كلية الحقوق
قسم القانون الجنائي

بحث مستخلص من رسالة الدكتوراه بعنوان

إجراءات جمع الأدلة في مجال إثبات جرائم الاعتداء على البرامج الإلكترونية

إعداد الباحث

محمد السيد عبد العزيز الأجاوي

إشـــــراف

أ.د/ أحمد لطفي السيد مرعي

أستاذ القانون الجنائي

كلية الحقوق - جامعة المنصورة

مقدمة

موضوع البحث:

يشهد العالم اليوم تنامياً ملحوظًا لاستعمال الأجهزة الإلكترونية وأدوات التوثيق الحديثة. مما جعل التعامل دون ورق. ولكن إذا كان استعمال التقنيات الحديثة والذي يترك أثراً كتابيًا بالمعنى التقليدي لا يثير في حقيقة الأمر مسائل معقدة، ويجب أن يكون الدليل الإلكتروني متحصلاً من وسائل مشروعة. ويعني مشروعية الدليل الجنائي بما يتضمنه من مخرجات ووسائل إلكترونية ضرورة اتفاق الإجراء مع القواعد القانونية. والأنظمة الثابتة في وجدان المجتمع المتحضر، ويترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها منها تكون باطلة، ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المادة الجنائية.

حيث إن جرائم الاعتداء على البرامج الإلكترونية يصعب حصرها؛ لأن هذه الجرائم تترك أثراً بمعاينته يتم التوصل إلى مرتكبها مثل الجرائم التقليدية التي دائماً تترك أثراً يقود إلى مرتكبها. بالنظر إلى الطبيعة الخاصة التي تتميز بها تلك الجرائم. والطبيعة شديدة الخصوصية التي يتسم بها مرتكبي تلك النوعية من الجرائم. والطبيعة شديدة الخصوصية التي يتسم بها مرتكبي تلك النوعية من الجرائم.

أهمية البحث:

تبدو أهمية هذا البحث جلياً من التطور المتسارع الذي يشهده العالم في ظل الثورة المعلوماتية الحديثة التي تلت الثورة الصناعية والتي فرضت الاعتماد على تقنيات تكنولوجية استعملها الإنسان في مجالات العمل والحياة, فأصبح بذلك العالم عبارة عن قرية صغيرة يمكن التواصل بين مجتمعاته, واستطاعت أن تقدم خدمات جليلة للأمم و الشعوب، إلا أن هذا الجانب الايجابي للتكنولوجيا المعلوماتية أفرز معه بعض الانعكاسات السلبية التي تولدت نتيجة إساءة استخدام الأنظمة المعلوماتية, واستغلالها على نحو غير شرعي قصد الإضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط وصور مستحدثة من الجرائم اصطلح الفقه على تسميتها

بالجرائم المعلوماتية.

إشكالية البحث:

إن الإشكالية الرئيسية للبحث تكمن في صعوبة جمع الأدلة في مجال إثبات جـرائم الاعتـداء على البرامج الإلكترونية، حيث يصعب في كثير من الاحيان العثور على أثـر مـادى للجريـة، والتي لا تكتشف – عادةً – إلا بمحض الصدفة، وكذلك ايقافها، وهذا بالنظر إلى سـرعه نسـخ البرامج الإلكترونية أو إتلافها، وسهولة محو الدليل في زمن قصـير، والتـي تعـد مـن أهـم الصعوبات التي تقترض عمليه الاثبات في محال جرائم الاعتداء علي البرامج الالكترونية؛ حيـث أن من الممكن للجاني محو أدلة الإدانة أو تدميرها في وقت وجيز، كمـا أن هنـاك صـعوبات أخري عملية تتعلق بمدى قابلية المكونات المادية والمعوية للحاسب الإلكتروني للتفتيش، وأيضـا هناك صعوبات جمة لوضع الضوابط الشكلية والموضوعية لعملية التفتيش وكيفيه اجراءها.

منهج البحث:

تعد اجراءات جمع الأدلة من السائل الدقيقة نظراً لأهميتها في إثبات جـرائم الاعتـداء علـى البرامج الالكترونية ، لذا ستكون دراستنا دراسة تحليلية لتلك الإجراءات، وأيضاً مقارنة للتعـرف علي دور جهات التحقيق في الدول محل المقارنة في مرحلة جمع الأدلة لإثبات جرائم الاعتـداء على البرامج الالكترونية.

خطة البحث:

ترتيباً علي ما سبق؛ سنقسم خطة البحث الى أربعه مطالب على النحو التالي:

المطلب الأول: المعاينة التقنية.

المطلب الثاني: تفتيش أنظمة الحاسب الإلكتروني.

المطلب الثالث: الشهادة الإلكترونية.

المطلب الرابع: الخبرة التقنية.

المطلب الأول

المعاينة التقنية لمسرح جرائم الاعتداء

على البرامج الإلكترونية

من المقرر أن الشرعية الإجرائية تقوم على افتراض براءة المتهم في كل إجراء من الإجراءات التي يتخذ قبله منذ البدء في جمع الاستدلالات وحتى استنفاذ طرق الطعن من الأحكام.

فإذا كانت الشرعية الإجرائية هي عماد البنيان الإجرائية على المستوى الجنائي فإن أصل البراءة المقرر للإنسان هو الركن الركين لتلك الشرعية.

ولما كانت إجراء المعاينة هي أحد هذه الإجراءات كان لزاماً أن نعرض لتعريف المعاينة في **(فرع أول)**، ثم كيفية المعاينة لمسرح جريمة الاعتداء على البرامج الإلكترونية **(فرع ثان)**. وذلك على النحو الآتي:

الفرع الأول

تعريف المعاينة التقنية لمسرح جرائم الاعتداء على البرامج الإلكترونية

تنص المادة ٩٠ إجراءات جنائية من القانون المصري على أن: "ينتقل قاضي التحقيق إلى مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديًا وكل ما يلزم إثبات حالته". كما تنص المادة ٩٣ "على قاضي التحقيق كلما رأى ضرورة للانتقال للأمكنة أو للتفتيش أن يخطر بذلك النيابة العامة. وأضافت المادة ١/٣١ من قانون الإجراءات التي تلزم مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة، وألزمته فضلاً عن ذلك أن يخطر النيابة العامة فوراً بانتقاله، ويجب على النيابة العامة بمجرد إخطارها بجناية متلبس بها الانتقال فوراً إلى محل الواقعة.

كما نظم المشرع بالمادة الخامسة من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري، تحديد مأموري الضبط القضائي، بشأن جرائم تقنية المعلومات، بأن أجازت بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين

بالجهاز أو غيرهم من تحددهم جهات الأمن القومي، بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم.

كما نظم المشرع بموجب المادة السادسة من القانون المشار إليه، الأوامر القضائية المؤقتة، حيث قررت أن لجهة التحقيق المختصة- بحسب الأحوال- أن تصدر أمر مسبباً، لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ٣٠ يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى هذا القانون بواحد أو أكثر مما يلي:

١- ضبط أو سحب أو جمع أو التحفظ على بيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي 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 لها مقتضٍ.

٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط.

٣- أن تامر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديهن وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني، وفي كل الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسبباً.

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة، في المواعيد ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية.

ويتضح من النصوص السابقة أن المشرع لم يحدد المقصود بالمعاينة، بل تركها للفقه، حيث عرفها البعض بأنه: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم

لكشف الحقيقة"[1].

والمعاينة في جوهرها يقصد بها إثبات حالة الأشـــخاص والأمكنـــة والأشـــياء ذات الصـــلة بالجريمة، قبل أن تنالها يد العبث والتخريب، والمعاينات لا تعدو إلا أن تكون صورة من صـــور استظهار الحقيقة في واقعة أو جريمة تبلغ أمرها إلي السلطات، وذلك لكشف عناصرها وأركانها وجمع أدلة إثبات كل ما يتعلق بماديات الجريمة، وتمحيصها لاستخلاص المدلولات منها لكشـــف الحقيقة، وإذا كان إجراء المعاينة الذي يوجب بحكم المنطق الانتقال إلى محل الواقعة سريعًا حتى لا يتطرق الشك إلى الدليل المستفاد منها.

ويظل إجراء المعاينة أمراً جوازيًّا لمأمور الضبط القضائي إن شاء أجراه وإن شاء أغفله، إلا أن المادة ٣١ من قانون الإجراءات الجنائية قد أوجبت على مأمور الضبط القضائي فـــي حالـــة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة، ويعاين الآثار المادية للجريمة، ويحـــافظ عليها، ويثبت حالة الأماكن والأشخاص، ويسمع أقوال من كان حاضراً، أو من يمكن الحصـــول منه على إيضاحات في شأن الواقعة ومرتكبها. ويجب عليه أن يُخطر النيابة العامة فوراً بانتقالـــه ويجب على النيابة العامة بمجرد إخطارها بجناية متلبس بها الانتقال فوراً إلى محل الواقعة.

ويلاحظ أن المعاينات التي يقصدها نص المادة ٢٤ إجراءات جنائية هي المعاينات التي يقـــوم بها مأموري الضبط القضائي باعتباره عمل من أعمال الاستدلال، ومن ثم وجب إجرائهـــا فـــي الأماكن العامة التي يباح للجمهور الدخول منها دون تميز، فإذا امتد أثرها إلى المساكن بطلـــت، وبطل ما نجم عنها من أدلة، وذلك أنها تأخذ حكم التفتيش المحظور على مأمور الضبط القضائي إجرائه إلا بإذن صادر من سلطة التحقيق أو رضاء قاطني هذه المساكن[2].

وترتيباً علي ما سبق؛ تُعد المعاينة لأحد إجراءات التحقيق أو الاستدلال، دون النظر إلي صفة

---

(١) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، عام ١٩٨٢، ص٦٥٥.

(٢) د. محمد عيد الغريب، الاختصاص القضائي لمأمور الضبط في الأحوال العادية والاستثنائية، النسر الـــذهبي للطباعة، القاهرة، ٢٠٠٠، ص٤٢.

من يقوم بإجرائها، بل تتوقف على مدى ما يقتضيه إجرائها من مساس بحقوق الأفراد[٣].

ولم يجعل الشارع المعاينة إجراءً وجوبياً يجب علي المحقق القيام به، بل جعل المعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره، سواء طلبها الخصوم أو لم يطلبوها، وإذا طلبها الخصوم فللمحكمة أن تجيب هذا الطلب أو ترفضه إذا قررت عدم جدواه، وهي تلتزم عندئذ بتسبيب هذا الرفض وإلا كان هذا الحكم معيباً. ولا يترتب علي مخالفة هذا الواجب البطلان في الإجراءات، بل مجرد المسئولية الإدارية[٤].

الفرع الثاني

كيفية إجراء المعاينة التقنية لمسرح جرائم الاعتداء على البرامج الإلكترونية

من المسلم به، أن من أهم ما تتميز به جرائم الاعتداء على البرامج الإلكترونية هو وقوعها في بيئة معلوماتية إلكترونية، مما يترتب علي ذلك نتائج جمة من أهمها صعوبة اكتشاف هذه الجرائم وإثباتها، وهذا عكس الجرائم التقليدية. فرجل الشرطة الذي يقوم بجمع التحريات في واقعة ما حتى يصل إلى المتهم، ويستصدر أمراً بالقبض عليه، واستجوابه وإحالته إلى محكمة الموضوع. فكل تلك الوقائع خاضعة لسيطرة أجهزة العدالة، والدليل فيها مرئي ومقروء عكس جريمة الاعتداء على البرامج حيث تتسم تلك الجرائم بأنها غير مرئية في العديد من حالاتها، ولا يلاحظها المجني عليه غالبا أو يدرك حتى بوقوعها، حيث تتم دون رؤية لدليل الإدانة، وحتى في حالة وجود الدليل يمكن للجاني طمس الدليل أو محوه عن طريق التلاعب في البيانات، كما أن أغلب الآثار الناجمة عن هذه الجرائم هي آثار إلكترونية، وهذه الآثار بدورها إنما هي عبارة عن

---

(٣) د. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، ٢٠١٨، ص ٦٩.

