مجلة جامعة الملك سعود (الحقوق والعلوم السياسية)، مج (٣٣)، ع (٢)، ص ص ١٢٩-١٤٩، الرياض (٢٠٢١م/ ١٤٤٢هـ)

التحقيق الجنائي الرقمي

حنان محمد الحسيني أحمد
أستاذ القانون الجنائي المساعد
كلية الحقوق والعلوم السياسية
جامعة الملك سعود

سحر علي عبدالله الهبدان
أستاذ القانون الجنائي المساعد
كلية الحقوق والعلوم السياسية
جامعة الملك سعود

(قدم للنشر في ٢٠/ ١/ ١٤٤١هـ، وقبل للنشر في ٢٢/ ٤/ ١٤٤١هـ)

ملخص البحث. أفرزت الثورة المعلوماتية الحديثة نوعاً جديداً من الجرائم وهو ما يسمى بالجرائم الرقمية أو الجرائم المعلوماتية والتي تمثل أنماطاً متعددة من السلوك الإجرامي تتم من خلال الأجهزة الحاسوبية والشبكة المعلوماتية، وحيث إن الجريمة الرقمية ترتكب في عالم افتراضي فقد أُثير التساؤل حول مدى تطور إجراءات التحقيق الجنائي حتى يمكن التعامل مع هذا النوع الجديد من الإجرام حيث إنها تخضع بالضرورة لإجراءات تختلف عن القواعد الإجرائية التقليدية لاستخلاص الدليل الجنائي، ولذلك تبدت أهمية موضوع البحث وهو التحقيق الجنائي الرقمي القائم على التحليل الجنائي الرقمي باستخدام التقنيات التكنولوجية الحديثة، للحصول على ما يسمى بالدليل الرقمي وتحقيقه بالطرق المثبتة علمياً والتي تؤكد على ضرورة مشروعيته، ولذلك ارتكز هذا البحث على معرفة الأصول القانونية للتحقيق الجنائي الرقمي من خلال بيان أصول وقواعد هذا التحقيق وما يعترضه من معوقات، وكذلك معرفة الآليات الإجرائية الحديثة لاستخراج الأدلة الرقمية من أجهزة الحاسب الآلي والشبكة المعلوماتية، وتم اتباع المنهج التحليلي في بيان قواعد وإجراءات هذا التحقيق.

الكلمات المفتاحية: جريمة، جرائم معلوماتية، إجراءات التحقيق، دليل رقمي.

DIGITAL CRIMINAL INVESTIGATION

Hanan Mohamed Elhoussini Ahamed
Assistant Professor, College of Law and Political Science
King Saud University

Sahar Ali Abdullah Alhabdan
Assistant Professor, College of Law and Political Science
King Saud University

(Received 20/01/1441 H., Accepted for Publication 22/04/1441 H.)

Abstract. Cybercrime is a new type of crime, which was produced by the modern information revolution. Cybercrime represents multiple types of criminal behavior conducted through computer hardware and the information network. Moreover, since cybercrime is committed in a virtual world, the question has been raised as to how criminal investigation procedures have evolved so it can deal with this new type of crime for the purpose of extracting digital evidence. Because the nature of cybercrime is different from traditional crimes, cybercrime must be subject to procedures that are different from the traditional procedural rules. Therefore, the research explains and analyzes the digital forensic investigation and modern technological techniques to obtain the so-called digital evidence and assure its legitimacy. It will also demonstrate the obstacles cyber investigation may encounter. This research follows the analytical approach in describing the rules and procedures of this investigation.

Keywords: Crime, Information crimes, Investigation procedures, Digital evidence.

مقدمة

موضوع البحث

يتناول موضوع البحث دراسة التحقيق الجنائي الرقمي في الجريمة الرقمية أو الإلكترونية والتي بدأت بالظهور في الوقت الحالي نتيجة الثورة المعلوماتية تلك التي جسدت في جانبها الإيجابي إبداعاً للعقل البشري وقفزة نوعية في حياة الأفراد والدول التي اعتمدت عليها في العمل في كثير من قطاعاتها من خلال استخدام الأنظمة المعلوماتية، ورغماً عن ذلك كان لهذه الثورة دورها السلبي وخاصة في مجال الجريمة؛ حيث أفرزت نوعاً جديداً لم يكن معهوداً من قبل وهي الجرائم الرقمية أو الجرائم المعلوماتية التي أصبحت شاغلاً مقلقاً على الصعيد المحلي والإقليمي والدولي نظراً لأنها الجرائم الأكثر تعقيداً وغموضاً في هذا العصر الرقمي، وتمثل أنماطاً متعددة من السلوك الإجرامي وتثير كثيراً من التحديات الإجرائية والتي من أهمها كيفية تحقيقها وإثباتها ومدى اقتناع القاضي بالدليل المتولد عنها؛ مما أدى إلى ضرورة البحث عن طرق قانونية إجرائية فاعلة ومتقدمة لمكافحتها مع ضرورة الاستفادة من معطيات التكنولوجيا الحديثة في الكشف عن هذا النوع الجديد من الجرائم وإثباتها وملاحقة مرتكبيها لتقديمهم إلى العدالة؛ مما حذا بالمشرع في العديد من الدول إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة إثبات هذه الجرائم حيث إنها تحتاج إلى طرق إلكترونية فنية وعلمية حديثة تتناسب مع طبيعتها وتكشف عن أدلة إثباتها ، تلك التي لابد أن تختلف عن القواعد الإجرائية التقليدية لاستخلاص الدليل، ولذلك تبدت أهمية ما يسمى بالتحقيق الجنائي الرقمي القائم على التحليل الجنائي الرقمي باستخدام التقنيات التكنولوجية الحديثة، والتي تتضمن فحص الجهاز أو المنظومة بهدف تحليل العمليات الحاسوبية واسترجاع البيانات والملفات من أجل الحصول على ما يسمى بالدليل الرقمي وتحقيقه بالطرق المثبتة علمياً للتحقق من مدى صحته في نسبة الجريمة إلى مرتكبها؛ ولذلك فالهدف الرئيسي من التحقيق الجنائي الرقمي هو التصدي للجرائم الرقمية التي ترتكب باستخدام الأجهزة الحاسوبية أو التي تقع على المنظومات أو الشبكات المعلوماتية، وذلك تحقيقاً للهدف العام من التحقيق الجنائي بوصفه عملية تستدعيها المصلحة العامة لحماية أمن المجتمع واستقراره من خلال التحري والتدقيق للكشف عن غموض الجريمة وتحديد مرتكبها والوقوف على كل الأدلة الخاصة بها؛ فإجراءات التحقيق الجنائي هي المعنية بتحقيق واجب العدل والإنصاف والتحقق من ثبوت أو نفي الاتهام ضد مرتكبها.

هدف البحث وأهميته

ترتكز هذه الدراسة على معرفة الأصول القانونية للتحقيق الجنائي الرقمي من خلال بيان أصول وقواعد هذا التحقيق وما يعترضه من معوقات وكذلك معرفة الآليات الإجرائية الحديثة لاستخراج الأدلة الرقمية من أجهزة الحاسب الآلي والشبكة المعلوماتية؛ تلك الأدلة الرقمية التي تكون على هيئة بيانات رقمية مخزنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، وكذلك معرفة كيفية التعامل مع هذا النوع الجديد من الأدلة والذي يتواجد في بيئة افتراضية غير تقليدية تواجه الكثير من الصعوبات والتحديات في إجراءات تحقيقها.

وتتأكد أهمية الدراسة في الكشف عن مدى ضرورة استخدام التقنيات الحديثة في إجراء هذا التحقيق الجنائي ومدى جدوى هذه التقنيات في استخلاص دليل رقمي يتسم بالمشروعية، وله حجية قانونية وقوة ثبوتية أمام جهات التحقيق والقضاء ويؤدى في النهاية إلى التصدي لهذا النوع الجديد من الإجرام المعلوماتي الذي يرتكب في بيئة الحاسب الآلي.

منهج الدراسة

ترتكز هذه الدراسة على المنهج التحليلي والتأصيلي لقواعد وإجراءات التحقيق الجنائي الرقمي وذلك من أجل تحديد الآليات الإجرائية لهذا التحقيق الجنائي، وما يعتريه من صعوبات تواجه سلطات التحقيق في استخلاص الأدلة الرقمية، وكذلك المنهج المقارن حيث تم تناول هذه الإجراءات في أكثر من نظام قانوني للوقوف على مدى فأعليتها في تحقيق الجريمة الرقمية كالنظام المصري.

مشكلة الدراسة

الجريمة الرقمية ترتكب في عالم افتراضي؛ لذلك فإن مسرح الجريمة الرقمية يختلف تماماً عن مسرح الجريمة التقليدية والتي تتميز بارتكابها في عالم مادي ملموس يسهل تحقيق أدلتها، وأمام هذا الوضع يثار التساؤل حول مدى تطور إجراءات التحقيق الجنائي حتى يمكن التعامل مع الجرائم الرقمية، وهل سيحقق استخدام التقنيات الحديثة في مجال التحقيق الجنائي الشرعية الإجرائية بما يفي بمتطلبات التحقيق في هذا النوع المستحدث من الجرائم الرقمية وبما يتلاءم مع طبيعتها، وذلك فيما يخص إجراءات التحقيق التي تثير صعوبات في التحقيق كالتفتيش والمعاينة والضبط والخبرة.

خطة البحث

ترتكز خطة البحث على بيان ماهية وخصائص ومعوقات التحقيق الجنائي الرقمي ثم بيان إجراءات هذا التحقيق وذلك في مبحثين مستقلين على النحو التالي:

- المبحث الأول: مقدمة حول التحقيق الجنائي الرقمي.
  - المطلب الأول: ماهية وخصائص ومعوقات التحقيق الجنائي الرقمي.
    - الفرع الأول: ماهية وخصائص التحقيق الجنائي الرقمي.
    - الفرع الثاني: معوقات التحقيق الجنائي الرقمي.
  - المطلب الثاني: محل التحقيق الجنائي الرقمي.
    - الفرع الأول: الجريمة الرقمية.
    - الفرع الثاني: الأدلة الرقمية.
- المبحث الثاني: إجراءات التحقيق الجنائي الرقمي.
  - المطلب الأول: المعاينة والتفتيش في الجرائم الرقمية.
    - الفرع الأول: إجراءات المعاينة في الجرائم الرقمية.
    - الفرع الثاني: إجراءات التفتيش في الجرائم الرقمية.
  - المطلب الثاني: الشهادة والخبرة والضبط في الجرائم الرقمية.
    - الفرع الأول: إجراءات الشهادة والخبرة في الجرائم الرقمية.
    - الفرع الثاني: ضبط الأدلة في الجرائم الرقمية.
- الخاتمة.

المبحث الأول:
مقدمة حول التحقيق الجنائي الرقمي

التحقيق الجنائي الرقمي هو في ذاته تحقيق ابتدائي ولكن في نوع خاص من الجرائم وهي الجرائم الرقمية وينطوي على تحقيق الأدلة الرقمية الخاصة بهذه الجرائم، وسنتناول في هذا المبحث ماهية هذا التحقيق وخصائصه ومعوقاته في مطلب أول ثم نتناول في مطلب ثان محل هذا التحقيق.

