الدليل الإلكتروني لإثبات الجريمة الإلكترونية

د. مسعود بن حميد المعمري*

الملخص:

يتناول هذا البحث موضوع الدليل الإلكتروني لإثبات الجريمة الإلكترونية وإجراءات جمعه، سواء أكانت تلك الإجراءات تقليدية أم حديثة، ويكتسي هذا الموضوع أهمية متزايدة في ضوء التطورات التقنية المتراكمة والسعي المحموم من قبل المجرمين لتوظيف ذلك في جرائمهم، وكذلك بسبب ظهور مجالات إلكترونية جديدة ممثلة بساحات ووسائل التواصل الاجتماعي، مما يطرح تحديات عدة خاصة في مجال الجرائم الإلكترونية التي لا تزال في عداد الجرائم الأكثر صعوبة في مجال الإثبات الجنائي، بسبب المتطلبات الفنية والقانونية في هذا المجال.

ويهدف هذا البحث إلى بيان خصوصية وطبيعة الدليل الإلكتروني في ضوء التطورات التي شهدها الدليل الإلكتروني سواء في المجال الفني أو في مجال المشروعية والتقنين، حيث يعرض لموقف تشريعات مقارنة واجتهادات فقهية عدة فيما يتعلق بإجراءات جمع وتمحيص وتنظيم هذا النوع من الأدلة. وقد اعتمد الباحث على المنهجين الوصفي والمقارن لرصد الإشكاليات التي يثيرها هذا الموضوع، مع تحليل الأنظمة والتطبيقات التي تقدمها التشريعات والاجتهادات المختلفة وبيان أوجه النقص أو الثغرات التي تعتريها.

وقد خلص البحث إلى عدة نتائج من بينها تأكيد التطورات الفنية والقانونية الجارية على الطبيعة الخاصة للجرائم الإلكترونية التي تميزها عن مختلف الجرائم سواء من حيث الوسائل التي ترتكب بها أم من حيث المحل الذي تقع عليه، وكذلك من حيث الجناة الذين يرتكبون هذه الجرائم. ومن هذه النتائج أيضاً هو أن سلطات التحقيق لا تزال تواجه العديد من الصعوبات في مجال الإثبات الجنائي للجريمة الإلكترونية وإجراءاتها. ولذلك فقد أوصى البحث بضرورة مواكبة التطور التقني الحاصل بإدخال وسائل وطرق حديثة للكشف عن الجرائم والحصول على الأدلة التي تتناسب وطبيعتها الخاصة، وهو ما سيسمح لرجال البحث والتحري بالقيام بمهامهم على أكمل وجه.

كلمات دالة:

أدلة الإثبات الحديثة، الإنترنت، القرصنة، الإثبات الجنائي، الدليل الجنائي.

---

* مساعد العميد للتدريب وخدمة المجتمع، وأستاذ مساعد بقسم القانون العام ورئيس قسم القانون العام سابقاً، كلية الحقوق، جامعة السلطان قابوس، مسقط، سلطنة عمان.

المقدمة:

إن الطابع الخاص الذي تتميز به الجريمة الإلكترونية وما تثيره من صعوبات على عملية إثبات هذه الجريمة، يؤكد القول بأن للجريمة الإلكترونية طبيعة خاصة تحتاج بدورها إلى أدلة ذات طبيعة خاصة، تختلف عما هو عليه الحال في الجرائم التقليدية، حيث تحتاج الجريمة الإلكترونية لأدلة من ذات طبيعتها من أجل إثباتها. وتتمثل هذه الأدلة في الدليل الإلكتروني، أي أن عملية إثبات الجريمة الإلكترونية تستند على الدليل الإلكتروني باعتباره الوسيلة لإثبات هذه الجريمة.

ويعد الإثبات عموماً من أهم وأدق المسائل التى تواجه العدالة القضائية عند الفصل في الحقوق المتنازع عليها والمعروضة أمامها، حيث إن قواعد ووسائل الإثبات تهدف إلى كشف الحقيقة والتي تتجسد بالنهاية في الحكم الذي يصدره القضاء، ولا يكون ذلك إلا بتوفر دليل يؤكد تلك الحقيقة سواء أكانت بإدانة المتهم أم ببراءته، فالدليل هو ما يؤدي إلى إظهار الحقيقة. وعلى مستوى الجريمة الإلكترونية، فإن التطور المطرد في أنواع هذه الجرائم وأسلوب ارتكابها والوسائل المستخدمة في تنفيذها يجعل من القائمين على مكافحتها في سباق مع الزمن من أجل مواكبة ذلك التطور، ولذلك فإنه يقع على السلطات القضائية تطوير وسائل مكافحة هذه الجرائم ووسائل إثباتها، حيث إن اتباع الإجراءات التقليدية لا يجدي لمواجهة هذه الجرائم في كثير من الأحيان، لما تثيره من إشكاليات نتيجة طبيعيتها غير المادية وما تنتجه من أدلة غير ملموسة.

وقد شمل هذا التطور الإجراءات القانونية المتخذة في جمع الأدلة ووسائل الحصول عليها: فعلى مستوى الإجراءات أدركت جهات جمع الاستدلالات والتحقيق كيفية التعامل مع الحاسب الآلي، وكيفية المحافظة على الأدلة التى تحتويها وكذلك كيفية التعامل مع الأجهزة الحديثة ووسائل التقنية المختلفة واستخراج الأدلة منها، وأما على مستوى وسائل الحصول على تلك الأدلة، فقد أدى التطور إلى توظيف التكنولوجيا الحديثة وإمكانياتها في استخراج الأدلة والحصول عليها، مما ساهم في مكافحة هذه الجرائم وفي عملية إثباتها، ومن هذه التقنيات الحديثة كاميرات المراقبة، وأجهزة التسجيل الحديثة، وتعقب المجرمين على شبكة المعلومات عن طريق العنوان الإلكتروني الخاص بكل منهم على الشبكة، وغير ذلك.

أهمية الموضوع:

تعد الجرائم الإلكترونية من الجرائم الأكثر صعوبة في عملية إثباتها، نظراً للطبيعة الخاصة التى تميزها، مقارنة بالجرائم التقليدية وكيفية مواجهتها، فالإثبات الجنائي

الذي يعتمد على الأدلة الإلكترونية يعد من أبرز تطورات العصر الحديث في مجال الإثبات الجنائي في مختلف النظم القانونية، فلم تعد الأنظمة والقواعد التقليدية في إجراءات البحث عن الجريمة والإثبات الجنائي لها تلائم إثبات الجرائم الإلكترونية، سواء من الناحية القانونية أم الفنية، مما يستوجب الاعتماد على الدليل الإلكتروني الذي يلائم طبيعة هذه الجرائم التي تحتاج لنوعية خاصة من الأدلة لإثباتها والوصول إلى مرتكبها. وتبرز أهمية الموضوع لكونه مرتبطاً بظاهرة جديدة من الإجرام وهي الجرائم الإلكترونية، التي بدأت في الظهور والانتشار في الفترة الأخيرة، ودفعت بالدول إلى إصدار التشريعات المنظمة لمكافحتها داخلياً، وإلى إبرام الاتفاقيات الدولية والإقليمية للتعاون في مواجهتها خارجياً، كما شغلت هذه القضية أيضاً فكر الفقه الجنائي من خلال المؤتمرات والندوات.

خطة البحث:

بالنظرية لأهمية الموضوع وخصوصيته، فإننا سنعرض في المبحث الأول لتعريف الدليل الإلكتروني وبيان ماهيته وطبيعته وخصائصه وتقسيماته، ثم نعمد لتفصيل جوانب مشروعيته في نظامي الإثبات المقيد والإثبات الحر وفي النظام القانوني العماني، على أن نبين في المبحث الثاني إجراءات جمع الدليل الإلكتروني والتي تشمل الإجراءات المتعلقة بنظم التشغيل والبيانات الساكنة وتلك المتعلقة بالبيانات المتحركة في شبكة المعلومات، بالإضافة إلى إجراءات الحصول على بروتوكول العنوان الإلكتروني.

المبحث الأول
الدليل الإلكتروني: ماهيته ومشروعيته

تحتاج الجريمة الإلكترونية لأدلة من ذات طبيعتها من أجل إثباتها، وتتمثل هذه الأدلة في الدليل الإلكتروني، أي أن عملية إثبات الجريمة الإلكترونية تستند على الدليل الإلكتروني باعتباره الوسيلة لإثبات هذه الجريمة، وعليه سيكون محور حديثنا في هذا المبحث هو ماهية الدليل الإلكتروني في (المطلب الأول)، ومشروعية الدليل الإلكتروني في (المطلب الثاني).

المطلب الأول
ماهية الدليل الإلكتروني

لابد من توضيح ماهية الدليل الإلكتروني وذلك قبل التطرق لمراحل إثبات الجريمة الإلكترونية، وعليه سنتناول هذا الموضوع من خلال تعريف الدليل الإلكتروني (الفرع الأول)، وبيان طبيعة الدليل الإلكتروني (الفرع الثاني)، ثم التطرق لخصائص الدليل الإلكتروني (الفرع الثالث) وتقسيماته في (الفرع الرابع).

الفرع الأول
تعريف الدليل الإلكتروني

أولاً- الدليل لغةً:

يقصد بالدليل لغةً المرشد وما يتم به الإرشاد، وما يستدل به، وهو أيضاً الدال، والجمع أدلة ودلائل[1]. والدليل ما يستدل به، ودلّه على الطريق أي أرشده، يدلُه بالضم، ودلالة بفتح الدال وكسرها ودلولة بالضم والفتح أعلى، ويقال أدل، والاسم الدال بتشديد اللام، فلان يدل فلاناً أي يثق به، قال أبو عبيدة: الدال قريب المعنى من الهدى وهما في السكينة والوقار في الهيئة والمنظر وغير ذلك[2].

ثانياً- الدليل اصطلاحاً:

أما الدليل اصطلاحاً فهو الذي يلزم من العلم به علم بشيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل إلى معرفة الحقيقة، وأيضاً يقصد بالدليل ما يمكن التوصل به إلى معرفة الحقيقة[3].

(1) د. جميل صليبا، المعجم الفلسفي، الجزء الأول، دار الكتاب العالمي، مكتبة المدرسة، بيروت، 1994، ص 564.
(2) محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، المطبعة الأميرية، القاهرة، 2016 م/ 1338هـ، ص 209.
(3) المرجع السابق، ص 564-565.

ثالثاً- الدليل في القانون:

أما الدليل في الاصطلاح القانوني فيقصد به الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، ويقصد بالحقيقة في هذا السياق بأنها: كل ما يتعلق بالإجراءات والوقائع المعروضة على القاضي لإعمال حكم القانون عليها، ويقصد بالدليل أيضًا الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها[4]. كما يشار إلى الدليل بأنه كل إظهار لنشاط عام أو خاص داخل الخصومة أو من أجلها يؤدي مباشرة إلى التأثير في تطور رابطة الخصومة، أو بمعنى آخر: هو كل عمل يجري في الخصومة أو يهدف إلى إعدادها أو له قيمة في الخصومة -أياً كانت طبيعته أو معناه- نظمه القانون بقصد الوصول إلى تطبيق القانون الموضوعي فيها[5].

وعليه يمكن القول من ذلك بأن الدليل الجنائي بشكل عام هو الوسيلة التي تؤدي بالقاضي إلى الحقيقة التي يطلبها عن طريق إجراءات قانونية لإثبات واقعة معينة، وبعد تعريف الدليل في اللغة والاصطلاح والمجال القانوني له بشكل عام، نتطرق بعد ذلك إلى تعريف الدليل الإلكتروني باعتباره كما أسلفنا هو ما يُستند عليه لإثبات الجريمة الإلكترونية.

رابعاً- تعريف الدليل الإلكتروني:

تعددت تعريفات الدليل الإلكتروني واختلف الفقه فيها، فاتجه البعض منه نحو التوسع في تعريف الدليل الإلكتروني، والبعض الآخر نحو تضييقه وحصره في نواحٍ معينة، وذلك بحسب الزاوية والمجال الذي ينظرون إليه، وعليه سنتناول أهم التعريفات التي وردت حول الدليل الإلكتروني، فقد عرف البعض الدليل الإلكتروني بأنه: «الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة»[6]، وكذلك عُرِّف بأنه: «معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية من خلال ترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه»[7]. كما تم تعريف الدليل

(4) د. عبدالرزاق السنهوري، الوسيط في شرح القانون المدني الجديد، الجزء الثاني، دار النهضة العربية، القاهرة، 1968، ص 13.

(5) د. أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه منشورة، كلية الحقوق، جامعة عين شمس، القاهرة، 1982، ص 473.

(6) د. أشرف عبد القادر قنديل، مرجع سابق، ص 123.

(7) د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص 234.

الإلكتروني بأنه: «بيانات يمكن إعدادها وتراسلها وتخزينها رقمياً بحيث تمكن الحاسب الآلي من تأدية مهمة ما»[8]، وقد أخذ بهذا التعريف الأخير التقرير الأمريكي المقدم إلى ندوة الأنتربول العلمية حول الدليل الرقمي عام 2001، وأيضاً عُرف بأنه: «الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون»[9].

الفرع الثاني

طبيعة الدليل الإلكتروني

إن الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني عن الأدلة الجنائية الأخرى، والبيئة التي يتواجد فيها كذلك وهي بيئة افتراضية غير مادية تختلف عن بيئة الأدلة المادية، إضافة إلى تعدد صور وأشكال الدليل الإلكتروني، أدت إلى الاختلاف والتساؤل حول موقع الدليل الإلكتروني من بين تقسيمات الأدلة الجنائية بشكل عام، وقبل التطرق لذلك نوضح تقسيمات الدليل الجنائي بصفة عامة وهي تتمثل في: تقسيم الأدلة من حيث مصدرها، تقسيم الأدلة من حيث الجهة التي قدم إليها، تقسيم الأدلة من حيث الواقعة المراد إثباتها، وتقسيم الأدلة من حيث الأثر المترتب على الدليل.

وما يهمنا في هذا المجال أن نوضح تقسيم الأدلة من حيث مصدرها، فهو الأساس الذي يمكن المقارنة من خلاله بين الدليل الإلكتروني والأدلة الجنائية الأخرى، حيث تنقسم الأدلة من حيث المصدر إلى أدلة قانونية، وأدلة قولية، وأدلة مادية، وأدلة فنية، وسنوضح معنى كل دليل منها وفق التالي:

أولاً– الأدلة القانونية:

وهي الأدلة التي حددها المشرع وحدد قوة كل منها، حيث لا يمكن الإثبات بغيرها، كما لا يمكن للقاضي أن يمنح أي دليل منها قوة أكبر مما حدد لها المشرع، وهذا هو الأصل

(8) "Digital Evidence: information of probative values stored or transmitted in digital form": Mark M. Pollit, Report on Digital Evidence, presented to 13th Interpol Forensic Science Symposium, Lyon, France, Oct 162001, 19,– P5.

د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي– المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، 2008.

(9) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص 2.

في الدعوى المدنية، أما الدعوى الجنائية فإن للقاضي حرية تكوين قناعته من أي دليل مطروح في الدعوى، فالأدلة غير محصورة، إلا أنه يرد على ذلك استثناءات معينة على حرية القاضي، حيث يحدد القانون أدلة معينة يجب أن تتوافر في الدعوى من أجل إدانة المتهم فيها، وتكون لهذه التفرقة في حرية القاضي أهمية للأدلة المادية والقولية، أما للأدلة القانونية فإنها تنحسر، ومثال ذلك أن يشترط المشرع وجوب تواجد أربعة شهود في جريمة الزنا[10].

ثانياً- الأدلة القولية:

وهي الأدلة التي مصدرها الأشخاص الذين أدركوا معلومات مفيدة للإثبات، وتتمثل فيما يصدره الغير من أقوال وهي الاعتراف وأقوال الشهود، وتؤثر الأدلة القولية في اقتناع القاضي بطريقة غير مباشرة من خلال تأكده من صدق الأقوال والشهادة، وتسمى كذلك بالأدلة المعنوية أو النفسية أو الشفوية.

ثالثاً- الأدلة المادية:

وهي التي تنتج من عناصر مادية ناطقة بنفسها، ويمكن إدراكها بالحواس، وتؤثر في اقتناع القاضي بطريقة مباشرة[11]، وذلك مثل ما يتركه الجاني من أدوات في مسرح الجريمة كبصمات الإصبع أو السكين، ويتم الحصول على هذه الأدلة المادية عن طريقة المعاينة أو الضبط أو التفتيش أو الخبرة.

رابعاً- الأدلة الفنية:

وهي الأدلة التي تصدر من رأي الخبير الفني عند تقديره لدليل مادي أو دليل قولي قائم في الدعوى، وذلك وفق معايير ووسائل علمية معتمدة في ذات المجال، كتقدير عيوب سلعة معينة في جريمة احتيال كالسيارات والبضائع وغيرها.

فأين تكون الأدلة الإلكترونية ضمن هذه الأدلة، فهل تكون أدلة مادية باعتبارها ناتجة من عناصر مادية وتستخرج في هيئة مادية ملموسة، أم أنها معنوية غير مرئية، أو أنها أدلة فنية كذلك باعتبارها صادرة من خبير فني وعلى أساس علمي؟

اختلفت آراء الفقه في هذا الشأن حول طبيعة الدليل الإلكتروني، ويمكن إجمال هذا الاختلاف في ثلاثة اتجاهات، ونذكرها تفصيلاً فيما يلي:

(10) د. أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي: دراسة مقارنة، دار النهضة العربية، القاهرة، 2015، ص 14.

(11) د. أشرف عبد القادر قنديل، مرجع سابق، ص 129.

الاتجاه الأول:

يرى أنصار هذا الاتجاه[12] أن الدليل الإلكتروني هو دليل مادي، حيث إنه يُشكِّل مرحلة متقدمة من الأدلة المادية الملموسة التي تدرك بالحواس، ويرى هذا الاتجاه أن الأدلة الإلكترونية بأنواعها ومختلف أشكالها سواء أكانت في شكل مخرجات ورقية أم غير ورقية هي أدلة مادية، حيث إنه يمكن استخراج المخرجات غير الورقية في شكل دعامات كالأشرطة الممغنطة أو الأقراص المغناطيسية أو أوراق، وبالتالي تصبح ذات طبيعة مادية. فإذا تم التحفظ على الحاسب الآلي أو القطع الصلبة التي تكونه، فإنها لا تعتبر أدلة إلكترونية وإنما أدلة مادية عادية، أما إذا كان التحفظ على قرص ممغنط ويحتوي على أرقام سرية لبطاقات ائتمان أو بريد إلكتروني، فهذه تعتبر أدلة إلكترونية حتى وإن كان التحفظ على القرص إلا أنه يعتبر البيئة التي يتواجد بها الدليل الإلكتروني، وذلك بسبب الطبيعة التي عليها الدليل الإلكتروني، مما يجعل من البيئة التي يتواجد فيها ذات أهمية، فبدون تلك البيئة لا يمكن التعويل على الدليل الإلكتروني في الإثبات، فلا يمكن الحكم استناداً إلى تقرير يؤكد وجود قرص متحفظ عليه يحتوي على ملفات محل الجريمة، بل لابد من فتح القرص أمام القضاء والاطلاع عليه، ومن ثم تقدير ذلك الدليل وتحديد قيمته[13].

ويرى أنصار هذا الرأي كذلك أنه ليس لزاماً لمس الدليل باليد وإنما يكفي إدراكه بالنظر أو السمع عن طريق شاشة الجهاز، كملفات الكتابة (word) أو الأفلام والمقاطع المرئية (video)، لاعتبار الدليل الإلكتروني من الأدلة المادية. وقد تم الرد على هذا الاتجاه بأن هناك حالات من الأدلة لا تعد دليلاً مادياً مثل الأدلة المستمدة من الوسائل التي تمس سلامة جسم الإنسان كجهاز كشف الكذب والتنويم المغناطيسي، وكذلك الوسائل السمعية والبصرية التي يترتب على استخدامها تعدٍ على الحياة الخاصة للإنسان مثل كاميرات المراقبة وأجهزة التنصت[14].

الاتجاه الثاني:

يرى أنصار هذا الرأي أن الأدلة الإلكترونية هي أدلة معنوية، فهي أدلة غير ملموسة، وإذن فالدليل الإلكتروني وفق هذا الاتجاه عبارة عن مجالات مغناطيسية أو كهربائية، الأمر الذي يترتب عليه أن إخراج الدليل الإلكتروني في شكل مادي ملموس لا يدل على

(12) من بينهم د. حازم محمد حنفي، في مؤلفه الدليل الإلكتروني ودوره في المجال الجنائي، مرجع سابق، ص 15.

(13) د. حازم محمد حنفي، مرجع سابق، ص 15.

(14) د. أحمد أبو القاسم، الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1991م، ص 17.

أن المخرجات هي الدليل، وإنما هي عملية نقل تلك المجالات من طبيعتها التقنية والرقمية إلى هيئة يمكن الاستدلال بها على معلومة معينة[15]. ويرى أنصار هذا الرأي كذلك أن فهم مضمون الدليل الإلكتروني يعتمد على استخدام أجهزة تقنية خاصة لتحليل محتوى الدليل، وأن ما لا يمكن تحليله وفهم محتواه لا يعتبر ضمن الأدلة الإلكترونية، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، مما يُلغي قيمته في إثبات الجريمة ومعرفة مرتكبها.

