شكل الإجراءات المتعلقة بجمع الدلائل الإلكترونية والصعوبات المتعلقة بها

الباحث/ ليث عمر سالم السواخنة

(ISSN: 2537- 0758)

شكل الإجراءات المتعلقة بجمع الدلائل الإلكترونية والصعوبات المتعلقة بها

الباحث/ ليث عمر سالم السواخنة

الملخص

بعد انتهاينا من دراسة "**شكل الإجراءات المتعلقة بجمع الدلائل الإلكترونية والصعوبات المتعلقة بها**" والذى تناولنا فيه الكيفة التى يتم بها جمع الادلة الرقمية داخل هذه الوسط الافتراضى الذى لاتتلمسه الايدى ولاتراه الاعين سواء كان ذلك من خلال التفتيش أو الخبرة أو الشهادة، أما فيما يتعلق بالتفيش تناولنا الكيفية التى يتم بها تفتيش مكونات الحاسب الالى المادية والمعنوية وشبكات الاتصالات وبدات المشكلة واضحا جلية عندما يكون التفتيش خارج حدود الدولة وذلك عندما يقوم مجرمى المعلوماتية بتخزين بياناتهم خارج حدود الدولة وذلك عن طريق ما يعرف باسم شبكات الاتصالات البعدية وان حل هذه الاشكالية يكون عن طريق الاتفاقيات الدولية سواء أكانت ثنائية او جماعية، أما عن الخبرة فان دور الخبير مهم فى السيطرة على العملية الاثباتية وذلك على أساس أن البحث عن الدليل الرقمى داخل الوسط الافتراضى من المسائل التى يتعذر على القاضى الجنائى أن يشق الطريق إيها، وفيما يتعلق بالشهادة تناولنا الالتزامات الملقاه على عاتق الشاهد المعلوماتى وهل من واجبه الافصاح عن كلمات المرور، وكيف ان الاتجاهات الفقهية قد انقسمت فى هذا الصدد إلى مؤيد ومعارض لذلك.

أما عن قيمته نجد ان المشرع المصرى فى قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ قد اعترف للدليل الرقمى بقيمته فى الاثبات طالما توافرات فيه الشروط والضوابط التي يجب توافرها في الدليل الفني لقبوله والاعتراف بأثباته وقيمته الاستدلالية حسبما أشارت إلى ذلك اللائحة التنفيذية لهذا القانون الصادرة بموجب قرار مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠.

Summary

After we finished studying "the form of procedures related to the collection of electronic evidence and the difficulties related to it", in which we dealt with the manner in which digital evidence is collected within this virtual environment that neither hands nor eyes see, whether through inspection, experience or testimony, as for inspection, we have dealt with The way in which the material and moral components of the computer and communication

networks are inspected, and the problem began to become clear when the inspection was outside the borders of the state, when the informatics criminals stored their data outside the borders of the state, through what is known as the telecommunications networks, and the solution to this problem is through international agreements Whether it is bilateral or collective, as for experience, the role of the expert is important in controlling the evidentiary process, on the basis that searching for digital evidence within the virtual medium is one of the issues that the criminal judge is unable to pave the way for, and with regard to testimony, we dealt with the obligations of the witness Is it his duty to disclose passwords, and how the jurisprudential trends have been divided in this regard into supporters and opponents of that.

As for its value, we find that the Egyptian legislator, in Law No. 175 of 2018 on Combating Information Technology Crimes, recognized the value of the digital evidence in proof as long as it fulfills the conditions and controls that must be met in the technical evidence in order to accept it and recognize its proof and evidentiary value, as indicated by the executive regulations of this law issued pursuant to Cabinet Resolution No. 1699 of 2020.

المقدمة

ان الأحكام الإجرائية هي مجموعة من المبادئ والنصوص التي تحدد وتنظم الإجراءات التي يجب اتباعها من لحظة ارتكاب الجريمة حتى إعمال حق الدولة في العقوبة. وهو ما دعا إليه المشرع عند إصدار القانون رقم ١٧٥ لسنة ٢٠١٨ بضمان سن وتنظيم مجموعة مناسبة من الأحكام الإجرائية اللازمة التي يجب اتباعها لمكافحة جرائم المعلوماتية، وتحقيق نوع من التوازن بين ممارسة الحريات الإنسانية والحريات. الحقوق التي تواكب التطور التكنولوجي الحاصل، وما يقتضيه حق الدولة والأفراد في حالة الإخلال بممارسة هذا الحق.

ولابد من جمع عناصر التحقيق والدعوى ورفعها إلى هيئة التحقيق الابتدائي لتقوم بدورها في التحقق من الأدلة وتقديمها إلى المحكمة في حال توافرها لإثبات التهمة المنسوبة إليه. الجاني، وبعد ذلك تمارس المحكمة دورها في القضية بإدانة المتهم أو تبرئته حسب سلطتها التقديرية عن الأدلة المقدمة إليها في القضية.. حيث تعتبر الأدلة بشكل عام من أهم وأدق القضايا التي تواجه العدالة القضائية عند الفصل في الحقوق

(ISSN: 2537- 0758)

المتنازع عليها المعروضة عليها، حيث تهدف قواعد ووسائل الإثبات إلى كشف الحقيقة[١].

أهمية البحث

على مستوى الجرائم الإلكترونية، فإن التطور المطرد في أنواع هذه الجرائم وطريقة ارتكابها والوسائل المستخدمة في تنفيذها يجعل القائمين على مكافحتها في سباق مع الزمن لمواكبة ذلك التطور.، ويدعو الجهات القضائية إلى مراجعة كيفية التعامل مع هذه التطورات، حيث إن اتباع الإجراءات لا تعمل الجرائم التقليدية في كثير من الأحيان على مواجهة هذه الجرائم، بسبب المشاكل التي تثيرها نتيجة طبيعتها غير المادية والأدلة غير الملموسة التي تقدمها..

إشكاليات البحث

مما لاشك فيه أن موضوع شكل الإجراءات المتعلقة بجمع الدلائل الإلكترونية والصعوبات المتعلقة بها يثير العديد من الاشكاليات لعل من أهمها:-

١- ماهى إجراءات جمع الدليل الرقمى

٢- ماهو التفيش فى الجريمة المعوماتية

٣- وهل هناك التزام على الشاهد المعلوماتى فى الافصاح عن كلمات المرور

٤- وما هى قيمة الدليل الرقمى فى الاثبات الجنائى

منهج البحث:

تعتمد الدراسة على المنهج الوصفي التحليلي الذي يقوم على شرح الموضوع محل الدراسة بصورة تفصيلية من كافة جوانبه؛ ثم تحليلها من خلال النصوص القانونية والآراء الفقهية من أجل التوصل إلى نتائج منطقية يمكن الاعتماد عليها في تقرير مدى حجية الدليل الرقمي في إثبات الجرائم الواقعة على البيانات الشخصية، الأمر الذي دعا إلى أن يكون المنهج المقارن طريقًا آخراً نستعرض من خلاله موقف التشريعات المقارنة التي تعرضت لهذه المشكلة محل الدراسة.

---

[١] وهو ما يتجسد في نهاية المطاف في الحكم الصادر عن القضاء، وهذا فقط مع توافر الأدلة التي تؤكد تلك الحقيقة، سواء أكان المتهم قد أدين أو بُرّئ، فالدليل هو ما يؤدي إلى كشف الحقيقة. من أجل التحقق من وجود الأدلة اللازمة لإثبات القضية.

تقسيم البحث:

وانطلاقا من أهمية البحث وأهدافه سالفة الذكر، فقد رأينا تقسيم هذا البحث إلى مبحثين وذلك كالآتي:

المبحث الأول: الإجراءات المتعلقة بجمع الأدلة الإلكترونية والاستدلالات التقنية

المطلب الأول: التفتيش

المطلب الثاني: إجراءات الاستعانة بالخبرة الفنية المناسبة.

المطلب الثالث: الشهادة

المبحث الثاني: الحجية القانونية للأدلة الرقمية والشكل الاجرائى المتبع فيها

المطلب الأول: الإجراءات المتعلقة بأنظمة التشغيل المختلفة الفرع الاول: الإجراءات المتعلقة بنقل البيانات في شبكة المعلومات

الفرع الثانى: إجراءات الحصول على بروتوكول العنوان الإلكتروني

المطلب الثاني: الحجية القانونية لتلك الأدلة المتحفظ عليها

المبحث الأول

الإجراءات المتعلقة بجمع الأدلة الإلكترونية والاستدلالات التقنية

تستخدم بشكل عام لجمع الأدلة في مختلف الجرائم، بما في ذلك الجرائم التقليدية والجرائم الجديدة. ومع ذلك، يختلف دور هذه الإجراءات في كل منها. في الجرائم التقليدية، يزداد هذا الدور بينما يتراجع في الجرائم الجديدة[٢]. مكان الجريمة عندما ارتكب جريمته مهما حاول محو كل الآثار الناتجة عن الجريمة والتخلص منها، ولكن في النهاية يجب أن يترك أثرا بفعلته، وهذا ويرجع حسب العلماء إلى الحالة النفسية والعواطف التي ترافق الجاني أثناء ارتكاب الجريمة[٣]. وقد نظمت التشريعات كيفية الحصول على الأدلة من خلال إجراءات المتابعة، والوصول إلى هدف إثبات الجريمة المرتكبة ومعرفة مرتكبها.

حيث نجد أن القانون أوكل العموري إلى الضابطة العدلية لتقوم بإجراءات ضبط الوقائع التي تحدد لها عقوبة جنائية، ويطالبها بجمع الأدلة لصالحها. والجناة حسب

---

[٢] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية،. عام ٢٠٠٩، ص. ٦٨.

[٣] د. إبراهيم صادق الجندي، ود. حسين حسن الحسيني، تطبيقات الحمض النووي في التحقيق والطب الشرعي، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٢، ص ٩.

(ISSN: 2537- 0758)

مقتضيات التحقيق والدعوى الجزائية[٤]، وبالتالي يختلفون في أداء واجباتهم بين رجال الشرطة الإدارية[٥].

كما اختلفت التشريعات والأنظمة الدولية فيما يتعلق بتحديد السلطة المختصة بالاستدلال والتحقيق في الجرائم، **وظهرت ثلاثة اتجاهات هي:**

الاتجاه الأول: يجمع بين صلاحيات الاستدلال والتحقيق والاتهام في يد هيئة واحدة، جهاز الشرطة، حيث تم اعتماد هذا الاتجاه من قبل تشريعات بعض الدول. العربية في الماضي[٦]، وتم تطبيقه لفترة زمنية من قبل إمارة دبي في دولة الإمارات العربية المتحدة[٧].

الاتجاه الثاني: هذا الاتجاه يحد من سلطة الاستدلال والتحقيق وبعض إجراءات التحقيق في حالة التكليف بجهاز الشرطة، فيما تتولى النيابة العامة صلاحيات التحقيق والاتهام[٨]، والبحريني[٩]، وقانون أصول المحاكمات الجزائية العماني[١٠].

---

[٤] د. حسن علام، قانون أصول المحاكمات الجزائية، الجزء الأول، المجلد الأول، مطبعة روز اليوسف، القاهرة، ١٩٨٢، ص ٨٠.

[٥] وتتمثل وظيفة الرقابة الإدارية في منع وقوع الجرائم من خلال اتخاذ الإجراءات الوقائية والاحتياجات اللازمة لحماية الأفراد في حياتهم وأموالهم وشرفهم، بالإضافة إلى حماية الأمن العام بشكل عام، بينما تبدأ وظيفة الرقابة القضائية بعد ذلك. وقوع الجريمة والمتمثل في جمع الاستدلالات المتعلقة بحدوثها ومرتكبها وملاحقتها وتسليمها إلى الجهات المختصة بالتحقيق، حيث إنها رقابية محكمة الجنايات ودليل إدانته أو براءته، ولمزيد من التفاصيل انظر: د. محمد أبو العلاء عقيدة، شرح قانون أصول المحاكمات الجزائية، الجزء الأول، دار النهضة العربية، ٢٠٠٣، ص. ٢٥٥ وما يليها.

[٦] د. جودة حسين جهاد، الوجيز في شرح الإجراءات الجزائية لدولة الإمارات العربية المتحدة، كلية شرطة دبي، طبعة، ١٩٩٤، ص. ٢٤٦

[٧] وتجدر الإشارة إلى أن إمارة دبي اعتمدت هذا النهج وفق قانون الإجراءات الجنائية في دبي العالمية ١٩٧١ م، حتى صدور القانون الاتحادي رقم ٣٥ لسنة ١٩٩٢م في شأن الإجراءات الجنائية، أثناء وجودها في سلطنة عمان. يتولى جهاز الشرطة هذه السلطة مباشرة حتى صدور المرسوم السلطاني رقم ١٩٩٩/٩٢م. وأسس القاضي النيابة العامة (النيابة العامة) كهيئة مستقلة لها صلاحيات التحقيق والاتهام.

[٨] د. جودة حسين جهاد، مرجع سابق، ص. ٢٤٧ وما يليها.

[٩] علي فضل البوعينين، مرحلة التفكير والأحكام العامة التي يخضع لها التحقيق في التشريع البحريني، دار النهضة العربية، القاهرة، ٢٠٠٤، ص. ٢٥.

الاتجاه الثالث: يستند هذا الاتجاه إلى إسناد صلاحيات الإثبات للشرطة، حيث تتولى النيابة العامة سلطة الاتهام وسلطة التحقيق لقاضي التحقيق[١١]، وقد اتخذت بعض التشريعات الإجرائية الجزائية الأجنبية والعربية. هذا الاتجاه مثل الفرنسية والألمانية والإيطالية والجزائرية والقانون اللبناني العربي[١٢].

ومن هنا حرص المشرع المصري على إصدار القانون رقم ١٧٥ لسنة ٢٠١٨ تنظم اللجنة الخاصة بمكافحة جرائم تقنية المعلومات ولائحتها التنفيذية إجراءات جمع الأدلة الفنية، حيث قامت بتقسيم هذه الإجراءات إلى ثلاثة أنواع. دليل على الأدلة الرقمية المستخرجة من الوسائل التقنية. وعليه نقسم هذا المبحث الى ثلاثة مطلب، التفتيش (مطلب أول)، إجراءات الاستعانة بالخبرة الفنية المناسبة (مطلب ثان)، الشهادة (مطلب ثالث)، **وذلك على النحو الاتى:-**

المطلب الأول
التفتيش

أولا: تعريف التفتيش وأهميته

١- **تعريف التفتيش:** وقد تم تعريفه من حيث الفقه بعدة تعريفات منها: "رؤية بعين مكان أو شخص أو شيء لإثبات حالته والتحكم في كل ما يلزم لإظهار الحقيقة".

