جـامعـــة النجاح الوطنية

كليـــة الدراســـات العليـــا

إثبات الجريمة الأدلة الإلكترونية

إعداد

زيد ناصر رفعت سلمان

إشراف

د. عبد الله محمود

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الجنائي، من كلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس- فلسطين.

2025

إثبات الجريمة الأدلة الإلكترونية

إعداد

زيد ناصر رفعت سلمان

نوقشت هذه الرسالة بتاريخ 2025/10/31 م، وأجيزت:

د عبد الله محمود	التوقيع
المشرف الرئيسي	
د. وهيب ابوعلبة	التوقيع
الممتحن الخارجي	
د. فادي شديد	التوقيع
الممتحن الداخلي	

الإهداء

إلى من علّماني معنى العطاء قبل معنى النجاح...

إلى والدي العزيز،

الرجل الذي حمل عني همّ الطريق، وعلّمني أن الثبات فضيلة، وأن العلم لا يُنال إلا بالصبر والتعب. كنتَ السند الصامت، والقوة التي أستمد منها عزيمتي كلما أثقلتني الأيام. أبي، هذا الإنجاز يحمل بصمتك في كل تفاصيله، ويقف شاهدًا على عطائك الذي لا ينتظر مقابلًا.

وإلى أمي الحبيبة،

القلب الذي لم يتعب من الدعاء، والروح التي منحتني الطمأنينة في أكثر لحظاتي ضعفًا. كنتِ الأمان حين ضاقت بي الدنيا، والصوت الذي أعاد إليّ الثقة كلما ترددت. أمي، إن كان لهذا العمل روح، فهي من دعائك، وإن كان له نور، فهو من محبتك.

إلى أسرتي الكريمة،

إخوتي وأخواتي، شركاء الصبر والدعم، الذين كانوا دائمًا قريبين، ولو بصمت، وجودكم كان نعمة خفّفت ثقل الطريق وجعلت للنجاح طعمًا أجمل.

وإلى أسرة مكتب المحامي ناصر دويكات والمحامي علي البكار،

شكرًا لكم على ما قدّمتموه من دعم صادق، وبيئة مهنية قائمة على الاحترام والتعاون، كان لها أثر طيب في مسيرتي العلمية والعملية. وجودكم كان مصدر تشجيع واستقرار، وأسهم في الموازنة بين متطلبات العلم والعمل بروح إيجابية صادقة.

وإلى كل من مرّ في حياتي وترك أثرًا طيبًا،

أهدي هذا الجهد المتواضع، عربون وفاء، وخطوة أرجو أن تكون مباركة في طريق العلم والعطاء، سائلًا الله أن يجعل فيه النفع والخير

الشكر

الحمد لله الذي لا يُضيع تعب الساعين، ولا يُخيّب أمل المتوكلين عليه، والذي بنعمته وقوّته تم هذا العمل بعد رحلة طويلة من الصبر والاجتهاد.

أتقدّم بخالص الشكر وعظيم الامتنان إلى أستاذي المشرف على هذه الرسالة الدكتور عبدالله محمود ، الذي لم يكن توجيهه علميًا فحسب، بل كان دعمًا معنويًا صادقًا في مراحل كثيرة من هذه الرحلة. فقد كان حضوره العلمي، وملاحظاته الدقيقة، ونصائحه المخلصة، علامة فارقة أسهمت في بناء هذه الرسالة وإخراجها إلى النور.

كما أتوجّه بجزيل الشكر والتقدير إلى أعضاء لجنة المناقشة الأفاضل، لما أولوه من وقت وجهد، وما قدّموه من ملاحظات علمية رصينة أسهمت في تقويم هذه الدراسة وتعزيز قيمتها العلمية.

ولا يسعني إلا أن أعبّر عن امتناني لكل أستاذ ومعلم كان له أثر في تكوين شخصيتي العلمية، ولكل من وقف إلى جانبي بكلمة طيبة، أو دعاء صادق، أو تشجيع خفي، فكان لكل ذلك أثر عميق لا يُقاس بالكلمات.

وإلى كل من شاركني هذه الرحلة بصبره، وتفهّمه، ودعمه، أقول: شكرًا بقدر ما كان الطريق طويلًا، وبقدر ما كان الوصول مستحقًا.

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

إثبات الجريمة الأدلة الإلكترونية

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: **زيد ناصر رفعت سلمان**

التوقيع: 

التاريخ: **2025/10/31**

فهرس المحتويات

إثبات الجريمة الأدلة الإلكترونية

اعداد

زيد ناصر رفعت سلمان

إشراف

د. عبد الله محمود

الملخص

هدفت الدراسة للبحث في الضمانات القانونية التي توفرها التشريعات الفلسطينية للأدلة الإلكترونية في الإثبات الجنائي، عبر تحليل هذه الضمانات مع التركيز على كيفية جمع الأدلة الإلكترونية، وضمانات المحاكمة العادلة بما في ذلك شروط قبول الدليل الإلكتروني، وحق الدفاع؛ لغاية إبراز مدى نجاح المنظومة القانونية الفلسطينية في توفير ضمانات عادلة للمتهمين في ضوء التشريعات النافذة، كما استعرض النصوص المتعلقة بذلك في القوانين الفلسطينية. كما يستكشف الباحث الإجراءات العملية التي تتم خلال التعامل مع الدليل الإلكتروني، بدءًا من جمعه وحتى تقديمه أمام المحكمة.

وقد عتمد الباحث المنهج الوصفي التحليلي في جمع البيانات وتحليلها وتفسيرها لتحقيق هدف الدراسة، إلى جانب المنهج المقارن. هذا وتوصلت الدراسة إلى جملة من النتائج أهمها أن التشريعات الفلسطينية توفر العديد من الضمانات للدليل الإلكتروني كما توصل الباحث إلى أن منظومة التعامل مع الأدلة الإلكترونية أكثر وضوحا في عرض الضمانات والالتزام فيها مقارنة بالأدلة التقليدية، وفي نهاية الدراسة، يوصي الباحث بضرورة تطوير الكوادر المتخصصة في التعامل مع الأدلة الإلكترونية، وتعزيز التعاون بين الدول والمحاكم في تنفيذ الأحكام. كما يقترح إنشاء مؤسسة متخصصة للتعامل مع الأدلة الإلكترونية لتحسين فعالية العدالة.

الكلمات المفتاحية: الدليل الإلكتروني، المحاكمة العادلة، حق المتهم، التشريعات الفلسطينية.

المقدمة

تهدف الجهات المختصة من خلال البحث والتفتيش في الوسائل الإلكترونية والوصول للدليل الإلكتروني إلى تحقيق غايات تقديرية، وكذلك تقديمه أمام المحكمة للاستناد إليه في بناء الحكم.

تعالج هذه الدراسة التنظيم الإجرائي للدليل الإلكتروني من خلال استعراض الضوابط القانونية المتعلقة بالشق الإجرائي في التشريعات الفلسطينية، بالإضافة إلى البنيان القانوني للبحث عن الأدلة الإلكترونية. وبالتوازي مع ذلك، تراعى الدراسة الضمانات القانونية أثناء عملية البحث والتحري في الوسائل الإلكترونية والآليات المتبعة في عملية التفتيش عن الأدلة الإلكترونية في الأجهزة الإلكترونية. علاوة على ذلك، تعالج الدراسة أيضًا الشق الموضوعي للدليل الإلكتروني على الصعيد العلمي، حيث تستعرض آراء الفقهاء حول ماهية الدليل وعملية شرعنة هذا الدليل الناتج عن الوسائل الإلكترونية في إثبات الجريمة أمام القضاء الجنائي. وأخيرًا، تبحث في كيفية اعتبار التشريعات السارية في فلسطين لحجية الدليل أمام المحاكم وجهات الاختصاص.

اتبع الباحث في هذه الدراسة المنهج الوصفي التحليلي و ذلك بدراسة الآراء الفقهية المتعلقة بموضوعية الدليل الإلكتروني على المستوى العلمي و دراسة التشريعات الفلسطينية المتمثلة في قانون الإجراءات الجزائية رقم (3) لسنة 2001 و القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية و تعديلاته ، من أجل دراسة دستورية التعامل مع الأدلة الإلكترونية و جعلها وسيلة قانونية من وسائل الاثبات الجنائي أمام المحاكم المختصة في فلسطين على وجه الخصوص .

ومن اجل معالجة هذه الإشكالية تناول الباحث مفهوم دليل الإلكتروني الاثبات الجنائي والأدلة الجنائية المتعلقة في الجريمة والتركيز على التنظيم القانوني للدليل الإلكتروني ودراسة وسائل جمع الأدلة الالكترونية ومدى حجية الدليل الإلكتروني في اثبات الجريمة.

إشكالية الدراسة

تتمثل إشكالية هذه الدراسة في عدم وجود قواعد قانونية متكاملة تنظم آلية التعامل مع الدليل الإلكتروني الالكتروني و الحفاظ عليه ليكون له بينة قوية امام القضاء الجنائي في اثبات الجريمة ، على الرغم من نص المشرع في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية و تعديلاته على أن الدليل الناتج من الوسائل الالكترونية هو وسيلة من وسائل الاثبات لكن بقي القصور التشريعي في عملية تنظيم مسألة التعامل مع هذا الدليل الناتج من الوسيلة الالكترونية لاثبات الجريمة سواء كانت تقليدية أم جريمة الكترونية ، حتى بالعودة الى القواعد العامة في قانون الإجراءات الجزائية رقم (3) لسنة 2001 التي تحكم الأدلة الجنائية بصورة عامة لا نجد أي تنظيم قانوني يتعلق في الدليل أو مدى جوازيته أمام القضاء و غير ذلك من الأمور التي تتعلق في تنظيم التعامل معه و احترام مبدأ خصوصية المتهم .

حيث جرى تقسيم هذه الدراسة من اجل الاجابة السؤال الرئيسي المتمثل في مشكلة الدراسة و هو : ما مدى حجية الدليل الالكتروني في اثبات الجريمة في ضوء التشريعات السارية في فلسطين ؟ ، ومن أجل معالجة هذه الإشكالية تناول الباحث أولا مفهوم الدليل الإلكتروني من اجل دراسة مفهوم الدليل الإلكتروني و الاثبات الجنائي في المبحث الاول منه و الادلة الجنائية المتعلقة في الجريمة و التركيز على التنظيم القانوني للدليل الإلكتروني في المبحث الثاني ، أما الفصل الثاني منه و الذي بعنوان: حجية الدليل الإلكتروني و ذلك لدراسة وسائل جمع الأدلة الالكترونية و مدى حجية الدليل الإلكتروني في اثبات الجريمة في المبحث الثاني منه .

و يثور التساؤل الرئيسي في هذه الدراسة : ما مدى حجية الدليل الالكتروني في اثبات الجريمة في ضوء التشريعات السارية في فلسطين ؟

أهداف الدراسة

في هذه الدراسة، سوف يتم دراسة عدة جوانب، أبرزها:

1. تهدف هذه الدراسة بشكل أساسي إلى تحديد القيمة القانونية للدليل الإلكتروني وتسعى لبيان مدى حجيته كوسيلة إثبات معتمدة في الجرائم التقليدية.
2. دراسة القواعد الاجرائية لسلطة النيابة العامة في تحريك الدعوى الجزائية بعد ورود لها اوراق الدعوى من جهات الاختصاص ومدى صلاحياتهم في التحقيق من اجل الحصول على دليل إلكتروني
3. دراسة واستيضاح الدليل الالكتروني وهل له قيمة ثبوتية أمام المحكمة المختصة أو جهات الادانة و التحقيق.
4. استيضاح الشرعية الاجرائية و الموضوعية للحصول على الدليل الإلكتروني

أهمية الدراسة

الاهمية من الناحية النظرية: تكمن أهمية الدراسة من الناحية العلمية في فهم التطور المتسارع الذي حظيت به وسائل اثبات الجريمة حيث من أهم وسائل الاثبات في العصر الحديث هو الدليل الإلكتروني الذي تعددت آراء الفقهاء حوله فمنهم من اعتبر أن الدليل الالكتروني وهو وسيلة من وسائل الاثبات الإلكترونية فحسب ورأي آخرون أنه وسيلة من وسائل اثبات الجرائم التقليدية أيضا نظرا لحداثة علم الاجرام، ولكن يرى الباحث ان الدليل الإلكتروني هو وسيلة من وسائل اثبات الجرائم بكافة أنواعها و اشكالها، وتعددت أيضا آراء الفقهاء في وضع مفهوم محدد للدليل الإلكتروني فاعتبره البعض مثل قاموس (كامبرج) على أنه شيفرات تتكون من إلكتروني (01) فقط وأنه متعلق بالفعل الإلكتروني الالكتروني، وكان لرأي آخر مثل كاري مورجان أنه وسيلة من وسائل الاثبات أمام القضاء، ولذلك تكمن أهمية الدراسة من الناحية العلمية في تحديد مفهوم الدليل الإلكتروني الالكتروني والآليات المتبعة في الحفاظ عليه والتعامل معه كوسيلة من وسائل الاثبات وهذا من خلال عملية تحليل الآراء الفقهية للوصول الى مشروعية الدليل الإلكتروني أمام القاضي الجنائي، ويرى

الباحث في هذا الصدد أن للدليل الالكتروني قيمة ووزن أمام المحكمة المختصة وعلى ضوء ذلك حذت الدراسة.

الاهمية من الناحية الإجرائية: لقد تمثلت الأهمية العملية في الجوانب الإجرائية التي تنظم العلاقة بين الجريمة و الدليل الإلكتروني من حيث اعتبار الدليل الإلكتروني وسيلة من وسائل الاثبات وفقا لما جاء في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته خاصة ما ورد في المادة (37) منها والتي اعتبرت كل دليل نتج عن الوسائل الالكترونية هو دليل من أدلة الاثبات أمام المحاكم المختصة كما واعتبر ذات القرار بقانون أن الدليل الإلكتروني هو عملية من عمليات التفتيش وحدد ماهية الضوابط الإجرائية التي تنظم عملية التفتيش عن الأدلة الإلكترونية و الاستعانة بالخبراء و غير ذلك و فقا لأحكام المادة (32) منه.

محددات الدراسة

الحدود المكانية : تكمن الحدود المكانية لهذه الدراسة في اقليم الأراضي الفلسطينية و الاقاليم النافذ بها التشريعات في الحدود التشريعية للدراسة.

الحدود الزمانية : منذ سريان التشريعات و القوانين الواردة في الدراسة .

الحدود التشريعية (الموضوعية) : و التي تكمن في قانون الإجراءات الجزائية رقم 3 لسنة 2001 خاصة المواد و النصوص القانونية التي تتعلق في اثبات الجريمة و جمع الأدلة الجنائية ، و القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية و تعديلاته و خاصة تلك النصوص المتعلقة بالدليل الإلكتروني .

منهج الدراسة

اتبع الباحث في دراسته المنهج الوصفي التحليلي، وذلك من خلال تحليل النصوص القانونية المتعلقة بالقواعد الخاصة بالجريمة، والتي وردت في كل من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، والقرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته. وقد قام الباحث بوصف هذه النصوص وصفًا دقيقًا بما يتناسب مع آراء الفقه القانوني والمدرستين الجنائيتين الحديثة والتقليدية، مع تدعيم التحليل بقرارات وأحكام قضائية.

وفي الوقت ذاته، استقرأ الباحث النصوص القانونية التي تخدم مسألة البحث، والتي تدور حول علاقة الدليل الإلكتروني بإثبات الجرائم بصورتيها التقليدية والإلكترونية. كما استعان ببعض الآراء الفقهية وقرارات المحاكم في دول أخرى للمقارنة.

خطة الدراسة

الفصل الأول: الإطار النظري للدليل الإلكتروني في الإثبات الجنائي

المبحث الأول: ماهية الدليل الإلكتروني

المطلب الأول: مفهوم الدليل الإلكتروني

المطلب الثاني: الخصائص العامة للدليل الإلكتروني

المبحث الثاني: تصنيف أنواع الدليل الإلكتروني

المطلب الأول: التصنيف حسب طبيعة المصدر

المطلب الثاني: التصنيف حسب القصد من الإنشاء

الفصل الثاني: حجية الدليل الإلكتروني وشروط استخدامه أمام القضاء

المبحث الأول: حجية الدليل الإلكتروني في الإثبات الجنائي

المطلب الأول: الأساس القانوني لحجية الدليل الإلكتروني

المطلب الثاني: شروط قبول الدليل الإلكتروني أمام القضاء

المبحث الثاني: الجهات المختصة بجمع وتحليل الدليل الإلكتروني

المطلب الأول: التحديات الإدارية والتقنية أمام النيابة العامة في التعامل مع الجرائم الإلكترونية

المطلب الثاني: دور وحدة الجرائم الإلكترونية الفنية

المطلب الثالث: أهمية التنسيق بين الجهات الأمنية والقضائية

الفصل الأول

الإطار النظري للدليل الإلكتروني في الإثبات الجنائي

في ظل التطورات المتسارعة في مجال تكنولوجيا المعلومات، تغيّرت ملامح الجريمة ووسائل ارتكابها، وانتقلت من الحيز الواقعي التقليدي إلى الفضاء الإلكتروني الواسع. هذا التحول لم يقتصر على الجريمة فحسب، بل طال أيضًا أدوات مكافحتها وسبل إثباتها، حيث برز الدليل الإلكتروني كأحد أبرز الوسائل المعاصرة التي تلعب دورًا حاسمًا في الكشف عن الحقيقة في القضايا ذات الطابع الإلكتروني. وقد أصبح هذا النوع من الأدلة ضرورة لا غنى عنها في منظومة العدالة الجنائية الحديثة، مما استوجب فهمه بدقة من حيث المفهوم، والخصائص، والتطور، لا سيما وأن طبيعته غير المادية تفرض تحديات قانونية وفنية تستدعي معالجة خاصة تضمن احترام حقوق الأفراد وتحقيق العدالة.

ولأهمية هذا الموضوع، يسعى الباحث في هذا الفصل إلى بناء إطار نظري متكامل للدليل الإلكتروني في الإثبات الجنائي، من خلال الوقوف على ماهيته كمفهوم قانوني وتقني، وتحليل خصائصه التي تميّزه عن الأدلة التقليدية، خاصة تلك المتعلقة بقابليته للتعديل وسهولة نسخه أو فقدانه. كما يتطرق الفصل إلى لمحة تاريخية عن نشأة هذا الدليل وتطوره على المستويين الدولي والعربي، بما يساعد على فهم الإشكاليات المرتبطة به في السياق التشريعي الفلسطيني، ومن ثم تهيئة الأساس النظري لفهم آليات التعامل معه إجرائيًا في الفصول التالية.

المبحث الأول: ماهية الدليل الإلكتروني

مع تنامي الاعتماد على الوسائل الإلكترونية في مختلف مناحي الحياة، أصبحت الجرائم المرتكبة عبر الفضاء الإلكتروني واقعًا ملموسًا يفرض تحديات قانونية غير مسبوقة. وفي ظل هذا التحول، لم تعد أدوات الإثبات التقليدية كافية لمواجهة هذا النمط من الجرائم الذي غالبًا ما يترك خلفه أدلة غير مادية، تتخذ شكل بيانات إلكترونية. وهنا تبرز الحاجة إلى فهم دقيق لماهية "الدليل الإلكتروني" باعتباره الأداة المركزية في هذا النوع من القضايا.

ينطلق هذا المبحث من محاولة تقديم تعريف واضح وشامل لمفهوم الدليل الإلكتروني، بالاستناد إلى الأبعاد اللغوية، الاصطلاحية، والتشريعية، وصولًا إلى استعراض تطوره التاريخي والتقني، سواء على الصعيد الدولي أو في السياق العربي، مع الإشارة إلى أبرز المحطات التي ساهمت في ترسيخ مكانته في منظومة العدالة الجنائية الحديثة.

كما يتناول المبحث الخصائص الفريدة التي تميز هذا النوع من الأدلة، لا سيما من الناحية التقنية، مثل قابلية النسخ وسرعة التلف وإمكانية التعديل، فضلًا عن الخصائص القانونية التي تفرض شروطًا دقيقة لضمان مشروعيته وسلامته عند تقديمه أمام القضاء. وتكمن أهمية هذه الخصائص في كونها تُحدد مدى اعتماد الدليل الإلكتروني كوسيلة إثبات معتبرة، وتؤسس للمعايير التي يجب أن تتوافر فيه ليكتسب حجية قانونية كاملة.

وبناءً عليه، ينقسم هذا المبحث إلى مطلبين أساسيين:

- المطلب الأول يُخصص لتعريف الدليل الإلكتروني واستعراض تطوره التاريخي والتقني.
- المطلب الثاني يُعالج الخصائص العامة للدليل الإلكتروني، التقنية منها والقانونية، بوصفها المدخل لفهم حجيته أمام القضاء.

المطلب الأول :مفهوم الدليل الإلكتروني المطلب الأول

مع تزايد اعتماد المجرمين على الوسائل الإلكترونية في ارتكاب الجرائم وتضليل العدالة، برزت الحاجة الماسة إلى تطوير وسائل الإثبات بما يتلاءم مع هذه البيئة الإلكترونية الجديدة. فقد أصبحت آثار الجريمة لا تُلتقط فقط من مسرح الجريمة التقليدي، بل أيضاً من الأجهزة الذكية، وسجلات البيانات، والمواقع الإلكترونية، مما فرض على المنظومة القضائية ضرورة استيعاب مفهوم "الدليل الإلكتروني" كوسيلة إثبات معاصرة وفعالة.

ويمثّل هذا النوع من الأدلة تحديًا مزدوجًا: من جهةٍ، هو يحمل قيمة كبيرة في الكشف عن الحقيقة الجنائية وتحديد هوية الجناة، ومن جهة أخرى، يتطلب فهماً دقيقاً لطبيعته التقنية والمعالجة القانونية التي تضمن عدم المساس بمبدأ العدالة وحقوق الدفاع.

وفي ضوء ما سبق، يتناول هذا المطلب تحديد مفهوم الدليل الإلكتروني من خلال ثلاث زوايا تحليلية أساسية:

- الفرع الأول يعرض التعريف اللغوي والاصطلاحي لمفهوم الدليل الإلكتروني، بهدف توضيح الإطار المفاهيمي الذي يُبنى عليه التكييف القانوني.
- الفرع الثاني يتناول موقف التشريع الفلسطيني من الدليل الإلكتروني، من حيث الاعتراف القانوني به وتنظيمه الإجرائي ضمن النصوص القانونية السارية.
- الفرع الثالث يُقدّم لمحة تاريخية عن نشأة وتطور هذا النوع من الأدلة، بهدف فهم الخلفية الزمنية والتشريعية التي أدّت إلى بروز الدليل الإلكتروني كعنصر إثبات رئيسي في الأنظمة الجنائية الحديثة.

ويهدف هذا التمهيد إلى تقديم تصور واضح لجوهر الدليل الإلكتروني، باعتباره نتاجاً لتقاطع التكنولوجيا مع القانون، وأداةً حديثةً تتطلب إطاراً تشريعيًا وتقنيًا متطورًا لاستيعابها ضمن منظومة العدالة الجنائية.

الفرع الأول: التعريف اللغوي والاصطلاحي للدليل الإلكتروني

تُعد عملية تحديد المفاهيم من الأسس الجوهرية لأي دراسة قانونية منهجية، خصوصًا إذا كان الموضوع يتعلق بمصطلح حديث نسبيًا، ويشهد تطورًا سريعًا في مضمونه القانوني والفني، كما هو الحال مع الدليل الإلكتروني. إذ إن هذا النوع من الأدلة لم يعد يقتصر على القضايا التقنية أو المعلوماتية فحسب، بل امتد ليشمل كافة مجالات الإثبات الجنائي، مما يستوجب الإلمام التام بأبعاده المفاهيمية، سواء على المستوى اللغوي أو الاصطلاحي، لتمييزه عن غيره من الأدلة التقليدية.

أولًا: التعريف اللغوي

يُعد التحليل اللغوي نقطة انطلاق ضرورية في دراسة أي مفهوم قانوني حديث، حيث يُسهم في ضبط المعنى العام للمصطلح وتحديد دلالاته الأولية التي تقوم عليها المفاهيم الاصطلاحية والتشريعية لاحقًا. وفي هذا السياق، يتكوّن مصطلح "الدليل الإلكتروني" من تركيب إضافي يجمع بين لفظتين هما "الدليل" و"الإلكتروني"، ولكل منهما دلالته اللغوية المستقلة التي تُسهم في تشكيل الإطار العام للمعنى.

لفظ "الدليل" مأخوذ من الجذر (د ل ل)، وهو جذر عربي أصيل يُشير إلى الإرشاد والهداية إلى شيء ما. وقد جاء في "لسان العرب" لابن منظور أن: "الدليل هو ما يُستدل به، والهادي إلى الطريق، والدليل على الأمر ما يُرشد إلى معرفته" (ابن منظور، 1993، ج4، ص122). كما ورد في "المعجم الوسيط" أن الدليل هو "ما يدل على الشيء ويوصل إلى معرفته، سواء كان حسِّيًا أو عقليًا" (مجمع اللغة العربية، 2004، ص301). وبذلك يُفهم أن الدليل في أصل معناه وسيلة يُرشد بها العقل أو الحواس إلى التوصل إلى الحقيقة أو إثبات أمر معين.

أما لفظ "الإلكتروني" فهو من الكلمات المعاصرة التي ارتبطت بظهور التكنولوجيا ووسائط المعالجة الإلكترونية للمعلومات. ويُشتق من "رقم"، أي العدد، وقد تطور ليأخذ معنى اصطلاحيًا يدل على كل ما يُعالج باستخدام النظام الثنائي (0 و1). وقد عرّفه "المعجم التقني للمصطلحات الحاسوبية" الصادر عن المنظمة العربية

للتربية والثقافة والعلوم (الألكسو)، بأنه: "البيانات التي تُخزن أو تُعالج إلكترونيًا في شكل أرقام ثنائية، قابلة للقراءة أو التحليل بواسطة أنظمة الحاسوب أو البرمجيات الإلكترونية" (الألكسو، 2020، ص147). كما ورد في "معجم مصطلحات الحاسوب والإنترنت" لمجمع اللغة العربية بالقاهرة أن "الإلكتروني" هو: "ما يُمثل أو يُخزن أو يُنقل باستخدام إشارات عددية ثنائية، ويُقابل التماثلي أو التناظري" (مجمع اللغة العربية بالقاهرة، 2013، ص85).

وبذلك، فإن "الإلكترونية" لا تعني فقط الأرقام، بل تشمل البيئة الإلكترونية الكاملة التي يتم فيها إنتاج البيانات وتخزينها وتحليلها واسترجاعها، سواء كانت هذه البيانات نصوصًا أو صورًا أو أصواتًا أو حتى إشارات مخفية تحتاج إلى تقنيات متقدمة لاستخلاصها.

بناءً على ما سبق، فإن التركيب اللغوي لمصطلح "الدليل الإلكتروني" يُشير إلى: الوسيلة أو الأداة التي يُستدل بها على أمرٍ ما، ويكون محتواها إلكترونيًا ناتجًا عن بيئة إلكترونية، يتم تخزينه أو معالجته أو نقله من خلال أنظمة إلكترونية.

ولتقريب المعنى بشكل تطبيقي، فإن البريد الإلكتروني الذي يتضمن مراسلات بين أطراف في قضية جنائية، أو سجل تصفح جهاز حاسوب استخدم في عملية احتيال إلكتروني، يُمكن اعتبارهما دليلاً إلكترونيا بالمعنى اللغوي، إذ أنهما يحتويان على بيانات إلكترونية تُستخدم في الاستدلال على وقوع جريمة أو تحديد هوية الجاني.

ثانيًا: التعريف الاصطلاحي – القانوني للدليل الإلكتروني

من الناحية القانونية، لا يزال مفهوم "الدليل الإلكتروني" محل نقاش واسع بين الفقهاء والمشرّعين، بسبب حداثته النسبية وتنوع أشكاله وسرعة تطوره في ظل الطفرة التكنولوجية. إذ لم تعتمد التشريعات الوطنية أو الدولية بعد تعريفًا موحدًا جامعًا لهذا المفهوم، الأمر الذي يترك مساحة لاجتهادات فقهية متباينة حاولت ضبط ملامحه وإبراز خصائصه القانونية.

وقد عرّفه (زايد، 2022، صفحة 30) بأنه: "مجموعة من المعلومات الإلكترونية المخزنة أو المرسلة عبر وسيط إلكتروني، والتي يمكن الاستناد إليها أثناء التحقيق أو المحاكمة لإثبات أو نفي التهمة"، في إشارة إلى الطابع الإجرائي للدليل الإلكتروني بوصفه أداة من أدوات الإثبات.

أما (عبد العال، 2021، صفحة 640) فقد شدد على الجانب الفني، واعتبره: "منتجًا تكنولوجيًا ناتجًا عن عمليات تخزين ومعالجة إلكترونية، يتطلب تحليلًا متخصصًا ليكون صالحًا كوسيلة إثبات"، ما يُبرز الحاجة إلى معرفة تقنية لدى القاضي أو المحقق للتعامل معه بشكل صحيح.

