- بوجه عام- ذلك أن التفتيش يشمل الشخص ذاته وكل ما فى حوزته وقت التفتيش، سواء كان مملوكا له أو لغيره[١١٧].

وقد أكد القضاء الأمريكى فى العديد من أحكامه أن التفتيش الواقع على الحاسوب هو تفتيش صحيح متى كان إذن التفتيش جاء عاما بالمكان الموجود فيه هذا الجهاز، فلا يشترط صدور إذن صريح بتفتيش جهاز الحاسوب[١١٨].

ورغم ما انتهى إليه الفقه من صحة تفتيش أجهزة الحاسوب حتى ولو لم يتضمنها الإذن على سبيل التخصيص، فإن التطبيقات القضائية فى مصر قد بينت أن أذون التفتيش الصادرة بحثًا عن الأدلة المتصلة بالجرائم التقنية قد تضمنت على وجه الخصوص تفتيش أجهزة الحاسوب الموجودة فى المكان محل الإذن[١١٩]، ومع ذلك فنرى أن تفتيش الأجهزة التقنية يكون متفقًا وصحيح القانون حتى ولو كان إذن

التفتيش قد جاء عاما ولم ينص فيه على تفتيش الأجهزة التقنية بشرط عدم تجاوز الغرض من التفتيش.

- مدى اعتبار الحاسوب صندوقًا واحدًا مغلقًا:

ويثار التساؤل فى حالة صدور الإذن مخصصًا للبحث على ملف محدد داخل جهاز الحاسوب: فهل كل ملف من ملفات الحاسوب يعتبر صندوقًا مغلقًا بحيث يحتاج كل ملف منها إلى إذن قضائى مستقل عن الآخر؟ وهل يلتزم رجال الضبط القضائى بفحص الملفات التى تدل ظاهريًا على محتواها فقط دون غيرها أم يمتد التفتيش ليشمل جميع محتويات الحاسوب؟ وقد أثيرت هذه التساؤلات بسبب الطبيعة الخاصة لأجهزة الحاسوب التى تحوى بدورها على عدد كبير جدًا من الملفات التى يمكن تشفيرها أو وضع عناوين مضللة لها وتخزينها فى ملفات غير تقليدية، أو أن يتم خلطها بملايين الملفات التى ليس لها علاقة بالموضوع مما قد يشكل صعوبة على رجال الضبط القضائى عند فحص هذه الملفات، وصعوبة كذلك فى الالتزام بالغرض من التفتيش.

أجابت الأحكام الأمريكية عن هذه التساؤلات، فذهبت بعض الأحكام إلى اعتبار جهاز الكمبيوتر بما يحتويه من ملفات صندوقًا مغلقًا واحدًا، فلا يشترط صدور إذن قضائى لكل ملف على حدة[١٢٠]، فى حين ذهبت الأحكام الأخرى إلى أن كل ملف يحويه جهاز الحاسوب يعتبر صندوقًا مغلقًا قائمًا بذاته، ورتبت على ذلك وجوب صدور إذن خاص لكل ملف على حدة[١٢١].

وقد رأى اتجاه من الفقه فى مصر أنه لا ينبغى تفتيش كل الملفات التى يحويها جهاز الحاسوب بموجب إذن واحد فقط، ذلك لأن الإذن الذى صدر يكون بشأن جريمة محددة (جريمة قرصنة برامج مثلًا) وبإمكان المأذون بالتفتيش أن يصادف أثناء تنفيذ الإذن جريمة عرضية أخرى مثل حيازة صور داعرة، واستند هذا

الرأى أيضًا إلى أنه لا يتصور امتداد إذن التفتيش إلى كل ملفات الحاسوب لأن التفتيش ليس إذنًا باستباحة حرمة الشخص أو حرمة مسكنه بغير قيد كما أن التطور التقنى يجعل السعة التخزينية للحاسوب الملايين من الملفات، فلا يعقل أن يصدر الإذن ليشمل جميع هذه الملفات[١٢٢].

ونرى اعتبار الحاسوب ملفًا واحدًا بحيث يشمل الإذن كل الملفات الموجودة بالحاسوب طالما لم يوصم التفتيش بالتعسف، ذلك أنه- كما سبق القول- قد يتعمد الجانى إخفاء الملفات المطلوبة بوضع عناوين مضللة لها أو بخلطها مع العديد من الملفات التى لا علاقة لها بالموضوع فإذا اعتبرنا أن كل ملف صندوق مغلق بذاته لترتب على ذلك أن مأمور الضبط القضائى قد يحتاج إلى عدد لا نهائى من الأذون عند تفتيش جهاز الحاسوب من ناحية، ومن ناحية أخرى فإنه إذا عثر مأمور الضبط على جريمة عرضية أخرى مثل حيازة صور داعرة لأطفال فإن هذه الجريمة تكون متلبسًا بها، وبالتالى يحق لمأمور الضبط استكمال التفتيش للبحث عن أدلتها دون أن يكون قد تجاوز الغرض من الإذن الصادر له بداية.

- وضع الحاسوب المشترك:

قد يتشارك أكثر من شخص فى جهاز حاسوب واحد، فى حين يكون أحد أصحاب الحق فيه متهما دون الآخرين وصدر إذن بتفتيشه هو وحده أو تفتيش المكان الذى يوجد فيه، فهل يصح هذا التفتيش أم لا؟ تقضى القاعدة بأن تفتيش المكان المشترك جائز ما دام المتهم يشارك فيه كأن يكون منزلًا مشتركًا أو مكتبًا مشتركًا بشرط ألا يكون أحد هؤلاء الشركاء من أحد أصحاب الحصانات (كعضو مجلس الشعب أو أحد القضاة) إذا كان ابنه متهمًا ويقيم معه فى ذات المسكن[١٢٣]. ولذلك نرى جواز تفتيش الحاسوب الذى يشارك فيه المأذون بتفتيشه آخرين[١٢٤].

٤- تنفيذ الإذن بالتفتيش والضبط التقنى:

الغرض من التفتيش هو الوصول إلى ضبط البيانات والمعلومات التى تكون لها فائدة فى ظهور الحقيقة على ارتكاب جريمة من جرائم تقنية المعلومات وفق نص المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨.

ويختلف الضبط فى الجريمة التقنية عن الضبط فى غير ذلك من الجرائم من حيث الموضوع- كما سبق وأن بينا- ذلك أن الأول يرد على أِشياء ذات طبيعة معنوية البيانات والمعلومات، أما الثانى فيرد على أشياء ذات طبيعة مادية.

وضبط المعلومات التقنية يثير تساؤلات عديدة، منها ما تصدينا لها؛ من اعتبار جهاز الحاسوب بما يحتويه ملفًا واحدًا، وكذا مشروعية ضبط ملفات تقنية مخزنة على جهاز آخر إذا كانت تلك المعلومات يتم الدخول إليها من الحاسوب الأصلى محل الإذن بالتفتيش والضبط. إلا أننا نتساءل: إذا صدر إذن التفتيش لضبط ملفات معينة فهل قيام رجال الضبط القضائى بضبط ملفات أخرى- الجهاز بأكمله- يوصم بالبطلان؟ وذلك استنادًا إلى أن القائم بالتفتيش قد خالف الإذن الصادر له؟

نقول فى هذا الشأن أن ضبط المعلومات والبيانات الموجودة داخل جهاز الحاسوب تثير الكثير من الصعوبات مما قد يضطر رجل الضبط أن يقوم بتفتيش وضبط جهاز الحاسوب بالكامل وملحقاته، ومن ثم فنرى أن صدور الإذن لضبط ملفات معينة لا يحول من ضبط الجهاز بالكامل[١٢٥]، بل إن الإذن الصادر بتفتيش جهاز الحاسوب يمتد ليشمل أدوات ذلك الجهاز مثل الطباعة والأقراص الممغنطة[١٢٦].

ولا يؤثر فى صحة تنفيذ الإذن أن يتم تفتيش الحاسوب الخاص بالمتهم بحثًا عن الملفات المجرمة فى قسم الشرطة أو المعمل الجنائى، لا سيما وأن بعض

الأجهزة قد تكون محمية بكلمات مرور، الأمر الذى يقتضى ضبط الجهاز بالكامل للتغلب على هذه العقبة من الناحية الفنية[١٢٧].

