الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق

« في النظام الجزائي المصري والسعودي »

الدكتـــــور
طه السيد أحمد الرشيدي
أستاذ القانون المساعد بكلية الشريعة والأنظمة
جامعة الطائف

﴿ قَالُواْ سُبۡحَٰنَكَ لَا عِلۡمَ لَنَآ إِلَّا مَا عَلَّمۡتَنَآۖ إِنَّكَ أَنتَ ٱلۡعَلِيمُ ٱلۡحَكِيمُ ٣٢ ﴾

من سورة البقرة الآية ٣٢

مُقَدِّمَة

إن التطـور التكنولـوجي المعاصـر في مجـال تقنيـة المعلومـات وشـبكات الاتصالات عمل على التقارب بين ملايين البشر وأتاح فرصـا جديـدة للاطـلاع على المعلومات وتبادلها ؛ حتى وصف هذا العصر بعصر المعلومات، إلا أن هذه التقنية جلبت معها كثير من الآثار السلبية، تمثلت في استغلال بعض المجرمين هذا التطور في تقنية المعلومات وما يقدمـه مـن وسـائل حديثـة ومتقدمـة في ارتكـاب العديـد مـن الجـرائم التقليديـة، كالسـرقة والنصـب وخيانـة الأمانـة، وتزويـر المحررات، والاعتداء على حرمة الحياة الخاصة، وغير ذلك من الجرائم[١].

ومع شيوع الانترنت ووسائل الاتصالات الحديثة بزغ فجر ظاهرة إجرامية جديدة، تعرف بالإجرام ألمعلوماتي أو جرائم تقنية المعلومات؛ فتم السـطو علـى البنوك بمساعدة هذه الوسائل، ونمت الجريمة المنظمة وترعرعت في ظل هذه الثورة العلمية في مجال المعلومات والاتصالات، وخصوصاً في مجالات الإرهاب وتجارة المخدرات، والاتجار بالسلاح والدعارة المنظمة باستخدام الإنترنت[٢].

---

(١) د/ محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة دار الثقافة للنشر والتوزيع، عمان، سنة ١٤٣٠ هـ - ٢٠٠٩م، ص ٦٠٥.

(٢) د/ محمد أبو العلا عقيدة،التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع كلية الحقوق جامعة المنصورة - http://www.f-law.net ص ١، د/ عبد الفتاح بيومي حجازي،

وعلي الرغم من هذا الكم الرهيب من الجرائم التي ترتكب علي شبكة الانترنت إلا أن هناك فراغا تشريعيا في مواجهة هذه الجرائم التي مازالت تخضع لقانون الإجراءات العادي الذي أصبح غير قادر علي مواجهة هذه النوعية من الجرائم المستحدثة التي تحتاج إلي تكييفها قانونا محدد.

خاصة وأن الجريمة المعلوماتية لها طبيعتها الخاصة وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

وهذه الطبيعة الخاصة وهذا الاختلاف يعني أن الإجراءات الجنائية التقليدية لا تتناسب بالقدر الكافي لمكافحة هذه الجرائم وتثير مشكلات كبيرة في مجال إجراءات تحقيق الدعوى الجنائية، ومنها صعوبة التحري والتفتيش والضبط وجمع الأدلة الجنائية وإثبات هذه الجرائم، وهذا يتطلب صدور قوانين إجرائية خاصة بهذه الجرائم تعالج مشكلات التفتيش والضبط والتحقيق والاختصاص القضائي تتواكب مع طبيعة هذه الجرائم، وتضمن تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة،

خاصة وأن نصوص قانون الإجراءات الجنائية وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو

مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر سنة ٢٠٠٦م، ص ١٩.

التحقيق فيها وجميع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتبدأ المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا وكيانات غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذه المجال كما اشرنا سلفا، سرعة ودقة تنفيذ الجرائم الإلكترونية 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 أو شبكات إلكترونية موجودة بالخارج، ويثير 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، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال. وقد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، فيصعب إثباتها.

ويثير التفتيش أو الضبط أو المصادرة في مجال 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.

وتقتضي مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام تحقيق أمور عدة، منها : ضرورة إعداد كوادر أمنية وقضائية للبحث والتحقيق والمحاكمة في هذا النوع من الجرائم، كذلك تطوير التشريعات الجنائية الحالية سواء الموضوعية أو الإجرائية بإدخال نصوص التجريم والعقاب والنصوص الإجرائية اللازمة لمواجهة هذا الإجرام المستحدث. فضلا عن ذلك فإن التعاون الدولي في مجال الأمن والتحقيق وتسليم المجرمين وتنفيذ الأحكام يعد ضرورة لا مفر منها[1].

وقد أحسن المشرع العربي بوضع القانون العربي النموذجي الموحد في شان مكافحة سوء استخدام وسائل تكنولوجيا المعلومات والاتصالات، وأفرد الباب الرابع منه لبعض قواعد الإجراءات الجنائية في شأن جرائم الكمبيوتر والانترنت، وهي القواعد الأكثر أهمية، محيلاً فيما عداها إلى القواعد العامة في قانون الإجراءات الجنائية المصري.

---

(١) د/ محمد أبو العلا عقيدة،التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٢، ٣.، د/ نبيله هبة هروال، الجوانب الاجرائية في مرحلة جمع الاستدلال، طبعة دار الفكر الجامعي، مصر سنة ٢٠٠٦م، ص ١٣، د/ عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع منتدى هيئة التحقيق والادعاء السعودي ص ٣١.

وركزت المادة ٢٣ من القانون العربي النموذجي الموحد على وجوب الاستعانة بالخبير ألمعلوماتي المتخصص في البرامج واستخدام الانترنت، تلافيا لحدوث أضرار بالبرامج والبيانات كما ألزم مأمور الضبط القضائي بالبحث عن الجرائم المعلوماتية ومرتكبيها وجمع الاستدلالات اللازمة للتحقيق، شرط أن يكون مؤهلا للتعامل مع الطبيعة الخاصة لجرائم المعلومات. وهذا الأمر ينسحب بطبيعة الحال على تأهيل أعضاء النيابة العامة، وقضاة الحكم في هذا النوع من الجرائم

كما ركزت المادة ٢٦ من ذات القانون على ضمانات حماية سرية البيانات المخزنة في الحاسب الآلي أو الوسيط الإليكتروني، وعدم المساس بحقوق الغير التي تتعلق بالبيانات والبرامج المخزنة، وذلك عند القيام بعمليات التفتيش والضبط في نطاق الجريمة المعلوماتية[١].

وقد ساهمت بعض الدول العربية في هذا الشأن فأصدر المقنن المصري قانون التوقيع الاليكتروني رقم ١٥ لسنة ٢٠٠٤م كما أصدر المقنن الإماراتي القانون رقم ٢ لسنة ٢٠٠٦ لمكافحة جرائم تقنية المعلومات، كما أصدر المقنن السعودي نظام مكافحة جرائم المعلوماتية سنة ١٤٢٨هـ ٢٠٠٧م[٢].

---

(١) د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، ، ص ١٠، ١١.

(٢) د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي الموحد، دار الفكر الجامعي، مصر سنة ٢٠٠٦م، ص ٨، ٩.

ومما جاء في نظام مكافحة جرائم المعلوماتية السعودي المذكور في شأن الجوانب الإجرائية في المادة ١٥ :" تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام". وأشار في المادة ١٤ منه إلى تقديم الدعم والمساندة لجهة التحقيق من الجهات المختصة بقوله:" تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة"

وقد خصصت البحث على المشاكل الإجرائية في مرحلة التحقيق لأنها مرحلة ذات أهمية عملية تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة [(١)].

وتبدو أهميته في أنه مرحلة تحضيرية للمحاكمة؛ إذ يكفل أن تعرض الدعوى الجنائية على القضاء وهي معدة لأن يفصل فيها. ومن شأن التحقيق الابتدائي اكتشاف الأدلة قبل الإحالة إلى المحاكمة واستظهار قيمتها واستبعاد الأدلة الضعيفة، واستخلاص رأي مبدئي في شأن قيمة هذه الأدلة، فتستطيع المحكمة أن تنظر في الدعوى وقد اتضحت عناصرها وتكشف أهم أدلتها، فيدعم ذلك الاحتمال في أن يجيء حكمها أدنى إلى الحقيقة والعدالة. ويتصل بذلك أن بعض الأدلة لا يتيسر التنقيب عنه وقت المحاكمة، وإنما يتعين أن يكون ذلك في وقت معاصر لارتكاب الجريمة، ومن ثم كان دور

(١) د/ محمد عيد الغريب، شرح قانون الإجراءات الجنائية، طبعة النسر الذهبي للطباعة ١٩٩٦- ١٩٩٧، ص ٧٢٢، د/ نبيله هبة هروال، الجوانب الإجرائية في مرحلة جمع الاستدلال، ، ص ١٢.

التحقيق الابتدائي التنقيب عن أدلة الجريمة في الوقت الملائم لذلك. وللتحقيق الابتدائي أهميته كذلك في أنه يكفل ألا تحال إلى المحاكمة غير الحالات التي تتوافر فيها أدلة كافية تدعم احتمال الإدانة؛ وفي ذلك توفير لوقت القضاء وجهده، وصيانة لاعتبار المتهم من أن يمثل أمام القضاء إذا كانت الأدلة ضده غير كافية[1].

وقد حصر قانون الإجراءات الجنائية الإجراءات التي تملكها سلطات التحقيق بقصد الوصول إلى إثبات ارتكاب الفعل الإجرامي ونسبته إلى فاعل معين، في إجراءين.

أولهما: هو إجراءات جمع الأدلة، وثانيهما: هو التحفظ على شخص المتهم، وعدم تمكينه من الهرب أو التأثير في أدلة الجريمة، كالتكلف بالحضور، والقبض عليه، وحبسه احتياطياً.

وسوف يقتصر بحثنا هذا على الإجراءات الخاصة بجمع الأدلة فقط – على اعتبار أن الإجراءات الاحتياطية لا إشكال فيها ؛ فهي إجراءات تقليدية، وإجراءات جمع الأدلة التي أوردها القانون هي ندب الخبراء، والانتقال للمعاينة، والتفتيش، وضبط الأشياء المتعلقة بالجريمة والتصرف فيها، وسماع الشهود، والاستجواب والمواجهة. وهي لم ترد على سبيل الحصر لأن

---

(١) د/ محمود نجيب حسني: شرح قانون الإجراءات الجنائية، طبعة دار النهضة العربية، الطبعة الثانية ١٩٨٨، ص٦١٤، د/ فوزية عبد الستار، شرح قانون الإجراءات الجنائية، طبعة مطبعة جامعة القاهرة، نشر دار النهضة العربية، سنة ١٩٨٦، ص ٣٢١، د/ أحمد حسني أحمد طه، مبادئ قانون الإجراءات الجنائية في التشريع المصري، مطبعة بهجات للطباعة، الجزء الأول ص ٣٨٥.

للمحقق أن يستعين بأية وسيلة مشروعة مفيدة في الإثبات لا تنال من حريات الأفراد ولا حرمة مساكنهم وأسرارهم، ولو لم يرد لها ذكر في القانون، مثل عملية العرض القانوني للاستعراف على الشخص، أو الاستعانة بالبصمات، أو الكلاب[1].

مشكلة وأسئلة البحث:-

تتمثل المشكلة الرئيسية لهذا البحث في أن الجريمة المعلوماتية لها طبيعتها الخاصة وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

وهذه الطبيعة الخاصة وهذا الاختلاف يعني أن الإجراءات الجنائية التقليدية لا تتناسب بالقدر الكافي لمكافحة هذه الجرائم وتثير مشكلات كبيرة للمحقق في مجال إجراءات تحقيق الدعوى الجنائية، ومنها صعوبة التحري والتفتيش والضبط وجمع الأدلة الجنائية وإثبات هذه الجرائم، في إطار تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة، خاصة وأن نصوص قانون الإجراءات الجنائية وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجميع الأدلة المتعلقة بها وعلى ذلك فالحاجة تدعو إلى الإجابة على الأسئلة الآتية :-

---

(١) د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، طبعة دار الوزان، سنة ١٩٨٩، ص٢٣٠.

١ - ما أوجه الذاتية التي تميز جرائم تقنية المعلومات، وما مدي الاختلاف بين الجرائم التقليدية وجرائم تقنية المعلومات، وهل تصلح إجراءات التحقيق التقليدية للتطبيق على جرائم تقنية المعلومات ؟

٢- كيف يمكن للمحقق التغلب علي المشكلات الإجرائية في جرائم تقنية المعلومات، وكيف يتم التفتيش والضبط والمعاينة في هذا العالم الافتراضي في ضوء الأدلة غير المرئية ومسرح الجريمة غير التقليدي؟

٣- هل تحتاج مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام إعداد كوادر أمنية وقضائية للبحث والتحقيق والمحاكمة، وكذا تطوير التشريعات الجنائية الحالية سواء الموضوعية أو الإجرائية بإدخال نصوص التجريم والعقاب والنصوص الإجرائية اللازمة لمواجهة هذا الإجرام المستحدث؟

٤- كيف يمكن تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة ؟

أهمية البحث :

تكمن أهمية البحث في تنامي دور التعاملات الالكترونية الأمر الذي طرح تحديات عديدة أمام رجال القانون في مجال مكافحة جرائم تقنية المعلومات؛ ذلك أن هذه الجرائم تنوعت أساليب ارتكابها وتزايدت مخاطرها و حجم الخسائر الناجمة عنها حتى باتت تهدد الاقتصاد و الأمن القومي للدول التي ترتكز مصالحها الحيوية على التقنية بشكل عام وعلى المعلوماتية بشكل خاص؛ فقد أجرت منظمة ال **Alliance Business Software** دراسة عن أضرار جرائم الانترنت في بعض دول الشرق الأوسط. أظهرت هذه الدراسة آن هناك تباين بين الدول في حجم خسائر**damages** جرائم الانترنت جرائم الحاسب الآلي حيث تراوحت بين

ثلاثين مليون دولار أمريكي في المملكة العربية السعودية و الإمارات العربية المتحدة و مليون و أربعمائة ألف دولار أمريكي فقط في لبنان.

وجاء في صحيفة عكاظ السعودية يوم السبت ٢٨/ ١٠/ ١٤٣٣ العدد٤١٠٨ ص١٩ شئون وطن

قدر الخبراء في ختام مؤتمرهم ملتقى الجودة الشاملة في الأمن العام تحت شعار «الجودة والتميز واجب وإبداع»بجدة حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا، و بالإضافة لما سبق فانه من الضروري التعرف على جرائم تقنية المعلومات ودراسة خصائصها و طبيعتها الخاصة وما تتميز به عن الجرائم التقليدية، في أسلوب و طريقة ارتكابها؛ حيث يكون الحاسب الآلي هو أداة ارتكابها، وأنها ترتكب عبر شبكة الانترنت، وأنها عابرة للحدود، و أن مرتكبها يتمتع بخبرة فائقة في مجال الحاسب الآلي. الأمر الذي يستدعي تسليط الضوء على الصعوبات والإشكاليات العملية التي تقف كحجر عائق أمام أجهزة العدالة في مواجهتها لهذه الطائفة من الجرائم، ولاسيما أن أجهزة التحقيق الجنائي عند مباشرتها لإجراءات جمع الأدلة فإنها تواجه مشاكل إجرائية في الكشف عن هذا النوع من الجرائم و ملاحقة مرتكبيها و تقديمهم للمحاكمة سواء في المعاينة أو التفتيش أو الضبط، مما يتطلب من هذه الأجهزة دراسة هذه الجرائم وتأهيل كوادر متخصصة للتحقيق فيها والعمل على إيجاد تعاون إقليمي ودولي لمكافحتها.

■ **أسباب اختيار البحث:**

اختارت هذا البحث للأسباب الآتية:

١- أن الأخذ بمستجدات العصر من وسائل الاتصالات الحديثة أصبح ضرورة عصرية وأن جرائم تقنية المعلومات تنوعت أساليب ارتكابها و تزايدت مخاطرها و حجم الخسائر الناجمة عنها حتى باتت تهدد الاقتصاد و الأمن القومي للدول التي ترتكز مصالحها الحيوية على التقنية بشكل عام وعلى المعلوماتية بشكل خاص، وأن المصلحة المجتمعية داعية إلى تذليل كل الصعاب نحو مكافحة هذه الجرائم.

٢- صدور القانون العربي النموذجي الموحد في شان مكافحة سوء استخدام وسائل تكنولوجيا المعلومات والاتصالات، وقانون التوقيع الاليكتروني المصري رقم ١٥ لسنة ٢٠٠٤م والقانون رقم ٢ لسنة ٢٠٠٦ م الإماراتي لمكافحة جرائم تقنية المعلومات، ونظام مكافحة جرائم المعلوماتية السعودي سنة ١٤٢٨هـ ٢٠٠٧م.

٣- دراسة مدى نجاح الأنظمة السابقة في معالجة المشكلات والصعوبات التي تواجه أجهزة التحقيق الجنائي عند مباشرتها لإجراءات جمع الأدلة والكشف عن هذا النوع من الجرائم و ملاحقة مرتكبيها و تقديمهم للمحاكمة سواء تلك المتعلقة بالمعاينة أو التفتيش أو الضبط، أو تأهيل كوادر متخصصة للتحقيق فيها أو العمل على إيجاد تعاون إقليمي ودولي لمكافحة هذا النوع من الجرائم.

▪ **منهج البحث**:

سوف أعتمد في هذا البحث على منهج الاستقراء والتحليل لموضوعات البحث، وعلى البحث المكتبي فيما يتعلق بدراسة عناصر خطة العمل في ضوء التشريعات المختلفة، مع التركيز على النظام الجزائي المصري، والسعودي، والأبحاث والدراسات التي تناولت مجالات الدراسة، فضلا عن الاستعانة بالتقارير الصادرة عن الجهات الحكومية المعنية ٠

▪ **خطة البحث**:

سوف أتناول هذا البحث من خلال مقدمة وأربعة فصول وخاتمة كالتالي:

المقدمة: وتشتمل على أهمية موضوع البحث، وأسباب اختياره، والمنهج العلمي المتبع فيه، وخطة البحث.

الفصل الأول : **الطبيعة الخاصة لجرائم تقنية المعلومات** ؛ **وفيه مبحثين كالتالي**:

المبحث الأول : التعريف بجرائم تقنية المعلومات

المبحث الثاني :خصائص جرائم تقنية المعلومات وفيه مطلبان :

المطلب الأول :الخصائص المشتركة مع بعض الجرائم.

المطلب الثاني :الخصائص التي تنفرد بها جرائم المعلومات.

الفصل الثاني : **ماهية التحقيق الجنائي في جرائم تقنية المعلومات**، **وفيه مباحث**:

المبحث الأول : التعريف بالتحقيق الابتدائي وخصائصه.

المبحث الثاني : السلطة المختصة بالتحقيق الابتدائي.

المبحث الثالث : التأهيل الفني اللازم للمحقق في جرائم تقنية المعلومات، وفيه مطلبين :

المطلب الأول : إجادة التعامل مع خدمات الانترنت وشبكات الاتصال المختلفة.

المطلب الثاني : الاطلاع على الجوانب المتعلقة بجرائم المعلومات.

المبحث الرابع : مهام أجهزة التحقق في جرائم تقنية المعلومات، وفيه ثلاثة مطالب:

المطلب الأول : تلقي البلاغات والشكاوى.

المطلب الثاني : تحديد خطة العمل وتكوين فريق التحقيق.

المطلب الثالث : سرعة جمع أدلة الجريمة.

الفصل الثالث : إجراءات التحقيق في جرائم تقنية المعلومات وفيه ست مطالب:

المبحث الأول : معاينة مسرح الجريمة في جرائم تقنية المعلومات.

المبحث الثاني : التفتيش في جرائم تقنية المعلومات.

المبحث الثالث : الضبط في جرائم تقنية المعلومات.

المبحث الرابع : الشهادة في جرائم تقنية المعلومات.

المبحث الخامس : الخبرة في جرائم تقنية المعلومات.

المبحث السادس : استجواب المتهم ومواجهته في جرائم تقنية المعلومات.

الفصل الرابع : معوقات التحقيق في جرائم تقنية المعلومات، وفيه أربعة مباحث:

المبحث الأول: الإحجام عن الإبلاغ عن الجريمة.

المبحث الثاني: عدم توافر الكفاءة البشرية المؤهلة للتحقيق.

المبحث الثالث : خفاء الجريمة المعلوماتية، وغياب الدليل المرئي.

المبحث الرابع : صعوبة التعاون الدولي في مكافحة الجريمة المعلوماتية.

الخاتمة، وتشتمل على أهم النتائج والتوصيات.

الفهرست

الفصل الأول
الطبيعة الخاصة لجرائم تقنية المعلومات

تمهيد وتقسيم:

إن جرائم تقنية المعلومات [(١)].لها طبيعة خاصة؛ وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما

(١) يوجد تعدد بشان الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر وفيما بعد بيئة الشبكات، وهو تعدد رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط أو المتصل بتقنية المعلومات، فابتدءا من اصطلاح إساءة استخدام الكمبيوتر، مرورا باصطلاح احتيال الكمبيوتر، الجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر أو جرائم الحاسب الآلي، والجريمة المرتبطة بالكمبيوتر، جرائم التقنية العالية، والجرائم المعلوماتيّة، وغيرها، إلى جرائم الهاكرز أو الاختراقات فجرائم الانترنت فجرائم الكمبيوتر والانترنت، والجرائم الرقمية، وجريمة أصحاب الياقات البيضاء، والجرائم الناعمة، والجرائم النظيفة، وأخيرا السيبر كرايم، وهذا التعدد في ألألفاظ، والمصطلحات المعبرة عن الجريمة الإلكترونية أو جرائم تقنية المعلومات تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد. د/ محمد الأمين البشري تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت بحث مقدم إلى الحلقة العلمية (الانترنت والإرهاب) خلال الفترة من: ١٧-٢١ /١١/ ١٤٢٩هـ الموافق ١٥-١٩ /١١/ ٢٠٠٨م بالتعاون مع جامعة عين شمس، منشور على موقع جامعة نايف العربية للعلوم الأمنية، ص٨، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، إعداد:إدارة الدراسات والبحوث، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز،التعقيب) في الدول العربية المنعقد في جمهورية السودان خلال الفترة ٢٣ـ٢٥/ ٩/ م الموافق ٧-٩/ ١١/ ١٤٣٣هـ، جرائم الكمبيوتر والانترنت المعنى

يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.

كما أن هذه الجرائم تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها). وهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت. هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده - عبر دلالته العامة - يظهر مدى خطورة جرائم الكمبيوتر، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري[1].

لذا فان إدراك ماهية هذه الجرائم، وخصائصها، وسمات مرتكبيها ودوافعهم، وبيان أنواع هذه الجرائم، وطرق ارتكابها وكيفية مواجهتها؛ يتخذ أهمية بالغة لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية، وهذا ما سأتناوله في المباحث التالية:

والخصائص والصور وإستراتيجية المواجهة القانونية، بحث منشور على موقع: **www.Lawyers-Gate.Com**

(١) يونس عرب، جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل ١ مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ / ٢/ ٢٠٠٢ ص٢.

المبحث الأول
التعريف بجرائم تقنية المعلومات

إن تعريف الجريمة المعلوماتية أو جرائم تقنية المعلومات كان محلاً لاجتهادات الفقهاء، وذهبوا في ذلك مذاهب شتى ووضعوا تعريفات مختلفة، وبالتالي فليس هناك اتفاق على تعريف محدد لجرائم تقنية المعلومات، نتيجة للاجتهادات الفقهية المتشعبة في هذا المجال.

فهناك من تناول تعريف هذه الجريمة من زاوية تقنية) فنية) وهناك من تناولها من زاوية قانونية؛ فالتعريفات القائمة على معيار قانوني، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة، وتعريفات قائمة على معيار شخصي، وتحديدا متطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها. وهناك تعريفات تنظر إلى موضوع الجريمة وأنماطها وبعض العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو سمات مرتكبها وهذه التعريفات كالتالي[1].

---

(١) د/عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر، ، ص ٢٠، د/ محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من ١-٣/ ٥/ ٢٠٠٠م، ص ٦، عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، بحث منشور بمركز دراسات الكوفة، العدد السابع ٢٠٠٨م ص ١١١، ١١٢، عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة مكملة لمتطلبات الحصول على الماجستير، مقدمة لجامعة نايف العربية للعلوم الأمنية، ص ٦٣وما بعدها.

أولاً : التعريفات التي تنظر إلى زاوية التقنية:

القائلون بالتعريف التقني يذهبون إلى القول بأن الجريمة المعلوماتية هي": نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[١].

ويذهب أنصار هذا الاتجاه الفقهي إلى القول بان تعريف جرائم الحاسب الآلي من الناحية القانونية وتصنيف صورها يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جريمة الحاسب الآلي وهي : الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات، الخدمات الحيوية [٢].

وهناك جانب آخر من الفقه يذهب إلى تعريف جريمة الحاسب الآلي بأنها : الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنيت. ويرى أنصار هذا الجانب الفقهي أن من سمات هذه الجريمة أنها جريمة مستترة، وتتسم بالسرعة والتطور في وسائل ارتكابها، وهي أقل عنف في التنفيذ من الجرائم التقليدية، وعابرة للحدود، ويصعب إثباتها لعدم وجود أدلة مادية عليها، كما يسهل إتلاف الأدلة الخاصة بها، ونقص الخبرة

---

(١) د/ محمد الأمين البشري التحقيق في جرائم الحاسب الآلي، ص ٦، عادل يوسف عبد النبي، الجريمة المعلوماتية، ص ١١١، ١١٢.

(٢) د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر، ص ٢٠.

العلمية لدى الجهات القائمة على ضبطها، وعدم كفاية القوانين القائمة التي تعالجها[١].

ثانياً : التعريفات التي تنظر إلى موضوع الجريمة:

من التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجريم، تعريفها بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه " [٢]. وتعريفها بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "[٣]. أو هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "[٤].

---

(١) د/ محمد عبد الرحيم سلطان العلماء جرائم الانترنت والاحتساب عليها بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت جامعة الإمارات مايو ٢٠٠٥ ص ٥.

(٢) تعريف الأستاذ **Rosenblatt**، مشار إليه لدى د/ هشام رستم، ورقة عمل بعنوان:" جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، منشورة بمجلة الدراسات القانونية، تصدره كلية الحقوق، جامعة أسيوط، عدد ١٧ عام ١٩٩٥م، ص ٣١.

(٣) تعريف الدكتورة هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، ١٩٩٢، ص ٢٠

(٤) واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للولايات المتحدة الأمريكية **GOA** انظر :- **www.goa.gov**

ثالثاً : التعريفات التي تنظر إلى وسيلة ارتكاب الجريمة :

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة، فان أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، من هذه التعريفات، يعرفها الأستاذ جون فورستر[١]. بأنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تاديمان Tiedemaun بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا" [٢].

رابعاً : التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل :

جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع، وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل، وهي تحديدا سمة الدراية والمعرفة التقنية. من هذه التعريفات، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام ١٩٧٩، حيث عرفتها بأنها " أية جريمة لفاعلها معرفة

---

(١) **Tom Forester, Essential problems to High-Tech Society First MIT Pres edition, Cambridge, Massachusetts, ١٩٨٩, P. ١٠٤**

واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للولايات المتحدة الأمريكية **GOA** انظر : - **www.goa.gov**

(٢) مشار إلى هذه التعريفات لدى د. هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ص ٢٩ و ٣٠.

فنية بالحاسبات تمكنه من ارتكابها ". ومن هذه التعريفات أيضا تعريف David Thompson بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب ". وتعريف Stein Schjlberg بأنها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا " [١].

ومن أهم التعريفات لجريمة الكمبيوتر تعريف خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD، بأنها " كل فعل أو امتناع من شانه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" [٢].

وهذا التعريف متبنى من قبل العديد من الفقهاء والدارسين[٣]. بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح إمكانية التعامل مع التطورات المستقبلية التقنية.

---

(١) د. هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ص ٣٢.

(٢) انظر موقع: www.oecd.org

(٣) د. هشام رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ص ٣٥.

وكذا تعريف جريمة الكمبيوتر لخبراء منظمة التعاون الاقتصادي والتنمية، بأنها : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" [(١)].

وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام ١٩٨٣ ضمن حلقة (الإجرام المرتبط بتقنية المعلومات)، ويتبنى هذا التعريف الفقيه الألماني **Ulrich Sieher**، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

وعَرَّف نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم م/ ١٧ وتاريخ: ٨/ ٣/ ١٤٢٨هـ بناءً على قرار مجلس الوزراء رقم: (٧٩) وتاريخ: ٧/ ٣/ ١٤٢٨هـ الجريمة المعلوماتية بأنها:" أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" [(٢)].

وبالنظر إلى جملة التعريفات السابقة يتضح عدم وجود تعريف متفق عليه لهذه الجريمة ولذا فالتعريف الراجح في نظري لهذه الجريمة هو أنها :"سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية محله معطيات

---

(١) انظر موقع المنظمة على شبكة الانترنت.

(٢) عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية، ص٦٣ وما بعدها.

الكمبيوتر" [١]. فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الإجرامية، ومعاقب عليه قانونا لان إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق. ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها، المعلومات المستخرجة، والمتبادلة بين النظم) وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوج بين تقنيات الحوسبة والاتصال، بما في ذلك شبكات المعلومات [٢].

(١) وهو تعريف الأستاذ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، طبعة دار الفكر الجامعي، ٢٠٠٦م ص ١٧٩. ورجحه الاستاذ / يونس عرب، جرائم الكمبيوتر والانترنت، ص١١، جرائم الكمبيوتر والانترنت، المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، منشور على موقع :**www.Lawyers-Gate.com** ،محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني طبقا للقانون السعودي، منشور على موقع : **http://www.f-law.net** كلية الحقوق جامعة المنصورة

(٢) المراجع السابقة نفس الموضع.

المبحث الثاني
خصائص جرائم تقنية المعلومات

تمهيد وتقسيم:

تعد جرائم المعلوماتية إفرازا ونتاجاً لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما اكسبها لوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الصفات قد يتطابق بعضها مع صفات طوائف أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فأن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية.

وسوف أقسم هذا المبحث إلى مطلبين: أتناول في المطلب الأول خصائص جرائم تقنية المعلومات المشتركة مع بعض الجرائم الأخرى، وأتناول في المطلب الثاني الخصائص التي تنفرد بها جرائم تقنية المعلومات.

المطلب الأول
الخصائص المشتركة مع بعض الجرائم

من خصائص جرائم تقنية المعلومات خطورتها البالغة والحجم الكبير للخسائر والأضرار التي تنشأ عنها، إضافة إلى أنها توصف بأنها من الجرائم العابرة للحدود، وهي بذلك تشترك مع بعض الجرائم الأخرى كالإرهاب، والاتجار بالمخدرات، وغسيل الأموال، وسوف أتناول هذه الخصائص بشيء من التفصيل في الفرعين التاليين:

الفرع الأول
خطورة جرائم تقنية المعلومات

تكتسب دراسة جرائم الحاسب الآلي أهمية خاصة نظراً لخطورتها، وذلك لأنها تمس الإنسان في فكره وحياته الخاصة، وتمس المؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي.

كذلك فإن الخسائر الناشئة عن هذه الجرائم توصف بأنها فادحة[(١)]. فقد جاء في صحيفة عكاظ السعودية [(٢)]:"كشف خبير عالمي أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم يبلغ ١١٤ مليار دولار، وأكد في ختام ملتقى الجودة الشاملة في الأمن العام تحت شعار «الجودة والتميز واجب وإبداع» نحن أمام تحد جوهري يحتم الإسراع في ضخ ثقافة أمن المعلومات لحماية الأفراد من الابتزاز والجهات والممتلكات من الخسائر الناجمة عن

(١) د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ١٩٩٤، ص١٩، د/ محمود عبابنة، جرائم الحاسوب وأبعادها الدولية، ص٣٢.

(٢) الصادرة يوم السبت٢٨/ ١٠/ ١٤٣٣ العدد ٤١٠٨ ص١٩ شئون وطن.