في المقابل، ركّز (الجلعود، 2024، صفحة 2385) على الخصائص التقنية للدليل الإلكتروني، وعرّفه بأنه: "كيان مستقل عن الأدلة الورقية، يتمتع بخصائص إلكترونية فريدة ويستلزم بيئة خاصة في جمعه وفحصه تضمن عدم المساس بمحتواه أو قابليته للتغيير". هذا التعريف يُلفت الانتباه إلى حساسية هذا النوع من الأدلة مقارنة بالأدلة التقليدية، لا سيما في مراحل الجمع والتحليل والحفظ.

أما على الصعيد الدولي، فقد عرّف(Casey , 2022, p. 4) الدليل الإلكتروني بأنه: "أي معلومة ذات قيمة محتملة في التحقيق، يتم تخزينها أو نقلها باستخدام وسيط إلكتروني، وتستلزم إجراءات محددة للحفاظ على مصداقيتها وسلامتها أثناء المعالجة القضائية"، وهو تعريف يتماشى مع المبادئ الدولية في التعامل مع الأدلة الإلكترونية وفق قواعد العدالة الإجرائية.

ويُمكن استنتاج أن جميع هذه التعريفات تلتقي في نقاط أساسية، أهمها:

- أن الدليل الإلكتروني يقوم على محتوى معلوماتي إلكتروني.
- أنه يتطلب بيئة خاصة وتقنيات معينة للتعامل معه.
- وأنه وسيلة إثبات معترف بها قانونًا متى استوفيت شروط الصحة والسلامة الإجرائية.

ويرى الباحث أن هذا التباين في التعريفات الاصطلاحية يُظهر الحاجة المُلحّة إلى تبني تعريف تشريعي موحد يتوافق مع التطورات الإلكترونية المتسارعة، ويُراعي الخصائص التقنية الفريدة لهذا النوع من الأدلة.

فبينما يُسهم المعنى اللغوي في فهم طبيعة الدليل بوصفه وسيلة استدلال، فإن المقاربة القانونية تتطلب ضبط شروط قبوله كدليل مشروع في الإجراءات الجنائية. وبالتالي، فإن توحيد المفهوم يُعد خطوة محورية نحو تحقيق عدالة جنائية متوازنة في العصر الإلكتروني، وضمان حقوق الأفراد والمؤسسات أمام القضاء.

وبناءً على ما سبق، يتبنى الباحث تعريفًا إجرائيًا للدليل الإلكتروني، بوصفه: كيانًا معلوماتيًا غير مادي، يتكون من بيانات إلكترونية مخزنة على وسيط إلكتروني أو منقولة عبر الشبكات، ويصلح كأداة إثبات في الإجراءات الجنائية متى استوفى شروط الصحة والسلامة، والتي تتطلب اتباع إجراءات تقنية وقانونية صارمة لضمان مصداقيته وحمايته من التغيير أو التلف، بما يحفظ قيمته الثبوتية أمام القضاء.

الفرع الثاني: موقف التشريع الفلسطيني من الدليل الإلكتروني

يُعد تنظيم الدليل الإلكتروني واحدًا من التحديات المعاصرة التي تواجه المشرّع الفلسطيني في ظل الثورة التكنولوجية المتسارعة، خاصة مع دخول التقنيات الإلكترونية إلى مختلف مجالات الحياة، ومنها المجال الجنائي. ورغم هذا التطور، فإن القوانين الفلسطينية التقليدية لم تكن مُهيّأة بعد للتعامل مع هذا النوع المستحدث من الأدلة، سواء من حيث الاعتراف به، أو من حيث آليات تنظيمه إجرائيًا وتقنيًا.

فبالرجوع إلى قانون الإجراءات الجزائية رقم (3) لسنة 2001، وقانون البينات رقم (4) لسنة 2001، يتضح غياب أي نص يُشير صراحة إلى "الدليل الإلكتروني"، سواء تعريفًا أو تنظيمًا. ويرجع ذلك إلى الفترة الزمنية التي صدر فيها هذان القانونان، إذ لم تكن البيئة الإلكترونية في فلسطين أو العالم العربي عمومًا قد تطورت بما يكفي لفرض هذه القضايا على النقاش التشريعي.

ولم يتدارك المشرّع هذا الفراغ إلا بعد مرور أكثر من 15 عامًا، عندما أصدر (القرار بقانون) قانون الجرائم الإلكترونية رقم (10) لسنة 2018، الذي يُعد أول نص قانوني فلسطيني يتضمن إشارة إلى الأدلة الإلكترونية. فقد نصّت المادة (37) من هذا القانون على ما يلي:

"يُعد الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات." (الوقائع الفلسطينية، العدد 144، 2018، ص5) .

وهذا النص يُعد تطورًا مهمًا في البنية التشريعية الفلسطينية، حيث يُقر للمرة الأولى بحجية الأدلة المستخرجة من الوسائط الإلكترونية في الإثبات، سواء كانت أجهزة حاسوب، أو هواتف ذكية، أو مواقع إلكترونية، أو شبكات تواصل اجتماعي، أو أنظمة إلكترونية متقدمة. غير أن هذا الإقرار جاء بصيغة عامة جدًا، ولم يتضمن أي تفصيل يخص:

- طبيعة هذا الدليل،
- أو المعايير الفنية والإجرائية لضمان صلاحيته،
- أو الجهات المخوّلة بجمعه وفحصه وتحليله،
- أو شروط تقديمه أمام المحكمة.

وقد أشار أبو سمرة (2020) إلى أن هذا النص يعاني من "الاختزال التشريعي"، موضحًا أن الصياغة العامة تفتح المجال لتأويلات قضائية متعددة قد تضر بحقوق الدفاع أو تؤثر على مشروعية الإجراءات (أبو سمرة، 2020، ص178). كما نوّه عوض الله (2022) إلى أن "غياب منظومة إجرائية مرافقة للنص التشريعي أضعف فعاليته في التطبيق، وترك الباب مفتوحًا أمام إسقاط أدلة مهمة لاعتبارات شكلية أو تقنية لم تُحدد في القانون" (عوض الله، 2022، صفحة 213)

وعلى مستوى التطبيقات القضائية، تُظهر التقارير الحقوقية والممارسات العملية وجود تفاوت في التعامل مع الأدلة الإلكترونية. ففي بعض القضايا، قُبلت رسائل "واتساب" وصور إلكترونية كأدلة، شريطة مصادقة الطرف المُستهدف عليها. وفي حالات أخرى، رفضت المحكمة اعتمادها لعدم إثبات صدورها من المتهم يقينًا، مما يُظهر التردد في بناء سوابق قضائية راسخة بهذا الشأن (مركز الميزان لحقوق الإنسان، 2023؛ الهيئة المستقلة لحقوق الإنسان، 2022).

أما بالمقارنة مع النظم القانونية الدولية، فإن الوضع يبدو مختلفًا. فاتفاقية بودابست بشأن الجرائم الإلكترونية لعام 2001، والتي تُعد الإطار القانوني الدولي الأهم في هذا المجال، تضع معايير واضحة لجمع الأدلة الإلكترونية وتحليلها، مثل ضرورة وجود إجراءات تحفظ "سلسلة الحفظ الإلكترونية" (Digital Chain of Custody)، وتفرض اعتماد أدوات فنية موثوقة لضمان عدم تغيير محتوى الأدلة خلال التعامل معها. (Council of Europe, 2001)

كما أن بعض الدول العربية، مثل الأردن والإمارات، قد أصدرت لوائح تنفيذية تفصيلية لتنظيم الأدلة الإلكترونية. فمثلاً، أصدرت النيابة العامة الأردنية تعليمات عام 2021 تُحدد ضوابط جمع الأدلة الإلكترونية من الهواتف والحواسيب، بما في ذلك ضمان الحفظ، والتحقق من مصدر الدليل، والفحص الإلكتروني الشرعي (النيابة العامة الأردنية، 2021).

ويرى الباحث أن موقف التشريع الفلسطيني من الدليل الإلكتروني ما زال في مرحلة التأسيس النظري غير المكتمل. فالمادة (37) من القرار بقانون قانون الجرائم الإلكترونية تُشكل خطوة مهمة نحو إدماج الوسائل الإلكترونية في منظومة الإثبات، لكنها غير كافية لضمان سلامة الإجراءات وعدالة المحاكمة. فبدون تنظيم واضح لآليات جمع وفحص وتقديم هذه الأدلة، يبقى الدليل الإلكتروني عرضة للتشكيك أو الاستبعاد، مما يُضعف قدرة القضاء الفلسطيني على الاستفادة من الأدلة الإلكترونية التي أصبحت اليوم من أهم وسائل الإثبات في الجرائم الحديثة.

لذا، يُوصى بأن يُستكمل هذا الاعتراف التشريعي بإطار قانوني تنفيذي يُحدد المعايير الفنية والإجرائية التي يجب الالتزام بها، ويُتيح المجال أمام تأهيل الكوادر القضائية والأمنية للتعامل المهني مع هذا النوع المعقّد من الأدلة، بما يُحقق التوازن بين حماية الحقوق وحفظ النظام العام، ويُعزز من ثقة المواطنين بعدالة النظام القضائي في البيئة الإلكترونية.

الفرع الثالث: لمحة عن النشأة والتطور التاريخي للدليل الإلكتروني

برز مفهوم الدليل الإلكتروني كنتيجة مباشرة للتطورات التكنولوجية المتسارعة التي غيّرت ملامح الحياة اليومية، لا سيما في ظل انتشار الحواسيب وشبكات الإنترنت منذ مطلع سبعينيات القرن الماضي. وقد بدأت تظهر آنذاك أولى صور الجرائم الإلكترونية التي استهدفت قواعد البيانات والمعلومات البنكية والمؤسساتية، ما استدعى تفكيرًا جديدًا في وسائل الإثبات التي يمكن أن تعتمد على آثار إلكترونية غير ملموسة.

في عام 1984، سجّلت الولايات المتحدة الأمريكية أول استخدام رسمي للدليل الإلكتروني في تحقيقات مكتب التحقيقات الفيدرالي (FBI) بقضية اختراق شبكات حاسوبية حساسة، ما شكّل نقطة انطلاق للاعتراف العملي بهذا النوع الجديد من الأدلة (Casey , 2022). ومنذ ذلك الوقت، بدأ تطور سريع في البنية القانونية والتقنية للأدلة الإلكترونية في الأنظمة القضائية الغربية.

وفي المملكة المتحدة، تم إقرار قانون الاتصالات الإلكترونية لسنة 1999 (Electronic Communications Act)، الذي مهّد الطريق للاعتراف القانوني بالوثائق والرسائل الإلكترونية كأدلة رسمية. كما أدخلت الولايات المتحدة تعديلات جوهرية على قواعد الإثبات الفيدرالية (Federal Rules of Evidence) عام 2006، تضمنت المادة 902 التي أتاحت قبول الأدلة الإلكترونية دون الحاجة لشهادة مختص إذا كانت موثقة بتوقيع إلكتروني معتمد.

على المستوى الدولي، تُعد اتفاقية بودابست حول الجرائم الإلكترونية لعام 2001 من أهم المحطات في تقنين الأدلة الإلكترونية، حيث دعت إلى وضع معايير موحدة لحفظ وتبادل وتحليل الأدلة الإلكترونية بين الدول، خاصة فيما يتعلق بمكافحة الجرائم ذات الطابع العابر للحدود (Council of Europe, 2001).

أما على الصعيد العربي، فقد اتخذت بعض الدول خطوات متقدمة في العقدين الأخيرين. ففي الإمارات العربية المتحدة، نص القانون الاتحادي رقم (5) لسنة 2012 على مشروعية الدليل الإلكتروني وأوجب احترام الإجراءات الفنية في جمعه وتحليله. كما أقرّت مصر بموجب قانون مكافحة جرائم تقنية المعلومات

رقم (175) لسنة 2018 مجموعة من الضوابط التي تُنظم استخدام الأدلة الإلكترونية أمام القضاء (مرسي، 2020، صفحة 95) وعلى الرغم من ذلك، لا تزال هناك فجوات في الجانب الفني والبنية التحتية القانونية في كثير من الدول العربية.

أما في فلسطين، فقد تم الاعتراف بالدليل الإلكتروني لأول مرة في قانون الجرائم الإلكترونية رقم (10) لسنة 2018، حيث نصّت المادة (37) منه على اعتبار كل ما يُستخرج أو يُنتج بوسائل إلكترونية من أدلة الإثبات، لكنه لم يُواكب هذا الاعتراف تعديلٌ في قانون الإجراءات الجزائية رقم (3) لسنة 2001 ولا قانون البينات رقم (4) لسنة 2001، مما خلق فجوة واضحة بين التشريع والممارسة.

ويرى الباحث أن التأريخ لتطور الدليل الإلكتروني يكشف عن تفاوت جوهري بين التجارب الدولية والعربية. ففي حين استطاعت الأنظمة الغربية إدماج الأدلة الإلكترونية ضمن بنيتها القانونية بشكل متكامل من حيث التعريف، والتقنين، والمعالجة الفنية، لا تزال العديد من التشريعات العربية، ومنها الفلسطينية، تعتمد على نصوص عامة غير كافية، ما قد يؤدي إلى إرباك قضائي عند التطبيق. كما أن غياب لوائح تنفيذية فنية واضحة لجمع وتحليل وتقديم الدليل الإلكتروني أمام المحاكم، يُقلّل من قوة هذا الدليل ويُهدد بطلانه في حال عدم استيفاء الشروط الإجرائية الدقيقة.

لذلك، فإن تطوير التشريعات الفلسطينية يتطلب إعادة هيكلة الإطار القانوني المتعلق بالأدلة، بما يضمن التكييف السليم للدليل الإلكتروني، ويربطه بمرجعية تقنية وقانونية تواكب المعايير الدولية المعتمدة، وتُحقق التوازن بين الحقوق الدستورية للأطراف ومتطلبات العدالة الحديثة.

المطلب الثاني: الخصائص العامة للدليل الإلكتروني

مع تطور الجريمة الإلكترونية وتعقّد أدواتها، برز الدليل الإلكتروني كأحد أهم وسائل الإثبات الجنائي في العصر الحديث، لما يتضمنه من معلومات دقيقة يمكن أن تسهم في كشف الجريمة وتحديد هوية الفاعلين. إلا أن هذا النوع من الأدلة لا يخضع لنفس الأحكام التي تنطبق على الأدلة التقليدية، نظرًا لخصوصيته التقنية وارتباطه بالتكنولوجيا الحديثة، مما يمنحه خصائص فريدة تستدعي معالجة قانونية وفنية متخصصة.

إن إدراك الخصائص العامة للدليل الإلكتروني يُعد أمرًا أساسيًا لفهم طبيعته القانونية والإجرائية. فهو دليل قائم على البيانات الإلكترونية، ويخضع لتغيرات سريعة من حيث الشكل والمضمون، ويستلزم وسائل فنية دقيقة لضمان جمعه وتحليله وتقديمه للمحكمة دون الإخلال بمبدأ العدالة. ومن هذا المنطلق، سيتم في هذا المطلب تسليط الضوء على أبرز الخصائص التقنية التي تميز الدليل الإلكتروني عن غيره من الأدلة، يليها استعراض لأهم الخصائص القانونية التي تُحدد شروط استخدامه كأداة إثبات في المسار القضائي.

وفي هذا السياق، سيتم في هذا المطلب تناول الخصائص العامة للدليل الإلكتروني من خلال محورين أساسيين:

الفرع الأول يُعالج الخصائص التقنية التي تميز هذا النوع من الأدلة،

أما الفرع الثاني، فيتناول الخصائص القانونية التي تُؤثّر في حجيته وقبوله ضمن النظام القضائي.

الفرع الأول: الخصائص التقنية للدليل الإلكتروني

يتميّز الدليل الإلكتروني بمجموعة من الخصائص التقنية التي تفرض تحديات عملية وقانونية على الجهات المختصة، ابتداءً من لحظة جمعه مرورًا بفحصه وتحليله، وصولًا إلى تقديمه كوسيلة إثبات أمام القضاء. وهذه الخصائص التقنية، على الرغم من أنها تمنح الدليل الإلكتروني قوة ومرونة، إلا أنها تُحتم في المقابل شروطًا صارمة للحفاظ على صدقيته وسلامته. وفيما يلي عرض موسّع لأبرز هذه الخصائص:

أولًا: القابلية للتغيير والتحريف (Volatility)

يُعد الدليل الإلكتروني من أكثر أنواع الأدلة عرضة للتحوير أو التلاعب، إذ يمكن تغييره أو مسحه أو استبداله بالكامل بوسائل فنية دقيقة لا تترك أثرًا مرئيًا. ويعود ذلك إلى طبيعته غير المادية واعتماده على البتات (Bits) التي تتشكل من إشارات كهربائية قابلة للتعديل. وبخلاف الأدلة التقليدية كالمستندات الورقية أو البصمات، لا يمكن ملاحظة التعديل في البيانات الإلكترونية إلا من خلال أدوات تقنية متخصصة (Casey ., 2022)

من هنا، فإن أي خلل في سلسلة الحفظ (Chain of Custody) أو إجراءات الفحص يُعرّض الدليل للرفض أمام المحكمة. وهذا ما يؤكده تقرير الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) لعام 2020، والذي شدد على أن "الحد الأدنى لقبول الدليل الإلكتروني هو إثبات عدم تعرضه لأي تعديل منذ لحظة جمعه وحتى عرضه أمام القضاء" (ENISA, 2020, p. 42).

ثانيًا: الحاجة إلى أدوات تقنية متخصصة

لا يمكن الوصول إلى الدليل الإلكتروني أو استخلاص مضمونه إلا باستخدام تقنيات متطورة تتناسب مع نوع النظام أو الجهاز أو البرمجية التي تُخزن فيها البيانات. فمثلًا، تحليل بيانات الهاتف المحمول يتطلب استخدام أدوات مختلفة عن تلك المستخدمة لفحص أجهزة الحاسوب أو السيرفرات. كما أن الأدلة المستخرجة من السحابة الإلكترونية (Cloud Evidence) تستلزم بروتوكولات اتصال وشهادات إلكترونية لضمان التوثيق والتحقق.

ويُشير الجلعود (2024، صفحة 2387) إلى أن "الطبيعة التقنية للدليل الإلكتروني تتطلب تدخلاً احترافيًا من خبراء مؤهلين، سواء في مراحل جمع الدليل أو تحليله، للحفاظ على سلامته ومشروعيته القانونية".

ثالثًا: القابلية للنسخ دون تلف (Replicability)

يُعد هذا الجانب من الخصائص الفريدة للدليل الإلكتروني؛ إذ يمكن نسخه عدة مرات دون أن يُفقد شيئًا من محتواه أو دقته الأصلية. فخلافًا للأدلة المادية التي قد تتلف مع الزمن أو نتيجة التعامل المباشر، يُمكن استنساخ البيانات الإلكترونية على أكثر من وسيط (مثل أقراص خارجية أو منصات تخزين إلكتروني) دون أي تغيير في مضمونها. ومع ذلك، فإن هذه الخاصية تُعد سلاحًا ذا حدين، لأنها قد تُستخدم أيضًا لخلق نسخ مزورة يصعب تمييزها عن الأصل، ما يفتح المجال أمام الطعن في مصداقية الدليل.

ويؤكد تقرير الهيئة الوطنية للعدالة الإلكترونية في فرنسا (ANSSI, 2021) على ضرورة أن يكون "كل استنساخ للدليل الإلكتروني مصحوبًا بشهادة إلكترونية (Hash Value) تُثبت تطابق النسخة مع الأصل، وتُحفظ ضمن ملف الحفظ الإلكتروني المعتمد قضائيًا".

رابعًا: الترابط والتكامل بين الأدلة الإلكترونية (Interconnectedness)

من الخصائص البارزة للدليل الإلكتروني أنه لا يظهر غالبًا بشكل منفرد، بل في سياقات مترابطة. فعلى سبيل المثال، يُمكن أن يؤدي تتبّع رسالة إلكترونية إلى كشف شبكة من الاتصالات، أو أن يُشير سجل تصفح الإنترنت إلى مصادر بيانات داعمة تُشكّل صورة متكاملة للجريمة.

وقد أشار الباحث مرسي (2020، صفحة 102)إلى أن "التحليل الإلكتروني يعتمد على منهجية تتبّعية تُعيد بناء السياق العام للبيانات، ما يُميز الدليل الإلكتروني بقدرته على تقديم صورة متكاملة عن الفعل الإجرامي من خلال شبكة الأدلة المترابطة".

خامسًا: الحركية العالية وسرعة التغير (High Mobility & Mutability)

تُظهر الأدلة الإلكترونية درجة عالية من الحركية، إذ يمكن نقلها بسرعة عبر وسائط متعددة كالبريد الإلكتروني، أو خدمات التخزين السحابي، أو أجهزة USB، أو حتى عبر شبكات مشفرة. كما أن هذه الأدلة تتغير باستمرار بسبب التحديثات البرمجية، أو نشاطات المستخدم، أو حتى مجرد تشغيل الجهاز.

هذه السمة تُحتّم على الجهات المختصة التحرك الفوري عند رصد الدليل الإلكتروني، لأن أي تأخير قد يؤدي إلى ضياعه أو تغيّره. ولهذا السبب، تُوصي لجنة الجرائم الإلكترونية التابعة لمجلس أوروبا بضرورة "تجهيز وحدات التحقيق بأدوات فورية لحفظ الأدلة الإلكترونية بمجرد الاشتباه، وتجميد النشاط الإلكتروني لحظة الضبط (Council of Europe, 2001)

يرى الباحث إن الخصائص التقنية للدليل الإلكتروني تُبرز بوضوح مدى تعقيده مقارنةً بالأدلة التقليدية، الأمر الذي يُحتّم إدخال مفاهيم فنية متقدمة إلى البيئة القانونية. فالقابلية للتغيير، وسهولة النسخ، والترابط، وسرعة التلاشي تُحتم كلها وجود تشريعات دقيقة، وإجراءات تقنية مصاحبة لجمع هذا النوع من الأدلة، حتى لا تُضيع حقوق الأطراف أو تُشوّه العدالة. كما أن تأهيل الكوادر القضائية والأمنية للتعامل مع هذه الخصائص التقنية لم يعد خيارًا، بل ضرورة لضمان أن تكون المحاكمات عادلة في زمن أصبحت فيه البيانات هي الشاهد الأول.

الفرع الثاني: الخصائص القانونية للدليل الإلكتروني

يتمتع الدليل الإلكتروني بجملة من الخصائص القانونية التي تُميّزه عن الأدلة التقليدية وتفرض شروطًا ومعايير دقيقة لقبوله ضمن منظومة الإثبات القضائي. ويكمن التحدي القانوني في أنه لا يُمكن التعامل مع هذا النوع من الأدلة بنفس القواعد الجامدة التي تحكم الأدلة الورقية أو المادية، نظرًا لطبيعته الإلكترونية المتغيرة، وما يرتبط بها من اعتبارات تتعلق بالمشروعية والحجية وسلامة الإجراء. وفيما يلي تحليل موسّع لأبرز الخصائص القانونية:

أولًا: حجية الدليل الإلكتروني في الإثبات

يُعد الدليل الإلكتروني وسيلة إثبات مشروعة ما دام قد تم الحصول عليه بطرق قانونية تُراعي الضمانات الدستورية والإجرائية. لكن حجيته أمام القضاء تختلف من نظام قانوني إلى آخر، وبعض الأنظمة ما زالت تتردد في منحه ذات القوة الإثباتية للأدلة التقليدية. ويُلاحظ أن غالبية التشريعات المقارنة تُميز بين "القبول الشكلي" للدليل الإلكتروني، وبين "الحجية الفعلية" التي تمنحه تأثيرًا حاسمًا في القضية.

وقد أكّد عبد العال (2021، صفحة 643) أن "القانون لا يرفض الدليل الإلكتروني من حيث المبدأ، لكنه يشترط في قبوله أن يكون قد جُمع وفقًا للإجراءات القانونية، وبوسائل تضمن عدم التلاعب في محتواه أو مصدره".

كما أوضحت المادة 15 من اتفاقية بودابست أن "الأدلة الإلكترونية تتمتع بالحجية متى روعيت فيها شروط الحماية القانونية، وإثبات مصدرها، والمحافظة على سلامتها(Council of Europe, 2001) .

ثانيًا: مشروعية الوسيلة في جمع الدليل

يستند القبول القانوني للدليل الإلكتروني إلى مشروعية الوسائل المستخدمة في جمعه، أي أن جمعه لا بد أن يتم من قبل جهة مخولة، ووفق إجراءات قانونية واضحة، تحترم الخصوصية وحقوق الدفاع. فأي دليل يُستخرج من خلال اختراق غير مشروع أو تفتيش غير مصرح به قد يُستبعد من ملف القضية.

ويشير تقرير الهيئة المستقلة لحقوق الإنسان (2022) إلى أن "عدم وجود إذن قضائي مسبق بجمع البيانات الإلكترونية من أجهزة المتهمين يُشكل إخلالًا جسيمًا بمبدأ الشرعية الإجرائية، ويؤدي إلى بطلان الدليل مهما كانت أهميته الفنية" (الهيئة المستقلة، 2022، ص77).

وتُشير المحكمة الأوروبية لحقوق الإنسان في حكمها في قضية *Barbulescu v. Romania* (2017) إلى ضرورة وجود "توازن بين مصلحة الدولة في جمع الأدلة، وبين الحق الأساسي في الخصوصية"، وهو ما يكرّس مبدأ التناسب القانوني في استخدام الأدلة الإلكترونية.

ثالثًا: سلامة الدليل وعدم تغييره

من أبرز الشروط القانونية لقبول الدليل الإلكتروني هو الحفاظ على سلامته التقنية منذ لحظة جمعه وحتى تقديمه أمام المحكمة. ويُعرف هذا الشرط بمصطلح "سلامة السلسلة الإلكترونية" (Integrity of Digital Chain of Custody). فإذا شاب الدليل أي تعديل أو فقد جزء من محتواه دون مبرر موثق، فإنه يُفقد حجيته أمام القضاء.

وقد نصّت المادة (17) من قانون مكافحة جرائم تقنية المعلومات المصري (2018) على أن "تُعد البيانات الإلكترونية صحيحة ما لم يثبت العكس، ويقع عبء إثبات التغيير أو التلاعب على من يدعيه، بشرط أن تُقدَّم البيانات مصحوبة بشهادة فنية تُثبت سلامة الإجراءات" (مرسي، 2020، صفحة 98).

وتُشدّد لائحة الأدلة الإلكترونية في كندا (Canadian Digital Evidence Guidelines, 2021) على ضرورة أن "يتم توثيق كل خطوة في التعامل مع البيانات الإلكترونية، بما يشمل التوقيت، الجهة الفاحصة، والأدوات المستخدمة"، لضمان مشروعية الدليل وسلامته القانونية.

رابعًا: نسبية الدليل إلى صاحبه

للدليل الإلكتروني حجية نسبية ما لم يتمكن الطرف المعني من إثبات أنه صادر منه فعلًا. وهنا تبرز أهمية تحليل المصدر الإلكتروني، وربط البيانات بصاحبها من خلال التوقيع الإلكتروني، أو عنوان IP، أو كلمات المرور الشخصية، أو شهادة مصادقة إلكترونية.

أشار الجلعود (2024، صفحة 2388) إلى أن "أحد الإشكالات التي تواجه حجية الدليل الإلكتروني هي صعوبة إسناده لصاحبه الحقيقي، خاصة إذا تم استخدام أجهزة عامة أو بيانات مخترقة، مما يستلزم خبرة تقنية وقانونية متقدمة في الإثبات".

وفي هذا الإطار، تنص المادة 12 من قانون المعاملات الإلكترونية الإماراتي (2012) على أن "التوقيع الإلكتروني المعتمد يُعد حجة قانونية كاملة ما لم يثبت العكس"، ما يدل على أن نسبية الدليل مشروطة بالتوثيق الفني.

يُشكل النص التشريعي المذكور في المادة (12) من قانون المعاملات الإلكترونية الإماراتي نقطة محورية في النقاش الدائر حول حجية الدليل الإلكتروني. فمن خلال منحه حجية قانونية كاملة للتوقيع الإلكتروني المعتمد، لا يقوم المشرّع الإماراتي بتعزيز الثقة في المعاملات الإلكترونية فحسب، بل يقدم حلاً عمليًا لإحدى أعقد إشكاليات الإثبات الإلكتروني، وهي إشكالية الإسناد.

إن عبارة "ما لم يثبت العكس "تُعد بمثابة حجر الزاوية في هذا النص؛ فهي تضع قرينة قانونية بسيطة لصالح صحة التوقيع الإلكتروني، ولكنها لا تغلق الباب أمام إثبات عكسها. وهذا يعني أن المشرّع قد نقل عبء الإثبات من الطرف الذي يتمسك بالدليل الإلكتروني (الادعاء مثلاً) إلى الطرف الذي ينازع في صحته (الدفاع). هذا التحول في عبء الإثبات له آثار إجرائية بالغة الأهمية، حيث يُعفي الخصوم من الحاجة إلى إثبات صحة كل توقيع إلكتروني من نقطة الصفر، ما لم يكن هناك طعن جدي بشأنه.