وتظهر مشكلة أخرى وخاصة عند قيام رجال الضبط القضائى بالإفراط فى تنفيذ إذن الضبط، وذلك عن طريق عزل نظام بأكمله عن محيطه لفترة معينة، لا سيما إذا كان هذا النظام المعلوماتى متسعًا ومتشعبًا ويكون الحاسوب محل الضبط والتفتيش جزء من هذا النظام. كما لو قام مدير النظام بتخزين معلومات مسروقة ومسجلة فى مكان ما فى الشبكة. فإنه من الناحية الفنية فإن رجال الضبط القضائى يمكنهم الحصول على إذن بضبط الشبكة بالكامل، ذلك لأنها تحوى عناصر لا يمكن فصلها ويتعين ضبطها لأنها تتضمن عناصر مهمة للإثبات فى الجريمة. ولكن بشرط ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة (م ١/٦ بند١ من قانون مكافحة جرائم تقنية المعلومات)، وأن يكون هناك تناسب بين مصلحة الدولة فى كشف الحقيقة وبين مصلحة صاحب النظام فى تسيير أعماله[١٢٨]. فإذا لم يكن هناك تناسب، فلصاحب الشأن أن يستأنف قرارات الضبط والتحفظ (م ٦ فقرة أخيرة من القانون سالف الذكر) ولا يشترط أن يكون صاحب الشأن هنا هو المتهم نفسه، بل قد يكون صاحب النظام المتحفظ عليه. ويكون استئناف هذه القرارات أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة، وفق المواعيد المقررة بقانون الإجراءات الجنائية.

كما أن لمأمور الضبط القضائى أن يستعين بالمختصين لتنفيذ إذن التفتيش، فله مثلا أن يستعين بسكرتير المتهم لتفتيش بعض الملفات متى أبدى الأخير تعاونه مع مأمور الضبط وذلك للحصول على الملفات التى يقوم بالبحث عنها[١٢٩].

وإذا كان الأمر على هذا النحو وكان الإفراط فى تنفيذ الإذن يرتبط ارتباطًا وثيقًا بمدى تعاون المتهم والشاهد مع جهات التحقيق والضبط، فيثار التساؤل: هل

يلتزم المتهم والشاهد بكشف شفرة الدخول إلى المعلومات المجرمة؟ وتتم الإجابة عن هذا السؤال من خلال المبحث التالى.

٥- مدى جواز إجبار المتهم أو الشاهد على كشف شفرة الدخول إلى المعلومات المجرمة:

يتطلب التفتيش التقنى توافر إمكانية الوصول فى محتويات نظم المعالجة الآلية للبيانات، وقد يكون ذلك متعذرًا فى الحالات التى لا تتوافر فيها المعلومات والبيانات اللازمة للاتصال بالنظام والتعامل مع برامجه وملفات البيانات المخزنة داخله، كما هو الحال عند عدم الاهتداء إلى مفاتيح وأكواد الدخول وكلمات السر أو المرور، الأمر الذى يثير التساؤل عن مدى إمكانية الحصول عليها من المتهم نفسه أو من غيره إذا كان يعلمها؟ وللإجابة عن هذا التساؤل ينبغى أن نفرق بين المتهم وغيره.

أ- فيما يتعلق بالمتهم:

بداية نقول إن جميع النظم القانونية تعترف بحق المتهم فى الصمت، وإن المتهم له الحرية فى إبداء رفضه فى تقديم ما لديه من معلومات وإنه لا يثار أى جدل حول هذه الواقعة عند النظر فى إدانته(١٣٠).

وإذا كان ذلك هو المبدأ العام فإنه ينعكس بطبيعة الحال على القواعد الإجرائية الخاصة بالجريمة التقنية، حيث يكون المتهم غير مجبر على التعاون الفعال مع جهات التحقيق(١٣١).

وعلى ذلك فلا يجوز قانونًا إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية(١٣٢).

ففى المجر: لا يكون المتهم مكرهًا على إثبات براءته، كما أنه غير مجبر على الإدلاء بأى بيانات، بل وباستطاعته رفض الإجابة عن الأسئلة التى توجه إليه

أثناء التحقيق. وذلك يعنى بوضوح أن المتهم لا يكون مجبرًا على طبع سجلات الحاسب أو الإمداد بالأكواد أو كلمات السر[١٣٣] وذات الأمر فى بولندا[١٣٤] واليابان[١٣٥].

وفى الولايات المتحدة الأمريكية وطبقًا لما هو مقرر بمقتضى التعديل الخامس للدستور الأمريكى الذى يقضى بأنه لا يجوز إجبار أى شخص فى أى قضية جنائية على الشهادة ضد نفسه[١٣٦]؛ فقد انتهى الفقه الأمريكى إلى حق المتهم فى عدم الشهادة ضد نفسه.

ومع ذلك ظهرت بعض الآراء الفقهية واعتبرت أن إدلاء المتهم بالشفرات السرية لا تشملها الحماية المقررة بموجب التعديل الخامس للدستور الأمريكى، واستندوا إلى أن هذا التعديل لا يحول دون مطالبة المشتبه فيه من تمكين السلطات المختصة من التوصل إلى المعلومات التى تستلزمها مصلحة التحقيق، لأن هذا التعديل إنما يحمى الفرد فحسب ضد إجباره على الشهادة الكلامية، أى تلك التى تعتمد على مفردات اللغة والعبارات، وبالتالى فهو لا يَمنع مطالبة المشتبه فيه أن يتعاون فى تقديم دليل ليس له صيغة كلامية كما هو الحال فى مطالبته بتقديم عينة من دمه، إذ إن الأخيرة من الأدلة العلمية المادية. وقياسًا على ذلك يمكن مطالبة المشتبه فيه بأن يسلم قسرًا مفتاح الخزانة أو مفتاح فك الشفرة بالنسبة للمعلومات المخزنة فى نظام الحاسب[١٣٧].

ودلل أنصار هذا الرأى على صحته بما قضت به المحكمة العليا من تأييد أمر قضائى وجه إلى شخص يجرى التحقيق معه بأن يأذن لبنوك أجنبية بالكشف عن سجلاتها المتعلقة بحسابات لديها[١٣٨]. وقد انتُقِد هذا الرأى ذلك أنه قد يسبب إشكالًا قانونيًا يتعذر حله، لأن الشفرة التى تتيح الوصول إلى المعلومات يجب أن يتم نقلها أو الإعلام بها من خلال صيغ الكلام وهو ما لا يجوز إجبار المتهم عليه[١٣٩].

فى مصر: الأصل الإثباتى القائم على افتراض براءة المتهم من الاتهام الموجه إليه يقتضى الإعفاء من الإسهام بصورة مباشرة فى إثبات إدانته أو تأكيد إذنابه. فلا يجوز بالتالى إجباره على الإجابة عن أسئلة تؤدى إلى تجريم نفسه[١٤٠] أو الإدلاء بمعلومات يمكن أن ترتد عليه سوءً[١٤١]، ومعنى ذلك أن المتهم له الحق فى الامتناع عن الإجابة والاعتصام بالصمت[١٤٢]، دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام وتسليم بإدانته[١٤٣] لأن الأصل فى الإنسان البراءة[١٤٤] وعليه لا يكون جائزًا قانونًا إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعلومات أو إلزامه بالإفصاح والكشف عن مفاتيح وأكواد الدخول وكلمات المرور[١٤٥].

ب- فيما يتعلق بغير المتهم (الشاهد التقنى):

عرف الفقه[١٤٦] والقضاء[١٤٧] الشهادة بأنها تقرير شخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه.

ويختلف الخبير عن الشاهد فى أن الأخير يقدم إلى القاضى معلومات حصلها بالملاحظة الحسية، أما الخبير فيقدم إلى القاضى تقارير وآراء توصل إليها بتطبيق قوانين علمية أو أصول فنية[١٤٨].

وقد يجمع الشخص بين صفتى الشاهد والخبير كطبيب حاول إسعاف المجنى عليه قبل وفاته فأتيح له بذلك معرفة أسباب الوفاة[١٤٩].

ويقصد بالشاهد التقنى: الفنى صاحب الخبرة والتخصص فى تقنية الحاسب وعلومه، والذى يكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضى التنقيب عن أدلة الجريمة داخله[١٥٠].

والشاهد التقنى: بهذا المفهوم يشمل عدة طوائف من أهمها مشغلو الحاسب وخبراء البرمجة والمحللون ومهندسو الصيانة والاتصالات[١٥١].

