"الأدلة الإلكترونية من الناحيتين القانونية والتقنية"
دراسة تحليلية مقارنة

إعداد الفريق البحثي:

أحمد حمو علاء عواد ولاء عبد الله

2015

قائمة المحتويات

1. المقدمة:

الإثبات هو الأساس الذي يبنى عليه أي ملف تحقيقي، ويبدأ هذا الأساس منذ وقوع الجريمة ويستمر حتى صدور الحكم، فعندما تبدأ الضابطة العدلية بأولى مراحل التحقيق، فإنها تستند في عملها إلى بينات وأدلة، فلا يمكن أن يتم تحويل الملف إلى النيابة العامة وهي لا تملك السندات والأدلة القانونية لذلك، كما أنه، وتتمة لهذا العمل التحقيقي، تقوم النيابة العامة بتكملة الأدلة والبحث عن أدلة جديدة في المرحلة ذاتها، حيث لا يمكن أن تقوم بإيداع لائحة اتّهام في قلم المحكمة من غير استنادها إلى أدلة قوية قد تؤدي إلى إدانة المتهم. وأيضاً، وانطلاقا من الدور التكاملي للملف، فعندما يحين دور القاضي، فإنه يقوم بتقييم الأدلة وترشيحها والحكم استناداً إليها انطلاقاً من وجوبية تسبيب الحكم.

بسبب الأهمية الخاصة للأدلة في التحقيق، يتوجب مواكبة تطورها جنباً إلى جنب مع التشريعات النافذة، ومن هنا تكمن أهمية هذه الدراسة التي تعنى بالأدلة الحديثة، لاسيما الأدلة الإلكترونية. وعليه، يتوجب على الباحثين بيان الطبيعة التقنية للأدلة الإلكترونية، وتسليط الضوء على ماهية الدليل الإلكتروني من هذه الناحية.

لا يمكن التعمق في دراسة الجانب التقني للدليل الإلكتروني من غير توضيح معمق لماهية الدليل الإلكتروني من الناحية القانونية، وهذا ما سوف تعمل على توضيحه الدراسة. هذا إلى جانب العمل على معرفة الدليل الإلكتروني من الناحيتين التقنية والقانونية اللتين ستنصبان على ممارسات عملية يتم التعامل معها في مراحل البحث وجمع الاستدلالات، ومرحلة التحقيق الابتدائي، وصولاً إلى عرض الدليل الإلكتروني على المحكمة.

تهدف الدراسة إلى معرفة الإطارين العلمي والقانوني للأدلة الإلكترونية، من خلال قراءة شاملة ومعمقة للمنظومة القانونية محل الدراسة، وتقديم اقتراحات وحلول للثغرات القانونية من أجل تطورها لتوائم الواقع ومتطلباته. كما تهدف إلى إيجاد مقارنة واضحة ما بين الواقع والقانون فيما يتعلق بالدليل الإلكتروني.

تكمن إشكالية الدراسة في تحديد مدى مواءمة التشريعات المحلية مع موضوع الأدلة الإلكترونية، وسيتم اتباع المنهج الوصفي التحليلي من خلال توضيح القواعد العامة في الإثبات، وسكبها على الأدلة الإلكترونية، كما سيعتمد على المنهج المقارن في بعض الأجزاء لإثراء الدراسة بتجارب عربية أو أجنبية سباقة في هذا المجال.

وعليه، سيتم تقسيم الدراسة إلى ثلاثة محاور رئيسية، يتناول المحور الأول فيها الطبيعة التقنية للأدلة الإلكترونية، من خلال تعريف الدليل الإلكتروني من ناحية تقنية، وجمعه وتوثيقه وتحليله، أما المحور الثاني فيتطرق إلى الطبيعة القانونية للأدلة الإلكترونية، من خلال تحديد معنى الدليل الإلكتروني من الناحية القانونية، وتحديد موقف المشرع من خصوصية الأدلة الإلكترونية ومدى حجيتها في الإثبات، أما المحور الثالث فيستعرض علاقة الأدلة الإلكترونية بجرائم الفساد، وكيف يمكن الأخذ بحجية الدليل الإلكتروني في مرحلة جمع الاستدلالات ومرحلة التحقيق الابتدائي وصولاً إلى مرحلة المحاكمة.

2. الدليل الإلكتروني – نظرة تقنية

سيتم التطرق في هذا المحور إلى الدليل الإلكتروني من الناحية التقنية، وفهم جوانبه الفنية التي تساهم في فهم ماهيته وحدوده. في القسم الأول، سيتم التفريق بين الدليل من الناحية الفيزيائية والناحية الإلكترونية، وفهم العلاقة بينهما، وربط ذلك بالتحقيق الجنائي التقليدي. بعدها سيتم التطرق إلى أهم نظريات تفسير الأدلة والأسس التي يبنى عليها التحقيق الجنائي الإلكتروني. أما القسم الثاني، فسيستعرض منهجيات التعامل مع الأدلة الإلكترونية وعرض منهجية مبسطة لتحصيل الدليل الإلكتروني، وفي القسم الثالث سيتم التطرق للبرمجيات والأدوات التي يتم استخدامها في التحقيق الجنائي الإلكتروني، حيث سيتم وضع المعايير لقبولها وبيان أصنافها، ومن ثم استعراض أهم تلك البرمجيات والأدوات.

1.2 مدخل إلى الدليل الإلكتروني وصوره

إن الدليل هو الأداة التي يستعين بها القاضي لمعرفة وقائع الدعوى، وبها يبني قناعته. وطبيعة الدليل تختلف باختلاف الوسائل التي تم استخدامها في ارتكاب المخالفة القانونية موضوع الدعوى، ولا بد أن يسبق عرض الأدلة أمام القاضي القيام بالتحقيق الجنائي الذي يعمل على تحضير الأدلة وتوثيقها ليتم عرضها والأخذ بها في المحكمة.

الدليل الإلكتروني محل الدراسة لا يخرج عن هذا المنهج، فالتساؤلات التي تدور حول التحقيق الجنائي الإلكتروني هي كيف يتم نشوء الدليل والأثر الإلكتروني؟ وكيف يتم إيجاده والتعرف عليه؟ وكيف يتم حفظه وعرضه أمام المحكمة؟

يُعرَّف الدليل الرقمي بأنه "الدليل المأخوذ من أجهزة الكمبيوتر، ويكون على شكل مجالات أو نبضات مغناطيسية وكهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجيا المعلومات، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة، أو الصور، أو الأصوات، أو الأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون وتطبيقه".[1]

[1] ممدوح عبد الحميد. **البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت**، القاهرة: دار الكتب القانونية، 2000، ص88.

وكذلك يعرف الدليل الرقمي بأنه "الأثر الذي يبنى على البيانات المخزنة بالحواسيب، أو يتم نقله بواسطتها، والذي يثبت أو ينفي وقوع جريمة ما".[2]

1.1.2 الآثار الفيزيائية والرقمية

التعريفات السابقة للدليل الإلكتروني تلزمنا التمييز بين الأثر الفيزيائي والأثر الإلكتروني (الرقمي) للبيانات في الحواسيب، فالآثار الفيزيائية تكون موجودة على القرص الصلب على شكل كهرومغناطيسي، أو موجودة بشكل مؤقت في ترانزستورات الذاكرة المؤقتة، أو موجودة في الأطياف الكهرومغناطيسية في الكوابل، وهي لا يمكن رؤيتها من قبل المحققين. أما الآثار الإلكترونية، فهي عبارة عن تفسير لهذه الآثار الفيزيائية بواسطة أدوات وبرمجيات خاصة.

يبيّن الشكل التالي العلاقة بين الآثار الفيزيائية والرقمية:

شكل 1: العلاقة بين الآثار الفيزيائية والرقمية

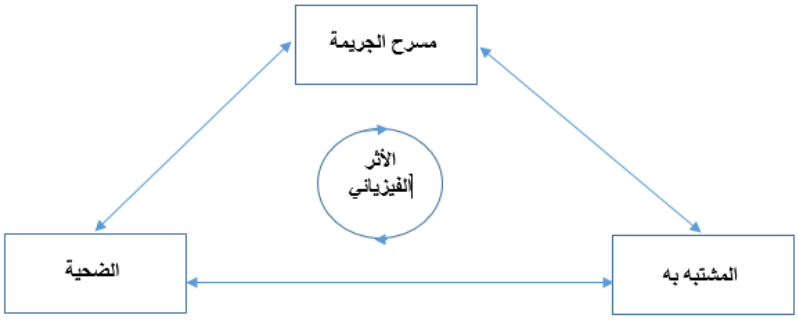
نلاحظ من الشكل السابق أن الأثر الفيزيائي لا يمكن رؤيته بشكل مباشر، كما توجد مستويات عدة لتفسيره، وبالتالي حدوث خطأ في التفسير يُعد أمراً وارداً في أي مرحلة من هذه المراحل، وينشأ هنا تساؤل: كيف يمكن للخبير المحقق أن يتعرف على التفسيرات الخاطئة؟

[2] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence and computer crime*, page 7.

يمكن أن يحصل خطأ في التفسير الفيزيائي للأثر؛ مثلاً عند تفسير البت في أحد هذه المستويات السابقة بطريقة مختلفة تؤدي إلى فهم مختلف، فمثلاً لو قام شخص ما بتغيير اسم ونوع أحد الملفات التي تحتوي على صورة ممنوعة كملف نصي، وظهرت أمام المحقق كملف نصي، يحصل هنا خطأ في التفسير للوهلة الأولى، لذا لا بد من استخدام أدوات خاصة تحلل الملف على المستوى الأدنى كما سيأتي لاحقاً.

- **مبدأ لوكارد**[3]

قام الطبيب الفرنسي أدموند لوكارد بوضع أسس التحقيق الجنائي التقليدي من خلال مبدأه الذي يعرف باسمه، والذي عرف بمبدأ التبادل أيضاً. ويبين هذا المبدأ العلاقة بين مسرح الجريمة والجاني والمجني عليه من جهة، والأثر الفيزيائي المادي من جهة أخرى كما هو مبين في الشكل التالي:



شكل 2: الأثر الفيزيائي يربط المتهم بالضحية في مسرح الجريمة

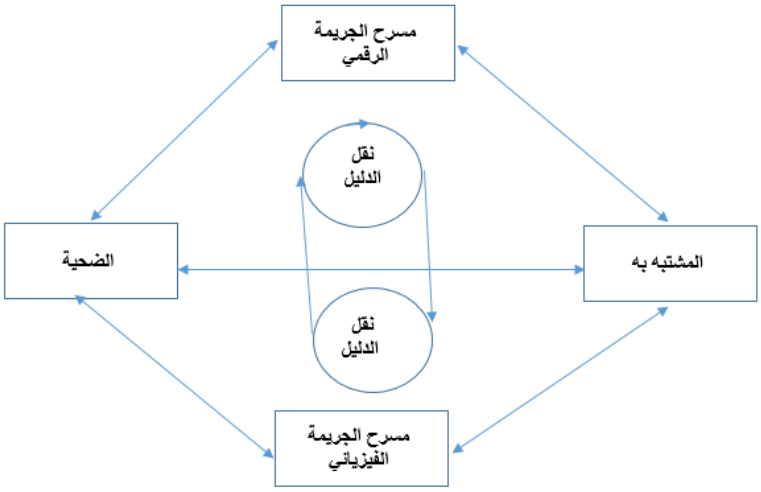
ينص هذا المبدأ على أنه في حالة حدوث اتصال بين عنصرين يحدث بينهما تبادل بشكل حتمي، فلا بد لكل من يكون في مسرح الجريمة أن يأخذ معه شيئاً أو يترك خلفه أثراً،[4] فهو ينطبق على أي تواصل يحدث في مسرح الجريمة، بين المتهم والضحية، أو بين الأشخاص ومسرح الجريمة.

فهل ينطبق هذا المبدأ على الدليل والأثر الإلكتروني؟ يشير كاسي في المصدر السابق إلى أنه في الجرائم الإلكترونية ينطبق هذا المبدأ، ليس فقط في الركن المادي للجريمة الإلكترونية، كلوحة المفاتيح حيث يترك بصماته مثلاً، وإنما يحدث انتقال بين الدليل المادي والإلكتروني كما يوضح شكل 3. هذا يعني أنه يحصل تعاون بين البعدين التقليدي، أي المادي، والإلكتروني في التحقيق الجنائي وبالتالي

[3] http://en.wikipedia.org/wiki/Locard%27s_exchange_principle.

[4] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence* and computer crime, 16.

فإن وسائل التحقيق التقليدية تعمل بشكل مشترك مع وسائل التحقيق الرقمية في فهم الجرائم الإلكترونية وتحليلها.



شكل 3: نقل الدليل بين البعدين المادي والإلكتروني

2.1.2 خصائص الأدلة الإلكترونية

هناك نوعان من الآثار التي يتم إنشاؤها من قبل البرمجيات المختلفة من حيث القصد في بنائها، الأول يتم إنشاؤه بشكل متعمد من قبل نظام التشغيل وبرامج العمل المختلفة، فمثلاً تنتج أنظمة التشغيل بشكل دائم ما يسمى "اللوج فايل"[5] الذي يدون بيانات كاملة عن كل برنامج أو إجراء يتم تنفيذه في بيئة نظام التشغيل، يتم مثلاً تسجيل اسم الإجراء، ومن قام بتنفيذه، ووقت التنفيذ، والمعوقات أثناء التنفيذ، ونتيجة التنفيذ، أو غيرها من المعلومات الواصفة. أما النوع الثاني من الآثار، فيتم إنشاؤها بشكل غير مقصود، وفي الغالب دون علم من قام بإنشائها بوجودها. ويحتاج الوصول إلى هذه الآثار أدوات وخبرات خاصة، فمثلاً الملفات التي يتم حذفها عن النظام، والتي تتم استعادتها بعد ذلك من قبل الخبراء، تمثل هذا النوع الثاني من الآثار.

إن دور المحقق الجنائي هو تتبع هذه الآثار، ولاسيما النوع الثاني، حيث يظهر بها القصد في الجرم عن طريق محاولة إخفاء الدليل، ويمكن لهذه الآثار أن تخفى أو تتلف بشكل معتمد أو غير متعمد، حيث يمكن لمجرم محترف أن يستخدم وسائل تكنولوجية متقدمة تخفي هذه الآثار بالكامل، كما يمكن لمحقق جنائي مبتدئ أو ذي خبرة قليلة أن يتلف هذه الأدلة أثناء عملية التحقيق الجنائي، وبالتالي يصعب نسبتها لشخص معين.

[5] Operating system log file.

من ميزات الدليل الإلكتروني أنه، وإن أمكن إتلافه بسهولة، فإنه يتم استرجاعه، حيث أن الملفات المحذوفة تبقي لمدة طويلة بحالة يمكن استردادها، وهذا يؤكد مبدأ لوكارد السابق، بأن الأثر الإلكتروني لا يمكن إخفاؤه بالكامل.