التساهل في أنظمة الحماية. وشدد عدد من الخبراء العالميين المشاركين في الملتقى، على أن الجريمة إلكترونية أكبر عائق يواجه التعامل مع مختلف القضايا، مشيرين إلى أن أمن المعلومات والاختراق والجرائم الإلكترونية، يحتم على وزارت الاتصالات وتقنية المعلومات الإسراع في نشر المعلومات والإحصاءات في سبيل حماية الوطن ومقدراته من الخسائر والجرائم الإلكترونية الناجمة عن عدم نشر تلك الإحصاءات.

وقدر الخبراء في ختام مؤتمرهم بجدة حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا، متوقعين ارتفاع هذه الأرقام نظرا لتزايد استخدام الإنترنت على نطاق واسع للتواصل وعقد المعاملات والصفقات التجارية من قبل كل من الأفراد والمؤسسات على حد سواء.

ودعا الخبراء لضرورة العمل على مراجعة وتطوير قانون الجرائم الإلكترونية وتطوير أقسام أكاديمية في الجامعات للتعامل مع الجرائم الإلكترونية، إضافة إلى التعاون مع شركات عالمية متخصصة لتقديم استشارات في مجالات الحماية وأمن المعلومات.

ومن جهته أكد الدكتور عايض طالع العمري رئيس مجلس الجودة السعودي في المنطقة الغربية أن العالم يشهد اليوم ثورة هائلة في مجال تقنية المعلومات، وانتشار استخدام الشبكة المعلوماتية (الانترنت) على نطاق واسع

حول العالم، حيث تشير آخر الإحصائيات أن عدد مستخدمي الانترنت في العالم أكثر من ٢ مليار مستخدم العام الماضي، وأن عدد مستخدمي الإنترنت في الشرق الأوسط ٦٨.٦ مليون مستخدم، مشيرا إلى أن الدولة الأولى في العالم من حيث عدد مستخدمي الإنترنت هي الصين وبين أن هذا الرقم أدى لانتشار الجرائم الإلكترونية بشكل سريع

وأكد عضو مجلس الجودة السعودي الدكتور هاني حسن فتياني، أن إحصاءات نشرت مؤخرا أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم يبلغ ١١٤ مليار دولار، وقال: كل ذلك يضعنا أمام تحد جوهري يتمثل في الإسراع في ضخ ثقافة أمن المعلومات لحماية الأفراد من الابتزاز والجهات والممتلكات من الخسائر الناجمة عن التساهل في أنظمة الحماية. وأشار إلى أن الجرائم الإلكترونية كبدت دول مجلس التعاون الخليجي خسائر تقدر بـ ٧٣٥ مليون دولار سنويا، لافتا إلى أن تلك الجرائم إذا كانت تستهدف المؤسسات فإنها تنطوي على أضرار وأخطار جسيمة تلحق بالمؤسسات المستهدفة".

وجاء في الأهرام المسائي المصري[1]: "حذر خبراء من تزايد معدلات الجريمة الالكترونية في مصر واعتبروها تمثل مشكلة كبري لقطاع الاتصالات والتكنولوجيا المتنامي في الفترة الأخيرة. وقدرت إحدى شركات برامج الحماية من مخاطر الإنترنت حجم الخسائر الناجمة عن جرائم اختراق شبكات الإنترنت والكمبيوتر عالميا بـ٤٠ مليار دولار، في حين تصل سوق برامج الحماية المقلدة والمنسوخة إلى ٢٥٪ من حجم السوق الإقليمية

(١) الصادرة في نوفمبر ٢٠٠٩ العدد٣ ا.محمد رمضان.

من جانبه اعترف المهندس محمد حجازي مدير مكتب حماية الملكية الفكرية التابع لـ إيتيدا بوزارة الاتصالات بأن نسبة القرصنة التي تتعرض لها برامج الحماية والسوفت وير في مصر تصل إلى ٥٩٪ وفقا لآخر إحصائية تم إجراؤها في ٢٠٠٩م.

وبالإضافة لذلك تعتبر البنوك هي الهدف الرئيسي للنسل الجديد من مجرمي التقنية العالية؛ ذلك لأنها تعتمد اعتمادا كليا ورئيسيا على أنظمة نقل التمويل إلكترونيا EFT ؛ إذ أن بنوك نيويورك وحدها تتناقل ٢٠٠ بليون دولار يومياً فما الذي سيكون عليه الحال إذا ما استطاعت الأيدي المنحرفة على الحصول على رموز التخويل الالكترونية المستخدمة في EFT ؟ وكم من الأموال يمكن نقلها في ثوان معدودة إلى خارج البلاد؟".

إضافة إلى هذا النوع من الإجرام، فإن هناك أنواعا أخرى كالقروض الوهمية وفتح اعتمادات وأشكال أخرى من التلاعب ونصب بطاقات التسليف[1].

وخلاصة الأمر أنه يمكن القول أن جرائم تقنية المعلومات تطال المعلومات، ذلك الحق الذي يمس البناء العلمي والثقافي والاقتصادي والذي ينعكس بدوره، ويقف عائقاً في طريق التنمية، كما أن هذه الجرائم تطال حياة الأفراد الخاصة ؛ فالاطلاع على خصوصيات الأفراد جريمة كفلتها كل التشريعات، إضافة إلى تهديدها الأمن القومي للدول، فالاختراقات التي تمت بواسطة الحواسيب التابعة لوزارة الدفاع الأمريكية هددت الأمن القومي

(١) د/ محمود عبابنة، جرائم الحاسوب، ص٣٣.

الأمريكي، إضافة لمخاطر متعددة، كفقدان الثقة بالتقنية وتهديد الملكية الفكرية وقتل روح الإبداع الإنساني[١].

الفرع الثاني
جرائم تقنية المعلومات جرائم عابرة للحدود

أخذت تكنولوجيا الحاسب الآلي تلعب دوراً بالغ الأهمية في العالم المعاصر، وغزت الأسواق سواء الخاصة بالدول المتقدمة صناعياً أو دول العالم الثالث؛ فالدول المتقدمة صناعياً تقوم بتصنيع أجهزة الحاسب الآلي وابتكار برامج ومصنفات لتحقيق الربح المادي، وتقوم دول العالم الثالث باستقبال هذه المبتكرات واستخدامها على نطاق واسع نظراً لصغر حجمها وقلة كلفتها وتزايد الحاجة إليها.

هذا التطور التكنولوجي في مجال الحاسبات وبرامجها وشبكات الاتصال، وخاصة شبكة الانترنت جعل الإنتاج الذهني يتصف بالعالمية لأنه لا يقتصر على دولة دون أخرى ؛ فالبشرية كلها شريكة في الاستفادة من هذا الإنتاج الأدبي والذهني[٢].

كما ربطت الانترنت العالم بشبكة اتصال متميزة و فعالة من خلال الأقمار الصناعية و الفضائيات، وجعلت الانتشار الثقافي وعولمة الثقافة و الجريمة أمراً ممكناً و شائعاً.و قربت شعوب العالم بأجناسهم و ثقافتهم

---

(١) د/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي)، الكتاب الأول، دار النهضة العربية، ١٩٩٢، ص ١٧.

(٢) د/ محمود عبابنة، جرائم الحاسوب، ص٣٣.

المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال. واستخدام هذه الشبكة أدى إلى سلبيات تمثلت في انتشار الجريمة، وأصبحت الجرائم المستحدثة و المنتشرة بواسطة الإنترنت مشكلة عالمية لا تعترف بالحدود الجغرافية للدول؛ لارتباط العالم بشبكة واحدة، فغالباً ما يكون الجاني في بلد و المجني عليه في بلد آخر،كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه.وهذا ملاحظ من خلال نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي[١].

وبذلك أعطى انتشار شبكة الانترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، ونتج عن ذلك أن الاستخدام غير الشرعي الناجم عن الاتصال بالحاسوب أيضاً اتصف بالعالمية أو بالعابر للحدود، فالجرائم لم تعد تقتصر على إقليم ولا تتعداه، بل أصبح بالإمكان ارتكاب الجرائم عن طريق الحواسيب باختراقه لحواسيب في بلد آخر أو إتلاف معطياتها، فالتعدي في بلد وأثره في بلد آخر، وصار من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر كما سبق، وهكذا [٢].

ولهذا فان جرائم الحاسوب تشترك مع غيرها من الجرائم في إنها تتخطى حدود الدول، كتجارة المخدرات و غسيل الأموال، إلا أنها تتميز عن

---

(١) الجرائم المعلوماتية ونظام مكافحتها في المملكة العربية السعودية بحث منشور على موقع: g.com٤٤http://www.f

(٢) د/ محمود عبابنة، جرائم الحاسوب، ص٣٤..

الأخيرة حيث يمكن ارتكابها دون مغادرة المقعد المقابل للحاسب الآلي بعكس جرائم المخدرات وغسيل الأموال التي تتطلب حركة بين الدول.

ومن الأمثلة على هذه الجرائم عابرة الحدود، تمكن احد الهواة في أوروبا من حل شفرة احد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) و من ثم أصبح المجال مفتوحا للعبث ببيانات هذا المركز، و كذلك الحال في إنتاج الفيروسات[1].

هذا التباعد أدى إلى إن تتشتت الجهود في مواجهة هذا النوع من الإجرام، فوجود الجاني على سبيل المثال في أوروبا والمتضرر في أمريكا يجعل التصدي لهذا النوع من الإجرام أمرا عسيرا، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق، الأمر الذي حدا بالبعض للقول" بان المجتمعات المعاصرة في ظل التقنية الحديثة، اقتصادا بلا حدود و ثقافة بلا حدود، عن جريمة منظمة بلا حدود حيث تم استغلال الحاسب الآلي فيها أسوا استغلال، فعن طريق الانترنت تم تحويل الأموال الكترونيا و غسلها" [2]

(١) د/ عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الآلي، بحث منشور في كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، ١٩٩١م.

(٢) د/ محمود عبابنة، جرائم الحاسوب وأبعادها الدولية ، ص٣٥..

المطلب الثاني
الخصائص التي تنفرد بها جرائم المعلومات

تعد جرائم المعلوماتية إفرازا ونتاجاً لتقنية المعلومات ولذا فهي تتميز عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الخصائص، وهي كالتالي[١]:

أولاً: الحاسب الآلي هو أداة ارتكاب جرائم تقنية المعلومات:

الحاسب الآلي هو دائما أداة الجريمة في الجرائم التي ترتكب على شبكة الانترنت وهى خاصية متفردة عن أي جريمة أخرى؛ ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الانترنت و قيامه بتنفيذ جريمته أيا كان نوعها[٢].

---

(١) عادل يوسف عبد النبي، الجريمة المعلوماتية، ص ١١٤وما بعدها.

(٢) تقسيم الجرائم المعلوماتية بحسب ما يستهدفه المجرمون من هذه الجريمة إلى أربعة أنواع، كالتالي:

النوع الأول : يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو بواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية. ومع أن وجود هذه البرامج في جهاز الحاسب الآلي لا يعنى إطلاقا الحماية التامة من أي هجوم فيروسي وأن ما هو احد سبل الوقاية والتي قد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديث وغير معروف من السابق.

وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الانترنت[١].

النوع الثاني: يستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة، وما يميز هذا النوع من الجرائم انه من الصعوبة بمكان اكتشافه مالم يكن هناك تشابهه في بعض أسماء أصحاب هذه البطاقات.

النوع الثالث: يشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة.

النوع الرابع: يشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل. د/علي جبار الحسيني، جرائم الحاسوب والانترنت، طبعة دار اليازوري العلمية للنشر والتوزيع، الأردن، ٢٠٠٩م ص ٥٥،٥٦، منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي، ص٢٢، ٢٣، محمد عبد الله المنشاوي، جرائم الإنترنت من منظور شرعي وقانوني طبقا للقانون السعودي، منشور على موقع : **http://www.f-law.net**، عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية، ص ٦٨وما بعدها

(١) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي، ص١٤،.

ثانياً: أنها جرائم ترتكب عبر شبكة الانترنت:

تعد شبكة الانترنت هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك و الشركات الصناعية و غيرها من الأهداف التي ما تكون غالبا الضحية لتلك الجرائم و هو ما دعا تلك الأهداف إلى اللجوء إلى نظم الأمن الالكترونية في محاولة منها لحماية نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم[١].

ثالثاً: مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي:

لاستخدام الحاسب الآلي لارتكاب جريمة على شبكة الانترنت لابد وان يكون مستخدم هذا الحاسب الآلي على دراية فائقة و ذو خبرة كبيرة في مجال استخدامه و إلا فأين له بالخبرة اللازمة التي تمكنه من تنفيذ جريمته والعمل على عدم كشفها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي و أن الشرطة أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم [٢].

رابعاً: صعوبة الكشف عن الجريمة المعلوماتية وإثباتها:

لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الالكتروني إلى أي عنف أو سفك للدماء أو آثار اقتحام لسرقة الأموال، وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحي كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الالكتروني، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها [٣].

---

(١) د/ نبيله هبه هروال الجوانب الإجرائية، ص ٣٧.

(٢) ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي، ص١٤،.

(٣) شمس الدين إبراهيم احمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري دراسة مقارنة، طبعة دار النهضة

وهناك صعوبة أخرى تتعلق بإثبات الجرائم المعلوماتية حيث إن هذه الجرائم لا تترك أي اثر خارجي ومرئي لها، ومما يزيد من صعوبة إثباتها ارتكابها في الخفاء وعدم وجود أي اثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات فهذه الجرائم تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا[1]

كما توجد صعوبات أخرى تكتنف إثبات هذه الجرائم تكمن في المجرمين الذين يخططون لمثل هذا النوع من الجرائم هم دائماً أصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة تكفل نجاحهم في ارتكاب الجريمة وفرارهم من أعين السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها بالإضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي لإثبات هذه الجرائم، بالشكل الذي يوجب البحث عن أدلة جديدة وحديثة ناتجة من ذات الحاسب الآلي، وهنا تبدأ صعوبات البحث والتحري عن الدليل، وجمع هذا الدليل، وتبدأ إشكالية

العربية القاهرة ط ١ ٢٠٠٥م، ص ١٠٤، عادل يوسف عبد النبي، الجريمة المعلوماتية ، ص ١١٤وما بعدها.

(١) د/ هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي العدد(٢)، ١٩٩٩م، محمد عبد الله أبو بكر سلامة موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت منشأة المعارف، الإسكندرية ٢٠٠٦ ص٢٠.

قبوله إن وجد ومدى مصداقيته على إثبات جريمة تنصب على عناصر غير مادية معلومات وبرامج[١].

خامساً: أنها جرائم ناعمة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، الاغتصاب، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي[٢].

سادساً: خصوصية مجرم المعلومات:

قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة ولكن الأمر مختلف تماما بالنسبة للمجرم ألمعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات[٣]. ويوصف الإجرام ألمعلوماتي بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم ألمعلوماتي إنسان على مستوى من الذكاء، إضافة إلى انه مجرم متكيف اجتماعياً لا يناصب العداء للمجتمع[٤].

---

(١) د/ عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص ٤٢.

(٢) مقدمة في الجرائم الالكترونية، بحث منشور على موقع : http://www.startimes.com

(٣) مصعب القطاونة، الإجراءات الجزائية الخاصة في الجرائم المعلوماتية، بحث منشور على موقع: http://www.lawjo.net

(٤) د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، ص ٨.

الفصل الثاني
ماهية التحقيق الجنائي في جرائم تقنية المعلومات

تمهيد وتقسيم:

التحقيق الجنائي هو أحد الوظائف الأساسية للقضاء الجنائي؛ فلا يمكن الفصل في أي دعوى جنائية دون تحقيق. والتحقيق الجنائي نوعان: تحقيق بمعناه الواسع، وآخر بمعناه الضيق.

ويشمل التحقيق بمعناه الواسع – قبل الجلسة- مجموع الإجراءات التي تستهدف جميع الأدلة والعناصر اللازمة التي تتيح لسلطة الحكم الفصل في الدعوى الجنائية. ويدخل في التحقيق بهذا المعنى إجراءات الاستدلال باعتبارها إجراءات ضرورية في كل دعوى أياً كانت أهميتها، سواء أجريت بمعرفة مأموري الضبط القضائي، أم بمعرفة النيابة العامة استثناء. أما التحقيق بمعناه الضيق، فلا ينصرف إلا إلى ما تجريه سلطات التحقيق المختلفة من إجراءات بشأن جمع الأدلة والكشف عن الحقيقة، أي ما يتم بمعرفة النيابة العامة أو هيئة التحقيق والادعاء العام بوصفهما سلطة تحقيق، أو بمعرفة قاضي التحقيق ومن في حكمه إذا ما ندب لتحقيق قضية معينة بذاتها. وما يتم منها بمعرفة مأموري الضبط القضائي في أحوال الانتداب من إحدى سلطات التحقيق.

ويمثل التحقيق بهذا المعنى المرحلة الأولى للدعوى الجنائية، وهي المرحلة التي تمهد للمحاكمة. ويطلق على هذا التحقيق وصف التحقيق الابتدائي[1].

---

(١) د/ محمد عيد الغريب، شرح قانون الإجراءات الجنائية، ص٧٢٢.

ونظرا لان جرائم تقنية المعلومات لها طبيعة خاصة تتميز بها عن الجرائم التقليدية، وبالتالي فإن تحقيق هذه الجرائم سوف يتطلب تأهيل فني خاص للمحقق وسرعة في الإجراءات، وسوف أتحدث فيما يلي عن التعريف بالتحقيق الابتدائي، وخصائصه، والسلطة المختصة بالتحقيق الابتدائي، والتأهيل الفني اللازم للمحقق، ومهام أجهزة التحقق في جرائم تقنية المعلومات.وذلك من خلال المباحث التالية:-

المبحث الأول
التعريف بالتحقيق الابتدائي وخصائصه

تقسيم:

سوف أتحدث في هذا المبحث عن التعريف بالتحقيق الابتدائي وخصائصه، من خلال المطلبين التاليين:

المطلب الأول
التعريف بالتحقيق الابتدائي

يُعرف التحقيق الابتدائي بأنه مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة(١). كما يعرف بأنه :" مجموعة من الإجراءات الحقيقية تنهض بها هيئة التحقيق والادعاء العام بغية كشف الحقيقة في أمر الجريمة الواقعة قبل إحالتها لقضاء الحكم" (٢). وقد وصف التحقيق بأنه (ابتدائي) لأن غايته ليست كامنة فيه، وإنما يستهدف التمهيد لمرحلة المحاكمة؛ وليس من شأنه الفصل في الدعوى بالإدانة أو البراءة، وإنما مجرد استجماع العناصر التي تتيح لسلطة أخرى ذلك الفصل(٣).

---

(١) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ص٤، د/ عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية جـ ١، رقم ٢١٤، ص٣٤٩.

(٢) د/ زكى محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، طبعة ٢٠١١م، ص٢٥٢.

(٣) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ص٦١٤.

ولا يجب إجراء تحقيق ابتدائي بمعرفة سلطات التحقيق - الممثلة في النيابة العامة أو قاضي التحقيق في النظام الجنائي المصري وهيئة التحقيق والادعاء العام في النظام الجزائي السعودي - في جميع الدعاوى[1]. هذا

(١) أوجب القانون المصري التحقيق الابتدائي في الجنايات قبل رفعها إلى المحكمة لأنها جرائم تستوجب عقوبة شديدة، أما الجنح والمخالفات فلم يوجب القانون فيها تحقيق ابتدائي؛ فيجوز رفعها إلى المحكمة دون تحقيق اكتفاء بما ورد في محضر جمع الاستدلال، وعلى ذلك نصت المادة ٦٣من قانون الإجراءات الجنائية بقولها:" إذا رأت النيابة العامة في مواد المخالفات والجنح أن الدعوى صالحة لرفعها بناء على الاستدلالات التي جمعت، تكلف المتهم بالحضور مباشرة أمام المحكمة المختصة". وكذلك الأمر في نظام الإجراءات الجزائية السعودي؛ فهو يوجب التحقيق قي الجرائم الكبيرة، بينما التحقيق في غير هذه الجرائم جوازي حسب ظروف كل دعوى وعلى ذلك نصت المادة ٦٤ من نظام الإجراءات الجزائية بقولها:". ..... ويجب على المُحقِّق أن يقوم بالتحقيق في جميع الجرائم الكبيرة وِفقاً لما هو منصوص عليه في هذا النِظام. ولهُ في غير هذه الجرائم أن يقوم بالتحقيق فيها إذا وجد أن ظروفِها أو أهميتُها تستلزم ذلك، أو أن يرفع الدعوى بتكليف المُتهم بالحضور مُباشرة أمام المحكمة المُختصة."

وقد أصدر وزير الداخلية – بناءً على توصية رئيس هيئة التحقيق والادِعاء العام وفقا لنص المادة ١١٢ من نظام الإجراءات الجزائية السعودي – القرار الوزاري رقم (١٩٠٠) وتاريخ ٩/ ٧/ ١٤٢٨ هـ بتحديد الجرائم الكبيرة. وهي كالتالي:

١ - الحدود المعاقب عليها بالقتل أو القطع. ٢- القتل العمد أو شبه العمد. ٣- جرائم الإرهاب والجرائم المخلة بأمن الدولة. ٤- قضايا المخدرات والمؤثرات العقلية أو الأسلحة والذخائر أو تزييف أو تقليد النقود أو التزوير أو الرشوة أو انتحال صفة رجل السلطة العامة أو غسل الأموال ؛ المعاقب على أي منها نظاماً

بخلاف إجراءات التحقيق بمعرفة المحكمة التي ترفع إليها الدعوى؛ فالأصل أن المحكمة يجب عليها أن تحقق الدعوى بنفسها، وتحكم فيها بناء على ما تنتهي إليه من تحقيق.وتبدو أهمية التحقيق الابتدائي في أنه (مرحلة تحضيرية) للمحاكمة، إذ يكفل أن تعرض الدعوى الجنائية على القضاء وهي معدة لأن يفصل فيها. ومن شأن التحقيق الابتدائي اكتشاف الأدلة قبل الإحالة إلى المحاكمة واستظهار قيمتها واستبعاد الأدلة الضعيفة، واستخلاص رأي مبدئي في شأن قيمة هذه الأدلة، فتستطيع المحكمة أن تنظر في الدعوى وقد اتضحت عناصرها وتكشف أهم أدلتها، فيدعم ذلك الاحتمال في أن يجيء حكمها أقرب إلى الحقيقة والعدالة. ويتصل بذلك أن بعض الأدلة لا يتيسر التنقيب

بسجن يزيد عن سنتين. ٥- سرقة السيارات. ٦- القوادة أو إعداد أماكن الدعارة. ٧- ترويج المسكرات أو قصد الترويج في حال تهريبها أو تصنيعها أو حيازتها. ٨- اختلاس الأموال الحكومية أو أموال الشركات المساهمة أو البنوك أو المصارف ما لم يرد المبلغ المختلس.٩- الاعتداء عمداً على ما دون النفس الناتج عنها زوال عضو أو تعطيل منفعة أو جزء منها أو إصابة مدة الشفاء منها تزيد عن خمسة عشر يوماً، ما لم يتنازل صاحب الحق الخاص. ١٠- الاعتداء عمداً على الأموال أو الممتلكات العامة أو الخاصة بأي وسيلة من وسائل الإتلاف بما يزيد قيمة التالف عن(٥.٠٠٠ ريال) خمسة آلاف ريال ما لم يتنازل صاحب الحق الخاص. ١١- الاعتداء على رجل الأمن أثناء مباشرته مهام وظيفته، أو الإضرار بمركبته الرسمية، أو بما يستخدمه من تجهيزات. ١٢- استعمال أو إشهار السلاح الناري بقصد الاعتداء أو التهديد به. ١٣- انتهاك حرمة المنازل بالدخول بقصد الاعتداء على النفس أو العرض أو المال. ١٤- انتهاك الأعراض بالتصوير والنشر أو التهديد بالنشر. ١٥- الاعتداء على أحد الوالدين بالضرب ما لم يحصل التنازل.

عنه وقت المحاكمة، وإنما يتعين أن يكون ذلك في وقت معاصر لارتكاب الجريمة، ومن ثم كان دور التحقيق الابتدائي التنقيب عن أدلة الجريمة في الوقت الملائم لذلك. وللتحقيق الابتدائي أهميته كذلك في أنه يكفل ألا تحال إلى المحاكمة غير الحالات التي تتوافر فيها أدلة كافية تدعم احتمال الإدانة؛ وفي ذلك توفير لوقت القضاء وجهده، وصيانة لاعتبار المتهم من أن يمثل أمام القضاء إذا كانت الأدلة ضده غير كافية[١].

المطلب الثاني
خصائص التحقيق الابتدائي

إن أهم الخصائص التي يتسم بها التحقيق الجنائي الذي يتم بمعرفة إحدى سلطات التحقيق، هي أن يكون هذا التحقيق علنياً بالنسبة للخصوم وأن يكون سرياً عن الجمهور وضرورة أن يتم تدوين محضر التحقيق بحضور كاتب[٢]. وسوف أتناول ذلك في الفروع الآتية:-

الفرع الأول
تدوين التحقيق بمعرفة كاتب

لكي يكون محضر التحقيق الابتدائي حجة على الكافة، ولكي يكون أساساً صالحاً لما يبنى عليه من نتائج، فإنه لا بد وأن يدون بمعرفة كاتب، وذلك لأنه لا يمكن الاعتماد على ذاكرة المحقق والتي قد تخونه بمرور الزمن، هذا بالإضافة إلى رغبة القانون في أن يتفرغ ذهن المحقق للعمل الفني فقط، ومن أجل ذلك فقد استلزم القانون على المحقق ضرورة أن يستصحب معه

---

(١) د/ محمد عيد الغريب، شرح قانون الإجراءات الجنائية، ص٧٢٤.

(٢) د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، ص ٢٢١.

كاتب من كتاب المحكمة أو من كتاب النيابة لتدوين محضر التحقيق، ولذلك نصت المادة ٧٣ إجراءات على أن "يستصحب قاضي التحقيق في جميع إجراءاته كاتباً من كتاب المحكمة يوقع معه المحاضر وتحفظ هذه المحاضر مع الأوامر وباقي الأوراق في قلم كتاب المحكمة". وعلى ذلك نصت المادة ٩٦ من نظام الإجراءات الجزائية السعودي على أنه :" على المُحقِّق أن يُثبِت في المحضر البيانات الكامِلة عن كُل شاهِد، تشمل: اسم الشاهد ولقبِه وسنِه، ومهنتِه، وجنسيتِه ومحل إقامتِه، وصِلتِه بالمُتهم، والمجني عليه، والمُدعي بالحق الخاص. وتُدَوَّن تِلك البيانات وشهادة الشهود، وإجراءات سماعِها في المحضر من غير تعديل أو شطب أو كشط أو تحشير أو إضافة. ولا يُعتمد شيء من ذلك، إلا إذا صدق عليه المُحقِّق والكاتِب والشاهِد".

وعلى ذلك فإن تدوين محضر التحقيق بمعرفة كاتب هو من أهم خصائص التحقيق الابتدائي، أما إذا دون المحقق التحقيق بنفسه بدون حضور كاتب، فإن ذلك لا يترتب عليه بطلان محضر التحقيق وإنما يؤدي إلى أن يكون هذا الإجراء الذي اتخذه صحيحاً باعتبار المحضر محضر جمع استدلالات وليس محضر تحقيق، ذلك لأن عضو النيابة أو عضو هيئة التحقيق والادعاء العام يجمع بين صفتين، صفة الضبطية القضائية، فهو يعد أحد من لهم هذه الصفة ويعتبر رئيساً للضبطية القضائية، وصفة التحقيق[1].

(١) د/ رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مطبعة الاستقلال الكبرى سنة ١٩٨٣م ص٣٨٤. وتطبيقاً لذلك قضت محكمة النقض بأن " ما يوجبه القانون من حضور كاتب مع عضو النيابة الذي يباشر التحقيق يوقع معه على كل

على أنه مما تجدر ملاحظته أن وجوب تدوين محضر التحقيق بمعرفة كاتب لا يكون لازماً إلا في الحالات التي يلزم لها تحرير محضر بإجراءات التحقيق التي تمت، مثل سماع الشهود، أما استجواب المتهم أو المعاينة أو إجراءات التحقيق التي لا تستدعي تحرير محاضر فإنها لا تستوجب على المحقق ضرورة استصحاب كاتب معه لتدوينها، ويمكن تحريرها بمعرفة المحقق ذاته مثل أوامر القبض والتفتيش والحبس الاحتياطي [(١)]، وعدم تدوين محضر التحقيق بمعرفة كاتب في الحالات التي يلزم فيها هذا لا يترتب عليه بطلان مطلق، وإنما بطلان نسبي يجب على صاحب المصلحة من الخصوم التمسك به أمام محكمة الموضوع، ولا يجوز لهم التمسك به لأول مرة أمام محكمة النقض، ولذلك قضي بأن الدفع ببطلان تحقيق النيابة العامة لعدم

المحاضر ومن تحليف الشهود يميناً بأن يشهدوا بالحق، ولا يقولوا إلا الحق، وإن كان هو الأصل الواجب الإتباع إلا أنه لا يترتب على عدم إتباعه بطلان ما يتخذه وكيل النيابة من إجراءات في حالة الاستعجال وقبل أن يحضر كاتب للتحقيق، وذلك لأن عضو النيابة يوصف كونه صاحب الحق في إجراء التحقيق ورئيس الضبطية القضائية، له من الاختصاص ما خوله القانون لسائر رجال الضبطية في المادتين ٢٤، ٣١ من قانون الإجراءات الجنائية من إثبات ما يرى أن الحالة تستدعي إثباته قبل حضور كاتب التحقيق، بل أن هذا هو الواجب الذي يتعين عليه القيام به سواء أكان أحد مرؤوسيه قد قام بذلك قبل حضوره أو لم يكن". نقض ٢٤/ ١١/ ١٩٥٢، مجموعة أحكام النقض، س٤، رقم٦٠، ص١٤٦، نقض ٢٠/ ٢/ ١٩٦١ مجموعة أحكام النقض، س١٢، رقم ٤٠، ص٢٣٢.

(١) نقض ٢٣/ ١٠/ ١٩٦١، مجموعة أحكام النقض، س١٢، رقم ١٦٥، ص٨٤١.

استصحاب كاتب وندبه غيره للقيام بعمله بغير أن توجد ضرورة لـذلك هـو دفع بإجراءات سابقة على المحاكمة وعلى ذلك فإنه يجب أن تبدى أمام محكمة الموضوع ولا يصح إبداؤها لأول مرة أمام محكمة النقض [(١)].

ولا يكفي لاعتبار المحضر محضر تحقيق أن يدون بمعرفة كاتب، بل يلـزم أن يوقع عليه كل من المحقق والكاتب (المادة ٧٣ إجراءات مصري، المادة ٩٧ إجراءات سعودي) ولا يغني عن التوقيع تحرير المحضر بخـط الكاتـب، ومتـى وقع كل من المحقق والكاتب فإنه لا يشترط بعـد ذلـك أن يوقـع الخصـوم أو الشهود على ما أدلوا به من أقوال، لأن توقيع المحقق والمكاتب كاف لإثبـات صحة الإجراءات التي دونت بالمحضر [(٢)].

الفرع الثاني
علانية التحقيق بالنسبة للخصوم

لقد استلزم قانون الإجراءات المصري ضرورة أن يتم التحقيـق بحضـور الخصوم، حيث نص في المادة ٧٧ إجراءات على أن "للنيابة العامـة وللمـتهم وللمجني عليـه وللمـدعي بـالحقوق المدنيـة وللمسـئول عنهـا ولـوكلائهم أن يحضروا جميع إجراءات التحقيق". كما ألزمت المادة (٧٨) إجراءات سـلطات

(١) نقض ٥/ ٦/ ١٩٦٧، مجموعة أحكام النقض، س١٨، رقم ١٥٤.

(٢) د/ مأمون سلامة : الإجراءات الجنائية في التشريع المصري، دار النهضة العربية سنة ٢٠٠٠م، جـ١، ص ٤٤٣. د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، ص٢٢١-٢٢٩، د/ زكى محمد شنَّاق، الوجيز في نظام الإجراءات الجزائية السعودي، ص٢٥٨.

التحقيق بإبلاغ الخصوم باليوم الذي سوف يتم فيه التحقيق، فنصت على أن "يخطر الخصوم باليوم الذي يباشر فيه القاضي إجراءات التحقيق ومكانها".