(٤) د. سعد أحمد محمود سلامة، مسرح الجريمة، دار النهضة العربية، ٢٠٠٧م، ص ٣٧؛ د. عوض محمد، قانون الإجراءات الجنائية، مؤسسة الثقافة الجامعية، الجزء الأول، ١٩٨٩، ص٤٧.

ذبذبات إلكترونية غير مرئية بالعين المجردة، فهي لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية(٥).

وعند إجراء المعاينة يلتزم من يقوم بها اتباع القواعد التي المعمول به عند إجراءات المحاكمة، مثل إخطار الخصوم بمكان المعاينة وزمانها إن أمكن ذلك(٦).

كما يجب الإسراع في الانتقال للمعاينة. وقد أجازت المادة ١٤٥ من قانون المرافعات المدنية الفرنسي الجديد، إجراء المعاينة عن طريق المحضر أو البير بناءً على طلب الشخص المعني بعد موافقة القاضي المختص بناء على طلب على عريضة خاصة إذا كانت المعاينة تجري في مكان خاص حتى ولو كان مفتوحاً للجمهور مثل مقاهي الإنترنت، ويجب على الطالب أن يقدم تبريراً لطلبه بإجراء المعاينة بأن يقدم ما يفيد أن هناك اعتداء وقع على أحد حقوقه، وأن إثبات الاعتداء أمر ضروري لإقامة الدليل على الدعوى التي سيقوم برفعها، وذلك خشية زوال هذه المعلومات من على الشبكة أو إتلافها(٧).

وفقاً لنص المادة ٢٥٤ من قانون الإجراءات الجنائية الفرنسي تنصب على الأشخاص والأشياء والأماكن، لا يخضع للانتقال لأي قيود، إلا أنه يتعين النزول إلى الأماكن التي ارتكبت بها الجريمة على وجه السرعة، في أعقاب اكتشاف الجريمة، رغم أن القانون لا يحدد أجلاً يتعين الانتقال في خلاله، ويمكن الانتقال إلى الأماكن سواء أثناء التحقيق الابتدائي بواسطة قاضي التحقيق وضباط البوليس القضائي، أو في خلال التحقيق النهائي الذي تجريه المحكمة

---

(5) Bensousson a loin intérêt et respect juridique 2éme éd revue et augmentée, hèmes Paris 1998, p. 192.

(٦) د. توفيق عبد الله أحمد الخشاشنة، معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ٢٠١٦م، ص ٢٣.

(٧) د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠١، ص٢٨؛ د. محمد يوسف جاسم النعيمي، إجراءات التعامل مع مسرح الجريمة الالكترونية في التشريع الإماراتي: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩م، ص ١٠٩.

المختصة[٨].

هذا وقد أجاز المشرع الأمريكي لعضو النيابة العامة أن يعجل بإجراء المعاينة خشية ضياع الأدلة، وذلك بإرسال رسالة إلى مزود خدمة الإنترنت يلزمه فيها بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذ هذا الإجراء أو غيره[٩]. وعلى سلطات التحقيق جمع الاستدلالات أن يتعامل مع مكان وقوع جريمة الاعتداء على البرامج الإلكترونية على أنه يتكون من مكانين أحدهما تقليدي، والآخر افتراضي والأول مثل غيره من أماكن وقوع الجريمة التقليدية يتكون بشكل أساسي من مكونات مادية ملموسة مثل أجهزة الحاسب وشاشاتها وملحقاتها والذي يمكن أن يترك الجاني فيه الكثير من الآثار المادية كبصمات أصابعه أو بعضها من مقتنياته الشخصية، وهو بصورة عامة يقع خارج البيئة الإلكترونية، تنطبق عليه كافة القواعد المتبعة في معاينة مكان وقوع الجريمة التقليدية، أما الثاني فإنه يقع داخل البيئة الإلكترونية وتتكون من بيانات رقمية إلكترونية، موجودة في داخل حواسب أو على شبكة الإنترنت وهو الأمر الذي يتطلب ضرورة الاستعانة بالخبراء نظراً للطابع الفني لأساليب ارتكاب الجريمة أثناء المعاينة.

وإذا كانت المعاينة تتم بالانتقال إلى محل وقوع الجريمة كقاعدة عامة[١٠] إجرائية مقررة في هذا الشأن، إلا أنه في إطار جرائم الإنترنت والخاصة بالاعتداء على البرامج الإلكترونية، فإن الانتقال يعد من الموضوعات الجديدة، وذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي، وإنما من الممكن أن تكون بالضرورة عبر العالم الافتراضي فيستطيع عضو سلطة التحقيق أن يقوم بالمعاينة من مكتبه من خلال الحاسب الآلي الخاص به، كما يمكن أن يلجأ إلى

---

(٨) د. محمد كمال شاهين، الجوانب الاجرائية للجريمة اللكترونية في مرحلة التحقيق الابتدائي: دراسة مقارنة، مرجع سابق، ص ١٣١.

(9) Daniel Morris- Tracking a computer Hacker USA ttomeys bulletin 2/2001, p. 3 available at: www.U.S.Agov/criminal/cybercrimeUSAmay2001/htm.

(١٠) د. خالد حسن أحمد، الأدلة الجنائية الحديثة في إثبات الجريمة الإلكترونية، دار الفكر الجامعي، ٢٠٢٣م، ص ٢٣؛ د. محمد محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراه- أكاديمية الشرطة، كلية الدراسات العليا، القاهرة، ١٩٨٨، ص١٣ وما بعدها.

مقهى الإنترنت أو ينتقل إلى مقر مزود الخدمة الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة، ذلك انه في كل الأحوال يلزم أن يقوم المحقق بالمعاينة من خلال حاسب أو حاسب خادم، وينبغي مراعاة عدة قواعد فنية عند إجراء معاينة مسرح جرائم الاعتداء على البرامج الإلكترونية منها(١١):

١- تصوير جهاز الحاسب الآلي الذي تُرتكب الجرائم عن طريقه، وما يتصل به من أجهزة فرعية ومحتوياته وأوضاع المكان الذي يتواجد به بصفة عامة، مع مراعاة تصوير أجزاءه الخلفية وملحقاته الأخرى، وتدوين زمان ومكان تاريخ التقاط الصور.

٢- إثبات طريقة إعداد النظم والعمليات الإلكترونية، وخاصة ما تحوي عليه من السجلات الإلكترونية التي تزود بها شبكة المعلومات، لمعرفة موقع الاتصال، ونوع الجهاز الذي تم عن طريقة التسجيل علي النظام.

٣- وقف نقل أي مواد أو بيانات معلوماتية متحفظ عليها من موقع الجريمة؛ قبل التيقن من عدم وجود أي مجالات لقوة مغناطيسية بالمحيط الخارجي للحاسب الآلي، يمكن أن تسبب في محو أو إتلاف البيانات المسجلة عليها بسبب تداخل المجالات المغناطيسية مع بعضها البعض.

٤- إثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام كله، لتسهيل إجراء تحليل البيانات وعمل مقارنة لدى عرض الأمر على القضاء.

٥- حفظ الموقع والبيانات المخزنة علي الأجهزة عن طريق:

- استخدام خاصية الحفظ save as المتوفرة في نظام التشغيل، ويترتب عليها بطبيعة الحال حفظ الموقع المخالف الذي سطح على الشاشة.
- تحميل نسخة من البرنامج المقلد Downloading أو طباعتها أو استخراجه في هيئة

---

(١١) د. محمود رجب فتح الله، مسرح الجريمة الإلكترونية: دراسة تطبيقية مقارنة، دار الجامعة الجامعية، الإسكندرية، ٢٠٢١م، ص ٨٣؛ د. خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠٢٠م، ص ٧٥.

مستندات ورقية، أو نسخها على أقراص صلبة أو مرنة.

- التأكد من سلامة الحاسب الآلي أو الحاسب الخادم، بحيث تكون سلطة التحقيق قد احتفظت بما يسمح بالتأكيد على دقة مصدر الدليل الإلكتروني.

٦- التحفظ على الأجهزة وملحقاتها، وحفظ المستندات المتاحة من المخرجات الورقية وشرائط وأقراص ممغنطة، وغيرها من الأشياء التي يعتقد أنها ذات صلة وثيقة بالجريمة.

٧- وجوب اقتصار عملية المعاينة على مأموري الضبط القضائي – سواء من الباحثين أو المحققين – ممن يتوافر فيهم الكفاءة العلمية والخبرة الفنية والتقنية في المجال المعلوماتي، وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم الإلكترونية، وبناء الدليل الرقمي وكيفية التعامل معه وكيفية صياغة عريضة الاتهام قبل تقديمها للمحاكمة، لتوجيه الاتهام بشكل صحيح، وهو ما يتطلب نيابة متخصصة حتى لا ينجو المجرم بفعلته.

٨- وضع حرس ذوو كفاءة فنية وتقنية على كل جهاز حتى لا يتمكن أحد المتهمين أو معاونيه من إتلاف البيانات المخزنة عليه، من على بعد أو من جهاز آخر داخلي.

المطلب الثاني

تفتيش أنظمة الحاسب الإلكتروني

تتزايد أهمية التفتيش في نظم الإجراءات الجنائية الحديثة لكونه يعد أقوى الأساليب الجنائية المقررة لمكافحة تصاعد الإجرام وتطوراته الحديثة، وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبرراً في القانون لإجرائه، وكونه من الإجراءات الخطرة فإن المشرع قننه ليكون في ضمانة سلطات التحقيق التي يقع على عاتقها التزام تكثيف استخدام الضمانات لصالح المتهم فإن تهاونت في القيام بالمحافظة على هذه الضمانات حق على عملها البطلان[١].

(١) د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية،ـ دراسة تحليلية، دار الكتب القانونية، ٢٠١١م، =

ولقد عرفت محكمة النقض المصرية التفتيش في أحد أحكامها – التفتيش كما هو معروف في القانون – هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق تحت إشراف محكمة الموضوع وإذ كانت المحكمة قد اقتنعت بتوافر مسوغات إصدار هذا الأمر فلا يجوز المجادلة في ذلك أمام محكمة النقض، كما أنه ذلك الإجراء الذي رخص به الشارع فيه التعرض لحرمة الشخص بسبب جريمة وقعت أو ترجح وقوعها منه، ذلك تغليباً للمصلحة العامة على مصالح الأفراد الخاصة واحتمال الوصول إلى دليل مادي يكشف الحقيقة(١).

ونتيجة للثورة التكنولوجية الحديثة أمكن الاعتداء على البرامج الإلكترونية عبر شبكات الحاسب الآلي والإنترنت. وهنا يثار التساؤل بمدى قابلية شبكات الحاسب الآلي المستخدمة في ارتكاب تلك الجرائم للتفتيش وما هي ضوابط هذا التفتيش؟ وما النتائج المترتبة على هذا التفتيش؟ ولذا سنقسم هذا المطلب إلى:

الفرع الأول: مدى قابلية مكونات وشبكات الحاسب للتفتيش.

الفرع الثاني: ضوابط تفتيش نظم الحساب الآلي.

الفرع الثالث: النتائج المترتبة على تفتيش نظم الحاسب الآلي.

الفرع الأول

مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

إن الولوج غير القانوني إلى شبكات الحاسب الآلي عبر أنظمتها المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة قد يتشكل جريمة ، ويعد التفتيش إجراء من إجراءات التحقيق تقتضيه مصلحة وظروف التحقيق بُغية كشف الحقيقة ومعرفة مرتكبها،

= ٢٠١١م، ص ٢٦؛ د. علي عدنان الفيل، اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية،٢٠١٢م، ص ٦٢.