من القواعد المهمة في التعامل مع الأدلة والآثار الإلكترونية، أنه لا يجوز أن يتم الفحص على النسخة الأصلية للدليل، حيث يتم عمل نسخة طبق الأصل باستخدام أدوات خاصة، وترك النسخ الأصلية لفحص أي تغير يمكن أن يكون طرأ على الدليل أثناء عملية التحليل والمعالجة.

من الصعوبات التي تواجه المحقق الإلكتروني، بشكل رئيسي، حجم البيانات الضخمة التي يتعامل معها المحقق، حيث أن عليه فصل البيانات غير المهمة عن البيانات المهمة بالتحقيق، وكذلك التفسير الصحيح للملفات قيد البحث، إضافة إلى ذلك الخبرة المختصة بإعداد النسخة طبق الأصل عن الدليل وحفظها من الذاكرة المؤقتة للأجهزة، واستخدام برمجيات آمنة لا تترك آثاراً جديدة أو تعدل آثاراً موجودة.

3.1.2 درجات اليقين في التحليل الإلكتروني

تحليل الدليل الإلكتروني يتطلب التفسير للآثار الإلكترونية وتقييمها، وهو يشكل القاعدة الأساسية للاستنتاجات فيما بعد.[6] ويطلب من خبراء التحقيق الإلكتروني أن يقدروا ويصفوا درجة اليقين في استنتاجاتهم، لتمكين المحققين فيما بعد من وضع القيمة الحقيقية للدليل الذي تم تقديمه من قبلهم. ولا يمتلك التحقيق الإلكتروني معادلات رياضية واضحة تعطي التقديرات السابقة قيماً قطعية، وإنما تعتمد قوة الدليل على خبرة المحققين الذين لا يعملون بالغالب تبعاً لمنهجية واحدة. كما أن تعقيد قضايا الجرائم الإلكترونية وتفرعها يضيفان صعوبة أخرى في سبيل الوصول إلى قطعية التحليل.

يوضح المثال التالي المتغيرات في المشاهدات، وكيفية حصول التفسيرات المختلفة:[7]

2009-04-03 02:38:10 W3SVC1 10.10.10.50 GET /images/snakeoil3.jpg—80—
192.168.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0

[6] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence and computer crime*, 68.

[7] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence and computer crime*, 69.

هذا المثال يبين تسجيلة أخذت من اللوج فايل لأحد أجهزة خوادم الإنترنت.

يمكن لأحد الخبراء أن يدعي أن جهاز الخادم هذا تمت زيارته بتاريخ 3-4-2009 الساعة 2 و38 دقيقة و10 ثوان من قبل جهاز رقم بروتوكول الإنترنت خاصته آنذاك، هو 192.186.1.1. ويتم تدوين ذلك في ملف القضية. وقد يكون من الممكن أن جريمة اختراق لهذا الخادم قد حصلت في تلك الأثناء.

يمكن لخبير آخر ذي خبرة أعلى أن يقوم بفحص حيثيات أخرى قبل إطلاق الحكم والتفسير، فقد يفحص التوقيت ونوعه والمنطقة الجغرافية التي يتبعها جهاز الخادم، فإن كان هناك فرق بضع ثوانٍ لساعة الخادم عن ساعة المحقق، فإنه يتم التشكيك بحصول الاختراق في هذا الوقت، وقد يتبع الخادم نظام توقيت آخر، كأن يكون فرق التوقيت يزيد ساعة أو ساعتين عن توقيت المحققين، فإن ذلك يعطي مزيد من الشك في حصول الاختراق في ذلك الوقت.

إن درجة اليقين في هذا المثال تعتمد على هذه المتغيرات ومتغيرات أخرى وكيفية تفسيرها من قبل الخبراء المختلفين.

يقترح ايجون كاسي على خبراء القضايا الإلكترونية أن يتبعوا سلم الدرجات التالية لكل مشاهدة وعنصر من عناصر الدليل الإلكتروني عند فحصه وتقييمه كما يلي:[8]

جدول 1: درجات اليقين في الدليل الرقمي

التأهيل	الوصف	درجة اليقين
خاطئ	الدليل يتعارض مع الحقائق المعروفة	c0
غير أكيد بشكل كبير	الدليل تثار تساؤلات كثيرة حوله	c1
غير أكيد نوعاً ما	تم تأكيده من قبل دليل واحد غير محمي ضد التزوير	c2
ممكن	مصادر الأدلة يصعب تزويرها، ولكنها لا تدعم الادّعاء	c3
مرجّح	الدليل محمي من التزوير، ولكن توجد مصادر أخرى مستقلة للدليل يمكن تزويرها	c4
مرجّح بالأغلب	اتفاق على الدليل من مصادر مستقلة عدة غير قابلة للتزوير، ولكن يوجد	c5

[8] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence and computer crime*, 71.

	عدم تأكد بسبب ظهور خطأ لحظي أو ضياع بعض الأدلة	
أكيد	الدليل لا يمكن تزويره وغير قابل للنقاش	c6

فمثلاً، عند التحقق من ملف وجد في حاسوب متهم بحيازة صور مخالفة للقانون، وتم فحص قيمة "الهاش" له ومطابقتها بالدليل المقدم للمحكمة، واحتواء هذا الملف على المادة الممنوعة، يستطيع الخبير أن يعطيه درجة أكيد.

2.2 التحقيق الجنائي الإلكتروني ومنهجية التعامل مع الدليل الإلكتروني

يهدف التحقيق الجنائي، بشكل رئيسي، إلى كشف الحقيقة وعرضها أمام المحكمة، ولا يختلف الجرم الإلكتروني عن الجرم بمفهومه التقليدي هنا، فقد تتوقف عليه إدانة شخص ما ومعاقبته، لذلك لا بد من اعتماد منهجية وأدوات موثوقة في تحليل وتفسير الأدلة التي يتم التعامل معها، كذلك لا بد أن تكون هذه المنهجية قد تمت تجربتها وتأكيد فعاليتها وموضوعيتها وشفافيتها.[9]

يوجد هناك العديد من المنهجيات التي تتعامل مع الدليل الإلكتروني من حيث جمعه وتوثيقه وعرضه، وعليه ستعرض الدراسة أهم المراحل المشتركة بين هذه المنهجيات، كما ستقوم قبل ذلك باستعراض أهداف التحقيق الإلكتروني، وبيان خصائص المنهجية المطلوبة في التحقيق، وفي النهاية سيتم عرض منهجية (تأمين، تحليل، عرض)،[10] التي تلخص أهم الخطوات الضرورية للتعامل مع الدليل الإلكتروني.

1.2.2 أهداف التحقيق الإلكتروني

بعد اتباع المنهجية الصحيحة في التحقيق، يهدف التحقيق الجنائي الإلكتروني، عند حصول اختراق أو تعدٍ إلكتروني، إلى تحقيق الأهداف التالية:[11]

- معرفة أدوات الاختراق ونقاط الضعف في النظام التي قد تكون السبب في حصول الاختراق.

[9] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence and computer crime*, 187.

[10] Alexander Geschonneck (2011). *Computer-Forensik, Computerstraftaten erkennen, ermit-teln, aufklären*, page 68.

[11] Alexander Geschonneck 2011, page 65.

- بيان حجم الخسائر والتخريب بسبب الاختراق.
- تحديد هوية المخترق والمكان الذي انطلق منه الاختراق.
- تأمين الأدلة الإلكترونية من أجل البدء في الإجراءات القضائية.

2.2.2 خصائص منهجية التحقيق الإلكتروني

لكي يتمكن المحقق الجنائي من عرض أدلته بقوة، وأن يتم قبول هذه الأدلة، لا بد أن تلقى هذه المنهجية والآلية القبول من المحكمة، أو من تعهد إليه ليقوم بذلك، فعلى المحقق أن يراعي بمنهاجيته النقاط التالية:[12]

- **القبول:** على المحقق أن يستخدم الأدوات والآليات المعروفة لدى أصحاب الاختصاص التي قد تم فحص نجاعتها في السابق، ويفضل أن يكون محقق سابق ذو خبرة وشهرة قد استعمل هذه الأدوات، لكن إن قرر المحقق أن يستخدم أدوات غير معروفة، يمكنه ذلك بالطبع، ولكن سيخضع لكثير من الاستجواب والتبرير عن سبب استخدام هذه الأدوات.
- **المصداقية:** لا بد أن تكون آلية العمل ذات مصداقية وقابلة للصمود أمام أي استفسار حولها.
- **التكرار:** لا بد أن تكون المنهجية قابلة للتكرار، وبالتالي يمكن لأي محقق آخر، باتّباع الخطوات ذاتها، الحصول على النتائج نفسها.
- **سلامة الدليل:** يجب أن تحرص الآلية على حفظ الدليل وتوفير إمكانية تتبع الخطوات التي استعملت عليه ونتائجها.
- **السبب والمسبب:** لا بد أن تكون المنهجية لديها المقدرة على الربط بين الأشخاص والآثار والنتائج التي يتم التوصل إليها من خلال التحقيق.
- **التوثيق:** لا بد للمنهجية أن تراعي توثيق جميع خطوات العمل على الأدلة بشكل مفصل وخطوات متلاحقة.

3.2.2 منهجيات التعامل مع الدليل الإلكتروني

لقد تم تطوير العديد من المنهجيات للتعامل مع الأدلة الإلكترونية التي كانت تحرص على خدمة عملية التحقيق وإرشادها، ولم تكن شروطاً إجبارية عليها. ومن المعروف أن عمليات التحقيق تختلف باختلاف الواقعة قيد البحث، لذلك كان لا بد لهذه المنهجيات أن تكون عامة وقابلة للتطبيق على مختلف القضايا الإلكترونية.

[12] Alexander Geschonneck, 2011, page 66.

لقد تمت دراسة هذه المنهجيات ومقارنتها بشكل مفصل بدراسات سابقة.[13] وقد اقترح كاسي في ختام دراسته النموذج كما في شكل 4، وعليه سيكتفى هنا بذكر الخطوات المشتركة بين هذه المنهجيات، وسيتم لاحقاً عرض منهجية (تأمين، تحليل، عرض)،[14] التي تلخص أهم الخطوات الضرورية للتعامل مع الدليل الإلكتروني.

تشترك هذه المنهجيات المختلفة في المراحل التالية:

- التحضير.
- المسح والتحديد.
- الحفظ.
- الفحص والتحليل.
- العرض.

شكل 4: نموذج كاسي المقترح للتحقيق الإلكتروني[15]

[13] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence* and computer crime, page 189 figure 6.1.

[14] Alexander Geschonneck 2011, page 68.

[15] Eoghan Casey, Susan W. Brenner (2011). *Digital evidence* and computer crime, 193.

- **منهجية (تأمين، تحليل، عرض)**

تتميز هذه المنهجية من بين المنهجيات السابقة بالبساطة والعموم، ما يجعل تطبيقها من الناحية العملية أمر يسير. وتكمن بساطة هذه المنهجية بسبب قيامها على ثلاث خطوات واضحة أثناء عملية التحقيق، كما أن عموم الخطوات يقلل من القيود التي توضع على المحقق الإلكتروني.

تقوم منهجية (S-A-P)[16] على ثلاث مراحل في التعامل مع الدليل، وهي:

- توثيق الدليل الإلكتروني وتأمينه (Secure).
- تحليل الدليل الإلكتروني (Analyze).
- عرض الدليل الإلكتروني (Present).

1. توثيق الدليل الإلكتروني وتأمينه

يعتبر التوثيق من المراحل الدقيقة والمهمة في كل خطوة من خطوات جمع الدليل وتحليله، وهناك طرق عدة للقيام بالتوثيق، لعل من أهمها وأنجعها الطريقة التقليدية باستخدام الورق والقلم، حيث أنه يصعب تزويرها كما هو الحال في الملفات الإلكترونية. وهناك بعض البرمجيات الخاصة التي تساعد في عملية التوثيق، لكن من الضروري توثيق استخدامها أيضاً، كما يتم استخدام التصوير وتسجيلات الفيديو في عملية التوثيق.

يمكن الجمع بين الوسائل السابقة، ولكن لا بد من التوقيع على كل صفحة وملف، وإعطاء أرقام تسلسلية لها أثناء عملية التوثيق من أجل ضمان المصداقية، ويشترط البعض وجود شهود أثناء عملية التوثيق هذه، وضرورة توقيع الشهود عليها جميعها.

وتنبعث أهمية التوثيق لكل مرحلة من ضرورة فهم الآخرين لما تم أثناء عملية جمع الدليل ومعالجته، إضافة إلى بيان وعرض كيف يمكن إنتاج هذه المستخلصات مرة أخرى، وبالعادة يتم وضع بروتوكول يمكّن الخبراء الذين سيعاينون النتائج لاحقاً من متابعة الخطوات المدونة به والنتائج المتوقعة لكل خطوة.

[16] Secure-Analyze-Present

تبدأ هنا مرحلة التحضير لعملية الجمع، حيث توضع الأهداف لما يراد جمعه ودراسته، ويتم وصف عملية الجمع بشكل دقيق، بحيث لا يتم إهمال أو ضياع عنصر من عناصر الدليل، كذلك يتم التركيز على موضوع الخصوصية للبيانات التي يتم جمعها، حيث لا بد من مراعاة القوانين والإجراءات المتعلقة بخصوصيات الأفراد، ولاسيما تلك التي ليس لها مكان في التحقق الإلكتروني.

إن عدم اتباع هذه المعايير في هذه المرحلة يجعل الدليل بأكمله في موضع شك. ويتم بعد ذلك حفظ الدليل من خلال سلسلة من الخطوات المعيارية، يتم التأكد من خلالها أن الدليل لا يمكن تغييره بعد الآن. وكذلك يتم حفظ وحماية البيئة التي تحتضن الدليل لمنع الدخول إليه أو الاتصال به من خلال حماية فيزيائية، باستخدام القاصة مثلاً، كذلك استخدام أدوات حماية الشبكات التي تمنع الوصول لهذه الأجهزة والأدلة، وتتم هنا تعبئة نماذج خاصة بكل دليل ومكان وجوده، كما يتم كذلك التفريق بين الدليل الذي يتم حفظه في حالة أن الأجهزة كانت في حالة عمل أو كانت مغلقة.

2. تحليل الدليل الإلكتروني

من الضروري في هذه المرحلة بدء العمل على نسخة طبق الأصل من الدليل، وليس النسخة الأصلية التي تبقى للمراجعة فيما بعد، حيث تبدأ هذه المرحلة بفصل البيانات غير الضرورية لعملية التفتيش، وذلك لوجود أعداد ضخمة من المواد في الأجهزة المتحفظ عليها، التي تحتاج دراستها واحدة تلو الأخرى إلى عشرات السنين إن فحصت جميعها. ويتم في البداية فصل ما هو ضروري عما هو غير ضروري للقضية موضع البحث، كذلك يتم الفصل حسب أماكن تواجد الأدلة تبعاً لطبيعة القضية قيد البحث، فمثلاً إن كان البحث يقتضي إيجاد صور تحتوي على مواد ممنوعة يتم التركيز فقط على الملفات من نوع صورة، ويتم استثناء غيرها.

