إجراءات التحقيق الابتدائي في الجريمة المعلوماتية

(دراسة مقارنة)

علي عدنان الفيل

(ماجستير قانون) مدرس القانون الجنائي المساعد
جامعة الموصل / كلية الحقوق

الخلاصة

تعد ظاهرة الجريمة المعلوماتية جديدة مستحدثة تستهدف الاعتداء على معطيات الحاسبة الإلكترونية. فالجريمة المعلوماتية، جريمة تقنية تنشأ في الخفاء يرتكبها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية.

وقد اقترن بظهور تقنية المعلومات مشكلات إجرائية خاصة ومستحدثة فالتفتيش والتحفظ على المعلومات وإلزام الشاهد باسترجاع وكتابة المعلومات والحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات الإلكترونية وجمعها وتخزينها وضم المعلومات الرسمية إلى الدعوى الجزائية ، فأهم ما يميز الجرائم المعلوماتية صعوبة اكتشافها وإثباتها، كما أن إجراءات جمع الأدلة فيها لها ذاتية خاصة إجراءات التحري وجمع الأدلة والتحقيق الابتدائي كالمعاينة وندب الخبراء والتفتيش والضبط وسماع الشهود التي يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة الغامضة في الجريمة المعلوماتية، وهو غير ملزم أساساً بمباشرتها كلها، بل يباشر منها ما تمليه مصلحة التحقيق وظروفه.

وقد جاء هذا البحث ليوضح مدى توافق هذه الإجراءات الجزائية مع الجريمة المعلوماتية ويبين حكم التشريعات الجنائية في هذا الصدد.

Abstract

The information crime is considered a novelty phenomenon that aims at violating the data of computer. It is a technical crime secretly committed by intelligent criminals who are acquainted with technical knowledge.

Information technology has been associated with special procedural problems concerning inspection، information reservation، obligating the witness to restore and type the data، giving right to monitor، enter، collect and save data transferred by systems of electronic communication and inserting the official information to the penal action. The crime against the information technology is too difficult to detect or prove. This is the most important characteristic of such crimes. Also، proceedings of evidences collection in such crimes are self-acting especially those of investigation، collection of criminal evidences and preliminary interrogation such as inspection، mandate of experts، verification، arrest and hearing the witnesses that should be made، according to the investigator>s view، in order to detect the mystery in the information crime، but he is not obligated to execute all these proceedings. He may executes only the proceedings that help in investigation.

The present study clarifies the degree of accordance between these penal proceedings and the information crime and shows the situation of criminal legislations in this respect.

أولاً: المقدمة

أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات وتدفقها في العقود الثلاثة الأخيرة، ثورة إلكترونية تطبق الآن في كافة مجالات الحياة، وأضحى من الصعوبة بمكان الاستغناء عن خدماتها وفوائدها العظيمة والمتنامية، وقد تميل النفس البشرية أحيانا إلى فعل الشر،حيث يستغل بعض الأشرار المكتشفات العلمية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المخترعات، أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات الحديثة التي تصير محلاً لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الآخرين على وجه الخصوص، بصورة أدت إلى بزوغ ظاهرة إجرامية جديدة، تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني (La delinquance informatique، ou la cybercriminalite) .

فتم السطو على المصارف بمساعدة هذه المكتشفات الجديدة، ونمت الجريمة المنظمة وترعرعت في ظل هذه الثورة العلمية في نطاق المعلومات والاتصالات، على وجه التحديد جرائم الإرهاب وتجارة المخدرات، والاتجار بالسلاح والدعارة المنظمة باستخدام الإنترنت، وارتكبت العديد من الجرائم التقليدية كالسرقة والاحتيال وخيانة الأمانة، وتزوير المحررات، والاعتداء على حرمة الحياة الخاصة، وعلى البيانات الشخصية، والتجسس، وظهرت جرائم ملازمة لهذه المستحدثات، منها الغش الإلكتروني[1] بالتلاعب في المدخلات وفي البرامج، والنسخ غير المشروع للبرامج، والعديد من الجرائم المتعلقة بالتجارة الإلكترونية، وإتلاف الأجهزة الإلكترونية، وإتلاف السجلات المدونة على الحاسبة الالكترونية[2] وبث الصور أو الأفلام الجنسية من خلال الأجهزة، والقذف أو السب عن طريق البريد الإلكتروني، وغسيل الأموال القذرة باستخدام النقود الإلكترونية[3].

وخطورة هذه الظاهرة الإجرامية المستحدثة، أن الجريمة يسهل ارتكابها على هذه الأجهزة أو بواسطتها، وأن تنفيذها لا يستغرق في أكثر الأحيان إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة، فضلا عن أن مرتكبي هذه الجرائم، وبالذات في نطاق الجريمة المنظمة يلجأون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استخدام شفرات أو رموز سرية لإخفائها عن أعين

(1) O.C.D.E.: La fraud liee a l'ingormatique. Paris. 1986.
(2) Padova (Y.): Un apercu de la lutte contre la cybercriminalite en France. R.S.C. 2002. P. 765. Meunier (C): La loi du 28 nov. 2000 relative a la crimi nalite informatique. Rev. dr. pen. Crim. 2002. p.611.
(3) M. Pinguet: La douane et la cyber-delinquance G.P. 1996. doetr. 1325.

أجهزة العدالة مما يثير مشكلات كبيرة في جمع الأدلة الجنائية وإثبات هذه الجرائم قبلهم.

تستدعي خصوصية الجرائم المتعلقة بالحاسبة الإلكترونية بأن يتم تطوير أساليب التحقيق الجنائي وإجراءاته بصوره تتلاءم مع هذه الخصوصية، وتمكن رجل الشرطة، والمحقق من كشف الجريمة والتعرف إلى مرتكبيها بالسرعة والدقة اللازمتين.

ولتحقيق ذلك يجب من ناحية تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال، فضلاً عن تطوير الإجراءات الجنائية، لتحقيق الغرض المطلوب، وهو ما بدأت التشريعات منذ بضع سنوات في تحقيقه، ومنها القانون البلجيكي الصادر في 23 /11/ 2000.

ثانياً: مشكلة البحث

أثارت ظاهرة الإجرام الإلكتروني العديد من المشكلات في نطاق القانون الجنائي الإجرائي، إذ وضعت نصوص قانون أصول المحاكمات الجزائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، حيث لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتبدأ المشكلات الإجرائية في نطاق الجرائم المعلوماتية بتعلقها في كنير من الأحيان ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية، من ثم يصعب كشف هذه الجرائم من ناحية، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات سرعة ودقة تنفيذ الجرائم المعلوماتية وإمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلقان ببيانات مخزنة في أنظمة او شبكات إلكترونية موجودة في دول مختلفة، تثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات. وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة، وتسليم المجرمين، وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال.

وقد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، فيصعب إثباتها، ويثار التساؤل حول حرية تدفق المعلومات، فهل يصلح تدفق البيانات الموجودة خارج الدولة المتعلقة بالجريمة محل البحث ؟

ويثير التفتيش أو الضبط أو المصادرة في نطاق أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد، وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية، وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليها والتحقيق معهم وتقديمهم للمحكمة.

ومن المشكلات الإجرائية التي يثيرها هذا النوع من الجرائم مدى التزام الشهود، أو المشتبه فيهم في كشف الرموز أو الأرقام أو كلمات السر المتعلقة بالبيانات أو البرامج ذات الصلة بالجريمة. كذلك يثار التساؤل عن مدى حجية المخرجات الإلكترونية في الإثبات، نظرا إلى طبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية.

ثالثاً: خطة البحث

تم تقسيم دراسة هذا الموضوع حسب خطة البحث الآتية:-

المبحث الأول: تدريب الكوادر والاستعانة بالخبرة الفنية.

المطلب الأول: تدريب الكوادر.

المطلب الثاني: الخبرة الفنية.

المبحث الثاني: المعاينة.

المبحث الثالث: التفتيش.

المطلب الأول: مدى قابلية المكونات المادية للحاسبة الإلكترونية للتفتيش.

المطلب الثاني: مدى قابلية المكونات المنطقية للحاسبة الإلكترونية للتفتيش.

المطلب الثالث: التفتيش عن بعد.

المطلب الرابع: شروط تفتيش نظم الحاسبة الإلكترونية.

المبحث الرابع: الضبط.

المطلب الأول: الأشياء المادية.

المطلب الثاني: البيانات الإلكترونية.

المبحث الخامس: الشهادة

المطلب الأول: التعريف بالشاهد في الجريمة المعلوماتية.

المطلب الثاني: التزامات الشاهد المعلوماتي.

المبحث الأول

تدريب الكوادر والاستعانة بالخبرة الفنية

تقتضي دراسة هذا المبحث تقسيمه إلى مطلبين، نتناول في المطلب الأول موضوع تدريب الكوادر وفي المطلب الثاني موضوع الاستعانة بالخبرة الفنية.

المطلب الأول

تدريب الكوادر

إن طبيعة الجرائم ذات الصلة بالحاسبة الإلكترونية تقتضي معرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة استعمالها من قبل مستخدمها، ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم المعلوماتية، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال.

ويجب أن يشتمل التدريب على كيفية تشغيل الحاسبات، بعد التعرف إلى أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات، والمعالجة الإلكترونية للبيانات والجرائم التي تقع على الحاسبات، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن الحاسبات، ووسائل اختراقها، مع دراسة حالات تطبيقه لجرائم وقعت سلفا، وكيف تم مواجهتها.

وفي كثير من بلدان العالم تعتد الدورات التدريبية المتخصصة لرجال الشرطة وأعضاء النيابة العامة، سواء في مراكز تابعة لوزارة الداخلية أو في المراكز المتخصصة التابعة لوزارة العدل، كما هو الحال في أمريكا وبريطانيا، وكندا. وعند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المعلوماتية فإننا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها كل محقق فهي مهارات أساسية يفترض بداهة توافرها في المحقق بالضرورة، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعد من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق.