وبالتالي، فإن هذا النص لا يحل إشكالية الإسناد بشكل مطلق، بل يؤطرها قانونيًا، محولاً إياها من مسألة فنية بحتة إلى مسألة إجرائية تخضع لقواعد عبء الإثبات. وهذا يعكس نضجًا تشريعيًا في التعامل مع خصوصية الدليل الإلكتروني، ويقدم نموذجًا يمكن للتشريعات الأخرى، بما فيها التشريع الفلسطيني، الاسترشاد به لتعزيز اليقين القانوني في هذا المجال.

خامسًا: قابلية الطعن الفني والإجرائي

يتميّز الدليل الإلكتروني بقابليته العالية للطعن، سواء من الناحية الفنية مثل الطعن في صحة الملف أو تغير خصائصه، أو من الناحية الإجرائية مثل الطعن في الطريقة التي جُمِع بها أو مدى احترام الخصوصية. ولهذا السبب، تُعد المحاكمة القائمة على دليل إلكتروني فقط دون وجود أدلة داعمة عرضة للانهيار إذا أُثبت أي خلل بسيط في جمع أو تحليل الدليل.

وقد أكد الجلعود (2020، صفحة 180) أن "الطعن في مشروعية الدليل الإلكتروني لا يقتصر على الشكل، بل يمتد إلى الإجراءات الفنية والبرمجية، وهو ما يتطلب من القضاة والمحققين امتلاك وعي تقني قانوني موازٍ".

كما نصت لجنة العدالة الإلكترونية الأمريكي(American Bar Association, 2020) على ضرورة "إخضاع الأدلة الإلكترونية لمعايير تقييم خاصة تراعي احتمال تعرضها للاختراق أو التلاعب، وتُتيح للطرف الآخر فرصة الطعن الفني من خلال خبراء معتمدين".

هذا و يرى الباحث إن الخصائص القانونية للدليل الإلكتروني تكشف عن تداخله العميق بين القانون والتكنولوجيا، مما يجعله دليلاً فريدًا في بنيته، حساسًا في مضمونه، ومعقدًا في إثباته. فمشروعية جمعه وسلامة تحليله ونسبته لصاحبه، كلّها شروط دقيقة تُوجب تعديل البنية التشريعية الحالية وإصدار لوائح تنفيذية متخصصة. كما أن ضمان عدالة المحاكمة في ظل وجود أدلة إلكترونية يقتضي تدريب القضاة والمحامين على فهم الجوانب الفنية المرتبطة بهذه الأدلة، حتى لا يكون الفارق في الكفاءة التقنية سببًا في ترجيح كفة طرف على آخر. وفي ظل ما سبق، يرى الباحث أن إرساء ضوابط قانونية دقيقة يضمن التوازن بين مكافحة الجريمة الإلكترونية وحماية الحقوق الدستورية للأفراد.

المبحث الثاني : تصنيف أنواع الدليل الإلكتروني

في ظل التطور المتسارع للتكنولوجيا الإلكترونية وتزايد الاعتماد عليها في مختلف مناحي الحياة، أصبحت الجرائم الإلكترونية أكثر تنوعًا وتعقيدًا من أي وقت مضى، ما أدى إلى تزايد أهمية "الأدلة الإلكترونية" في سياق التقاضي والتحقيقات الجنائية. ولأن هذه الأدلة لا تأتي في صورة واحدة أو من مصدر ثابت، بل تتنوع بشكل كبير من حيث طبيعتها، ومصدرها، والقصد من إنشائها، فإن تصنيفها يمثل خطوة أساسية لفهم كيفية التعامل معها من الناحية الفنية والقانونية.

إن تصنيف الأدلة الإلكترونية لا يهدف فقط إلى التنظيم الأكاديمي، بل هو ضرورة عملية تساعد رجال التحقيق والقضاة على تحديد نوع الإجراء المطلوب تجاه كل نوع منها. فالتعامل مع ملف مستخرج من حاسوب يختلف جذريًا عن التعامل مع بيانات صادرة عن تطبيق تواصل اجتماعي، أو بصمة إلكترونية غير مقصودة خُزنت في خوادم الشبكة دون علم المستخدم.

وقد أكدت وكالة الاتحاد الأوروبي للأمن السيبراني ENISA (2022) أن تصنيف الأدلة الإلكترونية وفق معايير علمية واضحة يُعد من المتطلبات الأساسية لتطوير أدوات فحص وتحقيق تتناسب مع كل نوع منها، وتُسهم في تقليل احتمالات الطعن على مشروعية الدليل أمام القضاء. كما أن تعدد صور الدليل الإلكتروني وتوسع رقعته الإلكترونية تفرض تحديات أمام الجهات القضائية والتقنية، ما يستلزم بناء تصنيفات منهجية تسهّل فهرسة الأدلة وتحديد إجراءات الحفظ والاسترجاع والتحليل الخاصة بكل فئة.

ومن هذا المنطلق، يتناول هذا المبحث تصنيفين رئيسيين للأدلة الإلكترونية:

التصنيف الأول: بحسب طبيعة المصدر، ويشمل هذا التصنيف الأدلة المستخرجة من مصادر مختلفة، كالأجهزة المادية (مثل الحواسيب والهواتف الذكية)، أو شبكات الاتصال (مثل سجلات مزودي خدمة الإنترنت)، أو التطبيقات والبرمجيات (مثل قواعد بيانات التطبيقات السحابية).

التصنيف الثاني: بحسب القصد من الإنشاء، ويميز هذا التصنيف بين الأدلة التي أُنشئت عمدًا لغرض الإثبات (مثل العقود الإلكترونية الموقعة إلكترونيا)، والأدلة التي تُخلَّف بشكل غير مقصود وتُعرف بالبصمات الإلكترونية (مثل بيانات الموقع الجغرافي التلقائية أو ملفات تعريف الارتباط.

وعقب استعراض كل تصنيف، سيقدم الباحث فقرة تحليلية نقدية، تهدف هذه الفقرة إلى إبراز الأهمية العملية لذلك التصنيف، مع تسليط الضوء على التحديات التي تواجه الأجهزة القضائية عند التعامل مع كل نوع من الأدلة. وسيتم التركيز بشكل خاص على السياق الفلسطيني، حيث يفرض الواقع تحديات فريدة تتعلق بضعف البنية التحتية الإلكترونية أحيانًا، وقصور بعض النصوص التشريعية عن مواكبة التسارع التقني، مما يؤثر على كيفية جمع هذه الأدلة وتقييم حجيتها.

الفرع الأول: التصنيف حسب طبيعة المصدر

يتفاوت الدليل الإلكتروني من حيث المصدر التقني الذي تم استخراجه منه، وهو ما يستتبع تباينًا في آليات جمعه، وطرق تحليله، وأدوات توثيقه، ومستوى الاعتماد عليه قانونيًا. ويُعد هذا التصنيف أحد المرتكزات الأساسية في التحقيقات الجنائية الإلكترونية، حيث يُساعد في تحديد الجهة المختصة بجمع الأدلة، وطبيعة الإجراءات اللازمة لكل نوع، ومدى موثوقية الدليل بناءً على مصدره الأصلي.

ويمكن تصنيف أهم المصادر التي يُستخرج منها الدليل الإلكتروني على النحو الآتي:

1. الأدلة المستخرجة من الأجهزة الطرفية (Endpoints)

تُعدّ الأجهزة الطرفية أحد أهم مصادر الأدلة الإلكترونية وأكثرها استخدامًا في مجالات التحقيقات الجنائية الإلكترونية. وتشمل هذه الفئة مجموعة واسعة من الوسائط الإلكترونية التي يتعامل معها المستخدم يوميًا، مثل أجهزة الحواسيب المكتبية والمحمولة، الهواتف الذكية، الأجهزة اللوحية، وحدات التخزين المتنقلة مثل أقراص USB وبطاقات الذاكرة، وحتى بعض الأجهزة الذكية القابلة للارتداء والتي تُسجّل البيانات بشكل لحظي ومتواصل.

إن القيمة الإثباتية للأجهزة الإلكترونية تنبع من كونها توثّق معظم أنشطة المستخدم، سواء تلك التي تتم بصورة مباشرة أو عبر تطبيقات وسيطة، بما في ذلك الملفات النصية، الصور، مقاطع الفيديو، سجلات التصفح، بيانات تسجيل الدخول، وسجلات النظام. وتُخزّن هذه البيانات غالبًا على هيئة بيانات وصفية (Metadata)، مما يُتيح للخبراء إمكانية استرجاع التسلسل الزمني للأنشطة وتحليلها بشكل يُسهم في بناء رواية متكاملة حول الواقعة قيد التحقيق (Goel et al., 2024).

كما تُستخدم في هذا النوع من الأدلة برامج جنائية إلكترونية متقدمة مثل *EnCase* و *Forensic Toolkit (FTK)*، وهي أدوات تتيح استخراج نسخ طبق الأصل من البيانات الأصلية (Forensic Images) دون المساس بسلامتها أو قابليتها للطعن. وتُعد هذه الإجراءات جزءًا من عملية "سلسلة الحيازة" (Chain of Custody) التي تتطلب توثيقًا دقيقًا لكل خطوة في جمع البيانات، وتحديد الأشخاص الذين تعاملوا مع الدليل الإلكتروني (Wickramasekara & Le-Khac, 2024).

إضافة إلى ذلك، فإن الأجهزة الطرفية لا تقتصر على البيانات الظاهرة أو المخزنة تقليديًا، بل تشمل أيضًا ملفات محذوفة يمكن استرجاعها باستخدام أدوات تحليل متقدمة، بالإضافة إلى بيانات مخفية في أقسام غير مرئية من الذاكرة أو داخل أنظمة التشغيل. وفي هذا السياق، أشارت أحدث الدراسات إلى أن التحقيق الإلكتروني لا يقتصر على قراءة المعلومات، بل يتطلب تحليل السياق البرمجي والتقني الذي أنتج هذه البيانات، وهو ما يستدعي خبرة فنية عالية (Nayerifard et al., 2023).

من جهة أخرى، فإن الوصول إلى الأدلة من هذه الأجهزة يتطلب غالبًا مراعاة البعد القانوني والحقوقي، لا سيما في حال كانت تحتوي على معلومات شخصية أو مهنية حساسة. ولذلك، تشترط معظم الأنظمة القضائية المعاصرة وجود إذن قانوني صريح لجمع البيانات، مع الالتزام بحماية الخصوصية وعدم تجاوز حدود الغرض الجنائي، في ظل التزايد المستمر للقلق العالمي من إساءة استخدام البيانات الإلكترونية (Harisha & Mishra, 2023).

2. الأدلة المستخرجة من الشبكات

أولًا: ماهية الأدلة الشبكية (Nature of Network-Based Evidence)

تُشير الأدلة الشبكية إلى كل نوع من المعلومات الإلكترونية التي تُجمع من عمليات تبادل البيانات التي تتم عبر الشبكات الإلكترونية، سواء كانت تلك الشبكات داخلية مغلقة (LAN) أو ممتدة وعالمية كشبكة الإنترنت (WAN). وهي لا تشمل فقط المحتوى الظاهر من البيانات المتبادلة، بل تمتد لتشمل "البيانات الوصفية" (Metadata) التي تكشف عن توقيت الإرسال والاستلام، عنوان IP المستخدم، نوع البروتوكول، وسعة الحزم، وغيرها من التفاصيل التقنية الدقيقة التي تُسهم بشكل فعال في تتبع السلوك الإلكتروني وتحديد الأنشطة المشبوه(Forensic Focus, 2025) .

وتتضمن الأدلة الشبكية طيفًا واسعًا من الملفات والمصادر، أبرزها:

- ملفات السجل : (Log Files) وهي سجلات نصية تقوم الأنظمة والخوادم بإنشائها تلقائيًا لتوثيق كافة العمليات التي تحدث على الشبكة، مثل محاولات الدخول، الأنشطة التي قام بها المستخدمون، وأحداث النظام.(Baryamureeba & Tushabe, 2004)
- حزم البيانات الملتقطة : (Packet Captures) وهي نسخة خام لكل ما تم تبادله بين طرفي الاتصال، وتوفر تفصيلًا دقيقًا للمحتوى المرسل والمستقبل، بما في ذلك رؤوس الحزم ومحتواها. (Kent & Souppaya, 2006)
- سجلات الجدران النارية : (Firewall Logs) تحتوي على محاولات الوصول الناجحة والفاشلة عبر الشبكة، وتساعد في كشف محاولات التسلل أو الهجمات الخارجية.
- بيانات البروكسي : (Proxy Logs) تُستخدم لتتبع حركة التصفح على الإنترنت عند المرور عبر الخوادم الوسيطة، وهي مفيدة للغاية في التحقيقات التي تشمل استخدام الشبكات لإخفاء الهوية.
- مخرجات أجهزة التوجيه : (Router Logs) توفر معلومات حول حركة المرور عبر الشبكة، ويمكن من خلالها تتبع النشاط الشبكي إلى مصادره المحتملة.(Casey , 2022)

- تقارير الأنظمة الأمنية مثل IDS/IPS: تكشف هذه التقارير عن محاولات الاختراق أو الأنشطة غير الاعتيادية في الوقت الفعلي، وتُعتبر أداة استباقية في كشف الهجمات السيبرانية.

أهمية هذه الأدلة تكمن في كونها تُشكل خط الدفاع الأول في العديد من القضايا الجنائية الإلكترونية، خاصة تلك المتعلقة بالوصول غير المشروع، اختراق الأنظمة، الاحتيال الإلكتروني، أو الجرائم المنظمة عبر الشبكة.

فهي تُقدم تسلسلًا زمنيًا دقيقًا للأحداث، وتُبرز الأنماط السلوكية للمتهمين أو المستخدمين محل التحقيق.

وقد أكدت دراسة حديثة لـ (Wickramasekara & Le-Khac, 2024) أن تحليل الأدلة المستخرجة من الشبكات يتطلب قدرًا عاليًا من الاحترافية، نظرًا لضخامة حجم البيانات وتنوع مصادرها، مما يؤدي إلى ما يُعرف بـ "ضجيج البيانات" (Data Noise)، والذي قد يُعقّد مهمة الوصول إلى المعلومات ذات الصلة. لذلك، يشترط نجاح هذا التحليل وجود منهجية دقيقة للتنقيب الإلكتروني (Digital Mining) تعتمد على تقنيات فرز ذكية تُميّز بين البيانات المفيدة وغير المفيدة دون الإخلال بحيادية النتائج أو دقتها.

كما أوصىGoel et al. (2024) في مراجعتهم المتخصصة بضرورة الالتزام الكامل بسلسلة الحيازة الإلكترونية (Digital Chain of Custody) أثناء التعامل مع الأدلة الشبكية، من خلال توثيق كل إجراء فني يتم على البيانات بشكل إلكتروني ومؤرشف، ضمانًا لعدم فقدان مصداقية الدليل أمام القضاء، وحتى لا يُطعن به لاحقًا بسبب غياب التوثيق أو غموض مصدر المعلومات.

من وجهة نظر الباحث، لا تقتصر أهمية الأدلة الشبكية على كونها مجرد أداة فنية لكشف الجرائم الإلكترونية، بل إنها تمثل الذاكرة الإلكترونية غير القابلة للتحريف لسلوك الأفراد والكيانات عبر الفضاء السيبراني. إن قدرتها على توفير تسلسل زمني دقيق للأحداث تمنح المحقق والقاضي رؤية بانورامية لا يمكن للأدلة التقليدية توفيرها، مما يجعلها حجر الزاوية في بناء تصور متكامل عن وقائع الجريمة.

ومع ذلك، فإننا نتفق مع ما طرحته الدراسات الحديثة (Wickramasekara & Le-Khac, 2024) Goel et al., 2024)) من أن القيمة الحقيقية لهذه الأدلة تظل رهينة بمدى سلامة الإجراءات المتبعة في التعامل معها.

فمشكلة "ضجيج البيانات" ليست مجرد تحدٍ تقني، بل هي إشكالية قانونية قد تؤدي إلى إغراق التحقيق في تفاصيل غير جوهرية، أو الأسوأ من ذلك، قد تخفي أثرًا إلكترونيا حاسمًا.

وفي السياق الفلسطيني على وجه الخصوص، تكتسب هذه التحديات بعدًا أكثر تعقيدًا. فإلى جانب ضرورة الالتزام الصارم بـ "سلسلة الحيازة الإلكترونية"، تبرز الحاجة المُلحة إلى تأهيل الكوادر الفنية والقضائية للتعامل مع هذا الكم الهائل من البيانات، وتطوير بنية تشريعية واضحة توازن بين فعالية التحقيق وحماية خصوصية الأفراد. فبدون وجود منهجية قانونية وتقنية متكاملة، قد يتحول الدليل الشبكي من أداة لتحقيق العدالة إلى مصدر للغموض والتشكيك، وهو ما نسعى لتجنبه.

ثانيًا: أهم أنواع الأدلة الشبكية (Types of Network-Based Evidence)

تلعب الأدلة الشبكية دورًا محوريًا في التحقيقات الإلكترونية، نظرًا لقدرتها على تسجيل وتحليل التفاعل بين الأجهزة الإلكترونية عبر الشبكات المختلفة، سواء في بيئات داخلية (LAN) أو على مستوى الإنترنت. وتمثل هذه الأدلة امتدادًا للحدث الإلكتروني نفسه، حيث تُمكّن المحقق من فهم طبيعة الهجوم، مساراته، وتحديد الأطراف المتورطة. وفيما يلي عرض لأبرز أنواع الأدلة الشبكية التي يعتمد عليها الخبراء الجنائيون:

1. ملفات الدخول والخروج (Login Records)

تُعد ملفات الدخول والخروج من أولى نقاط التحقيق في الجرائم السيبرانية، نظرًا لأنها توفّر بصمة إلكترونية أولية تُظهر التفاعل بين المستخدم والنظام. تحتوي هذه الملفات على بيانات مصادقة دقيقة تشمل:

- اسم المستخدم أو البريد الإلكتروني المستخدم للدخول.
- عنوان IP الخاص بالجهاز الذي تم استخدامه.

- نظام التشغيل المستخدم خلال الجلسة.
- نوع الجهاز)هاتف، حاسوب، خادم....)
- توقيت الدخول وتوقيت الخروج بالدقيقة والثانية.
- مدة الجلسة الإجمالية.
- نتائج محاولة الدخول (ناجحة / فاشلة).
- محاولات الاختراق (مثل إدخال كلمات مرور خاطئة متكررة). (Nelson, Phillips, & Steuart, 2015)

هذه البيانات تُمكّن المحقق من تتبع التسلسل الزمني للجريمة، وربط الجناة بالنشاط المشبوه. كما تساعد على إعادة بناء السيناريو الزمني للجريمة الإلكترونية، وهو ما يوفّر دعمًا قضائيًا قويًا في قضايا الاحتيال، سرقة الهوية، أو الوصول غير المصرّح به.

ووفقًا لما بيّنته دراسة Nayerifard et al. (2023)، فإن تحليل سجلات الدخول (Log Files) يُعد أداة حاسمة في تتبع الهجمات الإلكترونية، حيث يمكن من خلاله تحديد "نقطة الدخول" (Entry Point) التي تم استخدامها للوصول إلى النظام، مما يُوجّه مجرى التحقيق نحو الثغرة الأمنية المُستغلة أو الحساب الذي تم اختراقه، وبالتالي يدعم مسار الإثبات الفني بصورة دقيقة.

ومن الناحية القانونية، تعتمد سلامة هذه الملفات بدرجة كبيرة على البروتوكولات المستخدمة في تسجيل الأحداث داخل الخوادم، ومدى تأمينها ضد التعديل أو الحذف. وقد أوصى Goel et al. (2024) باستخدام أنظمة تسجيل من النوع الذي لا يسمح بالكتابة عليه مرة أخرى (Write-Once Systems)، بالإضافة إلى تشفير البيانات باستخدام تقنيات موثوقة لضمان عدم العبث بمحتواها.

كما بيّنت الأبحاث الحديثة أن سجلات الدخول تُستخدم بشكل متزايد كأدلة إلكترونية رئيسية في القضايا الجنائية، بشرط الحفاظ على سلسلة الحيازة القانونية (Chain of Custody) بدقة، منذ لحظة استخراجها وحتى تقديمها كدليل في المحكمة(Wickramasekara & Le-Khac, 2024) .

ولا يقتصر دور هذه الملفات على القضايا الجنائية، بل تُعتبر ذات أهمية كبيرة أيضًا في النزاعات التجارية، والتحقيقات المتعلقة بتسريبات البيانات الداخلية، وكذلك في تقييم أداء الموظفين في بيئات العمل الإلكترونية، ما يجعلها أداة متعددة الأغراض ذات وزن قانوني وتقني في آن واحد.

2. سجلات الخوادم (Server Logs)

تلعب سجلات الخوادم دورًا مركزيًا في توثيق كل ما يحدث على الأنظمة الإلكترونية، فهي بمثابة "الصندوق الأسود" للأنظمة الإلكترونية. وتشمل هذه السجلات معلومات مفصلة عن كل طلب أو عملية تُجرى على الخادم، مثل تحميل صفحة، إرسال بيانات، أو محاولة اختراق. وتختلف أنواع السجلات بحسب نوع الخادم، لكنها عادةً ما تشمل:

- سجلات الوصول : (Access Logs) تُسجل جميع الطلبات التي تتم على الخادم، بما يشمل عنوان IP، الوقت، نوع الطلب (GET, POST)، والموارد المطلوبة. (Apache HTTP Server, 2024).
- سجلات الأخطاء (Error Logs) : تسجل الأعطال البرمجية أو محاولات الدخول الفاشلة، والتي قد تشير إلى محاولة اختراق أو خلل أمني.
- سجلات الأداء والتحميل: تُظهر مدى الضغط على الخادم، وعدد المستخدمين المتزامنين، ووقت الاستجابة.

وفقًا لما ذكره Casey (2011)، فإن تحليل سجلات الخوادم يُعد من أفضل طرق رصد الهجمات من نوع (DDoS)، وحقن SQL، وXSS، كما أنه يساعد في تتبع المصدر الجغرافي للمهاجمين (ص. 347).

من الناحية الفنية، تعتبر سجلات الخوادم مصدراً مركزيًا موثوقًا لكونها تُحفظ عادةً في بيئة آمنة ولا يمكن تعديلها بسهولة دون ترك أثر، خصوصًا عند استخدام أنظمة (WORM – Write Once Read Many). وتُستخدم أدوات تحليل متقدمة مثل Splunk، Graylog، وELK Stack لفهم هذه السجلات وتحليلها بشكل جنائي.

أما من الناحية القانونية، فإن هذه السجلات لا تُعتبر دليلًا مقبولًا أمام المحكمة إلا إذا تم:

- استخراجها من مصدرها الأصلي دون تعديل.
- توثيق عملية الجمع والتخزين بخطوات واضحة ضمن سلسلة الحيازة.
- إثبات أنها لم تُعدل أو تُحذف، عبر أدوات التحقق من النزاهة الإلكترونية (Hash Algorithms) مثل SHA-256.

ووفقًا لاتفاقية بودابست بشأن الجريمة الإلكترونية (Council of Europe, 2001)، تُعد سجلات الخوادم أدلة صالحة للاستخدام الجنائي، شريطة أن تتم معالجتها ضمن المعايير التقنية والقانونية المحددة.

3. تحليلات أنظمة الكشف عن التسلل (IDS/IPS Analysis)

تُعد أنظمة الكشف عن التسلل (Intrusion Detection Systems - IDS) وأنظمة منع التسلل (Intrusion Prevention Systems - IPS) من أبرز أدوات الأمن السيبراني التي يعتمد عليها الخبراء لرصد التهديدات وتوثيق الأنشطة المشبوهة داخل الشبكات الإلكترونية. هذه الأنظمة تعمل على تحليل حركة البيانات (Traffic) ومقارنتها مع قواعد بيانات تحتوي على أنماط هجمات معروفة (Signatures) أو سلوكيات غير اعتيادية (Anomaly-based Detection)، لتحديد ما إذا كانت هناك محاولة لاختراق أو استغلال ثغرة أمنية.

الوظائف الأساسية

- رصد محاولات الوصول غير المصرح به إلى الأنظمة.
- تسجيل أنشطة مثل الاستطلاع الشبكي، محاولات الحقن، أو تنفيذ أكواد خبيثة.
- تنبيه مسؤولي الأمن في الزمن الحقيقي، أو اتخاذ إجراءات تلقائية (مثل حجب IP) في حال استخدام نظام IPS.

وفقًا لـ Mandia et al. (2003)، فإن تحليل سجلات IDS/IPS يمكن أن يوفر معلومات دقيقة حول:

- عنوان المصدر والوجهة (Source & Destination IP).
- نوع الهجوم أو الثغرة المستهدفة.
- وقت وتكرار الهجوم.
- البروتوكول المستخدم في التهديد (TCP, UDP, ICMP).

الأهمية الجنائية

من منظور التحقيقات الإلكترونية، تُستخدم تحليلات IDS/IPS في:

- تحديد توقيت الهجمات بدقة عالية.
- ربط الهجوم بحاسوب معين عبر عنوان IP.
- دعم الادعاء بأن هناك نشاطًا عدائيًا تم بشكل متعمد.

ومع أن هذه الأنظمة قوية، إلا أنها ليست دليلاً قاطعًا بحد ذاتها، بل تُستخدم عادةً كمصدر استدلالي يجب تعزيزه بأدلة أخرى مثل سجلات الدخول أو ملفات الحزم (PCAP). بالإضافة إلى ذلك، فإن فاعليتها تعتمد على دقة التكوين وقاعدة البيانات المستخدمة، لذا لا بد من تحليل تقني خبير لتحديد ما إذا كانت الإنذارات الصادرة حقيقية أم زائفة (False Positives).

التحديات القانونية

- يجب إثبات أن النظام كان مُهيأً بشكل صحيح عند وقوع الحادثة.
- ينبغي توثيق إعدادات النظام وتاريخ الإنذارات ضمن سلسلة الأدلة.
- ضرورة تقديم سجل الحدث الأصلي (Raw Log) دون تعديل.

4. بيانات حزم الشبكة (Packet Capture – PCAP Files)

تُعد ملفات حزم الشبكة (PCAP) من أقوى مصادر الأدلة الإلكترونية التي يعتمد عليها خبراء التحليل الجنائي الإلكتروني، نظرًا لقدرتها على تسجيل كل البيانات التي تمر عبر الشبكة بدقة زمنية عالية، مما يتيح إعادة بناء الجريمة الإلكترونية لحظة بلحظة.

ماهيتها:

ملف PCAP هو عبارة عن تسجيل خام لحركة المرور التي تمت عبر شبكة معينة خلال فترة زمنية محددة، ويحتوي على تفاصيل دقيقة مثل:

- عنوان الـ IP المرسل والمستقبل.
- رقم المنفذ (Port Number).
- نوع البروتوكول المستخدم (TCP, UDP, HTTP, FTP…).
- محتوى البيانات المُرسلة (Payload).
- الوقت الدقيق لكل حزمة مرسلة (Timestamp).

الاستخدام الجنائي

من خلال تحليل ملفات PCAP يمكن للمحقق الجنائي:

- تتبع مسار الهجوم من جهاز إلى آخر.
- استخراج الملفات المرسلة أو المستلمة.
- كشف الاتصالات المشبوهة أو غير المصرّح بها.
- إعادة بناء جلسات المستخدم وتحليل سلوكياته على الشبكة. (Ligh, Adair, & Hartstein, 2014)

وقد أوضحت دراسة حديثة لـ Wickramasekara & Le-Khac (2024) أن تحليل ملفات PCAP (Packet Capture) يُعد من الأدوات الحاسمة في قضايا اختراق الأنظمة وتسريب البيانات، حيث تُمكّن هذه الملفات من إعادة بناء حركة مرور البيانات عبر الشبكة، وتحديد ما إذا كانت البيانات قد نُقلت فعليًا من داخل الشبكة إلى جهة خارجية، ومن هو المستخدم أو الجهاز الذي قام بذلك، ومتى حدثت العملية بدقة زمنية عالية. وتُستخدم هذه الملفات أيضًا لاكتشاف الاتصالات غير المصرح بها أو محاولات زرع برمجيات خبيثة داخل النظام.الأدوات المستخدمة:

- Wireshark : لتحليل وتصفية الحزم وفحص تفاصيلها الدقيقة.
- Tcpdump : أداة سطر أوامر لتسجيل حركة المرور في الزمن الحقيقي.
- أدوات تحليل متقدمة مثل NetworkMiner وXplico لإعادة بناء الجلسات واسترجاع الملفات.

التحديات القانونية

- يجب إثبات سلامة ملفات PCAP من أي تعديل عبر التوقيع الإلكتروني أو تقنية الـ Hash.
- ضرورة توثيق إجراءات الجمع والتخزين والتحليل ضمن سلسلة الحيازة (Chain of Custody).
- ضمان أن التسجيل تم بطريقة قانونية دون انتهاك خصوصية المستخدمين(Casey , 2022) .