وكذلك الأمر في النظام الجزائي السعودي؛ فقد نصت المادة (٦٩) من نظام الإجراءات الجزائية على أنه:" للمُتهم والمجني عليه والمُدعي بالحق الخاص ووكيل كُلٍ مِنهُم أو مُحاميه، أن يحضُروا جميع إجراءات التحقيق.. " وكذلك ألزمت المادة (٧١) إجراءات سلطات التحقيق بإبلاغ الخصوم بالساعة واليوم الذي يباشر فيه التحقيق والمكان الذي تُجْرى فيه ؛ فنصت على أن " يُبلغ الخصوم بالساعة واليوم الذي يُباشِر فيه المُحقِّق إجراءات التحقيق، والمكان الذي تُجْرى فيه".

وإذا كان الأصل العام في النظام الإجرائي المصري والسعودي هو ضرورة أن يتم إجراء التحقيق في مواجهة الخصوم إلا أنه أجاز في أحوال استثنائية حصول التحقيق في غيبة الخصوم أو غيبة أحدهم، وهذه الحالات هي، حالة الاستعجال وحالة الضرورة[1].

---

(١) وهذا ما أكدته المادة ٧٧/ ٢ إجراءات مصري، ومع ذلك فلقاضي التحقيق أن يباشر في حالة الاستعجال بعض إجراءات التحقيق في غيبة الخصوم، ولهؤلاء الحق في الإطلاع على الأوراق المثبتة لهذه الإجراءات.

حيث نصت على أنه ".... ولقاضي التحقيق أن يجري التحقيق في غيبتهم متى رأى ضرورة ذلك لإظهار الحقيقة، وبمجرد انتهاء تلك الضرورة يبيح لهم الإطلاع على التحقيق".

فهذه المادة قد أعطت المحقق مباشرة بعض إجراءات التحقيق في غيبة الخصوم متى توافرت حالة الاستعجال، كسماع أقوال أحد الشهود قبل وفاته، أو معاينة مكان

هذا ومما تجدر ملاحظته، أن تقرير سرية التحقيق بالنسبة للخصوم في غير حالتي الضرورة والاستعجال يترتب عليه البطلان، وقد ذهب بعض الفقهاء إلى القول بأنا لبطلان في هذه الحالة هو بطلان مطلق أي بطلان متعلق بالنظام العام [(١)]، ومن ثم فإنه يجوز للمحكمة أ تحكم به من تلقاء نفسها، حتى ولو لم يتمسك به الخصوم، ويجوز للخصوم التمسك به حتى ولو كان ذلك لأول مرة أمام محكمة النقض، ولكننا نرى مع البعض [(٢)] أن البطلان في هذه الحالة إنما هو بطلان نسبي لأنه متعلق بمصلحة الخصوم، ومن ثم فإنه لا يجوز للمحكمة أن تقضي بالبطلان ما لم يحدث تمسك به من قبل أحد الخصوم، ولا يجوز التمسك به لأول مرة أمام محكمة النقض.

وإذا كانت حالة الضرورة تبيح للمحقق جعل التحقيق سرياً عن الخصوم أو بعضهم إلا أن بعض إجراءات التحقيق لا يجوز أن يتم إلا في حضور الخصوم وهذه الإجراءات هي التفتيش والمعاينة، ولكن بعض

ارتكاب الجريمة المتلبس بها قبل زوال آثارها. أو حالة الضرورة كأن يسمع المحقق أقوال أحد الشهود في غيبة المتهم إذا كان هذا المتهم له تأثير عليه كأن يكون رئيساً له في العمل. نقض ٤/ ١/ ١٩٧٦، مجموعة أحكام النقض، س٢٧، رقم١، ص٩، ٢٤/ ١/ ١٩٧٩، س٣٠، رقم ١٤٦، ص٦٨٥، ٧/ ٣/ ١٩٧١، س٢٢، رقم٤٧، ص١٩٤. وعلى ذلك نصت المادة (٦٩ / ٢) إجراءات سعودي بقولها:" وللمُحقِّق أن يُجري التحقيق بغيبة المذكورين أو بعضِهم متى رأى ضرورة ذلك لإظهار الحقيقة، وبمُجرد انتِهاء الضرورة يُتيح لهُم الإطلاع على التحقيق".

(١) د/ محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، دار النهضة العربيةسنة١٩٨٨م، ص١٩٩.

(٢) د/ مأمون سلامة، الإجراءات الجنائية، ص٤٣٨.

الفقهاء[١] منع أن يتم التفتيش إلا في حضور الخصوم وأجاز أن تتم المعاينة في غيبة الخصوم وهذا ما أخذت به محكمة النقض [٢]، ويرى البعض [٣] أنه لا يجوز التفرقة بين التفتيش والمعاينة. وجواز منع الخصوم من الحضور في المعاينة، وعدم جواز منعهم في التفتيش، لأن مصلحة التحقيق تتطلب ضرورة أن يتم التفتيش أو المعاينة في حضور الخصوم وليس في غيبتهم وهذا ما أكدته المادة ٩٢ إجراءات "يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن..."، وذلك لأن التفتيش إجراء لا يجوز أن يعاد مرة ثانية بمعرفة المحكمة إذا طعن فيه أمامها، هذا علاوة على أن الدليل الذي أسفر عنه التفتيش يتحقق في نفس الوقت الذي تم فيه هذا التفتيش، ولهذا فإنه يجب أن يكون التفتيش في حضور الخصوم ويواجهوا به حتى لا يشككوا فيه بعد ذلك أمام المحكمة ويدفعوا ببطلانه لأول مرة أمامها، فإذا حدث ذلك، كان الدفع ببطلان التفتيش عديم الفائدة.

وأما بالنسبة للمعاينة فيجب أن تتم في حضور الخصوم وذلك لأن إجراءها في غيبتهم يعطيهم فرصة المنازعة في الدليل المستمد منها، ولا يتيسر للمحكمة إعادة المعاينة لأنها ستكون عديمة الفائدة حيث تكون معالم الجريمة قد زالت [٤].

---

(١) د/ رءوف عبيد، مبادئ الإجراءات الجنائية، ص٣٨٧.

(٢) نقض ٧/ ١٢/ ١٩٥٩، مجموعة أحكام النقص، س١٠، رقم ٢٠٠، ص٩٧٧.

(٣) د / سامح جاد: الإجراءات الجنائية، ص ٢٢٢.

(٤) د/ محمود مصطفى، ص١٩٨-١٩٩، د/ عمر السعيد، ص٢٨٦، د/ مأمون سلامة، ص٤٣٧.

الفرع الثالث
سرية التحقيق بالنسبة للجمهور

إذا كان القانون قد أوجب أن يكون التحقيق علنياً في مواجهة الخصوم إلا في حالة الضرورة والاستعجال حيث يجوز للمحقق عدم دعوة الخصوم أو بعضهم لحضور التحقيق إذا كان في ذلك إظهار للحقيقة (م٧٧ إجراءات) أو لم يكن أمام المحقق متسع من الوقت لدعوة الخصوم (م ٧٧/ ٢ إجراءات)، فإن الأمر على النقيض من ذلك حيث جعل القانون التحقيق سرياً بالنسبة لما عدا الخصوم، أي جعل التحقيق سرياً بالنسبة للجمهور وجعل النتائج التي يسفر عنها التحقيق من ضمن الأسرار التي يعاقب على إفشائها متى تم هذا الإفشاء بواسطة قضاة التحقيق أو أعضاء النيابة ومساعديهم من كتاب وخبراء وغيرهم ممن يتصلون بالتحقيق أو يحضرونه بسبب وظائفهم أو مهنهم وهذا ما أكدته المادة ٧٥ إجراءات حيث نصت على أنه "تعتبر إجراءات التحقيق ذاتها والنتائج التي تسفر عنها من الأسرار".

ويجب على قضاة التحقيق وأعضاء النيابة العامة ومساعديهم من كتاب وخبراء وغيرهم ممن يتصلون بالتحقيق أو يحضرونه بسبب وظيفتهم أو مهنتهم عدم إفشائها، ومن يخالف ذلك منهم يعاقب طبقاً للمادة ٣١٠ من قانون العقوبات" [(١)].

---

(١) وعلى ذلك فمن يفشي أسرار التحقيق الابتدائي من غير من عددتهم المادة (٧٥)إجراءات لا يخضع للعقاب المقرر بالمادة ٣١٠ عقوبات كالشاهد والمتهم متى أفشى أسرار التحقيق أو أفشى ما أسفر عنه من نتائج تكون قد وصلت إلى علمه.

وعلى ذلك أيضاً نص نظام الإجراءات الجزائية السعودي في المادة(٦٧) بقولها:" تُعد إجراءات التحقيق ذاتُها والنتائج التي تُسفِر عنها من الأسرار التي يجب على المُحقِّقين ومُساعديه – من كُتاب وخُبراء وغيرِهم، مِّمن يتصِلون بالتحقيق أو يحضُرونه بسبَّب وظيفتِهم أو مِهنتِهم – عدم إفشائِها، ومن يُخالِف مِنهُم تعينت مُساءلتُه.

ومتى أفشى أي ممن عددتهم المادة ٧٥ إجراءات، أسرار التحقيق فإنه لا يترتب على ذلك بطلان لإجراءات التحقيق التي تمت، ولكن فقط يعاقبون وفقاً للمادة ٣١٠ عقوبات بالحبس مدة لا تتجاوز ستة شهور أو الغرامة التي لا تتجاوز قيمتها خمسمائة جنيه مصري في النظام الجزائي المصري[1]. وتتقرر مساءلته وفقا للمادة (٦٧) من نظام الإجراءات الجزائية السعودي.

(١) د / سامح جاد: الإجراءات الجنائية، ص ٢٢٥ وما بعدها.

المبحث الثاني
السلطة المختصة بالتحقيق الابتدائي

تختص النيابة العامة، وفقاً لأحكام قانون الإجراءات الجنائية المصري (م١٩٩ إجراءات) بمباشرة التحقيق في مواد الجنح والجنايات[1]. واختصاصها بهذا المعنى أصيل وعام. ومع ذلك فقد قيد القانون سلطتها في أحوال معينة وأوجب عليها عرض الأمر على جهة القضاء لاستئذانه في مباشرة بعض الإجراءات. ويبدو ذلك بوجه خاص بالنسبة لتفتيش غير المتهمين وتفتيش منازلهم، وكذلك بالنسبة لضبط الخطابات وما في حكمها لدى مكاتب البريد والبرق، ومراقبة المحادثات وتسجيلها، فقد أوجب القانون عليها الرجوع في هذه الأحوال إلى القاضي الجزئي لاستئذانه في مباشرة الإجراء (م٢٠٦ إجراءات). ولكن بصدور القانون رقم ٩٥ لسنة ٢٠٠٣، قد أضيفت المادة ٢٠٦ مكرراً إجراءات جنائية حيث تنص على أنه يكون لأعضاء النيابة العامة من درجة رئيس نيابة على الأقل. بالإضافة إلى الاختصاصات المقررة للنيابة العامة – سلطات قاضي التحقيق في تحقيق الجنايات المنصوص عليها في الأبواب الأول والثاني والثاني مكرر والرابع من الكتاب الثاني من قانون العقوبات.

---

(١) تنص المادة ١٩٩على أنه:" فيما عدا الجرائم التي يختص قاضى التحقيق بتحقيقها وفقا لأحكام المادة ٦٤ تباشر النيابة العامة لتحقيق فى مواد الجنح والجنايات طبقا للأحكام المقررة من قاضى التحقيق مع مراعاة ما هو منصوص عليه في المواد التالية".

ويكون لهم فضلاً عن ذلك سلطة محكمة الجنح المستأنفة منعقدة في غرفة المشورة المبينة في المادة ١٤٣ من هذا القانون في تحقيق الجرائم المنصوص عليها في القسم الأول من الباب الثاني المشار إليه.

و يكون لهؤلاء الأعضاء من تلك الدرجة سلطات قاضي التحقيق فيما عدا مدد الحبس الاحتياطي المنصوص عليها في المادة ١٤٢ من هذا القانون، وذلك في تحقيق الجنايات المنصوص عليها في الباب الثالث من الكتاب الثاني من قانون العقوبات.

ويفهم من هذا التعديل أن المشرع قد جعل للنيابة العامة من درجة رئيس نيابة على الأقل سلطات قاضي التحقيق في تحقيق الجنايات، وسلطة محكمة الجنح المستأنفة منعقدة في غرفة المشورة المبينة في المادة ١٤٣ من هذا القانون.

ويكون لهؤلاء الأعضاء من تلك الدرجة سلطات قاضي التحقيق فيما عدا مدد الحبس الاحتياطي المنصوص عليها في الباب الثالث من الكتاب الثاني من قانون العقوبات.

وفي مجال الحبس الاحتياطي أوجب القانون على النيابة العامة إذا رأت مد الحبس لأكثر من أربعة أيام أن تعرض الأمر على القاضي الجزئي ليأمر بما يراه (م ٢٠٢ إجراءات جنائية) [١].

---

(١) د/ أحمد فتحي سرور، مركز القانوني للنيابة العامة، مجلة القضاة سنة ١٩٦٨، ص١٢٦، د/ عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ص٣٦١. وانظر نقض ١٩٠٧٣/١١/٢٥، مجموعة أحكام النقض، س٢٤، رقم٢١٩، ص١٠٥٣.

وفي النظام الجزائي السعودي تختص بالتحقيق الجنائي هيئة التحقيق والادعاء العام؛ فتنص المادة (١٤) من نظام الإجراءات الجزائية على أنه:" تتولى هيئة التحقيق والادِعاء العام التحقيق والادِعاء العام، طِبقاً لنِظامِها ولائحتِها". كما أكدت ذلك المادة (٣) من نظام هيئة التحقيق والادعاء العام بقولها:" تختص الهيئة وِفقاً للأنظِمة وما تُحدِّدُه اللائحة التنظيمية، بما يلي: أ - التحقيق في الجرائم. ب - التصرُف في التحقيق برفع الدعوى أو حِفظِها طِبقاً لِما تُحدِّدُه اللوائح. ت - الادعاء أمام الجهات القضائية وِفقاً للائحة التنظيمية....." وعلى ذلك فإن الهيئة هي التي تتولى تحريك الدعوى الجزائية والتحقيق فيها، ومباشرتها أمام المحاكم الجزائية على اختلاف درجاتها، ولا تحرك من غيرها إلا في الأحوال الاستثنائية التي نصت عليها الأنظمة النافذة[1].

وفي مجال الجرائم المعلوماتية نصت المادة (١٥) من نظام مكافحة جرائم المعلوماتية على ذلك بقولها :" تتولى هيئة التحقيق والادِعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام"

ولقد أجاز المشرع المصري إجراء التحقيق بصفة استثنائية بمعرفة قاضي للتحقيق، فنصت المادة ٦٤ من قانون الإجراءات الجنائية على أنه "إذا رأت النيابة العامة في مواد الجنايات والجنح أن تحقيق الدعوى بمعرفة قاضي التحقيق أكثر ملاءمة بالنظر إلى ظروفها الخاصة، جاز لها في أية حالة كانت عليها الدعوى أن تطلب إلى رئيس المحكمة الابتدائية ندب أحد قضاة المحكمة

(١) د/ زكى محمد شنّاق، الوجيز في نظام الإجراءات الجزائية السعودي، ص٣٩،٤٠.

لمباشرة هذا التحقيق ويجوز للمتهم أو المدعي بالحقوق المدنية إذا لم تكن الدعوى موجهة ضد موظف أو مستخدم عام أو أحد رجال الضبط لجريمة وقعت منه أثناء تأدية وظيفته أو بسببها أو يطلب من رئيس المحكمة الابتدائية إصدار قرار بهذا الندب، ويصدر رئيس المحكمة هذا القرار إذا تحققت الأسباب المبينة بالفقرة السابقة بعد سماع أقوال النيابة العامة، ويكون قراره غير قابل للطعن، وتستمر النيابة العامة في التحقيق حتى يباشره القاضي المندوب في حالة صدور قرار بذلك[١].

على أن ندب قاضي التحقيق لا يكون إلا في الجنايات والجنح إما بناء على ندب النيابة العامة وهنا يلتزم رئيس المحكمة بإجابة الطلب، وإما بناءً على طلب المتهم أو المدعي بالحقوق المدنية، وهنا يكون لرئيس المحكمة سلطة تقديرية في إجابة الطلب أو عدم إجابته [٢]. وذلك بعد سماع أقوال النيابة العامة سواء قبل بدئها التحقيق أو بعده حين تنكشف أن للواقعة ظروفاً خاصة ترى من الملائمة أن لا تقوم هي بالتحقيق ويتعين عليها أن تتنحى عن مباشرته، ويتعين صدور قرار بالندب في كل قضية على حدة، فلا يجوز تخصيص قاضي دائم ثابت للتحقيق في أية قضية [٣].

ومتى انتهى التحقيق يرسل قاضي التحقيق الأوراق إلى النيابة العامة، وعليها أن تقدم له طلباتها كتابة خلال ثلاثة أيام إذا كان المتهم محبوساً وعشرة

---

(١) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ص٥١١.

(٢) د/ محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، ص٢٤٣.

(٣) د/ عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ص٣٥١.

أيام إذا كان مفرجاً عنه، وعليه أن يرى باقي الخصوم ليبدوا ما قد يكون لديهم من أقوال، ثم يصدر قراره بإحالة المتهم إلى المحكمة المختصة[١].

وللنيابة العامة الطعن في كافة ما يصدره قاضي التحقيق من قرارات، بينما لا يجوز لباقي الخصوم الطعن في قراراته إلا المتعلقة بمسائل الاختصاص فقط (م١٦٣ إجراءات).

كما أجاز المشرع المصري في المادة ٦٥ إجراءات جنائية "لوزير العدل أن يطلب من محكمة الاستئناف ندب مستشار لتحقيق جريمة معينة أو جرائم من نوع معين ويكون الندب بقرار من الجمعية العامة. وفي هذه الحالة يكون المستشار المندوب هو المختص دون غيره بإجراء التحقيق من وقت مباشرته

(١) د/ مأمون سلامة، الإجراءات الجنائية، ص ٦٠١، وقد نصت المادة ١٥٦ إجراءات على أنه "إذا رأى قاضي التحقيق أن الواقعة جنحة يحيل المتهم إلى المحكمة الجزئية ما لم تكن الجريمة من الجنح التي تقع بواسطة الصحف أو غيرها من طرق النشر – عدا الجنح المضرة بأفراد الناس- فيحيلها إلى محكمة الجنايات" فإذا كانت الواقعة جناية، يصدر أمره بإحالة الدعوى إلى محكمة الجنايات. فقد نصت المادة ١٥٨ إجراءات جنائية على أنه "إذا رأى قاضي التحقيق أن الواقعة جناية وأن الأدلة على المتهم كافية يحيل الدعوى إلى محكمة الجنايات ويكلف النيابة العامة بإرسال الأوراق إليها فوراً"، كما نصت المادة ١٥٩ إجراءات جنائية على أن "يفصل قاضي التحقيق في الأمر الصادر بالإحالة إلى المحكمة الجزئية أو محكمة الجنايات في استمرار حبس المتهم احتياطياً أو الإفراج عنه أو في القبض عليه وحبسه احتياطياً إذا لم يكن قد قبض عليه أو كان قد أفرج عنه". من جهة أخرى، يجوز لقاضي التحقيق أن يصدر أمراً بعدم وجود وجه لإقامة الدعوى الثانية، وتملك النيابة العامة الطعن في هذا الأمر ولكنها لا تملك الطعن في أوامر الإحالة التي يصدرها.

العمل". فمن القضايا -كما جاء بالمذكرة الإيضاحية- ما قد يتطلب ضمانات غير عادية أو خبرة خاصة لتحقيقه، فيكون تحقيقها بواسطة مستشار أكثر ملائمة من تركها للنيابة أو ندب قاض لتحقيقها.

ويصدر القرار بندب مستشار للتحقيق؛ من الجمعية العامة لمحكمة الاستئناف المختصة [١]، - وليس من رئيس المحكمة- بناء على طلب وزير العدل، وهو جائز في مواد الجنايات والجنح، لكنه غير جائز في المخالفات لتفاهتها وتدخل الدعوى حوزة مستشار التحقيق وتخرج من ولاية النيابة العامة، ويصبح وحده مختصاً دون غيره بتحقيقها من وقت مباشرته للعمل الذي ندب له من الجمعية العامة للمحكمة، ومن الملحوظ أن ندب مستشار التحقيق يمكن ندبه على النحو السابق، لتحقيق جريمة بعينها، أو جرائم من نوع معين، على عكس قاضي التحقيق الذي يلزم أن يندب "لدعوى بذاتها" وليس لمجموعة دعاوى، إلا أنه يتفق معه في سلطاته على الدعوى، وفي تقيده بالحدود العينية دون الشخصية لها [٢].

---

(١) د/ عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ص٣٦٠.

(٢) د/ أحمد حسني أحمد طه، مبادئ قانون الإجراءات الجنائية في التشريع المصري، ص٣٩٢ – ٣٩٣.

المبحث الثالث
التأهيل الفني اللازم للمحقق في جرائم تقنية المعلومات

تمهيد وتقسيم:

بالإضافة إلى المهارات الفنية 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 والتي تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق. فإنه يجب أن يكتسب المحقق في جرائم تقنية المعلومات مهارات أخرى تتسم بالجدة والحداثة وتعتبر إفرازاً للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمراً مستجداً في من يتعامل مع هذه الجرائم المستحدثة، وسوف نتناول ذلك من خلال مطلبين : نتناول في المطلب الأول: إجادة التعامل مع أنظمة الحاسب وخدمات الانترنت وشبكات الاتصال المختلفة.وفي المطلب الثاني:الاطلاع على الجوانب المتعلقة بجرائم المعلومات.

المطلب الأول
إجادة التعامل مع أنظمة الحاسب وخدمات الانترنت وشبكات الاتصال المختلفة

إن المحقق في جرائم تقنية المعلومات ينبغي أن يكون على معرفة متميزة بالمكونات المادية للحاسب الآلي والتعامل المبدئي معها، ومعرفة بالشكل المميز للحواسيب وملحقاتها ومسمى كل منها. والهدف من استخدامه وما احتمالات توظيفه لارتكابه أي من الجرائم الإلكترونية؛ حيث أن عدم تعرفه عليها قد يؤدي إلى إهمالها أو حتى إتلافها بدون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها. ليس هذا فحسب بل لابد وأن يلم المحقق

بكيفية التعامل مع تلك المكونات من أجهزة وملحقات ووسائط تخزين بصفتها أدلة محتملة، ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم الإلكترونية، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال[1].

كما يجب أن يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسب الآلي وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها، 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 امن الحاسبات، ووسائل اختراقها، مع دراسة حالات تطبيقه لجرائم وقعت سلفا، وكيف تم مواجهتها.

وفي كثير من بلدان العالم تعقد الدورات التدريبية المتخصصة لرجال الشرطة وأعضاء النيابة العامة، سواء في مراكز تابعة لوزارة الداخلية أو في

---

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٤، د/ غنام محمد غنام، ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات ن بحث منشور بمجلة البحوث القانونية والاقتصادية، العدد الرابع والأربعون، أكتوبر ٢٠٠٨، ص ١١٣.

المراكز المتخصصة التابعة لوزارة العدل، كما هو الحال في أمريكا وانجلترا، وكندا[١].وهذا هو الحاصل في مصر والمملكة العربية السعودية[٢].

---

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٥، د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، بحث منشور على موقع: **http://www.eastlaws.com**. ص٢ وقد أشار إلى:

ISTS, Institute for security Technology Studies (2002). Law Enforcement Tools and Technologies for investigating cyber attacks: A National Needs Assessment

Thompson, David (1990). Computer Crime The Improvement Of Investigative Skills: Final Report: www.acpr.gov.au/pdf/acpr101

(٢) ففي مصر المركز القومي للدراسات القضائية: وهو مركز متخصص في تدريس العلوم القضائية للعاملين في مجال السلك القضائي من أعضاء النيابة العامة في مصر ورجال القضاء يتبع وزارة العدل المصرية ويرأسه مستشاراً مساعداً لوزير العدل. يرتكن المركز علي عدد كبير من كبار وأشهر رجال القضاء في مصر المشهود لهم بالخبرة الطويلة ويهدف إلي نقل هذه الخبرات للأجيال الأحدث عهداً بالعمل. يقع المركز في عاصمة جمهورية مصر العربية القاهرة وله فرع بمدينة الإسكندرية. وللمركز أنشطة وخدمات أخرى مثل الترجمة تدريب الهيئات القضائية علي دراسة وتعلم اللغة الإنجليزية-مستويات عامة وقانونية- والفرنسية والحاسب الآلي، ولا يقتصر المركز على تدريب أعضاء الهيئات القضائية المصرية وإنما يقوم أيضاً بدور كبير في تدريب الكوادر القضائية والقانونية في الدول العربية والإسلامية والصديقة.انظر موقع: **http://ar.wikipedia.org/wiki**

كما تم إنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق في عام ٢٠٠٢م، وذلك للأخذ بزمام المبادرة لمواجهة تلك الجرائم، وتقديم الدعم الفني لجميع جهات الوزارة في كافة القضايا والوقائع المرتبطة بمجال نظم وبرامج وأجهزة وشبكات المعلومات، وتوفير كافة المساعدات الفنية وإبداء الرأي والمشورة للجهات سواء من داخل الوزارة أو خارجها للمعاونة في عمليات ضبط الجرائم التي تتم باستخدام الحاسب الآلي.

كما يوجد معهد علوم نظم المعلومات، يتبع الإدارة العامة للمعلومات والتوثيق، يقوم بعمل فرقا تدريبية يتولى فيها تدريب الضباط وأمناء الشرطة والمدنيين العاملين أو المرشحين للعمل في مجال الحاسبات وشبكات المعلومات، ومنها الفرق الأساسية لمكافحة الجريمة المعلوماتية، التي تهدف إلى إعداد وتأهيل الضباط وتعريفهم بالجريمة المعلوماتية، وطرق ارتكابها، والإجراءات الفنية لمكافحتها. د/ مصطفى محمد موسى،التحقيق الجنائي في الجرائم الالكترونية،طبعة مطابع الشرطة، القاهرة سنة ٢٠٠٩م، ص٣١٣،٣١٢.

وفي المملكة العربية السعودية فإن نظام مكافحة جرائم المعلوماتية، ينص في المادة (١٤) منه على أنه :" تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة "

كما تقوم الجمعية العلمية السعودية للدراسات القضائية، التابعة لجامعة الإمام محمد بن سعود الإسلامية بتقديم الدراسات التي تجلي تميز القضاء الإسلامي وأصوله وقواعده وتطبيقاته، والعناية بالتراث القضائي الإسلامي تحقيقاً ودراسة ونشراً ورصداً، ودراسة ما له علاقة بالقضاء من النوازل والحوادث والقضايا المعاصرة، وعقد المحاضرات والندوات وحلقات النقاش لتنشيط التواصل العلمي بين المتخصصين وإثراء الدراسات العلمية والعملية، وتقديم المشورة العلمية في مجال

فمعرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية حتى يشارك في متابعة وفحص وتفتيش مسرح الجريمة. وأحياناً يجد المحقق نفسه أمام قرار فني صعب يجب أن يتخذ قرار بشأنه بالتشاور مع الخبير، وبدون توافر الحد الأدنى من المعرفة التقنية لهذا القائد فإن القرار على الأرجح سوف يكون للخبير وحده. وأكثر أنظمة التشغيل شيوعاً وشهرة والتي يجب أن تتوفر في أي برنامج تدريبي هي: أنظمة ويندوز وأنظمة يونكيس واليـنكس ونظام ماكنتوش.

كما ينبغي أن يكون المحقق لديه القدرة على معرفة الصيغ المختلفة للملفات وتطبيقات الحاسوب الرئيسية التي نتعامل معها؛ إذ تعد الملفات الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا المتعلقة بشبكة الإنترنت بما

التخصص، والتنسيق بين المتخصصين من القضاة والمحامين والباحثين في الشئون العلمية القضائية ومد الجسور بينهم وبين الجهات العلمية والإعلامية ونحوها، إلى جانب تبادل النتاج العلمي في مجال اهتمامات الجمعية بين الجهات والأفراد ذوي الاهتمام داخل المملكة وخارجها، وتطوير الأداء العلمي والعملي لأعضاء الجمعية، وتقديم الدراسات لتطوير مرفق القضاء وعلاج ما يعرض من مشكلات(٢).انظر موقع: **http://www.aleqt.com**

كما تم إنشاء إدارة خاصة – كما في فرنسا وكندا– من رجال المباحث الجنائية تتخصص في جرائم الكمبيوتر وكذلك أجهزة مركزية للمتابعة. د/ شيماء عبدا لغني محمد عطا الله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧/ ٣/ ١٤٢٨هـ الموافق ٢٦/ ٣/ ٢٠٠٧م بحث منشور على موقع: **http://www.f-law.net**

تحويه من معلومات[١]، وبالتالي 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 أمر في غاية الأهمية.

وبالإضافة إلى ذلك فإنه ينبغي أن يكون المحقق لديه معرفة تامة بكيفية التعامل مع خدمات الإنترنت الرئيسية؛ حيث إن شبكة الإنترنت تمثل أداة جمع وتحريات مناسبة للمحقق، حيث أنها خلقت مجتمعاً افتراضياً شبيهاً إلى حد ما بالمجتمعات الحقيقية، ويدور في مجتمع الإنترنت هذا الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم [٢]. ومن الممكن أيضاً أن يستخدم الإنترنت كأداة تعليمية للإطلاع على مستجدات جرائم الحاسب

---

(١) غالباً ما يتم حفظ البيانات الرقمية داخل جهاز الحاسب الآلي على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى ملفات، حيث يتميز كل ملف ببيئة وصيغة خاصة تسمى **Format** تميزه عن غيره وغالباً ما ترتبط بكل صيغة بنوع محدد من المحتوى. كأن يحتوي الملف على بيانات تمثل صورة أو صوت أو فيديو أو مستند خطي أو غير ذلك. محمد بن نصير محمد السرجاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت "دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤ م منشور على موقع: **http://www.creativity.ps/library/details.php?id**. ص ٩٥ – ٩٦.

(٢) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص ٣ وقد أشار إلى:

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

الآلي والإنترنت وطرق التصدي لها. وكوسيلة اتصال وتبادل المعلومات فيما بين رجال نفاذ القانون

كما ينبغي أن تتوافر لدى المحقق معرفة بأساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاتها؛ فالكثير من الجرائم المعلوماتية يتم ارتكابها من خلال شبكة الإنترنت، وبالتالي 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[1]. وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصور كيفية ارتكاب الفعل الإجرامي في الفضاء الإلكتروني من اختراق للشبكات والحواسيب واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها. كما أنها تعطي المحقق تصوراً جيداً عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات الفنية التي تحول دون ذلك.

وكذلك فإن معرفة أهم تقنيات أمن الحاسوب والإنترنت وأدواتها وطريقة عملها أمر ضروري للمحقق، واكتساب هذه المهارة وإن كان يبدوا في الظاهر أمراً معقداً بعض الشيء، إلا أن الأمر في حقيقته ليس كذلك، حيث أن المطلوب أن يساعد معرفة هذه التقنيات المحقق استيعابها وربطها بمجريات التحقيق بشكل عام وليس أن يجعله خبيراً فيها[2].

---

(١) محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص ٩٥ – ٩٦.

(٢) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٣.

المطلب الثاني
الإطلاع على الجوانب المتعلقة بجرائم الإنترنت

لا يكفي المحقق الجنائي – خاصة في جرائم تقنية المعلومات - أن يكون ملماً بالقوانين الجنائية التي يتشكل منها التحقيق الجنائي، بل عليه أن يستزيد من المعلومات العامة وسائر العلوم والقوانين الأخرى التي تتصل بمهنته الأساسية، سواء اتصال مباشر أو غير مباشر، سيما القوانين المتعلقة بتكنولوجيا المعلومات والاتصالات وشبكة الإنترنت، وكلما زادت معلوماته العامة وثقافته كلما أدى ذلك إلى زيادة خبرته ودرايته بشئون الحياة العامة، وأدى ذلك لنجاحه وتحقيق هدفه الذي يصبو إليه[1].

ومن تلك القوانين، القانون الإلكتروني **Cyber Law**، وقانون المعاملات والعقود الإلكترونية، وقانون الإثبات باستخدام التوقيع الإلكتروني، وقانون مكافحة جرائم النظم المعلوماتية، ومن العلوم علم النفس بوجه عام وعلم النفس الجنائي بوجه خاص، وعلم الاجتماع، وعلم الإجرام، وعلم البصمات، وعلم الطب الشرعي، وإلمام المُحقق بهذه العلوم لا يقتضي إلمام

---

(١) دكتور/ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٠، ص ١١٨. وقد نصت المادة (١٥٩) من تعليمات النيابة على أنه:" يجب أن يكون المُحقق على علم تام بأحكام القانون الجنائي وبعلم الإجرام وبعلم العقاب، وأن يكون على دراية بمبادئ الطب الشرعي وعلم النفس الجنائي وأن يكون ملماً بمختلف الظروف المحيطة بالمجتمع وبالمعلومات العامة التي تتصل بالوقائع التي يتولى تحقيقها، كما يجب أن يكون على جانب كبير من الثقافة العامة، متنوع الإطلاع والمعارف التي تتصل بالحياة البشرية على مختلف صورها وطبائعها".