(١) حكم محكمة النقض – جنائي – أحكام غير منشورة، الطعن رقم ١٣٤٤٨ لسنة ٩١ ق، بتاريخ ٢٤ مايو ٢٠٢٣.

https://www.eastlaws.com/data/ahkam/details/1365369/4638135

فالتفتيش إجراء جائز قانوناً – ولو لم ينص عليه صراحة – باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه[١].

وتتفرع مكونات نظم الحاسب الآلي من مكونات مادية Hardware ومكونات منطقية software، كما أنه تربطه بغيره من الحسابات شبكات اتصال بعدية على المستوى المحلي أو الدولي[٢]، لذا فقد ثار التساؤل الخاص بمدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش على النحو التالي:

أولاً: مدى قابلية مكونات الحاسب الإلكتروني المادية المستخدمة في جرائم الاعتداء على البرامج الإلكترونية للتفتيش:

رغم أنه لا يمكن اخضاع مكونات الحاسوب من برامج وبيانات علمية للتفتيش والضبط التقليدية، إلا أنه مما لا شك فيه؛ أن فحص المكونات المادية للحاسب الإلكتروني بحثًا عن شيء علي صلة وثيقة بجريمة الاعتداء على البرامج الإلكترونية، يساهم في إظهار الحقيقة وكشف مرتكبها، ويخضع هذا الفحص للإجراءات القانونية الخاصة بالتفتيش، حيث أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة وخصوصية المكان الموجودة فيه تلك المكونات، وهل هي من الأماكن العامة أم الخاصة[٣].

---

(١) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوطن ١٩٩٤، ص٥٧؛ د. حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، دار النهضة العربية، ٢٠٠٩م، ص ١٠٩.

(٢) د. عادل حامد بشير، الاثبات الجنائي للجريمة الالكترونية، دار النهضة العربية، ٢٠١٩، ص ٥١؛ د. محمد فهمي طلبة، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة ١٩٩١، مطابع الكتب المصري الحديث، ١٩٩٢، ص١٠.

(٣) د. أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات – كلية الحقوق, المجلد الثامن, العدد الثاني، ٣٠ يونيو ٢٠٢٢م، ص ١ – ٥٣؛ د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص ٣٤.

وتبرز الأهمية القصوى لصفة وطبيعة مكان المكونات المادية خاصة في مجال التفتيش، فإذا كان الحاسب الإلكتروني موجود في مكان خاص، كمسكن المتهم أو أحد ملحقاته، فإنه يأخذ حكم تفتيش المسكن بنفس الضمانات والإجراءات المقررة قانوناً، فلا يجوز تفتيش مكوناته إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم، ولابد الأخذ في الاعتبار مراعاة ما إذا كانت مكونات الحاسب الإلكتروني المراد تفتيشها متصلة بحاسبات أخرى في مكان آخر كمسكن غير المتهم مثلاً، أم منعزلة عن غيرها من الحاسبات الإلكترونية(١).

وهذا ما ذهبت غليه العديد من التشريعات المقارنة، حيث تجيز تفتيش مكونات الحاسب الإلكتروني المادية، مثل المادة ٢٥١ من قانون الإجراءات الجنائية اليوناني(٢)، والمادة ٤٨٧ من قانون الإجراءات الجنائية الكندي(٣)، والقانون الإنجليزي الصادر في ٢٩ يونيه سنة ١٩٩٠ والذي يطلق عليه قانون إساءة استخدام الحاسب computer Misuse Act(٤)، وكذلك هناك بعض القوانين التي تتضمن قواعد تفصيلية للتفتيش تطبق على مكونات الحاسب مثل القسم رقم ١/١٦ من قانون المنافسة في كندا فهذا القسم يزود الشخص الذي يحمل إذناً للتفتيش إمكانية أن يستخدم أو يعمل على استخدام أي نظام معلوماتي، لتفتيش أي مكون مادي.

ثانياً: مدى قابلية مكونات الحاسب الإلكتروني المنطقية المستخدمة في جرائم الاعتداء على البرامج الإلكترونية للتفتيش:

لقد ثار الخلاف بشأن جواز تفتيش مكونات الحاسب الإلكتروني المنطقية، حيث يذهب بعض الفقه القانوني أنه إذا كانت غاية التفتيش هو ضبط الأدلة المادية التي تساهم في كشف الحقيقة،

---

(١) د. ممدوح عبد الحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية; ٢٠٠٦، ص ٥٨.

(2) Vassilaki (Irini): "computer crimes and other crimes against information Technology in Greece "R.I.D.P. 1993, p. 371.

(3) Piragoff (Domald D.): computer crimes and Other crimes against information technology in Canada "R.I.D.P. 1993, p. 241.

(4) Ferbrache (Davide) pathology of computer viruses springer- verlag London LTD. 1992, p. 233.

فإن التفتيش يمتد ليشمل البيانات الإلكترونية بمختلف صورها[١].

وقد ذهب إلي هذا الاتجاه قانون الإجراءات الجنائي اليوناني، حيث تعطي المادة ٢٥١ منه سلطات التحقيق إمكانية القيام بكل ما تراه ضرورياً لجمع الأدلة وحمايتها، ويفسر ذلك الفقه اليوناني بأن التفتيش يشمل بالفحص والتتبع والضبط البيانات المخزنة أو المعالجة إلكترونيًا، حيث أن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الإلكتروني لا تعد مشكلة في اليونان، إذ بإمكان سلطة التحقيق أن تعطي أمراً للخبير بجمع البيانات التي قد تكون مقبولة كدليل في المحاكمة الجنائية[٢]، بينما ذهبت المادة ٤٨٧ من القانون الجنائي الكندي إلي أنه لابد من صدور إذن لضبط أي شيء طالما تتوفر براهين معقولة يعتقد معها بأن الجريمة ارتكبت أو يشتبه في ارتكابها، أو أن هناك نية مبيته في استخدامه في ارتكاب الجريمة أو اعتبار نتائجه دليلاً على وقوع الجريمة[٣].

ومما سبق يتضح جلياً أنه يسمح للمحقق تتبع وضبط وفحص بيانات الحاسب غير الملموسة، وعلى النقيض من ذلك يري رأي آخر أنه إذا كانت الغرض من التفتيش هي ضبط الأدلة المادية التي تساهم في كشف الحقيقة، فإن ذلك لا ينطبق على بيانات الحاسب الإلكتروني غير الملموسة، ولمواجهة هذا القصور التشريعي يري هذا الاتجاه حتمية إضافة إلي الهدف التقليدي التفتيش عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي"، وفي ظل التطورات التقنية الحديثة المتلاحقة يضحي الغاية الجديدة من التفتيش هي الفحص والبحث عن الأدلة المادية والمواد المعالجة بواسطة الحاسب [٤].

وفي فرنسا يرى البعض أن الموجات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد

---

(1) John R.Vacca. computer forensics: computer crime scene Investigation- computers- 2005, p. 85.

(2) Vassil Aki (Irini): computer crimes and other crimes against information technology in Greece "R.I.D.P. 1993, p. 355.

(3) http://www.f.law.net/law/archive/index.php/t-1797.

(4) Bruce Middleton, cyber grime investigator's field Guide, op.cit., p. 66.

من قبيل الأشياء الملموسة، وبالتالي لا تعد شيئًا ماديًا بالمعنى المألوف للمصطلح، ولذا لا يمكن ضبطه[1]. وفي المقابل يذهب رأي آخر إلى أنه يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية، وبين طبيعة هذه البرامج والكيانات، فإذا رجعنا لمدلول كلمة المادة في العلوم الطبيعية فهي كل ما يملأ حيزاً ماديًا في فراغ معين، وأنه يمكن قياس هذا الحيز والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزاً ماديًا في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معين، وإنها أيضًا تأخذ شكل موجات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقًا لذلك ذات كيان مادي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية.

ويرى الباحث أن هذه المسألة لا تمثل عقبة تعترض التفتيش البيانات المخزنة إلكترونيًا في القانون المصري، وذلك أن المادة (٩١) من قانون الإجراءات الجنائية سمحت لقاضي التحقيق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة ما يحتمل أنه استعمل في ارتكاب الجريمة، أو نتج عنها، أو وقعت عليه، وكل ما يفيد في كشف الحقيقة، فعبارة "كل ما يفيد في كشف الحقيقة" تفيد بجواز أن يقع التفتيش على أي شيء يفيد في كشف الحقيقة ومن ذلك الأدلة الرقمية أو المعنوية والمتمثلة في البرامج الإلكترونية.

ثالثًا: شبكات الحاسب الآلي ومدى خضوعها للتفتيش:

إن طبيعة البرامج الإلكترونية والقدرة على التواصل عن بعد عبر شبكات الحاسب، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة الحاسب في أماكن مجهولة، فهل يمتد تفتيش الحاسب الآلي إلى الأجهزة المرتبطة به؟ وللإجابة على هذا التساؤل يستلزم الأمر التفرقة بين ثلاث حالات:

الحالة الأولى: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجود في مكان آخر داخل الدولة:

وفي هذه الحالة يثار التساؤل حول مدى إمكانية امتداد السلطة في التفتيش إذا تبين أن

(1) http://www.doha-shares.com/vb/f48/t21952,html.

الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص آخر غير المتهم؟

ذهب الفقه الألماني إلى جواز امتداد حق التفتيش إذا تأكد أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بشخص آخر غير المتهم(١).

ونجد صدي هذا الرأي في المادة ٨٨ من قانون تحقيق الجنايات البلجيكي التي تنص على: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي: أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد مكان آخر غير مكان البحث الأصلي ويتم هذا الامتداد وفقًا لضابطين(٢):

أ – إذا كان ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث.

ب– إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث.

وفي هذا الصدد فقد نصت الفقرة (أ) من المادة ١٧ من القانون الفرنسي رقم ٣٩ لسنة ٢٠٠٣ بشأن الأمن الداخلي الصادر في ١٨ مارس لسنة ٢٠٠٣ بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات، أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي"(٣).

وتسمح الاتفاقية الأوروبية لجرائم الإنترنت لعام ٢٠٠١ للدول الأعضاء أن تمد نطاق التفتيش لجهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به

---

(1) http://www.qataru.com/vb/showthread.php.pt20845.

(٢) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، دبي، الإمارات العربية المتحدة، في الفترة من ٢٦– ٢٠٠٣/٢٨م، ص١٠.

(3) Loi 18 Mars 2003 pour la sécurité intérieure Article 17 www.legifrance. Govfarias pad'un texte degor? Numjo 21/6/2003.

معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش فتنص المادة ١٩ من القسم الرابع على أنه: "من حق السلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال عبر نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من خلال الكمبيوتر الأصلي محل التفتيش.

الحالة الثانية: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة:

تثار هذه الإشكالية عندما يتعمد معتادي الجرائم على البرامج الإلكترونية علي تخزين بياناتهم علي حواسب الكترونية خارج الدولة مستخدمين في ذلك شبكة الاتصالات والانترنت بُغية عرقلة التحقيقات، حيث يمتد التفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي للدولة الأخرى، وهو ما يسمى بالولوج أو التفتيش عبر الحدود، ولذلك تسمح بعض التشريعات المقارنة بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، فقد أجازت المادة ١٧ فقرة (٢) من قانون الأمن الداخلي الفرنسي السالف الذكر لمأموري الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[1].

وقد أجاز المجلس الأوروبي من خلال توصي رقم ١٣ لسنة ١٩٩٥ المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات من التفتيش الالكتروني للحاسب إلى الشبكة المتصلة به ولو كانت تلك الشبكة واقعة في إقليم دولة أخرى، وأكد على أنّه يجوز لسلطة التحقيق والاستدلال بمناسبة التفتيش الإلكتروني بسط مجال تفتيش حاسب معين يدخل في دائرة اختصاصها إلى غيرها من الأجهزة الإلكترونية المرتبطة به بواسطة شبكة الإنترنت بما فيها المتواجدة خارج الاختصاص الوطني وضبط المعطيات المتواجدة فيها، كلما كان التدخل

(1) Loi 18 Mars 2003 pour la sécurité intérieur article 1712 www.legifrancegouv.fr/wAspd/untext/degorf/Nunjo=21/6/2003.