الاتجاه الثالث:

يذهب أنصار هذا الاتجاه إلى القول بأن الدليل الإلكتروني هو نوع متميز ومختلف من وسائل الإثبات، ويتضمن مواصفات وخصائص تميزه عن الأدلة الجنائية الأخرى، مما يؤهل الأدلة الإلكترونية لتكون كإضافة للأدلة الجنائية الأخرى (المادية والمعنوية والقولية والفنية)، لما تتمتع به من خصائص تميزها أن تكون تحت مظلة أحد أنواع الأدلة الجنائية السابقة[16].

الفرع الثالث

خصائص الدليل الإلكتروني

إن البيئة الافتراضية التي يتواجد بها الدليل الإلكتروني وهي البيئة الرقمية، تحتوي على بيانات رقمية متعددة الأنواع، وهي ما تكون دليلاً سواء بصورة منفردة أو مجتمعة، لذا فهي بيئة متطورة بطبيعتها، وينعكس ذلك على الدليل الإلكتروني ذاته الذي يتأثر بالبيئة التي يعيش فيها، فقد أضفت هذه البيئة عليه طبيعة خاصة وخصائص تميزه كدليل جنائي عن الأدلة الجنائية التقليدية الأخرى، ويمكن الإشارة إلى تلك الخصائص التي تميزه وفق الآتي:

أولاً- الدليل الإلكتروني دليل علمي:

إن الطبيعة الخاصة للدليل الإلكتروني والوسط الذي يتواجد به وهي بيئة افتراضية غير ملموسة، تجعل من الدليل دليلاً غير مادي كذلك، فهو دليل غير ملموس يتكون من بيانات ومعلومات على هيئة إلكترونية، حيث إن العالم الافتراضي التقني هو عالم أعده متخصصون في التقنية، وبالتالي لا يمكن الحصول على البيانات والمعلومات في ذلك العالم التقني إلا بأساليب علمية وتقنية كذلك، وهو ما يميز الدليل الإلكتروني بهذه

(15) د. أحمد يوسف الطحطاوي، مرجع سابق، ص 28.
(16) د. محمد الأمين البشري، مرجع سابق، ص 235.

الخاصية بأنه دليل علمي[17]، فاستخراج الدليل الإلكتروني يحتاج إلى بيئة مشابهة للبيئة التي نتج عنها، لذا يتطلب الاستعانة بأجهزة وأدوات التقنية واستخدام برامج حاسوبية ملائمة، للاطلاع عليه أو استخراجه في هيئة ملموسة أو مادية، وهي تُعد أساليب علمية[18].

ثانياً– الدليل الإلكتروني دليل تقني:

يقصد بالتقنية: العلم التطبيقي لوسائل وأدوات تم اختراعها من أجل تسهيل حياة الفرد والمجتمع[19]، وهي تقوم على أساس علمي، مثلها مثل الدليل الإلكتروني الذي هو كذلك دليل علمي، لذا يمكن استنتاج أن الدليل الإلكتروني يتميز بأنه دليل تقني، استناداً للمصدر الذي جاء منه وهو البيئة الرقمية أو التقنية، مثلما هو دليل علمي استناداً للبيئة التي يتواجد بها والتي تم انشاؤها من قبل مختصين فنيين على أساس علمي. إن الدليل الإلكتروني التقني ليس كالأدلة الجنائية التقليدية الأخرى، فالتقنية لا تنتج أدلة مادية ملموسة كالسلاح أو البصمات أو الاعتراف المكتوب تدل على مرتكب الجريمة، إنما ما تنتجه التقنية نبضات رقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل بين أجزاء وسائل التقنية وشبكات الاتصال متعدية حدود المكان والزمان الواحد[20].

وتفيد هذه الخاصية للدليل الإلكتروني أنه لابد لمأموري الضبط القضائي وسلطات التحقيق أن يبنوا عملهم على أساس الخبرة في التقنية، فلدى بعض الدول المتقدمة يكون لسلطات التحقيق المقومات التقنية الكاملة التي تحتاجها، ويكون هناك فصل بين الخبرة وسلطة التحقيق في الجرائم التي يكون الاعتماد فيها على الدليل الإلكتروني، حيث تضم سلطة التحقيق عناصر ذات كفاءة عالية تمتلك الخبرة في التقنية كما هو الحال في الولايات المتحدة الأمريكية[21]، أما سلطات التحقيق التي لا تمتلك ذلك فإنها تعتمد على الخبرة في تحقيق مثل هذه الجرائم الإلكترونية التي تستند على الدليل الإلكتروني لإثباتها، وبالتالي لا يتحقق الفصل بين سلطة التحقيق والخبرة، حيث إن الخبرة تقوم بدور في التحقيق لمساعدة سلطة التحقيق لإثبات الجريمة والدليل التقني.

(17) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ص 61–62.
(18) د. أشرف عبد القادر قنديل، مرجع سابق، ص 126.
(19) د. حازم محمد حنفي، مرجع سابق، ص 17.
(20) عائشة بن قارة مصطفى، مرجع سابق، ص 62.
(21) د. فتحي محمد أنور عزت، مرجع سابق، ص 648.

ثالثاً– الدليل الإلكتروني دليل متنوع ومتطور:

إن مصطلح الدليل الإلكتروني يشمل كافة أنواع وأشكال البيانات الرقمية والتي من الممكن تداولها تقنياً بين وسائل تقنية المعلومات، بحيث تكون بين تلك البيانات وبين الجريمة المرتكبة رابطة معينة وتتصل من الجانب الآخر بالمجني عليه، كما يكون للجاني صلة بها، ومن ذلك تتضح خاصية أن الدليل الإلكتروني هو دليل متنوع، ولو كان الدليل متحد التكوين بلغة التقنية. وتعني هذه الخاصية من حيث التنوع أن الدليل الإلكتروني يمكن أن يظهر على هيئات مختلفة، فقد يكون غير مقروء للأشخاص مثلما هو الحال في المراقبة عبر الشبكات أو الخوادم التقنية للشبكات، وقد يكون مقروءاً ومفهوماً للأشخاص مثلما يكون عليه الدليل في صورة وثيقة أو صورة مخزنة بجهاز حاسب آلي أو في البريد الإلكتروني. أما خاصية الدليل الإلكتروني كدليل متطور فهي تفيد أنها تستخدم في جرائم مستحدثة، فجريمة النصب مثلاً يمكن ارتكابها بالطرق التقليدية التي تنتج أدلة مادية، وكذلك أصبح مع التقدم التكنولوجي من الممكن ارتكابها باستخدام التقنية سواء أكانت باستخدام جهاز حاسب آلي، أم أن يكون الحاسب الآلي محلاً لارتكاب جريمة النصب[22].

وهذا التطور في مجال الدليل الإلكتروني وتطور الجرائم معه، ومع التقدم المستمر في مجال التكنولوجيا، فإن ذلك قد يشكل عائقاً في الوصول للأدلة الإلكترونية والتي تفيد في اكتشاف الجريمة ومرتكبيها، لذا فإنه يكون من الواجب مواكبة التطور التقني، سواء من حيث الأجهزة المستحدثة أو البرامج التشغيلية والمستخدمة داخل هذه الأجهزة وبرامج الحصول على الأدلة الإلكترونية، إلى جانب الاطلاع على تلك التطورات والتحديثات المستمرة للأجهزة والبرامج، وهو ما يساعد على الكشف عن الأدلة الإلكترونية وإثبات الجريمة بطريقة أسهل وأسرع.

رابعاً– الدليل الإلكتروني يصعب التخلص منه:

تعتبر هذه الخاصية من أهم الخصائص التي يتميز بها الدليل الإلكتروني عن الأدلة التقليدية الأخرى[23]، حيث إنه يمكن التخلص بسهولة من الأدلة الأخرى كالأوراق والسلاح والأموال المزورة بإتلافها وحرقها لتختفي معالمها، وأيضاً بالنسبة لبصمات الإصبع، حيث يمكن مسحها بسهولة وإخفاؤها من موضعها، أما الدليل الإلكتروني بشكل خاص وكل ما يتعلق بتكنولوجيا المعلومات بشكل عام، فإنه كلما حدث ارتباط أو اتصال مع شبكة الاتصال أو وسيلة تقنية المعلومات وبمعنى إدخال لبيانات معينة،

(22) د. حازم محمد حنفي، مرجع سابق، ص 19–20.
(23) عائشة بن قارة مصطفى، مرجع سابق، ص 62.

فإنه يصبح من الصعب التخلص من ذلك ولو استخدمت أدوات الحذف والإلغاء. وكما أن التخلص من الدليل الإلكتروني باستخدام الأدوات المتوفرة في وسيلة التقنية مثل خيارات الحذف أو الإلغاء أو الإزالة، لا تعتبر من العوائق التي تمنع من استرجاع الدليل، فهناك برامج متخصصة من ذات طبيعة الدليل التقني تُمكِّن الجهات القضائية المختصة من الحصول على الدليل المحذوف واسترجاع البيانات الملغاة من الجهاز محل ارتكاب الجريمة.

ويترتب على أن الدليل الإلكتروني يصعب التخلص منه مسائل قانونية مهمة، ومنها مسألة التخلص من الدليل محل ارتكاب الجريمة التي تعتبر جريمة مستقلة كذلك، فإعداد أو استخدام برامج من قبل مرتكبي الجريمة الإلكترونية تكون مهمتها حذف البيانات وإزالتها من الجهاز أو شبكات الاتصال، تشكل بذاتها جريمة، وبالتالي فإنه يمكن إدانة الجناة على ذلك حسب تجريم قوانين الجزاء لها، فإذا أثبت الخبير التقني حدوث الجريمة واستخدام تلك البرامج، التي قد تكون غير قانونية في الأصل، فتشملهم عقوبة ذلك الجرم[24].

وعليه فإن المشرع مطالب بوجود نصوص قانونية تجرم تلك الأفعال التي تتضمن التخلص من الأدلة الجنائية التي يمكن الاستناد عليها لإثبات جريمة معينة، فالتشديد في هذا المجال يمنع إفلات المجرم من العقاب إذا ما قام بحذف وإلغاء الأدلة التي تدينه على ارتكاب جريمة ما، وكما أنه لابد من مواكبة التطور نحو استخدام برامج تساعد على استخراج الأدلة حتى لو قام الجاني بحذفها ببرامج متخصصة أخرى. وأيضاً هناك مسألة قانونية تقابل مسألة التخلص من الدليل الإلكتروني، وهي مسألة اعتبار أن الدليل الإلكتروني أو التقني ذو طبيعة مرنة، ونتيجة ضعفه فإنه يسهل إتلافه وفقده، وبالتالي يمكن التخلص منه بغير طريقة الحذف والإلغاء، وذلك مثل عملية إتلاف الدليل المادي، على أن هذا القول قد واجه انتقاداً باعتبار أن الإتلاف نتيجة القصور من الجهات القضائية المختصة في قدراتها التكنولوجية وليس في الدليل ذاته، كما اعتبر أنصار هذا الرأي الذي لا يعيب الدليل الإلكتروني أن الدليل بطبيعته المرنة يصل إلى استحالة التخلص منه[25].

خامساً: الدليل الإلكتروني قابل للنسخ:

الأصل أنه عند إعداد نسخة من محتوى دليل معين فإن قوته لن تكون مثل قوة الأصل في

(24) د. حازم محمد حنفي، مرجع سابق، ص 22.

(25) د. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، الإسكندرية، 2010، ص 655.

حجية إثباته، سواء أكان في المجال الجنائي أم المدني، كما أن الأدلة التقليدية الأخرى على خلاف الدليل الإلكتروني، إذ لا يمكن الحصول على نسخ من تلك الأدلة لتقديمها كدليل بديلاً عن الأصل، فالمحرر المزور لابد من مضاهاته مع الأصل عن طريق المستند المزور وليس نسخة له، إلا أن ذلك يختلف في مجال الدليل الإلكتروني فهو دليل يمكن استخراج نسخ منه مطابقة للأصل ويكون لتلك النسخة ذات القيمة العلمية للأصل[26]، فتعتبر هذه الخاصية ضمانة للحفاظ على الدليل من الفقد أو الحذف أو التغيير أو التلف، وذلك من خلال نسخ الدليل لنسخ تكون طبق الأصل ولها ذات الحجية الثبوتية، فالوثيقة المحفوظة على هيئة مستند في جهاز الحاسب الآلي يمكن نسخها بسهولة من الأصل وتقديم الملف المنسوخ كدليل إثبات دون الحاجة لتقديم الأصل، ويكون لتلك النسخة ذات القيمة العلمية والحجية التي يمتلكها الأصل.

الفرع الرابع
تقسيمات الدليل الإلكتروني

إن من خصائص الدليل الإلكتروني أنه دليل متنوع، إذ هو مستخرج لا يظهر في صورة واحدة، بل له العديد من الأشكال والصور، لذلك فقد ذهب الفقه والتشريعات إلى تقسيم الأدلة الإلكترونية إلى أربعة أقسام رئيسية، هي:

- الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكاتها.
- الأدلة الرقمية الخاصة بالإنترنت.
- الأدلة الرقمية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

ويتشابه التقسيم السابق للفقه مع تقسيم آخر له حول الجريمة عبر الكمبيوتر، حيث يرى بعض الفقه أن المقصود بهذه الجريمة بأنها: «الجرائم التي لها علاقة بالكمبيوتر والشبكة المعلوماتية أو ما يعرف باسم الويب والإنترنت، أما الإنترنت فهي آلية نقل المعلومات عن طريق البروتوكولات الخاصة بالاتصال السلكي واللاسلكي»[27]، وبناء على ذلك التعريف قاموا بتقسيم الجريمة إلى أربعة أنواع وهي كالتالي:

- **النوع الأول:** جرائم الكمبيوتر ويقصد بها سلوك إنساني يشكل فعلاً غير مشروع قانوناً ويقع على أجهزة الكمبيوتر، سواء وقع هذا السلوك على المكونات المادية أو

(26) عائشة بن قارة مصطفى، مرجع سابق، ص 64.

(27) د. ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز بحوث الشرطة، الشارقة، 2005، ص 18.

المكونات المعنوية أو قواعد البيانات الرئيسية[28].

– **النوع الثاني:** جرائم الشبكة العالمية وهي أي سلوك إنساني يكون فعلاً غير مشروع قانوناً ويقع على أي وثيقة أو نص موجود بالشبكة[29]، كجريمة الاعتداء على بطاقات الائتمان، الاعتداء على حقوق الملكية الفكرية، وجرائم الاختراق.

– **النوع الثالث:** جرائم الإنترنت ويقصد بها سلوك إنساني يشكل فعلاً غير مشروع قانوناً وتقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات[30]، كجرائم استخدام عناوين بروتوكول إنترنت (IP – Protocl Internet) غير حقيقية، والدخول غير المشروع لمواقع غير مصرح بالدخول إليها.

– **النوع الرابع:** جرائم باستخدام الكمبيوتر، وفي هذه الجرائم لا يتم استخدام الكمبيوتر أو الشبكة العالمية للمعلومات أو الإنترنت في الفعل الجرمي وإنما يتم استخدامها كوسيلة مساعدة لارتكاب الجرائم، وذلك مثل جرائم غسيل الأموال، وجرائم تهريب المخدرات.

ويتضح من ذلك مدى التقارب والتطابق بين التقسيم الفقهي للدليل الإلكتروني والتقسيم الفقهي كذلك للجريمة عبر الكمبيوتر. كما أن هناك اتجاهاً فقهياً آخر بشأن تقسيم الدليل الإلكتروني يرى بأنه يمكن تقسيم الدليل الإلكتروني إلى نوعين رئيسين هما:

النوع الأول– أدلة أعدت لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية يمكن إجماله فيما يلي:

1. السجلات التي تم إنشاؤها بواسطة الجهاز الإلكتروني تلقائياً، وتعتبر هذه السجلات من مخرجات الجهاز التي لم يسهم الإنسان في إنشائها، مثل سجلات جهاز الهاتف النقال وسجلات البطاقة البنكية، حيث يحفظ الهاتف النقال سجل المكالمات دون الحاجة لتدخل الشخص لحفظها يدوياً وكذلك بالنسبة لجهاز السحب الآلي للبنك.
2. السجلات التي تم حفظ جزء منها بالإدخال، وجزء تم إنشاؤه بواسطة الجهاز، مثل رسائل البريد الإلكتروني، حيث يقوم الشخص بكتابة الرسالة ويقوم الجهاز بإكمال البيانات مثل توقيت الإرسال والاستلام وحفظها في البريد المرسل[31].

(28) عائشة بن قارة مصطفى، مرجع سابق، ص 72.
(29) د. ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 18.
(30) د. أشرف عبد القادر قنديل، مرجع سابق، ص 132.
(31) أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2016، ص 290.

النوع الثاني– أدلة لم تعد لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية ينشأ دون إرادة الشخص، فهو يعد أثراً يتركه الشخص دون أن يكون قاصداً بوجوده، ويسمى هذا النوع من الأدلة بالبصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية، وتتمثل هذه الآثار فيما يتركه الشخص عند استخدام الجهاز أو الشبكة المعلوماتية من سجلات أو بيانات يتم تسجيلها عند إرسال أو استقبال الرسائل والمكالمات سواء من خلال الجهاز أو شبكة المعلومات العالمية. والأصل أن هذا النوع من الأدلة لم يعد أساساً للحفظ من قبل الشخص المستخدم للجهاز أو الشبكة، إلا أن هذه الأجهزة والوسائل التقنية تقوم بحفظها حتى ولو بعد فترة زمنية من حدوثها، فكافة العمليات التي يتم إجراؤها من قبل المستخدم على الجهاز أو الشبكة والمراسلات والاتصالات التي تتم، يمكن ضبطها كأدلة من قبل المختصين أو بواسطة التقنيات والبرامج الخاصة بذلك[32].

وتبدو أهمية التمييز بين هذين النوعين من الأدلة فيما يلي:

أ. يتميز النوع الأول من الأدلة الإلكترونية بسهولة الحصول عليه، باعتباره أعد أصلاً ليكون دليل إثبات على الوقائع التي يتضمنها، أما النوع الثاني من الأدلة فيتم الحصول عليه باتباع الأساليب التقنية الخاصة بذلك والذي لا يمكن الحصول عليه بسهولة دون وجود خبرة أو برامج خاصة لذلك.

ب. يتم الاحتفاظ بالنوع الأول من الأدلة للاحتجاج به لاحقاً، وذلك لأنه أعد كوسيلة لإثبات الوقائع مما يقلل من إمكانية فقده، أما النوع الثاني من الأدلة فهو عرضة للفقد لأسباب منها فصل التيار الكهربائي عن الجهاز، وذلك لأنه لم يعد للحفظ ويحتاج لبعض الأساسيات للاحتفاظ به وعدم فقدانه.

ج- يكون النوع الثاني من الأدلة أكثر أهمية من النوع الأول من الأدلة، وذلك باعتبار أن النوع الثاني لم يعد أصلاً ليكون أثراً لمن صدر منه، لذا فإنه عادة ما يتضمن معلومات وبيانات تفيد في إثبات الجريمة ومعرفة مرتكبها.

المطلب الثاني

مشروعية الدليل الإلكتروني

يقصد بمشروعية الدليل الإلكتروني في هذا الإطار هو الاعتراف به أمام القانون والقضاء، فمشروعية وجود الدليل الإلكتروني تدل على أن القانون يجيز للقاضي الأخذ

(32) أمير فرج يوسف، مرجع سابق، ص 290–291.

بهذا الدليل وأن يستند عليه في حكمه ضد المتهم، أو لا يجيز له ذلك فيكون غير مشروع. وسوف نتناول ذلك تفصيلاً في نظام الإثبات المقيد (الفرع الأول)، وفي نظام الإثبات الحر(الفرع الثاني)، وأخيراً في القانون العماني (الفرع الثالث).

الفرع الأول

مشروعية الدليل الإلكتروني في نظام الإثبات المقيد

في هذا النظام تكون إرادة المشرع هي الأقوى، وهي التي تحدد الأدلة التي يكون على القاضي اتباعها والأخذ بها عند بناء حكمه في الدعوى، أما إرادة القاضي فتكون في مرتبة أدنى من ذلك، حيث إن تدخّل إرادة المشرع تؤدي إلى تراجع إرادة وحرية القاضي، كما أن إرادة المشرع هي التي تحدد القوة القانونية للأدلة، فعند توافر شروط وعناصر الأدلة يكون على القاضي الحكم بالاستناد إليها دون تدخل إرادته وقناعته في قوة هذه الأدلة، ولا يبقى لديه سوى تنفيذ إرادة المشرع دون غيرها[33]. وعليه لا يمكن للقاضي الاستناد إلى دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، لذا يسمى هذا النظام كذلك بالنظام القانوني أو نظام التحديد، حيث يحدد القانون قائمة من الأدلة مع قيمتها الإثباتية يكون على القاضي الالتزام بها عند نظر الدعوى، وينتمي هذا النظام للنظم ذات الثقافة الأنجلو- سكسونية، كالولايات المتحدة الأمريكية والمملكة المتحدة البريطانية.

لذلك فإن النظم التي تأخذ بهذا النظام لا يمكن الاعتراف من خلالها للدليل الإلكتروني بأي قيمة إثباتية أو القول بمشروعية وجوده، إلا إذا نص القانون صراحة عليه ضمن قائمة الأدلة التي يجب على القاضي الأخذ بها، وبالتالي فإنها تخضع لما يحدده المشرع من اعترافه بالدليل الإلكتروني من عدمه وبالقوة القانونية التي يمنحها له. أما خلو القانون من وجود نص على الدليل الإلكتروني في نظام الإثبات المقيد، فإنه يؤدي إلى طرح قيمته الإثباتية ويصبح عديم القيمة مهما توافرت فيه شروط اليقين به لدى القاضي، فلا يجوز له أن يستند إليه عند تكوين عقيدته في الدعوى والحكم بها، وبالتالي قد يحكم القاضي في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من الأدلة المعروضة عليه والتي لا يعترف به المشرع قانوناً.