المتخصص فيها والعالم ببواطن ودقائق الأمور في هذه العلوم، بل يكفي أن يكون ملماً بأساسيات تلك العلوم وما يفيده في أداء رسالته[١].

ومن أهم الجوانب التي ينبغي على المحقق الاطلاع عليها: الواقع الحالي والاتجاهات المستقبلية للجرائم المتعلقة بشبكة الإنترنت، ودراسة الفئات المختلفة التي ينقسم إليها مرتكبو هذه الجرائم والخصائص المشتركة التي تميز كل فئة، ومعرفة وفهم التشريعات المختلفة المتعلقة بهذه الجرائم والإلمام باتجاهات القوانين والتشريعات في البلدان المختلفة، ودراسة وتحليل بعض القضايا المشهورة للاستفادة من تجارب رجال العدالة في مواجهة هذه الجرائم، والوقوف على الأبعاد الدولية لهذه الجرائم وآليات التعاون المشترك بين الدول والتعرف على الاتفاقيات والمعاهدات الموجودة بهذا الخصوص، ومعرفة مصادر المعلومات المتوفرة على مواقع الإنترنت عن هذه الجرائم من خلال المواقع المتخصصة ذات المحتوى الجيد والمصداقية والاستفادة منها.

كذلك معرفة الجرائم المتعلقة بالإنترنت والخصائص التي تتميز بها؛ فالوعي الجيد بهذه الجرائم وبأنواعها المختلفة يعتبر بمثابة حجر الأساس في مواجهتها وبدونه لن تنجح السبل والوسائل الأخرى فلا يعقل أن تتم مواجهة جريمة ما إذا كان رجل العدالة المناط به هذا الأمر يجهل ماهيتها، ومعرفة الأدوات والأساليب المستخدمة في ارتكاب جرائم تقنية المعلومات؛ فمعرفة رجال العدالة بهذه الأساليب وكيفية استخدام هذه الأدوات أمر في

---

(١) دكتور/ خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، ٢٠٠٨.ص١٢٠.

غاية الأهمية خاصة لمن يتولون مناقشة الشهود واستجواب المتهمين فبدونه لن يستطيعوا طرح الأسئلة التي تتصل مباشرة بالفعل الإجرامي وأسلوب ارتكابه. كما أنها تساعد المحقق على التواصل مع خبير الحاسوب الجنائي عند شرح الأخير ما توصل إليه من أدلة أو قرائن عن الأساليب المستخدمة في ارتكاب الجريمة والأدوات التي تساعده على القيام بذلك[١].

وهناك علوم أخرى يجب على المُحقق الإلمام بها، ومنها علوم الكمبيوتر، وعلوم الأدلة الجنائية، وعلوم التحليل السلوكي للأدلة الرقمية حيث أن علوم الكمبيوتر تقدم المعلومات التكنولوجية الدقيقة وهي مطلوبة لفهم المظهر أو الهيئة أو الكينونة الفريدة للدليل الرقمي، بينما علوم الأدلة الجنائية من شأنها أن تقدم منظوراً علمياً لتحليل أي شكل من أشكال الأدلة الرقمية وتساهم علوم التحليل السلوكي للأدلة الرقمية في الربط المحدد بين المعارف التكنولوجية وبين الطرق العلمية لاستخلاص الدليل الرقمي، لفهم أفضل للسلوك الإجرامي التقني.

وعلى ذلك فإن هذه العلوم مجتمعة تساهم فيما يلي[٢]:

- الكشف عن الدليل الرقمي.
- إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ وتطبيق القانون.

---

(١) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٣، ٤.

(٢) د/ خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، ص١٢١.

- تحديد الخصائص الفريدة للدليل الرقمي.

- إصلاح الدليل وإعادة تجميعه من المكونات المادية للكمبيوتر **HardDrive**.

- عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

جمع الآثار المعلوماتية الرقمية **Cyber Trail Digital** التي قد تكون تبدلت خلال الشبكة المعلوماتية.

تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.

تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية مثل المستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، الأصوات، وغيرها.

وينبغي عند بدء التحقيق في الجرائم المعلوماتية إتباع الخطوات الآتية [(١)]:

١- قبل البدء في أخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين، يقوم المحقق وخبير الحاسب الآلي بتبادل المعلومات فيما بينهما، بحيث يوضح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم.

٢- يتم حصر النقاط المطلوب إيضاحها من قبل الخبير والمحقق، ومن ثم يتولى المحقق ترتيب تلك النقاط.

---

(١) دكتور/ محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، ص ٣٦٨ وما بعدها، د/ سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، ٢٠١٣م، ص ٣٤٧ -٣٥٠.

٣- يقوم المحقق بالحصول على كافة المصطلحات التي يمكن استخدامها مع بيان لمعاني تلك المصطلحات للاستفادة منها عند الضرورة.

٤- يضع المحقق خطة التحقيق على ضوء المعطيات الأخرى التي يراها.

٥- يبدأ اخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير، والذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب، وذلك وفق كيفية يتم الاتفاق عليها.

٦- مراعاة القوانين الوطنية فيما يتصل بسلطة التحقيق، والمدى المسموح به للخبير في مشاركة المحقق وحضور الاستجواب، ومن الأنسب – في حالة الدول التي لا تسمح قوانينها بمثل هذه المشاركة- استصدار قرارات بتشكيل لجان تحقيق تضم في عضويتها الخبرات الفنية المطلوبة في كل حالة.

٧- مراعاة التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الإلكتروني وملحقاته الخاصة بالمتهم أو الشاهد الذي يتم التحقيق معه، إذ أن المجرم المتخصص في جرائم الحاسب الآلي يحتفظ بمعلوماته وخططه في الحاسب الآلي أو على أقراص.

ويمكن للمحقق أو الخبير أن يتوصلا إلى تلك البيانات وأساليب فتحها من خلال التحقيق مع الأشخاص ذوي العلاقة بجرائم الحاسب الآلي أو الإنترنت، علماً بأن أقل خطأ في مثل هذه الحالات يقضي على كافة البيانات المخزنة في الحاسب الآلي.

وهناك قواعد عامة ينبغي مراعاتها لضمان نجاح التحقيق مع الأشخاص ذوي العلاقة بالحاسب الآلي والإنترنت وهي:

أ - تفادي ضياع الوقت في التحقيق حول جرائم الحاسب الآلي التي لا يمكن اكتشافها أو من المؤكد أن الأدلة اللازمة للاكتشاف وإثبات التهمة قد قضى عليها. إذ أن جريمة الحاسب الآلي جريمة تتصل بالتقنيات العالية ذات المعالم العلمية الواضحة والمؤكدة، ولا يتم إثباتها إلا بأدلة علمية خاصة.

ب - مراعاة التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المتضررة من الجريمة، فقد يكون خبراء المؤسسة المتضررة شهوداً أو مساهمين في الجريمة عن قصد أو جهل أو إهمال.

ج - التركيز في البحث عن البرامج اللينة اللازمة لكشف البيانات المخزنة ووضع التدابير للمحافظة عليها وحسن استخدامها.

د - مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني، وغير ذلك من الحقوق الخاصة، حتى لا تضار البينة التي حصل عليها المحقق.

هـ - العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها اللينة.

و - مراعاة حفظ الأدلة الجنائية بالطرق المناسبة لكل حالة، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبط عليها، إذ أن أي تأثير أو تعديل للأدلة ينهي القضية لصالح المتهم الذي يفسر الشك لصالحه كقاعدة عامة.

المبحث الرابع
مهام أجهزة التحقيق
في جرائم تقنية المعلومات

تمهيد وتقسيم:

ينبغي أن يكون لدى المُحقق موهبة فن التحقيق: بمعنى الإبداع والتمكن والقدرة على الاستنتاج والتحليل وفن التحقيق في الجرائم المعلوماتية ليس فقط قدرة المُحقق على استجلاء مدى توافر أركان الجريمة المعروضة وعناصرها القانونية من خلال الأفعال المسندة إلى المتهم وكذلك قدرته على تحقيق مدى صحة ما يبديه المجرم المعلوماتي من دفاع ودفوع قانونية وصولاً إلى مدى الحق فيها، وإنما هو قدرته أيضاً على مناقشة الشهود لاستجلاء أقوالهم مما يكون قد شابها من غموض وفيما بدتا من تناقض أو تعارض وصولاً إلى حقيقة الواقع.

وبالنسبة للتحقيق في الجرائم المعلوماتية – والتحقيقات الجنائية بصفة عامة – لا ينبغي أن يكون المُحقق مجرد آله ميكانيكية تسجل فقط الأسئلة والأجوبة، بل عليه أن يوجه إلى المتهم والشهود الأسئلة التي يقتضيها التحقيق ويحتمها مجري الأسئلة والأجوبة السابقة، واضعاً نصب عينيه تحقيق الغرض من التحقيق الجنائي ألا وهو جمع أدلة الجريمة وتمحيصها والتثبت من صحة إسناد الفعل الجنائي إلى المتهم، واستيضاح الباعث على ارتكاب الجريمة[1].

---

(١) دكتور/ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٠، ص ٩٨، وما بعدها.

والمهام أو الأعمال التي تقوم بها أجهزة التحقيق في جرائم تقنية المعلومات لكي تصل إلى الحقيقة تتمثل في الآتي:

أولاً : تلقي البلاغات والشكاوى. ثانياً : تحديد خطة العمل وتكوين فريق التحقيق.

ثالثاً : سرعة جمع الأدلة. وسوف أتناول هذه الأعمال في المطالب الثلاثة التالية:

المطلب الأول
تلقي البلاغات والشكاوى

البلاغ بصورة عامة إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هناك اتفاقاً جنائياً على ارتكابها. والمبلغ في الجرائم المتعلقة بشبكة الإنترنت لابد وأن يكون لديه معرفة مقبولة بالجوانب الفنية للحاسب الآلي وشبكة الإنترنت حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد يمكن للمحقق الوقوف على طبيعة الجريمة وبشكل مقبول يمكنه من مباشرة التحقيق فيها. وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسب الآلي والشبكات حتى يستطيع مناقشة المُبلغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ[1].

والمعلومات التي يجب على المحقق استيفاؤها من المُبلغ عند تلقي البلاغ تختلف باختلاف فئات جرائم الحاسب الآلي والإنترنت والطبيعة الفنية التي تتميز بها كل فئة عن غيرها. وعلى الرغم من أن لكل فئة من هذه الجرائم

(١) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص٦٨.

المستحدثة معلوماتها الخاصة التي ينبغي الحرص قدر الإمكان على استيفائها عند تلقي البلاغ، إلا أن هناك معلومات تكاد تكون مشتركة بين معظم هذه الفئات، ويمكن الحصول عليها عن طريق طرح أسئلة تتناول جوانب محدده منها ما يلي[١]:

- تاريخ ووقت تلقي البلاغ.
- المعلومات الخاصة بالمبلغ.
- المعلومات الخاصة بمتلقي البلاغ.
- طبيعة ونوع جريمة الحاسب الآلي محل البلاغ.
- الأسئلة المشهورة والمتعلقة بالجريمة ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟.
- المعلومات ذات العلاقة بالأنظمة الحاسوبية، مثل نوعية البرمجيات والمسئولين عن الأنظمة وطريقة الاتصال بهم وغيرها.

ومع أن عملية تلقي البلاغ لا تعدو أن تكون محادثة قصيرة وسريعة تهدف إلى تمكين المحقق من وضع تصور مبدئي عن ظروف وملابسات الحادث قبل الانتقال إلى مسرح الجريمة إلا أن دقة وتكامل المعلومات محل البلاغ على درجة كبيرة من الأهمية، حيث أنه من الممكن أن تسهم في مساعدة المحقق على تحديد ما إذا كان السلوك محل البلاغ يعد سلوكاً إجرامياً

---

(١) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٥ وقد أشار إلى:

Stern Eckert, Alan (2004). Critical incident Management. Boca Raton, Florida: CRC Press.

يندرج ضمن جرائم الحاسب الآلي والإنترنت، ووضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الحادث، وتحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع وتحريز الأدلة من موقع الحادث، والعمل على سرعة استدعاء الخبراء القادرين على إنجاز ذلك.

وقبل أن يُنهي المحقق عملية تلقي البلاغ يجب أن يؤكد على المُبلغ بضرورة تجهيز قائمة بأسماء العاملين في المؤسسة ممن لهم علاقة بالأجهزة المتضررة، أو علاقة بأي مشروع للأجهزة المتضررة، وتجهيز النسخ الاحتياطية من بيانات الأجهزة المتضررة، لاستخدامها من قبل فريق التحقيق فور وصوله الموقع، والتأكيد على عدم إبلاغ أحد بالحادث إلا من كانت الضرورة القصوى تحتم إبلاغه[(١)].

المطلب الثاني
تحديد خطة العمل وتكوين فريق العمل

تمهيد وتقسيم:

بعد الانتهاء من جمع المعلومات اللازمة عن الحادث، يبدأ المحقق وعلى ضوء تلك المعلومات التي توافرت لديه بتحديد خطة العمل المناسبة[(٢)] وفريق

---

(١) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص٦٩، د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٥، وقد أشارا إلى:

Middleton, Bruce (2002) Cyber Crime Investigator's Field Guid. .Boca Raton, Florida: Auerbach Publications

(٢) ويرى البعض أنه ينبغي أن يسبق خطة عمل المحقق هذه : ١ - تخطيط استراتيجي: وهو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية، من

العمل اللازم للتحقيق في الحادث، وهذه الخطة يجب أن تكون قد اكتملت في ذهن المحقق بمجرد انتهائه من معاينة موقع الحادث واتضحت لديه الصورة الأولية عن الحادث. وسوف أتناول تحديد خطة العمل وتكوين فريق العمل في الفرعين التاليين:

خلال تحديد مصادر الخطر المحتملة التي قد تمثل تهديداً لها وتحديدها، ويهتم بوضع تصورات على درجة من المرونة تكون كفيلة بالتصدي لهذا النوع من الجرائم قبل وقوعها وضبطها والحد من آثارها في حال وقوعها، ويتم هذا التخطيط على مستوى واضعي السياسات الأمنية، حيث يهدف بشكل عام إلى منع هذا النوع من الجرائم من الوقوع داخل إقليم الدولة، والحد من قابلية الحواسيب والشبكات الوطنية من التعرض للهجوم، ومن ثم السيطرة على الحوادث إن وقعت وضبطها والحد من آثارها. ومن أهم ما يميز هذا النوع من التخطيط أنه يضع الخطوط الاسترشادية التي تسترشد بها الجهات المختلفة ذات العلاقة في وضع خطط التعامل مع هذا النوع من الجرائم، كما يحدد الآليات اللازمة لتنفيذ الخطة.

٢ - تخطيط تكتيكي: ينبثق من الخطة الاستراتيجية ويتم على مستوى الجهات الرسمية والغير رسمية التي لها علاقة بتقنية المعلومات ويدعم غايات وأهداف الخطة الإستراتيجية للتعامل مع جرائم الحاسوب والإنترنت. ويمتاز بأن له طابع تفصيلي أكثر من التخطيط الاستراتيجي، والخطط التكتيكية الخاصة بالتعامل مع جرائم الإنترنت يجب أن تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل والوضوح للتحقيق في هذه الجرائم. محمد بن نصير محمد السرحاني، ص ٧٠.

الفرع الأول
تحديد خطة العمل

يقصد بخطة العمل: التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادث بعينه، وذلك في الإطار العام للإجراءات الواردة في الخطة التكتيكية وبما يتناسب مع خصوصية ظروف وملابسات الحادث.

ومن أهم الأمور التي يجب على المحقق أخذها في الاعتبار كمرتكزات تساعده في تحديد خطة العمل المناسبة للتحقيق في أي جريمة من جرائم تقنية المعلومات[1]:

١ - حجم ونوع الحادث التي يكون المحقق بصدد التحقيق فيه يرتبط به تحديد حجم ونوع فريق التحقيق، فجرائم الإنترنت منها الصغير ومنها الكبير ولكل جريمة مهما كان حجمها، طبيعتها الفنية الخاصة التي تفرض على أعضاء فريق التحقيق امتلاك مهارات فنية خاصة تعتبر ضرورية

---

(١) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٦، وقد أشار إلى:

Icove, D, Segar. K& Vons torch, W (1995). Computer Crime: A Crime fighter's handbook Sebastopol. California: O'Reilly & Associates ,

Schultz, E & Shumway, R (2002) incident Response: A Strategic Guide to Handling System and Network Secueity Breaches, Indianapolis, Indian: New Riders Publishing,

Mandia &, K. & Prosise, C. (2001). Incident response: Investigating Computer. Crime. Berkeley, California: McGraw-Hill.

للتعامل مع هذا النوع من الجرائم، وهو أمر يجب مراعاته عند اختيار أعضاء الفريق.

٢ - طبيعة مسرح الجريمة تفرض الأسلوب الأمثل للتفتيش بحثاً عن الأدلة التي تكون موجودة فيه والذي يعتبر من أهم خطوات عملية التحقيق وعدم نجاح المحقق في تحديد هذا الأسلوب قد يؤدي إما إلى عدم الحصول على أية نتائج أو الحصول على كم كبير من النتائج التي لا فائدة منها؛ فقائد فريق التحقيق مسئول عن تحديد حجم المهمة ونوع الأدلة التي يتم البحث عنها بحسب نوع الجريمة، وكذلك تحديد أنسب الطرق لتنفيذ عملية التفتيش وما يتبع ذلك من توزيع للأدوار والواجبات على فريق التحقيق.

٣ - بعض الظروف المحيطة بالحادث تمثل عوامل مهمة يجب مراعاتها عند وضع خطة العمل، لما يترتب عليها من قرارات على درجة كبيرة من الأهمية تتعلق بالتحقيق، ومن هذه العوامل:

- مدى أهمية الأجهزة الحاسوبية والشبكات المتضررة لعمل المنظمة أو المؤسسة.
- مدى حساسية البيانات التي قد تكون محل الجريمة الحاسوبية.
- المتهمون المحتملون.
- إطلاع الرأي العام على الجريمة أم لا.
- مستوى الاختراق الأمني الذي تسبب فيه الجاني.
- مستوى المهارة الفنية التي يتمتع بها الجاني.

٤ - تعيين الأشخاص الذين سيتم استجوابهم، وتحديد النقاط التي يجب استيضاحهم بشأنها، وكذلك تقدير مدى الحاجة إلى الاستعانة

ببعض الأشخاص من ذوي الاختصاصات الفنية التي يتطلبها التحقيق ولا تتوافر ضمن أفراد التحقيق.

الفرع الثاني
تكوين فريق التحقيق

هناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذوو معرفة واسعة، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في الاثنين معاً[(١)]. سيما وأن عالم الحاسوب والشبكات عالم متعدد ومتشعب وعلى درجة كبيرة من التعقيد وسرعة التطور. ولذلك كان من الضروري أن يستعين المحقق بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملابساتها. كما وأن التحقيق في هذه الجرائم قد يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير الذين يعتبرون من الخبراء الأساسيين في معظم أنواع الجرائم. وعلى هذا الأساس فإن فريق التحقيق في هذا النوع من الجرائم ينبغي أن يتكون من[(٢)]:

---

(١)محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص٧٣، وقد أشار إلى:

Groover, Richard (1996). Overcoming Obstacles: Preparing for Computer – related Crime. (online): www.fbi.gov/publications/leb/1996/aug962.txt (06/06/2003.)

(٢) محمد بن نصير محمد السرجاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص٧٥، د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص ٨، وقد أشارا إلى:

١ - الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم، إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة لجرائم الحاسب الآلي، وقلما يخلوا مسرح أي جريمة مهما كان نوعها من وجودهم، مثل أفراد حماية وتأمين المسرح وأفراد القبض وأفراد التحريات وغيرهم، وتحديد الأعضاء نوعاً وكماً متروك لتقدير المحقق على ضوء المعلومات المتوفرة لديه عن الجريمة، وحسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها.

٢ - الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي والإنترنت ولا يمكن التحقيق في أي جريمة تنتمي إلى هذه النوعية من الجرائم إلا بهم، ووجودهم ضروري في مسرح الجريمة ويمكن تحديد أعضاء هذه الفئة على النحو التالي:

- قائد الفريق: يشترط فيه أن يكون له خبرة طويلة في مجال التحقيق الجنائي، ولديه معرفة بالطبيعة الخاصة بجرائم الحاسب الآلي والإنترنت يتولى السيطرة الكاملة على مسرح الجريمة، وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم، والتنسيق مع الجهات ذات العلاقة، واتخاذ كافة القرارات المتصلة بالتحقيق.

- محقق جنائي: شخص أو أكثر بحسب ظروف الجريمة، لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرائم

Icove, D, Segar. K& Vons torch, W et al, 1999 & Wright, 2000d, Weight, Timothy (2000) (d). The Field Guide for Investigating computer Crime: Search and (Seizure Planning (on line) www.secuotyfocus.com/ingocus/1247(05-09-2003).

الحاسوب والإنترنت وكيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة.

- خبير حاسب آلي وشبكات: شخص أو أكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة ويكون مسئولاً عن رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض على المحكمة.

- خبير حسابات: متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية والآليات المختلفة التي يتم بواسطتها تبادل النقد الإلكتروني، ويعمل مع خبير الحاسب الآلي والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة.

- خبير تصوير: يتولى تصوير مسرح الجريمة كالمتبع في جميع الجرائم، بالتصوير الفوتوغرافي والفيديو.

- خبير رسم تخطيطي: يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدماً مقياساً مناسباً للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه

- خبير بصمات: لرفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسيب والشبكات

المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح والفأرة، وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسوب.

المطلب الثالث
سرعة جمع الأدلة

تتميز الإجراءات الجنائية بطابع خاص هو السرعة فيها، وذلك لأن معرفة أمر الجريمة وتوقيع العقوبات على مرتكبها يؤدي أثره من ناحية فلسفة العقاب في ردع المتهم عن معاودة ارتكاب الجريمة وردع غيره عن أن يفكر في سلوك سبيل الإجرام، وتمشياً من هذه الحكمة وجب أن يكون المحقق سريع التصرف.

وقد نصت تعليمات النيابة على ذلك في المادة (١٥٦) بقولها:" يجب على المحقق عدم التباطؤ في جمع الأدلة في الحالات التي تقتضي ذلك والابتعاد عن التردد في مباشرة الإجراءات الذي يراه سليماً حتى لا تضيع الفائدة من اتخاذه في وقته المناسب" كما نصت في المادة (١٥٥) على أنه :" يجب أن يراعي عضو النيابة أن تسير إجراءات التحقيق بالسرعة الواجبة لإنجازه دفعة واحدة وفي جلسات قريبة متلاحقة وذلك بغير إهدار لحقوق الخصوم أو إخلال بمقتضيات الدفاع"

وعلى هذا المعنى تنص المادة (٧٩ / ٤) من اللائحة التنفيذية لنظام الإجراءات الجزائية السعودي، بقولها:" يبدأ المحقق فور وصوله إلى مكان الحادث بإجراء المعاينة اللازمة، وإلقاء نظرة فاحصه وشامله على مسرح الجريمة، ويثبت حالة الأشخاص والأشياء والآثار المادية المتخلفة عن الجريمة،

والاستماع بصورة سريعة وشفهية للمعلومات الأولية المتوفرة عن كيفية حدوثها، ووقت ارتكابها، وهوية مرتكبيها والشهود ".

وسرعة التصرف في إجراءات التحقيق تعني السرعة من عدة جوانب منها، السرعة في الانتهاء من إجراءات السير في الدعوى، والسرعة في التصرف، والسرعة في سؤال الشهود، السرعة في إخطار الخبير المتخصص في مجال الجرائم المعلوماتية، ونتناولها على النحو التالي[1]:

١ - السرعة في الانتهاء من إجراءات السير في الدعوى.

سرعة تصرف المحقق تعني أن ينتهي من إجراءات السير في الدعوى التي أمامه في أقصر وقت ممكن، وذلك إما بإصدار أمر بألا وجه لإقامتها إن رأى عدم السير فيها، أو تقديمها للمحاكمة إن رأى أن الواقعة تكون جريمة وأن الأدلة على المتهم كافية ضده، وفي هذه الحالة يجب على عضو النيابة المُحقق أن يقوم بإعداد القضية إعداداً سليماً بحيث لا تطرح على هيئة المحكمة إلا الاتهامات المرتكزة على أساس قوي ليس من الواقع فحسب بل ومن القانون.

على أن سرعة تصرف المُحقق في التحقيق الجنائي لا تعني الانتهاء منه بطريق تؤثر على معرفة حقيقة الواقعة محل التحقيق، ولذلك يجب على المحقق – مع التزام عنصر السرعة- أن يلتزم العناصر التي يجب بيانها في الجريمة المعلوماتية وهي:

---

(١) دكتور/ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٠، ص ٩٨، وما بعدها.

(أ) السير في التحقيق من كافة جوانبه والبحث عن الحقيقة ومرتكب الواقعة وسؤال الشهود وإجراء المعاينة والإذن بالتفتيش وضبط المستندات وندب الخبراء.

(ب) استظهار أركان الجريمة وبيان ركنها المادي والمعنوي مع بيان الظروف المشددة أو المخففة والتي قد يؤدي توافرها إلى تعديل وصف الجريمة.

(ج) البحث عن جميع الأدلة التي قد تتوافر في التحقيق، إذ يجب على المُحقق أن يقوم بكل الوسائل القانونية التي تمكنه من الحصول على الأدلة سواء التقليدية أو الإلكترونية التي تمكنه من الوصول إلى الحقيقة.

(د) يجب على المُحقق الاعتناء بالتصرف في المضبوطات والأحراز التي تضبط في الجريمة، حيث يجب أن يتصرف فيها على النحو المبين بالقانون وفي ضوء التعليمات العامة للنيابات.

٢ - **سرعة التصرف في إجراء التحقيق**:

والسرعة في التصرف بالنسبة إلى كل إجراء من إجراءات التحقق على حدة، ذلك أن هناك من الإجراءات ما إذا لم تنفذ فوراً تضيع الفائدة من مباشرتها، ولهذا ينبغي أن لا يتردد المحقق في مباشرة الإجراء الذي يراه سليماً فيكون سريعاً حازماً في قراره، فإن عرض عليه وجب البت في الحال بعد استجوابه ما إذا كان يصدر أمراً بإطلاقه سراحه أو بحبسه احتياطياً، وإذا طلب إليه إصدار الإذن بتفتيش متهم أو منزله كان البت في ذلك فور تقديم الطلب.

٣ - **سرعة سؤال الشهود**:

سرعة التصرف في التحقيق تعني أيضاً سرعة سؤال الشهود، إذ يجب على المُحقق أن يسرع بمناقشة الشهود والتحفظ عليهم وذلك لأن التأخر في سؤال الشاهد من شأنه أن يؤدي إلى نسيانه بعض الوقائع الهامة أو يخلط فكرة بوقائع بأخرى لا تمت لها بصلة، فضلاً عن ذلك قد يتعرض الشاهد لتأثير خارجي من المتهمين أو أهليتهم[1].

٤ - سرعة إخطار خبير الجرائم المعلوماتية:

تقتضي سرعة التصرف في التحقيق سرعة إخطار الخبراء المختصين، إذ يجب على المحقق فور انتقاله لمكان الواقعة إخطار الخبراء للانتقال ورفع الآثار المتخلفة عن الحادث، على أن يحدد المحقق فور انتقاله لمكان البلاغ نوعية الخبراء الذين يخطروا بالانتقال ورفع الآثار وفقاً لنوعية الحوادث، ونقصد في هذا المجال الخبير المتخصص في مجال الجرائم المعلوماتية والإلكترونية.

على أنه من الأصول الأساسية في ذلك المجال المصور الجنائي هو الخبير الأول الذي ينبغي أن يبدأ في العمل قبل غيره من الخبراء، والتأخير في انتقال الخبراء من شأنه ضياع المعالم وطمس الأدلة والآثار أو صعوبة رفعها والتعامل معها، لذا نجد المادة (١٨٨) من تعليمات النيابة تنص على أنه "على عضو النيابة أن يصطحب معه إلى مكان الحادث وكلما كان ذلك لازماً وممكناً خبراء

(١) عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن بين النظرية والتطبيق، بدون ناشر ١٩٩٣م ص ٣١.

التصوير الجنائي ورفع الآثار والبصمات، وكذلك من يرى الاستعانة بهم من الخبراء حرصاً على أدلة الجريمة وتجنباً للعبث فيما يفيد مصلحة التحقيق.

على أنه ينبغي التنبيه إلى مسألة على جانب من الأهمية، هي أن لا تكون في سرعة تصرف المحقق أي إهدار لحقوق الخصوم أو مساس بالعدالة، فمثلاً حرية الشخص أو حرمة مسكنه ليست من المسائل التي يهون الاعتداء عليها لمجرد بعض الظواهر التي قد تكون خادعة، فسرعة البت في الأمور لا تتنافى أبداً مع التأني حين توجب ظروف الواقعة والتحقيق أن يتريث المحقق بعض الوقت ليصدر قراره.

الفصل الثالث
إجراءات التحقيق الابتدائي
في جرائم تقنية المعلومات

إجراءات التحقيق هي مجموعة الأعمال التي يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة. وتنقسم هذه الإجراءات إلى قسمين: قسم يهدف إلى الحصول على الدليل كالتفتيش وسماع الشهود وقسم يمهد للدليل ويؤدي إليه كالقبض والحبس الاحتياطي. وتسمى المجموعة الأولى: إجراءات جمع الأدلة أما الثانية: فتعرف بالإجراءات الاحتياطية ضد المتهم[1]. وسوف يقتصر بحثنا هذا على الإجراءات الخاصة بجمع الأدلة فقط؛ على اعتبار أن الإجراءات الاحتياطية لا إشكال فيها ؛ فهي إجراءات تقليدية.

وإجراءات جمع الأدلة هي الانتقال للمعاينة، وندب الخبراء، والتفتيش، وضبط الأشياء المتعلقة بالجريمة والتصرف فيها، وسماع الشهود، والاستجواب والمواجهة. وهي لم ترد على سبيل الحصر لأن للمحقق أن يستعين بأية وسيلة مشروعة مفيدة في الإثبات لا تنال من حريات الأفراد ولا حرمة مساكنهم وأسرارهم، ولو لم يرد لها ذكر في القانون، مثل عملية العرض القانوني للاستعراف على الشخص، أو الاستعانة بالبصمات، أو الكلاب.

---

(١) د/ أحمد حسني أحمد طه، مبادئ قانون الإجراءات الجنائية في التشريع المصري، ص٤٠٦، د/عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٣٣.

وليس على المحقق الالتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا لمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضي به المصلحة وما تسمح به هذه الظروف[1]. وسوف أتناول هذه الإجراءات في المباحث الآتية:

المبحث الأول: معاينة مسرح الجريمة في جرائم تقنية المعلومات.

المبحث الثاني: التفتيش في جرائم تقنية المعلومات.

المبحث الثالث: الضبط في جرائم تقنية المعلومات.

المبحث الرابع: الشهادة في جرائم تقنية المعلومات.

المبحث الخامس: الخبرة في جرائم تقنية المعلومات.

المبحث السادس: استجواب المتهم ومواجهته في جرائم تقنية المعلومات.

---

(١) د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، ص٢٣٠.

المبحث الأول
معاينة مسرح الجريمة في جرائم تقنية المعلومات

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها، أو محوها أو تعديلها[١]. وعرفها البعض[٢]. بأنها :" إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة" وقيل هي:" رؤية بالعين لمكان أو شخص أو شئ لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة[٣].

فالمعاينة في جوهرها ملاحظة و فحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته و الكشف و التحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة.

والمعانية قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراء تحقيق[٤].

---

(١) د. محمد أبو العلا عقيدة التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٦.

(٢) د/ مأمون محمد سلامه الإجراءات الجنائية في التشريع المصري، ص٦٤٢.

