إجراءات التحقيق الابتدائي في الجريمة المعلوماتية

(دراسة مقارنة)

علي عدنان الفيل(*)

أولا- المقدمة:

أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات وتدفقها في العقود الثلاثة الأخيرة، ثورة إلكترونية تطبق الآن في كل مجالات الحياة، وأضحى من الصعوبة بمكان الاستغناء عن خدماتها وفوائدها العظيمة والمتنامية. وقد تميل النفس البشرية أحيانا إلى فعل الشر؛ إذ يستغل بعض الأشرار المكتشفات العلمية وما تقدمه من وسائل متقدمة في ارتكاب كثير من الجرائم التقليدية، مستغلين الإمكانات الهائلة لهذه المخترعات، أو استحداث صور أخرى من الإجرام، ترتبط بهذه التقنيات الحديثة التي تصير محلا لهذه الجرائم، أو وسيلة لارتكابها. وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين خاصة، بصورة أدت إلى بزوغ فجر ظاهرة إجرامية جديدة، تعرف بالإجرام المعلوماتي، أو الإجرام الإلكتروني

.(La delinquance informatique, ou la cybercriminalite)

فقد تم السطو على المصارف بمساعدة هذه المكتشفات الجديدة، ونمت الجريمة المنظمة، وترعرعت، في ظل هذه الثورة العلمية، في نطاق المعلومات والاتصالات، وعلى وجه التحديد جرائم الإرهاب، وتجارة المخدرات، والاتجار بالسلاح، والدعارة المنظمة باستخدام الإنترنت، وارتكب كثير من

(*) مدرس القانون الجنائي المساعد، كلية الحقوق - جامعة الموصل - العراق.

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 فى المدخلات وفى البرامج، والنسخ غير المشروع للبرامج، وكثير من الجرائم المتعلقة بالتجارة الإلكترونية، وإتلاف الأجهزة الإلكترونية، وإتلاف السجلات المدونة على الحاسب الإلكتروني[2]، وبث الصور والأفلام الجنسية من خلال الأجهزة، والقذف والسب عن طريق البريد الإلكتروني، وغسيل الأموال القذرة باستخدام النقود الإلكترونية[3].

وخطورة هذه الظاهرة الإجرامية المستحدثة، أن الجريمة يسهل ارتكابها على هذه الأجهزة أو بوساطتها، وأن تنفيذها لا يستغرق فى أكثر الأحيان إلا دقائق معدودة، وأحيانا يتم فى بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه الجانى عقب ارتكابه للجريمة، فضلا عن أن مرتكبى هذه الجرائم، خاصة فى نطاق الجريمة المنظمة، يلجأون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية فى أنظمة إلكترونية، مع استخدام شفرات أو رموز سرية، لإخفائها عن أعين أجهزة العدالة؛ وهو مما يثير مشكلات كبيرة فى جمع الأدلة الجنائية، وإثبات هذه الجرائم.

تستدعى خصوصية الجرائم المتعلقة بالحاسب الإلكترونى، أن يتم تطوير أساليب التحقيق الجنائى وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن رجل الشرطة والمحقق من كشف الجريمة، ومعرفة مرتكبيها، بالسرعة والدقة اللازمين.

ولتحقيق ذلك يجب من ناحية تدريب الكوادر التى تباشر التحريات والتحقيقات، مع الاستعانة بذوى الخبرة الفنية المستمرة فى هذا المجال، فضلا عن تطوير الإجراءات الجنائية، لتحقيق الغرض المطلوب، وهو ما بدأت

التشريعات منذ بضع سنوات فى تحقيقه، ومنها القانون البلجيكى الصادر فى ٢٠٠٠/١١/٢٣.

ثانيا- مشكلة البحث:

أثارت ظاهرة الإجرام الإلكترونى كثيرا من المشكلات فى نطاق القانون الجنائى الإجرامى؛ إذ وضعت نصوص قانون أصول المحاكمات الجزائية لتحكم الإجراءات المتعلقة بجرائم تقليدية؛ إذ لا توجد صعوبات كبيرة فى إثباتها، أو التحقيق فيها، وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ حرية القاضى الجنائى فى الاقتناع، وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

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

وقد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، فيصعب إثباتها، ويثور التساؤل عن حرية تدفق المعلومات،

وهل يصلح تدفق البيانات الموجودة خارج الدولة المتعلقة بالجريمة محل البحث؟

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

ومن المشكلات الإجرائية التى يثيرها هذا النوع من الجرائم مدى التزام الشهود أو المشتبه بهم، فى كشف الرموز أو الأرقام أو كلمات السر المتعلقة بالبيانات أو البرامج ذات الصلة بالجريمة. كذلك يثور التساؤل عن مدى حجية المخرجات الإلكترونية فى الإثبات، نظرا إلى طبيعتها الخاصة، مقارنة بوسائل الإثبات التقليدية.

١ – تدريب الكوادر والاستعانة بالخبرة الفنية:

أ- تدريب الكوادر:

إن طبيعة الجرائم ذات الصلة بالحاسب الإلكترونى تقتضى معرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة استعمالها من قبل مستخدمها. ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحرى، والمباشرين للتحقيق فى مجال الجرائم المعلوماتية، إلى الحد الذى دعا بعض الباحثين إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة فى هذا المجال.

ويجب أن يشتمل التدريب على كيفية تشغيل الحاسبات، بعد تعرف أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات،

والمعالجة الإلكترونية للبيانات والجرائم التى تقع على الحاسبات، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن الحاسبات، ووسائل اختراقها، مع دراسة حالات لجرائم وقعت سلفا، وكيف تم مواجهتها.

وفى كثير من بلدان العالم، تعتمد الدورات التدريبية المتخصصة لرجال الشرطة وأعضاء النيابة العامة، سواء فى مراكز تابعة لوزارة الداخلية، أو فى المراكز المتخصصة التابعة لوزارة العدل، كما هى الحال فى أمريكا وبريطانيا، وكندا.

وعند الحديث عن المهارات الفنية التى ينبغى للمحقق أن يكتسبها فى الجرائم المعلوماتية، فإننا لا نقصد بها المهارات التقليدية التى يجب أن يتمتع بها كل محق، فهى مهارات أساسية يفترض بداهة توافرها فى المحقق بالضرورة، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعد من أساسيات التحقيق التى لا يتوقع أحد عدم توافرها لدى المحقق.

وعليه، فإن التركيز هنا سينصب على تلك المهارات التى تتسم بالجدة والحداثة، وتعد إفرازا للتطور الإنسانى، فى مجال تقنية الاتصالات والحوسبة، وأمرا مستجدا على من يتعامل مع هذه الجرائم المستحدثة، وهى:

١ـ معرفة المكونات المادية للحاسب الإلكترونى والتعامل المبدئى معها:

المهم هنا أن يتمكن المحقق من معرفة الشكل المميز للحاسبات الإلكترونية وملحقاتها ومسمى كل منها، والهدف من استخدامه، وما احتمالات توظيفه لارتكاب أى من الجرائم المعلوماتية؛ إذ إن عدم معرفته بها قد يؤدى إلى إهمالها، أو حتى إتلافها بدون قصد، أو تعديل البيانات الموجودة فيها، نتيجة الجهل بها[٤].

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

واكتساب هذه المهارة يعد أحد الأهداف المرجوة من البرامج التدريبية الخاصة بالتحقيق فى الجرائم المعلوماتية لدى كثير من الدول (كالولايات المتحدة، وكندا، وأستراليا)[٥].

٢ـ معرفة أساسيات عمل شبكات الحاسب الإلكترونى وأهم مصطلحاتها:

كثير من الجرائم المعلوماتية يرتكب من خلال شبكة الإنترنت، ومن ثم فإن المحقق محتاج إلى معرفة مبادئ الاتصال الشبكى، وأنواعه المختلفة، وكيفية انتقال البيانات من جهاز إلى آخر على شكل حزم، ومبادئ البروتوكولات الرئيسة الخاصة بالاتصال بالشبكة[٦].

وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات فى كونها ضرورة لتصور كيفية ارتكاب الفعل الإجرامى فى فضاء الإنترنت (Cyber-space)، من اختراق للشبكات والحاسبات، واعتراض حزم البيانات فى أثناء انتقالها من خلال الشبكة، والتجسس عليها، وتحويل مسارها. كما أنها تعطى المحقق تصورا جيدا عن مدى إمكان متابعة مصدر الاعتداء على الشبكة، والمعضلات الفنية التى تحول دون ذلك[٧].

٣ـ تمييز أنظمة تشغيل الحاسب الإلكترونى والتعامل المبدئى معها:

يجب أن يكون لدى المحقق على الأقل، فهم مبدئى بأنواع الأنظمة التشغيلية لأجهزة الحاسب الإلكترونى، وخصائص كل نظام ومميزاته، ومبادئ أنظمة الملفات التى يعتمد عليها[٨].

إن معرفة المحقق الجنائى الأولية بهذه الأنظمة ضرورية، حتى يشارك فى متابعة مسرح الجريمة وفحصه وتفتيشه، وأحيانا يجد المحقق نفسه أمام موقف فنى صعب، يجب أن يتخذ قرارا بشأنه، بالتشاور مع الخبير. وبدون توافر الحد الأدنى من المعرفة التقنية لهذا المحقق؛ فإن القرار على الأرجح سوف يكون للخبير وحده.

وأكثر أنظمة التشغيل شيوعا وشهرة التى يجب أن تتوافر فى أى برنامج تدريبى هى: أنظمة (Windows) وأنظمة (Unix, Macintosh and Linux).

٤- تعرف الصيغ المختلفة للملفات وتطبيقات الحاسب الإلكترونى الرئيسة التى تتعامل معها:

تعد الملفات الوعاء الحقيقى لأدلة الإدانة فى كثير من القضايا المتعلقة بشبكة الإنترنت، بما تحويه من معلومات[٩]، ومن ثم فإن قدرة المحقق على معرفة صيغ هذه الملفات، وما يمكن أن تحويه، ومعرفته بأهم التطبيقات التى يمكنه من خلالها قراءة محتوى هذا الملف أو سماعه أو مشاهدته، يعد أمرا غاية فى الأهمية.

٥- إجادة التعامل مع خدمات الإنترنت الرئيسة:

تمثل شبكة الإنترنت أداة جمع وتحريات مناسبة للمحقق؛ إذ إنها خلقت مجتمعا افتراضيا شبيها إلى حد ما بالمجتمعات الحقيقية، ويدور فى مجتمع الإنترنت هذا كثير من الحديث الذى قد يفيد المحقق فى توضيح غموض بعض الجرائم[١٠]. ومن الممكن أيضا أن يستخدم الإنترنت أداة تعليمية للاطلاع على مستجدات جرائم الحاسب الإلكترونى والإنترنت، وطرق التصدى لها، ووسيلة اتصال وتبادل للمعلومات فيما بين أعضاء السلطة التحقيقية.

٦ـ معرفة الأدوات والأساليب المستخدمة فى ارتكاب الجرائم المعلوماتية:

إن معرفة رجال العدالة بهذه الأساليب وكيفية استخدام هذه الأدوات يعد أمرا غاية فى الأهمية، خاصة لمن يتولون مناقشة الشهود واستجواب المتهمين، فبدونه لن يستطيعوا طرح الأسئلة التى تتصل مباشرة بالسلوك الإجرامى وأسلوب ارتكابه. كما أنها تساعد المحقق على التواصل مع خبير الحاسب الإلكترونى الجنائى عند شرح الأخير ما توصل إليه من أدلة أو قرائن عن الأساليب المستخدمة فى ارتكاب الجريمة والأدوات التى تساعده على القيام بذلك.

٧ـ معرفة أهم تقنيات أمن الحاسب الإلكترونى والإنترنت وأدواتها وطريقة عملها:

اكتساب هذه المهارة وإن كان يبدو فى الظاهر أمرا معقدا بعض الشىء؛ فإن الأمر فى حقيقته ليس كذلك؛ إذ إن المطلوب أن تعين معرفة هذه التقنيات المحقق على استيعابها وربطها بمجريات التحقيق بشكل عام، وليس أن يجعله خبيرا فيها.