إن نظام الإثبات المقيد بدأ ينحصر نطاقه حتى لدى التشريعات التي تأخذ به والأكثر اعتناقاً له كالتشريع البريطاني، حيث ظهر لديها ما يعرف بقاعدة الإدانة دون أدنى شك، وهي قاعدة تعني أن القاضي يستطيع أن يُكوِّن عقيدته استناداً إلى أي دليل، حتى وإن لم يكن من الأدلة التي ينص عليها المشرع، متى ما كان ذلك الدليل قاطعاً في دلالته.

(33) يمكن الرجوع إلى ما سبق ذكره حول أنظمة أدلة الإثبات الجنائي في دراستنا هذه.

الفرع الثاني
مشروعية الدليل الإلكتروني في نظام الإثبات الحر

يسود نظام الإثبات الحر في الدول ذات الصياغة اللاتينية، ويتمتع القاضي في ظل هذه الأنظمة بحرية في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بقائمة معينة من الأدلة عند تكوين عقيدته، فله أن يبني ذلك استناداً لأي دليل وإن لم يكن منصوصاً عليه من المشرع، بل إن الأدلة تتساوى في قيمتها الإثباتية في نظر المشرع، فالقاضي هو الذي يختار من الأدلة المعروضة عليه في الدعوى للوصول إلى الحقيقة، وبالتالي يتمتع بحرية مطلقة في قبول الدليل، ورغم توافر شروط لصحة الدليل إلا أن للقاضي رده بحجة عدم الاقتناع به[34]. إن الأساس الذي يقوم عليه نظام الإثبات الحر هو اقتناع القاضي بالأدلة المعروضة عليه، ويقصد بذلك ما يبذله القاضي من جهد عقلي أثناء نظر الدعوى انتهاء إلى الوصول إلى الحقيقة بالحكم الذي يصدره، وهو يتم بالبحث والتحري عن الدليل الذي يوصل للحقيقة المنشودة. فاقتناع القاضي هو البديل لنظام الأدلة القانونية وهو تقدير مسبب لعناصر الإثبات في الدعوى، وبالتالي يكون اقتناع القاضي فيما يرى أن للدولة حق معاقبة المتهم جزاء فعله، أو ليس لها الحق في ذلك لعدم ثبوت التهمة عليه أو وجود شك فيما ارتكبه من فعل، حيث إن الشك يفسر لمصلحة المتهم.

إلا أن حرية الاختيار والتقدير للقاضي وفق قناعته لا تعني أنها مطلقة، فليس له أن يدخل تخميناته وتصوراته الشخصية ضمن أدلة الإثبات التي يبني عليها حكمه، أو يحلها محل الأدلة المقدمة، بل عليه أن يعتمد على الأدلة المقدمة وأن يبعد تصوراته الشخصية، ويستخدم العقل والمنطق في ذلك، حتى يقوداه إلى الدليل الذي اعتمد عليه في النتيجة والحقيقة التي يبتغيها[35]. وعلى مستوى الدليل الإلكتروني فإن مشكلة مشروعيته لا تثور في ظل نظام الإثبات الحر، فللقاضي الأخذ بأي دليل ومنها الدليل الإلكتروني، فالأصل مشروعية وجود الدليل الإلكتروني ويبقى مدى اقتناع القاضي بالدليل المعروض عليه سواء بقبوله أو رده. إن الحرية التي يتمتع بها القاضي الجنائي تعود لصعوبة الحصول على الأدلة في المواد الجنائية، فالوصول إلى الحقيقة من الدليل المقدم يتم بمعرفة القاضي ومدى قدرته على الوصول إليها، لذا فهو يقوم بدور إيجابي في الدعوى الجنائية، ونظراً لما يتمتع به الدليل الإلكتروني من طبيعة خاصة وصعوبة استخراجه من الوسائل الإلكترونية، فإن قبوله في الإثبات قد يثير العديد من المشكلات

(34) يمكن الرجوع إلى ما سبق ذكره حول أنظمة أدلة الإثبات الجنائي في دراستنا هذه.
(35) د. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، مكتبة دار الثقافة، عمان – الأردن، 1999، ص 258.

أهمها التلاعب في الدليل، وتغيير الحقيقة التي يجب أن تعبر عنها، فالمشكلة تتمثل في ضمان مصداقية هذه الأدلة وليس إمكانية اعتبارها من طرق الإثبات[36].

الفرع الثالث

مشروعية الدليل الإلكتروني في التشريع العماني

باستقراء نصوص القانون العماني حول الإثبات الجنائي يتضح بأنه يأخذ بنظام الإثبات الحر، حيث إن الأدلة الجزائية غير محددة أو معينة قانوناً، وهو الأمر الذي يترك المجال للقاضي الجزائي لقبول ما يراه مناسباً من الأدلة وفق ما تمليه عليه قناعته وضميره تجاه الأدلة المعروضة في الدعوى، وهو ما يؤكده قانون الإجراءات الجزائية العماني وتحديداً المادة (2015) منه، حيث تنص على أنه: «يحكم القاضي في الدعوى حسب القناعة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح على الخصوم أمامه في الجلسة أو على معلوماته الشخصية». فعند إحالة ملف الدعوى من قبل الادعاء العام وما يتضمنه من أدلة إثبات تجاه المتهم، فإن تلك الأدلة لا تلزم القاضي بأن يستند إليها في حكمه، وإنما يكون على القاضي أن يطرح تلك الأدلة أمام الخصوم للاستماع إلى أقوالهم ودفاعهم ومناقشتهم حول تلك الأدلة من أجل أن يُكوِّن قناعته تجاهها ويتثبت من صحتها وصلاحيتها لتكون دليل إثبات، ومن ثم يبني حكمه وفق ما وصل إليه من قناعة وعقيدة».

أما على مستوى الدليل الإلكتروني ومشروعيته لدى المشرع العماني، حيث إن الجريمة الإلكترونية بشكل عام قد تم تجريمها والنص عليها لأول مرة باسم جرائم الحاسب الآلي في عام 2001، وذلك على ضوء تعديل قانون الجزاء العماني بموجب المرسوم السلطاني رقم 72/2001 بإضافة فصل خاص لهذه الجرائم، ومن ثم تتابعت التعديلات والإضافات التشريعية حول هذه الجريمة إلى أن صدر قانون خاص بالجريمة الإلكترونية في عام 2011 بالمرسوم السلطاني رقم 12/2011، وهو قانون مكافحة جرائم تقنية المعلومات، وكذلك صدور قانون الجزاء الجديد بالمرسوم السلطاني رقم 7/2018، إلا أن النصوص الإجرائية لهذه الجريمة لم يرد عليها تعديل أو إضافة نصوص خاصة بها، وعليه يبقى القول إن نظام الإثبات الحر هو السائد على هذه الجرائم كذلك، ما يعني مشروعية الدليل الإلكتروني في ظل نظام الإثبات الحر، والذي يمكن من خلاله للقاضي أن يأخذ بأي دليل ومن ضمنه الدليل الإلكتروني، فهذا هو الأصل في هذا النظام، ويبقى الأمر موقوفاً على مدى اقتناع القاضي بالدليل المعروض عليه في الدعوى سواء بقبوله أو رده. ومع الإقرار بحرية القاضي الجزائي في الإثبات وفقاً لهذا النظام، إلا أنه يجب أن يمارس تلك الحرية

(36) أمير فرج يوسف، مرجع سابق، ص 351–352.

وفق منطق سليم وتفكير صحيح، ويتضح ذلك التطبيق في الحكم الذي يصدره إذا ما كان متفقاً مع الإجراءات المتبعة، والأسباب التي اعتمد عليها، ومضمون ما تم الفصل فيه، للوصول إلى ذلك الحكم في الدعوى، أما إذا كانت تلك الإجراءات والأسباب والمضمون متناقضة مع الحكم، فإنه سيكون عرضة للنقض من المحكمة العليا.

لذا فقد أوجد المشرع بعض الاستثناءات على تلك الحرية التي منحها للقاضي، لضمان حسن سير العدالة، وتتمثل تلك الاستثناءات في وجوب أن يستمد القاضي اقتناعه من أدلة صحيحة لها قوتها في الإثبات، وأن تكون تلك الأدلة قد طرحت على بساط البحث وأتيحت للمناقشة أثناء المحاكمة، وأن يلتزم القاضي بطرق الإثبات الخاصة في المسائل غير الجزائية، وبتسبيب حكمه، وهي ما تعتبر قيوداً على حرية القاضي الجزائي في تكوين قناعته[37].

(37) د. مزهر جعفر عبيد، شرح قانون الإجراءات الجزائية العماني، الجزء الأول، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2008، ص 209–211.

المبحث الثاني
إجراءات جمع الدليل الإلكتروني

يُعد الإثبات عموماً من أهم وأدق المسائل التي تواجه العدالة القضائية عند الفصل في الحقوق المتنازع عليها والمعروضة أمامها، حيث إن قواعد ووسائل الإثبات تهدف إلى كشف الحقيقة والتي تتجسد في النهاية في الحكم الذي يصدره القضاء، ولا يكون ذلك إلا بتوفر دليل يؤكد تلك الحقيقة سواء أكانت بإدانة المتهم أم ببراءته، فالدليل هو ما يؤدي إلى إظهار الحقيقة. ومن أجل تحقق وجود الدليل اللازم لإثبات الدعوى، فإنه لابد من جمع عناصر التحقيق والدعوى وتقديمها إلى سلطة التحقيق الابتدائي، لتقوم بدورها في التحقق من الأدلة وتقديمها إلى المحكمة إذا ما تحقق توفر الدليل لإثبات التهمة المنسوبة للفاعل، لتمارس بعدها المحكمة دورها في الدعوى بإدانة المتهم أو الحكم ببراءته وفق سلطتها التقديرية للأدلة المعروضة عليها بالدعوى.

وعلى مستوى الجريمة الإلكترونية، فإن التطور المطرد في أنواع هذه الجرائم وأسلوب ارتكابها والوسائل المستخدمة في تنفيذها، تجعل من القائمين على مكافحتها في سباق مع الزمن من أجل مواكبة ذلك التطور، كما تدعو السلطات القضائية إلى مراجعة كيفية التعامل مع هذه المستجدات، حيث إن اتباع الإجراءات التقليدية لا تجدي نفعاً لمواجهة هذه الجرائم في كثير من الأحيان، لما تثيره من إشكاليات نتيجة طبيعتها غير المادية وما تنتجه من أدلة غير ملموسة.

وعليه سنتناول موضوع إجراءات جمع الدليل الإلكتروني من خلال التطرق إلى الإجراءات التقليدية لجمع الدليل الإلكتروني (المطلب الأول)، ثم إلى الإجراءات الحديثة لجمع الدليل الإلكتروني (المطلب الثاني).

المطلب الأول
الإجراءات التقليدية لجمع الدليل الإلكتروني

غالباً ما يترك الجاني آثاراً مادية في مكان الجريمة عند ارتكابه لجريمته، فمهما حاول محو كل الآثار الناتجة عن الجريمة والتخلص منها، إلا أنه وفي النهاية لابد وأن يترك أثراً نتيجة فعله، وذلك يعود حسبما يرى العلماء إلى الحالة النفسية والانفعالات التي تصاحب الجاني أثناء ارتكاب الجريمة[38]. وقد نظمت التشريعات كيفية الحصول على

(38) د. إبراهيم صادق الجندي، ود. حسين حسن الحصيني، تطبيقات البصمة الوراثية في التحقيق والطب الشرعي، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002م، ص 9.

الأدلة باتخاذ إجراءات تتبع وصولاً للغاية منها وهي إثبات الجريمة المرتكبة ومعرفة فاعلها، وتستخدم هذه الإجراءات بصفة عامة لجمع الأدلة في مختلف الجرائم، فتشمل الجرائم التقليدية والجرائم المستحدثة منها، إلا أن دور تلك الإجراءات يختلف في كل منها، ففي الجرائم التقليدية يتعاظم هذا الدور فيما يتراجع في الجرائم المستحدثة([39]).

ورغم التقدم العلمي الذي أدى إلى استحداث وسائل علمية حديثة في نظام الإثبات الجنائي لتجنب تضليل المتهم للعدالة وكشف ما يقوم به من محو وإتلاف لآثار الجريمة من أجل إثبات براءته منها بشتى الطرق، إلا أن الدليل المادي يبقى ذا دور رئيسي في كشف الجريمة ومعرفة فاعلها، فتغير أبعاد الجريمة وتميزها بسمات خاصة وأنماط جديدة، يقتضي ضرورة أن يتغير تبعاً لذلك أسلوب اكتشافها وطريقة إثباتها. وعليه يبقى للإجراءات التقليدية لجمع الأدلة الجنائية دور مهم – مهما كان في إثبات الجريمة– بالنسبة لجمع الدليل الإلكتروني، فتغير طريقة المعاينة والتفتيش لا يعني أنها ليست من الإجراءات التقليدية لجمع الدليل الجنائي، واتباع الإجراءات التي حددها المشرع يجعل من الدليل المستخرج والمعروض أمام القضاء مشروعاً ويساعد على إثبات الجريمة والوصول إلى الحقيقة.

وبناء على ذلك سوف نعرض بالدراسة لإجراءات جمع الأدلة الجنائية، بدءًا من المعاينة (الفرع الأول)، ومروراً بالتفتيش (الفرع الثاني)، والخبرة (الفرع الثالث)، وانتهاء بالشهادة (الفرع الرابع).

الفرع الأول

المعاينة

عُرِّفت المعاينة من جانب الفقه بعدة تعريفات، من بينها أنها: «رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة»([40])، ومن بينها كذلك أنها: «إثبات الحالة التي يكون عليها مسرح الجريمة عند انتقال المحقق إليه، وإثبات ما به من آثار وحالة الأشخاص المتواجدين به، والتحفظ على كل ما من شأنه أن يغير في كشف الحقيقة»([41]).

(39) عائشة بن قارة مصطفى، مرجع سابق، ص 68.

(40) د. محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، 2002، ص 233.

(41) د. نجاتي سيد أحمد سند، مبادئ الإجراءات الجنائية في التشريع المصري، الجزء الأول، كلية الحقوق، جامعة الزقازيق، القاهرة، 2008، ص 530.

أولاً- أحكام عامة في المعاينة الجنائية:

تكتسي المعاينة أهمية معتبرة في التيسير على سلطات التحقيق في الكشف والمحافظة على العناصر المادية المتعلقة بالجريمة والتي تفيد في التحقيق، ومع انعدام جدوى العناصر المادية في التحقيق فإنه لا يكون هناك ثمة فائدة من إجراء المعاينة، فبعض الجرائم لا تحتاج أو ليس بها مجال لإجراء المعاينة كجريمة التزوير المعنوية وجريمتي القذف والسب اللتين تقعان بالقول في غير العلانية[42].

ثانياً- المعاينة في الجريمة الإلكترونية:

تتخذ المعاينة في الجرائم الإلكترونية عدة أشكال، وذلك حسب نوعية الجريمة المرتكبة، ففي جريمة الاعتداء على الملكية الفكرية يتم تنزيل نسخة من المصنف الفكري المعتدى عليه أو التحفظ على نسخة منه بطباعتها في صورة ورقية أو استخراجها في قرص صلب، وهناك طرق عامة تتوافق مع الطبيعة التقنية، مثل تصوير شاشة الجهاز الإلكتروني عن طريقة آلة تصوير تقليدية أو عن طريق استخدام برمجة الجهاز المتخصصة في أخذ صورة لما يظهر على الشاشة، أو عن طريق حفظ الموقع باستخدام خاصية الحفظ المتوفرة في نظام تشغيل الجهاز[43].

فعند العلم بوقوع الجريمة، فإن أول خطوة يقوم بها مأمور الضبط القضائي هي الانتقال إلى مسرح الجريمة، فهو محل آثار الجريمة والأدلة المادية لها، وفي الجريمة الإلكترونية ينبغي التفرقة بين مسرحين:

- **مسرح تقليدي:** وهو ما يقع خارج بيئة الحاسب الآلي والإنترنت، ويتكون من المكونات المادية المحسوسة في المكان الذي وقعت فيه الجريمة، وهو كمسرح أية جريمة تقليدية، يترك فيها الجاني عدة آثار، كالبصمات أو متعلقاته الشخصية أو وسائط تخزينية رقمية، ويتعامل أعضاء فريق التحقيق أو المعاينة كل حسب تخصصه[44].

- **مسرح افتراضي (إلكتروني):** وهو ما يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد أو تنتقل داخل الحاسب الآلي وشبكة الإنترنت، وفي ذاكرة الأقراص الصلبة الموجودة بداخلها، والتعامل مع الأدلة الموجودة في هذا المسرح لابد أن تتم على أيدي مختصين وذوي خبرة في التعامل مع الأدلة الإلكترونية[45].

(42) د. محمد زكي أبو عامر، مرجع سابق، ص 212.
(43) د. أشرف عبد القادر قنديل، مرجع سابق، ص 137-138.
(44) عائشة بن قارة مصطفى، مرجع سابق، ص 84.
(45) د. حازم محمد حنفي، مرجع سابق، ص 55-56.

إن المعاينة في مسرح الجريمة الإلكترونية تظهر عدة صعوبات في مجال كشف الجريمة وضبط الأشياء التي تفيد في وقوعها ومعرفة فاعلها، ويمكن تلخيص تلك الصعوبات وفق التالي:

1. قلة الآثار المادية التي تترتب عن الجرائم الإلكترونية.
2. تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً ما بين وقوع الجريمة والكشف عنها، وهو ما يتيح الفرصة للعبث وإتلاف وتغيير الآثار المادية، وهو ما يدخل الشك في الأدلة المستمدة من المعاينة.
3. إمكانية تلاعب الجاني في البيانات والمعلومات عن بعد أو محوها أو إتلافها عن طريق التدخل من خلال وحدة طرفية خارجة، لذا ينبغي على المشرع أن يضع جزاءات جنائية على من يقوم بإجراء أي تغيير أو تعديل في المعلومات والبيانات المخزنة والمتوفرة في الجهاز الإلكتروني قبل قيام مأموري الضبط القضائي بإجراء المعاينة.
4. تبخر الأدلة الإلكترونية التي يمكن محوها أو تعديلها أو تغييرها في ثوانٍ معدودة، لذا أجازت بعض التشريعات لأعضاء النيابة العامة تعجيل إجراء المعاينة خشية ضياع الأدلة، من خلال إرسال رسالة إلى مزود الخدمة بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذ هذا الإجراء أو غيره[46].

ونتيجة الاختلاف في مسرح الجريمة الإلكترونية عن غيره في الجرائم التقليدية الأخرى، لأن هذا المسرح يتميز بوجود أدلة ذات طبيعة غير مرئية، تقتضي التعامل معه بحرص وبشكل خاص، وذلك من خلال اتباع بعض القواعد الفنية والإرشادات قبل الانتقال إلى مسرح الجريمة الإلكترونية، ومن أهمها ما يلي:

1. الإعداد الجيد قبل المعاينة لعدم تسرب الأدلة أو إتلافها.
2. إعداد فريق المعاينة من المختصين بتقنية المعلومات وشبكات الإنترنت.
3. إعداد خريطة للموقع الذي تتم المعاينة فيه وتحديد معلومات مسبقة عنه.
4. الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل.
5. تأمين تيار كهربائي احتياطي تجنباً للانقطاع المفاجئ أثناء الفحص وإتلاف مكونات

(46) رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، 2013م، ص 125–128.

الجهاز أو تلف الدليل[47].

ويرى جانب من الفقه ضرورة اتباع بعض القواعد الفنية والإرشادات كذلك عند معاينة مسرح الجريمة الإلكترونية، وتتمثل هذه الإجراءات فيما يلي:

1. تصوير الحاسب الآلي أو الجهاز الإلكتروني الذي ترتكب من خلاله الجريمة، وما قد يتصل به من أجهزة طرفية وملحقاتها ومحتوياته وأوضاع المكان الذي يتواجد به بصفة عامة كغرفة المتهم، مع الأخذ في الاعتبار تصوير أجزائه الخلفية وملحقاته الأخرى، مع مراعاة تسجيل التاريخ والمكان الذي تم التقاط الصور فيهما[48].
2. العناية البالغة بملاحظة طريقة إعداد نظام الحاسب الآلي والآثار الإلكترونية التي تترتب عند الدخول في النظام أو على الموقع بشبكة المعلومات، والسجلات الإلكترونية التي تزود بها شبكة المعلومات لمعرفة موقع الاتصال ونوع الجهاز المستخدم للدخول في النظام أو الموقع أو الدخول معه في حوار[49].
3. إثبات الحالة التي تكون عليها توصيلات وكابلات الحاسب الآلي، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليلها عند عرض الموضوع على المحكمة[50].
4. عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي، حتى لا تؤدي إلى إتلاف البيانات المخزنة نتيجة تداخل المجالات المغناطيسية مع بعضها البعض[51].
5. حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة، والشرائط والأقراص الممغنطة غير السليمة أو المتلفة وفحصها، ورفع البصمات التي قد تكون لها علاقة بالجريمة المرتكبة[52].
6. حفظ المستندات الخاصة بالإدخال، وكذلك مخرجات الحاسب الآلي الورقية التي قد تكون ذات صلة بالجريمة، ورفع ما قد يكون عليها من بصمات أو آثار مادية[53].