---

[١٠] تناولت المادة (٤) من قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم ١٩٩٩/٩٧ وتعديلاته اختصاص النيابة العامة في إقامة الدعاوى العامة حيث نصت على أن "النيابة العامة مختصة برفع الدعاوى العامة. رفعها أمام المحكمة المختصة.... تقابلها المادة (١) من قانون المرافعات محكمة الجنايات المصرية طبقا للقانون الجديد رقم ١٧٤ لسنة ١٩٩٨ م.

[١١] ويرى من يتبع هذا النهج أن النيابة العامة (النيابة العامة) تجمع بين صلاحيات الاتهام والتحقيق بشكل يجعلها معارضة وقاضية في نفس الوقت مما يؤثر على إجراءات التحقيق وسير القضية، وهو خشي أن تؤثر قدرة الخصم على صفة القاضي. لمزيد من التفاصيل انظر: د. المستشار عبد الفتاح بيومي حجازي، مكافحة جرائم الحاسوب والانترنت العربي النموذجي، دار الفكر الجامعي، ٢٠٠٦، ص. ١٢٣.

[١٢] بذرة. جلال ثروت، أصول المحاكمات الجنائية، دار الجامعة للطباعة والنشر، Root BY، ١٩٨٨، ص ٧٥.

(ISSN: 2537- 0758)

وإثبات[١٣] آثارها وحالة الموجودين فيها، وتحفظ كل ما من شأنه تغييرها. تكشف الحقيقة[١٤].

٢- **أهمية التفتيش:** التفتيش من أهم إجراءات التحقيق في كشف الحقيقة لأنه غالباً ما ينتج عنه أدلة مادية تدعم نسب الجريمة للمتهم[١٥]. هو إجراء تحقيق يقوم به موظف مختص وفقاً للإجراءات القانونية في مكان يتمتع بالحرمة، بهدف الحصول على أدلة مادية على جناية أو جنحة، والتحقق من وقوعها لإثبات ارتكابها أو نسبها إلى المتهم، أو هو إجراء تحقيق تجريه سلطة يحددها[١٦]، القانون. يتم البحث في المستودع السري عن أدلة على الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة. المستودع السري هو شخص المتهم أو المكان الذي يعمل فيه أو يقيم فيه[١٧].

تتميز الجرائم التقنية الناتجة عن الاستخدام غير المشروع أو الاستغلال غير المشروع لوسائل تقنية المعلومات وما ينتج عنها من آثار تقنية معقدة بطابع خاص، وتتطلب متخصصين في نفس المجال لديهم درجة من المعرفة والمعرفة التقنية والقدرة على ذلك. كشف غموض هذه الجرائم وكشف أسرارها بالقبض على مرتكبيها ومعاينتهم أو من ساعد أو سهل ارتكابها. في فرنسا، تم تكليف فريق مكون من ١٣ شرطيًا بمهمة الإشراف على تنفيذ المهام الفنية الموكلة إليهم من قبل المدعين العامين والمحققين، وجميعهم تلقوا تدريبات تخصصية بالإضافة إلى كفاءتهم الأساسية في مجال التكنولوجيا الحديثة، ويرافقون المحققين أثناء التفتيش ويقومون بفحص كل جهاز ويقومون بنقل نسخة من القرص الصلب وبيانات البريد الإلكتروني، ثم يقدمون محضرًا يتم إرساله إلى قاضي التحقيق. بالنسبة للمعدات والبرمجيات، فهم يستخدمون برامج يمكنها استعادة

---

[١٣] د. محمد زكي أبو عامر، الإجراءات الجزائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٢، ص ٢٣٣.

[١٤] د. نجاتي سيد أحمد سند، أصول الإجراءات الجزائية في التشريع المصري، الجزء الأول، كلية الحقوق، جامعة الزقازيق، القاهرة، ٢٠٠٨، ص. ٥٣٠.

[١٥] عائشة بن قره مصطفى، مرجع سابق، ص. ٨٧.

[١٦] د. عبد الفتاح بيومي حجازي، مرجع سابق، ص. ٢٤٤.

[١٧] د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦م، ص٢٧٨-٢٧٩.

المعلومات من القرص الصلب، ويمكنهم أيضًا قراءة الأقراص المرنة والصلبة والتالفة، وهناك برامج تحت تصرفهم تمكنهم من قراءة أجهزة الحاسب الالي المحمولة[١٨].

ثانيا: مدى خضوع مكونات الحاسب الالى للتفتيش

١- التفتيش المتعلق بالمكونات المادية للجهاز الإلكتروني:

وصف المكان له أهمية قصوى في تحديد إجراءات التفتيش عليه، فإذا كان موقع المكونات المادية مع الشخص في مكان عام وحيازته، سواء كان المكان عامًا بطبيعته مثل الطرق العامة والساحات، أو هو مكان عام بمواصفات مثل المقاهي والحافلات العامة، ثم يخضع التفتيش هنا للحالات التي قد يتم فيها تفتيش الأشخاص بذات الضمانات والقيود المنصوص عليها في هذا الشأن. التفتيش على المكونات المادية للجهاز الإلكتروني بحثا عن أدلة أو أي شيء يتعلق بالجريمة الإلكترونية يفيد في كشف الحقيقة عنها أو الفاعل، يخضع للإجراءات القانونية والقواعد العامة لإجراء التفتيش، مثل الإجراءات التي هي يتم عند البحث في جريمة تقليدية لأن الغرض هنا هو البحث عن الأجزاء والمكونات المادية، كما يحدث عند تفتيش منزل أو شخص في جريمة سرقة أو قتل. وهذا يعني أن حكم فحص المكونات المادية للجهاز الإلكتروني يتوقف على طبيعة المكان الذي توجد فيه هذه المكونات المادية، سواء كان مكانًا عامًا أو مكانًا خاصًا[١٩].

لا يجوز تفتيش المكونات المادية إلا في الحالات التي يمكن فيها تفتيش المساكن، بنفس الضمانات والإجراءات المنصوص عليها في القانون في هذا المجال، مع مراعاة التمييز إذا كانت المكونات المادية للجهاز المراد تفتيشه معزولة عن الأجهزة الأخرى، أو متصلة بأجهزة أو أجهزة كمبيوتر أخرى في مكان أو مسكن. مكان آخر لغير المتهمين، وبالتالي إخضاعهم لإجراءات تفتيش مسكن غير المتهم[٢٠]. أما إذا كان مكان المكونات

---

[١٨] د. صالح أحمد البربري- دور الشرطة في مكافحة الجرائم الإلكترونية في إطار الاتفاقية الأوروبية الموقعة في بودابست بتاريخ ٢٠٠١/١١/٢٣- بحث منشور على الإنترنت على موقع الدليل الإلكتروني (www)..(arablawinfo.com. ٢٠٠٦/٩/٢. في التاريخ المحدد

[١٩] نبيلة هبة حروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الأدلة: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠١٣، ص. ٢٣٧.

[٢٠] د. علي حسن الطوالبة، شرعية الأدلة الرقمية المستمدة من التفتيش الجنائي ((دراسة مقارنة))، بحث منشور على الإنترنت، ص. ٦.
www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc

(ISSN: 2537- 0758)

المادية للجهاز الإلكتروني في مكان خاص، مثل محل إقامة المتهم أو أحد ملحقاته، فيكون لهذا المكان نفس الحكم أيضًا.

٢- الفحص ذو الصلة بالمكونات غير الملموسة للجهاز الإلكتروني:

تنقسم المكونات غير الملموسة للأجهزة الإلكترونية بشكل عام، وأجهزة الحاسب الالي بشكل خاص، إلى نوعين رئيسيين: قد تكون هذه المعلومات والبيانات موجودة على الشبكة وليس في نفس الجهاز المستخدم في الجريمة، لذلك تحتاج إلى أشخاص ذوي خبرة في هذه الشبكات والتقنيات لاستخراجها عند فحص المحتوى غير المادي للأجهزة، كما قد تحتاج إلى أذونات وتحقيقات مع مالكي مواقع الويب للحصول على معلومات مفيدة في اكتشاف الجريمة[٢١]. **أولهما** يختص بتشغيل الجهاز نفسه وتحسين أدائه بالبرامج المثبتة في الجهاز التي تعمل على ذلك، مثل عرض الشاشة الرئيسية للجهاز ونظام التشغيل الخاص به، **والنوع الثاني** منها يساعد لأداء عمله وتسهيل استخدامه للجهاز مثل برامج المكتب. عند استخدام هذه البرامج وحفظها، يتم إضافة ملف ومحتوى جديد إلى الجهاز لم يكن موجودًا من قبل، ويكون ذلك نتيجة استخدام المستخدم للجهاز[٢٢].

٣- فحص شبكات الجهاز الالكتروني: يقوم فحص هذه الشبكات على الفرضيات الاتية:-

- **الفرضية الأولى- حالة الاتصال لجهاز المتهم بجهاز آخر موجود في مكان آخر داخل الدولة:**

في هذه الفرضية، يبرز التساؤل حول احتمال أن يمتد الحق في التفتيش إلى جهاز أو محطة طرفية في مكان آخر يملكه شخص غير المتهم، إذا تبين أن جهاز المتهم أو الجهاز الطرفي في مسكنه متصل بـ هو- هي. في هذه الحالة، لا تنشأ المشكلة إذا كان المكانان يخضعان لنفس النظام. القانونية والولاية القضائية، كما هو الحال في الولايات المتحدة الأمريكية، مما يسمح بإجراء تفتيش صادر لمقر شركة معينة ويمتد إلى فروعها

تاريخ الزيارة ٢٠٠٩/٢٢/٨، ص. ٨٢.

[٢١] د. د. سامي جلال فقي حسين، التفتيش في جرائم المعلومات: دراسة تحليلية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، ٢٠١١، ص. ٢٣٩.

[٢٢] د. سامي جلال فقي حسين، التفتيش في جرائم المعلومات: دراسة تحليلية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، ٢٠١١، ص ٢١٧-٢١٨.

الموجودة في نفس العقار، ومن بين تطبيقات هذا الرأي وكذلك ما نص المشرع البلجيكي في المادة (٨٨) من قانون التحقيقات الجنائية البلجيكي، والتي تنص على أنه: "إذا أمر قاضي التحقيق بالبحث في نظام معلومات أو جزء منه، فيمكن أن يمتد هذا البحث إلى نظام معلومات آخر هو يقع في مكان غير مكان البحث الأصلي، ويتم هذا الامتداد وفق ضابطين: **أولاً**– إذا كان من الضروري الكشف عن حقيقة الجريمة المعنية. يبحث. **ثانياً**– إذا كانت هناك مخاطر تتعلق بفقدان بعض الأدلة بسبب سهولة محو البيانات أو إتلافها أو نقلها.

أما المشرع مصري، فقرر انه لا يجوز ذلك كما نصت المادة ٢١ يقوم مأمور الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الأدلة اللازمة للتحقيق والملاحقة.

وكذلك المادة ٢٢ مأمورو الضبط القضائي يتبعون النيابة العامة ويخضعون لإشرافه في أعمالهم الوظيفية.

للنائب العام أن يطلب من الجهة المختصة النظر في أمر من يرتكب مخالفة لواجباته أو تقصيراً في عمله، وله أن يطلب رفع الدعوى التأديبية ضده. كل هذا لا يمنع من رفع الدعوى الجنائية.

- **الفرضية الثانية– فرضية أن الجهاز المتهم متصل بجهاز أو طرف آخر موجود في مكان آخر خارج الدولة:**

في هذه الحالة، لا يمكن أن يتم تمديد أمر التفتيش إلى وكالة خارج الإقليم الجغرافي للدولة التي صدر منها أمر التفتيش بسبب التزام كل دولة بسيادتها وولايتها القضائية، إلا في وجود ثنائي خاص أو دولي الاتفاقات التي تسمح بهذا الإجراء، وهو ما يسمى التفتيش عبر الحدود أو البحث بعد[٢٣]. من الصعوبات التي تواجه جهات التحقيق في تتبع الأدلة الإلكترونية أن مرتكبي الجرائم الإلكترونية يقومون بتخزين المعلومات والبيانات في شبكات وأنظمة معلومات خارج الدولة باستخدام شبكات اتصال دولية بهدف عرقلة إجراءات التحقيق والوصول إليها.

لذلك، لا يمكن لهذه الجهات الحصول على المعلومات والبيانات المطلوبة إلا من خلال الاتفاقيات والمعاهدات والتعاون المشترك بين الدول، بالإضافة إلى تقنين شروط

[٢٣] نبيلة هبة حروال، مرجع سابق، ص. ٢٤٠.

(ISSN: 2537- 0758)

وأحكام هذه المواقع قدر الإمكان[٢٤]. من خلال نشر شائعات تضر بالأمن القومي للدولة على أحد مواقع التواصل الاجتماعي مثل تويتر أو فيسبوك، هنا على سلطات التحقيق، عند الرغبة في إثبات دليل المستخدم، الحصول على عنوان البريد الإلكتروني للمستخدم على الموقع، ثم مقارنته. بالبيانات المسجلة لدى شركة الاتصالات التي استخدمها المستخدم. من أجل الوصول إلى الموقع، إلا أن المسؤولين عن هذه المواقع، حفاظًا على سرية عملائهم وسمعة الموقع وكسب ثقتهم، يطالبون بشروط تعسفية ومعقدة وإجراءات طويلة من أجل منح المعلومات المطلوبة من قبل سلطات التحقيق.

المطلب الثاني
إجراءات الاستعانة بالخبرة الفنية المناسبة

عُرِّفت الخبرة القضائية بالعديد من التعريفات من قبل الفقه، ونذكر بعضاً منها، فقد عرفت بأنها: «إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص الدليل منه»[٢٥].

كما عُرفت بـ: "القدرة الفنية أو العلمية التي يفتقر إليها الشخص الذي يجري التحقيق، فيطلبها من أصحابها لحل مسألة تتعلق بها. التحقيق في الدعوى العامة المرفوعة أمامه، ويعرف كذلك"[٢٦]. مما لا شك فيه أن الجرائم المتعلقة بتقنية المعلومات تفرض الآن وجودها، وتنتشر بشكل كبير، لذلك كان لابد من الاستعانة بخبراء فنيين لمساعدة ضباط التحقيق والتحقيق والمحاكمة، وتزويدهم بالمعلومات الفنية. يُقصد بالمشورة عند الطلب، ومن خلال الخبرة، وفقًا لأحكام قانون تكنولوجيا المعلومات المصري، كل عمل يتعلق بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في المجالات الفنية. المعلومات[٢٧]. قام المشرع المصري بعمل جيد من خلال

---

[٢٤] د. حازم محمد حنفي، الأدلة الإلكترونية ودورها في المجال الجنائي، دار النهضة العربية، عام ٢٠١٧ ص. ٥٢.