وإذا كانت القاعدة العامة تقضى بأن الشاهد يلتزم بالإفضاء بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها والإدلاء بكل ما يفيد فى كشف الحقيقة من وقائع أخرى، أما الشاهد التقنى– وفق رأى من الفقه– فبالإضافة إلى ذلك فإنه يجب أن يلتزم بتقديم المعلومات الجوهرية اللازمة لاختراق نظام المعالجة الآلية للبيانات بحثًا عن أدلة للجريمة داخل ذلك النظام وتتطلبها مصلحة التحقيق، حيث يكون مطالبًا بأن يُعلم بها سلطات التحقيق والتحرى على سبيل الإلزام وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة(١٥٢). وتظهر أهمية ذلك فى أن سلطات التحقيق والتحرى مهما بلغت خبرتها الفنية فى المجال التقنى سيستحيل عليها– بدون معرفة كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة– الولوج إلى الأوعية التقنية محل الواقعة التى تكون فى حوزة هؤلاء الشهود. مع ما فى ذلك من أخطار وأضرار تهدد ليس فقط نظام العدالة الجنائية ولكن أيضًا شبكة الاتصالات ذاتها، خاصة إذا كانت البيانات المطلوبة مخزنة فى وحدة معالجة مركزية فى حاسب ضمن شبكة معلومات ممتدة.

ويثار التساؤل: هل يلتزم الشاهد فى الجرائم التقنية بأن يتعاون مع سلطة التحقيق، كأن يقوم مثلًا بعمليات معينة على جهاز الحاسوب إذا كان من المتخصصين فى هذا المجال كى يساعد العدالة، خاصة وأن الخبير الفنى المنتدب من الجهة القضائية قد لا يمكنه معرفة الأساليب الفنية التى يمكن اتباعها للكشف عن الأدلة التى من الممكن أن تفيد فى كشف الحقيقة والتى لا يعلمها إلا هذا الشاهد مثل كلمة المرور والبرامج المستخدمة لتشغيل النظم التى استعان بها المتهم فى ارتكاب جريمته التقنية.

اختلف الفقه المقارن فى الإجابة عن هذا السؤال بين مؤيد ومعارض لفكرة قيام الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات وذلك إلى اتجاهين[١٥٣]:

- الاتجاه الأول:

يذهب أنصار هذا الاتجاه إلى أنه ليس من واجب الشاهد- وفقًا لالتزامات الشهادة التقليدية- أن يقوم بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة. ووجد هذا الاتجاه صداه فى عدة دول:

ففى ألمانيا: يرى غالبية الفقه أن الشاهد لا يلتزم بطبع البيانات المخزنة داخل ذاكرة الحاسب تأسيسًا على عدم انطواء الالتزام بأداء الشهادة على هذا الواجب[١٥٤].

وفى تركيا: لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[١٥٥].

وفى لوكسمبرج: وإن كان يوجد الالتزام بأداء الشهادة فالشهود يجب أن يحلفوا اليمين بقول الحقيقة وإلا ارتكبوا جريمة الشهادة الزور. لكن ليس من المؤكد أن يكون الشاهد مجبرًا على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه فى ذاكرة الحاسب. وإن كان يستطيع الوصول إليها نظرًا لمعرفته كلمات المرور السرية، إذا تعاون الشاهد على هذا النحو فإن دوره يكون أُقرب إلى الخبرة منه إلى الشهادة[١٥٦].

وفى تشيلى: يرى الفقه أنه فى ظل غياب النصوص التشريعية الصريحة فإنه ليس من الملائم الحديث عن وجود التزام قانونى لبعض الأفراد على طبع سجلات الحاسب أو الكشف عن كلمات المرور السرية[١٥٧].

- الاتجاه الثانى:

يرى أنصار هذا الاتجاه أن من واجب الشاهد التعاون مع جهات التحقيق المختلفة. وبهذا يكون الشاهد ملتزمًا بأن يساعد الجهة القضائية بأن يقدم الدليل أو يسهل الدخول إلى المواقع التى تفيد فى كشف الحقيقة(١٥٨).

ففى القانون الإنجليزى الصادر فى ١٩٨٤ فى شأن الأدلة الجنائية يوجب على الشاهد أن يقدم إلى العدالة ما يعرفه من معلومات يتضمنها جهاز الحاسوب(١٥٩).

وفى هولندا توجب المادة ١٢٥ من قانون الإجراءات الجنائية الهولندى على الشاهد الالتزام بالتعاون مع جهات التحقيق، حيث يمكن توجيه الأمر إلى القائم على تشغيل النظام التقنى للإفصاح عن المعلومات والبيانات اللازمة للدخول عليه والتعامل مع برامجه وملفات بياناته كمفاتيح تشغيل النظام وأكواد الدخول وكلمات السر أو المرور. وإذا كانت المعلومات تقتضى مصلحة التحقيق الحصول عليها فى صورة رموز داخل ذاكرة الحاسوب يمكن تكليفه كذلك بتقديم الأكواد والمفاتيح اللازمة لفك الشفرة.

وتجيز المادة سالفة الذكر لقاضى التحقيق أن يأمر أى شخص، يفترض فيه أنه على علم بكيفية الدخول إلى المعلومات المخزنة فى الحاسبات الآلية، للمساهمة مع سلطات التحقيق فى كشف الحقيقة، طالما أن هذه المعلومات تم تخزينها أو معالجتها أو نقلها عن طريق نظام المعالجة الآلية للبيانات أو يُمكن قاضى التحقيق من الدخول إلى هذه المعلومات. والأمر هنا يقتصر على المعلومات التى استخدمت فى ارتكاب الجريمة فحسب(١٦٠).

وفى بولندا: وفقًا لنص المادة ١٦٦ من قانون الإجراءات الجنائية البولندى على الشاهد أن يجيب على كل الأسئلة التى توجه إليه، ومنها الكشف عن الشفرات

السرية للبرامج. بل وعليه أن يقوم بطبع سجلات الحاسوب– إلا إذا كان من شأن ذلك أن يعرضه للمسئولية الجنائية[١٦١].

وفى فرنسا: يرى بعض الفقه أنه فى ظل غياب التنظيم التشريعى لهذه المسألة فإنه لا مناص من تطبيق القواعد العامة فى الشهادة. وعلى ذلك فإن الشهود الذين يقع على عاتقهم الالتزام بأداء الشهادة فى المواد– ١٠٩، ٤٣٨ من قانون الإجراءات الجنائية الفرنسى– يكونون مكلفين بالكشف عن كلمات المرور السرية التى يعرفونها وشفرات تشغيل البرامج باستثناء حالات المحافظة على سر المهنة، فإنهم يكونون فى حل عن الالتزام بأداء الشهادة[١٦٢].

وفى اليونان: يمكن الحصول من القائم على تشغيل الحاسب على كلمة السر للولوج إلى نظام المعلومات، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمنى، لكن ليس على الشاهد أية التزامات بالنسبة لطباعة ملفات بيانات مخزنة فى ذاكرة الحاسب. وذلك لأن شهادته تنصب على معلومات لديه بالفعل وليس الكشف عن معلومات جديدة وذلك وفق المواد ٢٢٣ وما بعدها من قانون الإجراءات الجنائية اليونانى[١٦٣].

وفى المجر: يرى الفقه أن الشاهد يقع على عاتقه التزام بالإدلاء بما لديه من معلومات لازمة لولوج نظام الحاسب سواء تعلق ذلك بالكشف عن كلمات المرور السرية أو الإفصاح عن الشفرات الخاصة بالبرامج، بل عليه واجب التعاون فى طباعة سجلات الحاسب. وإن كان جائزًا له رفض الإجابة والإدلاء بشهادته إذا كانت ستؤدى إلى اتهامه أو اتهام أحد أقربائه. وفى حالة امتناعه عن أداء الشهادة فى غير الأحوال التى يخولها القانون فيها ذلك يُعد مرتكبًا لجريمة الشهادة الزور، والتى يمكن أن تتحقق بسلوك تعبيرى سلبى قوامه الصمت والسكوت عمدًا عن قول الحقيقة[١٦٤].

وبشأن الوضع فى مصر: فقد خول قانون الإجراءات الجنائية المصرى لمأمور الضبط القضائى سماع أقوال من تكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها- المادة ٢٩ من قانون الإجراءات الجنائية- وأن يسمع فى حالة التلبس بالجريمة أقوال الأشخاص الحاضرين فى محل الواقعة ومن يمكن الحصول منه على إيضاحات فى شأن الجريمة- المادة ٣١ من القانون ذاته- وأن يطلب من الحاضرين عدم مبارحة محل الواقعة أو الابتعاد عنها، وأن يطلب فى الحال من يمكن الحصول منهم على إيضاحات فى شأن الواقعة- المادة ٣٢ من ذات قانون- ويلتزم الشاهد بالحضور بنفسه فى المكان والزمان المحددين للاستماع إلى شهادته وأن يؤدى الشهادة بعد حلف اليمين وأن يقول الحقيقة.