٨ـ الاطلاع على بعض الجوانب المتعلقة بالجرائم المعلوماتية:

تتميز هذه الجوانب بأنه يغلب عليها الطابع النظرى؛ إذ يمكن اكتسابها من خلال القراءة والاطلاع، سواء من خلال المطبوعات أو الإنترنت، ومن أهم هذه الجوانب:

أ- الواقع الحالى والاتجاهات المستقبلية للجرائم المتعلقة بشبكة الإنترنت.

ب- الفئات المختلفة التى ينقسم إليها مرتكبو هذه الجرائم، والخصائص المشتركة التى تميز كل فئة.

ج- معرفة التشريعات المختلفة المتعلقة بهذه الجرائم وفهمها، والإلمام باتجاهات القوانين والتشريعات فى البلدان المختلفة.

د- دراسة بعض القضايا المشهورة وتحليلها، للاستفادة من تجارب رجال العدالة فى مواجهة هذه الجرائم.

هـ- الوقوف على الأبعاد الدولية لهذه الجرائم، وآليات التعاون المشترك بين الدول، وتعرف الاتفاقيات والمعاهدات الموجودة بهذا الخصوص.

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

ب- الخبرة الفنية:

يرى المحقق فى بعض الأحيان، ضرورة الاستعانة بالخبير، لإيضاح مسألة تستعصى ثقافته العامة على فهمها؛ كتحديد سبب الوفاة، أو ساعتها، أو رفع بصمة وجدت فى مكان الجريمة، أو فحص سيارة لبيان ما فيها من خلل.

ومنذ بدء ظهور الجرائم ذات الصلة بالحاسب الإلكترونى، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة فى مجال الحاسب الإلكترونى، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق على كشف جوانب الغموض فى العمليات الإلكترونية الدقيقة، ذات الصلة بالجريمة محل التحقيق؛ إذ تكتسب الخبرة أهمية بالغة فى مجال الجريمة المعلوماتية؛ لأن الحاسبات وشبكات الاتصال مختلفة الأنواع، ونماذجها متعددة، لذلك فإن العلوم والتقنيات المتصلة بها تنتمى إلى تخصصات علمية وفنية دقيقة ومتنوعة، والتطورات فى مجالها

سريعة ومتلاحقة بدرجة قد يصعب على المتخصص تتبعها واستيعابها. ويمكن القول بصفة عامة، بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة فى سائر أنواع الحاسبات وبرامجها وشبكاتها، كذلك لا يوجد خبير قادر على التعامل مع كل أنماط الجرائم التى تقع عليها، أو ترتكب بوساطتها[١١].

لذا، ترك المشرع للمحقق الحرية الكاملة فى هذا الشأن، ليمكنه من كشف الحقيقة بالسرعة اللازمة، وبالطريقة التى يراها مناسبة[١٢]، وللمحقق فى أى وقت أن ينهى التحقيق إلى أن يندب من يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق، فليس فى القانون ما يلزمه بالاستجابة للمتهم، ولا لغيره من الخصوم، إذا طلبوا ندب الخبير. ومن ثم فإذا كانت الاستعانة بخبير فنى أمرا جوازيا للمحقق أو لجهة التحقيق والحكم؛ فإنه فى المسائل الفنية التى لا يمكن للقاضى أن يقطع فيها برأى من دون استطلاع رأى أهل الخبرة، فى هذه الحالة يجب عليه أن يستعين بالخبرة، فإذا تصدى للمسألة الفنية، وفصل فيها من دون تحقيقها بوساطة خبير، كان حكمه معيبا مستوجبا نقضه، وهذا المبدأ استقر عليه قضاء محكمة النقض المصرية[١٣].

وبناء عليه، فإذا كانت الاستعانة بخبير فنى فى المسائل الفنية أمرا واجبا على جهة التحقيق والقاضى؛ فهى أوجب فى مجال الجرائم المعلوماتية؛ إذ تتعلق بمسائل فنية غاية فى التعقيد، ومحل الجريمة فيها غير مادى، والتطور فى أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص، على درجة كبيرة من التميز فى مجال تخصصه، فإجرام الذكاء والفن، لا يكشفه ولا يفله إلا ذكاء وفن مماثلين.

وأهمية الاستعانة بالخبير الفنى فى مجال الجرائم المعلوماتية، تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هى أو جهة

التحقيق عن جمع الأدلة عن الجريمة، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه[١٤].

والخبير لا يشترط فيه كفاءة علمية عالية فى مجال التخصص فحسب، بل يجب أن يضاف إليها سنوات من أعمال الخبرة فى المجال الذى تميز فيه، وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الإلكترونى، فقد يتعلق الأمر بتزوير المستندات، أو بالتلاعب فى البيانات، أو بالغش فى أثناء نقلها أو بثها، أو بجريمة من جرائم الأموال، أو بالاعتداء على حرمة الحياة الخاصة، أو بعرض صور أو أفلام مخلة بالآداب العامة.

ويحدد المحقق للخبير مهمته، والميعاد الذى يقدم فيه تقريره، وعليه أن يحلفه اليمين على أن يبدى رأيه بالذمة. وهذا الإجراء جوهرى يترتب على إغفاله بطلان عمل الخبير[١٥]. والأصل أن يباشر الخبير عمله فى حضور المحقق، وتحت إشرافه، والاستثناء أن يتم ذلك فى غيابه.

وللخصوم حق الحضور فى أثناء عمل الخبير، ويجوز مع ذلك أن يباشر الخبير عمله فى غياب الخصوم، وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب. ويعد الحصول على المستندات فى خلال عملية التفتيش أمرا سهلا؛ إذ يمكن تعرفها بالرؤية، ولن يحتاج المحقق لأية مساعدة من الخبراء، ومن هذه المستندات: أدلة عمل النظام، وسجلات إدارة الحاسب الإلكترونى، ووثائق البرامج، والسجلات، وصيغ مدخلات البيانات والبرامج، وكذلك صيغ مخرجات الحاسب الإلكترونى المطبوعة. ويتم التخطيط على هذه المستندات، ويمكن تحديد ما إذا كانت كاملة، أصلية، أو صورا، من خلال استجواب القائمين على حفظها.

وقد يكون التخطيط على المواد المتعلقة بوسائل الحاسب الإلكترونى الأخرى أمرا أكثر تعقيدا؛ مثل: الأشرطة الممغنطة، والأقراص، والبرامج،

ويحتاج المحقق إلى معونة أحد الخبراء الموثوق بهم، حتى يتمكن من الإلمام بمحتويات الأشرطة أو الأقراص من دون إحداث أى تغيير فيها.

وبالطبع، فإن البحث عن المعلومات داخل جهاز الحاسب الإلكترونى ذاته يعد أمرا بالغ التعقيد، ويحتاج إلى وجود خبير[١٦]. وأهم المسائل التى يستعان فيها بالخبرة فى مجال الجرائم المعلوماتية ما يأتى:

أولا- الوصف:

أ- تركيب الحاسب، وصناعته، وطرازه، ونوع نظام التشغيل، وأهم الأنظمة الفرعية التى يستخدمها، إضافة إلى الأجهزة الطرفية الملحقة به، وكلمات المرور أو السر، ونظام التشفير... إلخ.

ب- طبيعة بيئة الحاسب الإلكترونى أو الشبكة، من حيث التنظيم ومدى توزيع عمل المعالجة الآلية، ونمط وسائط الاتصالات، وتردد موجات البث، وأمكنة اختزانها.

ج- الموضع المحتمل لأدلة الإثبات، والهيئة التى تكون عليها.

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

ثانيا- البيان:

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

ب- كيف يمكن عند الاقتضاء نقل أدلة الإثباتات إلى أوعية ورقية، بغير أن يلحقها تلف.

ج- كيفية تجسيد الأدلة فى صورة مادية، بنقلها إذا أمكن، إلى أوعية

ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[١٧].

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم المعلوماتية، القانون البلجيكي الصادر في ٢٠٠٠/١١/٢٣[١٨].

فقد نصت المادة (٨٨) من القانون المذكور على أنه يجوز لقاضي التحقيق، وللشرطة القضائية، الاستعانة بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول إليه، أو الدخول إلى البيانات المخزنة أو المعالجة أو المنقولة بوساطته، ويعطى القانون كذلك لسلطة التحقيق الحق في 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[١٩].

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 الموافقة على عملية التفتيش هذه[٢٠]. 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 أقراص مرنة، أو على أقراص ممغنطة، أو على ورق[٢١].

والتزام الخبير هو التزام ببذل عناية، فلا يساءل إذا لم يصل إلى النتيجة المطلوبة بسبب 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[٢٢].

فضلا عن التزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، ويلتزم

كذلك بالمحافظة على سر المهنة، وفى حالة إفشائه السر يعاقب بالعقوبة المقررة لهذه الجريمة[٢٣].

٢ - المعاينة:

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

والمعاينة من إجراءات التحقيق الابتدائى، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق. والأصل أن يحضر أطراف الدعوى الجزائية المعاينة، وقد يقرر المحقق أن يجريها فى غيابهم، ولا يلتزم بدعوة محامى المتهم للحضور[٢٤]. ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها[٢٥].

وتظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية؛ إذ يوجد مسرح فعلى للجريمة، يحتوى على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها، لبيان مدى صحتها فى الإثبات، فليست الحال كذلك بالنسبة إلى جرائم المعلوماتية؛ إذ يندر أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها؛ وهو ما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها[٢٦].

فمع التسليم بأهمية المعاينة فى كشف غموض كثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة والأولوية - فيما عدا حالات استثنائية - على ما عداها من الإجراءات الاستقصائية الأخرى؛ فإن دورها فى مجال كشف غموض الجرائم المعلوماتية، وضبط الأشياء التى قد تفيد فى إثبات وقوعها، ونسبتها إلى مرتكبيها، لا ترقى إلى الدرجة نفسها من الأهمية، ومرد ذلك إلى الآتى[٢٧]:

١- أن الجرائم التى تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها آثار مادية.

٢- أن أعدادا كثيرة من الأشخاص قد يترددون على المكان أو مسرح الجريمة فى خلال الفترة الزمنية الطويلة نسبيا التى تتوسط عادة بين زمن ارتكاب الجريمة واكتشافها؛ وهو ما يفسح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية، أو زوال بعضها، وهو ما يلقى ظلالا من الشك على الدليل المستمد من المعاينة.

وحتى يكون للمعاينة فى الجرائم المتعلقة بشبكة الإنترنت فائدة فى كشف الحقيقة عنها وعن مرتكبيها؛ ينبغى مراعاة عدة قواعد وإرشادات فنية، أبرزها ما يأتى[٢٨]:

١- تصوير الحاسب الإلكترونى والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة فى مكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته، ومراعاة تسجيل وقت التقاط كل صورة وتاريخه ومكانه.

٢- العناية البالغة بملاحظة الطريقة التى تم بها إمداد النظام والآثار الإلكترونية الخاصة بالشبكات الإلكترونية التى تتزود بها شبكات المعلومات بموافقة موقع الاتصال، ونوع الجهاز الذى تم عن طريقه الولوج فى النظام أو الموقع.

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

٤- وضع مخطط تفصيلى للمنشأة التى وقعت بها الجريمة، مع كشف تفصيلى بالمسئولين بها، ودور كل واحد منهم.

٥- فصل الكهرباء عن موقع المعاينة لشل فاعلية الجانى فى القيام بأى فعل من شأنه التأثير فى آثار الجريمة.

٦- إبعاد الموظفين عن أجهزة الحاسب الإلكترونى، وكذلك عن الأماكن الأخرى التى توجد بها أجهزة للحاسب الإلكترونى.

٧- عدم نقل أية معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجى لموقع الحاسب الإلكترونى من أى مجال مغناطيسى ممكن أن يتسبب فى محو البيانات المسجلة[٢٩].

٨- التحفظ عما قد يوجد بسلة المهملات[٣٠] من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة، وفحصها، ورفع البصمات التى قد تكون لها صلة بالجريمة المرتكبة.

٩- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ما قد يوجد بها من بصمات.