وعليه فإن التركيز هنا سينصب على تلك المهارات التي تتسم بالجدة والحداثة وتعد إفرازا للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمرا مستجدا في من يتعامل مع هذه الجرائم المستحدثة وهي:

1 - التعرف إلى المكونات المادية للحاسبة الإلكترونية والتعامل المبدئي معها.

المهم هنا أن يتمكن المحقق من معرفة الشكل المميز للحاسبات الإلكترونية وملحقاتها وام كل منها، والهدف من استخدامه وما هي احتمالات توظيفه لارتكابه أي من الجرائم المعلوماتية، حيث إن عدم تعرفه إليها قد يؤدي إلى إهمالها أو حتى إتلافها دون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها[4].

ليس هذا فحسب بل لا بد أن يلم المحقق بكيفية التعامل مع تلك المكونات من أجهزة وملحقات ووسائط تخزين بصفتها أدلة محتملة.

واكتساب هذه المهارة يعد أحد الأهداف المرجوة من البرامج التدريبية الخاصة بالتحقيق في الجرائم المعلوماتية لدي العديد من الدول كالولايات المتحدة وكندا واستراليا[5].

2 - معرفة أساسيات عمل شبكات الحاسبة الإلكترونية وأهم مصطلحاتها:

الكثير من الجرائم المعلوماتية يتم ارتكابها من خلال شبكة الإنترنت، ومن ثم فإن المحقق بحاجة إلى معرفة مبادئ الاتصال الشبكي وأنواعه المختلفة وكيفية انتقال البيانات من جهاز إلى آخر على شكل حزم، ومبادئ البرتوكولات الرئيسية الخاصة بالاتصال بالشبكة[6].

وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصور كيفية ارتكاب الفعل الإجرامي في فضاء الإنترنت Cyber-space)) من اختراق للشبكات و الحاسبات واعتراض حزم البيانات في أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها. كما أنها تعطي المحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعضلات الفنية التي تحول دون ذلك[7].

---

(4) United States Secret Service (USSS) (2002). Best Practices for Seizing Electronic Evidence. on line: www.secretservice.gov/electronic__evidence.shtml

(5) Thompson. David (1990). Computer Crime The Improvement of Investigative Skills: Final Report: Part Two. www.acpr.gov.au/pdf/ACPR101.pdf 212003/10/

(6) محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت «دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية»، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص95-96.

(7) Shindre. Debra (2000). Scene of the Cyber crime: Computer Forensics Hand Book. Rockland. MA: Syngress Publishing. P.56

3 - تمييز أنظمة تشغيل الحاسبة الإلكترونية المتمثلة والتعامل المبدئي معها:

يجب أن يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسبة الإلكترونية وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها[8].

فمعرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية حتى يشارك في متابعة وفحص وتفتيش مسرح الجريمة. وأحيانا يجد المحقق نفسه أمام موقف فني صعب يجب أن يتخذ قراراً بشأنه بالتشاور مع الخبير، ودون توافر الحد الأدنى من المعرفة التقنية لهذا المحقق فإن القرار على الأرجح سوف يكون للخبير وحده.

وأكثر أنظمة التشغيل شيوعا وشهرة والتي يجب أن تتوافر في أي برنامج تدريبي هي: أنظمة (Windows) وأنظمة (Unix، Macintosh and Alinux) .

4 - التعرف إلى الصيغ المختلفة للملفات وتطبيقات الحاسبة الإلكترونية الرئيسية التي نتعامل معها:

تعد الملفات الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا المتعلقة بشبكة الإنترنت بما تحويه من معلومات[9]، ومن ثم فإن قدرة المحقق على معرفة صيغ هذه الملفات وما يمكن أن تحويه، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو سماع أو مشاهدة محتوى هذا الملف يعد أمراً في غاية الأهمية.

5 - إجادة التعامل مع خدمات الإنترنت الرئيسية:

تمثل شبكة الإنترنت أداة جمع وتحريات مناسبة للمحقق، حيث إنها خلقت مجتمعا افتراضيا شبيها إلى حد ما بالمجتمعات الحقيقية، ويدور في مجتمع الإنترنت هذا الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم [10]. ومن الممكن أيضا أن يستخدم الإنترنت كأداة تعليمية للاطلاع على مستجدات جرائم الحاسبة الإلكترونية والإنترنت وطرق التصدي لها .وكوسيلة اتصال وتبادل المعلومات فيما بين أعضاء السلطة التحقيقية.

(8) Institute for security Technology Studies (ISTS) (2002). Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment. available on line at 42003/6/: www.ists.dartmouth.eud/TAG/need/ISTS__NA.pdf

(9) غالبا ما يتم حفظ البيانات الرقمية داخل جهاز الحاسبة الالكترونية على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمي ملفات ، حيث يتميز كل ملف ببيئة وصيغة خاصة تسمى (Format) تميزه عن غيره وغالبا ما ترتبط كل صيغة بنوع محدد من المحتوى كأن يحتوى الملف على بيانات تمثل صورة أو صوت أو فيديو أو مستند خطي أو غير ذلك. انظر محمد بن نصير محمد السرحاني، مصدر سابق، ص 97.

(10) Davis. David (1998). Internet Detective: An Investigator's Guide. West Midland. UK: Police Research Group. P.73

6 - معرفة الأدوات والأساليب المستخدمة في ارتكاب الجرائم المعلوماتية:

إن معرفة رجال العدالة بهذه الأساليب وكيفية استخدام هذه الأدوات يعد أمراً في غاية الأهمية خاصة لمن يتولون مناقشة الشهود واستجواب المتهمين فمن دونه لن يستطيعوا طرح الأسئلة التي تتصل مباشرة بالسلوك الإجرامي وأسلوب ارتكابه. كما أنها تساعد المحقق على التواصل مع خبير الحاسبة الإلكترونية الجنائي عند شرح الأخير ما توصل إليه من أدلة أو قرائن عن الأساليب المستخدمة في ارتكاب الجريمة والأدوات التي تساعده على القيام بذلك.

7 - معرفة أهم تقنيات أمن الحاسبة الإلكترونية والإنترنت وأدواتها وطريقة عملها:

اكتساب هذه المهارة مهم وإن كان يبدو في الظاهر أمرا معقدا بعض الشيء، إلا أن الأمر في حقيقته ليس كذلك، حيث إن المطلوب أن تساعد معرفة هذه التقنيات المحقق في استيعابها وربطها بمجريات التحقيق بشكل عام وليس أن يجعله خبيرا فيها.

8 - الاطلاع على بعض الجوانب المتعلقة بالجرائم المعلوماتية:

تتميز هذه الجوانب بغلبه الطابع النظري عليها بحيث يمكن اكتسابها من خلال القراءة والاطلاع سواء من خلال المطبوعات أو الإنترنت، ومن أهم هذه الجوانب:

الواقع الحالي والاتجاهات المستقبلية للجرائم المتعلقة بشبكة الإنترنت.

الفئات المختلفة التي ينقسم إليها مرتكبو هذه الجرائم والخصائص المشتركة التي تميز كل فئة.

معرفة وفهم التشريعات المختلفة المتعلقة بهذه الجرائم والإلمام باتجاهات القوانين والتشريعات في البلدان المختلفة.

دراسة وتحليل بعض القضايا المشهورة للاستفادة من تجارب رجال العدالة في مواجهة هذه الجرائم.

الوقوف على الأبعاد الدولية لهذه الجرائم وآليات التعاون المشترك بين الدول والتعرف إلى الاتفاقيات والمعاهدات الموجودة بهذا الخصوص.

معرفة مصادر المعلومات المتوافرة على مواقع الإنترنت عن هذه الجرائم من خلال المواقع المتخصصة ذات المحتوى الجيد والمصداقية والاستفادة منها.

9 - معرفة الجرائم المعلوماتية والخصائص التي تتميز بها:

الوعي الجيد بهذه الجرائم وبأنواعها المختلفة يعد بمثابة حجر الأساس في مواجهتها ومن دونه لن تنجح السبل والوسائل الأخرى فلا يعقل أن تتم مواجهة جريمة ما إذا كان رجل العدالة المناط به هذا الأمر يجهل ماهيتها.

المطلب الثاني

الخبرة الفنية

يرى المحقق في بعض الأحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافته العامة عن فهمها كتحديد سبب الوفاة أو ساعتها أو رفع بصمة وجدت في مكان الجريمة أو فحص سيارة لبيان ما فيها من خلل.

ومنذ بدء ظهور الجرائم ذات الصلة بالحاسبة الإلكترونية، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسبة الإلكترونية، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق. حيث تكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظراً لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج متعددة كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها ويمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة بسائر أنواع الحاسبات وبرامجها وشبكتها كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[11].

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة[12]، وللمحقق في أي وقت إلى أن ينتهي التحقيق – أن يندب من يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق؛ فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب الخبير. ومن ثم فإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي

(11) Philip M. Stanley computer crime investigation and investigators computer & security. Nort Holland. 1986. pp. 310311-.
(12) Franklin Clark den Dilbert. Investigation computer crime. p. 147.

دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبرة فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيباً مستوجباً نقضه، وهذا المبدأ استقر عليه قضاء محكمة النقض المصرية[13].

وبناء عليه فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمراً واجباً على جهة التحقيق والقاضي، فهي أوجب في مجال الجرائم المعلوماتية، حيث تتعلق بمسائل فنية غاية في التعقيد ومحل الجريمة فيها غير مادي والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن، لا يكشفه ولا يفله إلا ذكاء وفن مماثلان.

وأهمية الاستعانة بالخبير الفني في مجال الجرائم المعلوماتية، تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة، وقد تدمر الدليل أو تمحوه، بسبب الجهل أو الإهمال عند التعامل معه[14].

والخبير لا يشترط فيه فحسب كفاءة علمية عالية في مجال التخصص بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، وعلى وجه الخصوص الجرائم ذات الصلة بالحاسبة الإلكترونية، فقد يتعلق الأمر بتزوير المستندات، أو بالتلاعب في البيانات أو الغش في أثناء نقل أو بث البيانات أو جريمة من جرائم الأموال أو الاعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة.