[٢٥] د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار الفكر العربي، القاهرة، ١٩٨٨م، ص٦٤٥.

[٢٦] د. مظهر جعفر عبيد، شرح قانون الإجراءات الجنائية العماني، الجزء الأول، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، ٢٠٠٨ م، ص. ٥٤١.

[٢٧] مراجعة نص المادة الأولى من قانون تكنولوجيا المعلومات المصري المتعلق ببيان المعاني والمصطلحات.

تناوله صراحة لما ورد في الفقرة الأولى من المادة ١٠ من قانون جرائم تقنية المعلومات بشأن الحاجة إلى الاستعانة بخبراء فنيين في عملية البحث والتحقيق وجمع الاستنتاجات[٢٨].

من هذه التعريفات يتضح أن القاضي أو المحقق يلجأ إلى الخبرة الفنية في الجرائم بشكل عام في الوقائع التي تتطلب معرفة أو تفسير معرفة خاصة لا يملكها، فتلك الحقائق غير واضحة وغير مثبتة له ولا يمكن. أن يثبت بأية وسيلة أخرى من خلال ملف الدعوى والأدلة المقدمة فيه. يستخدم الخبير الفني لتوضيح ما يربكه بمعرفته ويقدم الرأي الفني الذي يحتاجه للوصول إلى الحقيقة. وإذا كان للتجربة ذلك الدور والأهمية في الجرائم التقليدية بشكل عام، فإن هذه الأهمية تزداد وتصبح ضرورية في إجراءات جمع الأدلة الإلكترونية لإثبات الجرائم الإلكترونية، حيث تتعلق هذه الجرائم بمسائل فنية معقدة للغاية، ومثل مسرح الجريمة فيها. ليست مادية، بالإضافة إلى التطوير المستمر في أساليب ارتكابها وتطوير وتنوع الأدوات المستخدمة فيها والتقنية بشكل عام، فالأجهزة الإلكترونية متنوعة ومتعددة، وكذلك شبكات الاتصال، وتنتمي التكنولوجيا إلى علوم مختلفة ولها تخصصات علمية وتقنية دقيقة ومتعددة، مما يتطلب وجود الخبرة لكشف سر الجريمة ومعرفة الفاعل والوصول إلى العدالة[٢٩].

وعليه سنتناول القواعد القانونية التي تحكم عمل الخبير بشكل عام. وإيجازاً، ومن ثم القواعد الفنية التي تحكم عمل الخبير الإلكتروني، **على النحو التالي:**

أولاً- القواعد القانونية المنظمة للخبرة الإلكترونية:

في هذه القواعد سنتطرق إلى اختيار الخبراء وواجبات الخبير الفني على النحو التالي:

أ. اختيار الخبراء:

كثيرا ما تحدد التشريعات طريقة اختيار الخبراء من خلال التسجيل في قائمة الخبراء التي تعدها وزارة العدل أو المجالس القضائية المختصة. ثم يتم اختيار الخبراء منه.

---

[٢٨] نصت الفقرة الأولى من المادة العاشرة على أنه "ينشأ سجلان بالوكالة لتسجيل الخبراء، يسجل أولهما الفنيون والفنيون العاملون بالوكالة، وفي الآخر خبراء الفنيين. وسيتم تسجيل الفنيين الذين لا يعملون بها".

[٢٩] عائشة بن قره مصطفى، مرجع سابق، ص ١٣٨– ١٣٩.

(ISSN: 2537- 0758)

وعليه تكون شروط اختيار الخبير وفق ما تحدده تلك الجهات عند إعلان التسجيل في تلك القوائم.

وفي الفقرة الثانية من نفس المادة تناول المشرع المصري تنظيم عمل الخبراء الفنيين، مبيناً التزاماتهم وواجباتهم وحقوقهم وضوابط المساءلة التأديبية مع الإشارة إلى مجموعة القواعد والأحكام التقليدية المعترف بها لتنظيم عمل الخبراء. قبل القضاء[٣٠].

وإدراكًا منه لأهمية دور الخبراء الفنيين في مجال تكنولوجيا المعلومات، فقد تناول المشرع المصري اللائحة التنفيذية للقانون الصادرة بموجب قرار مجلس الوزراء رقم (٢) للوزراء رقم ١٦٩٩ لسنة ٢٠٢٠، وطرق وشروط اختيار الخبراء وتنظيم عملهم وضوابط التسجيل في كل من السجلين المنصوص عليهما في القانون على النحو التالي:

أولا: قواعد وشروط قيد الخبراء في السجل الأول الخاص بالفنيين والتقنيين العاملين بالجهاز[٣١]:

١- أن يكون حاصلاً على مؤهل علمي أو تقني يتناسب مع مجال الخبرة. ٢- أن يكون قد أمضى سنة على الأقل في عمله بالمؤسسة. ٣- أن يجتاز الاختبارات الفنية التي يجريها الجهاز لمقدم الطلب. ثانياً: ضوابط وشروط قيد الخبراء في السجل الثاني للفنيين (٤) والفنيين غير العاملين بالهيئة: ١- أن يكون مصرياً بكامل الأهلية المدنية، ويجوز تسجيل الأجنبي بشرط أن يتعهد خطياً بأنه سيخضع للقوانين المصرية. ٢- أن يكون محمود السيرة حسن السمعة. ٣- ألا يكون قد سبق الحكم عليه بحكم نهائي في جريمة مخلة بالشرف. ٤- أن تكون لديه سيرة ذاتية تتضمن خبرة عمل مناسبة. ٥- موافقة الجهات المختصة بالأمن الوطني على القيد في السجل. في حالة عدم توفر أي من الشروط السابقة في الخبير يؤدي ذلك إلى شطب الخبير من السجل بقرار من الهيئة.

---

[٣٠] نصت الفقرة الثانية من المادة العاشرة على أن "... تطبق القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام القضاء على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم. واستثناء من تلك القواعد تسري قواعد وأحكام المساءلة الإدارية على الخبراء المقيدين بالسجل الثاني. وتحدد الإجراءات التأديبية المنصوص عليها في قانون تنظيم عملهم إن وجدت، واللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد في كل من السجلين".

[٣١] يراجع نص المادة (٤) من اللائحة التنفيذية للقانون سالفة البيان.

القواعد الفنية التي تحكم عمل الخبير الإلكتروني:

هناك بعض القواعد الفنية الخاصة التي تنفرد بها الخبير الإلكتروني عند تنفيذها، وقبل تحديد تلك القواعد ومعالجتها سنناقش أهم الأمور التي يحتاجها مأمور الضبط القضائي أو أحد أعضاء هيئة التحقيق من الخبير الإلكتروني ويكلفه بها، وكذلك كيفية القيام ببعض الإجراءات التي يحتاجها المفتش أو التفتيش، ويجب أن يكون الخبير على دراية بها وطريقة إجرائها، **وهي على النحو التالي:**

١. الإلمام بالموضوع المحتمل للدليل المادي والمعنوي ووصفه وشكله ونوعه وشكله.
٢. الإلمام ووصف تركيب الجهاز الإلكتروني وصنعه وطرازه، ونوع نظام التشغيل الذي يعمل عليه، وأهم الأنظمة والبرامج الفرعية المستخدمة في الجهاز، والأجهزة والملحقات المرفقة به، بالإضافة إلى إلى كلمات المرور والأسرار الخاصة بنظام التشفير ومسائل أخرى مماثلة.
٣. عزل نظام المعلومات دون إتلاف أو إتلاف الأدلة أو إلحاق الضرر بالجهاز، وبيان كيفية القيام بذلك.
٤. الإلمام بطبيعة بيئة الجهاز الإلكتروني وشبكاته ووصفها، من حيث تنظيمها، ومدة التركيز وعمل المعالجة التلقائية، ونوع وسائل الاتصال، وترددات موجات البث، ومواقع التخزين.
٥. القدرة على نقل الأدلة غير المرئية من الأدلة وتحويلها إلى دليل مرئي مقروء، حتى يتمكن الموظف القضائي أو عضو سلطة التحقيق من مشاهدتها وفهمها، مع إثبات مطابقة الدليل لصورته غير المرئية.
٦. نقل الأدلة الاستدلالية إلى الوسائط التقنية المناسبة والحاويات دون تلف أو تغيير، وشرح كيفية القيام بذلك[٣٢].

وحيث أن عملية جمع الأدلة الإلكترونية من أهم وأصعب الأمور في إثبات الجرائم الإلكترونية، وذلك لتعدد أشكال وصور الجرائم الإلكترونية، والتي تدور بين الحصول على معلومات للاستيلاء عليها أو إتلافها أو اختراق الأنظمة من خلالها، أو الاحتيال. وسرقة الأموال، أو مهاجمة الأجهزة الإلكترونية لتدميرها وتخريبها، أو لمجرد إظهار الذات وإثبات قدرتها في هذا المجال، لذا فإن الاستعانة بخبير إلكتروني وتقني أمر مهم

[٣٢] د. هشام فريد رستم، الجوانب الإجرائية لجرائم المعلومات، دار النهضة العربية، القاهرة ١٩٩٤، ص١٤٢-١٤٣.

(ISSN: 2537- 0758)

وملزم للوصول إلى اكتشاف الجريمة. وجانيها. يرى بعض المختصين في هذا الشأن أن عملية جمع الأدلة الإلكترونية في الجرائم الإلكترونية عبر الإنترنت تتم من خلال ثلاث مراحل رئيسية[٣٣] **وهي:**

- **المرحلة الأولى:** جمع المعلومات المخزنة في نهاية مزود خدمة الاتصال والوصول إلى شبكة المعلومات، من خلال تتبع الخوادم التي دخل منها الجاني، ومحاولة العثور على أي أثر إلكتروني له.
- **المرحلة الثانية:** وهي مرحلة المراقبة، وهي مبنية على افتراض وجوب عودة الجاني إلى مسرح جريمته، سواء بدخوله مرة أخرى أو بمراقبته والنظر إليه عن كثب. هناك طرق عديدة لمراقبة هذه الأجهزة وهي تختلف حسب ما تنتجه التكنولوجيا من تحديثات وبرامج خاصة لهذه المراقبة.
- **المرحلة الثالثة:** وهي مرحلة ضبط الأجهزة المشبوهة وفحصها فنياً وقانونياً. في هذه المرحلة يبدأ عمل الخبير الإلكتروني في فحص نظام الجهاز المشتبه به بكافة مكوناته المادية والمعنوية والشبكية، لاستخراج أدلة على إدانة الجاني وتحديد مدى قدرة الأدلة على ذلك، أو للوصول إلى حكم بالبراءة. النظام والأجهزة المشتبه في استخدامها في الجريمة.

عند قيام الخبير الإلكتروني باستخراج هذه الأدلة وجمعها، يجب عليه الالتزام ببعض القواعد والخطوات الفنية في هذا المجال. تتمثل هذه الخطوات والقواعد الفنية في المراحل التالية:

أ. خطوات ما قبل التشغيل والتفتيش:

- تأكد من أن وحدات نظام التشغيل صالحة.
- التأكد من مطابقة محتويات الضبطيات لما هو مكتوب عليها.
- تسجيل بيانات وحدات مكونات المجموعة مثل نوعها وطرازها ورقمها التسلسلي.

ب. خطوات التشغيل والفحص:

- إظهار الملفات المخبأة والنصوص المخفية داخل الملفات.
- استكمال تسجيل باقي بيانات الوحدات من خلال القراءات التي يوفرها الجهاز.
- عمل نسخة من جميع وسائط التخزين المضبوطة وأهمها القرص الصلب لإجراء المسح الأولي على هذه النسخة لحماية الأصل من أي خسارة أو تلف أو إتلاف

[٣٣] د. حازم محمد حنفي، مرجع سابق، ص ٦٩-٧٠.

سواء من سوء الاستخدام أو وجود فيروسات أو برمجيات. قنابل.

- تحديد أنواع وأسماء مجموعات البرامج مثل برامج النظام والتطبيقات وبرامج الاتصالات.
- استرجع الملفات التي تم محوها من الأصل باستخدام برامج استعادة البيانات، وكذلك الملفات المكسورة أو التالفة عن طريق إعادة تشغيلها وإصلاحها. ثم يتم تخزين هذه الملفات ويتم عمل نسخ مكررة من القرص أو القرص قيد الفحص من خلال تطبيق الخطوات المذكورة أعلاه.
- تحويل الأدلة الإلكترونية إلى شكل مادي عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صورًا أو نصوصًا أو وضعها في أي حاوية أخرى حسب نوع المعلومات والبيانات المكونة للأدلة. إعداد قائمة يسرد فيها الخبير الإلكتروني جميع الأدلة الإلكترونية التي تم الحصول عليها في حاوية خاصة، مع إجراء مراجعة لجميع الملفات المحفوظة في الحاوية في جهاز آخر للتأكد من سلامة القائمة.

ج- مدى العلاقة بين الدليل المادي والدليل الإلكتروني:

في هذه المرحلة، يتم فحص كل من الأدلة المادية المضبوطة والأدلة الإلكترونية في شكلها المادي، ومن ثم ربطها لإعطاء الأدلة الموثوقية واليقين، مما يؤدي إلى قبولها من قبل سلطة التحقيق والمحاكمة.

وأخيراً نشيد بسلوك المشرع المصري وحرصه على إسناد بعض الأعمال الفنية الدقيقة لخبراء فنيين على دراية كافية بشؤون وأنظمة تكنولوجيا المعلومات يتم اختيارهم وفق ضوابط وشروط معينة ليكونوا عوناً. ودعم جهات التحقيق والمحاكمة في مكافحة الجريمة التقنية وضبط أدلتها وهو سلوك جدير بالثناء لم نشهده. مثال على التشريع المقارن الذي لم يتعامل معه لا من قريب ولا من بعيد. وعلى الرغم من ذلك، فإننا ننتقد المشرع المصري لنصه في الرجوع إلى القواعد التقليدية التي تنظم عمل الخبراء والمطبقة أمام المحاكم، خاصة وأن عمل الخبير الفني يختلف تمامًا عن العمل العادي والتقليدي. الخبراء، لذلك كان لا بد له من طرح نصوص صريحة وواضحة لتنظيم عمل الخبراء التقنيين وتحديد اختصاصاتهم. التعبير صراحة عن جوهر هذا القانون أو اللائحة دون الرجوع إلى نصوص تقليدية قد لا تتناسب مع عمل الخبراء الفنيين وبعيدة عن أن تكون عامة في النص.