(47) د. محمد الأمين البشري، مرجع سابق، ص 357.
(48) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 213.
(49) عائشة بن قارة مصطفى، مرجع سابق، ص 86.
(50) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 213.
(51) د. حازم محمد حنفي، مرجع سابق، ص 59.
(52) د. أحمد يوسف الطحطاوي، مرجع سابق، ص 135.
(53) د. أشرف عبد القادر قنديل، مرجع سابق، ص 139.

7. ربط الأقراص المغنطة التي ربما قد تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها، مما يتيح للمحققين قراءة بياناتها من دون تغييرها[54].

8. يجب قصر عملية المعاينة على مأموري الضبط القضائي، سواء أكانوا من الباحثين أم المحققين ممن تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال تقنية المعلومات واسترجاع المعلومات[55].

ويتم توثيق مسرح الجريمة بالكامل من خلال وصف محتوياته بشكل جيد، وتوثيق كل دليل على حدة بما فيها الأدلة الإلكترونية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها وما قام برفعه وتحريزه وكيف ومتى تم ذلك، وهناك البعض ممن يرى بأن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل المعاينة، ولعل أبرز الأماكن التي يحتمل تواجد الأدلة الجنائية فيها والمتعلقة بالجرائم الإلكترونية فيها، ما يلي:

- الورق: ويتم الحصول عليه من خلال البحث في سلة المهملات عن أوراق مطبوعة ذات علاقة بالحاسب الآلي محل المعاينة، ويعتبر من الأدلة التي ينبغي الاهتمام بها عند البحث عن الحقيقة.

- المكونات المادية: كأجهزة الحاسب الآلي بأنواعها المختلفة، والأقراص الصلبة الخارجية، والملحقات المرتبطة بأجهزة الحواسيب ذات الصلة بالجريمة، كالطابعات والماسحات الضوئية والكاميرات الرقمية وغيرها من الأجهزة المادية الأخرى.

- البرامج: إذا كان الدليل الإلكتروني نشأ نتيجة برنامج خاص أو أنه ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج يعد أمراً في غاية الأهمية عند فحص الدليل.

- وسائط التخزين المتحركة: كالأقراص المدمجة والأقراص المرنة والشرائط المغناطيسية، وأي من أشكال أشرطة التخزين الخارجية المختلفة مثل (فلاش ميموري).

- دليل الاستخدام الخاص بالمكونات المادية والتقنية للجهاز الإلكتروني، والذي يفيد في معرفة التفاصيل الدقيقة لكيفية عمله.

- كلمات السر أو أرقام الهاتف، والتي قد تكون مكتوبة على أوراق ملصقة بالحاسب الآلي أو بقربها، وقد تكون خاصة بحسابات الاتصال بشبكة الإنترنت أو بعض

(54) عائشة بن قارة مصطفى، مرجع سابق، ص 87.
(55) عبد الفتاح بيومي حجازي، مرجع سابق، ص 213–214.

خدمات الإنترنت المختلفة، وقد تكون خاصة بفك شفرات بعض البيانات التي تتضمن أدلة مهمة في الدعوى[56].

وبناء على ما سبق ذكره، ولكي تؤتي المعاينة ثمارها عند القيام بها من قبل مأموري الضبط القضائي، فإنه لابد من تأهيلهم وتعليمهم علوم الحاسب الآلي وتقنية المعلومات، وكيفية التعامل مع الأجهزة الإلكترونية المختلفة، والتي أصبح لها الدور الهام في مختلف مجالات الحياة ومنها المجال الأمني للكشف عن الجرائم وضبطها وتحليلها والحصول على الأدلة منها. ويرى جانب من الفقه الجنائي أن مأمور الضبط القضائي عند قيامه بالمعاينة من أجل الاستدلالات وجمع التحريات، يلزمه القيام بالآتي:

1. تحديد نوع نظام المعالجة الآلي للمعلومات هل هو متصل بالشبكة أم لا، وذلك لأن عملية البحث والتحري تكون صعبة في حالة وجود ملحقات طرفية أو شبكات أخرى متصلة بالجهاز الإلكتروني محل المعاينة.
2. وضع خطة شاملة للمنشأة ككل وإعداد كشف بأسماء المسؤولين عنها ودور كل منهم، فهناك من يقوم بالمعالجة الآلية للمعلومات، وهناك من يقوم بإدارة الدراسات والتطوير وإدارة وتشغيل نظم المعلومات.
3. إذا كان الأمر يتعلق بشبكة، فيجب إحصاء الطرفيات وتحديد طبيعة الروابط الموجودة بينها لمعرفة الطريقة التي تتم بها نقل المعلومات من موقع لآخر.
4. مراعاة أن الدليل في مجال المعالجة الآلية للبيانات يمكن أن يختفي خلال وقت قصير جداً، إذ يمكن للجاني أن يتدخل من خلال وحدة طرفية لإتلاف المعلومات المخزنة في الجهاز، عن طريق ساعة في معصم اليد أو هاتفه المحمول، وغيرها من وسائل تقنية المعلومات.
5. ضرورة فصل التيار الكهربائي من مكان خارج الموقع قبل دخوله، وهذا الإجراء يمنع المستخدم من التلاعب في المعلومات أو محوها، وإن كان لذلك أثره في فقد المعلومات المخزنة في الذاكرة العشوائية لأجهزة الحاسبات الآلية، وللقضاء على تداخل المجالات المغناطيسية مع بعضها على نحو يؤدي إلى إتلاف البيانات.
6. فصل خطوط الهاتف تحسباً لاستعمال "المودم" في جهاز المعالجة الآلية للمعلومات، والمراد ضبطه.
7. التأكد من عدم استخدام خاصية تحويل المكالمات والتأكد من أن رقم الهاتف يخص جهاز الحاسب الآلي محل المعاينة.

(56) د. حازم محمد حنفي، مرجع سابق، ص 59–60.

8. يجب إبعاد جميع الموظفين عن أجهزة الحاسبات الآلية، مع محاول الحصول منهم على معلومات حول كلمات السر أو شفرات الدخول والأماكن الأخرى التي توجد بها أجهزة الحاسبات الآلية المرتبطة بهم.
9. تصوير الأجهزة محل المعاينة من الأمام والخلف لإثبات أنها كانت تعمل، وللمساعدة في إعادة تركيبها لأغراض التحقيق[57].

الفرع الثاني
التفتيش

التفتيش هو إجراء من إجراءات التحقيق يقوم به موظف مختص طبقاً للإجراءات القانونية في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة، تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم[58]، أو هو إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة، ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه[59]، لذا فهو يعد من أهم إجراءات التحقيق في كشف الحقيقة لأنه غالباً ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم[60].

كما عُرِّف تفتيش أجهزة ونظم الحاسوب والإنترنت بأنه: «البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه، أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت»[61].

أولاً- أحكام عامة في التفتيش:

الأصل أن التفتيش هو إجراء من إجراءات التحقيق تختص به سلطة التحقيق بصفة أصلية، إلا أنه استثناء يمكن لمأموري الضبط القضائي أن يقوموا به في حالات حددها قانون الإجراءات الجزائية[62]، فهو إجراء بطبيعته يمس حق المتهم في سرية حياته

(57) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 219-220.
(58) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 244.
(59) د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986م، ص 278-279.
(60) عائشة بن قارة مصطفى، مرجع سابق، ص 87.
(61) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت: دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004م، ص 12-13.
(62) تنص المادة 36 من قانون الإجراءات الجزائية على أنه: «إذا رأى أحد مأموري الضبط القضائي عند=

الخاصة، ولا يجوز أن يترتب على حق الدولة في العقاب المساس بسرية الحياة الخاص للأفراد إلا وفقاً للإجراءات القانونية الخاصة بذلك وفي أضيق الحدود. وينقسم التفتيش وفقاً للقواعد العامة من حيث محله إلى قسمين: الأول ينصب على المساكن، وهو إجراء من إجراءات التحقيق يقوم به عضو سلطة التحقيق أو من يندبه من مأموري الضبطية القضائية بالبحث في مسكن شخص معين على أشياء تتعلق بجناية أو جنحة قامت قرائن قوية على حيازته لها، والثاني تفتيش يقع على الأشخاص، وهو إجراء من إجراءات التحقيق كذلك يستهدف ضبط ما يحوزه الشخص الخاضع للتفتيش من أشياء تفيد في كشف الحقيقة[63].

والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية البحث في مستودع السر عن دليل يتعلق بالجريمة الواقعة، ونتيجة لذلك فإن تفتيش أجهزة ووسائل تقنية المعلومات الحديثة من أخطر المراحل عند اتخاذ الإجراءات الجزائية في الجريمة الإلكترونية وغيرها من الجرائم التي تتضمن دليلاً إلكترونياً؛ لاعتبار أن محل التفتيش وهو جهاز الحاسب الآلي أو شبكات أو وسائل تقنية المعلومات، محل جدل فقهي واسع ومتزايد وخاصة فيما يخص تفتيش المكونات المعنوية لتلك الأجهزة والوسائل، فهي لا وجود لماديتها وإنما بيانات ومعلومات رقمية[64]

فما مدى قابلية هذه المكونات للتفتيش؟ وما هي الضوابط التي ينبغي مراعاتها عند إجراء التفتيش عليها؟ وهو ما نتناوله على النحو التالي:

ثانياً- التفتيش في الجريمة الإلكترونية:

إن التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة عن التفتيش التقليدي للمساكن والأشخاص، إلا أنه يخضع في إجراءاته لنصوص قانون الإجراءات الجزائية التي تتطلب وقوع جريمة واتهام شخص أو أشخاص معينين بارتكابها، بالإضافة لوجود قرائن ودلائل على ما يفيد في كشف الحقيقة في الجهاز الإلكتروني لدى المتهم

= قيامه بجمع الاستدلالات ضرورة إجراء تفتيش شخص أو مسكن معين، تعين عليه أن يحصل على إذن بذلك من الادعاء العام». كما تنص المادة 46 من ذات القانون على أنه: «لمن يقوم بتنفيذ القبض من مأموري الضبط القضائي أن يفتش المقبوض عليه لتجريده من أية أسلحة أو أشياء قد يستعملها في المقاومة أو في إيذاء نفسه أو غيره...». وتنص كذلك المادة 77 من القانون ذاته على أنه: «لمأموري الضبط القضائي تفتيش المتهم في الأحوال التي يجوز فيها قانوناً القبض عليه، كما يجوز تفتيش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة، ويشمل التفتيش جسمه وملابسه وأمتعته».

(63) د. حازم محمد حنفي، مرجع سابق، ص 40.

(64) عائشة بن قارة مصطفى، مرجع سابق، ص 88.

أو غيره، ومع توفر تلك الشروط فإنه يحق لسلطة التحقيق تفتيش الجهاز وملحقاته ومكوناته المادية والمعنوية، للوصول للأدلة محل الجريمة، وما يحتمل أن يكون قد استعمل لارتكابها أو نتج عنها، وكل ما من شأنه أن يفيد في كشف الحقيقة[65].

وتتكون تلك الأجهزة وجهاز الحاسب الآلي من مكونات مادية ومكونات أخرى معنوية، وترتبط هذه الأجهزة مع بعضها البعض بشبكات اتصال ونهايات طرفية محلية أو دولية، ويثور التساؤل في هذا المجال حول قابلية هذه المكونات للتفتيش وطريقة تفتيشها، وسنتناول الإجابة عن ذلك لكل مكون على حدة، وفق التفصيل التالي:

أ. تفتيش مكونات الجهاز الإلكتروني المادية:

إن تفتيش المكونات المادية للجهاز الإلكتروني بحثاً عن الأدلة أو أي شيء يتصل بالجريمة الإلكترونية يفيد في كشف الحقيقة عنها أو مرتكبها، يخضع للإجراءات القانونية والقواعد العامة لإجراء التفتيش، كالإجراءات التي يقام بها عند التفتيش في الجريمة التقليدية، لأن الغاية هنا هي تفتيش أجزاء ومكونات مادية مثلما يتم إجراؤه عند تفتيش مسكن أو شخص في جريمة سرقة أو قتل. ويعني ذلك أن حكم التفتيش للمكونات المادية للجهاز الإلكتروني يعتمد في ذلك على طبيعة المكان الذي تتواجد فيه تلك المكونات المادية، سواء أكان مكاناً عاماً أم مكاناً خاصاً، حيث إن لصفة المكان أهمية قصوى في تحديد إجراءات تفتيشه، فإذا كان مكان تواجد المكونات المادية مع الشخص في مكان عام وهو حائز لها، سواء أكان المكان عاماً بطبيعته كالطرق العامة والميادين، أم كان مكاناً عاماً بالتخصيص كالمقاهي والحافلات العامة، فإن التفتيش هنا يخضع للحالات التي يجوز فيها تفتيش الأشخاص بذات الضمانات والقيود المنصوص عليها في هذا الشأن[66].

أما إذا كان مكان تواجد المكونات المادية للجهاز الإلكتروني في مكان خاص كمسكن المتهم أو أحد ملحقاته، كان لذلك المكان حكمه كذلك، أي أنه لا يجوز تفتيش المكونات المادية إلا في الحالات التي يجوز فيها تفتيش المساكن، وبذات الضمانات والإجراءات المقررة قانوناً في هذا المجال، مع مراعاة التمييز إذا ما كانت المكونات المادية للجهاز المراد تفتيشها منعزلة عن غيرها من الأجهزة، أو متصلة بأجهزة أو حواسيب أخرى في مكان أو مسكن آخر لغير المتهم وبالتالي خضوعها لإجراءات تفتيش مسكن غير المتهم[67].

وتفتيش المكونات المادية للجهاز الإلكتروني لا يعني البحث عن البصمات والآثار المادية

(65) د. حازم محمد حنفي، مرجع سابق، ص 41–42.

(66) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص 237.

(67) د. علي حسن محمد الطوالبة، مرجع سابق، ص 82.

الأخرى مثلما هو حاصل في الجرائم الجنائية التقليدية الأخرى، وإنما يكون بالبحث عن الأجهزة والملحقات المرتبطة بها، كالبحث عن طابعة أو جهاز ماسح ضوئي لقيامه بجريمة تزوير، أو البحث عن جهاز الوصول للإنترنت (مودم) لقيامه بجريمة اختراق لمواقع إلكترونية.

ب. تفتيش مكونات الجهاز الإلكتروني المعنوية:

تنقسم المكونات المعنوية للأجهزة الإلكترونية بشكل عام وللحاسب الآلي بشكل خاص، إلى نوعين رئيسين: الأول منهما يختص بتشغيل الجهاز ذاته وتحسين أدائه ببرامج تكون ثابتة في الجهاز تعمل على ذلك مثل عرض الشاشة الرئيسية للجهاز ونظام تشغيله، والنوع الثاني منهما يساعد المستخدم على القيام بأداء أعماله وتسهيل استخدامه للجهاز مثل البرامج المكتبية، فعند استخدام هذه البرامج وحفظها يتم إضافة ملف ومحتوى جديدين بالجهاز غير موجودين مسبقاً، وهو نتيجة استخدام المستخدم للجهاز[68]. وهناك نوع آخر من المحتويات المعنوية وهي المحتويات المتعلقة بشبكة المعلومات والإنترنت، وهي قد تكون عالمية أو محلية، وهذا النوع من المحتوى يحتاج لخبرة عند تفتيشه، ومهارة عالية عند التعامل معه لاستخراج المعلومات والبيانات التي تحتويها، فقد تكون هذه المعلومات والبيانات موجودة على الشبكة ولا تتواجد في الجهاز ذاته المستخدم في الجريمة، لذا تحتاج لأشخاص ذوي خبرة في هذه الشبكات والتقنيات لاستخراجها عند تفتيش المحتوى المعنوي للأجهزة، كما أنها قد تحتاج إلى أذونات والتحقيق مع أصحاب مواقع إلكترونية للحصول على المعلومات التي تفيد في كشف الجريمة[69].

فإذا ما قام أحد المستخدمين لمواقع التواصل الاجتماعي بسب أو قذف أحد الأشخاص الآخرين في ذات الموقع، فإنه لمعرفة المتهم في هذه الجريمة لابد أن تقوم سلطات التحري والتحقيق بالتواصل مع المختصين بذلك الموقع للحصول على العنوان الإلكتروني الخاص بالمتهم الذي قام بالسب أو القذف، وهي من الإجراءات الحديثة التي سيتم بيانها تفصيلاً عند معرض الحديث عن الإجراءات الحديثة لجمع الدليل الإلكتروني.

أما المشرع العماني فقد نص في المادة (33) من قانون الإجراءات الجزائية على قيام مأمور الضبط القضائي بضبط كل ما يتعلق بالجريمة ويفيد التحقيق، كما نص في المادة (88) من ذات القانون على أنه لمأمور الضبط القضائي أن يضبط الأشياء التي يحتمل

(68) د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية: دراسة تحليلية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011، ص 217–218.

(69) د. سامي جلال فقي حسين، مرجع سابق، ص 239.

أن تكون قد استعملت في ارتكاب الجريمة أو نتجت عن ارتكابها أو يحتمل أن تكون قد وقعت عليها الجريمة وكل ما يفيد في كشف الحقيقة، وهو ما يعني أن المشرع العماني أخذ كذلك بالاتجاه الذي يرى بأن ضبط الأدلة الإلكترونية يمكن أن يتم من جميع أشكال البيانات التي تتيحها الأجهزة الإلكترونية، ومنها المكونات المعنوية وبالتالي مشروعية تفتيش هذه المكونات وإمكانية ضبطها.

ج - تفتيش شبكات الجهاز الإلكتروني:

ازدادت صعوبات التفتيش وضبط الأدلة التي يتم إجراؤها في الجرائم الإلكترونية بسبب الطبيعة الخاصة لتكنولوجيا المعلومات، حيث إن تلك الأدلة الإلكترونية التي هي عبارة عن بيانات أو معلومات يمكنها أن تتوزع عبر أكثر من شبكة خارج نطاق شبكة الجهاز محل التفتيش، فقد تكون في ذات المبنى الذي يتم تفتيشه ولكنها في أجهزة أخرى، وقد تكون خارج الموقع الذي يتم تفتيشه وتدخل في اختصاص قضائي آخر داخل البلد الواحد أو اختصاص دولة أخرى خارج الدولة محل التفتيش، ويؤدي التدخل في اختصاص تلك الدولة إلى انزعاج من السلطات فيها من التدخل في شؤونها وسيادتها، وهو ما يظهر أهمية تبادل المساعدات القانونية والقضائية في هذا المجال، ولمعرفة كيف يمكن تفتيش هذه الشبكات وفق تلك الصعوبات والتداخلات يمكن التفرقة بين فرضين أساسيين على النحو الآتي:

- **الفرض الأول– اتصال جهاز المتهم بجهاز آخر موجود في مكان آخر داخل الدولة:**

يثور التساؤل في هذه الفرضية حول إمكانية أن يمتد الحق في التفتيش إلى جهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم، إذا تبين أن جهاز المتهم أو النهاية الطرفية في مسكنه متصلة به، ففي هذه الحالة لا تثار المشكلة إذا كان المكانان يخضعان لنفس النظام القانوني والولاية القضائية مثلما هو حاصل في الولايات المتحدة الأمريكية والتي تجيز إجراء التفتيش الصادر لمقر شركة معينة وأن يمتد لفروعها الكائنة في ذات العقار، ومن تطبيقات هذا الرأي كذلك ما نص عليه المشرع البلجيكي في المادة (88) من قانون تحقيق الجنايات البلجيكي والتي تنص على أنه: «إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين هما: أولاً– إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث. ثانياً– إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات.

أما المشرع العماني فلم يُجِزْ القيام بهذا الأمر حيث تنص المادة (36) من قانون الإجراءات الجزائية على أنه: «إذا رأى أحد مأموري الضبط القضائي عند قيامه بجمع الاستدلالات ضرورة إجراء تفتيش شخص أو مسكن معين، تعين عليه أن يحصل على إذن بذلك من الادعاء العام»، وكذلك نصت المادة (80) من ذات القانون على عدم جوازية تفتيش المساكن إلا بإذن كتابي مسبب من الادعاء العام بناء على اتهام موجه إلى شخص يقيم في المسكن المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة ما لم تكن الجريمة متلبساً بها، وعليه يتضح من ذلك أنه يجب الحصول على إذن تفتيش من الولاية القضائية المختصة لمكان تواجد الجهاز الآخر، إلا أن المشرع العماني كذلك يجيز تفتيش الأشخاص دون الحاجة لإذن من غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة ، ويشمل التفتيش جسمه وملابسه وأمتعته، كما يجوز تفتيشه كذلك في حالة تفتيش مسكن المتهم إذا ما قامت قرائن قوية ضد شخص موجود فيه على أنه يخفي معه شيئاً يفيد في كشف الحقيقة، وهو ما ورد في المادتين (77) و(82) تواليا من قانون الإجراءات الجزائية.