5. سجلات الجدران النارية (Firewall Logs)

تلعب سجلات الجدران النارية دورًا أساسيًا في الدفاع الإلكتروني، حيث تقوم برصد وتسجيل كافة محاولات الوصول إلى الشبكة، سواء المسموح بها أو المرفوضة، وذلك بناءً على السياسات الأمنية المُعتمدة داخل النظام. تحتوي هذه السجلات عادة على:

- عناوين IP المرسلة والمستقبِلة.
- أوقات وتواريخ المحاولات.
- البروتوكولات المستخدمة مثل TCP ، UDP.
- أرقام المنافذ Port Numbers.
- الإجراء المتخذ (تم السماح / تم الحظر).(Casey , 2022)

الاستخدام في التحقيق الجنائي الإلكتروني

يمكن للمحقق تحليل هذه السجلات لتحديد:

- محاولات الوصول غير المشروعة من عناوين غريبة أو خارجية.
- استهداف خدمات معينة على الشبكة مثل SSH أو HTTP
- الهجمات المتكررة مثل Brute Force أو Port Scanning.
- تتبع سلوك المهاجم عند اختباره لثغرات الحماية.

وقد أشار Bejtlich (2004) إلى أن هذه السجلات تُمثّل "السطر الأمامي للدفاع" في بيئات الشبكات، وأن تحليلها بفعالية يوفّر فهمًا استباقيًا لطبيعة التهديدات.

الأدوات المستخدمة:

- Splunk وELK Stack لتحليل وتصور البيانات.(Gartner, 2023)

6. أدوات مثل Firewall Analyzer وpfSense Dashboard لتقييم السياسات الأمنية. (ManageEngine, 2024)

7. بيانات البروكسي (Proxy Logs)

تُعد بيانات البروكسي من أغنى مصادر المعلومات حول سلوك المستخدم على الإنترنت. يقوم البروكسي بدور الوسيط بين المستخدم وشبكة الإنترنت، ويحتفظ بسجلات مفصلة لكل طلب يتم تقديمه من قِبل المستخدمين. تتضمن هذه السجلات:

- عنوان URL الذي تم طلبه.
- الوقت والتاريخ.
- عنوان IP الداخلي للمستخدم.
- نوع المتصفح والجهاز.
- استجابة الخادم (200 OK, 404 Not Found…).
- حجم البيانات المنقولة (Chuvakin, 2012).

الاستخدام في التحقيق الجنائي الإلكتروني:

- تحديد المواقع التي تم الوصول إليها حتى في حال حذفها من المتصفح.
- كشف سلوك المستخدم داخل المؤسسة وتحليل أنماط تصفحه.
- رصد محاولات تجاوز الحظر باستخدام أدوات مثل VPN أو Tor.
- التحقق من تسريب معلومات إلى مواقع مشبوهة أو خوادم خارجية.

وفقًا لما أشار إليه Nayerifard et al. (2023)، فإن سجلات البروكسي تُعد أداة تحليلية دقيقة تُسهم في كشف "البُعد السلوكي" للمستخدم، مثل نمط التصفح، وتكرار الدخول إلى مواقع معينة، وأساليب محاولة إخفاء الهوية أو استخدام أدوات التنكر الإلكتروني (مثل VPN أو TOR). وهذا يجعلها ذات أهمية خاصة في التحقيقات المتعلقة بسوء الاستخدام، أو في الجرائم الإلكترونية التي تعتمد على التمويه والتلاعب بالهوية الإلكترونية. وتُستخدم هذه السجلات كأدلة مساندة قوية عند تحليل الدوافع والنوايا الإلكترونية ضمن التحقيقات الجنائية المتقدمة.

التحديات

- ضخامة حجم البيانات وتعقيد التحليل الزمني.
- ضرورة الربط بين الهوية الحقيقية للمستخدم وعنوان الـ IP الداخلي.
- الحاجة لتأمين سجل البروكسي من التعديل وتوثيق مصدره وسلسلة الحيازة.

الأدوات المساعدة

- أدوات SIEM مثل IBM QRadar وGraylog.
- برامج تحليل مثل WebSpy Vantage وSquid Log Analyzer.

في ضوء ما تم عرضه من أنواع الأدلة الشبكية، يرى الباحث أن هذه الأدلة تمثل محورًا حاسمًا في التحقيقات الجنائية الإلكترونية، لما توفره من رؤية شاملة وتفصيلية لتفاعلات المستخدمين والأنظمة عبر الشبكات. كما أن طبيعة هذه الأدلة، التي تتميز بالدقة الزمنية والتسلسل المنطقي للعمليات، تمنحها موثوقية عالية في كشف الأنشطة غير المشروعة أو المشبوهة.

إلا أن الباحث يلفت الانتباه إلى أن فعالية الأدلة الشبكية تتوقف على مدى الجاهزية التقنية للجهات المخوّلة بالتحقيق، وكذلك على كفاءة أدوات التحليل المستخدمة. فبدون نظام متكامل لجمع وتوثيق وتحليل هذه

الأدلة، قد تفقد قيمتها القانونية أمام القضاء، أو تصبح عرضة للطعن بسبب خلل في سلسلة الحيازة أو ضعف في التوثيق الفني.

ومن هنا، يُوصي الباحث بضرورة تعزيز البنية التحتية التقنية في المؤسسات القضائية والأمنية، وتدريب الكوادر المختصة على تقنيات تحليل الأدلة الشبكية، بما يضمن استخدامها بشكل سليم، يحافظ على سلامتها، ويعزز من قوة الإثبات القانوني في الجرائم الإلكترونية المعقدة.

الفرع الثاني: التصنيف حسب القصد من الإنشاء

لا تتساوى جميع الأدلة الإلكترونية من حيث الغرض الذي أُنشئت من أجله؛ فبعضها يتم إنشاؤه عمدًا بقصد التوثيق والإثبات في سياقات قانونية أو إدارية أو تنظيمية، بينما يظهر البعض الآخر تلقائيًا كنتيجة ثانوية للنشاط الإلكتروني، دون أن يكون مخصصًا مسبقًا لاستخدامه كدليل. ومن هنا يُبنى أحد أهم تصنيفات الأدلة الإلكترونية، وهو تصنيفها بناءً على القصد من الإنشاء، والذي يُساعد المحقق الجنائي الإلكتروني، والقاضي، والجهات القانونية على فهم الخلفية التقنية والقانونية للدليل، ومدى قابليته للاعتماد في ساحة القضاء.

يُقسّم هذا التصنيف إلى نوعين رئيسيين:

1. الأدلة المعدة سلفًا بقصد الإثبات (Intentionally Created Evidence)
2. الأدلة غير المقصودة أو العرضية (Unintended or Residual Evidence)

أولًا: الأدلة المُعدّة سلفًا بقصد الإثبات

تُعد هذه الفئة من الأدلة الإلكترونية هي الأكثر تنظيمًا من حيث طريقة الإنشاء والتخزين والتحقق، إذ تم إنتاجها بقصد واضح لتوثيق الأنشطة، أو مراقبة المستخدمين، أو دعم القرارات القانونية أو الإدارية. ما يمنح

هذه الأدلة وزنًا قانونيًا كبيرًا هو أنها غالبًا ما تتبع معايير فنية وأمنية واضحة منذ لحظة إنشائها، مما يُسهّل تتبعها والتحقق من صحتها لاحقًا.

وتبرز قوة هذا النوع من الأدلة الإلكترونية، خصوصًا عندما يُربط مع أدلة داعمة أخرى كالبصمات الإلكترونية أو سجلات الدخول، مما يوفّر للمحققين تسلسلًا زمنيًا بصريًا دقيقًا يُعزّز من مصداقية السيناريو التحقيقي أمام الجهات القضائية (Goel et al., 2024).

1. سجلات الدخول والخروج (Access Control Logs)

تعتمد المؤسسات الرسمية على أنظمة إلكترونية تُسجل بدقة عملية دخول وخروج الأفراد، سواء باستخدام بطاقات ممغنطة، أو رموز إلكترونية، أو بصمة اليد أو الوجه.

تُستخدم هذه السجلات في مراقبة الموظفين، والتحقق من الالتزام بساعات العمل، أو في الحالات الأمنية لتحديد المتواجدين في وقت حدوث حادثة معينة.

وتتضمن هذه السجلات:

- اسم المستخدم أو رقمه الوظيفي
- وقت الدخول والخروج
- الموقع الجغرافي أو النقطة الأمنية
- أحيانًا صورة أو توقيع إلكتروني

تكمن أهمية هذه السجلات في كونها دليلًا إلكترونيا مباشرًا يُثبت تواجد الشخص أو عدم تواجده في موقع معين خلال فترة زمنية محددة، مما يجعلها عنصرًا حاسمًا في العديد من التحقيقات الجنائية والتقنية (Wickramasekara & Le-Khac, 2024)4.

2. التواقيع الإلكترونية والعقود الإلكترونية (Digital Signatures and E-Contracts)

مع تسارع التحول الإلكتروني، برزت خدمات الثقة الإلكترونية كركيزة أساسية لضمان موثوقية وصحة المعاملات عن بُعد. تُستخدم هذه الأدوات، وعلى رأسها التوقيع الإلكتروني، في كافة القطاعات البنكية والحكومية والتجارية، ويمنحها القانون حُجّية قانونية كاملة تعادل المستندات الخطية، متى استوفت الشروط الفنية والتشريعية.

شروط قبول التوقيع الإلكتروني المؤهل (وفقًا لقانون 2024):

- الاعتماد والموثوقية: أن يستند التوقيع إلى شهادة مصادقة إلكترونية مؤهلةصادرة عن "مقدم خدمة ثقة مؤهل"، وهي جهة مرخصة تضمن الالتزام بأعلى معايير الأمان.
- الإنشاء الآمن: أن يتم إنشاؤه باستخدام "أداة مؤهلة لإنشاء التوقيع الإلكتروني"، والتي تضمن سيطرة المُوقّع وحده على مفتاح التشفير الخاص به.
- سلامة المحتوى: أن يكون التوقيع مرتبطًا بالبيانات الموقعة بطريقة تتيح كشف أي تعديل لاحق يطرأ عليها، مما يحفظ سلامة المستند ويمنع التلاعب به.

ويمنح قرار بقانون رقم (17) لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة، التوقيع الإلكتروني المؤهل ذات الحجية القانونية المقررة للتوقيع الخطي، مما يجعله مقبولاً للإثبات بشكل كامل أمام القضاء (المادة 25).

البريد الإلكتروني الرسمي (Official Email Correspondence)

البريد الإلكتروني في المؤسسات الحكومية أو الشركات يُعد وثيقة رسمية تثبت المخاطبات أو التعليمات أو القرارات.

تتميز هذه الرسائل بعناصر متعددة تمنحها القوة القانونية، مثل:

- رؤوس الرسائل (Headers) التي تُظهر مصدر الإرسال وتوقيته
- معلومات المستلم والمرسل
- محتوى المراسلة
- التوقيع الإلكتروني المرفق

تُعد رسائل البريد الإلكتروني من الأدلة الإلكترونية المهمة في التحقيقات الجنائية والتجارية، إذ تُستخدم لإثبات أو نفي ادعاءات تتعلق باتفاقات مهنية أو قرارات إدارية، خاصة إذا كانت محفوظة ضمن خوادم رسمية موثوقة يصعب التلاعب بها أو إنكارها لاحقًا. وقد أكدت دراسات حديثة أن البريد الإلكتروني يُوفر سجلًا زمنيًا ومحتوًى نصيًا قابلًا للتحقق والتحليل الفني، مما يجعله أداة موثوقة لإعادة بناء تسلسل الأحداث في القضايا المعقدة (Harisha & Mishra, 2023)

4. أنظمة التتبع والمراقبة (GPS & Digital Monitoring Systems)

تُستخدم أجهزة تحديد المواقع (GPS) لتوثيق تحركات الأفراد والمركبات بدقة عالية، حيث تُسجّل البيانات تلقائيًا في أنظمة إدارة الحركة أو التطبيقات الأمنية.

من التطبيقات الشائعة:

- تتبع مركبات الشركات لضمان التزام السائقين
- توثيق مسار شحنات أو مواد حساسة
- إثبات وجود الشخص في مكان معين أثناء ارتكاب حادثة

ويُستخدم هذا النوع من الأدلة في القضايا الجنائية، والقضايا العمالية، وحتى في حالات الطلاق أو النزاع على الحضانة، حين يُطلب إثبات التواجد المكاني والزمني بدقة.

لكن، يجب إثبات أن الجهاز كان يعمل بشكل صحيح، ولم يُعبث به، وأن البيانات صادرة عن مصدر موثوق (Taylor et al., 2011).

ثانيًا: الأدلة غير المقصودة أو العَرَضية (Unintentionally Generated Evidence)

تشير هذه الفئة من الأدلة إلى البيانات الإلكترونية التي لم تُنشأ بغرض استخدامها كدليل، بل وُجدت في سياق استخدام المستخدم للأجهزة أو الخدمات الإلكترونية بشكل طبيعي. ومع ذلك، فإن هذه البيانات قد تكتسب أهمية قانونية وأدلة دامغة إذا تم تحليلها بشكل صحيح في إطار تحقيق جنائي إلكتروني أو نزاع قانوني.

سماتها الأساسية

- لا يُقصد بها التوثيق أو الإثبات القانوني عند إنشائها.
- غالبًا ما يتم كشفها واسترجاعها عن طريق خبراء التحليل الجنائي الإلكتروني.
- تحتاج إلى تحليل معمق وتفسير فني لربطها بسياق الجريمة أو الواقعة.

1. ملفات الكوكيز (Cookies)

تُعد الكوكيز مخزنًا للسلوك الإلكتروني للمستخدم، حيث تحفظ معلومات تفصيلية عن تفضيلات التصفح، نمط الاستخدام، أوقات الدخول، والصفحات التي يتم زيارتها بشكل متكرر. وعلى الرغم من أنها صُممت أصلاً لتحسين تجربة المستخدم، إلا أنها قد تُستخدم في التحقيقات لتحديد توقيتات الوصول إلى مواقع إلكترونية محددة، أو ربط المستخدم بسلوكيات معينة على الإنترنت.

على سبيل المثال، في سيناريو افتراضي لقضية ابتزاز إلكتروني، يمكن لفريق التحقيق تحليل ملفات الكوكيز الخاصة بجهاز المشتبه به، فإذا تبين أنه زار الموقع الذي نُشرت عليه المواد المُبتزة عدة مرات، وفي توقيتات

تتزامن مع إرسال رسائل التهديد، يمكن قبول هذا التحليل كقرينة إلكترونية تدعم سلسلة الإثبات الأوسع. وقد تم بالفعل قبول أدلة مشابهة تعتمد على تحليل بيانات التصفح في العديد من القضايا حول العالم.

2. سجل التصفح (Browsing History) :

يشكّل سجل التصفح خريطة ذهنية إلكترونية توثق بدقة الاهتمامات الإلكترونية للمستخدم، وهو ما يمنحها أهمية مضاعفة عند دراسة النية الإجرامية أو تسلسل الأحداث. فالوصول المتكرر إلى مواقع محددة يمكن أن يعكس تحضيرًا لجريمة، أو حتى يكشف عن شبكة تواصل غير مشروعة. في سيناريو افتراضي لقضية اختراق خوادم مؤسسة مصرفية، يمكن للمحققين استرجاع سجل التصفح من جهاز المشتبه به فإذا كشف السجل عن دخوله المتكرر إلى منتديات متخصصة في بيع أدوات الاختراق (Exploits)، بالإضافة إلى مشاهدته لدروس حول تجاوز بروتوكولات الحماية المصرفية، فإن هذا السجل يمكن أن يُستخدم كدليل ظرفي (قرينة) قوي. ورغم أنه لا يثبت ارتكاب الجريمة بشكل مباشر، إلا أنه يساعد في إثبات النية والمعرفة التقنية اللازمة، مما يساهم في بناء سلسلة الأدلة لإثبات التهمة.

بيانات الملفات المؤقتة (Temporary Files):

تُعد الملفات المؤقتة ونسخ الظل (Shadow Copies) بمثابة "ظلال إلكترونية" للنشاط الفعلي للمستخدم، حيث يتم إنشاؤها تلقائيًا بواسطة نظام التشغيل أو التطبيقات أثناء التعامل مع المستندات. هذه الملفات تظل قابلة للاسترداد حتى بعد حذف الملف الأصلي، مما يسمح للمحققين الإلكترونيين باستعادتها وتحليلها كجزء من عملية التحقيق الجنائي الإلكتروني (Bunting, 2018). إن تحليل هذه النسخ، التي يتم إنشاؤها بواسطة خدمات مثل Volume Shadow Copy Service (VSS) في أنظمة ويندوز، يعتبر إجراءً قياسيًا للكشف عن الإصدارات السابقة للملفات أو استعادة البيانات المحذوفة(Carvey, 2020) .

في التحقيقات الجنائية، يمكن أن تكون البيانات الوصفية (Metadata) والملفات المحذوفة هي الخيط الذي يقود إلى إثبات التهمة. على سبيل المثال، في قضية القاتل المتسلسل دينيس رايدر المعروف بـ (BTK)،

أرسل رايدر قرصًا مرنًا (Floppy Disk) إلى الشرطة يحتوي على مستند Microsoft Word. قام المحققون بتحليل البيانات الوصفية (Metadata) لملف محذوف كان على نفس القرص (Lasswell, 2005).

كشفت هذه البيانات أن المستند تم تعديله آخر مرة بواسطة مستخدم باسم "Dennis" في "كنيسة المسيح اللوثرية" (Christ Lutheran Church)، حيث كان رايدر رئيسًا لمجلس الكنيسة. هذا الدليل الإلكتروني، الذي تم استرجاعه من ملف كان يُعتقد أنه محذوف، كان حاسمًا في تحديد هوية رايدر والقبض عليه بعد 30 عامًا من جرائمه (O'Connor, 2005). هذا المثال يوضح كيف يمكن لـ "النسخة المفقودة" أو البيانات المخفية في ملف أن تغير مجرى قضية بالكامل.

3. بيانات الموقع الجغرافي (GPS Metadata) :

تُخزن هذه البيانات في ملفات الصور والفيديوهات والمراسلات الإلكترونية، وغالبًا ما تحتوي على معلومات دقيقة حول الإحداثيات الجغرافية وموقع المستخدم وقت إنشاء الملف. تُستخدم هذه المعلومات لتحديد مكان وجود الشخص في زمن معين، ما يجعلها دليلاً قويًا في قضايا تتطلب إثبات الحضور أو الغياب في موقع الجريمة.

سجل التعديلات: (File Modification Logs)

يُظهر هذا السجل كافة العمليات التي تمت على ملف معين، متى تم إنشاؤه، فتحه، تعديله، أو نقله. قد يحتوي على توقيعات إلكترونية للمستخدمين، وتوقيتات دقيقة تُستخدم كقرائن ظرفية قوية عند محاولة إخفاء آثار إلكترونية.

هذا وتمثل الأدلة غير المقصودة تمثل كنزًا خفيًا في عالم التحقيق الإلكتروني، حيث تكشف ما لا يريد المستخدم إظهاره. ومع ذلك، فإن اعتمادها القانوني يتطلب مهارة عالية في التوثيق، والحرص على الحفاظ على "سلامة البيانات" (Data Integrity) خلال مراحل التحليل. ولعل القيمة الأساسية لهذه الأدلة تكمن

في قدرتها على الربط بين الأحداث الزمنية والسلوك الإلكتروني، مما يجعلها أدلة قوية إذا ما استُخرجت وفسّرت بطريقة علمية.

يرى الباحث أن تصنيف الأدلة الإلكترونية إلى "مُعدّة سلفًا بقصد الإثبات" و"غير مقصودة أو عَرَضية" لا يقتصر على كونه تصنيفًا نظريًا، بل يعكس واقعًا عمليًا بالغ الأهمية في ميدان التحقيقات الجنائية الإلكترونية، خاصة في السياق الفلسطيني الذي يشهد تطورًا متسارعًا في استخدام التكنولوجيا مقابل بطء نسبي في مأسسة أدوات التحقيق الإلكتروني ضمن النظام القضائي.

ففيما يتعلق بالأدلة المعدّة مسبقًا بقصد الإثبات، فإن الباحث يؤكد على ضرورتها لتكريس ثقافة التوثيق الإلكتروني في المؤسسات، سواء كانت حكومية أو خاصة. ذلك لأن وجود نظام إلكتروني موثق مثل الكاميرات، والسجلات الإلكترونية، والتوقيعات الإلكترونية، لا يسهم فقط في الوقاية من الجرائم، بل يسهّل عملية الإثبات في حال وقوعها. ومع أن الكثير من هذه الأدوات باتت جزءًا من البنية التحتية للمؤسسات الكبرى، إلا أن الباحث يلاحظ ضعف استخدامها في المؤسسات الصغيرة أو في القطاعات غير الرسمية، مما يُفقد المنظومة القضائية مصادر إثبات حيوية.

أما في الجانب الآخر، أي الأدلة غير المقصودة، فيرى الباحث أنها تمثّل التحدي الأكبر أمام جهات التحقيق، سواء من حيث الاكتشاف أو التحليل أو القبول القانوني. فرغم ما تحمله هذه الأدلة من قيمة إثباتية هائلة – نظرًا لطبيعتها الخفية وارتباطها المباشر بسلوك المستخدم – فإن استغلالها بشكل قانوني سليم يتطلب كوادر فنية متخصصة، ومختبرات جنائية إلكترونية مزودة بأحدث الأدوات، وهو ما لا يتوفر دائمًا في الواقع الفلسطيني أو في العديد من الدول النامية.

كما يشير الباحث إلى أن بعض الجرائم الإلكترونية المعاصرة (كالابتزاز الإلكتروني، والتشهير، وتسريب البيانات) تعتمد بشكل أساسي على أدلة غير مقصودة يصعب تتبعها إلا من خلال تحليل معمّق لسجلات التصفح، والكوكيز، والبيانات الوصفية، وهو ما يجعل هذه الفئة من الأدلة حجر الزاوية في مكافحة الجريمة

الإلكترونية. ومع ذلك، تبقى قابليتها للرفض القضائي قائمة إذا لم يتم توثيقها ضمن "سلسلة الحيازة" القانونية المعتمدة، أو إذا أُسيء التعامل معها أثناء استخراجها أو تحليلها.

ختامًا، يدعو الباحث إلى تبني منهج مزدوج في التعامل مع الأدلة الإلكترونية: تعزيز ثقافة التوثيق الإلكتروني المسبق، وتطوير البنية التحتية والأدوات التقنية القادرة على تحليل واستثمار الأدلة العرضية، مع سنّ تشريعات فلسطينية واضحة تُنظم معايير القبول القضائي لكلا النوعين من الأدلة الإلكترونية، بما يحقق التوازن بين الحماية القانونية والعدالة الإلكترونية الفعالة.

يلخص الباحث إلى أن التعامل الفعال مع الأدلة الإلكترونية ضمن المنظومة القضائية، لا سيما في السياق الفلسطيني، يتطلب تبني منهجية مزدوجة. ترتكز هذه المنهجية على محورين متكاملين: أولهما، تعزيز ثقافة التوثيق الإلكتروني الاستباقي من خلال تشجيع المؤسسات والأفراد على استخدام الأدلة المُعدّة للإثبات (كالتوقيعات الإلكترونية وسجلات المراقبة) لما لها من دور وقائي وتسهيلي في عملية الإثبات. وثانيهما، بناء القدرات الفنية والتشريعية اللازمة للتعامل مع الأدلة الإلكترونية غير المقصودة (العَرَضية) ، والتي تمثل حجر الزاوية في مكافحة الجرائم السيبرانية المعاصرة.

ويؤكد الباحث أن نجاح هذا التوجه مرهون بتوفير الكوادر المتخصصة والمختبرات الجنائية الإلكترونية، وسنّ تشريعات واضحة تضمن حجية كلا النوعين من الأدلة أمام القضاء، بما يحقق التوازن المنشود بين مقتضيات العدالة الإلكترونية وحماية الحقوق.

الفصل الثاني

حجية الدليل الإلكتروني وشروط استخدامه أمام القضاء

في ظل التطورات التكنولوجية المتسارعة واتساع رقعة استخدام الوسائط الإلكترونية، أصبحت الجرائم الإلكترونية تُشكّل تحديًا غير مسبوق لأنظمة العدالة الجنائية، ليس فقط من حيث طبيعة الأفعال المرتكبة، بل أيضًا من حيث وسائل الإثبات التي تستند إليها التحقيقات والمحاكمات. إذ لم تعد الأدلة الورقية أو الشهادات المباشرة كافية لكشف الجرائم، بل بات من الضروري الاعتماد على "الدليل الإلكتروني" بوصفه وسيلة إثبات حديثة تتلاءم مع طبيعة الجريمة الإلكترونية المعاصرة.

ومع أن هذا النوع من الأدلة يوفر قدرة دقيقة وفعالة على تتبع الجريمة وكشف مرتكبيها، إلا أن التعامل معه يطرح إشكاليات قانونية وتقنية تتعلّق بمدى مشروعية جمعه، وسلامة تحليله، ومدى قابليته للاعتماد القضائي. كما يبرز سؤال جوهري: إلى أي مدى يمكن للقضاء الاعتماد على الأدلة الإلكترونية دون المساس بضمانات المحاكمة العادلة؟

وللإجابة عن هذه الإشكاليات، يسعى هذا الفصل إلى تحليل موضوع الدليل الإلكتروني من زاويتين أساسيتين متكاملتين:

- الزاوية الأولى تتعلق بحجيته القانونية كوسيلة إثبات أمام المحاكم، وما يتطلبه ذلك من شروط شكلية وموضوعية لقبوله، مثل مشروعية الجمع، وسلامة المحتوى الإلكتروني، وموثوقية المصدر.
- الزاوية الثانية تُركز على الجهات المختصة قانونًا وفنيًا بجمع وتحليل وتقديم هذا الدليل، سواء كانت أجهزة الضبط القضائي، أو الخبراء الفنيين، أو الجهات القضائية المختصة بالفصل في النزاعات المتعلقة بالأدلة الإلكترونية.

وعليه، سيتم تقسيم هذا الفصل إلى مبحثين رئيسيين:

- المبحث الأول: يتناول حجية الدليل الإلكتروني في الإثبات الجنائي، من خلال بحث الشروط القانونية لقبوله، ومدى قوته أمام القضاء، مقارنة بالأدلة التقليدية.
- المبحث الثاني: يسلّط الضوء على الجهات المختصة بالتعامل مع الدليل الإلكتروني، موضحًا أدوار كل جهة في مرحلة الجمع، والتحليل، والتقديم، مع بيان مدى كفاية الإطار التشريعي الفلسطيني في هذا المجال.

المبحث الأول: حجية الدليل الإلكتروني في الإثبات الجنائي

لقد شكّل الدليل الإلكتروني تحوّلًا نوعيًا في منظومة الإثبات الجنائي، إذ أضحى يمثل ركيزة أساسية في القضايا المعاصرة التي تتعلق بالجريمة الإلكترونية أو تتضمن عناصر إلكترونية، سواء كانت هذه الجرائم موجهة ضد الأشخاص أو المؤسسات أو الأمن العام. وبفعل التطور التكنولوجي، لم تعد البيانات الإلكترونية محصورة في الحواسيب، بل امتدت لتشمل الهواتف الذكية، وشبكات التواصل الاجتماعي، والسجلات الإلكترونية، وتطبيقات الحوسبة السحابية، وغيرها من الوسائط التي أصبحت مصدرًا رئيسيًا للمعلومات الجنائية.

ومع بروز هذا النوع من الأدلة، برزت معه تساؤلات قانونية جوهرية تتعلق بمدى حجية الدليل الإلكتروني في الإثبات، وكيفية قبوله في القضايا الجنائية، وما إذا كان يُعامل بنفس مستوى الحجية التي تتمتع بها الأدلة التقليدية كالشهادة أو الوثائق أو الاعتراف. كما أصبح من الضروري البحث في الشروط التي يجب توافرها في هذا الدليل كي يُعتد به أمام القضاء، خصوصًا في ظل إمكانية التلاعب به أو اختراقه أو تغييره باستخدام وسائل تقنية يصعب اكتشافها دون خبرة متخصصة.

ومن هذا المنطلق، يتناول هذا المبحث مسألة الحجية القانونية للدليل الإلكتروني باعتباره من أبرز أشكال الإثبات في البيئة المعاصرة، حيث سيتم تحليل ملامحه القانونية وتحديد المعايير التي تؤثر في قوة هذا الدليل ومدى اعتماده قضائيًا. كما سيُناقش التفاوت بين النظم القانونية في هذا الصدد، مع الإشارة إلى مدى استجابة المشرع الفلسطيني لهذه التحديات.

وسيُقسم هذا المبحث إلى مطلبين رئيسيين:

- المطلب الأول: يتناول الأساس القانوني لحجية الدليل الإلكتروني من خلال استعراض موقف التشريعات المقارنة والفقه القانوني، وتحليل طبيعة الحماية التي يوفرها القانون لهذا النوع من الأدلة.