المطلب الأول: ماهية وخصائص ومعوقات التحقيق الجنائي الرقمي

يقصد بماهية التحقيق الجنائي الرقمي إيضاح مفهومه لمعرفة القواعد القانونية التي تحكمه؛ لذا سنتناول في هذا المطلب ماهيته وخصائصه وذلك في الفرع الأول؛ ثم نتناول في الفرع الثاني معوقات هذا التحقيق.

الفرع الأول: ماهية وخصائص التحقيق الجنائي الرقمي

البند الأول: ماهية التحقيق الجنائي الرقمي

التحقيق لغة هو إثبات المسألة بدليلها.(الكاملي، ٢٠١٥م)، أما التحقيق الجنائي اصطلاحاً فهو ما عرفه جانب من الفقه بأنه مجموعة من الإجراءات القضائية تمارسها سلطات التحقيق بالشكل المحدد قانوناً بغية التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها في إحالة المتهم إلى المحاكمة، أو الأمر بألا وجه لإقامة الدعوى (سلامة، ١٩٧٧م)، وعرفه جانب آخر من الفقه بأنه عبارة عن سلسلة من الإجراءات التي تتخذها السلطات المختصة بهدف التنقيب عن الأدلة في شأن الجريمة المرتكبة لتحديد مدى كفايتها لإحالة المتهم إلى المحكمة المختصة (حسني، ١٩٩٨م).

ومن التعريفات السابقة يتبين أن التحقيق الجنائي له مفهومين أحدهما المفهوم الواسع ويأخذ به النظام الأنجلو أمريكي، والذي يقصد به مجموعة الإجراءات التي تهدف إلى البحث عن الأدلة بشأن الجريمة التي وقعت وتجميعها ومن ثم تقديرها لتحديد كفايتها لإحالة المتهم إلى المحكمة المختصة (الخفاجي، ٢٠١٥م)؛ أما المفهوم الثاني للتحقيق

الابتدائي فهو المفهوم بمعناه الضيق والسائد في النظام الإجرائي اللاتيني والذي أخذت به الكثير من الدول العربية ويقصد به تلك الإجراءات التي تباشرها سلطة التحقيق وحدها بشأن جمع الأدلة وكشف الجريمة؛ أو ما يتخذه قاضي التحقيق إذا ما ندب لتحقيق قضية معينة وما يتم من إجراءات يختص بها مأمور الضبط القضائي في حال التلبس والندب (تاج الدين، ٢٠١٤م).

ويرتكز التحقيق الجنائي على أصول شرعية وقانونية وقواعد فنية تباشرها جهة التحقيق للكشف عن الجريمة وحفظ الأدلة وإسنادها لمرتكبها، ولهذا فإن علم التحقيق الجنائي يبين الأصول الإجرائية التي يجب على المحقق اتباعها بدقة لتتصف أعماله بالمشروعية، كما ينطوي على قواعد وأساليب فنية تعنى بفحص الأدلة وتحقيق شخصية الجاني (القحطاني، ٢٠١٤م).

ويعد التحقيق المرحلة الأولى في الخصومة الجنائية؛ فهو يهدف إلى مدى جدوى تقديم المتهم للمحكمة لإقرار حق الدولة في العقاب (سرور، ١٩٩٦م) "ووصف هذا التحقيق بأنه ابتدائي لأن غايته ليست كامنة فيه، فهو لا يستهدف الفصل في الدعوى وإنما يستهدف التمهيد لمرحلة تالية هي مرحلة المحاكمة وذلك بجعل الدعوى صالحة للحكم، وتسهيل وتسريع الفصل فيها" (الغافري، ٢٠٠٩م).

وتتميز إجراءات التحقيق الابتدائي بأنها ذات طبيعة قضائية، ليس فقط لكون من يقوم بها النيابة العامة – إذ تصدر عنها كذلك بعض أعمال الاستدلال – بل لتوافر صفة الحياد فيها، بحسبانها جهة تحقيق، ولإسباغ طابع القهر والإجبار على هذه الإجراءات؛ وعلى ذلك فإن التحقيق الابتدائي يستهدف تحقيق أمرين معاً وهما جمع أدلة الجريمة والمحافظة عليها من ناحية، وتحديد الوضع المؤقت للمتهم من ناحية أخرى (شريف، ٢٠١٦م).

والتحقيق الجنائي الرقمي يحمل ذات المضمون السابق ويعتبر تحقيقاً ابتدائياً موضوعه تحقيق الأدلة الرقمية ولكن بصفة خاصة في الجرائم الرقمية، ويمكن تعريفه وفقاً لما يراه الباحث بأنه تحقيقاً ابتدائياً شاملاً لجميع الإجراءات التي يباشرها المحقق عند وقوع جريمة أو حادث توصلاً إلى معرفة الحقيقة ولكن فيما يسمى بالجرائم الرقمية؛ فهو ينطوي على عملية الفحص والتدقيق لأي جهاز كمبيوتر أو أي جهاز ملحق به لتحديد ما إذا كان هذا الجهاز قد تم استخدامه في جريمة رقمية أو عمل غير مشروع ثم تحقيق الأدلة الخاصة بذلك.

وقد عرفه البعض بأنه كافة الجهود التي يبذلها فريق التحقيق في سبيل استنطاق الأدلة الرقمية لكشف غموض جرائم الحاسوب والإنترنت وتحديد شخصية مرتكبها وإثباتها بما يقدمه من أدلة إثبات (السرحاني، ٢٠٠٤م).

ويختلف التحقيق الجنائي سواء في الجرائم الإلكترونية (الجرائم الرقمية) أو في غيرها من الجرائم عن إجراءات الاستدلال والتي تعتبر مرحلة سابقة على تحريك الدعوى الجنائية؛ حيث إنه يعتبر مرحلة أساسية من الدعوى الجنائية مما يستتبع حقيقة مؤداها أن أعمال الاستدلال لا تتولد عنها أدلة في مضمونها القانوني، ولا يجوز أن يكون كل سند القاضي في حكمه محضر الاستدلال حيث لا تتوافر فيها ضمانات الدفاع المتطلبة لنشوء الدليل، كما أن الدعوى الجنائية لا تتحرك بها ولو في حالة التلبس بالجريمة، ولكن تبدو أهميتها في أنها تتيح لسلطة التحقيق أن تتصرف في شأن تحريك الدعوى الجنائية وهي على بينة وعلم كافيين بحقائق الأمور[1] (حسني، ٢٠١٣م).

البند الثاني: خصائص التحقيق الجنائي الرقمي

يتميز التحقيق الجنائي الرقمي بضرورة تعامله مع بيئة الحاسب الآلي وكل ما يتعلق بها ولذلك فمن أهم خصائصه الآتي:

- أولاً: التعامل مع نوع متخصص من الجرائم وهي الجرائم الرقمية التي ترتكب عبر نظام الحاسوب والشبكة العنكبوتية.

(١) ونوضح أن السلطة المختصة بأعمال الاستدلال هي سلطة الضبط الجنائي، وقد جاء في نظام الإجراءات الجزائية السعودي الصادر بالمرسوم الملكي رقم (م/ ٣٩) وبتاريخ ٢٨/ ٧/ ١٤٢٢هـ بتحديد عمل رجال الضبط القضائي بمرحلة الاستدلال فقط والذي أصبح اختصاصاً أصيلاً لرجال الضبط القضائي؛ لا يجوز لهم الخروج عنه إلا في حالة التلبس بالجريمة، أو الندب من سلطة التحقيق؛ فلهم مباشرة بعض إجراءات التحقيق استثناء في هذين المرحلتين.

- ثانياً: تحقيق ما يسمى بالأدلة الرقمية المتعلقة ببيئة الحاسب الآلي والإنترنت.
- ثالثاً: التعامل مع الاتصال الشبكي وأنواعه المختلفة ومعرفة كيفية انتقال البيانات عبر الأجهزة المختلفة وعبر شبكة الإنترنت.
- رابعاً: التعامل مع الأنظمة المختلفة لتشغيل الحاسب الآلي.
- خامساً: التعامل مع صيغ الملفات الإلكترونية المختلفة وتطبيقات الحاسوب الرئيسية.
- سادساً: التعامل مع خدمة الإنترنت كأداة لجمع البيانات والتحريات عن الجرائم الإلكترونية.
- سابعاً: التعامل مع تقنيات أمن الحاسوب والإنترنت لإمكانية ربطها بمجريات التحقيق.
- ثامناً: استخدام الأدوات الفنية التي تستخدم في بنية نظم المعلومات وأهمها البريد الإلكتروني وبرامج المحادثة وعناوين IP.

الفرع الثاني: معوقات التحقيق الجنائي الرقمي

هناك عدة معوقات تعترض التحقيق الجنائي الرقمي منها ما يتعلق بالجاني والمجني عليه ومنها ما يتعلق من ناحية أخرى بجهات التحقيق، وسنوضح ذلك في البندين التاليين.

البند الأول: معوقات تتعلق بالجاني والمجني عليه

أولاً: المعوقات المتعلقة بالجاني

من الصعوبات التي تواجه التحقيق الجنائي الرقمي هو ما يتعلق بشخصية مرتكب الجرائم الرقمية حيث إنه لا يعد مجرماً تقليدياً بل له سمات خاصة تتناسب مع هذا النوع الجديد من الإجرام؛ ففي الغالب ترتكب هذه الجرائم من قبل مجرمين لهم دراية عالية باستخدام وسائل التقنية الحديثة وينفذون أعمالهم الإجرامية بذكاء ومهارة (العريان، ٢٠٠٤م)؛ بالإضافة إلى أن الجناة لهم المفردات والمصطلحات الخاصة بهم حتى إنهم يطلقون على أنفسهم اسم النخبة بدعوى أنهم الأكثر معرفة وخبرة بأسرار الحاسب الآلي ولغاته المتميزة (حجازي، ٢٠٠٢م).

وتعد كذلك من أهم سمات المجرم المعلوماتي الدقة والتخصص لهذا النوع من الإجرام والاحترافية العالية في هذا المجال والتي تمكنه من التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسب الآلي (البوسعيدي، ٢٠٠٩م).

ويمكن تصنيف مرتكبي الجرائم الرقمية إلى عدة فئات كالتالي:

١- المخترقون أو المتطفلون: وهم المخترقون كالهاكرز والكراكرز، فالهاكرز هم متطفلون يتحدون إجراءات أمن النظم والشبكات ولا تتوافر لديهم في الغالب الأعم دوافع تخريبية أو حاقدة؛ أما الكراكرز هم الذين يقومون بأنشطة غير قانونية تخريبية تدمر الأنظمة المعلوماتية ولديهم ميولاً إجرامية.

٢- المحترفون: تعد هذه الطائفة هي الأخطر بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم بارتكاب الجرائم الرقمية المختلفة، ومن هذه الطائفة على سبيل المثال محترفي التجسس الصناعي ومجرمي الاحتيال والتزوير.