الفوري للقيام بذلك ضرورياً[١].

ولابد أن يتم التتبع والفحص والتفتيش الإلكتروني العابر للحدود داخل إطار اتفاقيات دولية خاصة تعقد بين الدول المعنية وتجيز هذا الامتداد، وبالتالي لا يجوز التتبع والفحص والتفتيش العابر للحدود في غياب تلك الاتفاقيات، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المعلوماتية[٢].

ومع ذلك فقد أجازت المادة ٣٢ من اتفاقية بودابست ٢٠٠١ إمكانية الدخول بغرض التتبع والفحص والتفتيش في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى: إذا تعلق التتبع والفحص والتفتيش بمعلومات أو بيانات مباحة للجمهور، والثانية: إذا وافق صاحب أو حائز هذه البيانات بهذا التفتيش[٣].

الحالة الثالثة: التصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي:

حيث إن التصنت والمراقبة الإلكترونية – رغم إنها مثيرة للجدل – إلا أنه مسموح – في بعض الدول – بها تحت ظروف معينة، فيجيز القانون الفرنسي الصادر في ١٩٩١/٧/١٠ اعتراض الاتصالات البعدية، وفرض الرقابة عليها، بما في ذلك شبكات تبادل المعلومات[٤].

وقد أجاز القانون الهولندي بناء علي أمر أو إذن من قاضي التحقيق إجراء التنصت على

---

(١) د. أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة، مرجع سابق، ص ١ – ٥٣.

(٢) د. محمد أبو العلا عقيدة، مرجع سابق، ص٢٠، ٢١.

(٣) تنص المادة ٣٢ من الاتفاقية: يجوز للدولة الطرف في الاتفاقية، وبدون تفويض من دولة أخرى طرف بالاتفاقية أ – الدخول علناً وبشكل متاح على بيانات الكمبيوتر المخزنة بغض النظر عن مكان تواجد البيانات جغرافيّا، أو ب– الدخول على، أو تلقي عن طريق منظومة كمبيوتر بأراضيها بيانات الكمبيوتر المخزنة الموجودة بدولة أخرى طرفاً بالاتفاقية وذلك في حالة حصول الدولة الطرف على الموافقة القانونية والطوعية من الشخص الذي له حق التفويض قانونًا في الكشف عن البيانات للدولة الطرف بالاتفاقية من خلال منظومة الكمبيوتر هذه.

(4) Francillon (Jacques): “Les crimes informatique set d’autres crimes dans le domaino de la technologie in formatique en France “R.I.D.P. 1993, p. 309.

شبكة الحاسوب الآلي، متى ثبت أن المتهم كان ضالعًا في جرائم خطيرة، ويشمل ذلك كل وسائل الاتصال بما في ذلك التلكس والفاكس ونقل البيانات، وكان القضاء الياباني قد أجاز هذا الإجراء بالرغم من أن القانون هناك لم ينص على السماح به بشكل صريح، تجلى ذلك فيما انتهت إلى محكمة مقاطعة Kofu سنة ١٩٩١، غذ أقرت مشروعية التنصت على شبكات الحاسب الآلي في سبيل البحث عن الدليل(١).

وقد ذهب المشرع المصري لهذا الاتجاه بالنص في المادة (١١) من الباب الثاني من قانون مكافحة جرائم تقنية المعلومات، بشأن الأدلة الرقمية في جرائم تقنية المعلومات، تحت إطار الأحكام والقواعد الإجرائية، حيث تضمنت هذه المادة على أن: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية.

وفي إسرائيل يقترح مشروع قانون الحاسبات شمول تعريف التنصت والمراقبة الإلكترونية ليشمل استقبال المعلومات بواسطة اتصال الحاسبات الآلية(٢) وفي فنلندا اشترط صدور إذن من القاضي المختص(٣).

---

(١) د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٨، ص ٩٢؛ د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي- دراسة مقارنة، ص٧٩-٨٠.

(2) Leder Man (Eli) and Shapira (Ron): "computer crime and other crimes against information technology in Israel "R.I.D.P. 1993. P. 421.

(3) Pihl. Ajamaki (Ant). "computer crime and other crimes against information technology in Finland R.I.D.R.P. 1993, p. 286.

الفرع الثاني

ضوابط تفتيش نظم الحاسب الآلي

في جرائم الاعتداء على البرامج الإلكترونية

يُعد التفتيش أحد مظاهر التي تقيد الحريات الأساسية للإنسان، والتي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها، كذا أجاز المشرع خرق الخصوصية لدى الأشخاص من خلال بعض الإجراءات منها التفتيش، وفق قواعد شكلية وموضوعية أوضحتها أغلب التشريعات وأثبتها أحكام المحاكم[1]، وعلى ذلك يمكن تقسيم الضوابط العامة لتفتيش نظم الحاسب الآلي إلى ضوابط موضوعية وأخرى شكلية على النحو الآتي:

أولاً: الضوابط الموضوعية لتفتيش نظم الحاسب الآلي المستخدم في جرائم الاعتداء على البرامج الإلكترونية:

يمكن حصر تلك الضوابط في عدة شروط هي:

١- سبب التفتيش:

يشترط لمباشرة إجراء التفتيش على جرائم الاعتداء على البرامج الإلكترونية أن يكون التفتيش مشروعًا بأن نكون بصدد جريمة واقعة بالفعل، سواء أكانت جناية أو جنحة، ثم لابد من اتهام شخص أو أشخاص معنيين بارتكاب هذه الجريمة أو المشاركة في ارتكابها، وأخيراً لابد من توافر أمارات ودلالات قوية أو قرائن على وجود أجهزة أو أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم ونتناول ذلك في النقاط الآتية:

---

(١) د. ممدوح عبد الحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٦م، ص ٥١؛ د. علي حسن محمد الطوالية، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ٢٠١٠م، ص٥٣.

أ – وقوع جريمة من جرائم الاعتداء على البرامج الإلكترونية:

يلزم للتفتيش حتى يكون صحيحاً أن يتعلق بجريمة وقعت بالفعل وليست جريمة مستقبلة، وهذا أمر منطقي، إذ إن الدعوى الجنائية تترتب علي تواجد الجريمة أصلاً، ولا أهمية بعد ذلك أن يتعلق الأمر بجناية أو جنحة تامة وقعت بالفعل أو لم تكتمل ووقفت عند حد الشروع، والجريمة المتعلقة الاعتداء على البرامج الإلكترونية يرتبط ارتباطًا وثيقة بتحقيق أغراض غير مشروعة، وقد نص المشرع المصري على هذه الجرائم في المادة ١٨١ من القانون رقم ٨٢ لسنة ٢٠٠٢ والخاص بحماية الملكية الفكرية(١)، وكذلك في المادة ١٧ من القانون رقم ١٧٥ لسنة ٢٠١٨ والخاص بمكافحة جرائم تقنية المعلومات(٢)، مثل الإضرار ببرامج الحاسب من إتلاف أو محو أو تخريب، ويمكن الرجوع إليها لعدم التكرار.

ب– اتهام شخص أو أشخاص معينين بارتكاب جرائم الاعتداء على البرامج الإلكترونية:

يجب لإجراء التفتيش أن تتوافر دلائل قوية وكافية، إما على توجيه اتهام شخص معين بارتكابها، وإما على حيازته لأشياء تتعلق بها حتى يمكن تفتيشه، سواء بصفته فاعلاً أصليًا لها، أو شريكًا فيها، ولا يلزم أن تكون هناك جريمة قد وقعت للحديث بجواز التفتيش(٣).

ج– توافر أمارات ودلالات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم:

لا يتم الإذن بالتفتيش إلا إذا توافرت لدى المحققين أسباب كافية على أنه يوجد لدى الشخص

---

(١) راجع نص المادة ١٨١ من قانون حماية حقوق الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ منشور بالجريدة الرسمية بالعدد ٢٢ مكرر ٢ يونيه ٢٠٠٢.

(٢) راجع نص المادة ١٧ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ منشور بالجريدة الرسمية العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.

(٣) د. علي عدنان الفيل، اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية،٢٠١٢م، ص ٥٦؛ د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، ٢٠٠٩؛ ص ٨٨؛ د. هلال عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي "دراسة مقارنة"، دار النهضة العربية، ٢٠٠٦، ص١١٥ وما بعدها.

– المراد تفتيشه أو المكان المراد تفتيشه – أدوات ومواد استعملت في الجريمة أو أشياء متحصلة منها، أو أية مستندات إلكترونية يحتمل أن يكون لها الأثر في استجلاء وكشف الحقيقة، وتقدير كفاية تلك الدلائل، موكول لسلطة التحقيق تحت رقابة محكمة الموضوع.

٢– محل التفتيش الخاص بنظم الحاسب الآلي المستخدم في جرائم الاعتداء على البرامج الإلكترونية:

يُعد محل التفيش هو كل مكونات البرامج الإلكترونية المادية أو المعنوية، أو الشبكات المتصل بها، بالإضافة إلى الأشخاص المالكين لتلك البرامج، أو الأماكن التي تحويها، والشخص بوصفه محلاً لتفتيش نظم الحاسب الآلي قد يكون من مشغلي أو مستخدمي الحاسب الآلي أو من خبراء البرامج، سواء أكانت برامج تشغيل أم برامج تطبيق، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حارس آلي(١).

ويُقصد بالمنازل وما في حكمها كمحل لتفتيش نظم الحاسب الآلي المستخدم في جرائم الاعتداء على البرامج الإلكترونية كافة محل الإقامة والملحقات المخصصة لشغلها، سواء بصفة دائمة أو مؤقتة، وسواء كانت ثابتة أم متنقلة متى ما وجدت فيها مكونات الحاسب الآلي أو شبكات اتصال خاصة.

وإذا ما كان المكان محدداً، ولم يكن هناك حظر على تفتيشه، كان لسلطة التحقيق أن تجري التفتيش، أو يأمر به في أي مكان يتعلق بالشخص المراد تفتيش مسكنه، وقد نص على ذلك المشرع في الفقرة الأخيرة من المادة ٩١ إجراءات جنائية، حيث ورد بها أن للمحقق أن يفتش أي مكان، ويضبط فيه الأوراق، والأسلحة، والآلات وكل ما يفيد في كشف الحقيقة.

٣– السلطة المختصة بتفتيش نظم الحاسب الآلي المستخدمة في جرائم الاعتداء على البرامج الإلكترونية:

حدد المشرع المصري هذه السلطة للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات

---

(١) د. محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠٠٥م، ص ١٦٢.

خاصة ويتميز قاضي التحقيق عن النيابة العامة في سلطته في تفتيش غير المتهم، سواء في شخصه (المادة ٩٤. إ.ج) أو منزله (المادة ٩٣. إ.ج)، أما النيابة العامة فلا تملك ذلك بمفردها، بل يجب عليها لاتخاذ هذا الإجراء الحصول مقدماً على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق ولا يتولى مأمور الضبط القضائي التفتيش إلا في حالتين:

أ – التلبس. ويجوز له تفتيش شخص المتهم في الجنايات والجنح المعاقب عليها بالحبس مدة تزيد على ثلاثة اشهر (المادة ٣٤، ٤٦ إجراءات جنائية).

ب– الانتداب من قبل المحقق المختص لتفتيش منزل أو شخص المتهم (المادة ٧٠ إجراءات)، ولا يختلف الأمر في حالة ارتكاب جرائم البرامج الإلكترونية. أما في فقد أناط القانون الفرنسي الاختصاص الأصل بقاضي التحقيق، أما النيابة العامة فلا تختص بالتفيش إلا في حالات معينة، كالتلبس.