يبين الجدول التالي مواضع البحث التقليدية وأنواع الملفات والأدلة التي يتم تحريها لجريمة غسل وتزوير أموال تم استخدام الحواسيب من قبل المتهمين بها.

جدول رقم 2: نطاق التفتيش للأدلة في جريمة غسل وتزوير أموال

Address books	دفاتر العناوين
Calendar	التقويم
Currency images	صور العملات
Check and money order images	صور الشيكات والأموال
Customer information	معلومات العملاء

Databases	قواعد البيانات
notes and letters،E-mails	رسائل البريد الإلكتروني والمذكرات والرسائل
False identification	انتحالات الشخصية
Financial asset records	سجلات الأصول المالية
Images of signatures	صور التوقيعات
Internet activity logs	سجلات نشاطات الإنترنت
On-line banking software	برمجيات البنوك على الإنترنت
Counterfeit currency images	صور العملة المزيفة
Bank logs	سجلات البنك
Credit card numbers	أرقام بطاقات الائتمان

تتم بعد ذلك عملية البحث عن الملفات التي تم حذفها من الأجهزة أو أجزاء منها وإعادة تركيبها، وتتم محاولة بناء فرضيات حول ما حصل ومتى حصل من خلال هذه الملفات، حيث أن تاريخ الملف ومحتواه يساعدان في معرفة تسلسل الأحداث.

يتم بعد ذلك إجراء بعض التجارب على هذه الأدلة، ومعرفة ما إذا تم إنتاجها من قبل نظام يعمل بشكل صحيح ومستقر أم أنه تم وضعها على النظام من خلال عملية اختراق أو بفعل فايروس معين مثلاً، وهل تم استغلال ثغرة أمنية موجودة في النظام أم تم إنتاج الدليل بطريقة متعمدة. وتتم مقارنة ما تم التنبؤ به بما تم إيجاده والوصول إلى التحليل الصحيح. ويتضح هنا أنه تم استخدام الطريقة العلمية في البحث من مشاهدة وتنبؤ واستنتاج من أجل الوصول إلى الفهم الصحيح حول حقيقة ما حصل.

3. عرض الدليل الإلكتروني

مرحلة العرض هي المرحلة النهائية في الإثبات أو النفي للأدلة الإلكترونية التي تمت معالجتها في مراحل التحقيق. ويتوقف نجاح هذه المرحلة بالدرجة الأولى على مصداقية الخبير الذي قام بهذه العملية في كيفية عرضه للأدلة وثقته بما يعرض وعدم وجود تناقص أو غموض في شهادته، كذلك يلعب ملف التوثيق الذي قام بإعداده دوراً كبيراً، حيث يتم فحص مدى التزامه بالمهنية والدقة والقيام بالإجراءات المعروفة والمتفق عليها في هذا المجال. ولا بد من التركيز حين عرض الأدلة على الدقة ومخاطبة الآخرين حسب درجة معرفتهم التقنية، فمثلاً يتم تحضير وعرض دليل مفصل للخبراء التقنيين ومن يهتم بذلك، أما أمام القضاء والادّعاء، فلا بد من عرض النتائج والملخصات وسلسلة الإجراءات التي تمت في تحليل الدليل دون التعمق في التفاصيل الجزئية.

وعليه، يتضح أن الصعوبات التي تواجه الشاهد الخبير هو عدم وجود الخبرة التقنية للجمهور في المحكمة، على عكس ما تم توثيقه من أدلة تقنية تفصيلية، وكذلك إمكانية فحص عمله من قبل خبراء تقنيين آخرين يمكن أن يطعنوا في بعض الإجراءات التي قام بها أو أهمل بعضها.

3.2 برمجيات وأدوات معالجة الأدلة الإلكترونية

في السابق، كان يعتمد الخبير الجنائي الرقمي على برمجيات يقوم هو، في أغلب الأحيان، بكتابتها وتطويرها. وتتميز هذه البرمجيات بكونها آمنة ومجربة من قبله، وتفي بالغرض الذي يقوم به. إلا أن هذه البرامج، ومع تطور التقنيات والبرمجيات، أصبحت أقل فاعلية وأقل قبولاً لدى الأوساط القانونية، ولاسيما أنها تحتاج إلى مدة أطول لتحضير التقرير الجنائي بالشكل المطلوب.

ظهرت، فيما بعد، برمجيات تجارية وأخرى من قبل مراكز بحثية وأكاديمية أكثر فاعلية، ولاسيما أنها تستطيع القيام بغالبية العمليات المطلوبة على الدليل من حفظ وتحليل وإعداد التقرير النهائي في الوقت نفسه، وخلال فترة زمنية قصيرة.

وأصبح قبول هذه البرمجيات أمام المحكمة يعتمد على شروط لا بد من توفرها حتى يتم قبول الدليل الذي تم الحصول عليه وتحليله.

1.3.2 شروط قبول أدوات وبرمجيات معالجة الدليل الإلكتروني[17]

تتميز الخصائص الواجب توفرها في أدوات الحصول على الأدلة الإلكترونية وتحليلها حتى يتم اعتمادها أمام المحكمة بأنها:

1. يمكن تعريفها وتوضيحها بدقة: من الضروري في أي عملية من عمليات التحقيق الجنائي، أن يتم تعريف وتحديد الكيفية التي تعمل بها الأداة المستخدمة، إضافة إلى الهدف المرجو الوصول إليه منها، لذلك لا بد من عرض المشكلة، بشكل واضح، وتفصيل المخرجات المتوقعة بعد إتمامها، ومن ثم بيان آلية وخطوات العمل للأداة، وفي النهاية لا بد من تبني معايير لقياس وتقييم الإجراء المتبع، وبهذا يتم فهم –والتأكد من– أن الأداة المتبعة في معالجة الدليل تقوم بعمل واضح ومحدد بطريقة معرّفة ومحددة.

[17] Larry E. Daniel (2012). *Digital Forensics for Legal Professionals*, page 33.

2. يمكن التنبؤ بمخرجاتها: لا بد من معرفة المهام التي تقوم بها الأداة المستخدمة، فإن تعذر التنبؤ والمعرفة السابقة للمخرجات المطلوب القيام بها، فإن الأداة تعتبر غير مقبولة. فمثلاً؛ من أجل البحث عن نصوص معينة داخل ملفات تم حفظها لغاية التحقيق، لا بد من المعرفة السابقة أن هذه الأداة تعرض الملف الذي وجد فيه النص، إضافة إلى موضع النص في الملف، فإن قامت الأداة، عوضاً عن ذلك، بتجميع الملفات التي تحتوي على النص، وتغيير موقعها في جهاز الحاسوب، فإن هذه الأداة تعتبر غير مقبولة.
3. يمكن تكرارها: من الضروري أن تستطيع الأداة المستخدمة ضمن الظروف نفسها إعطاء النتيجة نفسها في حال تكرار العملية مرة أخرى، وضمن مقدار مقبول من الخطأ يتم السماح به.[18]
4. يمكن التأكد من صحتها: من الشروط المهمة للأداة المتبعة في التحقيق أن يتم التأكد من صدق وصحة النتائج التي يتم التوصل إليها بواسطتها، ليس في بيئة فحص مخصصة لذلك فحسب، وإنما من خلال مقارنة النتائج باستخدام أدوات أخرى تستخدم للغرض نفسه.

فمثلاً، لو تم استخدام أحد المحققين أدوات التحقيق الجنائي المعروفة (EnCase)، واستخدم محقق آخر برمجيات التحقيق (Forensic Tool Kit)، فهل يتوقع الحصول على النتيجة نفسها؟ إن لم يحصل ذلك، لا بد من إثارة السؤال: هل حصل خطأ من قبل البرمجيات المستخدمة أم من قبل المحققين؟ بالعادة يحصل الخطأ من قبل المحققين في تفسير الدليل كما تم التعرض له في بداية الدراسة.

2.3.2 تصنيف برمجيات معالجة الأدلة الإلكترونية:

عند التعامل مع أدوات وبرمجيات التحقيق الجنائي الرقمي، لا بد من فهم ومراعات الأبعاد التالية لهذه البرمجيات:

1. الجهة التي أصدرتها

- جهة تجارية: برمجيات يتم شراؤها من قبل شركات تجارية، وتكون قد خضعت للفحص بشكل كبير قبل البدء بإنتاجها.
- برمجيات مفتوحة المصدر: برمجيات يتم تطويرها بالعادة في معاهد تعليمية أو على يد مبرمجين مستقلين، وتكون مجانية في أغلب الأحيان. لا تخضع هذه البرمجيات لمعايير

[18] Larry E. Daniel (2012). Digital Forensics for Legal Professionals, page 35

الفحص نفسها كما هو الحال في البرمجيات التجارية، ولكنها تتميز بكونها قابلة للتحقق والفحص وفهم آلية عملها من داخلها، بسبب توفر نص البرمجيات التي كتبت بها.

2. نطاق الاستخدام

- تطبيقات شاملة لمراحل التحقيق كافة: تتميز هذه البرمجيات بكونها قادرة على القيام بمعالجة الدليل الإلكتروني من مرحلة التبليغ عن وقوع الجريمة لغاية عرض الدليل أمام المحكمة، مروراً بجمعه وحفظه وتحليله وتوثيقه وإنتاج تقريره. وتحتاج هذه البرمجيات إلى تدريب واسع ومفصل من قبل الشركات المنتجة قبل البدء باستخدامها، وفي كثير من الأحيان يتطلب استخدام هذه البرمجيات الحصول على شهادة دولية معترف بها بعد اجتياز الاختبارات والفحوصات النظرية والعملية اللازمة.

  ومن الأمثلة على هذه البرمجيات:

  - EnCase (Guidance Software Corporation).
  - FTK Forensic Tool Kit (Access Data Corporation).
  - iLook LEO and iLookPI (Perlustro Corporation).
  - SMART (ASR Data, Data Acquisition and Analysis, LLC).

- تطبيقات تقوم بعمل واحد فقط: تقوم هذه البرمجيات بفحص محدد للدليل، وفي مرحلة محددة، وتكون أقل تعقيداً من البرمجيات السابقة. ومن الأمثلة على هذه البرمجيات واستخداماتها:
  - **برمجيات إعداد نسخة طبق الأصل للدليل:** إن نسخ الملفات لغرض التحقيق الجنائي يختلف كلياً عن النسخ الاعتيادي عن طريق أدوات أنظمة التشغيل الاعتيادية، فالنسخ هنا يتطلب نسخاً على مستوى البت كما هو موضح في الشكل 1. وتوجد هنا العديد من الأدوات المجانية مثل (dd) ومشتقاتها، حيث تقوم بهذا العمل في بيئات أنظمة التشغيل المختلفة، بعد ذلك يتم إنشاء الهاش (hash) الخاص بكل ملف يراد حفظه كدليل، حيث يعمل كهوية تثبت حقيقة الملف، ويتم بناء هذا الهاش من جزء من محتوى الملف إضافة إلى الوقت والتاريخ على جهاز الحاسوب، ما يتعذر إشراكه مع ملف آخر، والهاش يستعمل لاحقاً للتأكد من مصداقية الدليل، وأنه لم يطاله تغيير خلال فترة التحقيق، كما تتوفر كذلك برمجيات مجانية لذلك مثل (md5)، من البرمجيات التجارية التي تقوم بذلك (Encase) و(ProDiscover).
  - **برمجيات استعادة الملفات المحذوفة:** إن حذف البيانات من الكمبيوتر لا يعني بالضرورة محوها نهائياً، بحيث لا يمكن استعادتها. وتتوفر العديد من البرمجيات التي تحتاج إلى بعض الخبرة حتى تتم استعادة الملفات المحذوفة، وإن سبق أن تم إجراء

عملية تهيئة للقرص الصلب (format) قبل ذلك. ومن هذه البرمجيات (Recuva) و (Undelete 360).[19]

- **المحررات السادس عشرية:** يمكن الاطلاع بواسطة هذه المحررات على الملف بشكله الثنائي، أي المستوى القريب من القرص الصلب كما هو موضح في الشكل 1. ويستطيع الخبير بواسطتها تحليل الملف ومعرفة نوعه وطبيعة البيانات التي يحتويها. ومن أشهر البرامج لهذه الفئة برنامج (WinHex) و(Gander).
- **برمجيات استعادة كلمات السر:** يلجأ الكثير من الأشخاص والمؤسسات إلى حماية بياناتهم عن طريق تشفيرها وحمايتها بواسطة كلمات السر، كذلك يلجأ الكثيرون إلى حماية أجهزتهم الحاسوبية باستخدام كلمات مرور. ويحتاج المحقق إلى الخبرة وإلى البرمجيات المتنوعة التي تمكنه من استعادة كلمات السر أو تغيير كلمات المرور حتى يستطيع الدخول إلى النظام والملفات، وتختلف هذه البرمجيات باختلاف نوع الملفات التي تم تشفيرها. فللاطلاع على ملفات تم إنشاؤها ببرمجيات مايكروسوفت أوفس مثلاً، يوجد برمجيات مثل (Office Recovery)، لاستعادة كلمات المرور من ملفات تم إنشاؤها بواسطة برمجيات أدوبي أكروبات، كما توجد برامج مثل (Advanced PDF Password Recovery).
- **برمجيات تتبع الشبكة:** عند حصول اختراق للحاسوب باستخدام الشبكة الداخلية أو شبكة الإنترنت العالمية، يمكن تتبع مصدر الاختراق باستخدام برمجيات خاصة، ويتوفر العديد من هذه الأدوات والبرمجيات بشكل مجاني ضمن أنظمة التشغيل مثل (Tracert)، وكذلك يتوفر العديد من البرمجيات التجارية التي تعطي معلومات إضافية مثل (Visualroute) التي تظهر خارطة العالم وتتتبع سير الاتصال عبر الخوادم المختلفة في العالم وصولاً إلى مصدر الاختراق، حيث تعطي هذه البرمجيات العنوان الشبكي (IP Address) الذي تم الاختراق بواسطته، ومزود الخدمة (Internet Provider) لشبكة الحاسوب الخاصة به.

[19] http://www.techradar.com/news/software/applications/best-free-recovery-software-1141256
تم الاطلاع عليها في: 2013/12/20.

3. طبيعة الأدوات المستخدمة لجمع الدليل الإلكتروني

- **برمجيات (Software) لنسخ الأدلة:** ومن الأمثلة على ذلك:

- Linen (Guidance Software Corporation)
- FTK Imager (Access Data Corporation)
- Forensic Replicator (Paraben Corporation)

- **عتاد (Hardware) جمع الأدلة:** يأتي هذا النوع من الأدوات على شكل عتاد لحماية الأدلة عند القيام بنسخها (write-blocker) كما تم الإشارة إليه سابقاً. ومن أشهر الأدوات التي تقوم بذلك:

- Tableau
- Logicube
- Weibetech
- Intelligent Computer Solutions
- Voom Technologies

ويبين الشكل التالي كيف يتم ربط هذه الأدوات مع وسائل التخزين عند النسخ.