ويحدد المحقق للخبير مهمته والميعاد الذي يقدم فيه تقريره وعليه أن يحلفه اليمين على أن يبدي رأيه بالذمة وهذا الإجراء جوهري يترتب على إغفاله بطلان عمل الخبير[15]. والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه والاستثناء أن يتم ذلك في غيابه.

وللخصوم حق الحضور في أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش أمراً سهلاً حيث يمكن التعرف إليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء وهذه المستندات مثل: أدلة عمل النظام، سجلات إدارة الحاسبة الالكترونية،

(13) أنظر الأحكام التالية التي وردت بمجموعة أحكام محكمة النقض المصرية، الدائرة الجنائية، نقض 1961/6/13، س12، رقم 131، ص671؛ نقض 1974/9/15، س25، رقم 183 ص849؛ نقض 1983/1/4، س34، رقم 5، ص52.

(14) Robert Taylor: Computer crime. "in criminal investigation edited" by Charles Swanson. n. chamelin and L. Territto. Hill. inc. 5 edition 1992. P.1.

(15) نقض مصري 1926/12/26 المحاماة س 7 ص 789 و 1972/2/8 س 8 ص 1958 ؛ 1972/3/1 مجموعة القواعد القانونية ج 4 ص 52 رقم 43.

ووثائق البرامج، والسجلات، وصيغ مدخلات البيانات والبرامج، وكذلك صيغ مخرجات الحاسبة الإلكترونية المطبوعة ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة، وأصلية، أو صوراً من خلال استجواب القائمين على حفظها.

وقد يكون التخطيط على المواد المتعلقة بوسائل الحاسبة الإلكترونية الأخرى أمراً أكثر تعقيداً مثل: الأشرطة المغنطة الأسطوانات، والبرامج ويحتاج إلى معونة أحد الخبراء الموثوق فيهم حتى يتمكن المحقق من الإلمام بمحتويات الأشرطة أو الاسطوانات دون إحداث أي تغيير فيها.

وبالطبع، فإن البحث عن المعلومات داخل جهاز الحاسبة الإلكترونية ذاته يعد أمراً بالغ التعقيد ويحتاج إلى وجود خبير[16]. وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

أولاً: وصف:

أ- تركيب الحاسب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير ... الخ.

ب- طبيعة بيئة الحاسبة الإلكترونية أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها.

ج- الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

د- أثر التحقيق من الوجهة الاقتصادية والمالية في المشاركين في استخدام النظام.

ثانياً: بيان:

أ- كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

ب- كيف يمكن عند الاقتضاء نقل أدلة الاثباتات إلى أوعية ملائمة دون أن يلحقها تلف.

ج- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسبة أو النظام أو الشبكة أو الدعامة المغنطة[17].

(16) أنظر جرائم الكمبيوتر، بحث مقدم من مركز البحوث والدراسات ، أكاديمية شرطة دبي، 1998 ، ص2.
(17) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسيوط، 1994.

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم المعلوماتية، القانون البلجيكي الصادر في 23/ 11/2000[18].

فقد نصت المادة (88) من القانون المذكور على أنه يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة

أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق[19].

ووفقا للقانون البلجيكي المذكور سلفا فإن الالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه، يرجع إلى قاضي التحقيق بصفة أصلية، ويجوز ذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس بالجريمة، أو عند الرضا بعملية التفتيش هذه[20]. فمهمة الخبير وفقا للنص القانوني البلجيكي السابق تتمثل من ناحية في تشغيل النظام، ومن ناحية أخرى في تقديم البيانات المطلوبة، حسب الطريقة التي تريدها جهة التحقيق، فقد تريد البيانات مسجلة على دسك (disc) أو على سيديروم (CDROM)، أو على الأقراص المغنطة، أو على ورق[21].

والتزام الخبير هو التزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقبات التي واجهته في أثناء مباشرته لمهمته، ويمكن أن تثور مسئوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمدا البيانات المطلوب منه التعامل معها، أو حفظها[22].

فضلاً عن التزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، يلتزم كذلك بالمحافظة على سر المهنة، وفي حالة إفشائه السر، يعاقب بالعقوبة المقررة لهذه الجريمة[23].

(18) Meunier (c) La loi du 28 November 2000 relative a la criminalite informatique. Rev. dr. pen. Crim. 2002. p. 611 et s.
(19) Meunier (C.): art. Prec. P. 681.
(20) Meunier (C.): art. Prec. P. 682.
(21) Meunier (C.): art. Prec. P. 683.
(22) ibid.p. 683
(23) Meunier (C.): op. cit. p. 684

المبحث الثاني

المعاينة

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها، أو محوها أو تعديلها.

والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، والأصل أن يحضر أطراف الدعوى الجزائية المعاينة، وقد يقرر المحقق أن يجريها في غيابهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور [24]. ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها[25].

وإذ تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجد مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم المعلوماتية، حيث يندر أن يتخلف عن ارتكابها آثار مادية، وقد تطول المدة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها[26].

فمع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة والأولوية فيما عدا حالات استثنائية على ما عداها من الإجراءات الاستقصائية الأخرى، إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها لا ترقى إلى نفس الدرجة من الأهمية، ومرد ذلك اعتباران هما [27]:

1 - أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يتخلف عن ارتكابها آثار مادية.

2 - أن عددا كبيرا من الأشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا التي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يفسح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالا من الشك على

(24) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3،دار النهضة العربية،القاهرة، 1998، ص528-529 ؛ د.محمد أبو العلا عقيدة، «شرح قانون الإجراءات الجنائية، ج2، دار النهضة العربية،القاهرة، 2001، ص644 وما بعدها.
(25) نقض 1980/1/31، مجموعة أحكام النقض، س31، رقم 29، ص148.

(26) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية،القاهرة، 1994، ص59.
(27) د.عبد الله حسين علي محمود،إجراءات جمع الأدلة في مجال سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، إمارة دبي بدولة الإمارات العربية المتحدة 26-2003/4/28م، المجلد الأول ، ص598.

الدليل المستمد من المعاينة.

وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الإنترنت فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[28]:

1 - تصوير الحاسبة الإلكترونية والأجهزة الطرفية المتصلة بها والمحتويات والأوضاع العامة في مكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسبة وملحقاتها ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2 - العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع.

3 - ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

4 - وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي بالمسئولين فيها ودور كل واحد منهم.

5 - فصل الكهرباء عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير في آثار الجريمة.

6 - إبعاد الموظفين عن أجهزة الحاسبة الإلكترونية، وكذلك عن الأماكن الأخرى التي توجد بها أجهزة للحاسبة الإلكترونية.

7 - عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسبة الإلكترونية من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة[29].

8 - التحفظ عما قد يوجد بسلة المهملات[30] من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة، وفحصها ورفع البصمات التي قد تكون

(28) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، سابق الإشارة إليه ، ص30-31؛ د. عبد الله حسين علي محمود، مصدر سابق، ص559-560.

(29) القاضي وليد عاكوم ، التحقيق في جرائم الحاسوب، بحث منشور على شبكة الانترنت، موقع الدليل الإلكتروني للقانون العربي www.arablawinfo.com .

(30) من فحص بعض البطاقات المثقبة المعثور عليها بسلة المهملات في المكان الموجود به جهاز الحاسبة الالكترونية أمكن كشف غموض جريمة شهيرة لسرقة البرمجيات عن بعد وقعت أحداثها بسانتا كلارا بالولايات المتحدة الأمريكية. حول التفاصيل الفنية لارتكاب هذه الجريمة . أنظر د.هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص126-127.

لها صلة بالجريمة المرتكبة.

9 - التحفظ على مستندات الإدخال والمخرجات الورقية للحاسبة ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد بها من بصمات.

10 - قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبة الإلكترونية والشبكات ونظم المعلومات(31)، واسترجاع المعلومات، الذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية. ففي فرنسا مثلا يقوم فريق مكون من (13) ثلاثة عشر شرطياً بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققون وجميعهم تلقوا تدريباً متخصصاً إلى جانب اختصاصهم الأساسي في مجال التقنية الحديثة. وهم يقومون بمرافقة المحققين في أثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الأسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بعمل تقرير يرسل إلى القاضي الذي يتولى التحقيق. أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعادة المعلومات من على الاسطوانة الصلبة كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات الإلكترونية المحمولة (Laptop).

وبعد وصول فريق التحقيق إلى مسرح الجريمة أو مكان الغارة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو الآتي:

أ- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الغارة وذلك عن طريق إغلاق الطرق والمداخل.

ب- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

ج- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.

د- تحديد أجهزة الحاسبة الالكترونية الموجودة في مكان الإغارة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات اتصالات يجب البحث عن خادم الملف (file server) لتعطيل حركة الاتصالات.

(31) Taylor (R.W). op. cit. p. 450

هـ- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى.

و- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيداً عن أجهزة الحاسبة الإلكترونية[32].

ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق.

ولعل من أبرز الأماكن التي يحتمل وجود الأدلة الجنائية المتعلقة بالجرائم المعلوماتية فيها ما يلي:

1 - الورق: على الرغم من أن وجود أجهزة الحاسبة الإلكترونية قلل من حجم الأوراق والملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسبة الإلكترونية، نجد الكثيرين ممن يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، ومن ثم فهي تعد من الأدلة التي ينبغي الاهتمام بها في البحث عن الحقيقة.

2 - جهاز الحاسبة الإلكترونية وملحقاته: وجود جهاز الحاسبة الإلكترونية مهم جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية، وإنها مرتبطة بالمكان أو الشخص الحائز على الجهاز، ولأجهزة الحاسبة الإلكترونية أشكال وأحجام وألوان مختلفة وخبير الحاسبة الإلكترونية وحده الذي يستطيع أن يتعرف إلى الحاسبة الإلكترونية ومواصفاتها بسرعة فائقة.

3 - البرمجيات(Software): إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل[33].