وإذا كان الأمر كذلك فإنه فى ظل غياب نصوص صريحة فقد استقر الفقه على أن المشرع المصرى يلزم الشاهد بتقديم ما يعرفه عن الجريمة وليس القيام بعمل معين[١٦٥]. حيث نصت المادة ٢٨٤ من قانون الإجراءات الجنائية على أنه (إذا امتنع الشاهد عن أداء اليمين أو عن الإجابة فى غير الأحوال التى يجيز له القانون فيها ذلك، حُكم عليه) وعلى ذلك، فإن الالتزامات التى فرضها التشريع الإجرائى على الشاهد لا تتضمن أو تفيد التزام الشاهد بالمعاونة الفعالة فى التحقيق الجنائى الذى يجرى بشأن الجريمة التى يدلى فيها بشهادته. فما يفرضه القانون على الشاهد، بعد الحضور وحلف اليمين القانونية هو ذكر الحقيقة فى إجابته عن الأسئلة المنصبة حول مدركاته للوقائع المتعلقة بثبوت وقوع الجريمة وظروفها ونسبتها إلى المتهم أو براءته منها، ومؤدى ذلك أنه لا مجال لأن يلزم بالقيام بعمل معين أو الإدلاء بما لديه من معلومات لازمة لولوج نظام المعالجة الآلية للبيانات تنقيبًا عن أدلة الجريمة داخله. ولا مجال من باب أولى لتحميل غير الملتزمين بالشهادة قانونًا بواجب الإدلاء

بمثل هذه المعلومات[١٦٦]. ومن ثم يجب أن يتدخل المشرع لإدخال وسيلة قانونية جديدة تتحقق ما لم تستطع فكرة الالتزام بأداء الشهادة أن تؤديه.

كما يجب أن يكون هناك بعض من الوسائل التى تجبر الشهود على التعاون الإيجابى مع سلطات التحقيق. كما هو الشأن فى بعض الدول حيث يسأل الشاهد الذى يخفى الشفرة أو كلمة السر أو يعطى أوامر خاطئة عن جريمة شهادة الزور لأنه يعوق سير العدالة، أو يسأل باعتباره شريكًا فى الجريمة موضوع المحاكمة[١٦٧]. وكذلك التهديد بضبط النظام المعلوماتى بالكامل فهذه الإجراءات الخطيرة قد تدفع الشاهد إلى التعاون الفعال والإيجابى مع سلطات التحقيق والحكم[١٦٨]. لذلك نرى إضافة المادة ٦ مكررًا من القانون رقم ١٧٥ لسنة ٢٠١٨ يكون نصها (ويعد مرتكبا لجريمة الشهادة الزور كل شاهد يرفض الكشف عن كلمات المرور السرية وشفرات تشغيل البرامج التى يعرفها).

الخاتمة

تتعرض هذه الدراسة لجانب مهم من الجوانب الإجرائية الحديثة التى تتعلق بالبحث والتنقيب عن الدليل فى جرائم تقنية المعلومات؛ ألا وهو تفتيش أجهزة الحاسوب. وهو الأمر الذى تصدى له المشرع المصرى وفق نص المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات.

وعرضنا فى البداية لتفتيش الحاسب الآلى والأنظمة المتصل به. وقسمناه إلى نقطتين: الأولى ناقشنا فيها تفتيش الحاسب الآلى والأنظمة المتصل بها فى الداخل، والثانية: تكلمنا فيه عن تفتيش الحاسب الآلى والأجهزة المتصلة به فى الخارج. وأوضحنا موقف التشريع المصرى من تفتيش أنظمة الحاسب الآلى وذلك وفق نص المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ سالف البيان، وأن التشريع المصرى لم يحسم الخلاف حول امتداد إذن التفتيش للنظام التقنى المتصل بالنظام

محل الإذن. فضلًا عن ذلك فإن الواقع العملى كشف عن عدم فهم بعض من رجال الضبط القضائى وسلطة التحقيق– للمقصود بعبارة (تتبع البيانات) الواردة بالبند (١) من الفقرة الأولى من المادة السادسة من القانون سالف الذكر.

أما الجزء الثانى خصصناه للتفتيش التقنى بناء على إذن من سلطة التحقيق المختصة. وطرحنا عدة تساؤلات أجبنا عنها فى خمس عناصر، الأول والثانى بينا فيهما الشروط الشكلية والموضوعية لإذن التفتيش التقنى. والثالث أوضحنا كيفية تعيين محل التفتيش التقنى. وانتقلنا فى الرابع إلى تنفيذ الإذن بالتفتيش والضبط التقنى. وسلطنا الضوء فى المبحث الأخير عن مدى جواز إجبار المتهم أو الشاهد على كشف شفرة الدخول إلى المعلومات المجرمة.

نرى أنه يجب تعديل المادة السادسة من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات بحيث يسمح لمأمور الضبط القضائى المأذون له بتتبع البيانات والمعلومات فى أى مكان أو نظام أو حاسب تكون موجودة فيه، بحيث يكون نصها (لجهة التحقيق المختصة بحسب الأحوال... ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه أو فى نظام معلوماتى آخر ما دامت هذه البيانات متصلة فى شبكة واحدة مع النظام الرئيسى أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسى).

كما يجب إضافة مادة تجبر الشاهد التقنى على كشف كلمات المرور السرية وشفرات تشغيل البرامج بحيث يكون هناك تعاون مع سلطات التحقيق المختصة، لذلك نرى إضافة المادة ٦ مكررًا من القانون رقم ١٧٥ لسنة ٢٠١٨ يكون نصها (ويعد مرتكبًا لجريمة الشهادة الزور كل شاهد يرفض الكشف عن كلمات المرور السرية وشفرات تشغيل البرامج التى يعرفها).

الهوامش

١- هشام فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائى والفنى واقتراح إنشاء آلية عربية موحدة للتدريب التخصصى- بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعه الإمارات، ٢٠٠٤، ص ٤٠١.

٢- كلمة معلوماتية هى اختصار مزجى لكلمتى معلومة وكلمة آلية، وهى تعنى المعالجة الآلية للمعلومة. د. أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلى، دراسة مقارنة، دار النهضة العربية، ٢٠٠٠، ص٢٢.

٣- غازى عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية الحاسب والإنترنت) رسالة دكتوراه كلية الحقوق الجامعة الإسلامية لبنان، ٢٠٠٤، ص ٩٢؛ عبد الفتاح بيومى حجازى، التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول، دار الفكر الجامعى، الإسكندرية، ٢٠٠٤، ص ٩ وما بعدها.

٤- عائشة بن قارة مصطفى، حجية الدليل الإلكترونى فى مجال الإثبات الجنائى فى القانون الجزائرى والقانون المقارن، دار الجامعه الجديدة، الإسكندرية، ٢٠١٠، ص١٣.

5- Kurbalija Jovan, Gelbstein Eduardo, Gouvernance de L'internet– enjeux, acteurs et fractures, publié par diplofoundation et global knowledge partnership, Suisse, 2005, p98; Mohamed Buzunar: la Criminalité informatique sur L'internet, Journal of law, (Kwait University), Nô.1, Vol.26, March 2002, P. 21 et š.

- عبد الله العلوى البلغيثى، "الإجرام المعاصر- أسبابه وأساليب مواجهته"، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول (السياسة الجنائية بالمغرب: واقع وآفاق)، التى نظمتها وزارة العدل بمكناس خلال الفترة من ٩-١١ ديسمبر ٢٠٠٤، المجلد الأول، (الأعمال التحضيرية)، الطبعة الثانية، منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية، العدد (٣)، ٢٠٠٤، ص٢٢٢؛ دياب البداينة: المنظور الاقتصادى والتقنى والجريمة المنظمة، ضمن أبحاث حلقة علمية حول الجريمة المنظمة وأساليب مكافحتها، التى نظمتها أكاديمية نايف العربية للعلوم الأمنية، ١٤-١٨ نوفمبر ١٩٩٨، مركز الدراسات والبحوث- الرياض، ١٩٩٩، ص٢٠٩ وما بعدها؛ حسنين المحمودى بوادى: إرهاب الإنترنت- الخطر القادم، الطبعة الأولى، دار الفكر العربى- الإسكندرية، ٢٠٠٦، ص٤٩ وما بعدها؛ محمد أمين

الرومى، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية– الإسكندرية، ٢٠٠٤، ص٧؛ د. موسى مسعود ارحومة، الإرهاب والإنترنت، بحث مقدم إلى المؤتمر الدولى لجامعة الحسين بن طلال بعنوان: الإرهاب فى العصر الرقمى، المنعقد بمدينة معان– الأردن، خلال الفترة ١٠– ٢٠٠٨/٧/١٣، ص١.