شكل 5: أدوات حفظ الدليل أثناء النسخ.

3. الطبيعة القانونية للأدلة الإلكترونية

إن محور اهتمام القانونين ينصب على كيفية إيصال الحق لصاحبه، وحتى يكون لهذا الحق قيمة من المنطلق القانوني، فلا بد لصاحبه أن يثبته، فالحق المجرد من أي وسيلة إثبات هو حقاً دون أي قيمة، ومن هنا تبرز أهمية وجود وسائل لإثبات الحق.

لقد كان موضوع إقامة الدليل، منذ الأزل، محل انشغال الكثيرين، حتى أمست هناك أنظمة مختلفة تنظم موضوع الإثبات، فهناك نظام الإثبات الحر الذي بمقتضاه لا يتم تحديد وسائل الإثبات سواء للخصوم أو للقاضي، بحيث يقوم القاضي بإصدار حكمه بناءً على قناعته الشخصية، وليس من خلال الاحتكام لوسائل معينة. وهناك نظام معاكس تماماً للنظام الحر، ويسمى النظام المقيد، ويعني هذا النظام تقيّد الخصوم والقضاة بوسائل محددة لا يجوز تناول غيرها في الإثبات، وإلا وقع الحكم باطلاً، وعليه لا يحق للقاضي أن يستند في حكمه إلى دليل مخالف لما نص عليه المشرع، مدعياً بعلمه الشخصي، فهذا النظام جرد القاضي من أي دور إيجابي. وأخيراً، ولتفادي مساوئ كلا النظامين، ظهر هناك نظام وسطي يسمى بالنظام التوفيقي أو المختلط، حيث يدمج بين النظام المقيد والنظام الحر.[20] ولعل المشرع الفلسطيني أخذ بالنظام التوفيقي في قانون البينات الفلسطيني رقم (4) لسنة 2001،[21] وفي النظام الحر في الإثبات الجزائي كما سيوضح في البحث.

وعليه، فإثبات الحق يكون من خلال وسائل قانونية معينة كالكتابة، والشهادة، وغيرهما من الأدلة التقليدية المتعارف عليها، وفي ظل الثورة العلمية وأثرها على جميع مجالات الحياة، فإن هذا الأثر طال أيضاً أدلة الإثبات، لتفرض هذه الثورة أدلة جديدة لم تكن بالحسبان وهي الأدلة الإلكترونية.

---

[20] عباس العبودي. **شرح أحكام قانون البينات**، عمان: دار الثقافة للنشر والتوزيع، 2005، ط1، 26-29.

[21] وأستند بذلك إلى أنه أخذ بالنظام المقيد تارة وبالنظام الحر تارة أخرى من خلال مواده وخير مثال على ذلك :

نصت المادة (1) من قانون البينات الفلسطيني رقم 4 لسنة 2001 على: "لا يجوز للقاضي أن يحكم بعلمه الشخصي"، وهذا يعني أن المشرع في هذه المادة أخذ بالنظام المقيد.

ونصت المادة (80) من القانون ذاته على: "1- للمحكمة من تلقاء نفسها أن تأمر بالإثبات بشهادة الشهود في الأحوال التي يجيز القانون فيها الإثبات بالشهادة متى رأت في ذلك فائدة للحقيقة. 2- يكون للمحكمة في جميع الأحوال كلما أمرت بالإثبات بشهادة الشهود أن تستدعي للشهادة من ترى لزوماً لسماع شهادته إظهاراً للحقيقة". وهذا دلالة الدور الإيجابي للقاضي؛ أي الأخذ بالمذهب الحر في هذه المادة.

وبناءً على ما تقدم، فإن البحث قدماً في الأدلة الإلكترونية يتطلب –بلا أدنى شك– تسليط الضوء على الإطار أو الطبيعة القانونية للدليل الإلكتروني، ويكون ذلك بشرحٍ وافٍ لمفهوم الدليل الإلكتروني من الناحية القانونية، وذلك من خلال طرحه في القسم الأول من هذا المحور، كما سيتم التعريف من وجهة نظر الفقه القانوني في القسم الثاني، الأمر الذي يستدعي معه بيان موقف المشرع من هذه المسألة، ولاسيما أنها حديثة على التشريعات إلى حدٍّ ما. أما القسم الثالث، فيتضمن حجية وقوة الدليل الإلكتروني في الإثبات، وذلك بالضرورة يكون مع طرح أدلة عملية من قاعات المحاكم مع فرد خصوصية معينة لقضايا الفساد.

1.3 ماهية الدليل الإلكتروني وأهميته من الناحية القانونية

يقصد بالدليل –لغة– المرشد وما يستند به، ويقصد به، أيضاً، البرهان والحجة، [22] أما عن الدليل قانوناً، فهو إقامة البيّنة والبرهان والحجة على شخص أمام القضاء ووفقاً لإحكام القانون على واقعة قانونية متنازع عليها بين الخصوم.[23] هذا التعريف متعلق بالدليل التقليدي، أما الدليل الإلكتروني، فهو وإن كان متشابهاً في الغاية، فإنه مختلف في المضمون، حيث أن المقصود بالدليل الإلكتروني، ذلك الدليل الذي يتم الحصول عليه من الأجهزة الإلكترونية، ويكون في شكل مجالات نبضات مغناطيسية أو كهربائية، يتم تحليلها بأساليب معينة، وينتج عن ذلك تبيان نصوص مكتوبة أو صور أو أشكال معينة يتم ربطها بين الجريمة والجاني والمجني عليه، كل ذلك بطرق لا تتعارض وأحكام القانون.[24]

كما أن هناك العديد من التعريفات التي انصبت على الأدلة الإلكترونية، فمنها أن الدليل الإلكتروني هو "الدليل الذي يجد أساساً له في العالم الافتراضي ويقود إلى الجريمة، فهو كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني، بحيث تمكن الحاسوب من إنجاز مهمة ما". كما عرف أيضاً بأنه "ذلك الشيء الذي يتم الحصول عليه بواسطة التقنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنت والأجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصالات، من خلال إجراءات قانونية، لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة".[25]

---

[22] إبراهيم مصطفى وآخرون : المعجم الوسيط، ط3، مجمع اللغة العربية . القاهرة،سنة 1998، ج 1، 294 .

[23] مفلح عواد القضاة، البينات في المواد المدنية والتجارية،جمعية عمال المطابع التعاونية،ط1,عمان,1990. 23

[24] ممدوح عبد الحميد عبد المطلب، مرجع سابق، 88 .

[25] أبو حجيلة، مادة تدريبية حول الأدلة الإلكترونية، دورة قانونية، جامعة بير زيت – معهد الحقوق، 20-2013/10/21 .

ونظراً لتمايز الدليل الإلكتروني على الدليل التقليدي، فهناك العديد من الخصائص التي ينفرد بها الدليل الإلكتروني بسبب طبيعته المغايرة، أبرزها أن الدليل الإلكتروني غير ملموس، فهو دليل غير مادي، لا يمكن إدراكه بالحواس العادية، وإنما يتطلب فهمه وإدراكه الاستعانة بالأجهزة الإلكترونية، كما أنه دليل يمكن نسخة بصورة متطابقة للأصل لأكثر من مرة بالقيمة العلمية نفسها، والقوة في الإثبات نفسها، كما يمكن محوها وإرجاعها بسهوله، وبالتالي يصعب التخلص من الدليل الإلكتروني بصورة نهائية، وغيرها من الخصائص.[26]

وفي معرض هذا القول، يمكن أن نقسم الدليل الإلكتروني إلى قسمين: قسم يتعلق بالدليل الإلكتروني الذي أعد خصيصاً ليكون دليلاً مثل سجلات الهاتف والفواتير والبطاقات البنكية ورسائل البريد الإلكترونية، وهناك قسم آخر يتعلق بالدليل الذي لم يعد أصلاً ليكون كذلك، بحيث تنشأ بدون إرادة فاعلها، ومن أهم الأمثلة على ذلك البصمة الإلكترونية.[27]

ذُكر، آنفاً، أن الثورة العلمية المستمرة أضفت بظلالها على جميع مجالات الحياة، بما فيها أدلة الإثبات، ولكي تتم مواكبة هذه الثورة، لا بد من ضرورة وجود آلية لاعتماد مثل تلك الأدلة، وتنبع هذه الضرورة الملحة من أهمية تلك الأدلة من حيث كونها تسهّل عملية الوصول إلى الحقيقة بشكل أسرع من الأدلة التقليدية، هذا من ناحية، ومن ناحية أخرى، فهناك حاجة لتقبل مثل هذه الأدلة لأنها فرضت على الواقع العملي والقانوني، فهناك العديد من الجرائم التي ترتكب ولا تثبت إلا بوسيلة إلكترونية، ومثال على ذلك رفع السرية المصرفية في جرائم الفساد، بحيث يمكن إثبات جريمة الاختلاس على أحد الموظفين من خلال الكشوف البنكية الخاصة بحسابه المصرفي. وحتى في الجرائم العادية التقليدية كجريمة السب، والقذف، والتحقير عبر أجهزة الحاسوب، فيمكن إثباتها من خلال استخراج سجل المحادثات عبر جهاز الحاسوب.

ولما كانت الأدلة الإلكترونية ذات أهمية لا يمكن تجاهلها، فلا بد من وجود أثر وموقف تشريعي يتماشى مع متطلبات الثورة العلمية، حتى نكون أمام إجراءات قانونية سليمة وممنهجة، وعليه سيتم التطرق إلى موقف المشرع من الأدلة الإلكترونية.

---

[26] أبو حجيلة، مرجع سابق.

[27] المرجع السابق.

2.3 موقف المشرع من الأدلة الإلكترونية

ذُكرت، سابقاً، اتجاهات الفقه القانوني فيما يتعلق بأدلة الإثبات، وبيَّنا موقف المشرع الفلسطيني الذي أخذ بالاتجاه التوفيقي في الإثبات، لكن هذا الأمر يتطلب معه بيان موقفه من الأدلة الإلكترونية.

إن المشرع الفلسطيني كان متأخراً في هذه المسألة، بحيث أنه لم يواكب الثورة العلمية إلا في القليل من النصوص، وحتى في ظل عدم وجود منظومة قانونية متكاملة، كانت تلك النصوص مع وقف التنفيذ – إن جاز التعبير– وعليه سيتم توضيح الأدلة الإلكترونية الحديثة التي تم ذكرها في التشريع الفلسطيني، مثل التلكس، والفاكس، والبريد الإلكتروني، ولا بد من تبيان الأدلة الإلكترونية التي لم يتداركها التشريع الفلسطيني، محدثاً بذلك فراغاً تشريعياً لا يمكن تداركه، وهناك أيضاً وسائل إلكترونية تم تنظيمها في مشاريع قانونية لم تدخل حيز التنفيذ.

1.2.3 الوسائل الحديثة المنظمة في القوانين الفلسطينية

نصت المادة 2/19 من قانون البيّنات الفلسطيني رقم 4 لسنة 2001 على ما يلي:

"تكون للبرقيات ومكاتبات التلكس والفاكس والبريد الإلكتروني هذه القوة أيضاً،[28] إذا كان أصلها المودع في مكتب التصدير موقعاً عليها من مرسلها، وتعتبر البرقيات مطابقة لأصلها حتى يقوم الدليل على عكس ذلك". وهذا أيضاً مشابه –إلى حد ما– لما هو الحال عليه في قانون البيّنات الأردني وفي المادة 13.

- **التلكس (Telex–massages)**، ويعني وسيلة اتصال بين شخصين عن طريق امتلاكهما الجهاز ذاته لكل شخص من خلال رموز أو أحرف أو أرقام تصل لهما بثوانٍ وسرعة عالية، حيث يقوم بتحويل المعلومات إلى نبضات كهربائية تصل بصيغة الحروف المرسلة.[29]
  ويشترط في التلكس حتى يؤخذ به كدليل إثبات وفقاً للنص المذكور أن يكون أصلها لا يزال موجوداً في مكتب التصدير، وأن يكون موقعاً عليها من قبل مرسلها، وأن لا يتم إثبات المعارضة للأصل.
- **الفاكس (Fax–massages)**،[30] وهو جهاز مقترن بالهاتف يتم عن طريقه نقل المعلومات الموجودة في سند ما طبقاً للأصل، بسرعة 30 ثانية على الأكثر، وعند وصول الفاكس يتم

[28] أي لها قيمة السند العرفي ذاتها للرسائل المنصوص عليها في الفقرة الأولى من المادة ذاتها.

[29] عباس العبودي، مرجع سابق، 256.

إشعار المرسل بعلم الوصول.[31] ويشترط فيه الشروط ذاتها الموجودة في التلكس من توقيع وكتابة ووجود القبول بعدم المعارضة بالأصل.

- "**البريد الإلكتروني (E-mail massages)**، وهو وسيلة الاتصال العصرية، حيث يتم بموجبها تبادل الرسائل بين طرفين، أحدهما مرسل والآخر مستقبل، من خلال عنوان لكل منهما.[32] ويتمثل البريد الإلكتروني لأي شخص في صفحة بـ "شبكة الإنترنت".[33]

وحتى يعتد بالمستندات أو المعلومات الواردة في البريد الإلكتروني أو الأدلة السابقة، يجب توافر شروط معينة سوف يتم التطرق إليها في البند الثالث.

لعل المشرع الفلسطيني خيراً فعل عندما أخضع الوسائل السابقة لمزيد من الأطر القانونية المحيطة في الجوانب العملية له، وبخاصة في ظل التسارع الهائل لانتشار استخدام الوسائل السابقة بشكل يومي ومستمر. إلا أن هذا لا يكفي، حيث أننا بحاجة إلى منظومة قانونية متكاملة تستند إلى بعضها البعض لسد هذا الفراغ التشريعي. وفي معرض هذا القول، وجنباً إلى جنب مع موقف المشرع الفلسطيني في تبني نظام الإثبات الحر في القضايا الجزائية، نجد أنه وفي حال ورد الدليل على واقعة ما، مثل تمكن النيابة العامة من الحصول على سجلات مودعة في حساب البريد الإلكتروني الخاص بالمتهم تثبت تورطه في جرائم غسل أموال، وبصورة لا تدع مجالاً للشك، فإن القاضي من الممكن، وبصورة مطمئنة، إصدار حكم بالإدانة طالما لم يقدم المتهم أدلة دفاعية تنفي التهم المنسوبة إليه.[34]

أيضاً، نصت المادة 1 من القرار بقانون رقم 9 لسنة 2007 بشأن مكافحة غسل الأموال، حيث وفي إطار تعريف الأموال، تم ذكر أن السندات القانونية الإلكترونية والرقمية تعتبر من الأموال، فلو أثبت وجود سندات إلكترونية تدل على الاشتباه بوقوع جريمة غسل الأموال، وتم إثبات ذلك بتلك السندات، فهنا يكون الحكم قد استند إلى دليل إلكتروني.

---

[30] ويشار إليها بالرمز التالي (facsimile transmit transmission) (fax) وتعني نقل وإرسال نسخة. عباس العبودي، المرجع السابق، 253.