(ISSN: 2537- 0758)

المطلب الثالث
الشهادة

يُقصد بالشهادة عمومًا: "التعبير عن المضمون الملموس للشاهد بما رآه أو سمعه بنفسه من حيث المعلومات عن الآخرين التي لا تتوافق مع حقيقة الواقعة التي شهدها القضاء بعد حلف اليمين لمن كانت شهادتهم" المقبولين ومن لهم حق من غير الخصوم في الدعوى"[٣٤]. كما عُرِّفت بانها: "أقوال غير الخصوم أمام التحقيق أو المرجع القضائي بخصوص جريمة وقعت سواء كانت تتعلق بأدلة الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها"[٣٥].

يتضح لنا أن المشرع أجاز الإثبات بالشهادة إذا كان هناك مانع من الحصول على أدلة كتابية سواء كانت مادية أو أدبية، حتى لو تجاوزت قيمة الصفقة مائتي دينار أردني، وبالتالي يمكن قبول الشهادة في جميع الحالات التي يشترط فيها القانون كتابتها للإثبات وهذا النص يتفق مع نص المشرع المصري والمشرع الأردني[٣٦]. والمقصود بالاستحالة المادية من خلال ما ورد في النصوص السابقة، وهي الحالة التي يمنع فيها الحصول على المستند المكتوب لظروف استثنائية أو حوادث مفاجئة كالحريق أو الفيضانات، وهذا يشمل على سبيل المثال.، الإيداع العاجل الذي يتم في الظروف التي يخشى فيها الشخص من وجود خطر وشيك على الشيء دون أن يدرك أنه يجب أن يكون لديه الوقت أو الوسائل الكافية للحصول على صك مكتوب من الوديع[٣٧]. لذلك

---

[٣٤] د. سليمان مرقص، أصول الإثبات وإجراءاتها، الأدلة المقيدة، الجزء الثالث، دار الحلبي لإصدارات حقوق الإنسان، بيروت، ١٩٩٨، ص ١١.

[٣٥] عائشة بن قره مصطفى، مرجع سابق، ص. ١٢٥.

[٣٦] نصت المادة (٦٣) من قانون الإثبات المصري على ما يلي: ((يجوز إثبات بشهادة الشهود ما كان ينبغي إثباته بشهادة خطية: بينة، (ب) إذا فقد الدائن دعمه للكتاب لسبب أجنبي لا يثبت ذلك)).
– نصت المادة (٣٠) من قانون الإثبات الأردني المعدل لسنة ٢٠٠١ على ما يلي: ((يجوز الإثبات بالشهادة في الالتزامات التعاقدية حتى لو تجاوزت القيمة المطلوبة مائة دينار، ٢– إذا كان هناك مانع مادي أو معنوي يمنع الحصول على دليل مكتوب أو إذا كان العرف والعرف لا يتطلبان ربطه بسند)).

[٣٧] د. جامع، مرجع سابق، ص. ٦٤ نقلاً عن الأستاذ الدكتور عبد الودود يحيى، موجز في قانون الإثبات، ص. ١٢٥ وما يليها، الأستاذ الدكتور سليمان مرقص، مرجع سابق، الجزء الثاني، فقرة ٣٦٤ وما بعدها، ص ٤٠٠.

أعفى القانون الأطراف المتعاقدة من واجب الإثبات خطيًا، وسمح لهم بإثبات الإجراءات القانونية التي يختمونها بالشهادة، مشيرًا إلى أن وجود هذه الأسباب في حد ذاته لا يعني وجود مانع معنوى.، كما قد يكون هؤلاء ولا تمنع الدعوى من الحصول على بينة خطية، وهذا ما ذهبت إليه محكمة التمييز الأردنية بقولها: ((هذا وإن كانت المادة (٣٠) من قانون الإثبات تسمح بقبول الشهادة في إثبات معاملة المديونية بين أقارب الثاني)). الدرجة، إلا أن المدعي لم يكن مبنيًا. تم ربط المعاملة بينه وبين أخيه المدعى عليه كتابةً، مما يعني عدم وجود ثقة متبادلة بين الطرفين، وبالتالي عدم وجود المانع المعنوى الذي يسمح بالاعتماد على الشهادة السمعية في المعاملات بين الأقارب[٣٨]. كذلك، قد يكون هناك عائق لعدم التعامل كتابيًا في نوع معين من المعاملات نتيجة العادات أو العادات، وهو أمر غير مطلوب من أطراف المعاملة القانونية لإثباتها كتابيًا، وهنا أجاز المشرع لهم إثبات ذلك. هذه المعاملات بكل طرق الإثبات بالإضافة إلى الشهادة، وهذا ما ذهبت إليه محكمة التمييز الأردنية بقولها:

((تُقبل الأدلة الشخصية لإثبات الدين الناشئ عن سعر البدلات إذا ثبت أن العرف والعرف لا يتطلبان ربط المعاملة بين الخياط وزبونه بسند))[٣٩]. لكن السؤال الذي يطرح نفسه في هذا المجال هو هل إنشاء المستند الإلكتروني على سند إلكتروني مثل العقبة التي تحول دون الحصول على دليل مكتوب كامل؟

الشهادة هي حجة الإثبات، فإذا وقعت جريمة يسمع شهودها من غير أطراف الخصومة فيها لإثبات الجريمة ومعرفة وقائعها وتفاصيلها، ويكون سماع الشهود بالسماح لهم بالإدلاء بها. معلوماتهم حول الحادث الذي هو موضوع الاستدلال أو التحقيق أو المحاكمة. يجب أن يكون الشاهد الإعلامي وفق هذا المفهوم من ذوي الخبرة الفنية في مجال الجهاز الإلكتروني، وبالتالي يكون الشاهد الإعلامي ضمن الفئات أو الطوائف المتخصصة في هذا المجال، ونذكر أهم هذه الطوائف التي منها الشهود. في الجريمة الإلكترونية هي كما يلي:

---

[٣٨] التمييز القانوني رقم (٣٠٧-٧٥) مجلة نقابة المحامين الأردنيين، صادرة عام ١٩٧٦، العدد (٥-٦)، ص ٨٨١.

[٣٩] نقض الحقوق رقم (٤١٩/٦٥) مجلة نقابة المحامين الأردنيين الصادرة عام ١٩٦٦ العدد (٣-٤) ص ١١٣.

(ISSN: 2537- 0758)

أولا: **مشغلي الجهاز الالكتروني**:

هم الأشخاص ذوي الخبرة الذين لديهم معرفة كاملة بتشغيل الجهاز الإلكتروني وما يرتبط به من معدات وملحقات، واستخدامها، وإدخال البيانات ونقلها من وإلى الجهاز[٤٠].

ثانيا: **المحللون**:

المحلل هو الشخص الذي يحلل الخطوات ويجمع بيانات النظام المعني ويدرس هذه البيانات ثم يحللها أي يقسمها إلى وحدات منفصلة ويستنتج العلاقات الوظيفية من هذه الوحدات. كمبيوتر[٤١].

ثالثا: **مهندسو الصيانة والاتصالات**:

هم مسؤولون عن أعمال الصيانة المتعلقة بالأجهزة الإلكترونية ومكوناتها وشبكات الاتصال[٤٢].

رابعا: **مدراء النظام**:

هم المكلفون بعمل الإدارة في نظم المعلومات[٤٣].

هناك أيضًا بعض التشريعات التي أصدرت لوائح وقرارات خاصة تقيد الشهود على الجرائم الإلكترونية، بما في ذلك المشرع في ولاية كاليفورنيا الأمريكية[٤٤]،

خامسا: **التزامات الشاهد المعلوماتي**:

لا تختلف التزامات الشاهد في الجرائم الإلكترونية عن تلك الموجودة في الجرائم العادية والتقليدية إلا فيما يتعلق بالجانب العملي منها، إذ يمكنه تقديم شهادته مصحوبة

---

[٤٠] د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الآلي، مطبعة المكتب المصري الحديث، القاهرة، ١٩٩١، ص. ٢٣.

[٤١] د. هلالي عبد الله أحمد، التزام الشاهد على الإعلام بجريمة المعلومات، مرجع سابق، ص. ٢٤.

[٤٢] د. عبدالله حسين علي محمود، إجراءات جمع الأدلة في مجال جرائم سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، خلال الفترة ما بين ٢٦-٢٨ أبريل ٢٠٠٣. م، ص. ٦١٦.

[٤٣] د. هلالي عبد الله أحمد، التزام الشاهد على الإعلام بجريمة المعلومات، مرجع سابق، ص. ٢٤.

[٤٤] د. عمر محمد بن يونس، الإجراءات الجنائية على الإنترنت في القانون الأمريكي- الدليل الفيدرالي الأمريكي لفحص وضبط أجهزة الكمبيوتر للدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٨، ص. ٥٥.

بأدوات مساعدة مثل أجهزة عرض أو جهاز إلكتروني محمول، والشاهد في يجب على الجرائم الإلكترونية تزويد مأموري الضبط القضائي وسلطة التحقيق بالمعلومات الأساسية اللازمة للدخول إلى نظام وأجهزة المعالجة الآلية، وكذلك المواقع التي تحتوي على معلومات تشكل جريمة، من أجل البحث عن أدلة تثبت ذلك، باستثناء الحالة التي يحميه فيها القانون بعدم إفشاء معلومات مثل أسرار مهنة الطبيب أو المحامي، المصرح له قانونًا بالحفاظ على أسرار موكليهم[٤٥].

مع التأكيد على التزام الشاهد بتوفير المعلومات الأساسية اللازمة للدخول إلى نظام المعالجة التلقائية للجهاز، يُطرح السؤال هنا حول التزام الشاهد بتسليم الملفات المخزنة في الجهاز في شكل مادي ومطبوع وحول الكشف عن كلمات المرور والأسرار للدخول إلى الأنظمة والبرامج المختلفة، فهذا أمر مهم، فقد لا يكون على علم بتلك المعلومات. البيانات وكلمات المرور مخصصة للشاهد فقط ولا يمكن للخبير المفوض الوصول إليها. اختلف الفقه في هذه المسألة في قولين مختلفين، **نوضحهما كالتالي:**

الاتجاه الأول: يعتقد أنصار هذا الاتجاه أنه ليس من واجب الشاهد، وفقًا للالتزامات التقليدية للشهادة، طباعة الملفات والبيانات أو الكشف عن كلمات المرور أو الرموز للأنظمة والبرامج المختلفة في الجهاز، وبعض تميل إلى هذا الرأي التشريعات، بما في ذلك تونس وتشيلي[٤٦].

الاتجاه الثاني: خلافاً للاتجاه الأول، يعتقد مؤيدو هذا الرأي أن من بين الالتزامات التي يتحملها الشاهد طباعة ملفات البيانات والكشف عن كلمات المرور أو الرموز الخاصة بالبرامج المختلفة. المسألة أن القواعد العامة مطبقة في نطاق الإجراءات الجنائية، في نطاق إجراءات الجرائم الإلكترونية، وبالتالي يلتزم الشاهد بالإدلاء بشهادته بموجب قانون الإجراءات الجنائية من خلال الكشف عن كلمات المرور السرية التي يعرفها، وهذا الرأي هو كما تم تبنيها من خلال العديد من التشريعات، بما في ذلك تشريعات هولندا واليونان واليابان[٤٧].

في سياق الترجيح والموازنة بين المقاربتين السابقتين، من الضروري الرجوع إلى القواعد والالتزامات العامة التي يفرضها التشريع على الشاهد بشكل عام. **التالي:**

---

[٤٥] د. حازم محمد حنفي، مرجع سابق، ص. ٧٣.

[٤٦] د. عبد الله حسين علي محمود، مرجع سابق، ص. ٣٩٠.

[٤٧] د. هلالي عبد الله أحمد، مرجع سابق، ص ٢٥- ٢٦.

(ISSN: 2537- 0758)

١. حضور الشاهد:

ويلزم المشرع الشاهد قبل الإدلاء بشهادته بأداء اليمين ضمانًا لمنح الثقة لأقواله ولعضو هيئة التحقيق أو القاضي بالاستناد إلى شهادته كدليل في الدعوى، ويعطيها قيمة قانونية.، إضافة إلى لفت انتباه الشاهد إلى خطورة ما سيشهد به في شهادته وجعله حريصًا على قول الحقيقة.

٢. الالتزام بالشهادة:

وهي من أهم الالتزامات المفروضة على الشاهد وجوهر رسالته، وهذا الالتزام يعني أن الشاهد يتكلم **أولاً**، فهو على عكس المتهم الذي له حق الصمت. يعاقب على ذلك. **ثانياً**، يعني هذا الالتزام أن الشاهد ملزم فقط بذكر ما يعرفه من معلومات عن الجريمة، ولا يجوز إجباره على فعل معين. في غير الحالات التي يسمح له فيها القانون بذلك، يُحكم عليه... "وهذا يعني أن الشاهد ملزم بالإجابة على الأسئلة التي توجهها إليه المحكمة، ومقابل ذلك لا تلزمه المحكمة للقيام بعمل محدد، وفي هذا الصدد، تقول محكمة التمييز المصرية": الشهادة هي[٤٨] تقرير الشخص عما رآه أو سمعه أو أدركه بشكل عام بحواسه.

نستنتج من هذه الالتزامات التي ألقيت على الشاهد أنه ليس من واجبه في الجريمة الإلكترونية طباعة الملفات والبيانات المخزنة في ذاكرة الجهاز الإلكتروني، حسب طبيعة الشهادة ونوعها كدليل عند تقسيمها. حيث تجعله مصطلحات مصدره دليلًا روائيًا، وهو الدليل الذي يأتي من الأشخاص الذين أدركوا المعلومات المفيدة للإثبات. بأحد معانيهم المتمثلة في أقوال الآخرين، وبالتالي فإن الشاهد غير ملزم بتقديم الملفات والبيانات بشكل مطبوع، وإنما يدلي بشهادته وفق ما يراه من المعلومات في محادثة شفوية. أو يقدم عرضا مبسطا عنها، ويمكنه تقديمها في صورة مطبوعة، لكنه غير ملزم أمامه.

أما الإفصاح عن كلمات المرور أو الرموز الخاصة بالبرامج المختلفة فهو التزام يتجاوز نطاق الشهادة المنصوص عليها والالتزامات السابقة التي حددها المشرع. التزام الشاهد بتقديم المعلومات المتعلقة بالجريمة المرتكبة وما يعرفه من معلومات عنها وعن مرتكبها، وليس التزاما بتقديم معلومات تتعلق بالنظام موضوع الجريمة. وهو نفس الشيء إذا كان الشخص يشهد جريمة قتل أمامه، فيتعين عليه أن يقول ما رآه يحدث أمامه في هذه الجريمة، ولا يلزمه بالإدلاء بمعلومات عن الرقم السري الذي وضع الجاني عند فتح

[٤٨] محكمة التمييز المصرية، جلسة ١٥ يوليو/ تموز ١٩٦٤م، المربع ١٥ رقم ٩٨، ص ٤٩٣.