٦– مثال ذلك، ما قام به المتهم من قتل المجنى عليها– زوجته– التى كانت تتلقى العلاج بالمستشفى، بأن دخل عن طريق شبكة المعلومات الخاصة بالمستشفى وغيَّر المعلومات الخاصة بالمجنى عليها مما أدى إلى وفاتها.

Demarco (Estelle) le droit pénal applicable sur internet, Memory, Montpellier 1,1998, p.27.

٧– المواد ١٢ وما بعدها من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات.

٨– جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى، دار النهضة العربية، ٢٠٠٢، ص٤١.

٩– فى إحدى القضايا دخل الجانى على أحد المواقع الإلكترونية للعثور على أحد معتادى الإجرام للاتفاق معه على قتل امرأة ما، وبالفعل تم الاتفاق على أن يتم ذلك الفعل لقاء مبلغ مالى ٤٠٠ دولار كدفعة مقدمة، وأرسل الجانى صورة المجنى عليها لذلك الشخص عن طريق ذات الموقع، وبعد الاتفاق فيما بين الجانى وذلك الشخص تقابلا لدفع المبلغ المتفق عليه. وتم ضبط الجانى لأن ذلك الشخص كان أحد رجال الشرطة:

Chuck Easttom and Det. Jeff Taylo: Computer Crime, Investigation, and the Law , Course Technology PTR A part of Cengage Learning , Library of Congress 2011, p. 25.

١٠– عبد الرءوف مهدى، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية ٢٠٠٧، ص ١٧.

11– http://www.cc.gov.eg/Images/L/386006.pdf ٢٠١٩/١/١٣ تاريخ الدخول.

١٢– عبد الرءوف مهدى، شرح القواعد العامة للإجراءات الجنائية، المرجع السابق ص ٤٨٩؛ عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٤، ص ٩٦١.

١٣- عوض محمد عوض، المبادئ العامة فى قانون الإجراءات الجنائية، منشأة المعارف الإسكندرية بدون سنة نشر، ص ٣٩٧.

١٤- أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة ٢٠١٢، ص ٧٥٣ وما بعدها، د. حسن شلبى يوسف، الضمانات الدستورية للحرية الشخصية فى التفتيش، رسالة دكتوراه، جامعة القاهرة، ١٩٩٢.

١٥- هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص ٦٢؛ حسين بن سعيد الغافرى، التحقيق وجمع الأدلة فى الجرائم المتعلقة بشبكة الإنترنت، بحث مقدم إلى المؤتمر الإقليمى الأول عن الجريمة الإلكترونية، القاهرة ٢٦-٢٧ نوفمبر ٢٠٠٧، ص ١٢٣. ومنشور على موقع الويب: http://previous.eastlaws.com/Uploads/Morafaat/33.pdf تاريخ الدخول ٢٠١٩/١/٢١.

وقد فضل البعض أن الإصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة المرتكبة فى العالم الافتراضى هو الولوج، باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش بمعناه الضيق فيعنى البحث والقراءة والتفحص وهو مصطلح تقليدى أكثر، وهناك من استخدم المصطلحين معا كما ورد فى المادة ١٩ من اتفاقية بودابست؛ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، دار الفكر الجامعى، الإسكندرية ٢٠٠٧، ص ٢٢٣ وما بعدها.

١٦- نشر القانون فى الجريدة الرسمية، العدد ٣٢ مكرر (ج) فى الرابع عشر من شهر أغسطس عام ٢٠١٨.

تاريخ الدخول ٢٠١٩/١/٢١ http://www.cc.gov.eg/Images/L/386006.pdf

١٧- انظر فى هذا الشأن مصطفى على خلف، الضوابط الإجرائية لجرائم التقنية الحديثة، نادى القضاة ٢٠١٧، ص ٥٧ وما بعدها.

18- Article 19 – Search and seizure of stored computer data
Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a computer system or part of it and computer data stored therein; and
a computer-data storage medium in which computer data may be stored in its territory.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 تاريخ الدخول ٢٠١٩/١/١٣

شيماء عبد الغنى، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة ٢٠٠٧ ص٣٠٠.

١٩- عمر محمد أبو بكر بن يونس، الاتفاقية الأوروبية حول جرائم الجريمة الافتراضية (المذكرة التفسيرية) مكتبة الكتب العربية، ٢٠٠٥، ص ١٥٤ وما بعدها.

20- http://www.cc.gov.eg/Images/L/324594.pdf تاريخ الدخول ٢٠١٩/١/١٣

21- Article 57-1 Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars, 2003:
Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.»
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199 تاريخ الدخول ٢٠١٩/١/١٣

شيماء عبد الغنى، المرجع السابق، ص ٢٩٩؛ أ. عائشة بنت قارة، المرجع السابق، ص ٩٣.

22- Artikel 125j
In geval van een doorzoeking kan vanaf de plaats waar de doorzoeking plaatsvindt, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar in dat werk opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen, dan kunnen zij worden vastgelegd.
http://www.wetboekonline.nl/wet/Wetboek%20van%20Strafvordering/125j.html تاريخ الدخول ٢٠١٩/١/٢٠

Kaspersen (W.K. Henrik) : Computer crimes and other crimes against information technology in the Netherlands R.I.D.P 1993, P. 479.

هشام زكى رستم، المرجع السابق، ص ٧١؛ أ. نبيلة هروال، المرجع السابق، ص ٢٣٩؛ طارق إبراهيم الدسوقى عطية، الأمن المعلوماتى (النظام القانونى لحماية المعلومات)، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٩، ص ٣٨٧؛ د. شيماء عبد الغنى، المرجع السابق، ص ٣٠١.

23- Mohrenschlager (Manfred) : Op.cit., P. 351.

24- 103: Durchsuchung bei anderen Personen

Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Zum Zwecke der Ergreifung eines Beschuldigten, der dringend verdächtig ist, eine Straftat nach § 89a oder § 89c Absatz 1 bis 4 des Strafgesetzbuchs oder nach § 129a, auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuches oder eine der in dieser Vorschrift bezeichneten Straftaten begangen zu haben, ist eine Durchsuchung von Wohnungen und anderen Räumen auch zulässig, wenn diese sich in einem Gebäude befinden, von dem auf Grund von Tatsachen anzunehmen ist, daß sich der Beschuldigte in ihm aufhält.
Die Beschränkungen des Absatzes 1 Satz 1 gelten nicht für Räume, in denen der Beschuldigte ergriffen worden ist oder die er während der Verfolgung betreten hat.
http://www.gesetzeiminternet.de/stpo/BJNR006290950.html#BJNR006290950BJNG000902301 تاريخ الدخول ٢٠١٩/١/٢٠

25- A person authorized under this section to search a computer system in a building or place for data may: (a) use or cause to be used any computer= system at the building or place to search any data contained in or available to the computer system;
http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-46/latest/rsc-1985-c-c-46.html تاريخ الدخول ٢٠١٩/١/٢٠

شيماء عبد الغنى، المرجع السابق، ص ٢٩٩؛ أ. عائشة بنت قارة، المرجع السابق، ص ٩٣.

26- Competition Act (R.S.C., 1985, c. C-34)
16. (1) A person who is authorized pursuant to subsection 15(1) to search premises for a record may use or cause to be used any computer system on the premises to search any data contained in or available to the computer system, may reproduce the record or cause it to be reproduced from the data in the form of a printout or other intelligible output and may seize the printout or other output for examination or copying.
http://laws-lois.justice.gc.ca/eng/acts/C-34/page-8.html#docCont تاريخ الدخول ٢٠١٩/١/٢٠

27- Art. 88ter.
1. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre

lieu que celui où la recherche est effectuée:
si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et
si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi تاريخ الدخول ٢٠١٩/١/٢٠

محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، ص ٣٤ وما بعدها.

٢٨- حسين بن سعيد الغافرى، التحقيق وجمع الأدلة فى الجرائم المتعلقة بشبكة الإنترنت، المرجع السابق على موقع الويب، ص ١٣.

http://previous.eastlaws.com/Uploads/Morafaat/33.pdf تاريخ الدخول ٢٠١٩/١/٢٠.