[31] عباس العبودي، مرجع سابق، 253.

[32] عباس العبودي، مرجع سابق، 259.

[33] تعرف شبكة الإنترنت بأنها: "شبكة حاسب موسعة عالمية ضخمة جداً، تربط بين عشرات الآلاف من شبكات وأجهزة الحاسب في مختلف أنحاء العالم"، وهذا الاسم مشتق من International Network أو (الشبكة العالمية). على الرابط التالي- مع العلم أنه لم يدون في الموقع اسم الكاتب:

Visited on 15-11-2013 at 09:22 pm http://groups.google.com/group/ali_alsaher34

[34] أبو حجيلة، مرجع سابق.

2.2.3 الوسائل الحديثة غير المنظمة في التشريعات الفلسطينية

بسبب الفراغ التشريعي، أصبح القضاء محل عجز في مواجهة الإشكاليات المتعلقة بوسائل الإثبات حديثة النشأة، وبخاصة في حلول السندات المعلوماتية بدلاً عن السندات المكتوبة في نقل النقود وتحويلها.[35]

ومن أهم الوسائل الحديثة غير المنظمة ما يلي:

أولاً. بطاقة الصرف الآلي: وهي تلك البطاقة المبرمجة بمعلومات شخصية عن صاحبها، التي تستخدم لسحب النقود الورقية من خلال إدخالها في شباك يدعى (الصراف الآلي)،[36] حيث يتم وضع كلمة سر لا يعرفها سوى صاحب البطاقة، وإذا كانت هذه الكلمة مغلوطة لا يتم استقبالها.[37]

وبعد إدخال الرمز الصحيح الخاص بالشخص العميل، يتم الضغط على مفتاح القبول الذي يدل على انصراف إرادة الشخص بسحب المبلغ، وهو بمثابة توقيع إلكتروني.[38]

---

[35] رقية السحيمي. **حرية الإثبات في الميدان التجاري وفق أحكام التشريع المغربي** (أطروحة دكتوراه)، أكدال: جامعة محمد الخامس، 2006، 131 -133.

[36] "ماكينة الصراف الآلي ببساطة محطة صرفية للبيانات مزودة بجهازي إدخال وأربعة أجهزة إخراج. وكأي محطة صرفية عادية للبيانات، لا بد أن يتصل الصراف الآلي بالمعالج المضيف الذي يعادل في طبيعة وظيفته الشركات التي توفر خدمات الإنترنت.

بقول آخر، يمثل المعالج المضيف العبارة التي تتصل بها كل شبكات الصراف الآلي، وبالتالي تكون متاحة أمام حاملي البطاقات الائتمانية. وتستطيع غالبية المعالجات دعم خطوط الاتصال على اختلاف نوعيها؛ الطلب الهاتفي أو الخطوط المستأجرة. وبالنسبة للآلات العاملة بالخطوط المستأجرة، فإنها تتصل مباشرة بالمعالج المضيف من خلال خط هاتفي مخصص يربط بين نقطتين، ويصل به أربعة كابلات، أما الماكينات العامة بخطوط الطلب الهاتفي، فإنها تتصل بالمعالج عن طريق خط هاتفي عادي يستخدم جهاز مودم ورقماً هاتفياً مجانياً. وآلات الصراف الآلي (ATM) تتولى مهمة القيام بالعديد من المعاملات التي لولاها لشغلت انتباه الموظفين. فهي تتميز بقدرتها على تنفيذ العديد من المهام مثل توفير معلومات الحساب، وقبول الإيداعات، وسحب القروض التي تمت الموافقة عليها من قبل، فضلاً عن تحويل الأموال. ويزيح استخدام آلات الصراف الآلي عن كاهل الموظفين المسؤولين عن القروض عناء الاهتمام بالخدمات الشخصية. وفي الوقت نفسه بإمكانها تقديم مجموعة أوسع نطاقاً من الخدمات.

وتعتبر آلات الصراف الآلي أكثر فعالية بالنسبة إلى مؤسسات التمويل الأصغر التي تقبل المدخرات، وتنشد خدمة العملاء في أماكن عدة و/أو أثناء ساعات خارج دوام العمل.

لكن نظراً لتكلفة الآلة الواحدة التي قد تصل إلى 35 ألف دولار أمريكي، فضلاً عن ضرورة وجود شبكات اتصالات وكهرباء يمكن الاعتماد عليها، فقد لا تكون تقنية آلات الصراف الآلي هي الخيار الأول بالنسبة لمؤسسات التمويل الأصغر كافة" عبد المنعم، على، الرابط التالي:

http://www.almohandes.org/vb/showthread.php?t=2833

visited on 15-11-2013 at 11:48.

[37] رقية السحيمي، مرجع سابق، 158.

[38] طارق عبد الرحمن ناجي كميل. **التعاقد عبر الإنترنت وآثاره** (رسالة دكتوراه)، أكدال: جامعة محمد الخامس – كلية العلوم القانونية والاقتصادية، 2003-2004، ص131.

ماذا لو سحب الشخص أكثر من المبلغ الذي يمتلكه فعلاً؟ ما هو التكيف القانوني لتلك الحالة؟

اختلف الفقهاء في تحديد طبيعة المسؤولية، فمنهم من قال إنها مسؤولية عقدية، ومنهم من قال مسؤولية جزائية تتمثل بجريمة النصب والاحتيال.[39]

ثانياً. بطاقة الائتمان: التي تصدر من شركة أو مؤسسة، حيث تمنح عميلها الحصول على ائتمان في حد أعلى لا يجوز تجاوزه يستخدمها للشراء، ومن أبرز الأمثلة عليها بطاقة الفيزا كارد (**Visa cards**)،[40] حيث تسهّل عليه الإنفاق في الأوقات التي لا تكون النقود بحوزته.

ثالثاً. الكمبيالة المعلوماتية: وهي تقارب الكمبيالة التقليدية من حيث كونها وسيلة لسداد واستحقاق الديون، حيث تبدأ بصورة كمبيالة تقليدية يدون فيها جميع البيانات الشكلية، وتسلم للبنك الذي يقوم بدوره بترجمة هذه البيانات على بطاقة ممغنطة تاركاً أصلها في حوزته.[41]

وهناك العديد من الوسائل الإلكترونية التي تجاهلتها التشريعات الفلسطينية، مثل التوقيع الإلكتروني، والسجل الإلكتروني، والبصمة الإلكترونية، وغيرها.

ومن خلال ما سبق، ما هي البدائل في ظل الفراغ التشريعي من جهة، وفي ظل عدم جواز التنصل القضائي من معالجة هذه الوسائل في ضوء جريمة إنكار العدالة من جهة أخرى؟ هذا ما سيتم توضيحه في البند اللاحق.

3.2.3 الأدلة الإلكترونية في مشروع قانون العقوبات الفلسطيني، ومشروع قانون المعاملات الإلكترونية، ومشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني

ذكرت المادة 1 من مشروع قانون المعاملات الإلكترونية لسنة 2010، مصطلح المعاملات الإلكترونية، والبيانات الإلكترونية، والسند الإلكتروني، والتوقيع الإلكتروني، وكلها وسائل حديثة نحن بأمس الحاجة لإدخالها حيز التنفيذ، بل وجاء هذا المشروع ليجعل من الوسائل السابقة قوة وحجة ترتب آثاراً قانونية، كما نص في الفصل العاشر منه على الجرائم والعقوبات التي تتعلق بهذا الموضوع.

---

[39] رقية السحيمي، المرجع السابق، 159.

[40] المرجع السابق، 161.

[41] المرجع السابق، 135 – 136.

أما مشروع قانون العقوبات الفلسطيني، فقد أفرد باباً خاصاً في جرائم الحاسوب، وذلك في المواد 379 حتى المادة 396. فعلى سبيل المثال، نص المشروع في المادة 380 على جريمة الدخول غير المشروع لنظام معلوماتي عبر الحاسوب، فإن مثل هذه الجريمة الإلكترونية لا يمكن إثباتها إلا بطريقة إلكترونية، بحيث يتم إثبات دخول الجاني عن طريق الحاسوب. كما نص المشروع في المادة 394 على جريمة ملاحقة ومضايقة الغير عبر الإنترنت، من خلال البريد الإلكتروني، أو بواسطة أي وسيلة أخرى، وهنا اعتراف صريح من قبل المشرع لاعتماد البريد الإلكتروني بيّنة في الإثبات.

أما عن مشروع قانون التجارة الإلكترونية، فقد نصت المادة 9 على منح (رسالة البيانات)[42] حجية كاملة في الإثبات كسند عرفي، ولم يجعل المشرع من كون تلك الرسائل إلكترونيةً وليست رسائل مكتوبة على ورق، انتقاصاً من حجيتها في الإثبات، إضافة إلى امتداد هذه الحجية على صورة المحررات المسحوبة عن الأصل،[43] لكن ما يهم هنا هو اعتمادها كدليل إلكتروني في الإثبات.

كما أن المشرع الفلسطيني في مشروع التجارة الإلكترونية، عالج موضوع التوقيع الإلكتروني في الفصل الثالث من المشروع في المواد 20 و21 و22.[44]

ولا بد من التأكيد على أنه لا يمكن فصل الأدلة التقليدية في الإثبات تماماً عن الأدلة الإلكترونية، فحتى الدليل الإلكتروني يمكن أن نعتمده من خلال وسيلة تقليدية، فكثير من الأحيان لا يمكن إدراك هذا الدليل الحديث إلا بواسطة الخبرة مثلاً، التي تعتبر دليلاً ووسيلة تقليدية، فتكون الخبرة على الدليل الإلكتروني.

3.3 حجية الأدلة الإلكترونية في الإثبات

ذكر سابقاً أن هناك أكثر من اتجاه في أنظمة الإثبات، كما أشير إلى أن المشرع الفلسطيني في قانون البينات أخذ في النظام المختلط، وهذا ينطبق على الإثبات في الإطار المدني، أما في الإثبات الجزائي فقد اتبع المشرع الفلسطيني النظام الحر، حيث نصت المادة 1/273 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 على: "تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها

---

[42] وتعني وفقاً للمادة الأولى من المشروع "رسالة البيانات: المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، ويشمل ذلك تبادل البيانات الإلكترونية، أو البريد الإلكتروني، أو البرق، أو التلكس، أو النسخ البرقي".

[43] رقية السحيمي، مرجع سابق، 270.

[44] أبو حجيلة، مرجع سابق.

بكامل حريتها ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة، أو تم التوصل إليه بطريق غير مشروع".

وعليه، فإن للقاضي، وحسب قناعته الوجدانية، اعتماد أي وسيلة طرحت أمامه واقتنع بها في حكمه، طالما كانت طريقة الحصول عليها مشروعة. وفي ظل ما سبق، لا تثور أمامنا إشكالية في مشروعية الدليل الإلكتروني طالما أن القاضي حر في تبني أي دليل، ما دام هذا الدليل مشروعاً، حيث أن المشرع الجزائي لم ينص على قائمة من الأدلة على سبيل الحصر والتحديد.[45]

إذاً حتى نكون أمام دليل إلكتروني مقبول ومعتمد، لا بد من أن تكون طريقة الحصول عليه من قبل السلطات المختصة مشروعة، وأن هذه المشروعية لا تتعلق أو تقتصر على الدليل الإلكتروني فحسب، بل على جل الأدلة، فمثلاً لو تم ضبط كمية من المخدرات داخل منزل ما دون وجود مذكرة تفتيش، فعندها يعتبر هذا التفتيش باطلاً لأن وسيلة إثباته باطلة، وهذا ينطبق على الدليل الإلكتروني، فمثلاً لو تم ضبط سجلات في جهاز حاسوب يعود للمتهم، ويفيد بتورطه بجرائم معينة، ووجد هذا الجهاز في منزل ما وتم ضبطه من غير مذكرة تفتيش، فإن هذه الوسيلة باطلة أيضاً.

وفيما يتعلق بأجهزة الحاسوب، فإن هناك خلافاً فقهياً حول موضوع التفتيش عليه، بحيث أن القواعد العامة تفترض وجود شيء مادي ليقع عليه التفتيش، حيث أن جانباً من الفقه لا يعتبر الحاسوب شيئاً مادياً يصح أن تنطبق عليه قواعد التفتيش، وذهب جانب آخر إلى اعتبار أن التفتيش بقواعده ينطبق على الحاسوب، لأن البحث عن دليل في الحاسوب بالضرورة يعني أن هذا الدليل يشغل حيزاً في ذاكرة الحاسوب، وبالتالي يمكن القياس عليه، لكن، وبغض النظر عن تلك الاتجاهات، فإن العبرة تكمن في مكان وجود الحاسوب، وبالتالي فإن الأجهزة الإلكترونية تأخذ حكم المكان الذي توجد فيه.[46]

إذاً، طالما تم الحصول على الدليل بطرق مشروعة، وتوفرت فيه جميع الشروط، وطالما وصلت إلى حد إقناع القاضي بشكل لا يحتمل معه الشك، فليس هناك أي حرج من اعتماد القاضي على هذا الدليل لتبرئة المتهم أو إدانته في الحكم شريطة أن يكون كل ذلك مسبباً.

وعليه، يمكن القول إنه لا يمكن الاستغناء، ولا بأي حال، عن تطبيق القواعد العامة في اعتماد أي دليل إلكتروني مهما كان حديثاً، ومهما كانت تلك القواعد تقليدية وقديمة.

---

[46] أبو حجيلة، مرجع سابق.

وقبل ختام هذا المحور، لا بد من الإشارة إلى الدليل الإلكتروني في جرائم الفساد، حيث نصت المادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد على أنه "من أجل مكافحة الفساد مكافحة فعالة، تقوم كل دولة طرف، بقدر ما تسمح به المبادئ الأساسية لنظامها القانوني الداخلي، وضمن حدود إمكانياتها، ووفقاً للشروط المنصوص عليها في قانونها الداخلي، باتّخاذ ما قد يلزم من تدابير لتمكين سلطاتها المختصة من استخدام أسلوب التسلم المراقب على النحو المناسب، وكذلك، حيثما تراه مناسباً، اتباع أساليب تحرٍّ خاصة كالترصد الإلكتروني وغيره من أشكال الترصد والعمليات السرية، استخداماً مناسباً داخل إقليمها، وكذلك لقبول المحاكم ما يستمد من تلك الأساليب من أدلة".[47]

4. الأدلة الإلكترونية وجرائم الفساد

كثيرة هي الجرائم التي ترتكب إلكترونياً أو بواسطة الحاسب الآلي والإنترنت، والجرائم المرتكبة بهذه الصورة تتميز بنوع من الحداثة نظراً لتوافر تقنية تكنولوجية تسهل ارتكابها من مسافات بعيدة أو قريبة دون اشتراط لتواجد الفاعل في مكان ارتكابها. وقد لجأ المجرمون إلى استخدام الحاسوب لتسهيل نشاطاتهم الإجرامية منذ بداية عصر الكمبيوتر، والكمبيوتر ما هو إلا أداة يستخدمها المجرمون كما تستخدم أي أداة أخرى لفتح قفل ما، أو آلة لتزوير أوراق أو عملة، وعادة ما يتبع مرتكبو الجرائم بواسطة الحاسوب منهجية معينة لدى قيامهم بالنشاط الجرمي، تصعّب عمل مأموري الضبط القضائي وأعضاء النيابة العامة في ملاحقتهم وإثبات ارتكابهم للجريمة، وبالتالي يتعين على هذه الجهات أن تستعين بطواقم مؤهلة ومدربة ولديها الخبرة والكفاءة العلمية في التعامل مع مثل تلك الجرائم، التي قد تكون جرائم أموال، أو أشخاص، أو أمن دولة، أو جرائم فساد ... وغيرها.