4 - وسائط التخزين المتحركة: كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة والأشرطة المغناطيسية والفلاش ممورى وغيرها، وتعد هذه الوسائط جزءاً من الجريمة المعلوماتية متى ما

(32) د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي ، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1-2000/5/3، المجلد الثالث ،ص1030.

(33) Sammes T & Jenkinson B. (2000). Forensic Computing: A pratitioner's Guide London: Springer.p.59

كانت محتوياتها عنصراً من عناصر الجريمة.

5 - المراشد Manuals)) الخاصة بالمكونات المادية والمنطقية للحاسبة الإلكترونية التي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها[34].

6 - المودم Modem)): وهو الوسيلة التي تمّكن أجهزة الحاسبة الإلكترونية من الاتصال ببعضها عبر خطوط الهاتف. وفي الوقت الحالي تطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

7 - الطابعات: والتي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها[35].

المبحث الثالث

التفتيش

يعرّف التفتيش بوجه عام بأنه إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة[36].

وفي الجرائم المعلوماتية نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها. وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية هو إجراء جائز قانونا ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه.

وللتفتيش في الجرائم التقليدية شروط موضوعية تتعلق بمايلي:

1 - بسببه: وقوع جريمة بالفعل تعد جناية او جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه.

2 - الغاية منه: ضبط أشياء تفيد في كشف الحقيقة.

أما الشروط الشكلية فتتحدد بمايلي:

(34) محمد بن نصير محمد السرحاني، مصدر سابق، ص81.

(35) د. عبد الله حسين علي محمود، مصدر سابق، ص624-627؛ د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1-2000/5/3، المجلد الثالث ص1025-1059.

(36) د. هلالي عبد ألاله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ط1، دار النهضة العربية، القاهرة، 1997، ص47.

1 - أن يكون الأمر بالتفتيش مسبباً.

2 - حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش

3 - تحرير محضر بالتفتيش[37].

ويثور السؤال عن إمكانية التفتيش وفقا للضوابط السابقة والغاية منه في مجال الجرائم المعلوماتية. والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي. ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص المغنطة، ومخرجات الحاسبة الإلكترونية[38]. لهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة إلكترونياً، والمخزنة بالحاسبة الإلكترونية، ثم ضبطها والتحفظ عليها، أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات. والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام.

وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني[39].

فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة[40].

ونظرا لكون التفتيش يتضمن تقييدا للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته ومنها أن يتم صدور أمر قضائي مسبب بشأنه وأن يباشره الشخص أو الجهة المختصة (النيابة العامة، أو مأمور الضبط القضائي في حالة ندبه، في غير حالات التلبس بالجريمة).

وبحسب الأصل يجب أن يصدر إذن التفتيش مكتوبا إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر

(37) د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية»، ج1، دار النهضة العربية، القاهرة، 2001، ص431 وما بعدها.

(38) Moherenschlager. M.. computer crimes and others crimes against information technology in the Germany. Rev. int.dr.pen.1993. p. 319. spec. 349.

(39) Conseil de L'eurpe: Problems de procedure penale lies a la technologie de l' information. Recommendation n. R(95) 13 et expose des motifs. Ed. Conseil de l' Europe. 1996. p. 28.

(40) Meunier (C.): Art. Prec. P. 663.

في نظام معلوماتي آخر غير الذي صدر بشأن الإذن المكتوب. والمخاطر تتمثل في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال المدة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث[41].

ويرى البعض أنه في حالة امتداد الاختصاص، يمكن أن يصدر الأمر بالامتداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته[42].

ومحل التفتيش وما يتبعه من ضبط يشمل البرامج أو الكيانات المنطقية (Les logiciels) والبيانات المسجلة في ذاكرة الحاسبة أو في مخرجاتها – السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات – ودفتر يومية التشغيل وسجل المعاملات – السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، ومايتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة [43].

وعليه، سيتم تقسيم هذا المبحث إلى أربعة مطالب، ففي المطلب الأول تمت دراسة مدى قابلية المكونات المادية للحاسبة الإلكترونية للتفتيش، وفي المطلب الثاني مدى قابلية المكونات المنطقية للحاسبة الإلكترونية للتفتيش، وفي المطلب الثالث مدى خضوع شبكات الحاسبة الإلكترونية للتفتيش، وأخيرا خلصنا في المطلب الرابع إلى تحديد شروط تفتيش نظم الحاسبة الإلكترونية.

المطلب الأول

مدى قابلية المكونات المادية للحاسبة الإلكترونية للتفتيش

لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسبة الإلكترونية (Hardware) بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث إن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز

(41) Meunier (C.): Art. Prec. P. 664.
(42) Meunier(C.): art. Prec. P. 668.
(43) د. هشام محمد فريد رستم، مصدر سابق، ص77-78.

فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا في التشريعات المختلفة [44]، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسبة المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أم إنها متصلة بحاسبة إلكترونية أخرى أو بنهاية طرفية (Terminal) في مكان أخر كمسكن غير المتهم مثلا، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن. أما لو وجد شخص يحمل مكونات الحاسبة الإلكترونية المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[45].

المطلب الثاني

مدى قابلية المكونات المنطقية للحاسبة الإلكترونية للتفتيش

تفتيش المكونات المنطقية للحاسبة الإلكترونية (Software) أثار خلافا كبيرا في الفقه بشأن جواز تفتيشها وكما يلي:

الرأي الأول: يرى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء) فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسبة المحسوسة وغير المحسوسة [46]، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفي هذا المعنى نجد المادة (251) من قانون الإجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضرورياً لجمع وحماية الدليل) ويفسر الفقه الجنائي اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إلكترونياً، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسبة الإلكترونية لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمراً للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة

(44) د. هلالي عبد اللاه أحمد، مصدر سابق، ص73.

(45) د. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث منشور على شبكة الانترنت، موقع الدليل الإلكتروني للقانون العربي www.arablawinfo.com .

(46) Vassilaki (Irini): computer crimes and other crimes against information technology in Greece. Rev. Intern De. Dr. Pen. P. 371.

الجنائية[47].

وتمنح المادة (487) من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها أو ان هناك نية في أن يستخدم في ارتكاب الجريمة أو انه سوف ينتج دليلاً على وقوع الجريمة.

الرأي الثاني: على نقيض الرأي الأول ،يرى عدم انطباق المفهوم المادي على بيانات الحاسبة غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسبة الإلكترونية لابد أن يشمل (المواد المعالجة عن طريق الحاسبة الإلكترونية أو بيانات الحاسبة الإلكترونية). بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسبة[48].

الرأي الثالث: في مقابل الرأيين أعلاه، فإن هذا الرأي قد نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسبة الإلكترونية أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي الذي يتطلب أن يقع الضبط على بيانات الحاسبة الإلكترونية إذا اتخذت شكلا ماديا[49].

ويذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسبة الإلكترونية يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكائنات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما شغل حيزا مادياً في فراغ معين وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسبة الإلكترونية ويمكن قياسها بمقياس معين، وإنها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقا لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية. وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم (34) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة

(47) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة،1997،ص27.

(48) Piragoff (Donald K): Computer crimes and other crimes against information technology in Canada: Rev. Intern. De. Dr. Pen. 1993. P. 241.

(49) L informatique J.C.P. 1989 333 no 16. Gassin® Le droit penal et L informatique D. 1982. p. 38

الحاسبة الإلكترونية والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[50].

وتتركز أذون التفتيش القياسية الصادرة عند التفتيش في إحدى الجرائم المعلوماتية على ضبط الوثائق المكتوبة إضافة إلى أجهزة الحاسبة وتتضمن هذه الوثائق على وجه التحديد: النسخ الضوئية، ومطبوعات الحاسبة ، وفواتير التليفون، سجلات العناوين، المذكرات والمراسلات[51].

المطلب الثالث

التفتيش عن بعد

إن طبيعة التقنية الرقمية قد عقّدت من التحدي أمام أعمال التفتيش والضبط. فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول إليها من خلال حاسبات إلكترونية تقع في الأبنية الجاري تفتيشها. وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر. وفي حين أن السلطات في بعض البلدان قد لا تنزعج من أن تقودها تحقيقاتها إلكترونيا إلى اختصاص قضائي سيادي آخر، إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج. وهذا يزيد من تعقيد مشاكل الجريمة المعلوماتية العابرة للحدود ويزيد من أهمية تبادل المساعدة القانونية، ونستطيع أن نميز في هذه الصورة بين ثلاثة احتمالات على النحو الآتي:

الاحتمال الأول: اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

يُثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسبة أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم.

يرى الفقه الجنائي الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم (103) من قانون الإجراءات الجنائية الألماني[52]. ونجد إرهاصات هذا الرأي في المادة (88) من قانون تحقيق الجنايات البلجيكي الصادر في (23 /2000/11) التي تنص على أنه» إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان

(50) Linda Voloniono , op.cit. p. 2.
(51) Brucisterling. op.cit. P.165
(52) Kaspersen. (H.W.K.): "computer crime and other crime against Information Technology in Netherlands" R.I.D.P 1993. p. 479.

البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين : (أ) إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث.(ب) إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث» [53]. وذات الشيء نجده في القانون الاتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة، فقد توخى قانون جرائم الانترنت لعام 2001 إمكانية أن تتوزع بيانات الأدلة على شبكة حاسبات إلكترونية، ويسمح هذا القانون بعمليات تفتيش لبيانات خارج المواقع التي يمكن اختراقها من خلال حاسبات توجد في الأبنية الجاري تفتيشها. و يشير مصطلح «البيانات المحتجزة في حاسبة ما» إلى «أية بيانات محتجزة في جهاز تخزين على شبكة حاسبات تشكّل الحاسبة الالكترونية جزءا منها». فلا توجد حدود جغرافية محددة، ولا أي اشتراط بالحصول على موافقة طرف ثالث. غير أن المادة (3LB) من قانون الجرائم لعام 1914، والتي أدرجها قانون جرائم الانترنت، تشترط إخطار شاغل المبنى النائي قدر الإمكان عمليا. وهذا قد يكون أكثر تعقيدا مما يبدو عليه، إذ إنه في مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكياً، فإن المرء لا يكون متأكدا دائما من مكان وجوده[54]. كما نص مشروع قانون جرائم الحاسب الآلي في هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود[55].