29- Pascal Vergucht : La répression de délit informatique dans une perspective internationale, thèse, Montpellier 1996, p.368.

شيماء عبد الغنى، المرجع السابق، ص ٢٩٨، عائشة بنت قارة، المرجع السابق، ص ٩٣.

30- agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations.

31- Article 41.b (1) a magistrate judge with authority in the district or if none is reasonably available, a judge of a state court of record in the district has authority to issue a warrant to search for and seize a person or property located within the district;

https://www.law.cornell.edu/rules/frcrmp/rule_41 تاريخ الدخول ٢٠١٩/١/٢١.

32- United States V. New York Telephone co, 434 U.S. 159 (1977)

https://casetext.com/case/united-states-v-new-york-telephone-co تاريخ الدخول ٢٠١٩/١/٢١

https://supreme.justia.com/cases/federal/us/434/159/ تاريخ الدخول ٢٠١٩/١/٢١

٣٣- عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكى، ٢٠٠٥ بدون ناشر، ص ٢٠٣ وما بعدها.

٣٤- شيماء عبد الغنى، المرجع السابق، ص ٣٠١؛ أ. عائشة بنت قارة، المرجع السابق، ص ٩٥.

٣٥- أحمد سعد محمد الحسينى، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس ٢٠١٢، ص ١٩٤ وما بعدها.

٣٦- المرجع السابق، ص ١٩٥.

٣٧- بكرى يوسف بكرى، التفتيش عن المعلومات فى وسائل التقنية الحديثة، دار الفكر الجامعى، الإسكندرية ٢٠١١، ص ٧٠؛ محمد سالم الزعابى، الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية، دراسة مقارنه، الإمارات، ٢٠١٤ بدون ناشر، ص ١٢٢.

٣٨- عائشة بنت قارة مصطفى، المرجع السابق، ص ٩٥ ومشار إلى حكم النقض جلسة ١٩٨٣/٦/١٣، س ٥٣، ص ٣٤، رقم ٥٦٤.

٣٩- هشام فريد رستم، المرجع السابق، ص ٧٠؛ عائشة بنت قارة، المرجع السابق، ص ٩٥.

٤٠- عائشة بنت قارة، المرجع السابق، ص ٩٥.

٤١- شيماء عبد الغنى، المرجع السابق، ص ٣٠١.

٤٢- المرجع السابق، ص ٣٠٠.

٤٣- انظر ص ٢٥ من هذا البحث.

٤٤- القضية رقم ١٥٠٠١، لسنة ٢٠١٤، جنح بولاق الدكرور؛ وفى ذات الأمر القضية رقم ١٢٢٩٩، لسنة ٢٠١٤، جنح مركز الجيزة.

٤٥- القضية رقم ٣١٣٧٩، لسنة ٢٠١٤ جنح الهرم.

46- Sieber (Ulrich): Computer crimes and other crimes against information technology in Wurzburg. R.I.D.P. 1993, P. 77.

٤٧- هشام فريد رستم، المرجع السابق، ص ٧١.

Cybercrime Convention Committee (T-CY), Report of the Transborder Group adopted by the T-CY on 6 December 2012, T-CY (2012)3 Strasbourg, 6 December 2012 (provisional).

https://rm.coe.int/16802e79e8 تاريخ الدخول ٢٠١٩/١/٢٠

48- Article 3. During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by

means of a network and to seize the data therein, provided that immediate action is required.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 تاريخ الدخول ٢٠١٩/١/٢١

49- Article 17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 تاريخ الدخول ٢٠١٩/١/٢١

50- Article 18. Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 تاريخ الدخول ٢٠١٩/١/٢١

شيماء عبد الغنى، المرجع السابق ص ٣٠٣.

51- Article 32. Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080f0b تاريخ الدخول ٢٠١٩/١/٢١

٥٢- أحمد سعد الحسينى، المرجع السابق، ص ١٩٦.

٥٣- عائشة بنت قارة مصطفى، المرجع السابق، ص ٩٨؛ شيماء عبد الغنى، المرجع السابق، ص٣٠٤.

54- Recommendation No. R (89) 9 on crime related to the computer and the final report of the European Committee on Crime Problems / Council of Europe. http://www.oas.org/juridico/english/89-9&final%20Report.pdf تاريخ الدخول ٢٠١٩/١٠/١٠

عائشة بنت قارة مصطفى، المرجع السابق، ص ٩٨ وما بعدها.

٥٥- شيماء عبد الغنى، المرجع السابق، ص ٣٠٤.

٥٦- المرجع السابق، ص ٣٠١ وما بعدها.

57- Article 57-1 Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003
S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.».
http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=295C707D9A1EC414926950B1BAED3EBE.tpdila15v_1?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575037&dateTexte=20151106&categorieLien=id#LEGIARTI000006575037 تاريخ الدخول ٢٠١٩/١٠/١٠

58- Kertesz (Imre) and Pusztai (Iaszlo) : Computer crimes and other crimes against information technology in the Hungary R.I.D.P 1993. P. 387
هلالى عبد اللاه، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى دراسة مقارنة، دار النهضة العربية، ٢٠٠٨، ص ٧٩.

59- Mohrenschlager (Manfred): op. cit., p. 351.

٦٠- هشام فريد رستم، المرجع السابق، ص ٧٢.

61- Mohrenschlager (Manfred): op. cit., p. 356.

٦٢- عمر بن يونس، الإجراءات الجنائية عبر الإنترنت، المرجع السابق، ص ٢٠٢ وما بعدها.

٦٣- حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الإنترنت، رسالة دكتوراه جامعة عين شمس ٢٠٠٨، ص ٣٧٨ وما بعدها؛ أحمد سعد الحسينى، المرجع السابق، ص ١٩٦ وما بعدها.

٦٤- نقض ١٩٣٧/١١/٢٢، مجموعة القواعد القانونية، ج٤، ص ٩٨، رقم ١١٢.

٦٥- نقض ١٩٤٤/١/١٧، مجموعة القواعد القانونية، ج٦، ص ٣٨٦، رقم ٢٨٨.

٦٦- نقض ١٩٦٠/١٠/٣١، مجموعة أحكام النقض، س ١١، ص ٧٣٠، رقم ١٣٩.

٦٧- نقض ١٩٧٠/١٠/١٢، مجموعة أحكام النقض، س ٢١، ص ٩٧٢، رقم ٢٣١.

٦٨- عبد الرءوف مهدى، المرجع السابق، ص ٤٩١ وما بعدها؛ رءوف عبيد، المرجع السابق، ص ٣٩٢.

69- Durham (Cole): op. cit., p. 111.

٧٠- عمر بن يونس، رسالة دكتوراه، المرجع السابق، ص ٨٦٢.

٧١- مشار إليه لدى سامى الحسينى، النظرية العامة للتفتيش فى القانون المصرى والمقارن، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس ١٩٧٢، ص ١٣٣ هامش (١٠٧)؛ هشام فريد رستم، المرجع السابق، ص ٧٥ هامش (٢).

72- Rostoker, Michael D. and Rines, Robert H. : Computer jurisprudence . legal Responses to the information Revolution , Oceana Publication , INC., 1986 p.249

٧٣- هشام فريد رستم، المرجع السابق، ص ٧٧.

74- Waterplas, J. R. : Informatique et délinquance : un nouveau défi pour les magistrats et les policies, Rev. D.P.C., Août – Septembre 1985, P. 743.

٧٥- شيماء عبد الغنى، مرجع سابق، ص ٢٨٢.

76- UNITED STATES V. MUSSON, (D.COLO. 1986), 650 F. Supp. 525 (D. Colo. 198 https://casetext.com/case/united-states-v-musson تاريخ الدخول ٢٠١٩/١٠/١٠

٧٧- عبد الرءوف مهدى، المرجع السابق، ص ٤٩٣.

٧٨- نقض ١٩٨٠/٢/٢٤، مجموعة أحكام النقض، س ٣١، ص ٢٧١، رقم ٥٣.

٧٩- عبد الرءوف مهدى، المرجع السابق، ص ٥٠٠.

٨٠- عوض محمد عوض، المرجع السابق، ص ٣٧٩.

٨١- عبد الرءوف مهدى، المرجع السابق، ص ٥٠٠.

٨٢- نقض ١٩٦٢/١/١، مجموعة أحكام النقض، س ١٣، ص ٢٠، رقم ٥.

٨٣- محمد مصطفى القللى، أصول تحقيق الجنايات ١٩٤٢، ص ٣٨٦.