٣- الحاقدون: وهم الذين يمارسون أنشطتهم الإجرامية في مجال الجريمة الرقمية بدافع الانتقام ولا يسعون إلى تحقيق مكاسب مادية أو سياسية ولا يتسمون بالتقنية الاحترافية؛ فهم إما مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة أو غرباء عن النظام تتوفر لديهم أسباب الانتقام من أشخاص أو جهات معينة.

٤- صغار أذكياء المعلوماتية: وهم صغار السن من مستخدمي الشبكة المعلوماتية والمولعون بالحاسبات والاتصالات، ويصنفهم البعض ضمن مجرمي الحاسب نظراً لخطورة أفعالهم التي تتميز بانتهاك وخرق الأنظمة الرقمية (صالح، ٢٠١٥م).

وتسعى الدراسات الحديثة في علم الإجرام إلى إيجاد تقسيم منضبط لمجرمي التقنية لكنها تجد صعوبة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة؛ والمرتبط بالتسارع في مجال النظام المعلوماتي والإنترنت (عبدالله، ٢٠١٥م).

ثانياً: المعوقات المتعلقة بالمجني عليه

من معوقات التحقيق أيضاً تلك المتعلقة بالمجني عليه والذي قد يكون شخصاً طبيعياً أو معنوياً.

ففي حال كان المجني عليه شخصاً طبيعياً فإن ما يعيق عملية التحقيق هو الإحجام عن الإبلاغ عن الجريمة؛ فالكثير على سبيل المثال يتحدثون عن اختراق حواسيبهم، أو بريدهم الإلكتروني، أو صفحات الفيسبوك الخاصة بهم ومع ذلك لا يتقدمون بالشكوى للسلطات المختصة خوفاً من نشر خصوصياتهم أو حفاظاً على مركزهم الاجتماعي.

أما إذا كان المجني عليه شخصاً معنوياً والذي قد يتمثل في مؤسسات أو هيئات أو شركات تعتمد في عملها على أنظمة الحاسب الآلي كالبنوك وشركات التأمين؛ فإن ما يعيق عملية التحقيق هو عدم إدراك المسؤولين في هذه المؤسسات بخطورة هذا النوع من الجرائم، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة واقتصار تركيزها على تقديم الخدمة، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة هذه الجرائم، وعدم التركيز على الجانب الأمني مما يؤدي إلى الإحجام عن الإبلاغ عن هذه الجرائم حتى لا تظهر الجهات المجني عليها بمظهر مشين قوامه الإهمال وقلة الخبرة وعدم الوعي الأمني اللازم لحماية معلوماتها (الحلبي، ٢٠١١م).

البند الثاني: معوقات تتعلق بجهات التحقيق

يواجه التحقيق الجنائي الرقمي عدداً من المعوقات والتي تتعلق بسلطة التحقيق، فحداثة هذه الجرائم وقلة خبرة القائمين بالتحقيق بها (السرحاني، ٢٠٠٤م) بالإضافة إلى عدم توفير الأجهزة والبرامج المناسبة للتحقيق وتكلفتها العالية تعد من أهم المعوقات، ومما يزيد من صعوبة التحقيق هو قدرة الحواسيب الهائلة على تخزين البيانات مما يصعب معه عملية فرز الأدلة ومعرفة المشروع منها وغير المشروع، وبالتالي إعاقة الوصول إلى الدليل الرقمي (عبدالرحمن، ٢٠١٥م) وصعوبة معرفة المسؤول عن الجريمة (حجازي، ٢٠٠٢م)، ولأن البيئة المعلوماتية مؤلفة من شبكات منتشرة في كافة أنحاء العالم ومرتبطة ببعضها البعض؛ بحيث تتيح للمستخدمين الوصول عن بعد إلى البيانات الإلكترونية المخزونة داخل أو خارج حدود الدولة، فإن سلطة التحقيق أثناء القيام بعملها تصطدم بسيادة الدول الأخرى في حال وقعت البيانات خارج حدود الدولة (خلف، ٢٠١٦م).

ويقع على عاتق المحقق الجنائي عدة التزامات لها أثر في الحد من هذه المعوقات، كوجوب احترام القواعد النظامية التي تحددها الأنظمة المختلفة للقيام بعملية الضبط والتحقيق، وأن يكون القائم بالتحقيق موضوعياً متجرداً من كل ما يؤثر عليه في تحقيق الواقعة المرتكبة؛ بالإضافة إلى احترام حقوق المتهم في كل إجراءات التحقيق؛ كما أنه يؤثر في نجاح عملية التحقيق إنجاز المحقق مهام الضبط والتحقيق بالسرعة والدقة اللازمين؛ كسرعة الانتقال إلى مسرح الجريمة وسماع الشهود وضبط المتهم واستجوابه والاستعانة بالمتخصصين في الحاسب الآلي ليكونوا ضمن كوادر الأجهزة الأمنية والقضائية، ويجب على المحقق أيضاً البحث عن الحقيقة بالطرق المشروعة والمحافظة على السرية حيث لا يجوز إفشاء المعلومات المتعلقة بكل إجراءات التحقيق (الكاملي، ٢٠١٥م).

ومما لا شك فيه أن لطريقة التحقيق في الجرائم الرقمية أثراً كبيراً في الحد من هذه المعوقات والوصول إلى الدليل؛ حيث إن خبير الحاسب الآلي له دور مهم في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته والمتعلقة بالجريمة الرقمية، وعليه فإنه يجب على المحقق إجراء التحقيق بحضور الخبير وتبادل المعلومات معه قبل البدء في التحقيق وذلك لمعرفة الأبعاد الفنية والنقاط التي يجب استجلاؤها أثناء التحقيق، وللتوصل لهذا الاسلوب الخاص للتحقيق في هذه الجرائم والذي يجمع بين الخبرة الفنية والكفاءة المهنية فإنه لابد من عقد المؤتمرات والندوات بصفة دورية المعرفة للجوانب التقنية الحديثة في مجال الحاسب الآلي وتدريب رجال الضبط القضائي وسلطات التحقيق على أنظمة الحاسب الآلي لاكتساب المهارات اللازمة لتحقيق الأدلة الرقمية (البشري، ٢٠٠٠م).

المطلب الثاني: محل التحقيق الجنائي الرقمي

محل التحقيق الجنائي الرقمي هو الجريمة الرقمية والأدلة الرقمية وسنتناول كل منهما في فرع مستقل.

الفرع الأول: الجريمة الرقمية

البند الأول: مفهوم الجريمة الرقمية

ثمة تباين كبير بشأن المصطلحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة نظم المعلومات وبيئة الشبكات ومنها على سبيل المثال مصطلح جرائم الكمبيوتر، والجريمة المعلوماتية، وجرائم التقنية العالية (عبدالله، ٢٠١٥م)، والجرائم الإلكترونية، والجرائم الافتراضية، والجرائم الرقمية، ولذلك تعددت التعريفات الدالة على هذه الجرائم ومنها تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينيا عام ٢٠٠٠م للجريمة الإلكترونية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية أو داخل نظام حاسوب ، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية" (مصطفى، ٢٠١٠م).

وتعددت التعريفات الفقهية للجريمة الرقمية حيث لم يتفق الفقه الجنائي على تعريف موحد لها، وعرفها البعض على نطاق واسع كأي مخالفة ترتكب ضد أفراد أو جماعات بدافع إجرامي كالأعمال الإجرامية التي تتعلق بالبنية التحتية لتكنولوجيا المعلومات، بما في ذلك الوصول غير المشروع للبيانات أو المعلومات، والاعتراض غير القانوني للبيانات عن طريق نقلها من وإلى أي جهاز حاسوب، وإدخال بيانات خاطئة أو تغيير البيانات الموجودة والعبث بها، وإساءة استخدام الأجهزة والتزوير كسرقة الهوية، والاحتيال الإلكتروني[٢] (تقرير وزارة الداخلية بالبحرين، بدون تاريخ).

ويرى الباحث وفقاً لاجتهاده بأنه يمكن تعريف الجريمة الرقمية بأنها أي عمل غير مشروع يرتكب في بيئة الحاسب الآلي باستخدام وسائل التقنية الحديثة.

ورغم أن الجريمة التقليدية تختلف من حيث طبيعتها عن الجريمة الرقمية التي من أهم سماتها استخدام المجرم المعلوماتي لوسائل التقنيات الحديثة في ارتكاب جريمته، إلا أنه يمكن تصور كل أشكال الجرائم التقليدية في الجرائم الرقمية.

ويمكن حصر بعض الأفعال التي تشكل الجرائم الالكترونية (الجرائم الرقمية) كالتالي:

- الأفعال ضد السرية والنزاهة ومنها الدخول غير المشروع لنظام الحاسوب، واعتراض أو الاستيلاء على بيانات الحاسوب، وإنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب، واختراق الخصوصية أو أساليب حماية البيانات.
- أفعال خاصة بتحقيق مصالح شخصية أو مادية أو إيذاء عبر الحاسب الآلي كالاحتيال، والتزوير، والجرائم ذات الصلة بالهوية، وحقوق الطبع والنشر، وجرائم العلامة التجارية، وإرسال أو السيطرة على إرسال البريد المزعج.
- الأعمال ذات الصلة بأجهزة الحاسوب الشخصية التي تسبب الضرر ومنها إنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال، والأعمال ذات الصلة بأجهزة الكمبيوتر في دعم جرائم الإرهاب والجرائم المنظمة (البداينة، ٢٠١٤م).

البند الثاني: خصائص الجرائم الرقمية

تعتبر الجرائم الرقمية شكلاً متطوراً من أشكال الجريمة الجنائية نظراً لتطور وسائل التقنية الحديثة وانتشارها على نطاق واسع، وبالتالي فهي تنفرد بخصائص تميزها عن الجريمة التقليدية، ومن أهم هذه الخصائص أنها ترتكب في بيئة الحاسب الآلي وبأحد وسائل التقنية الحديثة؛ أي أن الجريمة توجه إلى النظام المعلوماتي، ولأن الجريمة ترتكب في بيئة غير تقليدية وهي بيئة الحاسب الآلي فهي لا تخلف آثاراً مادية كتلك التي تخلفها الجريمة التقليدية، وهذا ما يجعلها توصف بأنها جريمة هادئة أي أنها ترتكب دون استخدام أية وسائل للعنف، بالإضافة إلى عدم ارتباط الجريمة بحدود دولة معينة حيث إنه يمكن وصفها بالجريمة الدولية مخترقة الحدود، وأخيراً تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني حيث إن القواعد القانونية التقليدية لم تكن مخصصة لهذا النوع من الجرائم وخاصة في مجال الإثبات الجنائي؛ كما في

(٢) وعرف نظام مكافحة الجريمة الإلكترونية السعودي الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ بناء على قرار مجلس الوزراء رقم (٧٩) بتاريخ ١٤٢٨/٣/٧هـ الجريمة الإلكترونية بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة الإلكترونية بالمخالفة لأحكام هذا النظام".

حالة تفتيش الشبكات أو عمليات اعتراض الاتصال التي تكون على بيانات في الغالب مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة ومن هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة (هجيج، ٢٠٠٧م).