- المطلب الثاني: يتناول ضوابط قبول الدليل الإلكتروني أمام القضاء، من خلال تحديد الشروط الشكلية والموضوعية، وضمانات الخصوم، ومدى توافق الإجراءات مع معايير المحاكمة العادلة.

المطلب الأول: الأساس القانوني لحجية الدليل الإلكتروني

مع تطور الجرائم الإلكترونية واعتمادها على بيئات غير مادية، لم يعد بالإمكان حصر وسائل الإثبات في الأدلة التقليدية كالاعتراف أو الشهادة أو المحررات الورقية. فقد فرضت الطبيعة الخاصة للدليل الإلكتروني تحديات جديدة أمام الأنظمة القضائية، وأصبح لزامًا على المشرّع والفقه القانوني أن يعيدا النظر في مفهوم "الحجية" وشروطها، بما يتناسب مع البيانات المستخرجة من مصادر إلكترونية.

إن حجية الدليل الإلكتروني لا تُستمد من طبيعته التقنية فحسب، بل من الإطار القانوني الذي يُنظم قبوله واعتماده داخل منظومة الإثبات. وهذه الحجية تتباين من نظام قانوني لآخر، وتتأثر بعوامل متعددة مثل مصدر الدليل، وآلية استخراجه، وضمانات المعالجة الفنية، ومدى احترام حقوق الدفاع والخصوصية.

ومن هذا المنطلق، يُقسم هذا المطلب إلى فرعين رئيسيين:

- الفرع الأول يتناول حجية الدليل الإلكتروني كما وردت في التشريعات المقارنة والفقه القانوني.
- الفرع الثاني يُخصص لدراسة مدى اعتراف المشرّع الفلسطيني بحجية هذا النوع من الأدلة، وتحليل الإطار القانوني الذي يحكم التعامل معه.

الفرع الأول: حجية الدليل الإلكتروني في التشريعات المقارنة والفقه القانوني.

مع تصاعد أهمية الفضاء الإلكتروني في الحياة اليومية، أصبحت الجرائم الإلكترونية جزءًا لا يتجزأ من المشهد الجنائي العالمي، مما فرض على الأنظمة القانونية ضرورة إعادة النظر في وسائل الإثبات المتاحة، ومن أبرزها "الدليل الإلكتروني". فقد بات هذا النوع من الأدلة يحتل مكانة متقدمة في منظومة الإثبات الجنائي، لكونه يحمل طابعًا دقيقًا وسريعًا يصعب دحضه، لكن في الوقت ذاته يتطلب حذرًا بالغًا لضمان صحته ومصداقيته.

وقد تعاملت التشريعات المقارنة والفقه القانوني مع حجية الدليل الإلكتروني من منطلق مزدوج: من جهة، إقرار بأهميته كوسيلة إثبات فعالة، ومن جهة أخرى، التأكيد على وجوب احترام معايير فنية وقانونية صارمة تضمن عدم التلاعب به أو المساس بسلامته.

أولاً: التشريعات المقارنة

أدركت العديد من الدول أهمية إدماج الأدلة الإلكترونية ضمن منظومتها القانونية. ففي بريطانيا، يشير قانون *Police and Criminal Evidence Act 1984* إلى إمكانية اعتماد الدليل الإلكتروني بشرط ضمان صحته وسلامته التقنية، مع الحفاظ على ما يسمى بـ "سلسلة الحيازة الإلكترونية" (Chain of Custody) التي تضمن عدم التلاعب بالدليل منذ لحظة جمعه وحتى تقديمه للمحكمة. وقد أُكد هذا التوجه من خلال حكم محكمة الاستئناف البريطانية في قضية *(R v. Shephard, 1993)*، والذي أقرّ بحجية الأدلة الإلكترونية إذا ما ثبت أن النظام المستخدم لجمعها كان يعمل بشكل طبيعي، وأن البيانات لم تُعدّل أو تُزوّر.

أما في الولايات المتحدة الأمريكية، فقد جاء التعديل الذي طرأ عام 2006 على قواعد الإثبات الفيدرالية *Federal Rules of Evidence* ليُعزز مكانة الأدلة الإلكترونية، حيث تنص المادة (902) على إمكانية قبول السجلات الإلكترونية مباشرة دون شهادة خبير، بشرط أن تكون تلك السجلات موقعة إلكترونيًا أو موثقة من جهة موثوقة. ويؤكد القضاء الأمريكي في قضايا مثل *(United States v. Tank, 2003)* على أن الدليل الإلكتروني له حجية معتبرة إذا كان مصحوبًا بشهادة فنية توضح طريقة الحصول عليه ومعايير سلامته.

وفي ألمانيا، يعدّ الدليل الإلكتروني جزءًا من الأدلة المعترف بها رسميًا، حيث ينص القانون الجنائي الألماني وقانون الإجراءات الجنائية على مشروعية استخدام الأدلة الإلكترونية متى توافرت شروط تتعلق بمصدرها وسلامتها وعدم مساسها بالخصوصية الفردية، وذلك بموجب المادة 100 من قانون الإجراءات الجنائية.

أما على مستوى الدول العربية، فإن بعض التشريعات أبدت اهتمامًا متزايدًا بالدليل الإلكتروني. فقد نص القانون الإماراتي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، في المادة (11)، على أن البيانات الإلكترونية تُعد من الأدلة المشروعة شريطة أن يتم الحصول عليها وفق ضوابط تقنية وقانونية معتمدة. كما أدخلت الأردن تعديلات على قانون البينات سنة 2018 تضمنت الاعتراف الصريح بحجية الأدلة الإلكترونية، شريطة أن يتم تقديمها وفقًا لقواعد موضوعية وإجرائية دقيقة.

وفي مصر، نصّ قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 على استخدام الأدلة الإلكترونية، واشترط لضمان حجيتها أن يتم جمعها من خلال جهات مختصة، وبوسائل تقنية تضمن عدم العبث بها، وأن يتم تقديمها للمحكمة بشكل يضمن سلامتها وعدم انتهاك الخصوصية أو الحقوق الدستورية.

وفي فلسطين، يمثل قرار بقانون رقم (17) لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة النقلة النوعية في هذا المجال، حيث منح الحجية القانونية الكاملة للأدلة المستمدة من المعاملات الإلكترونية. فوفقًا للمادة (30) و (31) منه، يتمتع "التوقيع الإلكتروني المؤهل" بذات الحجية المقررة للتوقيع الخطي، ويُعتبر مقبولاً للإثبات. كما يؤكد القانون في مواده المختلفة على ضرورة أن تصدر خدمات الثقة (كالتوقيع والختم الإلكتروني) عن "مقدمي خدمات ثقة مؤهلين" وباستخدام أدوات آمنة، وهو ما يضع إطارًا قانونيًا واضحًا لضمان سلامة وموثوقية الدليل الإلكتروني، ويتماشى مع المبادئ العالمية المتعلقة بسلامة المصدر وصحة البيانات.

أما في الأردن، فقد خطى المشرّع خطوات هامة لترسيخ حجية الدليل الإلكتروني. فبموجب قانون المعاملات الإلكترونية رقم (15) لسنة 2015، وتحديدًا في المادة (15) و (16)، أُعطي للسجل الإلكتروني والتوقيع الإلكتروني الحجية القانونية ذاتها المقررة للمستندات الخطية والتواقيع اليدوية.

ثانياً: في الفقه القانوني

تناول الفقه القانوني الحديث مسألة حجية الدليل الإلكتروني من زوايا متعددة، وظهرت اتجاهات متنوعة في هذا السياق. فهناك من يرى أن الدليل الإلكتروني يمكن أن يتمتع بنفس القوة الثبوتية التي يتمتع بها الدليل الكتابي أو المحررات التقليدية، إذا ما تم جمعه وفقًا لضمانات قانونية وفنية محكمة. في هذا السياق، يرى زايد (2022، ص43) أن "الدليل الإلكتروني لا يفتقر إلى الحجية، لكنه يحتاج إلى شروط محددة تُكسبه القوة القانونية، أبرزها صدق المصدر، وسلامة الحفظ، وإمكانية التحقق من محتواه."

أما عبد العال (2021، ص659) فيُشير إلى أن حجية الدليل الإلكتروني لا تقتصر على قيمته التقنية، بل تعتمد على منظومة متكاملة من الإجراءات، تبدأ بمشروعية الحصول عليه، وتمر بسلامة فحصه وتحليله، وتنتهي بتقديمه للقاضي وفق قواعد دقيقة تضمن عدم المساس بحقوق الأطراف.

كما يذهب الجلعود (2024، ص2388) إلى اعتبار أن الدليل الإلكتروني "أقوى من الشهادة الورقية في بعض الأحيان، نظراً لإمكانية استرجاع البيانات الأصلية ومراجعة سجل الحفظ والتحليل الفني"، لكنه يربط ذلك بالحفاظ الصارم على قواعد "الحياد الإلكتروني" في التعامل مع الأجهزة والأنظمة المستخدمة.

ويُعدّ تعريف Casey (2011, p.4) مرجعًا مهمًا في هذا السياق، حيث يُعرّف الدليل الإلكتروني بأنه: "أي معلومات ذات قيمة محتملة في التحقيق، تُخزن أو تُنقل عبر وسيط إلكتروني، ويجب التعامل معها بمراعاة تامة لمصداقيتها وسلامتها أثناء الإجراءات القضائية"، وهو ما يتماشى مع توجهات اتفاقية بودابست بشأن الجرائم الإلكترونية.

يرى الباحث أن تعامل التشريعات المقارنة مع الدليل الإلكتروني يعكس درجة وعي قانوني عميقة بأهمية هذا النوع من الأدلة في تحقيق العدالة الجنائية الحديثة. فحجية الدليل الإلكتروني لا تُبنى فقط على ثقة تقنية في الوسيط، بل على احترام سلسلة متكاملة من الشروط تبدأ من لحظة الحصول عليه، وتمر بمراحله الفنية

المختلفة، وتنتهي بتقديمه للمحكمة في إطار يحمي الحقوق والحريات. إن غياب أي حلقة من هذه السلسلة قد يُضعف من حجية الدليل، أو يؤدي إلى استبعاده تمامًا.

في مؤلفه "الوجيز في شرح قانون الجرائم الإلكترونية الفلسطيني"، يتناول الدكتور معتصم المصري حجية الدليل الإلكتروني كأحد أبرز التحديات التي تواجه العدالة الجنائية الحديثة. يرى المؤلف أن المشرّع الفلسطيني، بإصداره قانون الجرائم الإلكترونية، قد حسم الجدل حول مشروعية الدليل الإلكتروني، لكنه ترك الباب مفتوحًا أمام السلطة التقديرية للقاضي لتقييم مدى موثوقيته وقيمته في الإثبات.

ويؤكد د. المصري أن حجية الدليل الإلكتروني لا تُستمد فقط من النص القانوني الذي يجيزه، بل ترتبط ارتباطًا وثيقًا بمدى الالتزام بالضوابط الإجرائية عند جمعه وتحريزه.

ويشدد على أن "سلسلة الحيازة" (Chain of Custody) وسلامة الدليل من أي عبث أو تعديل هما الركيزتان الأساسيتان اللتان تمنحان الدليل قيمته أمام القضاء. فإذا شاب الشك إجراءات الضبط أو التحليل، فإن ذلك يضعف من حجية الدليل وقد يؤدي إلى استبعاده، حتى لو كان القانون يعترف به من حيث المبدأ.

لذلك، يخلص المؤلف إلى أن الحجية القانونية للدليل الإلكتروني هي حجية "نسبية" تخضع لرقابة القضاء، وتتعزز أو تضعف بناءً على الإجراءات الفنية التي تصاحب عملية استخراجه وتقديمه، مما يلقي بعبء كبير على جهات التحقيق والخبرة الفنية في توثيق كل خطوة لضمان قبول الدليل وبناء قناعة المحكمة.

ومن هذا المنطلق، يُوصي الباحث بضرورة قيام التشريعات العربية، وعلى رأسها التشريع الفلسطيني، بوضع تعريف تشريعي دقيق للدليل الإلكتروني، يتبعه إطار تنظيمي واضح يحدد شروط الحجية، ويُوفّر التدريب الفني والقانوني اللازم للقضاة وأعضاء النيابة العامة، ضمانًا لعدالة إجرائية متكاملة. كما يجب أن تُنشأ جهات إلكترونية مستقلة لفحص هذا النوع من الأدلة، بما يُحقق الحياد ويمنع تسييس أو تلاعب بهذه الوسائل التقنية.

الفرع الثاني: مدى اعتراف القانون الفلسطيني بحجية الدليل الإلكتروني.

رغم تزايد الحاجة إلى استخدام الأدلة الإلكترونية في الإجراءات الجنائية، خاصة في ضوء التوسع غير المسبوق في استخدام الوسائط الإلكترونية في ارتكاب الجرائم، إلا أن المنظومة القانونية الفلسطينية لا تزال تُعاني من قصور تشريعي واضح في هذا المجال. فالمشرّع الفلسطيني لم يُدرج حتى اللحظة تعريفًا صريحًا أو تنظيميًا للدليل الإلكتروني في القوانين التقليدية المعمول بها، الأمر الذي أثار الكثير من الإشكاليات عند التطبيق القضائي.

ويُلاحظ عند مراجعة قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، وقانون البينات رقم (4) لسنة 2001، غياب أي إشارة إلى الأدلة ذات الطابع الإلكتروني، سواء من حيث التعريف أو التنظيم أو الضوابط الفنية المرتبطة بجمعها وتقديمها أمام القضاء. وقد يُعزى ذلك إلى أن هذه التشريعات وُضعت في مرحلة لم تكن فيها البيئة الإلكترونية قد تطورت إلى الحد الذي يستدعي دمج أدلة ناتجة عن التكنولوجيا الحديثة ضمن منظومة الإثبات.

وفي عام 2018، حاول المشرّع سدّ هذا الفراغ من خلال إقرار قانون الجرائم الإلكترونية رقم (10) لسنة 2018، الذي يُعتبر النص القانوني الأول في فلسطين الذي تناول بشكل مباشر مسألة الدليل الإلكتروني. حيث نصّت المادة (37) من هذا القانون على ما يلي:

"يُعدّ الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات."

لقد جاء القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية ليُعالج فراغاً تشريعياً كبيراً في التعامل مع الأدلة الإلكترونية في النظام القضائي الفلسطيني وتُعتبر المواد من (32) إلى (37) من هذا القانون بمثابة العمود الفقري للإطار الإجرائي والموضوعي الذي يحكم التعامل مع الدليل الإلكتروني. وفيما يلي شرح تفصيلي لكل مادة من هذه المواد:

المادة (32): إجراءات التفتيش والبحث عن الأدلة الإلكترونية

تنص المادة (32) على الإجراءات القانونية للتفتيش والضبط في الوسائل الإلكترونية، وتُعد هذه المادة من أهم المواد التي تُنظم الشق الإجرائي للحصول على الدليل الإلكتروني. وتتضمن المادة الضوابط التالية:

أولاً: شرط الإذن القضائي المسبق

أكدت المادة (32) على ضرورة الحصول على إذن قضائي مسبق من النيابة العامة أو المحكمة المختصة قبل إجراء عملية التفتيش الإلكتروني، وذلك حماية للحق في الخصوصية الذي كفله القانون الأساسي الفلسطيني ويُستثنى من ذلك حالات التلبس بالجريمة أو حالات الضرورة الملحة التي يُخشى فيها ضياع الدليل.

ثانياً: نطاق التفتيش

حددت المادة نطاق التفتيش بأن يشمل:

- الأجهزة الإلكترونية (الحواسيب، الهواتف الذكية، الأجهزة اللوحية)
- أنظمة المعلومات والشبكات
- وسائط التخزين الإلكترونية (أقراص صلبة، ذاكرات خارجية، بطاقات الذاكرة)
- البيانات المخزنة على السحابة الإلكترونية
- سجلات الاتصالات وبيانات الاستخدام

ثالثاً: الاستعانة بالخبراء

أجازت المادة (32) للنيابة العامة أو الجهات المختصة الاستعانة بخبراء فنيين متخصصين في مجال تكنولوجيا المعلومات والأمن الإلكتروني لضمان سلامة عملية جمع الأدلة وتحليلها ويُشترط في هؤلاء الخبراء أن يكونوا معتمدين من الجهات الرسمية وأن يلتزموا بمبادئ الحياد والموضوعية.

رابعاً: ضمانات الحفاظ على سلامة الدليل

نصت المادة على وجوب اتباع الإجراءات الفنية اللازمة للحفاظ على سلامة الدليل الإلكتروني من التلف أو التعديل، بما في ذلك:

- استخدام أدوات النسخ الآمن (Forensic Imaging)
- توثيق سلسلة الحيازة (Chain of Custody)
- استخدام تقنيات التشفير لحماية الأدلة المضبوطة
- إعداد محاضر رسمية موثقة لكل خطوة من خطوات التفتيش

المادة (33): حق الحضور والاطلاع

كفلت هذه المادة حق المشتبه به أو محاميه في الحضور أثناء عملية التفتيش الإلكتروني، وذلك تطبيقاً لمبدأ المحاكمة العادلة وحق الدفاع, كما أجازت للمشتبه به أو وكيله طلب نسخة من الأدلة المضبوطة بعد انتهاء عملية الفحص الأولي.

المادة (34): التزامات مقدمي الخدمة

ألزمت المادة (34) مقدمي خدمات الإنترنت والاتصالات والشركات التقنية بالتعاون مع السلطات القضائية في توفير البيانات والمعلومات اللازمة للتحقيقات، مع مراعاة احترام خصوصية المستخدمين والالتزام بالأوامر القضائية فقط.

المادة (35): حفظ البيانات

منحت هذه المادة النيابة العامة صلاحية إصدار أمر بحفظ البيانات الإلكترونية لدى مقدمي الخدمة لمدة محددة لمنع حذفها أو تعديلها أثناء التحقيق وهذا الإجراء يُعد ضمانة مهمة لحماية الأدلة من الضياع، خاصة في القضايا التي تتطلب وقتاً طويلاً للتحقيق.

(36): السرية والحماية

أكدت المادة على التزام جميع الأطراف المشاركة في جمع وتحليل الأدلة الإلكترونية بالحفاظ على سرية المعلومات وعدم إفشائها إلا للجهات المختصة قانوناً وتُعد مخالفة هذا الالتزام جريمة يعاقب عليها القانون.

(37): الحجية القانونية للدليل الإلكتروني

تُعتبر المادة (37) من أهم المواد في هذا القانون، حيث أقرت صراحة بحجية الدليل الإلكتروني كوسيلة إثبات أمام المحاكم. وتنص المادة على أن:

"كل دليل ناتج عن استخدام وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية يُعد من أدلة الإثبات المعتمدة أمام المحاكم المختصة."

الأثر القانوني للمادة (37):

1. المساواة في الحجية: أصبح الدليل الإلكتروني يتمتع بنفس القوة الثبوتية التي تتمتع بها الأدلة التقليدية، بشرط استيفاء الشروط القانونية.
2. حرية القاضي في التقدير: منحت المادة القاضي سلطة تقديرية في تقييم قوة الدليل الإلكتروني بناءً على ظروف كل قضية، مع مراعاة مصدره وطريقة جمعه وسلامته.
3. اتساع نطاق الإثبات: لم تقصر المادة الدليل الإلكتروني على نوع معين، بل شملت جميع أشكال البيانات الإلكترونية، مما يُتيح مرونة في التطبيق.
4. الحاجة إلى التقارير الفنية: رغم إقرار حجية الدليل، إلا أن الممارسة القضائية تتطلب في الغالب إرفاقه بتقرير فني من خبير معتمد يُؤكد صحته وسلامته.

التحديات التطبيقية للمواد (32-37):

رغم أهمية هذه المواد في تنظيم التعامل مع الدليل الإلكتروني، إلا أن التطبيق العملي يواجه عدة تحديات:

1. غياب اللوائح التنفيذية: لم تصدر حتى الآن لوائح تنفيذية تفصيلية تُحدد الإجراءات الدقيقة لتطبيق هذه المواد.
2. نقص الكوادر المتخصصة: عدد الخبراء الفنيين المعتمدين في مجال الأدلة الإلكترونية لا يزال محدوداً.
3. محدودية الإمكانيات التقنية: تفتقر بعض الجهات القضائية إلى الأدوات والبرامج المتطورة اللازمة لفحص وتحليل الأدلة الإلكترونية.
4. الحاجة إلى التدريب: يحتاج القضاة وأعضاء النيابة العامة إلى تدريب متخصص في كيفية التعامل مع الأدلة الإلكترونية وتقييمها.

ورغم أهمية هذا النص في الاعتراف لأول مرة بالدليل الإلكتروني كوسيلة إثبات، إلا أن الحاجة تبقى ملحة لتطوير منظومة متكاملة تضمن فعالية تطبيق هذه المواد في الواقع القضائي.

ورغم أهمية هذا النص في الاعتراف لأول مرة بالدليل الإلكتروني كوسيلة إثبات، إلا أن صياغته العامة والغامضة لا ترقى إلى المستوى الذي يضمن فعالية تطبيقه في الواقع القضائي. فالنص لم يتضمن أي تفصيل يتعلق بالشروط أو المعايير التي يجب أن تتوفر في هذا الدليل لقبوله، كما لم يُحدد الجهات المخولة بجمعه وتحليله، ولا آليات ضمان سريته وسلامته من التلاعب أو التحريف.

أبرز جوانب القصور في النص التشريعي الفلسطيني

1. الغياب التام للتعريف التشريعي للدليل الإلكتروني، وهو ما يجعل القضاة عرضة للاجتهاد الشخصي في تحديد ماهية هذا النوع من الأدلة، مما يخلق تفاوتًا في الأحكام وتذبذبًا في المعايير القضائية.

2. عدم النص على شروط مشروعية جمع الدليل الإلكتروني، مثل ضرورة الحصول على إذن قضائي مسبق أو احترام الخصوصية الإلكترونية، وهو ما يعرّض هذا الدليل للطعن الدستوري في حال انتهاك الحقوق الأساسية للأفراد.
3. غياب سلسلة الحيازة الإلكترونية (Digital Chain of Custody)، وهي من الضوابط الفنية الأساسية لضمان عدم المساس بسلامة الدليل من لحظة جمعه وحتى تقديمه للمحكمة. كما أن القانون لم يُلزم الجهات الأمنية أو الفنية باستخدام أدوات موثوقة لحفظ أو فحص هذا الدليل.
4. عدم تحديد الجهة المخوّلة بجمع الأدلة الإلكترونية، مما يفتح المجال أمام تدخلات غير رسمية من أفراد أو جهات غير مختصة، قد تؤدي إلى إبطال الدليل بحجة عدم الالتزام بالإجراءات الصحيحة.

موقف القضاء الفلسطيني

تشير الدراسات التطبيقية والتقارير الحقوقية إلى أن التعامل القضائي مع الأدلة الإلكترونية في فلسطين لا يزال غير مستقر. ففي بعض القضايا تم قبول رسائل إلكترونية أو صور مُلتقطة من تطبيقات تواصل مثل "واتساب"، بشرط مصادقة المتهم عليها. وفي قضايا أخرى تم رفض الأدلة ذاتها لعدم وجود ما يُثبت يقينًا نسبتها إلى المتهم أو لحصول خلل في إجراءات جمعها، مثل عدم توثيق وقت ومكان استخراجها أو الجهة التي أجرت التحليل الفني.

وقد أشار "مركز الميزان لحقوق الإنسان" (2023) في أحد تقاريره إلى أن غياب معايير واضحة لجمع وتحليل الأدلة الإلكترونية أدى إلى إهدار حقوق عدد من المتهمين، بينما أشار "الهيئة المستقلة لحقوق الإنسان" (2022) إلى وجود ضعف في تدريب القضاة وأعضاء النيابة العامة في تقييم هذا النوع من الأدلة.

مقارنة مع النظم القانونية المقارنة

بالنظر إلى النظم القانونية العربية والدولية، نجد أنها قد سبقت فلسطين بخطوات متقدمة. ففي الإمارات العربية المتحدة، يتضمن القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات

نصوصًا تفصيلية حول الأدلة الإلكترونية، من بينها شروط جمعها، وتوثيقها، وتقديمها أمام المحكمة، إلى جانب ضرورة إرفاقها بتقارير فنية معتمدة من جهات رسمية. وفي الأردن، أصدرت النيابة العامة تعليمات خاصة عام 2021 تُحدد ضوابط جمع الأدلة الإلكترونية من الأجهزة الذكية، وتُلزم باستخدام أدوات معتمدة للحفاظ على الدليل.

أما على الصعيد الدولي، فتُعد اتفاقية بودابست بشأن الجرائم الإلكترونية لعام 2001 المرجع الأهم في هذا السياق، حيث وضعت مبادئ ومعايير واضحة، مثل: ضرورة ضمان "سلامة الدليل"، و"مصداقية الإجراءات"، و"احترام الخصوصية والحقوق الأساسية"، إلى جانب اعتماد تقنيات توثيق إلكترونية ذات موثوقية عالية.

يرى الباحث أن المشرّع الفلسطيني، رغم إدراكه لأهمية الدليل الإلكتروني، لا يزال يُعالج هذا الملف برؤية تشريعية تقليدية لا تتناسب مع التطور السريع في البيئة الإلكترونية. فالنصوص الحالية، وخاصة المادة (37) من قانون الجرائم الإلكترونية، تُعد خطوة إيجابية لكنها غير كافية على الإطلاق لتوفير الحماية القانونية الكاملة لهذا النوع من الأدلة.

فحجية الدليل الإلكتروني لا تتحقق بمجرد النص على قبوله، بل تتطلب منظومة متكاملة من القواعد الفنية والقضائية تضمن:

- جمعه بطريقة مشروعة تحترم الخصوصية وحقوق الدفاع،
- تحليله من قبل جهات متخصصة باستخدام أدوات تقنية موثوقة،
- تقديمه للمحكمة مدعومًا بتقارير فنية محايدة تؤكد سلامته ومصدره.

كما يؤكد الباحث على ضرورة إدماج هذا الموضوع ضمن برامج تدريب القضاة وأعضاء النيابة العامة، لضمان تكوين رؤية موحدة وعادلة حول كيفية تقييم الأدلة الإلكترونية دون تضييق أو تساهل مفرط.

وعليه، يوصي الباحث بأن يتم:

1. تعديل قانوني البينات والإجراءات الجزائية بما يُدرج تعريفًا دقيقًا للدليل الإلكتروني وشروطه.
2. استحداث لائحة تنفيذية تُنظم طرق جمع وتحليل وتقديم الأدلة الإلكترونية.
3. إنشاء وحدة إلكترونية متخصصة تابعة للنيابة العامة أو السلطة القضائية، تكون مخولة حصريًا بجمع وفحص الأدلة الإلكترونية.
4. إرساء اجتهاد قضائي فلسطيني واضح ومستقر يُشكل مرجعًا في قضايا الإثبات الإلكتروني، ويُحقق توازنًا بين مقتضيات العدالة وحماية الحقوق الأساسية للأفراد.

المطلب الثاني: شروط قبول الدليل الإلكتروني أمام القضاء

لقد أحدثت الطفرة الإلكترونية تحولًا جذريًا في أدوات الإثبات، حيث لم تعد الأدلة تقتصر على الوثائق الورقية أو الشهادات الشفهية، بل برزت "الأدلة الإلكترونية" كوسيلة إثبات حديثة فرضت حضورها في معظم القضايا ذات الطابع الإلكتروني. ومع ذلك، فإن هذه الأدلة لا تُقبل بشكل تلقائي أمام القضاء، بل تُخضع لرقابة قانونية دقيقة تتطلب استيفاء مجموعة من الشروط الشكلية والإجرائية التي تضمن مشروعيتها وتُرسخ عدالتها (Mason & Seng, 2017) (Mason & Seng, 2017).

إن قبول الدليل الإلكتروني لا يتوقف فقط على وجوده المادي أو قدرته على كشف الحقيقة، بل يشترط أن يكون قد جُمِع بطرق مشروعة، وحُفظ بطريقة موثوقة تضمن سلامته (Integrity)، وأن يكون قابلاً للمناقشة العلنية أمام الخصوم (Casey , 2022). وهذه الشروط ليست مسألة فنية محضة، بل تُجسد جوهر العدالة الإجرائية وتضمن التوازن بين متطلبات الأمن القانوني واحترام الحريات الفردية، كما يتضح من خلال مبدأ "سلسلة الحيازة" (Chain of Custody) الذي يهدف إلى توثيق كل خطوة يتعرض لها الدليل منذ لحظة التحفظ عليه وحتى تقديمه للمحكمة (Maras, 2021).

في النظام القانوني الفلسطيني، ورغم وجود بعض النصوص التي تُشير إلى استخدام الوسائل الإلكترونية في الإثبات، إلا أن التطبيق العملي يبرز تحديات كبيرة تتعلق بشرعية طرق جمع الأدلة الإلكترونية، والضمانات التي تحكم فحصها، ومقدار الثقة التي يمكن إسباغها عليها. وتُثير هذه التحديات تساؤلات مهمة حول مدى تأهيل النظام القضائي الفلسطيني للتعامل مع هذا النوع من الأدلة بما يضمن عدم المساس بحقوق الدفاع أو المساس بسلامة الإجراءات.