84- Gorphe (f): L'appréciation des preuves en justice, essai d'une méthode technique. Sirey 1947.p.247; Merle et Vitu : Traité de droit criminal éd. Cujas. Tome 2 Procédure Pénale 4é éd. 1989 no. 784.p.757; Carey (John): Les critères minimaux de la justice criminelle aux Etats- Unis. 1966, P. 77.

٨٥- محمد نيازى حتاتة، تحريات الشرطة، مجلة الأمن العام يوليو ١٩٦٤ السنة ٧، العدد ٢٦، ص ٣؛ رابح لطفى جمعه، تحريات البوليس ومدى جديتها لاستصدار إذن تفتيش صحيح، مجلة الأمن العام يوليو ١٩٥٩، العدد ٦، ص ٤٧.

٨٦- عبد الرءوف مهدى، المرجع السابق، ص ٥٠٢.

٨٧- نبيلة هروال، المرجع السابق، ص ٢٣٣.

٨٨- هلالى عبد اللاه، تفتيش الحاسب الآلى، المرجع السابق، ص ١٢١؛ أحمد سعد الحسينى: المرجع السابق، ص ١٩٨؛ نبيلة هروال، المرجع السابق، ص ٢٣٣؛ عائشة بنت قارة مصطفى، المرجع السابق، ص ١٠٣.

٨٩- عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ج١ دار النهضة العربية ١٩٩٣، ص٣٨١ وما بعدها؛ نقض ١٩٥٤/١/٥، مجموعة أحكام النقض، س٥، ص ٢١٣، رقم ٧٢؛ نقض ١٩٥٨/٦/٣، س ٩، ص ٦٠٢، رقم ١٥٤؛ نقض ١٩٧٠/١/١٨، س ٢١، ص ١٢٥، رقم ٣٠.

٩٠- عوض محمد عوض، المرجع السابق، ص٣٨٠.

٩١- عوض محمد عوض، المرجع السابق، ص٣٨١.

٩٢- محمد زكى أبو عامر، المرجع السابق، ص٦٨٨؛ نقض ١٩٧٩/٢/١٢، مجموعة أحكام النقض، س٣٠، ص٢٦٥، رقم ٥٢.

٩٣- محمود نجيب حسنى، المرجع السابق، ص ٥٤٧.

94- Garraud, traité théorique et Pratique d'Instruction criminelle et de Procédure Pénal ш 1907, no. 913 .p.219; El Shawi , Théorie général de= perquisitions en droit pénal français et éyptien, thèse Paris 1950 no. 67, p. 75.

هشام فريد رستم، المرجع السابق، ص ٧٣ وما بعدها.

٩٥- هلالى عبد اللاه، التفتيش نظم الحاسب الآلى، المرجع السابق، ص ١٢٢ وما بعدها؛ عبد الرءوف مهدى، المرجع السابق، ص ٥٨.

96- El shawi no. 69, op. cit. p. 77.

٩٧- هلالى عبد اللاه، تفتيش نظم الحاسب الآلى المرجع السابق، ص ١٣٣ وما بعدها.

98- Williams (Glanville): The power to prosecute , Criminal Law Review, London 1955. p. 596; Humphreys (Christmas): The duties and responsibilities of prosecuting counsel , criminal law review 1955, p.739.

٩٩- هلالى عبد اللاه، تفتيش نظم الحاسب الآلى، المرجع السابق، ص ١٣٥.

١٠٠- محمود محمد مصطفى، شرح قانون الإجـراءات الجنائـيـة، دار النهضـة العربية ط ١٠، ١٩٧٠، ص ٢٧٧، بند ٢٠٦.

١٠١- محمود نجيب حسنى، مرجع سابق، ص٥٤٩ وما بعدها.

١٠٢- عبد الرءوف مهدى، مرجع سابق، ص٤٩٦.

١٠٣- نقض ١٩٥٤/٥/١٢، مجموعة أحكام النقض، س٥، ص٦٢٢، رقم ٢١٠.

١٠٤- نقض ١٩٤٢/٦/٢٢، مجموعة القواعد القانونية، جـ٥، ص٦٨١، رقم ٤٣٢.

١٠٥- نقض ١٩٤٢/١١/٢، مجموعة القواعد القانونية، جـ٦، ص ١١، رقم ١١.

١٠٦- محمود نجيب حسنى، مرجع سابق، ص ٤٨٩ وما بعدها؛ نقض ١٩٣٨/١٢/١٩، مجموعة القواعد القانونية، جـ٤، ص ٤٠٧، رقم ٣١٣.

١٠٧- نقض ١٩٤٢/١٢/٢، مجموعة القواعد القانونية، جـ٦، ص ١١، رقم ١١.

١٠٨- نقض ١٩٣٨/١٢/١٩، مجموعة القواعد القانونية، جـ٤، ص ٤٠٧، رقم ٣١٣.

١٠٩- عمر بن يونس، رسالة دكتوراه، مرجع سابق، ص ٨٦٤؛ نبيلة هروال، المرجع السابق، ص ٢٣٤.

١١٠- عبد الرءوف مهدى، مرجع سابق، ص ٥٠٨.

١١١- محمود نجيب حسنى، مرجع سابق، ص ٥٤٦.

١١٢- عبد الرءوف مهدى، مـرجع سـابـق، ص ٥٠٩؛ عـمـر السعيد رمضان، مرجع سابق، ص ٣٨١؛ عوض محمد عوض، مرجع سابق، ص ٣٨١.

١١٣- نقض ١٩٥١/٤/١٦، مجموعة أحكام النقض، س ٢، ص ٩٧٤، رقم ٣٥٧.

١١٤- نقض ١٩٥٩/١١/٣، مجموعة أحكام النقض، س ١٠، ص ٨٥٢، رقم ١٨٢.

١١٥- هلالى عبد اللاه، تفتيش نظم الحاسب الآلى، مرجع سابق، ص ١٦٠.

١١٦- عائشة بنت قارة مصطفى، مرجع سابق، ص ٨٦، ١٠٤؛ سامى حسين الحسينى، المرجع السابق، ص ١٦٣؛ هشام فريد رستم، مرجع سابق، ص ٦٩ وما بعدها.

١١٧- هشام فريد رستم، مرجع سابق، ص ٧٣.

١١٨- شيماء عبد الغنى، مرجع سابق، ص ٢٦٠.

١١٩- القضية رقم ٨٩، لسنه ٢٠١٣، جنح الشيخ زايد؛ القضية رقم ١٢٩٩، لسنه ٢٠١٤، مركز الجيزة؛ القضية، رقم ٣١٣٧٩، لسنة ٢٠١٤، جنح الهرم.

120- U.S. V. RUNYAN, 275 F.3d 449 (5th Cir. 2001) https://casetext.com/case/us-v-runyan-3 الدخول ٢٠١٩/١/١٩

121- U.S. V. WALSER, 275 F.3d 981 (10th Cir. 2001) https://casetext.com/case/us-v-walser-2 تاريخ الدخول ٢٠١٩/١/١٩

١٢٢- شيماء عبد الغنى، مرجع سابق، ص ٢٩٠؛ عائشة بنت قارة، مرجع سابق، ص ١٠٧.

١٢٣- عبد الرءوف مهدى، مرجع سابق، ص ٥٢١ وما بعدها؛ نقض ١٩٥٩/٦/٢٢، مجموعة أحكام النقض، س ١٠، ص ٦٤٤، رقم ١٤٤.

١٢٤- شيماء عبد الغنى، مرجع سابق، ص ٢٦٠.

125- U.S. V. HARGUS, 128 F.3d 1358 (10th Cir. 1997) https://casetext.com/case/us-v-hargus تاريخ الدخول ٢٠١٩/١/١٩

126- U.S. V. SCHANDL, 947 F.2d 462 (11th Cir. 1991) https://casetext.com/case/us-v-schandl تاريخ الدخول ٢٠١٩/١/١٩

127- U.S. V. LAMB, (N.D.N.Y. 1996), 945 F. Supp. 441 (N.D.N.Y. 1996) https://casetext.com/case/us-v-lamb-4 تاريخ الدخول٢٠١٩/١/١٩

١٢٨- فقد قضت المحكمة الفيدرالية الألمانية بإلغاء قرار الضبط على ٢٢٠ ديسكا بالإضافة إلى الوحدة المركزية وذلك لمخالفة مبدأ التناسب:

Verguchi Pascal: La répressionde délit informatique dans une perspective internationale, thèse, Montepllier, 1996, p. 365.

شيماء عبد الغنى، مرجع سابق، ص ٣٥٨؛ هشام فريد رستم، مرجع سابق، ص ٩٩ وما بعدها؛ أ. عائشة بنت قاره، مرجع سابق، ص ١١٥.