المسألة الرئيسية التي سيعالجها هذا المحور هي مدى قبول الأدلة الإلكترونية في إثبات جرائم الفساد (مثل الاختلاس، والرشوة، واستثمار الوظيفة) وفق نصوص القوانين الفلسطينية، ودور وكيل النيابة العامة في مرحلة التحقيق الابتدائي من جهة، وكذلك سلطة القاضي الجزائي في تقدير الدليل الإلكتروني المقدم لإثبات وقوع جريمة فساد.

وعليه، سيتم تقسيم هذا المحور إلى ثلاثة أقسام، يبحث الأول مرحلة جمع الاستدلالات ودور الضابطة القضائية، فيما سيبحث القسم الثاني مرحلة التحقيق الابتدائي ودور وكيل النيابة العامة فيه، مع تسليط

[47] أبو حجيلة، مرجع سابق.

الضوء على ما يجب على وكيل النيابة اتباعه في مرحلة التحقيق، أما القسم الثالث فيبحث مرحلة المحاكمة وتقديم الدليل الإلكتروني وعرضه أمام المحكمة وسلطة القاضي في تقدير هذا الدليل، وسيستعرض مبدأ القناعة الوجدانية الذي يقوم على حرية الإثبات الجزائي، هذا إلى جانب استعراض بعض التطبيقات العملية لما يجري العمل به أمام محكمة جرائم الفساد.

1.4 مرحلة جمع الاستدلالات ودور الضابطة القضائية

من المعروف قانوناً وفقهاً أن أعضاء الضابطة القضائية هم من يباشرون مرحلة جمع الاستدلالات أو ما يعرف بالبحث الأولي. وتنبع أهمية هذه المرحلة من أنها المرحلة التي تكتشف فيها الجريمة وتتصل بها جهات إنفاذ القانون للمرة الأولى، ولهذا في حال كانت الجريمة قد ارتكبت بواسطة أدوات إلكترونية تكون طرق التعامل مع مسرح الجريمة مختلفة عن طرق التعامل مع مسرح الجريمة العادية، كون أن الجريمة المرتكبة بواسطة أدوات إلكترونية تحتاج إلى طرق خاصة للتعامل معها، وذلك نظراً لأن الأدلة الإلكترونية قد تحفظ وتنقل بشكل رقمي، ويتم الحصول عليها من أجهزة الحاسوب التي يتم ضبطها، أو من خلال الصفحات الإلكترونية، أو من خلال أجهزة الاتصال الخلوي، أو من كاميرات التصوير الثابتة أو المتنقلة ... وغيرها.

- **الضابطة القضائية المختصة**

نصت المادتان 8 و9 من قانون مكافحة الفساد المعدل بموجب القرار بقانون رقم 7 لسنة 2010، على اختصاصات وصلاحيات هيئة مكافحة الفساد، حيث جاء في الفقرة الثالثة من المادة 8 أن الهيئة تختص بما يلي: 3- التحقيق في الشكاوى التي تقدم عن جريمة الفساد. 4- التحقق من شبهات الفساد التي يقترفها الأشخاص الخاضعون لأحكام هذا القانون، وكذلك نصت المادة 9 من القانون نفسه: "على الرغم مما ورد في قانون الإجراءات الجزائية والقوانين الأخرى ذات العلاقة، يكون للهيئة في سبيل تنفيذ مهامها واختصاصاتها ما يلي:

1. تلقي التقارير والبلاغات والشكاوى بخصوص جرائم الفساد المقدمة لها ودراستها ومتابعتها، والقيام بأعمال التحري وجمع الاستدلالات بشأنها، والكشف عن المخالفات والتجاوزات وجمع الأدلة والمعلومات الخاصة بذلك، ومباشرة التحقيق والسير في الإجراءات الإدارية والقانونية اللازمة وفقاً لأحكام هذا القانون والتشريعات ذات العلاقة.
2. ملاحقة كل من يخالف أحكام هذا القانون، وحجز أمواله المنقولة وغير المنقولة، ومنعه من السفر، وطلب كف يده عن العمل من الجهات المعنية، ووقف راتبه وعلاواته وسائر

استحقاقاته المالية عند اللزوم، وتعديل أيٍّ من تلك القرارات أو إلغاؤها وفق التشريعات النافذة.

3. استدعاء الشهود والمعنيين من الموظفين العموميين أو موظفي القطاع الخاص، أو أي شخص له علاقة للاستفسار والتحري حول واقعة تتعلق بجريمة الفساد.
4. طلب أي ملفات أو بيانات أو أوراق أو مستندات أو معلومات، أو الاطلاع عليها، أو الحصول على صور منها من الجهة الموجودة لديها، بما في ذلك الجهات التي تعتبر كل ذلك سري التداول وفقاً للإجراءات القانونية النافذة.
5. التنسيق مع الجهات المختصة لتعقب وضبط وحجز واسترداد الأموال والعائدات المتحصلة من جرائم الفساد، على أن يصدر قرار المصادرة بشأنها عن المحكمة المختصة بنظر الدعوى.
6. للهيئة أن تباشر التحريات والتحقيقات اللازمة لمتابعة أيٍّ من قضايا الفساد من تلقاء نفسها، أو بناء على إخبار أو شكوى ترد إليها من أي جهة، وإذا تبين، بنتيجة الدعوى أو التحقيق، أن الأخبار أو الشكوى الواردة إلى الهيئة كاذبة أو كيدية، يتم تحويل مقدمها إلى الجهات القضائية المختصة لمعاقبته وفقاً للأصول القانونية المتّبعة.
7. كل شركة أو جمعية أو هيئة أهلية أو نقابة أو أي هيئة أخرى من الخاضعين لأحكام هذا القانون، فيما عدا الإدارات العامة إذا اقترف مديروها أو أعضاء إداراتها أو ممثلوها أو عمالها باسمها أو بإحدى وسائلها جريمة من الجرائم المحددة بهذا القانون، يحق للهيئة، وحسب واقع الحال، أن تطلب من المحكمة وقفها عن العمل، أو حل أي من هذا الهيئات وتصفية أموالها، وحرمان كل من له علاقة بالجريمة المرتكبة من تأسيس أي هيئة مماثلة أو أن يكون عضواً في مجلس إدارتها أو مديراً لها لمدة لا تقل عن سنة ولا تزيد على خمس سنوات.
8. حق تحريك الدعاوى الخاصة بالجرائم المحددة بهذا القانون من خلال النيابة العامة ومباشرتها وفقاً لأحكام هذا القانون والتشريعات الأخرى ذات العلاقة، ولا تقام هذه الدعاوى من غيرها، إلا في الأحوال المبيّنة في القانون، ولا يجوز وقف الدعوى بعد تحريكها أو التنازل عنها أو تركها أو التصالح عليها إلا في الحالات المحددة في القانون.
9. على الرغم مما ورد في أي تشريع آخر، تلتزم الهيئة بإصدار قرارتها بالملفات المتابعة من قبلها فور الانتهاء من إجراءاتها المحددة في القانون".

لقد نصت المادة 9 مكرر 2 من قانون مكافحة الفساد المعدل المشار إليه، وبالتحديد في فقرتها الرابعة، على: "تباشر النيابة العامة المنتدبة بمساعدة موظفي الهيئة الذين يتمتعون بصفة الضابطة

القضائية، إجراءات التحقيق التي يتوجب عليهم القيام بها على وجه الاستعجال، ودون أي تأخير أو تباطؤ مبرر له في تلك الإجراءات.

يتضح من استقراء تلك النصوص السابقة، أن موظفي هيئة مكافحة الفساد، يتمتعون بصفة الضابطة القضائية، وهذا جاء متوافقاً مع صريح نص المادة 21 من قانون الإجراءات الجزائية رقم 3 لسنة 2001، التي حددت في فقراتها الثلاث الأولى من يكون من مأموري الضبط القضائي، وفي فقرتها الرابعة نصت على الموظفين الذين خولوا صلاحيات الضبط القضائي بموجب القانون، وبالتالي يتوجب على موظفي هيئة مكافحة الفساد القيام بكافة أعمال البحث والتحري اللازمة للكشف على الجريمة ومرتكبيها عندما يتعلق الأمر بجريمة فساد ارتكبت بوسائل إلكترونية، بصفتهم من مأموري الضبط القضائي.

في ظل الوضع القائم في الأراضي الفلسطينية الذي يشير، وبشكل عام، إلى أننا ما زلنا نفتقر إلى عناصر الخبرة المتخصصة في مجال تفتيش وضبط الأدلة الإلكترونية، وعلى الرغم من وجود عدد لا بأس به من الكفاءات في مجال أجهزة الحاسوب وبرامجها المختلفة، فإنه يتوجب تدريب هؤلاء أيضاً على آليات استخراج الدليل الإلكتروني.

عندما تكتشف الضابطة القضائية وقوع جريمة ما عليها أن تبادر في الحال ودون إبطاء، إلى جمع الأدلة التي تثبت وقوع الجريمة من جهة، ومن جهة أخرى نسبة تلك الجريمة إلى فاعل معين، وهذا يتطلب من الضابطة القضائية القيام بأمور عدة:

أولاً. الانتقال والمعاينة: يتوجب على الضابطة القضائية التوجه فوراً إلى مكان وقوع الجريمة –كدائرة من دوائر الحكومة ارتكبت فيها جريمة اختلاس أو استثمار وظيفي بواسطة جهاز حاسوب مثلاً– وفور الوصول يتم إجراء المعاينة للمكان؛ أي إجراء الكشف الحسي الذي يهدف إلى تحديد مكان الجريمة وظروفها وأدوات ارتكابها ونتائجها، وكذلك يجب التحفظ على الأشخاص والأدوات والأجهزة.[48]

ويجب هنا على أفراد الضابطة القضائية أن يراعوا أموراً عدة، وبخاصة إن كانت الجريمة قد تم ارتكابها بواسطة أدوات إلكترونية، حيث أنه من الممكن أن يكون هنالك كم كبير من التكنولوجيا

[48] أسامة المناعسة وآخرون. جرائم الحاسب الآلي والإنترنت، دار وائل الطبعة الأولى 2001. 248.

المستخدمة في ارتكاب الجريمة، فيجب –ابتداءً– الحصول على معلومات كافية عن عدد الأجهزة المستعملة، وأنواعها، ومن ثم تحديد الجهاز أو الأجهزة الواجب التعامل معها، ومعرفة ما يلزم من إمكانيات لتأمين وحفظ المعلومات، وإذا كانت تلك الأدوات بحاجة إلى شخص مختص لتأمينها، فإنه من المهم جداً على أفراد الضابطة القضائية أن يراعوا بعض المسائل كعدم إطفاء جهاز الحاسوب، أو حتى تشغيله قبل التشاور مع خبير، وكذلك عليه ألا يحاول العبث بجهاز حاسوب أو جهاز إلكتروني قد يحتوي على دليل محتمل.[49]

ثانياً. الاستعانة بالخبرة: نصت المادة 22 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 على مهام مأموري الضبط القضائي، وفي الفقرة الثانية منها نصت على إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق والاستعانة بالخبراء المختصين والشهود دون حلف يمين.

وبسبب الفراغ التشريعي في فلسطين لقوانين خاصة تنظم الجرائم الإلكترونية، أو تنظم كل ما يتعلق بالأدلة الإلكترونية، كما سبق بيانه، فإنه يتعين عند التعامل مع مثل تلك الجرائم والأدلة، الرجوع إلى القواعد العامة، فقانون الإجراءات الجزائية الفلسطيني منح الضابطة القضائية الحق في الاستعانة بالخبراء المختصين، وبالتالي عند دخول أفراد الضابطة القضائية إلى مسرح جريمة، إن كانت الجريمة ضمن إطار الجرائم الإلكترونية، حيث التكنولوجيا المتطورة والمعقدة والأساليب الإجرامية الجديدة التي تنم عن ذكاء المجرم وفطنته.

فالحاجة إلى الاستعانة بأهل الخبرة والمعرفة العلمية تظهر لأعضاء الضابطة القضائية أثناء قيامهم بمهام عملهم. وللاستعانة بخبير أصول، إذ يجب التأكد من أن الخبير المنتدب يقوم بالمهمة الموكلة إليه بنفسه، فلا يجوز له أن ينيب عنه غيره سواء جزئياً أو كلياً في العمل الموكل إليه، كما أن عليه عند الانتهاء من عمله، أن يعدَّ تقريراً مسبباً يفصل فيه ما تم من إجراءات وإعمال خبرته ليثبت واقع الحال.

ثالثاً. سماع أقوال المشتبه فيه: جاءت المادة 34 من قانون الإجراءات الجزائية الفلسطيني لتعطي الحق لمأمور الضبط القضائي أن يسمع أقوال المقبوض عليه فوراً. إن أهمية ذلك في مرحلة جمع الاستدلالات تنبع من أن أصدق أقوال يرويها المشتبه فيه تكون في مراحل القبض الأولى،

[49] بوس نورجن. تأمين الادلة الرقمية، ورقة دراسية ،ص 12

ذلك أنه يكون من الصعب عليه أن يختلق وقائع كاذبة في فترة وجيزة، أو أن يحاول إيجاد أعذار أو مبررات، وهذا أيضاً يعطي مصداقية أكثر عند إبراز إفادته المعطاة أمام الضابطة القضائية أمام المحكمة المختصة، وبخاصة أن الجرائم المرتكبة بالوسائل الإلكترونية لا تكتشف في الغالب الأعم إلا وفقاً لاعتراف الفاعل، أو بالاعتماد على عامل الصدفة، ومن هنا تبرز أهمية الاعتراف في إثبات تلك الجرائم.[50]

مأمور الضبط القضائي عليه أن يراعي "عند سؤال المقبوض عليه في جريمة إلكترونية أو مرتكبة بواسطة وسائل إلكترونية"، أن يوجه له أسئلة تهدف إلى الحصول على كلمات مرور أو تشفير كان المشتبه فيه قد وضعها على أحد أجهزته الإلكترونية، لأن ذلك غالباً يساعد الأشخاص ذوي الخبرة في الوصول إلى ملفات موجودة داخل الأجهزة الإلكترونية، مثل أجهزة الاتصال الخلوي، أو أجهزة الحاسوب.