١٠- قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية فى مجال الحاسب الإلكترونى والشبكات ونظم المعلومات[٣١]، واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على كيفية التعامل مع نوعية الآثار والأدلة التى يحويها مسرح الجريمة المعلوماتية. ففى فرنسا مثلا يقوم فريق مكون من ثلاثة عشر شرطيا بالإشراف على تنفيذ المهمات التى يعهد بها إليه وكلاء النيابة والمحققون، وجميعهم تلقوا تدريبا متخصصا، إلى جانب اختصاصهم الأساسى فى مجال التقنية الحديثة. وهم يقومون بمرافقة المحققين فى أثناء التفتيش، فيفحصون كل جهاز، وينقلون نسخا من القرص الصلب وبيانات البريد الإلكترونى، ثم يقومون بعمل تقرير مرسل إلى القاضى الذى يتولى التحقيق. أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعادة المعلومات من القرص الصلب، كما يمكنها

قراءة الأقراص المرنة والصلبة التالفة، كما توجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات الإلكترونية المحمولة (Laptop).

وبعد وصول فريق التحقيق إلى مسرح الجريمة أو مكان الإغارة، يتم التأمين والسيطرة على المكان، والبدء فى التفتيش على النحو الآتى:

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

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

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

د- تحديد أجهزة الحاسب الإلكترونى الموجودة فى مكان الإغارة، وتحديد مواقعها بأسرع فرصة ممكنة. وفى حالة وجود شبكات اتصالات، يجب البحث عن خادم الملف (File Server) لتعطيل حركة الاتصالات.

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

و- اختيار مكان لمقابلة المتهمين والشهود، على أن يكون المكان بعيدا عن أجهزة الحاسب الإلكترونى[٣٢].

من المهم أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدة، بما فى ذلك الأدلة الرقمية، حتى يتم توضيح مكان الضبط، والهيئة التى كان عليها، ومن قام برفعه وتحريزه، وكيف تم ذلك

ومتى؟ بل إن هناك من يرى أن التوثيق يجب أن يشمل كل المصادر المتاحة على الشبكة التى ترتبط بها الأجهزة محل التحقيق.

ولعل من أبرز الأماكن التى يحتمل وجود الأدلة الجنائية المتعلقة بالجرائم المعلوماتية بها، ما يأتى:

١- **الورق**: على الرغم من أن وجود أجهزة الحاسب قلل من حجم الأوراق والملفات التقليدية المستخدمة؛ إذ يتم حفظ المعلومات والبيانات على أجهزة الحاسب الإلكترونى؛ فإننا نجد كثيرين ممن يقومون بطباعة المعلومات لأغراض المراجعة، أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، ومن ثم فهى تعد من الأدلة التى ينبغى الاهتمام بها فى البحث عن الحقيقة.

٢- **جهاز الحاسب الإلكترونى وملحقاته**: وجود جهاز الحاسب الإلكترونى مهم جدا للقول إن الجريمة الواقعة هى جريمة معلوماتية أو جريمة حاسوبية، وإنها مرتبطة بالمكان أو الشخص الذى يحوز جهاز الحاسب الإلكترونى وملحقاته. ولأجهزة الحاسب الإلكترونى أشكال وأحجام وألوان مختلفة، وخبير الحاسب الإلكترونى وحده الذى يستطيع أن يتعرفها، ويتعرف مواصفاتها بسرعة فائقة.

٣- **البرمجيات** (Software): إذا كان الدليل الرقمى ينشأ باستخدام برنامج خاص ليس واسع الانتشار؛ فإن أخذ الأقراص الخاصة بتثبيت هذا البرنامج أمر غاية فى الأهمية عند فحص الدليل[٣٣].

٤- **وسائط التخزين المتحركة**: كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة، والأشرطة المغناطيسية، والفلاش ممورى وغيرها. وتعد هذه الوسائط جزءا من الجريمة المعلوماتية، متى كانت محتوياتها عنصرا من عناصر الجريمة.

٥- **كتيبات الإرشادات** (Manuals): الخاصة بالمكونات المادية والمنطقية للحاسب الإلكتروني التي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها[٣٤].

٦- **المودم** (Modem): هو الوسيلة التي تمكن أجهزة الحاسب الإلكتروني من الاتصال فيما بينها من خلال خطوط الهاتف. وفي الوقت الحالي تطورت أجهزة المودم لتكون أجهزة إرسال واستقبال فاكس، والرد على المكالمات الهاتفية، وتبادل البيانات، وتعديلها.

٧- **الطابعات**: التي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها[٣٥].

٣ - التفتيش:

يعرَّف 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[٣٦].

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 التحقيق في الجرائم المعلوماتية وظروفه، وهو إجراء جائز قانونا، ولو لم ينص عليه صراحة، بوصفه يدخل في نطاق التفتيش بمعناه القانوني، ويندرج تحت مفهومه.

وللتفتيش في الجرائم شروط موضوعية تتعلق بما يأتي:

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

٢- الغاية منه: ضبط أشياء تفيد فى كشف الحقيقة.

أما الشروط الشكلية فتتحدد بما يأتى:

١- أن يكون الأمر بالتفتيش مسببا.

٢- حضور المتهم أو مَن ينيبه أو الغير أو مَن ينيبه، التفتيش.

٣- تحرير محضر بالتفتيش[٣٧].

ويثور السؤال عن إمكان التفتيش وفقا للضوابط السابقة، والغاية منه، فى مجال الجرائم المعلوماتية؟ والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدى يهدف إلى حفظ أشياء مادية تتعلق بالجريمة، وتفيد فى كشف الحقيقة، أما البيانات الإلكترونية فليس لها بحسب جوهرها مظهر مادى ملموس فى العالم الخارجى. ومع ذلك، يمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأقراص، ومخرجات الحاسب الإلكترونى[٣٨]. لهذا فقد أجاز الفقه والتشريعات التى صدرت فى هذا المجال، إمكان أن يكون محلّ التفتيش البياناتُ المعالجة إلكترونيا، والمخزنة بالحاسب الإلكترونى، ثم ضبطها والتحفظ عليها، أو ضبط الوسائط الإلكترونية التى سجلت عليها هذه البيانات. والتفتيش فى هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدى من ضوابط وأحكام.

وقد عرّف المجلس الأوربى هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكترونى[٣٩].

فالتفتيش أو البحث فى الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث فى أى مكان عن البيانات أو الأدلة المطلوبة[٤٠].

ولكون التفتيش يتضمن تقييدا للحرية الفردية، ويمثل اعتداء على حرمة الحياة الخاصة، لذا وجب 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 في نظام معلوماتي آخر غير الذي صدر بشأنه الإذن المكتوب. والمخاطر تتمثل في إمكان قيام الجاني بتدمير البيانات، أو محوها، أو نقلها، أو تعديلها، في خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، هناك من يرى أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث[٤١].

وهناك من يرى 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[٤٢].

ومحل التفتيش وما يتبعه من ضبط، يشمل البرامج أو الكيانات المنطقية (Les logiciels)، والبيانات المسجلة في ذاكرة الحاسب أو في مخرجاتها (السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات)، ودفتر يومية التشغيل، وسجل المعاملات (السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات)، وما يتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة[٤٣].

أ- مدى قابلية المكونات المادية للحاسب الإلكتروني للتفتيش:

لا يختلف اثنان أن الولوج في المكونات المادية للحاسب الإلكتروني

(Hardware) بحثًا عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد فى كشف الحقيقة عنها، وعن مرتكبها، يخضع للإجراءات القانونية الخاصة بالتفتيش؛ أى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الذى توجد به تلك المكونات، وهل هو من الأماكن العامة أو من الأماكن الخاصة؟ إذ إن لصفة المكان وطبيعته أهمية قصوى خاصة فى مجال التفتيش، فإذا كانت موجودة فى مكان خاص كمسكن المتهم أو أحد ملحقاته؛ كان لها حكمه، فلا يجوز تفتيشها إلا فى الحالات التى يجوز فيها تفتيش مسكنه، وبالضمانات والإجراءات نفسها المقررة قانونا فى التشريعات المختلفة[٤٤]، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى، أو أنها متصلة بحاسب إلكترونى آخر، أو بنهاية طرفية (Terminal) فى مكان آخر، كمسكن غير المتهم مثلا. فإذا كانت كذلك، وكانت هناك بيانات مخزنة فى أوعية هذا النظام الأخير، من شأنها كشف الحقيقة، تعين مراعاة القيود والضمانات التى يستلزمها المشرع لتفتيش هذه الأماكن. أما لو وجد شخص يحمل مكونات الحاسب الإلكترونى المادية، أو كان مسيطرا عليها، أو حائزا لها فى مكان ما من الأماكن العامة، سواء أكانت عامة بطبيعتها (كالطرق العامة، والميادين، والشوارع)، أو كانت من الأماكن العامة بالتخصيص (كالمقاهى، والمطاعم، والسيارات العامة)؛ فإن تفتيشها لا يكون إلا فى الحالات التى يجوز فيها تفتيش الأشخاص، وبالضمانات والقيود نفسها المنصوص عليها فى هذا المجال[٤٥].

ب- مدى قابلية المكونات المنطقية للحاسب الإلكترونى للتفتيش:

تفتيش المكونات المنطقية للحاسب الإلكترونى (Software)، أثار خلافا كبيرا فى الفقه، بشأن جواز تفتيشها، وذلك كما يأتى:

الرأى الأول: يرى جواز ضبط البيانات الإلكترونية بمختلف أشكالها،

ويستند هذا الرأى إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أى شىء)، فإن ذلك يجب تفسره؛ إذ يشمل بيانات الحاسب المحسوسة وغير المحسوسة[٤٦]؛ لأن الغاية من التفتيش هى ضبط الأدلة المادية التى تفيد فى كشف الحقيقة، فالمفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفى هذا المعنى نجد المادة (٢٥١) من قانون الإجراءات الجنائية اليونانى تعطى سلطات التحقيق إمكان القيام (بأى شىء يكون ضروريا لجمع الدليل وحمايته). ويفسر الفقه الجنائى اليونانى عبارة (أى شىء) بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إلكترونيا، ولذلك فإن ضبط البيانات المخزنة فى الذاكرة الداخلية للحاسب الإلكترونى لا تشكل أية مشكلة فى اليونان؛ إذ إن المحقق يمكنه إعطاء أمر للخبير بجمع البيانات التى يمكن أن تكون مقبولة بوصفها دليلا فى المحاكمة الجنائية[٤٧].

وتمنح المادة (٤٨٧) من القانون الجنائى الكندى سلطة إصدار إذن لضبط أى شىء، إذا توافرت أسس معقولة للاعتقاد بأن الجريمة ارتكبت، أو يشتبه فى ارتكابها، أو أن هناك نية فى أن يستخدم فى ارتكاب الجريمة، أو أنه سوف ينتج دليلا على وقوع الجريمة.

الرأى الثانى: (هو على النقيض من الرأى الأول) يرى عدم انطباق المفهوم المادى على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعى بالنص صراحة على أن تفتيش الحاسب الإلكترونى لابد أن يشمل المواد المعالجة عن طريق الحاسب الإلكترونى، أو بيانات الحاسب الإلكترونى؛ إذ تصبح الغاية الجديدة من التفتيش بعد التطور التقنى الذى حدث بسبب ثورة الاتصالات من بعد، تتركز فى البحث عن الأدلة المادية أو أية مادة معالجة بوساطة الحاسب[٤٨].

الرأى الثالث: فى مقابل الرأيين أعلاه، فإن هذا الرأى قد نأى بنفسه عن

البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسب الإلكتروني أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي الذي يتطلب أن يقع الضبط على بيانات الحاسب الإلكتروني، إذا اتخذت شكلا ماديا[٤٩].

ويذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة إلى مكونات الحاسب الإلكتروني، يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية، وطبيعة هذه البرامج والكيانات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة (المادة) في العلوم الطبيعية. فإذا كانت المادة تعرف بأنها كل ما شغل حيزا ماديا في فراغ معين، وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسب الإلكتروني، ويمكن قياسها بمقياس معين، وأنها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد؛ فإنها تعد طبقا لذلك ذات كيان مادي، وتتشابه مع التيار الكهربائي الذي عده الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية. وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم (٣٤) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام ١٩٧٠، لتنص على السماح بتفتيش أجهزة الحاسب الإلكتروني، وكشف الوسائط الإلكترونية، بما في ذلك البريد الإلكتروني، والبريد الصوتي، والبريد المنقول، وعن طريق الفاكس[٥٠].