129- U.S. V. LONGO, 70 F. Supp. 2d 225 (W.D.N.Y. 1999) https://casetext.com/case/us-v-longo-2 تاريخ الدخول ٢٠١٩/١/١٩

130- Compte rendu en R.D.C. 1960 p. 750, résolutions du congrès d'athènes de la commission international de jurists: Primauté du droit et droits de I'homme" Genève, 1966. p. 30.

131- Durham (Cole) : op.cit., p. 714.

132- Daragon (Elise): Droit de la prevue, These, Grenoble 1996 p.242.

جميل عبد الباقى الصغير، أدلة الإثبات الجنائى، مرجع سابق، ص ١١٨ وما بعدها.

133- Kertesz: op. cit., p. 386.

134- Buchala (Kazimierz) op. cit., p. 515.

135- Yanaguchi (Atsushi): op. cit., p. 448.

136- nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself,

https://www.law.cornell.edu/constitution/fifth_amendment تاريخ الدخول ٢٠١٩/١/١٩

مصطفى العوجى، حقوق الإنسان فى الدعوى الجنائية، بيروت، مؤسسة نوفل ١٩٨٩، ص٥٧٩.

137- Edward M. Wise: Computer crimes and other crimes against information technology in United States , R.I.D.P. 1993 p. 666.

138- Edward. M. Wise, op.cit., p. 667.

هلالى عبد اللاه، التفتيش نظم الحاسب الآلى، المرجع السابق، ص ٢٠٩؛ هشام رستم، مرجع سابق، ص ٨٤ هامش(١).

١٣٩- هشام فريد رستم، المرجع السابق، ص ٨٤.

١٤٠- محمد محى الدين عوض، حقوق الإنسان فى الإجراءات الجنائية، بدون ناشر، ١٩٨٩، ص٥١٢.

١٤١- مصطفى العوجى، حقوق الإنسان فى الدعوى الجزائية، بيروت- مؤسسة نوفل ط١، ١٩٨٩، ص ٥٨١.

١٤٢- محمد زكى أبو عامر، الإثبات فى المواد الجنائية، الإسكندرية، الفنية للطباعة والنشر، بدون سنة نشر، ص ٥٠؛ محمد سامى النبراوى، استجواب المتهم، رسالة دكتوراه، كلية الحقوق- جامعة القاهرة، ص١٤٩؛ محمد محمد شنب شجاع، الحماية الجنائية لحقوق المتهم- دراسة مقارنة بين الفقه الإسلامى والقانون الوضعى، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ١٩٩٠، ص ٣٦٤.

١٤٣- نقض ١٩٦٠/٥/١٧، مجموعة أحكام النقض، س١١، ص٤٦٧ رقم٩٠.

144- François lacasse, La police et le droit à l'avocat au Canda, Rev. S. C. 1993 p.666.

145- Imre Ketés and Laszlo pusztai: computer crimes and other crimes against information technology in Hungary R.I.D.P 1993. p. 386.

١٤٦- عبد الرءوف مهدى، مرجع سابق، ص ١٤٥٧؛ د. آمال عثمان، مرجع سابق، ص ٤٣٦؛ د. جميل عبد الباقى الصغير، المرجع السابق، ص ١٢٠.

١٤٧- نقض ١٩٧٩/٤/٢، مجموعة أحكام النقض، س ٣٠، ص ٤٢٦، رقم ٩٠.

١٤٨- محمود نجيب حسنى، مرجع سابق، ص ٨٤٧.

١٤٩- جميل عبد الباقى الصغير، مرجع سابق، ص ١٢٠.

١٥٠- محمد على محمد عبيد الحمودى، مرجع سابق، ص ١٨٧ وما بعدها؛ هلالى عبد اللاه، التزام الشاهد بالإعلام فى الجرائم المعلوماتية، المرجع السابق، ص ٢٣ وما بعدها.

١٥١- هلالى عبد اللاه، التزام الشاهد بالإعلان، المرجع السابق، ص ٢٣ وما بعدها.

ويعتبر من قبيل الشهود فى مجال المعلوماتية، متعهدو الوصول ومتعهدو الإيواء، ويقصد بمتعهدو الوصول أى شخص طبيعى أو معنوى يقوم بدور فنى لتوصيل المستخدم- الجمهور- إلى شبكة الانترنت وذلك بمقتضى عقد اشتراك تضمن توصيل العميل إلى المواقع التى يريدها، يراجع مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ٢٠٠١، ص ٥٧، ويقصد بمتعهدى الإيواء، أى شخص طبيعى أو معنوى يعرض إيواء صفحات الويب على حساباته الخادمة مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة. يراجع عبد الفتاح بيومى حجازى، التجارة الإلكترونية، المجلد الثانى، دار الفكر الجامعى ٢٠٠٢، ص ١٤١؛ حسن مظفر الرزو، المفاهيم المعلوماتية لجرائم الفضاء

الافتراضى بالحاسوب، مجلة الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات، العدد ١٦ يناير ٢٠٠٢، ص ٢٥١ وما بعدها.

١٥٢- هلالى عبد اللاه، التزام الشاهد بالإعلام، المرجع السابق، ص ٢٥؛ محمد الحمودى، المرجع السابق، ص ١٨٧ وما بعدها.

١٥٣- عبد الفتاح بيومى حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، دار الفكر الجامعى، الإسكندرية ٢٠٠٦، ص ١٦١.

154- Mohrenschlager (Manfred): op.cit., p. 351.

155- Erman (Sahir) les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie, R.I.D.P 1993, p. 624.

هشام فريد رستم، مرجع سابق، ص ٩١ وما بعدها، هامش رقم (٢).

156- Jaeger (Marc) : Les crimes informatiques d'autres crimes dans le domaine de la technologie informatique en Luxembourg. R.I.D.P.1993 R.I.D.P. p. 468.

157- Kunsemuller (Calos): computer crimes and other crimes against information technology in Chile R.I.D.P 1993 p. 259.

١٥٨- شيماء عبد الغنى، مرجع سابق، ص٣٦٤؛ هلالى عبد اللاه، التزام الشاهد بالإعلام، مرجع سابق، ص ٥٣؛ شيماء عبد الغنى، مرجع سابق، ص ١٤٧.

159- Pascal Vergucht, op. cit., p. 398.

شيماء عبد الغنى، مرجع سابق، ص ٣٦٤.

160- Kaspersen (W.K. Henrik) : op.cit., p. 497.

محمد طارق عبد الرءوف الخن، جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبى الحقوقية، ط١، بدون سنه نشر، ص ٣٠٦.

161- Buchala "Kazimierz" : computer crimes and other crimes against information technology in Poland. R.I.D.P. 1993 p. 515.

162- Francillon "Jacques: : Les crimes informatiques d'autres crimes dans le domaine de la technologie informatique en France. R.I.D.P. 1993 p. 309.

هشام فريد رستم، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، جامعة أسيوط العدد ١٧، ١٩٩٥، ص ١١٧.

163- Vassilaki "Irini" : op.cit., p. 371, 372.

164- Kertesz "Imrc" and Pusztai "Laszlo" : op.cit., p. 515.

١٦٥- جميل عبد الباقى الصغير، أدلة الإثبات الجنائى والتكنولوجيا الحديثة، نادى القضاة ٢٠١٠، ص ١٢٤ وما بعدها.

١٦٦- هشام فريد رستم، المرجع السابق، ص ٩١ وما بعدها؛ شيماء عبد الغنى، مرجع سابق، ص ٣٦٤؛ هلالى عبد اللاه، التزام الشاهد بالإعلام، مرجع سابق، ص ٥٦؛ محمد محمود مصطفى، المرجع السابق، ص ١٤٨.

167- Vergucht (Pascal) , La répression des délits informatiques dans une perspective internationale, Thèse, Montpellier 1, 1996. No2. 322,p1.399.

١٦٨- جميل عبد الباقى الصغير، أدلة الإثبات الجنائى، مرجع سابق، ص ١٢٤ وما بعدها.

Inspection in Accordance with the Provisions of Law No. 175 of 2018 Regarding Combating Data Mining Crimes

Moustafa Ali Khalaf

This study deals with an important procedural aspect related to searching evidence in IT crimes. This aspect includes computer inspection in light of law no. 175 of 2018 regarding combating data mining crimes. In this context, this paper discusses the issue of computer inspection and the inside and outside systems connected with it. It also tackles the issue of IT inspection based on permission from the investigation authority and the way of determining the location of the inspection and implementing the permission.