الفرع الثاني: الأدلة الرقمية

البند الأول: ماهية الدليل الرقمي وخصائصه وأنواعه

الدليل لغة هو المرشد، والجمع أدلة وأدلاء ودلائل (المعجم الوسيط، ٢٠١١م)، أما الدليل في الاصطلاح القانوني هو الوسيلة المشروعة التي يستعين بها القاضي لتمكنه من الوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا السياق كل ما يتعلق بالوقائع المعروضة على القاضي وإعمال حكم القانون عليها (سرور، ١٩٩٦م).

ويمكن تعريف الدليل الرقمي بأنه "أية معلومات إلكترونية (رقمية) لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، والممكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة أي فعل له علاقة بالجريمة الرقمية" (قنديل، ٢٠١٥م).

ومما سبق يتبين أن الدليل الرقمي هو ذاته الدليل الإلكتروني وقد عرفه البعض بأنه عبارة عن معلومات يقبلها العقل مأخوذة من أجهزة الحاسوب، ويأخذ ذلك الدليل شكل مجالات أو نبضات مغناطيسية أو كهربائية من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، ويمكن تقديمها في شكل دليل يعتمده القضاء (الحلبي، ٢٠١١م)، وعرفه البعض الآخر بأنه "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما" (مصطفى، ٢٠١٠م)، وعلى ذلك ترتكز عملية الإثبات الجنائي للجرائم الرقمية على الدليل الرقمي باعتباره الوسيلة الوحيدة لإثبات هذا النوع من الجرائم.

وتتميز الأدلة الرقمية بعدة خصائص من أهمها أنها أدلة غير مادية وغير مرئية لأنها متعلقة بالنظام المعلوماتي في بيئة الحاسب الآلي، ولا يمكن التوصل إليها إلا من خلال الأجهزة الحاسوبية، وأيضاً يمكن استخراج نسخ من الأدلة الرقمية مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية، كما يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها (الحلبي، ٢٠١١م). ومن خصائص الدليل الرقمي أيضاً أنه متعلق بوسائل التقنية الحديثة سريعة التطور، وغير مرئي (الغافري، ٢٠٠٩م)، مما ينتج عنه صعوبة تتبع الدليل بالطرق التقليدية المتبعة في الجريمة التقليدية كالمشاهدة والتتبع والتسمع وغيرها.

ويوجد نوعين من الأدلة الرقمية الأول منها أدلة أعدت لتكون وسيلة إثبات، كالسجلات التي تم إنشاؤها بواسطة الآلة تلقائياً مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي والسجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤه بواسطة الآلة، كالبيانات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات (مركز هردو لدعم التعبير الرقمي، ٢٠١٤م)، وثانيها أدلة لم تعد لتكون وسيلة إثبات، وهذا النوع من الأدلة الرقمية عبارة عن أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى "بالبصمة الرقمية"، وهي ما يمكن تسميته أيضاً "بالآثار المعلوماتية الرقمية"، والتي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل أو استقبال الرسائل المرسلة منه أو إليه، وكذلك كافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العنكبوتية، ومن الجدير بالذكر أن الوسائل التقنية الخاصة والحديثة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من وقت نشوئها (حجازي، ٢٠٠٩م).

وأبرز الأماكن التي يحتمل وجود الدليل الرقمي فيها هي:

١- أجهز الحاسب بأنواعها المختلفة.
٢- البرمجيات.
٣- ملحقات الحاسب كالمودم والطابعات.
٤- وسائط التخزين المتحركة كالأقراص المدمجة والأقراص المرنة والأقراص الصلبة.
٥- المراشد الخاصة بالعتاد أو البرمجيات.

٦- كلمات السر أو أرقام الهاتف التي تكون مكتوبة على أوراق ملصقة بالحواسيب أو بقربها.
٧- سلة المهملات وما بها من أوراق مطبوعة ذات علاقة بالحاسب محل الفحص (عبدالرحمن، ٢٠١٥م).

البند الثاني: حجية الدليل الجنائي الرقمي في الإثبات

يخضع الدليل الإلكتروني (الدليل الرقمي) إلى طبيعة نظام الإثبات السائد في الدولة سواء كانت تتبنى مبدأ حرية الإثبات كالقانون الفرنسي؛ أو مبدأ تحديد الأدلة التي يجوز للقاضي الجنائي قبولها كالقانون الهولندي، أو مبدأ حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة. أما في مرحلة تحديد العقوبة يكون مبدأ حرية الإثبات كتشريعات الدول الأنجلو سكسونية (قنديل، ٢٠١٥م).

والدليل الرقمي شأنه شأن باقي الأدلة التقليدية يخضع لنفس القواعد من حيث مدى مشروعيته واقتناع القاضي الجنائي به، ولذلك فلابد أن يكون الدليل يقينياً ويخضع لسلطة القاضي الجنائي في تقدير الأدلة وذلك على التفصيل التالي.

أولاً: قوة الدليل الإلكتروني في الإثبات

اتجه مشرعي دول أوروبا منذ منتصف الثمانينيات لإقرار حجية الوثائق الإلكترونية ومساواتها بالوثائق الكتابية من حيث الحكم، وقد امتد هذا الرأي ليشمل الأدلة الجنائية الرقمية باعتبارها أحد أقسام الأدلة المادية العلمية بل إنها تعد أكثر منها حجية في الإثبات لأنها محكمة بقواعد علمية وحسابية لا تقبل التأويل ومعالجة بوسائل التقنية المعلوماتية[٣] (عبدالرحمن، ٢٠١٥م)، وهذا ما أدى إلى مشروعية الدليل الرقمي من حيث وجوده ضمن الأدلة الجنائية المعتبرة قانوناً.

وهناك قواعد محددة يجب أن تتبع للتأكد من سلامة الدليل الرقمي منها علم الكمبيوتر والمعلومات الفنية التي تساهم بدورها في فهم مضمون الدليل الرقمي، وكذلك الاستعانة بفكرة التحليل التناظري الرقمي التي تساهم في الكشف عن مدى مصداقية الدليل الرقمي؛ بالإضافة إلى ما يعرف بالدليل المحايد والذي يساعد في التأكد من صحة الدليل الرقمي، ولمناقشة الدليل أثناء المرافعة أيضاً دور مهم للتأكد من سلامته (سهيل، ٢٠١٨م)، وفي هذا الخصوص يجب عدم إهمال دور الخبير الفني حيث إن الخبرة وسيلة إثبات تهدف إلى الكشف عن مدى صحة الدليل ويقينيته وتقوم بدور فعال في مساعدة القضاء لتشكيل أساسٍ رصينٍ في تقدير الأدلة الرقمية.

وأيضاً من القواعد الفنية التي تساهم في تقييم الدليل الرقمي من حيث مدى سلامته ما يعرف باختبارات "داو بورت" والتي تتمثل في إخضاع الأداة المستخدمة في استخلاص الدليل لعدة تجارب تقنية للتأكد من مدى دقتها في صحة وسيلة استخلاص الدليل وتحقيق النتائج المبتغاة منه (الحلبي، ٢٠١١م).

وحتى تعتبر الأدلة الالكترونية مقبولة لابد من توافر عدة شروط أهمها أن تكون هذه الأدلة يقينية مبنية على الجزم واليقين وليس على الشك والاحتمال، وأن يتم مناقشة الدليل الرقمي أثناء المرافعة من الخصوم بعد مواجهتهم به ليتمكنوا من الرد عليه تحقيقاً لحق الدفاع؛ بالإضافة إلى أنه لابد أن يتم الحصول على الدليل الرقمي بوسيلة مشروعة بما يتفق مع القواعد القانونية الخاصة بجمع الأدلة وتحقيقها والضمانات الواجب توافرها فيها، وألا يستمد الدليل من إجراء باطل.

ثانياً: سلطة القاضي الجنائي في تقدير الدليل الرقمي

للقاضي السلطة التقديرية الكاملة في تقييم كل دليل مقدم إليه ومدى حجيته في إثبات الواقعة الإجرامية حيث يستطيع أن يأخذ به أو يطرحه جانباً، وهو ما يعرف بمبدأ الاقتناع القضائي والذي أقرته معظم التشريعات الحديثة[٤].

(٣) صدر قرار الهيئة العامة للمحكمة العليا بالمملكة العربية السعودية رقم (٣٤) بتاريخ ١٤٣٩/٤/٢٤هـ وقد نص على أن "الدليل الرقمي حجة معتبرة في الإثبات القضائي، متى سلم من العوارض، ويختلف قوة وضعفاً حسب الواقعة وملابساتها وما يحتف بها من قرائن" (غير منشور).

(٤) نص المشرع الفرنسي على مبدأ حرية القاضي في الاقتناع بالمادة (٣٤٢) من قانون التحقيقات الجنائية وتم تكريس هذا المبدأ في المواد من (٤٢٧-٥٣٦) من قانون الإجراءات الجنائية الفرنسية، وورد ذلك المبدأ في المادة (٢٠٢/ ١) من قانون الإجراءات الجنائية المصرية حيث نصت على أنه "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته".

ورغم القوة الثبوتية للدليل الرقمي فإنه يثير بعض المشاكل التي من الممكن أن تؤثر على القاضي في تكوين عقيدته ومنها - كما سبق وأوضحنا جزءاً من هذه المشكلات - أنه دليل غير مرئي، وأن الأصالة في الدليل الإلكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي التقليدي الذي يعبر عن وضعية مادية ملموسة، وأخيراً أن الدليل الرقمي ذو طبيعة ديناميكية ويصعب تعقبه وضبطه خاصة إذا ارتكبت الجريمة أو جزء منها خارج حدود الدولة (قنديل، ٢٠١٥م).

هذا بالإضافة إلى المشكلات الإجرائية التي يثيرها التحقيق في هذا الدليل والسابق الإشارة إليها ومنها ارتفاع تكاليف الحصول عليه ونقص المعرفة التقنية لدى المحققين.

ولكي يتم التغلب على هذه المشكلات لابد للقاضي أثناء تقديره للدليل الرقمي أن يلتزم بالضوابط الخاصة بمبدأ اقتناعه القضائي في تقدير الأدلة الجنائية؛ كضرورة أن يستمد القاضي اقتناعه من أدلة لها أصل وارد في أوراق الدعوى وأن تكون طرحت عليه في الجلسة، وأن تكون هذه الأدلة مشروعة غير مستمدة من إجراءات باطلة، وألا يبني القاضي اقتناعه على القرائن والدلائل وحدها (حمو، ٢٠١٧م)؛ بالإضافة إلى أنه يجب على القاضي الجنائي أن يبني اقتناعه على اليقين وأن يكون تقديره مبنياً على أسباب معقولة (يونس، ٢٠١٤م)، أيضاً يجب أن يكون اقتناع القاضي مبنياً على أدلة متساندة؛ تكمل بعضها البعض، وتتكون عقيدة القاضي منها مجتمعة وهو ما يعرف بمبدأ "تساند الأدلة في الإثبات الجنائي"، وأن يبين الأدلة التي اعتمد عليها في تكوين عقيدته وذلك من خلال تسبيب حكمه في الدعوى الجنائية(٥)، وأخيراً يجب أن تكون قناعة القاضي بالدليل ليست مبنية على مجرد اليقين الشخصي وإنما على اليقين القضائي الذي يمكن أن يصل إليه الكافة لسلامة حجته ومنطقه.