وتتركز أذون التفتيش القياسية الصادرة عند التفتيش في إحدى الجرائم المعلوماتية، على ضبط الوثائق المكتوبة، إضافة إلى أجهزة الحاسب، وتضمن هذه الوثائق على وجه التحديد: النسخ الضوئية، ومطبوعات الحاسب، وفواتير التليفون، وسجلات العناوين، والمذكرات، والمراسلات[٥١].

ج- التفتيش من بعد:

إن طبيعة التقنية الرقمية قد عقدت من التحدي أمام أعمال التفتيش

والضبط. فالبيانات التى تحتوى على أدلة قد تتوزع من خلال شبكة حاسوبية فى أماكن مجهولة، بعيدة تماما عن الموقع المادى للتفتيش، وإن ظل من الممكن الوصول إليها من خلال حاسبات إلكترونية تقع فى الأبنية الجارى تفتيشها. وقد يكون الموقع الفعلى للبيانات داخل اختصاص قضائى آخر، أو حتى فى بلد آخر. وفى حين أن السلطات فى بعض البلدان قد لا تنزعج من أن تقودها تحقيقاتها إلكترونيا إلى اختصاص قضائى سيادى آخر؛ فإن السلطات فى ذلك الاختصاص السيادى قد تشعر ببالغ الانزعاج. وهذا يزيد من تعقيد مشاكل الجريمة المعلوماتية العابرة للحدود، ويزيد من أهمية تبادل المساعدة القانونية. ونستطيع أن نميز فى هذه الصورة بين ثلاثة احتمالات، هى على النحو الآتى:

الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة فى مكان آخر داخل الدولة:

يثار التساؤل عن مدى إمكان امتداد الحق فى التفتيش إذا تبين أن الحاسب أو النهاية الطرفية فى منزل المتهم متصلة بجهاز أو نهاية طرفية فى مكان آخر مملوك لشخص غير المتهم.

ويرى الفقه الجنائى الألمانى إمكان امتداد التفتيش إلى سجلات البيانات التى تكون فى موقع آخر، استنادا إلى مقتضيات القسم (١٠٣) من قانون الإجراءات الجنائية الألمانى[٥٢].

ونجد إرهاصات هذا الرأى فى المادة (٨٨) من قانون تحقيق الجنايات البلجيكى الصادر فى (٢٣ /١١/ ٢٠٠٠) التى تنص على أنه "إذا أمر قاضى التحقيق بالتفتيش فى نظام معلوماتى، أو فى جزء منه؛ فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتى آخر يوجد فى مكان آخر غير مكان البحث الأصلى، ويتم هذا الامتداد وفقا لضابطين: (أ) إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث. (ب) إذا وجدت مخاطر تتعلق بضياع بعض الأدلة؛

لسهولة عملية محو البيانات محل البحث أو إتلافها أو نقلها"[٥٣].

والشيء ذاته نجده فى القانون الاتحادى الأسترالى؛ إذ لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة، فقد توخى قانون جرائم الإنترنت لعام ٢٠٠١، إمكان أن تتوزع بيانات الأدلة على شبكة حاسبات إلكترونية، وسمح هذا القانون بعمليات تفتيش لبيانات خارج المواقع التى يمكن اختراقها من خلال حاسبات توجد فى الأبنية الجارى تفتيشها.

ويشير مصطلح "البيانات المختجزة فى حاسب ما" إلى "أية بيانات محتجزة فى جهاز تخزين على شبكة حاسبات يشكل الحاسب الإلكترونى جزءا منها". فلا توجد حدود جغرافية محددة، ولا أى اشتراط للحصول على موافقة طرف ثالث. غير أن المادة (3LB) من قانون الجرائم لعام ١٩١٤ التى أدرجها قانون جرائم الإنترنت، تشترط إخطار شاغل المبنى الثانى قدر الإمكان عمليا. وهذا قد يكون أكثر تعقيدا مما يبدو عليه؛ إذ إنه فى مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكيا، فإن المرء لا يكون متأكدا دائما من مكان وجوده[٥٤].

كما نص مشروع قانون جرائم الحاسب الآلى فى هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة فى موقع آخر، بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة ١٢٥)، وذلك بمراعاة بعض القيود[٥٥].

الاحتمال الثانى: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة فى مكان آخر خارج الدولة:

من المشكلات التى تواجه سلطة الادعاء فى جمع الأدلة، قيام مرتكبى الجرائم بتخزين بياناتهم فى أنظمة تقنية خارج الدولة، مستخدمين فى ذلك شبكة الاتصالات المعلوماتية، مستهدفين عرقلة الادعاء فى جمع الأدلة والتحقيقات[٥٦].

وفى هذه الحالة، فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافى للدولة التى صدر من جهتها الإذن، ودخوله فى المجال الجغرافى لدولة أخرى، وهو ما يسمى بالولوج أو التفتيش عبر الحدود، قد يتعذر القيام بسبب تمسك كل دولة بسيادتها.

لذا، فإن جانبا من الفقه يرى أن التفتيش الإلكترونى العابر للحدود، لا بد أن يتم فى إطار اتفاقيات خاصة، ثنائية أو دولية، تجيز هذا الامتداد، وتعقد بين الدول المعنية، ومن ثم فإنه لا يجوز القيام بذلك التفتيش العابر للحدود، فى غياب تلك الاتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى. وهذا يؤكد أهمية التعاون الدولى فى مجال مكافحة الجرائم التى تقع فى المجال الإلكترونى[٥٧].

وتطبيقا لهذا الإجراء الأخير، فقد حدث فى ألمانيا فى أثناء جمع إجراءات التحقيق عن جريمة غش وقعت فى بيانات حاسب إلكترونى، تبين وجود اتصال بين الحاسب الإلكترونى الموجود فى ألمانيا، وشبكة اتصالات فى سويسرا، يتم تخزين بيانات المشروعات فيها. وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، لم تتمكن من ذلك إلا عن طريق التماس المساعدة الذى تم بالتبادل بين الدولتين[٥٨].

ومع ذلك، أجازت المادة (٣٢) من الاتفاقية الأوربية، بشأن الجرائم المعلوماتية التى أعدها المجلس الأوربى، وتم التوقيع عليها فى بودابست، فى (٢٠٠١/١١/٢٣)، إمكان الدخول بغرض التفتيش والضبط إلى أجهزة أو شبكات تابعة لدولة أخرى بدون إذن فى حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، والأخرى إذا رضى صاحب هذه البيانات أو حائزها بهذا التفتيش.

ومع ذلك، فإن تطبيق هذا النص يمكن أن يثير مشكلات جمة[٥٩]، ولا

مناص من التعاون الدولى فى هذا المجال، بمقتضى اتفاقية ثنائية أو متعددة الأطراف، أو على الأقل الحصول على إذن الدولة التى يتم التفتيش فى مجالها الإقليمى، وهذا ما قامت به الشرطة اليابانية؛ إذ ساورها الاعتقاد بأن مجموعة من المخربين قد استخدمت أجهزة الحاسب الإلكترونى فى الصين والولايات المتحدة لمهاجمة كثير من المواقع الخاصة بالحكومة اليابانية على الشبكة، وقد طالبت الشرطة اليابانية بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الحاسب الإلكترونى فى كل من هاتين الدولتين، حتى تمكن من الوصول إلى جذور هذه العملية الإرهابية[٦٠].

الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الإلكترونى:

التنصت والأشكال الأخرى للمراقبة الإلكترونية، برغم أنها مثيرة للجدل فإنه مسموح بها تحت ظروف معينة فى جميع الدول تقريبا. فالقانون الفرنسى الصادر فى (١٩٩١/٧/١٠) يجيز اعتراض الاتصالات البعدية، بما فى ذلك شبكات تبادل المعلومات[٦١].

وفى هولندا أجاز المشرع لقاضى التفتيش أن يأمر بالتنصت على شبكات الاتصالات، إذا كانت هناك جرائم خطيرة ضالع فيها المتهم، وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات[٦٢].

وفى الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية، بما فيها شبكات الحاسب، بشرط الحصول على إذن تفتيش صادر من القاضى[٦٣].

وفى اليابان أقرت محكمة مقاطعة (KOFU) سنة ١٩٩١، شرعية التنصت على شبكات الحاسب الإلكترونى للبحث عن دليل[٦٤].

وتفتيش نظم الحاسب الإلكترونى يمكن أن يتم بطرق عدة؛ فمثلا المرشد الفيدرالى الأمريكى[٦٥] جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق، هى[٦٦]:

١- تفتيش الحاسب الإلكترونى، وطبع نسخة ورقية من ملفات معينة فى الوقت نفسه.

٢- تفتيش الحاسب الإلكترونى، وعمل نسخة إلكترونية من ملفات معينة فى الوقت نفسه.

٣- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل فى الموقع، وبعد ذلك يعاد عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.

٤- ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

د- شروط تفتيش نظم الحاسب الإلكترونى:

يمكن تقسيم شروط تفتيش نظم الحاسب الإلكترونى إلى نوعين: موضوعية والأخرى شكلية.

أولا- الشروط الموضوعية لتفتيش نظم الحاسب الإلكترونى:

تنحصر هذه الشروط فيما يأتى:

أ- وقوع جريمة معلوماتية: الجريمة المعلوماتية هى كل فعل غير مشروع مرتبط باستخدام الحاسب الإلكترونى لتحقيق أغراض غير مشروعة[٦٧]. وهناك كثير من التشريعات التى حرصت على استحداث نص خاص للجريمة المعلوماتية، كما هى الحال بالنسبة إلى إنجلترا التى أصدرت قانون إساءة استخدام الحاسب الإلكترونى (Computer misuse) فى

١٩٩٠/٦/٢٩، وفى الولايات المتحدة الأمريكية، حيث صدر قانون الاحتيال وإساءة استخدام الحاسب الإلكترونى سنة ١٩٨٦، الذى طبق على المستوى الفيدرالى، إضافة إلى قوانين بعض الولايات المتحدة الأمريكية؛ كقانون ولاية تكساس الصادر فى ١٩٨٥/٩/١ بشأن الدخول غير المشروع فى نظام الحاسب. وفى فرنسا صدر القانون رقم (١٩-٨٨) فى ١٩٨٨/١/٥، وهو الخاص بالغش المعلوماتى. وقد أدرج المشرع الإماراتى برامج الحاسب الإلكترونى ضمن المصنفات الفكرية المحمية بالقانون الاتحادى رقم (٤٠) لسنة ١٩٩٢، كذلك عد المشرع المصرى مصنفات الحاسب الإلكترونى من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها فى المادة الثانية، بمقتضى القانون رقم (٣٨) لسنة ١٩٩٢.

ب- تورط شخص أو أشخاص معينين فى ارتكاب الجريمة المعلوماتية أو الاشتراك فيها: ينبغى أن تتوافر فى الشخص المراد تفتيشه دلائل كافية، تدعو إلى الاعتقاد بأنه قد أسهم فى ارتكاب الجريمة المعلوماتية، سواء بوصفه فاعلا لها، أو شريكا فيها. وفى مجال الحاسب الإلكترونى يمكن القول إن تعبير (الدلائل الكافية) يقصد به مجموعة من المظاهر أو العلامات التى تقوم على المضمون العقلى والمنطقى لملابسات الواقعة، وكذلك على خبرة القائم بالتفتيش وحرفيته التى تؤيد نسبة الجريمة المعلوماتية إلى شخص معين، سواء بوصفه فاعلا أو شريكا.

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

د- محل التفتيش الخاص بنظم الحاسب الإلكترونى هى كل مكونات

الحاسب، سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة بها، إضافة إلى الأشخاص الذين يستخدمون الحاسب الإلكترونى محل التفتيش.