(٣) د. محمد زكى أبو عامر، الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٤،ص٦٧٩.

(٤) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٢٨٧.

والانتقال إلى محل الواقعة من أهم إجراءات جمع الأدلة فهو لازم لمعاينة حالة الأمكنة والأشياء والأشخاص، ووجود الجريمة مادياً، وكل ما يلزم إثبات حالته. (م٩٠ إجراءات مصري، م٧٩ إجراءات سعودي)[١].

وتستحسن المبادرة إليه قبل أن تزول آثار الجريمة أو تتغير معالم المكان. وكثيراً ما يكون الانتقال مصحوباً بالتفتيش وضبط الأشياء، كما قد ييسر للمحقق سماع الشهود دفعة واحدة قبل أن يخضعوا لشتى المؤثرات الخارجية، ومطابقة أقوالهم على معالم المكان وآثار الجريمة. وقد تتيح المعاينة فرصة استجواب المتهم متى أمكن الاستجواب طبقاً للقانون وبحضور محاميه إذا كانت الواقعة جناية، ومواجهته بالأدلة المادية في مكان الحادث إذا كان حاضراً. وإذا كان المتهم غائباً فيمكن إجراء المعاينة في غيبته دون بطلان [٢].

وتقدير وجوب الانتقال من عدم وجوبه أمر متروك للمحقق في النظامين الجزائيين المصري والسعودي؛ فقد نصت المادة (٩٠) إجراءات مصري على أنه :" ينتقل قاضى التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته"، ونصت المادة (٧٩) إجراءات سعودي على أنه:" ينتقِل المُحقِّق – عند الاقتِضاء – فور إبلاغِه بوقوع جريمة داخِلةٌ في اختِصاصِه إلى مكان

(١) د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، ص٢٢٢، د/ عصام عفيفي عبد البصير،التعليق على نظام الإجراءات الجزائية في المملكة العربية السعودية، طبعة دار النهضة العربية،سنة ٢٠٠٥م ص ٧٢.

(٢) نقض ٩/ ٦/ ١٩٥٢، أحكام النقض، س٢، رقم ٣٩٣، ص١٠٥٢.

وقوعِها، لإجراء المُعاينة اللازِمة قبل زوالِها أو طمس معالِمِها أو تغييرِها" إلا أن مشروع اللائحة التنفيذية لنظام الإجراءات الجزائية السعودي يوجب على المحقق الانتقال فور إبلاغه بالجرائم الكبيرة والحوادث المهمة حتى لو وجد شك أو قام نزاع حول الاختصاص المكاني أو النوعي، ويرسل محضر الانتقال والمعاينة بعد انجازه إلى رئيسه لتحديد المحقق المختص، وإذا تعذر على المحقق الانتقال للتحقيق في جريمة أُبلغ عنها فعليه إبلاغ رئيس الدائرة التابع لها ؛ لاتخاذ اللازم في هذا الشأن، أو النظر في ندب غيره"[(١)].

في حين ألزم النظام الجزائي المصري والسعودي مأمور الضبط بالانتقال والمعاينة في حالة التلبس بالجريمة ؛ فنصت المادة (٢٤/ ١) إجراءات مصري على أنه :" يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشأن الجرائم، وأن يبعثوا بها فورا إلى النيابة العانة ويجب على مرؤوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأي كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة.

وأوجبت المادة (٣١/ ٢) إجراءات مصري على مأمور الضبط إخطار النيابة فوراً بانتقاله في الجرائم الملتبس بها، وجرى العمل على قصر الإخطار على الجنايات والجنح العامة فحسب لتقرير النيابة ما إذا كان هناك وجه لانتقالها أم لا، وأوجبت على النيابة العامة الانتقال فوراً إلى محل الواقعة بمجرد إخطارها

---

(١) م٧٩/ ٢ / ٣ من مشروع اللائحة التنفيذية لنظام الإجراءات الجزائية.

بجناية متلبس بها. وقد يترتب على عدم الإخطار أو عدم الانتقال مسئولية إدارية على المخالف، لكن لا يترتب على أيهما بطلان ما [١].

كما نصت المادة (٢٧) إجراءات سعودي على أنه:" على رِجال الضبط الجنائي – كُلٌ حسب اختِصاصِه – أن يقبلوا البلاغات والشكاوى التي ترِد إليهم في جميع الجرائم، وأن يقوموا بفحصِها وجمع المعلومات المُتعلِقة بِها في محضر موقع عليه مِنهُم، وتسجيل مُلخصِها في سجل يُعدّ لذلِك، مع إبلاغ هيئة التحقيق والادِعاء العام بذلك فوراً. ويجب أن ينتقِل رجُل الضبط الجنائي بنفسِه إلى محل الحادِث للمُحافظة عليه، وضبط كُل ما يتعلق بالجريمة، والمُحافظة على أدلتِها، والقيام بالإجراءات التي تقتضيها الحال. وعليه أن يُثبِت جميع هذه الإجراءات في المحضر الخاص بذلك."

والأصل أن يحضر إطراف الدعوى المعاينة، وقد يقرر المحقق أن يجريها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور. ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها[٢].

والمعاينة في جرائم تقنية المعلومات يمكن أن تتم بتصوير شاشة الحاسب الآلي حيث تظهر المعلومات أو الصور المطلوب معاينتها. أو أن يتم ذلك باستخدام برمجية حاسوب متخصصة في اخذ صور لما يظهر على الشاشة و تعرف بطريقة تجميد مخرجات الشاشة **frozen** كما يمكن ان يتم ذلك عن

---

(١) د/ رؤوف عبيد، مبادئ الإجراءات الجنائية، ص ٤١٣، ٤١٤.

(٢) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٢٨٧.

طريق حفظ الموقع باستخدام خاصية الحفظ **save as** ويمكن استخدام خاصية **history** لفحص الحاسب الآلي ، حيث انه في حالة ولوج الحاسب الآلي إلى الانترنت فانه يقوم باستنساخ نسخة من كل صفحة أو موقع يتم استدعائه و يقوم بحفظها في ملف خاص يصنعه نظام التشغيل[١].

ويمكن إجراء المعاينة من خلال تحميل **download** نسخة من الصنف أو الرسالة أو البيانات أو المعلومات التي تم التعدي عليها عبر الانترنت ، ثم يتم طباعتها للحصول على نسخة ورقية عن طريق الطابعة المتصلة بالحاسب الآلي **printer**

وإذ تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب 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 الإلكترونية، حيث يندر أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها[٢]. وبالإضافة إلى ذلك فإن عدداً كبيراً من الأشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يفسح المجال لحدوث تغير أو إتلاف أو عبث

---

(١) المرجع السابق،وقد أشار إلى: **Suzan Brener-model code of cyber crime investigation p. ٢٤ crimes-uni- Dayton school of law.. http://cyber.**

(٢) د. محمد أبو العلا عقيدة التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٦.

بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالاً من الشك على الدليل المستمد من المعاينة[١].

وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الإنترنت فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[٢]:

تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

- 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.

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

---

(١) الدكتور: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، : ص٥٩، د/ عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص ٣٤.

(٢) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٦، د/ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، ص ٦٠، د/ عبد الله حسن على محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٣٤، ٣٥.

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

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

- إبعاد الموظفين عن أجهزة الحاسب الآلي، وكذلك عن الأماكن الأخرى التي توجد بها أجهزة للحاسب الآلي.

- التحفظ عما قد يوجد بسلة المهملات[1] من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة، وفحصلها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

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

- عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة.

- قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الآلي والشبكات

---

(١) من فحص بعض البطاقات المثقبة المعثور عليها بسلة المهملات في المكان الموجود به جهاز الحاسب الآلي أمكن كشف غموض جريمة شهيرة لسرقة البرمجيات عن بعد وقعت أحداثها بسانتا كلارا بالولايات المتحدة الأمريكية. حول التفاصيل الفنية لارتكاب هذه الجريمة انظر: الدكتور/ هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط ١٩٩٢، م ص ١٢٦-١٢٧.

ونظم المعلومات. واسترجاع المعلومات، والذين تلقوا تدريباً كافياً على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية.

وتجدر الملاحظة أنه ينبغي توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حده 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 بجرائم الإنترنت فيها ما يلي[1]:

- **الورق**: على الرغم من إن وجود أجهزة الحاسب الآلي قلل من حجم الأوراق والملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسب الآلي، نجد الكثيرين ممن يقوموا بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها في البحث عن الحقيقة.

---

(١) د/ محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، ص ٣٦٠، د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص١٠، محمد بن نصير محمد السرجاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت ص٨١، وقد أشارا إلى:

Sammes T & Jenkinson B, (2000) Forensic Copmputing: Apratitioner's Guide London Springer.

- **جهاز الحاسب الآلي وملحقاته**: وجود جهاز الحاسب الآلي هام جداً للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية، وإنها مرتبطة بالمكان أو الشخص الحائز على الجهاز، ولأجهزة الحاسب الآلي أشكال وأحكام وألوان مختلفة وخبير الحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة.

- **البرمجيات Software** : إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص أو ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

- **وسائط التخزين المتحركة**: كالأقراص المدمجة "أقراص الليزر" والأقراص المرنة والأشرطة المغناطيسية والفلاش موري وغيرها، وتعد هذه الوسائط جزء من الجريمة الإلكترونية متى ما كانت محتوياتها عنصر من عناصر الجريمة.

- **المراشد Manuals** : الخاصة بالمكونات المادية والمنطقية للحاسب الآلي والتي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها.

- **المودم Modem** : وهو الوسيلة التي تُمكن أجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف. وفي الوقت الحالي تطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

- **الطابعات** : والتي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعاتها.

المبحث الثاني
التفتيش في جرائم تقنية المعلومات

التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بجريمة وقعت، وكل ما يفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحيط هذا التفتيش بضمانات عديدة، ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعية قد يكون متعلقا بالمتهم أو بغيره وهو في كل أحواله جائز مع اختلاف في بعض الشروط [(١)].

وقد تضمنت شروط التفتيش في التشريع المصري المادة ٩١ من قانون الإجراءات المصري؛ فنصت على أن: "تفتيش المنازل عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة. ولقاضي التحقيق أن يفتش أي مكان. وفي جميع الأحوال يجب أن يكون أمر التفتيش مسبباً".

ووفقاً للمادة ١٩٩ إجراءات مصري تباشر النيابة العامة التحقيق في مواد الجنح والجنايات طبقاً للأحكام المقررة لقاضي التحقيق. وذلك مع

---

(١) د/ مأمون محمد سلامة، قانون الإجراءات الجنائية،ص ٣٤٩ وما بعدها، د/ فوزية عبد الستار : شرح قانون الإجراءات الجنائية، ص٣٣٥ وما بعدها، د/عوض محمد عوض، قانون الإجراءات الجنائية،جـ ١، طبعة مؤسسة الثقافة الجامعية ١٩٨٩م ص٤٧٥.

ملاحظة ما نصت عليه المادة ٢٠٦ من أنه يشترط لقيام النيابة بتفتيش غير المتهم أو بتفتيش منزل غير منزله الحصول على أمر مسبب بذلك من القاضي الجزئي بعد إطلاعه على الأوراق.

بينما تضمنت شروط التفتيش في التشريع السعودي المادة٨٠ من نظام الإجراءات الجزائية؛ فنصت على أن:" تفتيش المساكن عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا بناء على اتهام موجه إلى شخصٍ يقيم في المسكن المراد تفتيشه بارتكاب جريمة، أو باشتراكه
في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة. وللمحقق
أن يفتش أي مكان ويضبط كل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها، وكل ما يفيد في كشف الحقيقة بما في ذلك الأوراق والأسلحة، وفي جميع الأحوال يجب
أن يُعِد محضراً عن واقعة التفتيش يتضمن الأسباب التي بُني عليها ونتائجه، مع مراعاة
أنه لا يجوز دخول المساكن أو تفتيشها إلا في الأحوال المنصوص عليها نظاماً وبأمر
مسبب من هيئة التحقيق والادعاء العام" كما نصت المادة ٨١ إجراءات على أن :" للمحقق أن يفتش المتهم، وله تفتيش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة "

من النصوص السابقة يتبين أنه يشترط لصحة التفتيش الشروط الآتية:ـ

أولاً : يجب أن يكون هناك اتهام موجه إلى الشخص الذي يراد تفتيشه أو تفتيش مسكنه، أو وردت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، ويترتب على ذلك أمران:

الأمر الأول: أن الاستناد في إجراء التفتيش إلى مجرد التبليغ عن الجريمة أو الشكوى منها لا يكفي لصحة التفتيش وإنما يجب أن يسبقه على الأقل التحري وجمع الاستدلالات عما ورد في البلاغ [(١)]، فإذا تبين من التحري وجود دلائل كافية على نسبة الجريمة إلى شخص معين جاز تفتيش مسكنه، يستوي في ذلك أن يكون هو فاعل الجريمة أو شريكاً فيها. كذلك يجوز تفتيش منزل غير المتهم بشرط أن توجد قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة. وتوافر القرائن الكافية متروك لتقدير المحقق تحت رقابة محكمة الموضوع [(٢)].

الأمر الثاني: أنه لا يجوز تفتيش عدد من المنازل الكائنة في منطقة معينة، لأن القانون يجيز تفتيش منزل الشخص الذي يشتبه في ارتكابه الجريمة أو في حيازته لأشياء تتعلق بها، ولكنه لا يجيز تفتيش المنازل للبحث عن المجرم، أو

---

(١) فلا يشترط لاتخاذ إجراءات التفتيش أن يكون مسبوقاً بتحقيق أجري بمعرفة سلطة التحقيق، نقض ٥/ ١/ ١٩٥٤، مجموعة أحكام محكمة النقض، س٥، رقم٧٢، ص٢١٣.

(٢) نقض ٦/ ٢/ ١٩٧٢ مجموعة أحكام محكمة النقض، س٢٣، رقم٣٤، ص١٢٦.

عن الجريمة [١]. ولذلك يجب أن يكون تعيين الشخص المراد تفتيشه أو تفتيش منزله واضحاً ومحدداً له تحديداً نافياً للجهالة وقت صدور الإذن [٢].

ثانياً : يجب أن يكون التفتيش - وفقاً لنص المادة (م٩١) إجراءات مصري - بصدد جناية أو جنحة وقعت فعلاً فلا يجوز التفتيش في المخالفات، لأن ضآلة شأنها تحول دون إجازة التعرض لحرمة المسكن أو الشخص، في حين لم يحدد التشريع السعودي نوع الجريمة التي تكون سبباً ومبرراً للتفتيش؛ فيكون التفتيش في جميع الجرائم الجسيمة وغيرها[٣].

---

(١) د/ محمود مجمود مصطفى، شرح قانون الاجراءات الجنائية، ص٢٧٢.

(٢) نقض ٢٢/ ٥/ ١٩٧٢ مجموعة أحكام محكمة النقض، س٢٣،رقم١٧٧، ص٧٨٦، ومع ذلك ذهبت محكمة النقض في بعض أحكامها إلى إغفال اسم المطلوب تفتيشه أو الخطأ فيه لا يبطل التفتيش طالما اقتنعت المحكمة بأن الشخص الذي حصل تفتيشه هو المقصود بأمر التفتيش: نقض ٢٠/ ٦/ ١٩٦٦، س١٧، رقم١٦١، ص٨٥٢، ونقض ٢٨/ ١٠/ ٢٩٦٣، س١٤، رقم ١٢٨، ص ٧١٠، كما قضت بأن عدم إيراد اسم المتهم كاملاً ومحل إقامته محدداً في محضر الاستدلال لا يقدح بذاته في جدية التحريات: نقض ٢٤/ ٤/ ١٩٨٠، س٣١، رقم١٠٥، ص٥٥٢.

(٣) د/ ممدوح رشيد العنزي، ضمانات المتهم أثناء مرحلة التحقيق الابتدائي في النظام السعودي، دراسة مقارنة، رسالة دكتوراه في الحقوق، جامعة القاهرة، سنة ٢٠٠٩م، ص ٢٨١.

كذلك لا يجوز التفتيش الذي يتعلق بجريمة مستقبلة ولو قامت دلائل قوية على أنها ستقع فعلاً [١]، وتبرير ذلك أن التفتيش باعتباره إجراء من إجراءات التحقيق تتحرك به الدعوى الجنائية، والدعوى الجنائية لا وجود لها قبل وقوع الجريمة.

ثالثاً: يجب أن يهدف التفتيش إلى ضبط الأشياء المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة، فإن لم يكن هناك فائدة ترجى لصالح التحقيق من مباشرة التفتيش كان إجراء تحكمياً. ويخضع المحقق في تقدير مدى الفائدة من التفتيش لرقابة محكمة الموضوع [٢]، وضماناً لتوافر هذا الشرط نص في المادة ٩١/ ٣ إجراءات مصري[٣]. والمادة ٨٠ إجراءات سعودي على أنه يجب أن يكون أمر التفتيش مسبباً.

---

(١) نقض ١٢/ ٣/ ١٩٧٢، مجموعة أحكام محكمة النقض، س٢٣، رقم ٨٠، ص٣٤٩، نقض ١٦/ ٢/ ١٩٧٣، س٢٤، رقم٤٩، ص٢٢٣، ونقض ١١/ ٣/ ١٩٧٣، س٢٤، رقم٦٧، ص٣١٠.

(٢) نقض ١٦/ ٦/ ١٩٥٤، مجموعة أحكام محكمة النقض، س٥، رقم٢٥٥، ص٧٨٧.

(٣) أضيفت هذه الفقرة إلى المادة ٩١ بمقتضى القانون رقم ٣٧ لسنة ١٩٧٢ وذلك تجاوباً مع نص المادة ٤٤ من الدستور التي تقضي بأنه لا يجوز دخول المساكن ولا تفتيشها إلا بأمر القاضي مسبب. ويلاحظ أن المادة ٤٤ من الدستور لا توجب تسبيب الأمر القضائي إلا إذا كان منصباً على تفتيش المساكن. ولذلك لا يبطل الإذن الصادر بتفتيش الشخص لعدم تسبيبه، انظر نقض ٢٢/ ٤/ ١٩٧٣ مجموعة أحكام محكمة النقض، س ٢٤، رقم١١٢، ص٥٤٤، ونقض ٢٤/ ٢/ ١٩٨٠، س٣١، رقم٥٣، ص٢٧١.

وعن كيفية تنفيذ التفتيش ينص القانون على أن يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك. وإذا حصل التفتيش في منزل غير المتهم يدعي صاحبه للحضور بنفسه أو بواسطة من ينيبه عنه إن أمكن ذلك (م٩٢) إجراءات مصري[١] (م ٤٦) إجراءات سعودي[٢] ومع ذلك فحضور المتهم أو من ينيبه عنه ليس شرطاً جوهرياً لصحة التفتيش فلا يترتب على تخلفه البطلان [٣]، ولم يتطلب المشرع المصري حضور شاهدين إذا تعذر حضور المتهم أو من ينيبه كما هو الشأن بالنسبة للتفتيش الذي يجريه مأمور الضبط القضائي (م٥١) إجراءات مصري وذلك تقديراً منه أن في إجراء التفتيش بمعرفة سلطة التحقيق – وهي صاحبة الاختصاص الأصيل بالتحقيق- الضمان الكافي للمتهم، في حين تطلب التشريع السعودي ذلك ؛ إذ أنه لم

(١) تنص المادة ٩٢ من قانون الإجراءات الجنائية على أنه :" يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك. وإذا حصل التفتيش فى منزل غير المتهم يدعى صاحبه للحضور بنفسه أو بواسطة من ينيبه عنه إن أمكن ذلك "

(٢) تنص المادة ٤٦ من نظام الإجراءات الجزائية السعودي على أنه:" يتم تفتيش المسكن بحضور صاحبه أو من ينيبه أو أحد أفراد أسرته البالغين المقيمين معه، وإذا تعذر حضور أحد هؤلاء وجب أن يكون التفتيش بحضور عمدة الحي أو من في حكمه أو شاهدين، ويمكن صاحب المسكن أو من ينوب عنه من الاطلاع على إذن التفتيش ويثبت ذلك في المحضر "

(٣) نقض ١٩/ ٦/ ١٩٧٢، مجموعة أحكام محكمة النقض، س٢٣، رقم ٢٠٩، ص٩٣٦، نقض ٢٤/ ١١/ ١٩٨٠، س٣١، رقم١٩٩، ص١٠٢٩.

يفرق بين التفتيش الصادر من المحقق (عضو هيئة التحقيق والادعاء) والصادر من مأمور الضبط القضائي(م ٤٦) إجراءات سعودي[١].

ويلتزم المحقق عند إجراء التفتيش حدود الغرض منه، فلا يرمي به إلا للبحث عن الأشياء المتعلقة بالجريمة التي يجري التحقيق بشأنها، ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز للمحقق أن يضبطها (م٥٠) إجراءات مصري. (م٤٥) إجراءات سعودي.

ولم يحدد التشريع المصري وقتاً للتفتيش وترك ذلك لتقدير سلطة التحقيق، في حين حدد التشريع السعودي الوقت الذي يكون فيه التفتيش؛ فنص في المادة (٥١) من نظام الاجراءات الجزائية على أنه:" يجب أن يكون التفتيش نهاراً بعد شروق الشمس وقبل غروبها في حدود السلطة التي يخولها النظام، ولا يجوز دخول المساكن ليلاً إلا في حال التلبس بالجريمة". وإذا بدأ التفتيش نهاراً أمكن أن يمتد تنفيذه إلى الليل مادام إجراء التفتيش كان متصلا" (مادة ٥١/ ١ من مشروع النظام الجزائي) [٢].

وبالإضافة لذلك يجب تحرير محضر بالتفتيش يتضمن إجراءاته، وما أسفر عنه من أدلة' ويجب أن يخضع هذا المحضر لنفس الخصائص التي تخضع

(١)د/ ممدوح رشيد العنزي، ضمانات المتهم أثناء مرحلة التحقيق الابتدائي، ص ٢٨٨.
(٢) المرجع السابق، ص ٢٩٦.

لها محاضر النيابة من حيث التدوين بمعرفة كاتب مختص ، والسرية عن الجمهور دون الخصوم [١].

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية فيقصد به: أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها [٢].

ويثير موضوع التفتيش في جرائم تقنية المعلومات مسائل عديدة للبحث: كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتفتيش الحاسبات خاصة، وضوابط هذا التتفيش. وسوف أتناول هذه المسائل فيما يلي:

تفتيش الكيانات المعنوية:

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة، فإن البعض قد تشكك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنوية للحاسبات الآلية، وهو ما حدا ببعض التشريعات بأن تنص صراحة على أن التفتيش يتم بالنسبة لجميع أنظمة الحاسب الآلي، ومثال ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا

(١) د/ زكى محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، ، ص١٧٣.

(٢) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: http://www.fg.com٤٤

الصادر في سنة ١٩٩٠ حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي. وهناك تشريعات أخرى قد أجازت تفتيش أي "شيء" أو اتخاذ أي أجراء يكون لازما لجمع أدلة الجريمة، وعلى ضوء ذلك فإن تفتيش المكونات المعنوية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاما دون تقييد، وكمثال لهذه التشريعات: المادة (٢٥١) من قانون الإجراءات الجنائي اليوناني التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو شيء يكون لازما لجمع الدليل، ويفسر الفقه اليوناني عبارة "أي شيء" بأنها تشمل جميع بيانات الحاسب الآلية المادية والمعنوية سواء أكانت هذه البيانات مخزنة في حاملتها أم كانت معالجة آليا في الذاكرة الداخلية.

وعلى هذا النهج نجد أن المادة (٤٨٧) من القانون الجنائي الكندي تعطي للسلطة المختصة الحق في إصدار الإذن بضبط "أي شيء" ويفسر الفقه عبارة "أي شيء" بأنها تشمل المكونات المادية والمعنوية في الحاسبات الآلية.

ولقد نظر الفقه في الكثير من دول العالم إلى مصطلح "الأشياء" التي ترد عليها جرائم الاعتداء على المال نظرة واقعية، بحيث أن هذا المصطلح لا يجب أن يظل جامدا عند معناه الحرفي وإنما التي قد تصلحن يكون متضمنا لكل ما يصلح أن يكون من جنسه. ولذلك نجد أن بعض الفقهاء في فرنسا قد ذهب إلى أن برامج الحاسبات الآلية ذات كيان مادي ملموس يتمثل في نبضات وإشارات وذبذبات إلكترونية مغناطيسية أو كهرومغناطيسية.

وبالتالي فالشيء يكون محلا للحماية الجنائية بالنظر إلى القيمة التي يتمتع بها والتي قد تتمثل في منفعة مالية أو اقتصادية قد يحصل عليها صاحبه من

ورائه لا فرق في ذلك بين الأشياء المادية والأشياء المعنوية، بل إن بعض الأشياء المعنوية قد تكون لها قيمة اقتصادية تعلو بكثير على الأشياء المادية كالأسرار التجارية والصناعية.

وواقع الأمر أن تفسير مصطلح "الأشياء" عند الأشياء المادية، قد يصطدم مع المذهب السائد اليوم في تفسير النصوص الجنائية والذي لا يعتمد على التفسير الحرفي للفظ فقط وإنما يعتمد وبشكل أوسع على مذهب التفسير المنطقي، والذي يطبق إذا كان النص محل التفسير غامضا أو خافيا في المعنى المقصود منه.

وعلى ذلك فيمكن تفسير مصطلح الأشياء وفقا لمعناها وحقيقتها وبما يتفق مع قصد المشرع من تجريم صور الاعتداء عليها بأنها كل ما يعود بفائدة ويحقق مصلحة لصاحبه، لا فرق في ذلك بين كيانها المادي أو المعنوي.

ويترتب على ذلك أنه يتصور وقوع جرائم الاعتداء على المال على الكيانات المعنوية كالسرقة وخيانة الأمانة والنصب، وأيضا جرائم التخريب والإتلاف، حيث يمكن أن تقع هذه الجريمة الأخيرة على البرنامج أو الدعامة المسجل عليها، أو عليهما معا، وقد تقع كذلك عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد.

ونجد أن الكثير من الدول الأوروبية وعلى النحو الذي يسير عليه الفقه الأمريكي المعاصر تمد سريان النصوص الجنائية الخاصة بجرائم خيانة الأمانة والاستيلاء غير المشروع لتطيق على الأسرار التجارية والصناعية وذلك إذا شكل الاعتداء عليها حالة من حالات التجسس ألمعلوماتي.

وعلى ضوء هذه الآراء الفقهية وعلى النحو الـذي قننتـه التشـريعات صراحة في نصوصها على النحو سالف الإشارة إليه، فـإن التفتـيش كـإجراء من إجراءات التحقيق يمكن أن يرد على الكيانات المعنوية في الحاسبات الآلية، بحسبان أن هذه الكيانات المعنوية وإن كانت غير مادية إلا أنهـا تنطبـق عليهـا سمات أو خصائص المادية ومن ثم فيمكن أن تدخل في نطاق الأشياء المادية. ويترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة إلكترونيا كالاسطوانات والأقراص والأشـرطة الممغنطة ومخرجات الحاسب. ويدخل في هذا التفتيش أيضا المحتويات المخزنـة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته[١].

وفي مواجهة هذا الخلاف والقصور التشريعي لدى بعض الـدول؛ فـإنني أقترح مع البعض[٢] ضرورة أن يضـاف إلى الغايـة التقليديـة للتفتـيش عبـارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلـي) وبـذلك تصبح الغاية من التفتيش بعد هذا التطور الـتقني الحـديث هـي البحـث عـن الأدلة المادية أو أي مادة معالجه بواسطة الحاسب.

---

(١) المرجع السابق نفس الموضع.

(٢) د/ هلال عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة،١٩٩٧م ص٨٤.

تفتيش وسائل تقنية المعلومات المتصلة عبر شبكات محلية أو دولية:

تتميز الحاسبات الآلية بأنها قد تتصل مع بعضها البعض داخل الدولة عن طريق الشبكة المحلية، أو قد تتصل بحاسبات أخرى تقع خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة. وهنا تثور مشكلة لدى جهة التحقيق تتعلق بصدور إذن التفتيش والاختصاص القضائي.

أولاً : حالة وقوع جريمة في نظم حاسب آلي متصل بآخر داخل حدود الدولة:

في هذه الحالة فإن صدور إذن التفتيش وفقا للضوابط القانونية ينفذ بالنسبة للحاسب الآلي الصادر بالنسبة له الإذن فقط، ويترتب على ذلك أنه لا يمكن أن يمتد إذن التفتيش إلي الحاسب الآخر، حتى ولو كان يحتوي على جريمة، إذ يلزم في هذه الحالة أن يصدر إذن جديد بالتفتيش من السلطة المختصة بذلك قانونا. وقد ينتج عن ذلك مخاطر تتمثل في قيام الجاني بتدمير، أو محو البيانات المستهدف التوصل إليها عن طريق التفتيش والتي قد تكون مخزنة لدى هذا الشخص الآخر، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن بالتفتيش فيها.

ولمواجهة هذه المخاطر؛ يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي أخر يوجد في أي مكان غير مكان البحث، واستند هذا الرأي إلى نص المادة ١٠٣ من قانون الإجراءات الجنائية الألماني [(١)].

---

(١) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: **g.com٤٤http://www.f**، د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية،ص ٧.

ويثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، يرى البعض في هذه الحالة عدم استمرار أو امتداد البحث لديه إلا في حالتي التلبس، أو رضائه بالتفتيش. وتضيف المادة ٢٣/ ٢ و ٦٢ مكررا/ ٢ من قانون تحقيق الجنايات البلجيكي أن الإذن يتجاوز حدود الاختصاص المحلي، من اجل البحث عن أدلة الجريمة، يشترط لصحته فضلا عن صدوره من الجهة المختصة أن يتم إبلاغ ممثل النيابة الداخل في نطاق اختصاصه الجغرافي الموضع الجديد محل التفتيش. وقد أدى هذا إلى إدخال المادة رقم ٨٨ في قانون تحقيق الجنايات بمقتضى القانون الصادر في ٢٣ نوفمبر سنة ٢٠٠٠، 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 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.

ويرى البعض أنه في حالة امتداد الاختصاص، فيمكن 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 [١].

ثانياً : حالة وقوع جريمة في نظم حاسب آلي متصل بآخر خارج حدود الدولة: يلاحظ أن بعض الجناة قد يقومون بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية ومستهدفين عدم إمكان الوصول إليها، وفي هذه الحالة فإن تفتيش هذه الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.

ولمواجهة هذه الحالة ؛ يرى جانب من الفقه أن هذا التفتيش الإلكتروني العابر للحدود لا يجوز في غياب اتفاقية دولية بين الدولتين تجيز هذا الامتداد، أو على الأقل الحصول على إذن الدولة الأخرى. وهذا يؤكد أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني. ومع ذلك فقد أجازت المادة ٣٢ من الاتفاقية الأوروبية التي أعدها المجلس الأوروبي في صيغتها النهائية في ٢٥ مايو سنة ٢٠٠١ إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها، وذلك في حالتين :

أ- إذا تعلق بمعلومات أو بيانات مباحة للجمهور.

ب- إذا رضي صاحب او حائز هذه البيانات بهذا التفتيش.

---

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص ٨.

ومع ذلك فإن تطبيق هذا النص يمكن ان يثير مشكلات جمة، 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.

ولقد أدرك المجلس الأوروبي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية في أكثر من دولة فأصدر التوصية رقم ٩٥١٣R والتي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود.

تفتيش الحاسبات الشخصية:

تفتيش الحاسبات الآلية التي تقع في أماكن عامة كالحاسبات الشخصية التي يحملها الشخص خارج منزله، فإن تفتيش أنظمتها لا يكون جائزا إلا في الأحوال التي يجيز فيها القانون تفتيش شخصه، باعتبار أن تفتيش الشخص يشمل ذاته وكل ما في حوزته وقت هذا التفتيش وسواء أكان مملوكا له أم لغيره. وفي الحالة التي يكون فيها الحاسب الآلي المراد تفتيش نظمه داخل منزل أحد الأشخاص، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش مسكن المتهم أو تفتيش منزل غير المتهم[1].

---

(١) د/عوض محمد، قانون الإجراءات الجنائية،جـ ١، طبعة دار المطبوعات الجامعية ١٩٩١م ص٣٧٧، د/ هلال عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة،١٩٩٧م ص٧٤.