(٥) نصت المادة (١٣٠/ ١) من نظام الإجراءات الجزائية السعودي على أنه "يجب أن تحرر مسودة الحكم قبل النطق به وأن تشتمل على رقم الدعوى وتاريخها وأسبابه .....".

المبحث الثاني:
إجراءات التحقق الجنائي الرقمي

يتسع مجال إجراءات التحقيق في أي جريمة ليشمل التحقيق في أي دليل يصلح أن يثبت أو ينفي حقيقة ما في الدعوى الجنائية وذلك تطبيقاً لمبدأ حرية الإثبات، وسنقتصر في هذا المبحث على الإجراءات التي تصلح أن تكون محلاً للتحقيق الجنائي الرقمي في بيئة المعالجة الآلية للبيانات وهي المعاينة والتفتيش والشهادة والخبرة والضبط، وسنتناولها في مطلبين مستقلين.

المطلب الأول: المعاينة والتفتيش في الجرائم الرقمية

سنتناول في هذا المطلب إجراءات المعاينة والتفتيش في الجرائم الرقمية كل في فرع مستقل.

الفرع الأول: إجراءات المعاينة في الجرائم الرقمية

البند الأول: الأحكام العامة للمعاينة في الجرائم الرقمية

المعاينة هي المشاهدة والملاحظة المباشرة لمسرح الجريمة، وإثبات حالته الراهنة والآثار المادية التي خلفها ارتكاب الجريمة، والتغيرات التي طرأت على الأشخاص والأشياء الموجودة فيه، واستنتاج الحقائق منه (الكاملي، ٢٠١٥م).

وتبدو أهمية المعاينة في أنها تعتبر بمثابة الفحص المادي الدقيق للجريمة وآثارها، ومكان وقوعها أو مادتها، والأدوات التي تم استعمالها في ارتكابها، وبيان كافة الآثار والقرائن التي يستعان بها في الاستدلال على المتهم، وكذلك تبدو أهمية نتائج المعاينة في أنها تمد التحقيق بفكرة مادية محسوسة ذات إثبات مادي محقق، وهذا القدر في نتائج المعاينة لا تساويه الثبوتيات الأخرى كالأقوال والإفادات التي ترد في محاضر الدعوى وتقارير الخبراء، وهذا كله إذا ما تم إثبات المعاينة في إجراءات موثقة تمت بجدية تامة (الدرعان، ٢٠١٣م).

ومعاينة مسرح الجريمة المعلوماتية (الجريمة الرقمية) يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية وتشمل كافة رسائله وكافة اتصالاته التي تمت من خلال الكمبيوتر والشبكة العالمية (ممدوح، ٢٠٠٩م).

ويلاحظ أن دور المعاينة في مجال كشف غموض الجرائم الرقمية أو المعلوماتية لا ترقَى إلى نفس الدرجة من الأهمية في الجرائم التقليدية وذلك لأن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها آثاراً مادية، وأن كثيراً من الأشخاص قد يترددون على مسرح الجريمة خلال الفترة الزمنية من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبياً، الأمر الذي يعطي الفرصة للجاني أو للآخرين أن يعبثوا بالآثار المادية للجريمة إن وجدت مما يدعو للشك في قيمة هذه الأدلة المستمدة من المعاينة (حجازي، ٢٠٠٢م).

البند الثاني: كيفية إجراء المعاينة

تتم المعاينة في الجرائم الالكترونية (الجرائم الرقمية) كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، ولكن طبيعة الانتقال تختلف حسب طبيعة الجريمة الرقمية المرتكبة، وما إذا كانت الجريمة واقعة على المكونات المادية للأجهزة الإلكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص المغنطة، حيث يكون الانتقال مادياً إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على ما يعد من الأدلة؛ أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الإنترنت فيكون الانتقال للمعاينة افتراضياً أو إلكترونياً، ويمكن إجراؤه بالانتقال إلى مسرح الجريمة عبر الإنترنت من مكتب المحقق بواسطة الحاسب الموضوع تحت تصرفه، أو إحدى مقرات مزود خدمات الإنترنت (جمال، ٢٠١٨م).

ويكون محل المعاينة الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر حيث إنها قد تكون ثرية جداً فيما تحتويه من معلومات مثل "صفحات المواقع المختلفة Web Pages والبريد الإلكتروني E-mail، والفيديو الرقمي Video Digital، والصوت الرقمي Digital Audio، وغرف الدردشة والمحادثة Digital Logs of Synchronous Chat Sessions، والملفات المخزنة في الكمبيوتر الشخصي Files Stored on Personal Computer، والصورة المرئية Digitized Still Images، والدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات Computer Logs from an Internet Service Provider (ISP)" (ممدوح، ٢٠٠٩م).

وحتى تنتج المعاينة أثرها في كشف الحقيقة في الجرائم الرقمية يجب الأخذ بعين الاعتبار عدداً من الإجراءات المهمة التي لابد أن تتبع كضرورة تصوير الحاسب والأجهزة الطرفية المتصلة به، وذلك حتى يتم تسجيل وقت وتاريخ ومكان التقاط الصورة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، وأيضاً لابد من إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها، بالإضافة إلى التأكيد من عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة؛ كما يجب التحفظ على ما يكون بسلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص المغنطة غير السليمة، وفحصها، ورفع ما عليها من بصمات، والتحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة[٦] (فرغلي، ٢٠٠٧م).

الفرع الثاني: إجراءات التفتيش في الجرائم الرقمية

البند الأول: الأحكام العامة للتفتيش في الجرائم الرقمية

يعتبر التفتيش من أهم إجراءات التحقيق التي تهدف إلى ضبط الأدلة ويعرف بأنه البحث في مستودع السر للوصول إلى أدلة وبيانات عن الجريمة (الطريسي، ٢٠١٦م)، ويمكن تعريف التفتيش أيضاً بأنه البحث عن الأشياء المتعلقة بالجريمة وكل ما يفيد في كشف حقيقتها على سند من القانون.

ويتفق التفتيش مع المعاينة في أن كلاً منهما إجراء من إجراءات التحقيق الغرض منه جمع الأدلة المادية عن الجريمة المرتكبة؛ إلا أنهما يختلفان في أن الهدف من إجراء التفتيش هو الحصول على دليل مادي؛ بينما المعاينة إجراء يهدف إلى إثبات حالة الأمكنة والأشياء والأشخاص وكافة الآثار المتعلقة

(٦) انظر أيضاً: إدارة الدراسات والبحوث، *دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول*. المركز العربي، (٢٠١١م)، ص ص ١-١٨.

بالجريمة؛ كما أن التفتيش يلزم أن يتم في حضور المتهم أو من ينوب عنه أما هذا الأمر غير مطلوب في المعاينة؛ بالإضافة إلى أن للمحقق سلطة تقديرية في القيام بالتفتيش من عدمه؛ أما المعاينة فهي إجراء إلزامي على المحقق يجب القيام به بمجرد إخطاره بالجريمة (العاقل، ٢٠٠٣م).

ويقصد بالتفتيش في الجرائم الرقمية البحث في النظم المعلوماتية محل التحقيق، وهو ما يسمى بالوعاء الإلكتروني والذي يشمل جهاز الكمبيوتر والأجهزة المتصلة به، والشبكة التي تشمل في مكوناتها مقدم الخدمة، والمزود الآلي، والمضيف، والملحقات التقنية ولذلك ينصب التفتيش على المكونات التالية:

١- مكونات مادية Hardware، وأخرى منطقية Software، أو ما يصطلح على تسميته بالقطع الصلبة والبرمجيات.
٢- شبكات اتصال بعدية Networks Telecommunication سلكية ولا سلكية محلية ودولية (مصري، ٢٠١٢م).

ويجب للتفتيش في هذا النوع من الجرائم توافر عدة شروط موضوعية وشكلية؛ أما أهم الشروط الموضوعية فهي سبق وقوع جريمة رقمية، ووجود دلائل كافية لتوجيه الاتهام ضد شخص أو أشخاص معينين بارتكاب الجريمة، بالإضافة إلى وجود محل للجريمة كأجهزة الحاسب وما تحويه من بيانات؛ أما بالنسبة للشروط الشكلية فلابد من صدور إذن مسببٍ بالتفتيش من السلطة المختصة بإصداره وتحرير محضر يشمل على كافة التفصيلات والإجراءات المتعلقة بعملية التفتيش وما أسفر عنها.

ويجب على سلطات التفتيش والضبط المحافظة على البيانات المنسوخة أو المرفوعة وذلك بالتحفظ عليها في الحالة التي تم العثور عليها لحظة الضبط وذلك عن طريق ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها، ومراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية وتأمين نقلها وحملها؛ بالإضافة إلى تأمين البرامج المضبوطة قبل تشغيلها بعمل نسخ سليمة وكاملة منها مع ضرورة الالتزام بالتسلسل الإجرائي للضبط (عبدالرحمن، ٢٠١٥م).

وقد نصت المادة (٢٣/ ١) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل".

البند الثاني: كيفية إجراء التفتيش

قد يقع إجراء التفتيش في الجرائم الرقمية على الحاسب الآلي أو المكونات المادية والمعنوية الخاصة به أو على أجهزة الحاسب الآلي المتصلة مع بعضها البعض والتي تقع في أماكن متفرقة داخل وخارج الدولة.

أولاً: تفتيش الحاسب الآلي

يمكن أن يتم تفتيش الحاسب الآلي بعدة طرق أهمها:

١- تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.
٢- تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.
٣- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.
٤- ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.
٥- مراعاة دور القطع الصلبة الخاصة بالحاسوب في ارتكاب الجريمة (الغافري، ٢٠٠٩م).

ثانياً: تفتيش المكونات المادية والمعنوية للحاسب الآلي

قد يكون التفتيش على مكونات الحاسب المادية مثل Hardware أو المعنوية (البرمجية) مثل Software أو على شبكات اتصال Network Telecommunications سلكية ولاسلكية محلية ودولية.

وإذا كان التفتيش على المكونات المادية للحاسب الآلي فإنها تخضع للتفتيش والضبط وفقاً لقانون الإجراءات الجزائية حسب التشريعات المختلفة؛ فإذا كان الحاسب موجوداً في مكان خاص كمسكن المتهم أو أحد ملحقاته فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المسكن وبالضمانات

المقررة قانوناً؛ أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب المادية أو كان حائزاً لها أو مسيطراً عليها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبذات الضمانات القانونية اللازمة لهذا الأمر؛ أما إذا كان التفتيش على مكونات الحاسب المعنوية فإن البيانات والمعلومات المخزنة في الحاسب الآلي تصلح أن تكون محلاً للتفتيش، ويمكن ضبطها واستنساخها على الورق أو على الأقراص أو على أي دعامة أخرى كالفلاش ميموري Flash Memory؛ بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم للجريمة (العبيدي، ٢٠١٣م).