وما سار عليه العمل الإجرائي في السلطنة هو إمكانية الدخول لجهاز آخر موجود داخل السلطنة إذا كان ذلك عن طريق الجهاز محل التفتيش، دون الحاجة لاستصدار إذن تفتيش آخر من الولاية القضائية للجهاز المتصل به. وفي هذا الصدد يمكن معرفة حكم تفتيش جهاز آخر مرتبط بالجهاز المأذون بتفتيشه والموجود داخل إقليم الدولة، بقياس هذه الحالة مع الحالة التي يقوم فيها صاحب المسكن المأذون بتفتيشه بإلقاء حقيبة أو لفة من مخدر معين في أحد المساكن المجاورة، وحسمت هذا الجدل محكمة النقض المصرية حيث منعت المأذون له بالتفتيش تعقب ما ألقي في المسكن المجاور بدخوله وتفتيشه[70].

- **الفرض الثاني– اتصال جهاز المتهم بجهاز آخر أو نهاية طرفية موجود في مكان آخر خارج الدولة:**

من الصعوبات التي تواجه سلطات التحقيق في تعقب الأدلة الإلكترونية، قيام مرتكبي الجرائم الإلكترونية بتخزين المعلومات والبيانات في شبكات وأنظمة معلوماتية خارج الدولة باستخدام شبكات الاتصال الدولية بهدف عرقلة إجراءات التحقيق والوصول إليهم، وفي هذه الحالة فإن امتداد إذن التفتيش إلى جهاز خارج الإقليم الجغرافي للدولة التي صدر من قبلها إذن التفتيش لا يمكن أن يتم بسبب

(70) حكم محكمة النقض المصرية رقم 564 لسنة 53 الصادر في 13/6/1983م.

تمسك كل دولة بسيادتها وولايتها القضائية إلا بوجود اتفاقيات ثنائية خاصة أو دولية تجيز ذلك الإجراء، وهو ما يسمى بالتفتيش عبر الحدود أو التفتيش عن بعد[71].

أما عند صعوبة الحصول على المعلومات والبيانات إلا بوجود إذن من موقع معين، كما لو قام شخص بنشر إشاعات تضر بالأمن القومي للدولة على أحد مواقع التواصل الاجتماعي مثل تويتر أو فيسبوك، هنا يكون على سلطات التحقيق عند الرغبة في إثبات الدليل على المستخدم أن تحصل على العنوان الإلكتروني للمستخدم والموجود على الموقع، ومن ثم مضاهاتها مع البيانات المسجلة لدى شركة الاتصال التي استخدمها المستخدم للوصول إلى الموقع، إلا أن المسؤولين عن هذه المواقع حفاظاً منهم على سرية عملائهم وعلى سمعة الموقع واكتساب ثقتهم يطلبون شروطاً تعسفية ومعقدة وإجراءات طويلة من أجل منح المعلومات التي تطلبها سلطات التحقيق، وبالتالي لا يمكن لهذه السلطات إلا الحصول على المعلومات والبيانات المطلوبة عن طريق الاتفاقيات والمعاهدات والتعاون المشترك بين الدول، بالإضافة لتقنين أوضاع وشروط هذه المواقع لأكبر قدر ممكن[72].

أما المشرع العماني فلم يعالج هذا الموضوع ولم يتطرق إليه ضمن نصوص قانون الإجراءات الجزائية، وبالتالي يمكن القول بتطبيق القواعد العامة والتي تعتمد على الاتفاقيات والمعاهدات في هذا الأمر كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبرالوطنية والتي انضمت إليها السلطنة بالمرسوم السلطاني رقم 2005/37، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي صادقت عليها السلطنة بالمرسوم السلطاني رقم 2015/5، والاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي صادقت عليها السلطنة بالمرسوم السلطاني رقم 2015/6، وذلك عند الرغبة بتفتيش الشبكات ووجود اتصال بين جهاز المتهم وجهاز آخر أو نهاية طرفية أخرى خارج الدولة، كما أن الواقع العملي لبعض الجرائم يتيح لأعضاء الادعاء العام ومأموري الضبط القضائي الحصول على المعلومات التي تكون متاحة للجمهور، وكذلك المعلومات والبيانات الموجودة لدى غير المتهم والمتصلة بجهازه مع المتهم، حيث إن الواقع العملي يكشف بعض الحالات التي يتم من خلالها الدخول لأنظمة وملفات متصلة بالشبكة وموجودة خارج الدولة، ويرى الباحث أن مبرر ذلك أن هذه الشبكات والمواقع وسجلاتها التقنية موجودة في الأصل خارج الدولة

(71) نبيلة هبة هروال، مرجع سابق، ص 240.
(72) د. حازم محمد حنفي، مرجع سابق، ص 52.

أي في الدولة التي تملك الموقع أو النظام، وبالتالي فإن الدخول عبر هذه الأنظمة والمواقع من خلال جهاز موجود في الدولة لا يعتبر اعتداء على سيادة دولة أخرى، حيث إنه يمكن للدولة أن تعاقب على الجرائم التي ترتكب على إقليمها أو يقع أي ركن من أركان الجريمة عليه، وباعتبار أن جهاز المتهم موجود داخل الدولة فبالتالي يعتبر من الممكن الدخول من خلاله إلى أنظمة أو أجهزة متصلة بها تقع في مكان آخر خارج الدولة.

ثالثاً- شروط التفتيش في البيئة الإلكترونية:

عند إجراء التفتيش من قبل سلطات التحقيق لابد من اتباع إجراءات وقيود معينة تنص عليها التشريعات ولابد من توفير ضمانات للأشخاص عند إجراء التفتيش سواء كان على المسكن أو الشخص، باعتبارها إجراءات تمس الحرية الشخصية، وكذلك ينطبق الأمر عند إجراء التفتيش في الجريمة الإلكترونية، سواء أكان تفتيشاً على المكونات المادية أم المعنوية للأجهزة الإلكترونية أو شبكات هذه الأجهزة، وتنقسم شروط التفتيش عموماً إلى شروط موضوعية وأخرى شكلية، وسنبين كلاً منها على النحو التالي:

أ. الشروط الشكلية لتفتيش الأجهزة الإلكترونية:

وهي الشروط التي يجب مراعاتها عند إجراء التفتيش على الأجهزة الإلكترونية وشبكاتها صوناً للحريات الفردية من التعسف أو الانحراف في استخدام السلطة، وهي تأخذ الطابع الشكلي، وتتمثل في الشروط الآتية:

1. حضور بعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية:

عند إجراء التفتيش على الأشخاص لم تشترط أغلب التشريعات وجود شهود أو حضور أشخاص معينين عند القيام بهذا الإجراء، أما فيما يتعلق بتفتيش المساكن وما في حكمها فالأمر مختلف، فنصت غالبية التشريعات على وجود شهود عند القيام بالتفتيش[73]، ومنها ما نص عليه المشرع المصري من اشتراط حضور شاهدين عند إجراء التفتيش بمعرفة أحد مأموري الضبط القضائي، كما اشترط أن يكون الشاهدان بقدر الإمكان من أقارب المتهم البالغين أو القاطنين معه بالمسكن أو من الجيران[74]، أما المشرع الجزائري فقد قام بتعديل المادة [45] من قانون الإجراءات

(73) د. علي حسن محمد الطوالبة، مرجع سابق، ص 48.

(74) تنص المادة (51) من قانون الإجراءات الجنائية المصري على أنه: «يحصل التفتيش بحضور المتهم أو من ينيبه عنه كلما أمكن ذلك، وإلا فيجب أن يكون بحضور شاهدين، ويكون هذان الشاهدان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران، ويثبت ذلك في المحضر».

الجزائية حيث استغنى بموجب القانون رقم (6-22) عن شرط حضور أشخاص محددين كما ورد في الفقرة الأولى من المادة المشار إليها في جرائم معينة ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات. ومن جهته، نص المشرع العماني كذلك على وجوب حضور بعض الأشخاص الذين حدد صفاتهم وذلك في قانون الإجراءات الجزائية في المادة (84) والتي تنص على أنه: «يجري التفتيش بحضور المتهم أو من ينيبه عنه كلما أمكن ذلك، وإلا تم بحضور شيخ أو رشيد منطقته أو شاهدين يكونان بقدر الإمكان من أقاربه الراشدين أو من القاطنين معه بالمسكن أو من جيرانه ويثبت ذلك بالمحضر، وإذا حصل التفتيش في مسكن غير المتهم يدعى صاحبه للحضور بنفسه أو من ينيبه عنه إن أمكن».

2. الميقات الزمني لإجراء التفتيش في الجرائم الإلكترونية:

ويقصد بهذا الشرط أن يقوم المختصون بالتفتيش بإجرائه خلال فترة زمنية معينة يحددها المشرع، وذلك من أجل تضييق نطاق المساس بالحرية الشخصية للأفراد وحرمة مساكنهم، ولا يقصد بذلك أن يتم الإجراء في توقيت زمني محدد كتحديد ساعة معينة يجب أن يتم خلالها الانتهاء من إجراء التفتيش وعند انتهائها ينتهي ذلك الإجراء[75]، ومن التشريعات التي أخذت بذلك المشرع الجزائري الذي نص على أن تفتيش المنازل يجب أن يكون بين الساعة الخامسة صباحاً والثامنة مساءً، إلا أنه أورد استثناءات على ذلك مثل حالة طلب صاحب المنزل أو وجهت نداءات استغاثة من المنزل، وكما أن المشرع الجزائري استثنى عدة جرائم من تحديد توقيت زمني لها عند إجراء التفتيش، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك لاعتبار رئيسي يتمثل في أن الدليل الإلكتروني قابل للمحو والتدمير في وقت زمني قصير يصل لثوانٍ معدودة[76].

وهناك تشريعات تركت تحديد أمر الوقت المناسب لإجراء التفتيش للقائمين عليه، وبالتالي فيمكن إجراؤه في أي وقت سواء أكان ليلاً أم نهاراً، ومنها المشرع المصري الذي نص على ذلك في قانون الإجراءات الجنائية المصري بموجب المادة (45) منه. وكذلك المشرع العماني الذي لم ينص على توقيت معين لإجراء التفتيش وترك الأمر لأعضاء الادعاء العام ومأموري الضبط القضائي في تحديد الوقت المناسب للقيام بهذا الإجراء، إلا أنه حدد مدة معينة لإجرائه وهي سبعة أيام من تاريخ صدور إذن

(75) د. سامي جلال فقي حسين، مرجع سابق، ص 163.

(76) تنص الفقرة الأولى من المادة (47) من قانون الإجراءات الجزائية الجزائري على أنه: «لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحاً، ولا بعد الساعة الثامنة مساءً، إلا إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانوناً».

التفتيش، وبالتالي عدم جواز القيام بالتفتيش بعد مضي هذه المدة، وهو ما نصت عليه الفقرة الأخيرة من المادة (80) من قانون الإجراءات الجزائية والتي تنص على أنه: «لا يجوز تنفيذ الإذن بالتفتيش بعد مضي سبعة أيام من تاريخ صدوره ما لم يصدر إذن جديد».

3. محضر التفتيش في الجرائم الإلكترونية:

بما أن التفتيش هو إجراء من إجراءات التحقيق، فينبغي عند القيام به تحرير محضر يوثق فيه ما تم من إجراءات، وما نتج عن إجراء التفتيش من أدلة، وتوقيت ومكان إجرائه، ولم تشترط التشريعات شكلاً خاصاً لمحضر التفتيش، وبالتالي فإنه لا يشترط لصحته شروطاً محددة إلا ما تحدده القواعد العامة عن تحرير المحاضر بشكل عام. وكذلك هو الأمر عند إجراء التفتيش في الجرائم الإلكترونية، فإنه علاوة على ما تم ذكره فينبغي تواجد شخص متخصص في مجال تقنية المعلومات عند تحرير محضر التفتيش، من أجل إطلاع سلطة التحقيق والمحكمة بما تم من إجراءات صحيحة وإحاطتهما بتقنية المعلومات[77].

أ- الشروط الموضوعية لتفتيش الأجهزة الإلكترونية:

وهي الضوابط اللازمة لإجراء تفتيش صحيح، وتكون في الغالب سابقة له، أي أنه لابد من توفرها قبل إجراء عملية التفتيش، وتتمثل هذه الشروط الموضوعية في ثلاثة شروط أساسية هي: السبب، المحل، والسلطة المختصة بالقيام بالتفتيش، وسنبين تفصيل كل شرط على حدة على النحو التالي:

- **سبب التفتيش في البيئة الإلكترونية:**

سبب التفتيش بشكل عام هو السعي للحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[78]، ويتمثل ذلك في وقوع جناية أو جنحة ووجود متهم أو متهمين بارتكاب تلك الجريمة أو الاشتراك فيها، بالإضافة لتوفر قرائن قوية على وجود أشياء تفيد في كشف الحقيقة في مسكن المتهم أو مسكن آخر أو لديه بشخصه أو شخص آخر. وعليه يمكن القول إن سبب التفتيش في الجرائم الإلكترونية يجب أن يكون مستنداً إلى ثلاثة شروط فرعية، الأول هو وقوع جريمة من الجرائم الإلكترونية بالفعل من نوع الجناية أو الجنحة، وذلك يكون وفق الأفعال التي يحددها المشرع في هذا المجال، والثاني هو اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو الاشتراك فيها، وذلك يكون وفق دلائل كافية ومظاهر وأمارات

(77) د. سامي جلال فقي حسين، مرجع سابق، ص 171.
(78) عائشة بن قارة مصطفى، مرجع سابق، ص 99.

قائمة على العقل والمنطق والخبرة الفنية تدل على أن الشخص هو من قام بارتكاب الجريمة، والثالث هو توافر قرائن قوية على وجود معلومات أو بيانات أو معدات مادية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره، وهو ما يعني توافر أسباب كافية لدى سلطة التحقيق بوجود تلك المعلومات أو البيانات أو أي دليل إلكتروني آخر يفيد في كشف الجريمة لدى المتهم أو غيره[79].

- **محل التفتيش:**

يقصد بمحل التفتيش عموماً المستودع الذي يحتفظ فيه الشخص بأشيائه المادية التي تتضمن أسراره، والسر الذي يوفر القانون له الحماية هو المكان الذي يتوافر به حرمة خاصة من الاعتداء عليها، كالمسكن والمكالمات والرسائل الشخصية والشخص نفسه، ومحل التفتيش في الجريمة الإلكترونية هو الجهاز الإلكتروني والشبكات المرتبطة به وما يرتبط بهما من ملحقات مادية وتقنية[80]. وقد تطرقنا سابقاً في هذا الفرع للحديث عن التفتيش ومدى قابلية المكونات المادية والمعنوية للأجهزة الإلكترونية للتفتيش والشبكات المرتبطة بها، وموقف التشريعات والفقه بشأن ذلك، ولا مجال لتكرار ذلك.

- **السلطة المختصة بالتفتيش:**

إن الأصل أن يقوم الادعاء العام أو قاضي التحقيق في الأنظمة الإجرائية بإجراء التفتيش، وهو ما نصت عليه غالبية التشريعات، ومنها المشرع السعودي والمصري والأردني، إلا أنه يصعب حدوث ذلك عملياً، وعليه يمكن لمأموري الضبط القضائي القيام بإجراء التفتيش في حالات استثنائية وهما حالتان: حالة التلبس، ويجوز لمأموري الضبط القضائي كذلك تفتيش المتهم بشخصه في حالات يحددها المشرع دون حالة التلبس. وحالة انتداب مأموري الضبط القضائي للقيام بالتفتيش سواء مسكن المتهم أو شخصه من قبل سلطة التحقيق، وفي هذه الحالة لابد من تحديد المكان المراد تفتيشه أو الشخص، أو الأشياء محل التفتيش، في أمر الانتداب[81].

الفرع الثالث

الخبرة

عُرِّفت الخبرة القضائية بالعديد من التعريفات من قبل الفقه، ونذكر بعضاً منها، فقد عرفت بأنها: «إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص

(79) د. سامي جلال فقي حسين، مرجع سابق، ص 117–126.
(80) د. أشرف عبد القادر قنديل، مرجع سابق، ص 149.
(81) المادتان (46) و(80) من قانون الإجراءات الجزائية العماني.

الدليل منه»[82]، كما عرفت كذلك بأنها: «الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته، نحو المسائل التي يحتاج تقديرها لمعرفة خاصة ودراية علمية أو فنية لا تتوفر لديه بحكم عمله وثقافته، أما الخبير فهو كل شخص له دراية خاصة بمسألة من المسائل»[83]، كما أنها عُرِّفت أيضاً بأنها: «قدرة فنية أو علمية يفتقر إليها القائم بالتحقيق، فيطلبها ممن تتوافر فيه لحل مسألة تتعلق في التحقيق في الدعوى العمومية المعروضة عليه»[84].

ومن تلك التعريفات يتضح أن القاضي أو المحقق يلجأ إلى الخبرة الفنية في الجرائم عموماً في الوقائع التي يتطلب العلم بها أو تفسيرها معرفة خاصة لا تتوافر فيه، فتكون تلك الوقائع غير واضحة وغير ثابتة لديه ولا يمكن إثباتها بوسيلة أخرى من خلال ملف الدعوى والأدلة المعروضة فيه، فيستعين بالخبير الفني لتوضيح ما أشكل عليه معرفته وتقديم الرأي الفني الذي يحتاجه للوصول إلى الحقيقة. وإذا كان للخبرة ذلك الدور والأهمية في الجرائم التقليدية بشكل عام، فإن تلك الأهمية تتعاظم وتصبح ضرورية في إجراءات جمع الأدلة الإلكترونية لإثبات الجريمة الإلكترونية، حيث إن هذه الجرائم تتعلق بمسائل فنية غاية في التعقيد، وكما أن محل الجريمة فيها ليس بصورة مادية، إضافة للتطور المستمر في أساليب ارتكابها وتطور وتنوع الأدوات المستخدمة فيها والتكنولوجيا بشكل عام، فالأجهزة الإلكترونية متنوعة ومتعددة وكذلك شبكات الاتصال، وتنتمي التقنية لعلوم مختلفة ولها تخصصات علمية وفنية دقيقة ومتعددة، مما يتطلب وجود الخبرة لكشف غموض الجريمة ومعرفة مرتكبها والوصول لتحقيق العدالة[85].

الخبرة في الجريمة الإلكترونية:

منذ ظهور الجرائم ذات الصلة بالتقنية والحاسب الآلي، بدأت جهات الاستدلال والتحقيق الاستعانة بأصحاب الخبرة الفنية في هذا المجال، بهدف كشف الجريمة وجمع الأدلة ومساعدة سلطات التحقيق في كشف غموض هذه الجرائم الإلكترونية محل التحقيق، وتتأثر أهمية الاستعانة بالخبرة في الجريمة الإلكترونية عند غيابها، فبغياب الخبرة عن جهات الاستدلال والتحقيق تغدو عاجزة عن فك شفرات الجريمة وكشفها، فلا يمكنها

(82) د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار الفكر العربي، القاهرة، 1988م، ص 645.

(83) د. أحمد يوسف الطحطاوي، مرجع سابق، ص 304.

(84) د. مزهر جعفر عبيد، شرح قانون الإجراءات الجزائية العماني، الجزء الأول، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2008م، ص 541.

(85) عائشة بن قارة مصطفى، مرجع سابق، ص 138–139.

تجميع الأدلة الجنائية التي تثبتها، وبسبب جهلها في هذا التخصص قد تدمر أو تمحو تلك الأدلة عند التعامل معها، ولابد من أن يكون الخبير ذا كفاءة علمية في مجال التخصص، بالإضافة إلى الخبرة في مجال العمل المراد الاستعانة به وهي الجريمة الإلكترونية، وهو ما يطلق عليه بالخبير الإلكتروني، ويمكن تعريفه بأنه: «الشخص الذي تَعمَّق في دراسة عمل من الأعمال الإلكترونية وتخصص في أدائه فترة زمنية طويلة، مما أكسبه خبرة عملية بحيث أصبح ملماً بتفصيلاته وجعله متفوقاً على الشخص العادي وقادراً على إبداء الرأي الإلكتروني الرقمي في الأمور المتصلة بهذا العمل»[86].

والخبرة الإلكترونية شأنها شأن الخبرة القضائية في الجرائم التقليدية من حيث القواعد القانونية التي تحكمها عموماً سواء في اختيار الخبراء أو عمليات الخبرة في حد ذاتها، ولكنها تختلف عنها فيما يتعلق بالقواعد الفنية التي تحكم عمل الخبير الإلكتروني، وعليه سنتطرق إلى القواعد القانونية التي تحكم عمل الخبرة بشكل مختصر، ومن ثم القواعد الفنية التي تحكم عمل الخبير الإلكتروني، على النحو التالي:

أولاً- القواعد القانونية التي تحكم الخبرة الإلكترونية:

وسنتناول في هذه القواعد اختيار الخبراء وواجبات الخبير التقني، وذلك فيما يلي:

أ. اختيار الخبراء:

غالباً ما تحدد التشريعات طريقة اختيار الخبراء عن طريق القيد في جدول الخبراء الذي تعده وزارة العدل أو المجالس القضائية المختصة، ويتم اختيار الخبراء بعد ذلك منه، وعليه تكون شروط اختيار الخبير وفق ما تحدده تلك الجهات عند إعلان التسجيل في تلك الجداول. ونص قانون الإجراءات الجزائية العماني على أن الاستعانة بالخبير تكون بأمر ندب يصدر من عضو الادعاء العام وهو ما نصت عليه المادة (116)، وسواء أكان هذا الخبير مقيداً في جدول الخبراء أم لم يكن، فعضو الادعاء العام حر في اختياره. ولا يشترط أن تحدد طبيعة الخبير سواء أكان شخصاً طبيعياً أم معنوياً، فيمكن اختيار الخبير بشخصه أو كمؤسسة تعمل في هذا المجال، وفي مجال الجريمة الإلكترونية غالباً ما يتم اختيار شركات أو منظمات أو مؤسسات متخصصة في مجال تقنية المعلومات لما تملكه من خبرة في المجال، وتوفر الخبرة في تنوعها في أكثر من مجال من المجالات والتخصصات التي تشملها التقنية المعلوماتية[87].

