ضوابط التفتيش الجنائي على أنظمة تقنية المعلومات
دراسة في ضوء التشريع العماني والمقارن

الرائد الدكتور/ علي بن خلفان بن علي الهنائي*
الدكتور/ محمود أحمد العطا مبيوع *

الملخص:
تناول موضوع البحث دراسة معايير وضوابط التفتيش الجنائي على أنظمة تقنية المعلومات، من خلال دراسة مسرح الجريمة المعلوماتية، والضوابط الإجرائية المتعلقة بجمع الأدلة في مجال هذا النوع من الجرائم، ومدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش، بعد أن أصبحت الجرائم المعلوماتية من أبرز معالم العصر الحديث، ومسألة الإثبات الجنائي وكيفية ضبط الأدلة الرقمية وجمعها في هذا النوع من الجرائم يثير صعوبة بالغة أمام جهات التحقيق، وأجهزة العدالة الجنائية بسبب الطبيعة المعنوية لمحل الجريمة؛ كونها غير مادية، وتتعلق بالمعالجة الآلية للبيانات، ولكونها من الموضوعات المستجدة في العالم، وسلطات التحقيق اعتادت على كون الإثبات مادياً وملموساً، كما إن الجاني يمكنه ارتكاب الجريمة من دول أخرى، فالجرائم المعلوماتية غالباً ما تكون دولية.
وتوصلت الدراسة إلى أن الجرائم المعلوماتية مستحدثة، ومتغيرة ومتطورة بتطور التكنولوجيا والعالم الافتراضي؛ لذلك فإن الوضع يتطلب وضع حماية قانونية، وجزائية للبيانات والمعلومات الإلكترونية؛ للحد من وقوعها أهدافاً للمجرمين، وتطوير القوانين الإجرائية لتنظم الإجراءات التي تتعلق بالتحري وجمع الأدلة، وتضع ضوابط لإجراءات التحقيق في مثل هذه الطائفة من الجرائم بصفة عامة، والتفتيش بصفة خاصة، وضرورة أن تواكب القوانين الوطنية هذا التطور؛ لضمان تجريم جميع الأفعال التي تشكل جرائم حتى لا يفلت أي مجرم من العقاب، أو تضيع الحقوق.

الكلمات المفتاحية: تكنولوجيا المعلومات – جرائم تقنية المعلومات – التفتيش – التفتيش الإلكتروني – نظم تقنية المعلومات.

---

*أستاذ القانون الجنائي المساعد – أكاديمية السلطان قابوس لعلوم الشرطة.
*أستاذ علوم الشرطة المساعد – أكاديمية السلطان قابوس لعلوم الشرطة.

Criminal Inspection Rules on Information Technology Systems (A study in Light of Omani and Comparative Legislation)

Major Dr. Ali Khalfan Ali Al Hinai*
Dr. Mahmoud Ahmed El Atta Mabyoua*

Abstract:

This research discusses the standards and rules of criminal inspection on Information Technology (IT) Systems by carrying out a study on the IT crime scene, the procedural rules concerning evidence gathering in the field of this kind of crimes, and the extent to which the components of IT systems are fit for inspection. This is at a time when IT crimes have become one of the most prominent features of the recent era, and evidence substantiation as well as control and collection of digital evidence constitute utmost difficulty for authorities responsible for investigation and criminal justice due to the nature of criminal place, being unphysical and relate to the mechanical treatment of data, whereby these authorities are used to work on material and tangible evidence. It is also at a time when the committers of crimes are from other states as these crimes are international in nature.

The study reaches the conclusion that IT crimes are newly established, evolving and developing along with technology and virtual world. Therefore, the situation requires putting in place legal and criminal protection for electronic data and information to eliminate they become target for criminals, and developing the procedural laws to regulate effectively the procedures related to investigation and collection of evidence and set rules for procedures of investigation in this kind of crimes generally, and inspection specifically. In addition, national laws have to move in line with the ongoing developments to ensure criminalization of all acts that constitute crimes to prevent impunity and loss of rights.

Keywords: Information Technology - Information Technology Crimes – Inspection - Electronic Inspection - Information Technology Systems.

---

*Assistant Professor of Criminal Law, Sultan Qaboos Academy of Police Sciences.

*Assistant Professor of Police Sciences, Sultan Qaboos Academy of Police Sciences.

المقدمة

لقد كان الهدف الأساسى من إيجاد أجهزة تقنية المعلومات هو تسخيرها لخدمة الإنسان فى المجالات المختلفة، إلا أنه تم استغلال طائفة من المجرمين لهذه الوسائل بشكل سلبي، من خلال ارتكاب أفعال تشكل جرائم، الأمر الذي يتطلب إيجاد الوسائل المناسبة للسيطرة عليها، وتنظيم استخدامها.

حيث ثبت ارتكاب العديد من الجرائم من خلال هذه الأجهزة بحق الأشخاص، والأموال والمؤسسات المختلفة، خاصة وأن زيادة الاعتماد على أجهزة التقنية، أو غيرها من الوسائط في هذه المجالات داخل الدول يزيد من انتشار هذا النوع من الجرائم، سواء كان ذلك بسبب سوء استخدام البيانات، أم سوء تخزينها، فاختراق أجهزة التقنية يمكن حدوثه عبر الدول، فيصعب تحديد المصدر، أو الوقت الذي حدث فيه، فهذه الجرائم تعدت القيم المادية إلى المعنوية كالبرامج الخاصة بأجهزة التقنية، مثل الحواسيب والبيانات المخزنة فيها.

وتختلف الجرائم التي تقع على أجهزة تقنية المعلومات أو بسببها، عن الجرائم التقليدية، سواء من حيث طبيعتها أو سمات مرتكبيها أو وسائلها، حيث اسهمت عدة عوامل في انتشارها – سنبرزها من خلال هذه الدراسة – وارتفاع نسبة ضحاياها، خاصة مع صعوبة الرقابة أو قصورها، وضعف التشريعات القانونية، وفرض العقوبات لتحجيم تأثيرات هذا النوع من الجرائم المستحدثة، التي تستهدف الأفراد والبيانات والدول، وترهق كاهلها بالخسائر الفادحة في مختلف قطاعات الحياة، وكان أبرزها عجز القوانين الجزائية التي وضعت نصوصها في ظروف تختلف عن الظروف الحالية المرتبطة بتقنية المعلومات عن مواجهة هذه الأنواع الجديدة من الجرائم، كما انعكس تأثير الوسائل الإلكترونية على القوانين الإجرائية، خاصة فيما يتعلق بصعوبة إثبات هذا النوع الجديد من الجرائم، الأمر الذي استدعى أن تصدر الكثير من الدول قوانين تختص بتنظيم هذا القطاع، وتجرم الأفعال التي تقع مخالفة لنصوصها، ومنها سلطنة عُمان التي أصدرت قانون مكافحة جرائم تقنية المعلومات، وقانون المعاملات الإلكترونية، وقانون تنظيم الاتصالات، كما صدر المرسوم السلطاني رقم ٢٠٢٠/٦٤ بإنشاء مركز الدفاع الإلكتروني بهدف تعزيز قدرة الجهات الحكومية ومؤسسات القطاع الخاص والأفراد، وبناء القدرات المتخصصة في مجال الأمن الإلكتروني.

ومع ظهور هذه الطائفة من الجرائم، والتي جلبتها ثورة تقنية المعلومات فقد صدرت قوانيين خاصة في هذا المجال، من أجل التصدي لهذه الجرائم حماية للأفراد والمجتمع من أي أفعال تشكل جرائم قد تقع بواسطة هذه الوسائل أو عليها، إلا أن السمة البارزة في هذه القوانين، أنها جاءت بقواعد موضوعية، ولم تتطرق إلى القواعد الإجرائية، ومن ثم قد تواجه جهات إنفاذ القانون العديد من المشكلات، خاصة فيما يتعلق بقواعد التفتيش وضبط الأدلة، الأمر الذي يتطلب انسجاماً تشريعياً داخل النظام القانوني، بحيث يساعد قانون الإجراءات الجزائية في تنفيذ أحكام قانون الجزاء والقوانين العقابية الأخرى على الجرائم المستحدثة في هذا المجال، حتى لا يفلت أي مجرم من العقاب، ومن جانب آخر نضمن عدم وقوع أي إعتداءات، أو انتهاكات على الحريات، أو الحياة الخاصة.

وفي ضوء ما سبق ستقوم الدراسة الحالية بدراسة معايير وضوابط التفتيش الجنائي على أنظمة تقنية المعلومات من خلال دراسة مسرح الجريمة المعلوماتية، والضوابط الإجرائية المتعلقة بجمع الأدلة في مجال الجريمة المعلوماتية، ومدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش.

أهمية الدراسة:

تأتي أهمية هذ البحث من خلال دراسة التطور الهائل الذي حدث في مجال جرائم تقنية المعلومات، وما خلّفه من آثار سلبية على الأشخاص أو الدول، وما تطرحه هذه الجرائم من تحديات في سبيل مكافحتها وضبطها، ومن ضمنها إجراء التفتيش على محل هذه الجريمة، ومكوناتها، وحدود مسرحها، والضوابط التي تتخذ في سبيل ذلك، ومدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش.

ونحاول في هذا البحث إبراز أهمية هذه الدراسة، ومعرفة توجُهات المشرعين العُماني والمقارن في مكافحة هذا النوع من الجرائم، وكيفية معالجتها لضوابط تفتيش أجهزة تقنية المعلومات بمكوناتها المادية والمعنوية، والتعامل مع الأدلة وضبطها.

إشكالية الدراسة:

أدى ظهور طائفة من الجرائم التي جلبتها ثورة تقنية المعلومات إلى قيام أغلب الدول، ومنها سلطنة عُمان، بإصدار قوانين خاصة بغية التصدي لهذا النوع من الجرائم، والتي تقع بواسطة هذه الوسائل أو عليها، إلا أن هذه القوانين جاءت

بقواعد موضوعية موضحة الأفعال التي تشكل جرائم، والعقوبات المقررة لها، ولم تتطرق إلى القواعد الإجرائية، ومن ثم قد تواجه جهات إنفاذ القانون العديد من المشكلات، خاصة فيما يتعلق بمسرح الجريمة المعلوماتية، وقواعد التفتيش وضبط الأدلة؛ وذلك نظراً لطبيعة هذه الجريمة، وطرق ارتكابها، وصعوبة تتبعها، إذا ما علمنا أنها قد ترتكب من خارج إقليم الدولة، وحتى لا تضيع الحقوق أو يفلت أي مجرم من العقاب، ولضمان عدم وقوع أي اعتداءات، أو انتهاكات على الحريات، أو الحياة الخاصة، أو الأموال، أو أسرار الدول، فإنه يتطلب معالجة قانونية سريعة تنظم القواعد الإجرائية وضوابطها؛ لأن نصوص قانون الإجراءات الجزائية قد لا تستوعب تنظيم التعامل مع طبيعة مسارح الجرائم المستحدثة في هذا المجال، وتفتيشها والتعامل مع أدلتها.

وبصفة عامة فإن الدراسة الحالية تستهدف الإجابة على بعض التساؤلات التي ترتبط بجرائم تقنية المعلومات ومن أهمها :

- ما هو مسرح الجريمة المعلوماتية؟
- ما هي الكيفية التي يتم بها التفتيش في مجال جرائم تقنية المعلومات؟
- ما هي الضوابط الإجرائية المتعلقة بجمع الأدلة في مجال الجريمة المعلوماتية؟
- ما مدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش؟
- هل الأدلة فى جرائم تقنية المعلومات تتشابه مع باقى الجرائم الأخرى؟
- هل نظم المشرع العُماني تفتيش أجهزة تقنية المعلومات المرتبطة ببعضها سواء داخل الإطار الوطني أو خارجه؟

مصطلحات البحث:

- **تقنية المعلومات:** الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة.
- **وسيلة تقنية المعلومات:** جهاز إلكتروني يستخدم لمعالجة البيانات والمعلومات الإلكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الآلي وأجهزة الاتصال.

- **جرائم تقنية المعلومات:** الأفعال غير المشروعة التي ترتكب بواسطة إحدى وسائل تقنية المعلومات أو عليها أو تستهدفها إضراراً بحق أو مصلحة أسبغ عليها المشرع الحماية الجزائية.
- **التفتيش:** هو إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لفعل مجرم تم ارتكابه في محل يتمتع بحرمة المسكن أو الشخص، وذلك من أجل إثبات ارتكاب هذا الفعل أو نفيه، وفقاً للإجراءات القانونية المقررة.
- **التفتيش الالكتروني:** هو إجراء من إجراءات التحقيق، تقوم به السلطات للبحث عن أدلة الجريمة الرقمية في وسيلة تقنية المعلومات، أو الأجهزة الرقمية الأخرى وفقاً للإجراءات القانونية المقررة.

منهجية الدراسة:

اعتمدت الدراسة المنهج الوصفي التحليلي لملاءمته للموضوع، وذلك من خلال وصف الظاهرة، وجمع البيانات عنها للإجابة على أسئلة الدراسة، وتحليل النصوص القانونية ذات العلاقة، وبيان مدى انطباقها على إجراءات التفتيش للجرائم المعلوماتية وجمع الأدلة، وتحليل الآراء التي قيلت بشأنها، للخروج بحصيلة من شأنها وضع الحلول النظرية والعملية للموضوع، واستخلاص الغايات والأهداف التي من أجلها أعدت هذه الدراسة.