ثالثاً: تفتيش أجهزة الحاسب الآلي المتصلة مع بعضها البعض والتي تقع في أماكن متفرقة داخل وخارج الدولة

١- اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم (١٠٣) من قانون الإجراءات الجزائية الألماني، كما نصت المادة (٨٨) من قانون تحقيق الجنايات البلجيكي على أنه "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث ممكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي ويتم هذا الامتداد وفقاً لضابطين، أولاً: إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث، وثانياً: إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث، وبالتالي فإن التفتيش في هذه الحالة لابد أن يخضع للقيود والضمانات التي يوجبها النظام الإجرائي لتفتيش الأمكنة" (الغافري، ٢٠٠٩م).

٢- اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة خارج إقليم الدولة

المادة (٢٥/أ) من قانون الحاسوب الهولندي استثنت هذه الحالة، فيمكن الحصول على الأدلة حتى لو كانت في إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمني والقضائي والخاصة بالتفتيش وضبط الأدلة (الطوالبة، ٢٠٠٩م)، وقد أكدت ذلك المادة (٣٢) من الاتفاقية الأوروبية بشأن الجرائم المعلوماتية والتي أعدها المجلس الأوروبي وتم التوقيع عليها في بودابست عام ٢٠٠١م حيث نصت (مجلس أوروبا، ٢٠٠١م) على أنه "يجوز للدولة الطرف في الاتفاقية وبدون تفويض من دولة أخرى طرف في بالاتفاقية وبدون تفويض من دولة أخرى طرف في الاتفاقية: (أ) الدخول علناً وبشكل متاح على بيانات الكمبيوتر المخزنة بغض النظر عن مكان تواجد البيانات جغرافياً. (ب) الدخول على أو تلقي عن طريق منظومة كمبيوتر بأراضيها بيانات الكمبيوتر المخزنة الموجودة بدولة أخرى طرفاً بالاتفاقية وذلك حالة حصول الدولة الطرف على الموافقة القانونية والطواعية من الشخص الذي له حق التفويض قانوناً في الكشف عن البيانات للدولة الطرف بالاتفاقية من خلال منظومة الكمبيوتر هذه".

٣- المراقبة الإلكترونية لشبكات الحاسب الآلي

يرى جانب من الفقه أن المراقبة الإلكترونية لشبكات الحاسب الآلي والتنصت على الشبكات الدولية والمراقبة الهاتفية واعتراض اتصالات عبر شبكات تبادل المعلومات مسموح به في جميع الدول تقريباً حماية لأمن هذه الدول، ويؤكد ذلك أن القضاء في هولندا قد أمر بالتنصت على شبكات اتصالات الحاسوب إذا كانت هناك جرائم خطيرة متورطاً فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسوب بشرط الحصول على إذن تفتيش صادر من القاضي (الحلبي، ٢٠١١م)، وفي جنوب أفريقيا يمكن مشروع تعديل قوانين الاستخبارات العامة من فرض المراقبة على الاتصالات الأجنبية خارج جنوب أفريقيا أو التي تمر عبر أراضيها، وفي ديسمبر ٢٠١٢م اعتمدت الجمعية الوطنية في باكستان القانون المتعلق بالمحاكمة العادلة لعام ٢٠١٢م الذي ينص في الفقرة (٣١) منه على تنفيذ أوامر المراقبة في ولايات قضائية أجنبية،

وفي عام ٢٠١٢م أيضاً أنشأ المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية مشروع معايير يمكّن الحكومات الأوروبية من اعتراض الخدمات السحابية(٧).

المطلب الثاني: الشهادة والخبرة والضبط في الجرائم الرقمية

سنتناول في هذا المطلب إجراءات الخبرة والشهادة والضبط في الجرائم الرقمية في فرعين مستقلين باعتبارها من إجراءات التحقيق الهامة في الجرائم الرقمية.

الفرع الأول: إجراءات الشهادة والخبرة في الجرائم الرقمية

البند الأول: الشهادة في الجرائم الرقمية

الشهادة هي أحد إجراءات التحقيق وتتضمن الإدلاء بمعلومات أدركها الشاهد بإحدى حواسه أو بأكثر من حاسة وذلك أمام سلطات التحقيق وفق الضوابط التي نص عليها القانون؛ فالشهادة هي إخبار عن إدراك الشاهد لواقعة ما عبر حاسة من حواسه (الطريسي، ٢٠١٦م)، ويجب أخذ إفادة الشهود فور وقوع الجريمة حيث يعد ذلك أمراً بالغ الأهمية لأن الشهادة تنصب على وقائع مادية تقع فجأة دون أن يترتب إثباتها بالكتابة، ولا يدخلها أي من التعديل أو التغيير (الدرعان، ٢٠١٣م).

وتعد الشهادة من أقدم وأبرز وسائل الإثبات والحصول على الأدلة الجنائية سواء في مرحلة التحقيق أو المحاكمة.

وتخول القوانين الإجرائية المختلفة سلطة تقديرية واسعة للمحقق في سماع من يرى لزوم سماعهم من الشهود حتى ولو بناء على طلب الخصوم؛ فللمحقق أن يرفض سماع أحد الشهود سواء طلب الخصوم سماعه أو حضر من تلقاء نفسه، وكذلك سماع من يرغب فالهدف من ذلك تمكينه من تحديد الشهود الذين يرجح أن تكون لشهادتهم قيمة في كشف الحقيقة وذلك عن الوقائع التي تؤدي إلى ثبوت الجريمة وإسنادها إلى المتهم أو نفيها عنه (تاج الدين، ٢٠١٤م).

ويرى جانب من الفقه يرجحه الباحث من جانبه أن الشهادة في مجال الجريمة المعلوماتية (الجريمة الرقمية) لا تختلف من حيث ماهيتها عن الجريمة التقليدية (العدواني، ٢٠١٥م).

وقد يكون الشاهد المعلوماتي في الجريمة الرقمية – في رأي جانب من الفقه – هو الفني صاحب الخبرة والتخصص في مجال تقنية المعلومات والحاسب الآلي وشبكات الاتصال الرقمية الذي تكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للبيانات في حال ما إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله (أحمد، ٢٠٠٦م).

والشاهد المعلوماتي قد يكون واحداً من عدة طوائف هم:

١- مشغلو الحاسب الآلي: وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به وتكون لديهم معلومات عن قواعد كتابة البرامج.

٢- المحللون: والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتقسيمها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها، وكذلك تتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

٣- المبرمجون: وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

- الفئة الأولى: هم مخططو برامج التطبيقات ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة لتحقيق هذه المواصفات.
- الفئة الثانية: هم مخططو برامج النظم ويقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها.

(٧) فرانك لا رو، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير. مجلس حقوق الإنسان، الدورة الثالثة والعشرون، البند (٣) من جدول الأعمال، تعزيز وحماية جميع حقوق الإنسان المدنية والسياسية والاقتصادية والاجتماعية والثقافية بما في ذلك الحق في التنمية. متاح على الرابط الإلكتروني:
https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y

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

٥- مديرو النظم: وهم الذين يتولون أعمال الإدارة في النظم المعلوماتية (آل ثنيان، ٢٠١٢م).

ويقع على عاتق الشاهد عدة التزامات كأهمية الحضور أمام المحقق للإدلاء بالشهادة في المكان والوقت المحددين للاستماع إلى شهادته، ويكون ذلك بناء على إعلانه بالحضور بواسطة السلطة المختصة بذلك، ويجب عليه أيضاً الالتزام بحلف اليمين قبل أداء الشهادة بالإضافة إلى قول الحقيقة والالتزام بتقديم كافة المعلومات اللازمة للولوج إلى نظام الحاسوب والتعاون مع سلطة التحقيق في هذا المجال.

وأثير تساؤل حول مدى إمكانية التزام الشاهد المعلوماتي بطبع الملفات والإفصاح عن كلمات المرور والشفرات حيث يرى جانب من الفقه الألماني أنه ليس من واجب الشاهد أن يقوم بذلك لأن الالتزام بالإدلاء بالشهادة لا يتضمن هذا الواجب؛ كما يعتبر هذا البحث من اختصاص الخبير القضائي، وتبنت كل من ألمانيا وتركيا هذا الاتجاه؛ بينما يرى جانب آخر من الفقه الفرنسي أن من بين الالتزامات التي يتحمل بها الشاهد المعلوماتي طبع الملفات والإفصاح عن كلمات المرور والشفرات لأن القواعد العامة في مجال الإجراءات تحتفظ بذات سلطاتها في مجال الإجراءات المعلوماتية (مصطفى، ٢٠١٠م)، ويرى الباحث من جانبه أنه يجب على الشاهد أن يمد جهات التحقيق بكل ما لديه من معلومات جوهرية ولازمة للولوج إلى نظام معالجة البيانات بالحاسب الآلي للتمكن من إثبات أو نفي الجريمة الرقمية.

إجراءات سماع الشهادة أمام المحقق

يوجد عدد من الإجراءات المهمة التي تحكم سماع المحقق للشهادة كضرورة تدوين بيانات الشاهد في محضر التحقيق، وكذلك بيانات المحقق والكاتب، أيضاً لابد من التزام المحقق بعدم التأثير على الشاهد أثناء إدلائه بشهادته، ومناقشته في مضمون الشهادة وتدوين أقوال الشاهد في محضر التحقيق ثم التوقيع على المحضر منه ومن المحقق والكاتب، وللمحقق أن يستمع لكل شاهد على انفراد وله أن يواجه بالشهود الأخرى والخصوم أو بكليهما، ويتم توجيه الأسئلة من المحقق إلى الشاهد حتى لو كانت من أحد الخصوم إلا أنه يجوز أن توجه الأسئلة من الخصوم مباشرة إلى الشاهد بعد إذن المحقق.

البند الثاني: الخبرة في الجرائم الرقمية

الخبرة هي وسيلة يقررها المشرع لمساعدة القاضي في تقدير المسائل التي يحتاج إثباتها إلى معرفة خاصة علمية أو فنية من خلال إبداء رأي فني من شخص مختص فنياً في الدعوى الجنائية، وقد ازدادت الخبرة في الوقت الحاضر نظراً لتقدم العلوم التي تشمل دراستها الوقائع التي تتصل بوقوع الجريمة (حمد، ٢٠١١م)، ويزداد هذا الأمر أهمية في نطاق الجرائم الرقمية التي تعتمد على التطور المستمر في آليات تكنولوجيا المعلومات والاتصالات في هذا العصر الرقمي والذي أفرز العديد من الأنشطة المستحدثة التي تتم باستخدام الوسائل الإلكترونية، التي قوامها نظم وبرمجيات الحاسب الآلي، والشبكات الحاسوبية وشبكات الاتصالات العالمية (الإنترنت).

وتجيز كافة الأنظمة لأعضاء سلطتي الاستدلال والتحقيق ندب الخبراء للإفادة بمعلوماتهم في المسائل الفنية المتعلقة بالدعوى الجنائية، والخبير في إفادته بمعلوماته الفنية يأخذ حكم الشاهد إلا أنه يختلف عنه من حيث الوقائع التي يشهد بها، فالشاهد يدلي بالمعلومات التي أدركها بأحد حواسه عن الواقعة الإجرامية؛ أما الخبير فشهادته فنية يحكمها تخصصها العلمي الدقيق (تاج الدين، ٢٠١٤م)، وهذا ما يؤيده الباحث من جانبه.