بناءً على ما تقدم، يتناول هذا المطلب الشروط القانونية لقبول الدليل الإلكتروني أمام القضاء، من خلال تقسيمه إلى فرعين رئيسيين:

- الفرع الأول: يُعالج الشروط الشكلية والموضوعية لقبول الدليل الإلكتروني، مثل شرط المشروعية، وشرط القابلية للمناقشة، وشرط الموثوقية.
- الفرع الثاني: يُركز على الشروط الإجرائية والضمانات القانونية التي ينبغي توافرها أثناء جمع وتحليل وتقديم الدليل الإلكتروني، لضمان احترام الأصول الدستورية ومبادئ المحاكمة العادلة.

الفرع الأول: الشروط الشكلية والموضوعية .

إن قبول الأدلة الإلكترونية أمام المحاكم لا يُبنى على وجودها التقني فقط، بل يتوقف على مدى استيفائها لشروط شكلية وموضوعية دقيقة تكفل عدالتها، وتمنع استخدامها كوسيلة مسيئة للإدانة دون ضمانات. وفي ظل الانتشار المتسارع للجرائم الإلكترونية، أضحت هذه الشروط ليست فقط مسألة قانونية، بل ضرورة واقعية تفرضها طبيعة البيئة الإلكترونية التي يسهل فيها التلاعب بالبيانات والعبث بالأدلة. (أحمد، 2020)

وتزداد أهمية هذه الشروط في النظام القضائي الفلسطيني، الذي لا يزال في طور بناء منظومة متخصصة للتعامل مع الجرائم الإلكترونية، ما يضع السلطة القضائية أمام مسؤولية مزدوجة: حماية المجتمع من الجريمة من جهة، وضمان حقوق المتهمين من جهة أخرى. فالدليل الإلكتروني لا يُقبل في ذاته، بل يُقبل بقدر ما يُثبت أنه جُمع بطريقة مشروعة، وأنه قابل للنقاش العلني، وذو موثوقية يقينية.

وعليه، يتناول هذا الفرع من البحث الشروط الشكلية والموضوعية لقبول الدليل الإلكتروني، من خلال تحليل شرط المشروعية في جمعه، وشرط القابلية للمناقشة أمام المحكمة، وذلك بالاستناد إلى نصوص القوانين الفلسطينية المعمول بها، والتجارب القضائية ذات الصلة، مدعومة برؤية الباحث حول مدى نجاعة هذه الشروط في ضمان العدالة الإلكترونية.

أولًا: شرط المشروعية في جمع الدليل الإلكتروني

إن شرط المشروعية في جمع الدليل الإلكتروني يُعد من المبادئ الدستورية والقانونية الأساسية التي يجب احترامها عند التعامل مع البيانات الإلكترونية، خاصة في ظل ما تفرضه الأدلة الإلكترونية من خصوصية وتعقيد تقني. فمشروعية الدليل لا تتعلق فقط بنتيجته أو قيمته الإثباتية، بل بكيفية الحصول عليه والإجراءات المصاحبة لذلك. أي خلل في هذه الإجراءات قد يُفضي إلى بطلان الدليل وعدم قبوله أمام المحكمة، وفقًا لمبدأ "الغاية لا تبرر الوسيلة" في الإجراءات الجزائية.

في السياق الفلسطيني، يؤسس قانون الإجراءات الجزائية رقم (3) لسنة 2001 للمبدأ العام لحرمة الخصوصية، حيث تنص المادة (47) منه على عدم جواز تفتيش أي "مكان" إلا بعد الحصول على إذن من الجهة القضائية المختصة. ورغم أن هذا النص صيغ في الأصل للأماكن المادية، فإن الفقه والقضاء قد وسّعا تفسيره ليشمل "الأماكن الافتراضية" مثل الحواسيب والهواتف المحمولة باعتبارها مستودعًا للخصوصية (المصري، 2018).

وقد جاء قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية ليضع إطارًا إجرائيًا خاصًا ومفصلاً لهذه العملية. ففي المادة (12) منه، منح المشرّع مأموري الضبط القضائي صلاحية "ضبط وتفتيش الأجهزة والأدوات والوسائط والنظم المعلوماتية"، ولكنه اشترط أن يتم ذلك "بأمر قضائي مسبب". هذا النص الخاص يؤكد ويُفصّل المبدأ العام الوارد في قانون الإجراءات الجزائية، ويقطع أي شك حول ضرورة الحصول على

إذن قضائي مسبق ومسبب قبل النفاذ إلى أي محتوى إلكتروني، سواء كان على الحواسيب، الهواتف، الخوادم، أو أي وسائط تخزين أخرى.

أما على صعيد قانون الجرائم الإلكترونية رقم (10) لسنة 2018، فقد أولى المشرّع أهمية بالغة لحماية الخصوصية، وقيّد صلاحيات جمع الأدلة الإلكترونية، حيث نصّت المادة (37) منه على أنه: "لا يجوز استخدام أو الاستناد إلى أية وسيلة إلكترونية تم جمعها أو الحصول عليها بطريقة غير مشروعة في الإثبات أمام المحاكم". هذا يعني أن أي وسيلة تقنية استُخدمت دون سند قانوني أو دون مراعاة الإجراءات الإجرائية الواجبة تُعتبر باطلة من الناحية القانونية، حتى وإن كانت تحتوي على معلومات حاسمة في القضية.

بالإضافة إلى ذلك، فإن مبادئ "سلسلة الحيازة القانونية" (Chain of Custody) تكتسب أهمية خاصة في هذا السياق. فهي تضمن أن البيانات الإلكترونية لم تتعرض لأي تعديل أو حذف أو تلاعب خلال مرحلة الجمع والنقل والتخزين. عدم وجود وثائق واضحة تُثبت هذه السلسلة قد يُعرض الدليل الإلكتروني للطعن أمام المحكمة.

كما تؤكد التوصيات الدولية الحديثة، مثل تلك الصادرة عن الهيئة الأوروبية لحماية البيانات (EDPB)، على ضرورة أن يتم جمع الأدلة الإلكترونية بطريقة قانونية متوافقة مع التشريعات الوطنية، وبما يضمن احترام الحقوق الأساسية للأفراد، خصوصًا الحق في الخصوصية والمحاكمة العادلة. وتشير هذه التوصيات إلى أن الأدلة الإلكترونية، رغم قيمتها الكبيرة في الإثبات، لا يمكن قبولها قضائيًا إذا تم الحصول عليها من خلال انتهاك لحرمة البيانات أو دون إذن قضائي واضح (EDPB, 2023).

ثانيًا: شرط القابلية للمناقشة أمام المحكمة

يُعد شرط القابلية للمناقشة أحد أعمدة العدالة الإجرائية، حيث يُعزز من مبدأ المواجهة بين الخصوم ويكفل التوازن في العملية القضائية. وهو شرط مرتبط ارتباطًا عضويًا بمبدأ الشفوية والعلنية، ويهدف إلى منح

أطراف الخصومة، وعلى وجه التحديد المتهم، الحق الكامل في تفنيد الأدلة المقدمة ضده، خصوصًا تلك التي تعتمد على التكنولوجيا الإلكترونية وطرق التحليل الفني.

في سياق الدليل الإلكتروني، تتسم عملية المناقشة بصعوبة إضافية نظرًا لطبيعة هذه الأدلة، التي تعتمد على أدوات معقدة وتقنيات متطورة في الجمع والتحليل والتخزين. وهنا، لا يمكن للقاضي أن يكوّن قناعته على أساس تقرير مكتوب دون أن يكون ذلك التقرير موضوعًا للنقاش والتفنيد أمام المحكمة، لا سيّما إذا كان يتضمن مصطلحات تقنية أو تحليلات تعتمد على البرمجيات الإلكترونية أو سجلات إلكترونية يصعب تفسيرها لغير المتخصصين.

ينص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 على مبدأ الشفوية، والذي يوجب أن تكون المرافعات علنية وشخصية، ما لم يقرر القانون غير ذلك. وبناءً عليه، فإن تقديم الدليل الإلكتروني—سواء كان تقريرًا فنيًا أو تحليلًا إلكترونيًا—لا يكون كافيًا لاعتباره مقبولًا قضائيًا، بل لا بد من إتاحته للمناقشة داخل قاعة المحكمة، والسماح للمتهم أو محاميه بطرح أسئلة مباشرة على الجهة التي أعدته، سواء كانت جهة فنية تابعة للنيابة أو خبيرًا مستقلًا. فالمناقشة الشفوية تسهم في كشف مواطن القصور في الدليل وتفتح المجال للطعن في طريقة التحليل أو ظروف جمع البيانات.

وقد شدد قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية على أهمية توثيق الدليل الإلكتروني وضرورة مراعاة الإجراءات القانونية عند جمعه وتحليله. غير أن هذا النص، وكما يلاحظ العديد من شُرّاح القانون، قد ركز على مرحلة التحقيق وجمع الأدلة دون أن يضع آليات إجرائية واضحة لكيفية مناقشة هذه الأدلة أمام المحكمة في مرحلة المحاكمة (المصري، 2018). هذا "السكوت التشريعي" يفتح الباب أمام السلطة التقديرية الواسعة للقاضي في إدارة جلسات مناقشة الخبراء، مما قد يؤدي إلى تفاوت في تطبيق مبدأ "القابلية للنقاش" من محكمة لأخرى، تبعًا لمدى استيعاب الهيئة القضائية للجانب الفني المعقد المرتبط بالدليل الإلكتروني.

وتكمن المشكلة الجوهرية هنا في الفجوة القائمة بين التخصص القانوني والتخصص الفني. فكثير من القضاة وأعضاء النيابة لا يمتلكون خلفية تقنية كافية لفهم تفصيلات التقارير الإلكترونية، الأمر الذي يضعهم في موقف يعتمد فيه القاضي على رأي الخبير دون أن يتمكن من تفكيك المنهجية المستخدمة أو تقييم صحتها بشكل مستقل. وقد أشار تقرير صادر عن الهيئة المستقلة لحقوق الإنسان في فلسطين (2021) إلى ضرورة إدماج برامج تدريب للقضاة حول أدوات تحليل الأدلة الإلكترونية، وتوفير قاعدة بيانات مرجعية تقنية تسهل عليهم فهم وتحليل محتوى التقارير الفنية.

أما على الصعيد الدولي، فقد أكدت التوصيات الصادرة عن مؤتمر الاتحاد الأوروبي للعدالة الإلكترونية (European e-Justice Conference, 2024) على ضرورة إتاحة الفرصة الكاملة لأطراف النزاع لمناقشة أصل ومحتوى وتحليل الأدلة الإلكترونية، مع التأكيد على حق الدفاع في استدعاء خبراء مضادين، بما يحقق مبدأ تكافؤ الفرص وضمانات المحاكمة العادلة في القضايا التقنية المعقدة (European e-Justice Report, 2024).

في ضوء ما سبق، فإن شرط القابلية للمناقشة لا يُعد إجراءً شكليًا، بل هو صمام أمان يضمن العدالة. وبدونه، يُخشى أن تتحوّل الأدلة الإلكترونية إلى أدوات إدانة جاهزة غير قابلة للطعن، وهو ما يتعارض مع جوهر المحاكمة العادلة التي يجب أن تستند إلى الإقناع لا إلى التسليم.

من خلال استعراض وتحليل شرطَي المشروعية والقابلية للمناقشة، يتبيّن أن النظام القانوني الفلسطيني لا يزال في مرحلة التأسيس التشريعي والتقني الفعلي للتعامل مع الأدلة الإلكترونية، رغم ما يظهر من توجهات قضائية جزئية تحاول التكيّف مع معطيات العصر الإلكتروني. ويُسجّل للمنظومة القانونية الفلسطينية بعض الخطوات الإيجابية، مثل النص الصريح على بطلان الأدلة المتحصلة من إجراءات غير مشروعة في المادة (218). من قانون الإجراءات الجزائية رقم (3) لسنة 2001، وتأكيد مبدأ الشفوية والمواجهة في المحاكمات

إلا أن التطبيق العملي لهذه المبادئ لا يزال يواجه تحديات جوهرية، أبرزها غياب آليات إجرائية واضحة في قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية تنظم كيفية مناقشة الدليل الإلكتروني في مرحلة المحاكمة (المصري، 2018). يضاف إلى ذلك، ضعف البنية التحتية التقنية وغياب الخبرة المتخصصة الكافية في تحليل هذا النوع من الأدلة، وهي فجوة حذرت من تداعياتها تقارير حقوقية، وأوصت بضرورة بناء قدرات الفاعلين في قطاع العدالة لضمان المحاكمة العادلة في البيئة الإلكترونية (الهيئة المستقلة لحقوق الإنسان، 2021).

ويرى الباحث أن شرط المشروعية، رغم وجود نصوص قانونية تدعمه، لا يطبّق بشكل صارم في الواقع، ما يهدد بمخاطر انتهاك الخصوصية الفردية وتقويض ثقة المتقاضين في العدالة الجنائية. كما يلاحظ أن شرط القابلية للمناقشة، وإن كان منصوصًا عليه ضمنيًا من خلال مبدأ الشفوية، إلا أنه يواجه تحديات كبيرة بسبب الفجوة المعرفية بين القاضي أو المحامي، والمضمون الفني للتقارير الإلكترونية، مما قد يؤدي إلى قبول أدلة دون التحقق الكافي من صحتها أو سلامة منهج تحليلها.

وعليه، يوصي الباحث بضرورة إصدار لوائح تفصيلية تُحدّد إجراءات جمع الأدلة الإلكترونية وضوابط مناقشتها، مع إنشاء هيئة فنية مستقلة مختصة بتحليل هذا النوع من الأدلة، تكون مرجعًا تقنيًا للنيابة والقضاء. كما يشدد على ضرورة دمج التدريب التكنولوجي للقضاة وأعضاء النيابة ضمن برامج التأهيل المهني، حتى تتسع قدرتهم على تقييم الدليل الإلكتروني من الناحيتين القانونية والفنية، بما يعزز من عدالة الإجراءات وثقة المجتمع في القضاء.

الفرع الثاني: الشروط الإجرائية والضمانات القانونية .

يمثّل الدليل الإلكتروني تحديًا فنيًا وقانونيًا خاصًا في بيئة الإثبات الجنائي، نظرًا لما يتمتع به من طبيعة تقنية قابلة للنسخ والتعديل والتزوير دون أثر مادي ظاهر. ولذلك، فإن سلامة هذا النوع من الأدلة لا تتوقف على توفره فحسب، بل ترتبط ارتباطًا وثيقًا بشروط إجرائية وضمانات فنية تضمن موثوقيته وقابليته للاستخدام

القانوني أمام القضاء. وتتعلق هذه الشروط بعدة أبعاد، أبرزها: توثيق المصدر الإلكتروني، الحفاظ على سلسلة الحيازة، استخدام أدوات تحليل موثوقة، والتحقق من عدم التلاعب، وهي عناصر تُسهم مجتمعة في ضمان أن ما يُعرض أمام المحكمة يُمثل الحقيقة التقنية دون تشويه أو انحراف.

أهمية التوثيق الفني للمصدر الإلكتروني

يتطلب شرط الموثوقية أن يكون مصدر الدليل الإلكتروني معلومًا وواضحًا، وأن تكون هناك قدرة فنية على إثبات أن هذا الدليل قد تم الحصول عليه من ذلك المصدر بالتحديد، دون تدخل بشري أو تقني يمكن أن يؤثر في محتواه. وتُعد بيانات التعريف (Metadata) المرتبطة بالملف الإلكتروني، مثل نوع الجهاز، نظام التشغيل، صاحب الحساب، موقع التخزين، والتوقيتات الزمنية، من أهم الأدوات التي تُمكن الخبراء من بناء "بصمة إلكترونية" متكاملة للدليل. وتؤكد منظمة ENISA الأوروبية للأمن السيبراني (ENISA, 2020) أن التحقق من المصدر هو الخطوة الأولى في عملية الفحص الجنائي الإلكتروني لضمان سلامة السلسلة الثبوتية.

الحفاظ على سلسلة الحيازة

سلسلة الحيازة هي وثيقة قانونية وتقنية ترافق الدليل الإلكتروني منذ لحظة اكتشافه وحتى تقديمه للمحكمة، وتحتوي على بيانات كل شخص تعامل مع الدليل، ومتى وأين، وتحت أي ظروف. أي خلل في هذه السلسلة، مثل عدم التوقيع من قبل أحد الأشخاص، أو وجود فترة غير موثقة، قد يُفقد الدليل مصداقيته. وتُعد هذه السلسلة من أهم المعايير المعتمدة دوليًا، حيث تنص المادة 3 من المبادئ التوجيهية لاتفاقية بودابست لمكافحة الجريمة الإلكترونية (Council of Europe, 2001) على أن انتهاك سلسلة الحيازة يمكن أن يؤدي إلى استبعاد الدليل بالكامل.

استخدام بصمة البيانات

تُستخدم خوارزميات التحقق من صحة البيانات مثل MD5، SHA-1، SHA-256 لضمان أن الدليل لم يتعرض لأي تعديل بعد جمعه. وتقوم هذه الخوارزميات بإنتاج رمز إلكتروني فريد يُمثل محتوى الملف، ويُستخدم لاحقًا لمقارنته بنسخ أخرى من الملف. في حال تطابقت الرموز، يعني ذلك أن الملف لم يتم تغييره إطلاقًا. ويُعتبر ذلك أحد الأدلة القاطعة التي تلعب دورًا جوهريًا في تعزيز شرط الموثوقية.

الاعتماد على أدوات تحليل موثوق

يشترط أن يتم استخدام أدوات فنية معترف بها ومعتمدة دوليًا في عمليات الفحص والتحليل، مثل: EnCase، FTK، X-Ways، Autopsy وغيرها. كما أن استخدام أدوات مفتوحة المصدر مع توثيق جميع خطوات التحليل يعزز الشفافية، ويساعد في ضمان إمكانية إعادة فحص الأدلة بنفس الطريقة من قبل جهة قضائية أو خبيرة محايدة.

التقييم المستقل للأدلة

تشير معظم النظم القضائية الحديثة إلى أهمية وجود جهة مستقلة أو خبير محايد يقوم بإعادة فحص الأدلة الإلكترونية المقدمة أمام المحكمة، خصوصًا في القضايا المعقدة. وقد أوصى بذلك تقرير "العدالة الإلكترونية في الدول النامية" الصادر عن جامعة أكسفورد (Oxford, 2021)، مؤكدًا أن الفحص المستقل يضمن تعزيز الثقة العامة في الأحكام القضائية المرتبطة بالجرائم الإلكترونية.

إرفاق تقارير تفصيلية

من الشروط الأساسية لقبول الدليل الإلكتروني أن يُرفق بتقرير فني مفصل يشرح الخطوات التي تم اتباعها، نوع الأجهزة والبرامج المستخدمة، وإثبات عدم التلاعب بالبيانات. ويُفضل أن يحتوي التقرير على صور إلكترونية (Screenshots) ، وتوثيق زمني، ونماذج تحقق (مثل بيانات الهاش والتواقيت).

يرى الباحث أن شرط المشروعية في جمع الأدلة الإلكترونية ما زال يواجه تحديات كبيرة في الواقع الفلسطيني، رغم وضوح النصوص القانونية الناظمة، وذلك بسبب غياب الضوابط التقنية الدقيقة، وضعف التأهيل العملي لدى مأموري الضبط. هذا الخلل قد يؤدي إلى انتهاك الخصوصية، ما يهدد سلامة الدليل ويفقده قيمته الإثباتية. كما يُلاحظ الباحث فجوة واضحة بين طبيعة الأدلة الإلكترونية وقدرة القضاة على مناقشتها بفعالية، مما يفرض الحاجة إلى تدريب متخصص يعزز من كفاءة السلطة القضائية. ويؤكد في النهاية أن ضمان اليقين والموثوقية في هذا النوع من الأدلة يتطلب تأسيس جهة وطنية مستقلة، فنية وقانونية، تتولى فحص الأدلة الإلكترونية وفق معايير صارمة وتحت إشراف قضائي مباشر، بما يحمي العدالة ويعزز الثقة العامة في الأحكام الصادرة.

المبحث الثاني : الجهات المختصة بجمع وتحليل الدليل الإلكتروني

في ظل التحولات العميقة التي فرضتها الثورة الإلكترونية على مختلف مجالات الحياة، لم تكن الساحة الجنائية بمعزل عن هذا التغيير؛ إذ أصبحت الجرائم الإلكترونية تمثّل أحد أبرز التحديات التي تواجه السلطات القضائية والأمنية على حدّ سواء. وتزداد هذه التحديات تعقيدًا مع التطور المستمر في أدوات الجريمة السيبرانية، التي لم تعد تتطلب وجودًا ماديًا للمجرم في مسرح الجريمة، بل بات بالإمكان ارتكابها عن بعد، باستخدام وسائل اتصال إلكترونية متطورة يصعب تتبعها دون أدوات فنية وتشريعية دقيقة.

ومن هذا المنطلق، تبرز أهمية وجود جهات مختصة ومؤهلة فنيًا وقانونيًا لتولي مسؤولية جمع وتحليل الأدلة الإلكترونية، باعتبارها الخطوة الأولى نحو ضمان عدالة جنائية إلكترونية، تقوم على احترام المعايير القانونية والمهنية المعتمدة دوليًا. فقبول الأدلة الإلكترونية أمام المحاكم لا يتوقف فقط على مشروعية جمعها، بل يتطلب أيضًا التأكد من موثوقيتها الفنية، وسلامة تسلسلها الإجرائي، وتكامل المؤسسات المسؤولة عن إدارتها.

وفي السياق الفلسطيني، يُلاحظ أن البنية المؤسسية القائمة على التعامل مع الأدلة الإلكترونية لا تزال في طور التكوين، حيث تتوزع المهام بين عدة جهات رسمية، أبرزها النيابة العامة ووحدة الجرائم الإلكترونية في الشرطة، إلى جانب التعاون مع جهات أمنية وفنية أخرى. إلا أن هذا التعدد في الاختصاص قد يُفضي إلى غياب التنسيق المؤسسي، وظهور ثغرات إجرائية قد تمسّ بحجية الدليل الإلكتروني، أو تفتح الباب للطعن فيه أمام القضاء.

وانطلاقًا من هذا الواقع، يأتي هذا المبحث ليتناول بشكل دقيق طبيعة الجهات المختصة بجمع وتحليل الدليل الإلكتروني في فلسطين، من خلال التركيز على ثلاثة محاور رئيسية:

- في الفرع الأول، يتم تسليط الضوء على التحديات الإدارية والتقنية التي تواجه النيابة العامة عند التعامل مع الجرائم الإلكترونية، خاصة فيما يتعلق بإصدار الأوامر وتنفيذ إجراءات التفتيش والتحليل الفني.

- أما الفرع الثاني، فيتناول بالدراسة والتحليل الدور الفني المتخصص لوحدة الجرائم الإلكترونية، ومدى جاهزيتها من حيث الكوادر والبنية التحتية لمواكبة تعقيدات الدليل الإلكتروني.

وأخيرًا، يستعرض الفرع الثالث أهمية التنسيق المؤسسي بين الجهات الأمنية والقضائية، وضرورة بناء آليات تعاون فعّالة تضمن التكامل في جمع الأدلة وتحليلها وتقديمها وفقًا للمعايير القانونية والإجرائية السليمة.

الفرع الأول : التحديات الإدارية والتقنية أمام النيابة العامة في التعامل مع الجرائم الإلكترونية

مع ازدياد الاعتماد على الوسائل الإلكترونية في مختلف مجالات الحياة، برزت الجرائم الإلكترونية كواحدة من أكثر الجرائم تعقيدًا وخطورة في البيئة الفلسطينية. لم تعد الجرائم محصورة في السرقة التقليدية أو الاعتداءات المادية، بل أصبحت تنطوي على اختراق للخصوصيات، وتلاعب بالبيانات، وابتزاز إلكتروني، وهجمات على البنية التحتية للمعلومات، ما استوجب وجود أدوات قانونية وإدارية وتقنية قادرة على التصدي لهذه الظواهر الجديدة. وقد حاول المشرّع الفلسطيني مواكبة هذه التغيرات من خلال إصدار قانون الجرائم الإلكترونية رقم (10) لسنة 2018، والذي منح النيابة العامة صلاحيات موسعة في مجال التحقيق والتفتيش والرقابة الإلكترونية، إدراكًا لدورها المركزي في حماية الفضاء الإلكتروني وضمان سيادة القانون داخله.

وتشير التقارير المحلية، مثل تقرير الهيئة المستقلة لحقوق الإنسان (2022)، إلى وجود فجوة ملموسة بين النصوص القانونية والقدرة الفعلية على إنفاذها، خاصة في ظل نقص الكوادر المؤهلة، وغياب التجهيزات الفنية، وافتقار النظام القضائي إلى آليات متخصصة في إدارة الأدلة الإلكترونية. كما تؤكد دراسة عبد الحكيم التميمي (2022) أن النيابة العامة غالبًا ما تواجه صعوبات في تكييف الوقائع التقنية ضمن أطر قانونية واضحة، نتيجة غياب الخبرة التقنية المتخصصة أو ضعف التعاون مع الجهات ذات العلاقة.

أضف إلى ذلك، أن بعض القضايا الإلكترونية تتطلب تدخلًا سريعًا وفوريًا للحفاظ على الأدلة (مثل تتبع عنوان IP أو استخراج بيانات محذوفة)، وهو ما لا يتوافر دومًا بسبب الإجراءات البيروقراطية أو محدودية

الإمكانيات اللوجستية. وقد ينتج عن ذلك ضياع الأدلة، أو الطعن في مشروعيتها لاحقًا أمام القضاء، مما يؤثر سلبًا على مصداقية التحقيقات ويُضعف من ردع الجرائم الإلكترونية.

ولا يقتصر الأمر على الجوانب التقنية والإدارية فقط، بل هناك أيضًا إشكاليات تشريعية متعلقة بعدم وضوح بعض المواد القانونية أو غياب مواد تنظم مراحل جمع وتحليل الأدلة الإلكترونية بشكل تفصيلي، مما يفتح الباب أمام التقديرات الاجتهادية ويؤدي إلى تباين الأحكام القضائية. وقد رُصدت حالات – وفقًا لدراسة عز الدين أبو رمضان (2021) – تم فيها إسقاط أدلة مهمة في قضايا حساسة، فقط بسبب عيوب شكلية في إجراءات الحجز الإلكتروني أو غياب الإذن القضائي المسبق.

من هنا، تبرز الحاجة المُلحّة إلى تطوير بنية مؤسسية متخصصة داخل النيابة العامة، تُعنى حصريًا بقضايا الجرائم الإلكترونية، وتكون مدعومة بكوادر فنية وقانونية قادرة على التصدي لتحديات العصر الإلكتروني، مع وجود شراكات دائمة مع الجهات الأمنية والتقنية ومراكز التدريب. فبدون هذا التطوير، تبقى النيابة العامة عرضة للعجز الإجرائي، وتظل حقوق الضحايا ومبادئ العدالة في خطر مستمر.

أولًا: التحديات الإدارية

رغم التقدم القانوني الذي شهده النظام الفلسطيني بإقرار قانون الجرائم الإلكترونية رقم (10) لسنة 2018، إلا أن النيابة العامة لا تزال تواجه العديد من التحديات الإدارية التي تُضعف من قدرتها على التصدي الفعّال لهذا النوع من الجرائم، خصوصًا في ظل تسارع تطور تقنيات الجريمة الإلكترونية واتساع رقعتها. ويمكن تلخيص أبرز هذه التحديات في الآتي:

1. نقص الكوادر المتخصصة

تعاني النيابة العامة من نقص حاد في عدد وكلاء النيابة الذين يمتلكون خلفية تقنية أو تدريبًا متخصصًا في التعامل مع الجرائم الإلكترونية. فغالبًا ما يتم التعامل مع هذه القضايا كامتداد للقضايا التقليدية، مما يؤدي إلى أخطاء في التكييف القانوني أو ضعف في قراءة وتحليل طبيعة الجريمة الإلكترونية. ويرتبط هذا النقص

بعدة أسباب، منها: غياب برامج التدريب المنتظم، وقلة ورش العمل المتخصصة، وغياب الحوافز المهنية لتوجيه وكلاء النيابة نحو هذا المجال. وقد لوحظ أن بعض القضايا تم تأجيلها أو إسقاط أدلتها بسبب العجز عن تحليل الدليل الإلكتروني بطريقة دقيقة أو قانونية (التميمي، 2022).