ضوابط التفتيش في جرائم تقنية المعلومات:

نظرا لكون التفتيش يتضمن تقييداً 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 هيئة التحقيق والادعاء العام، أو مأمور الضبط القضائي في حالة ندبه، في غير حالات التلبس بالجريمة – كما يجب أن يصدر إذن بالتفتيش من الجهة المختصة. وفيا يلي بيان لهذه الضوابط:

أولا: سبب التفتيش

للتفتيش في جرائم تقنية المعلومات ؛ يجب أن تكون هناك جريمة قد وقعت على الوسائل الإلكترونية أو من هذه الوسائل، وأن تكون هذه الجريمة جناية أو جنحة، وفقاً للتشريع المصري أو أي جريمة الكترونية وفقاً للتشريع السعودي، ومن أمثلة هذه الجرائم، الغش المرتبط بالحاسب الآلي: ويشمل الإدخال، الإتلاف، المحو، أو الطمس لبيانات أو برامج الحاسب الآلي، التزوير ألمعلوماتي: يتضمن الإدخال، الإتلاف، المحو أو الطمس البيانات أو برامج الحاسب، الإضرار ببيانات وبرنامج الحاسبات: ويشمل المحو، الإتلاف، التعطيل أو الطمس غير المشروع لبيانات وبرامج المعلوماتية، تخريب الحاسبات: ويحتوي على الإدخال، الإتلاف، المحو، أو الطمس لبيانات وبرامج الحاسب، الدخول غير المصرح به: وهو الدخول غير المشروع لنظام معلوماتي أو مجموعة نظم، وأخيرا: الاعتراض غير المصرح به: وهو اعتراض غير مصرح به ويتم بدون وجه حق عن طريق استخدام وسائل فنية للاتصال.

ويلاحظ أنه لا محل لإصدار الإذن بتفتيش الحاسبات الآلية إلا إذا كان المشرع قد نص على الجرائم التي تشكل اعتداء عليها في شكل نصوص التجريم والعقاب تطبيقا لمبدأ شرعية الجرائم والعقوبات، وعلى النحو الذي فعلته الكثير من التشريعات المقارنة، وفعله المشرع المصري بالنسبة لبرامج الحاسب الآلي وقواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره، إذ أنزل عليها حماية جنائية وجعل الاعتداء عليها يعد جريمة من نوع الجنح على النحو الذي نصت عليه المادتين (١٤٠ و ١٨١ من القانون رقم ٨٢ لسنة ٢٠٠٢) بشأن حماية حقوق الملكية الفكرية.وكذلك فقد أنزل المشرع المصري حمايته الجنائية على البرامج وقواعد البيانات المتعلقة بالأحوال المدنية للمواطنين، والبيانات الفردية التي تقتضي إجراء إحصاء للسكان[1].

---

(١) تنص المادة ١٤٠ من القانون رقم ٨٢ لسنة ٢٠٠٢م على أنه :" تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص المصنفات الآتية:..... ٢. برامج الحاسب الآلي. ٣. قواعد البيانات سواء كانت ومقروءة من الحاسب الآلي أو غيره. .."

وتنص المادة ١٨١ من القانون رقم ٨٢ لسنة ٢٠٠٢م على أنه :" مع عدم الإخلال بأية عقوبة اشد في قانون آخر يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلاف جنية ولا تجاوز عشرة آلاف جنية أو بإحدى هاتين العقوبتين كل من ارتكب احد الأفعال الآتية:....رابعا: نشر مصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمى طبقا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الانترنت أو شبكة المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابي مسبق من المؤلف أو صاحب حق المجاور....خامسا: التصنيع أو التجميع أو الاستيراد بغرض البيع أو التأجير لأي جهاز أو وسيلة أو أداه مصممه

أو معدة للتحايل على حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره....سادسا : الإزالة أو التعطيل أو التعييب بسوء نية لأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره".

كما تنص المادة ٧٤ من القانون رقم ١٤٣ لسنة ١٩٩٤ الخاص بحماية البيانات والمعلومات الخاصة بالأحوال المدنية للمواطنين والتي تشتمل عليها السجلات والدفاتر والحسابات الآلية ووسائط التخزين الخاصة بمصلحة الأحوال المدنية بوزارة الداخلية علي أنه " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين يعاقب بالحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد علي خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع أو شرع في الإطلاع أو حصل أو شرع في الحصول علي البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقا للإجراءات المنصوص عليها فيه ، فإذا وقعت الجريمة علي البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة الحبس".

وتنص المادة ٧٥ من ذات القانون سالف الذكر علي أنه " يعاقب بالحبس مدة لا تجاوز ستة أشهر وغرامة لا تقل عن مائتي جنيه ولا تزيد علي خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزءا منها وكان ذلك ناشئا عن إهماله أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة. فإذا وقع الفعل عمدا تكون العقوبة السجن مع عدم الإخلال بحق التعويض في الحالتين ".

ومما سبق يتضح أن المشرع المصري لم يجرم جميع صور الإجرام المعلوماتي وإنما اقتصر في الحماية علي حماية البيانات والبرامج المشمولة بحماية حقوق المؤلف وحماية

وبالنسبة للمنظم السعودي فقد أحسن صنعاً، وأصدر نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم م/ ١٧ وتاريخ: ٨/ ٣/ ١٤٢٨هـ بناءً على قرار مجلس الوزراء رقم : (٧٩) وتاريخ : ٧/ ٣/ ١٤٢٨هـ ونص في المواد من ٣-٧ على الجرائم المعلوماتية[1].

البيانات الفردية الخاصة بالإحصاءات السكانية والبيانات الخاصة بالأحوال المدنية للمواطنين ، أما باقي صور الإحرام المعلوماتي التي تقع بواسطة أو علي وسائل تقنية المعلومات الحديثة كالكومبيوتر والتليفون المحمول بصورة خاصة فلم يتعرض لها مما أوجد فراغا تشريعا دفع الفقه إلي بسط سلطان قواعد قانون العقوبات التقليدية علي هذه الصور للإجرام المعلوماتي ، إلا أن هذا وكما سبق أن ذكرنا يتعارض مع مبدأ الشرعية ومبدأ حظر القياس في مواد التجريم والعقاب مما يتطلب تدخلا تشريعيا سريعا لسد هذا الفراغ التشريعي ومواجهة هذه الصور المستحدثة للإجرام المعلوماتي .

(١) تنص المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودي على أنه :"يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه. ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً. ٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه. ٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها. ٥- التشهير بالآخرين، وإلحاق الضرر بهم،

عبر وسائل تقنيات المعلومات المختلفة. وتنص المادة الرابعة على أنه :"يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة. ٢- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات. وتنص المادة الخامسة على أنه :" يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية : ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها. ٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها. ٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت". وتنص المادة السادسة على أنه :"يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- إنتاج ما من شأنه المساس بالنظام العام، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي. ٢- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به. ٣- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها. ٤- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة

ولا يكفي لإصدار الإذن بتفتيش الوسائل الإلكترونية مجرد الإبلاغ بوقوع جريمة من قبيل الجناية أو الجنحة وإنما التي قد تصلح لأن تكون قد تجمعت بالنسبة لها إمارات قوية تفيد وقوعها بما يبرر المساس بحرية الأفراد عند تفتيش أشخاصهم، أو بحرمة منازلهم عند تفتيش هذه المنازل.

والمعيار لإصدار الإذن بالتفتيش أن تكون الدلائل التي تجمعت حول الجريمة تدعو للاعتقاد المعقول بوقوعها سواء أكان من تجمعت حوله هذه الدلائل فاعلا أصليا لها ام يقف دوره الإجرامي عند الشريك. وتقدير هذه الدلائل متروك للسلطة التي تصدر الإذن بالتفتيش بشرط ان يكون تقديرها منطقيا ومتفقا مع الواقع بحيث تكشف هذه الدلائل بجدية عن وقوع الجريمة محل الإذن بالتفتيش وأن هناك جانيا تنسب إليه.

الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها". وتنص المادة السابعة على أنه :"يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية : ١- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية. ٢- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".

وفيما يتعلق بالجرائم التي تقع على الوسائل الإلكترونية ويصدر الإذن بالتفتيش لضبط أدلة تفيد في وقوعها فإنه يقصد بالدلائل الكافية بالنسبة لها مجموعة المظاهر والإمارات التي تكفي وفقا للسياق العقلي والمنطقي أن ترجح ارتكابها ونبتها إلى شخص معين سواء أكان وصفه فاعلا لها أم شريكا.

وإذا كان الغرض من إذن التفتيش جمع الأدلة بشأن الجريمة التي تكون قد وقعت على الوسائل الإلكترونية أو عن طريق هذه الوسائل فإنه يلزم أن تكشف الإمارات القوية والقرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم وترجح ارتكابه للجريمة، ومثال ذلك وجود أدوات تكون قد استعملت في ارتكاب الجريمة أو لضبط أشياء متحصله منها أو مستندات إلكترونية أو دعامات تفيد في إماطة اللثام عنها.

فالإذن بالتفتيش الذي يقع على الوسائل الإلكترونية قد يصدر لجمع أدلة عن جرائم تكون قد وقعت على البرنامج أو الكيان المنطقي، أو نظام التشغيل، أو النظم الفرعية، أو البرامج والخدمات المساعدة أيا كان شكلها أو دعاماتها المادية أو وعائها، أو على المستندات التي تكون متعلقة بهذا البرنامج أو الكيان المنطقي بما في ذلك البيانات المعدة للتسجيل أو المسجلة في ذاكرة الحاسب أو في مخرجاته أيا كانت شكلها أو دعامتها أو وعائها، أو على السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات أيا كان شكل هذه السجلات أو الدعامة المادية التي تجسدها، أو على السجلات الخاصة بعمليات دخول نظم المعالجة الآلية للبيانات كسجلات كلمات السر ومفاتيح الدخول ومفاتيح فك الشفرة أيا كان شكلها أو دعامتها أو وعائها.

ولعل الطبيعة الخاصة بالجرائم التي تقع في محيط الوسائل الإلكترونية تتطلب تأهيلا فنيا خاصة بالنسبة لمأموري الضبط القضائي الذين يناط بهم ضبط هذه الجرائم وجمع الأدلة بشأنها وذلك لكي يمكنهم التعامل السليم مع مخرجات هذه الوسائل ومع دعائمها وبرامجها للحفاظ على سلامة الأدلة ألمتحصله عنها من كل تلف أو مسح.[١].

محل التفتيش في جرائم تقنية المعلومات:

يشمل التفتيش في جرائم تقنية المعلومات كل المكونات المادية والمعنوية للوسائل الإلكترونية. ويمكن أن يشمل التفتيش أيضا شبكات الاتصال الخاصة بها والأشخاص الذين يستخدمون هذه الوسائل، وتتكون المكونات المادية لهذه الوسائل من وحدة المدخلات ووحدة الذاكرة الرئيسة، ووحدة الحساب والمنطق، ووحدة التحكم، ووحدة المخرجات، ووحدات التخزين الثانوية، وأما المكونات المعنوية فهي عبارة عن برامج النظام وبرامج التطبيقات.

ويضاف إلى ذلك أن الوسائل الإلكترونية بمكوناتها المختلفة تستلزم لتشغيلها وجود مجموعة من الأشخاص أصحاب الخبرة والتخصص في مجال تقنية المعلومات وهم مشغلوا الحاسب، خبراء البرمجة سواء كانوا مخططي برامج تطبيقات أم مخططي برامج نظم، والمحللين ومهندسي الصيانة والاتصالات، ومديري النظم المعلوماتية[٢].

---

(١) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: **g.com٤٤http://www.f**

(٢) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٧، د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٠٧.

شروط صحة التفتيش:

يشترط لصحة التفتيش أن يكون من أصدر الإذن بالتفتيش مختصا بالتحقيق في الجريمة التي يصدر الإذن بشأنها، وهذا الاختصاص قد يتحدد بمحل الواقعة أو المكان الذي ضبط فيه الجاني أو بمحل إقامته. ويجوز أن تمتد بعض الإجراءات خارج هذا الاختصاص إذا استوجبت ظروف التحقيق ذلك بشرط أن يكون المحقق قد بدأ إجراءات التحقيق بدائرة اختصاصه المكاني.

ويلزم كذلك أن يكون المحقق مختصا بالإجراء الذي يتخذه، فلا يجوز له ندب مأمور الضبط القضائي لتفتيش غير المتهم أو غير منزله لأن هذا التفتيش يخرج عن اختصاصه. ويجب لصحة إذن التفتيش الصادر في محيط الجرائم التي تقع على الوسائل الإلكترونية أو عن طريقها أن يكون من صدر له الإذن بالتفتيش من مأموري الضبط القضائي المختصين بذلك وظيفيا ومكانيا ونوعيا، ولا يشترط بعد ذلك التزام المحقق بندب مأمور ضبط معين. ويشترط في الإذن بالتفتيش الصادر بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية أن يكون مكتوبا ومحددا التاريخ وموقعا ممن أصدره، وان يكون صريحا في الدلالة على التفويض في مباشرة التفتيش، وان يتضمن من البيانات ما يحدد نوع الجريمة المطلوب جمع الأدلة عنها. ويجب كذلك تحديد محل التفتيش والذي قد يكون شخصا أو منزلا، وتحديد المدة الزمنية التي يراها المحقق كافية لتنفيذ الإذن[1].

وعلى ما سبق فإنه لا خلاف في الجملة بين الضوابط المتطلبة في التفتيش في جرائم تقنية المعلومات عنها في جرائم التقليدية، وهذا محل اتفاق بين النظام الجزائي المصري والسعودي.

---

(١) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: **g.com٤٤http://www.f**، د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٠٥، ٣٠٦

المبحث الثالث
الضبط في جرائم تقنية المعلومات

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها[١]. 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 عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال[٢].

والتفتيش لا يقرر لذاته وإنما يقرر بهدف ضبط أدلة الجريمة وكل شيء يفيد في كشف الحقيقة سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيء نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة[٣] (م٩١/ ٢ إجراءات مصري، م٨٠ إجراءات سعودي).

وقد خول المنظم المصري والسعودي لجهة التحقيق سلطات واسعة في الضبط ؛ فتنص المادة (م٩٥/ ١) على أنه :" لقاضى التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد

---

(١) د/ عوض محمد، قانون الإجراءات الجنائية، ص٢١٥.

(٢) د/ عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٤٤.

(٣) د/ رؤوف عبيد، مبادئ الإجراءات الجنائية، ص ٤٤٥، د/ فوزية عبد الستار : شرح قانون الإجراءات الجنائية، ص٣٤٢ وما بعدها.

وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفى جميع الأحوال يجب أن يكون الضبط أو الإطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو لمدد أخرى مماثلة " وتنص المادة (٥٦) إجراءات سعودي على أنه:" لرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل والخطابات والمطبوعات والطرود، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها، متى كان لذلك فائدة في ظهور الحقيقة في جريمة وقعت، على أن يكون الإذن مسبباً ومحدداً بمدة لا تزيد على عشرة أيام قابلة للتجديد وفقاً لمقتضيات التحقيق".

ومن خلال النصين السابقين يتضح أنهما أجازا لسلطة التحقيق ضبط الرسائل ومراقبة المحادثات السلكية واللاسلكية وتسجيلها؛ متى كان لذلك فائدة في ظهور الحقيقة. ولكن المنظم المصري أشترط أن يكون ذلك في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد عن ثلاثة أشهر، في حين لم يحدد المنظم السعودي نوع الجريمة كما اشترط المنظم المصري وكذا المنظم السعودي أن يكون الضبط أو الإطلاع أو المراقبة أو التسجيل بناء على أمر مسبب من جهة التحقيق، ولكنهما اختلفا في المدة المحددة لذلك؛ فنجدها في النظام المصري لا تزيد عن ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة (م٩٥/ ٢) وهذا ما قررته المادة (٤٥) من الدستور التي تقضي بأن:" لحياة المواطنين الخاصة حرمة يحميها القانون. وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمه، وسريتها مكفولة،

ولا تجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقاً لأحكام القانون".

فإذا كانت النيابة العامة هي التي تقوم بضبط هذه الأشياء فإنه يشترط لصحة الضبط حينئذ الحصول مقدماً على أمر مسبب بذلك من القاضي الجزئي بعد إطلاعه على الأوراق[(١)]، كما يشترط أن يكون الأمر بالضبط أو الإطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوماً، ويجوز للقاضي الجزئي أن يجدد هذا الأمر مدة أو مدد أخرى مماثلة (م٢٠٦ إجراءات مصري)، وواضح أن العلة في اشتراطا استئذان القاضي الجزئي فيما تجريه النيابة العامة من ضبط الرسائل ومراقبة المحادثات وإجراء التسجيلات أن هذه الأمور تتعلق بها مصلحة لغير المتهم [(٢)]. ويخضع لمطلق تقدير القاضي الجزئي إصدار الإذن بالإجراء أو عدم إصداره تحت إشراف محكمة الموضوع [(٣)].

---

(١) فإذا كان الحكم قد أبان أن القاضي قد أصدر الإذن بمراقبة تليفون الطعنة بعد أن أثبت إطلاعه على التحريات التي أوردها الضابط في محضره، وأفصح عن اطمئنانه إلى كفايتها فإنه بذلك يكون قد اتخذ تلك التحريات أسباباً لإذنه بالمراقبة، وفي هذا ما يكفي لاعتبار إذنه مسبباً حسبما تطلبه المشرع بما نص عليه في المادة ٢٠٦ إجراءات، انظر نقض ١٩٧٣/١١/٢٥ مجموعة أحكام محكمة النقض، س٢٤، رقم٢١٩، ص١٠٥٣.

(٢) وهي نفس العلة التي يستند إليها استئذان القاضي الجزئي عندما تقوم النيابة العامة بتفتيش غير المتهم أو تفتيش منزل غير منزله.

(٣) وقد قضى بأن (سلطة القاضي الجزئي في مراقبة المكالمات التليفونية محدودة بمجرد إصداره الإذن أو رفضه دون أن يخلع عليه القانون ولاية القيام بإجراء موضوع الإذن بنفسه، إذ أنه من شأن النيابة العامة –سلطة التحقيق– إن شاءت قامت به بنفسها أو ندبت من تختاره من مأموري الضبط القضائي، وليس للقاضي الجزئي أن

في حين أن المدة المحددة للإذن بالضبط والمراقبة في النظام السعودي لا تزيد عن عشرة أيام، قابلة للتجديد حسب مقتضيات التحقيق(م٥٦ إجراءات سعودي)

وقد استثنى المنظم المصري والسعودي من قواعد الضبط المذكورة أنه لا يجوز للمحقق أن يضبط لدى المحامي المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي عهد إليهما بها، والمراسلات المتبادلة بينهم في القضية (م٩٦ إجراءات مصري، م٨٤ إجراءات سعودي) ويبرر هذا الاستثناء حرص المشرع على كفالة حرية الدفاع للمتهم. ويلاحظ أنه وإن كان المشرع قد نص على عدم جواز ضبط الأوراق والمستندات لدى المدافع أو الخبير، إلا أن حكمة الاستثناء توجب مد نطاقه إلى ضبط هذه الأوراق والمستندات أينما وجدت أي سواء لدى المدافع أو الخبير أو في مكاتب البريد أو البرق [1]. بل أنها توجب مد نطاقه إلى المحادثات التليفونية والأحاديث الخاصة التي تجري بين المتهم والمدافع أو الخبير

يندب أحد هؤلاء مباشرة لتنفيذ الإجراء المذكور. فإذا كان الثابت أن وكيل النيابة المختص قد استصدر إذناً من القاضي الجزئي بمراقبة تليفوني المتهمين، فقام الضابط الذي أجرى التحريات بتنفيذه دون أن يندب لذلك من النيابة العامة فإن ما قام به الضابط من إجراءات المراقبة والتفتيش يكون باطلاً لحصولهما على خلاف القانون ولا يصح التعويل على الدليل المستمد منهما: نقض ١٢/ ٢/ ١٩٦٢ مجموعة أحكام محكمة النقض، س١٣، رقم٣٧، ص١٣٥.

(١) د/ محمود محمود مصطفى: شرح قانون الإجراءات الجنائية، ص٢٨١.

الاستشاري فإذا تم ضبط هذه الأوراق أو المحادثات كان الضبط باطلاً، فيبطل الدليل المستند إليه.

وقد خول المشرع للمحقق وحده أن يطلع على الخطابات والرسائل والأوراق الأخرى المضبوطة، على أن يتم ذلك إذا أمكن بحضور المتهم والحائز لها أو المرسلة إليه، ويدون ملاحظاتهم عليها، ولقاضي التحقيق عند الضرورة أن يكلف أحد أعضاء النيابة العامة بفرز الأوراق المذكورة، وللمحقق سواء كان قاضي التحقيق أو النيابة العامة، أو عضو هيئة التحقيق والادعاء – حسب ما يظهر من الفحص- أن يأمر بضم تلك الأوراق إلى ملف القضية أو يردها إلى من كان حائزاً لها أو إلى المرسلة إليه (م٩٧، ٢٠٦إجراءات مصري، م٥٧ إجراءات سعودي)،

ونظراً إلى أن الأوراق المضبوطة قد يكون بها ما يتطلب تبليغه إلى صاحبه في الوقت المناسب فإن المشرع أوجب أن تبلغ الخطابات والرسائل التلغرافية المضبوطة إلى المتهم أو المرسلة إليه أو تعطى إليه صورة منها في أقرب وقت إلا إذا كان في ذلك إضراراً بسير التحقيق. (م١٠٠ إجراءات مصري، م٥٨ إجراءات سعودي)

وتوضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن ويختم عليها[1]، ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط

---

(١) ولم يستلزم القانون أن يكون الخاتم المستعمل في التحريز لمأمور الضبط القضائي، نقض ١٧/ ١٠/ ١٩٧١ مج٢٣، رقم ١٣٠، ص٥٣٩، نقض ١١/ ٦/ ١٩٧٩، س٣٠، رقم١٤٥، ص٦٧٩.

تلك الأشياء ويشار إلى الموضوع الذي حصل الضبط من أجله (م٥٦، ٩٨ إجراءات مصري، م٤٩ إجراءات سعودي) [١].

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

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

---

(١) ويجري قضاء محكمة النقض على أن إجراءات تحريز الأشياء والأوراق المضبوطة ليست من الإجراءات الجوهرية وإنما هي من الإجراءات التي يقصد بها تنظيم العمل للمحافظة على الدليل خشية توهينه فلا يترتب على مخالفتها بطلان الضبط، ويترك أمر تقدير مدى سلامة الدليل إلى محكمة الموضوع ومدى اطمئنانها إلى ذلك، انظر نقض ٢٨/ ١٠/ ١٩٥٨ مجموعة أحكام محكمة النقض، س٩، رقم٢١٠، ص٨٥٥، ونقض ٤/ ٢/ ١٩٦٣ س١٤، رقم١٩، ص٨٨، ونقض ٨/ ١٠/ ١٩٨٢ س٢٣، رقم ٢١٨، ص٩٧٩، ونقض ١٢/ ٣/ ١٩٧٢، س٢٣، رقم٨١، ص٣٥٧، ونقض ٢٥/ ٦/ ١٩٧٣، س٢٤، رقم٨١، ص٣٥٧، نقض ١٢/ ٢/ ١٩٧٩، س٣٠، رقم٤٩، ص٢٤٣.

وبالنسبة للضبط في جرائم تقنية المعلوماتية، فإن محله قد يكون الأدلة المادية أو المعنوية:

وفيما يلي أتناول ضبط الأدلة المادية والمعنوية في جرائم تقنية المعلومات:

أولاً : ضبط الأدلة المادية:

الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات جرائم الحاسب الآلي ونسبتها إلى المتهم هي[1] :

١. الورق : كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد ان الكثيرين يقومون بطباعة المعلومات **print out** لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدرا كبيرا من الأوراق في وقت قصير عليه يعتبر 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.

---

(١) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣١٨، د/عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٤٥.

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 الحاسب الآلي.

٢. جهاز الحاسب الآلي وملحقاته: **Computer paraphernalia**

وجود جهاز حاسب الي مهم للقول بأن هناك جريمة ولاجهزة الحاسب الآلي اشكال وأحجام والوان مختلفة وخبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى وتحديد اسلوب التعامل معه في حالة الضبط والتحريز.

٣. الحاسب الآلي، لوحة المفتاح والشاشة: من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية **CUP**، لوحة المفاتيح **Key board** والشاشة **Monitor** ومع التطورات السريعة التي يمر بها الحاسب الآلي نجد إضافات جديدة مثل المودم والماوس والسماعات والسيرفر، وإذا كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أن اشكالها تتغير بإستمرار خاصة من حيث الحجم والهيكل ومن الضروري اطلاع العاملين في مجال التحقيق على مختلف أشكال اجهزة الحاسب الآلي فور ظهورها.

٤. **أقراص الليزر**: **Disks and diskettes**

مع جهاز الحاسب آلي شخصي عادي تجد قدرا كبيرا من أقراض الليزر علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك قد تجد فيها الآلاف من الاقراص 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 حاسب آلي ومع ذلك يعد جزءا من جريمة حاسب آلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

٥. **الشرائط المغنطة** **Magnetic Tapes**

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

٦. **لوحة الدوائر**: **circuit boards and components**

٧. **المودم**: **Modem**

والمودم **demodulator/ Modulator** هي الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف وقد تطورت المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الآلي.

٨. **الطابعات**: **Printers**

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

٩. **Pcmcia Cards** وتستعمل بطاقات الـ **Pcmcia** في أجهزة الحاسب الآلي الصغيرة النوت بوك **Notebook** واللاب توب **Laptop** وهي في شكل البطاقات الائتمانية.

١٠. **البرامج اللينة والمراشد**: المراشد **Manuals** المصاحبة للحاسب الآلي مفيدة في التعرف على الجهاز والبرامج المستعملة فيها.

١١. **البطاقات الممغنطة وبطاقات الائتمان القديمة** والمواد البلاستيكية المستعملة في إعداد تلك البطاقات تعتبر قرائن للإثبات في جرائم الحاسب الآلي.

كل ذلك يعد أثرا أو جزءا من جسم الجريمة ينبغي البحث عنها وفحصها والاستفادة منها في التحقيق علما بأن التعامل مع مثل هذه الآثار يحتاج إلى خبرة فنية في مجال الحاسب الآلي ومعرفة بالقانون وقواعد البيئة.

ثانياً: **ضبط الكيانات المعنوية**:

هناك صعوبة في التفتيش عن الكيانات المعنوية في جرائم تقنية المعلوماتية كالبيانات المعالجة الكترونيا والمراسلات والاتصالات الالكترونية نظرا لصعوبة وصفها بالأشياء

المادية [(١)] المتحصلة من الجريمة والتي يقع عليها التفتيش ، وسبق أن ذكرت أنه يجب أن يدخل في نطاق التفتيش ، التفتيش عن المعنويات المعلوماتية ، وإلا أدي ذلك إلي إيجاد العديد من الصعوبات أمام سلطات التحقيق فيما يخص جمع الأدلة التي تفيد في الكشف عن الحقيقة في الجريمة

(١) د/ بكري يوسف،التفتيش عن المعلومات في وسائل التقنية الحديثة، بحث منشور بمجلة كلية الشريعة والقانون بدمنهور، سنة ٢٠٠٧م، ص٥٢٠.

المعلوماتية ، بل قد يؤدي عدم اعتبار المكونات المعنوية المعلوماتية من الأشياء التي تخضع للتفتيش إلي عدم قيام الجريمة المعلوماتية وذلك متي كانت هذه المكونات المعلوماتية المعنوية هي السبيل الوحيد لإظهار حقيقة الجريمة المعلوماتية.

وإذا كان الأمر قد انتهي بنا إلي ضرورة أن يشمل التفتيش المكونات المعنوية لوسائل التقنية الحديثة فإنه من الضروري أن يترتب علي ذلك إباحة ضبطها ، وإن كان تحقيق هذا الأمر قد يواجه صعوبات كثيرة من الناحية التشريعية لعدم وجود نصوص خاصة بذلك ، خاصة في التشريعين المصري والسعودي ، الأمر الذي يتطلب تدخلا تشريعيا لمواجهة هذه الصعوبات ، كذلك فإن تحقيق هذا الأمر قد يواجه صعوبات من الناحية العملية لعدم وجود رجل الضبط القضائي المتخصص وذو الخبرة الفنية في مثل تلك الأمور الفنية ذات التقنية العالية والمعقدة ، الأمر التي يتطلب رفع كفاءة رجل الضبط القضائي حتى يتمكن من مواجهة مثل تلك الحالات.

إلا أن الأمر قد يختلف بعض الشيء فيما يخص ضبط المراسلات والاتصالات الالكترونية كالبريد الاليكتروني والمحادثات الالكترونية حيث أن هناك أرضية مشتركة بين هذه الأنواع من الاتصالات وبين البريد العادي والمحادثات التليفونية العادية مما يتضح معه كفاية النصوص الحالية ، في التشريعين المصري والسعودي، لمواجهة تلك الإجراء المستحدث والمتمثل في **ضبط البريد الالكتروني أو مراقبة المحادثات الالكترونية**:

والمراسلات الالكترونية : ما هي إلا مراسلات ذات صبغة تقليدية من ناحية المضمون ، ولا تختلف عن المراسلات العادية إلا من حيث الوسيلة التي

تستخدم لنقلها. ففي حين أن المراسلات التقليدية تتم عن البريد العادي فإن المراسلات الالكترونية تتم عن طريق الكومبيوتر أو التليفون المحمول الذي ينقلها عن طريق شبكة المعلومات الدولية " الانترنت " ، حيث يخصص لكل شخص موقع بريد الكتروني ، Le courrier boxe Electronique ، وهذا الموقع عبارة عن ملف يستخدم لاستقبال الرسائل Les messages بواسطة معالج الرسائل Le messagerie ، وعندما يريد أي مستخدم الحصول علي الرسائل الخاصة به فإنه يستدعيها باستخدام أي وصلة طرفية " وصلة الانترنت المرتبطة بالكومبيوتر أو التليفون " ، كما يمكن له عن طريق هذه الوصلة أن يبعث رسائله إلي أي مكان في العالم باستخدام خطوط التليفون أو الموجات اللاسلكية أو الأقمار الصناعية [(١)].

والمحادثات الالكترونية : هي عبارة عن محادثات تتم عن طريق التليفون المحمول أو عن طريق الكومبيوتر ، بواسطة خطوط التليفون العادي ، مع الاستعانة بجهاز معدل الموجات والذي يعرف اختصارا بالمودم Modem ، وهو الجهاز الذي يحول الإشارات الرقمية Digitale المستخدمة بواسطة الكومبيوتر أو التليفون المحمول إلي موجات تناظرية أو تماثلية Analogue تنتقل مع الموجات الصوتية من خلال خطوط التليفون العادي أو المحمول. ولكي

(١) د/ هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، ص ٢١١ وما بعدها، د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص ٣٢١ د/ بكري يوسف،التفتيش عن المعلومات في وسائل التقنية الحديثة، بحث منشور بمجلة كلية الشريعة والقانون بدمنهور، سنة ٢٠٠٧م، ص٥٢٠.

تستطيع هذه الخطوط التليفونية المخصصة أساسا لنقل الموجات الصوتية حمل الموجات التناظرية يستخدم معدل للموجات **Modulateur** لتحويل الإشارات الرقمية إلي موجات تناظرية في محطات الاستقبال ، ومعدل أخر **Démodulateur** لتحويل الموجات التناظرية إلي موجات رقمية في محطات الإرسال.

ومما سبق يتضح أن هناك أرضية مشتركة بين الاتصالات والمحادثات الالكترونية وبين البريد العادي والمحادثات التليفونية العادية مما قد يدفعنا إلي تطبيق النصوص القانونية التقليدية ، خاصة المصرية ، لمواجهة تلك الإجراء المستحدث والمتمثل في ضبط البريد الالكتروني أو مراقبة المحادثات الالكترونية [١].

(١) د/ هلالي عبد أللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، ص ٢١١ وما بعدها.

صعوبات ضبط الكيانات المعنوية:

تواجه عملية ضبط الكيانات المعنوية والبيانات المعالجة إلكترونيا صعوبات منها [١]:

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

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

ج- يمثل التفتيش والضبط أحيانا اعتداء على حقوق الغير، أو على حرمه حياته الخاصة، فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات ولضمان الحفاظ على البيانات محل البحث ومقارنتها بالنسخة المخرجة من الجهاز في حالة جحدها 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 ٢٩ مكررا / ٣).

ووفقا للمادة ٣٩ مكررا من القانون البلجيكي يتم سحب البيانات التي سبق أخذ نسخة منها، من الجهاز في الحالات الآتية:

١- إذا كانت تمثل خطرا على الأنظمة الإلكترونية.