وللخبير التقني في سبيل تحري الحقيقة في الجريمة الرقمية أن يقوم بكل ما يمكنه التوصل إليه من معلومات تفيد في كشف الحقيقة كالقيام بتجميع وتحصيل المواقع التي تشكل جريمة في ذاتها، القيام بتجميع وتحصيل الوقائع التي لا تشكل جريمة في ذاتها وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب الجرائم (الغافري، ٢٠٠٩م).

ومن أهم واجبات الخبير التقني حلف اليمين، وأدائه لمهمته بنفسه في حدود القانون، واستجابته للطلبات التي

يوجهها الأطراف أثناء مباشرة مهمته في الدعوى؛ ثم تقديم التقرير الفني خلال المدة المحددة قانوناً لذلك.

وأما عن مدى حجية تقرير الخبير، فالخبرة شأنها شأن باقي أدلة الإثبات تخضع حجيتها لتقدير القاضي ومدى تأثير أعمال الخبرة في الاقتناع الذاتي للقاضي، ولذلك محكمة الموضوع لها كامل السلطة في تقدير القوة الدليلية لعناصر الدعوى المطروحة على بساط البحث، وهي الخبير الأعلى في كل ما تستطيع هي أن تفصل فيه بنفسها ما دامت المسألة المطروحة ليست من المسائل الفنية البحتة التي لا تستطيع المحكمة بنفسها أن تشق طريقها لإبداء الرأي فيها (فرغلي، ٢٠٠٠م).

الفرع الثاني: ضبط الأدلة في الجرائم الرقمية

البند الأول: الأحكام العامة للضبط في الجرائم الرقمية

يحقق الضبط الغاية من التفتيش وهذه الغاية هي التي تمثل مشروعية التفتيش، وضبط الأشياء يعني التحفظ عليها ووضعها تحت يد المحقق ليقرر ما يراه في شأنها وفقاً لما تقتضي به مجريات التحقيق في جريمة وقعت بالفعل نظراً لأن هذه الأشياء ذات ارتباط بالجريمة وتفيد في كشف الحقيقة[٨] (شريف، ٢٠١٦م).

ويختلف الضبط في الجريمة الإلكترونية (الجريمة الرقمية) عن الضبط في غير ذلك من الجرائم من حيث المحل؛ فالأول قد يرد على أشياء ذات طبيعة معنوية كالبيانات، والمراسلات والاتصالات الإلكترونية؛ أما الثاني فيرد على أشياء مادية سواء كانت منقولات أو عقارات (قنديل، ٢٠١٥م).

ويعتبر من أدوات الضبط الوسائل المادية التي تساعد في ضبط الجريمة الرقمية كبرامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التنصت على الشبكة، ومراجعة قاعدة البيانات وبرامج النسخ الاحتياطي للأقراص الصلبة.

وكذلك من الوسائل والبرمجيات التي تساعد على الضبط في الجريمة الرقمية ما يلي:

١- البريد الإلكتروني وبرامج المحادثة.
٢- البروكسي Proxy.
٣- برامج التتبع.
٤- نظام كشف الاختراق IDS.

البند الثاني: محل الضبط

قد يكون محل الضبط في الجريمة الرقمية الأدلة المادية أو الأدلة المعنوية على التفصيل التالي.

أولاً: الأدلة المادية

ويتمثل معظمها فيما يلي:

١- الأوراق وتشمل الأوراق التحضيرية كالمسودات التي تكون بخط اليد، والأوراق التالفة التي تم إلقاؤها في سلة المهملات بعد طباعتها، والأوراق الأصلية التي تم طباعتها والاحتفاظ بها كمرجع، وكذلك الأوراق الأساسية والقانونية المحفوظة في الملفات العادية أو دفاتر الحسابات والتي لها علاقة بالجريمة.
٢- أجهزة الحاسب الآلي وملحقاتها كالمودم Modem ولوحة المفاتيح Keyboard ووحدة المعالجة المركزية CPU والسماعات Speakers والماوس Mouse والشاشة Monitor والسيرفر Server والطابعة Printer.
٣- أقراص الليزر حتى ولو لم يكن معها أجهزة الحاسب الآلي متى كانت محتوياتها عنصراً من عناصر الجريمة.
٤- البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستعملة في إعداد تلك البطاقات.
٥- الشرائط الممغنطة Magnetic Tapes.
٦- لوحة الدوائر Circuit Boards and Components (الفيل، ٢٠١٥م).

---

(٨) وحددت المادة (٨٠) من نظام الإجراءات الجزائية السعودي الأشياء التي يمكن ضبطها بقولها: "..... 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 ....."، كما نصت المادة (٥٥) من قانون الإجراءات الجنائية المصري على أنه "لمأمور الضبط القضائي أن يضبط الأوراق والأسلحة والآلات وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليه الجريمة وكل ما يفيد في كشف الحقيقة ....."

ثانياً: الأدلة المعنوية

تتمثل الأدلة المعنوية في البيانات الرقمية، ولقد أثار ضبط هذا النوع من الأدلة خلافاً فقهياً بين فقهاء القانون الجنائي وانقسم الفقه إلى رأيين:

- الرأي الأول: يذهب مؤيدو هذا الرأي ومعظمهم من الفقهاء الألمان إلى أنه لا يمكن ضبط البيانات المعلوماتية (الرقمية) ووضع اليد عليها لأنها ليس لها مظهر خارجي مادي محسوس كالأشياء المادية، ولذلك لا يمكن ضبطها إلا إذا تم تفريغها في كيان مادي محسوس مثل طبع هذه البيانات على الورق أو خزنها على دعامة مادية كالأقراص المغناطيسية أو تصوير البيانات على الشاشة أو أي واسطة تخزين أخرى.
- الرأي الثاني: يرى أنصار هذا الرأي ومنهم جانب آخر من الفقه الألماني أنه لا يوجد ما يمنع من ضبط البيانات المعلوماتية (الرقمية) حيث إن المادة (٢٥١) من قانون الإجراءات الجنائية اليوناني تعطي الإمكانية لسلطات التحقيق بالقيام بأي شيء يكون لازماً وضرورياً لجمع وحماية الدليل (حسين، ٢٠١١م).

ويؤيد الباحث من جانبه الاتجاه الأول حيث إنه لا يمكن ضبط البيانات الرقمية إلا إذا تم تفريغها في شيء مادي ملموس كالديسكات مثلاً أو الأسطوانات الممغنطة، ويجب أن يقوم بهذا الإجراء الخبير المعلوماتي[٩].

وقد دعا هذا الخلاف المشرع الجنائي في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلاً عن الأشياء المادية البيانات المعالجة إلكترونياً كقانون تحقيق الجنايات البلجيكي في المادة (٣٩) المدخلة في التقنين بمقتضى القانون الصادر في ٢٣/ ١١/ ٢٠٠٠م والتي بمقتضاها يشمل الحجز الأشياء المادية وكذلك البيانات المعالجة إلكترونياً (الفيل، ٢٠١٥م).

(٩) حدد نظام مكافحة جرائم المعلوماتية السعودي الجهة التي تقوم بمساعدة جهات التحقيق في ضبط الأدلة الرقمية بهيئة الاتصالات وتقنية المعلومات حيث نصت المادة (١٤) من هذا النظام 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".

الخاتمة

لقد حاول الباحث من خلال هذا البحث أن يوضح الآليات التي يقوم عليها التحقيق الجنائي في مجال الجرائم الرقمية أو المعلوماتية التي ترتكب في بيئة الحاسب الآلي وعبر الشبكات المعلوماتية، حيث إن التحقيق بالطرق التقليدية لن يجدي أثره بالنسبة لهذا النوع المستحدث من الجرائم بصورها المختلفة، وقد تناول الباحث في هذا البحث مقدمة حول التحقيق الجنائي الرقمي اشتملت على ماهية وخصائص هذا التحقيق ثم محل التحقيق الجنائي الرقمي فيما يتعلق بالجريمة الرقمية والأدلة الرقمية وذلك في مبحث أول؛ ثم تناول الباحث في مبحث ثاني أهم إجراءات التحقيق الجنائي الرقمي التي تثير بعض الصعوبات وهي المعاينة والتفتيش والشهادة والخبرة والضبط، ولقد توصل الباحث في هذا البحث إلى العديد من النتائج والتوصيات أهمها ما يلي.

أولاً: النتائج

١- خطورة الجرائم الرقمية وصعوبة إثباتها وسهولة إتلاف أدلتها لأنها لا تخلف آثاراً مادية.
٢- الدليل الجنائي الرقمي يحتاج إلى خبرات تقنية عالية ومتميزة في مجال الحاسب الآلي وتقنية المعلومات وشبكات الاتصال لإمكانية استخلاصه بطريقة تزيل الشك عنه وتؤكد قوته الثبوتية.
٣- عدم إلمام بعض المحققين بالإجراءات الفنية الواجب اتباعها عند التعامل مع أجهزة الحاسوب بمسرح الجريمة، وكيفية التعامل مع الأدلة الرقمية.
٤- ندرة الخبراء الفنيين الجنائيين في مجال تكنولوجيا المعلومات.
٥- إن الجريمة الرقمية بكافة صورها لها خصوصيتها وطبيعتها المختلفة عن الجريمة التقليدية وتفترض بذل جهود إضافية لتحقيقها والتعامل مع أدلتها.

ثانياً: التوصيات

١- ضرورة تعرف جهات التحقيق على أحدث التقنيات في مجال تكنولوجيا المعلومات والتدرب عليها وإجادة

استخدامها حتى يمكن الكشف عن هذه الجرائم وملاحقة مرتكبيها ومعرفة الأساليب الفنية التي تستخدم لارتكاب هذه الجرائم.

٢- ضرورة التعاون الدولي الإجرائي بين جهات التحقيق المختلفة وذلك في مجال التدريب وتبادل الخبرات ونقل المعلومات وتحقيق قاعدة ازدواجية التجريم أي أن تكون الجريمة معاقباً عليها في كل من قانون دولة الجاني والمجني عليه.

٣- إنشاء قضاء إلكتروني متخصص لنظر قضايا الجرائم الرقمية ويراعى فيها التطور التكنولوجي في عالم الجريمة الرقمية.

٤- تخصيص دائرة مستقلة في النيابات العامة للتحقيق في الجرائم الرقمية.

٥- توفير تجهيزات ضرورية للحصول على الدليل الرقمي كالأجهزة المختصة بتسجيل حركة البيانات في الشبكات، وأجهزة وبرامج إدارة ومراقبة الشبكات.

٦- تدريس مقررات في كلية الحقوق تتناول مفردات وآليات التحقيق الجنائي الرقمي.

٧- رصد وتتبع المواقع المشتبه فيها على الشبكة المعلوماتية.

٨- استخدام الحاسب الآلي في استخراج صحيفة الحالة الجنائية وحفظ صور البصمات آلياً حتى يسهل الكشف عن شخصية مرتكب الجريمة.