وتشمل المكونات المادية الحاسب الإلكترونى وحدات الإدخال، ووحدة المعالجة المركزية، ووحدات الإخراج، وأخيرا وحدات التخزين الثانوى.

كما تنقسم المكونات المادية المعنوية للحاسب الإلكترونى إلى الكيانات المنطقية الأساسية (برامج النظام)، والكيانات المنطقية التطبيقية (برامج التطبيقات بنوعيها: برامج التطبيقات سابقة التجهيز، وبرامج التطبيقات، طبقا لاحتياجات العميل)، ويتطلب الحاسب بمكوناته السابقة مجموعة من الأشخاص ذوى الخبرة والمهارة فى تقنية نظم المعلومات، وهم مشغلو الحاسب، وخبراء البرامج، سواء كانوا مخططى برامج تطبيقات، أم كانوا مخططى برامج نظم ومحللين ومهندسى الصيانة والاتصالات ومدربى النظم المعلوماتية.

ثانيا- الشروط الشكلية لتفتيش نظم الحاسب الإلكترونى:

أ- الأسلوب الأمثل لتنفيذ التفتيش فى نظم الحاسب الإلكترونى: نظم القانون الأمريكى أسلوب تنفيذ التفتيش فى نظم الحاسب الإلكترونى، وذلك على النحو الآتى:

الخطوة الأولى: تقتحم قوات الشرطة المكان بصورة سريعة، ومن كل منافذه، فى وقت 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 كل أنظمة الحاسب الإلكترونى ومعداته الموجودة فى المكان على الفور، حتى لا يتمكنوا من تشويه أى دليل إلكترونى أو تدميره، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كمبيوتر، ودائما ما تكون غرفة المعيشة، ويوضعون تحت

حراسة مشددة. وفى هذه الخطوة يتم تقديم التفتيش الصادر من النيابة إليهم، ويتم تحذيرهم بأن كل أقوالهم ستحسب عليهم منذ هذه اللحظة، وقد تؤخذ دليل إدانة ضدهم. ودائما ما سنجد لدى كثير منهم كثيرا من الحديث، خاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث بمنزلهم، وفى مكان ما من المنزل، سنجد جهاز الحاسب الإلكترونى متصلا بخط تليفون، أو ربما نجد أكثر من جهاز، وأكثر من خط فى المنزل الواحد، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين.

الخطوة الثالثة: توضع النقطة الساخنة فى عهدة فريق يضم اثنين من العملاء (مكتشف ومسجل)، ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريبا متقدما على نظم المعلومات، ودائما ما يقوم بهذا الدور العميل المعنى بالقضية الذى عاصرها منذ البداية، واستصدر إذنا بالتفتيش الخاص بها من القاضى، فهذا الشخص يعرف تماما الشىء أو الأشياء التى يبحث عنها، ويتفهم طبيعتها تماما، ولن نتجاوز إذا قلنا إنه هو الذى يقوم بفتح الأدراج والبحث عن الأقراص الممغنطة والسلفات وحاويات الأقراص... إلخ.

أما المسجل فيتولى تصوير كل الأجهزة والمعدات على الكيفية نفسها التى تم ضبطها عليها، ويقوم المسجل كذلك بتصوير كل الغرف الأخرى الموجودة بالمنزل، حتى لا يدعى أحد المجرمين الماكرين أن الشرطة قد سرقت منزله فى أثناء التفتيش.

ب- فريق التفتيش: هو الفريق المعنى بإجراءات التحقيق، وهو جزء داخل فريق الإغارة الذى يضم إلى جانب 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:

١- **المشرف على التحقيق:** هو الذى يجب أن يكون من ذوى الخبرات الطويلة فى مجال التحقيق الجنائى فى الجرائم المعقدة، ويتولى المشرف إدارة العميل فى مسرح الجريمة، وتوزيع المهام على أعضاء الفريق.

٢- **فريق أخذ الإفادات:** يحدد عدد أعضاء هذا الفريق حسب حجم الجريمة، والمتورطين فيها، وعدد الشهود الذين قد يوجدون فى مسرح الجريمة، وعليه قد يكون الفريق من شخصين أو أكثر.

٣- **فريق الرسم والتصوير:** يضم شخصا أو أكثر، يقومون برسم الخرائط لمسرح الجريمة، وتحديد موقع الأجهزة والملفات والأشخاص، والتقاط الصور الفوتوغرافية، والتصوير بالفيديو، مع مراعاة أن يتم تنبيه جميع العاملين فى مسرح الجريمة عند استعمال الفيديو، تحسبا لتسجيل أصوات المشاركين فى التفتيش.

٤- **فريق التفتيش العملى:** يضم شخصا واحدا أو أكثر، حسب الأحوال، ويتولى هذا الشخص عملية البحث والتدقيق على مسرح الجريمة، وفقا للنظم الفنية التى تتبع فى تفتيش الأماكن، وتفتيش مسرح الجريمة، ويقوم هذا الفريق بالمرور على جميع الغرف والمخازن، ويفحص المخازن والمخابئ، وليس من الضرورى أن يكون أعضاء هذا الفريق من خبراء الحاسب، ولكن يفضل أن يتم إطلاعهم على الأشياء التى ينبغى البحث عنها.

٥- **فريق التأمين والقبض:** ويعنى هذا الفريق بالسيطرة أمنيا على مسرح الجريمة، وضبط مخارجها ومنافذها، وحركة الموجودين بالمبنى والمبانى المجاورة لمسرح الجريمة، وتنفذ عملية القبض على المشتبه فيهم، واحتجازهم وفق ما يأمر به المشرف، ويتكون هذا الفريق من

رجال الأمن بالزى الرسمى.

٦- **فريق ضبط الأدلة وتحريرها**: ويضم هذا الفريق اثنين أو أكثر من خبراء الحاسب الإلكترونى، يتولون ضبط المعلومات المضبوطة وإدخالها إلى الحاسب الإلكترونى، وتصنيف الأدلة، وتحريزها فى الصناديق، ووضع العلامات الموضحة عليها، ويقوم هذا الفريق بنقل أجهزة الحاسب الإلكترونى المضبوطة بعد إجراءات الرسم والتصوير، ويجب أن يكون من بين أعضاء هذا الفريق شخصان على الأقل؛ أحدهما محقق فى مجال الحاسب الإلكترونى، والآخر خبير فى الحاسب الإلكترونى، مدرب على التعامل مع الأدلة وطرق تقييمها.

٧- **خبير مسرح الجريمة العادية**: ويتم اختيارهم حسب الحال، وقد يحتاج المحقق فى بعض جرائم الحاسب إلى كل أعضاء الفريق أو بعضهم؛ مثل خبراء البصمات، والمهندسين، وخبراء المتفجرات...إلخ.

٤ - الضبط:

الغاية من التفتيش ضبط شىء يتعلق بالجريمة، ويفيد فى التحقيق الجارى بشأنها، سواء كان هذا الشىء أدوات استعملت فى ارتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد فى كشف الحقيقة[٦٨]. ويقصد بالضبط فى قانون الإجراءات وضع اليد على شىء يتصل بجريمة وقعت، ويفيد فى كشف الحقيقة وكشف مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق.

وتتحدد طبيعته بحسب الطريقة التى يتم بها وضع اليد على الشىء المضبوط، فإذا كان الشىء وقت ضبطه فى حيازة شخص، واقتضى الأمر

تجريده من حيازته، كان الضبط إجراء تحقيق، أما إذا كان الاستيلاء عليها بدون الاعتداء على حيازة قائمة، فإنه يكون إجراء استدلال.

الضبط بطبيعته وبحسب تنظيمه القانونى وغايته لا يرد إلا على الأشياء، أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق، وإذا كان قانون الإجراءات يتحدث فى بعض التصرف عن ضبط الأشخاص وإحضارهم؛ فإنه يعنى القبض عليهم وإحضارهم، والقبض نظام قانونى يختلف تماما عن ضبط الأشياء.

ولا يفرق القانون فى مجال الضبط بين المنقول والعقار، فكلاهما يمكن ضبطه، كذلك فإنه يستوى أن يكون الشىء المضبوط مملوكا للمتهم أو لغيره، والقاعدة أن الضبط لا يرد إلا على شىء مادى، أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط، والشرط اللازم لصحته أن يكون الشىء مفيدا فى كشف الحقيقة، فكل ما يحقق هذه الغاية يصح ضبطه.

أ- الأشياء المادية:

الأدلة المادية التى يجوز ضبطها فى الجريمة المعلوماتية التى لها قيمة خاصة فى إثبات جرائم الحاسب الإلكترونى ونسبتها إلى المتهم، هى:

١- الورق: أكثر الجرائم الواقعة على المال أو على جسم الإنسان، يترك خلفه قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها فى الحاسب الإلكترونى؛ وهو ما قلل حجم الأوراق والملفات، ومع ذلك نجد كثيرين يقومون بطباعة المعلومات لأغراض المراجعة، أو التأكد من الشكل العام للمستند، أو الرسالة، أو الرسومات موضوع الجريمة، وأجهزة الحاسب الإلكترونى، والطابعات المتطورة ذات السرعات الفائقة، تطبع قدرا كبيرا من الأوراق فى وقت قصير،

ومن ثم يعد الورق من الأدلة التى ينبغى الاهتمام بها فى البحث، وتفتيش مسرح الجريمة.

والورق أربعة أنواع:

أ- أوراق تحضيرية، يتم إعدادها بخط اليد بوصفها مسودة، أو تصور للعملية التى يتم برمجتها.

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

ج- أوراق أصلية تتم طباعتها والاحتفاظ بها بوصفها مرجعا، أو لأغراض تنفيذ الجريمة.

د- أوراق أساسية وقانونية محفوظة فى الملفات العادية أو دفاتر الحسابات، وتكون لها علاقة بالجريمة، خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الإلكترونى.

٢- **جهاز الحاسب الإلكترونى وملحقاته:** وجود جهاز حاسب إلكترونى مهم للقول بأن هناك جريمة، ولأجهزة الحاسبات الإلكترونية أشكال وأحجام وألوان مختلفة، وخبير الحاسب الإلكترونى يستطيع تعرف الحاسب الإلكترونى ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى، وتحديد أسلوب التعامل معه، فى حالة الضبط والتحريز.

٣- **الحاسب الإلكترونى، لوحة المفاتيح، والشاشة:** من السهل تعرف جهاز الحاسب الشخصى الذى أصبح مألوفا اليوم، فهو يتكون من وحدة المعالجة المركزية (CPU)، ولوحة المفاتيح (Keyboard)، والشاشة (Monitor). ومع التطورات السريعة التى يمر بها الحاسب الإلكترونى، فإننا 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 الضرورى

إطلاع العاملين فى مجال التحقيق على مختلف أشكال أجهزة الحاسب الإلكترونى فور ظهورها.

٤- **أقراص الليزر:** تجد قدرا كبيرا من أقراص الليزر مع جهاز الحاسب إلكترونى الشخصية العادية، علاوة على أن مراكز الحاسب الإلكترونى فى الشركات والبنوك قد تجد فيها ملايين من الأقراص، قد تكون على أغلفتها بيانات توضح محتويات كل قرص، وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد فى مكان ما أقراص الليزر ولا تجد معا أجهزة الحاسب الإلكترونى، ومع ذلك يعد جزءا من جريمة إلكترونية متى كانت محتوياتها عنصرا من عناصر الجريمة.

٥- **الشرائط الممغنطة (Magnetic Tapes):** وتستعمل الشرائط الممغنطة عادة لحفظ الاحتياطى، وقد تكون فى مكان بعيد أمن، كما يقوم بعض الناس بإيداعها فى خزائن البنوك التجارية، أو مراكز التوثيق الحكومية الأمنة.

٦- **لوحة الدوائر (Circuit Boards and Components).**

٧- **المودم (Modem):** المودم وسيلة تمكن أجهزة الحاسب الإلكترونى من الاتصال فيما بينها من خلال خطوط الهاتف. وقد تطور المودم إلى أجهزة إرسال الفاكس، والرد على المكالمات الهاتفية، وتبادل البيانات وتعديلها، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الإلكترونى.

٨- **الطابعات:** للطابعات أنواع؛ منها العادية، ومنها طابعات ليزرية، ومنها الملونة، ومنها غير الملونة.