باب منزل المجني عليه، كما أن الشهود في الجرائم الإلكترونية متخصصون وخبراء. في تقنية المعلومات والنظام الذي حدثت فيه الجريمة، يمكنهم تزويد جهات التحقيق بالبيانات والمعلومات المطلوبة عن النظام والجاني وسجلات البيانات دون الحاجة إلى حصول وكالة التحقيق على كلمات المرور الخاصة بالنظام الذي تم فيه. وقعت الجريمة، وبناءً عليه، إذا رأت السلطات حاجتها إلى كلمات المرور أثناء إجراءات التحقيق أو جمع الأدلة، يجب أن يكون هناك تدخل تشريعي بإضافة أحكام قانونية خاصة تتطلب من الشاهد التعاون مع السلطات القضائية أثناء التحقيقات والمحاكمة، وتحديد هذا الشرط في نصوص الشهادات ضمن إجراءات الجريمة الإلكترونية.

المبحث الثاني
الحجية القانونية للأدلة الرقمية والشكل الاجرائى المتبع فيها

من أهم الصعوبات التي تواجه الجهات في جمع الاستدلالات والتحقيق في الجرائم الإلكترونية هي عملية إثباتها، ولا تثبت الجريمة إلا بتوافر الأدلة التي تؤكد ذلك، لذا فإن عملية جمع الأدلة الإلكترونية من تلك الصعوبات. التي تواجه أحد أعضاء هيئة التحقيق، ومن الصعوبات التي تواجه الخبير الإلكتروني، رغم تخصصه ومعرفته في مجال تقنية المعلومات وشبكاتها، التطور المستمر في وسائل تقنية المعلومات والأجهزة الإلكترونية الحديثة التي تستخدم شبكات الاتصال ونقل البيانات، مما أدى إلى مواكبة ذلك التطور مع تطوير أساليب وأدوات لارتكاب الجرائم الإلكترونية والتقليدية على حد سواء، نتيجة الاستخدام السلبي لهذه التكنولوجيا الجديدة. في هذا المطلب، سنتناول الإجراءات الحديثة التي تساعد في جمع الأدلة الإلكترونية، الإجراءات المتعلقة بأنظمة التشغيل المختلفة المطلب الأول). الحجية القانونية لتلك الأدلة المتحفظ عليها، (المطلب الثاني)، وذلك على النحو الاتى:-

المطلب الأول
الإجراءات المتعلقة بأنظمة التشغيل المختلفة

شكلت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية أول محاولة قانونية دولية لمعالجة مشكلة زيادة الجريمة السيبرانية، وكان الهدف الرئيسي من الموافقة عليها هو تطوير سياسة جزائية مشتركة لمكافحة الجريمة السيبرانية من خلال مواءمة القوانين الوطنية مع أحكام الاتفاقية لضمان حماية المجتمع من هذه الجرائم[٤٩]. تعتبر الاتفاقية

[٤٩] د. عادل عزام سقف الحيط، جرائم القذف والسب والازدراء المرتكبة عبر الوسائط الإلكترونية، دراسة مقارنة، دار الثقافة، القاهرة، ٢٠١١ م، ص. ٣٦٥.

(ISSN: 2537- 0758)

الأوروبية لمكافحة الجريمة الإلكترونية، التي تم التوقيع عليها في بودابست، عاصمة المجر في ٢٣ نوفمبر ٢٠٠١، من أولى الاتفاقيات الدولية المتعلقة بمكافحة جرائم الإنترنت. أفريقيا والولايات المتحدة الأمريكية، ودخلت الاتفاقية حيز التنفيذ في يوليو ٢٠٠٤.

حيث تنص المادة (١٦) من هذه الاتفاقية على أن تتبنى كل دولة طرف ما قد يلزم من تشريعات أو تدابير أخرى، بحيث يمكن للسلطات المختصة في هذا المجال أن تأمر أو تطلب الحجز العاجل لبيانات محددة في جهاز كمبيوتر، بما في ذلك مسار البيانات المخزنة بواسطة نظام الحاسب الالي، خاصة إذا كانت هناك أسباب للاعتقاد بأن البيانات قد تكون عرضة للضياع أو التعديل. تضمنت هذه الاتفاقية حكماً لأول مرة للتمييز بين نوعين من البيانات، وهما البيانات المخزنة أو الثابتة، ونقل البيانات أو البيانات المتعلقة بمسار المعلومات. من خلال قراءة نصوص هذه الاتفاقية، وجدنا أنها نصت على إجراءات جديدة لجمع الأدلة في الجرائم الإلكترونية، بما في ذلك إجراءات الرصف. تسبق عملية جمع الأدلة، بما في ذلك الإجراءات الخاصة لجمع الأدلة [٥٠]. من أهم أحكام اتفاقية بودابست بشأن مكافحة الجريمة السيبرانية النص على التحفظ السريع أو الصريح لبيانات الحاسب الالي المخزنة،

نصت اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية على إجراء آخر، وهو سلطة إصدار الأوامر، حيث جاء ذلك بموجب الفقرة الأولى من المادة (١٨) من الاتفاقية[٥١].

---

[٥٠] د. حازم محمد حنفي، مرجع سابق، ص. ٩٥.

[٥١] التي تنص على أن تتبنى كل دولة طرف التشريعات اللازمة وغيرها من التدابير لمنح سلطاتها المختصة سلطة إصدار الأمر، إلى أي شخص موجود في إقليم الدولة لتقديم بيانات محددة عن الكمبيوتر الذي بحوزته أو تحت سيطرته وتخزينها في نظام كمبيوتر أو على أي وسيط تخزين بيانات آخر، وكذلك توجيه الطلب إلى أي مزود خدمة يقدم خدماته في أراضي الدولة لتوفير معلومات المشترك فيما يتعلق بتلك الخدمات التي في حوزة مقدم الخدمة أو تحت سيطرته، ويعني مزود الخدمة في نطاق هذه الاتفاقية أنه أي كيان عام أو خاص يوفر لمستخدمي خدمته الخاصة القدرة على الاتصال من خلال نظام كمبيوتر، وأي كيان آخر يقوم بمعالجة أو تخزين الكمبيوتر البيانات نيابة عن خدمة الاتصال المذكورة أو مستخدمي هذه الخدمة.

حيث يمكن لسلطة التحقيق أو الخبير الإلكتروني المفوض استخدام هذه البرامج الخاصة لكسر هذا النوع من الحماية وعرض المحتوى المستندات[٥٢]. ومن الإجراءات الحديثة التي تستخدم أيضًا في جمع الأدلة الإلكترونية، استخدام التكنولوجيا في هذه الإجراءات، ويشمل ذلك استخدام البرامج الفنية المتخصصة لمساعدة الضباط القضائيين وسلطات التحقيق في جمع الأدلة، بما في ذلك استخدام برامج تكسير كلمات المرور للبعض. المستندات كما هي موجودة في بعض برامج الاجهزة الالكترونية ميزة تعيين كلمة مرور للمستندات التي يتم إنشاؤها من خلال هذا البرنامج تمنع المستخدم من الوصول إليها وعرض محتواها إلا بعد إدخال كلمة مرور خاصة تسمح له بفتح الملف.

الفرع الاول

الإجراءات المتعلقة بنقل البيانات في شبكة المعلومات

أمن المعلومات هو بالإنجليزية (Information Security) علم متخصص في تأمين المعلومات المتداولة عبر الإنترنت من المخاطر التي تهددها تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة، أو ما يسمى بنقل البيانات من خلال الشبكة من موقع إلى آخر، أصبح أمن تلك البيانات والمعلومات هاجسًا وموضوعًا حيويًا للغاية. يمكن تعريف الأمن المعلومات هي العلم الذي يوفر الحماية للمعلومات من الأخطار التي تهددها أو الحاجز الذي يمنع الاعتداء عليها، من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي الأشخاص غير المصرح لهم من خلال الاتصالات ولضمان صحة وصحة هذه الاتصالات.

ما ساعد على انتشار استخدام شبكات المعلومات في جميع أنحاء العالم هو ثورة تكنولوجيا المعلومات وتطورها المستمر، حيث أصبحت معظم أجهزة الحاسب الالي أجهزة محمولة سهلة الاستخدام والحمل، وتلك ثورة المعلومات لم تتوقف عند هذا الحد، بل أنتجت إلكترونية حديثة. الأجهزة التي تحتوي على برامج شبيهة بالبرامج الموجودة في الحاسب الالي مثل الأجهزة المحمولة والأجهزة اللوحية، فهي أشبه بأجهزة الحاسب الالي المصغرة التي يمكن لأي شخص حملها واستخدامها في أي مكان والوصول إلى شبكة المعلومات بسهولة أكبر دون الحاجة إلى المكونات المادية المعقدة للكمبيوتر التي تحتاج إلى موصل كهربائي دائم للعمل، مما أدى إلى نقل مسرح الجريمة إلى هذه

[٥٢] د. حازم محمد حنفي، مرجع سابق، ص. ٧٨.

(ISSN: 2537- 0758)

الشبكات والأجهزة، وهي أدوات الجريمة المتقدمة. ساهمت العديد من العوامل بشكل عام في الصعوبات وخلقت عقبات جديدة أمام السلطات للتحقيق في الجرائم الإلكترونية، وأهمها:

أولاً- طبيعة شبكة المعلومات هي اتصال بأكثر من شبكة وجهاز:

ونتيجة لذلك، تم توزيع مسرح الجريمة والأدلة الإلكترونية في عدة أماكن مختلفة، مما يؤدي إلى صعوبات عملية وتشريعية في نفس الوقت، خاصة مع اختلاف نصوص القوانين بين تلك الأماكن. في معظم الحالات، إذا تم العثور على أدلة في دولة أخرى، فلا يمكن الحصول عليها حتى مع الإجراءات الدولية التي تسهل عملية تبادل مثل هذه الأدلة الإلكترونية، لأن معظم هذه الإجراءات معقدة[٥٣]، وهي غير عملية إلا عندما تكون جريمة خطيرة يحدث، وفي ذلك الوقت يتم استدعاء المعلومات رسميًا من دول أخرى.

ثانياً- طبيعة المعلومات والبيانات الإلكترونية نفسها:

إذا أتيحت للمجرم فرصة المعرفة والمهارة، فإنه يتلف الأدلة أو يعدلها أو يمسحها هرباً من يد العدالة ويبرئ اسمه من الأدلة التي تدينه. حيث أنه يمكن أن يخضع للمحو أو التغيير بسهولة، لذلك يصبح من الضروري جمعه وتخزينه بسرعة كلما أمكن ذلك، وعلى الرغم من أن مرور هذه المعلومات والبيانات في الشبكات لا يستغرق سوى أجزاء من الثانية وهي قصيرة جدًا بالإضافة إلى حجم تلك المعلومات والبيانات الكبير والمتزايد بشكل فوري، يصبح من غير الممكن تخزين المعلومات والبيانات لفترة طويلة.. فضلاً عن ذلك،

ثالثًا- قلة الخبرة الفنية على هذه الشبكات لتنوعها واختلافها من شبكة لأخرى:

من أهم الأمور التي يمكن الحديث عنها في مجال تقارير الخبرة الفنية حول انتهاكات شبكات الاتصالات، وبصرف النظر عن السبب، لا بد من الرجوع إلى القواعد والمحددات الأساسية التي يستند إليها التقرير، **وهي:**

---

[٥٣] بناءً على نتائج المشروع المشترك للمعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) والمعهد الكندي للمحاسبين (CICA)، تم تحديد المبادئ الأساسية لأمن المعلومات (Webtrust) وأمن أنظمة المعلومات(Systrust) على أنها ما يلي: حماية النظام، وجاهزية نظام المعلومات على الويب، وتكامل معالجات نظام المعلومات، وضمان الخصوصية على الويب، وسرية نظام المعلومات.

أولاً: وقت إحداث الضرر، وهذا يساهم في رفع أو خفض قيمة التعويض وقيمة الإصلاح الاقتصادي. من المعروف أن قيم إنشاء وصيانة شبكات الاتصالات آخذة في الانخفاض لأسباب عديدة، وهي توفر مواد الإصلاح بكثرة مع تقدم الوقت ووفرة العرض مقابل انخفاض الطلب. الإصلاح في فترات النهار والليل.

ثانياً: مكان إصلاح الضرر والتعدي. هذه مسألة عامة، خاصة وأن التعديات على شبكات الاتصال تتطلب أعمال إصلاح محدودة. لذلك، كلما كان مكان إصلاح الضرر بعيدًا عن مراكز المدن، يؤدي ذلك إلى زيادة التكاليف المتعلقة بنقل المواد من مكان توريدها إلى مكان تركيبها داخل الشبكات المخالفة.

ثالثاً: مقدار الضرر والتعدي، وهذا أمر مهم. ليس من المعقول أن الكميات الصغيرة للإصلاح تتطلب نفس القيمة المادية للكميات الكبيرة التي يتم إصلاحها، بحيث يشعر الشخص الذي يعقد الاتفاقية أن العمل الذي قدمه، سواء كان مقاولاً أو عملاً فرديًا، له فائدة يعادل حجم العمل.

رابعاً: الأسعار والضرائب الدولية والمحلية المضافة لأجزاء إصلاح شبكات الاتصالات مع مراعاة ربط هذا المعيار بمعيار الموقع وتكاليف النقل لهذه الأجزاء.

وهذا يجعل الأمر صعبًا على الخبير الذي لا يكون على دراية بالتعامل مع جميع أنواع الشبكات واختلافاتها، الأمر الذي يتطلب المزيد من الأشخاص الأكفاء للتعامل مع التكنولوجيا والحصول على أدلة منها.

رابعاً- حجم البيانات الكبيرة المستخدمة في التحقيق والمستخرجة من أنظمة الأجهزة محل التحقيق:

يواجه عضو هيئة التحقيق أو الخبير الفني المكلف العديد من الصعوبات عند جمع الأدلة الإلكترونية من شبكات المعلومات، بالإضافة إلى الصعوبات التي سبق ذكرها، وتتلخص هذه الصعوبات في الشبكات وإخفاء الهوية والشبكات وإخفاء المعلومات، وعلى الرغم من ذلك. الذي– التي. عند القيام بإجراءات التحقيق المختلفة والبحث عن الأدلة يتم ذلك بكمية كبيرة من المعلومات والبيانات الإلكترونية، الأمر الذي يتطلب مجهودًا كبيرًا ومهارة عالية[٥٤]. لذلك فإن تلك المعلومات والبيانات المستخرجة من شبكات المعلومات تعتبر بيانات متحركة، وهناك العديد من التطبيقات التي تقوم بتحميل الملفات

[٥٤] د. ممدوح عبد الحميد عبد المطلب، دليل الصور الرقمية لجرائم الحاسوب، مركز أبحاث الشرطة، الشارقة، ٢٠٠٥، ص. ١٢٠.