٩- إنشاء قاعدة معلوماتية جنائية متطورة تربط بين كافة حدود الدولة.

١٠- إنشاء معامل جنائية إلكترونية لفحص الأوراق والمستندات المتحصلة من الجريمة.

قائمة المراجع

أولاً: الكتب والأبحاث العربية

أحمد، هلالي عبدالله (٢٠٠٦م). *التزام الشاهد بالإعلام في الجريمة المعلوماتية (دراسة مقارنة)*. القاهرة: دار النهضة العربية.

إدارة الدراسات والبحوث (٢٠١١م). دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول. *المركز العربي*، ص ص ١-١٨.

آل ثنيان، ثنيان ناصر (٢٠١٢م). *إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، تخصص السياسة الجنائية، ص ٩٣.

البداينة، ذياب موسى (٢-٤ سبتمبر ٢٠١٤م). *الجرائم الإلكترونية: المفهوم والأسباب*. ورقة علمية مقدمة في الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، ص ٨.

البشري، محمد الأمين (١-٣ مايو ٢٠٠٠م). *التحقيق في جرائم الحاسب الآلي*. بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ص ١٠٧٣.

البوسعيدي، هلال بن محمد بن حارب (٢٠٠٩م). *الحماية القانونية والتقنية لقواعد المعلومات المحوسبة (دراسة قانونية وفنية مقارنة)*. القاهرة: دار النهضة العربية.

تاج الدين، مدني (٢٠٠٤م). *أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية: دراسة مقارنة*. منشورات الجوهر.

جمال، براهيمي (٢٠١٨م). *التحقيق الجنائي في الجرائم الإلكترونية*. أطروحة، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، ص ص ٥٧-٥٨.

حجازي، عبدالفتاح بيومي (٢٠٠٢م). *الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت*. القاهرة: دار الكتب القانونية.

حجازي، عبدالفتاح بيومي (٢٠٠٩م). *الدليل الرقمي في جرائم الكمبيوتر والإنترنت*. القاهرة: دار بهجت للطباعة والنشر.

حسني، محمود نجيب (١٩٩٨م). *شرح قانون الإجراءات الجنائية*. ط٣، القاهرة: دار النهضة العربية.

حسني، محمود نجيب (٢٠١٣م). *شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات التشريعية*. ج١، القاهرة: دار النهضة العربية.

حسين، سامي جلال فقي (٢٠١١م). *التفتيش في الجرائم المعلوماتية (دراسة تحليلية)*. مصر: دار الكتب القانونية.

الحلبي، خالد عياد (٢٠١١م). *إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت*. دار الثقافة للنشر والتوزيع.

حمد، أيمن فاروق عبدالمعبود (٢٠١١م). *الإثبات الجنائي في القانون المقارن والفقه الإسلامي وتطبيقاته في النظام السعودي: دراسة مقارنة*. ط١.

حمو، نضال ياسين الحاج (٢٠١٧م). مبدأ اقتناع القاضي الجنائي (دراسة تحليلية في ضوء التشريع البحريني والمقارن). *مجلة كلية القانون للعلوم القانونية والسياسية*، جامعة كركوك، مج(٦)، ع(٢٢)، ص ٥١٤.

الخفاجي، علي حمزة عسل (٢٠١٥م). التحقيق الابتدائي. *مجلة العلوم الإنسانية*، كلية التربية للعلوم الإنسانية، جامعة كربلاء، مج(٣٣)، ع(١)، ص ٤١٩.

الدرعان، عبدالله بن عبدالعزيز (٢٠١٣م). *المبسوط في قواعد الإجراءات الجزائية مع مقدمة في القضاء*. ط١، الرياض: مكتبة التوبة.

السرحاني، محمد بن نصير محمد (٢٠٠٤م). *مهارات التحقيق الفني في جرائم الحاسوب والإنترنت*. رسالة ماجستير، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، ص ص ٢٠-٧١.

سرور، أحمد فتحي (١٩٩٦م). *الوسيط في قانون الإجراءات الجنائية*. ط٧، القاهرة: دار النهضة العربية.

سلامة، مأمون محمد (١٩٧٧م). *الإجراءات الجنائية في التشريع المصري*. القاهرة: دار الفكر العربي.

سهيل، بن قدوم وأمال، بهنوس (٢٠١٨م). *الدليل الرقمي في الإثبات الجنائي*. رسالة ماجستير، جامعة عبدالرحمن نيرة بجاية، ص ٨٠.

شريف، السيد محمد (٢٠١٦م). *الوجيز في نظام الإجراءات الجزائية السعودي*. ط١، مكتبة دار النشر العربي.

صالح، ابن منصور وأنيسة، كوش (٢٠١٥م). *السلوك الإجرامي للمجرم المعلوماتي*. رسالة ماجستير في الحقوق، جامعة عبدالرحمن نيرة بجاية، ص ص ٣٦-٣٩.

الطريسي، فهد نايف محمد (٢٠١٦م). *الإجراءات الجزائية في المملكة العربية السعودية*. ط١، الرياض: دار الكتاب الجامعي للنشر والتوزيع.

الطوالبة، علي حسن (٢٠٠٩م). مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة). *مركز الإعلام الأمني*، ص ١١.

العاقل، إلهام محمد حسن (٢٠٠٣م). *التفتيش في قانون الإجراءات الجزائية اليمني (دراسة مقارنة)*. ط١.

عبدالله، أيمن (٢٠١٥م). *الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية*. الرياض: مكتبة القانون والاقتصاد للنشر والتوزيع.

عبدالرحمن، محمد جلال (٢٠١٥م). *الجرائم الإلكترونية في الفقه الإسلامي (دراسة مقارنة)*. الرياض: مكتبة القانون والاقتصاد للنشر والتوزيع.

العبيدي، أسامة بن غانم (٢٠١٣م). التفتيش عن الدليل في الجرائم المعلوماتية. *المجلة العربية للدراسات الأمنية والتدريب*، مج(٢٩)، ع(٥٨)، ص ٨٩.

العدواني، محمد نافع فالح رشدان (٢٠١٥م). *حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانون الكويتي والأردني)*. رسالة ماجستير، جامعة الشرق الأوسط، القانون العام، ص ٨٢.

العريان، محمد علي (٢٠٠٤م). *الجرائم المعلوماتية*. الإسكندرية: دار الجامعة الجديدة للنشر.

الغافري، حسين بن سعد (٢٠٠٩م). *السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)*. القاهرة: دار النهضة العربية.

فرغلي، خبير عبدالناصر محمد محمود والمسماري، محمد عبيد سيف سعيد (١٢-١٤ نوفمبر ٢٠٠٧م). *الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)*. المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ص ص ١-١٨.

الفيل، علي عدنان (٢٠١٥م). *إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)*. الموصل: المكتب الجامعي الحديث.

القحطاني، عبدالله بن حسين آل حجراف (٢٠١٤م). *تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية*. رسالة ماجستير، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية بالرياض، ص ١٢.

قنديل، أشرف عبدالقادر (٢٠١٥م). *الإثبات الجنائي في الجريمة الإلكترونية*. الإسكندرية: دار الجامعة الجديدة للنشر.

الكاملي، محمد بن علي (٢٠١٥م). *إشكالات في إجراءات التحقيق الجنائي (دراسة تطبيقية)*. ط١، الرياض: مكتبة القانون والاقتصاد.

محمد، عوض (١٩٩٠م). *قانون الإجراءات الجنائية*. ج١، الإسكندرية: دار المطبوعات الجنائية.

مصري، عبدالصبور عبدالقوي علي (٢٠١٢م). *المحكمة الرقمية والجريمة المعلوماتية (دراسة مقارنة)*. ط١، الرياض: مكتبة القانون والاقتصاد.

مصطفى، عائشة بن قارة (٢٠١٠م). *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن*. الإسكندرية: دار الجامعة الجديدة للنشر.

المعجم الوسيط (٢٠١١م). إصدار مجمع اللغة العربية بالقاهرة، ط٥.

هجيج، محمد علي سالم وعبيد، حسون (٢٠٠٧م). الجرائم المعلوماتية. *مجلة بابل*، العلوم الإنسانية، مج(١٤)، ع(٢)، ص ص ٩١-٩٢.

يونس، بدر الدين (٢٠١٤م). *سلطة القاضي في تقدير الدليل الجنائي (دراسة مقارنة)*. أطروحة، جامعة قسنطينة، ص ١٢٤.

ثانياً: القوانين والأنظمة والقرارات

- قانون التحقيقات الجنائية الفرنسي، المادة (٣٤٢).
- قانون الإجراءات الجنائية الفرنسية المواد من (٤٢٧-٥٣٦).
- قانون الإجراءات الجنائية المصرية المادة (٢٠٢/ ١).
- نظام الإجراءات الجزائية السعودي المادة (١٣٠/ ١).
- نظام مكافحة جرائم المعلوماتية السعودي المادة (٨٠).
- قانون مكافحة جرائم تقنية المعلومات المصري، مادة رقم (١)، الباب الأول، رقم (١٧٥) لسنة ٢٠١٨م.
- قرار الهيئة العامة للمحكمة العليا بالمملكة العربية السعودية رقم ٣٤ بتاريخ ١٤٣٩/٤/٢٤هـ، غير منشور.

ثالثاً: مواقع الإنترنت

- خلف، جاسم خريبط. "صعوبة الدليل الجنائي في الجرائم المعلوماتية". كلية شط العرب الجامعة، متاح على الرابط الإلكتروني:
https://utq.edu.iq/Magazines/docxlaw2016/1.docx
- وزارة الداخلية بالبحرين. "الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني". إدارة مكافحة الجرائم الإلكترونية، متاح على الرابط الإلكتروني:
http://www.acees.gov.bh/cyber-crime/the-concept-of-e-crimes
- مركز هردو لدعم التعبير الرقمي (٢٠١٤م). "الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات". القاهرة، متاح على الرابط الإلكتروني:
http://hrdoegypt.org/wp-content/uploads/2014/12/ تقرير-الجريمة-الالكترونية-_٢_.pdf
- ممدوح، خالد (٢٠٠٩م). "معاينة مسرح الجريمة الإلكترونية". متاح على الرابط الإلكتروني:
https://kenanaonline.com/users/KhaledMamdouh/posts/81659
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، متاح على الرابط الإلكتروني:
http://haqqi.info/ar/haqqi/legislation/arab-convention-cyber-%E2%80%8B%E2%80%8Bcrimes
- مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم (١٨٥)، التقرير التفسيري لاتفاقية الجريمة الإلكترونية،

بودابيست، تاريخ ٢٣/ ١١/ ٢٠٠١م، ص ٥٠. متاح على الرابط الإلكتروني:
https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174

- فرانك لارو، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، مجلس حقوق الإنسان، الدورة الثالثة والعشرون، البند (٣) من جدول الأعمال، تعزيز وحماية جميع حقوق الإنسان المدنية والسياسية والاقتصادية والاجتماعية والثقافية بما في ذلك الحق في التنمية. متاح على الرابط الإلكتروني:
https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y