رابعاً. الضبط:[51] استكمالاً لعمليات جمع الأدلة، فإنه يتعين على أفراد الضابطة القضائية أن يقوموا بضبط كل الأوراق أو الأشياء الموجودة في مسرح الجريمة، وبخاصة إن كانت تلك الأشياء معدة لارتكاب الجريمة مثل الآت النسخ الخاصة بنسخ ملفات الحاسب الآلي، فالجرائم المرتكبة بواسطة أدوات إلكترونية كغيرها من الجرائم، يمكن إثباتها بالأدلة كافة المعتبرة شرعاً وقانوناً، لكنها قد تختلف من حيث نوع تلك الأدلة وطبيعتها، مثل الأدلة الورقية؛ سواء أكان على صورة أوراق أولية كمسودات للعملية الجرمية المراد ارتكابها، أم أوراق طبعت لبيان مدى جاهزية الحاسب الآلي للقيام بالجريمة، وكذلك قد تكون الأوراق أصلية.[52]

ومن الأدلة الأخرى أيضاً جهاز الحاسب الآلي نفسه، وكذلك ملحقاته، كأجهزة الطباعة، والإدخال، وأجهزة اتصالات، إضافة إلى الأقراص المرنة وأقراص الليزر والشرائط الممغنطة وبطاقات الائتمان وأجهزة الاتصالات البعدية والمواد البلاستيكية المستعملة في صنع البطاقات إن وجدت، مع التأكيد أن ضبط مثل تلك الأدلة يحتاج إلى وجود خبير مختص يتولى الإشراف الكامل على ضبط تلك الأجهزة والأدوات، وكذلك لديه المعرفة الكاملة في آلية حفظ تلك الأجهزة والأدوات حتى لا تتعرض للتلف.

---

[50] أسامة المناعسة وآخرون، مرجع سابق، 251.

[51] الضبط عبارة عن شهادة مكتوبة من قبل عضو الضابطة القضائية صاحب الاختصاص، يثبت بها ما جرى أو قيل بحضوره، أو بما شاهد أو سمع.

[52] المناعسة، مرجع سابق، 250.

خامساً. تنظيم محاضر الضبط: بما أن المشرع في المادة 212 من قانون الإجراءات الجزائية الفلسطيني قد اعتبر المحاضر، التي ينظمها مأمورو الضبط القضائي في الجنح والمخالفات المكلفون بإثباتها بموجب أحكام القوانين، حجة يصلح الاستناد إليها بالنسبة للوقائع المثبتة فيها إلى أن يثبت ما ينفيها، فإنه يتوجب على مأموري الضبط القضائي إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية توقع منهم ومن المعنيين بها. وحتى يكون المحضر مقبولاً وذا قوة ثبوتية، يجب توافر ثلاثة شروط فيه نصت عليها صراحة المادة 213 من قانون الإجراءات الجزائية الفلسطيني، وهي أن يكون صحيحاً من حيث الشكل، وأن يكون محرره قد عاين الواقعة بنفسه أو أبلغ عنها، وأن يكون محرره قد دوّنه ضمن حدود اختصاصية وأثناء قيامه بمهام وظيفته.

ختاماً، يثور تساؤل يتعلق بجرائم فساد ارتكبت بواسطة أدوات إلكترونية، ومثالها قيام موظف يعمل في إحدى الدوائر الرسمية باستغلال مهام وظيفته واختلاس مبلغ من المال، وذلك عن طريق درايته ببرنامج محاسبي على جهاز الحاسوب الخاص بالدائرة التي يعمل بها، وقيامه بإغلاق حسابات تتعلق بالضرائب عن المكلفين بدفعها على البرنامج، حيث استغل الموظف درايته ومعرفته بالبرنامج لتنفيذ أفعاله الجرمية، فمن هي الضابطة القضائية المختصة في إجراء أعمال البحث والتحري في هذه الحالة؟

إننا نرى أنه، وبموجب قانون مكافحة الفساد المعدل، الذي منح موظفي هيئة مكافحة الفساد وفق ما بيناه سابقاً صفة الضابطة القضائية، فإنه يتوجب على موظفي هيئة مكافحة الفساد، الاضطلاع بدورهم كمأموري ضبط قضائي، والقيام بأنفسهم بضبط جهاز الحاسوب الذي كان يعمل عليه الموظف في مثالنا المذكور، وتولي كافة أعمال التحري وجمع الاستدلالات من ضبط بمعرفة خبير يندبونه إن لم يكن يوجد في ضمنهم مثله، وسماع أقوال المقبوض عليه، والشهود، وتدوينها أصولاً، ثم رفع الأمر إلى رئيس هيئة مكافحة الفساد لإحالة الأوراق إلى النيابة المنتدبة لدى هيئة مكافحة الفساد، وإنَّ في هذا التطبيقَ السليمَ لنصوص قانون مكافحة الفساد الفلسطيني.

2.4 مرحلة التحقيق الابتدائي

بعد أن تنتهي الضابطة القضائية من جمع استدلالاتها، تقوم بإحالة الأوراق والضبوط والمحاضر إلى النيابة العامة، فهي صاحبة الاختصاص بتحريك دعوى الحق العام وفق نص المادة (1) من قانون الإجراءات الجزائية الفلسطيني. وبدخول الدعوى العمومية في اختصاص النيابة العامة وفقاً للأصول،

تملك النيابة العامة في مباشرة أعمالها، إجراء أعمال تحقيق متنوعة تهدف بالأساس إلى التثبت والوصول إلى الحقيقة، من أجل أن تصل في نهاية إجراءاتها تلك إلى اتّخاذ قرار يتعلق بمدى ملاءمة إحالة الدعوى التحقيقية إلى المحكمة المختصة من عدمه.

- **صلاحيات وكيل النيابة:**

بمجرد دخول الدعوى العامة في اختصاص وكيل النيابة، فإن له اتّخاذ الإجراءات التحقيقية كافة التي يراها لازمة وفق تقديره بهدف الوصول في ختام تلك الإجراءات إلى قرار، إما بإحالة المتهم إلى المحكمة المختصة لمحاكمته، وإما بحفظ أوراق الدعوى.

إن الإجراءات التحقيقية التي يتولاها وكيل النيابة كثيرة، ولم يحدد المشرع تلك الأعمال حصراً في القانون، ولكن كون الدراسة تتعلق بالأدلة الإلكترونية، سيتم اقتصار الدراسة على ثلاثة إجراءات جوهرية متصلة بموضوع الأدلة الإلكترونية وجرائم الفساد، الأول يتعلق بالتفتيش، والثاني يتعلق بالخبرة الفنية العلمية وماهيتها في مرحلة التحقيق في مثل تلك الجرائم، والثالث استجواب المتهم في جرائم الفساد المرتكبة بواسطة أدوات إلكترونية.

أولاً. التفتيش: التفتيش عمل من أعمال التحقيق التي تختص بها النيابة العامة دون سواها، ويهدف مثل هذا الإجراء إلى جمع أدلة مادية تثبت وقوع الجريمة ونسبتها إلى فاعل معين.

عندما يتعلق الأمر بجريمة ارتكبت بوسائل إلكترونية، يثور تساؤل حول ما هي الأصول الواجب اتباعها في التفتيش؟ لعل من أهم ما يواجه الإثبات في الجرائم الإلكترونية، بشكل عام، من معوقات، هي المعوقات التشريعية، وذلك بسبب افتقار القوانين الموجودة في الأراضي الفلسطينية إلى أي نصوص تواجه الطبيعة الخاصة بالجرائم الإلكترونية، ولا يوجد في تلك القوانين ما يسعف جهات التحقيق بشكل صريح في أصول التعامل مع أدلة إلكترونية؛ مثل النصوص التي تتعلق بضوابط التفتيش في بيئة الحاسب الآلي، وبخاصة إذا كان الحاسب المراد تفتيشه مرتبطاً ومتصلاً بحاسب آخر خارج الدولة.

لذلك، فإن واقع الحال يحتم اللجوء إلى القواعد العامة في التفتيش الواردة في الفصل الرابع من الباب الثاني من قانون الإجراءات الجزائية الفلسطيني، وذلك في ظل غياب النصوص القانونية، وكذلك غياب القوانين الخاصة بمثل تلك الحالات. وبالاطلاع على أحكام الفصل الرابع، نجد أن المشرع الفلسطيني قد حصر التفتيش بالنيابة العامة، تجريه بحضورها أو تصدر الإذن اللازم

لإجرائه حتى لا يقع التفتيش باطلاً، وهذا بالطبع يسري إذا كان التفتيش على الأدلة الإلكترونية سيجري في منزل أحد المشتبه فيهم، أو أحد المتهمين، ذلك أن المواد 39 – 43 من قانون الإجراءات الجزائية، قد تناولت فقط تفتيش المنازل ودخولها، وحصرت هذا العمل بالنيابة العامة، ولا يتم إلا بمذكرة صادرة عنها، أو في حضورها، بمناسبة جريمة وقعت، وتحديد نسبتها إلى شخص بعينه.

وبالتالي، وعند اقتضاء الأمر إجراء التفتيش عن أدوات الجريمة، فإنه يتوجب أن يتوجه وكيل النيابة إلى المنزل المراد تفتيشه ويشرف بنفسه على التفتيش أو يصدر مذكرة تفتيش وفق الشروط الواردة في الفصل الرابع من قانون الإجراءات الجزائية الفلسطيني، فلا خلاف أن التفتيش عن أدوات إلكترونية ارتكبت بها الجريمة إن كانت موجودة بداخل منزل المتهم، فإنه يقتضي ذلك الحصول على إذن النيابة العامة، أو أن يتولى وكيل النيابة التفتيش بنفسه. ولكن السؤال الذي يطرح بعد ذلك، هل هناك ما يوجب إصدار مذكرة من أجل تفتيش جهاز حاسوب مثلاً، بمعنى تفتيش محتويات ذلك الجهاز والبرامج الموجودة فيه، التي قد تحتوي على أدلة إلكترونية لازمة لإثبات الجريمة ونسبتها إلى الفاعل؟ وهل هناك أصول معينة يجب اتّباعها عند إجراء مثل ذلك التفتيش؟

في ظل غياب قانون خاص بالجرائم الإلكترونية ينظم أصول التعامل مع مثل تلك الحالة، فإنه يقتضي على جهات إنفاذ القانون أن تعود إلى القواعد العامة عند إجراء التفتيش، وإن قانون الإجراءات الجزائية قد خلا تماماً من تنظيم مسألة تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل إلى استعمالها في ارتكاب الجرائم الجاري التحقيق فيها، وما دام الأمر كذلك، وما دام أن الدعوى الجزائية يمكن إثباتها بطرق الإثبات كافة، فإننا نرى أنه لا يوجد ما يمنع أفراد الضابطة القضائية أو وكيل النيابة من إجراء التفتيش في الأجهزة والأدوات الإلكترونية المستخدمة في ارتكاب الجريمة بشرط أن يجري هذا التفتيش بمعرفة خبير مختص في استخراج الدليل الإلكتروني من داخل الجهاز.

ولو اطّلعنا على قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010 الأردني، وبالتحديد المادة 12 منه، نجدها قد نصت على أصول وقواعد معينة تتعلق بالتفتيش، بضرورة الحصول على إذن من المدعي العام أو من المحكمة المختصة عند التفتيش، وكذلك أصول تتعلق بإجراء

الضبط من موظفي الضابطة العدلية، وتنظيم محضر بكل الإجراءات وتقديمه إلى المدعي العام.[53]

وباستقراء هذا النص، نجده، في الأغلب، لا يختلف كثيراً عن أصول وقواعد التفتيش بشكل عام، وكل ما في الأمر أنه قد جاء في قانون خاص يتعلق بالأدلة الإلكترونية وبالجرائم المرتكبة بواسطة أدوات إلكترونية.

بعد الانتهاء من التفتيش في الأجهزة، يتوجب أن يتم تنظيم محضر بالتفتيش يثبت فيه تفاصيل الأعمال والإجراءات التي تمت، وكذلك النتائج التي أفضى إليها التفتيش، وما إذا تم ضبط أيٍّ من أدوات الجريمة الإلكترونية والحالة التي ضبطت فيها.

ثانياً. ندب الخبراء: عندما يتعلق الأمر بالإثبات الجزائي في جرائم إلكترونية أو جرائم فساد ارتكبت بواسطة أدوات إلكترونية، فإننا نرى لزاماً على النيابة العامة أن تستعين بالخبرة الفنية العلمية في إثبات مثل تلك الجرائم، وذلك بالنظر إلى الطبيعة الخاصة لها، وصعوبة إثباتها بطرق الإثبات التقليدية من جهة، ومن جهة أخرى صعوبة استخراج مثل تلك الأدلة وحفظها.

فالخبرة هي إبداء رأي فني من شخص مختص في واقعة ذات أهمية في الدعوى الجزائية، لأنها تفترض استعانة بخبير لديه معلومات علمية أو فنية،[54] ويجب أن تكون مهمة الخبير محددة وواضحة، وقد نظمت المواد 64 إلى 71 من قانون الإجراءات الجزائية الفلسطيني أصول ندب الخبراء من قبل وكيل النيابة، ويتعين على الخبير أن يقدم تقديره مسبباً، ويوقع على كل صفحة منه، يبين فيه آراء وتقييمات توصل إليها بتطبيق قواعد علمية أو فنية تعينه فيها دراساته وخبراته السابقة، يصل من خلالها إلى نتيجة معينة تساعد وكيل النيابة في إثبات مادة الجريمة المرتكبة.

ولوكيل النيابة أن يأمر بإجراء أعمال الخبرة تحت إشرافه، أو يأمر الخبير أن يقوم بعمله وحده، وذلك بحسب طبيعة الحال، كما يجوز للخصوم أن يحضروا إجراء أعمال الخبرة إذا قدر وكيل النيابة أن مصلحة التحقيق قد تقتضي ذلك، وفي جميع الأحوال يحلف الخبير اليمين بأن يؤدي عمله بنزاهة وصدق، ويتعين على الخبير تقديم تقريره في الموعد الذي يحدده وكيل النيابة.

---

[53] أبو حجيلة، مرجع سابق، ص 25.

[54] أبو حجيلة، مرجع سابق، ص 36.

ثالثاً. الاستجواب: بعد أن ينتهي وكيل النيابة من إجراءات التفتيش والضبط اللازمين، وسماع الشهود في جريمة الفساد، ويقوم بتدقيق التقارير المقدمة إليه من الخبراء المكلفين، ويستمع إلى شروحاتهم حول أعمال خبرتهم –وهذا ما يجري العمل به لدى النيابة المنتدبة لدى هيئة مكافحة الفساد– يصل إلى أهم مراحل التحقيق الابتدائي؛ ألا وهي استجواب المتهم ومواجهته بالأدلة التي توصل إليها وكيل النيابة.