---

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص١٠.

٢- إذا كانت تمثل خطرا بالنسبة للمعلومات المخزنة أو المعالجة أو المرسلة بهذه الأنظمة.

٣- إذا كانت محلا للجريمة أو ناتجة عنها.

٤- إذا كانت مخالفة للنظام العام أو حسن الآداب.

كيفية تحريز المضبوطات المعلوماتية و طرق تأمينها:

نظرا للطبيعة الخاصة للبيانات و المعلومات المتاحة بالحاسب الآلي فان المحقق أو مأمور الضبط القضائي إذا لم يكن مدربا و مؤهلا على التعامل معها مدركا لنظم الحاسب الآلي فقد يغفل أو يهمل دليلا الكترونيا أو يتسبب في إتلافه و إفساده كدليل يعول عليه، لذا فانه يجب تأمينها، كما يجب بالإضافة إلى الإجراءات التي وضعها المشرع للمحافظة على سلامة المضبوطات من المنقولات عامة (م ٥٦، ٩٨، ١٩٩ إجراءات الجنائية) اتخاذ بعض الإجراءات الخاصة للحفاظ عليها و صيانتها من العبث و ذلك على النحو التالي[(١)]:

١ - ضبط الدعائم الأصلية و عدم اقتصار على ضبط نسخها.

٢ - التزام القواعد الفنية المتعلقة بكيفية نقل الأحراز المعلوماتية و حملها.

٣ - مراعاة ظروف الحرارة و الرطوبة المناسبة لتخزين الأحراز المعلوماتية.

٤ - تامين البرامج المطلوبة قبل تشغيلها.

٥ - إحكام الحلقات الإجرائية لضبط.

٦ - تمييز المادة المضبوطة.

---

(١) د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية.ص١٢٧، د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٢٥.

المبحث الرابع
الشهادة في جرائم تقنية المعلومات

يقصد بالشهادة : تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواسه [(١)]. أو هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها [(٢)].وموضوعها واقعة ذات أهمية قانونية، وقد حددها المنظم بأنها الواقعة" التي تثبت أن تؤدي إلى ثبوت الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها"، ويعني ذلك أنه لا يجوز أن يكون موضوع الشهادة رأياً أو حكماً فيما يبديه الشاهد. وللشهادة أهمية كبيرة في التحقيق الابتدائي، بل أن الاستماع للشهود يكاد يكون أهم إجراءاته: فالجريمة – في إبراز عناصرها- واقعة مادية، ومن ثم كانت الشهادة أهم دليل على ارتكابها وعلى تحديد مرتكبها[(٣)].

---

(١) د/ محمود نجيب حسني: شرح قانون الإجراءات الجنائية، ص ٤٥٢

(٢) د/عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٤٠.

(٣) وحتى يكون الشاهد أهلاً للشهادة في مدلولها القانوني فيتعين أن يكون مميزاً وحر الاختيار وألا تلحقه حالة من حالات عدم الصلاحية للشهادة كعدم جواز شهادة الموظف العام بعد تركه الخدمة عما يكون قد وصل إلى علمه أثناء قيامه بعمله من معلومات لم تنشر بالطريق القانوني (م ٦٥ من قانون الإثبات)، وكذلك المحامي والطبيب، وغيرهما عما وصل إلى علمهم من معلومات عن طريق مهنتهم ولو بعد زوال هذه الصفة ما لم يكن ذكرها لهم مقصوداً به ارتكاب جناية أو جنحة (م ٦٦ من قانون الإثبات).

وقد عدها المنظم المصري والسعودي من الأدلة التي يتطلبها التحقيق الجنائي ؛ فنصت المادة (١١٠ إجراءات مصري) على أنه: "يسمع قاضي التحقيق شهادة الشهود الذين يطلب الخصوم سماعهم ما لم ير عدم الفائدة من سماعهم. وله أن يسمع شهادة من يرى لزوم سماعه من الشهود عن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها". ونصت المادة (٩٥ إجراءات سعودي)على أنه :" على المحقق أن يستمع إلى أقوال الشهود الذين يطلب الخصوم سماع أقوالهم ما لم ير عدم الفائدة من سماعها. وله أن يستمع إلى أقوال من يرى لزوم سماعه من الشهود عن الوقائع التي تؤدي إلى إثبات الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها"

ومن خلال النصين السابقين يتضح أن هناك سلطة تقديرية واسعة للمحقق في سماع الشهود، وذلك بهدف تمكينه من انتفاء الشهود الذين يرجح أن تكون لشهادتهم أهميتها، وتمكينه بعد ذلك من سؤالهم على النحو الذي يكفل استخلاص المعلومات ذات الأهمية في التحقيق. والأصل أن يطلب الخصوم (وخاصة المتهم) سماع شهود معينين، ولكن طلب الخصم ليس شرطاً لسماع الشاهد. فللمحقق أن يستدعي من يقدر أهمية شهادته،

ويتعين كذلك في الشاهد ألا يكون فاقداً للحاسة التي يستطيع عن طريقها العلم بالواقعة محل الشهادة فمثلاً الأعمى لا يصلح شاهد رؤية إنما يصلح أن يكون شاهد سماع. د/ محمود نجيب حسني: شرح قانون الإجراءات الجنائية، ص ٤٤١ وما بعدها، وص ٦٤٥، ٦٤٦.

وله أن (يسمع شهادة أي شاهد يحضر من تلقاء نفسه). ويجوز للمحقق أن يرفض سماع الشاهد –سواء طلب الخصوم سماعه أو حضر من تلقاء نفسه– إذا رأى عدم الفائدة من سماعه

وللمحقق أن يقدر قيمة الشهادة بعد أدائها: فله أن يأخذ بها كدليل، وله أن يهدرها؛ وله أن يأخذ ببعض أقوال الشاهد دون بعض؛ وإذا تعدد الشهود وتناقضت أو تعارضت شهاداتهم فله أن يرجح بينها وفق بما يمليه عليه محض اقتناعه.

التزامات الشاهد وجزاء الإخلال بها :

يحمل الشاهد التزامات أربعة: التزامه بالحضور أمام المحقق والتزامه بحلف اليمين، والتزامه بأداء الشهادة، والتزامه بذكر الحقيقة، ولا يترك الشارع لاختيار الشاهد الوفاء بهذه الالتزامات: ذلك أنه يؤدي مهمة تتصل بسير التحقيق، وتتعلق بالمصلحة العامة للمجتمع، فإذا أحجم عن الوفاء بالالتزامات التي تتمثل فيها هذه المهمة تعطل سير التحقيق، وتعذر الفصل في الدعوى الجنائية. ولذلك يكرهه الشارع على ذلك، ووسيلته هي تجريم نكوله، وإن كان يتسامح معه فيعفيه من العقوبة إذا قدم عذراً مقولاً لنكوله أو عدل في الوقت المناسب عن امتناعه.

فبالنسبة لالتزامه بالحضور أمام المحقق نصت المادة (١١٧ إجراءات مصري) على أنه "يجب على من دعي للحضور أمام قاضي التحقيق لتأدية شهادة أن يحضر بناء على الطلب المحرر إليه، وإلا جاز للقاضي الحكم عليه بعد سماع أقوال النيابة العامة بدفع غرامة لا تتجاوز خمسين جنيهاً. ويجوز له أن يصدر أمراً بضبطه وإحضاره". وقد تقبل الشارع التنفيذ العيني لهذا

الالتزام، فأجاز إصدار الأمر بضبط الشاهد وإحضاره إذا كان قد تخلف فحكم عليه بالغرامة. وقد أعقب الشارع ذلك بأن قرر أنه "إذا حضر الشاهد أمام القاضي بعد تكليفه بالحضور ثانياً أو من تلقاء نفسه وأبدى أعذاراً مقبولة، جاز إعفاؤه من الغرامة بعد سماع أقوال النيابة العامة، كما يجوز إعفاؤه بناء على طلب يقدم منه إذا لم يستطع الحضور بنفسه" (المادة ١١٨ إجراءات).

وبالنسبة لالتزام الشاهد بحلف اليمين والتزامه بأداء الشهادة نصت المادة (١١٩ إجراءات مصري) على أنه "إذا حضر الشاهد أمام القاضي وامتنع عن أداء الشهادة أو عن حلف اليمين، يحكم عليه القاضي في الجنح والجنايات بعد سماع أقوال النيابة العامة بغرامة لا تزيد على مائتي جنيه. ويجوز إعفاءه من كل أو بعض العقوبة إذا عدل عن امتناعه قبل انتهاء التحقيق".

ولم يتضمن نظام الإجراءات السعودي أي نص يوجب على الشاهد الالتزام بأداء الشهادة أمام المحقق، بينما نجده ألزم الشاهد بالحضور خلال مرحلة المحاكمة في المادة(١٦٦إجراءات)، والتي تنص على أنه:" مع مراعاة ما تقرر شرعاً في الشهادة بالحدود، يجب على كل شخص دعي لأداء الشهادة بأمر من القاضي الحضور في الموعد والمكان المحددين"

ولكن المادة (٢٤) من مشروع اللائحة التنظيمية لنظام هيئة التحقيق والادعاء العام ألزمت الشاهد بالحضور أمام المحقق للإدلاء بشهادته غير أنها لم تقرر أية عقوبة على امتناعه؛ إذ نصت على انه:" يلتزم من يدعى للشهادة

بالحضور أمام المحقق في الزمان والمكان المحددين، وإذا امتنع دون عذر مقبول جاز للمحقق الأمر بإحضاره".

ولذا فإنني أوصي مع البعض[١]. بتدخل المنظم السعودي لإيجاد نص يلزم الشاهد بالحضور للإدلاء بالشهادة أثناء مرحلة التحقيق الابتدائي أمام السلطة المختصة به، وأن توقع عليه عقوبة مناسبة إذا امتنع عن ذلك.

ومن الملاحظ أن الأشخاص الذين يتعاملون مع الوسائل الإلكترونية بحكم طبيعة عملهم لا يعتبرون شهودا وفقا لمدلول الشهادة كدليل إثبات في المواد الجنائية، والتي يقصد بها المعلومات الصادرة من شهود يكونوا قد شاهدوا بأبصارهم الجريمة لحظة وقوعها أو قد تجمعت لديهم أدلة تفيد في إثبات وقوعها، ولكن الشاهد في الجريمة المعلوماتية هو ذلك الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة 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 تمييزا له عن الشاهد التقليدي[٢].

---

(١) د/ ممدوح رشيد العنزي، ضمانات المتهم أثناء مرحلة التحقيق الابتدائي في النظام السعودي، ص ٢٤٨.

(٢) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: **g.com٤٤http://www.f**

ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها[١]:

١. القائم على تشغيل الحاسب الآلي: وهو المسئول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به 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.

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

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

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

---

(١) د/ عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٤١.

٣. 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 سمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

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

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

ويحصل قانون الدليل الخاص بولاية كاليفورنيا شهود الجريمة المعلوماتية في: محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي أنتج الدليل. المبرمج الذي قام بتحرير البرنامج واختباره. المشغل الذي يقوم بتشغيل البرامج. طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة). أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة. مهندس الصيانة الالكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة. موظفو المدخلات والمخرجات والمسئولون عن معالجة المدخلات المستخدم في تنفيذ برامجه. المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها.

التزامات الشاهد المعلوماتي:

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

هناك اتجاهان في هذا الصدد[1]:

الاتجاه الأول: ويرى 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 الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.

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

الاتجاه الثاني : ويرى 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 الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد ٦٢، ١٠٩، ١٣٨ من قانون الإجراءات الجنائية الفرنسية)

---

(١) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٣٤،وما بعدها، د/ عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات،٤٢.

ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة.

وفي هولندا يتيح مشروع قانون الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.

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

ولا شك في أن وجود الالتزام القانوني الذي بموجبه يمكن مطالبة المهنيين والحرفيين من الشهود ومستخدمي الوسائل الإلكترونية بالإعلام عن المعلومات والبيانات الجوهرية التي في حوزتهم، ليمثل أهمية عظيمة في إمكانية جمع الأدلة التي ترتكب على هذه الوسائل، وأنه يلعب دورا وقائيا هاما إذ أن تطبيقه يمكن من ضبط النظام الشبكي بأكمله وعدم عزله عن البيئة المعلوماتية المحيطة به[1].

---

(١) د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، منشور على موقع: http://www.f٤٤g.com

المبحث الخامس
الخبرة في جرائم تقنية المعلومات

الخبرة هي إبداء رأي فني من شخص مختص فنيا في شأن واقعة ذات أهمية في الدعوى الجنائية، والخبير هو كل شخص له إلمام خاص بأي علم أو فن[١]. وقد يتطلب التحقيق الاستعانة بخبير متخصص، والقانون أباح ذلك للمحقق من تلقاء نفسه أو بناء على طلب الخصوم[٢].

والأصل في الخبرة أنها من إجراءات التحقيق الابتدائي، ونصت عليها المواد ٨٥-٨٩ من قانون الإجراءات الجنائية المصري (٣). والمواد (٧٦- ٧٨)

---

(١) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ص٤٧٤.

(٢) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٤٠.

(٣) تنص المادة (٨٥ إجراءات مصري) على أنه :" إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء يجب على قاضى التحقيق الحضور وقت العمل وملاحظته وإذا أقتضى الأمر إثبات الحالة بدون حضور قاضى التحقيق نظرا إلى ضرورة القيام بأعمال تحضيرية أو تجارب متكررة أو لأي سبب أخر وجب على قاضى التحقيق أن يصدر أمرا يبين فيه أنواع التحقيقات وما يرد إثبات حالته. ويجوز في جميع الأحوال أن يؤدى الخبير مأموريته بغير حضور الخصوم" وتنص المادة (٨٦ إجراءات مصري) على أنه :" يجب على الخبراء أن يحلفوا أمام قاضى التحقيق يمينا على أن يبدوا رأيهم بالذمة وعليهم أن يقدموا تقريرهم كتابة". وتنص المادة (٨٧ إجراءات مصري) على أنه :" يحدد قاضى التحقيق ميعادا للخبير ليقدم تقريره فيه وللقاضي أن يستبدل به خبيرا أخر إذا لم يقدم التقرير في الميعاد المدد". وتنص المادة (٨٨ إجراءات مصري) على أنه :" للمتهم أن يستعين

إجراءات سعودي[١]. كما يستعان بالخبرة في مرحلة جمع الاستدلالات ؛ فلمأمور الضبط القضائي الاستعانة بالخبراء و الاستماع إلى تقاريرهم الشفوية أو الكتابية (م٢٩ إجراءات مصري، م ٢٨ إجراءات سعودي)[٢]. و يصح

بخبير استشاري ويطلب تمكينه من الإطلاع على الأوراق وسائر ما سبق تقديمه للخبير المعين من القاضي على ألا يترتب على ذلك تأخير السير فلا الدعوى ". وتنص المادة (٨٩ إجراءات مصري) على أنه :" - للخصوم رد الخبير إذا وجدت أسباب قوية تدعو لذلك ويقدم طلب الرد إلى قاضى التحقيق للفصل فيه، ويجب أن تبين بفيه أسباب الرد، وعلى القاضي الفصل فيه في مدة ثلاثة أيام من يوم تقديمه. ويترتب على هذا الطلب عدم استمرار الخبير في عمله إلا في حالة الاستعجال بأمر من القاضي".

(١) تنص المادة (٧٦ إجراءات سعودي) على أنه :" للمُحقِّق أن يستعين بخبير مُختص لإبداء الرأي في أيِّ مسألة مُتعلِقة بالتحقيق الذي يُجريه." وتنص المادة (٧٧ إجراءات سعودي) على أنه :" على الخبير أن يُقدِّم تقريرُه كِتابة في الموعِد الذي حُدِّد من قِبل المُحقِّق، وللمُحقِّق أن يستبدِل به خبيراً آخر إذا لم يُقدَّم التقرير في الميعاد المُحدَّد لهُ أو وجِد مُقتضى لذلك. ولكُلِ واحِد من الخصوم أن يُقدِّم تقريراً من خبير آخر بصِفة استشارية". وتنص المادة (٧٨ إجراءات سعودي) على أنه :" للخصوم الاعتِراض على الخبير إذا وجِدت أسباب قوية تدعو إلى ذلك، ويُقدَّم الاعتِراض إلى المُحقِّق للفصل فيه، ويجب أن يُبيِّن فيه أسباب الاعتِراض، وعلى المُحقِّق الفصل فيه في مُدة ثلاثة أيام مِن تقديمُه. ويترتب على هذا الاعتِراض عدم استِمرار الخبير في عملِه، إلا إذا اقتضى الحال الاستِعجال، فيأمُر المُحقِّق باستمرارِه".

(٢) تنص المادة (٢٩ إجراءات مصري) على أنه :" لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يسمعوا أقوال من يكون لديه معلومات عن الوقائع الجنائية

للمحكمة طبقا للمادة ٢٩٢ من قانون الإجراءات الجنائية المصري، والمادة ١٧٢ إجراءات سعودي[1]. أن تندب خبيرا أو أكثر متى رأت وجها لذلك، وحق المحكمة في ندب الخبير في غنى عن نص يقرره، فهو نتيجة حتمية لواجبها في تحرى الحقيقة في شان الوقائع ذات الأهمية في الدعوي الجنائية، أي الوقائع التي تتصل بوقوع الجريمة و نسبتها إلى المتهم، بل إن نطاق الخبرة

ومرتكبها وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهيا أو بالكتابة. ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما عد سماع الشهادة بيمين". وتنص المادة (٢٨ إجراءات سعودي) على أنه :" لرِجال الضبط الجنائي في أثناء جمع المعلومات، أن يستمِعوا إلى أقوال من لديهم معلومات عن الوقائع الجنائية ومُرتكِبيها، وأن يسألوا من نُسِب إليه ارتِكابُها ويُثبِتوا ذلك في محاضِرِهم. ولهُم أن يستعينوا بأهل الخِبرة من أطِباء وغيرِهم، ويطلبوا رأيهُم كتابة".

(١) تنص المادة (٢٩٢ إجراءات مصري) على أنه :" للمحكمة سواء من تلقاء نفسها، أو بناء على طلب الخصوم أن تعين خبيرا واحدا أو أكثر في الدعوى". وتنص المادة (١٧٢ إجراءات سعودي) على أنه :" للمحكمة أن تندُب خبيراً أو أكثر لإبداء الرأي في مسألة فنية مُتعلِقة بالقضية. ويُقدِّم الخبير إلى المحكمة تقريراً مكتوباً يُبيِّن فيه رأيُه خِلال المُدة التي تُحدِّدُها لهُ، وللخصوم الحصول على صورة من التقرير. وإذا كان الخصوم أو الشهود أو أحد مِنهُم لا يفهم اللُّغة العربية، فعلى المحكمة أن تستعين بمُترجمين. وإذا ثبت أن أحداً من الخُبراء أو المُترجمين تعمد التقصير أو الكذِب، فعلى المحكمة الحُكم بتعزيره على ذلك".

يمتد إلى تحديد مدى مسئولية المتهم ومدى جدارته بالعقوبة أو التدبير الاحترازي[١].

وفي مجال الجريمة المعلوماتية نصت المادة (١٤) من نظام مكافحة جرائم المعلوماتية السعودي على أنه :" تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة ".

ويجب على الخبراء أن يحلفوا يميناً أمام المحقق على أن يبدوا رأيهم بالذمة (م٨٦). وهذه هي يمين الخبرة، ويترتب على إغفالها بطلان الحكم الذي يبنى على تقرر الخبير. وقد قضى بأن هذا البطلان ليس من النظام العام فلا يجوز إبداؤه لأول مرة أمام محكمة النقض [٢]. ولا محل ليمين الخبرة إذا كان الخبير قد سبق له الحلف عند تقريره أمام المحاكم، أو عند بدء ممارسته مهنته، كالطبيب الشرعي [٣]، وإذا دعي الخبير للشهادة تعين عليه أن يحلف يمين الشهادة وشأن المترجم شأن الخبير في ذلك.

ويعد استعانة الجهات القائمة بالتحري و التحقيق و الحكم بالخبراء حين تتعامل مع جرائم الحاسبات ضرورة لاغني عنها نظرا للطابع الفني الخاص لأساليب ارتكابها و الطبيعة غير المادية لمحل الاعتداء، و يقرر البعض أن نجاح أو فشل الادعاء العام في مثل هذه النوعية من الجرائم يرتهن بدرجة التخصص الفني لهؤلاء الخبراء و مسلكهم حينما يناقشون أمام القضاء كشهود

---

(١) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ص٤٧٥.

(٢) نقض ١/ ٣/ ١٩٣٧ القواعد القانونية، جـ٤، رقم ٥٣، ص٥٢، ٣٠/ ١٢/ ١٩٤٦، جـ٥، رقم ١٧٨، ص٣٢٧، ٢٣/ ٣/ ١٩٤٩ المحاماة ص٣٠، رقم٦٨، ص٦٨.

(٣) نقض ١/ ١٢/ ١٩٥٢ م أحكام النقض، س٤، رقم ٦٠، ص١٧٦.

، و لذلك فان اختيار خبراء على درجة عالية من التخصص و الكفاءة يعد ضرورة حيوية في هذه الأحوال[١].

وفي واقع الأمر فإنه منذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، 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؛ 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 دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيبا مستوجبا نقضه، وهذا المبدأ استقر عليه قضاء محكمة النقض المصرية[٢].

وبناء عليه فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي، فهي أوجب في مجال الجرائم الإلكترونية، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير

---

(١) د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٤٠.وقد أشار إلى:

Jack, Bologna. corporate, fraud the basics of prevention and detection, butterworth publisher, 1984, p.7

(٢) نقض ٢١/ ٣/ ١٩٦٥ مجموعة القواعد القانونية رقم ٥٢ ص٣١، نقض ٢٢/ ٦/ ١٩٧٧، مجلة المحامون سنة ٤٢، رقم ٧٥٩، ص٥٨٣.

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 مماثلين.

وأهمية الاستعانة بالخبير في مجال الجرائم الإلكترونية، تظهر عند غيابهِ، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقق عن جميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل او الإهمال عند التعامل معه.

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 بالحاسب الحالي، فقد يتعلق الأمر بتزوير المستندات، أو بالتلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من جرائم الأموال أو الاعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة[1].

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية، القانون البلجيكي الصادر في ٢٣ نوفمبر سنة ٢٠٠٠ م؛ فقد نصت المادة ٨٨ من القانون المذكور على انه يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة او المعالجة

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٥، د/ سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٤٢.

أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة للتحقيق إن 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.

ووفقا للقانون المشار إليه 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، او عند الرضاء بعملية التفتيش هذه.

فمهمة الخبير وفقا للنص 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 **disq** أو على سيد يروم **CD-ROM**، أو على الأقراص الممغنطة، أو على ورق.

والتزام الخبير هو التزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، ويمكن أن تثور مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمدا البيانات المطلوب منه التعامل معها، أو حفظها. وفضلاً 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[1].

(١) د/ محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٦.

وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي[١]:

١ - وصف تركيب الحاسبات وصناعته وطرازه ونوع نظام التشغيل واهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير...الخ.

٢ - وصف طبيعة بيئة الحاسب أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها.

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

٤ - وصف أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام.

٥ – بيان كيف يمكن عند الاقتضاء عزل النظام ألمعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

---

(١) د/عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، ص٦، د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) ص٣٤٢، ٣٤٣، د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد بتاريخ ٢٦ - ٢٨نيسان ٢٠٠٣ م بمركز البحوث والدراسات بأكاديمية شرطة دبي، عدد رقم: ١ سنة : ٢٠٠٣ م، منشور على موقع: **g.com٤٤http://www.f**

٦ - بيان كيف يمكن عند الاقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير أن يلحقها تلف.

٧ – بيان 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 الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة.

المبحث السادس
استجواب المتهم ومواجهته في جرائم تقنية المعلومات

الاستجواب: إجراء من إجراءات التحقيق يتثبت المحقق بمقتضاه من شخصية المتهم ويناقشه في التهمة المنسوبة إليه على وجه مفصل في الأدلة القائمة في الدعوى إثباتا ونفيا(١).

والاستجواب بهذا المعنى يتميز عن سؤال المتهم الذي يقوم به مأمور الضبط القضائي، ويعد إجراء من إجراءات الاستدلال، إذ يقتصر على مجرد سؤال المتهم عن التهمة المنسوبة إليه ومطالبته بالرد على ذلك وإبداء ما يشاء من أقوال في شأنها، دون أن يناقشه تفصيلاً أو يواجهه بالأدلة القائمة ضده (٢).

ومن ثم فإن الاستجواب قُصد به أمران : الأول : أنه طريق دفاع لينفذ الأدلة القائمة ضده فيتمكن من تبرير تصرفاته، والآخر : أنه وسيلة تحقيق لاستجلاء الحقيقة والوصول إلى معرفة مرتكب الجريمة.

ولما كان هذا هو المقصد من الاستجواب فإنه ينبغي أن لا يكون طريق إكراه لانتزاع اعتراف من المتهم، كما لا يجوز تحليفه عند استجوابه لأنه يؤدي إلى وضعه في مركز حرج ويؤدي إلى بطلان الاستجواب (٣).

---

(١) د/ محمد سامي النبراوي، استجواب المتهم، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ١٩٦٨م، ص٣٥.

(٢) د/ فوزية عبد الستار : شرح قانون الإجراءات الجنائية، ص٣٥٢..

(٣) تنص المادة ٣٠٢/ ٢ من قانون الإجراءات الجنائية المصري على أنه:" . .... وكل قول يثبت أنه صدر من أحد المتهمين أو الشهود تحت وطأة الإكراه أو التهديد

مدى وجوب الاستجواب :

الأصل هو جواز استجواب المتهم في التحقيق الابتدائي. أما في التحقيق النهائي الذي يجري أثناء المحاكمة فهو ممنوع بحسب الأصل إلا إذا قبله المتهم (م ٢٧٤ إجراءات مصري). وله في الحالتين رفض الإجابة على ما قد يوجه إليه من أسئلة، ولا يجوز أن يعد امتناعه هذا قرينة ضده، وإذا تكلم المتهم فإنما ليبدي دفاعه، ومن حقه دون غيره أن يختار الوقت والطريقة التي يبدي بها هذا الدفاع. فلا يصح أن يتخذ من امتناع المتهم عن الإجابة قرينة على ثبوت التهمة [(١)].

والأصل أن الاستجواب يكون في أي وقت خلال مرحلة التحقيق ولم يحدد له وقتاً معيناً لإجرائه إلا أن التشريع المصري والسعودي قد أوجب استجواب المتهم أثناء التحقيق الابتدائي في أحوال معينة، كما في حالة كون المتهم مقبوضاً عليه؛ فقد أوجبا على المحقق أن يستجوب فوراً المتهم المقبوض عليه ؛ فتنص المادة (١٣١ إجراءات مصري) على أنه:" يجب على قاضي التحقيق أن يستجوب فورا المتهم المقبوض عليه وإذا تعذر ذلك يودع في السجن إلى حين استجوابه ويجب ألا تزيد مدة إيداعه على أربع وعشرين ساعة فإذا مضت هذه المدة وجب على مأمور السجن تسليمه إلى النيابة

به يهدر ولا يعول عليه". وتنص المادة ١٠٢ من نظام الإجراءات الجزائية السعودي على :" يجب أن يتم الاستِجواب في حال لا تأثير فيها على إرادة المُتهم في إبداء أقوالِه، ولا يجوز تحليفُه ولا استِعمال وسائل الإكراه ضِدَه. ولا يجوز استِجواب المُتهم خارِج مقر جِهة التحقيق، إلا لضرورة يُقدِرُها المُحقِّق".

(١) نقض ١٧/ ٥/ ١٩٦٠، أحكام النقض، س١١، رقم ٩٠، ص٤٦٧.

العامة، وعليها أن تطلب فى الحال إلى قاضى التحقيق استجوابه. وعند الاقتضاء تطلب ذلك إلى القاضي الجزئي أو رئيس المحكمة أو أي قاضى أخر يعينه رئيس المحكمة وإلا أمرت بإخلاء سبيله" وتنص المادة (٣٤ إجراءات سعودي) على أنه :" يجب على رجل الضبط الجنائي أن يسمع فوراً أقوال المتهم المقبوض عليه، وإذا لم يأت بما يبرئه يرسله خلال أربع وعشرين ساعة مع المحضر إلى المحقق الذي يجب عليه أن يستجوب المتهم المقبوض عليه خلال أربع وعشرين ساعة، ثم يأمر بإيقافه أو إطلاقه"

وفي حالة حضور المتهم لأول مرة في التحقيق؛ فقد أوجبا على المحقق، عند حضور المتهم لأول مرة في التحقيق أن يتثبت من شخصيته ثم يحيطه علماً بالتهمة المنسوبة إليه ويثبت أقواله في (م ١٢٣ إجراءات مصري، م ١٠١ إجراءات سعودي) [(١)] وفي حالة الحبس الاحتياطي؛ فأوجبا استجواب المتهم عند حبسه احتياطياً (م ١٣٤/ ١ إجراءات، م ١١٣ إجراءات سعودي).

المواجهة:

مواجهة المتهم بغيره هي وضعه وجهاً لوجه إزاء متهم آخر أو شاهد أو أكثر كيما يسمع بنفسه ما قد يصدر منهم من أقوال في صدد ما أدلوا به من معلومات متعلقة بواقعة أو أكثر فيتولى الإجابة تأييداً أو تفنيداً.

---

(١) د/ فوزية عبد الستار : شرح قانون الإجراءات الجنائية، ص٣٥٣. وانظر نقض ٢٥/ ٤/ ١٩٧١، مجموعة أحكام محكمة النقض، س٢٢، رقم ٩١، ص ٣٧٢.

وهي تشبه الاستجواب في أنها تتضمن معنى المواجهة بدليل أو بأدلة قائمة قبله، كما هو الشأن في هذا الأخير، لكنها تختلف عنه لأنها مقصورة على المواجهة بشاهد واحد أو أكثر فحسب، وبالنسبة لواقعة واحدة أو أكثر. والمواجهة كالاستجواب قد تدفع المتهم إلى الاعتراف أو إلى تقرير ما ليس في صالحه –إن صدقا أو كذبا– لذا أحاطها القانون بنفس الضمانات التي أحاط بها الاستجواب.

ومجرد حضور المتهم أثناء سماع شاهد أو متهم آخر غيره لا يعد مواجهة، حتى لو سأله المحق عما إذا كانت لديه ملاحظات على أقوال هذا الأخير. ما دام ذلك في حدود الاستفهام الإجمالي، ودون ما استرسال في المجابهة بالأدلة ومناقشته فيها. وإلا لأصبح الأمر استجواباً صريحاً. وفي الواقع لا توجد حدوداً فاصلة بين الأمرين، ولعل هذا هو الاعتبار الذي حدا بالتشريع إلى الجمع بينهما في ضمانات مشتركة[1].

ولا يختلف الاستجواب والمواجهة بالنسبة للمتهم وكذا جهة التحقيق من حيث حقيقته وضماناته في حالة التحقيق في الجرائم التقليدية عنه في جرائم تقنية المعلومات؛ لأنه يتعلق بالمتهم ذاته ولا يتعلق بطبيعة الجريمة.

---

(١) د/ رؤوف عبيد، مبادئ الإجراءات الجنائية،ص ٤٦١ وما بعدها، د/ محمد سامي النبراوي، استجواب المتهم، ص٣٦، د/ زكى محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، ص٢٠٠.

الفصل الرابع
معوقات التحقيق في جرائم تقنية المعلومات

التحقيق في الجرائم المتعلقة بالإنترنت وملاحقة مرتكبيها جنائياً يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق، بل يمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضاً على المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه، الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشد ضرراً على المجتمع المحلي أو المجتمعات الأخرى[(١)]. ومن أهم المعوقات التي قد تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق فيها: عوائق تتعلق بالإحجام عن الإبلاغ عن الجريمة، وعوائق تتعلق بعدم توافر الكفاءة البشرية المؤهلة للتحقيق، وعوائق تتعلق بخفاء الجريمة المعلوماتية، وغياب الدليل المرئي، وعوائق تتعلق بصعوبة التعاون الدولي في مكافحة الجريمة المعلوماتية[(٢)]. وسوف أتناوله بشيء من التفصيل في المباحث التالية:

---

(١) عبد الرحمن بحر: معوقات التحقيق في جرائم الإنترنت "دراسة مسحية على ضباط الشرطة بدولة البحرين: رسالة ماجستير: جامعة نايف العربية للعلوم الأمنية، الرياض ١٩٩٩م، ص ٥١، سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض٢٠٠٣، ص ١١٣.