٩- **Pcmcia cards:** تستعمل بطاقات الـ Pcmcia فى أجهزة الحاسب الإلكترونى الصغيرة (Notebook)، والحاسبات الإلكترونية المحمولة (Laptop)، وهى فى شكل البطاقات الائتمانية.

١٠ ـ **البـرامج اللينـة والكتيبـات الإرشـادية:** الكتيبـات الإرشـادية (Manuals) المصاحبة للحاسب الإلكترونى مفيدة فى تعرف الجهاز والبرامج المستعملة فيه.

١١ ـ **البطاقات الممغنطة** وبطاقات الائتمان القديمة والمواد البلاستيكية المستعملة فى إعداد تلك البطاقات، تعد قرائن للإثبات فى الجرائم الإلكترونية.

كل ذلك يعد أثرا أو جزءا من جسم الجريمة، ينبغى البحث عنها، وفحصها، والاستفادة منها فى التحقيق. علما بأن التعامل مع مثل هذه الآثار يحتاج إلى خبرة فنية فى مجال الحاسب الإلكترونى، ومعرفة بالقانون.

ب- البيانات الإلكترونية:

فى مجال الجرائم المعلوماتية، قد يكون الضبط محله بيانات معالجة إلكترونيا، عندئذ يثار التساؤل الآتى:

هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط الذى يعنى كما رأينا، وضع اليد على شىء مادى ملموس؟

انقسم الفقه الجنائى إلى رأيين كما يأتى:

الرأى الأول: يرى أن بيانات الحاسب الإلكترونى لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادى عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادى ملموس، عن طريق التصوير الفوتوغرافى، أو نقلها على دعامة أو غيرها من الوسائل المادية[٦٦]. ويستند هذا الرأى إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة.

الرأى الثانى: يرى أن البيانات المعالجة إلكترونيا إن هى إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، ويمكن نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادى لا

يمكن إنكاره[٧٠]. ويستند هذا الرأى إلى بعض النصوص التشريعية، كالمادة (٢/٢٩) من قانون الإثبات الكندى التى تنص على الآتى: "إن تفتيش الدفاتر والسجلات الخاصة بمؤسسة مالية وضبطها، يقتصر على تفتيش المكان، بغرض تفقده، وأخذ نسخة من المواد المكتوبة، يستوى فى ذلك أن تكون السجلات مكتوبة أو فى شكل إلكتروني"[٧١].

وهذا الخلاف دعا المشرع الجنائى فى بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط، ليشمل فضلا عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونيا، وهو ما نصت عليه المادة (٣٩) من قانون تحقيق الجنايات البلچيكى، المدخلة فى التقنين بمقتضى القانون الصادر فى ٢٠٠٠/١١/٢٣؛ إذ يشمل الحجز وفقا لهذا النص الأشياء المادية، والبيانات المعالجة إلكترونيا[٧٢].

وخشية من محو الأدلة التى يتم الحصول عليها بطريق التفتيش أو إتلافها أو نقلها أو ضياعها، فقد أعطت المادة (٨٨) من قانون تحقيق الجنايات البلچيكى لقاضى التحقيق، سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلچيكية، أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات محل الجريمة، إن وجدت لدى دولة أجنبية.

ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التى استخدمت فى ارتكابها، أو الآثار المتخلفة عنها، وتفيد فى كشف الحقيقة[٧٣].

ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى تحت تصرفها، إلى حين انتهاء المحاكمة، وهناك من يرى ضرورة حفظ نسخة أخرى لدى المحضرين بالمحكمة، خشية تلف النسخة الوحيدة الموجودة تحت تصرف جهة التحقيق أو المحكمة أو ضياعها[٧٤].

ويواجه إجراء الضبط للبيانات المعالجة إلكترونيا صعوبات؛ منها:

أ- حجم الشبكة التى تحتوى على المعلومات المعالجة إلكترونيا المطلوب ضبطها، من ذلك البحث فى نظام إلكترونى لشركة متعددة الجنسيات.

ب- وجود هذه البيانات فى شبكات أو أجهزة تابعة لدولة أجنبية؛ وهو ما يستدعى تعاونها مع جهات الشرطة والتحقيق فى عملية التفتيش والضبط والتحفظ.

ج- 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 فى حالة إنكارها من المتهم، فقد أعطى القانون البلجيكى للنيابة العامة سلطة الأمر بغلق هذه البيانات (Blocage de donees)، لمنع الوصول إليها، أو إلى النسخة المستخرجة منها الموجودة لدى من يستعملون النظام (م٢٩ مكرر /٣)[٧٥].

ووفقا للمادة (٣٩ مكرر) من القانون البلجيكى يتم سحب البيانات التى سبق أخذ نسخة منها من الجهاز، فى الحالات الآتية:

أ- إذا كانت محلا للجريمة أو ناتجة عنها.

ب- إذا كانت مخالفة للنظام العام أو حسن الآداب.

ج- إذا كانت تمثل خطرا على الأنظمة الإلكترونية.

د- إذا كانت تمثل خطرا بالنسبة إلى المعلومات المخزنة أو المعالجة أو المرسلة بهذه الأنظمة[٧٦].

وقد أجازت المادة (٨٨) من القانون البلجيكى لسنة ٢٠٠٠ لقاضى التحقيق، فى حالة امتداد البحث الإلكترونى عن أدلة الجريمة، خارج نطاق بلجيكا، أن يحصل على نسخة من البيانات التى يحتاج إليها. وهذا معناه أن

الحصول على هذه النسخة يتم من دون إذن الدولة التى توجد فى نطاق إقليمها البيانات المطلوبة. ويبرر الفقه البلچيكى هذا النص بالقول إن سلطة التحقيق يمكنها الدخول إلى النظام، والاطلاع على البيانات المطلوبة، من دون أن تدرك أن هذه البيانات توجد من الناحية المادية خارج إقليم بلچيكا. والبديل لهذا النص هو إرسال لجنة قضائية إلى الدولة المعنية، تطلب من السلطة المختصة بها أن 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.

٥ - الشهادة:

الشهادة هى الأقوال التى يدلى بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم، أو براءته منها[٧٧]. وللشهادة فى مجال الإجراءات الجنائية أهمية بالغة؛ لأن الجريمة ليست تصرفا قانونيا، ولكنها عمل غير مشروع، يجتهد الجانى فى التكتم عند ارتكابه، ويحرص على إخفائه عن أعين الناس.

ولهذا فإن العثور على شاهد يعد مكسبا كبيرا للعدالة. ومن هنا جاءت قاعدة عدم رد الشهود. وسماع الشهود - كسائر إجراءات التحقيق - من الأمور التقليدية للمحقق، فله أن يسمع الشهود، أو يستغنى عنهم. فإذا قرر سماعهم فهو الذى يحدد مَن يجب الاستماع إليه، ومَن يمكن الاستغناء عنه. والأمر متروك إلى فطنة المحقق، ومرتبط بظروف التحقيق، والأصل أن يطلب الخصوم سماع مَن يرون من الشهود. غير أن للمحقق أن يجيبهم إلى طلبهم، أو يرفضه، وله أن يدعو للشهادة مَن يُقدر أن لشهادته أهمية، بل له أن يسمع شهادة أى شاهد يتقدم من تلقاء نفسه. ومن المبادئ المستقرة، أن الشاهد لا يرد، ولو غلب على الظن أنه لن يتحرى الصدق فى شهادته، سواء كان ذلك راجعا لانحطاط

فى خُلقه، أو لوجود صلة مودة، أو لعداوة بينه وبين المتهم، تجعله يميل له أو ضده.

أ- التعريف بالشاهد فى الجريمة المعلوماتية:

الشاهد فى الجريمة المعلوماتية هو الفنى صاحب الخبرة والتخصص فى تقنية الحاسب الإلكترونى الذى تكون لديه معلومات جوهرية أو مهمة لازمة للولوج فى نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضى التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتى، وذلك تمييزا له عن الشاهد التقليدى.

ويشمل الشاهد المعلوماتى بهذا المفهوم عدة طوائف من أهمها:

١- القائم على تشغيل الحاسب الإلكترونى:

وهو المسئول عن تشغيل الحاسب الإلكترونى والمعدات المتصلة بها. ويجب أن تكون لديه خبرة كبيرة فى تشغيل الجهاز، واستخدام لوحة المفاتيح فى إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج[٧٨].

٢- المبرمجون:

هم الأشخاص المتخصصون فى كتابة البرامج. ويمكن تقسيمهم إلى فئتين على النحو الآتى:

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

إذ يقوم مخططو برامج التطبيقات بالحصول على خصائص النظام

المطلوب من محلل النظم، ثم يقوم بتحويلها إلى برامج دقيقة وموثقة، لتحقيق هذه الخصائص، أما مخططو برامج النظم فيقومون باختيار برامج نظام الحاسب الداخلية وتعديلها وتصحيحها؛ أى أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التى تتحكم فى وحدات الإدخال والإخراج ووسائط التخزين، إضافة إلى إدخال أية تعديلات أو إضافات لهذه البرامج.

٣- المحللون:

المحلل هو الشخص الذى يحلل الخطوات، ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات، ثم تحليل النظام؛ أى تقسيمه إلى وحدات منفصلة، واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام، عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التى يمكن ميكنتها بوساطة الحاسب الإلكترونى.

٤- مهندسو الصيانة والاتصالات:

هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب، بمكوناتها وشبكات الاتصال المتعلقة بها.

٥- مديرو النظم:

هم الذين يوكل إليهم أعمال الإدارة فى النظم المعلوماتية[٧٩].

ويحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية شهود الجريمة المعلوماتية فى الآتى:

أ- محلل النظم الذى صمم برنامج الحاسب الإلكترونى الذى أنتج الدليل.

ب- المبرمج الذى قام بتحرير البرنامج واختباره.

ج- المشغل الذى يقوم بتشغيل البرنامج.

د- طاقم عمليات البيانات الذى يعد البيانات بالصورة التى يستطيع الكمبيوتر قراءتها (شريط أو قرص).

هـ- أمناء مكتبة الأشرطة الذين يتحملون مسئولية توفير الأشرطة أو الأقراص التى تشتمل على البيانات المصدرية الصحيحة.

و- مهندس الصيانة الإلكترونية الذى يقوم على صيانة الجهاز الأصلى، والتأكد من عمله بصورة صحيحة.

ز- موظفو المدخلات والمخرجات والمسئولون عن معالجة المدخلات المستخدمة فى تنفيذ برامجه.

ح- المستخدم النهائى الذى يمد بالمعلومات المدخلة، ويصرح بتنفيذ برامج الحاسب الإلكترونى، ويستخدم نواتجها[٨٠].

ب- التزامات الشاهد المعلوماتى:

يتعين على الشاهد المعلوماتى أن يقدم لسلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج فى نظام المعالجة الآلة للبيانات، بحثا عن أدلة الجريمة بداخله. والسؤال الذى يطرح نفسه: هل يلتزم الشاهد بطبع الملفات، والإفصاح عن كلمات المرور والشفرات؟

هناك اتجاهان فى هذا الصدد؛ هما:

الاتجاه الأول: يرى أنه ليس من واجب الشاهد، وفقا للالتزامات التقليدية للشهادة، أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة. ويميل إلى هذا الاتجاه الفقه الجنائى الألمانى؛ إذ يرى عدم التزام الشاهد بطبع البيانات المخزنة فى ذاكرة الحاسب، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[٨١].

وكذلك لا يجوز فى تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة[٨٢].

الاتجاه الآخر: يرى أنصار هذا الاتجاه أن من بين الالتزامات التى يتحملها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة؛ إذ يرى اتجاه فى الفقه الجنائى الفرنسى أن القواعد العامة فى مجال الإجراءات الجنائية تحتفظ بسلطاتها فى مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود - من حيث المبدأ - الالتزام بتقديم شهادتهم[٨٣]، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التى يعلمونها. ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا فى مرحلة التحقيق والمحاكمة[٨٤].