(ISSN: 2537- 0758)

من الجهاز أو وسائل تقنية المعلومات إلى الشبكة العالمية للمعلومات، والتي يمكن من خلالها الحصول على نسخة من تلك المعلومات أو البيانات من قبل أي شخص آخر عبر نفس الشبكة،

ومن بين هذه الإجراءات التي يستخدمها المجرمون استخدام جهاز كمبيوتر من مقهى إنترنت عام، وفي المقابل هناك العديد من البرامج والتطبيقات المختلفة التي تعمل على إخفاء هوية المستخدم عند دخوله شبكة المعلومات، مما يزيد من هذه الصعوبة بالنسبة لعضو هيئة التحقيق أو الخبير الإلكتروني عند تحليل الأدلة التي تم العثور عليها وجمعها[٥٥]. من حيث عدم الكشف عن هويته، تواجه عملية جمع الأدلة الجنائية الإلكترونية من مسرح الجريمة صعوبة أخرى تتمثل في إخفاء المستخدم لهويته، مما يشكل تحديًا أمنيًا عند إخفاء الهوية دون أن يبذل الجاني جهدًا في ذلك، إذ يستطيع. التخلص من التهمة الموجهة إليه بالادعاء بعدم مسؤوليته عن فعل الإخفاء، وقد يلجأ المجرمون إلى إجراءات بسيطة لإخفاء هوياتهم عن الشبكة حتى تظل أنشطتهم مجهولة لمحاولة التهرب من إجراءات التوقيف،

من ناحية إخفاء المعلومات فهي صعوبة أخرى تضاف إلى تحديات هيئة التحقيق والخبير الإلكتروني في الجرائم الإلكترونية، ويتم ذلك من أجل وضع هذه المعلومات المشبوهة أو المخالفة بعيدًا عن متناول الناس والرقابة والتحقيق. السلطات، وقد تتحد هذه الصعوبات في الشبكة بين إخفاء هوية المستخدم والمعلومات أو البيانات، الأمر الذي يجعل من التعقيد والصعوبة للغاية اكتشاف وتحديد الجاني في مثل هذه الجرائم، ولكن هناك بعض البرامج التي تمكن جهات التحقيق والخبير الإلكتروني في فك هذه الصعوبات وتعمل هذه البرامج على استعادة كافة المعلومات والبيانات المخبأة في الشبكات بما في ذلك البرنامج المعروف باسم Marotoki[٥٦] Marutukku.

تختلف البيانات المتحركة المحفوظة على شبكة المعلومات إلى أنواع مختلفة، حيث تختلف أنواع البيانات هذه في طريقة تشكيلها وانتشارها ونقلها على شبكة المعلومات العالمية. يمكننا تقديم أربعة أمثلة مختلفة تتبنى طبيعة نقل البيانات، **على النحو التالي:**

١. بريد إلكتروني:

نتيجة الاستخدام السلبي للبريد الإلكتروني، تم رفع درجة سرية محتواه والرسائل المستلمة من خلال تشفيره ببرامج خاصة لا تسمح بعرض أي رسالة فيه إلا لمن لديه

---

[٥٥] د. حازم محمد حنفي، مراجع سابق، ص. ٨٢.

[٥٦] المرجع نفسه، ص. ٨٣.

كود خاص به، مما ساعد أيضًا في ظهور التوقيع الإلكتروني، حيث يقوم برنامج التصفح للبريد بتخزين توقيع المستخدم على كل رسالة يرسلها بحيث تصبح رمزه [٥٧]. تعتبر من الخدمات الهامة والإيجابية التي تقدمها ثورة المعلومات للمجتمعات، فهي شكل من أشكال الاتصال الإلكتروني الذي يسمح لمستخدم الشبكة بتبادل الرسائل النصية بدلاً من الوسائل الورقية التقليدية، وكأنه صندوق بريد خاص على شبكة المعلومات، حيث تتيح للمستخدم الدخول إليها، والتحقق من الرسائل الواردة إليها، وإرسال الرسائل لأشخاص آخرين. البريد الإلكتروني مثله مثل الخدمات الأخرى التي تقدمها الشبكة وتكنولوجيا المعلومات بشكل عام[٥٨].

في مصر، يُعرَّف التوقيع الإلكتروني بأنه جميع العلامات أو الرموز أو[٥٩] الحروف المصرح بها من قبل السلطة المختصة بالموافقة على التوقيع ويرتبط ارتباطًا وثيقًا بالسلوك القانوني، ويسمح بتمييز شخص مالكه وتحديد هويته، ويتم ذلك بدون غموض حول رضاه عن هذا السلوك القانوني. هوية الشخص الذي ينسب إليه التوقيع بقصد إحداث آثاره القانونية بطريقة مشابهة للتوقيع بخط اليد أو هو إجراء محدد يقوم به الشخص الذي يُراد توقيعه للتوقيع على المستند، سواء كان هذا الإجراء في شكل رقم أو علامة إلكترونية محددة أو رمز خاص. الوسيط الإلكتروني[٦٠].

مع زيادة التطور المعلوماتي والدور المهم الذي تلعبه في مختلف مجالات الحياة البشرية، أقر التشريع بصحة هذه الوثائق التي يتم استخدامها عبر البريد الإلكتروني، تمامًا مثل المستندات الورقية. إن اعتبار رسائل البريد الإلكتروني في مرتبة الرسائل

---

[٥٧] لمزيد من المعلومات، يمكنك الرجوع إلى المواقع الرسمية التي تقدم خدمة البريد الإلكتروني، مثل http://www.office.com

[٥٨] د. خالد ممدوح إبراهيم، أمن جرائم المعلومات، دار الجامعة، الإسكندرية، ٢٠٠٨، ص. ٩٠.

[٥٩] د. ثروت عبد الحميد: التوقيع الإلكتروني، ماهيته، مخاطره، وكيفية مواجهته، مدى صلاحيته في الإثبات، الطبعة الثانية، مكتبة الجلاء الجديدة بالمنصورة ٢٠٠٣-٢٠٠٢، ص. ٥٠ نقلاً عن: د. محمد علي سويلم الحماية الجنائية لمعلومات المعاملات الإلكترونية والجرائم الإلكترونية بين الجوانب الإجرائية والأحكام الموضوعية. الطبعة الأولى ٢٠١٨، مطبعة الجامعة، ص. ١٢٥.

[٦٠] نجوى أبو هبة: التوقيع الإلكتروني، تعريفه، مدى صلاحيته في الإثبات، بحث مقدم إلى مؤتمر المصرفية الإلكترونية بين الشريعة والقانون بكلية الشريعة والقانون، جامعة الإمارات، دبي الغرفة التجارية الصناعية في الفترة من ٩-١١ ربيع الأول الموافق ١٠-١٢ مايو ٢٠٠٣م الجزء الأول ص ٤٤٢-٤٤٣.

(ISSN: 2537- 0758)

الشخصية يستلزم حماية جنائية متزايدة لهم وتمتعهم بنفس الحماية التي تتمتع بها الرسائل الورقية. ولا يجوز الإطلاع عليها وعلى الأسرار التي تحتويها إلا وفق الإجراءات والقواعد العامة التي يحددها القانون. وبناءً عليه، لا يجوز لعضو في سلطة التحقيق اختراق البريد الإلكتروني. والوصول إلى الأنظمة التي يتم فيها تخزين الرسائل البريدية أو ضبطها إلا وفق الإجراءات المنصوص عليها في قوانين الإجراءات الجنائية المنظمة لذلك. هذا الأمر[٦١].

٢. بيانات وسائل التواصل الاجتماعي:

أصبحت هذه المواقع والمعلومات والبيانات التي تحتويها من أخطر أنواع بيانات الجوال[٦٢]، حيث تتيح للمستخدم أن يكون أداة ومصدرًا لنشر أي معلومة أو وثيقة كأنه قناة إعلامية مستقلة، ويستطيع تصل إلى أجزاء مختلفة من الأرض في غضون دقائق قليلة، مما يؤدي إلى الاستخدام السلبي لهذه المواقع. تنشر المواقع الإلكترونية إشاعات تمس المجتمعات والأسر والأشخاص، وتنشر الفتنة وتنشر الرذيلة من خلال الصور والأفلام دون رقابة أو ردع. من يتابع هذه المواقع يدرك مدى خطورتها وما ساهمت فيه من هدم المجتمعات والدول بسبب ما ينشر عنها. تختلف هذه المواقع من حيث العدد وهي كبيرة جدًا، ومن أشهرها Twitter وFacebook وInstagram وحيث تتيح هذه المواقع للمستخدم تحميل ملفات متنوعة عليها مثل الصور ومقاطع الفيديو والمستندات والروابط، وتسمح بنشرها على شبكة المعلومات لجميع المستخدمين، وفي المقابل يمكن لمستخدم آخر تنزيلها والحصول على نسخة منها أو إعادة نشرها بسهولة.

٣. البيانات المحفوظة على الشبكة:

يتم تمثيل هذه البيانات والمعلومات من خلال الخدمات التي تقدمها بعض المواقع أيضًا. من خلال هذا الموقع، يمكن لأي شخص الاحتفاظ بأي بيانات وملفات يريدها وتحميلها على هذا الموقع والحصول على كلمة مرور خاصة يمتلكها هو وحده، يستطيع من خلالها إدخال وعرض ملفاته وبياناته التي قام بتخزينها. كلما أراد ذلك، مع إمكانية إضافة المزيد من الملفات والبيانات أيضًا، وفقًا لمساحة تخزين عالية متاحة لكل مستخدم، ويتيح الموقع للمستخدم مشاركة هذه الملفات لمن يشاء دون كلمة مرور، ويحدد الأشخاص من يمكنه عرض الملفات، من خلال هذه الملفات يمكن إدارة المحتوى

---

[٦١] د. علي محمود علي حمودة، مرجع سابق، ص. ٨.

[٦٢] د. حازم محمد حنفي، مرجع سابق، ص. ٨٥.

مجموعة معينة من الأشخاص دون القدرة على الحصول عليه أو مشاهدته من الآخرين ودون إذن مالكه، والتي قد يساء استخدامها في إدارة المحتويات غير القانونية أو الملفات المحظورة و تسليمها إلى الشخص المقصود دون خوف من انتشارها عبر شبكة المعلومات أو الوصول إلى الآخرين دون إذن.

الفرع الثاني
إجراءات الحصول على بروتوكول العنوان الإلكتروني

وذلك بوضع مجموعة من الأسس والضوابط والحلول الأمنية التي تساعد على مكافحته وتقليل معدل ارتكابه ورفع معدل كشف ومعرفة الجناة بأفضل الطرق وأكثرها فاعلية لتحقيق هذا الهدف. مع تزايد عدد مستخدمي الشبكة العالمية للمعلومات عبر المجتمعات الدولية المختلفة، قد يكون هذا الاستخدام الكبير إيجابيًا جزئيًا وبعضه سلبيًا، أي استخدام الشبكة بطريقة خاطئة للخدمات والتطبيقات التي تحتوي عليها وليس لغرض توفيرها، وهذه السلوكيات الخاطئة والسلبية قد تؤدي إلى توافر أركان الجريمة المتعلقة بها، مما يؤدي إلى زيادة عدد الجرائم المرتكبة عبر شبكة المعلومات، لذلك كان لا بد من ذلك. للمشرع للحد من هذه الجرائم ومكافحة هذه الظاهرة الإجرامية المتقدمة،

ومن أهم الأسس والحلول التي تم وضعها في هذا المجال تحديد عنوان إلكتروني لكل جهاز متصل بشبكة المعلومات، سواء كان هذا الاتصال من جهاز كمبيوتر أو هاتف محمول أو جهاز لوحي أو أجهزة أخرى، حيث يكون يتم تعيين العنوان لكل جهاز مهما كان نوعه أو طبيعته. له اتصال بالشبكة العالمية للمعلومات، ويسمى هذا العنوان بروتوكول العنوان الإلكتروني وهو اختصار يعرف بـ (IP).

يعود تاريخ هذا البروتوكول إلى أوائل السبعينيات، عندما تم تمويله من قبل وزارة الدفاع الأمريكية كمشروع بالتعاون مع جامعة كاليفورنيا بالولايات المتحدة الأمريكية، لأنه صمم نظام اتصال إلكتروني يعتمد على اللامركزية في إدارته، بحيث عند وجود عطل في مركز الاتصال الرئيسي لا يؤثر على تلك الشبكة بشكل كامل. عندما احتاجت وزارة الدفاع إلى ربط جميع وحدات الجيش الأمريكي التي كانت تعمل باستخدام شبكة خاصة لكل وحدة في نقل البيانات، تحت إدارة مركز رئيسي واحد، ظهرت مشاكل عدم التوافق بين الوحدات المختلفة، وكانت جميعها تعطلت عند استهداف مركزهم الرئيسي أثناء الحروب. أو الكوارث، وبسبب هذا المشروع الممول، تم بناء شبكات ضخمة بدون مركز رئيسي للتحكم أو الإدارة، وتعمل هذه الشبكات تلقائيًا للاتصال بالشبكة في حالة حدوث

(ISSN: 2537- 0758)

أي عطل أو توقف[٦٣]. يقصد ببروتوكول العنوان الإلكتروني حزمة من القواعد والمعايير المتعددة (البروتوكولات)[٦٤] مرتبطة ببعضها البعض وتعمل على تحقيق التوافق التقني اللازم لنجاح عمليات الاتصال الإلكتروني بين الأجهزة الإلكترونية بأنظمة وخصائص مختلفة، ويأتي اسمها من مصطلح بروتوكول الإنترنت/ بروتوكول التحكم في الإرسال يتم اختصاره كـ IP/TCP.

حيث يتم فحص البريد الإلكتروني للضحية والرسالة الواردة موضوع الجريمة ومعرفة عنوان IP الخاص بالمرسل، ومن ثم يتم توجيه الشركة التي تتبع رقم عنوان IP للحصول على بيانات المستخدم الذي أرسل الرسالة. أما دور هيئة التحقيق والخبير الإلكتروني في هذا الأمر فهو وقت ارتكاب الجريمة والبحث عن الفاعل، حيث تختلف طريقة الحصول على عنوان IP باختلاف نوع الجريمة المرتكبة، وحسب إلى المكان الذي ارتكبت منه الجريمة، عند وجود شكوى حول رسالة في البريد الإلكتروني تحتوي على إهانات أو تهديدات.