خطة الدراسة:

المبحث الأول: مسرح الجريمة المعلوماتية.

المبحث الثاني: التفتيش في مجال الجريمة المعلوماتية.

المبحث الثالث: مدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش.

الخاتمة:

المبحث الأول
مسرح الجريمة المعلوماتية

الجريمة المعلوماتية المرتكبة على أجهزة تقنية المعلومات أو بواسطتها تتطلب لارتكابها وجود وسيلة تقنية معلوماتية، وتتطلب معرفة تقنية لاستخدام هذه الوسيلة التقنية المعلوماتية، فهي إذن جريمة تقنية بيئتها تقنية ووسيلة مقارفتها تقنية، ونمط السلوك الإجرامي فيها ذو مضمون فني تقني[١].

ويمكن القول بأن المعرفة التقنية بأجهزة تقنية المعلومات كأساس نسبي ضروري للقيام بالأفعال المتطلب آداؤها لارتكاب الجريمة، وتتفاوت من حيث البساطة والتعقيد تبعاً للفعل نفسه، فتجاوز إجراءات الأمن ككلمة السر، والاستخدام غير المصرح به لشبكة المعلومات يحتاج إلى معرفة أعمق من نشاط نسخ برنامج، في حين قد تحتاج جريمة زرع فيروس في النظام بغية إتلاف كامل النظام، أو جزء منه معرفة تقنية أكثر عمقاً وشمولاً من الفعلين المذكورين، قد لا تقف عند حد المعرفة باستخدام أجهزة التقنية، بل تتطلب إلماماً بالبرمجة؛ فالطبيعة القانونية لمحل الاعتداء في جرائم تقنية المعلومات تنطلق إبتداء من تناول الحقائق الآتية:

أ. إن القوانين الجزائية قد كفلت من حيث الأصل، وشيدت على ذلك نظرياتها وقواعدها حماية الأموال المادية، وسنت النصوص لتجريم الاعتداءات الواقعة على الأموال، والجرائم التي تتناول الاعتداء، أو تهدد بالخطر الحقوق ذات القيمة المالية، ويدخل في نطاق هذه الحقوق كل حق ذي قيمة اقتصادية، أياً كانت وداخل في دائرة التعامل، ومتضامن على هذا النحو في تكوين الذمة المالية[٢].

ب. إن جرائم أجهزة تقنية المعلومات وقبلها جرائم سرقة المعلومات دون دعاماتها المالية (سنداً أو ورقياً.. مثلاً) أثارت جدلاً فقهياً عميقاً، مصدره طبيعة المعلومات (معطيات الأجهزة) المعنوية؛ فالطبيعة المعنوية للمعلومات، وغياب الطبيعة المادية، أساس الجدل بإمكانية الحماية الجزائية في حدود حماية المال المادي إلى

---

[١] د. نسرين محسن نعمة الحسيني و د. محمد حسن مرعي، الجرائم الالكترونية الواقعة على الأموال دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠م، ص١٦.

[٢] د. محمود نجيب حسنى، شرح قانون العقوبات/القسم الثاني(جرائم الاعتداء على الأموال)، الطبعة السادسة، دار النهضة العربية، القاهرة، ١٩٨٩م، ص١٤.

حماية المعلومات (أو المال المعنوي)، أي أن أساس الجدل في قابلية النص الجزائي الذي يحمي الأشياء المادية للإنطباق على المعطيات ذات الطبيعة المادية[٣].

وعليه يمكن الإقرار أن جرائم تقنية المعلومات، والجرائم الناشئة عن إساءة استخدام أجهزة تقنية المعلومات التي تقترن بأنماط ودرجات التقنية بمختلف درجاتها، يلزم عند التحقيق فيها، وإستجلاء حقيقتها جانبين متضامنين هما:

أولاً: قواعد وأساليب التحقيق الجنائي الفني التقليدية المعروفة ذات التقنيات الخاصة غير المسبوقة.

ثانياً: امتلاك من يتولى التحقيق فيها أن يكون متخصصاً في التحقيق الجنائي، ومعالجة البيانات الحاسوبية، وغيرها من متطلبات المعرفة بفنيات أجهزة تقنية المعلومات.

الانتقال والمعاينة لمسرح الجريمة المعلوماتية:

الانتقال إلى محل الواقعة من أهم إجراءات جمع الأدلة، فهو لازم لمعاينة حالة الأمكنة والأشياء والأشخاص، ووجود الجريمة ماديا، ويستحسن المبادرة إليه قبل أن تزول آثار الجريمة، أو تتغير معالم المكان، وكثيراً ما يكون مصحوباً بالتفتيش وضبط الأشياء[٤].

إذن المعاينة هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة، ليشاهد بنفسه، ويجمع الآثار المتعلقة بالجريمة، وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تُفيد في كشف الحقيقة[٥].

والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى ما رأى لذلك ضرورة تتعلق بالتحقيق، والأصل أن يحضر أطراف الدعوى المعاينة، وقد يقرر المحقق أن يجري المعاينة في غيبتهم، لاسيما وأن غياب المتهم عند

---

[٣] د. نسرين محسن نعمة الحسيني و د. محمد حسن مرعي، مرجع سابق، ص١٢٣.

[٤] أحمد بسيوني أبو الروس، التحقيق الجنائي والأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٩م، ص١٧.

[٥] المستشار أحمد محمود خليل، الوسيط في شرح قانون الإجراءات الجزائية العماني، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٧م، ص١٧٣.

إجراء المعاينة ليس من شأنه أن يبطلها[٦]، ويجب على المحقق عند إجراء المعاينة إثبات المكان ووصفه تفصيلاً.

وللمعاينة أهمية كبرى بعد ارتكاب الجرائم التقليدية، لوجود مسرح جريمة واقعي، يحتوي على الآثار المادية الحقيقية التي يستهدف فريق التفتيش الحفاظ عليها عند التحضير لهذا الإجراء لإثبات صحتها كدليل، ويختلف الأمر في الجرائم المعلوماتية، فلا ينتج عنها آثار مادية ملموسة[٧].

ومفهوم المعاينة إجرائياً بالدراسة الحالية تعني ملاحظة وفحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة لإثبات حالته، والكشف والتحفظ على كل ما قد يُفيد من الأشياء في كشف الحقيقة عن الجريمة ومرتكبها، وإن كانت إجراء يجوز الالتجاء إليه في كافة الجرائم، إلا أنها ليست إجراءً مجدياً أو صالحاً لكشف الحقيقة في الجرائم كلها؛ فهي ليست إجراءً تلقائياً في مباشرتها، بل إجراءً هادفاً غايته كشف وصيانة العناصر المادية الخاصة التي تتعلق بالجريمة، وتفيد في التحقيق الجاري بشأنها، فإذا انعدمت بالنسبة إلى التحقيق الجاري بشأنها جدواها وفائدتها، كما هو الحال في جريمة التزوير المعنوي، وجريمة السب التي تقع بالقول في غير علانية، وغيرهما، مما لا يُجدي كشف الحقيقة بشأن معاينة لم يكن ثمة مجال أو مقتضى لإجرائها، مع التسليم بأهمية المعاينة في كشف غموض أكثر الجرائم التقليدية، وجدارتها بتبوأ مكان الصدارة والأولوية، فيما عدا حالات استثنائية على ما عداها من الإجراءات الاستقصائية الأخرى، بحكم المكانة المحورية لدورها في تصور كيفية وقوع الجريمة، وظروف وملابسات ارتكابها، وتوفير الأدلة المادية من المادة التي يجمع عن طريقها، وتمحيص وتقييم الأدلة الأخرى، والتنسيق بينها في ضوء المعلومات التي تستقي منها، بما يكفل في الوقت نفسه التخطيط السليم لعمليات البحث، والتحقيق الجنائي وتطويرها، إلا أن دورها

---

[٦] د. محمد أبو العلا عقيدة، شرح قانون الإجراءات، الجزء الثاني، دار النهضة العربية القاهرة، ٢٠٠١م، ص٦٤٤.

[٧] علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠م، ص٢٤.

في مجال كشف غموض الجرائم المعلوماتية، وضبط الأشياء التي قد تفيد في إثبات وقوعها، ونسبتها إلى مرتكبيها لا ترقى إلى نفس الدرجة من الأهمية.

ويمكن رد ذلك إلى أن هناك على الدوام تقريباً مسرحاً للجريمة التقليدية عليه جرت الأحداث، وتركت آثارها المادية، ومنه تنبثق الأدلة، ويُتيح مثل هذا المسرح المجال أمام المحقق الجنائي الكشف عن طريق المعاينة عن الآثار المادية التي خلفها ارتكاب الجريمة، والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها، بينما لا يوجد عادة مسرح للجريمة المعلوماتية مماثل، وأقرب تشبيه لمسرحها قد يكون الموقع، أو المكتب الذي توجد فيه الأجهزة، والأنظمة المعلوماتية التي كانت محلاً للجريمة أو أداتها، ومسرح للجريمة كهذا تقل إلى حد كبير فرص إفصاحه عن الحقائق المستهدف التوصل إليها من وراء معاينته للأسباب الآتية:

١. إن الأفعال التي تقع على النظم المعلوماتية، أو بواسطتها قلما يتخلف عن ارتكابها آثار مادية.
٢. إن عدداً كبيراً من الأشخاص يكون قد تردد على مكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً، التي تنقضي عادة بين ارتكاب الجريمة واكتشافها، مما يُفسح المجال لحدوث تغيير، أو إتلاف أو عبث بالآثار المادية، أو زوال بعضها أو تلفه، وهو ما يلقي ظلالاً من الشك على الدليل المستمد من المعاينة.

ولمعاينة مسرح الجريمة المعلوماتية فائدة في كشف الحقيقة عنها وعن مرتكبيها، ولذلك كان متعيناً عند مباشرتها مراعاة الآتي[٨]:

١. تصوير الأجهزة والوحدات الطرفية المتصلة به، والمحتويات والأوضاع العامة بالمكان، مع التركيز على تصوير الأجزاء الخلفية للجهاز وملحقاته، ويراعى تسجيل وقت وتاريخ ومكان التقاط الصور.
٢. الملاحظة والتركيز على الطريقة التي تم بها إعداد النظام.
٣. ملاحظة وإثبات حالة التوصيلات المتصلة بكل مكونات النظام؛ حتى يمكن إجراء عمليات المقارنة والتحليل إذا دعت الضرورة إلى ذلك لاحقاً.

---

(٨) الدكتور عبدالعال الديربي والأستاذ محمد صالح اسماعيل، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢م، ص٢٩٦.

٤. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات؛ للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات مغناطيسية، أو كهربائية أو غيرها، يمكن أن تتسبب في محو البيانات المسجلة.

٥. التحفظ على مستندات الإدخال، والمخرجات الورقية للجهاز ذات الصلة بالجريمة؛ لرفع ومضاهاة ما قد يوجد عليها من بصمات.

٦. التحفظ على الموجودات في سلة المهملات من الأوراق الملغاة والممزقة، وأوراق الكربون المستعملة، والشرائط والأقراص الممغنطة غير اللائقة، وفحصها ورفع البصمات المتعلقة بالجريمة.

٧. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر لهم الكفاءة العلمية، والخبرة الفنية في مجال تقنية المعلومات، والذين تلقوا تدريباً ومعرفة كافية للتعامل مع نوعية الآثار، والأدلة التي يمكن أن يحويها مسرح الجريمة المعلوماتية.

٨. القيام بتحري مبدئي[٩] يستهدف الحصول على أكبر قدر من المعلومات عن السلوك المكون للجريمة المعلوماتية، وأسلوب وظروف ارتكابها في فترة زمنية قصيرة نسبياً، وجمع هذه المعلومات يمكن أن يتم بصفة مبدئية عن طريق المقابلات الاستقصائية التي تجرى مع ممثلي الجهة المجني عليها، وعلى طبيعة السلوك الإجرامي المرتكب.

كما ينبغي ملاحظة أن هناك اعتبارات مهمة، يتعين وضعها في الحسبان عند إجراء هذا التحري الأولي، أهمها:

أ. إن الدليل المستند إلى المعالجة الآلية يمكن أن يكون متاحاً لفترة قصيرة من الزمن.

ب. إن الجريمة المعلوماتية التي يجري التحري الأولي بشأنها يمكن أن تكون مستمرة سواء من حيث نتائجها أو تنفيذها.

---

[٩] د. هشام رستم، أصول التحقيق الجنائي الفني للجرائم المعلوماتية، مجلة الأمن والقانون، العدد الثاني، كلية الشرطة بدبي، الإمارات العربية المتحدة، ١٩٩٩م، ص٩٤.

ج. إن الجريمة المعلوماتية التي يجري التحري الأولي بشأنها يمكن أن تكون ستاراً لفعل إجرامي آخر، فإذا توفرت أدلة تفيد أن هذا هو الوضع فيكون من الضروري إجراء تحقيق أكثر دقة وعمقاً حول الواقعة.