وهناك جانب من الفقه يرى بأنه لا يشترط في الخبير بأن يكون متخرجاً من جامعات أو كليات متخصصة في تقنية المعلومات، بل يكفي أن يمتلك مهارة وخبرة في استعمال

(86) أمير فرج يوسف، مرجع سابق، ص 328.
(87) عائشة بن قارة مصطفى، مرجع سابق، ص 142.

الأجهزة الإلكترونية والتعامل مع التقنية، ويستند هذا الرأي إلى أن بعض أمهر مبرمجي نظم المعلومات الذين لم يكن تحصليهم العلمي يصل لدراسة التخصص في هذا المجال، وكذلك مخترقو الأنظمة والشبكات، فالكثير منهم لا تتجاوز أعمارهم مرحلة التعليم العام[88]. ورغم وجاهة الرأي السابق، إلا أنه يؤخذ عليه بأنه يتعارض مع الواقع القانوني عند اختيار الخبير وبعد الانتهاء من عمله، فيشترط أن يسلم الخبير في نهاية أعمال الخبرة تقريراً عنها، ويلزم أن يكون التقرير متكاملاً شاملا للعناصر الشكلية والموضوعية في أعمال الخبرة، وهو ما لا يمكن أن يتم إلا من الأشخاص المتخصصين في ذات المجال.

ب. واجبات الخبير الإلكتروني:

يمكن بيان هذه الواجبات من الناحية القانونية وفق ما يلي:

1. **أداء اليمين:**

إن من أهم الواجبات القانونية التي تقع على الخبير الإلكتروني هي أداء اليمين، فقد أوجب المشرع عليه أداء اليمين قبل أداء أعماله، وإلا اعتبر ما يقوم به باطلاً، فأداء اليمين إجراء جوهري يستهدف المشرع من خلاله أن يحمل الخبير على القيام به وفق مبدأي الصدق والأمانة، وذلك لأطراف الخصومة ومن جانب عضو سلطة التحقيق أو مأمور الضبط القضائي الذي يصدر أمره بانتدابه. وفي هذا الأمر فقد نصت المادة (118) من قانون الإجراءات الجزائية العماني على أنه: «إذا كان الخبير من غير المقيدين في الجدول وجب أن يحلف أمام عضو الادعاء العام يميناً بأن يؤدي عمله بالذمة والصدق.

2. **أن يؤدي الخبير أعماله ومهامه بنفسه:**

وذلك وفق حدود القانون ووفق حدود الأمر الذي يصدر بندبه للقيام بأعمال الخبرة، فعليه القيام بعمله وفق ما يحدد له في أمر الندب من الأعمال المطلوب منه إبداء رأيه الفني فيها دون الدخول في وقائع أخرى خارج نطاق الأمر الصادر، وهو ما تؤكده المادة (116) من قانون الإجراءات الجزائية العماني.

3. **خضوع الخبير الإلكتروني لرقابة وإشراف عضو سلطة التحقيق أو مأمور الضبط القضائي:**

(88) د. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص 598.

على الخبير أن يبقى على اتصال دائم مع عضو سلطة التحقيق أو مأمور الضبط القضائي ويخضع لتوجيهه من أجل إحاطته بالتطورات والأعمال التي يقوم بها، فهو مساعد فني له. وتنص المادة (117) من قانون الإجراءات الجزائية العماني في هذا الأمر بأنه: «يمارس الخبير مهمته تحت إشراف وتوجيه عضو الادعاء العام، ويجوز للخبير القيام بالإجراءات الضرورية التي يراها لازمة لإنجاز مهمته، وذلك بعد الرجوع إلى عضو الادعاء العام كلما أمكن ذلك».

4. **الاستعانة بأطراف الخصومة والسماع إلى أقوالهم وما يقدمون من طلبات كإجراء أبحاث معينة أو سماع شهود.**

5. **تقديم تقرير فني بعد انتهاء أعمال الخبرة**

وذلك وفق الوقت المحدد في أمر الندب، ويحق استبداله إذا لم يقم بتقديم تقريره في الوقت المحدد مع إلزامه برد جميع الأشياء والأوراق والوثائق التي تكون قد منحت إليه بموجب أمر الندب. وقد ألزم قانون الإجراءات الجزائية العماني الخبير بتقديم تقرير عن مهمته التي يكلف بها، وعليه تقديمه كتابة في الميعاد الذي يحدده عضو الادعاء العام له، وهو ما جاءت به المادتان (116) و(119) من قانون الإجراءات الجزائية. وغالباً ما يبني عضو سلطة التحقيق أو مأمور الضبط القضائي رأيه الفني على تقرير الخبير ويساعده في ضبط الأدلة الإلكترونية والوصول إليها وبناء رأيه استناداً على تقرير الخبير الفني.

ثانياً- القواعد الفنية التي تحكم عمل الخبير الإلكتروني:

توجد بعض القواعد الفنية الخاصة التي تنفرد بها الخبرة الإلكترونية عند القيام بها، وقبل تحديد تلك القواعد والتطرق إليها، سنتناول أهم المسائل التي يحتاجها مأمور الضبط القضائي أو عضو سلطة التحقيق من الخبير الإلكتروني ويقوم بانتدابه من أجلها، وكذلك كيفية القيام ببعض الإجراءات التي يحتاجها القائم بالمعاينة أو التفتيش، وعلى الخبير أن يكون ملماً بها وبطريقة إجرائها، وهي كالتالي:

1. الإلمام ووصف تركيب وصناعة الجهاز الإلكتروني وطرازه ونوع نظام التشغيل الذي يعمل عليه، وأهم الأنظمة والبرامج الفرعية التي تستخدم بالجهاز، والأجهزة والنهايات الطرفية الملحقة به، بالإضافة لكلمات المرور والسر لنظام التشفير وغيرها من الأمور المماثلة.

2. الإلمام ووصف الموضوع المحتمل لأدلة الإثبات المادية والمعنوية وشكلها ونوعها

والهيئة التي تكون عليها.

3. الإلمام ووصف طبيعة بيئة الجهاز الإلكتروني وشبكاته، من حيث تنظيمها ومدة تركيز وعمل المعالجة الآلية، ونمط وسائل الاتصالات وترددات موجات البث وأماكن تخزينها.

4. التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مرئية مقروءة، بحيث يتاح لمأمور الضبط القضائي أو عضو سلطة التحقيق الاطلاع عليها وفهمها، مع إثبات أن الدليل مطابق لصورته غير المرئية.

5. عزل النظام المعلوماتي دون إتلاف للأدلة أو تدميرها أو إلحاق الضرر بالجهاز، وبيان كيفية إجراء ذلك.

6. نقل أدلة الإثبات إلى أوعية ووسائط تقنية ملائمة دون أن يلحقها تلف أو تغيير، وبيان طريقة إجراء ذلك[89].

ولما كانت عملية جمع الأدلة الإلكترونية تعد من أهم وأصعب الأمور في إثبات الجريمة الإلكترونية، بسبب تعدد أشكال وصور الجرائم الإلكترونية، والتي تدور ما بين الحصول على المعلومات للاستيلاء عليها أو تدميرها أو اختراق الأنظمة عن طريقها، أو الاحتيال وسرقة الأموال، أو الهجوم على الأجهزة الإلكترونية لإتلافها وتخريبها، أو لمجرد إظهار الذات وإثبات مقدرتها في هذا المجال، لذا يكون اللجوء إلى خبير إلكتروني وتقني أمراً مهماً وملزماً للوصول إلى كشف الجريمة ومرتكبها. ويرى بعض المختصين في هذا الأمر أن القيام بعملية تجميع الأدلة الإلكترونية في الجريمة الإلكترونية من خلال شبكة الإنترنت تتم عبر ثلاث مراحل رئيسية[90]، وهي:

- **المرحلة الأولى:** تجميع المعلومات المخزنة لدى طرف مقدم خدمة الاتصال والوصول إلى شبكة المعلومات، من خلال تتبع الخوادم التي دخل الفاعل منها، ومحاولة إيجاد أي أثر إلكتروني له.
- **المرحلة الثانية:** وهي مرحلة المراقبة، وتقوم على فرضية أن الفاعل لابد من أن يعود لمسرح جريمته سواء بالدخول إليه مرة أخرى أو بمشاهدته والاطلاع عليه عن قرب، وتتعدد طرق مراقبة هذه الأجهزة وتتنوع وفق ما تنتجه التقنية من تحديثات وبرامج خاصة لهذه المراقبة.

(89) د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية، القاهرة، 1994م، ص 142–143.

(90) د. حازم محمد حنفي، مرجع سابق، ص 69–70.

- **المرحلة الثالثة:** وهي مرحلة ضبط الأجهزة المشتبه بها وفحصها فحصاً فنياً وقانونياً، ويبدأ في هذه المرحلة عمل الخبير الإلكتروني في فحص نظام الجهاز المشتبه فيه بجميع مكوناته المادية والمعنوية والشبكية، من أجل استخراج دليل إدانة الفاعل وتحديد مدى قدرة الأدلة على ذلك، أو الوصول إلى براءة النظام والأجهزة المشتبه بها من استخدامها في الجريمة.

وعند استخراج الخبير الإلكتروني لتلك الأدلة وتجميعها، عليه الالتزام ببعض القواعد الفنية والخطوات في هذا المجال، وتتمثل هذه الخطوات والقواعد الفنية في المراحل التالية:

أ. خطوات ما قبل التشغيل والفحص:

- التأكد من مطابقة محتويات إحراز المضبوطات لما هو مكتوب عليها.
- التأكد من صلاحية وحدات نظام التشغيل.
- تسجيل بيانات وحدات المكونات المضبوطة، كنوعها وطرازها والرقم المتسلسل لها.

ب. خطوات التشغيل والفحص:

- عمل نسخة من كل وسائط التخزين المضبوطة وأهمها القرص الصلب، لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجية.
- استكمال تسجيل باقي بيانات الوحدات من خلال القراءات التي يوفرها الجهاز.
- تحديد أنواع وأسماء المجموعات البرامجية، كبرامج النظام وبرامج التطبيقات، وبرامج الاتصالات.
- إظهار الملفات المخبأة والنصوص المخفية داخل الملفات.
- استرجاع الملفات التي تم محوها من الأصل وذلك باستخدام برامج استعادة البيانات، وكذلك بالنسبة للملفات المعطلة أو التالفة من خلال إعادة تشغيلها وإصلاحها، وتخزن هذه الملفات بعد ذلك ويعمل لها نسخ طبق الأصل من الأسطوانة أو القرص محل الفحص عن طريق تطبيق الخطوات سالفة الذكر.
- إعداد قائمة يجرد فيها الخبير الإلكتروني كل الأدلة الإلكترونية التي تم الحصول عليها في وعاء خاص، مع إجراء مراجعة لكل الملفات المحتفظ بها في الوعاء في جهاز آخر للتأكد من سلامة القائمة.
- تحويل الدليل الإلكتروني إلى هيئة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صوراً أو نصوصاً، أو وضعها في أي وعاء آخر حسب نوع المعلومات والبيانات المكونة للدليل.

ج. تحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني:

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط والدليل الإلكتروني في شكله المادي، ومن ثم الربط بينهما لإكساب الدليل الموثوقية واليقينية مما يؤدي لقبوله لدى جهة التحقيق والمحاكمة.

د . مرحلة تدوين النتائج وإعداد التقارير:

يتم خلال هذه المرحلة إعداد تقرير يشمل جميع الخطوات وإجراءات البحث، ويرفق به الملاحق الإيضاحية المصورة أو المسجلة والمطبوعة وغيرها لاعتمادها، ثم تسلم إلى جهة التحقيق أو المحاكمة[91].

الفرع الرابع
الشهادة

يقصد بالشهادة بشكل عام بأنها: «التعبير عن المضمون الحسي للشاهد بما رآه أو سمعه بنفسه من معلومات عن الغير مطابقة لحقيقة الواقعة التي يشهد عليها في القضاء بعد أداء اليمين ممن تقبل شهادتهم وممن يسمح لهم بها ومن غير الخصوم في الدعوى»[92]. كما عُرِّفت كذلك بأنها: «تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواسه»[93]، وعرَّفها جانب آخر من الفقه بأنها: «الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء أكانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أم براءته منها»[94].

فالشهادة هي دليل من أدلة الإثبات، فعند وقوع جريمة ما، يتم الاستماع إلى شهودها من غير أطراف الخصومة فيها من أجل إثبات الجريمة والوقوف على وقائعها وتفاصيلها، والاستماع إلى الشهود يكون بالسماح لهم بالإدلاء بما لديهم من معلومات حول الواقعة محل الاستدلال أو التحقيق أو المحاكمة، فالشاهد المعلوماتي وفق ذلك المفهوم، لابد أن يكون ذا خبرة فنية في مجال الجهاز الإلكتروني، وعليه يكون الشاهد المعلوماتي ضمن فئات أو طوائف مختصة بذلك المجال، ونذكر أهم تلك الطوائف التي يكون منها الشهود في الجريمة الإلكترونية، على النحو التالي:

(91) د. أشرف عبد القادر قنديل، مرجع سابق، ص 173–174.
(92) د. سليمان مرقص، أصول الإثبات وإجراءاته، الأدلة المقيدة، الجزء الثالث، دار الحلبي للمنشورات الحقوقية، بيروت، 1998، ص 11.
(93) د. محمود نجيب حسني، مرجع سابق، ص 453.
(94) عائشة بن قارة مصطفى، مرجع سابق، ص 125.

أولاً- مشغلو الجهاز الإلكتروني:

وهم أصحاب الخبرة الذين تكون لديهم الدراية التامة بتشغيل الجهاز الإلكتروني والمعدات والملحقات المتصلة به واستخدامها، وإدخال البيانات ونقلها من وإلى الجهاز[95].

ثانياً- المحللون:

المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراسة هذه البيانات، ومن ثم تحليلها أي تقسيمها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظم عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن معالجتها بواسطة الحاسب الآلي[96].

ثالثاً- المبرمجون:

أو خبراء البرمجة أو مخططو البرامج، وهم الأشخاص المتخصصون في كتابة أوامر البرامج، وأمكن تصنيفهم إلى فئتين هما: الفئة الأولى: وهم مخططو برامج التطبيقات، وتقوم هذه الفئة بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات، ويقوم بذلك العمل مخطط برامج واحد أو عدة مخططين حسب حجم النظام ومتطلباته. الفئة الثانية: وهم مخططو برامج النظم، ويقوم أصحاب هذه الفئة باختبار وتعديل وتصحيح برامج نظام الجهاز الإلكتروني الداخلية، أي أنهم يقومون بتجهيز الجهاز الإلكتروني والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج أو الأجزاء[97].

رابعاً- مهندسو الصيانة والاتصالات:

وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الجهاز الإلكتروني بمكوناته وشبكات الاتصال المتعلقة به[98].

---

(95) د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الآلي الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991م، ص 23.

(96) د. هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، مرجع سابق، ص 24.

(97) المرجع السابق، ص 25.

(98) د. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، خلال الفترة بين 26-28 أبريل 2003م، ص 616.

خامساً- مديرو النظم:

وهم الذين توكل إليهم أعمال الإدارة في النظم المعلوماتية[99].

وهؤلاء جميعاً يعدون من الشهود في الجريمة الإلكترونية عند استدعائهم للإدلاء بمعلوماتهم من قبل مأمور الضبط القضائي أو عضو سلطة التحقيق، مع مراعاة أدائهم لليمين أمام سلطة التحقيق دون أدائها أمام سلطة جمع الاستدلالات، كما أن هناك أشخاصاً آخرين يعدون بمثابة شهود في الجريمة الإلكترونية، من بينهم مقدمو الخدمات الوسطية في مجال المعلوماتية والإنترنت[100]. كما أن هناك بعض التشريعات التي أصدرت لوائح وقرارات خاصة تحصر فيها شهود الجريمة الإلكترونية، من بينها المشرع في ولاية كاليفورنيا الأمريكية[101]، ولم يتطرق المشرع العماني إلى هذا الأمر، ولم يحدد فئات محددة من الشهود للجريمة الإلكترونية، وإن كانت نصوص قانون الإجراءات الجزائية تشمل الشهود بجميع فئاتهم دون حصر لهم في جرائم معينة.

سادساً- التزامات الشاهد المعلوماتي:

لا تختلف التزامات الشاهد في الجريمة الإلكترونية عنها في الجرائم العادية التقليدية سوى فيما يخص الجانب العملي لها، إذ إنه يمكن أن يقدم شهادته مصحوبة بأدوات مساعدة كأجهزة العرض أو جهاز إلكتروني محمول، ويجب على الشاهد في الجريمة الإلكترونية أن يقدم لمأموري الضبط القضائي وسلطة التحقيق المعلومات الجوهرية اللازمة للدخول إلى نظام المعالجة الآلية والأجهزة وكذلك المواقع التي تحتوي على المعلومات التي تشكل جريمة، من أجل البحث عن أدلة تثبتها، ويستثنى من ذلك في حالة حماية القانون له بعدم إفشاء تلك المعلومات كأسرار مهنة الطبيب أو المحامي، اللذين خَوَّل لهما القانون الاحتفاظ بأسرار عملائهم[102].

ومع القول بالتزام الشاهد بالإدلاء بالمعلومات الجوهرية اللازمة للدخول إلى نظام المعالجة الآلية للجهاز، يُثَار التساؤل هنا حول التزام الشاهد بتسليم الملفات المخزنة في الجهاز بصورة مادية مطبوعة وحول الإفصاح عن كلمات المرور والسر للدخول إلى الأنظمة والبرامج المختلفة، حيث إن لذلك أهميته، فقد لا يعلم بتلك المعلومات والبيانات وكلمات المرور إلا الشاهد ولا يمكن الوصول إليها عن طريق الخبير المنتدب، وقد اختلف

(99) د. هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، مرجع سابق، ص 24.

(100) د. أشرف عبد القادر قنديل، مرجع سابق، ص 163.

(101) د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي- المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، 2008م، ص 55.

(102) د. حازم حمد حنفي، مجرع سابق، ص 73.

الفقه حول هذه المسألة في رأيين مختلفين نوضحهما فيما يلي:

الاتجاه الأول: يرى أنصار هذا الاتجاه أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطباعة الملفات والبيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالأنظمة والبرامج المختلفة بالجهاز، ويميل إلى هذا الرأي بعض التشريعات منها تونس وتشيلي[103].

الاتجاه الثاني: ويرى أنصار هذا الرأي على عكس الاتجاه الأول، أن من بين الالتزامات التي يتحملها الشاهد، القيام بطباعة ملفات البيانات والإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ويؤيد هذا الاتجاه جانب من الفقه الفرنسي الذي يرى بأنه طالما لم ينظم المشرع الفرنسي هذه المسألة، فإنه يتم تطبيق القواعد العامة في نطاق الإجراءات الجنائية، على نطاق إجراءات الجريمة الإلكترونية، وعليه يلتزم الشاهد بالشهادة بموجب قانون الإجراءات الجنائية بالإفصاح عن كلمات المرور السرية التي يعلمها، ويتبنى هذا الرأي كذلك العديد من التشريعات منها تشريعات هولندا واليونان واليابان[104].

وفي إطار الترجيح والموازنة بين الاتجاهين السابقين، فإنه يجب الرجوع إلى القواعد العامة والالتزامات التي أوجبتها التشريعات على الشاهد بصفة عامة، فوفقاً لتلك النصوص والقواعد فإن الشاهد يلتزم بثلاثة التزامات أساسية وهي الحضور أمام الجهة التي استدعته، وأداء اليمين، والإدلاء بالشهادة، وسنوضحها تباعاً على النحو التالي:

1. حضور الشاهد:

وهو يعني أن يلتزم الشاهد بالحضور بنفسه في المكان والزمان المحددين للاستماع إلى شهادته، والبقاء فيه حتى يؤذن له بالانصراف، وذلك بناء على تكليف بالحضور من الجهة التي تستدعيه[105]، فاستدعاء الشاهد والاستماع لأقواله يمكن أن يكون من مأمور الضبط القضائي أو سلطة التحقيق أو القاضي، وعدم حضوره أمامهم يمكن أن يرتب عليه عقوبات جزائية وفق قانون الإجراءات الجزائية. ولدى المشرع العماني، فقد ورد النص على عقوبة التخلف عن الحضور لأداء الشهادة في قانون الجزاء وتحديداً بالمادة (240) منه والتي وضعت عقوبة السجن من عشرة أيام إلى ستة أشهر لكل من كلف بأداء

(103) د. عبد الله حسين علي محمود، مرجع سابق، ص 390.
(104) د. هلالي عبد اللاه أحمد، مرجع سابق، ص 25–26.
(105) د. محمود نجيب حسني، مرجع سابق، ص 448.

الشهادة أمام جهة قضائية، أو سلطة التحقيق، وامتنع عن الحضور، أو حلف اليمين، أو أداء الشهادة، ما لم يكن امتناعه لعذر مقبول، ويعفى من العقوبة إذا عدل عن امتناعه قبل صدور الحكم في موضوع الدعوى.