المطالب الثانى
الحجية القانونية لتلك الأدلة المتحفظ عليها

تُعرِّف المادة ١ من قانون جرائم تقنية المعلومات الأدلة الرقمية بأنها أي معلومات إلكترونية لها قوة أو قيمة إثباتية يتم تخزينها أو نقلها أو استخراجها أو أخذها من أجهزة الحاسب الالي أو شبكات المعلومات وما شابه ذلك. تم تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تقنية مسجلة الملكية[٦٥].

ووفقًا لنص المادة الحادية عشرة من القانون، فإن المشرع المصري اعترف بهذه الأدلة الرقمية المستمدة من وسائل التكنولوجيا الحديثة بقيمتها الإثباتية، ومنحها نفس القيمة القانونية والأدلة الصحيحة الممنوحة لأدلة الطب الشرعي المادية في الأدلة الجنائية، المنشأة بموجب قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠

---

[٦٣] د. حازم محمد حنفي، مرجع سابق، ص. ٨٧.

[٦٤] تعني البروتوكولات بنية تصميم تحدد مجموعة من الأنظمة المستخدمة للاتصال بشبكات الكمبيوتر التي يعتمد عليها الإنترنت العالمي، حيث توفر التوافق بين بروتوكولات الحزمة المختلفة والشبكات المختلفة حول العالم مع بعضها البعض.

[٦٥] مراجعة نص المادة الأولى من قانون تكنولوجيا المعلومات المصري الصادر في شأن مكافحة جرائم التكنولوجيا

وتعديلاته، وقواعد الإثبات المقبولة عمومًا. الفقه والفقه والقانون. في الواقع، هذه الأدلة الفنية هي أدلة معقدة تحتاج إلى قبولها في عملية الإثبات، وضرورة شروط ومواصفات معينة تختلف عن الأدلة المادية التقليدية. لها بعض الشروط والضوابط والمواصفات الفنية المحددة التي تمنحها هذه الصلاحية الاستدلالية، وقد تمت إحالتها إلى نصوص اللائحة التنفيذية لقانون مكافحة جرائم التكنولوجيا (المصري)[٦٦].

أشارت اللائحة التنفيذية للقانون الصادرة بموجب قرار مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ إلى أهم الشروط والضوابط التي يجب توافرها في الدليل الفني لقبوله والاعتراف بأثباته وقيمته الاستدلالية، بالإضافة إلى الإجراءات المحددة المطلوبة. لعرض هذا الدليل على الجهات المختصة **على النحو التالي:**

أولاً: فيما يتعلق بالشروط والمواصفات التي يجب توافرها في الأدلة الفنية: حددت المادة (٩) من اللائحة التنفيذية المشار إليها هذه الشروط والضوابط والمواصفات بنصها على أن "الأدلة الرقمية ذات القيمة والأدلة المادية الحجية يجب الحصول عليها جنائياً". دليل إذا تم استيفاء الشروط والضوابط التالية".

١- أن عملية جمع الأدلة الرقمية أو الحصول عليها أو استخلاصها أو استخلاصها في موضوع الواقعة تتم باستخدام تقنيات تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة والبيانات والمعلومات أو أي تغيير. أو تحديث أو إتلاف الأجهزة أو المعدات أو البيانات أو المعلومات أو الأنظمة للمعلومات أو البرامج أو الدعم الإلكتروني أو غير ذلك. على وجه الخصوص، تقنية الكتابة، Hash Images Digital، Blocker وغيرها من التقنيات المماثلة.

٢- أن تكون الأدلة الرقمية مرتبطة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، حسب نطاق قرار سلطة التحقيق أو المحكمة المختصة.

٣- أن يتم جمع الأدلة الرقمية واستخراجها وحفظها وضبطها من قبل مأمور الضابطة العدلية المخولين بالتعامل مع هذا النوع من الأدلة أو من قبل الخبراء أو المختصين

---

[٦٦] تنص المادة ١١ من نفس القانون على أن "الأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو أنظمة المعلومات أو برامج الكمبيوتر أو أي وسيلة من وسائل تكنولوجيا المعلومات يجب أن يكون لها قيمة وسلطة أدلة الطب الشرعي المادي في الأدلة الجنائية.." عندما تتوفر فيه الشروط الفنية التي تحددها اللائحة التنفيذية لهذا القانون.

(ISSN: 2537- 0758)

الذين تكلّفهم جهات التحقيق أو المحاكمة، وأن يتم الإشارة إليها. في تقارير المراقبة أو التقارير الفنية عن نوع ومواصفات البرامج والأدوات والأجهزة. والمعدات التي تم استخدامها مع توثيق كود الهاش والخوارزميات الناتجة عن استخراج نسخ متشابهة ومطابقة من الدليل الرقمي في تقرير المراقبة أو تقرير الفحص الفني، مع التأكد من أن الأصل لا يزال محفوظاً دون العبث به.

٤- في حالة تعذر فحص نسخة الدليل الرقمي وتعذر الاحتفاظ بالأجهزة قيد الفحص لأي سبب من الأسباب يتم فحص الأصل وتدوين كل ذلك في محضر الضبط أو تقرير الفحص أو التحليل.

٥- أن يتم توثيق الدليل الرقمي في سجل الإجراءات من قبل المختص قبل فحصه وتحليله وتوثيق مكان ضبطه ومكان تخزينه ومكان التعامل به ومواصفاته.

ثانياً: فيما يتعلق بإجراءات تقديم الأدلة الفنية من حيث التوثيق والوصف والاعتماد:

وحددت المادة ١٠ من نفس اللائحة هذه الإجراءات بالنص على أن "وصف الأدلة الرقمية وتوثيقها يتم بطباعة نسخ من الملفات المخزنة عليها أو تصويرها بأي وسيلة مرئية أو رقمية، واعتمادها من قبل الأشخاص. المسؤول عن جمع الأدلة الرقمية أو استخلاصها أو الحصول عليها أو تحليلها، **مع تدوين البيانات التالية على كل منها:**

١- تاريخ ووقت الطباعة والتصوير.

٢- اسم وتوقيع من قام بالطباعة والتصوير

٣- اسم أو نوع نظام التشغيل ورقم إصداره.

٤- اسم البرنامج ونوع الإصدار أو الأوامر المستخدمة في تحضير النسخ

٥- البيانات والمعلومات المتعلقة بمحتويات الأدلة المضبوطة.

٦- بيانات الأجهزة والمعدات والبرمجيات والأدوات المستخدمة.

وبالتالي، فإن المشرع يتماشى مع ما دخلت فيه معظم التشريعات الأوروبية والأجنبية في هذا الصدد، بما في ذلك التشريع الإنجليزي الصادر عام ١٩٨٤ الساري منذ عام ١٩٨٦ المتعلق بالأدلة، وقانون إساءة استخدام الحاسب الالي في عام ١٩٩٠، والذي تضمن لائحة محددة بشأن قضية قبول مخرجات الإنترنت (١) وأجهزة الحاسب الالي. كدليل في المسائل الجنائية[٦٧]، وكذلك التشريع الأمريكي المتعلق بالأدلة وقبول

[٦٧] ركز هذان القانونان بشكل أساسي على قبول مخرجات الكمبيوتر كدليل لإثبات أي حقيقة مسجلة فيه، والتي يتم توفيرها بشهادة شفوية مقبولة تقدرها المحكمة المختصة- انظر بالتفصيل: د. سعيد

الأدلة الإلكترونية والمخرجات في عملية الإثبات، والاعتراف (٢) بقيمتها وقوتها الاستدلالية[٦٨]. لقد أقرت صراحة بقيمة ومصداقية الأدلة الرقمية المستخرجة من الوسائل والأنظمة المعلوماتية التقنية، وأدركت قوتها التوضيحية في مجال الأدلة الجنائية، وبذلك يكون قد فعل أفضل من غيره في مواكبة التطورات في مجال تقنية المعلومات ووسائل التقنية الحديثة وإدراجها في الأنظمة التشريعية والقضائية.

لكي يكون المستند الإلكتروني دليلاً كاملاً على الإثبات، يجب أن يكون قادرًا على الاحتفاظ به في شكله الأصلي الذي نشأ فيه وتم الاتفاق عليه بين طرفي العلاقة. وهذا الشرط نصت عليه المادة (٨/ أ) من قانون المعاملات الإلكترونية الأردني[٦٩]. والمادة (٨) من قانون الأونسيترال النموذجي[٧٠] والمادة (١٢) من مشروع قانون التبادل الإلكتروني والتجارة الفلسطيني[٧١]. من الضروري الاحتفاظ بالسجل الإلكتروني بنفس

عبد اللطيف حسن– دليل. الجرائم الحاسوبية والجرائم المرتكبة عبر الإنترنت– دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩، ص. ١٩٤ وما يليها.

[٦٨] د. هلالي عبد الله أحمد– التفتيش على أنظمة الحاسبات والضمانات الإعلامية للمتهمين، دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٧، ص ٥٣.

[٦٩] نصت المادة (٨/ أ) من قانون المعاملات الإلكترونية الأردني رقم ٨٥ لسنة ٢٠٠١ على ما يلي: "أ– يستمد السجل الإلكتروني أثره القانوني ويكون له صفة النسخة الأصلية إذا استوفى الشروط التالية: أن تكون المعلومات الواردة في هذا السجل قادرة على الاحتفاظ بها وتخزينها بحيث يمكن الرجوع إليها في أي وقت ٢– القدرة على الاحتفاظ بالسجل النموذج الإلكتروني بالشكل الذي تم إنشاؤه به أو إرساله أو استلامه، أو بأي شكل يسهل إثبات دقة المعلومات الواردة فيه عند إنشائه أو إرساله أو استلامه.

[٧٠] تنص المادة (٨/ أ) من قانون الأونسيترال النموذجي على ما يلي: "١– عندما يتطلب القانون تقديم المعلومات أو الاحتفاظ بها في شكلها الأصلي، فإن رسالة البيانات تفي بهذا الشرط إذا: أ– هناك دليل موثوق به لتأكيد سلامة المعلومات من وقت إنشائها لأول مرة في شكلها النهائي، كرسالة بيانات أو غير ذلك". للمزيد انظر د. بندوق، وائل أنور، مرجع سابق، ص. ٢١.

[٧١] نصت المادة (١٢) من مشروع قانون التبادل والتجارة الإلكترونية الفلسطينية على ما يلي: "١– تحفظ رسالة البيانات على ناقل إلكتروني، على أن يراعى ما يلي: أ– تسهيل الوصول إلى المعلومات الواردة فيها. بطريقة تسمح باستخدامه عند الإشارة إليه لاحقًا. ب– الاحتفاظ برسالة البيانات بالشكل الذي أُنشئت به أو أرسلته أو استلمته، أو في نموذج يمكن إظهاره لتمثيل

(ISSN: 2537- 0758)

الشكل والمواصفات التي تم بها إنشاء السند أو إرساله أو استلامه عند إنشائه، بحيث إذا أشرنا إلى السند، فهو نفس السند الذي تم إنشاؤه أو إرساله أو استلامه دون أي تحريف أو تغيير أو تغيير، وهذا يعتمد بشكل كبير على وثائق الحزب وإجراءاته، على الرغم من التكنولوجيا الحديثة المستخدمة في حفظ المستندات الإلكترونية، ولكن تقدير مدى قدرة هذه التقنية على تأمين بيانات المستند، وإمكانية قبولها. أن يكون المستند الإلكتروني في الإثبات خاضعًا لسلطة قاضي الموضوع، كما أن ترك تقييم قيمة المستند الإلكتروني كدليل للقاضي من شأنه أن يضعف قوة وقيمة هذا المحرر مقارنة بالمستندات المكتوبة على الورق، التي يكون القاضي ملزمًا بقبولها كدليل كامل للأدلة كلما تم التوقيع عليها من قبل الأطراف، ولتجنب إضعاف الثقة في المستندات الإلكترونية، تدخل المشرع (٢)، من خلال النص صراحة على التكنولوجيا المعتمدة في التأمين بيانات المستند الإلكتروني[٧٢]، وهذا يجعله يفي بشرط عدم التعديل دون تدخل القاضي في تقييم توفر هذا الشرط[٧٣]. كنا نتمنى أن يراعي المشرع المصري عند اشتراطه على هذه الشروط

المعلومات التي تم إنشاؤها أو إرسالها أو استلامها بدقة. ج- الاحتفاظ بالمعلومات التي تمكن تحديد مرسل البيانات ووجهتها وتاريخ ووقت إرسالها واستلامها، في حالة وجود هذه المعلومات.
٢- لا ينطبق الالتزام بالتخزين في البند (١) من هذه المادة على أي معلومات يكون الغرض الوحيد منها هو تمكين إرسال أو تلقي رسالة. أي شخص آخر بشرط مراعاة الشروط المنصوص عليها في فقرات البند رقم (١) من هذه المادة.

[٧٢] اعتبر المشرع الفرنسي أن الدليل المكتوب يتحقق في كل سند يمكن طباعة الكتابة وحفظها وقراءتها، حتى لو كانت الكتابة غير مرئية أو ملحوظة عند وقوعها على الدعامة، ما دامت. يمكن قراءتها من خلال معالجة الدعم بأجهزة خاصة مثل وضع قرص في الكمبيوتر ليبدو قابلاً للقراءة على الشاشة، ولكن شريطة أن يكون استخدام مثل هذه الدعامات مصحوبًا بآليات تكلف بأمن الرسالة والتحقق من هوية المرسل ونسبته إليه. د. مشرف الدين، أحمد، أصول الإثبات في الأمور المدنية والتجارية، الطبعة الأولى، نادي القضاة، لسنة ٢٠٠٤، ص. ١٠١، نقلاً عن إريك كابريولز، الأمن والثقة في الكتابة الإلكترونية (التوقيع الرقمي وسلطات التصديق) الأسبوع القانوني (١٢٣-١-١٩٩٨).

[٧٣] د. كميل، طارق عبد الرحمن ناجي، التعاقد عبر الإنترنت، دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة محمد الخامس، الرباط، ٢٠٠٣-٢٠٠٤، ص ١٢١.

والمواصفات الواردة في اللائحة التنفيذية مجموعة الشروط العامة المتفق عليها في المجتمع الدولي ومعظم (٤) التشريعات الدولية لقبول صحة الأدلة الإلكترونية[٧٤]، يكمن السبب الرئيسي وراء هذا الاعتراف في القيمة الاستدلالية للأدلة التقنية الرقمية. والموافقة على سلطتها في مجال الأدلة الجنائية من وجهة نظر الفقهاء يعود إلى أن هذه الأدلة هي أدلة واضحة المعالم وقواعد علمية ورياضية دقيقة وحاسمة لا تقبل التأويل أو الشك، في بالإضافة إلى وضوحها ودقتها في إثبات الصلة بين الجاني والضحية أو بين الجاني والسلوك غير المشروع. مما يعزز يقين هذه الادلة والمقتطفات في المحكمة الابتدائية.