(٢) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص ١٩،محمد بن نصير محمد السرجاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص ٨١ وما بعدها.

المبحث الأول
الإحجام عن الإبلاغ عن الجريمة

الإحجام عن الإبلاغ: من أهم وأخطر المشكلات التي تتعلق بكشف جرائم الإنترنت، حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم، خاصة المؤسسات والشركات التجارية، حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم. ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت ١٢٧ من العاملين في مجال التحقيق في جرائم الحاسوب والإنترنت يمثلون ١١٤ وكالة رسمية، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسوب والإنترنت التي يتم اكتشافها لا يبلغ عنها للشرطة. كما توصلت دراسة أخرى أجراها معهد أمن الحاسوب CSI بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي ٧٠٪ من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها لسلطات إنفاذ العدالة.

ويمكن أن يعزي إحجام البعض عن الإبلاغ لعدة أسباب[١]:

- عدم إدراك الأفراد أو مدراء الأنظمة الحاسوبية ومسئولي الشركات أن مثل هذه الأفعال والهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دولياً.

---

(١) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص٢٠،محمد بن نصير محمد السرجاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، ص ٨١ وما بعدها.

- خوف الجهات التي وقعت عليها الجرائم[١]، خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعاً بإهمالها أو قلة خبرتها أو عدم وعيها الأمني[٢]، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي قد ينعكس سلباً على أرباحها وقيمة أسهمها[٣].

- خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق إلى احتجاز حواسبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة

---

(١) وهناك عوائق تتعلق بالجهات المتضررة : كعدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معوقات التحقيق، وإغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بشبكة الإنترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، على سبيل المثال مستخدمو شبكة الإنترنت عبر مزودي الخدمة أو بطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم "عملية ربط رقم المستخدم مع هويته" عند الاشتراك في خدمة الإنترنت، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة. باسم الحمادي: إثبات جرائم الإنترنت صعب، بحث منشور على شبكة الإنترنت بتاريخ ٧ محرم ١٤٢٣هـ على موقع: **www.alrvada.com.sa**

(٢) طارق عبد الله الشدي: آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض ١٤٢٣هـ، ص ٢١٠.

(٣) باسم الحمادي، إثبات جرائم الإنترنت صعب، ص ٢٣.

خسائرها المالية جراء التحقيق، عطفاً على ما قد تسببت الجريمة خسارتها أصلاً.

- بعض الضحايا قد تساوره الشكوك حول مقدرة رجال إنفاذ القانون على التعامل مع هذا النوع المستحدث من الجرائم.

- الرغبة في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلاً[1].

- قد تكون بعض هذه الجرائم محدودة الأثر، مما يدفع بعدم الإبلاغ عنها، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية، أو يقوم مجرم آخر بإرسال فيروس حاسب آلي إلى جهاز المستفيد ويكون هذا الفيروس محدود الأثر، أو تقوم برامج الحماية من الفيروسات بالقضاء عليه.

- قد يكون الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي. فقد يحرم الموظف في الجهة من خدمات معينة على الإنترنت أو قد يحرم من خدمات الإنترنت عموماً حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها.

- عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة إنها ممكن أن تحدث في مؤسسته.

---

(١) د/ زكي أمين حسونة: جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، ص ٤٧٦.

المبحث الثاني
عدم توفر الكفاءة البشرية المؤهلة للتحقيق

من العوائق التي تتعلق بجهات التحقيق عدم توفر الكفاءة البشرية المؤهلة للتحقيق؛ فهناك معوقات ترجع إلى شخصية المحقق، مثل التهيب من استخدام الحاسب الآلي والتهيب من استخدام شبكة الإنترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

وهناك معوقات تتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، ونقص المهارة في استخدام الحاسب الآلي والإنترنت، وعدم توفر المعرفة بأساليب ارتكاب جرائم الحاسب الآلي والإنترنت، وقلة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت والمعرفة باللغة الإنجليزية[1]. سيما وإن للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، وليس هذا فحسب بل أختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة متطورة ومتجددة.

ومن أجل ذلك فإنه لابد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم أسلوب يجمع بين الخبرة الفنية والكفاءة المهنية ومن الممكن حيال ذلك إتباع الخطوات التالية[2].

---

(١) سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، ص ١١٩.

(٢) د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت،ص ٢٠، محمد بن نصير محمد السرجاني، مهارات التحقيق الجنائي الفني

أ - تبادل المعلومات بين المحقق وخبير الحاسب الآلي وذلك قبل البدء في التحقيق وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلائها من الأشخاص. وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معانيها ليتم الاستفادة منها عند الضرورة.

ب - يتم حصر النقاط المطلوب استجلائها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

ج - يتم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي تتم الاتفاق عليها مسبقاً قبل بدء التحقيق.

د - التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه. مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه.

ولضمان نجاح التحقيق في الجرائم المعلوماتية فهناك بعض القواعد التي ينبغي مراعاتها أهمها:

أ - تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها أو أن الأدلة اللازمة لاكتشافها وإثبات التهمة قد قضي عليها.

في جرائم الحاسوب والإنترنت، ص ٨١ وما بعدها، د/ محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، ص ٧٣.

ب - ضرورة مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها.

ج - مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغيرها من الحقوق.

د - العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها.

هـ - مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدا، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.

و - الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية، ولا سيما وأن هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الإتهامية وتحليل القرائن واستنتاج الحقائق.

المبحث الثالث
خفاء الجريمة وغياب الدليل المرئي

من العوائق التي تتعلق بالجريمة : خفاء الجريمة وغياب الدليل المرئي، وافتقاد أكثر الآثار التقليدية، وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها؛ وذلك لسهولة محو الدليل أو تدميره في زمن قصير جداً فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، وبالتالي تنصله من مسئولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة[1].

---

(١) من الأمثلة على ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة. لمزيد من التفاصيل انظر الدكتور/ هشام محمد فريد رستم: الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"، ص ٤٣٠.

وفي واقعة مماثلة حدثت وقائعها بدولة الإمارات العربية المتحدة تتمثل في قيام مشغل حاسب آلي بتهديد المؤسسة التي يعمل بها لتنفيذ مجموعة من المطالب وذلك بعد أن قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة. وإزاء رفض المؤسسة الاستجابة لمطالبه أقدم على الانتحار مما سبب صعوبة بالغة في استرجاع

ويعزز ذلك الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها، وإمكانية خروجها عن نطاق

إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية، بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بشبكة الإنترنت من قبل بعض الأطراف المعينة[1].

البيانات التي كان قد حذفها. انظر، خالد الستاني، أمن المعلومات وتحليل المخاطر، ورقة عمل مقدمة إلى ندوة فيروسات الحاسب التي عقدها معهد التنمية الإدارية بالمجمع الثقافي بإمارة أبو ظبي بدولة الإمارات العربية المتحدة في ٢٣/ ٩/ ١٩٩٦م.

(١)عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت، ص ٤٦، سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، ص ١١٤.

المبحث الرابع
صعوبة التعاون الدولي في مكافحة الجريمة المعلوماتية

التطور التكنولوجي في مجال الحاسبات وبرامجها وشبكات الاتصال، وخاصة شبكة الانترنت جعل الإنتاج الذهني يتصف بالعالمية لأنه لا يقتصر على دولة دون أخرى ؛ فالبشرية كلها شريكة في الاستفادة من هذا الإنتاج الأدبي والذهني[١].

وبعد أن ربطت الانترنت العالم بشبكة اتصال متميزة و فعالة من خلال الأقمار الصناعية و الفضائيات، وجعلت الانتشار الثقافي وعولمة الثقافة و الجريمة أمراً ممكناً و شائعاً.و قربت شعوب العالم بأجناسهم و ثقافتهم المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال. واستخدام هذه الشبكة أدى إلى سلبيات تمثلت في انتشار الجريمة، وأصبحت الجرائم المستحدثة و المنتشرة بواسطة الإنترنت مشكلة عالمية لا تعترف بالحدود الجغرافية للدول؛ لارتباط العالم بشبكة واحدة، فغالباً ما يكون الجاني في بلد و المجني عليه في بلد آخر،كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه.وهذا ملاحظ من خلال نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي[٢].

وبذلك أعطى انتشار شبكة الانترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان

---

(١) د/ محمود عبابنة، جرائم الحاسوب، ص٣٣.

(٢) الجرائم المعلوماتية ونظام مكافحتها في المملكة العربية السعودية بحث منشور على موقع: **http://www.f44g.com**

والمكان، ونتج عن ذلك أن الاستخدام غير الشرعي الناجم عن الاتصال بالحاسوب أيضاً اتصف بالعالمية أو بالعابر للحدود [١].

ومن أمثلة ذلك أن يقوم بعض الجناة بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية ومستهدفين عدم إمكان الوصول إليها، وفي هذه الحالة فإن تفتيش هذه الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.

ولمواجهة هذه الحالة ؛ يرى جانب من الفقه أن هذا التفتيش الإلكتروني العابر للحدود لا يجوز في غياب اتفاقية دولية بين الدولتين تجيز هذا الامتداد، أو على الأقل الحصول على إذن الدولة الأخرى. وهذا يؤكد أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال

الإلكتروني. ومع ذلك فقد أجازت المادة ٣٢ من الاتفاقية الأوروبية التي أعدها المجلس الأوروبي في صيغتها النهائية في ٢٥ مايو سنة ٢٠٠١ إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها، وذلك في حالتين :

أ- إذا تعلق بمعلومات أو بيانات مباحة للجمهور.

ب- إذا رضي صاحب او حائز هذه البيانات بهذا التفتيش.

ومع ذلك فإن تطبيق هذا النص يمكن أن يثير مشكلات جمة، ولا مناص من التعاون الدولي في هذا المجال بمقتضى اتفاقية ثنائية أو متعددة

---

(١) د/ محمود عبابنة، جرائم الحاسوب، ص٣٤.

الأطراف، أو على الأقل الحصول على إذن الدولة التي يتم التفتيش في مجالها الإقليمي.

ولقد أدرك المجلس الأوروبي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية في أكثر من دولة فأصدر التوصية رقم ٩٥١٣R والتي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود.

وبناءاً على ما سبق فإن التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، والأمن والتحقيق وتسليم المجرمين وتنفيذ الأحكام يعد ضرورة لا مفر منه[١]. إلا أن هناك صعوبات تعوق مثل هذا التعاون كعدم وجود اتفاق حول مفهوم هذه الجريمة، وعدم التنسيق بين قوانيين الإجراءات الجنائية بالنسبة لإجراءات التحري أو التحقيق، وعدم وجود معاهدات لتسليم المجرمين وتنفيذ الأحكام[٢].

---

(١) د/ محمد أبو العلا عقيدة،التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص٢، ٣.، د/ نبيله هبة هروال، الجوانب الإجرائية في مرحلة جمع الاستدلال، ص ١٣، د/ عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، ص ١.

(٢) د/ سليمان فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، ص٣٤٧.

الخاتمة

في ختام هذا البحث أشكر الله سبحانه وتعالى جزيل الشكر وخالصه على أن وفقني ويسر لي أداء هذا البحث.

ولقد تناولت في هذا البحث دراسة الموضوعات المتعلقة بالطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق الجنائي في النظام الجزائي المصري والسعودي.

ولقد تبين لي من خلال هذه الدراسة النتائج والتوصيات التالية:

أولاً: نتائج البحث:

- إن جرائم المعلومات لها طبيعة خاصة؛ وتختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الالكترونية أو بواسطتها، كما يسهل ارتكابها عبر الحدود، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة.
- أنها جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، توجه للنيل من الحق في المعلومات ، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت .
- أنها كما تطال الحق في المعلومات ، تمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري..

- أن التعريف الراجح في نظري لهذه الجريمة هو أنها :"سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية محله معطيات الكمبيوتر"
- أنها جرائم بالغة الخطورة ولها أضرار بالغة ، كما أنها عابرة للحدود، وهي بذلك تشترك مع بعض الجرائم الأخرى كالإرهاب، والاتجار بالمخدرات، وغسيل الأموال؛ فقد قدر الخبراء في أحد المؤتمرات أن حجم الخسائر الناجمة عن الجرائم الإلكترونية في العالم سنويا بنحو تريليون دولار، في حين تخسر أمريكا ١٠ مليارات دولار سنويا، وبينوا أن عدد الجرائم التي ترتكب يوميا ألف جريمة وقدروا خسائر الجرائم الإلكترونية في دول مجلس التعاون الخليجي بمعدل سنوي يتراوح بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا.
- أن هناك قصور تشريعي في بعض البلدان العربية التي تتصدي لهذا النمط من الجرائم ، الأمر الذي يستدعي أن يسارع المشرع في هذه البلاد لسن تشريعات جديدة أو تعديل التشريعات القائمة حتى تلائم في تطبيقها ثورة الاتصالات المعلوماتية التي تحياها البشرية بالشكل الذي يجعلها كفيلة بحماية النظام ألمعلوماتي ومكافحة الإجرام الناشئ عن استخدامه أو الواقع عليه
- أنه في سبيل مكافحة الجريمة المعلوماتية أصدر المشرع المصري قانون خاص للاتصالات (رقم١٠ / ٢٠٠٣م) لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكتروني (رقم ١٥/ ٢٠٠٤م) لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"، فضلاً عن أنّ هناك جهودًا تبذل لإصدار قانون خاص بالمعاملات الإلكترونية لسلامة وتأمين المعاملات المختلفة من

كافة جوانبها القانونية والجنائية، وهناك دراسات جادة لإعداد مشروع قانون لمكافحة الجريمة المعلوماتية.

- اهتمت المملكة العربية السعودية بتنظيم التعاملات الإلكترونية ومكافحة الجرائم المعلوماتية ، وسارعت بإصدار نظامي مكافحة جرائم المعلوماتية والتعاملات الالكترونية؛ في ٧/ ٣/ ١٤٢٨هـالموافق ٢٦/ ٣/ ٢٠٠٧م ، وكان ذلك للحد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات.
- أن التحقيق الابتدائي عبارة عن مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة، ومن أهم خصائصه: أن يكون علنياً بالنسبة للخصوم وسرياً عن الجمهور وأن يتم تدوين محضر التحقيق بحضور كاتب. ويختص به في التشريع المصري النيابة العامة، وفي التشريع السعودي هيئة التحقيق والادعاء العام.
- إن تحقيق جرائم تقنية المعلومات يتطلب تأهيل فني خاص للمحقق، وسرعة في الإجراءات ؛ فبالإضافة إلى المهارات الفنية التقليدية ؛ فإنه يجب أن يكتسب المحقق في جرائم تقنية المعلومات مهارات أخرى تتسم بالجدة والحداثة في مجال تقنية الاتصالات والحوسبة كإجادة التعامل مع أنظمة الحاسب وخدمات الانترنت وشبكات الاتصال المختلفة.، والاطلاع على الجوانب المتعلقة بجرائم المعلومات، وأن يكون ملماً بالقوانين المتعلقة بتكنولوجيا المعلومات والاتصالات وشبكة الإنترنت، والوقوف على الأبعاد

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

- في كثير من بلدان العالم تعقد 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 وانجلترا وكندا ومصر والمملكة العربية السعودية.
- تتمثل المهام أو الأعمال التي تقوم بها أجهزة التحقيق في جرائم تقنية المعلومات لكي تصل إلى الحقيقة في تلقي البلاغات والشكاوى، وتحديد خطة العمل وتكوين فريق التحقيق، وسرعة جمع الأدلة.
- يمكن أن تتم المعاينة في جرائم تقنية المعلومات بتصوير شاشة الحاسب الآلي حيث تظهر المعلومات أو الصور المطلوب معاينتها. أو أن يتم ذلك باستخدام برمجية حاسوب متخصصة في اخذ صور لما يظهر على الشاشة و تعرف بطريقة تجميد مخرجات الشاشة frozen كما يمكن أن يتم ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ save as ويمكن استخدام خاصية history لفحص الحاسب الآلي ، حيث انه في حالة ولوج الحاسب الآلي إلى الانترنت فانه يقوم باستنساخ نسخة من كل صفحة أو موقع يتم استدعائه و يقوم بحفظها في ملف خاص يصنعه نظام التشغيل. ويمكن إجراء المعاينة من خلال تحميل download نسخة من الصنف أو الرسالة أو البيانات أو المعلومات التي تم التعدي عليها عبر الانترنت ، ثم يتم طباعتها للحصول على نسخة ورقية عن طريق الطابعة المتصلة بالحاسب الآلي printer .

- أنه قد يصادف المحقق صعوبه في المعاينه بالنسبة لجرائم تقنية المعلومات، حيث يندر أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها ، وبالإضافة إلى ذلك فإن عدداً كبيراً من الأشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يفسح المجال لحدوث تغير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالاً من الشك على الدليل المستمد من المعاينة.
- التفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية ؛ فهو إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها.
- يشمل محل التفتيش في جرائم تقنية المعلومات كل المكونات المادية والمعنوية للوسائل الإلكترونية. ويمكن أن يشمل التفتيش أيضا شبكات الاتصال الخاصة بها والأشخاص الذين يستخدمون هذه الوسائل.
- أن التفتيش الإلكتروني العابر للحدود - تفتيش الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الدولة - يتعذر القيام به بسبب تمسك كل دولة بسيادتها، ولا يجوز في غياب اتفاقية دولية بين الدولتين تجيز هذا الامتداد في التفتيش، أو على الأقل الحصول على إذن

الدولة الأخرى. وهذا يؤكد أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني.

- أنه لا خلاف في الجملة بين الضوابط القانونية المتطلبة في التفتيش في جرائم تقنية المعلومات عنها في جرائم التقليدية. ومنها أن تكون هناك جريمة قد وقعت على الوسائل الإلكترونية أو من هذه الوسائل، وأن يكون هناك اتهام موجه إلى الشخص الذي يراد تفتيشه أو تفتيش مسكنه، أو وردت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، وأن يباشره الشخص أو الجهة المختصة – النيابة العامة، أو هيئة التحقيق والادعاء العام، أو مأمور الضبط القضائي في حالة ندبه، في غير حالات التلبس بالجريمة – وأن يصدر إذن بالتفتيش من الجهة المختصة. وهذا محل اتفاق بين النظام الجزائي المصري والسعودي.
- أنه كما يشمل التفتيش الكيانات المعنوية في جرائم تقنية المعلومات؛ فإنه من الضروري أن يترتب علي ذلك إباحة ضبطها ، وإن كان تحقيق هذا الأمر قد يواجه صعوبات كثيرة من الناحية التشريعية لعدم وجود نصوص خاصة بذلك ، خاصة في التشريعين المصري والسعودي ، الأمر الذي يتطلب تدخلا تشريعيا لمواجهة هذه الصعوبات بالنص صراحة على ذلك في التشريع الجزائي لهما. ، كذلك فإن تحقيق هذا الأمر قد يواجه صعوبات من الناحية العملية لعدم وجود رجل الضبط القضائي المتخصص وذو الخبرة الفنية في مثل تلك الأمور الفنية ذات التقنية العالية والمعقدة ، الأمر التي يتطلب رفع كفاءة رجل الضبط القضائي حتى يتمكن من مواجهة مثل تلك الحالات.

- بالنسبة لضبط المراسلات والاتصالات الالكترونية، كالبريد الاليكتروني والمحادثات الالكترونية فأن الأمر قد يختلف بعض الشيء ؛ حيث إن هناك أرضية مشتركة بين هذه الأنواع من الاتصالات وبين البريد العادي والمحادثات التليفونية العادية مما يتضح معه كفاية النصوص الحالية ، في التشريعين المصري والسعودي،
- الشاهد في الجريمة المعلوماتية هو ذلك الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة 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 تمييزا له عن الشاهد التقليدي.
- يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، وفقا للرأي الراجح.
- أنه إذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي، فهي أوجب في مجال الجرائم الإلكترونية، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز ، وقد نصت المادة (١٤) من نظام مكافحة جرائم المعلوماتية السعودي على أنه :" تتولى هيئة الاتصالات وتقنية المعلومات وفقاً

لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة ".

- استجواب المتهم يعني أن يتثبت المحقق من شخصية المتهم ويناقشه في التهمة المنسوبة إليه على وجه مفصل في الأدلة القائمة في الدعوى إثباتا ونفيا. ومواجهة المتهم بغيره هي وضعه وجهاً لوجه إزاء متهم آخر أو شاهد أو أكثر كيما يسمع بنفسه ما قد يصدر منهم من أقوال في صدد ما أدلوا به من معلومات متعلقة بواقعة أو أكثر فيتولى الإجابة تأييداً أو تفنيداً.
- لا يختلف الاستجواب والمواجهة بالنسبة للمتهم وكذا جهة التحقيق من حيث حقيقته وضماناته في حالة التحقيق في الجرائم التقليدية عنه في جرائم تقنية المعلومات؛ لأنه يتعلق بالمتهم ذاته ولا يتعلق بطبيعة الجريمة.
- أن هناك معوقات تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق فيها؛ ومنها الإحجام عن الإبلاغ عن الجريمة، وعدم توافر الكفاءة البشرية المؤهلة للتحقيق، وخفاء الجريمة المعلوماتية، وغياب الدليل المرئي، وصعوبة التعاون الدولي في مكافحة الجريمة المعلوماتية.

ثانياً : التوصيات

في سبيل الحد من الجرائم المعلوماتية ، وتحقيقها على الوجه المطلوب لمكافحتها فإنني أوصي بالاتي:

- ضرورة أن يضاف إلى الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أي مادة معالجه بواسطة الحاسب.

- تدخل المنظم المصري والسعودي بالنص صراحة في نصوص النظام الإجرائي على ضبط المكونات المعنوية لوسائل تقنية المعلومات.
- تدخل المنظم السعودي لإيجاد نص يلزم الشاهد بالحضور للإدلاء بالشهادة أثناء مرحلة التحقيق الابتدائي أمام السلطة المختصة به، وأن توقع عليه عقوبة مناسبة إذا امتنع عن ذلك.
- إدخال مادة أخلاقيات الانترنت ضمن المناهج الدراسية في التعليم ما قبل الجامعي.
- نشر الوعي بين صفوف المواطنين خاصة الشباب بمخاطر التعامل مع المواقع السيئة على الانترنت.
- تعزيز التعاون مع المؤسسات الدولية المعنية بمكافحة مثل هذه الجرائم .
- سن قوانين خاصة لمعالجة هذه الجرائم.

وأخيراً وليس آخراً، وبعد أن من الله سبحانه وتعالى – عليَّ بإنجاز هذا البحث، فإنني لا أدعي إلمامي بكافة جوانب الموضوع، أو أنني قد أصبت الحقيقة في كل رأي أو اقتراح عرضته، ولكنها مجرد محاولة، فكل فكر يقبل الجدل والنقاش مهما كانت وجاهته ومنطقيته.

وأخيراً اسأل الله العلي القدير أن يوفقنا لما يحبه ويرضاه، وآخر دعوانا أن الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه، أفضل الصلاة وأتم التسليم.

تم بحمد الله وتوفيقه

فهرس لأهم مراجع البحث

أولاً: المراجع العربية:

- د/ أحمد حسني أحمد طه، مبادئ قانون الإجراءات الجنائية في التشريع المصري، مطبعة بهجات للطباعة، الجزء الأول، بدون تاريخ.
- د/ أحمد فتحي سرور، مركز القانوني للنيابة العامة، مجلة القضاة سنة ١٩٦٨
- د/ د/ باسم الحمادي: إثبات جرائم الإنترنت صعب، بحث منشور على شبكة الإنترنت بتاريخ ٧ محرم ١٤٢٣هـ على موقع: **www.alrvada.com.sa**
- د/ بكري يوسف،التفتيش عن المعلومات في وسائل التقنية الحديثة، بحث منشور بمجلة كلية الشريعة والقانون بدمنهور، سنة ٢٠٠٧م.
- د/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب الآلي)، الكتاب الأول، دار النهضة العربية، ١٩٩٢.

- د/ حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، بحث منشور على موقع: **http://www.eastlaws.com**.
- د/ خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، ٢٠٠٨
- د/ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ٢٠١٠.
- د/ رءوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مطبعة الاستقلال الكبرى سنة ١٩٨٣م.
- د/ زكى محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، طبعة ٢٠١١م.
- د/ زكي أمين حسونة: جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي.
- د/ سامح السيد جاد، الإجراءات الجنائية في القانون المصري، طبعة دار الوزان، سنة ١٩٨٩.
- د/ سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، ٢٠١٣م.
- سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض٢٠٠٣.

- د/ شمس الدين إبراهيم احمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري دراسة مقارنة، طبعة دار النهضة العربية القاهرة ط ١ ٢٠٠٥م.
- د/ شيماء عبد الغني محمد عطا الله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧/ ٣/ ١٤٢٨هـ الموافق ٢٦/ ٣/ ٢٠٠٧م بحث منشور على موقع: http://www.f- د/ law.net
- د/ طارق عبد الله الشدي: آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض ١٤٢٣هـ.
- د/ عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، بحث منشور بمركز دراسات الكوفة، العدد السابع ٢٠٠٨م .
- د/ عبد الرحمن بحر: معوقات التحقيق في جرائم الإنترنت ﴿دراسة مسحية على ضباط الشرطة بدولة البحرين: رسالة ماجستير: جامعة نايف العربية للعلوم الأمنية، الرياض ١٩٩٩م
- د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر سنة ٢٠٠٦م.
- د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي الموحد، دار الفكر الجامعي، مصر سنة ٢٠٠٦م.
- عبد الله بن عبد العزيز الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة مكملة لمتطلبات الحصول على

الماجستير، مقدمة لجامعة نايف العربية للعلوم الأمنية، عام ١٤٣٢هـ ٢٠١١م.

- د/ عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع منتدى هيئة التحقيق والادعاء السعودي.
- د/ عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن بين النظرية والتطبيق، بدون ناشر ١٩٩٣م.
- د/ عصام عفيفي عبد البصير،التعليق على نظام الإجراءات الجزائية في المملكة العربية السعودية، طبعة دار النهضة العربية،سنة ٢٠٠٥م
- د/ علي جبار الحسيني، جرائم الحاسوب والانترنت، طبعة دار اليازوري العلمية للنشر والتوزيع، الأردن، ٢٠٠٩م .
- د/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد بتاريخ ٢٦ - ٢٨نيسان ٢٠٠٣ م بمركز البحوث والدراسات بأكاديمية شرطة دبي، عدد رقم: ١ سنة : ٢٠٠٣ م، منشور على موقع: **http://www.f44g.com**
- د/ عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية جـ ١، رقم ٢١٤.

- د/ عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الآلي، بحث منشور في كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية، ١٩٩١م.
- د/ عوض محمد عوض، قانون الإجراءات الجنائية،جـ ١، طبعة مؤسسة الثقافة الجامعية ١٩٨٩م .
- د/ غنام محمد غنام، ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات ن بحث منشور بمجلة البحوث القانونية والاقتصادية، العدد الرابع والأربعون، أكتوبر ٢٠٠٨.
- د/ فوزية عبد الستار، شرح قانون الإجراءات الجنائية، طبعة مطبعة جامعة القاهرة، نشر دار النهضة العربية، سنة ١٩٨٦.
- د/ مأمون سلامة : الإجراءات الجنائية في التشريع المصري، دار النهضة العربية سنة ٢٠٠٠م.
- د/ محمد أبو العلا عقيدة،التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي، بتاريخ ٢٦ نيسان ٢٠٠٣حتى ٢٨ نيسان ٢٠٠٣ م – منشور على موقع كلية الحقوق جامعة المنصورة - **http://www.f-law.net**
- د/ محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من ١-٣/ ٥/ ٢٠٠٠م.

- محمد بن نصير محمد السرجاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت ﴿دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية﴾، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤ م منشور على موقع: **http://www.creativity.ps/library/details.php?id**
- د/ محمد زكى أبو عامر، الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٤
- د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ١٩٩٤.
- د/ محمد سامي النبراوي، استجواب المتهم، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ١٩٦٨م
- د/ محمد عبد الرحيم سلطان العلماء جرائم الانترنت والاحتساب عليها بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت جامعة الإمارات مايو ٢٠٠٥.
- د/ محمد عبد الله أبو بكر سلامة موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت منشأة المعارف، الإسكندرية ٢٠٠٦.
- د/ محمد عيد الغريب، شرح قانون الإجراءات الجنائية، طبعة النسر الذهبي للطباعة ١٩٩٦- ١٩٩٧م
- د/ محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة دار الثقافة للنشر والتوزيع، عمان، سنة ١٤٣٠ هـ - ٢٠٠٩م

- د/ محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، دار النهضة العربيةسنة١٩٨٨م.
- د/ محمود نجيب حسني: شرح قانون الإجراءات الجنائية، طبعة دار النهضة العربية، الطبعة الثانية ١٩٨٨م
- د/ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية،طبعة مطابع الشرطة، القاهرة سنة ٢٠٠٩م
- د/ مصعب القطاونة، الإجراءات الجزائية الخاصة في الجرائم المعلوماتية، بحث منشور على موقع: **http://www.lawjo.net**
- د/ ممدوح رشيد العنزي، ضمانات المتهم أثناء مرحلة التحقيق الابتدائي في النظام السعودي، دراسة مقارنة، رسالة دكتوراه في الحقوق، جامعة القاهرة، سنة ٢٠٠٩م.
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، طبعة دار الفكر الجامعي، ٢٠٠٦م.
- نبيله هبة هروال، الجوانب الاجرائية في مرحلة جمع الاستدلال، طبعة دار الفكر الجامعي، مصر سنة ٢٠٠٦م
- د/ هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، ١٩٩٢م.
- د/ هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي العدد(٢)، ١٩٩٩م.
- د/ هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط ١٩٩٢م

- د/ هلال عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة،١٩٩٧م
- يونس عرب، جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢ – تنظيم المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢ / ٢/ ٢٠٠٢

المجموعات والدوريات:

- مجلة المحامون
- مجموعة أحكام محكمة النقض
- مجموعة القواعد القانونية

ثانياً : المراجع الأجنبية:

- *Davis, David (1998)* Internet Detective: An Investigator's Guide. West Midland, UK: Police Research Group.
- *Groover, Richard (1996).* Overcoming Obstacles: Preparing for Computer–relatedCrime.(online): www.fbi.gov/publications/leb/1996/aug962.txt (06/06/2003.)
- *Icove, D, Segar. K& Vons torch, W (1995).* Computer Crime: A Crime fighter's handbook Sebastopol. California: O'Reilly & Associates.
- *Icove, D, Segar. K& Vons torch, W et al, 1999.*

-*ISTS, Institute for security Technology Studies (2002).* Law Enforcement Tools and Technologies for investigating cyber attacks: A National Needs Assessment, available On line www.ists.dartmouth.eud/ATG/need/ISTS_NA.pdf.,

- *Jack, bologna, corporate,* fraud the basics of prevention and detection, butterworth publisher, 1984, p.7

- *Mandia &, K. & Prosise, C. (2001).* Incident response: Investigating Computer. Crime. Berkeley, California: McGraw-Hill.

- *Middleton, Bruce (2002)* Cyber Crime Investigator's Field Guid. Boca Raton, Florida: Auerbach Publications.

- *Sammes T & Jenkinson B, (2000)* Forensic Copmputing: Apratitioner's Guide London Springer.

- *Schultz, E & Shumway, R (2002)* incident Response: A Strategic Guide to Handling System and Network Secueity Breaches, Indianapolis, Indian: New Riders Publishing.

- *Stern Eckert, Alan (2004).* Critical incident Management. Boca Raton, Florida: CRC Press.

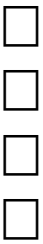
-*Suzan Brener.*model code of cyber crime investigation p.24-uni- dayton school of law.. http://cyber crimes. Net/mccip.htm

- *Thompson, David (1990).* Computer Crime The Improvement Of Investigative Skills: Final Report: Part Tow, www.acpr.gov.au/pdf/acpr101.pdf 21/10/2003.

- *Tom forester,* Essential problems to High-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104

- *Wright, 2000d, Weight, Timothy (2000)* (d). The Field Guide for Investigating computer Crime: Search and

(Seizure Planning (on line) www.secuotyfocus.com/ingocus/1247



الفهرست