وفى هولندا يتيح قانون الحاسب الإلكترونى لسلطات التحرى والتحقيق إصدار الأمر للقائم بتشغيل النظام، لتقديم المعلومات اللازمة لاختراقه، والولوج فى داخله؛ كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة. وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب، وكانت مصلحة التحقيق تستلزم التحقيق للحصول عليها؛ يتم تكليف القائم على تشغيل النظام المعلوماتى بحل رموز هذه البيانات[٨٥].

وفى اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب، على كلمة المرور السرية، للولوج فى نظام المعلومات، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمنى، لكن ليس على الشاهد أى التزام بالنسبة إلى طباعة ملفات بيانات مخزنة فى ذاكرة الحاسب؛ وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل، وليس كشف معلومات جديدة[٨٦].

خاتمة:

أولا- النتائج:

تناول البحث موضوع إجراءات التحرى وجمع الأدلة والتحقيق الابتدائى فى 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 التى أسهمت هذه الثورة فى ارتكابها، والتى تتميز بطبيعة فنية وعلمية معقدة، ويتصف مرتكبها بطبيعة ذكية ماكرة.

وعلى الرغم من وجود تشابه كبير بين التحقيق فى الجرائم المعلوماتية، والتحقيق فى الجرائم العادية؛ فهى جميعا تحتاج إلى إجراءات تتشابه فى عمومها؛ مثل المعاينة، والتفتيش، والمراقبة، والتحريات، والاستجواب، إضافة إلى جمع الأدلة، كما أنها تشترك فى كونها تسعى للإجابة عن الأسئلة المشهورة لدى المحقق: ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟

وتظل الجرائم المعلوماتية تمتاز عن غيرها من الجرائم، ببعض الخصائص، وهذا بالطبع يستدعى تطوير أساليب التحقيق الجنائى وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة ومعرفة مرتكبيها، بالسرعة والدقة اللازمين، فالتحقيق فى هذا النوع من الجرائم يستدعى الرجوع إلى عدد كبير من السجلات التى يجب الاطلاع عليها؛ مثل الكتيبات الخاصة بأجهزة الحاسب الإلكترونى، وملفات تسجيل العمليات الحاسوبية، إضافة إلى الاطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها.

إذ إن كثيرا من مراحل التحقيق الابتدائى سوف يتم فى بيئة رقمية، من خلال التعامل مع الحاسبات والشبكات ووسائط التخزين ووسائل الاتصال.

ومما تقدم يتضح أن التحرى والبحث والتحقيق وجمع الأدلة فى مجال

الجرائم المعلوماتية، يكتنفه الغموض، ويحيط به كثير من الصعاب، إلا أنه لا مناص من مواصلة البحث والتحقيق وجمع الأدلة، مع التطوير المستمر لوسائل البحث، ولأجهزة الشرطة، وسلطات التحقيق، وتدعيم التعاون الدولى فى هذا المجال .

لقد توصل البحث من خلال هذه الدراسة إلى النتائج الآتية:

١- أظهر البحث أن هناك قصورا واضحا فى كثير من التشريعات الجنائية الإجرائية العربية فى مواجهة ظاهرة الإجرام الإلكترونى، فمازال كثير منها يخضع هذه الجرائم للنصوص التقليدية، وهو ما قد يترتب عليه الاعتداء على مبدأ شرعية الجرائم والعقوبات من جهة، وإفلات كثير من الجناة من العقاب من جهة أخرى.

٢- ألقى البحث الضوء على الحقيقة العلمية والحقيقة القضائية، وانتهى إلى أن الحقيقة العلمية قد تضلل الحقيقة القضائية؛ وهو ما يؤكد أهمية تدريب الخبراء والمحققين والقضاة؛ لفهم هذه الحقيقة العلمية، والعمل على مطابقة الحقيقة القضائية لها، بقدر المستطاع.

٣- إن الخطأ فى إجراء التفتيش وضبط الأدلة قد يؤدى إلى فوات فرصة كشف الجريمة، أو فوات الإدانة، حتى مع معرفة الجانى.

ثانيا- التوصيات:

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

١- ضرورة إعداد الكوادر الأمنية، وسلطات التحقيق من الناحية الفنية للبحث والتحقيق الابتدائى وجمع الأدلة فى مجال الجرائم المعلوماتية؛ وهو ما يستلزم إنشاء مراكز متخصصة فى البلاد العربية، تحقيقا لهذا الغرض.

٢- 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 التى كرمها الله وجعلها خير الأمم، فحقيق بها أن تكون كذلك، واقعا وفعلا.

٣- ضرورة التعاون بين الدول العربية المختلفة، بتبادل المعلومات والخبرات، والتعاون فى المجال الأمنى والقضائى، بصوره المختلفة، فضلا عن التعاون بينها وبين الدول الأخرى فى هذا المجال، وأسوة بالتعاون الدولى المتمثل فى الاجتماع الذى عقدته مجموعة الدول الصناعية الثمانى عام ١٩٩٧ حول جرائم الشبكات (Cyber Crimes) مع اجتماعات دورية أخرى عقدت فى باريس.

٤- 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 العدة لمواجهة ظاهرة الإجرام الإلكترونى التى من المنتظر أن تتزايد فى المستقبل، نتيجة للتطور العلمى المستمر الذى أحدثته ثورة المعلومات، حتى تجنى ثمار هذه الثورة؛ إذ يجب علينا مسايرة ركب التقدم العلمى فى مختلف مجالات الحياة.

٥- ضرورة عقد الندوات والمؤتمرات العربية، لبحث سبل مواجهة الإجرام الإلكترونى.

٦- ضرورة إعداد كوادر قضائية للبحث والتحقيق والمحاكمة، فى نطاق الجرائم المعلوماتية، مع استحداث قواعد مناسبة فى مجال الإجراءات الجنائية، بشأن التحقيق الابتدائى فى الجرائم المعلوماتية.

٧- عد المال المعلوماتى المعنوى على قدم المساواة فى الحماية الجنائية مع الأموال المنصوص عليها فى قوانين العقوبات التقليدية العربية، والاعتراف بإمكان إتلاف هذا المال، وتقرير العقوبة عنها المقررة أصلا على إتلاف فى المال المادى.

٨- إنشاء مركز قومى عربى لأمن الحاسبات والمعلومات، وضمان عدم إصابتها بالفيروس، أسوة بما قامت به فرنسا عندما أنشأت عام ٢٠٠٠ مكتبا مركزيا لمكافحة الجرائم المتصلة بتكنولوچيا المعلومات والاتصالات تابعا لوزارة الداخلية، كما استحدث جهاز (FBI) الأمريكى فى عام ٢٠٠٠ مركزا خاصا لمكافحة جرائم الإنترنت، مهمته بحث كيفية مجابهة الجرائم المعلوماتية.

٩- وفى موضوع ضبط الأدلة، نقترح ما يأتى:

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

ب- حث العاملين على النظام المعلوماتى على معاونة جهات التحقيق لضبط البيانات.

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

د- إعطاء أوسع الصلاحيات لجهات التحقيق، لاختراق نظام الحاسب الإلكترونى، وضبط ما يحويه من بيانات مخزنة، من دون إشعار مسبق بعملية التفتيش والضبط.

١٠- يلزم تعديل قوانين الإجراءات الجنائية ونظمها، بالقدر الذى يسمح ببيان الأحكام اللازم اتباعها حال إجراء التفتيش على الحاسبات الإلكترونية، وعند ضبط المعلومات التى تحتويها، وضبط البريد

الإلكترونـى، حتـى يستمد الـدليل مشـروعيته. كمـا ينبغـى السـماح لسلطات التحقيق بضبط البريد الإلكترونى، وأية تقنية أخرى قد تفيد فى إثبات الجريمة والحصول على دليل وكشف الحقيقة. ومن ثم يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب إلكترونى أخرى، يمكن أن تكـون ذات صـلة بالنظـام محـل التفتـيش، وضـبط مـا بهـا مـن معلومات.

الهوامش:

(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 novo 2000 relative a la criminalite informatique. Rev. Dr. Pen. Crime, 2002, p.611.

(3) Pinguet, M. (1996), La Douane et la Cyber-Delinquance G.P. 1996. doetr. 1325.

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

(5) Thompson, David (1990), Computer Crime: The Improvement of Investigative Skills: Final Report: Part 2. www.acpr.gov.au/pdf/ACPR101.pdf (21/10/2003)

(٦) محمد بن نصير محمد السرحانى: مهارات التحقيق الجنائى الفنى فى جرائم الحاسوب والإنترنت، "دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة ماجستير فى العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤، ص٩٥-٩٦.

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

(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 4/6/2003: www.ists.dartmouth.edu/TAG/need/ISTS_NA.pdf

(٩) غالبا ما يتم حفظ البيانات الرقمية داخل جهاز الحاسب الإلكتروني على شكل مجموعات أو كتل من البيانات، تمثل وحدة واحدة تسمى ملفات؛ إذ يتميز كل ملف ببينة وصيغة خاصة تسمى (Format) تميزه عن غيره، وغالبا ما ترتبط كل صيغة بنوع محدد من المحتوى، كأن يحتوى الملف على بيانات تمثل صورة أو صوتا أو فيديو أو مستندا خطيا أو غير ذلك. انظر: محمد بن نصير محمد السرحانى، مرجع سابق، ص ٩٧.

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

(11) Philip, M. (1986), Stanley Computer Crime Investigation and Investigators Computer & Security, Nort Holland, 1986, pp.310-311.

(12) Franklin Clark den Dilbert, Investigation Computer Crime, p.147.

(١٣) انظر الأحكام التالية التى وردت فى مجموعة أحكام محكمة النقض المصرية، الدائرة الجنائية، نقض ١٩٦١/٦/١٣، س١٢، رقم١٣١، ص٦٧١؛ نقض ١٩٧٤/٩/١٥، س٢٥، رقم١٨٣، ص٨٤٩؛ نقض ١٩٨٣/١/٤، س٣٤، رقم٥، ص٥٢.

(14) Robert Taylor: Computer Crime, "in Criminal Investigation Edited" by Charles Swanson, n. Chamelin and L. Territto, Hill, inc. 5 Edition, 1992, p.I.

(١٥) نقض مصرى ١٩٢٦/١٢/٢٦، المحاماة، س٧، ص٧٨٩؛ ١٩٧٢/٢/٨، س٨، ص١٩٥٨؛ ١٩٧٢/٣/١، مجموعة القواعد القانونية، ج٤، ص٥٢، رقم٤٣.

(١٦) انظر: جرائم الكمبيوتر، بحث مقدم من مركز البحوث والدراسات، أكاديمية شرطة دبى، ١٩٩٨، ص٢.

(١٧) د. هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.

(18) Meunier (C) La loi du 28 November 2000 relative a la crimlnalite infonnatique. Rev. Dr. Pen. Crim. 2002, p.611 et s.

(19) Meunier (C.): art. Prec, p.681.

(20) Op.cit, p.682.

(21) Op.cit, p.683.

(22) Ibid, p.683.

(23) Op.cit, p.684.

(٢٤) د. محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، ط٣، دار النهضة العربية، القاهرة، ١٩٩٨، ص٥٢٨-٥٢٩؛ د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، ج٢، دار النهضة العربية، القاهرة، ٢٠٠١، ص٦٤٤ وما بعدها.

(٢٥) نقض ١٩٨٠/١/٣١، مجموعة أحكام النقض، س٣١، رقم٢٩، ص١٤٨.

(٢٦) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية، القاهرة، ١٩٩٤، ص٥٩.

(٢٧) د.عبد الله حسين على محمود، إجراءات جمع الأدلة فى مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، إمارة دبى بدولة الإمارات العربية المتحدة ٢٦-٢٨/٤/٢٠٠٣م، المجلد الأول، ص٥٩٨.

(٢٨) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، سبقت الإشارة إليه، ص٣٠-٣١؛ د. عبد الله حسين على محمود، مرجع سابق، ص٥٥٩-٥٦٠.

(٢٩) القاضى وليد عاكوم، التحقيق فى جرائم الحاسوب، بحث منشور على شبكة الإنترنت، موقع الدليل الإلكترونى للقانون العربى

www.arablawinfo.com.