ومتى اختص قاضي التحقيق بالدعوى أصبح من حقه إجراء التفتيش على النحو الذي يراه مفيداً في كشف الحقيقة لدى المتهم، أو لدى غيره دون قيد على سلطاته، إلا ما تعلق بحق الدفاع[١]، ويجب أن يحدد في إذن الندب بتفتيش المكان أو الشخص المراد تفتيشه أو الأشياء المراد تفتيشها وضبطها، حتى لا يتردد شيء من ذلك للسلطة التقديرية لرجل الضبط القضائي، كما يجب أن يتقيد مأمور الضبط القضائي بحدود الفرض من التفتيش، واستطردت أحكام القضاء الأمريكي على أنه إذا كان الإذن صادر لتفتيش جهاز الكمبيوتر في موضعه فإن هذا الإذن يسمح بتفتيش ملحقات الجهاز من أدوات مثل الطابعة والديسكات والأقراص الممغنطة[٢].

---

(١) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص١٣٣.

(2) United States V.Schandl, 947f- 2d 462, 465- 466. www.cybercrime.gov/smanual 2002:htm, p. 50.

ثانيًا: الضوابط الشكلية لتفتيش نظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على البرامج الإلكترونية:

تتمثل هذه الضوابط في الشروط التالية:

١-تسبيب أمر التفتيش:

حين تتكشف معالم وقوع جريمة الاعتداء على البرامج الإلكترونية أو تتوافر شكوك حول قيام البعض بارتكاب جريمة الاعتداء على البرامج الإلكترونية، فإن ذلك يتطلب تسبب أمر التفتيش. وقد أكدت الفقرة الأخيرة من المادة ٩١ أج على هذا الشرط حين نصت على أنه: "يجب أن يكون أمر التفتيش مسببًا" – ولم يتطلب تسبيب أمر التفتيش – والحكمة من التسبيب واضحة، وذلك من أجل أن تتمكن محكمة الموضوع من فرض رقابتها على صحة هذا الإذن من حيث توافر شروطه، وخاصة فيما يتعلق بتوافر قرائن تدل على توافر اتهام جرى قبل المتهم. وكان من المقرر أن العبرة في صحة إذن التفتيش أن يثبت صدوره بالكتابة، وأنه لا يشترط وجود ورقة الإذن بيد مأمور الضبط القضائي المنتدب لتنفيذه لأن من شأن ذلك عرقلة إجراءات التحقيق وهي بطبيعتها تقتضي السرعة، ولما كان الثابت من الحكم المطعون فيه أن إذن التفتيش صدر فعلا، وهو ما لا ينازع فيه الطاعن، فإن تنفيذ الإذن بصورته دون ورقته الأصلية لا يترتب عليه ثمة بطلان في الإجراءات[١].

وبالنسبة لتفتيش غير المتهم فإن المادة ٩٤ من قانون الإجراءات الجنائية لا تسمح لقاضي التحقيق بتفتيش غير المتهم، إلا إذا اتضح من إمارات قوية أنه يخفي أشياء قد تفيد في كشف الحقيقة. ومن ثم، يجب في كل الأحوال أن يكون الأمر بتفتيش الأشخاص محمولاً على سبب، وليس من اللازم أن تشمل مدوناته على أسبابه، كما يلاحظ أن الإذن بتفتيش غير المتهم أو منزل غير منزله يكون بأمر مسبب من القاضي الجزئي بناءً على طلب من النيابة العامة (م٢٠٦

---

(١) محكمة النقض – جنائي، أحكام غير منشورة، الطعن رقم ٤٢٣٣ لسنة ٨٢ ق، بتاريخ ١٦ديسمبر ٢٠١٢.
https://www.eastlaws.com/data/ahkam/details/349552/543173

إ.ج)، وذلك على خلاف الإذن بتفتيش شخص المتهم الذي لا يتطلب فيه التسبيب والإذن بتفتيش منزل المتهم الذي يقتصر عليه وحده التسبيب أو مع صدور دستور عام ٢٠١٤، فقد سوى المشرع بين الأشخاص والمساكن في تسبيب أمر التفتيش(١)، وهو ما يكفل ضمانات قوية لحرمة المتهم في حال الإذن بتفتيشه، وهذا يعد من ثمار ثورة يناير.

٢-حضور بعض الأشخاص أثناء إجراء التفتيش نظم الحاسب الآلي المرتكبة في جرائم الاعتداء على البرامج الإلكترونية:

لم يشترط المشرع حضور شهود عند تفتيش الأشخاص، وبالنسبة لتفتيش المنازل لم يستلزم المشرع لصحة تفتيشها- باعتبارها إجراء من إجراءات التحقيق تباشره سلطة التحقيق- سوى حضور المتهم أو من ينيبه عنه إن أمكن ذلك، وذلك إذا كان التفتيش واقعاً على منزل المتهم. أما إذا كان التفتيش واقعاً على منزل غير المتهم، فيُدعى صاحبه للحضور بنفسه أو بواسطة من ينيب عنه إن أمكن ذلك(٢). والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط، ولا يترتب على عدم دعوة المتهم أو صاحب المنزل لحضور التفتيش بطلان التفتيش، ذلك ان حضور المتهم أثناء التفتيش بناءً على أمر سلطة التحقيق ليس شرطًا جوهريًّا. ومع ذلك يقع باطلاً إذا كان في الإمكان حضور المتهم أو من ينيبه، ولم يكن هناك مبرر لعدم دعوته، أو أن القائم بتنفيذ التفتيش منعه من الحضور. ويلاحظ هنا، أن مأمور الضبط القضائي إذا باشر التفتيش بناءً على انتداب من سلطة التحقيق، فلا يلزم حضور شاهدين، فالمشرع استلزم الشاهدين فقط حينما كان يقوم مأمور الضبط بمباشرة التفتيش بناءً على السلطات الاستثنائية المخولة له في

---

(١) حيث تنص المادة ٥٨ من الدستور على أن: "للمنازل حرمة، وفيما عدا حالات الخطر أو الاستغاثة لا يجوز دخولها ولا تفتيشها ولا مراقبتها، أو التنصت عليها، إلا بأمر قضائي مسبب يُحدد المكان، والتوقيت، والغرض منه، وذلك كله في الأحوال المبينة في القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، واطلاعهم على الأمر الصادر في هذا الشأن".

(٢) تنص المادة ٩٢ إج. على أنه: "يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك، وإذا حصل التفتيش في منزل غير المتهم يدع صاحبه للحضور بنفسه أو بواسطة من ينيبه عنه إن أمكن ذلك".

حالات التلبس قبل الحكم بعدم دستورية نص المادة ٤٧ إجراءات[١].

أما المشرع الإجرائي الفرنسي لا يقر التفرقة التي أقامها المشرع المصري، بل اشترط في جميع الحالات حضور شاهدين أثناء إجراء التفتيش، سواء أكان القائم به قاضي التحقيق أم مأمور الضبط القضائي، فقد استوجبت المادة (٥٧ إ.ج.ف)[٢] أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتي، فإذا استحال حضوره وجب على أمور الضبط القضائي أن يكلفه بتعيين من يمثله فغذا استحال ذلك، كان لمأمور الضبط القضائي أن يختار شخصين يشهدان الإجراء الذي يقوم به من غير الأشخاص الخاضعين لسلطته الإدارية، كما تنص المادة (٢/٥٩إ.ج.ف)[٣] على بطلان التفتيش الذي يباشره مأمور الضبط القضائي في غير حضور المتهم، وإحالة المادة (٢/٩٦/ إ.د.ف)[٤] على المواد (٢/٥٧، ٥٩ إ.ج.ف) فيما يتعلق بالتفيش الذي يجريه قاضي التحقيق.

ويرى الباحث أن هذه الأحكام التقليدية تنطبق على تفتيش نظم الحاسب الآلي من حيث ضرورة حضور شاهدين أثناء إجراء التفتيش، سواء كان القائم بالتفتيش قاضي التحقيق أم مأمور الضبط القضائي. فلا شك أن فيه ضماناً للمتهم، ورقابة على سلامة الإجراء وصحة الضبط إلا إذا خيف ضياع الدليل. وذلك لسرعة إتلافه في جرائم الاعتداء على البرامج الإلكترونية– ففي هذه الحالة من الأنسب إجراء التفتيش في عدم حضور أشخاص.

---

(١) د. مأمون محمد سلامة، قانون الإجراءات الجنائية، مرجع سابق، ص٣٨٩.

(2) Art 57: "…les opérations prescrites par ledit article sont faites en présence de la personne au domicile de laquelle la perquisition a lieu. En cas d'impossibilité, l'officier de police judiciaire aura l'obligation de l'inviter à désigner un représentant de son choix : à de faut, l'officier de police Judiciaire choisira deux témoins requis à cet effet par lui, en de hors des personnes relevant de son autorité administrative ».

(3) Art 59/2: "les formalites mentiannees aux articles 56, 56-1, 57 et au present article sont prescrites à peine de nullité « Modifie par loi 93- 1013 1993-08-24 art. 20 JORF 25 aout 1993 en Vigueur le 2 septembre 1993.

(4) Art 96/2: "le Juge d'instruction droit se conformer aux dispositions des articles 57 (alinéa 2) et 59 ».

٣- تحرير محضر بالتفتيش في ارتكاب جرائم الاعتداء على البرامج الإلكترونية: التفتيش كما هو معروف في القانون هو ذلك الإجراء الذي رخص به الشارع فيه التعرض لحرمة الشخص. فينفي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة. ويجب على من يقوم بإجراء التفتيش في التحقيقات الجنائية أن يُحرر محضراً يبين فيه المكان أو الشخص الذي حصل تفتيشه، واليوم والساعة اللذين حصل فيهما التفتيش، إلا أن ذلك غنما وضع لحسن سير الأعمال وتنظيم الإجراءات، ولا يترتب على مخالفته البطلان.

وبالنسبة لمحضر تفتيش نظم الحاسب الآلي فإنه يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق بتقنية المعلومات، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسب والبرمجة يرافقه للاستعانة به في مجال الخبرة التقنية الضرورية. فلا شك أن وجود خبير معالجة وبرمجة سوف يساعد في صياغة مسودة محضر التفتيش بحيث تتم تغطية كل الجوانب الفنية والتقنية بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح[1]، ويجب أن يوقع كاتب التحقيق على المحضر.

ويرى الباحث، ضرورة عقد دورات تدريبية مكثفة لمأمور الضبط القضائي على كافة مستوياتهم في تقنية الحاسب الآلي حتى نضمن نجاح المهمة التي تناط بمأموري الضبط القضائي.

٤-طريقة تنفيذ أمر التفتيش لنظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على البرامج الإلكترونية:

يعد تفتيش البرامج الإلكترونية المعتدى عليها في جهاز الحاسب الآلي من الأمور المعقدة، لكونها تحوى في طياتها عمليات إلكترونية غاية في التعقيد، فالبرامج يمكن تخزينها في قرص مرن أو عناوين مخبأة في الحاسب أو على خادم بعيداً جداً على بعد آلاف الأميال. فمستودع

(١) د. حسن محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الإنترنت، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ٢٠٠٥، ص١٧٢.

الجرائم اللالكترونية في الحاسب الألي يضمن وحدات معقدة، منها وحدات المعالجة اللالكترونيـــة، ووحدات التخزين أو ما يسمي بوحدة التحكم، فضلا عن البرامج التطبيقيـــة والبيانـــات، متصـــلة بشبكات اتصالات سلكية ولاسلكية محلية أو دولية، كما يمكن تشفير البرامج الإلكترونيـــة المقلـــدة مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية، أو أن يتم خلطها مع ملـــايين الملفات التي ليس لها علاقة بالموضوع(١).