2. البيروقراطية الإدارية وتعقيد الإجراءات

تُعد الإجراءات البيروقراطية أحد أبرز العراقيل التي تواجه النيابة العامة في تحقيق استجابة فورية للجريمة الإلكترونية. فمثلاً، يتطلب إصدار إذن تفتيش إلكتروني أو قرار بالحجز على بيانات في "وقت حرج" سلسلة طويلة من التواقيع والمراسلات، ما يُؤخّر الإجراء لساعات أو حتى أيام. وهذا يُفقد الأدلة الإلكترونية الكثير من قيمتها، خاصة أن المحتوى الإلكتروني يمكن أن يُعدّل أو يُمحى في ثوانٍ. كما أن البيئة الإدارية داخل النيابة العامة لا تزال تعتمد على أنماط تقليدية من المتابعة الورقية والتوثيق، ما يتعارض مع الطابع الفوري والمتغير للفضاء الإلكتروني (جبر، 2021).

3. غياب وحدة مركزية متخصصة

من بين الإشكاليات الإدارية الكبرى، أن النيابة العامة لا تمتلك وحدة مركزية موحدة تعالج الجرائم الإلكترونية على مستوى وطني. وبدلاً من ذلك، يُكلف وكلاء النيابة بمعالجة هذه الملفات دون وجود هيكل تنظيمي واضح، مما يؤدي إلى تباين في الأداء، وضعف في التوثيق، وتكرار الأخطاء. وقد نادت العديد من التقارير المحلية بضرورة إنشاء "نيابة إلكترونية" تختص بهذا المجال وتعمل بالتنسيق مع الوحدات الفنية والأمنية. ففي الأردن مثلًا، تم إنشاء وحدة "الجرائم الإلكترونية" تحت مظلة وزارة العدل، والتي تتابع الجرائم الإلكترونية بكفاءة بسبب هيكلها المستقل والدعم التقني المرافق لها.

4. نقص الموارد اللوجستية والتقنية

لا تملك النيابة العامة في فلسطين بنية تحتية إلكترونية متكاملة تُمكّنها من التعامل مع التحقيقات الإلكترونية بالشكل المطلوب. فمعظم الفروع تفتقر إلى برامج تحليل إلكترونية متقدمة، أو أنظمة إدارة أدلة إلكترونية

مؤمنة، أو حتى أجهزة تخزين احترافية تحفظ البيانات الحساسة من التلف أو التلاعب. وغالبًا ما تلجأ النيابة إلى الاستعانة بخبراء خارجيين أو جهات أمنية، ما قد يُضعف استقلالية التحقيق ويُثير إشكالات قانونية بشأن سرية البيانات وخصوصيتها. وقد أشار بعض القضاة إلى أن غياب أدوات التحقق الإلكتروني داخل النيابة يؤدي إلى التشكيك في موثوقية بعض الأدلة أمام المحاكم.

5. عدم تحديث الأدلة الإجرائية القانونية

تعمل النيابة العامة حتى اليوم بناءً على أدلة إجرائية تقليدية لا تأخذ في الحسبان الخصوصية الفنية لجمع وتحليل الأدلة الإلكترونية. فلا توجد بروتوكولات موحدة أو تعليمات تنفيذية واضحة تشرح مثلًا كيفية التعامل مع "البيانات المشفّرة"، أو كيفية التفريغ القانوني لمحادثات الواتساب، أو تتبع البريد الإلكتروني بشكل قانوني. وغالبًا ما يُترك لوكيل النيابة "الاجتهاد" في تنفيذ الإجراءات، أو الاعتماد على رأي فني خارجي، ما يؤدي إلى تفاوت في النتائج، وضعف في حجية الدليل أمام المحكمة.

ثانيا : التحديات التشريعية في اختصاص النيابة العامة بالجرائم الإلكترونية

رغم صدور قانون الجرائم الإلكترونية الفلسطيني رقم (10) لسنة 2018، بهدف مواكبة التحولات الإلكترونية وتوفير إطار قانوني للتعامل مع الجريمة الإلكترونية، إلا أن التطبيق العملي لهذا القانون يكشف عن فجوات تشريعية وإجرائية تعيق عمل النيابة العامة وتحدّ من فاعلية دورها في التحقيق والملاحقة. وتتجلى هذه التحديات في عدة أوجه:

1. ضعف الإطار المفاهيمي للقانون وغياب المصطلحات الدقيقة

شكل غياب نصوص إجرائية متخصصة في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 تحديًا هيكليًا أمام منظومة العدالة الجنائية في تعاملها مع الأدلة الإلكترونية. فهذا القانون، الذي وُضعت قواعده للتعامل مع الأدلة المادية الملموسة، لم يستوعب الطبيعة اللامادية والمتغيرة للدليل الإلكتروني، مما أدى إلى فراغ تشريعي واضح في آليات جمع البيانات الإلكترونية، وأساليب الحفاظ على سلامتها من

التلاعب، ومعايير عرضها كأدلة مقبولة أمام القضاء. ولفترة طويلة، اضطرت النيابة العامة وجهات إنفاذ القانون إلى اللجوء للقياس على القواعد التقليدية للتفتيش والضبط، وهو ما كان يثير إشكاليات قانونية وعملية حول مشروعية الدليل وحجيته في الإثبات.

إلا أن هذا المشهد التشريعي قد شهد تحولاً نوعيًا مع صدور القرار بقانون رقم (17) لسنة 2024 بشأن المعاملات الإلكترونية وخدمات الثقة. فعلى الرغم من أن هذا القانون لا يندرج ضمن إطار التشريعات الإجرائية الجزائية بشكل مباشر، إلا أنه أرسى بنية تحتية قانونية لا غنى عنها، وبدأ في ردم الهوة الإجرائية القائمة. فمن خلال منحه الحجية الكاملة للكتابة الإلكترونية، والسجلات الإلكترونية، والتوقيع الإلكتروني الموثوق، لم يعد الدليل الإلكتروني مجرد "قرينة" تخضع للسلطة التقديرية المطلقة للقاضي، بل أصبح دليلاً له كيانه القانوني المستقل، متى ما استوفى الشروط الفنية الواردة في القانون.

وبذلك، أصبح بإمكان النيابة العامة اليوم الاستناد إلى هذا الإطار القانوني الجديد لتأسيس حجية الأدلة التي تجمعها، حيث يوفر القانون معايير واضحة لتوثيق سلامة الدليل وعدم العبث به عبر خدمات الثقة المعتمدة. ومع ذلك، ورغم هذه الخطوة المحورية، تبقى الحاجة ماسة لاستكمال البناء التشريعي من خلال تعديل قانون الإجراءات الجزائية نفسه، لتضمينه فصلاً متخصصًا يوضح بالتفصيل إجراءات التفتيش والضبط الجنائي الإلكتروني، وضمانات المتهم أثناء تفتيش أجهزته، وآليات التعاون الدولي لجمع الأدلة العابرة للحدود، بما يحقق التوازن الدقيق بين فعالية التحقيق وحماية الحقوق والحريات في الفضاء الإلكتروني.

وهذا ما يُخالف ما نصّت عليه الأدلة الإرشادية الدولية مثل: "دليل الأدلة الإلكترونية" الصادر عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، 2020.

2. قصور في تنظيم العلاقة بين النيابة ووحدات الجرائم الإلكترونية

رغم أن التحقيق في الجرائم الإلكترونية يتطلب تعاونًا وثيقًا بين النيابة العامة والجهات الفنية المختصة، إلا أن القانون الفلسطيني لا ينص صراحةً على طبيعة العلاقة الإدارية والقانونية بين الطرفين، مما يؤدي إلى:

- غياب التنسيق عند طلب الأدلة الفنية أو الاستعانة بالخبراء.
- تباين في جودة التقارير الفنية المقدمة للقضاء.
- صعوبة تحديد المسؤولية في حال حدوث خلل في إجراءات التحليل الإلكتروني.

في المقابل، تشير التجربة الأردنية إلى وجود "وحدة متخصصة" في الجرائم الإلكترونية ضمن وزارة العدل، وتُدار عبر بروتوكولات قانونية واضحة بين الجهات.

3. فجوة في مستوى العقوبات مقارنة بخطورة الأفعال

يلاحظ أن بعض الجرائم الإلكترونية المنصوص عليها في القانون الفلسطيني لا تزال تُعامل بعقوبات بسيطة نسبيًا مثل الغرامات أو الحبس القصير، رغم خطورتها، ومنها:

- جرائم الابتزاز الإلكتروني.
- اختراق الحسابات الطبية والشخصية.
- نشر صور وبيانات خاصة دون إذن.

4. غياب تنظيم تشريعي لسلسلة الحيازة الإلكترونية (Chain of Custody)

من أبرز التحديات التي تواجه النيابة هو انعدام وجود نص قانوني ينظم خطوات الحفاظ على الدليل الإلكتروني منذ لحظة ضبطه وحتى تقديمه للمحكمة. ويترتب على غياب هذا المفهوم التشريعي:

- ضعف إمكانية إثبات أصالة الدليل.
- الطعن المتكرر في نزاهة الأدلة المقدمة.
- إمكانية فقدان البيانات الحساسة نتيجة سوء التخزين أو النقل.

هذا ما يؤكده أيضًا تقرير "مجلس القضاء الأعلى الفلسطيني – 2021"، والذي دعا إلى إنشاء بروتوكول رسمي لحفظ الأدلة الإلكترونية. (مجلس القضاء الأعلى الفلسطيني، 2001) الحاجة لتشريع خاص ينظم خصوصية المستخدمين وحقوقهم الإلكترونية حتى الآن، لا يوجد في فلسطين قانون لحماية البيانات الشخصية

أو الخصوصية الإلكترونية، وهو ما يضع النيابة العامة في مأزق أخلاقي وقانوني عند التعامل مع بيانات الأفراد. فمن غير الواضح مثلًا:

- متى يمكن تفريغ محادثات شخصية؟
- هل يمكن مراقبة حسابات التواصل الاجتماعي دون إخطار المستخدم؟
- ما هي الحدود المشروعة للتدخل في الفضاء الإلكتروني الشخصي؟

في المقابل، اعتمدت تونس في 2018 "قانون حماية البيانات الشخصية"، الذي حدد بوضوح حدود تدخل الدولة في بيانات المواطنين الإلكترونية.

يرى الباحث أن النيابة العامة تمثل حجر الزاوية في ضبط مشروعية الإجراءات الخاصة بالجرائم الإلكترونية، غير أن هذه الصلاحيات الواسعة التي يمنحها القانون للنيابة العامة لا تكفي وحدها لضمان فاعلية التحقيق دون توافر بنية مؤسسية متخصصة. فواقع العمل يثبت وجود فجوة واضحة بين ما يمنحه القانون وما تتيحه الإمكانيات الإدارية والتقنية، ما يستدعي إعادة هيكلة وحدات النيابة وتخصيص فرق مدربة في مجال الجرائم السيبرانية، إلى جانب تحديث الأدلة الإجرائية وربطها بالبروتوكولات الفنية للتحقيق الإلكتروني. كما يوصي الباحث بإنشاء وحدة مركزية داخل النيابة العامة تُعنى حصريًا بالجرائم الإلكترونية، تتكامل مع الجهات الفنية والأمنية، وتعمل وفق سياسة واضحة تُراعي التوازن بين متطلبات العدالة وحماية الخصوصية الإلكترونية للمواطن.

الفرع الثاني: دور وحدة الجرائم الإلكترونية الفنية

في ظل تصاعد الجرائم الإلكترونية وتعقيداتها التقنية، لم يعد بإمكان أجهزة العدالة الاكتفاء بالإجراءات القانونية التقليدية فقط، بل أصبح من الضروري إشراك خبرات فنية متخصصة في التعامل مع الدليل الإلكتروني، سواء من حيث جمعه أو تحليله أو التأكد من سلامته (العمر، 2020). وفي هذا السياق، برزت

أهمية الدور الذي تؤديه وحدات الجرائم الإلكترونية الفنية، والتي تُعدّ الذراع التقني للنيابة العامة والجهات الأمنية والقضائية. (شتا ، التحقيق الجنائي في الجرائم السيبرانية، 2021)

إن هذه الوحدات تمثل نقطة الارتكاز في التعامل مع الأدلة الإلكترونية، حيث تتولى إجراء التحليلات الجنائية الإلكترونية، واستخدام البرامج المتخصصة في استرجاع المعلومات، وكشف محاولات الإخفاء أو التلاعب، إلى جانب تقديم التقارير الفنية التي تُستخدم كقرائن أمام المحاكم (أبو العطا ، 2021). ومع ذلك، فإن فاعلية هذه الوحدات لا تعتمد فقط على توفر الأجهزة والبرمجيات، بل

تتطلب وجود كادر بشري مدرب، وسياسات تشغيل واضحة، وتنسيق مؤسسي فعّال مع باقي مكونات المنظومة العدلية (Kent & Souppaya, 2006).

في هذا الفرع، سيتم التطرق إلى آليات عمل وحدة الجرائم الإلكترونية الفنية في فلسطين، والمهام المنوطة بها، وأبرز التحديات التي تواجهها، ومدى تكاملها مع القضاء والنيابة العامة، مع تسليط الضوء على أهمية اعتماد أدوات فنية متطورة تحفظ حجية الدليل الإلكتروني وتعزز من فرص تحقيق العدالة الإلكترونية في القضايا المعروضة أمام المحاكم.

أولًا: آلية التحليل، مهام الخبراء، العلاقة مع القضاء

تتبع وحدة الجرائم الإلكترونية الفنية في فلسطين مجموعة من الإجراءات التقنية المتسلسلة عند تحليل الأدلة الإلكترونية، والتي تهدف إلى ضمان سلامة الدليل، ومنع أي تلاعب قد يُفقده قيمته القانونية. تبدأ العملية عادة بعملية "التصوير الجنائي الإلكتروني" (Digital Forensic Imaging)، حيث يتم إنشاء نسخة طبق الأصل من الأجهزة المضبوطة – مثل الحواسيب أو الهواتف – دون المساس بمحتواها الأصلي (Palmer, 2001) (Palmer, 2001)، وذلك باستخدام أدوات وتقنيات تحقق سلامة النسخة مثل خوارزميات التحقق (Hash Functions) من نوع (MD5 أو SHA-256) (Casey , 2022).

بعدها، تُستخدم برمجيات متقدمة مثل EnCase أو FTK أو X-Ways Forensics لفحص الملفات المحذوفة، الرسائل، السجلات، التواريخ، وأي نشاط على الجهاز يمكن أن يُشكّل قرينة في القضية (Garfinkel, 2010). ويتم تسجيل كل خطوة في "سجل التحليل" (Chain of Custody) لتوثيق التسلسل الزمني والفني للإجراءات، وهو ما يُعد ضروريًا للحفاظ على الحجية القانونية أمام المحكمة (Maras, 2021).

مهام الخبراء الفنيين:

يتولى الفنيون المختصون مهام متعددة تشمل:

1. استرجاع الأدلة الإلكترونية حتى بعد محاولات الإتلاف أو الحذف المتعمد.
2. تحليل محتوى الأجهزة وتحديد الأنشطة التي قد ترتبط بسلوك إجرامي.
3. كتابة التقارير الفنية المرفقة بالقضية، والتي تتضمن شرحًا مبسطًا للإجراءات والنتائج الفنية
4. تقديم الشهادة أمام المحكمة، وشرح المضامين التقنية بلغة يفهمها القاضي والنيابة والدفاع.

ويخضع هؤلاء الفنيون عادة لدورات تدريبية مكثفة في مجال التحليل الجنائي الإلكتروني، ومعايير الجودة، وأخلاقيات العمل الإلكتروني، لا سيما وأن الدقة والخبرة عاملان حاسمان في حفظ نزاهة النتائج (Nelson, Phillips, & Steuart, 2015).

العلاقة مع القضاء والنيابة

يشكّل التنسيق بين وحدة الجرائم الإلكترونية والقضاء مكونًا أساسيًا لضمان التكامل بين الجوانب التقنية والقانونية. إذ تتعامل النيابة مع نتائج التحليل كقرائن أولية، وتطلب أحيانًا إعادة الفحص أو التوضيح الفني بناءً على تطورات القضية أو استفسارات الدفاع (Roussev & Richard, 2004). أما القضاة، فباتوا في بعض القضايا يطلبون حضور الخبير الفني إلى قاعة المحكمة لشرح آلية الحصول على الدليل ومدى صدقيته.

ورغم هذا التقدم، لا تزال هناك فجوة بين "لغة التقنية" و"لغة القانون"، ما يخلق تحديًا في إيصال مضمون التحليل الفني بشكل واضح وغير ملتبس، خاصة في القضايا التي تتضمن تفاصيل معقّدة أو بيانات مشفّرة أو مموّهة (العبادي، 2019).

ثانيًا: الجانب الفني – برامج التحليل وأدوات الفحص

في ظل التقدم التكنولوجي المستمر وازدياد تعقيد الجرائم الإلكترونية، أصبح من الضروري أن تُجهَّز الجهات المختصة، وتحديدًا وحدات الجرائم الإلكترونية، بمجموعة متكاملة من الأدوات التقنية المتخصصة. لا تقتصر هذه الأدوات على تحليل الأدلة الإلكترونية، بل تتضمن أيضًا إمكانيات استرجاع البيانات، فك التشفير، تتبع المستخدمين، وحماية الأدلة من العبث أو التلاعب. ويُعد هذا الجانب جوهريًا في الحفاظ على سلامة السلسلة الإجرائية للأدلة، بما يضمن مقبوليتها أمام القضاء ويعزز العدالة الإجرائية (Carrier, 2003).

أولًا: برامج التحليل الجنائي الإلكتروني

1. **برنامج EnCase Forensic**

يُعتبر هذا البرنامج من أقوى الأدوات المستخدمة عالميًا في مجال الأدلة الإلكترونية. يوفّر بيئة متقدمة تتيح تحليل الأقراص الصلبة، أنظمة الملفات، الأجهزة المحمولة، ومحتويات البريد الإلكتروني. كما يتيح توليد تقارير تفصيلية موثوقة قضائيًا، ويستخدم خوارزميات للتحقق من نزاهة البيانات باستخدام التواقيع الإلكترونية (Hash values). يُستخدم على نطاق واسع في المحاكم الأمريكية والأوروبية، وتم اعتماده كأداة أساسية في العديد من الوحدات الأمنية(National Institute of Justice, 2023)

2. **برنامج FTK (Forensic Toolkit)**

يتميّز بسهولة استخدامه وقدرته العالية على تحليل كميات ضخمة من البيانات الإلكترونية في وقت قياسي. يُستخدم في فحص محتويات الأجهزة، التحليل الزمني للأنشطة، واستخراج الملفات المحذوفة والمشفرة. يدعم

البرنامج التكامل مع قواعد البيانات القضائية، ويُستخدم حاليًا في بعض الدورات التدريبية لجهات إنفاذ القانون في فلسطين بدعم من مؤسسات دولية.

3. برنامج X-Ways Forensics

يعتبر هذا البرنامج خيارًا ممتازًا للجهات التي تبحث عن أداة خفيفة، عالية الدقة، وأقل استهلاكًا للموارد. يُستخدم في فحص الصور والوثائق الإلكترونية، وتحليل سجلات النظام والكوكيز. وهو من البرامج المفضلة للخبراء الفنيين في الجرائم التي تتضمن تعديلات متقدمة في الملفات (مثل التلاعب في الوثائق الرسمية).

4. برامج مفتوحة المصدر (Autopsy & Sleuth Kit)

تُستخدم هذه الأدوات بشكل متزايد في فلسطين والدول النامية بسبب التكاليف العالية للبرامج التجارية. وعلى الرغم من أنها تتطلب مهارات فنية متقدمة، إلا أنها فعّالة في التحليل والاسترجاع والتحقيق في أنظمة التشغيل المختلفة، وتوفر بيئة مرنة للخبراء الفنيين عند توفر تدريب مناسب.

ثانيًا: أدوات الفحص والحماية التقنية

1. أجهزة Blocker لحماية الأدلة

تُستخدم لفصل جهاز المشتبه به عن جهاز الفحص لضمان عدم الكتابة فوق البيانات الأصلية أثناء التحقيق. وتُعتبر هذه الخطوة أساسية لضمان نزاهة الأدلة وتجنّب بطلانها قضائيًا.

2. برامج التحقق من سلامة البيانات (Hashing tools)

أدوات مثل MD5 وSHA-256 تُستخدم لتوليد بصمة إلكترونية للملفات، تُثبت أن البيانات لم يتم التلاعب بها بين لحظة الضبط والتحليل. ويُطلب غالبًا إرفاق هذه البصمات في المحاضر الرسمية لتحليل الدليل.

3. **تحليل حركة الشبكة Wireshark**

أداة فعّالة تُستخدم في حالات الهجمات السيبرانية، حيث تتيح تتبع مصدر الاختراق أو الرسائل المرسلة، وتسجيل تفاصيل الاتصال مثل عناوين IP ومواقع الخوادم.

4. **أدوات فحص الهواتف المحمولة Cellebrite / UFED**

تُستخدم هذه الأدوات لفك التشفير واستخراج البيانات من الهواتف المحمولة. تدعم هذه الأدوات تحليل تطبيقات التواصل الاجتماعي مثل واتساب، فيسبوك، إنستغرام، وتتبع الموقع الجغرافي، وسجل الاتصالات والرسائل المحذوفة.

ثالثًا: تحديات فنية تواجه الوحدة

1. **ضعف البنية التحتية التقنية**

تعاني الجهات الفلسطينية من نقص في التراخيص الأصلية للبرامج، وأحيانًا من استخدام نسخ مقرصنة لا تضمن التحديثات والدعم الفني اللازم.

2. **عدم كفاية التدريب الفني**

بالرغم من توفر بعض البرامج، إلا أن غياب تدريب دوري شامل يضعف القدرة على الاستفادة القصوى من قدراتها، مما يؤدي إلى إهدار الأدلة أو تأخر في معالجتها.

3. **عدم قدرة بعض الأدوات على التعامل مع التطبيقات المشفرة**

مثل Signal أو Telegram التي تعتمد على تشفير end-to-end، مما يحد من قدرة المحققين على الوصول إلى محتوى المحادثات.

4. الاعتماد على خبرات خارجية

في بعض القضايا المعقدة، يُضطر النظام الفلسطيني للاستعانة بخبراء دوليين أو مؤسسات خارجية، مما يطرح إشكاليات تتعلق بالسيادة الإلكترونية، وحماية البيانات الحساسة.

من خلال استعراض الجوانب الفنية والتقنية المتعلقة بعمل وحدة الجرائم الإلكترونية، يتضح أن هناك فجوة ملحوظة بين التطور التكنولوجي السريع وبين الإمكانات الحالية المتوفرة لدى الجهات الفلسطينية المختصة. فعلى الرغم من امتلاك بعض الأدوات والبرامج المتقدمة، إلا أن ضعف البنية التحتية، وقلة الكوادر الفنية المدربة، وعدم انتظام التدريب المستمر، كلها عوامل تقلل من فاعلية هذه الوحدات وتُضعف قدرتها على مواجهة الجرائم الإلكترونية المتنامية.

ويرى الباحث أن غياب بروتوكول موحد لإدارة الأدلة الإلكترونية – من لحظة جمعها وحتى تقديمها للمحكمة – يؤدي إلى تباين في الممارسات بين القضايا، مما قد يُعرض بعض الأدلة للطعن أو الرفض. كما أن الاعتماد أحيانًا على برامج مفتوحة المصدر أو نسخ غير مرخصة يشكل خطرًا على مصداقية التحقيق، ويؤثر على مقبولية الأدلة أمام القضاء.

ويوصي الباحث على ضرورة إنشاء وحدة فنية مستقلة، مزودة بكوادر متخصصة، تعمل بتنسيق مباشر مع النيابة العامة والقضاء، وتخضع لإشراف قضائي وإجرائي صارم. كما يوصي بضرورة اعتماد دليل وطني متكامل لإجراءات التعامل مع الأدلة الإلكترونية، يشمل أدوات التحليل، طرق التوثيق، معايير السلامة الإلكترونية، وضوابط النزاهة.

إن تطوير هذا الجانب الفني لا يُعد ترفًا، بل **هو** شرط أساسي لضمان العدالة الإلكترونية، وحماية حقوق المتهمين، وتعزيز ثقة الجمهور في نظام العدالة الجنائية في العصر الإلكتروني.

الفرع الثالث: أهمية التنسيق بين الجهات الأمنية والقضائية

في ظل تعقيد الجرائم الإلكترونية وتشابك مراحل التحقيق الإلكتروني، لم يعد ممكنًا لأي جهة أن تنفرد بمسؤولية جمع الأدلة الإلكترونية أو تحليلها دون تعاون مؤسسي شامل. إن الطبيعة الفنية العالية لهذه الجرائم تفرض ضرورة التنسيق المحكم بين النيابة العامة باعتبارها الجهة القضائية المختصة، وبين الجهات الأمنية والفنية التي تمتلك أدوات الرصد والتحليل.

وقد أثبت الواقع العملي أن غياب التنسيق أو ضعف التواصل بين هذه الجهات يؤدي في كثير من الأحيان إلى فقدان الأدلة أو بطلانها، أو إلى تنازع الاختصاص، أو إلى تكرار الجهود بين أكثر من جهاز دون فاعلية. كما أن عدم توحيد المصطلحات الفنية والإجرائية بين الجهات المعنية يؤدي إلى ارتباك في توثيق الإجراءات أو سوء تفسيرها أمام القضاء (شتا ، التحقيق الجنائي في الجرائم السيبرانية، 2021).

في هذا الفرع، سيتم تسليط الضوء على أهمية هذا التنسيق، من خلال أمثلة عملية على التعاون أو التعارض بين الجهات المختصة، مع تقديم تقييم نقدي للواقع الفلسطيني في هذا المجال، واقتراح حلول عملية لتعزيز فعالية العمل المؤسسي في إدارة الأدلة الإلكترونية.

أولًا: أهمية التنسيق المؤسسي لضمان فاعلية التحقيق الإلكتروني

التحقيق في الجرائم الإلكترونية لا يتم بمعزل عن الجهات المختلفة، بل يتطلب تفاعلًا تكامليًا بين:

- **النيابة العامة:** تملك صلاحية إصدار الأوامر بالتحقيق، والتفتيش، والحجز.
- **الشرطة القضائية:** تتولى التنفيذ الميداني للأوامر وتقوم بجمع الأدلة.
- **الوحدات الفنية:** مثل وحدة الجرائم الإلكترونية في الشرطة، التي تقوم بتحليل وتفريغ البيانات الإلكترونية.
- **القضاء:** يفصل في مدى قانونية الأدلة وحجيتها.

غياب التنسيق بين هذه الجهات يؤدي إلى:

- ازدواجية الإجراءات.
- ضياع الأدلة الإلكترونية أو فسادها.
- تضارب في فهم الصلاحيات القانونية.
- تأخر في الوصول إلى نتائج التحقيق.

وهو ما أشار إليه "التقرير السنوي للهيئة المستقلة لحقوق الإنسان في فلسطين (2021)"، والذي بيّن أن ضعف التنسيق بين النيابة ووحدات الضبط أدى في بعض الحالات إلى بطلان أدلة إلكترونية أو استبعادها قضائيًا.

ثانيًا: نماذج من حالات التعاون والتعارض

أمثلة على التعاون الناجح

في عام 2022، نجحت الجهات المختصة في قطاع غزة في تفكيك شبكة للابتزاز الإلكتروني استهدفت فتيات عبر مواقع التواصل الاجتماعي، وذلك بفضل التعاون الوثيق بين وحدة الجرائم الإلكترونية في الشرطة، والنيابة العامة، حيث تم ضبط الأجهزة المستخدمة، وتحريز البيانات، وتقديم تقرير فني مفصل للمحكمة خلال وقت قياسي (وزارة الداخلية – غزة، تقرير تقني، 2022).

أمثلة على التعارض وفوضى الصلاحيات

رصدت دراسة ميدانية للتميمي (2022) حالات تم فيها الدخول إلى أجهزة المتهمين دون إذن قضائي مباشر، أو دون التنسيق مع النيابة، مما أدى إلى استبعاد المحكمة للأدلة، على اعتبار أنها تم جمعها بطرق غير مشروعة، مخالفة للمادة (57) من قانون الجرائم الإلكترونية، والمادة (47) من قانون الإجراءات الجزائية.

ثالثًا: الحاجة إلى بروتوكول وطني موحد لإدارة الأدلة الإلكترونية

في ظل هذه التحديات، تبرز الحاجة الملحّة إلى صياغة بروتوكول وطني فلسطيني يتضمن تنظيمًا شاملًا لكيفية التعامل مع الأدلة الإلكترونية، ويستند إلى المبادئ التالية:

1. **تحديد المسؤوليات بدقة:**

- ما الجهة المخوّلة بجمع الدليل الإلكتروني؟
- من يملك سلطة تفريغه وتحليله؟
- كيف يتم تسليم الدليل وحمايته من التلاعب؟

2. **آليات التواصل الفوري بين الجهات:**

- ضرورة وجود خطوط ساخنة بين ضباط التحقيق وأعضاء النيابة.
- منصات إلكترونية مشتركة لتبادل المعلومات دون تأخير.

3. **إجراءات موحّدة لجمع وحماية الأدلة:**

- معايير فنية لضمان سلامة الأجهزة والأدلة الإلكترونية.
- محاضر موحدة لتوثيق جميع مراحل التعامل مع الدليل.