(٣٠) من فحص بعض البطاقات المثقبة المعثور عليها بسلة المهملات فى

المكان الموجود به جهاز الحاسب الإلكتروني، أمكن كشف غموض جريمة شهيرة لسرقة البرمجيات عن بعد، وقعت أحداثها بسانتا كلارا بالولايات المتحدة الأمريكية. حول التفاصيل الفنية لارتكاب هذه الجريمة انظر: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢، ص١٢٦-١٢٧.

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

(٣٢) د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة فى المدة من ١-٣/٥/٢٠٠٠، المجلد الثالث، ص١٠٣٠.

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

(٣٤) محمد بن نصير محمد السرحانى، مرجع سابق، ص٨١.

(٣٥) د.عبد الله حسين على محمود، مرجع سابق، ص٦٢٤-٦٢٧؛ د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة فى المدة من ١-٣/٥/٢٠٠٠، المجلد الثالث، ص١٠٢٥-١٠٥٩.

(٣٦) د. هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، ط١، دار النهضة العربية، القاهرة، ١٩٩٧، ص٤٧.

(٣٧) د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، ج١، دار النهضة العربية، القاهرة، ٢٠٠١، ص٤٣١ وما بعدها.

(38) Mohrenschlager, M. (1993), Computer Crimes and Others Crimes against Information Technology in Germany. Rev. Intern. De. Dr. Pen.1993, p.319, spec. 349.

(39) Conseil de L'eurpe (I 996), 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 (e): Art. Prec, p.663.

(41) Op.cit, p.664.

(42) Op.cit, p.668.

(٤٣) د. هشام محمد فريد رستم، مرجع سابق، ص٧٧-٧٨.

(٤٤) د. هلالى عبد اللاه أحمد، مرجع سابق، ص٧٣.

(٤٥) د. عبد الله حسين على محمود، إجراءات جمع الأدلة فى مجال سرقة المعلومات، بحث منشور على شبكة الإنترنت، موقع الدليل الإلكترونى للقانون العربى: www.arablawinfo.com.

(46) Vassilaki, Irini, Computer Crimes and other Crimes against Information Technology in Greece. Rev. Intern. De. Dr. Pen, p.371.

(٤٧) د. هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، ، مرجع سابق، ص٢٧.

(48) Piragoff (Donald K) (1993): Computer Crimes and Others 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.

(50) Linda Voloniono: op.,cit, p.2.

(51) Bnlclsterhng, op., cit, p.165.

(52) Kaspersen, H.W.K (I993), Computer Crimes and Others Crimes against Information Technology in Netherlands. Rev. Intern. De. Dr. Pen. 993, p.479.

(٥٣) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، مرجع سابق، ص٣٤-٣٥.

(٥٤) 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 المدة من ١٤-١٦/١١/٢٠٠٥، ص١٥.

(٥٥) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص٢٧.

(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, p.77.

(57) Padova, Y. (2002), Un Apercu 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.

(61) Francillon, J. (1993), Les Crimes Informatiques et D'autres Crimes Dans le domaine de la Technologie Informatique. Rev. Int. Dr. Pen. 1993, p.309.

(62) Kaspersen (H.W.K.): op., cit, p.500-501.

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

(64) Yamaguchi, Atsushi (1993), Computer Crimes and other Crimes against Information Technology in Japan. Rev. Intern. De. Dr. Pen. 1993, p.443 .

(٦٥) تم وضع هذا المرشد عام ١٩٩٤، وصدر له ملحقان في عامي ١٩٩٧، ١٩٩٩، وقد قام بإعداده مجموعة عمل في قسم جرائم الحاسب الإلكتروني والملكية الفكرية بإشراف أستاذ القانون الجنائي Orin Kerr،

وقد صدرت له عدة تعديلات، أخرها كان تعديل ٢٠٠٢ الذى تضمن تطبيقا للقانون الوطنى الأمريكى الصادر فى ٢٠٠١/١٠/٢٦.

(٦٦) المرشد الأمريكى، مرجع سابق، المادة (١٦٢).

(٦٧) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٣٠.

(٦٨) د. عوض محمد، المبادئ العامة فى قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٩٩، ص٣٨١.

(69) Kaspersen, H.W.K (1993), Computer Crimes and Others Crimes against Information Technology in Netherlands. Rev. Intern. De. Dr. Pen.1993, p.474. spec, p.502. Mohrenschlager, M. (1993), Computer Crimes and Others Crimes against Information Technology in Germany. Rev. Intern. De. Dr. Pen. 1993, p.349. spec, p.350.

(70) Spreutels, J.P. (1993), Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Belgique. Rev. Int. Dr. Pen. 1993, p.161, spec, p.170.

(71) Piragoff (Donald K) (1993): Computer Crimes and Others Crimes against Information Technology in Canada. Rev. Intern. De. Dr. Pen.1993, p.20.spec, p.340 ets.

(72) Meunier(C.): Art. Prec, p.670.

(73) Op.cit, p.669.

(74) Op.cit, p.673.

(75) Op.cit, p.674.

(76) Op.cit, p.674.

(٧٧) تعرف محكمة النقض المصرية الشهادة بأنها تقرير لشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، نقض

١٩٧٦/١/٢٥، أحكام النقض، س٢٧، ص٩٤، رقم ٢٠؛ ١٩٧٨/٢/٦، س٢٩، ص١٣٩، رقم٢٥؛ ١٩٧٩/٤/٢، س٢٧، ص٩٤، رقم٢٠؛ ١٩٧٨/٢/٦، س٢٩، ص١٣٩، رقم٢٥؛ ١٩٧٩/٤/٢، س٣٠، ص٤٢٦، رقم٩٠.

(٧٨) د. محمد فهمى، الموسوعة الشاملة لمصطلحات الحاسب الإلكترونى، مطابع المكتب المصرى الحديث، القاهرة ١٩٩١، ص٢٣.

(٧٩) د. محمد فهمى طلبة، الحاسبات الإلكترونية.. حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع المكتب المصرى الحديث، القاهرة ١٩٩٢، ص٦٢.

(٨٠) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنشور على شبكة الإنترنت، موقع الدليل الإلكترونى للقانون العربى، المتاح على الرابط الإلكترونى: .www.arablawinfo.com

(81) Mohrenschlager, M. (1993), Computer Crimes and Others Crimes against Information Technology in Germany. Rev. Intern. De. Dr. Pen. 1993 p.351.

(82) Erman, Sahir (1993), Les Crimes Informatiques et D'autres Crimes Dans le Domaine de la Technologic Informatique en Turquie. Rev. Int. Dr. Pen. 1993, p.64.

(٨٣) انظر نص المواد (٢، ١٠٩، ١٣٨) من قانون الإجراءات الجنائية الفرنسى.

(84) Jacques Francillon, op., cit, p.309.

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

(٨٦) انظر نص الفقرة (١) من المادة (٢٢٣) من قانون الإجراءات الجنائية اليونانى.

المصادر والمراجع:

أولا- الكتب العربية:

١ - د. عوض محمد، المبادئ العامة فى قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٩٩.

٢ - د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠١.

٣ - د. محمد فهمى طلبة، الموسوعة الشاملة لمصطلحات الحاسب الإلكترونى، مطابع المكتب المصرى الحديث، القاهرة، ١٩٩١.

٤ - د. محمد فهمى طلبة، الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصرى الحديث، القاهرة، ١٩٩٢.

٥ - د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢.

٦ - د. هشام محمد فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية، دار النهضة العربية، القاهرة ١٩٩٤.

٧ - د. هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، ط١، دار النهضة العربية، القاهرة، ١٩٩١.

ثانيا- الرسائل العلمية والبحوث:

١ - د.عبد الله حسين على محمود، إجراءات جمع الأدلة فى مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، إمارة دبى بدولة الإمارات العربية المتحدة ٢٦-٢٠٠٣/٤/٢٨.

٢ - د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمى الأول حول الجوانب القانونية

والأمنية للعمليات الإلكترونية.
٣ - د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الآلى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة فى المدة من ١-٣/٥/٢٠٠٠.
٤ - د. محمد بن نصير محمد السرحانى، مهارات التحقيق الجنائى الفنى فى جرائم الحاسوب والإنترنت - دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤.
٥ - د. محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، ط٣، دار النهضة العربية، القاهرة، ١٩٩٨.
٦ - القاضى وليد عاكوم، التحقيق فى جرائم الحاسوب، بحث منشور على شبكة الإنترنت، موقع الدليل الإلكترونى للقانون العربى، المتاح على الرابط الإلكترونى: www.arablawinfo.com.

ثالثا- مواقع الانترنت:

1. www.secretservice.gov/electronic_evidence.shtml
2. www.ists.dartmouth.edu/TAG/need/ISTS_NA.pdf
3. www.acpr.gov.au/pdf/ACPR101.pdf (21/10/2003)
4. www.arablawinfo.com

رابعا- الكتب الفرنسية:

1. Conseil de L'eurpe (I 996), Problems de procedure penale lies a la technologie de l'information. Recommendation n. R (95) 13 et expose des motifs. Ed. Conseil de I' Europe.
2. Erman, Sahir (1993), Les crimes informatiques et d'autres crimes dans le domaine de la technologic informatique en Turquie. Rev. Int. Dr. Pen.

3. Francillon, J. (1993), Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique. Rev. Int. Dr. Pen.
4. L'informatique J.C.P. 1989 333 no.16. Gassin® Le droit penal et L'informatique D. 1982.
5. Meunier, C. (2002), La loi du 28 Nov. 2000 relative a la criminalite informatique. Rev. Dr. Pen. Crim.
6. O.C.D.E. (1986), La fraud liee a l'informatique, Paris.
7. Padova, Y. (2002), Un apercu de la lutte contre la cybercriminalite en France. R.S.C.
8. Pinguet, M. (1996), La douane et la cyber-delinquance G.P.
9. Spreutels, J.P. (1993), Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Belgique. Rev. Int. Dr. Pen.

خامسا- الكتب الإنجليزية:

1. Davis, David (1998), Internet Detective: An Investigator's Guide. West Midland, UK: Police Research Group.
2. Franklin Clark den Dilbert, Investigation Computer Crime.
3. Institute for Security Technology Studies (ISTS) (2002), Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment.
4. Kaspersen, H.W.K (I993), Computer Crimes and Others Crimes against Information Technology in Netherlands. Rev. Intern. De. Dr. Pen.
5. Mohrenschlager, M. (1993), Computer Crimes and Others Crimes against Information Technology in Germany. Rev. Intern. De. Dr. Pen.

6. Philip, M. (1986), Stanley Computer Crime Investigation and Investigators Computer & Security, Nort Holland.

7. Piragoff (Donald K) (1993): Computer Crimes and Others Crimes against Information Technology in Canada. Rev. Intern. De. Dr. Pen.

8. Sammes, T. & Jenkinson, B. (2000), Forensic Computing: A Pratitioner's Guide London: Springer.

9. Shindre, Debra (2000), Scene of the Cyber Crime: Computer Forensics Hand Book. Rockland, MA: Syngress Publishing.

10. 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.

11. Taylor, R. (1992). Computer Crime, "in Criminal Investigation Edited", by Charles Swanson, n. Chamelin and L. Territto, Hill, inc. 5 Edition.

12. Thompson, David (1990), Computer Crime The Improvement of Investigative Skills: Final Report: Part 2.

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

14. Vassilaki, Irini, Computer Crimes and other Crimes against Information Technology in Greece. Rev. Intern. De. Dr. Pen.

15. Yamaguchi, Atsushi (1993), Computer Crimes and other Crimes against Information Technology in Japan. Rev. Intern. De. Dr. Pen.

سادسا- القوانين:

١ - قانون تحقيق الجنايات البلجيكى.
٢ - قانون الإجراءات الجنائية الألمانى.
٣ - قانون الإجراءات الجنائية الفرنسى.
٤ - قانون الإجراءات الجنائية اليونانى.
٥ - القانون الجنائى الكندى.
٦ - قانون الإثبات الكندى.

جامعة الدول العربية
معهد البحوث والدراسات العربية
INSTITUTE OF ARAB RESEARCH AND STUDIES
مكتب اتحاد إذاعات الدول العربية