لذا فإن تفتيش وضبط نظم الحاسب الآلي يعتبر فن بقدر ما هو علم وعلى الرغم من أن تنفيذ إذن التفتيش موكول إلى مأمور الضبط القضائي المأذون له بالتفتيش يجريها تحت إشراف سلطة التحقيق ورقابة محكمة الموضوع، إلا أن الأمر يتطلب الخبرة أثناء التفتـــيش حتـــى لـــا تتلـــف أو تتلاشى الأدلة من ذاكرة الحاسب الآلي.

ومما يزيد من صعوبة التفتيش سهولة محو الأدلة المتحصلة من الوسائل الإلكترونية الـــدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جداً، حيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بهـــا فإنه يستهدف بالمحور السريع عدم استطاعة هذه السلطات إقامة الدليل ضده(٢).

الفرع الثالث

النتائج المترتبة على التفتيش الصحيح لنظم الحاسب الآلي المستخدم في جرائم الاعتداء على البرامج الإلكترونية

الضبط هو الأثر المباشر للتفتيش، فإذا بطلت إجراءات التفتيش بطل بالتبعية إجراء الضـــبط،

---

(1) Jonathan BOURGUIGNON, La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat, in Société Française pour le Droit International, Colloque de Rouen sur "Internet et droit international", du 30 Mai au 1er juin 2013, éd. Pedone, Paris, 2014, note 1, p.357.

(٢) د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية،ـــ دراسة تحليلية، مرجـــع ســـابق، ص ٣٦؛ د. علي عدنان الفيل، اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع ســـابق، ص ٧٨.

وقد يتم الضبط من غير تفتيش، عندما يقدم المشتبه به باختياره الأدلة المتعلقة بالجريمة. والضبط هو "وضع اليد على الشيء وحبسه والمحافظة عليه لمصلحة التحقيق[١].

ولا خلاف حول إمكانية ضبط المكونات المادية للحاسب Hardware. ولكن اختلفت الآراء حول إمكانية ضبط المكونات المعنوية للحاسب الآلي Sftware.

ويرى البعض أن البرامج الإلكترونية أن 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[٢]، ويستند هذا الاتجاه إلى بعض النصوص التشريعية، كالمادة ٧/٢٩ من قانون الإثبات في كندا التي تنص على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، ويستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني"[٣].

وهناك جانب من الفقه يرى أن الضبط لا يشمل المكونات المعنوية للحاسب إلا إذا نص عليها المشرع صراحة (المواد المعالجة عن طريق الحاسب أو بيانات الحاسب الآلي)، وهو ما توخاه مشروع قانون الحاسبات الإسرائيلي[٤] في فقرته الأولى من المادة الخامسة عشرة.

وفي هولندا[٥] استثنت، تم استثناء بيانات الحاسب غير المادية من القواعد التقليدية للضبط، ولكن من خلال الدعامة المدونة عليها.

وفي فرنسا[٦] يرى بعض الفقهاء أن النبضات الإلكترونية لا تعد من قبل الأشياء المادية، ولذا

---

(١) د. توفيق الشناوي، فقه الإجراءات الجنائية، دار الكتاب العربي، القاهرة، ١٩٥٤ ، ص٣٦٣؛ د. أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة، مرجع سابق، ص ١ – ٥٣.

(2) http://Majdah-Maktoob.com/vb/showthread.php?t=13354.

(3) http://Majdah-Maktoob.com/vb/showthreadphp?t-13417.

(4) LEDERRMAN (Eli)- Shapira (Ron) art cit, p. 286.

(5) KASPEREN (W.K. Henrik): art. Cite. P. 490.

(6) Groze (H.) « LAPPORTDU Droit pénal a la théorie générale du droit de =

لا يمكن ضبطه، وفي ألمانيا نص قانون الإجراءات الجنائية في القسم ٩٤ وجوب أن تكون الأدلة المضبوطة أشياء ملموسة.

والخلاف بين الرأسين هو الخلط بين طبيعة حق صاحب الشيء على الشيء من حيث هو نتاج لفكره وبين طبيعة الشيء من ناحية أخرى. فالبرامج الإلكترونية عمل ذهني وهي بذلك تدخل ضمن حقوق المؤلف.

ومعظم التشريعات العقابية مدت مظلة الحماية الجنائية لحقوق المؤلف لتشمل البرامج الإلكترونية كما في مصر، حيث صدر قانون حماية الملكية الفكرية للمؤلف رقم ٨٢ لسنة ٢٠٠٢ وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

وفي فرنسا القانون رقم ٨٥- ٦٥٠ في ٣ يوليو سنة ١٩٨٥، والذي حل محله قانون الملكية الفكرية رقم ٩٢- ٥٩٧، والصادر في الأول من يوليه سنة ١٩٩٢ والمعدل بالقانون رقم ٩٤- ٢٥٠ الصادر في ١٠ مايو سنة ١٩٩٤[١].

وفي الولايات المتحدة صدر القانون رقم ٩٦- ٥١٧ في ١٢ ديسمبر سنة ١٩٨١، ويمكن قياس الكيان المنطقي بالحيز المادي الذي يشغله في الحساب الآلي بوحدة القياس Byte، والكيلو بايت KiloByte والميجابايت MegaByte والنبضات الإلكترونية تتمثل في رقمين ٠ و١ صفر وواحد وهي شبيهه بالتيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية.

وتدخل في نطاق الأشياء المادية، يستوي أن تكون برامج نظام أو برامج تطبيق ولا خلاف يوجد في الطبيعة بينهما، وهذا الرأي تبنته محكمة باريس الابتدائية[٢].

= l'informatique J.C. pp. 1988, 3333. No. 16.

(1) Grozf (H.), «L'apport du droit pénal a la théorie générale du droit de l'informatique J.C. pp. 1988, 3333. No. 16.

(٢) د. محمد فهمي طلبة وآخرون، الموسوعة الشاملة للحاسب الإلكتروني "موسوعة دلتا كمبيوتر"، المرجع السابق، ص٤١.

ويرى الباحث ضرورة أن ينص الضبط على جميع الأجهزة والأدوات التي تحتوي على البرامج الإلكترونية محل الضبط لأن ضبط البرامج الإلكترونية لا يمكن أن يتم بمعزل عن الوسائط المادية. فالوسائط المادية تعد جزءاً من مكوناتها في الإثبات. والنسخ في حالة عدم إمكانية لضبط القطع الصلبة التي تخزن عليها البرامج المقلدة فيتم مثلاً نسخ البرامج التي تحتاج شفرتها إلى ذلك لكي يتم التعرف على محتوياته وأسلوب النسخ يصلح تماماً كدليل مقبول أمام القضاء[1].

(1) Vassilaki (Irnl) computer crimes and other crimes against information technology in grece R.I.D.P., 1993, p. 371.

المطلب الثالث

الشهادة الإلكترونية في مجال جرائم الاعتداء على البرامج الإلكترونية

من المقرر أن الفلسفة العامة التي تسود الإثبات الجنائي أنه يعتمد على القاعدة الوجدانية، وذلك لأن الإثبات ينصب على واقعة طواها الزمن ويتعين إعادة تركيب صورتها كما وقعت حتى تنطبق الحقيقة القانونية مع الحقيقة الواقعية، وصعوبة ذلك تبرر اعتماد كل وسائل الإثبات المتاحة دون تقيد، خصوصاً وأن محل الإثبات يتسع ليشمل كل العناصر التكوينية للجريمة وما يلابسها من ظروف خاصة جريمة الاعتداء على البرامج الإلكترونية لما يتميز به من سهولة إخفاء آثار الجريمة، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، ومن ثم كان على القاضي أن يقوم بدور إيجابي فليس دوره فقط الموازنة بين الأدلة المقدمة أو ذاك بالإدانة أو البراءة، وإنما عليه اتخاذ كل الإجراءات الضرورية والتحقق من صدق أية وسيلة تثار في سبيل الكشف عن الحقيقة(١).

ونظراً للطفرة التي عرفتها مختلف العلوم واضطراد توسع دائرة التقنية خلال القرن الحالي، الأمر الذي نتج عنه تزايد الأفعال الممنوعة قانوناً أضحى الشهادة الإلكترونية تناديها العدالة بالأمس قبل اليوم وترتيباً على ذلك، نعرض تعريف الشهادة الإلكترونية، والمقصود بالشاهد في جرائم الاعتداء على البرامج الإلكترونية، ثم التزامات هذا الشاهد على النحو الآتي:

الفرع الأول

تعريف الشهادة الإلكترونية

الشهادة الإلكترونية هي الشهادة التي لا يكون فيها الشاهد حاضراً جلسة التحقيق (الابتدائي أو النهائي) جسدياً، وإنما تتم عبر وسائل إلكترونية التي يمكن من خلالها الحصول على أقواله بشلك

---

(١) د. سيد علي السيد محمد، الجرائم الالكترونية: ماهيتها – صورها – اثباتها، دار التعليم الجامعي، ٢٠٢٠م، ص ٢١١؛ د. خالد حسن أحمد، الأدلة الجنائية الحديثة في إثبات الجريمة الإلكترونية، مرجع سابق، ص ٦١.

سمعي حركي.

ولقد كانت بدايات الأخذ بنظام الشهادة الإلكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبولها الشهادة الإلكترونية الفورية طالما كانت هناك أسباب في القانون تدعو إليه، ففي قضية استلزمت إدلاء شخص محض في برنامج حماية الشهود(١).

قام القاضي Jack B.Weinstrin، بتقرير قبول طلب الاتهام بسماع شاهد عبر دوائر تلفزيونية مغلقة، كون أن الشاهد كان موضوعاً في برنامج حماية الشهود، شريطة أن يكون حضور الشاهد عبر الدوائر المذكورة كما لو كان حاضراً الجلسة بالفعل، بحيث يكون كل ما يدور في الجلسة مرئيًا له بالمقابل لرؤية من هو في الجلسة له.

ولقد تأسس قبول قاضي الموضوع للشهادة عبر الدوائر المرئية المغلقة على أساس أن قاعدة المواجهة الشخصية في الجلسة قد تعدلت بما هو مقرر في امتداد الاستثناءات المقررة في قاعدة شهادة السماع التي تسمح في حالات محددة على سبيل الحصر بالأخذ بشهادة سماع وردت خارج الإطار القضائي(٢)، كذلك قامت المحكمة العليا الأمريكية في ١٩٩٦/١٢/١ بتعديل تفسير المادة (٤٣) من القواعد الفيدرالية للإجراءات المدنية بحيث سمحت بالأخذ بالشهادة عبر الدوائر المغلقة عن بعد.

ويميز القضاء الأمريكي بين نوعين من الشهادة الإلكترونية المرئية ضمن ناحية يوجد نظام الشهادة المرئية ذات الاتجاه الواحد وفي هذه الحالة فإن الشاهد حين يدلي بشهادته لا يرى سوى الكاميرا المسلطة عليه، فالرؤيا من طرف واحد هو طرف المحكمة، ومن ناحية أخرى توجد الشهادة المرئية ذات الاتجاهين وفيها يرى الشاهد قاعة المحكمة ويراه من في المحكمة من

---

(1) United States V. Gigonte, 93 CR 368(July 21, 1997).

(٢) د. فيصل عايش عيد المطيري, الوعاء القانوني للدليل التقني في إطار إثبات الجريمة الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ٢٠١٩م، ص ١٨٢.

قاضي ومحلفين وأفراد[1] وتقرير اختيار أي من الشهادتين يخضع لتقدير المحكمة.

الفرع الثاني

المقصود بالشاهد في مجال جرائم الاعتداء على البرامج الإلكترونية

الشاهد في جريمة الاعتداء على البرامج الإلكترونية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الإلكتروني، والذي تكون لديه معلومات مهمة وجوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة ويطلق على هذه النوعية من الشهود مصطلح الشاهد المعلوماتي[2].