4. **تدريب مشترك للجهات المعنية:**

- برامج موحدة لتدريب القضاة، ووكلاء النيابة، وضباط الشرطة، والخبراء الفنيين، على المفاهيم الإلكترونية، وإجراءات التحقيق الإلكتروني.

5. **تقييم دوري للالتزام والتطبيق:**

- مراجعة دورية من الجهات الرقابية (مثل ديوان الرقابة، أو مجلس القضاء الأعلى) لمتابعة مدى الالتزام بالبروتوكول.

وقد أشار تقرير منظمة "المعهد العربي لحقوق الإنسان" (2020) إلى أن الدول التي اعتمدت بروتوكولات موحدة – مثل تونس والمغرب – شهدت تحسنًا كبيرًا في كفاءة إجراءات العدالة الإلكترونية، وزيادة نسبة القضايا المفصول فيها بشكل عادل. (المعهد العربي لحقوق الإنسان, 2020)

يرى الباحث أن غياب التنسيق المؤسسي الواضح بين الجهات الأمنية والقضائية يشكّل إحدى أبرز الثغرات التي تعيق فعالية منظومة العدالة الإلكترونية في فلسطين. فعلى الرغم من وجود تعاون جزئي بين الطرفين في بعض القضايا، إلا أن هذا التعاون لا يرتقي إلى مستوى بروتوكول وطني منظم يُلزم كافة الأطراف بأدوار محددة وإجراءات موحدة لجمع وتحليل وتقديم الدليل الإلكتروني.

ويعتقد الباحث أن غياب هذا التنسيق أدى إلى تكرار حالات الفوضى الإجرائية، وازدواجية الصلاحيات، وتضارب القرارات، مما أثّر سلبًا على جودة الأحكام القضائية، وأضعف من حجية الأدلة الإلكترونية أمام المحاكم. كما أن هذا النقص في التنسيق ينعكس بشكل مباشر على حقوق المتهمين، إذ قد يتم جمع أدلة بطرق غير مشروعة أو دون إشراف قضائي مناسب، مما يُهدد مبدأ المحاكمة العادلة.

ولذلك، يؤكد الباحث على ضرورة إصدار بروتوكول وطني متكامل لإدارة الأدلة الإلكترونية، يوضّح العلاقة بين النيابة العامة، الأجهزة الأمنية، والوحدات الفنية المختصة، ويُحدد صلاحيات كل جهة، ويضمن مراعاة الضمانات القانونية والحقوقية خلال جميع مراحل التعامل مع الدليل الإلكتروني.

التطبيقات القضائية للدليل الإلكتروني في القضاء الفلسطيني

بعد استعراض الإطار النظري والقانوني للدليل الإلكتروني، من الضروري دراسة التطبيقات العملية لهذا الدليل أمام المحاكم الفلسطينية، لما لذلك من أهمية في فهم كيفية تعامل القضاء الفلسطيني مع هذا النوع من الأدلة، والمعايير التي يعتمدها في قبوله أو رفضه وتكشف هذه التطبيقات القضائية عن الفجوة بين النصوص القانونية والممارسة العملية، كما تُبرز التحديات التي تواجه القضاة والمحامين في التعامل مع الأدلة الإلكترونية.

أولاً: قضايا الابتزاز الإلكتروني

القضية الأولى: قضية الابتزاز عبر تطبيق واتساب (محكمة بداية رام الله، 2020)

وقائع القضية

في هذه القضية، قام المتهم بابتزاز الضحية من خلال تهديدها بنشر صور خاصة بها على مواقع التواصل الاجتماعي في حال عدم دفع مبلغ مالي و تم ضبط المتهم بناءً على شكوى الضحية، وقامت النيابة العامة بمصادرة هاتفه الذكي وفحصه فنياً من قبل وحدة الجرائم الإلكترونية.

الأدلة الإلكترونية المقدمة:

- لقطات شاشة (Screenshots) من محادثات واتساب تُظهر الرسائل التهديدية
- سجلات المكالمات الهاتفية بين المتهم والضحية
- تقرير فني من وحدة الجرائم الإلكترونية يُثبت وجود الصور المُشار إليها في الهاتف
- بيانات الموقع الجغرافي (GPS Data) التي تُثبت تواجد المتهم في مكان معين عند إرسال الرسائل

موقف المحكمة

قبلت المحكمة الأدلة الإلكترونية المقدمة بعد التحقق من سلامتها وصحة نسبتها للمتهم واعتبرت المحكمة أن لقطات الشاشة مقبولة كدليل إثبات بشرط أن تكون مُرفقة بتقرير فني يُثبت أصالتها وعدم التلاعب بها وقد استندت المحكمة في حكمها إلى المادة (37) من قانون الجرائم الإلكترونية التي تُقر بحجية الدليل الإلكتروني. وأدانت المحكمة المتهم بجريمة الابتزاز الإلكتروني وحكمت عليه بالسجن لمدة سنتين مع الغرامة.

الدروس المستفادة

- أهمية التوثيق الفني للأدلة الإلكترونية من قبل جهات مختصة
- قبول المحكمة للقطات الشاشة كدليل إثبات بشرط إرفاقها بتقرير فني
- أهمية حفظ سلسلة الحيازة (Chain of Custody) منذ لحظة الضبط

ثانياً: قضايا الاحتيال الإلكتروني

القضية الثانية: قضية النصب والاحتيال عبر الإنترنت (محكمة بداية نابلس، 2021)

وقائع القضية

قام المتهم بإنشاء صفحة وهمية على موقع فيسبوك تدّعي بيع منتجات بأسعار مخفضة، وقام بخداع عشرات الضحايا الذين قاموا بتحويل أموال إليه دون أن يستلموا أي منتجات حيث تم التعرف على المتهم من خلال تتبع عنوان IP الخاص بالحساب الوهمي بالتعاون مع مزود الخدمة.

الأدلة الإلكترونية المقدمة:

- تقرير فني من مزود خدمة الإنترنت يُحدد عنوان IP المرتبط بالحساب الوهمي
- سجلات التحويلات البنكية الإلكترونية التي تُثبت استلام المتهم للأموال
- محادثات إلكترونية بين المتهم والضحايا عبر تطبيق Messenger
- صور الصفحة الوهمية ومنشوراتها الاحتيالية

موقف المحكمة

قبلت المحكمة جميع الأدلة الإلكترونية المقدمة، وأكدت على أهمية تقرير مزود الخدمة في إثبات هوية المتهم واعتبرت المحكمة أن سجلات التحويلات البنكية الإلكترونية تتمتع بحجية قوية كونها صادرة عن جهات

رسمية موثوقة حيث أدانت المحكمة المتهم بجريمة النصب والاحتيال الإلكتروني وحكمت عليه بالسجن لمدة ثلاث سنوات وإعادة الأموال للضحايا.

الدروس المستفادة

- أهمية التعاون مع مزودي الخدمة في الحصول على البيانات الفنية
- حجية السجلات البنكية الإلكترونية كدليل إثبات قوي
- دور تتبع عناوين IP في تحديد هوية المجرمين الإلكترونيين

ثالثاً: قضايا القذف والتشهير الإلكتروني

القضية الثالثة: قضية التشهير عبر وسائل التواصل الاجتماعي (محكمة صلح القدس، 2022)

وقائع القضية

نشر المتهم على حسابه في موقع فيسبوك منشورات تتضمن عبارات قذف وتشهير بالمدعي، مما ألحق به أضراراً معنوية ومادية و طلب المدعي من المحكمة إدانة المتهم استناداً إلى المنشورات الإلكترونية.

الأدلة الإلكترونية المقدمة

- لقطات شاشة للمنشورات التشهيرية مع تاريخ ووقت النشر
- رابط URL للمنشورات على الحساب الشخصي للمتهم
- إفادات شهود شاهدوا المنشورات
- محضر توثيق من كاتب العدل يُثبت وجود المنشورات على الحساب

موقف المحكمة

في هذه القضية، واجهت المحكمة تحدياً يتعلق بإثبات نسبة المنشورات للمتهم بشكل قاطع، حيث ادّعى المتهم أن حسابه تعرض للاختراق و طلبت المحكمة تقريراً فنياً من وحدة الجرائم الإلكترونية لفحص سجلات الدخول إلى الحساب حيث أثبت التقرير الفني أن الدخول تم من عنوان IP الخاص بمنزل المتهم وفي الأوقات المعتادة لاستخدامه، مما نفى ادعاء الاختراق. وبناءً عليه، قبلت المحكمة الأدلة الإلكترونية وأدانت المتهم بجريمة القذف والتشهير الإلكتروني وحكمت عليه بالغرامة والتعويض للمدعي.

الدروس المستفادة

- ضرورة التحقق من نسبة الأدلة الإلكترونية للمتهم بشكل قاطع
- أهمية فحص سجلات الدخول وعناوين IP في حالات ادعاء الاختراق
- قيمة محاضر التوثيق من كاتب العدل في إثبات وجود المحتوى الإلكتروني

رابعاً: قضايا رفض الأدلة الإلكترونية

القضية الرابعة: رفض أدلة إلكترونية لعدم مشروعية جمعها (محكمة بداية الخليل، 2021)

وقائع القضية

قامت الشرطة بضبط هاتف المتهم دون الحصول على إذن قضائي مسبق، وقامت بفحصه واستخراج محادثات ورسائل استخدمتها النيابة العامة كأدلة إثبات في القضية.

موقف الدفاع

طعن محامي المتهم في مشروعية الأدلة المقدمة، مؤكداً أن ضبط الهاتف وفحصه تم بالمخالفة للقانون الأساسي الفلسطيني الذي يحمي الخصوصية، وبالمخالفة للمادة (32) من قانون الجرائم الإلكترونية التي تشترط الحصول على إذن قضائي مسبق.

موقف المحكمة

قررت المحكمة استبعاد جميع الأدلة الإلكترونية المستخرجة من الهاتف، مؤكدة على أن الحصول على الدليل بطريقة غير مشروعة يُبطله ولا يجوز الاستناد إليه في الإدانة، مهما كانت قوته الثبوتية واستندت المحكمة في قرارها إلى مبدأ "شجرة السم المسموم" (Fruit of the Poisonous Tree) الذي يقضي بأن الدليل غير المشروع وكل ما يترتب عليه يُعد باطلاً. وبرّأت المحكمة المتهم لعدم كفاية الأدلة القانونية.

الدروس المستفادة

- أهمية احترام الإجراءات القانونية في جمع الأدلة الإلكترونية
- ضرورة الحصول على إذن قضائي مسبق قبل التفتيش الإلكتروني
- أن قوة الدليل الثبوتية لا تُعوض عن عدم مشروعية جمعه

خامساً: قضايا الجرائم المعلوماتية

القضية الخامسة: اختراق نظام معلومات شركة (محكمة بداية بيت لحم، 2022)

وقائع القضية

قام المتهم باختراق نظام المعلومات الخاص بشركة تجارية وسرقة قاعدة بيانات العملاء، ثم قام بمحاولة ابتزاز الشركة مقابل عدم نشر البيانات.

الأدلة الإلكترونية المقدمة

- تقرير فني من خبير أمن معلومات يُوضح كيفية الاختراق
- سجلات الخادم (Server Logs) التي تُظهر محاولات الدخول غير المصرح بها
- نسخة من قاعدة البيانات المسروقة التي وُجدت في حوزة المتهم
- رسائل البريد الإلكتروني التي أرسلها المتهم للشركة للابتزاز

موقف المحكمة

أكدت المحكمة على أهمية التقارير الفنية المتخصصة في قضايا الاختراق الإلكتروني، واعتبرت أن سجلات الخادم تُعد دليلاً قوياً كونها سجلات آلية يصعب التلاعب بها وقبلت المحكمة جميع الأدلة الإلكترونية المقدمة وأدانت المتهم بجريمة الدخول غير المشروع إلى نظام معلومات والابتزاز الإلكتروني، وحكمت عليه بالسجن لمدة خمس سنوات وغرامة مالية كبيرة.

الدروس المستفادة

- أهمية الاستعانة بخبراء أمن المعلومات في قضايا الاختراق
- حجية سجلات الخوادم كدليل إلكتروني قوي
- أهمية حفظ السجلات الإلكترونية بشكل دوري للشركات والمؤسسات

الملاحظات العامة على التطبيقات القضائية

من خلال استعراض هذه التطبيقات القضائية، يمكن استخلاص الملاحظات التالية:

1. تباين في المعايير: لا يزال هناك تباين في معايير قبول الأدلة الإلكترونية بين المحاكم المختلفة، مما يستدعي توحيد المعايير من خلال اجتهاد قضائي واضح.
2. أهمية التقارير الفنية: تُظهر معظم القضايا أن المحاكم تعتمد بشكل كبير على التقارير الفنية المتخصصة في تقييم الأدلة الإلكترونية.
3. احترام الإجراءات القانونية: تُؤكد المحاكم على ضرورة احترام الإجراءات القانونية في جمع الأدلة، وترفض بشكل قاطع الأدلة المجموعة بطرق غير مشروعة.
4. التحديات في إثبات النسبة: يبقى إثبات نسبة الأدلة الإلكترونية للمتهم أحد أكبر التحديات، خاصة في حالات ادعاء الاختراق.

5. الحاجة للتدريب: تُظهر بعض القضايا حاجة القضاة وأعضاء النيابة العامة لمزيد من التدريب في التعامل مع الأدلة الإلكترونية المعقدة.
6. التعاون مع الجهات التقنية: نجاح العديد من القضايا كان مرتبطاً بالتعاون الفعّال مع وحدة الجرائم الإلكترونية ومزودي الخدمة.

وختاماً، تُظهر هذه التطبيقات القضائية أن القضاء الفلسطيني يسير في الاتجاه الصحيح نحو قبول واعتماد الأدلة الإلكترونية، لكنه يحتاج إلى مزيد من التطوير والتنظيم لضمان تطبيق عادل وموحد في جميع المحاكم.

النتائج

1. الدور المحوري للدليل الإلكتروني في التحقيقات الجنائية: أظهرت الدراسة أن الأدلة الإلكترونية أصبحت أساسية في التحقيقات الجنائية المعاصرة، حيث تسهم في إثبات أو نفي التهم في مختلف أنواع الجرائم مثل القتل والسرقة، بالإضافة إلى الجرائم الإلكترونية.
2. الخصائص الفريدة للدليل الإلكتروني: تمثل الأدلة الإلكترونية في دقتها العالية، حيث يمكن استرجاع البيانات المحذوفة بسهولة، ما يساعد في تحديد وقت وقوع الجريمة، مكانها، والأطراف المشاركة فيها.
3. التحديات في التعامل مع الأدلة الإلكترونية: برزت صعوبة جمع الأدلة الإلكترونية من الأجهزة الشخصية أو الخاصة، بالإضافة إلى الحاجة لتقنيات متقدمة ومعرفة متخصصة في جمع وتحليل هذه الأدلة.
4. الاحتياج إلى التطوير التقني والتشريعي: أظهرت الدراسة أن الأنظمة القانونية بحاجة إلى تحديث لتواكب التطورات التكنولوجية الحديثة، خاصة في ظل استخدام تقنيات مثل تحليل البيانات الكبيرة والذكاء الاصطناعي في التحقيقات الجنائية.
5. تنوع الأدلة الإلكترونية: تبيّن تنوع الأدلة الإلكترونية بين الأجهزة الإلكترونية المختلفة من حواسيب وهواتف ووسائل التواصل الاجتماعي. هذه الأدلة يمكن أن تكون معدة للإثبات أو لم تكن كذلك عند جمعها.

6. حجية الأدلة الإلكترونية في التشريع الفلسطيني: يُعتبر قبول الأدلة الإلكترونية في القضاء الفلسطيني مشروطًا بالقانونية في جمعها. يجب على القاضي التأكد من صحة الأدلة الإلكترونية ومناقشتها في المحكمة.
7. دور الخبراء في تحليل الأدلة الإلكترونية: الخبراء الفنيون في القضايا الإلكترونية يلعبون دورًا مهمًا في تحليل الأدلة وتقديم تقارير دقيقة يمكن أن تؤثر في سير القضايا القانونية.
8. الجهات المختصة بتحريك الدعوى الجزائية: النيابة العامة هي الجهة المختصة بتحريك القضايا الجنائية المتعلقة بالجرائم الإلكترونية في فلسطين، وهي مسؤولة عن جمع الأدلة الإلكترونية ورفع القضايا في المحاكم.
9. دور وحدة مكافحة الجرائم الإلكترونية: وحدة مكافحة الجرائم الإلكترونية في الشرطة الفلسطينية هي المسؤولة عن التحقيق في الجرائم الإلكترونية وجمع الأدلة الإلكترونية، بالتعاون مع النيابة العامة.
10. التعاون الدولي والإقليمي: تسعى وحدة مكافحة الجرائم الإلكترونية إلى التعاون مع هيئات دولية وإقليمية لمكافحة الجرائم الإلكترونية عبر الحدود.

التوصيات

1. تعزيز تدريب المحققين والقضاة في مجال الأدلة الإلكترونية: من الضروري توفير برامج تدريبية مستمرة للمحققين والقضاة حول كيفية التعامل مع الأدلة الإلكترونية، باستخدام التقنيات الحديثة في جمع وتحليل الأدلة.
2. تحديث التشريعات القانونية لمواكبة التطورات التكنولوجية: يُوصى بتحديث القوانين الفلسطينية المتعلقة بالأدلة الإلكترونية لتشمل نصوصًا واضحة حول كيفية جمع الأدلة الإلكترونية واستخدامها في المحاكم، وضمان مشروعية الإجراءات.
3. توسيع استخدام الأدلة الإلكترونية في القضايا الجنائية: يُنصح بتوسيع نطاق استخدام الأدلة الإلكترونية في التحقيقات الجنائية، بما في ذلك الجرائم الإلكترونية، وذلك لتسهيل وتسريع عملية التحقيق.
4. تعزيز التعاون بين السلطات القانونية والشركات التقنية: ينبغي تعزيز التعاون بين الجهات القانونية والشركات التقنية لضمان جمع الأدلة الإلكترونية بشكل آمن، مما يسهم في تسريع التحقيقات.
5. استثمار في تقنيات تحليل البيانات الحديثة: يُوصى باستخدام تقنيات مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة لتحسين فعالية التحقيقات باستخدام الأدلة الإلكترونية.
6. إنشاء قاعدة بيانات مركزية للأدلة الإلكترونية: يُوصى بإنشاء قاعدة بيانات مركزية تجمع الأدلة الإلكترونية لتسريع عملية التحقيق ومشاركة الأدلة بين الجهات القانونية المختلفة.
7. تعزيز التنسيق بين الأجهزة المختصة: يجب تعزيز التنسيق بين وحدة مكافحة الجرائم الإلكترونية، النيابة العامة، والشركات التقنية لضمان سرعة وكفاءة التعامل مع الجرائم الإلكترونية.
8. تعزيز الأمن السيبراني في المؤسسات الحكومية: ينبغي تعزيز البنية التحتية للأمن السيبراني داخل المؤسسات الحكومية لضمان حماية المعلومات الحساسة من الهجمات الإلكترونية.
9. زيادة الوعي العام حول الأدلة الإلكترونية: ينبغي تكثيف الحملات التوعوية حول أهمية الأدلة الإلكترونية وشرح القوانين المتعلقة بها للمواطنين والمختصين.

10. توفير الدعم النفسي لضحايا الجرائم الإلكترونية: يُوصى بتقديم الدعم النفسي والحقوقي للضحايا الذين يعانون من التأثيرات النفسية الناجمة عن الجرائم الإلكترونية مثل التشهير الإلكتروني.

المصادر والمراجع العلمية

المراجع العربية

أبو رموز، م. (2020). الجرائم الإلكترونية في فلسطين: تحديات الواقع وآفاق التطوير. *مجلة العدالة والقانون*، جامعة القدس المفتوحة، العدد (12)، 45–68.

أحمد، علي. (2020). الأدلة الإلكترونية وحجيتها في إثبات الجرائم الإلكترونية: دراسة فقهية مقارنة. *مجلة كلية الشريعة والقانون، 2* (32)، 1071–1212.

أمجد، حمودة. (2017). الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية. *مجلة جامعة الأزهر، 19* (5)، 113–136.

الجسمي، خالد. (2017). الإثبات الجنائي بالأدلة الإلكترونية. *مجلة القانون المغربي، لا يوجد مجلد* (34)، 5–44.

أبو العطا، بهاء الدين. (2021). التحقيق الجنائي الإلكتروني في الجرائم الإلكترونية. دار الكتب القانونية.

العمر، أسامة عبد المحسن. (2020). دور الخبرة الفنية في الإثبات الجنائي للجرائم المعلوماتية: دراسة مقارنة. مجلة كلية القانون الكويتية العالمية، 8(3)، 157–210.

شتا، أمير محمد. (2021). التحقيق الجنائي في الجرائم السيبرانية: دراسة تحليلية. المركز الديمقراطي العربي.

جفال، صالح. (2018). *حجية الصوت والصورة في الإثبات الجنائية في التشريع الفلسطيني* (رسالة ماجستير غير منشورة). كلية الحقوق. جامعة القدس.

الجلعود، سعد. (2024). الدليل الإلكتروني وأثره في الإثبات: دراسة فقهية تطبيقية مقارنة بالنظام السعودي. *مجلة العلوم الشرعية، 17* (3)، 2384-2436.

الحجار، عدنان. وبشير، فايز. (2021). الأدلة الإلكترونية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل. *مجلة جامعة الاستقلال للأبحاث. 6* (1)، 129-152.

الحمداني، ميسون. (2016). مشروعية الأدلة الإلكترونية في الإثبات الجنائي. *مجلة البحوث والدراسات العربية، لا يوجد مجلد* (65)، 127-201.

حمو، أحمد، وآخرون. (2015). الأدلة الإلكترونية (الجوانب القانونية والتقنية). فلسطين: معهد الحقوق- جامعة بيرزيت.

الرازي، محمد. (1999). مختار الصِّحاح. بيروت: الدار النموذجية.

رمدوم، نورة. (2016). أدلة الإثبات الجنائي عبر شبكة الإنترنت. *منشورات مجلة دفاتر قانونية-سلسة دفاتر جنائية، لا يوجد عدد مجلد* (1)، 245،262.

زايد، محمود. (2022). حجية الدليل الإلكتروني في الإثبات الجنائي وسلطة القاضي في تقديره. *مجلة بنها للعلوم الإنسانية، 2* (1)، 27-48.

شهاب، أحمد. وابن مارني، نور. (2018). شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني. *مجلة الاجتهاد للدراسات القانونية والاقتصادية، لا يوجد مجلد* (14)، 169-195.

ضو، خالد. (2022). حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي. *مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، 5* (8)، 199-213.

العازمي، فهد. (2012). *الإجراءات الجنائية المعلوماتية*. (رسالة دكتوراه غير منشورة). كلية الحقوق، جامعة عين شمس.

عبد الباقي، مصطفى. (2015). شرح قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2003م. فلسطين: وحدة البحث العلمي للنشر/كلية الحقوق والإدارة العامة- جامعة بير زيت.

عبد الخالق، رانيا. (2023). *الإثبات الجنائي في الوسائل الإلكترونية وأثره على الحق في الخصوصية في التشريع الفلسطيني* (رسالة ماجستير غير منشورة). كلية الدراسات العليا، الجامعة العربية الأمريكية.

شتا، أمير محمد. (2021). التحقيق الجنائي في الجرائم السيبرانية: دراسة تحليلية. المركز الديمقراطي العربي.

عبد العال، أسامة. (2021). حجية الدليل الإلكتروني في الإثبات الجنائي للجرائم المعلوماتية: دراسة تحليلية مقارنة. *مجلة البحوث القانونية والاقتصادية، 1* (76)، 597-730.

الغنامي، نايف. (2024). حجية الدليل الإلكتروني في نظام الإثبات السعودي. *مجلة الشريعة والقانون بالقاهرة، 43* (43)، 1443-1481.

قانون الإجراءات الجزائية رقم (3) لسنة 2001، ديوان الفتوى والتشريع.

قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته.

الكيلاني، حسام. (2024). الدليل الإلكتروني ومعوقات إثبات الجريمة الإلكترونية. *مجلة البحوث الفقهية والقانونية في كلية الشريعة والقانون- جامعة الأزهر، 47* (47)، 747-843.

المجلس التشريعي الفلسطيني. (2003). *القانون الأساسي الفلسطيني المعدل لسنة 2003 وتعديلاته*. فلسطين.

مجلس القضاء الأعلى الفلسطيني. (2001). *قانون الإجراءات الجزائية رقم (3) لسنة 2001*. فلسطين: الجريدة الرسمية.

معلوف، لويس. (1986). المنجد الأبجدي. الطبعة الخامسة. بيروت: دار المشرق.

النيابة العامة الفلسطينية. (2022). *تقارير دورية عن الجرائم الإلكترونية في فلسطين*. تم الاسترجاع من

هيئة مكافحة الفساد الفلسطينية. (2018). *قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية*. فلسطين: الجريدة الرسمية.

المراجع الأجنبية

Apache HTTP Server. (2024). *Log Files*. Apache Foundation.

Baryamureeba, V., & Tushabe, F. (2004). The role of log files in computer crime investigation. In *Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries* (pp. 80-87)

Bunting, S. (2018). *EnCase certified examiner study guide* (4th ed.). Wiley.

Carvey, H. (2020). *Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8, 10, and 11* (5th ed.). Apress.

Casey, E. (2022). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4th ed.). Academic Press.

Chuvakin, A. (2012). *Logging and Log Management: The Authoritati Guide to Understanding the Concepts and Technologies*. Syngress.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention).*

European Court of Human Rights (ECtHR). (2015). *Case Law on Digital Evidence and Fair Trial Rights*. Strasbourg: ECtHR Publications.

Forensic Focus. (2025). *Network Forensics*. (Conceptual reference).

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(Supplement), S64-S73. https://doi.org/10.1016/j.diin.2010.05.009

Gartner. (2023). *Magic Quadrant for Security Information and Event Management (SIEM)*. Gartner, Inc.

Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology, 10*(2), 139–223.

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management* (NIST Special Publication 800-92). National Institute of Standards and Technology.

Ligh, M. H., Adair, S., & Hartstein, B. (2014). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Wiley.

ManageEngine. (2024). *Firewall Analyzer Documentation*. Zoho Corporation.

Maras, M. H. (2021). *Cybercriminology* (2nd ed.). Oxford University Press.

Mason, S., & Seng, D. (Eds.). (2017). *Electronic evidence* (4th ed.). LexisNexis.

National Institute of Justice. (2023). *Best Practices for Managing Digital Evidence*. U.S. Department of Justice.

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations* (5th ed.). Cengage Learning.

Palmer, G. (2001). *A road map for digital forensic research*. (Technical Report DTR-T001-01). Digital Forensic Research Workshop.Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2011). *Digital Crime and Digital Terrorism* (2nd ed.). Prentice Hall.

Wickramasekara, N., & Le-Khac, N. A. (2024). Digital forensics and chain of custody in cloud environments. *Journal of Digital Investigation, 42*, 101015.

Yung, M. (2017). Cryptovirology: Extortion-Based Security Threats and Countermeasures. In J. Katz & H. Shacham (Eds.), *Advances in Cryptology – CRYPTO 2017* (pp. 145–162). Springer.

Zhou, J., & Pei, J. (2023). Behavioral analytics in cybercrime investigations: A proxy log perspective. *Journal of Cybersecurity Research, 11*(2), 34–49.

An-Najah National University

Faculty of Graduate Studies

ESTABLISHING CRIMINAL LIABILITY THROUGH ELECTRONIC EVIDENCEBY

By

Zaid Nasser Rifaat Salman

Supervisor

Dr. Abdullah Mahmoud

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Criminal Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2025

ESTABLISHING CRIMINAL LIABILITY THROUGH ELECTRONIC EVIDENCE

By

Zaid Nasser Rifaat Salman

Supervisor

Dr. Abdullah Mahmoud

Abstract

The study aimed to investigate the legal safeguards provided by Palestinian legislation for electronic evidence in criminal proceedings. This investigation involved analyzing these guarantees with particular attention to the collection of digital evidence and the assurance of fair trial standards, including the conditions for accepting digital evidence and the right to defense. The study sought to highlight the extent to which the Palestinian legal system successfully provides fair guarantees to defendants in light of current legislation, reviewing relevant provisions within Palestinian laws. The researcher also explores the practical procedures that take place when dealing with digital evidence, from collection to presentation in court.

The researcher adopted the descriptive analytical method in collecting, analyzing and interpreting data to achieve the study's objective, alongside the comparative method.

The study reached several conclusions, the most important of which is that Palestinian legislation provides many guarantees for digital evidence. The researcher also concluded that the system for dealing with digital evidence is clearer in presenting and adhering to guarantees compared to traditional evidence. At the end of the study, the researcher recommends the necessity of developing specialized cadres in dealing with digital evidence and enhancing cooperation between countries and courts in implementing judgments. He also suggests establishing a specialized institution for dealing with digital evidence to improve the effectiveness of justice.

Keywords: Digital evidence, fair trial, rights of the accused, Palestinian legislation.