الاحتمال الثاني: اتصال حاسبة المتهم بحاسبة أخرى أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

من المشاكل التي تواجه سلطة الادعاء في جمع الأدلة قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات المعلوماتية مستهدفين عرقلة الادعاء في جمع الأدلة والتحقيقات[56]. وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر الإذن من جهتها المختصة الإذن ودخوله في المجال الجغرافي لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل

(53) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مصدر سابق، ص34-35.
(54) مقتضيات تعامل أجهزة النيابة العامة مع الجريمة السيبرنية (الحاسوبية)، ورقة عمل قدمت إلى مؤتمر القمة العالمي لأعضاء ورؤساء النيابة العامة، المنعقد بالعاصمة القطرية الدوحة في الفترة من 14-2005/11/16، ص15.
(55) د. هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة،1997،ص27.
(56) Sieber (Ulrich): "computer crime and other crime against Information Technology- Commentary and Preparatory question for the colloquium of the A.I.D.P in Wurzburg" R.I.D.P 1993. p77.

دولة بسيادتها.

لذا فإن جانباً من الفقه يرى بأن التفتيش الإلكتروني العابر للحدود لا بد وأن يتم في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد تُعقد بين الدول المعنية، ومن ثم فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الاتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني[57].

وكتطبيق لهذا الإجراء الأخير، فقد حدث في ألمانيا في أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسبة الكترونية، فقد تبين وجود اتصال بين الحاسبة الالكترونية المتواجدة في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها. وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين[58].

ومع ذلك أجازت المادة (32) من الاتفاقية الأوربية بشأن الجرائم المعلوماتية التي أعدها المجس الأوربي وتم التوقيع عليها في بودابست في (2001/11/23) إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى دون إذنها في حالتين الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

ومع ذلك فإن تطبيق هذا النص يمكن ان يثير مشكلات جمة[59]، ولا مناص من التعاون الدولي في هذا المجال بمقتضى اتفاقية ثنائية أو متعددة الأطراف، أو على الأقل الحصول على إذن الدولة التي يتم التفتيش في مجالها الإقليمي، وهذا ما قامت به الشرطة اليابانية، حيث ساورها الاعتقاد بأن مجموعة من المخربين قد استخدمت أجهزة الحاسبة الإلكترونية في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كلا من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الحاسبة الإلكترونية في كل من هاتين الدولتين حتى تتمكن من الوصول إلى جذور هذه العملية الإرهابية[60].

(57) Padova (Y.): unapercu de la lutte contre la cybercriminalite en France. R.S.C. 2002. p. 765. spec. p.777
(58) Mohrenschlager "Manfred": Op.. Cit.. P. 351.
(59) Padovo(Y.): art. Prec. P. 778.
(60) Linda volonino. op.cit.p.4.

الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسبة الإلكترونية.

التنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا. فالقانون الفرنسي الصادر في (1991/7/10) يجيز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات[61].

وفي هولندا أجاز المشرع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات[62].

وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسبة بشرط الحصول على إذن تفتيش صادر من القاضي[63].

وفي اليابان أقرت محكمة مقاطعة (KOFU) سنة 1991 شرعية التنصت على شبكات الحاسبة الإلكترونية للبحث عن دليل[64].

وتفتيش نظم الحاسبة الإلكترونية يمكن أن يتم بطرق عدة، فمثلا المرشد الفيدرالي الأمريكي [65] جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق هي[66]:

تفتيش الحاسبة الإلكترونية وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

تفتيش الحاسبة الإلكترونية وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.

عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.

ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

(61) Francillon (Jacques): "les crimes in formatiques et d'aulres crimes dans le domain de technologies informatique en France" R.I.D.P.1993. p.309.

(62) Kaspersen (H.W.K.): op-cit. p500501-.

(63) Brucisterling. op. cit. p.165..

(64) Yamaguchi (Atsushi): "computer crime and other crime against Information Technology in Japan" R.I.D.P.1993. p 443 .

(65) تم وضع هذا المرشد عام 1994م، وصدر له ملحقان في عامي 1999، 1997، ولقد قام بإعداده مجموعة عمل في قسم جرائم الحاسبة الالكترونية والملكية الفكرية بإشراف أستاذ القانون الجنائي Orin Kerr، ولقد صدرت له عدة تعديلات آخرها كان تعديل 2002 الذي تضمن تطبيقاً للقانون الوطني الأمريكي الصادر في 2001/10/26.

(66) المرشد الأمريكي، مصدر سابق، المادة(162).

المطلب الرابع

شروط تفتيش نظم الحاسبة الإلكترونية

يمكن تقسيم شروط تفتيش نظم الحاسبة الإلكترونية إلى نوعين:

موضوعية والأخرى شكلية

أولاً: الشروط الموضوعية لتفتيش نظم الحاسبة الإلكترونية:

وتنحصر هذه الشروط في:

أ- وقوع جريمة معلوماتية: والجريمة المعلوماتية هي كل فعل غير مشروع مرتبط باستخدام الحاسبة الإلكترونية لتحقيق أغراض غير مشروعة[67]. وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنكلترا التي أصدرت قانون إساءة استخدام الحاسبة الإلكترونية (computer misuse) في 29 / 6 /1990 وفي الولايات المتحدة الأمريكية حيث صدر قانون الاحتيال وإساءة استخدام الحاسبة الإلكترونية سنة 1986 الذي طبق على المستوى الفيدرالي بالإضافة إلى قوانين بعض الولايات المتحدة الأمريكية كقانون ولاية تكساس الصادر في 9/1 /1985 بشأن الدخول غير المشروع في نظام الحاسبة وفي فرنسا صدر قانون رقم (19-88) في 5 /1/ 1988 وهو الخاص بالغش المعلوماتي. وقد أدرج المشرع الإماراتي برامج الحاسبة الإلكترونية ضمن المصنفات الفكرية المحمية بالقانون الاتحادي رقم (40) لسنة 1992 كذلك اعتبر المشرع المصري مصنفات الحاسبة الالكترونية من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة الثانية بمقتضى القانون رقم (38) لسنة 1992.

ب- تورط شخص أو أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيها: ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلاً لها أو شريكاً فيها وفي مجال الحاسبة الإلكترونية يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلاً أو شريكاً.

(67) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مصدر سابق، ص30.

ج- توافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم، لا يوجد التفتيش إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة المعلوماتية أو أشياء متحصلة منها.

د- ومحل التفتيش الخاص بنظم الحاسبة الإلكترونية هو كل مكونات الحاسبة سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة بها بالإضافة إلى الأشخاص الذين يستخدمون الحاسبة الإلكترونية محل التفتيش.

وتشمل المكونات المادية الحاسبة الإلكترونية وحدة الإدخال ووحدة الذاكرة الرئيسة ووحدة الحساب والمنطق ووحدات الإخراج وأخيراً وحدات التخزين الثانوي.

كما تنقسم المكونات المادية المعنوية للحاسبة الإلكترونية إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها، وبرامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقاً لاحتياجات العميل، وتستلزم الحاسبة بمكوناتها سالفة الذكر مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسبة وخبراء البرامج سواء كانوا مخططي برامج تطبيقات أو كانوا مخططي برامج نظم ومحليين ومهندسي الصيانة والاتصالات ومديري النظم المعلوماتية.

ثانياً : الشروط الشكلية لتفتيش نظم الحاسبة الإلكترونية :

أ- الأسلوب الآلي لتنفيذ التفتيش في نظم الحاسبة الإلكترونية : نظم القانون الأمريكي أسلوب تنفيذ التفتيش في نظم الحاسبة الإلكترونية وذلك على النحو الآتي:

الخطوة الأولى:تقتحم قوات الشرطة المكان بصورة سريعة ومن كافة منافذه في آن واحد وذلك باستخدام القدر الأعظم من القوة بافتراض أن هذا التكتيك يقلل من احتمالية وقوع إصابات بين صفوف رجال الشرطة.

الخطوة الثانية:يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الحاسبة الإلكترونية الموجودة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل إلكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كمبيوتر ، ودائماً ما تكون غرفة المعيشة ويوضعون تحت حراسة مشددة، وفي هذه الخطوة يتم تقديم التفتيش الصادر من النيابة إليهم ويتم تحذيرهم بأن كافة أقوالهم ستحسب عليهم منذ هذه اللحظة وقد تؤخذ بمثابة دليل إدانة ضدهم ودائماً ما سنجد لدى العديد منهم الكثير من الحديث وخاصة إذا ما كانوا أولياء أمور

غافلين عن حقيقة ما يحدث بمنزلهم، وفي مكان ما من المنزل، سنجد النقطة الساخنة – جهاز الحاسبة الإلكترونية متصلاً بخط تليفون أو ربما نجد أكثر من جهاز وأكثر من خط في المنزل الواحد، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين.

الخطوة الثالثة:توضع النقطة الساخنة في عهدة فريق يضم اثنين من العملاء (مكتشف ومسجل) ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريباً متقدماً على نظم المعلومات ودائماً ما يقوم بهذا الدور العميل المعني بالقضية والذي عاصرها منذ البداية واستصدر إذن بالتفتيش الخاص بها من القاضي فهذا الشخص يعرف تماماً الشيء أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماماً ولن نتجاوز إذا ما قلنا إنه هو الذي يقوم بفتح الأدراج والبحث عن الأقراص الممغنطة والملفات وحاويات الأسطوانات ... الخ.

أما المسجل فيتولى تصوير كافة الأجهزة والمعدات على الهيئة التي تم ضبطها عليها، ويقوم المسجل كذلك بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعي أحد المجرمين الماكرين ان الشرطة قد سرقت منزله في أثناء التفتيش.