يقتضي الاستجواب مناقشة المتهم بصورة تفصيلية بشأن الأفعال المنسوبة إليه، ومواجهته بالأدلة والاستفسارات والأسئلة، ومطالبته بالإجابة عنها، وإن المتهم في الجرائم الإلكترونية أو الجرائم المرتكبة بواسطة أدوات إلكترونية يتميز عن غيره من باقي المتهمين العاديين بأنه يمتلك خبرة واسعة في توظيف الأدوات والأجهزة الإلكترونية في ارتكاب جريمته، ولديه من الحيل ما يمكّنه من المراوغة أثناء استجوابه من قبل وكيل النيابة الذي لا يفترض به أن يكون خبيراً بالأدوات الإلكترونية. وعليه، فإننا وباستقراء نصوص قانون الإجراءات الجزائية الفلسطيني المتعلقة بالاستجواب، وذلك في المواد 94 وحتى 105، وبحسب ما نرى لا نجد ما يمنع وكيل النيابة من أن يستعين أثناء استجوابه للمتهم بخبير من نوع خاص، بشرط أن لا يتولى الخبير نفسه توجيه الأسئلة إلى المتهم، وأن تقتصر مهمته على توضيح النقاط الغامضة لوكيل النيابة، أو حتى للمتهم نفسه، ويسهل التواصل بينهما، كما لا يوجد ما يمنع أن يعد الخبير ورقة يوضح فيها بعضاً من الاستفسارات والأسئلة الفنية ليتم سؤال المتهم عنها من خلال وكيل النيابة، كما أننا نرى أن اتّباع مثل هذه الطريقة في استجواب متهم ارتكب جريمة فساد مستعملاً في ارتكابها أدوات إلكترونية، تؤدي إلى نتائج أكثر دقة ومتفقة مع أحكام القانون، على أن يتم إثبات حضور الخبير في محضر الاستجواب.

3.4 مرحلة المحاكمة

بعد أن تنتهي النيابة العامة من أعمال التحقيق الخاصة بها، تحيل ملف التحقيق إذا ما رأت أن الأدلة التي وصلت إليها كافية لإدانة المتهم بعد إصدار قرار اتهام ولائحة اتهام، وبذلك تصل الدعوى إلى المحكمة المختصة لإجراء محاكمة المتهم أصولاً، وتعرف أيضاً هذه المرحلة بمرحلة التحقيق النهائي، يقدم فيها وكيل النيابة الأدلة التي قام بجمعها ويعرضها على محكمة الموضوع لتصل إلى نتيجة بعد تفحص تلك الأدلة وتدقيقها. إما بإدانة المتهم وإما الحكم بإعلان براءته.

وفي الجرائم الإلكترونية، بشكل عام، يواجه القضاة صعوبة في فهم التقنية الخاصة المستخدمة لارتكاب تلك الجرائم، وفي تحديد السلوكيات المجرمة، وبخاصة عند غياب النص، وكذلك في اكتشاف واستخلاص النية الإجرامية، عدا عن الصعوبات المتعلقة بالاختصاص المكاني.

أولاً. المحكمة المختصة: فيما يتعلق بجرائم الفساد المرتكبة، بشكل عام، وحتى وإن كانت مرتكبة بواسطة أدوات الإلكترونية، فإن المحكمة المختصة في نظر جرائم الفساد هي محكمة جرائم الفساد التي شكلت على إثر صدور القرار بقانون رقم 7 لسنة 2010، وذلك تطبيقاً لنص المادة 9 مكرر 1 من القرار بقانون آنف الذكر، حيث تختص محكمة جرائم الفساد بالنظر في قضايا جرائم الفساد أينما وقعت.

ثانياً. تقديم الدليل الإلكتروني وعرضه على المحكمة: يعتبر عرض الأدلة من خلال استخدام وسائل مساعدة مثل الرسومات وغيرها، أمراً مهماً في قضايا جرائم الفساد، حيث أنه يسهم، بشكل كبير، في تبسيط وتوضيح ماهية الدليل الإلكتروني لهيئة المحكمة، ما يسهل عليها التقرير بشأن اعتماد ذلك الدليل من عدمه، فجرائم الحاسب الآلي عموماً، تتم ضمن بيئة افتراضية غير مادية أي غير محسوسة، وبالتالي لا تترك أي دلائل مادية ملموسة، فيجب عندئذ أن يتم عرض الدليل الإلكتروني بطريقة سهلة أمام المحكمة، وذلك من خلال الخبير الأساسي الذي قام بإعداد الدليل واستخراجه وحفظه الذي يجب حضوره عند عرض الدليل، وأن يتم العرض من خلاله حتى يتسنى للدفاع وللمحكمة مناقشته وسؤاله عن أعمال الخبرة التي أداها في دور التحقيق الابتدائي.

يتولى وكيل النيابة تقديم الدليل أمام المحكمة وعرضه بمساعدة الخبير، وعليه تبيان الآلية والكيفية التي تم التوصل بها إلى ذلك الدليل، وكيف تم استخراجه. كما يجب على وكيل النيابة تقديم الدليل إلى المحكمة بصورة مفهومة نظرياً، وكذلك عليه أن يوضح، وبمساعدة الخبير، علاقة الدليل الإلكتروني المنوي تقديمه بجرم الفساد المرتكب، وكذلك توضيح الأمور التقنية والجوانب العلمية التي استند إليها الخبير، ولا يوجد ما يمنع من الاستعانة بأجهزة تقنية عند عرض الدليل وأثناء شهادة الخبير أمام المحكمة.[55] ومن التطبيقات العملية على ذلك، قيام وكيل النيابة، وأثناء مناقشة خبير في قضية فساد تمثلت في قيام المتهم باستغلال موقعه الوظيفي في أحد الأجهزة الأمنية، بأن قام وبعد ضبطه لجهاز كمبيوتر متنقل في منزل أحد

[55] David W. Hagy Regina B. Schofield .*Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* chapter3 page23.

المواطنين، باصطناع قائمة رشاوى على جهاز كمبيوتر آخر ونسخها على جهاز ذاكرة رقمية، ثم قام بنقلها على حاسوب المواطن الذي كان قد ضبطه سابقاً، ليبدو الأمر وكأن المواطن كان يقوم برشوة عدد من المسؤولين، وبعد انتداب الخبير تمكنت النيابة من إثبات أن تلك القائمة لم تكن موجودة من السابق على حاسوب المواطن، وتمكن الخبير من تحديد تاريخ إنشاء القائمة. وعند عرض الدليل أمام المحكمة، قام الخبير بفتح جهاز الحاسوب المتنقل أمام المحكمة والخصوم، وتم شرح كيفية الحصول على القائمة المذكورة، وكيف تم نقلها إلى حاسوب المواطن بصورة مبسطة تسهل على المحكمة تقدير قيمة ذلك الدليل.

ثالثاً. حجية الدليل الإلكتروني: استكمالاً لما تم بيانه في المطلب الثالث من المبحث الأول من هذا البحث، يمكن الإشارة إلى أنه إذا ما تم الحصول على الدليل الإلكتروني بطريقة مشروعة، ومن قبل أشخاص مختصين فنياً أو علمياً، فإنه يتمتع من حيث قوته الإثباتية بقيمة قد تصل إلى درجة اليقين، شأنه في هذا شأن الأدلة العلمية مثل البصمات، والأدلة البيولوجية، ويكون بينة قانونية مقبولة يجوز لمحكمة الموضوع الاستناد إليها في الإدانة، وعلى الرغم من ذلك فإن مجرد تقديم الدليل الإلكتروني يعطي للمحكمة الصلاحية المطلقة في تقدير هذا الدليل، ويدخل ذلك ضمن الصلاحية التقديرية لقاضي الموضوع، مع التأكيد أنه لا يسوغ للقاضي استبعاد الدليل الإلكتروني إلا بواسطة دليل فني أو إلكتروني آخر يولد قناعة لدى القاضي بعدم صحة الدليل الإلكتروني المقدم. وفي جميع الأحوال، فإن الأخذ بالدليل الإلكتروني يعود إلى قناعة القاضي الوجدانية بهذا الدليل، وله في ذلك التأكد من سلامة الدليل وصحة وسلامة إجراءات الحصول عليه، فإن طرحه القاضي من عداد البينة واستبعده، عليه أن يسبب قراره ويؤيده بأسباب عدم أخذه بالدليل الإلكتروني بما جاء لديه في أوراق الدعوى، وكذلك فإن لقاضي الموضوع، إذا لم يكن باستطاعته البت في أمر الدليل الإلكتروني، أن ينتدب خبيراً آخر لتقديم رأيه في الدليل المطروح أمامه في الدعوى، وإن حق القاضي هذا ما هو إلا نتيجة حتمية لواجب المحكمة في تحري الحقيقة بشأن الوقائع المطروحة أمامها، وتكون مهمة الخبير في الحالة هذه ذات طابع قضائي، فهو يساعد المحكمة أو القاضي، ويقدم له مشورته في ناحية فنية فقط لا اختصاص أو دراية للقاضي أو للمحكمة بها، وفي النتيجة فإن خلاصة عمل الخبير التي ترد في تقريره تخضع إلى تقدير القاضي وقناعته.[56]

[56] أبو حجيلة، مرجع سابق، ص 62.

خلاصة القول، إنه إذا كانت المسألة المطلوب انتداب خبير فيها ذات طابع فني وإلكتروني بحت، بحيث لا يتصور –عقلاً أو منطقاً– أن تكفي ثقافة القاضي القانونية في حسمها، فإن رفض القاضي انتداب خبير مختص والحالة هذه، فإن رفضه هذا يكون مجافياً للمنطق السليم في الأمور، ويكون عندها الحكم معيباً.

5. الخاتمة

كنتيجة لدراسة مفهوم الأدلة الإلكترونية وأهميتها واستيضاح الموضوعات المحيطة بها من خلال التشريعات العامة والتشريع الفلسطيني خاصة، من الناحيتين القانونية والتطبيقية، ومن الناحية التقنية، توصلنا إلى أن هناك ثغرات وفراغاً تشريعياً كبيراً يعتري الدليل الإلكتروني من خلال عدم وجود منظومة قانونية متكاملة تعالج الدليل الإلكتروني، إضافة إلى وجود ضعف عام في التعامل مع هذا الواقع التكنولوجي الذي فرض نفسه على القانون والقضاء، وذلك من خلال صعوبة التعامل مع الدليل الإلكتروني وتقبله من قبل العاملين في القانون والقضاء.

أهم التوصيات:

1. تنظيم قانون ينظم العملية الإلكترونية من بداية صناعة الإلكترونيات حتى يتم إتلافها.
2. التصديق على مشروع قانون العقوبات الفلسطيني الذي عالج الجرائم الإلكترونية، ناهيك عن أن قانون العقوبات الأردني بات غير قادر على مواكبة الواقع الجرمي.
3. إقرار مشروع قانون المبادلات والتجارة الإلكتروني الذي عالج بعضاً من الأفعال الضارة الإلكترونية.
4. تعزيز عمل القضاء الفلسطيني في إصدار أحكام تستند إلى الدليل الإلكتروني طالما حاز على حجية قانونية.
5. نشر التوعية الإلكترونية بين الأفراد لتتجنبهم تلك الأضرار التي تأتي من حيث لا يدرون.
6. ضرورة اتّباع منهجية موحدة في تحصيل الدليل الإلكتروني.
7. ضرورة تمييز درجات اليقين للأدلة الإلكترونية التي تم استخلاصها أثناء البحث الجنائي الإلكتروني واعتماد القطعي منه.
8. ضرورة استخدام برمجيات وأدوات موثوقة لمعالجة الدليل الإلكتروني.
9. تدريب الكوادر الفنية على تقنيات البحث الجنائي الإلكتروني.

وأخيراً، إن اللجوء إلى استخدام الأدلة الإلكترونية في الإثبات، يحتم علينا كمتعاملين في القانون من أعضاء نيابة وقضاة ومحامين وغيرهم، الاستمرار في عمليات البحث والتطوير المستمرين حتى نكون قادرين على فهم أهمية ذلك النوع من الأدلة، وبخاصة أنها قد تكون في بعض الحالات الأدلة الوحيدة المتوفرة في الدعوى، فعلينا عندئذٍ بذل الوقت والجهد الكافيين وضمن الإمكانيات المتاحة حتى نتمكن من الوصول إلى قناعات تامة بالبراءة أو الإدانة.

6. قائمة المصادر والمراجع

أولاً. المصادر:

أ- **المواثيق الدولية والتشريعات:**

- اتفاقية الأمم المتحدة لمكافحة الفساد للعام 2003.
- قانون البيّنات الفلسطيني رقم (4) لسنة 2001.
- القرار بقانون رقم 9 لسنة 2007 بشأن مكافحة غسل الأموال.
- قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.
- قانون مكافحة الفساد المعدل بموجب القرار بقانون رقم 7 لسنة 2010.

ب- مشاريع القوانين:

- مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني.
- مشروع قانون العقوبات الفلسطيني 2001/93.
- مشروع قانون المعاملات الإلكترونية.

ثانياً. المراجع:

أ- **الكتب العربية:**

- عبد المطلب، ممدوح عبد الحميد. **البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت**، القاهرة: دار الكتب القانونية، سنة 2000.
- العبودي، عباس. **شرح أحكام قانون البينات**، عمّان: دار الثقافة للنشر والتوزيع، ط1، 2005.
- القضاة، مفلح عواد. **البينات في المواد المدنية والتجارية**. عمان: جمعية عمال المطابع التعاونية، ط1، 1990.
- مصطفى، إبراهيم وآخرون. **المعجم الوسيط**، القاهرة: مجمع اللغة العربية، ج 1.10، ط3، 1998.

ب- **الكتب الأجنبية:**

- Alexander Geschonneck (2011). *Computer-Forensik، Computerstraftaten erkennen, ermitteln، aufklären*, 5. aktualisierte und erweiterte Auflage. dpunkt verlag.
- Eoghan Casey، Susan W. Brenner (2011). *Digital evidence* and computer crime: forensic science, computers and the internet, Third Edition. Elsevier Academic Press.
- Larry E. Daniel (2012). *Digital Forensics for Legal Professionals*. Elsevier Inc.

ج- رسائل وأطروحات:

- السحيمي، رقية. **حرية الإثبات في الميدان التجاري وفق أحكام التشريع المغربي**، أكدال: جامعة محمد الخامس.
- كميل، طارق عبد الرحمن ناجي. **التعاقد عبر الإنترنت وآثاره** (رسالة دكتوراه)، أكدال: جامعة محمد الخامس – كلية العلوم القانونية والاقتصادية، 2003-2004.

د- مراجع أخرى:

أبو حجيلة، علي. "مادة تدريبية حول الأدلة الإلكترونية"، دورة قانونية عقدت في جامعة بيرزيت –معهد الحقوق، 20-2013/10/21.

هـ- مراجع إلكترونية:

- http://groups.google.com/group/ali_alsaher34

تم الاطلاع عليها في: 2013/12/15.

- http://www.almohandes.org/vb/showthread.php?t=2833

تم الاطلاع عليها في: 2013/12/15.

- http://www.techradar.com/news/software/applications/best-free-recovery-software-1141256

تم الاطلاع عليها في: 2013/12/20.

- http://en.wikipedia.org/wiki/Locard%27s_exchange_principle

تم الاطلاع عليها في: 2013/12/29.