ويشمل الشاهد المعلوماتي عدة طوائف من أهمها:

١- **القائم على تشغيل الحاسب الآلي:** وهو المسئول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه معلومات عن قواعد كتابة البرامج الإلكترونية.

٢- **المبرمجون:** وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين:

- **الفئة الأولى:** هم مخططو برامج التطبيقات.
- **الفئة الثانية:** هم مخططو برامج النظم.

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية، أي إنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

---

(1) U.S.V. Johnny Etimony. No, 01-10435-D-C No CR-99-00383- SOM- App. Usdis Hawall Feb, 13, 2003 Cal filed April 201-2003.

(٢) د. هلالي عبد اللاه أحمد: التزامات الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، ٢٠٠٦، ص٢٣.

٣- **المحللون:** المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات، ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما سمي بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

٤- **مهندسو الصيانة والاتصالات:** وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

٥- **مديرو النظم:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

الفرع الثالث

التزامات الشاهد في مجال جرائم الاعتداء على البرامج الإلكترونية

يتعين على الشاهد المعلوماتي أن يفصح أمام سلطات التحقيق ما لديه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيًا عن أدلة الجريمة.

والسؤال الذي يطرح نفسه هل يلتزم الشاهد بالإفصاح عن كلمة المرور والشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج؟

هناك اتجاهان في هذا الصدد:

الاتجاه الأول: يرى أنصار هذا الاتجاه إلى أنه ليس من واجب الشاهد وفقًا للالتزامات التقليدية للشهادة أن يقوم بطبع ملفات البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل لهذا الاتجاه الفقه الألماني، حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية[1].

(1) Carol M. Bast & Margie Hawkins, Foundations of legal Research and writing-computers- 2002, p. 89

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد، القيام بطبع ملفات البيانات، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، حيث يرى اتجاه في الفقه الفرنسي(١) أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد ٦٢، ١٠٩، ١٣٨ من قانون الإجراءات الجنائية الفرنسية)(٢).

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للولوج في نظام المعلومات، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد إلى التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب، وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة (المادة ٢٢٣ فقرة ١ إجراءات جنائية يونانية)(٣).

أما التشريع الإجرائي المصري فخول مأمور الضبط القضائي سماع الأشخاص الحاضرين في محل الواقعة، ومن يمكن الحصول منه على إيضاحات بشأن الجريمة (م١٣ إجراءات)، أو من تكون لديهم معلومات عن الجريمة. وله أيضاً أن يطلب من الحاضرين عدم مبارحة محل الواقعة أو الابتعاد عنه (م٣٢ إجراءات).

وعليه فإن المشرع الإجرائي المصري فرض على الشاهد عدة التزامات، وهي الحضور لسماع شهادته والبقاء لحين يؤذن له بالانصراف والضبط والإحضار لمخالفة هذا الالتزام، وأوردت المادة ١١٧ إجراءات الحضور للشهادة في مرحلة التحقيق الابتدائي. والمادة ٢٧٩ إجراءات الحضور للشهادة وفرض المشرع عقوبات للإخلال بهما (في المادتين ١١٩، ٢٨٤ إجراءات)، والالتزام الثالث ذكر الحقيقة وحرم المشرع شهادة الزور أمام المحاكم بعد حلف

---

(1) http://www.doha-shares,com/vb/f48/t21952.html.

(2) Froncilio N (Jacques): "les crimes informatique d'autres crimes dans le domaine de la technologie informatique en France « RIDP. 1993, p. 422.

(3) Vassilaki (Irini): "computer crimes and other crimes against information technology in Greece" R.I.D.P. 1993, p. 325.

اليمين (بالمادة ٢٩٤ عقوبات وما يليها) وبالعقوبة الواردة بالمادة ١٤٥ عقوبات لتقرير غير الحقيقة أمام سلطات التحقيق الابتدائي[١].

المطلب الرابع

الخبرة التقنية في مجال جرائم الاعتداء على البرامج الإلكترونية

من المسلم به أن التطور التكنولوجي لتقنية المعلومات والطفرات المتواصلة في تطوير البرامج الإلكترونية، فقد اتسعت دائرة استخدام الحاسبات الإلكترونية في الآونة الأخيرة بشكل متسارع، وأصبحت الأشخاص العامة والخاصة تستخدم هذه البرامج الإلكترونية.

لذا فقد أصبح واجباً، على كافة الجهات المختصة بالدولة، أن تحمي هذا الكيان الإبداعي الجديد توفر له وسائل تأمينية تتفق وطبيعته والجانب القانوني[٢].

ذلك أن عملية التوصل للجناة في جرائم الاعتداء على البرامج الإلكترونية هي عملية ذات مزيج من أعمال البحث الجنائي التقليدية من جمع تحريات وأدلة بالإضافة إلى الجوانب الفنية المطلوبة للتوافق مع طبيعة جرائم الاعتداء على البرامج الإلكترونية.

كما إنها تحتاج لخبرة فنية ويصعب على المحقق التقليدي التعامل معها. ولما كانت هذه الجرائم غامضة يصعب إثباتها والتحقيق فيها، فإن الكثير من هذه الجرائم لا يتم الإبلاغ عنها، إما لعدم اكتشاف الضحية لها أو خشيته من التشهير، بالإضافة إلى أن مرتكبها يتسم بالذكاء الحاد وسعة الحيلة[٣].

وترتيباً على ما سبق، نعرض للخبرة التقنية في مجال جرائم الاعتداء على البرامج الإلكترونية، من خلال ثلاثة فروع علي النحو التالي:

---

(1) Bruce Middleton, cybercrime Investigator's field Guide, op. cit., p. 146.

(٢) د. سيد علي السيد محمد، الجرائم الالكترونية، مرجع سابق، ص ١٦٢.

(٣) د. عادل حامد بشير، الاثبات الجنائي للجريمة الالكترونية، مرجع سابق، ص ٢٠٦.

الفرع الأول: تعريف الخبرة.

الفرع الثاني: أنواع الخبرة.

الفرع الثالث: أساليب عمل الخبير التقني في مجال جرائم الاعتداء على البرامج الإلكترونية.

الفرع الأول

تعريف الخبرة التقنية

تُعرف الخبرة بأنها إجراء يتعلق بموضوع يتطلب إلماماً بمعلومات فنية لإمكان استخلاص الدليل منه، أو إنها الاستشارات الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقرير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لدى القضاة بحكم العمل أو الثقافة.

كما عرفها الفقه الجنائي[1] بأنها: "تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة، سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو آثارها".

ذلك أن انتداب الخبراء هو إجراء من إجراءات التحقيق تختص به سلطة التحقيق، سواء أكان قاضي التحقيق أو جهة التحقيق المختصة، غير أن هذا لا يمنع عضو الضبط القضائي من استدعاء أهل الخبرة بشأن الجريمة التي يباشر فيها التحقيق، سواء تعلقت الخبرة بجسم الجريمة أو موادها وآثارها. وحسناً فعل المشرع المصري، بالنص صراحة على حق سلطة الضبط

---

(١) د. سليم إبراهيم حربه وعبد الأحد العكيلي، شرح قانون أصول المحاكمات الجزائية، بغداد، ١٩٨٨، ص١٢٥.

القضائي باستدعاء الخبراء[1].

وقد عرف المشرع المصري الخبرة في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ بأنها: "كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في مجالات تقنية المعلومات"، إلا أنه أجاز بأن لعضو الضبط القضائي عند تحقيقه في الجريمة المشهورة أن يحضر في الحال كل شخص يمكن الحصول منه على الإيضاحات.

ويلاحظ أن ندب الخبراء يستهدف منه اكتشاف الجريمة ومرتكبيها وهو عمل يعتبر بحقيقة الأمر من صميم سلطة الضبط القضائي، غير أن قانون مكافحة جرائم تقنية المعلومات، لم ينظم الكيفية التي يجري انتداب الخبير بواسطتها، إلا أن المحاكم تلجأ عادة للاستعانة بأحد الخبراء المقيدين في الجدول المعد لذلك.

ويلاحظ أن الخبراء المسجلين في الجدول لا يمارسون أعمالهم لأول مرة إلا بعد حلفهم اليمين بأن يؤدوا خبرتهم بأمانة وإخلاص، أما الخبير الذي يستعين به القائم بالتحقيق من غير المسجلين في الجدول فإنه يحلف اليمين في كل مرة يكلف بها في قضية، ويستطيع القائم بالتحقيق استبدال الخبير متى ما وجد أن الأمر يستدعى ذلك، كما يستطيع القائم بالتحقيق مناقشة وتوجيه الأسئلة إليه بحضور ذوي العلاقة، كما أن رأي الخبير غير ملزم، طالما يستطيع القائم بالتحقيق استبداله.

وإذا كانت هذه هي قواعد الخبرة في المسائل الجنائية والتي نظمتها قوانين الإجراءات الجنائية لتحكم مهمة الخبير في أدائه لمأموريته وذلك أمام سلطة التحقيق أو محكمة الموضوع على السواء، فإنه يجب مراعاة ضرورة مشروعية الدليل المترتب على أعمال الخبرة، وذلك أن هذه الأعمال تهدف أولاً وأخيراً إلى الفصل في مسألة فنية علمية لا دراية لسلطة التحقيق أو المحكمة بها، وهذا لا يخل بقاعدة أن المحكمة هي الخبير الأعلى في الدعوى.

---

(١) حيث نصت المادة (٢٩) من قانون الإجراءات الجنائية المصري على أنه: "لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يسمعوا أقوال من تكون لديهم معلومات عن الوقائع الجنائية وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهيًا أو بالكتابة".

والخبرة في مجال البرامج الإلكترونية تتميز عن الخبرة في أي فرع آخر من الفروع التي يمكن أن تكون محلاً للخبرة أمام القضاء.

وقد نصت المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ بشأن الاستعانة بالخبراء، في تلك النوعية من الجرائم على أن: "ينشأ بالجهاز سجلان لقيد الخبراء يقيد بأولهما الفنيون والتقنيون العاملون به) ويقيد بالآخر الخبراء من الفنيين والتقنين من غير العاملين بالجهاز، ويطبق عليهم في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء واستثناء من تلك القواعد تسري قواعد المساءلة الإدارية والتأديبية على الخبراء المقيدين بالسجل الثاني قواعد وأحكام وإجراءات القيد في كل من السجلين".

الفرع الثاني

أنواع الخبرة في مجال جرائم الاعتداء على البرامج الإلكترونية

الخبرة في المجال التقني قد تكون خاصة وقد تكون عن طريق مؤسسات تعليمية وقد تكون عن طريق جهات الضبط القضائي كما يلي:

١- **الخبرة الخاصة:** وتشمل خبرة المنظمات الخاصة والخبرات الفردية وتعد الخبرة الفردية أهم مظاهر الخبرة في مجال تكنولوجيا المعلومات فهي تتوقف على كفاءة الأفراد في مجال البرامج والإنترنت، ولا يشترط بالضرورة تلك النوعية من الخبرة الدراسية، فدراسات الحاسب الآلي والإنترنت لا ترتبط بمنهج دراسي معين أو شهادة معينة، وإنما ترتبط بمهارات خاصة وموهبة التعامل مع تقنية المعلومات، كما توجد منظمات خاصة وتختلف المنظمات الخاصة ما بين أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الإلكترونية، وبين نوعية من المنظمات تسعى إلى فك طلاسم العالم الافتراضي على أسس تجارية. فمثلاً استطاعت إحدى الشركات الاسكتلندية المتخصصة في برمجيات الحاسوب والإنترنت وهي Scottish Software Co. من إعداد مشروع خريطة للعالم الافتراضي في عام ٢٠٠٠ وكان من أهم نتائج هذه الخريطة أن تمكنت الخبرة الخاصة من

رصد حركة الجريمة عبر الإنترنت، ولهذا استفاد أهل الخبرة الخاصة من رصد هذه الخريطة في التعرف على التهديدات الحقيقية التي تواجه الدول والأفراد[1].

٢- **مؤسسات تعليمية:** وهذه المؤسسات تعتمد على منهج علمي غير تجاري هدفها تطور العلم، ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهبة الاستعداد لمواجهة الجريمة عبر الإنترنت ومن ذلك دراسات الحاسب الآلي التي تتطور بشكل فائق في جامعة ستانفورد، وكذلك معهد التكنولوجيا في ما ساشوش الذي قدم للبشرية خبراء على درجة عالية من التفوق.

٣- **جهات الضبط القضائي:** شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإحرام عبر الإنترنت كالمشرع المصري بالمادة العاشرة من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ والتي سبق وأن أشرنا إليها للتكرار".

وكذلك الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الإنتربول.

الفرع الثالث

أساليب عمل الخبير التقني في مجال جرائم الاعتداء على البرامج الإلكترونية

يوجد أسلوبان لعمل الخبير التقني في جرائم تقنية المعلومات[2]:

---

(1) Marcus Gibson- in fowar. Finapcial times Oct 20, 2000 available on line in Oct. 2000 at: http://www.infowar.com/ear/ear/.shtml.

(٢) د. عمر أبو بكر بن يونس: الإثبات الجنائي عبر شبكة الإنترنت، ورقة بحث مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية خلال الفترة من ٢-٢٠٠٦/٤/٤ مسقط، سلطة عمان، ص٤٣.

الأسلوب الأول:

القيام بتجميع وتحصيل مجموعة المواقع التي تشكل جريمة في ذاتها كما هو الشأن في جرائم النسخ، ثم القيام بعملية تحليل رقمي لها، لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت الذي ينسب إلى جهاز الحاسب الذي صدر عنه هذا الموقع(٣).

الأسلوب الثاني:

القيام بتجميع وتحصيل مجموعة المواقع التي لا يشكل موضوعها جريمة. في ذاته، وإنما تؤدي حال تتبع موضوعاتها إلى قيام الأفراد بارتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناسب وزن الإنسان بادعاء أنه إذا تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان، وكيفية إعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها.

وحيث إن أسلوب عمل الخبير يكون بهذه الصورة، ولذلك يتعين التنسيق ما بين الخبير المعلوماتي والمحقق الجنائي قبل محاكمة الجاني في جريمة تقنية المعلومات، على أن يشمل اللقاء كافة الخبراء الذين ساهموا من سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط أو التفتيش أو فحص البرامج، على أن يتم في هذا اللقاء حصر الأدلة المتوفرة، وترتيبها وفقًا للأهمية، كما يجب على المحقق الجنائي أن يشرح للخبراء الجوانب القانونية لطبيعة عملهم.

ويلاحظ أنه من الأعمال المحظورة في عمل الخبير التقني هي الدراسات التاريخية التي يقوم بها الخبير، بهدف تحديد أسلوب مرتكب الجريمة، وهي دراسات محاطة بالسرية المطلقة لكونها تؤدي إلى فتح سجلات وملفات انتهى موضوعها.

---

(٣) د. عمر أبو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيًا، دار النهضة العربية، القاهرة، سنة ٢٠١٠، ص٤٣٨.

وتجدر الإشارة إلى أن المحكمة تملك سلطة تقديرية بالنسبة لتقرير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية ولا يجوز لها تنفيذها إلا بأساليب فنية تخضع للتقـــدير المطلـــق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تنفذها وترد عليها بأساليب فنية قد يصـــعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى.

الخاتمة

وفي خاتمة البحث المتعلق بإشكالية إجراءات جمع الأدلة في مجال إثبات جـــرائم الاعتـــداء على البرامج الإلكترونية والتي لها صدى غير محدود ويعاني منها جميع المجتمعات في الوقـــت الراهن.

ويجب التنويه إلى أن حصر الإثبات في وسائل محددة قد لا يؤدي إلى إرساء نظـــام نـــاجح لمقاومة الجريمة والوصول إلى الحقيقة، وخاصة أن الحقيقة المقصورة هي الحقيقة المثبتة للإدانة أو البراءة على حد سواء.

وهذه الحرية ليست مطلقة من كل قيد، فقد أوجب القانون قواعد يجب على ســـلطة التحقيـــق مراعاتها ضماناً للمصلحة العامة ولحقوق الأفراد.

كما يجب الإشارة إلى أن جرائم الاعتداء على البرامج الإلكترونية تتم على المستوى المحلـــي والدولي على السواء والتي يمكن أن تقع من فاعل واحد فقط مهما تعددت الأفعال، وقد يشـــترك في ارتكابها أكثر من شخصاً ولو كانت من فعل واحد فقط، كما يجب ألا نغفل عن ضحايا هـــذه الجرائم وما يجب توفيره لهؤلاء الضحايا من عدالة وإنصاف وحماية وتعويضهم عما لحقهم مـــن أضرار مادية وأدبية من جراء وقوع الجريمة.

ويتطلب مكافحة هذه الجرائم، حماية فنية تهدف إلى الحيلولة دون وقوع الجريمة، أو علـــى الأقل التقليل من إمكانية وقوعها, وذلك عن طريق الشركات المنتجة للبرامج.

وفي النهاية إذا كان قانوننا الموضوعي والإجرائي يعاني من فـــراغ تشـــريعي بخصـــوص القواعد التي تحكم تفتيش وضبط الأدلة في جرائم الاعتداء على البرامج الإلكترونية فإن المعالجة التشريعية لهذه الجرائم أصبحت واجبة وضرورية لملاحقة مرتكبي هذه الجرائم.

وقد توصل الباحث في نهاية الدراسة إلى عدة نتائج وبعض المقترحات، نذكرهما على النحو الآتي:

النتائج:

١- ضرورة إحداث إصلاحات تشريعية على المستوى الإجرائي لكي تتواكب مع التغيرات في جرائم الاعتداء على البرامج الإلكترونية في مجال الإجراءات الجنائية وبصفة خاصة إثبات جرائم الاعتداء على البرامج الإلكترونية حتى تستجيب لاحتياجات الأجهزة المكلفة بالتحقيق في هذا المجال من هذه الأساليب تفتيش نظم الحاسب الإلكتروني- المعاينة- الشهادة في مجال جرائم الاعتداء على البرامج الإلكترونية يقع إما على الكيانات المادية للحاسب الإلكتروني أو البرامج الإلكترونية.

٢- التفتيش في مجال إثبات جرائم الاعتداء على البرامج الإلكترونية يقع إما على الكيانات المادية للحاسب الإلكتروني أو البرامج الإلكترونية.

٣- الشهادة الإلكترونية يدلي فيها الشاهد عبر إحدى الخدمات المدمجة وقد تكون مسجلة أو مكتوبة أو فورية.

٤- الخبرة التقنية هي إبداء الرأي الفني من أحد المتخصصين فيناً في شأن واقعة ذات أهمية في دعوى متعلقة بإحدى جرائم الاعتداء على البرامج الإلكترونية.

التوصيات:

١- نوصي المشرع بالتدخل التشريعي لإجراء تعديلات إجرائية كأذون التفتيش والمراقبة الإلكترونية بما يتناسب وطبيعة جرائم الاعتداء على البرامج الإلكترونية ومرتكبها.

٢- نوصي مأموري الضبط القضائي الاعتماد على خبراء فنيين على أعلى مستوى مهاري تقني.

٣- نهيب بالمشرع ضرورة استحداث قواعد مناسبة في مجال الإجراءات الجائية بشأن التحقيق في الجرائم الإلكترونية.

قائمة المراجع

أولاً: المراجع العامة.

١- د. عوض محمد: قانون الإجراءات الجنائية، مؤسسة الثقافة الجامعية، ١٩٨٩.

٢- د. فوزية عبد الستار: شرح قانون الإجراءات الجنائية، دار النهضة العربية، ١٩٨٦.

٣- د. مأمون محمد سلامة: قانون الإجراءات الجنائية. معلقًا عليه بالفقه وأحكام النقض، دار الفكرة العربي، ط١، ١٩٨٠.

٤- د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، ١٩٨٢.

ثانيًا: المراجع المتخصصة.

١- د. توفيق الشناوي، فقه الإجراءات الجنائية، دار الكتب العربي، القاهرة، ١٩٥٤.

٢- د. حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، دار النهضة العربية، ٢٠٠٩م

٣- د. خالد حسن أحمد، الأدلة الجنائية الحديثة في إثبات الجريمة الإلكترونية، دار الفكر الجامعي، ٢٠٢٣م.

٤- د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٨.

٥- د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، درا النهضة العربية، ١٩٩٨.

٦- د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية،ـ دراسة تحليلية، دار الكتب القانونية، ٢٠١١م.

٧- د. سعد أحمد محمود سلامة، مسرح الجريمة، دار النهضة العربية، ٢٠٠٧م.

٨- د. سيد علي السيد محمد، الجرائم االلكترونية : ماهيتها – صورها – اثباتها – مكافحتها، دار التعليم الجامعي، ٢٠٢٠م.

٩- د. عادل حامد بشير، الاثبات الجنائي للجريمة االلكترونية، دار النهضة العربية، ٢٠١٩.

١٠- د. علي حسني محمد الطوالية، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ٢٠١٠.

١١- د. عمر أبو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيًا، دار النهضة العربية، القاهرة، ٢٠١٠.

١٢- د. علي عدنان الفيل، اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية،٢٠١٢م.

١٣- د. فتحي والي، قانون المحاكم الاقتصادية "القواعد الخاصة للاختصاصات والإجراءات"، دار النهضة العربية، ٢٠٠٨.

١٤- د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، ٢٠٠٩.

١٥- د. ممدوح عبد الحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٦م.

١٦- د. محمد كمال شاهين، الجوانب الاجرائية للجريمة االلكترونية في مرحلة التحقيق الابتدائي: دراسة مقارنة، دار الجامعة الجديدة، ٢٠١٨.

١٧- د. محمد عيد الغريب، الاختصاص القضائي لمأمور الضبط في الأحوال العادية والاستثنائية، النسر الذهبي للطباعة، القاهرة ٢٠٠٠.

١٨- د. محمود رجب فتح الله، مسرح الجريمة الإلكترونية: دراسة تطبيقية مقارنة، دار الجامعة الجامعية، الإسكندرية، ٢٠٢١م.

١٩- د. هلالي عبد اللاه أحمد، التزامات الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، ٢٠٠٦.

ثالثًا: الرسائل والأبحاث العلمية.

١- د. أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات – كلية الحقوق, المجلد الثامن, العدد الثاني، ٣٠ يونيو ٢٠٢٢م، ص ١ – ٥٣.

٢- د. السيد العتيق، النظرية العامة للدليل العلمي في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٩٣.

٣- د. حسن محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الإنترنت، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ٢٠٠٥.

٤- د. خالد حسن أحمد، الأدلة الجنائية الحديثة في إثبات الجريمة الإلكترونية، دار الفكر الجامعي، ٢٠٢٣م.

٥- د. خالد على نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠٢٠م.

٦- د. عمر أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه كلية الحقوق، جامعة عين شمس، ٢٠٠٤.

٧- د. فيصل عايش عيد المطيري, الوعاء القانوني للدليل التقني في إطار إثبات الجريمة الإلكترونية، رسالة دكتوراه، كلية الحقوق – جامعة عين شمس، ٢٠١٩م.

٨- د. محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠٠٥م

٩- د. محمد نجيب، معاينة مسرح الجريمة، رسالة دكتوراه، أكاديمية الشرطة- كلية الدراسات العليا، القاهرة، ١٩٨٨.

١٠- د. محمد يوسف جاسم النعيمى، إجراءات التعامل مع مسرح الجريمة الالكترونية في التشريع الإماراتي: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩م.

قائمة المحتويات