والحقائق المفترض إسهام التحري الأولي في إظهارها يمكن تجميعها في النقاط الآتية[١٠]:

- التثبت من وقوع الجريمة.
- نمط وطبيعة الجريمة المرتكبة.
- التقنيات المستخدمة في ارتكابها.
- الجاني أو الجناة المحتملون أو المشتبه فيهم.
- الأسباب والدوافع المحتملة لارتكاب الجريمة.
- الاستدلال على الشهود في حالة وجودهم.
- طبيعة الأدلة الجنائية ومصادرها.

ومن المؤكد أنه يتعين على فريق معاينة مسرح الجريمة المعلوماتية، وعلى المحقق تحديداً قبل إجراء التحري الأولي، والمقابلات الاستطلاعية الإعداد لها، وتحديد النقاط ذات الصلة بموضوع الجريمة، والمتعين استيضاحها مع العناية بتوثيق المقابلة؛ للرجوع إليها مستقبلاً، كما يجب أيضاً على فريق معاينة مسرح الجريمة المعلوماتية وضع خطة تحقيق شاملة تحدد فيها الخطوات التفصيلية لها واتجاهاتها، وما يجب إخضاعه للتحقيق من أشخاص، وعمليات، وإجراءات، ومكونات مادية أو برمجية للنظم، ويجب أن يرتبط نطاق هذه الخطة بجملة عوامل أبرزها: حجم الجهة المجني عليها، وطبيعة أعمالها، والنظام المعلوماتي المستخدم، وطبيعة الفعل الإجرامي المرتكب.

مرتكزات خطة معاينة مسرح الجريمة المعلوماتية:

تقوم مرتكزات خطة معاينة مسرح الجريمة المعلوماتية على العناصر والخطوط المهمة الآتية[١١]:

---

[١٠] د. هشام رستم، مرجع سابق، ص٩٦.

[١١] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١٧٩.

١. حصر المواقع والأماكن الحساسة بمبنى معالجة أو نقل البيانات، كمكتبة الوثائق، وأماكن خزن الأشرطة، والأقراص الممغنطة، وسائر مداخله وتحديد المسئولين عن أمنها.
٢. الوقوف على قواعد تشغيل النظام المعلوماتي، وكيفية تنظيم دورة المعالجة الإلكترونية للبيانات.
٣. تحديد أساليب التدقيق والمراجعة وغيرها من العمليات، يمكن إجراؤها بمساعدة حاسب الجهة المجني عليها، وتلك التي يلزم إجرائها عن طريق حاسب آخر غيره.
٤. فحص الإحتمالات المختلفة لنمط الدعامة، أو الوعاء المتعين استخدامه للحصول على الدليل وصيانته (ورق أو وسائط ضوئية أو ممغنطة وغيرها).
٥. مراعاة أن المعلومات التي قد تستلزم المعاينة لمسرح الجريمة الإلكترونية الحصول عليها من نظام المعالجة الإلكترونية للبيانات، يمكن أن تكون متاحة فقط لفترة زمنية محدودة، أو في فترة معينة داخل نظام معالجة البيانات، لاسيما وأنه من الممكن – وبسبب الكم الهائل للبيانات المعالجة – أن يتم محو بعضها دورياً؛ لإتاحة المجال لمعالجة بيانات جديدة.
٦. عند إجراء معاينة مسرح الجريمة المعلوماتية يجب مراعاة الاعتبارات الآتية:
أ. تقدير الوقت المتطلب لإجراء مراجعة دقيقة لنظام المعالجة الآلية للبيانات وأنظمة التشغيل.
ب. دقة وكفاية وكفاءة التقارير التي يخرجها الحاسب.
ج. الوقت المتطلب لتصميم برامج تتيح التغلغل في منظومات الحاسب، والبحث في ملفات النظام.

ونرى أن أهم مرتكزات خطة معاينة مسرح الجريمة المعلوماتية تقوم على فحص بيئة المعالجة الآلية للبيانات، التي سيمارس فريق المعاينة والتحقيق في إطارها عمله، وتحديد نوعية وكيفية تعامله معها، وتأثيرها في طبيعة ونطاق إجراءاته وتوقيتها.

ومن هذا المنطلق يمكن لفريق معاينة مسرح الجريمة المعلوماتية تصنيف هذه البيئة كالتصنيفات الآتية[١٢]:

أ. **بيئة عدائية:** وهى التي يكون الفاعل (أو الجاني) ما يزال داخلها، وعلى فريق معاينة مسرح الجريمة المعلوماتية في هذه الحالة توقع حدوث محاولات للتدخل للنظام بهدف الإطاحة بالدليل، ووجوب اتخاذ إجراءات فنية للحيلولة دون حدوثه.

ب. **بيئة مواتية:** وهى التي يكون فيها مستبعداً حدوث ما يعيق فريق معاينة مسرح الجريمة المعلوماتية.

ج. **بيئة غامضة:** وهى التي لا يكون موقف المتصلين بها معروفاً.

ومما سبق يتضح أن جرائم تقنية المعلومات تثير تحديات بشأن الإطار القانوني لإجراءات التفتيش والضبط، والتي ينبغي أن تباشرها سلطات التحقيق المكلفة بتقصي الجرائم وإحالة الجناة للقضاء، ويبدو أن هذا الإطار يغاير أطر التفتيش المتصلة بالجرائم التقليدية، ويرجع ذلك إلى أن تقنية الحاسوب تنطوي على حالات مختلفة من حيث ظروفها وأحوالها، وتتطلب لإجراء التفتيش تقنيات خاصة لتفتيش نظم المعلومات، ولاسيما أن ضبط الأدلة الإلكترونية يتصل بالمكونات المادية لأنظمة الأجهزة التقنية، وضبط المكونات المعنوية (البرمجيات)، وضبط البيانات التي تتناقل، أو يجري تناقلها وتبادلها في نطاق شبكة المعلومات التي تربط الأجهزة ببرامج وتطبيقات تقنية، وما يتصل بها، باعتبار أن مكونات النظام المعلوماتي المادية من الأشياء، فإنها في الأصل أشياء مادية يجوز ضبطها وتحريزها[١٣].

وعليه فإن مجال البحث والتحقيق الجنائي في جرائم تقنية المعلومات يحاول التعامل مع هذه الوقائع بواسطة تقديم وسيلة آمنة، وفاعلة، وشاملة للتحقيق في هذا النوع من الجرائم، حيث يتم جمع وحفظ الأدلة التي تم الحصول عليها؛ ليتم

---

[١٢] د. هشام رستم، مرجع سابق، ص١٣٠.

[١٣] د. حسين بن سعيد الغافري، منظومة سلطنة عُمان التشريعية لمكافحة جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، ٢٠١١م، ص٦.

استخدامها ضمن الإجراءات القانونية بالدعوى، وتتراوح الأدلة بين كونها مادية، أو منطقية أي إنها تشمل أجهزة، أو وسائط تخزين، أو قد تشمل معلومات فقط.

فالجانب المادي في مجال البحث والتحقيق الجنائي لجرائم تقنية المعلومات يشمل التفتيش والضبط، حيث ينتقل المحقق إلى مسرح الجريمة، ويبحث ويضبط الأجهزة والوسائط المستخدمة في الجريمة، أما الجانب المنطقي في هذا النوع من الجرائم، فيتعامل مع استخلاص المعلومات الخام من أي مصدر، (وهو ما يعرف باكتشاف المعلومات)، حيث يقوم المحقق بتصفح السجلات، واسترجاع المعلومات من قاعدة البيانات وغيرها.

وهناك قواعد وأصول عند التعامل مع مسرح الجريمة المعلوماتي، ينبغي على القائمين بالإجراءات مراعاتها، وذلك حسب الآتي:

١. من الأشياء التي ينبغي أن يراعيها المحقق في مسرح الجريمة الإلكترونية هو أن يحافظ على المعلومات التي يمكن استخراجها من الدليل، دون أن يتسبب في تغير الحالة الأصلية للدليل.

٢. كذلك يجب حفظ الحالة الأصلية للدليل خلال التحقيق، أي منذ لحظة تحديد الدليل ومكانه حتى انتهاء التحقيق، وربما بعد ذلك، أيضاً فإن فاعلية الدليل كتوثيق موضوعي تعتمد على كيفية حفظ الدليل لاسيما، وأن أي تغير في بيانات الدليل يكون له نتائج مؤثرة سالبة على سير عملية التحقيق، إذا لم يتم اتباع طرق وأساليب آمنة في جميع مراحل التحقيق.

٣. يتبين من ذلك أن التحقيق الفني في جرائم تقنية المعلومات في جميع مراحله ينصب على إجراءات تفتيش دقيق لأجهزة التقنية والحاسوب وشبكاته، فمنذ تلقي البلاغ عن الجريمة، فإنه يتوجب على المحقق التأكد من وقوع الجرم، ثم تبدأ عمليات الفحص الدقيق على الأجهزة وفق ما تم ذكره سلفاً، من خطة مدروسة لمحاولة الوصول للجاني، وذلك من خلال الأدلة التي يتم جمعها، ومن ثم فإن الجزء الفني من عملية التحقيق في جرائم الحاسوب وتقنية المعلومات ينصب على عملية التفتيش، والضبط للأجهزة وملحقاتها في مسرح الجريمة، وعلى عملية التفتيش الدقيق للأجهزة؛ للوصول إلى أدلة الجريمة وتتبع الجناة.

٤. فالعمل الجنائي يبدأ في مسرح الجريمة، إذ إن تأمين وجمع الأدلة يلعب دوراً مهماً في عملية التحقيق، ونرى أن هناك مسائل محورية يجب معالجتها عند التعامل مع مسرح الجريمة المعلوماتية هي:

أ. إجراء التخطيط قبل الدخول إلى مسرح الجريمة المعلوماتية.

ب. اتباع الأصول العلمية والعملية بشأن إيجاد الدليل للجريمة المعلوماتية.

ج. استرجاع الدليل المعلوماتي في الجريمة المعلوماتية.

د. مراعاة ضوابط وقواعد التفتيش والضبط في الجريمة المعلوماتية.

هـ. التعامل مع الفيروسات في الجريمة المعلوماتية.

أولاً- إجراءات التخطيط قبل الدخول إلى مسرح الجريمة المعلوماتية:

قبل تحرك فريق التحقيق إلى مسرح الجريمة المعلوماتية، يفترض أن تكون هناك خطة شاملة تم إعدادها مسبقاً، وفي هذا الشأن يوصي قسم جرائم الحاسوب في مكتب التحقيقات الفيدرالية الأمريكي FBI اتباع الخطوات الآتية[١٤]:

أ. إعداد المواد والملفات الضرورية لمثل هذا التفتيش باعتبارها الوسائل الآمنة لنقل الدليل من الموقع للمختبر الجنائي.

ب. إعداد الشكل المبدئي للأوراق المطلوبة لتوثيق التفتيش، بالنسبة إلى التفتيش والضبط هناك سجلان: (إلكتروني أو ورقي) سجل أدلة التفتيش والضبط، وسجل نقل الأجهزة، يستخدم الأول من أجل تتبع المعلومات عن أدلة الحاسوب أو وسائل التقنية الأخرى، بينما يستخدم الثاني لتسجيل الأدلة التي تنقل من مسرح الجريمة إلى المختبر، وبعد إرجاع الدليل للمختبر يتم فتح سجل ثالث (هو سجل أدلة المختبر)، بغرض تتبع الأدلة أثناء فحصها.

ج. التأكد من أن جميع المختصين يدركون أشكال الأدلة بالإضافة إلى القدرة على التعامل المناسب معها.

---

[١٤] كمال أحمد الكركي، التحقيق في جرائم الحاسوب، ورقه عمل المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، ٢٠٠٣م.

د. تقييم النتائج القانونية؛ لتفتيش مسرح الجريمة المعلوماتية، حيث يجب الإنتباه إلى مسألة حق الخصوصية للمشتبه بهم، كما يجب التأكد من الحصول على أذونات التفتيش القانونية التي تحوي تفتيش مسرح الجريمة.

هـ. مناقشة بنود التفتيش مع فريق التفتيش قبل الوصول لمسرح الجريمة المعلوماتية ما أمكن ذلك.

و. تعيين رئيس فريق معاينة مسرح الجريمة المعلوماتية، وتحديد مهام الفريق الأساسية قبل الوصول إلى مسرح الجريمة.

ز. الأخذ بعين الاعتبار أمن وراحة فريق التفتيش عند مواجهة مسرح جريمة معلوماتية خطير، أو ظروف بيئية وطبيعية شديدة الخطورة.

ح. تقييم مهام الطاقم، وفريق التفتيش، والمعاينة لمعالجة مسرح الجريمة المعلوماتية بشكل ناجح.

ثانياً- اتباع الأصول العلمية والعملية بشأن إيجاد الدليل للجريمة المعلوماتية:

من المؤكد أن جرائم تقنية المعلومات غير متشابهة، إلا أن إجراءات المعاينة والتفتيش والضبط لمسرح الجريمة تبدأ بالخطوات الإجرائية الآتية:

أ. بعد إعداد الخطة الأولية يتم الانتقال إلى مسرح الجريمة وتأمينه مادياً وإلكترونياً.

ب. ضرورة توثيق مسرح الجريمة المعلوماتية عن طريق الصور والملاحظات.

ج. بعد ذلك يتم التفتيش والبحث عن الأدلة.

وحين وصول فريق التفتيش والمعاينة لمسرح الجريمة المعلوماتية، يقوم رئيس الفريق بتوزيع المهام للقيام بالتفتيش، ومن المهم أن يكون لدى الفريق القدرة على فحص وتفنيد الأشياء التي يجدونها وكيفية التعامل معها.

ويجب على فريق التفتيش الانتباه إلى جميع المواقع التي قد تحتوي على أدلة في مسرح الجريمة، بما في ذلك سطح المكتب الذي قد يحتوي على تعليمات مهمة، أو وسائط متعددة، أو معدات أجهزة التقنية، وأيضاً الشاشات التي قد تحتوي على

تعليقات، أو كلمات مرور، أو هواتف، وأسماء، وأرقام المستخدمين، ومستندات مهمة، كما يمكن أن تحتوي سلة المهملات أيضاً على نسخة من دليل الأجهزة، أو على ملاحظات مهمة، ووثائق وأقراص مدمجة، وأقراص مضغوطة، وما إلى ذلك.

ثالثاً- استرجاع الدليل المعلوماتي في الجريمة المعلوماتية:

بعد التفتيش المبدئي لمسرح الجريمة، يتم توثيق الأجهزة والوسائط، وإعدادها للنقل إلى مختبر الأدلة، وتتألف هذه العملية حسب رأينا من مراحل عدة:

أ. تسجيل أدلة التفتيش والضبط.

ب. توثيق الأجهزة والوسائط والرسائل.

ج. تحديد ما إذا كان من الممكن إغلاق الأجهزة.

د. إغلاق الأجهزة التقنية العاملة بعد تقدير ملاءمة ذلك.

هـ. تمييز وترميز الأجهزة والوسائط.

و. تجهيز الأجهزة والوسائط والأدوات للنقل.

ز. نقل الأجهزة والأدوات والوسائط.

ح. تفريغ الأجهزة والأدوات والوسائط.

رابعاً- مراعاة قواعد التفتيش والضبط في الجريمة المعلوماتية[١٥]:

القواعد الأساسية للتفتيش، والضبط في الجريمة المعلوماتية ضرورية لتتبع الأدلة وإدارتها، كما أنها تشكل حماية ضد أي طعن بهذه الأدلة؛ بسبب احتمال سوء التعامل معها، وهذه القواعد تشمل:

١. **القاعدة الأولى: لا تغير في الدليل الأصلي،** فالنشاطات بالأدلة الجنائية الإلكترونية يجب أن تجري على أساس صورة لما هو موجود على الأجهزة، أي أخذ نسخة احتياطية من الجهاز، والعمل عليها لضمان عدم المساس بالدليل الأصلي؛ لذا لابد من التعامل مع النظام من قبل أشخاص مختصين.

---

[١٥] كمال أحمد الكركي ، مرجع سابق .

٢. **القاعدة الثانية: لا تُنفذ البرامج على الأجهزة بمسرح الجريمة،** حيث أن أي تنفيذ برنامج مباشر على الجهاز بمسرح الجريمة قد يسبب الضرر للأدلة الموجودة عليه، وإذا كان لابد من تنفيذ برامج على الجهاز بمسرح الجريمة؛ فيجب توخي الحذر والحرص وتوثيق جميع الخطوات.

٣. **القاعدة الثالثة: لا يسمح للمشتبه به التعامل مع الأجهزة في مسرح الجريمة.**

٤. **القاعدة الرابعة: إعداد نسخة احتياطية عن وسائط تخزين المعلومات الموجودة في مسرح الجريمة،** حيث يجب أن تقتصر نشاطات التحقيق على النسخ الاحتياطية؛ لضمان المحافظة على الدليل الأصلي.

٥. **القاعدة الخامسة: توثيق جميع نشاطات التحقيق،** وهذا مهم جداً للعمل الجنائي، فمنذ لحظة فتح القضية إلى لحظة إغلاقها، يجب توثيق كل ما يفعله المحقق بالوقت والتاريخ، والمهم حفظ المعلومات المسجلة، وعمل نسخة احتياطية آمنة.

٦. **القاعدة السادسة: تخزين دليل الأجهزة المعلوماتية،** حيث يجب تخزين أدلة الأجهزة والبرامج في بيئة مناسبة.

خامساً- استخدام أطر وقواعد التعامل مع الفيروسات في مسرح الجريمة المعلوماتية[١٦]:

يجب تحديد طريقة للتعامل مع تهديد فيروسات أجهزة التقنية فيما يتعلق بمسرح الجريمة المعلوماتية؛ ذلك إنه كلما كان تفاعل المحقق مع الدليل في الميدان أقل، كان ذلك أفضل، حيث يعد مختبر الأدلة أفضل مكان لتأدية النشاطات المتعلقة بالدليل؛ لأنه مكان آمن ومسيطر عليه، وسواء في المسرح، أو المختبر سيتعرض الدليل للتلف، إذا استخدم المحقق وسائط ملوثة بالفيروسات على جهاز مسرح الجريمة المعلوماتية، وكذلك فإن الدليل الملوث بالفيروسات يمكن أن يكون ضعيفاً

---

[١٦] د. ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم عبر الحدود، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبي، أبريل ٢٠٠٣م.

بدرجة كبيرة، فمن متطلبات التعامل مع جريمة المعلوماتية أن تكون جميع الوسائط نظيفة، ويجب أن تنظف هذه الوسائط جميعها بعد الاستخدام، باستثناء نسخة الاحتياط، ومن غير المفضل تنظيف وسائط تخزين النسخة الاحتياطية بعد استخدامها؛ لأن أي فيروسات مخزنة هناك قد تكون متعلقة بالدليل الجنائي، كما أن هذا التنظيف قد يتلف الأدلة الأخرى، وعلى هذا الأساس لا يجوز تنظيف الجهاز التقني في مسرح الجريمة، واذا وجدت فيروسات على نسخة الاحتياط، يجب توثيقها بحرص، ولا يجب تنظيفها إلا اذا شكلت تهديداً للأدلة.

المبحث الثاني
إجراءات التفتيش في بيئة جرائم تقنية المعلومات

يهدف التفتيش المتصل بجريمة وقعت، إلى كشف الغموض الذي يحيط بها ومرتكبيها، وجمع الأدلة المتعلقة بها، مما يوجب إجراء البحث في أماكن لها حرمة خاصة كالمساكن والمكاتب، وهذ يعني المساس بحقوقهم ولو لفترة قصيرة[١٧].

والتفتيش يعد إجراء من إجراءات التحقيق وفقاً لما هو مستقر فقهاً وقانوناً، ويهدف إلى البحث عن أدلة مادية لفعل مجرم تم ارتكابه في محل يتمتع بحرمة المسكن أو الشخص، وذلك من أجل إثبات ارتكاب هذا الفعل أو نفيه، وفقاً للإجراءات القانونية المقررة[١٨].

ومن أجل صحة الإذن بالتفتيش يتطلب توفر شروط للتفتيش، وقد جاء النص على معظم تلك الشروط في المادة (٨٠) من قانون الإجراءات الجزائية العماني، فالشروط الموضوعية تتعلق:

أ. **صدوره من جهة الاختصاص:** صدور الإذن بالتفتيش من الادعاء العام.

ب. **أن يكون الإذن مسببا:** وجوب وجود سبب أو مبرر لإصداره.

---

[١٧] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١١م، ص١٤٩.

[١٨] د. مزهر جعفر عبيد، الوسيط في شرح قانون الإجراءات الجزائية العماني، دار الثقافة للنشر والتوزيع ،عمّان، ٢٠١٥م، ص٤٦٢.

ج. **الغاية منه:** ضبط أشياء تفيد في كشف الحقيقة.

وللتفتيش شروط شكلية نصت عليها التشريعات الإجرائية المختلفة وأهم هذه الشروط:

أ. أن يكون إذن التفتيش مكتوباً، وأن يتم بحضور الشخص.

ب. أن يُجرى خلال مدة معينة.

لذلك فإن التفتيش يهدف للبحث عن الأدلة التي ترتبط بالجريمة مدار التحقيق، لذلك فهو يخضع أثناء القيام به إلى أحكام القانون، سواء من حيث أمر إصداره، وأسبابه، ومحله، واسم الشخص الذي سيتم تفتيشه، أم تفتيش مسكنه.

ويعد التفتيش وفقاً لهذا الوصف إجراءً من إجراءات التحقيق التي تتطلب أوامر قضائية، سواء من الادعاء العام أم من المحكمة المختصة، كيفما يكون الحال لمباشرته، لاسيما أن عمليات التفتيش بوجه عام تتصل بالمشروعية الإجرائية وقانونية الإجراء، وتتعلق بحقوق الأفراد وضمانات الدفاع، ويقف في مقدمة تحدياتها قواعد الخصوصية، وحق الأفراد في حماية حياتهم الخاصة، وعدم التجاوز على حرياتهم من قبل سلطات التحري والتحقيق.

وجرائم تقنية المعلومات تثير تحديات بشأن الإطار القانوني الملائم لإجراءات التفتيش والضبط، التي تباشرها سلطات الضبط والتحقيق المكلفة بتقصي الجرائم وإحالة الجناة للقضاء، حيث إن هذا الإطار يغاير أُطر التفتيش والضبط المتصلة بالجرائم التقليدية، ففي نطاق جرائم تقنية المعلومات يختلف الأمر، ومرد ذلك الاختلاف يرجع إلى أن تقنية المعلومات تنطوي على حالات مختلفة من حيث ظروفها وأحوالها، وتتطلب لإجراء التفتيش تقنيات خاصة، تُغاير حالات التفتيش للموجودات التقليدية، فبالنسبة إلى تفتيش نظم المعلومات قد لا يكون النظام محل التفتيش مملوكاً للمشتبه به، وليس ثمة وسيلة ميسرة لمعرفة ذلك، كما أن ملفات الأجهزة المعلوماتية قد تكون مخبأة أو محمية، وقد تنقل حول العالم من نظام إلى آخر في زمن قصير للغاية، كما أنه يسهل إتلافها، أو تعطيلها أيضاً في زمن وجيز، مما يتسبب بعرقلة إنجاز التفتيش، كما أن الدليل نفسه قد يصعب تحديد مكانه إبتداء، فقد يكون داخل النظام، أو محفوظاً في وسائط خارجية، وقد يكون الدليل موجوداً في جزء من الشبكة لا يرتبط بالمشتبه به مباشرة، لكنه يستخدم هذا الموقع لإخفاء الأدلة، أو لاستخدامه كمدخل إلى النظام المستهدف بالاعتداء، وربما

كانت الملفات مشفرة، ولا يظهر محتواها إلا بفك التشفير، وقد تكون البيانات التي أثبتت حصول الفعل المجرم جزء من نظام يقع خارج حدود الدولة، وقد يباشر الجاني نشاطه الإجرامي من جهاز لا يخصه، أو من جهاز محمول يسهل التخلص منه، أو إنكار ملكيته، ولكل ما ذكر فإن تحديد السبب الموجب للتفتيش قد يكون أمراً صعباً، ويجعل من تقديم وصف محدد لمحل التفتيش أمراً أكثر صعوبة.

وعليه فإننا نستنبط إن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة تُفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس، ومع ذلك يمكن أن يتم التفتيش على هذه البيانات غير المحسوسة، عن طريق الوسائط الإلكترونية بحفظها، وتخزينها في الأقراص الصلبة، والأقراص الممغنطة، أو مخرجات الأجهزة الأخرى.

ولهذا فقد أجازت التشريعات التي صدرت في مجال الجرائم المعلوماتية، إمكانية أن يكون محل التفتيش للبيانات المعالجة آلياً، والمخزنة بوسائل التقنية أجهزة تم ضبطها، والتحفظ عليها، أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات[١٩]؛ ولذلك فإن هذا النوع من التفتيش يعد إجراء يسمح بجمع الأدلة المخزنة، أو المسجلة بشكل إلكتروني- لاسيما وإن التفتيش - أو البحث في الشبكات الإلكترونية يُجيز استخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة، مع مراعاة كون التفتيش يتضمن تقييداً للحرية الفردية، ويمثل اعتداء على حرمة الحياة الخاصة؛ فيجب أن تتوفر فيه الضمانات والضوابط القانونية لصحته.

أما فيما يخص محل التفتيش، وما يتبعه من ضبط الأدلة الإلكترونية في مجال الجرائم المعلوماتية، فإنه يشمل البرامج، والكيانات المنطقية، والبيانات المسجلة في ذاكرة الحاسب أو في مخرجاته، واحتواء السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات، والسجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات سر، ومفاتيح الدخول ومفاتيح فك الشفرة، كما يشمل أيضاً ضبط المكونات المادية للنظام من أجهزة وخلافه؛ ونظراً

---

[١٩] د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبي، أبريل ٢٠٠٣م.

لكون محل الضبط في الجرائم المعلوماتية البيانات المعالجة إلكترونياً فقد ثار التساؤل: هل يصلح هذا النوع من البيانات لكونه محلاً للضبط الذي يعني وضع اليد على شيء مادي ملموس؟ فقد رأى جانب من الفقه إن بيانات الحاسب لا تصلح أن تكون محلاً للضبط؛ لإنتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي، أو نقلها إلى دعامة مادية، أو غيرها من الوسائل المادية، ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة[٢٠].

إلا أن هناك وجهة نظر أخرى تُفيد بإن البيانات المعالجة إلكترونياً ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية تقبل التسجيل، والحفظ، والتخزين على وسائط مادية، وبالإمكان نقلها، وبثها، واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره، ومن ثم يتبنى الباحثان وجهة النظر هذه بصلاحية البيانات المعالجة إلكترونياً كمحلاً للضبط.

الأحكام المقررة لخضوع مكونات أجهزة تقنية المعلومات للتفتيش:

أن التفتيش المتعلق بأجهزة تقنية المعلومات يتخذ ذات التعريف الذي أشرنا إليه سلفاً، والمتمثل في أنه إجراء من إجراءات التحقيق، يهدف إلى البحث عن أدلة مادية لفعل مجرم، تم ارتكابه في محل يتمتع بحرمة المسكن أو الشخص؛ وذلك من أجل إثبات ارتكاب هذا الفعل، أو نفيه، وفقاً للإجراءات القانونية المقررة، إلا أن محل التفتيش في إطار الجريمة المعلوماتية يقع على وسائل تقنية المعلومات بكياناتها المادية، والمعنوية، أو الجرائم والأفعال التي تتم بواسطتها[٢١].

وحتى لا تتعرض حريات الأشخاص وحرمة مساكنهم لأي انتهاك، أو تجاوز عند التفتيش لضبط أدلة الجريمة، أو فعل مجرم قد وقع، فإن هناك مجموعة من الضوابط يلزم مراعاتها عند اتخاذ إجراء التفتيش، تتمثل في محل تفتيش نظام الجهاز التقني وسبب هذا التفتيش.

---

[٢٠] د. عوض محمد، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، الأسكندرية، ١٩٩٩م، ص٤٢١.

[٢١] خالد الحلبي، مرجع سابق، ص١٥١.

شروط صحة الإذن بتفتيش أجهزة تقنية المعلومات

أولاً- سبب التفتيش:

الشرط الأول لصحة الإذن بتفتيش أجهزة ووسائط تقنية المعلومات هو أن يكون هنالك سبباً لهذا التفتيش، ويتمثل في ارتكاب أفعال معاقب عليها قانوناً، وقعت على هذه الأجهزة أو بواسطتها، وأما دون ذلك فلا محل للتفتيش، وقد ورد النص على هذه الأفعال غير المشروعة والمجرمة في قانون مكافحة جرائم تقنية المعلومات، وفي المادة (٥٢) من قانون المعاملات الإلكترونية، ومنها:

- **التسبب العمدي وغير المشروع في تعديل غير مرخص به في محتويات الجهاز:** ويشمل الإدخال، والإتلاف، والمحو، أو طمس البيانات، أو برامج الحاسب الآلي.
- **التزوير المعلوماتي:** ويتضمن الإدخال، الإتلاف، المحو، أو الطمس لبيانات، أو برامج الحاسب.
- **الإضرار ببيانات وبرامج الأجهزة التقنية:** ويشمل المحو، الإتلاف، التعطيل، أو الطمس غير المشروع لبيانات وبرامج المعلوماتية.
- **تخريب الأجهزة التقنية:** وتشمل الإدخال، الإتلاف، المحو، أو الطمس لبيانات وبرامج الجهاز التقني.
- **دخول بطريق الغش إلى نظام معلومات أو قاعدة بيانات:** وهو الدخول غير المشروع لنظام معلوماتي، أو مجموعة نظم.
- **اختراق أو اعتراض معلومات أو بيانات:** وهو اعتراض غير مصرح به، ويتم بدون وجه حق عن طريق استخدام وسائل فنية للاتصال[٢٢].

كما أنها جاءت ضمن توصيات المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي انعقد (ريو دي جانيرو) بالبرازيل في عام (١٩٩٤م)، وهذه القائمة من الأفعال غير المشروعة تمثل الحد الأدنى لما يجب تجريمه والعقاب عليه، ومع التطور الهائل في وسائط التقنية، وما يصاحب ذلك من استغلال هذه الوسائط في القيام بأفعال مجرمة، فأننا نرى ضرورة أن تواكب القوانيين الوطنية هذا

---

[٢٢] د. هلالي عبد الله ، تفتيش نظم الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٧م، ص٨٤ .

التطور؛ لضمان تجريم جميع الأفعال التي تشكل جرائم، حتى لا يفلت أي مجرم من العقاب، أو تضيع الحقوق.

ومعيار إصدار الأمر بالبحث والتفتيش في جرائم المعلوماتية، هو أن الأدلة التي تم جمعها حول الجريمة يُعتقد بشكل معقول أنها حدثت، سواء كانت الأدلة تستند إلى فاعل أصلي، أم أن دوره الإجرامي يقف عند الاشتراك، ويُترك تقييم هذه الأدلة لسلطة الادعاء العام التي يصدر هذا الأمر، شريطة أن يكون تقييمه واقعيا، ومتسقًا مع الحقائق والوقائع، حيث تكشف هذه الأدلة عن خطورة الجريمة التي بموجبها هو اصدر الأمر بالتفتيش، وأن هناك مجرم ينسب إليها، والمنطق المجرد غير المعقول لا يكفي لدحض المصداقية عن الأدلة التي تبرر التعدي على حريات الأشخاص، ولكن يجب أن يكون تقييم هذه الإمارات معقولاً ومتسقاً مع القواعد والمفاهيم العامة، حيث تشير الأدلة الكافية في مجال جرائم تقنية المعلومات إلى مجموعة من المظاهر والمؤشرات التي من المرجح وفقاً للسياق العقلي المنطقي، أن ترتكب وتنسب إلى شخص معين، سواء كان فاعلا أم شريكاً.

فالإذن بالتفتيش الذي يقع على أجهزة تقنية المعلومات، قد يصدر لجمع أدلة عن جرائم تكون قد وقعت على:

أ. البرنامج أو الكيان المنطقي، أو نظام التشغيل، أو النظم المساعدة الفرعية، أو النظم والبرامج المساعدة أياً كان شكلها، أو دعاماتها المادية، أو وعائها.

ب. المستندات التي تكون متعلقة بهذا البرنامج، أو الكيان المنطقي.

ج. البيانات التي تستخدم عن طريق البرنامج، أو الكيان المنطقي بما في ذلك البيانات المعدة للتسجيل.

د. البيانات المسجلة في ذاكرة الأجهزة التقنية، أو في مخرجاتها، أياً كانت أشكالها، أو دعاماتها، أو وعائها.

هـ. السجلات التي تستخدم في نظام المعالجة الآلية للبيانات، أياً كان شكل هذه السجلات، أو الدعامة المادية التي تجسدها.

و. السجلات الخاصة بعمليات دخول نظم المعالجة الآلية للبيانات كسجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة، أياً كان شكلها، أو دعاماتها، أو وعائها.

وحيث إن الجرائم التي تقع على أجهزة تقنية المعلومات لها طبيعة فنية، فإنه يمكن الاستعانة بأصحاب التخصص، والخبراء، والفنيين في هذا المجال، وبناءً على ذلك فإن الإذن بالتفتيش لا يكون صحيحاً إلا إذا:

أ. كان محدداً من حيث المحل الذي يرد عليه التفتيش.

ب. الأشياء المراد البحث عنها لضبطها.

ج. وجود دلائل جدية ومعقولة ترجح وقوع الجريمة الصادر بشأنها.

وقد أكد قانون الإجراءات الجزائية العماني على وجود المبررات والدلائل الكافية – كأحد المبررات لإصدار الإذن بالتفتيش – وذلك في المادة (٨٠) بتأكيده بأنه لا يجوز تفتيش المساكن، إلا بناء على إذن من الإدعاء العام، إذا ما وُجدت قرائن تدل على أن الشخص المقيم بالمسكن حائز على أشياء تتعلق بالجريمة.

وهو ما ذهب إليه قانون الإجراءات الجنائية الأمريكي، حيث عبّر عن الدلائل الكافية بمفهوم السبب المعقول أو المحتمل، وأكد على ذلك أيضاً التعديل الرابع للدستور الأمريكي، فبيّن بأنه لا يجوز إصدار أوامر القبض، أو التفتيش مالم تكن معتمدة على سبب معقول[٢٣].

وبالنسبة إلى الأفعال التي تُشكل جرائم، وتقع على أجهزة تقنية المعلومات، فإن الأمر بالتفتيش يصدر لضبط الأدلة التي تثبت ارتكابها، أو مرتبطة بها، ويقصد بالدلائل الكافية بالنسبة لها العلامات المستفادة من ظاهر الحال، وهي مجموعة المظاهر، والأمارات التي تكفي وفقاً للسياق العقلي، والمنطقي أن ترجح ارتكابها، ونسبتها إلى شخص معين، سواء أكان وصفه فاعلاً لها أم شريكاً[٢٤].

وإذا كان الغرض من أمر التفتيش هو جمع أدلة عن جريمة قد تكون وقعت على أجهزة تقنية المعلومات أو من خلالها، فمن الضروري أن تكشف هذه الأدلة، والقرائن القوية عن وجود أجهزة، أو وسائط مفيدة في الوصول للحقيقة بالنسبة إلى المتهم، وترجح ارتكاب الجريمة، مثل وجود الأدوات التي استخدمت لارتكاب

---

[٢٣] د. على محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبى، أبريل ٢٠٠٣م.

[٢٤] د. هلالي عبد الله، تفتيش نظم الحاسب الآلي دار النهضة العربية، القاهرة، ١٩٩٧م، ص٧٤، ود. على حمودة، مرجع سابق.

الجريمة، أو للاستيلاء على الأشياء التي تم الحصول عليها، أو وثائق إلكترونية، أو دعائم مفيدة تساعد في الكشف عن الجريمة.

ثانياً- محل تفتيش نظم تقنية المعلومات:

ويشمل التفتيش في أنظمة وأجهزة ووسائط تقنية المعلومات بجميع مكوناتها المادية والمعنوية، ويمكن أن يشمل أيضاً الشبكات الخاصة، والأشخاص الذين يستخدمون هذه الوسائط، خاصة وأنها أجهزة ذات مكونات مختلفة، تتطلب مجموعة من الأشخاص ذوي التخصص، والخبرة في مجال تقنية المعلومات، وهم مشغلو الأجهزة وخبراء البرمجة، سواء كانوا من مخططي برامج التطبيقات أم المحللين، كما تشمل فنيي الصيانة، والاتصالات ومديري نظم المعلومات، والمكونات المادية لنظم تقنية المعلومات، التي يتم تفتيشها تتضمن وحدة الإدخال، ووحدة الذاكرة الرئيسة، ووحدة التحكم، ووحدة الإخراج، ووحدة الحساب والمنطق، ووحدات التخزين الثانوية والوسائط الأخرى، وأما المكونات المعنوية فهي برامج النظام والتطبيق[٢٥].

ثالثاً- شروط صحة الإذن بتفتيش نظم تقنية المعلومات:

لاشك أن تحديد محل التفتيش تحديداً دقيقاً بالنسبة إلى جرائم تقنية المعلومات قد تكتنفه بعض الصعوبات، فتحديد كل أو بعض مكونات أجهزة تقنية المعلومات، وإيرادها في إذن التفتيش تحديداً دقيقاً، قد يستلزم ثقافة فنية عالية في تقنية المعلومات، لاسيما وإن الجرائم التي تقع في أجهزة تقنية المعلومات، أو بواسطتها تتميز بطبيعة فنية متأثرة في ذلك بالطبيعة الفنية لتقنية المعلومات؛ لذلك فقد أوصى التقرير العام لمؤتمر الجمعية الدولية لقانون العقوبات عام (١٩٩٤م) بضرورة وجود خبير معالجة بيانات، يُساعد في صياغة مسودة إذن التفتيش بحيث تتم تغطية كافة عمليات التفتيش، ووصف البنود التي يراد ضبطها[٢٦].

ويشترط في الإذن بالتفتيش الصادر بالنسبة إلى جرائم تقنية المعلومات التي تقع عليها أو بواسطتها:

١. أن يكون مكتوباً، ومحدداً التاريخ، وموقعاً ممن أصدره.

٢. أن يكون صريحاً في الدلالة على التفويض في مباشرة التفتيش.

---

[٢٥] د. هلالي عبد الله، تفتيش نظم الحاسب الآلي، مرجع سابق، ص١٢٥.

[٢٦] مؤتمر الجمعية الدولية لقانون العقوبات الذي عُقد في ريو دي جانيرو البرازيل، ١٩٩٤م.

٣. أن يتضمن البيانات التي تحدد بصورة قاطعة، وواضحة نوع الجريمة المطلوب جمع الأدلة عنها.
٤. يجب أن يتم تحديد محل التفتيش الذي قد يكون شخصاً، أو مكاناً، وتحديد المدة الزمنية الكافية لتنفيذه.

ونُشير إلى أنه يجب أن يكون إذن التفتيش مستكملاً بذاته شروط صحته، ومقومات وجوده كورقة رسمية، فلا يقبل تكملة من نقص فيه من بيانات جوهرية لاحقاً، ويبطل أي دليل غير مستمد منه بأي طريق من طرق الإثبات.

ومن شروط صحة الإذن بالتفتيش في الجرائم المعلوماتية:

١. أن يكون من صدر له الإذن بالتفتيش من المختصين وظيفياً ومكانياً ونوعياً.
٢. توفر الخبرة الفنية فيمن يقوم بتنفيذ أمر التفتيش في جرائم تقنية المعلومات، حتى تتم المحافظة على سلامة الأدلة المتحصلة من الجريمة المعلوماتية.
٣. يشترط في من أصدر الإذن بالتفتيش في جرائم تقنية المعلومات أن يكون مختصاً.

ويتحدد هذا الاختصاص بمحل الواقعة، أو المكان الذي ضبط فيه الجاني، أو بمحل إقامته، ويجوز أن تمتد بعض الإجراءات خارج هذا الاختصاص، إذا تطلبت ظروف وملابسات التحقيق، ذلك شريطة أن يكون المحقق قد بدأ إجراءات التحقيق بدائرة اختصاصه المكاني.

المبحث الثالث

مدى صلاحية مكونات جرائم تقنية المعلومات للتفتيش عن الأدلة

المقصود بالتفتيش عن الأدلة الرقمية هنا هو: التفتيش عن معطيات الأجهزة غير المادية والمخزنة بالجهاز، أو المخزنة في الوسائط الإلكترونية، كما يقصد بالتفتيش في هذه الحالة هو: البحث في النظم المعلوماتية عبر الشبكات الالكترونية للحصول على شئ يتصل بالجريمة المعلوماتية، ويتضح مما سبق بيانه أن المعطيات غير المادية للحاسوب وأجهزة التقنية الأخرى تخضع للتفتيش؛ لأنها عبارة عن ذبذبات إلكترونية قابلة للتخزين في الجهاز، أو التخزين في الوسائط

الإلكترونية، أما المعطيات المادية المخزنة على الجهاز، أو الوسائط فهي أشياء محسوسة، وبالتالي فهي تخضع للتفتيش ويمكن ضبطها[٢٧].

وإذا كان الأمر يبدو مقبولا من الناحية النظرية، إلا أن ضبط مكونات الجهاز التقني المعنوية بعد تفتيشها غير ممكنة، إلا إذا حولت إلى كيانات مادية، عن طريق مخرجات الطباعة المختلفة للجهاز، كنقلها على الورق، أو على أقراص، أو تسجيلها على دعامة أخرى، وبذلك يمكن ضبط الجهاز بكامله كدليل على الجريمة.

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي، يساعد في إثبات الجريمة، فإن البعض قد تشكك في مدى صلاحية البحث عن أدلة الجريمة في الكيانات المعنوية للأجهزة التقنية والحاسبات الآلية[٢٨]، وهو ما حدا ببعض التشريعات بأن تنص صراحة على أن التفتيش يشمل جميع أنظمة المعلومات[٢٩]، ومثال ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر في عام (١٩٩٠م) حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي[٣٠]، وهناك تشريعات أخرى قد أجازت تفتيش أي (شيء) أو اتخاذ أي إجراء يكون لازماً لجمع أدلة الجريمة[٣١]، ومنها المشرع العماني حيث نصت الفقرة الأخيرة من المادة (٨٠) من قانون الإجراءات الجزائية العمانى بأنه: "... ويكون التفتيش وضبط الأشياء والأوراق على النحو المبين بهذا القانون، ويتم البحث عن الأشياء والأوراق المطلوب ضبطها في المسكن وملحقاته ومحتوياته..."، حيث يتضح من هذا النص بأن التفتيش يتضمن المحل، أو المسكن ذاته، وجميع ملحقاته، وما يحتوي من الأشياء كالآلات والأجهزة والأوراق، ويجب التقيد بأن يتلاءم التفتيش مع طبيعة المادة المراد العثور عليها، ومنها وسائط وأجهزة تقنية المعلومات، وعلى ضوء ذلك فإن تفتيش المكونات المعنوية لأجهزة تقنية المعلومات يدخل في عداد الأشياء التي

---

[٢٧] خالد عياد الحلبي، مرجع سابق، ص١٥٧.

[٢٨] د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، ٢٠١٣م، ص٣٨.

[٢٩] د. على محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، مرجع سابق.

[30] Wasik (Martin), Computer crimes and other crimes against information Technology In The U. K., R.I.D.B. 1993, p.78.

[٣١] د. مزهر جعفر عبيد ، مرجع سابق، ص٤٧٨.

جاء النص عليها عاماً دون تقييد، ولقد نظر الفقه في الكثير من دول العالم إلى مصطلح الأشياء التي ترد عليها جرائم الاعتداء على المال نظرة واقعية، بحيث أن هذا المصطلح لا يجب أن يظل جامداً عند معناه الحرفي، وإنما لابد أن يكون متضمناً لكل ما يصلح أن يكون من جنسه.

فالشيء يكون محلاً للحماية الجزائية بالنظر إلى القيمة التي يتمتع بها، والتي قد تتمثل في منفعة مالية أو اقتصادية، قد يحصل عليها صاحبه من ورائه لا فرق في ذلك بين الأشياء المادية، والأشياء المعنوية، بل أن بعض الأشياء المعنوية قد تكون لها قيمة اقتصادية، تعلو بكثير على الأشياء المادية: كالأسرار التجارية والصناعية.

وتفسير مصطلح الأشياء في حالة الأشياء المادية قد يصطدم مع المذهب السائد اليوم في تفسير النصوص الجزائية، والذي لا يعتمد على التفسير الحرفي للفظ فقط، وإنما يعتمد وبشكل أوسع على مذهب التفسير المنطقي، والذي يطبق إذا كان النص محل التفسير غامضاً، أو خافياً في المعنى المقصود منه.

فإذا كان التفسير المنطقي يتم بدراسة رمز معين يعبر عن حقيقة موضوعية وفنية، وذلك بقصد الوصول إلى تلك الحقيقة[٣٢]، فتوصل الباحثان أنه وعلى ضوء هذه الحقيقة يمكن تفسير مصطلح الأشياء وفقاً لمعناها، وحقيقتها، وبما يتفق مع قصد المشرع من تجريم صور الاعتداء عليها بأنها كل ما يعود بفائدة، ويحقق مصلحة لصاحبه، لا فرق في ذلك بين كيانها المادي أو المعنوي، وأنه يلزم لانضباط التفسير بالنسبة إلى النص الجزائي إقامة علاقة بين المعنى العام المجرد للقاعدة الجزائية، لغاية الوصول إلى المعنى الحقيقي الذي يكمن في مضمونها لتطبيقه عليها.

ويترتب على ذلك أنه يتصور وقوع جرائم الاعتداء على المال على الكيانات المعنوية: كالسرقة، وخيانة الأمانة، والاحتيال، والإبتزاز، والنصب، وأيضاً جرائم التخريب، والإتلاف حيث يمكن أن تقع هذه الجريمة الأخيرة على البرنامج أو

---

[٣٢] د. مأمون سلامة، حدود سلطة القاضي في تطبيق القانون، دار الفكر العربي، القاهرة، ١٩٩٠م، ص٥١.

الدعامة المسجل عليها أو عليهما معاً، وقد تقع كذلك عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد.

وقد أشار بعض الفقهاء في فرنسا إلى أن وسائط التقنية وبرامج الحاسبات الآلية ذات كيان مادي ملموس، باعتبارها نبضات وإشارات وذبذبات إلكترونية مغناطيسية، أو كهرومغناطيسية[٣٣] – ومن وجهة نظر الباحثان التأكيد بإمكانية تسجيلها وحفظها وتخزينها على وسائط مادية – وأيضاً نقلها وبثها واستقبالها وإعادة إنتاجها؛ فوجودها المادي لا يمكن إنكاره، ويمكن ملاحظة أن الكثير من الدول الأوروبية تمد سريان النصوص الخاصة بجرائم خيانة الأمانة والاستيلاء غير المشروع للتطبيق على الأسرار التجارية والصناعية، وذلك إذا شكل الاعتداء عليها حالة من حالات التجسس المعلوماتي.

وفى ضوء هذه الآراء الفقهية وعلى النحو الذي قننته بعض التشريعات صراحة في نصوصها[٣٤]، فإن التفتيش كإجراء من إجراءات التحقيق يمكن أن يرد على الكيانات المعنوية في أجهزة تقنية المعلومات، بحسبان أن هذه الكيانات المعنوية وإن كانت غير مادية، إلا أنها تنطبق عليها السمات، أو الخصائص المادية، ومن ثم فيمكن أن تدخل في نطاق الأشياء المادية، ويترتب على ذلك أنه يمكن تفتيش نظام معلومات أجهزة التقنية كالحواسيب، ووسائط وأوعية حفظ وتخزين البيانات المعالجة إلكترونياً: كالأسطوانات، والأقراص، والأشرطة الممغنطة، ومخرجات الحاسب، ويدخل في هذا التفتيش أيضاً المحتويات المخزنة في الوحدة المركزية للنظام، والتي يمكن عزلها ككيان قائم بذاته.

---

[٣٣] د. على محمود حمودة، مرجع سابق.

[٣٤] كمثال لهذه التشريعات المادة ٢٥١ من قانون الإجراءات الجنائية اليوناني التي تجيز لسلطة التحقيق ان تتخذ أي اجراء أو شيء يكون لازماً لجمع الدليل، ويفسر الفقه اليوناني عبارة أي شيء بأنها تشمل جميع بيانات الحاسب الآلي المادية والمعنوية. وعلى هذا النهج نجد المادة ٤٨٧ من القانون الجنائي الكندي تعطى للسلطة المختصة الحق في إصدار الإذن بضبط أي شيء ويفسر الفقه عبارة أي شيء بانها تشمل المكونات المادية والمعنوية للحاسب.

مدى خضوع شبكات التقنية المتصلة للتفتيش

إن شبكات أجهزة تقنية المعلومات هي عبارة عن مجموعة مكونة من اثنين أو أكثر من الأجهزة، والمتصلة ببعضها اتصالاً سلكياً أو لا سلكياً، وهناك شبكات واسعة في أماكن متفرقة، ترتبط ببعضها البعض من خلال هذه الشبكات، سواء داخل الإطار الوطني أم خارجه[٣٥].

فعند وقوع جريمة في نظم المعلومات داخل الإطار الوطني، فيجوز للإدعاء العام إصدار أمر تفتيش، ومن ثم فإن إصدار هذا الأمر وفقاً لما ما هو منصوص عليه في قانون الإجراءات الجزائية، لا يتم إلا بالنسبة إلى الجهاز الذي صدر له التفتيش المأذون به، مما يعني أنه إذا كان الجهاز الذي سيتم تفتيشه متصلاً بجهاز آخر لم يصدر له أمر تفتيش، فلا يجوز أن يمتد التفتيش إليه، حتى لو كان يحتوي على أجزاء من متعلقات الجريمة، وفي هذه الحالة يجب أن يصدر أمر تفتيش جديد من قبل الإدعاء العام.

بينما أكدت بعض التشريعات المقارنة على جواز أن يمتد التفتيش إلى جهاز أو نطام معلومات في مكان آخر حتى ولو كان مملوكا لشخص غير المتهم، ومنها المشرع الألماني وفقاً للمادة (١٠٣) من قانون الإجراءات الجنائية، وكذلك الحال بالنسبة إلى المشرع الهولندي حيث نص مشروع قانون الحاسوب بأنه يجوز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر، شريطة أن تكوم البيانات الخاصة ضرورية لإظهار الحقيقة مع مراعاة بعض الضوابط والقيود المنصوص عليها.

إلا أنه قد تتصل هذه الأجهزة بأجهزة أخرى خارج الإطار الوطني، وعندها تكون هذه الأجهزة خارج نطاق الاختصاص القضائي الوطني، وبالتالي يتعذر الوصول إليها، وفي هذه الحالة قد يكون بالفعل يستحيل تفتيش أنظمة هذه الأجهزة؛ لأنه سيصطدم مع سيادة كل دولة على ترابها الوطني قضائيا، وقد لا يتم ذلك إلا من خلال إبرام اتفاقيات خاصة للتعاون القضائي بين الدول تختص بهذ الشأن، ومع ذلك فقد أجازات بعض القوانيين مثل مشروع قانون جرائم شبكات الحاسوب

---

[٣٥] خالد عياد الحلبي، مرجع سابق، ص١٦٣.

الهولندي، أن يمتد التفتيش إلى الأجهزة المرتبطة حتى وإن كانت موجودة في دولة أخرى، بشرط أن يكون هذا التدخل مؤقتا وضرورياً لإظهار الحقيقة.

ولا يجوز تفتيش أجهزة تقنية المعلومات مثل جهاز الحاسوب الشخصي، إذا كان بحوزة شخص، حيث أنها تأخذ حكم الشخص ذاته ، فلا يجوز لسلطة التحقيق تفتيشها، إلا إذا كان تفتيش الشخص جائزاً، حيث إن تفتيشه يشمل جسمه وكل ما كان بحوزته وقت البحث، سواء كان مملوكاً له أم لأي شخص آخر[٣٦].

وفي حالة وجود الجهاز المعلوماتي المراد تفتيشه داخل منزل، فتطبق ذات القيود المنصوص عليها قانونا في أحوال تفتيش المنازل في الجرائم التقليدية، وذات الضمانات المنصوص عليها لهذا النوع من التفتيش، سواء كان تفتيشاً لمنزل المتهم، أم تفتيشاً لمنزل شخص آخر.

وعند خضوع مكونات نظم تقنية المعلومات للتفتيش في إطار جرائم تقنية المعلومات، والأفعال الجنائية المجرمة المرتكبة، فإن الأمر يختلف عن تلك الحالات التي تصنف كجريمة تقليدية، ومرد ذلك إبتداء يرجع إلى أن تقنية المعلومات تنطوي على حالات مختلفة من حيث ظروفها وأحوالها، وتتطلب لإجراء التفتيش تقنيات خاصة، تُغاير حالات التفتيش للموجودات التقليدية، ذلك أن جرائم تقنية المعلومات تتمثل في طوائف، وهي جريمة الدخول غير المصرح به إلى النظام، وجريمة الدخول غير المصرح به لتسهيل ارتكاب جريمة أخرى، وجريمة إجراء التعديل والتغيير غير المصرح به لنظام تقنية المعلومات.

فبالنسبة إلى النوع الأول نرى أن التفتيش لا يتم إلا بناءً على أمر من سلطة مختصة، يستند إلى أسباب معقولة، ومنطقية تدفع للاعتقاد بوجود أدلة في المكان الخاص، يُمكن العثور عليها بشأن جريمة، أو فعل مجرم قد ارتكب، تتطلب صدور الأمر بالتفتيش من الجهة المختصة، والتشدد في شروطه ضرورة لأهمية الالتزام بحرية الأفراد، وحقوقهم في الوصول للمعلومات في إطار حماية حياتهم الخاصة.

أما في حالات الدخول غير المصرح به لتسهيل ارتكاب جريمة أخرى، أو في حالات إجراء التعديل، والتغيير غير المصرح به لنظام تقنية المعلومات؛ فإننا نرى ضرورة أن يتم التفتيش، والقبض على المتهم بسرعة، بعد الحصول على الأذونات

---

[٣٦] المستشار أحمد محمود خليل، مرجع سابق، ص١٨٠.

اللازمة، وذلك للحيلولة دون اكتمال نشاطه، وتحقيق غايته الإجرامية؛ وذلك مرده إلى خطورة هذه الأفعال المجرمة، وضرورة وسرعة التحقيق وإجراءات الملاحقة، فالنوع الأول الدخول غير المصرح به إلى النظام، فليس بالضرورة أن يعكس حالة لفعل مجرم، يشكل خطورة، إذ ربما يكون الدخول غير المصرح لا يلحق أي ضرر بالنظام، ولا يعكس خطورة تستدعي سرعة الوصول قبل إخفاء الفعل.

مدى التزام وإلزام المتهم أو غيره بالبوح بأسرار الدخول على وسائل تقنية المعلومات:

تفرض بعض التشريعات المقارنة التزاما قانونياً بالإدلاء، وبالإفصاح عن الشفرات، وكلمات السر، أو المرور التي تلزم للدخول لنظم المعلومات، وذلك من خلال التزام الشخص المعني، سواء المتهم أم الشاهد بالإجابة على الأسئلة التي تتعلق بها، ويقع عليهم واجب التعاون في طبع واستنساخ ما قد تستلزمه مصلحة التحقيق من ملفات بيانات مخزنة في ذاكرة الحاسب[٣٧].

فالمشرع الإجرائي الفرنسي مثلا، يُلزم الشهود الذين يقع عليهم التزام قانوني بأداء الشهادة بالكشف عن الشفرات، وكلمات السر للحواسيب، وأجهزة تقنية المعلومات، ولا يعفيهم من هذا الالتزام إلا التمسك باحترام السر المهني[٣٨].

مدى مشروعية إلزام المتهم الصادر قبله إذن التفتيش بالبوح بأسرار الدخول على وسائل تقنية المعلومات:

تكريساً لحقوق المتهم وحفظا لكرامته، فإنه يتمتع خلال مراحل الإجراءات الجزائية بالحماية القانونية المقررة له بموجب مبدأ افتراض براءته، إلى أن يثبت خلاف ذلك بموجب حكم جزائي بات صادر ضده، مما يعني أنه لا يجوز إجباره على تقديم أدلة يدين بها نفسه، بل له الحق في التزام الصمت ما لم تكن كلماته دفاعاً عنه، ويجب ألا يفسر صمته على أنه إقرار بصحة التهمة الموجهة إليه[٣٩]، لذلك نجد المادة (١٨٩) من قانون الإجراءات الجزائية العماني تؤكد على أنه: "لا يجوز

---

[٣٧] د. علي حمودة، الأدلة المتحصل عليها من الوسائل الالكترونية، مرجع سابق، ص٢٨١.

[٣٨] د. هلالي عبد الله، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٢٣.

[٣٩] انظر المواد ١٨٨ و ١٨٩ من قانون الاجراءات الجزائية العماني.

تحليف المتهم اليمين، ولا إكراهه، أو إغرائه على الإجابة، أو إبداء أقوال معينة بأية وسيلة من الوسائل، ولا يفسر سلوك المتهم أو امتناعه عن الإجابة بأنه إقرار بشيء، ويترتب على ذلك أنه لا يجوز إجبار المتهم على كشف مفاتيح الدخول إلى نظم تقنية المعلومات، أو طباعة ملفات بيانات مخزنة داخل هذه النظم"[٤٠].

إلزام أشخاص آخرين لم يصدر قبلهم الإذن بالتفتيش بالبوح بأسرار الدخول إلى الوسائل الإلكترونية:

وفقاً لمعنى الشهادة كدليل إثبات في المواد الجزائية، والتي يقصد بها المعلومات الصادرة من الشهود الذين عاصروا الجريمة لحظة وقوعها، أو جمعوا أدلة لإثباتها، فأن الأشخاص الذين يتعاملون مع أجهزة تقنية المعلومات بحكم طبيعة عملهم لا يعدون شهوداً وفقاً لهذا المدلول.

والشاهد في الجرائم الواقعة في محيط أجهزة تقنية المعلومات يُشار إليه على أنه من ذوي الخبرة، والمتخصصين في تكنولوجيا أجهزة التقنية الذي لديه المعلومات الأساسية اللازمة لدخول نظام معالجة البيانات الآلي، إذا كانت خدمة التحقيق تتطلب استكشاف الأدلة عن الجريمة في الداخل، وهؤلاء الشهود هم مشغلي الأجهزة، وخبراء البرمجة، ومحللي نظم المعلومات، ومهندسي الصيانة، وغيرهم من طاقم تكنولوجيا المعلومات.

وبناء على ذلك نستنتج إن الشاهد في جرائم تقنية المعلومات ملزم بالكشف عن كلمات المرور، والرموز، والشفرات التي بها أوامر لتنفيذ البرامج المختلفة، كما يتعين عليه أن يطبع البيانات المخزنة في ذاكرة أجهزة التقنية، أو ناقلات البيانات، أو غيرها من وسائل الحفظ والتسجيل الإلكترونية.

ونخلص إلى أن إجراءات تفتيش أجهزة تقنية المعلومات تتطلب وسائل تقنية، وتكتيكاً تقنياً، وقد تباينت وجهات النظر الفقهية، والقانونية حول مشروعية التنصت والمراقبة الإلكترونية، ومشروعية وسائلها التي تتزايد في بيئة الشبكات المعلوماتية.

والحقيقة أن هذا التباين في الرأي الفقهي والقانوني حول مشروعية التنصت والمراقبة الإلكترونية، ليست من المسائل الجديدة على القانون، وإن كانت وسائلها

---

[٤٠] د. علي حسن الطوالبه، أبحاث في جرائم تقنية المعلومات، دار الكتب والدراسات العربية، الإسكندريه، ٢٠١٨م، ص٨١.

الجديدة أثارت بعض المسائل المرتبطة في الغالب بطبيعة الوسيلة، وجوانب الرقابة الإجرائية وعلى الرغم من أن هذه المسائل قد ووجهت بالمعارضة الكبيرة لتعرضها لحقوق وحريات الأفراد، ومساسها بخصوصياتهم، فإن النظم القانونية، وفي ضوء اعتبارات المكافحة اتجهت إلى إقرار صحة وسائل الرقابة، والتنصت ضمن قيود معينة غالباً ما تكون مما يوصف بالقيود المتشددة، ويكون أثر عدم مراعاتها بطلان الأدلة المتحصلة منها، ونلاحظ إن قوانين مختلف الدول تجيز الرقابة الهاتفية، والالتقاط عن بعد للاتصالات[٤١]، وفي تطورات حديثة أجازت بعض التشريعات اعتراض البيانات، ومتابعة حركة المرور للمعطيات، شريطة حصول جهات التحقيق على إذن مسبق من جهات الاختصاص على هذا الإجراء، وتحت شرط أن يكون محدداً بوقت وبغرض معين، وعلى نظام بعينه مع توفر السبب المعقول والمنطقي لهذا الإجراء، حيث نجد المادة (٥) من قانون تنظيم الاتصالات العماني تنص على أنه "يحظر مراقبة وسائل الاتصالات ومضمونها، أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها أو اعتراضها، إلا بإذن مسبق من المحكمة المختصة، ما لم تنطو على إخلال بالنظام العام، أو الآداب العامة، أو اعتداء على حقوق الآخرين، وذلك مع عدم الإخلال بقانون الإجراءات الجزائية"، كما حظرت المادة (٩٠) من قانون الإجراءات الجزائية العماني تسجيل الأحاديث التي تجري في مكان خاص، أو مراقبة الهاتف، أو تسجيل المكالمات بغير إذن من الإدعاء العام.

وأما بشأن التنصت على الشبكات الدولية والمراقبة الهاتفية، فقد أصدرت بعض الدول قوانين تجيز عمليات التنصت والرقابة الهاتفية، متذرعة بمكافحة الإرهاب، وخاصة بعد عام (٢٠١١م)، ومنها النظام القانوني البريطاني الذي أجاز تشريعات تتيح الرقابة، والملاحظة، والقبض، والتفتيش دون الخضوع للمبادئ والأحكام القانونية التي أستقرت بموجب الاتفاقية الأوروبية لحقوق الإنسان، ومبادئ وتوجهات الإتحاد الأوروبي[٤٢]، وفي الولايات المتحدة الأمريكية فقد أصدر

---

[٤١] عبدالله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، المركز القومي للاصدارات القانونية، القاهرة،٢٠١٧م، ص١٥١.

[٤٢] خالد عياد الحلبي، مرجع سابق، ص١٦٦.

الكونجرس وعلى خلفية أحداث ١١/سبتمبر/٢٠٠١ وما تبعها من خطط أمريكية لمكافحة ما أطلق عليه الإرهاب، أصدر تشريعاً يرفع الكثير من القيود على عمليات التنصت والرقابة الهاتفية، ومراقبة الشبكة العالمية للمعلومات، والبريد الإلكتروني، خاصة بعد ما أثاره المحققون من أن الشبكة العالمية للمعلومات، والبريد الإلكتروني كانا الواسطة التي أتاحت للجهة التي قامت بتنفيذ الهجمات على برجي مركز التجارة العالمي والبنتاجون[٤٣]، وعلى الرغم من أن القانون المذكور قد وصف من العديد بأنه انكفاءه على الحقوق، والحريات الفردية، وإهداراً لمبادئ الخصوصية التي جاهد الشعب الأمريكي في تكريسها، إلا أنه حظي بالمقابل بقبول جماعي، خاصة مع حقيقة أنه قانون يسري لفترة محددة، تقرر أن تكون لسنة واحدة يعاد بعدها تقييم مدى سلامة الاستمرارية له[٤٤]، ويمثل السبب الرئيس الأول لقبول هذا التشريع رغماً عن تعارضه مع حقوق وحريات الأفراد، أنه تشريع موجه لغير المواطن الأمريكي مما يجعل الكثير من الأمريكيين مقتنعين أنه لا يطالهم من أحكامه ضرر، مع أن الواقع العملي لن يكون كذلك.

كما أن المشرع الفرنسي قد أجاز في القانون الصادر في١٠/ يوليو/١٩٩١م اعتراض الاتصالات البعدية، بما في ذلك شبكات تبادل المعلومات[٤٥]، كما أقر القانون في هولندا لقاضي التحقيق في أن يأمر بالتنصت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة متورط فيها المتهم، وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات[٤٦].

إن الحاجة إلى التنظيم التشريعي لجوانب التفتيش، والضبط في مجال جرائم تقنية المعلومات، ووسائل حماية البيانات الشخصية أيضاً، تجد منطقاً موضوعياً في

---

[٤٣] المحامي يونس عرب، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، الأردن، ٢٠٠٢م، ص٥١٨.