قضت محكمة النقض الفرنسية بأن أشرطة التسجيل المغناطيسية التي لها قيمة إثباتية يمكن أن تكون صالحة للعرض أمام العدالة الجنائية، وحكمت محكمة الاستئناف الكندية في أونتاريو في قضية MC Mullen بضرورة قبول سجلات الحاسب الالي كنسخ حقيقية من السجلات. يجب أن تحتوي على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية. قد يشمل ذلك أيضًا وصفًا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرجات التي تم الحصول عليها من (٢) الحاسب الالي موثوقة بدرجة كافية[٧٥].

وهذا ما يدعونا إلى ضرورة قيام مشرعي هذه الدول بالإسراع في وضع أسس وآليات وضوابط لقبول هذه الأدلة الفنية في مجال إثبات الجرائم المعلوماتية وضرورة ما فعله المشرع المصري تماشيا مع ذلك. التطورات في هذا الصدد. على العكس من ذلك، نجد المشرعين في بعض البلدان المقارنة يقفون مكتوفي الأيدي. نجد في التشريع العربي المقارن أي نصوص أو مراجع صريحة تعترف بقيمة وصحة الأدلة المستخرجة من الوسائل التقنية، على غرار التشريع المصري ومعظم التشريعات الأوروبية.

---

[٧٤] د. هلالي عبد الله أحمد، أصالة مخرجات الحاسوب في المسائل الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧، ص. ٤٢ وما بعدها. علي حسن طوالبة، شرعية الأدلة الإلكترونية المستمدة من التفتيش الجنائي، دراسة مقارنة، بحث منشور على الإنترنت، مركز الإعلام الأمني، البحرين، ٢٠٠٩، ص. ١٧.

[٧٥] د. هلالي عبد الله أحمد، أصالة مخرجات الحاسب الآلي، مرجع سابق، ص. ٥٥ وما بعدها. علي حسن الطوالبة، شرعية الدليل الإلكتروني، مرجع سابق، ص ١٨.

(ISSN: 2537- 0758)

أولاً: النتائج:-

١. البحث عن الدليل الرقمي في الوسيط الافتراضي والتحكم في محتوياته أمر مشروع.
٢. يجوز توسيع البحث في بيئة افتراضية خارج حدود الدولة احتراما لمبدأ السيادة. ومع ذلك، يمكن الحصول على الأدلة في بيئة افتراضية خارج حدود الدولة تطبيقاً لاتفاقيات الإنابة القضائية، أو وفقاً لنظام تبادل المساعدات. كما لا يجوز تفتيش نظام المعلومات الذي يمتد إلى منزل غير المتهم إلا في الحالات التي يجوز فيها تفتيش منزل غير المتهم.
٣. موضوع التفتيش على أجهزة ووسائل تكنولوجيا المعلومات الحديثة جدل فقهي واسع ومتزايد، خاصة فيما يتعلق بفحص المكونات المعنوية لهذه الأجهزة والوسائل. من أخطر المراحل عند اتخاذ الإجراءات الجنائية في الجرائم الإلكترونية والجرائم الأخرى التي تشمل الأدلة الإلكترونية؛ باعتبار أن موضوع التفتيش هو جهاز حاسوب أو شبكات أو وسيلة تقنية معلومات.
٤. المفتشون غير قادرين على الحصول على المشترك أو بيانات المستخدم لموقع على شبكة الإنترنت. يجب أن يطلبوا ذلك وكذلك الإذن الخاص بالموقع للحصول على هذه البيانات وفقًا للشروط وسياسة الخصوصية التي وضعها الموقع، ولا يمكن الوصول إليها من خلال الاتفاقيات والمعاهدات الدولية. لأنها بيانات مملوكة للمسؤولين عن الموقع نفسه، ولا تستطيع الدول إجبار هذه المواقع على الكشف عن بيانات مشتركيها.
٥. يشترط في الشخص الذي يقوم بالتفتيش أن يتمتع بجودة يحددها القانون، وبالتالي قد يكون من الصعب عليه إجراء التفتيش في البيئة الافتراضية بسبب نقص أو نقص الثقافة الفنية التي يتطلبها هذا الإجراء، وهناك لا سبيل للتغلب على هذه المشكلة في الوضع الراهن إلا بالاعتماد على الخبرة، مع العلم أن هذا النظام يظل قاصرًا في مواجهة حالة الاستعجال، كما تجسده حالة التلبس بالجرم.
٦. للأدلة الرقمية سلطة حاسمة في بيان الحقائق التي تحتويها، ويمكن التغلب على مشكلة الشكوك حول مصداقيتها بإخضاعها لاختبارات تمكنها من التأكد من صحتها.
٧. عدم وجود خبرة من السلطات المبنية على إجراءات الاستدلال والتحقيق تجعلها غير قادرة على فك رموز الجريمة وكشفها، حيث لا يمكنها جمع الأدلة الجنائية التي تثبتها لجهلها في هذا التخصص، ويمكنها إتلافها أو محوها عند التعامل معهم.
٨. كما يلزم لتأهيل القائمين على إجراءات الاستدلال والتحقيق وتعليمهم علوم الحاسب

وتقنية المعلومات وكيفية التعامل مع الأجهزة الإلكترونية المختلفة عند القيام بإجراءات الاستدلال والتحقيق في الجرائم الإلكترونية.

٩. التزام الشاهد الإعلامي هو التزام بتقديم المعلومات المتعلقة بالجريمة المرتكبة وما يعرفه من معلومات عنها وعن مرتكبها، وليس التزاما بتقديم المعلومات المتعلقة بالنظام موضوع الجريمة.

١٠. تعتبر عملية الاحتفاظ السريع بالبيانات من الإجراءات الحديثة التي لم تكن موجودة من قبل، بل تعتبر من الإجراءات الحديثة التي لم ينص عليها العديد من التشريعات حتى الوقت الحاضر.

ثانياً- التوصيات:

ومن خلال استعراض النتائج السابقة تم التوصل إلى التوصيات التالية والتي تندرج في إطار آليات عمل الجهات الأمنية والقضائية في إثبات الجرائم الإلكترونية **وهي:**

١. تأهيل أعضاء النيابة العامة المسؤولين عن الإدارات المتخصصة في قضايا تقنية المعلومات والتحقيق في الجرائم الإلكترونية، من خلال الدورات والبرامج العملية في مجال تقنية المعلومات.

٢. إنشاء إدارات مختصة بالجرائم الإلكترونية المتعلقة بالبيانات الإسمية في مقار ومراكز الشرطة بالمحافظات والمراكز التابعة لها، حيث تكون أول من يتلقى مثل هذه البلاغات حول هذه الجرائم، وتأهيل كادر متخصص من ضباط الضابطة العدلية وتزويدهم بالمعلومات اللازمة. أحدث المعدات لتنفيذ إجراءات الاستدلال في هذه الجرائم؛ ويرجع ذلك إلى الطبيعة الخاصة للأدلة على هذه الجرائم وسهولة إتلافها ومحوها في وقت قياسي.

٣. أو إنشاء جهاز شرطة متخصص في مكافحة جرائم المعلومات، بحيث يكون أعضاؤه مؤهلين للتعامل مع نظام المعلومات، وتمكينهم من البحث في الوسط الافتراضي والتحكم في محتوياته.

٤. إنشاء قانون دولي موحد، ومحاكم دولية خاصة محايدة تتولى التحقيق في الجرائم الإلكترونية، ولها صلاحية الأمر بالقبض على المجرم الإلكتروني وتقديمه للتحقيق فيه، بغض النظر عن مكان ودولة هذا المجرم، وهذا الاقتراح أو التوصية تتناسب مع موقف الجريمة السيبرانية حيث يتم تمثيل الكرة الأرضية بقرية صغيرة واحدة قريبة المدى.

٥. تفعيل القضاء المتخصص في مجال الجرائم الإلكترونية من خلال تأهيل القضاة وتدريبهم وتخصصهم لنظر القضايا الإلكترونية. لتكون قادرة على مناقشة الأدلة

(ISSN: 2537- 0758)

الإلكترونية المقدمة في القضية مع أطراف القضية من المجالات العلمية والتقنية، وكذلك لتمكينهم من تقييم التقارير المقدمة من قبل الخبراء وصياغة قناعاتهم بشكل صحيح بناءً على المعرفة ومراجعة البينة المعروضة أمامهم، والدفوع والمذكرات والآراء المقدمة في موضوع الدعوى.

٦. تفعيل دور المكافحة الوقائية التي تسبق وقوع الجريمة السيبرانية، من خلال تفعيل دور المؤسسات التعليمية (المسجد، الأسرة، المؤسسات التعليمية، الإعلام)، من خلال التوعية بخطورة الجرائم الإلكترونية على الأسرة والمجتمع، والسعي لتقوية دور المؤسسات التعليمية. الإيمان الديني

٧. سن قوانين وأنظمة خاصة لسد جميع الثغرات في الجرائم الإلكترونية، مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية والحفاظ عليها، ونص سبل إثباتها.

٨. تضمين المناهج على جميع المستويات، وعلى وجه الخصوص المناهج القانونية، فيما يتعلق بالجانب القانوني لأجهزة ووسائل تكنولوجيا المعلومات بما يتماشى مع التطور العلمي والحاجة العملية له.

المراجع

- د. إبراهيم صادق الجندي، ود. حسين حسن الحسيني، تطبيقات الحمض النووي في التحقيق والطب الشرعي، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٢.
- د. حسن علام، قانون أصول المحاكمات الجزائية، الجزء الأول، المجلد الأول، مطبعة روز اليوسف، القاهرة، ١٩٨٢.
- د. محمد أبو العلاء عقيدة، شرح قانون أصول المحاكمات الجزائية، الجزء الأول، دار النهضة العربية، ٢٠٠٣.
- د. جودة حسين جهاد، الوجيز في شرح الإجراءات الجزائية لدولة الإمارات العربية المتحدة، كلية شرطة دبي، طبعة، ١٩٩٤.
- علي فضل البوعينين، مرحلة التفكير والأحكام العامة التي يخضع لها التحقيق في التشريع البحريني، دار النهضة العربية، القاهرة، ٢٠٠٤.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، عام ٢٠٠٩.
- د. المستشار عبد الفتاح بيومي حجازي، مكافحة جرائم الحاسوب والانترنت العربي النموذجي، دار الفكر الجامعي، ٢٠٠٦.

- بذرة. جلال ثروت، أصول المحاكمات الجنائية، دار الجامعة للطباعة والنشر، BY Root، ١٩٨٨.
- د. محمد زكي أبو عامر، الإجراءات الجزائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٢.
- د. نجاتي سيد أحمد سند، أصول الإجراءات الجزائية في التشريع المصري، الجزء الأول، كلية الحقوق، جامعة الزقازيق، القاهرة، ٢٠٠٨.
- د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦م.
- د. صالح أحمد البربري– دور الشرطة في مكافحة الجرائم الإلكترونية في إطار الاتفاقية الأوروبية الموقعة في بودابست بتاريخ ٢٠٠١/١١/٢٣– بحث منشور على الإنترنت على موقع الدليل الإلكتروني (www)..(arablawinfo.com. ٢٠٠٦/٩/٢. في التاريخ المحدد
- نبيلة هبة حروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الأدلة: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠١٣.
- د د. سامي جلال فقي حسين، التفتيش في جرائم المعلومات: دراسة تحليلية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مضر، ٢٠١١.
- د. حازم محمد حنفي، الادلة الالكترونية ودورها فى الاثبات الجنائى، دار النهضة العربية، عام٢٠٠٩.
- د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار الفكر العربي، القاهرة، ١٩٨٨م.
- د. مظهر جعفر عبيد، شرح قانون الإجراءات الجنائية العماني، الجزء الأول، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، ٢٠٠٨م.
- د. فهد عبدالله العبيد العازمي، إجراءات المعلوماتية الجنائية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦.
- د. هشام فريد رستم، الجوانب الإجرائية لجرائم المعلومات، دار النهضة العربية، القاهرة ١٩٩٤.
- د. سليمان مرقص، أصول الإثبات وإجراءاتها، الأدلة المقيدة، الجزء الثالث، دار الحلبي لإصدارات حقوق الإنسان، بيروت، ١٩٩٨.
- د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الآلي، مطبعة المكتب المصري الحديث، القاهرة، ١٩٩١.

(ISSN: 2537- 0758)

- د. عبدالله حسين علي محمود، إجراءات جمع الأدلة في مجال جرائم سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، خلال الفترة ما بين ٢٦-٢٨ أبريل ٢٠٠٣م.
- د. عمر محمد بن يونس، الإجراءات الجنائية على الإنترنت في القانون الأمريكي- الدليل الفيدرالي الأمريكي لفحص وضبط أجهزة الكمبيوتر للدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٨.
- د. عادل عزام سقف الحيط، جرائم القذف والسب والازدراء المرتكبة عبر الوسائط الإلكترونية، دراسة مقارنة، دار الثقافة، القاهرة، ٢٠١١ م.
- د. ممدوح عبد الحميد عبد المطلب، دليل الصور الرقمية لجرائم الحاسوب، مركز أبحاث الشرطة، الشارقة، ٢٠٠٥.
- د. خالد ممدوح إبراهيم، أمن جرائم المعلومات، دار الجامعة، الإسكندرية، ٢٠٠٨.
- د. ثروت عبد الحميد: التوقيع الإلكتروني، ماهيته، مخاطره، وكيفية مواجهته، مدى صلاحيته في الإثبات، الطبعة الثانية، مكتبة الجلاء الجديدة بالمنصورة ٢٠٠٣-٢٠٠٢.
- د. محمد علي سويلم الحماية الجنائية لمعلومات المعاملات الإلكترونية والجرائم الإلكترونية بين الجوانب الإجرائية والأحكام الموضوعية. مطبعة الجامعة، الطبعة الأولى ٢٠١٨.
- نجوى أبو هبة: التوقيع الإلكتروني، تعريفه، مدى صلاحيته في الإثبات، بحث مقدم إلى مؤتمر المصرفية الإلكترونية بين الشريعة والقانون بكلية الشريعة والقانون، جامعة الإمارات، دبي الغرفة التجارية الصناعية في الفترة من ٩-١١ ربيع الأول الموافق ١٠-١٢ مايو ٢٠٠٣م.
- د. سعيد عبد اللطيف حسن- دليل. الجرائم الحاسوبية والجرائم المرتكبة عبر الإنترنت- دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩.
- د. هلالي عبد الله أحمد- التفتيش على أنظمة الحاسبات والضمانات الإعلامية للمتهمين، دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٧.
- كميل، طارق عبد الرحمن ناجي، التعاقد عبر الإنترنت، دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة محمد الخامس، الرباط، ٢٠٠٣-٢٠٠٤.