2. أداء اليمين:

ألزم المشرع الشاهد قبل الإدلاء بشاهدته بأداء اليمين، وذلك كضمانة تضفي الثقة على أقواله وعلى عضو سلطة التحقيق أو القاضي للاستناد إلى شهادته كدليل في الدعوى، وتعطي لها القيمة القانونية، بالإضافة إلى لفت انتباه الشاهد حول خطورة ما سيدلي به في شهادته وتجعله حريصاً على قول الحق، وتنص الفقرة الثانية من المادة (108) من قانون الإجراءات الجزائية العماني على أنه يجب على الشاهد الذي أتم ثماني عشرة سنة أن يحلف قبل أداء الشهادة يميناً بأن يشهد بالحق ولا شيء غير الحق، ويجوز سماع من لم يتم هذه السن على سبيل الاستئناس بغير يمين. كما حددت المادة (111) عقوبة عدم حلف اليمين أمام الادعاء العام. وأداء اليمين يكون ملزماً أمام سلطة التحقيق والقضاء وهي تعتبر من أدلة الإثبات، أما الشهادة أمام مأمور الضبط القضائي فلا يلزم أداء اليمين فيها وتكون من أعمال جمع الاستدلال (المادة (34) من قانون الإجراءات الجزائية). ويعتبر أداء اليمين من النظام العام، فلا يجوز للشاهد الامتناع عن أدائها بعدم الحضور وإلا ستطبق عليه العقوبة المقررة للامتناع عن أداء الشهادة، كما أنه لا يجوز للشاهد أن يطلب من عضو سلطة التحقيق أو القاضي إعفاءه من أداء اليمين.

3. الالتزام بالإدلاء بالشهادة:

وهو أهم الالتزامات المفروضة على الشاهد وجوهر مهمته، ويعني هذا الالتزام أن يقوم الشاهد أولاً بالحديث، فهو على عكس المتهم الذي من حقه الصمت، فعلى الشاهد أن يدلي بشهادته وعدم السكوت أمام الجهة التي استدعته، وإلا اعتبر ذلك من قبيل الامتناع عن أداء الشهادة وتنطبق عليه العقوبة المقررة لذلك. وثانياً فإن هذا الالتزام يعني ألا يلتزم الشاهد إلا بذكر ما يعلمه من معلومات عن الجريمة، ولا يجوز إجباره على القيام بعمل معين، وفي هذا الأمر ينص قانون الإجراءات المصري وبالتحديد في مادته (284) على أنه :«إذا امتنع الشاهد عن أداء اليمين أو الإجابة في غير الأحوال التي يجيز له القانون فيها ذلك، حكم عليه...»، ومعنى ذلك أن الشاهد يلتزم بالإجابة عن الأسئلة التي توجهها المحكمة له، وفي مقابل ذلك لا تلزمه المحكمة بالقيام بعمل معين، وفي ذات الشأن تقول محكمة النقض المصرية: «إن الشهادة هي تقرير شخص لما يكون قد رآه أو سمعه بنفسه

أو أدركه على وجه العموم بحواسه»[106]. أما قانون الإجراءات الجزائية العماني فقد نص على ذلك بموجب المادة (111) منه والتي جاء فيها: «إذا حضر الشاهد وامتنع عن أداء الشهادة أو عن حلف اليمين، يحكم عليه في الجنح والجنايات بعد سماع أقوال الادعاء العام بغرامة لا تقل عن مائتي ريال، ويجوز إعفاؤه من كل أو بعض العقوبة إذا عدل عن امتناعه قبل انتهاء التحقيق».

ونستنتج من هذه الالتزامات التي وضعت على عاتق الشاهد أنه ليس من واجبه في الجريمة الإلكترونية طبع الملفات والبيانات المخزنة في ذاكرة الجهاز الإلكتروني، حيث إن طبيعة الشهادة ونوعها كدليل عند تقسيمها من حيث مصدرها تجعلها من الأدلة القولية وهي الأدلة التي مصدرها الأشخاص والذين أدركوا معلومات مفيدة للإثبات بإحدى حواسهم، وتتمثل فيما يصدره الغير من أقوال، وعليه لا يصبح الشاهد ملزماً أن يقدم الملفات والبيانات بصورة مطبوعة، وإنما يدلي بشهادته وفق ما أدركه من معلومات بطريقة شفوية أو يقدم عرضاً مبسطاً عنها ، ويمكن أن يقدمها بشكل مادي مطبوع ولكنه غير ملزم له.

أما الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، فهو التزام يزيد عن نطاق الشهادة المقررة والالتزامات سالفة الذكر التي حددها المشرع، فالتزام الشاهد هو التزام بالإدلاء بمعلومات تخص الجريمة الواقعة وما يعلمه من معلومات عنها وعن فاعلها، وليس التزاماً بالإدلاء بمعلومات تخص النظام محل الجريمة، فهو ذات الأمر إذا شاهد شخص جريمة قتل تحصل أمامه فهو يلتزم بأن يدلي بما رآه يحصل أمامه في هذه الجريمة، ولا يلتزم أن يدلي بمعلومات عن الرقم السري الذي وضعه الجاني عند فتح باب منزل المجني عليه، كما أن الشهود في الجرائم الإلكترونية هم المختصون وخبراء في تقنية المعلومات والنظام الذي وقعت فيه الجريمة، يمكن أن يعطوا جهات التحقيق البيانات والمعلومات المطلوبة عن النظام وعن الجاني وسجلات البيانات دون الحاجة لحصول جهة التحقيق على كلمات المرور التي تخص النظام محل الجريمة، وعليه إذا كانت السلطات ترى حاجتها لكلمات المرور أثناء إجراءات التحقيق أو جمع الاستدلال ينبغي أن يكون هناك تدخل تشريعي عن طريق إضافة نصوص قانونية خاصة تفرض على الشاهد التعاون مع الجهات القضائية أثناء التحقيقات والمحاكمة، وتحديد هذا المتطلب في نصوص الشهادة ضمن الإجراءات الخاصة بالجريمة الإلكترونية.

(106) محكمة النقض المصرية جلسة 15 يوليو سنة 1964م، س15 ق رقم 98، ص 493.

المطلب الثاني
الإجراءات الحديثة لجمع الدليل الإلكتروني

إن من أهم الصعوبات التي تواجه سلطتي جمع الاستدلالات والتحقيق في الجريمة الإلكترونية عملية إثباتها، ولا يتم إثبات الجريمة إلا بتوافر الأدلة التي تؤكد ذلك، لذا فإن عملية جمع الأدلة الإلكترونية إحدى تلك الصعوبات التي تواجه عضو سلطة التحقيق، كما أنها تعد من الصعوبات التي تواجه حتى الخبير الإلكتروني رغم تخصصه ومعرفته بمجال تقنية المعلومات وشبكاتها، ويرجع ذلك للتطور الحادث والمستمر في وسائل تقنية المعلومات والأجهزة الإلكترونية الحديثة التي تستخدم شبكات الاتصال ونقل البيانات، وهو ما أدى إلى مواكبة ذلك التطور بتطور أساليب وأدوات ارتكاب الجريمة الإلكترونية والتقليدية على السواء، نتيجة الاستخدام السلبي لهذه التكنولوجيا الحديثة. وسوف نتطرق في هذا المطلب للإجراءات الحديثة التي تساعد في جمع الأدلة الإلكترونية، من خلال بيان الإجراءات المتعلقة بنظم التشغيل والبيانات الساكنة (الفرع الأول)، والإجراءات المتعلقة بالبيانات المتحركة في شبكة المعلومات (الفرع الثاني)، ومن ثم إجراءات الحصول على بروتوكول العنوان الإلكتروني (الفرع الثالث).

الفرع الأول
الإجراءات المتعلقة بنظم التشغيل والبيانات الساكنة

تُعَد الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية التي تم التوقيع عليها في بودابست عاصمة المجر بتاريخ 23 نوفمبر 2001 من أولى الاتفاقيات الدولية التي تختص بمكافحة الجرائم الإلكترونية، حيث جاءت هذه الاتفاقية بإشراف المجلس الأوروبي ووقعت عليها ثلاثون دولة، أربع منها من خارج الاتحاد الأوروبي هي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية، وقد دخلت الاتفاقية حيز التنفيذ في يوليو 2004، حيث شكلت أول محاولة قانونية دولية لمعالجة مشكلة تزايد الجرائم الإلكترونية، وكان الهدف الرئيسي من إقرارها هو وضع سياسة جزائية مشتركة لمكافحة الجريمة الإلكترونية عن طريق مواءمة القوانين الوطنية مع نصوص الاتفاقية لضمان توفير الحماية الكافية للمجتمع من هذه الجرائم[107].

وقد تضمنت هذه الاتفاقية النص لأول مرة على التفرقة بين نوعين من البيانات، وهي البيانات المخزنة أو الساكنة، والبيانات المتحركة أو البيانات المتعلقة بخط سير المعلومات،

(107) د. عادل عزام سقف الحيط، جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية، دراسة مقارنة، دار الثقافة، القاهرة، 2011م، ص 365.

ومن خلال قراءة نصوص هذه الاتفاقية نجد أنها نصت على إجراءات جديدة لجمع الأدلة في الجريمة الإلكترونية، منها إجراءات ممهدة تسبق عملية جمع الأدلة، ومنها إجراءات خاصة بجمع الأدلة[108]. ومن أهم ما جاءت به اتفاقية بودابست لمكافحة الجريمة الإلكترونية النص على التحفظ المعجل أو السريع على بيانات الحاسب المخزنة، حيث تنص المادة (16) من هذه الاتفاقية على أن تعتمد كل دولة طرف ما قد يلزم من تشريعات أو تدابير أخرى، حتى تتمكن السلطات المختصة فيها الأمر أو طلب التحفظ بصورة عاجلة على بيانات محددة في حاسب آلي، بما في ذلك خط سير البيانات المخزنة بواسطة منظومة حاسب آلي، خاصة في حالة وجود أسس للاعتقاد بإمكانية تعرض البيانات للفقد أو التعديل.

كما أن اتفاقية بودابست لمكافحة الجريمة الإلكترونية نصت على إجراء آخر وهو سلطة إصدار الأوامر، حيث جاء ذلك بموجب الفقرة الأولى من المادة (18) من الاتفاقية، والتي تنص على أن تعتمد كل دولة طرف ما يلزم من تشريعات وتدابير أخرى لمنح سلطاتها المختصة صلاحية توجيه الأمر، إلى أي شخص يتواجد في إقليم الدولة لتقديم بيانات محددة على الحاسب الآلي بحوزته أو تحت سيطرته ومخزنة داخل نظام حاسوبي أو على أي وسيط تخزين بيانات آخر، وكذلك توجيه الأمر إلى أي مقدم خدمة يعرض خدماته في إقليم الدولة لتقديم معلومات المشترك[109] لديه فيما يتعلق بتلك الخدمات الموجودة بحوزة مقدم الخدمة أو تحت سيطرته، ويقصد بمقدم الخدمة في نطاق هذه الاتفاقية بأنه أي كيان عام أو خاص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق منظومة حاسوب، وأي كيان آخر يقوم بمعالجة بيانات الحاسب أو تخزينها نيابة عن خدمة الاتصالات المذكورة أو مستخدمي هذه الخدمة.

ومن الإجراءات الحديثة كذلك التي تستخدم في جمع الأدلة الإلكترونية استخدام التكنولوجيا في هذه الإجراءات، وذلك يشمل استخدام البرامج التقنية المتخصصة

(108) د. حازم محمد حنفي، مرجع سابق، ص 95.

(109) عرَّفت الفقرة الثالثة من المادة (18) من اتفاقية بودابست لمكافحة الجريمة الإلكترونية مصطلح «معلومات المشترك» بأنه: أية معلومات في صورة بيانات حاسوب أو أية صورة أخرى يتم حفظها من جانب مقدم الخدمة، وهي التي تتعلق بالمشتركين في الخدمات الخاصة به، بخلاف خط سير البيانات أو مضمونها، التي يمكن التوصل بموجبها إلى:

أ- نوعية خدمة الاتصال المستخدمة، والشروط الفنية التي يتم اتخاذها في ذلك، والفترة الزمنية للخدمة.

ب- هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه، وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع، المتاحة بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

ج- أية معلومات أخرى، خاصة بواقع تركيب أجهزة الاتصالات ومعداتها، من التي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

لمساعدة مأموري الضبط القضائي وسلطات التحقيق في جمع الأدلة، ومنها استخدام برامج كسر كلمات المرور لبعض المستندات، حيث إنه توجد في بعض برامج الأجهزة الإلكترونية خاصية وضع كلمة مرور للمستندات التي يتم إنشاؤها عبر هذا البرنامج تمنع المستخدم من الدخول إليها والاطلاع على محتواها إلا بعد إدخال كلمة مرور خاصة تسمح له بفتح الملف، وبالتالي يمكن لسلطة التحقيق أو الخبير الإلكتروني المنتدب استخدام هذه البرامج الخاصة لكسر هذا النوع من الحماية والاطلاع على محتوى المستندات[110].

الفرع الثاني
الإجراءات المتعلقة بالبيانات المتحركة في شبكة المعلومات

مما ساعد على انتشار استخدام شبكات المعلومات عبر العالم أجمع هو ثورة تكنولوجيا المعلومات وتطورها المستمر، حيث أصبحت غالبية أجهزة الحاسب الآلي أجهزة محمولة سهلة الاستخدام والحمل، كما أن تلك الثورة المعلوماتية لم تقف عند ذلك الحد، بل أنتجت أجهزة إلكترونية حديثة تحتوي على برامج مشابهة للبرامج الموجودة في الحاسب الآلي كالأجهزة النقالة والأجهزة اللوحية، فهي أشبه بأجهزة حواسيب مصغرة يستطيع الشخص حملها واستخدامها في أي مكان والدخول لشبكة المعلومات بسهولة أكبر دون الحاجة للمكونات المادية للحاسب الآلي المعقدة والتي تحتاج إلى موصل كهربائي دائم لتشغيلها، مما أدى إلى انتقال مسرح الجريمة إلى هذه الشبكات والأجهزة، وتكون هي أدوات الجريمة المتطورة. وقد ساهمت العديد من العوامل بشكل عام في إثارة صعوبات وخلق عقبات جديدة أمام سلطات التحقيق في الجريمة الإلكترونية، من أهمها:

أولاً- طبيعة شبكة المعلومات هي عبارة عن اتصال لأكثر من شبكة وجهاز:

ونتيجة لذلك توزعت مسارح الجريمة وكذلك الأدلة الإلكترونية في عدة أماكن مختلفة مما يؤدي إلى صعوبات عملية وتشريعية في آن واحد، خاصة مع اختلاف نصوص القوانين بين تلك الأماكن، ففي أغلب الأحيان إذا وجدت أدلة في دولة أخرى لا يمكن الحصول عليها حتى مع اتخاذ إجراءات دولية تسهل عملية تبادل تلك الأدلة الإلكترونية، وذلك لأن معظم هذه الإجراءات معقدة، كما أنها ليست عملية إلا عند وقوع إحدى الجرائم الخطيرة والتي حينها يتم استدعاء المعلومات بصورة رسمية من الدول الأخرى.

ثانياً- طبيعة المعلومات والبيانات الإلكترونية ذاتها:

حيث إنها يمكن أن تخضع للمحو أو التغيير بسهولة، لذا يصبح من الضروري جمعها

(110)د. حازم محمد حنفي، مرجع سابق، ص 78.

والتحفظ عليها بسرعة كلما أمكن ذلك، ورغم أن مرور تلك المعلومات والبيانات في الشبكات لا يستغرق إلا أجزاء من الثانية وهي فترة قصيرة جداً، وكذلك حجم تلك المعلومات والبيانات الكبير والمتزايد بشكل لحظي، فإنه يصبح من غير الممكن التحفظ على المعلومات والبيانات لوقت طويل. وبالإضافة لذلك، فإذا ما توافرت فرصة المعرفة والمهارة لدى المجرم، فإنه يقوم بإتلاف الأدلة أو تعديلها أو محوها من أجل الهروب من يد العدالة وتبرئة ساحته من الأدلة التي تدينه.

ثالثاً- نقص الخبرة الفنية حول هذه الشبكات وذلك لتنوعها واختلافها من شبكة لأخرى:

وهو ما يصعب من مهمة الخبير الذي لا يمكن أن يكون ملماً بالتعامل مع جميع أنواع الشبكات واختلافها، وهو ما يتطلب أشخاصاً أكثر يمتلكون الكفاءة للتعامل مع التقنية والحصول منها على الأدلة.

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

فعند القيام بإجراءات التحقيق المختلفة والبحث عن الأدلة، فإن ذلك يتم في كم كبير من المعلومات والبيانات الإلكترونية وهو ما يحتاج لجهد كبير ومهارة عالية([111]). لذا فإن تلك المعلومات والبيانات المستخرجة من شبكات المعلومات، تعتبر من البيانات المتحركة، وتوجد العديد من التطبيقات التي تعمل على تحميل الملفات من الجهاز أو وسيلة تقنية المعلومات إلى الشبكة العالمية للمعلومات، ويمكن من خلالها الحصول على نسخة من تلك المعلومات أو البيانات من قبل أي شخص آخر عن طريق الشبكة ذاتها، ورغم ذلك فإن عضو سلطة التحقيق أو الخبير التقني المنتدب يواجه العديد من الصعوبات عند جمع الأدلة الإلكترونية من شبكات المعلومات، إضافة إلى الصعوبات التي تم ذكرها سابقاً، وتتلخص هذه الصعوبات في الشبكات وإخفاء الهوية، والشبكات وإخفاء المعلومات.

فمن ناحية إخفاء الهوية، فإن عملية جمع الأدلة الجنائية الإلكترونية من مسرح الجريمة تواجه صعوبة أخرى تتمثل في إخفاء المستخدم لهويته، وهو ما يشكل تحدياً أمنياً عندما يتم إخفاء الهوية دون أن يبذل الفاعل في ذلك مجهوداً، فهو يستطيع التخلص من التهمة الموجهة إليه من خلال الادعاء بعدم مسؤوليته عن فعل الإخفاء، وقد يستخدم المجرمون جهداً بسيطاً من الإجراءات لإخفاء هوياتهم من الشبكة لتظل أنشطتهم التي يقومون بها مجهولة الهوية من أجل محاولة الإفلات من إجراءات الاعتقال، ومن هذه الإجراءات التي

(111) د. ممدوح عبد المطلب عبد الحميد، مرجع سابق، ص 120.

يستخدمها المجرمون استخدام جهاز حاسب آلي من مقهى عام للإنترنت، وفي مقابل ذلك توجد العديد من البرامج والتطبيقات المختلفة التي تعمل على إخفاء هوية المستخدم عند دخوله لشبكة المعلومات، وهو ما يزيد من هذه الصعوبة لدى عضو سلطة التحقيق أو الخبير الإلكتروني عند تحليل الأدلة التي تم العثور عليها وتجميعها[112].

أما من ناحية إخفاء المعلومات، فهي صعوبة أخرى تضاف إلى تحديات سلطة التحقيق والخبير الإلكتروني في الجريمة الإلكترونية، وهي تتم من أجل وضع هذه المعلومات المشبوهة أو المخالفة خارج نطاق الاطلاع من الأشخاص وسلطات الضبط والتحقيق، وقد تجتمع هذه الصعوبات في الشبكة بين إخفاء هوية المستخدم والمعلومات أو البيانات، مما يجعل الأمر معقداً وفي غاية الصعوبة لكشف ومعرفة الفاعل في مثل هذه الجرائم، إلا أنه توجد بعض البرامج التي تمكن سلطات التحقيق والخبير الإلكتروني من فك شفرات تلك الصعوبات وتعمل هذه البرامج على استعادة كافة المعلومات والبيانات المخفية في الشبكات منها البرنامج المعروف باسم ماروتوكي Marutukku [113].

وتتنوع البيانات المتحركة المحفوظة على شبكة المعلومات إلى أنواع مختلفة، حيث تختلف أنواع البيانات هذه في طريقة تكوينها وانتشارها وحركتها على الشبكة العالمية للمعلومات، ويمكن أن نعرض أربعة أمثلة مختلفة تبين طبيعة البيانات المتحركة، وذلك على النحو التالي:

1. البريد الإلكتروني:

وهو يعتبر من الخدمات المهمة والإيجابية التي قدمتها الثورة المعلوماتية للمجتمعات، فهو يُعد شكلاً من أشكال التواصل الإلكتروني يسمح لمستخدم الشبكة بتبادل الرسائل النصية بدلاً عن الوسائل التقليدية الورقية، وكأنه صندوق بريدي خاص على شبكة المعلومات، حيث يتيح للمستخدم الدخول له وتفقد الرسائل الواردة إليه وإرسال الرسائل إلى أشخاص آخرين، وقد أصبح من أكثر وسائل التواصل شيوعاً واستخداماً عبر الإنترنت، ونظراً لسهولة استخدامه وعدم وجود ضوابط تحكمه، فإن ذلك أدى إلى وجود الاستخدامات السلبية وغير المشروعة للبريد الإلكتروني مثله مثل باقي الخدمات الأخرى التي تتيحها الشبكة والتقنية المعلوماتية بشكل عام[114]. وكنتيجة لذلك الاستخدام السلبي للبريد الإلكتروني، فقد تم رفع درجة سرية محتواه وما يرد إليه من

(112) د. حازم محمد حنفي، مرجع سابق، ص 82.
(113) المرجع السابق، ص 83.
(114) د. خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية، 2008، ص 90.