ب- فريق التفتيش: هو الفريق المعني بإجراءات التحقيق وهو جزء داخل فريق الإغارة الذي يضم بجانب فريق التفتيش والضبط رجال الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والعمال المهرة والسائقين وخبراء مسرح الجريمة العادية الملائمين للجريمة موضوع التحقيق، ويتكون فريق التفتيش والضبط من:

1 - المشرف على التحقيق:

الذي يجب أن يكون من ذوي الخبرات الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة ويتولى المشرف إدارة العمل في مسرح الجريمة وتوزيع المهام على أعضاء الفريق.

2 - فريق أخذ الإفادات:

ويحدد عدد أعضاء هذا الفريق حسب حجم الجريمة والمتورطين فيها وعدد الشهود الذين قد يوجدون في مسرح الجريمة وعليه قد يكون الفريق من شخصين أو أكثر.

3 - فريق الرسم والتصوير:

ويضم شخصاً أو أكثر يقومون برسم الخرائط لمسرح الجريمة وتحديد موقع الأجهزة والملفات والأشخاص والتقاط الصور الفوتوغرافية والتصوير بالفيديو، مع مراعاة أن يتم تنبيه جميع العاملين في مسرح الجريمة عند استعمال الفيديو تحسباً لتسجيل أصوات المشاركين في التفتيش.

4 - فريق التفتيش العملي:

ويضم شخصاً واحداً أو أكثر حسب الأحوال ويتولى هذا الفريق عملية البحث والتدقيق على مسرح الجريمة وفقاً للنظم الفنية التي تتبع في تفتيش الأماكن وتفتيش مسرح الجريمة ويقوم هذا الفريق بالمرور على جميع الغرف والمخازن ويفحص المخازن والمخابئ وليس من الضروري أن يكون أعضاء هذا الفريق من خبراء الحاسبة ولكن يفضل أن يتم تنويرهم بالأشياء التي ينبغي البحث عنها.

5 - فريق التأمين والقبض:

ويعنى هذا الفريق بالسيطرة أمنياً على مسرح الجريمة وضبط مخارجها ومنافذها وحركة الموجودين بالمبنى والمباني المجاورة لمسرح الجريمة، وتنفذ عملية القبض على المشتبه فيهم واحتجازهم وفق ما يأمر به المشرف ويتكون هذا الفريق من رجال الأمن بالزي الرسمي.

6 - فريق ضبط وتحرير الأدلة:

ويضم هذا الفريق اثنين أو أكثر من خبراء الحاسبة الإلكترونية يتولون ضبط وإدخال المعلومات المضبوطة في الحاسبة الإلكترونية وتصنيف الأدلة وتحريزها في الصناديق ووضع العلامات الموضحة عليها ويقوم هذا الفريق بنقل أجهزة الحاسبة الإلكترونية المضبوطة بعد إجراءات الرسم والتصوير ويجب ان يكون من بين أعضاء هذا الفريق شخصان على الأقل أحدهما محقق في مجال الحاسبة الإلكترونية، والثاني خبير في الحاسبة الإلكترونية مدرب على التعامل مع الأدلة وطرق تقييمها.

7 - خبير مسرح الجريمة العادية:

ويتم اختيارهم حسب الحال وقد يحتاج المحقق في بعض جرائم الحاسبة كامل أعضاء الفريق أو بعضهم مثل خبراء البصمات، المهندسون، وخبراء المتفجرات ... الخ.

المبحث الرابع

الضبط

الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أم شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة[68]. ويقصد بالضبط في قانون الإجراءات وضع اليد على شيء يتصل بجريمة وقعت

(68) د. عوض محمد، المبادئ العامة في قانون الإجراءات الجنائية ، دار النهضة العربية،القاهرة، 1999، ص381.

ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق.

وتتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليه دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال.

الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلاً للضبط بالمعنى الدقيق وإذا كان قانون الإجراءات يتحدث في بعض التصرف عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماماً عن ضبط الأشياء.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك فإنه يستوي أن يكون الشيء المضبوط مملوكاً للمتهم أو لغيره، والقاعدة أن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلاً للضبط والشرط اللازم لصحته أن يكون الشيء مفيداً في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه ولأن الضبط في الجريمة المعلوماتية قد يكون محله شيئاً مادياً أو بيانات معالجة إلكترونياً، فقد تم تقسيم هذا المبحث إلى مطلبين، تناولنا في المطلب الأول الأشياء المادية وفي المطلب الثاني البيانات الإلكترونية.

المطلب الأول

الأشياء المادية

الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات جرائم الحاسبة الإلكترونية ونسبتها إلى المتهم هي:

1. **الورق:** كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدراً كبيراً من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسبة يجعل كثيراً من المعلومات يتم حفظها في الحاسبة الإلكترونية، مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة وأجهزة الحاسبة الإلكترونية والطابعات المتطورة ذات السرعة الفائقة تطبق قدراً كبيراً من الأوراق في وقت قصير؛ لذا يعد الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة. والورق أربعة أنواع:

أ- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصور للعملية التي يتم برمجتها.

ب- أوراق تالفة تتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.

ج- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.

د- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسبة الإلكترونية.

2 - جهاز الحاسبة الإلكترونية وملحقاتها.

وجود جهاز حاسبة إلكترونية مهم للقول بأن هناك جريمة ولأجهزة الحاسبات الإلكترونية أشكال وأحجام وألوان مختلفة وخبير الحاسبة الإلكترونية يستطيع أن يتعرف إلى الحاسبة الإلكترونية ومواصفاتها بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز.

3 - الحاسبة الإلكترونية، لوحة المفاتيح، والشاشة: من السهل التعرف إلى جهاز الحاسب الشخصي الذي أصبح مألوفاً اليوم فهو يتكون من وحدة المعالجة المركزية (CPU)، ولوحة المفاتيح (Keyboard) والشاشة (Monitor) ومع التطورات السريعة التي تمر بها الحاسبة الإلكترونية نجد إضافات جديدة مثل المودم (Modem) والماوس (Mouse) والسماعات (Speakers) والسيرفر (Server)، وإذا كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أن أشكالها تتغير باستمرار خاصة من حيث الحجم والهيكل ومن الضروري إطلاع العاملين في مجال التحقيق على مختلف أشكال أجهزة الحاسبة الإلكترونية فور ظهورها.

4 - أقراص الليزر.

تجد قدراً كبيراً من أقراص الليزر مع جهاز الحاسبة الإلكترونية الشخصية العادية علاوة على أن مراكز الحاسبة الإلكترونية في الشركات والبنوك قد تجد فيها ملايين من الأقراص قد تكون على غلاف القرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة وقد تجد في مكان ما أقراص الليزر ولا تجد معها أجهزة الحاسبة الإلكترونية ومع ذلك يعد جزءاً من جريمة إلكترونية متى كانت محتوياتها عنصراً من عناصر الجريمة.

5 - الشرائط المغنطة (Magnetic Tapes)

وتستعمل الشرائط المغنطة عادة للحفظ الاحتياطي وقد تكون في مكان بعيد آمن كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة.

6 - **لوحة الدوائر** (circuit boards and components)

7 - **المودم** Modem

والمودم هي الوسيلة التي تمكن أجهزة الحاسبة الإلكترونية من الاتصال ببعضها عبر خطوط الهاتف وقد تطور المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسبة الإلكترونية.

8 - **الطابعات.**

وللطابعات أنواع منها العادية ومنها طابعات ليزرية منها الملونة ومنها غير الملونة.

9 - Pcmcia cards

وتستعمل بطاقات الـ pcmcia في أجهزة الحاسبة الإلكترونية الصغيرة Notebook)) والحاسبات الإلكترونية المحمولة ((Laptop وهي في شكل البطاقات الائتمانية.

10 - البرامج اللينة والمراشد: المراشد Manuals المصاحبة للحاسبة الإلكترونية مفيدة في التعرف إلى الجهاز والبرامج المستعملة فيه.

11 - البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستعملة في إعداد تلك البطاقات تعتبر قرائن للإثبات في الجرائم الإلكترونية.

كل ذلك يعد أثراً أو جزءاً من جسم الجريمة ينبغي البحث عنه وفحصه والاستفادة منه في التحقيق علماً بأن التعامل مع مثل هذه الآثار يحتاج إلى خبرة فنية في مجال الحاسبة الإلكترونية ومعرفة بالقانون.

المطلب الثاني

البيانات الإلكترونية

في مجال الجرائم المعلوماتية، قد يكون الضبط محله بيانات معالجة إلكترونياً، عندئذ يثار التساؤل الآتي:

هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط، الذي يعني كما رأينا وضع اليد على شيء مادي ملموس؟

انقسم الفقه الجنائي إلى رأيين هما:

الرأي الأول: يرى أن بيانات الحاسبة الإلكترونية لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية[69]. ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة.

الرأي الثاني: يرى أن البيانات المعالجة إلكترونيا إن 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[70]. ويستند هذا الرأي إلى بعض النصوص التشريعية، كالمادة (7/29) من قانون الإثبات الكندي التي تنص على (أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده واخذ نسخة من المواد المكتوبة، يستوي في ذلك ان تكون السجلات مكتوبة أو في شكل إلكتروني)[71].

وهذا الخلاف دعا المشرع الجنائي في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونيا، أو إصدار تشريعات تتعلق بجرائم الحاسبة الإلكترونية، تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات، وهو ما نصت عليه المادة (39) من قانون تحقيق الجنايات البلجيكي، المدخلة في التقنين بمقتضى القانون الصادر في 23 /2000/11، حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية، وعلى البيانات المعالجة إلكترونيا(72).

وخشية من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها

بطريق التفتيش، فقد أعطت المادة (88) من قانون تحقيق الجنايات البلجيكي،

لقاضي التحقيق سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلجيكية،

أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات محل الجريمة، إن وجدت لدى دولة

(69) Kaspersen (H.W.K.): Computer crimes and others crimes against information technology in the Netherlands. Rev. int.dr.pen.1993. p.474. spec. p. 502. Motherncblager (M.). Rapp. Prec. Rev. int. dr. pen. 1993. p. 349. spec. p. 350.

(70) Spreutels(J.P.): Les crimes informatiques et d' autres crimes dans le domaine de la technologie informatique en belgique: rapp. Rev. Int. dr.pen. 1993. p. 161. spec. p. 170.

(71)Piragoff (D. K.): Computer crimes and others crimes against information technology in Canada.. report. Rev. int. dr. pen. 1993 p.201.spec.p. 340 ets.

(72) Meunier(C.): Art. Prec. P. 670.

أجنبية.

ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة[73].

ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى تحت تصرفها إلى حين انتهاء المحاكمة، ويرى البعض ضرورة حفظ نسخة أخرى لدى المحضرين بالمحكمة، خشية تلف أو ضياع النسخة الوحيدة الموجودة، تحت تصرف جهة التحقيق أو المحكمة[74].

ويواجه إجراء الضبط للبيانات المعالجة إلكترونيا صعوبات منها:

حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها. من ذلك البحث في نظام إلكتروني لشركة متعددة الجنسيات.

وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية، مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط والتحفظ.

يمثل التفتيش والضبط أحيانا اعتداء على حقوق الغير، أو على حرمة حياته الخاصة، فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات.

ولضمان الحفاظ على البيانات محل البحث ومقارنتها بالنسخة المخرجة من الجهاز في حالة إنكارها من المتهم، فقد أعطى القانون البلجيكي للنيابة العامة سلطة الأمر بغلق هذه البيانات (Blocage de donees) لمنع الوصول إليها، أو إلى النسخة المستخرجة منها الموجودة لدى من يستعملون النظام (م 29 مكررا/3)[75].

ووفقا للمادة (39 مكررا) من القانون البلجيكي يتم سحب البيانات التي سبق أخذ نسخة منها من الجهاز في الحالات الآتية:

إذا كانت محلا للجريمة أو ناتجة عنها.

إذا كانت مخالفة للنظام العام أو حسن الآداب.

إذا كانت تمثل خطرا على الأنظمة الإلكترونية.

---

(73) Meunier(C.): Art. Prec. P. 669.
(74) Meunier (C.): Art. Prec. P.673.
(75) Meunier (C.): Art. Prec. P.674.

إذا كانت تمثل خطرا بالنسبة للمعلومات المخزنة أو المعالجة او المرسلة بهذه الأنظمة[76].

وقد أجازت المادة (88) من القانون البلجيكي لسنة 2000 لقاضي التحقيق في حالة امتداد البحث الإلكتروني عن أدلة الجريمة خارج نطاق بلجيكا أن يحصل على نسخة من البيانات التي يحتاجها. وهذا معناه أن الحصول على هذه النسخة يتم دون إذن الدولة التي توجد في نطاق إقليمها البيانات المطلوبة، ويبرر الفقه البلجيكي هذا النص بالقول بأن سلطة التحقيق يمكنها الدخول إلى النظام والإطلاع على البيانات المطلوبة دون ان تدرك ان هذه البيانات توجد من الناحية المادية خارج إقليم بلجيكا. والبديل لهذا النص، هو إرسال لجنة قضائية إلى الدولة المعنية وتطلب من السلطة المختصة بها ان تتحفظ على البيانات المكونة لمحل الجريمة، وتعطيها نسخة منها، وهذا يستغرق وقتا قد يدمر خلاله المتهم هذه البيانات. ومع ذلك يعترف الفقه بأن هذا النص يمثل اعتداء على سيادة الدولة.

المبحث الخامس

الشهادة

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة أوظروف ارتكابها أوإسنادها إلى متهم أو براءته منها[77]، وللشهادة في مجال الإجراءات الجنائية أهمية بالغة لأن الجريمة ليست تصرفاً قانونياً ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه وبحرص على إخفائه عن أعين الناس.

ولهذا فان العثور على شاهد يعتبر مكسباً كبيراً للعدالة ومن هنا جاءت قاعدة عدم رد الشهود. وسماع الشهود كسائر إجراءات التحقيق من الأمور التقليدية للمحقق فله أن يسمع الشهود أو يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك إلى فطنة المحقق ومرتبط بظروف التحقيق والأصل أن يطلب الخصوم سماع من يرون من الشهود غير أن للمحقق أن يجيبهم إلى طلبهم أو يرفضه وله أن يدعو للشهادة من يقدر أن لشهادته أهمية بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه، ومن المبادئ المستقرة أن الشاهد لا يرد ولو غلب على الظن أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعاً لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له أو ضده.

(76) Meunier (C.): op.cit. P.674.

(77) تعرف محكمة النقض المصرية الشهادة بأنها تقرير لشخص لما يكون قد راه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه (نقض 1976/1/25 أحكام النقض س 27 ص 94 رقم 20 و1978/2/6 س 29 ص 139 رقم 25 و1979/4/2 من 27ص 94 رقم 20 و2978/2/6 س 29ص 139 رقم 25 و1979/4/2 س30 ص426 رقم 90.

المطلب الأول

التعريف بالشاهد في الجريمة المعلوماتية

الشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسبة الإلكترونية والذي تكون لديه معلومات جوهرية أو مهمة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزاً له عن الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها:

1. القائم على تشغيل الحاسبة الإلكترونية:

وهو المسئول عن تشغيل الحاسبة الإلكترونية والمعدات المتصلة بها ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج[78].

2. 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 يقومون بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسبة الداخلية أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسبة بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

3. المحللون:

المحلل وهو 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

(78) د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة،1991، ص23.

التي يمكن مكننتها بواسطة الحاسبة الإلكترونية.

4. مهندسو الصيانة والاتصالات:

وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسبة بمكوناتها وشبكات الاتصال المتعلقة بها.

5. مديرو النظم:

وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[79].

ويحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية شهود الجريمة المعلوماتية في:

أ. محلل النظم الذي صمم وحدد برنامج الحاسبة الإلكترونية الذي أنتج الدليل.

ب. المبرمج الذي قام بتحرير البرنامج واختباره.

ج. المشغل الذي يقوم بتشغيل البرنامج.

د. طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو أسطوانة).

هـ. أمناء مكتبة الأشرطة الذين يتحملون مسئولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة.

و. مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.

ز. موظفي المدخلات والمخرجات والمسئولون عن معالجة المدخلات المستخدم في تنفيذ برامجه.

ح. المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الحاسبة الإلكترونية ويستخدم نواتجها[80].

(79) د. محمد فهمي طلبة، الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر ، مطابع الكتاب المصري لحديث،القاهرة،1992،ص62.

(80) محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية والمنشور على شبكة الانترنيت،موقع الدليل الالكتروني للقانون العربي والمتاح على الرابط الالكتروني www.arablawinfo.com

المطلب الثاني

التزامات الشاهد المعلوماتي

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات بحثاً عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟

هناك اتجاهان في هذا الصدد:

الاتجاه الأول:

يرى أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة.ويميل إلى هذا الاتجاه الفقه الجنائي الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسبة على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[81].

وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[82].

الاتجاه الثاني:

يرى أنصار 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 الجنائي الفرنسي أن القواعد العامة في مجال الإجراءات الجنائية تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم(83)،ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائياً إلا في مرحلة التحقيق والمحاكمة(84).

وفي هولندا يتيح مشروع قانون الحاسبة الإلكترونية لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن

(81) Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P. 1993 P. 351.

(82) Erman (Sahir) ،les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie R.I.D.P. 1993.P. 64.

(83) أنظر نص المواد (62، 109، 138) من قانون الإجراءات الجنائية الفرنسي.

(84) Jacques francillon. op.cit.p.309

كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسبة وكانت مصلحة التحقيق تستلزم التحقيق الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات[85].

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسبة على كلمة المرور السرية للولوج في نظام المعلومات، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسبة وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة[86].

(85) Kasbersen, op.cit. p. 496

(86) أنظر نص الفقرة(1) من المادة (223) من قانون الإجراءات الجنائية اليوناني.

الخاتمة

أولاً : النتائج

لقد تناول البحث موضوع إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، وهو أحد إفرازات ثورة المعلومات، فهذه الثورة كما نعلم على قدر ما أسعدت البشرية ويسرت لها سبل الحياة، فقد أتعستها بنوعية جديدة من الجرائم التي ساهمت هذه الثورة في ارتكابها والتي تتميز بطبيعة فنية وعلمية معقدة، ويتصف مرتكبوها بطبيعة ذكية ماكرة.

وعلى الرغم من وجود تشابه كبير بين التحقيق في الجرائم المعلوماتية وبين التحقيق في الجرائم العادية فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة عن الأسئلة المشهورة لدى المحقق:

ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟

تظل الجرائم المعلوماتية تمتاز عن غيرها من الجرائم ببعض الخصائص وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف إلى مرتكبيها بالسرعة والدقة اللازمتين فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الاطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسبة الإلكترونية، وملفات تسجيل العمليات الحاسوبية، بالإضافة إلى الاطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها.

حيث إن الكثير من مراحل التحقيق الابتدائي سوف يتم في بيئة رقمية، من خلال التعامل مع الحاسبات والشبكات ووسائط التخزين ووسائل الاتصال.

مما تقدم يتضح لنا أن التحري والبحث والتحقيق وجمع الأدلة في مجال الجرائم المعلوماتية يكتنفه الغموض، وتحيط به العديد من الصعاب، إلا انه لا مناص من مواصلة البحث والتحقيق وجمع الأدلة مع التطوير المستمر لوسائل البحث، ولأجهزة الشرطة وسلطات التحقيق، وتدعيم التعاون الدولي في هذا المجال.

لقد توصل البحث من خلال هذه الدراسة إلى النتائج الآتية:

1. أظهر البحث أن هناك قصوراً واضحاً في الكثير من التشريعات الجنائية الإجرائية العربية في مواجهة ظاهرة الإجرام الإلكتروني، فما زال الكثير منها يخضع هذه الجرائم للنصوص

التقليدية وهو ما قد يترتب عليه الاعتداء على مبدأ شرعية الجرائم والعقوبات من جهة، وإفلات الكثير من الجناة من العقاب من جهة أخرى.

2. ألقى البحث الضوء على كل من الحقيقة العلمية والحقيقة القضائية وانتهى إلى أن الحقيقة العلمية قد تشوش وتضلل الحقيقة القضائية، وهو ما يلقي مزيداً من الأهمية لتدريب الخبراء والمحققين والقضاة لأجل فهم هذه الحقيقة العلمية والعمل على مطابقة الحقيقة القضائية لها على قدر المستطاع.

3. إن الخطأ في إجراء التفتيش وضبط الأدلة قد يؤدي إلى فوات فرصة كشف الجريمة أو فوات الإدانة حتى مع معرفة الجاني.

ثانياً: التوصيات

على ضوء هذه النتائج، فإن البحث قد توصل إلى المقترحات الآتية:

أولاً : ضرورة إعداد الكوادر الأمنية، وسلطات التحقيق من الناحية الفنية للبحث والتحقيق الابتدائي وجمع الأدلة في مجال الجرائم المعلوماتية، مما يستلزم إنشاء مراكز متخصصة في البلاد العربية تحقيقا لهذا الغرض.

ثانياً : ضرورة تطوير التشريعات العربية القائمة سواء الموضوعية أو الإجرائية بإدخال نصوص التجريم والعقاب والنصوص الإجرائية اللازمة أو إصدار تشريعات جديدة لمواجهة هذه الظاهرة المستحدثة من الجرائم المعلوماتية، وليس هذا الأمر بعيد المنال على الدول العربية التي كرمها الله وجعلها خير الأمم، فإنه يكون حقيق بها بأن تكون كذلك واقعاً وفعلاً.

ثالثاً: ضرورة التعاون بين الدول العربية المختلفة بتبادل المعلومات والخبرات والتعاون في المجال الأمني والقضائي بصوره المختلفة فضلاً عن التعاون بينها وبين الدول الأخرى في هذا المجال، وأسوة بالتعاون الدولي المتمثل بالاجتماع الذي عقدته مجموعة الدول الصناعية الثمانية عام 1997 حول جرائم الشبكات (cyber crimes) مع اجتماعات دورية أخرى عقدت في باريس.

رابعا : ضرورة عقد اتفاقية عربية مشتركة لمواجهة ظاهرة الجرائم المعلوماتية على غرار الاتفاقيات العربية الأخرى ومنها الاتفاقية العربية لمكافحة الإرهاب، فيجب على الدول العربية أن تعد العُدة لمواجهة ظاهرة الإجرام الإلكتروني التي من المنتظر أن تتزايد في المستقبل نتيجة للتطور العلمي المستمر الذي أحدثته ثورة المعلومات بحيث تجني ثمار هذه الثورة، حيث يجب علينا مسايرة ركب التقدم العلمي في مختلف مجالات الحياة.

خامسا : ضرورة عقد الندوات والمؤتمرات العربية لبحث سبل مواجهة الإجرام الإلكتروني.

سادساً: ضرورة إعداد كوادر قضائية للبحث والتحقيق والمحاكمة في نطاق الجرائم المعلوماتية مع استحداث قواعد مناسبة في مجال الإجراءات الجنائية بشأن التحقيق الابتدائي في الجرائم المعلوماتية.

سابعاً: اعتبار المال المعلوماتي المعنوي على قدم المساواة في الحماية الجنائية مع الأموال المنصوص عليها في قوانين العقوبات التقليدية العربية والاعتراف بإمكان إتلاف هذا المال وتقرير العقوبة عنها المقرر أصلاً على إتلاف المال المادي.

ثامناً: إنشاء مركز قومي عربي لأمن الحاسبات والمعلومات وضمان عدم إصابتها بالفيروس، وأسوة بما قامت به فرنسا عندما أنشأت عام 2000 مكتباً مركزياً لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات تابعاً لوزارة الداخلية، كما استحدث جهاز (FBI) الامريكي في عام 2000 مركز خاصاً بمكافحة جرائم الإنترنت مهمته مجابهة الجرائم المعلوماتية.

تاسعاً: وفي موضوع ضبط الأدلة، نقترح ما يلي:

أ. تشجيع المجنى عليهم بالإبلاغ عن أية جريمة إلكترونية فور ملاحظتها.

ب. حث العاملين على النظام المعلوماتي على معاونة جهات التحقيق لضبط البيانات.

ج. من الضروري اتباع القواعد الفنية اللازمة لحماية البيانات وتجنيبها خطر الإتلاف.

د. إعطاء أوسع الصلاحيات لجهات التحقيق لاختراق نظام الحاسبة الإلكترونية وضبط ما يحويه من بيانات مخزنة دون إشعار مسبق بعملية التفتيش والضبط.

عاشراً: يلزم تعديل قوانين ونظم الإجراءات الجنائية بالقدر الذي يسمح ببيان الأحكام اللازم اتباعها حال إجراء التفتيش على الحاسبات الإلكترونية وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني، حتى يستمد الدليل مشروعيته، كما ينبغي السماح لسلطات التحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل والكشف عن الحقيقة. ومن ثم يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسبة إلكترونية أخرى يمكن أن تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات.

وأخيراً يكون هذا البحث قد اكتملت عناصره، فإن كان فيه كمال فهو لله سبحانه وتعالى، وإن اعتراه النقص فهو مني، ولم لا وأنا بشر أجتهد فأخطئ وأصيب، فإن أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين. ولله الأمر من قبل ومن بعد، والحمد لله رب العالمين.

المصادر والمراجع

أولاً: الكتب العربية.

د. عوض محمد، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية،القاهرة، 1999.

د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، دار النهضة العربية،القاهرة، 2001.

د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة،1991.

د. محمد فهمي طلبة، الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر ، مطابع الكتاب المصري الحديث،القاهرة،1992.

د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

د. هشام محمد فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية،ط1،دار النهضة العربية،القاهرة، 1994.

د. هلالي عبد أللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، 1997.

ثانياً: الرسائل العلمية والبحوث.

د.عبد الله حسين علي محمود،إجراءات جمع الأدلة في مجال سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، إمارة دبي بدولة الإمارات العربية المتحدة 26-2003/4/28.

محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية.

د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1-2000/5/3.

محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت» دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية»، رسالة ماجستير، كلية الدراسات العليا،جامعة نايف العربية للعلوم الامنية،الرياض،2004.

د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3،دار النهضة العربية،القاهرة، 1998.

القاضي وليد عاكوم ، التحقيق في جرائم الحاسوب، بحث منشور على شبكة الانترنت، موقع الدليل الإلكتروني القانوني العربي www.arablawinfo.com .

ثالثا.مواقع الانترنيت.

www.secretservice.gov/electronic__evidence.shtml

www.ists.dartmouth.eud/TAG/need/ISTS__NA.pdf

www.acpr.gov.au/pdf/ACPR101.pdf 212003/10/

www.secretservice.gov/electronic__evidence.shtml

www.arablawinfo.com

رابعاً: الكتب الفرنسية.

Conseil de Leurpe (1996). Problems de procedure penale lies a la technologie de l information. Recommendation n. R(95) 13 et expose des motifs. Ed. Conseil de l Europe.

Erman. Sahir (1993). Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie R.I.D.P.

Francillon. J. (1993). Les crimes in formatiques et d' autres crimes dans dommaine de la technologie informatique. Rev. Int. dr. pen.

L informatique J.C.P. 1989 333 no 16. Gassin® Le droit penal et L informatique D. 1982.

Meunier. C. (2002). La loi du 28 Nov. 2000 relative a la criminalite

informatique. Rev. Dr. pen. Crim.

O.C.D.E. (1986). La fraud liee a l'informatique. Paris.

Padova. Y. (2002). Un apercu de la lutte contre la cybercriminalite en France. R.S.C.

Pinguet. M. (1996). La douane et la cyber-delinquance G.P.

Spreutels. J.P. (1993). Les crimes informatiques ET d' autres crimes dans le domaine de la technologie informatique en Belgique. Rev. Int. dr. pen.

خامساً: الكتب الانكليزية.

Davis. David (1998). Internet Detective: An Investigator's Guide. West Midland. UK: Police Research Group.

Franklin Clark den Dilbert. Investigation computer crime.

Institute for security Technology Studies (ISTS) (2002). Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment.

Kaspersen. H.W.K (1993). computer crimes and others crimes against information technology in Netherlands. Rev. Int. dr. pen.

Mohrenschlager. M. (1993). computer crimes and others crimes against information technology in the Germany. Rev. Int. dr. pen.

Philip. M. (1986). Stanley computer crime investigation and investigators computer & security. Nort Holland.

Piragoff (Donald K) (1993): Computer crimes and other crimes against information technology in Canada: Rev. Intern. De. Dr. Pen..

Sammes، T. & Jenkinson، B. (2000). Forensic Computing: A pratitioner's Guide London: Springer.

Shindre، Debra (2000). Scene of the Cyber crime: Computer Forensics Hand Book. Rockland، MA: Syngress Publishing.

Sieber (Ulrich): "computer crime and other crime against Information Technology-Commentary and Preparatory question for the colloquium of the A.I.D.P in Wurzburg" R.I.D.P 1993.

Taylor، R. (1992). Computer crime، "in criminal investigation edited" by Charles Swanson، n. chamelin and L. Territto، Hill، inc. 5 edition.

Thompson، David (1990). Computer Crime The Improvement of Investigative Skills: Final Report: Part Two.

United States Secret Service (USSS) (2002). Best Practices for Seizing Electronic Evidence.

Vassilaki، Irini، computer crimes and other crimes against information technology in Greece. Rev. Intern De. Dr. Pen.

Yamaguchi، Atsushi (1993)، "computer crime and other crime against Information Technology in Japan" R.I.D.P.

سادساً: القوانين.

1 - قانون تحقيق الجنايات البلجيكي.

2 - قانون الإجراءات الجنائية الألماني.

3 - قانون الإجراءات الجنائية الفرنسي.

4 - قانون الإجراءات الجنائية اليوناني.

5 - القانون الجنائي الكندي.

6 - قانون الإثبات الكندي.