[٤٤] استمر العمل بذات القانون لفترات أخرى بذريعة استمرار التهديدات التي تمس الأمن القومي الأمريكي.

[٤٥] د. عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبي، أبريل ٢٠٠٣م.

[٤٦] د. عبد الله حسين علي محمود، مرجع سابق.

الحاجة إلى توفير معيار مقبول، يقيم توازناً بين حقوق وحريات الأفراد، وحماية خصوصياتهم، وبين موجبات المكافحة، وحاجتها إلى قواعد استثنائية فرضتها تحديات هذه الجرائم، التي تزيد عن تحديات غيرها من الجرائم التقليدية، ففي ظل سرعة إتلاف الدليل، وطبيعة ما يثبت الجريمة ذاتها من الأدلة، وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة، وفي ظل ارتباط مادة الجريمة، أو وسيلتها بأنظمة أطراف أخرى لا صلة لهم بها، أو بشبكات ونظم معلومات خارج الحدود، فإن المكافحة الفاعلة قد تنطوي على إهدار الحقوق وحريات الكثيرين، والتفريط بضمانات المتهم، وما توجبه قرينة البراءة المقررة له، وهذا التناقض لا مجال لفضه، إلا بإقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها، يعد مقبولاً في ضوء مصلحة المجتمع وأمنه، متى ما توفر بحق هذا المبرر، ومتى ما كان المعيار مدركاً أن الاستثناء لا يجوز التوسع فيه، ويتعين تقييده بالقيد التشريعي الواضح، الذي لا يتيح للسلطات التغول بما منحها القانون من حقوق، أو بما تفسره هي وفق رؤيتها لما قرره القانون من صلاحيات لها.

ضوابط تنفيذ تفتيش أنظمة تقنية المعلومات:

من حيث الأصل فإن التحري والتفتيش في بيئة جرائم تقنية المعلومات يتوقف على مدى دقة مذكرة التفتيش ونطاقها المكاني، ويتعين أن يحرص المحققون وجهات الضبط المكلفة بالتفتيش من قبل الجهة المختصة أن تغطي مذكرتهم أي مكان توجد فيه هذه البيانات الإلكترونية في نطاق الاختصاص المكاني.

وبالنظر إلى الشخص أو الجهة التي يدور التفتيش بشأنها، قد يتطلب التحري تفتيش أنظمة معلوماتية عائدة لجهات لا صلة لها بالفعل المجرم ونتيجته، كتفتيش أنظمة خارج الحدود، ولا يمكن أن يقبل قانوناً أن تغطي مذكرة التفتيش أماكن خارج نظام الاختصاص المكاني، لذلك جاءت الحاجة إلى تعاون دولي حقيقي في مجال أنشطة التحري، والتحقيق، والضبط، والتفتيش خارج الحدود.

والتفتيش يتطلب مذكرة قضائية، سواء من المحكمة، أم من الإدعاء العام – كيفما يكون الحال – تجيز تفتيش أجهزة تقنية المعلومات وأنظمتها، حيث إن إجراء التفتيش دون مذكرة من جهة ذات اختصاص، أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه به، فإنها مسائل تثير الكثير من المعارضة،

خاصة في ظل ما رسخ من قواعد تحمي حقوق الأفراد، وتوجب مشروعية الدليل، وسلامة مصدره، وتبطل كل إجراء يتم خلافاً للقواعد والأصول القانونية.

ومن الضروري أن يكون هناك علم ابتداء بوجود الأدلة المتصلة بالجريمة ضمن أحد أجهزة تقنية المعلومات أو أنظمتها، وإن الجريمةً بطبيعتها من الجرائم التي أفرزتها أجهزة تقنية المعلومات؛ لأن مذكرة التفتيش يجب أن تكون واضحة في تحديد النظام محل التفتيش، وإيراد وصف واسع له، وما يفترض أن يتصل ويتعلق به.

أما في الحالة التي يكون فيها الجهاز أو النظام المستهدف من التفتيش، أو مكان وجود الدليل غير محدد في النطاق المكاني لمحل التفتيش، فيجب أن تكون صياغة مذكرة التفتيش عامة قدر الإمكان، بحيث لا يحد نصها من نطاق الضبط والتفتيش.

وحتى تكون هذه الضوابط ذات قيمة، لابد من تدخل المشرع بوضع قواعد إجرائية تنظم إجراءات الضبط والتفتيش لمثل هذا النوع من الجرائم المستحدثة على النحو الذي قررته التشريعات الوطنية، والمقارنة، والمواثيق، والنظم الدولية.

الخاتمة

لقد انتهينا من كتابة هذه الدراسة عن ضوابط التفتيش الجنائي على أنظمة تقنية المعلومات فى ضوء التشريع العماني والمقارن، حيث تم التطرق في المبحث الأول إلى مسرح الجريمة المعلوماتية، ثم تناولنا في المبحث الثاني التفتيش في مجال الجريمة المعلوماتية، ثم خصصنا المبحث الثالث لمدى قابلية مكونات أجهزة تقنية المعلومات للتفتيش.

وتظهر قيمة هذه الدراسة من خلال الأهمية الكبرى للموضوع، لذلك فقد جاءت لوضع صورة عن الجريمة المعلوماتية، ومسرحها، وضوابط التفتيس في مجال هذا النوع من الجرائم، ومدى قابلية مكوناتها للتفتيش، والموقف التشريعي الوطني والمقارن حول الموضوع، وقد أفرزت الدراسة النتائج والتوصيات الآتية:

أولاً- النتائج:

١. تثير الجرائم المعلوماتية بعض الصعوبات في مجال الحصول على الأدلة الرقمية، فسلطات التحقيق اعتادت على كون الإثبات ماديا وملموسا، كما أن الجاني يمكنه ارتكاب الجريمة في دول أخرى، فالجرائم المعلوماتية قد تكون دولية.

٢. التفتيش في الجرائم المعلوماتية يكون للبحث عن الأدلة المادية أو الأدلة المعنوية، وكذلك الضبط ينصب على الكيانات المادية، أو المعطيات الإلكترونية، وعليه لابد من تفتيش الأنظمة المعلوماتية، وما تحتويه من بيانات ومعلومات.

٣. الإجراءات التحقيقية في الجرائم المعلوماتية تتخذ الإجراءات نفسها التي تتم مع الجرائم التقليدية، رغم اختلاف الأدلة في الجرائم المعلوماتية وحساسيتها.

٤. اقتصر المشرع العُماني في قانون مكافحة جرائم تقنية المعلومات على تحديد الجانب الموضوعي لجرائم تقنية المعلومات، دون التطرق للجانب الإجرائي الخاص لهذه الجرائم، وهو بالتالي أحال إلى قانون الإجراءات الجزائية الجانب المتعلق بالشق الاجرائي.

٥. لم يتناول قانون مكافحة جرائم تقنية المعلومات العماني جميع صور الجرائم المعلوماتية.

٦. يتسم التحقيق في الجرائم المعلوماتية بصعوبة وتعقيد بالغين، وعليه لابد للمحقق أو مأمور الضبط القضائي أن يكون ملما كحد أدنى بآلية عمل الأجهزة التقنية ووسائطها، حتى يستطيع التعامل معها، ومن ثم كشف الجرائم المعلوماتية وجمع الأدلة.

٧. على المحقق في الجرائم المعلوماتية القيام بكافة الإجراءات الاحتياطية التي ينبغي عليه اتخاذها في مسرح الجريمة في الجرائم التقليدية، والحرص على اتخاذ التدابير اللازمة أثناء التفتيش أو التحريز أو الحفظ، لحماية الأدلة المعلوماتية من التلف أو المحو أو الضياع أو العبث بها.

٨. لا توجد نصوص خاصة وصريحة في قانون الإجراءات الجزائية، أو قانون مكافحة جرائم تقنية المعلومات تنظم إجراءات تفتيش وسائل تقنية المعلومات والتعامل مع الدليل الرقمي.

ثانياً- التوصيات:

١. نوصي باستحداث نصوص قانونية أو تعديل للنصوص الحالية في القوانين العقابية أو المنظمة تضمن مكافحة الجرائم المعلوماتية بمختلف أنواعها، وتطويعها حسب تطور هذه الجرائم؛ لأنها مستحدثة ومتغيرة ومتطورة بتطور التكنولوجيا والعالم الإفتراضي.

٢. نرى ضرورة تطوير قانون الإجراءات الجزائية لينظم الإجراءات التي تتعلق بالتحري والتحقيق والتفتيش والضبط في الجرائم المعلوماتية، والتعامل مع الأدلة الرقمية.

٣. أهمية العمل على وضع حماية قانونية وجزائية للبيانات والمعلومات الإلكترونية، للحد من وقوعها أهدافاً للمجرمين.

٤. ضرورة استحداث نصوص قانونية جديدة تتعلق بالضمانات التي يجب أن يحاط بها المتهمين في الجرائم المعلوماتية، خاصة أصحاب الأجهزة التقنية التي يتم ضبطها وتفتيشها؛ نظراً لما تحتوي عليه من بيانات ذات طابع شخصي وحساس.

٥. تأهيل رجال الضبط والتحقيق تأهيلاً مناسباً في مجال وسائل التقنية، والوسائط الأخرى والإنترنت، وطرق مكافحة الجرائم المعلوماتية، وكيفية مواجهتها، وتدريبهم على آليات الوصول إلى الأدلة المعلوماتية، وحفظها من التلف أو الضياع تمهيدا لاستخدامها أمام المحاكم المختصة.

٦. النظر في المقررات الدراسية في الكليات الأمنية وكليات الحقوق وضرورة تضمنيها مادة عامة عن الجرائم المعلوماتية والإلكترونية والأمن السيبراني.

٧. نوصي بضرورة تنظيم المزيد من الندوات والمؤتمرات حول العلاقة بين المعلوماتية والقانون وآلية مواجهة هذا النوع من الجرائم على كافة الصعد، والانضمام إلى الاتفاقيات العربية والدولية التي تتعلق بمكافحة الجرائم المعلوماتية.

المراجع

١) أحمد بسيوني ابو الروس، التحقيق الجنائي والأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٩م.

٢) المستشار أحمد محمود خليل، الوسيط في شرح قانون الإجراءات الجزائية العماني، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٧م.

٣) د. جميل الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١م.

٤) د. حسين بن سعيد الغافري، منظومة سلطنة عمان التشريعية لمكافحة جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، ٢٠١١م.

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

٦) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.

٧) د. عبد الله حسين على محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبى، أبريل ٢٠٠٣م.

٨) د. على محمود حمودة، الأدلة المتحصلة من الوسائل الالكترونية، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبى، أبريل ٢٠٠٣م.

٩) د. علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات، دار الكتب والدراسات العربية، الأسكندرية، ٢٠١٨م.

١٠) د. عوض محمد، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٩م.

١١) د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، ٢٠١٣م .

١٢)د. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، ورقة عمل، كلية الشريعة والقانون، جامعة الإمارات، مايو ٢٠٠٠م.
١٣)د. مأمون سلامة، حدود سلطة القاضي في تطبيق القانون، دار الفكر العربي، القاهرة، ١٩٩٠م.
١٤)د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، الجزء الثاني، دار النهضة العربية القاهرة، ٢٠٠١م.
١٥)د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبى، أبريل ٢٠٠٣م.
١٦)د. محمود نجيب حسنى، شرح قانون العقوبات/القسم الثاني (جرائم الاعتداء على الأموال)، الطبعة السادسة، دار النهضة العربية، القاهرة ١٩٨٩م.
١٧)د. مزهر جعفر عبيد ، الوسيط في شرح قانون الإجراءات الجزائية العماني ، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٥م.
١٨)د. ممدوح عبد الحميد عبد المطلب ، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم عبر الحدود، ورقة عمل، المؤتمر العلمي الأول، أكاديمية شرطة دبي، أبريل ٢٠٠٣م.
١٩)د. نسرين محسن نعمة الحسيني و د. محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠م.
٢٠)د. هشام رستم، أصول التحقيق الجنائي الفني للجرائم المعلوماتية، مجلة الأمن والقانون، العدد الثاني، كلية الشرطة بدبي، الإمارات العربية المتحدة، ١٩٩٩.
٢١) د. هلالي عبد الله ، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٠م.
٢٢)د. هلالي عبد الله، تفتيش نظم الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٧م.

٢٣) عبدالله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، المركز القومي للاصدارات القانونية، القاهرة، ٢٠١٧م.
٢٤) علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠م.
٢٥) كمال أحمد الكركي، التحقيق في جرائم الحاسوب، ورقه عمل المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبى، أبريل ٢٠٠٣م.
٢٦) د. عبدالعال الديربي و أ. محمد صالح اسماعيل، الجرائم الالكترونية، المركز القومي للاصدارات القانونية، القاهرة، ٢٠١٢م.
٢٧) المحامي يونس عرب، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، الأردن، ٢٠٠٢م.
28) Wasik (Martin), Computer crimes and other crimes against information Technology In The U. K., R.I.D.B. 1993.