رسائل من خلال تشفيره ببرامج خاصة لا تسمح بالاطلاع على أي رسالة فيه إلا لمن يمتلك تلك الشفرة الخاصة به، وهو ما ساعد كذلك على ظهور التوقيع الإلكتروني، حيث يقوم برنامج التصفح للبريد بتخزين توقيع المستخدم على كل رسالة يرسلها بحيث تصبح هي الشفرة الخاصة به[115].

ومع تزايد التطور المعلوماتي وما يلعبه من دور مهم في مختلف مجالات الحياة البشرية، فقد اعترفت التشريعات بحجية هذه المستندات التي تستخدم عبر البريد الإلكتروني شأنها في ذلك شأن المستندات الورقية، وأصبحت كذلك محلاً لجريمة التزوير باعتبارها مستنداً له حجية في الإثبات ويحمل فكراً ويمكن قراءته. ويترتب على اعتبار رسائل البريد الإلكتروني في مرتبة الرسائل الشخصية تزايد الحماية الجنائية لها وتمتعها بذات الحماية التي تتمتع بها الرسائل الورقية، فلا يجوز الاطلاع عليها وعلى ما تحتويه من أسرار إلا وفق الإجراءات والقواعد العامة التي يحددها القانون، وعليه لا يمكن لعضو سلطة التحقيق اختراق البريد الإلكتروني والدخول إلى الأنظمة المخزنة بها رسائل البريد أو ضبطها إلا وفق الإجراءات المنصوص عليها في القوانين الإجرائية الجنائية التي تنظم هذا الأمر[116].

أما المشرع العماني فقد وضع للمراسلات والبرقيات حماية خاصة في قانون الإجراءات الجزائية، حيث نص على أنه: «لا يجوز ضبط المراسلات والبرقيات أو الاطلاع عليها أو ضبط الجرائد والمطبوعات والطرود أو تسجيل الأحاديث التي تجري في مكان خاص أو مراقبة الهاتف أو تسجيل المكالمات بغير إذن من الادعاء العام».

2. بيانات مواقع التواصل الاجتماعي:

وتتنوع هذه المواقع وعددها كبير جداً، ومن أشهرها مواقع Twitter، Facebook، Instagram، حيث إن هذه المواقع تتيح للمستخدم أن يرفع إليها ملفات مختلفة كالصور ومقاطع الفيديو والمستندات والروابط ويسمح بانتشارها على شبكة المعلومات لجميع المستخدمين، ويستطيع في المقابل أن يحملها مستخدم آخر ويحصل على نسخة منها أو يعيد نشرها بكل سهولة، ووفق هذه المميزات أصبحت هذه المواقع وما تحتويه من معلومات وبيانات أخطر أنواع البيانات المتحركة[117]، فهي تمنح المستخدم أن يكون أداة

(115) للمزيد من المعلومات يمكن الرجوع إلى المواقع الرسمية التي تتيح خدمة البريد الإلكتروني، مثل موقع https://www.office.com .

(116) د. علي محمود علي حموده، مرجع سابق، ص 8.

(117) د. حازم محمد حنفي، مرجع سابق، ص 85.

ومصدراً لنشر أية معلومة أو مستند وكأنه قناة إعلامية مستقلة، ويستطيع أن يصل إلى مختلف بقاع الأرض في دقائق معدودة، وهو ما ينتج الاستخدام السلبي لهذه المواقع في نشر الشائعات التي تمس بالمجتمعات والأسر والأشخاص، والترويج للفتن، ونشر الرذيلة عبر الصور والأفلام دون رقيب أو رادع له، والمتتبع لهذه المواقع يدرك مدى خطورتها وما ساهمت به من هدم للمجتمعات والدول بسبب ما ينشر عليها.

3. بيانات المواقع المتخصصة لبث المحتوى المرئي:

وهي نوع من المواقع الأخرى والتي تتيح لمستخدمها رفع ملفاته المصورة على شكل مقاطع مرئية (فيديو)، ورغم تنوعها إلا أن أشهر هذه المواقع على مستوى شبكة المعلومات العالمية هو موقع YouTube، وهو موقع يسمح للمستخدم بنشر ما يشاء من المقاطع المرئية المصورة وفق السياسات والشروط التي يسمح بها الموقع، ويستطيع كل شخص في العالم يمكنه الدخول للموقع مشاهدة تلك المقاطع، ولم تخل هذه المواقع كذلك من إساءة استخدامها من بعض المستخدمين والمجرمين من خلال نشر ما من شأنه زعزعة استقرار البلدان عبر تلفيق المقاطع المصورة، أو الاعتداء على حرمة الحياة الخاصة للأفراد عبر نشر مقاطع فيديو تسيء إليهم. كما أن هناك مواقع أخرى تتيح للمستخدم تصوير المقاطع بشكل مباشر أي أنه ينقل ما يشاء بشكل مباشر لكل الأشخاص الذين يتابعون المستخدم عند بثه، فيستطيع من خلالها المستخدم نقل أي وقائع أو أحداث تجري حوله للآخرين عبر هذه المواقع وكأنه مراسل لإحدى القنوات التلفزيونية.

4. بيانات محفوظة على الشبكة:

وتتمثل هذه البيانات والمعلومات عن طريق الخدمات التي تقدمها بعض المواقع كذلك، فمن خلال هذا الموقع يمكن للشخص أن يحتفظ بما يشاء من بيانات وملفات ورفعها في هذا الموقع ويحصل على كلمة مرور خاصة يمتلكها هو فقط، يستطيع من خلالها الدخول والاطلاع على ملفاته وبياناته التي قام بتخزينها متى ما أراد ذلك، مع إمكانيته إضافة المزيد من الملفات والبيانات كذلك وفق مساحة تخزينية عالية متاحة لكل مستخدم، كما أن الموقع يسمح للمستخدم أن يشارك هذه الملفات لمن يشاء دون كلمة مرور، ويحدد الأشخاص الذين يمكنهم مشاهدة الملفات، فيمكن من خلال هذه الملفات إدارة محتوى معين بين مجموعة من الأشخاص دون القدرة على الحصول أو الاطلاع عليها من الآخرين ودون إذن من المالك لها، وهو ما قد يسيء استخدامها في إدارة محتويات غير مشروعة أو ملفات محظورة وإيصالها إلى الشخص المقصود دون الخوف من انتشارها عبر شبكة المعلومات أو اطلاع الغير عليها دون إذن.

الفرع الثالث

إجراءات الحصول على بروتوكول العنوان الإلكتروني

مع تزايد عدد مستخدمي الشبكة العالمية للمعلومات عبر مختلف المجتمعات الدولية، فإن ذلك الاستخدام الكبير قد يكون في جزء منه إيجابياً ويكون البعض منه سلبياً، أي أن يكون استخدام الشبكة بطريقة خاطئة للخدمات والتطبيقات التي تتضمنها وليست نحو الغاية من توفيرها، وهذه السلوكيات الخاطئة والسلبية قد تؤدي إلى توافر أركان الجريمة بشأنها مما ينتج عنها تزايد في عدد الجرائم المرتكبة عبر شبكة المعلومات، لذا كان لزاماً على المشرع الحد من هذه الجرائم ومكافحة هذه الظاهرة الإجرامية المتطورة، عبر وضع مجموعة من الأسس والضوابط والحلول الأمنية التي تساعد على مكافحتها وتقليل نسبة ارتكابها ورفع نسبة اكتشافها ومعرفة مرتكبيها بأفضل وأنجع الأساليب لتحقيق تلك الغاية.

وضمن أهم الأسس والحلول التي تم وضعها في هذا المجال تحديد عنوان إلكتروني لكل جهاز يتصل بشبكة المعلومات، سواء أكان هذا الاتصال صادراً من حاسب آلي أم هاتف نقال أو جهاز لوحي أو غيرها من الأجهزة، حيث يتم وضع عنوان إلكتروني لكل جهاز مهما كان نوعه أو طبيعته ويتوفر به اتصال بالشبكة العالمية للمعلومات، ويطلق على هذا العنوان ببروتوكول العنوان الإلكتروني واختصاراً يعرف بـ (IP).

ويقصد ببروتوكول العنوان الإلكتروني حزمة من القواعد والمعايير متعددة (بروتوكولات)[118] مرتبطة مع بعضها البعض وتعمل على تحقيق توافق تقني لازم لإنجاح عمليات الاتصال الإلكتروني ما بين أجهزة إلكترونية مختلفة الأنظمة والخواص، وجاءت تسميتها من مصطلح Protocol Internet /Protocol Control Transmission وتختصر بـ IP/TCP، ويرجع تاريخ هذا البروتوكول إلى أوائل السبعينيات عندما تبنت تمويله وزارة الدفاع الأمريكية كمشروع بالتعاون مع جامعة كاليفورنيا الأمريكية، لقيامها بتصميم نظام اتصال إلكتروني يعتمد على اللامركزية في إدارته، بحيث إنه عند وجود عطل في المركز الرئيسي للاتصال لا يصيب ذلك الشبكة بشكل كامل. فعندما كانت وزارة الدفاع تحتاج إلى ربط جميع وحدات الجيش الأمريكي التي كانت تعمل باستخدام شبكة خاصة لكل وحدة منها في نقل البيانات، تحت إدارة مركز رئيسي واحد، ظهرت مشكلات عدم التوافقية بين مختلف هذه الوحدات، كما كانت تتعطل جميعاً

(118) يقصد بالبروتوكولات بنية تصميمية تحدد مجموعة من الأنظمة المستخدمة للاتصال بشبكات الحاسب الآلي والتي تقوم عليها شبكة الإنترنت العالمية، حيث تؤمن التوافقية بين بروتوكولات الحزمة المختلفة والشبكات المختلفة في أرجاء العالم مع بعضها البعض.

عند استهداف المركز الرئيسي لها أثناء الحروب أو الكوارث، وبسبب ذلك المشروع الممول تم بناء شبكات ضخمة بدون وجود مركز رئيسي لها للتحكم أو الإدارة، وتعمل هذه الشبكات أوتوماتيكياً للاتصال بالشبكة إذا ما حدث لها أي عطل أو توقف[119].

أما دور سلطة التحقيق والخبير الإلكتروني في هذا الأمر فهو يكون عند وقوع الجريمة والبحث عن مرتكبها، حيث تختلف طريقة الحصول على العنوان الإلكتروني IP حسب نوع الجريمة المرتكبة، وحسب الموقع الذي تم ارتكاب الجريمة من خلاله، فعند وجود شكوى حول رسالة في البريد الإلكتروني تحتوي على سب أو تهديد، فهنا يتم فحص البريد الإلكتروني للمجني عليه والرسالة الواردة محل الجريمة ومعرفة الـ IP الخاص بالشخص المرسل، ومن ثم يتم مخاطبة الشركة التي يتبعها رقم العنوان الإلكتروني IP للحصول على بيانات المستخدم مرسل الرسالة.

(119) د. حازم محمد حنفي، مرجع سابق، ص 87.

الخاتمة

سعت الدراسة إلى توضيح مفهوم الدليل الإلكتروني وخصائصه وما ينعكس من تلك الخصائص على إجراءات جمعه بالطرق التقليدية لجمع الدليل الجنائي، وقد توصلت إلى نتائج وتوصيات:

أولاً- النتائج:

1. للجريمة الإلكترونية طبيعة خاصة تميزها عن مختلف الجرائم، سواء من حيث الوسائل التي ترتكب بها، أو من حيث المحل الذي تقع عليه، وكذلك من حيث الجناة الذين يرتكبونها، ولهذه الطبيعة الخاصة العديد من الآثار والصعوبات على المجال القانوني سواء في شقه التجريمي أو الإجرائي.
2. تحتاج الجريمة الإلكترونية إلى خبرة فنية لدى سلطات الاستدلال والتحقيق والقضاء، حيث تتطلب هذه الجريمة إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات ووسائل التقنية الحديثة، من أجل ملاحقة مرتكبيها أو التحقيق فيها، وهو ما يشكل عائقاً في إثبات الجريمة الإلكترونية نتيجة نقص الخبرة.
3. للدليل المادي دور رئيسي في كشف الجريمة ومعرفة فاعلها، إلا أنه في ضوء تغير أبعاد الجريمة وتميزها بسمات خاصة وأنماط جديدة، فإنه يصبح من الضروري أن يتغير تبعاً لذلك أسلوب اكتشافها وطريقة إثباتها، لذا لا يمكن اتباع الإجراءات التقليدية وحدها لمواجهة الجرائم الإلكترونية، حيث إنها لا تكون مجدية في كثير من الأحيان، لما تثيره من إشكاليات نتيجة طبيعتها غير المادية وما تنتجه من أدلة غير ملموسة.
4. الدليل الإلكتروني هو نوع متميز عن الأدلة الأخرى، فهو ليس ضمن الأدلة المادية لكونه دليلاً غير ملموس وليس له وجود مادي خارجي يمكن لمسه باليد والتعامل معه وتحليله بشكل مادي، كما أنه ليس من الأدلة المعنوية التي يكون مصدرها الأشخاص، وليس كذلك من الأدلة القولية التي يمكن الاستناد إليها بمجرد سماعها، فهو دليلاً غير مرئي عبارة عن مجال كهرومغناطيسي مخزن في نظام حاسوبي على شكل ثنائي وبطريقة غير منظمة.
5. تفتيش أجهزة ووسائل تقنية المعلومات الحديثة من أخطر المراحل عند اتخاذ الإجراءات الجزائية في الجريمة الإلكترونية وغيرها من الجرائم التي تتضمن دليلاً إلكترونياً؛ لاعتبار أن محل التفتيش هو جهاز الحاسب الآلي أو الشبكات أو وسائل

تقنية المعلومات، محل جدل فقهي واسع ومتزايد وخاصة فيما يتعلق بتفتيش المكونات المعنوية لتلك الأجهزة والوسائل، فهي لا وجود لماديتها وإنما هي بيانات ومعلومات رقمية.

6. عدم تمكن القائمين على التفتيش من الحصول على بيانات المشترك أو المستخدم لأحد المواقع، يتوجب عليهم طلبها واستئذان الموقع ذاته للحصول على هذه البيانات وفق الشروط وسياسة الخصوصية التي يحددها الموقع، ولا يمكن الوصول إليها عن طريق الاتفاقيات والمعاهدات الدولية؛ لأنها بيانات يمتلكها القائمون على الموقع نفسه، ولا يمكن للدول أن تجبر هذه المواقع على الإدلاء ببيانات مشتركيها.

7. لابد من تأهيل القائمين على إجراءات الاستدلال والتحقيق وتعليمهم علوم الحاسب الآلي وتقنية المعلومات، وكيفية التعامل مع الأجهزة الإلكترونية المختلفة، عند القيام بإجراءات الاستدلالات والتحقيق في الجرائم الإلكترونية، فغياب الخبرة عن السلطات القائمة على هذه الإجراءات تغدو عاجزة عن فك شفرات الجريمة وكشفها، فلا يمكنها جمع الأدلة الجنائية التي تثبتها بسبب جهلها في هذا التخصص، وقد تدمر أو تمحو تلك الأدلة عند التعامل معها.

8. التزام الشاهد المعلوماتي هو التزام بالإدلاء عن معلومات تخص الجريمة الواقعة وما يعلمه من معلومات عنها وعن فاعلها، وليس التزاماً بالإدلاء عن معلومات تخص النظام محل الجريمة.

9. إجراء التحفظ السريع على البيانات هو من الإجراءات الحديثة التي لم تكن موجودة من قبل، بل إنه يعتبر من الإجراءات الحديثة غير المنصوص عليها في العديد من التشريعات حتى الوقت الحالي.

10. يتم وضع عنوان إلكتروني لكل جهاز مهما كان نوعه أو طبيعته عند اتصاله بالشبكة العالمية للمعلومات، ويطلق على هذه العنوان بروتوكول العنوان الإلكتروني ويعرف اختصاراً بـ IP.

ثانياً- التوصيات:

من خلال استعراض النتائج سالفة الذكر أعلاه، تم التوصل للتوصيات التالية، التي تندرج في إطار آليات عمل السلطات الأمنية والقضائية في إثبات الجريمة الإلكترونية، وهي:

1. إنشاء أقسام متخصصة بالجرائم الإلكترونية في قيادات ومراكز الشرطة بالمحافظات والولايات المختلفة، كونها أول من يتلقى البلاغات حول هذه الجرائم،

وتأهيل كادر متخصص من مأموري الضبط القضائي وتزويدهم بأحدث الأجهزة للقيام بإجراءات الاستدلال في هذه الجرائم؛ وذلك للطبيعة الخاصة بأدلة هذه الجرائم وسهولة تدميرها ومحوها في وقت قياسي.

2. تأهيل أعضاء الادعاء العام القائمين على الإدارات التخصصية بقضايا تقنية المعلومات والتحقيق في الجريمة الإلكترونية، من خلال دورات وبرامج عملية في مجال تقنية المعلومات.

3. تفعيل التعاون الإقليمي والدولي في مجال مكافحة الجرائم الإلكترونية، والوصول إلى العناوين الإلكترونية للمستخدمين بإجراءات أكثر سهولة، ودون تعقيدات وإجراءات مطولة، حيث يساهم ذلك في مكافحة الجريمة الإلكترونية والوصول إلى مرتكبيها، وتخفيف آثارها على المجتمعات والأفراد المتضررين من هذه الجرائم.

4. تفعيل القضاء المتخصص في مجال الجرائم الإلكترونية، من خلال تأهيل القضاة وتدريبهم وتخصصيهم لنظر القضايا الإلكترونية؛ ليكونوا قادرين على مناقشة الأدلة الإلكترونية المقدمة في الدعوى مع أطراف الدعوى من المجالين العلمي والتقني لها، كما يمكنهم ذلك من تقدير التقارير المقدمة من الخبراء وتكوين قناعاتهم بشكل سليم مستند على المعرفة والاطلاع على ما يقدم أمامهم من أدلة، وما يقدم من دفوع ومذكرات وآراء حول موضوع الدعوى.

5. تضمين المناهج الدراسية بمختلف مستوياتها، وعلى وجه الخصوص المناهج القانونية، بما يتعلق بالجانب القانوني لأجهزة ووسائل تقنية المعلومات بما يواكب التطور العلمي والحاجة العملية لها.

المراجع:

- إبراهيم عيد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية، القاهرة، 2000.
- د. أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، 2006.
- د. أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015.
- أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2016.
- د. أشرف عبدالقادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.
- د. أمين مصطفى محمد، حماية الشهود في قانون الإجراءات الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.
- هلالي عبد اللاه أحمد:
  - التزام الشاهد بالإعلام في الجريمة المعلوماتية: دراسة مقارنة، دار النهضة العربية، القاهرة، 2000.
  - تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.
- د. هشام محمد فريد رستم:
  - قانون العقوبات «مخاطر تقنية المعلومات»، مكتبة الآلات الحديثة بأسيوط، مصر، 1992.
  - الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية، القاهرة، 1994.
- د. حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017.
- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009.
- د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار الفكر العربي، القاهرة، 1988.
- د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004.

- د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005.
- د. محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
- د. محمد محي الدين عوض، حقوق الإنسان في الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1995.
- د. محمد يحيى مطر، مسائل الإثبات في القضايا المدنية والتجارية، الدار الجامعية، بيروت، 1989.
- د. محمود نجيب حسني:
  - شرح قانون العقوبات– القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1982.
  - شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 1998.
- مزهر جعفر عبيد:
  - شرح قانون الإجراءات الجزائية العماني، الجزء الأول، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2008.
  - شرح قانون الإجراءات الجزائية العماني، الجزء الثاني، الطبعة الأولى، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2014.
- د. ممدوح عبدالحميد عبدالمطلب، أدلة الصور الرقمية و في الجرائم عبر الكمبيوتر، مركز بحوث الشرطة، الشارقة، 2005.
- د. نجاتي سيد أحمد سند، مبادئ الإجراءات الجنائية في التشريع المصري، الجزء الأول، كلية الحقوق، جامعة الزقازيق، القاهرة، 2008.
- د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.
- د. عادل عزام سقف الحيط، جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية: دراسة مقارنة، دار الثقافة، مصر، 2011.
- د. عبد الرزاق السنهوري، الوسيط في شرح القانون المدني الجديد، الجزء الثاني، دار النهضة العربية، القاهرة، 1968.
- د. عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، 2007.
- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة: دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.

- د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت: دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، عمان–الأردن، 2004.
- د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي– المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، 2008.
- د. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة: دراسة مقارنة، الطبعة الأولى، مكتبة دار الثقافة للنشر والتوزيع، عمان– الأردن، 1999.
- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016.
- د. فتحي محمد أنور عزت:
  - الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، الإسكندرية، 2010.
  - الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثانية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، القاهرة، 2010.
  - ضوابط التدليل في الأحكام الجنائية، المجلد الأول، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2010.
- د. صالح بن علي الحراصي، الإثبات الإلكتروني في القضاء والتحكيم التجاري، الطبعة الأولى، مركز الغندور، القاهرة، 2016.
- د. صلاح محمد أحمد دياب، الحماية القانونية لحياة العامل الخاصة وضماناتها في ظل التكنولوجيا الحديثة، دار الكتب القانونية ودار شتات، الإمارات العربية، 2010.
- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية: دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، 2013.
- د. شيماء عبدالغني محمد، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.
- د. توفيق حسن فرج، قواعد الإثبات في المواد المدنية والتجارية، دون ناشر، القاهرة، 1981.
- د. خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية (الإنترنت): دراسة مقارنة، مطبعة الصفوة، القاهرة، 2014.
- د. خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية، 2008.

المحتوى: