الجامعة العربية الأمريكية

كلية الدراسات العليا

قسم العلوم القانونية

برنامج الماجستير في العلوم الجنائية

# الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني (دراسة مقارنة)

وائل أحمد سيف عيد

202216280

أسماء لجنة الإشراف:

د. عبد اللطيف ربايعة

د. عصام الأطرش

د. محمد اشتية

تم تقديم هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في تخصص العلوم الجنائية

فلسطين، شباط/2025م

**الجامعة العربية الأمريكية**

**كلية الدراسات العليا**

**قسم العلوم القانونية**

**برنامج الماجستير في العلوم الجنائية**

# صفحة إجازة الرسالة

## الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني (دراسة مقارنة)

وائل أحمد سيف عيد

202216280

نوقشت هذه الرسالة وأجيزت بتاريخ 2025/2/27م من لجنة المناقشة التالية أسماؤهم وتواقيعهم:

| الاسم | | التوقيع |
|---|---|---|
| 1. د. عبد اللطيف ربايعة | المشرف الرئيس | |
| 2. د. عصام الأطرش | عضو لجنة الرسالة | issam alatrash |
| 3. د. محمد اشتية | عضو لجنة الرسالة | |

فلسطين، شباط/2025م

# الإقرار

أنا الموقع أدناه مقدم الرسالة الموسومة:

الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني (دراسة مقارنة)

أقر بأن ما اشتملت عليه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وأن هذه الرسالة ككل، أو جزء منها لم يقدم من قبل لنيل درجة علمية أو بحث لدى أي مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: وائل أحمد سيف عيد

الرقم الجامعي: 202216280

التوقيع: وائل عيد

تاريخ تسليم النسخة النهائية من الرسالة: 2025/3/20م

# الإهداء

اهدي ثمرة جهدي وتعبي المتواضع

إلى من غرَسوا فيَّ بذور الطموح، وسقوني حبًّا ودعمًا حتى أينعت ثمار النجاح، وعلموني البر والاحسان: إلى والدي العزيز، الذي علَّمني أن الإرادة تصنع المستحيل، وكان سندي في كل خطوة. وإلى والدتي الحبيبة، ينبوع الحنان الذي لا ينضب، ومصدر القوة الذي لا يخفت.

إلى إخوتي وأخواتي، الذين كانوا لي دومًا خير رفاق الدرب، يساندونني بحبّهم وتشجيعهم.

إلى أساتذتي الأفاضل، الذين لم يبخلوا بعلمهم وتوجيههم، فكانوا نورًا يضيء لي طريق المعرفة.

إلى كل من وقف بجانبي، ووهبني من وقته وجهده دعماً وتشجيعاً، فكنتم لي العون بعد الله في هذا المشوار.

وإلى قدوتي وسندي الدائم وأخي الكبير، سعادة القاضي ناصر جرار، الذي كان لي مثالًا في الحكمة والنزاهة، فغمرني بدعمه وعطائه وتوجيهاته السديدة، وكان لي العون في مسيرتي العلمية والمهنية، فله مني كل الامتنان والتقدير.

أهديكم جميعًا ثمرة جهدي، عرفانًا وتقديرًا، راجيًا من الله أن يوفقني لردّ جميلكم يومًا ما.

الطالب: وائل أحمد سيف عيد

# الشكر والتقدير

الحمد لله الذي وفقني وأعانني على إتمام هذه الرسالة، وأسأله سبحانه أن يجعلها علمًا نافعًا يُنتفع به.

أتقدم بخالص الشكر والتقدير إلى قدوتي وسندي الدائم وأخي الكبير، سعادة القاضي ناصر جرار، الذي كان لي عونًا وسندًا، فلم يبخل عليّ بتوجيهاته السديدة ودعمه وعطائه المستمر، فله مني كل الامتنان والتقدير.

كما أتوجه بأسمى آيات الشكر والعرفان إلى مشرفي القدير الدكتور عبد اللطيف ربايعة، الذي كان نِعم الدليل في مسيرتي البحثية، فقدم لي دعمه العلمي والفكري بصبرٍ وتفانٍ.

ولا يفوتني أن أعبر عن خالص امتناني إلى أعضاء لجنة المناقشة كل من الدكتور عصام الأطرش والدكتور محمد اشتية، الذين شرفوني بقراءة هذه الرسالة، وقدموا لي من علمهم وتوجيهاتهم ما أسهم في إثرائها وتحسينها. وكل الشكر والتقدير لأساتذتي الكرام في الجامعة، الذين نهلت من علمهم الكثير، فكان لهم بالغ الأثر في صقل مهاراتي الأكاديمية والبحثية.

وإلى أسرتي العزيزة، والديّ الكريمين، اللذين كانا لي النور الذي أستنير به، والدعامة التي أستند إليها في كل مراحل حياتي، وإلى إخوتي وأخواتي، الذين غمروني بمحبتهم ودعواتهم الصادقة.

وأخيرًا، لا أنسى كل من قدَّم لي يد العون والمساعدة، من زملاء وأصدقاء، فلكم جميعًا مني خالص الشكر والتقدير، وأسأل الله أن يجزيكم عني خير الجزاء.

# الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني (دراسة مقارنة)

**وائل احمد سيف عيد**

**د. عبد اللطيف ربايعة**

**د. عصام الأطرش**

**د. محمد اشتية**

## ملخص

ان الهدف الأساسي من هذه الدراسة هو التعرف على الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني دراسة مقارنة مع القانون الأردني والمصري، وقد استخدم الباحث في كتابة هذه الدراسة المنهج الوصفي التحليلي والمنهج المقارن، وقد توصلت هذه الدراسة إلى مجموعة من النتائج أبرزها غياب تعريف واضح وشروط موحدة لقبول الأدلة الرقمية أدى إلى تفاوت في تفسيرها وقبولها أمام المحاكم الفلسطينية، إن كل من التشريعات الفلسطينية والأردنية والمصرية تؤكد على حجية الأدلة الرقمية في الإثبات الجنائي، وقد تم التوصية في أن يقوم المشرع الفلسطيني بمواكبة إصدار قوانين شاملة وواضحة ومترابطة ومتكاملة تُعنى بتنظيم الأدلة الرقمية، مع وضع تعريف واضح للأدلة الرقمية مع تحديد شروط مشروعيتها وقبولها أمام المحاكم، بما يتماشى مع التطورات التقنية الحديثة، وكذلك تعزيز الضمانات القانونية لحماية الخصوصية أثناء عمليات جمع الأدلة الرقمية وتحليلها، مع وضع قيود صارمة على استخدامها بما يحقق التوازن بين تحقيق العدالة وحماية الحقوق الفردية.

الكلمات المفتاحية: الأدلة الرقمية، الأدلة الإلكترونية، الأدلة التقليدية، القانون.

## فهرس المحتويات

**مقدمة الدراسة:**

للتقدم التكنولوجي في جميع أنحاء العالم المتمثل بإستخدام الحواسيب والشبكات الإلكترونية وأنظمة الحماية، أنتج منافع متعددة سواء في مجالات البحث العلمي وتوثيق المعلومات وتخزينها والحصول على معلومات تيسيراً لأعمال القطاعين الخاص والعام، ولذلك أحدثت تغيرات جذرية ونوعية بمختلف مناحي الحياة، متمثلة في كون هذا التقدم التكنولوجي له دور كبير في كشف مرتكبي الجرائم وتوثيق لحظة إرتكاب هذه الجرائم من خلال إستخدام الحواسيب والشبكات الإلكترونية وأنظمة الحماية.

ولذلك وجب على الجهات المختصة أن تتصدى للجريمة والمجرمين بالتقدم التكنولوجي لما لهذا التقدم العلمي التكنولوجي الهائل دور مهم يساعد الجهات المختصة في كشف الجرائم ومرتكبيها ومكافحة الجرائم والمجرمين والحد من إرتكابها، وهذا يتطلب وجود أنظمة وقوانين تواكب هذا التطور العلمي والتكنولوجي لإثبات حقيقة الجريمة المرتكبة، ففي وقتنا الحاضر أصبحت الدول تعتمد على حوسبة وأتمتة أعمالها ونشاطاتها وإتصالاتها وتنظيم إدارتها والإشراف على حسن سير أعمالها من خلال نظام إلكتروني، وأصبحت هذه التكنولوجيا المتمثلة بالحواسيب والشبكة العالمية جزءاً من الحياة اليومية للأفراد ونشاطه الإجتماعي وتعامله، بحيث أنه لا يمكن الإستغناء عنها لتسهيل تسيير الحياة بشكل عام.

وكون الأدلة الرقمية عبارة عن معلومات مرسلة أو مخزنة كبيانات رقمية يمكن أن يستعملها أحد أطراف الدعوى، وقد تكون هذه الأدلة على شكل صور فوتوغرافية، أو صور الأقمار الاصطناعية أو فيديو أو تسجيل صوتي أو بريد إلكتروني، وقد تكون على شكل موقع إلكتروني أو أحد مواقع التواصل الإجتماعي مثل (*Facebook*) أو (*Twitter*)، ولذلك نظراً لتميز الأدلة الرقمية بطبيعة خاصة وأهميتها وضروريتها في كشف الجرائم ومرتكبيها، أصبح هناك ضرورة لوجود نصوص قانونية خاصة تنظمها بشكل واضح، لإتصالها ببيانات

وكلمات ورموز وأرقام سواء من حيث تجميعها وتخزينها وتجهيزها وإسترجاعها وتصحيحها وتعديلها ومحوها وطباعتها ونسخها، فهي تتم من خلال المعالجة الآلية للبيانات بهدف الحصول على المعلومات المرجوة، ومن خلال الطبيعة الخاصة بالأدلة الرقمية من حيث طريقة التحقيق وتحليلها وربطها والحصول عليها ومتابعتها من قبل خبراء تكنولوجيا المعلومات، فهي تمتاز بطبيعة مزدوجة ما بين الحصول على الدليل وتحليله واتصاله بالنص القانوني، فإثبات الأدلة الرقمية بحاجة الى إجراءات خاصة لمتابعتها بشكل يوائم ويتماشى مع التقنيات المستخدمة والمستحدثة ليتوافق مع الخصوصية التي تتميز بها.

كما أن عدم وجود خبرة كبيرة للهيئات القضائية المختصة بمجال الأدلة الرقمية يضعنا أمام معادلة غير متكافئة، طرفها الجهات القضائية بنقص خبراتها في مجال مواكبة التطور المعلوماتي في إرتكاب الجرائم الالكترونية، والطرف الآخر قراصنة ومجرمون يتمتعون بمهارات وخبرات فنية عالية يواكبون كل جديد.

ونتيجة التطور العلمي الهائل الذي يشهده العالم، وما نتج عن هذا التطور العلمي من وسائل علمية حديثة في أدلة الإثبات الجنائي ومن أهمها الأدلة الرقمية، حيث ساهم هذا التطور العلمي في إستحداث أساليب ووسائل يستند إليها القاضي الجزائي في تكوين قناعته الوجدانية في إيقاع العقاب وتجريم المجرمين بالإستعانة بالأدلة الرقمية، ولأهميتها في كشف الجرائم ومرتكبيها فيتم من خلال هذه الدراسة بيان حجية الأدلة الرقمية في الإثبات الجنائي الفلسطيني ومقارنةً بالتشريع الأردني والمصري.

**الكلمات المفتاحية للدراسة:**

- الأدلة الرقمية
- الأدلة الإلكترونية
- الأدلة التقليدية
- القانون
- الإثبات الجنائي
- مبدأ الشرعية
- الدليل الجنائي
- القضاء الجنائي

**مراجعة التراث العلمي للدراسة:**

في فلسطين لا يوجد كثير من الدراسات المتخصصة عن الأدلة الرقمية وحجيتها في الإثبات الجنائي بشكل متخصص ومباشر بل هي الدراسة المتخصصة بشكل في حجية إثبات الأدلة الرقمية في فلسطين أمام القاضي الجزائي ويوجد في فلسطين دراسة متعلقة بشروط قبول الأدلة الرقمية وبعض الدراسات القليلة جداً في القوانين العربية الأخرى وهذه الدراسات هي عبارة عن بحوث ومقالات، إلا إنه لا يمكن إعتمادها بشكل أساسي لإختلاف التكييف بين القانون الفلسطيني والقوانين العربية الأخرى ولعل أبرزها.

1. الدراسة الأولى: أحمد شهاب و نور بن ماني بعنوان شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي

الفلسطيني، بحوث ومقالات، المركز الجامعي أمين العقال الحاج موسى أق أخموك لتامنغست – معهد الحقوق والعلوم السياسية2018.

وقد ناقش الباحثين في هذه الدراسة شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني وتم التوصل إلى أن الأدلة الإلكترونية هي السبيل لتكوين اليقين القضائي سواء بالبراءة أو الإدانة في الجريمة الإلكترونية، ومما يعني أن هذه الدراسة متخصصة عن الجريمة الإلكترونية وعن شروط قبول هذه الأدلة الناتجة عن الجريمة الإلكترونية وتحدثت هذه الدراسة لخلو التشريع الفلسطيني من قانون خاص ينظم العقوبات والقواعد الإجرائية الخاصة بالجريمة الإلكترونية، ولكن في المقابل سيتم التحدث في موضوع دراستي عن حجية الأدلة الرقمية في الإثبات الجنائي الفلسطيني بشكل عام وليس بجريمة معينة وكذلك سيتم التحدث في موضوع دراستي عن حجية الأدلة الرقمية في الإثبات الجنائي الفلسطيني وليس شروط هذه الأدلة فقط، والأكثر أهمية في موضوع دراستي هو أنه تم صدور قرار بقانون خاص بالجرائم الإلكترونية هو القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته وهذا على خلاف الدراسة السابقة التي تم البحث فيها قبل صدور قانون خاص بالجرائم الإلكترونية سيما وأنه في موضوع دراستي سيتم البحث في بعض نصوص القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات المعدل بالقرارين بقانون رقم 28 لسنة 2020، ورقم 38 لسنة 2021 ومواد قانون الإجراءات الجزائية رقم 3 لسنة 2001 وتعديلاته، والتي شابها حالة من الغموض بشأن إثبات الأدلة الرقمية ومدى حجيتها أمام القضاء الجنائي الفلسطيني، وقد أتاحت تلك النصوص مجالاً للتأويل والتفسير لدى جهات السلطة القضائية.

2. الدراسة الثانية: عدنان حجار وفايز بشير بعنوان الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل، بحوث ومقالات، جامعة الإستقلال 2021.

وقد ناقش الباحثين في هذه الدراسة الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل وتم التوصل فيها إلى أن حجية الأدلة الجنائية في مجال الإثبات الجنائي مقيدة بمجموعة من الشروط أهمها حصول سلطات التحقيق على الأدلة الرقمية بطريقة مشروعة، وأن القاضي الجنائي يتمتع بالدور الإيجابي في تقدير القيمة القانونية للأدلة الرقمية مثلها مثل باقي الأدلة، وأن هناك ثغرات وفراغ تشريعي يعتري الدليل الرقمي.

3. الدراسة الثالثة: فرج نويرات بعنوان الإثبات بالأدلة الرقمية في المواد الجنائية، بحوث ومقالات، جامعة الزيتونة 2020.

وقد ناقش الباحثين في هذه الدراسة الإثبات بالأدلة الرقمية في المواد الجنائية وتم التوصل فيها إلى أن الإثبات هو إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقاً لمعيار الحقيقة الواقعية، وذلك أن للدليل أهمية كبيرة في المواد الجنائية، حيث تناول الباحث مدى إمكانية إثبات الجرائم بالأدلة الرقمية أمام القاضي الجنائي وفقاً للقانون الليبي وتوصل إلى إمكانية الأخذ بالدليل الرقمي أمام القاضي الجنائي وذلك كله وفقاً لمبدأ حرية القاضي الجنائي في تكوين عقيدته وهذا كله وفقاً لنص المادة 275 من قانون الإجراءات الجنائية الليبي.

**إشكالية الدراسة:**

لاحظ الباحث وجود عدد من المشكلات التي تتعلق بالمشكلة الأساسية للبحث والمتمثلة في الإستفهام الآتي: ما مدى حجية الأدلة الرقمية أمام القضاء الجنائي الفلسطيني؟

ويتبع المشكلة الأساسية مشكلات أخرى، وهي في بعض نصوص القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته المعدل بالقرارين بقانون رقم 28 لسنة 2020م، ورقم 38 لسنة 2021م ومواد قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته، والتي

شابها حالة من الغموض بشأن إثبات الأدلة الرقمية ومدى حجيتها أمام القضاء الجنائي الفلسطيني، وقد أتاحت تلك النصوص مجالاً للتأويل والتفسير لدى جهات السلطة القضائية. ونتج عن ذلك، خلاف حول تفسيرها؛ في الوقت الذي يشير فيه الواقع إلى غياب السوابق القضائية الفلسطينية بشأنها.

**أسئلة الدراسة:**

تثير هذه الدراسة تساؤل رئيسي، وهو: ما مدى حجية الأدلة الرقمية أمام القضاء الجنائي الفلسطيني؟ ويتفرع عن هذا التساؤل جملة تساؤلات تتمثل في الآتي:

- ما هي الطبيعة القانونية للأدلة الرقمية في الإثبات الجنائي في الجريمة؟ وكيفية معالجتها في التشريع الفلسطيني؟
- هل خرج القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته عن الأحكام العامة للإثبات الجنائي الواردة في قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته؟
- هل تعالج نصوص قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته المسائل المستحدثة بخصوص الحصول على الأدلة الرقمية؟
- هل يعتبر الدليل الرقمي من أدلة الإثبات الجنائي في الجرائم الإلكترونية والتقليدية على حد سواء؟
- ما الشروط الواجب إتباعها للحصول على الدليل الرقمي بصورة مشروعة؟
- ما مدى إعتبار الأدلة الرقمية المتحصل عليها من خلال جهات التحقيق الوطنية والأجنبية من أدلة الإثبات؟

**أهمية الدراسة:**

تكتسب هذه الدراسة أهمية نظرية بارزة من خلال تناولها لأحد أبرز المستجدات القانونية والمتمثلة في الأدلة الرقمية، والتي تتسم بحداثتها وضرورة وضع أطر تشريعية واضحة لتنظيم إستخدامها. وتسلط الدراسة الضوء على الحاجة إلى سياسة جنائية متخصصة لضمان التعامل السليم مع هذا النوع من الأدلة، خاصة في ظل التطورات التشريعية الأخيرة في فلسطين، مثل صدور القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية. وقد أثار هذا التشريع اعتراضات كبيرة من مؤسسات المجتمع المدني التي دعت إلى تعديله بما ينسجم مع المعايير الدولية واتفاقيات حقوق الإنسان، ولا سيما في مجال الإثبات بالأدلة الرقمية. وإستجابة لهذه المطالب تم إصدار القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته، متضمناً تعديلات جوهرية تعالج بعض الإنتقادات الموجهة للتشريع السابق، بما في ذلك إلغاء النصوص العامة والغامضة المتعلقة بوسائل الإثبات، مما يعكس أهمية الدراسة في تسليط الضوء على هذه التطورات وإبراز الحاجة إلى توافق التشريعات مع المتطلبات الدولية.

تتجلى الأهمية العملية لهذه الدراسة في معالجتها للممارسات التي قد تصاحب جمع الأدلة الرقمية من قبل جهات إنفاذ القانون، مع التركيز على مدى إلتزام هذه الجهات بالتحقق من قانونية هذه الأدلة وصلاحيتها للاستخدام أمام القضاء. وتُبرز الدراسة ضرورة وضع معايير واضحة ومحددة لضمان جمع الأدلة الرقمية بطريقة تُراعي الأطر القانونية والإجرائية، مما يُعزز من مصداقيتها ويُحافظ على حقوق الأفراد الأساسية أثناء تحقيق العدالة. وعلاوة على ذلك، تهدف هذه الدراسة إلى أن تكون مرجعاً علمياً وعملياً يستفيد منه كافة العاملين في المجال القانوني، بما في ذلك القضاة، وأعضاء النيابة العامة، والمحامون، والمستشارون القانونيون. وكما تسهم في إثراء معرفة الباحثين القانونيين وطلبة الجامعات من خلال توفير فهم معمق للقواعد التي تحكم جمع

الأدلة الرقمية وإستخدامها. وبذلك، تُسهم الدراسة في تطوير الممارسات القانونية المرتبطة بالأدلة الرقمية، وتدعم تحقيق التوازن بين مكافحة كافة الجرائم بشكل عام والجرائم الإلكترونية بشكل خاص وضمان إحترام المعايير الحقوقية والقانونية.

**أهداف الدراسة:**

أسباب إختيار الباحث لمشكلة الدراسة هي:

1. تبيان ماهية الطبيعة القانونية للأدلة الرقمية في الإثبات الجنائي وكيفية معالجتها في التشريع الفلسطيني.
2. مناقشة هل القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته خرج عن الأحكام العامة للإثبات الجنائي الواردة في قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته.
3. بيان هل نصوص قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته عالجت المسائل المستحدثة بخصوص الحصول على الأدلة الرقمية.
4. توضيح هل الدليل الرقمي يعتبر من أدلة الإثبات الجنائي في الجرائم الإلكترونية والتقليدية على حد سواء.
5. تحديد الشروط الواجب إتباعها للحصول على الدليل الرقمي بصورة مشروعة.
6. التعرف على مدى إعتبار الأدلة الرقمية المتحصل عليها من خلال جهات التحقيق الوطنية والأجنبية من أدلة الإثبات.

**حدود الدراسة:**

- الحدود الزمنية: سيتم إنجاز الدراسة من شهر 11 من عام 2023 إلى شهر 11 من عام 2024 أي سيتم إنجاز الدراسة بحد أقصى سنة واحدة.
- الحدود المكانية: ستجري هذه الدراسة في فلسطين كونها دراسة تحليلية لنصوص والتشريعات والإجتهادات القضائية الفلسطينية المتعلقة في موضوع الدراسة مع مقارنتها بالتشريعات المصرية والأردنية.

**أدوات الدراسة:**

نطاق الدراسة سيكون في النصوص والتشريعات الفلسطينية المتعلقة بالموضوع وخاصة القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات المعدل بالقرارين بقانون ذوات الأرقام 28 لسنة 2020م و 38 لسنة 2021م وقانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته، بالإضافة إلى الرجوع إلى الأحكام والإجتهادات القضائية الفلسطينية الصادرة بهذا الشأن، بالإضافة للنصوص القانونية الواردة عن الموضوع في التشريعات العربية المقارنة.

**منهجية الدراسة:**

سوف يتم إتباع المنهج الوصفي التحليلي والمنهج المقارن وذلك من خلال إستقراء وتحليل النصوص ذات العلاقة في التشريعات الجنائية الفلسطينية ومقارنتها بالتشريعات الأردنية والمصرية، وذلك من خلال رصد المشكلة وتجميع المعلومات القانونية وتحليل النصوص القانونية والإجتهادات القضائية والأراء الفقهية لإستنتاج أهم الأحكام المرتبطة بالموضوع.

**محددات الدراسة:**

1- تتناول الدراسة موضوع الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني وتحديد الأساس القانوني لهذه الأدلة سيما وأن بعض نصوص القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات المعدل بالقرارين بقانون ذوات الأرقام 28 لسنة 2020م، و 38 لسنة 2021م ومواد قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته، والتي شابها حالة من الغموض والإرباك بشأن إثبات الأدلة الرقمية، وقد سمحت تلك النصوص لتأويل كل جهة لها وفق رؤيتها.

2- بسبب حداثة الموضوع نتيجة التقدم التكنولوجي في العالم، أدّى ذلك لقلة في الدراسات القانونية والكتابات الفقهية حوله، وقلة الأحكام والقرارات القضائية فيها، وذلك يلقي عبئاً كبيراً على الباحث لمحاولة التأصيل النظري والتطبيق العملي للموضوع.

**تقسيم الدراسة:**

سوف نقوم بتقسيم الدراسة إلى فصلين بحيث يشتمل كل فصل على مبحثين وهي على النحو التالي:

الفصل الأول: ماهية الأدلة الرقمية في الإثبات الجنائي.

المبحث الأول: تعريف الأدلة الرقمية.

المطلب الأول: مفهوم الأدلة الرقمية.

المطلب الثاني: خصائص الأدلة الرقمية وأهميتها في الإثبات الجنائي.

المطلب الثالث: أنواع الأدلة الرقمية.

المبحث الثاني: الضبط الإجرائي للأدلة الرقمية.

## الفصل الأول: ماهية الأدلة الرقمية في الإثبات الجنائي

تعتبر الأدلة الجنائية الرقمية من الركائز الأساسية في عملية الإثبات الجنائي، لا سيما في ظل التطورات التكنولوجية المتسارعة. فهي تلعب دورًا محوريًا في إثبات وقوع الجريمة وتحديد المسؤولين عنها. ومع ذلك، تواجه هذه الأدلة تحديات قانونية وفنية معقدة تتطلب التعامل معها بدقة في إطار قانوني شامل. وفي هذا الفصل، سيتم إستعراض ماهية الأدلة الجنائية الرقمية وخصائصها وأنواعها، بالإضافة إلى الضبط الإجرائي للأدلة الرقمية ومصادرها، وذلك من خلال إجراء دراسة مقارنة بين القانون الجنائي في فلسطين، والأردن، ومصر.

### المبحث الأول: تعريف الأدلة الرقمية

تُعد الأدلة الرقمية من أبرز التطورات التقنية الحديثة التي أحدثت تأثيرًا جوهريًا في مجال الإثبات الجنائي. ومع التطور التكنولوجي المتسارع، أصبحت الأدلة الرقمية تؤدي دورًا رئيسيًا في عمليات التحقيق والمحاكمات الجنائية، حيث تسهم بشكل كبير في كشف الجرائم وملاحقة الجناة وتقديمهم للعدالة. وبناءً على ذلك، سيتم في هذا السياق التطرق إلى تعريف الأدلة الجنائية الرقمية ومفهومها بشكل أعمق.

#### المطلب الأول: مفهوم الأدلة الرقمية

لا بد لنا ومن الضروري أن نبدأ بتعريف مصطلح "الأدلة" و "الرقمية". ونبدأ بتعريف الأدلة لغةً: تُعرّف كلمة "الأدلة" في اللغة العربية بأنها جمع كلمة "دليل"، والتي تعني الإرشاد أو العلامة التي تساعد في إثبات شيء معين. وتستند الكلمة إلى الجذر اللغوي "دل"، الذي يشير إلى الإرشاد أو الإيضاح. وبالتالي، فإن الأدلة

تمثل وسائل تُظهر صحة أو حقيقة ما. (العبادي، 2010، ص66 ؛ ابن منظور، 1955، ص19)، والأدلة إصطلاحًا: تُعرّف الأدلة إصطلاحًا بأنها كل ما يُستخدم لإثبات حقيقة أو دعم إدعاء في السياقات القانونية أو القضائية. وتشمل هذه الأدلة الوثائق، الشهادات، والمعلومات التي قد تؤثر على قرار المحكمة أو سير التحقيق. وعادةً ما تُصنّف الأدلة إلى عدة أنواع، مثل الأدلة المادية، الشهادات، والأدلة الرقمية. (زكي، 1987، ص211 ؛ الشريف، 2002، ص129)، والأدلة قانونيًا: في المجال القانوني، تُعرّف الأدلة بأنها أي معلومات أو مواد تُقدم إلى المحكمة لدعم موقف قانوني أو إدعاء. ويجب أن تكون هذه الأدلة مقبولة قانونيًا، مما يعني أنها يجب أن تلتزم بمعايير محددة في ما يتعلق بجمعها وتحليلها، ويجب أن تكون ذات صلة بالموضوع المطروح في القضية. (الدراوشة، 2015، ص22 ؛ العجارمة،2019، ص23).

ونعرف الرقمية لغةً: تُشتق كلمة "رقمية" من كلمة "رقم"، التي تشير إلى الكمية أو القيمة التي تعبر عن شيء ما بصورة عددية. وتستند الكلمة إلى الجذر "رقم" الذي يدل على العد أو الإحصاء، لذا تشير الرقمية إلى تمثيل المعلومات بإستخدام الأرقام. (البشري، 2002، ص109)، والرقمية إصطلاحًا: تُستخدم كلمة "رقمية" للإشارة إلى البيانات أو المعلومات التي يتم تمثيلها أو معالجتها في شكل أرقام، وخاصة في السياقات التقنية والإلكترونية. ويعتبر هذا النوع من البيانات أساسياً في مجال الحاسوب والتكنولوجيا الحديثة، حيث تُستخدم الأرقام لتمثيل المعلومات بطريقة تسهل معالجتها وتحليلها. (أحمد، 2020، ص1082)، ويتضح أن هذا المصطلح يُترجم من الكلمة الإنجليزية (Digital). وفقًا لقاموس كامبردج، يُعرَّف بأنه "تسجيل أو تخزين المعلومات كسلسلة من الأرقام (0،1) من خلال إظهار أو إخفاء الإشارة". يُعرف هذان الرقمان (0،1) بالأرقام الثنائية أو بالنظام الثنائي، وهو النظام الذي تُسجل فيه جميع البيانات من حروف ورموز وأشكال وغيرها داخل الحاسوب. ويطلق على الرقم الواحد أو الصفر مصطلح (بايت ، Bit)، وبعبارة أخرى، يتم تحويل المعلومات

إلى أرقام لتخزينها في جهاز الحاسوب. وعلى سبيل المثال، يمثل الرقم 65 الحرف (A)، بينما يمثل الرقم 66 الحرف (B)، يُعبَّر عن الرقم 65 بالشكل الثنائي (01000001) والرقم 66 بالشكل (01000010)، في حين يُعبر عن أمر المسافة (Space) بين كلمتين بالرقم 32، الذي يُمثَّل بالشكل (00100000). وهكذا، تتحول الأرقام إلى معلومات يمكن تخزينها في جهاز الحاسوب أو أجهزة مماثلة، من خلال النظام الثنائي الذي يُعتبر كرمز يُترجم جميع المعلومات ويخزنها. (المناعسة و الزعبي، 2014، ص290 ؛ جيتس، 1998، ص40-46). والرقمية قانونيًا: قانونيًا تشير الرقمية إلى المعلومات التي تُخزن أو تُنقل إلكترونيًا، مثل البيانات المخزنة على أجهزة الحاسوب، والهواتف الذكية، والإنترنت. وتشمل الأدلة الرقمية جميع أنواع المعلومات الرقمية التي يمكن إستخدامها كأدلة في الإجراءات القانونية، وتعتبر هذه الأدلة حيوية بشكل خاص في قضايا الجرائم الإلكترونية، حيث تلعب دورًا رئيسيًا في إثبات التهم. (عوض، 1971، ص896).

أما فيما يخص تعريف الأدلة الرقمية في القانون الفلسطيني، يتضمن القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته والقرار بقانون رقم 17 لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة في فلسطين إشارات هامة ضمن نصوص كل قانون منهما إلى الأدلة الرقمية وأن هذه الإشارات هي ذاتها أنواع الأدلة الرقمية، على الرغم من عدم وجود تعريف محدد وصريح لها ضمن مواده. وتبرز هذه القوانين أهمية الأدلة الإلكترونية في سياق الجرائم المرتكبة عبر الإنترنت، حيث تعتبر ضرورية لتوفير الإثباتات اللازمة في التحقيقات الجنائية. ورغم أن النصوص القانونية لا تقدم تعريفًا واضحًا للأدلة الرقمية، إلا أنها تؤكد على الدور المركزي لهذه الأدلة في الإجراءات القانونية، مما يستدعي تنظيمها بشكل دقيق. ويتناول القانون مجموعة من المواد التي توضح كيفية التعامل مع الأدلة الرقمية، مع التركيز على ضرورة إتباع الإجراءات القانونية الصحيحة عند جمعها، بما في ذلك الحصول على إذن

قضائي مسبق وهذا ما تم النص عليه في المادة 58 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته " تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي.". وما نصت عليه المادة الأولى من القرار بقانون رقم 17 لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة "البيانات الإلكترونية: بيانات ممثلة أو مرمزة إلكترونيًا سواء على شكل نص أو رمز أو صوت أو صورة أو غيرها من أشكال الترميز." وعرف كذلك في نفس المادة "السند الإلكتروني: المحتوى النصي أو الصوتي أو المرئي أو السمعي أو البصري الذي تم إنشاؤه وتخزينه ومعالجته وتداوله بوسيلة إلكترونية."وتعكس هذه النقاط إلتزام المشرع الفلسطيني بحماية حقوق الأفراد وضمان سلامة الأدلة الرقمية، مما يحول دون أي تلاعب أو تعديل يمكن أن يطالها. وبالتالي، يُظهر القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته والقرار بقانون رقم 17 لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة أهمية الأدلة الرقمية في مكافحة الجرائم الإلكترونية بشكل خاص والجرائم الأخرى بشكل عام، ويعزز الإطار القانوني الذي ينظم إستخدامها لتحقيق العدالة الجنائية، رغم عدم تقديم تعريف محدد للأدلة الرقمية.

على الرغم من أن القانون الأردني رقم 17 لسنة 2023م لا يحتوي ضمن نصوصه على تعريف محدد للأدلة الرقمية، بل يركز على تنظيم ومعالجة الجرائم التي تُرتكب عبر الوسائل الإلكترونية والفضاء السيبراني. ويقوم القانون على مفهوم الأدلة الرقمية، الذي يشمل أي بيانات يتم جمعها من الأجهزة الإلكترونية، مثل الحواسيب، الهواتف المحمولة، والشبكات، أو أي وسيلة تقنية أخرى. ويعكس ذلك الدور الحيوي للأدلة الرقمية في جهود مكافحة الجرائم الإلكترونية وتنظيم الإجراءات القانونية المرتبطة بها، إلا أنه وفقًا لقانون الجرائم

الإلكترونية الأردني رقم 17 لسنة 2023م، يُعرَّف الأدلة الرقمية بأنها أي معلومات أو بيانات يتم الحصول عليها أو تخزينها أو معالجتها بطريقة إلكترونية، والتي يمكن إستخدامها في الإجراءات القانونية لإثبات أو نفي حدوث جريمة. وتعتبر هذه الأدلة جزءًا أساسيًا من التحقيقات الجنائية المتعلقة بالجرائم الإلكترونية، بما في ذلك الجرائم المرتكبة عبر الإنترنت مثل القرصنة، الإحتيال الإلكتروني.

تُعرف الأدلة الرقمية بشكل عام في القانون الأردني بأنها البيانات التي تُخزن وتُعالج على وسائط إلكترونية، والتي يمكن إستخدامها لتقديم الأدلة في القضايا الجنائية. ويتضمن القانون الأردني مجموعة من الإجراءات القانونية المنظمة لجمع الأدلة الرقمية، وتشمل إستخدام تقنيات التشفير وتوثيق كل خطوة في سلسلة الحفظ. ويطلب من المحققين الإلتزام بإجراءات دقيقة لضمان موثوقية الأدلة، مثل إعتماد تقنيات التحقق من الهوية الرقمية وتوثيق جميع التعديلات أو عمليات نقل البيانات، بهدف الحفاظ على سلامة الأدلة وضمان قبولها في المحاكم.

أما فيما يتعلق بالأدلة الرقمية في القانون المصري، يُعرَّف الدليل الرقمي وفقًا لقانون الإجراءات الجنائية المعدل والقوانين المتعلقة بالجرائم الإلكترونية. وحيث أن القانون المصري قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات نص في المادة الأولى منه على تعريف محدد للأدلة الرقمية "هو أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، ويمكن تجميعها وتحليلها بإستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.". وهذا التعريف يبرز أهمية الأدلة الرقمية كأداة حيوية في الإجراءات القانونية، حيث تلعب دورًا محوريًا في تحقيق العدالة وكشف الحقائق في القضايا الجنائية.

وكذلك ما نصت علية المادة 11 من قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات يدلل على إهتمام القانون المصري بالأدلة الرقمية ودورها في الإثبات الجنائي " يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية."، وأن هذه الشروط الفنية الواردة في اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات نصت عليها المادة 9 من اللائحة سيتم التحدث عنها في الفصل الثاني من هذه الرسالة عند التحدث عن حجية هذه الأدلة ومدى مشروعيتها.

وتتطلب القوانين المصرية ذات العلاقة بالأدلة الرقمية من المحققين إتباع إجراءات دقيقة لجمع وحفظ الأدلة الرقمية، بما في ذلك الحفاظ على سلسلة الحفظ وتوثيق جميع العمليات المتعلقة بالبيانات. ويعتبر إستخدام تقنيات التشفير وحماية البيانات عنصرًا أساسيًا في هذه الإجراءات، لضمان عدم وقوع أي تلاعب أو تعديل غير مصرح به. وتهدف هذه الإجراءات إلى ضمان سلامة الأدلة الرقمية وفاعليتها في المحاكمات، مما يسهم في تعزيز نزاهة العملية القضائية.

وتعتبر الأدلة الرقمية من الناحية النظرية كأي دليل آخر، حيث تمثل معلومات تُجمع لإثبات العلاقة السببية بين الوقائع والأشخاص بغرض إثبات المسؤولية القانونية. وقد عرَّفها قانون الشرطة والأدلة الجنائية في المملكة المتحدة بأنها "جميع المعلومات الموجودة على جهاز الحاسوب". (عليان و الدبسي، 2003، ص127). ونلاحظ أن هذا التعريف يقتصر على حصر الأدلة الرقمية في أجهزة الحاسوب، بينما عرَّفتها المجموعة العلمية للعمل بالأدلة الرقمية، التي تضم دائرة مختبرات الجريمة الفيدرالية في واشنطن، في عام 1998 بأنها: "أي معلومات ذات قيمة إثباتية تُخزن في شكل ثنائي" – وقد تم لاحقًا تعديل المصطلح من

"ثنائي" إلى "رقمي". تشمل هذه الأدلة أدلة أجهزة الحاسوب، الفيديو الرقمي، الصوت الرقمي، أجهزة الفاكس الرقمية، الهواتف المحمولة، المواقع الإلكترونية، وغيرها. (جيتس، 1998، ص40–46). ونلاحظ أن هذا التعريف جاء أوسع من سابقه.

وهناك من يُعرِّف الأدلة الرقمية بأنها "معلومات وبيانات ذات قيمة للتحقيق، تُخزن على جهاز إلكتروني، أو تُستلم أو تُرسل بواسطة جهاز إلكتروني، ويتم الحصول عليها من خلال الحجز على الأجهزة الإلكترونية وتأمين بياناتها للفحص". وفي حين عرَّفها آخرون بأنها "البيانات الرقمية التي يمكن أن تثبت إرتكاب جريمة ما، وتعزز الصلة بين الجريمة وضحاياها أو بين الجريمة ومرتكبها". ومن الأمثلة على هذه الأدلة البيانات الموجودة في ذاكرة الحاسوب أو القرص الصلب أو الهاتف المحمول. (المناعسة والزعبي، 2014، ص290).

والأدلة الرقمية تُعرف أيضاً على أنها المعلومات أو البيانات التي تُخزن أو تُنقل إلكترونيًا، والتي يمكن الإعتماد عليها في إثبات الوقائع أو الأحداث المتعلقة بالجرائم الجنائية. ووفقًا لهذا التعريف فإن الأدلة الرقمية تشمل كافة البيانات والمعلومات المستخرجة والمحللة من الأنظمة الإلكترونية، مثل أجهزة الكمبيوتر، الهواتف الذكية، والشبكات الرقمية، والتي يمكن تقديمها كأدلة أمام المحاكم الجنائية. ومن جانب آخر تُعتبر الأدلة الرقمية معلومات تُجمع وتُخزن بإستخدام التكنولوجيا الرقمية، وتُستخدم لإثبات وقائع معينة في القضايا الجنائية. تشمل هذه الأدلة البيانات المحفوظة على الأجهزة الإلكترونية مثل الحواسيب والهواتف الذكية، مما يجعلها أداة أساسية في كشف الجرائم وتقديم الأدلة أمام المحاكم. (أحمد، 2020، ص1084).

والأدلة الرقمية تشمل كافة أنواع المعلومات المستخرجة من الأجهزة الإلكترونية ذات الصلة بالقضية المطروحة أمام القضاء. وتشمل هذه الأدلة، على سبيل المثال، رسائل البريد الإلكتروني، الملفات المحفوظة

على أجهزة الكمبيوتر، البيانات المستخرجة من الهواتف الذكية، وتسجيلات الكاميرات الرقمية. وتعد هذه الأدلة ذات أهمية كبيرة لما تتمتع به من قدرة على تقديم توضيح دقيق ومفصل للحقائق المرتبطة بالجريمة. (إبراهيم، 2010، ص214) (أبو القاسم، 2013، ص185).

وفي الصدد نفسه قد تطرح تساؤلات منها: لما كان هناك مسميات كالأدلة الإلكترونية أو أدلة الحاسوب، فهل يقصد بهذه الأدلة المعنى ذاته المتجسد بالأدلة الرقمية؟ وهل يدخل الدليل الناتج عن المواقع الإلكترونية في إطار الأدلة الإلكترونية أم الرقمية؟

ويستخلص الباحث بالنتيجة بأن دليل الحاسوب يعرف أحياناً بالدليل الإلكتروني، والأدلة الإلكترونية تشمل الأدلة التي يتم إنشاؤها وإنتاجها بواسطة الحاسوب، ومخرجاته، والأدلة المستندة إليه، والأدلة المرتبطة به، وجميع البيانات والمستندات الإلكترونية، وبشكل عام يمكن أن تشمل الأدلة الإلكترونية أي بيانات يتم إنشاؤها أو تخزينها في شكل رقمي بإستعمال جهاز الحاسوب. وعليه فإننا نعرف الأدلة الرقمية بأنها: "عبارة عن معلومات مرسلة أو مخزنة كبيانات رقمية يمكن أن يستعملها أحد أطراف الدعوى، وقد تكون هذه الأدلة على شكل صور فوتوغرافية أو صور الأقمار الإصطناعية أو فيديو أو تسجيل صوتي أو بريد إلكتروني، أو تكون على شكل موقع إلكتروني أو أحد مواقع التواصل الاجتماعي مثل ( Facebook أو Twitter)".

وفي هذا السياق يصح القول أن الأدلة الرقمية هي أوسع نطاقاً من الأدلة الإلكترونية، إذ أنها تشتمل فضلاً عن الأخيرة على ما ذكر في تعريف الأدلة الرقمية المذكورة آنفاَ.

أما على الصعيد الدولي فلم يكن هناك إتفاق على تعريف موحد سواء كان ما تعلق بالأدلة الإلكترونية أم بالأدلة الرقمية، وخصوصاً بعد المحاولة التي جرت في المؤتمر الذي عقد في مدريد في 14 كانون الأول 2006 من قبل الجمعية الأوروبية لخبراء الطاقة ، بشأن مشروع قبول الأدلة الإلكترونية في إجراءات المحاكم،

إذ لم يستطع هذا المشروع التوصل إلى تعريف موحد للأدلة الإلكترونية أو الرقمية، وبالرغم من ذلك لا يعد هذا التعريف ضرورياً في الإجراءات القانونية، لأن معظم السلطات القضائية في أغلب الدول تتعامل مع الأدلة الإلكترونية أو الرقمية كشكل من أشكال المستند، ويقصد بهذا الأخير: "أي شيء يسجل بأي شكل كان، ومُسْتَوفٍ لشروط المقبولية". وقد عرفت المحكمة الجنائية الدولية لرواندا (المستند) على نطاق واسع في قضية المدعي العام ضد ألفرد موسما إذ قالت: "يقصد بالمستند أي شيء يتم تسجيل المعلومات فيه، من أي وصف كان". وهذا التعريف واسع بما يكفي ليشمل فضلاً عن الوثائق الخطية، الخرائط والرسومات والخطط والرسوم البيانية والسجلات الحاسوبية والمواقع الإلكترونية والسجلات الكهرومغناطيسية والسجلات الرقمية وقواعد البيانات والمسارات الصوتية والأشرطة الصوتية وأشرطة الفيديو والشرائح والصور الفوتوغرافية وصور الأقمار الإصطناعية. (سفيان أبو زهيرة رئيس نيابة الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات، تواصل شخصي، 2024/11/17).

ويرى الباحث أن وسائل الإثبات الرقمية، ما هي إلا إمتداد وإستمرار للأدلة الخطية أو الكتابية لكن بوجهٍ متطور، لذا من المفترض أن تستجيب المحاكم الوطنية بشكل جيد ومستمر لما يطرأ من تطورات في جميع المجالات، من أجل توضيح ذلك لأغراض العدالة.

ويرى الباحث من خلال مراجعة التعريفات المتنوعة للأدلة الرقمية، سواء من الناحية النظرية أو من النصوص القانونية في القوانين الأردنية والمصرية، أن هذه الأدلة تُعد عنصرًا أساسيًا في التحقيقات الجنائية الحديثة، بسبب الإرتباط الوثيق بين الجرائم والتكنولوجيا المتقدمة. وتعتبر الأدلة الرقمية بمثابة تطور للأدلة الخطية أو الكتابية، رغم عدم وجود تعريف موحد لها في مختلف القوانين. ومع ذلك، تتفق جميع التعريفات على أن الأدلة الرقمية تشمل المعلومات والبيانات المستخرجة من أجهزة الحاسوب أين كان شكلها سواء صور

أو فيديو، والوسائط الإلكترونية، والأجهزة الذكية مثل الهواتف المحمولة، وأجهزة التخزين، والشبكات، والتي يمكن إستخدامها كأدلة في التحقيقات الجنائية والإثبات أمام المحاكم. ومن جانب آخر، يُشير الباحث إلى أن القانون الأردني رقم 17 لسنة 2023، رغم عدم تقديمه لتعريف محدد ودقيق للأدلة الرقمية، يُظهر إهتمامًا ملحوظًا بتنظيم إستخدام الأدلة المستخرجة من الوسائل الإلكترونية لمواجهة الجرائم المتزايدة في الفضاء السيبراني. وبينما يُعد قانون الإجراءات الجنائية المصري المعدل بالإضافة إلى القوانين المتعلقة بالجرائم الإلكترونية قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات، أكثر وضوحًا من القانون الفسطيني والأردني في تحديد مفهوم واضح وصريح للأدلة الرقمية وتعزيز إستخدامها في مكافحة الجرائم التقنية.

**المطلب الثاني: خصائص الأدلة الرقمية وأهميتها في الإثبات الجنائي**

تُعد الأدلة الرقمية من أبرز العناصر في مجال التحقيقات الجنائية الحديثة، نظرًا للتطور الملحوظ في تكنولوجيا المعلومات وإستخداماتها المتنوعة في الحياة اليومية. نشأت هذه الأدلة كإستجابة لإنتشار الجرائم الإلكترونية، مما جعلها جزءًا أساسيًا في عمليات جمع الأدلة والإثبات في القضايا الجنائية. وتتميز الأدلة الرقمية بخصائص فريدة تجعلها تختلف عن الأدلة التقليدية، حيث توفر تفاصيل دقيقة وشاملة حول الأحداث والوقائع المرتبطة بالوسائل التكنولوجية. وبالإضافة إلى ذلك، فإن سهولة تخزينها ومعالجتها، وإمكانية نقلها عبر الإنترنت دون أن تتأثر طبيعتها، يزيد من قيمتها كأدلة. ولذلك، يتطلب التعامل مع هذه الأدلة دقة عالية في جمعها وتحليلها لضمان عدم التلاعب بها، ولضمان صلاحيتها كأدلة قانونية موثوقة في المحاكم.

وبالتالي تتميز الأدلة الرقمية بالعديد من الخصائص التي تجعلها فريدة ومتميزة، ومن أهم هذه الخصائص:

1. **الطبيعة غير الملموسة للأدلة الرقمية**

تُعتبر الأدلة الرقمية غير ملموسة بطبيعتها، حيث تتواجد في شكل بيانات أو معلومات إلكترونية لا يمكن رؤيتها أو لمسها بشكل مباشر. ونظراً الطبيعة غير الملموسة فإنه يجعل من الصعب تقييم مصداقية الأدلة الرقمية بالمقارنة مع الأدلة التقليدية، مما يستلزم إستخدام تقنيات تحليل متقدمة للتحقق من صحتها. وتبرز هذه التحديات أهمية إعتماد منهجيات دقيقة ومتطورة لضمان موثوقية الأدلة الرقمية وقابليتها للإستخدام في الإجراءات القانونية. ومن جانب آخر، تُعتبر الأدلة الرقمية دليلاً غير ماديًا، إذ تظل غير ملموسة بطبيعتها. وحتى وإن تم إستخراجها في شكل مادي، فإنها لا تفقد صفاتها الأساسية، حيث تُعتبر عملية الإستخراج مجرد نقل من الطبيعة الرقمية غير الملموسة إلى هيئة صلبة أو ملموسة يمكن إستخدامها للإشارة إلى معلومة معينة، تُظهر الأدلة الرقمية عدم إمكانية إدراكها بواسطة الحواس العادية، مما يتطلب الإعتماد على خبراء وأجهزة متخصصة مثل الحاسوب، بالإضافة إلى أدوات خاصة مثل الطابعات والكاميرات الرقمية. وكما قد يتطلب تحليلها بعض البرامج الحاسوبية المعقدة. (أرحومة ، 2009، ص3).

2. **إمكانية النسخ والنقل بسهولة**

تتميز الأدلة الرقمية بإمكانية نسخها ونقلها بسهولة، مما يتيح الإحتفاظ بنسخ متعددة من نفس الدليل في مواقع مختلفة دون أن تفقد هذه النسخ أصالتها. فتوفر هذه الخاصية إمكانيات واسعة لتخزين الأدلة، وفي الوقت ذاته تثير مخاوف بشأن إمكانية التلاعب بها. ولذا، فإن هذه الخصوصية في الأدلة الرقمية تؤكد على ضرورة إتخاذ تدابير صارمة لضمان سلامتها وحمايتها من أي تدخل غير مشروع. وقد تكون

الأدلة الرقمية ذات حجم كبير جدًا، خاصةً في الحالات التي تتضمن بيانات من شبكات أو خوادم واسعة. ويشكل هذا الحجم الكبير تحديًا عند جمع الأدلة الرقمية وتحليلها، بحيث يتطلب ذلك إمكانيات تخزينية متقدمة وتقنيات متطورة لفحص البيانات وإستخراج المعلومات ذات الصلة. وتسلط هذه التحديات الضوء على الحاجة الملحة لتطوير إستراتيجيات فعّالة للتعامل مع كميات هائلة من البيانات، مما يضمن تحقيق العدالة بشكل فعّال. (عزت، 2010، ص655).

### 3. قابلية التلاعب والتغيير

تتعرض الأدلة الرقمية لخطر كبير من التلاعب والتغيير، حيث يمكن تعديلها أو حذفها أو إستبدالها دون أن تترك آثارًا واضحة. وتعتبر هذه القابلية للتلاعب تحديًا كبيرًا أمام السلطات القضائية، مما يستدعي إتخاذ إجراءات صارمة لضمان صحة الأدلة وسلامتها، يشمل ذلك توثيق سلسلة الحيازة بدقة وإستخدام أدوات تقنية متخصصة. وتبرز هذه التحديات أهمية تطوير إستراتيجيات فعّالة لضمان سلامة الأدلة الرقمية وموثوقيتها في الإجراءات القانونية. (حنفي، 2017، ص19-22).

### 4. يعد دليلاً عابراً للحدود

يمكن أن تتواجد الأدلة الرقمية في مجموعة واسعة من المصادر، بما في ذلك الأجهزة الشخصية مثل الحواسيب والهواتف الذكية، وكذلك الخوادم، وقواعد البيانات، ووسائل التواصل الإجتماعي، والبريد الإلكتروني، وغيرها. مما يستلزم هذا التنوع الكبير في مصادر الأدلة الرقمية فهمًا عميقًا للبيئة الرقمية، بالإضافة إلى إتخاذ إجراءات محددة لجمع الأدلة من كل فئة من هذه المصادر. وتظهر هذه الحاجة إلى أساليب مخصصة التعقيدات التي يواجهها المحققون عند التعامل مع الأدلة الرقمية، مما يساعد في ضمان

الحصول على معلومات دقيقة وموثوقة. وتتمتع الأدلة الرقمية بخاصية الإرتباط الزمني والمكاني، حيث تحمل توقيعات تشير إلى الوقت والمكان الذي تم فيه إنشاؤها أو تعديلها. تلعب هذه الخصائص دورًا حيويًا في إثبات الأنشطة غير القانونية وتحديد هوية الفاعلين في تلك اللحظات والأماكن المحددة. وتعزز هذه السمات من فعالية الأدلة الرقمية في التحقيقات الجنائية وتساعد في بناء قضايا قوية تُستخدم أمام المحاكم. (العربي، 2016، ص71).

### 5. إمكانية التشفير وحماية الخصوصية

تتمتع الأدلة الرقمية بميزة التشفير، مما يجعل الوصول إلى محتوياتها أو قراءتها أمرًا صعبًا دون إستخدام مفاتيح فك التشفير الصحيحة. ويعتبر التشفير تحديًا كبيرًا في جمع الأدلة الرقمية وتحليلها، حيث قد يتطلب الأمر تعاونًا دوليًا وإستخدام تقنيات متطورة لفك التشفير، وذلك دون المساس بحقوق الخصوصية. وتسلط هذه التحديات الضوء على ضرورة تطوير إستراتيجيات فعالة تلتزم بالمعايير القانونية والأخلاقية لضمان تحقيق العدالة. (حنفي، 2017، ص20-22).

### 6. قابلية التحليل بإستخدام البرمجيات المتقدمة

يمكن إستخدام برامج وأدوات متقدمة لتحليل الأدلة الرقمية، مما يتيح إمكانية إسترجاع البيانات المحذوفة أو المفقودة، وتحليل الأنماط، وإكتشاف الأنشطة المشبوهة. وتعزز هذه القدرة على التحليل البرمجي من فهم الجرائم الإلكترونية وتتبع الجناة، ولكنها تتطلب أيضًا موارد تقنية وبشرية متخصصة. ويظهر هذا الأمر الحاجة الملحة لتوظيف خبراء في مجال تحليل البيانات لضمان فعالية التحقيقات وتقديم الأدلة بشكل موثوق أمام المحاكم. (حنفي، 2017، ص19-22).

وبالنظر إلى خصائص الأدلة الرقمية في كل من القانون الأردني والمصري، نجد أن كل من القانون الأردني والمصري يعترف بمميزات وخصائص الأدلة الرقمية المذكورة جميعها. ولذلك، تم وضع إستراتيجيات محددة ميزه عن غيره من القوانين لضمان مصداقية هذه الأدلة أثناء المحاكمة، بما في ذلك توثيق سلسلة الحيازة وإستخدام تقنيات متقدمة في التحليل والحماية. وعلى الجانب الآخر، يركز القانون المصري أيضًا على الخصائص الفريدة للأدلة الرقمية، ويعزز أهمية إتباع إجراءات دقيقة لجمعها وتحليلها، لضمان عدم التلاعب بها والحفاظ على صحتها كأدلة قانونية موثوقة.

ويتم التعاطي مع الخصائص الفريدة للأدلة الرقمية في التشريع الأردني من خلال وضع إستراتيجيات قانونية لضمان سلامتها:

- **إجراءات الحفظ** :تشمل الإجراءات التقنية المعتمدة التشفير والتوقيع الرقمي كوسائل لضمان حماية البيانات من التلاعب. وتفرض القوانين الأردنية إستخدام تقنيات الحماية المناسبة للحفاظ على سلامة الأدلة الرقمية وضمان موثوقيتها في الإجراءات القانونية. وتسهم هذه الإجراءات في تعزيز الثقة بالأدلة المقدمة أمام المحاكم وتساعد في التصدي للتحديات المتعلقة بالتلاعب أو التعديل غير المصرح به. (الصغير، 2002، ص111).
- **توثيق سلسلة الحفظ** :يُلزم القانون الأردني توثيق جميع مراحل جمع وتخزين وتحليل الأدلة الرقمية، وذلك لضمان عدم تعرضها لأي تلاعب. وتشمل هذه العملية تسجيل الوقت والتاريخ والمكان، بالإضافة إلى توثيق هويات الأفراد الذين شاركوا في التعامل مع البيانات. ويهدف هذا التوثيق إلى ضمان سلسلة الحيازة وسلامة الأدلة، مما يعزز من مصداقيتها ويزيد من فرص قبولها كأدلة قانونية في المحكمة. (العازمي، 2012، ص421).

وتتضمن خصائص الأدلة الرقمية في القانون المصري جوانب تتعلق بحماية البيانات وكيفية إدارتها لضمان عدم تعرضها للتلاعب. ويركز القانون على ضرورة إتباع إجراءات دقيقة عند جمع وتحليل الأدلة الرقمية، بما في ذلك توثيق كافة العمليات المرتبطة بها. وبالإضافة إلى ذلك، يدعم إستخدام تقنيات حماية مثل التشفير، مما يسهم في تأمين سلامة الأدلة وزيادة موثوقيتها في الإجراءات القانونية.

وعلى الرغم من أنه نجد أن القانون المصري يعترف بمميزات وخصائص الأدلة الرقمية المذكورة جميعها إلا أنه يتميز القانون المصري بتناول الخصائص الخاصة بالأدلة الرقمية جميعها من خلال:

- **حماية البيانات** :يلزم القانون المصري تأمين البيانات ضد التلاعب والتعديل غير المصرح به عبر إستخدام تقنيات متطورة في جمع وتحليل الأدلة. ويتضمن ذلك تطبيق أساليب مثل التشفير وتقنيات التحقق من الهوية لضمان سلامة الأدلة الرقمية وحمايتها من أي تدخل غير قانوني. وتساهم هذه الإجراءات في تعزيز موثوقية الأدلة المقدمة أمام المحاكم وتضمن صلاحيتها للإستخدام القانوني. (بهنوس، 2017، ص185).

- **إجراءات جمع الأدلة** :تنص القوانين المصرية على ضرورة إتباع إجراءات دقيقة لجمع الأدلة الرقمية وتوثيقها، بما في ذلك إستخدام أدوات التحليل والتوثيق لضمان سلامتها ومنع العبث بها. تشمل هذه الإجراءات توثيق كافة مراحل عملية جمع الأدلة، بما في ذلك الوقت والتاريخ والمكان، إلى جانب هويات الأفراد المشاركين في هذه العملية. وتهدف هذه التدابير إلى تعزيز مصداقية الأدلة الرقمية وضمان قبولها في الإطار القانوني. (عبد العال، 2021، ص685-686).

وبدراسة خصائص القوانين المقارنة الفلسطيني والأردني والمصري موضوع الدراسة وكونهم يعترفان بنفس خصائص الأدلة الرقمية وبالتالي تكون لهذه القوانين نفس الأهمية للخصائص المميزة للأدلة الرقمية في الإثبات الجنائي وتتمثل هذه الأهمية بتعزيز الخصائص الفريدة للأدلة الرقمية بشكل كبير فعالية التحقيقات الجنائية، حيث تلعب دورًا محوريًا في تحديد هوية الجناة وتحليل الأنشطة الإجرامية، فضلاً عن تتبع الإتصالات والمعاملات المالية غير القانونية. وكما تمكن الأدلة الرقمية المحققين من الوصول إلى معلومات دقيقة وسريعة حول الجرائم المرتكبة، مما يُسهم في تحسين كفاءة التحقيقات ودعم تحقيق العدالة. وتساهم هذه الخصائص أيضًا في تعزيز القدرة على التعامل مع الجرائم المعقدة في العصر الرقمي، مما يسهل بناء قضايا قانونية قوية. (أحمد، 1994، ص179).

إضافةً إلى ذلك، تلعب خصائص الأدلة الرقمية، مثل سهولة تحليلها وتوافرها من مصادر متعددة، دورًا هامًا في تعزيز قدرة الجهات الأمنية على ربط الأنشطة المشبوهة عبر الحدود الجغرافية وتتبع الشبكات الإجرامية المعقدة. ويعتبر التنوع الكبير لمصادر الأدلة الرقمية وسهولة نقلها وتحليلها عوامل حاسمة تجعلها أداة فعالة للغاية، لا سيما في مواجهة الجرائم الجنائية بشكل عام والجرائم الإلكترونية بشكل خاص. ويظهر ذلك أهمية التعاون الدولي في التصدي للتحديات المرتبطة بالجرائم الرقمية، ويبرز الدور الحيوي للأدلة الرقمية في تعزيز الأمن والسلامة العامة. (الصغير، 2002، ص11) (نجيب، 2014، ص150).

ويرى الباحث ومن خلال إستعراض خصائص الأدلة الرقمية، يتجلى دور خصائص الأدلة الرقمية في تعزيز العدالة وكشف الجريمة، خاصة في ضوء التطورات التكنولوجية السريعة والزيادة الملحوظة في الجرائم الإلكترونية. تُعد هذه الأدلة فريدة بسبب طبيعتها غير الملموسة، مما يستدعي الإستعانة بتقنيات تحليل متطورة للتحقق من صحتها. كما أن سهولة نسخها ونقلها تمنح مرونة في عملية جمع الأدلة، لكنها في الوقت نفسه

ترفع من خطر التلاعب بها. وتفرض القابلية العالية للتلاعب والتغيير ضرورة إتخاذ الحيطة من قبل الجهات القضائية، مما يتطلب وضع إستراتيجيات دقيقة لضمان سلامة الأدلة. وعلاوة على ذلك، تعكس الكميات الضخمة من البيانات وتنوع مصادرها التحديات التي تواجه المحققين، مما يستدعي تطوير إستراتيجيات فعالة لإدارة وتحليل كميات هائلة من المعلومات. وتشمل هذه الخصائص أيضًا إمكانية التشفير، مما يجعل الوصول إلى البيانات أمرًا صعبًا دون توفر المفاتيح المناسبة، مما يستلزم التعاون الدولي وتطبيق تقنيات متطورة. ويبرز ذلك أهمية الإلتزام بالمعايير القانونية أثناء جمع الأدلة. وعند مقارنتنا بالقوانين الأردنية والمصرية، نجد أن كلا البلدين يعترفان بهذه الخصائص جميعها ويعتمدان إستراتيجيات محددة لحماية الأدلة الرقمية وضمان مصداقيتها، مما يعزز العدالة في الإجراءات القانونية. وتعتبر الإجراءات المتبعة، مثل توثيق سلسلة الحيازة وحماية البيانات، ضرورية لضمان سلامة الأدلة الرقمية وفاعليتها في المحاكم.

أما بالنسبة لأهمية الخصائص المميزة للأدلة الرقمية في الإثبات الجنائي فإن الباحث يرى ومن خلال دراسة أهمية خصائص الأدلة الرقمية في التحقيقات الجنائية، تعتبر الخصائص المميزة للأدلة الرقمية أساسية في تعزيز فعالية التحقيقات الجنائية، حيث تلعب دورًا محوريًا في تحديد هوية الجناة وتحليل الأنشطة الإجرامية بدقة وسرعة. وتتيح سهولة تحليل هذه الأدلة وتنوع مصادرها للجهات الأمنية إمكانية ربط الأنشطة المشبوهة عبر الحدود وتتبع الشبكات الإجرامية المعقدة، مما يعزز من قدرتها على مواجهة التحديات المتعلقة بالجرائم الجنائية بشكل عام والجرائم الإلكترونية بشكل خاص. ويبرز الباحث أهمية التعاون الدولي والتطوير المستمر لإستراتيجيات قانونية وتقنية متطورة تتماشى مع تطور الأدلة الرقمية، وذلك لضمان تحقيق العدالة بكفاءة وفاعلية.

**المطلب الثالث: أنواع الأدلة الرقمية**

تتنوع الأدلة الرقمية بناءً على طبيعتها ومصدرها وطريقة الحصول عليها. ويمكن تصنيف هذه الأدلة إلى عدة أنواع رئيسية، تشمل:

1. **البيانات المخزنة:**

تشمل البيانات المخزنة تلك المعلومات المحفوظة على وسائط التخزين الرقمية مثل الأقراص الصلبة، الأجهزة المحمولة، بطاقات الذاكرة، والخوادم. وتتضمن هذه البيانات ملفات نصية، صورًا، مقاطع فيديو، رسائل بريد إلكتروني، ومستندات إلكترونية. وتعتبر البيانات المخزنة من أكثر أنواع الأدلة الرقمية إستخدامًا وشيوعًا في التحقيقات الجنائية، نظرًا لما تحتويه من معلومات مهمة تتعلق بالأحداث والأشخاص المرتبطين بالقضية. وتتميز هذه البيانات بأنها تقدم سجلًا دقيقًا للأنشطة والمعلومات، مما يجعلها أدلة قوية سواء لإثبات الجرائم أو لدحض الإتهامات. وتجدر الإشارة إلى أن التعامل مع هذه البيانات يستلزم اتباع إجراءات قانونية دقيقة تضمن الحفاظ على سلامتها وصلاحيتها كأدلة قانونية، بما في ذلك تأمينها من أي تلاعب أو تعديل خلال مراحل جمعها وتحليلها. (القاضي، 2022، ص192 ؛ الحمداني، 2016، ص12).

2. **البيانات المنقولة:**

تشمل البيانات المنقولة جميع المعلومات التي يتم تبادلها عبر شبكات الإتصالات، سواء كانت تلك الشبكات الإنترنت أو الشبكات المحلية. وتتضمن هذه البيانات محادثات الرسائل الفورية، التسجيلات الصوتية، ورسائل البريد الإلكتروني أثناء إنتقالها بين الأطراف المعنية. وتعتبر البيانات المنقولة مهمة

للغاية في قضايا الجرائم الإلكترونية، إذ يمكن أن تُستخدم لإثبات التواصل غير المشروع بين المتورطين في الجريمة. وتتميز هذه البيانات بإمكانية الوصول السريع إليها وقدرتها على توفير أدلة لحظية تتعلق بالنشاط الإجرامي. ومع ذلك، فإن التعامل معها يتطلب أدوات وتقنيات متخصصة لضمان سلامتها وتوثيقها بدقة، حيث إن أي فقدان أو تعديل في هذه البيانات قد يؤثر على صلاحيتها كأدلة أمام المحكمة. ومن الضروري أيضًا مراعاة القوانين المتعلقة بالخصوصية عند جمع هذه البيانات، لضمان حماية حقوق الأفراد وعدم انتهاكها. (بهنوس، 2017، ص178–179).

3. **البيانات المسترجعة:**

تشير البيانات المسترجعة إلى المعلومات التي تم إستعادتها من الأجهزة بعد أن تم حذفها أو إتلافها عمدًا أو بغير قصد. وغالبًا ما تتطلب هذه الأدلة تقنيات متقدمة لإستعادتها، مثل إستخدام البرمجيات المتخصصة في إسترجاع البيانات المحذوفة. وتعد البيانات المسترجعة من الأدلة القوية التي يمكن أن تُظهر النية الإجرامية لدى المتهمين، خصوصًا في حالات محاولات إخفاء الأدلة. تلعب هذه البيانات دورًا مهمًا في التحقيقات الجنائية، حيث يمكن أن تكشف عن أنشطة مشبوهة أو معلومات حساسة تم حذفها عمدًا من قبل الجاني. ويتطلب إسترجاع هذه البيانات دقة عالية وخبرة فنية، لضمان عدم التلاعب بها أو فقدان أي معلومات مهمة. ولذا، تعتبر الأدلة المسترجعة من العناصر الحيوية التي يمكن أن تؤثر بشكل كبير على نتائج القضايا الجنائية. (الجاسم، 2021، ص176–177).

### 4. سجلات النظام:

تشمل سجلات النظام جميع الأنشطة والعمليات التي تحدث داخل الأجهزة الرقمية، مثل سجلات الدخول والخروج، سجلات التصفح، وسجلات العمليات المتنوعة. وتلعب هذه السجلات دورًا حيويًا في تحديد تصرفات الجناة وتعقب أنشطتهم على الأنظمة الرقمية. وكما تعتبر سجلات النظام أداة أساسية في التحقيقات الجنائية، حيث توفر معلومات دقيقة حول التفاعلات والأحداث التي وقعت ضمن النظام. من خلال تحليل هذه السجلات، يتمكن المحققون من التعرف على الأنماط السلوكية للجناة وإكتشاف أي تلاعب أو دخول غير مصرح به. وبالتالي، تمثل سجلات النظام دليلاً موثوقًا يمكن الإعتماد عليه في المحاكم لإثبات الأفعال الإجرامية وتوجيه الإتهامات بدقة. (القاضي، 2011، ص54).

### 5. الأدلة الناتجة عن البرامج الضارة:

تشمل الأدلة المستمدة من البرمجيات الضارة جميع المعلومات المتعلقة بالبرمجيات الخبيثة، مثل الفيروسات، برامج التجسس. وتعتبر هذه الأدلة أساسية في قضايا الجرائم الإلكترونية، حيث تسهم في إثبات إستخدام البرمجيات الضارة لأغراض إجرامية، مثل إختراق الأنظمة وسرقة البيانات. وبالإضافة إلى ذلك، توفر الأدلة الناتجة عن البرمجيات الضارة رؤى قيمة حول الأساليب والتقنيات التي يستخدمها الجناة في تنفيذ جرائمهم. ومن خلال تحليل هذه الأدلة، يصبح من الممكن كشف طرق عمل البرمجيات الضارة، مما يسهل على المحققين تتبع الجناة ويعزز فعالية الإجراءات القانونية المتخذة ضدهم. (الجاسم، 2021، ص178).

وبدراسة أنواع الأدلة الرقمية للقوانين المقارنة الفلسطيني والأردني والمصري موضوع الدراسة وكونهم يعترفان بنفس أنواع الأدلة الرقمية، إلا أنه تتضمن أكثر الأدلة الرقمية المستخدمة في القضايا الجنائية ضمن القانون الأردني الرسائل النصية، ملفات الصوت والفيديو، والسجلات الإلكترونية. ويتم تحديد إستخدامها وفقًا لمعايير قانونية معينة تضمن صحتها وقبولها في المحاكم.

ويتم تعريف أكثر الأدلة الرقمية شيوعاً في القانون الأردني وفق الآتي:

- **الرسائل النصية وملفات الوسائط** :تعتبر الصور والفيديوهات المخزنة على الهواتف الذكية والأجهزة المحمولة نوعًا حيويًا من الأدلة الرقمية. وتلعب هذه الوسائط دورًا محوريًا في التحقيقات، حيث يمكن إستخدامها لتأكيد أو نفي الوقائع المرتبطة بالقضية. (أحمد، 2020، ص1090–1092).
- **سجلات الحوسبة السحابية** :تعتبر البيانات المخزنة على السحابة من الأنواع الأساسية للأدلة الرقمية، لا سيما في العصر الحالي، حيث يعتمد العديد من الأفراد والمؤسسات على خدمات التخزين السحابي. ويمكن أن تتضمن هذه البيانات مستندات، صورًا، مقاطع فيديو، سجلات الإتصال، وغيرها من المعلومات التي تُخزن وتُدار عبر الإنترنت. (نجيب، 2014، ص50).

من ناحية أخرى، أكثر أنواع الأدلة الرقمية في القانون المصري المستخدمة في القضايا الجنائية إلى فئات عديدة، وتشمل بيانات الحسابات الإلكترونية، سجلات الشبكة، وملفات الحاسوب.

وتشمل أكثر الأدلة الرقمية شيوعاً في القانون المصري والمستخدمة في القضايا الجنائية وهي كالتالي:

- **بيانات الحسابات الإلكترونية** :تعتبر رسائل البريد الإلكتروني وحسابات وسائل التواصل الإجتماعي من المصادر الرئيسية للأدلة الرقمية، إذ تحتوي على معلومات مهمة يمكن الإستفادة منها في التحقيقات الجنائية. (الطحاوي، 2015، ص28).

- **سجلات الشبكة** :تتضمن سجلات الأنشطة على الإنترنت مجموعة من البيانات التي توثق تفاعلات المستخدمين مع المواقع والخدمات الرقمية. وتعتبر هذه السجلات أدوات أساسية في التحقيقات الجنائية، إذ يمكن الإعتماد عليها لتحديد الأنشطة المشبوهة أو الجرائم المرتكبة. (الجاسم، 2021، ص178).

ويرى الباحث مما سبق ذكره ومن خلال إستعراض أنواع الأدلة الرقمية، أن هذه الأدلة تمثل عنصرًا أساسيًا في سير التحقيقات الجنائية الحديثة وأن أنواع الأدلة الرقمية مشتركة بين القانون الفلسطيني والأردني والمصري، حيث تعكس تطور الأساليب المستخدمة لإستخلاص المعلومات الهامة من بيئات رقمية تزداد تعقيدًا. ويتضح من خلال هذا الإستعراض أن هناك تنوعًا كبيرًا في شكل الأدلة وطبيعتها، مما يعكس ضرورة تكيف الجهات القانونية مع البيئة الرقمية المتغيرة. وفي هذا السياق، تعد البيانات المخزنة أحد الركائز الأساسية، إذ تمثل المعلومات الموجودة على الأجهزة الرقمية مثل الحواسيب والهواتف الذكية دليلاً بالغ الأهمية، مما يمكن المحققين من الوصول إلى سجلات دقيقة تعكس أنشطة الأفراد. وتكمن أهمية هذه البيانات في تقديمها دليلاً قويًا يعزز من مصداقية التحقيقات، لكن يتطلب التعامل معها درجة عالية من الحذر لضمان عدم تعرضها للتلاعب. وتكتسب البيانات المنقولة أهمية خاصة في عصر التواصل الفوري، حيث يمكن أن تكشف عن تفاعلات مشبوهة بين الأفراد. وتعتبر هذه البيانات أدوات فعالة لإثبات العلاقة بين المتورطين في الجرائم، إلا أنه يجب توخي الحذر عند جمعها لضمان حماية حقوق الأفراد وعدم انتهاك خصوصيتهم. وأما البيانات المسترجعة، فهي تمثل أداة قوية في التحقيقات، إذ يمكن أن تكشف عن نوايا الجاني من خلال إستعادة معلومات محذوفة.

وإن إستخدام تقنيات متخصصة لإسترجاع هذه البيانات يعكس التقدم التكنولوجي الذي يمكن أن يسهم في تعزيز فرص كشف الجرائم وإثباتها. وعلاوة على ذلك، تلعب سجلات النظام دورًا محوريًا في تحديد الأنشطة الرقمية، حيث تقدم معلومات تفصيلية حول تصرفات الجناة. ويتيح تحليل هذه السجلات للمحققين فهم الأنماط السلوكية وإستنتاج النوايا الإجرامية، مما يجعلها مصادر رئيسية للأدلة. وأخيرًا، تمثل الأدلة الناتجة عن البرمجيات الضارة جانبًا بالغ الأهمية في التحقيقات المتعلقة بالجرائم الإلكترونية، حيث توضح الأساليب المتبعة من قبل الجناة وتساعد على تحديد كيفية تنفيذ الجرائم، مما يعزز فعالية الإجراءات القانونية المتخذة. وفي سياق المقارنة بين الأطر القانونية في كل من الأردن ومصر، ويشير الباحث إلى أهمية وجود معايير واضحة لقبول الأدلة الرقمية في المحاكم، مع توفير آليات قانونية تضمن سلامة جمعها وتحليلها دون المساس بحقوق الأفراد. وكما يؤكد على دور الأدلة الرقمية كأداة فعالة لتحقيق العدالة، داعيًا إلى تعزيز إستخدام التكنولوجيا المتقدمة ضمن إطار قانوني شامل يضمن قبول الأدلة الرقمية أمام المحاكم.

## المبحث الثاني: الضبط الإجرائي للأدلة الرقمية

تعتبر عملية ضبط الإجرائي الأدلة الرقمية من المراحل الأساسية في التحقيقات الجنائية، حيث يرتبط نجاح الأدلة المقدمة أمام المحكمة بمصداقية وكفاءة الإجراءات المتبعة في جمعها وتوثيقها. وتستلزم هذه الأدلة معالجة خاصة بسبب طبيعتها الرقمية، التي تجعلها عرضة للهشاشة والتعديل أو التلاعب. ويتناول هذا المبحث أولاً مصارد هذه الأدلة وثانياً الإجراءات القانونية والفنية المعتمدة لضبط الأدلة الرقمية، بدءًا من مراحل البحث والتحري، مرورًا بأساليب جمع الأدلة وتأمينها، وإنتهاء بتوثيقها لضمان سلامتها وقبولها في الإجراءات القضائية. وكما سيتم مقارنة الإجراءات المعمول بها في القانونين الأردني والمصري لتسليط الضوء على أوجه التشابه والإختلاف، وتقييم فعالية هذه الإجراءات في حماية نزاهة الأدلة وضمان حقوق جميع الأطراف المعنية.

### المطلب الأول: مصادر الأدلة الرقمية

وبدراسة القوانين الثلاث موضوع الدراسة نجد أنهم يشتركان بنفس مصادر الأدلة الرقمية، تتنوع مصادر الأدلة الرقمية بناءً على مكان وجودها وطريقة الوصول إليها. ومن أبرز هذه المصادر:

1. **الأجهزة الإلكترونية:**

تعتبر الأجهزة الإلكترونية، بما في ذلك الحواسيب، الهواتف الذكية، الأجهزة اللوحية، والخوادم، مصادر رئيسية للأدلة الرقمية، نظرًا لما تحتويه من بيانات متنوعة يمكن إستخدامها في التحقيقات الجنائية. وتعتبر هذه الأجهزة المصدر الأساسي للأدلة الرقمية، لأنها تحتوي على جميع أنواع البيانات المخزنة والمنقولة التي يمكن الإستفادة منها في سياق التحقيقات الجنائية. (أحمد، 2020، ص1082).

2. **الشبكات والإنترنت:**

تعتبر الشبكات بما في ذلك الإنترنت والشبكات المحلية، من المصادر الأساسية للأدلة الرقمية. وحيث توفر مجموعة واسعة من المعلومات التي يمكن إستغلالها في التحقيقات الجنائية. تشمل هذه الأدلة سجلات الخوادم، سجلات المرور، وبيانات التواصل عبر الشبكات. وكما تقدم الشبكات والإنترنت كمية كبيرة من البيانات التي تستخدم في تحديد مصادر الهجمات الإلكترونية وتتبعها. (الحسيني، 2013، ص156).

3. **الخدمات السحابية:**

مع تزايد الإعتماد على الخدمات السحابية في تخزين البيانات، أصبحت هذه الخدمات مصدرًا أساسيًا للأدلة الرقمية. وتحتوي الخدمات السحابية على ملفات المستخدمين، سجلات الوصول، والبيانات المحفوظة، مما يجعلها قابلة للإستخدام كأدلة في التحقيقات الجنائية. ومع ذلك، فإن الخدمات السحابية تطرح تحديات خاصة عند جمع الأدلة الرقمية، حيث يتم تخزين البيانات في مواقع بعيدة وقد تكون غير معروفة في بعض الأحيان. (نجيب، 2014، ص50) (فرغلي وآخر، 2007، ص14).

4. **الوسائط الإجتماعية:**

تعتبر منصات الوسائط الإجتماعية من المصادر الأساسية للأدلة الرقمية، حيث يمكن إستخدامها لجمع معلومات حول الأنشطة والتفاعلات والعلاقات بين الأفراد. وتشمل هذه المنصات بيانات مثل المنشورات، التعليقات، الرسائل الخاصة، والتفاعلات المختلفة، مما يتيح رؤية شاملة حول سلوك الأفراد وسياقات الأحداث المرتبطة بالقضايا الجنائية. وكما تحتوي الوسائط الإجتماعية على كميات ضخمة من

البيانات المتعلقة بالمستخدمين، والتي يمكن أن تكون ذات أهمية كبيرة في التحقيقات الجنائية. (الجاسم، 2021، ص178).

### 5. البيانات المستخلصة من التحليل الجنائي الرقمي:

تشمل البيانات المستخرجة عبر أدوات التحليل الجنائي الرقمي، مثل تحليل الحواسيب أو الهواتف الذكية بإستخدام تقنيات متخصصة. وتعتبر هذه الأدلة ذات قيمة كبيرة في التحقيقات الجنائية، حيث إنها غالبًا ما تكون مخفية عن الأنظار للمستخدم العادي. وكما يوفر التحليل الجنائي الرقمي فرصًا أكبر للوصول إلى الأدلة التي يصعب الحصول عليها بالأساليب التقليدية. (أحمد، 2002، ص67-70).

ويرى الباحث مما سبق ذكره ومن خلال إستعراض مصادر الأدلة الرقمية، أن هذه المصادر مشتركة بين القانون الفسطيني والأردني والمصري وتشكل عنصرًا أساسيًا في تحقيقات الجرائم المعاصرة، حيث تمثل قاعدة بيانات غنية تتنوع بحسب طبيعتها وطرق الوصول إليها. تتصدر الأجهزة الإلكترونية قائمة هذه المصادر، إذ تحتوي على معلومات متعلقة بكافة الأنشطة التي يقوم بها المستخدم، مثل الحواسيب والهواتف الذكية والأجهزة اللوحية. ولا تقتصر البيانات المتواجدة على هذه الأجهزة على كونها معلومات تخزينية فحسب، بل تعكس أيضًا سلوكيات وتفاعلات الأفراد، مما يعزز من إمكانية إستغلالها في التحقيقات الجنائية. ومن جهة أخرى، تتيح الشبكات والإنترنت آفاقًا جديدة للتحقيقات، حيث يمكن للمحققين الوصول إلى سجلات دقيقة مثل سجلات الخوادم وبيانات المرور، مما يمكنهم من تتبع الأنشطة المشبوهة وتحديد مصادر الهجمات الإلكترونية. ويتطلب إستغلال هذه البيانات مهارات تحليلية متقدمة، إذ تسهم في كشف الأنماط وسلوكيات المستخدمين. كما لا يمكن تجاهل أهمية الخدمات السحابية، التي أصبحت جزءًا لا يتجزأ من الحياة اليومية. وإن التحول نحو

التخزين السحابي قد طرح تحديات جديدة في مجال جمع الأدلة، حيث يستلزم الأمر معرفة متعمقة بكيفية إسترجاع البيانات المحفوظة في مواقع بعيدة. ومع ذلك، فإن هذه الخدمات توفر فرصًا غير مسبوقة للوصول إلى معلومات قد تكون حيوية في مسار التحقيقات. وتظهر الوسائط الإجتماعية أيضًا كمصدر غني بالأدلة الرقمية، إذ تكمن قوتها في تقديم رؤية شاملة عن الأنشطة والتفاعلات اليومية للأفراد. وتحتوي هذه المنصات على كميات هائلة من البيانات المتعلقة بالمنشورات والتعليقات والرسائل الخاصة، مما يمنح المحققين القدرة على فهم السياقات الإجتماعية والنفسية المحيطة بالأحداث، ويسهل رصد الأنماط السلوكية للمتهمين والمشتبه بهم. وأخيرًا، تشكل البيانات المستخلصة عبر التحليل الجنائي الرقمي أداة فعالة للكشف عن الأدلة المخفية. وتتيح التقنيات المستخدمة في هذا المجال للمحققين الوصول إلى معلومات قد تكون مغلقة أو محجوبة عن المستخدمين العاديين. ومن خلال إستخدام أدوات التحليل المتخصصة، يمكن فتح آفاق جديدة في تحقيقات الجرائم، مما يسهم في تعزيز فعالية العدالة وكشف الحقائق. وبالمجمل، تبرز هذه المصادر كعناصر حيوية في مشهد الأدلة الرقمية، ويتطلب التعامل معها فهماً عميقًا للتقنيات المستخدمة والتحديات المرتبطة بها. وإن قدرة المحققين على إستغلال هذه المصادر بشكل فعال قد تترك آثارًا كبيرة على سير التحقيقات ونتائجها، مما يسهم في تعزيز الأمن والسلامة العامة.

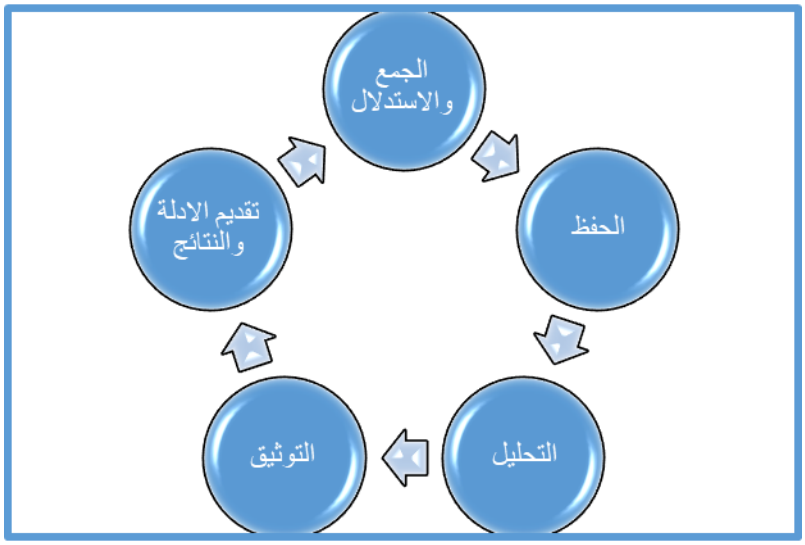
**المطلب الثاني: إجرءات الضبط القضائي للتحصل على الأدلة الرقمية**

تشير عملية ضبط الأدلة الرقمية إلى مجموعة من الإجراءات التي تهدف إلى جمع وتوثيق الأدلة الرقمية من موقع الجريمة أو من الأجهزة الإلكترونية المرتبطة بالنشاط الإجرامي. ويتطلب ذلك الحفاظ على سلامة هذه الأدلة وصحتها لضمان قبولها في المحاكم. ولأن طبيعة الأدلة الرقمية تجعلها عرضة للتلاعب، فإن هذه الإجراءات تتطلب مهارات متخصصة وإستخدام تقنيات متطورة، إن ضبط الدليل الرقمي من شأنه أن يُكوِن

نظرة واضحة عن الجريمة الإلكترونية، ويمنح إمكانية تقديم هذا الدليل أمام القضاء لإثبات التهم الموجهة إلى مرتكبي الجرائم. وكما أن عملية ضبط هذا الدليل من شأنها أن تضفي الصفة الشرعية للملاحقة الجزائية أمام القضاء. (الصغير، 2002، ص11).

تعتبر الأدلة الرقمية حساسة للغاية، مما يستدعي التعامل معها بعناية لضمان أصالتها ومصداقيتها. وتبدأ الخطوات الأولية لضبط هذه الأدلة بتحديد مواقعها وتحديد طبيعتها، تليها عملية جمعها بإستخدام أدوات متخصصة تهدف إلى حمايتها من أي تلاعب أو فقدان. (عبد العال، 2021، ص685-686).

إن سلسلة حيازة الدليل الرقمي ما هي إلا وسيلة تبين من حصل على الأدلة، وأين ومتى تم الحصول على هذه الأدلة، ومن قام بتأمين الأدلة والتعامل معها، والشكل التالي يوضح مراحل وفترة الحياة التي يمر بها الدليل الرقمي. (سفيان أبو زهيرة رئيس نيابة الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات، تواصل شخصي، 2024/11/17):



1. **الجمع والإستدلال:** ويمكن تسمية هذه المرحلة البحث والضبط، وتتم هذه المرحلة من خلال ضباط مدربين للقيام بهذه المهمة، ومن المهم أيضاً عند القيام بهذه المهمة مراعاة عدة أمور أثناء التواجد في مسرح الجريمة الإلكترونية:

- تأمين المشهد مادياً وإلكترونياً.
- فصل إتصالات البيانات الخارجية.
- تحديد الأجهزة والبيانات التي نود حفظها.
- يمكن أن تتضمن أي شكل من أشكال البيانات أو الأجهزة الإلكترونية مثل: ملفات محملة من موقع الكتروني، رسائل البريد الإلكتروني، أنشطة الإنترنت، أجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة ومحركات الأقراص الثابتة، الهواتف المحمولة وأجهزة المساعد الرقمي الشخصي والكاميرات الرقمية.

2. **حفظ الدليل الرقمي:** في هذه المرحلة يتم عزل الأدلة الرقمية وحمايتها تماماً كما وجدت دون تغيير، بحيث يمكن تحليلها لاحقاً، ومن المهم إتخاذ تدابير وقائية مهمة من أجل الحفاظ على الدليل الرقمي:

- إتخاذ جميع التدابير اللازمة لتجنب تغيير الأدلة أو إتلافها.
- النقل إلى خزانة الأدلة إن أمكن.
- إنتاج نسخة طبق الأصل من القرص الصلب (صورة) وأحياناً في مسرح الجريمة إن كان هذا ضرورياً.

3. **التحليل:** تتم في هذه المرحلة تحليل الأدلة الرقمية والعمل على النسخ المطابقة التي تم الحصول عليها من خلال الأدلة الرقمية، ومن المهم في هذه المرحلة التعامل مع العديد من الأمور والملفات، ومنها:

- إستكشاف وإستخراج كل الملفات.
- إستعادة كل (أو قدر الإمكان) من الملفات المحذوفة.

- الكشف عن محتويات الملفات المخفية وكذلك الملفات المؤقتة منها المستخدمة في كل من برامج التطبيق ونظام التشغيل.
- الوصول إلى محتويات الملفات المحمية والمشفرة.
- العثور على الملفات التي تم إستخدامها للجريمة.

4. **التوثيق وتقديم الأدلة:** وتعتبر هذه المرحلة هي المرحلة النهائية للتعامل مع الدليل الرقمي حيث يتم خلال هذه المرحلة:

- تقرير رسمي نهائي (يذكر الخبير ما فعله وما وجده).
- ملفات صور النظام.
- الأدلة المستخرجة.
- تقارير أدوات التحليل الرقمي المستخدمة للتحليل.
- تقديم النتائج والشهادة عليها.

وبالتالي فإنه وبالنسبة لإجراءات ضبط الأدلة الرقمية في فلسطين حسب ما تم ذكره، تتضمن إجراءات ضبط الأدلة الرقمية في فلسطين الخطوات التالية:

- **جمع الأدلة** :ينبغي جمع الأدلة الرقمية بإستخدام أدوات وتقنيات متخصصة لضمان سلامتها وعدم تعرضها للتلاعب. ويتضمن ذلك إستخدام برامج لإسترجاع البيانات وأجهزة مخصصة لجمع المعلومات من مختلف وسائط التخزين. (أحمد، 2020، ص1107-1108).

- **التوثيق** :يجب توثيق جميع مراحل جمع وتحليل الأدلة الرقمية بشكل دقيق، حيث يتضمن ذلك تسجيل تفاصيل مهمة مثل الوقت، التاريخ، المكان، والأشخاص المشاركين. وبالإضافة إلى ذلك، يتطلب

التوثيق إعداد تقارير فنية توضح الإجراءات المتبعة في جمع الأدلة وتحليلها. (العازمي، 2012، ص421).

- **حماية البيانات** :من الضروري الإعتماد على تقنيات متقدمة مثل التشفير والتخزين الآمن لضمان سلامة الأدلة الرقمية وحمايتها من التلاعب. ويتضمن ذلك إنشاء نسخ إحتياطية للبيانات وتأمينها ضد أي وصول غير مصرح به. (الحمداني، 2016، ص4-6).
- **الإجراءات القانونية** :يجب أن تتوافق إجراءات جمع الأدلة مع المعايير القانونية، بما في ذلك الحصول على الأذونات اللازمة من الجهات القضائية وتوثيق كل مرحلة بدقة. (يوسف، 2009، ص33).

أما بالنسبة لإجراءات ضبط الأدلة الرقمية في القانون الأردني، تشمل إجراءات ضبط الأدلة الرقمية في الأردن الخطوات التالية:

- **إستخدام الأدوات المتخصصة** :يتطلب القانون الأردني إستخدام أدوات وتقنيات متطورة لجمع وتحليل الأدلة الرقمية. ويشمل ذلك الإعتماد على برامج تحليل متقدمة وأجهزة متخصصة، لضمان سلامة الأدلة وحمايتها من أي تدخل غير مصرح به. (عبد العال، 2021، ص685-686).
- **توثيق سلسلة الحفظ** :يجب التأكد على الحفاظ على سلسلة الحفظ للأدلة الرقمية بدءا من لحظة جمعها وحتى تقديمها أمام المحكمة. ويتطلب ذلك توثيق كافة التفاصيل المتعلقة بالأدلة، بما في ذلك مراحل النقل والتخزين والتحليل، لضمان سلامتها ومصداقيتها. (بهنوس، 2017، ص7).

- **الإمتثال للإجراءات** :يفرض القانون الأردني ضرورة توثيق جميع خطوات جمع الأدلة الرقمية، مع التأكيد على التوافق التام للإجراءات المتبعة مع المعايير القانونية المعتمدة. ويتضمن ذلك إعداد تقارير شاملة تشرح كيفية جمع الأدلة وتحليلها بشكل دقيق. (أحمد، 2020، ص1108).

أما بالنسبة لإجراءات ضبط الأدلة الرقمية في القانون المصري، تشمل إجراءات ضبط الأدلة الرقمية في مصر الخطوات التالية:

- **جمع الأدلة** :يجب أن يتم جمع الأدلة الرقمية بإستخدام تقنيات متخصصة تضمن عدم تعرضها لأي تلاعب. ويتطلب ذلك إستخدام أدوات لإسترداد البيانات وبرامج متطورة لجمع المعلومات من الأجهزة المحمولة وأجهزة الكمبيوتر. (أحمد، 2000، ص42).

- **تسلسل الحفظ** :يجب الحفاظ على سلسلة الحفظ الكاملة للأدلة الرقمية، مع توثيق جميع الخطوات المتعلقة بجمعها وتحليلها. ويتضمن ذلك تسجيل كل عملية لضمان عدم تعرض الأدلة لأي تلاعب. (المعمري، 2018، ص203).

- **التقنيات المتقدمة** :يفرض القانون المصري ضرورة إستخدام تقنيات متطورة لضمان دقة وسلامة الأدلة الرقمية وحمايتها من التلاعب. ويتضمن ذلك إستخدام أدوات تحليل متقدمة وتوثيق جميع الإجراءات بشكل دقيق. (البشري، 2002، ص110).

لما كان الضبط بحسب الأصل لا يرد إلا على الأشياء المادية، فليس هناك صعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية للحاسوب كرفع البصمات مثلاً، وكذلك لا صعوبة أيضاً في ضبط الدعامة المادية للبرامج أو الوسائل المستخدمة في إتلاف البرامج. ولكن في ضبط بيانات الحاسوب ولعدم

وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات فلا بد أن يتم إتباع قواعد فنية لحماية البيانات وتجنيبها خطر الإتلاف. (قنديل، 2018، ص149).

مما حذا بالمشرع الفلسطيني لتوسيع صلاحيات سلطة التحقيق في ضبط ما يحويه الحاسوب من بيانات دون إخطار مسبق بعملية التفتيش والضبط، فنص المشرع الفلسطيني في المواد 52 53 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته، حيث نصت المادة 52 منه "1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية." ونصت المادة 33 منه "1. للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الإتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات

ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا إستحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية."، وبهذا يكون المشرع الفلسطيني منح بشكل صريح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، بتفتيش وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية والتحفظ على كامل نظام المعلومات أو أي وسيلة من وسائل تكنولوجيا المعلومات من شأنها أن تساعد على كشف الحقيقة.

وبالمقابل المشرع الأردني نص في المواد 32 و 33 من قانون الجرائم الإلكترونية رقم 17 لسنة 2023م على سلطة التحقيق في ضبط وتفتيش ما يحويه الحاسوب من بيانات، فنصت المادة 32 منه "أ- مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة وحقوق المشتكى عليه الشخصية، لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة:

1 -الدخول إلى أي مكان تشير الدلائل إلى إستخدامه لإرتكاب أي من الجرائم المنصوص عليها في هذا القانون وتفتيشها.

2 –تفتيش وفحص الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في إستخدامها لإرتكاب أي من تلك الجرائم.

ب–على الموظف الذي قام بالتفتيش أو الفحص أن ينظم محضرا بذلك ويقدمه إلى المدعي العام أو المحكمة المختصة.

ج–1– مع مراعاة الفقرة (أ) من هذه المادة وحقوق الغير حسن النية يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لإرتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

2– يستثنى من أحكام البند (1) من هذه الفقرة، المرخص لهم وفق أحكام قانون الإتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون."، ونصت المادة 33 " أ– للمدعي العام المختص أو للمحكمة المختصة وعند قيام نظام المعلومات أو موقع الكتروني أو مزود الخدمة داخل المملكة أو خارجها أو منصات التواصل الإجتماعي أو الشخص المسؤول عن أي حساب أو صفحة عامة أو مجموعة عامة أو قناة أو ما يماثلها بنشر أي مواد مخالفة لأحكام هذا القانون أو التشريعات النافذة في المملكة إصدار أمر الى القائمين عليها لاتخاذ ما يلي–:

1 –إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو إعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول اليه أو حظر المستخدم أو الناشر مؤقتاً خلال المدة المحددة في القرار.

2 –تزويدهما بجميع البيانات أو المعلومات اللازمة التي تساعد في اظهار الحقيقة ومنها بيانات مالك أو مستخدم الموقع الإلكتروني أو نظام المعلومات التي تساعد في تحديد هويته وإجراء الملاحقة القانونية.

3 –الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة وتخزينها والمحافظة على سلامتها.

4 –الحفاظ على السرية.

ب– في حال عدم إستجابة أو رفض القائمين على نظام المعلومات أو منصة التواصل الاجتماعي أو الموقع الإلكتروني أو مزود الخدمة للأمر المنصوص عليه في البند (1) من الفقرة (أ) من هذه المادة أو إذا اقتضت السرعة ذلك فيجوز للمدعي العام المختص او المحكمة المختصة وبقرار معلل إصدار أمر إلى الجهات المختصة بحظر نظام المعلومات أو الموقع الإلكتروني أو منصة التواصل الإجتماعي أو الخدمة عن الشبكة الوطنية أو حظر الوصول للمحتوى المخالف.

ج– يعاقب بغرامة لا تقل عن (15000) خمسة عشر ألف دينار ولا تزيد على (30000) ثلاثين ألف دينار كل من امتنع عن تنفيذ أوامر المدعي العام أو المحكمة المختصة أو خالفها."، وبهذه النصوص يكون المشرع الأردني نظم بشكل صريح عملية ضبط وتفتيش الأدلة الرقمية.

وكذلك الأمر نص المشرع المصري في المادة 6 من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م على سلطة التحقيق في ضبط وتفتيش ما تحويه الأجهزة الإلكترونية من بيانات، فنصت المادة 6 منه " لجهة التحقيق المختصة–بحسب الأحوال–أن تصدر أمراً مسبباً، لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على30 يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلى:

1–ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها فى أى مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على إستمرارية النظم وتقديم الخدمة أن كان لها مقتضى.

2–البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.

3–أن تأمر مقدم الخدمة بتسليم مالدية من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الإتصالات التى تمت على ذلك النظام أو الجهاز التقنى، وفى كل الأحوال يحب أن يكون أمر جهة التحقيق المختصة مسببا.

ويكون إستئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة فى المواعيد، ووفقا للإجراءات الجنائية."، وبهذه النصوص يكون المشرع المصري نظم عملية ضبط وتفتيش الأدلة الرقمية وعالجها بشكل صريح.

فقواعد الإثبات الجنائية التقليدية المعمول بها لا تصلح لإثبات الجرائم الإلكترونية بشكل مباشر، بل يحتاج ذلك لجهات إنفاذ قانون متخصصة وقضاة ووكلاء نيابة متخصصين بالشأن. وحتى يصبح الدليل الرقمي بشكل عام وذلك المتحصل من الموقع الإلكتروني على وجه الخصوص دليلاً يعتمد عليه في كشف وتتبع أثر الجريمة الإلكترونية تقوم جهات إنفاذ القانون المتخصصة بمكافحة الجرائم الإلكترونية بإستخدام برامج الكشف والتتبع، وإتخاذ إجراءات التفتيش الإلكتروني التي تشكل في مجملها وسائل لضبط أدلة يمكن التحرز عليها وضبطها والإستعانة بأهل الفن والدراسة والخبرة لمعرفة أماكن تخزين المعلومات وإجراءات إرسالها، ويبقى الحذر مطلوباً في هذا النوع من الجرائم وذلك من خلال خلق آلية متطورة لا يكلفها إلا التعاون الدولي وتبادل الخبرات والممارسات الفضلى في هذا المجال.

مما حذا بالمشرع الفلسطيني على غرار قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م للنص في المادة (57) من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم

الإتصالات وتكنولوجيا المعلومات وتعديلاته على أنه: "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات."، والمادة 58 منه "تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي."، حيث نصت المادة (11) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م على أنه: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون."، وكذلك نصت المادة (4) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م على أنه "تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن."، أما بالنسبة للمشرع الأردني تبنى إتجاه المشرع الفلسطيني والمصري ونص بشكل صريح على أن الأدلة الناتجة بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات الجنائي حيث نص في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023م في المادة 36 منه "أ–يكون للأدلة المقدمة أو المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الشبكة المعلوماتية أو التقنية المعلومات أو نظام أو برنامج الحاسوب أو

مزود الخدمة حجية الإثبات أمام الجهات القضائية. ب- تكون للبيانات والمعلومات التي يتم الحصول عليها من الجهات الرسمية من دول أخرى حجية الإثبات أمام الجهات القضائية الأردنية."، وبهذا كله يكون المشرع الفلسطيني والأردن والمصري نصا بشكل صريح أن الأدلة الناتجة بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات الجنائي.

ولضمان صحة الأدلة الرقمية وقبولها أمام المحاكم، يجب إتباع مجموعة من الخطوات الأساسية والإجراءات الفنية والقانونية عند ضبط الأدلة الرقمية وأن هذه الخطوات مشتركة بين القانون الفلسطيني والأردني والمصري وهي:

1. **الحفاظ على مسرح الجريمة الرقمي:**

يعد تأمين موقع الجريمة الرقمي أمرًا حيويًا لمنع أي تلاعب بالأدلة. وتتمثل الخطوة الأولى في ضبط الأدلة الرقمية في تأمين الموقع الذي توجد فيه هذه الأدلة، سواء كان ذلك على جهاز كمبيوتر أو شبكة أو وسائط تخزين، لضمان عدم تعديلها أو تدميرها. (البشري، 2002، ص91).

2. **التوثيق الفوري للموقع الرقمي:**

يتطلب ضبط الأدلة الرقمية توثيق الموقع الرقمي بشكل دقيق وشامل، يتضمن إلتقاط صور للشاشات وتسجيل جميع المعلومات المتعلقة بالأجهزة والبرامج المستخدمة. ويعتبر التوثيق الجيد لمسرح الجريمة

الرقمي خطوة أساسية لضمان سلامة الأدلة وتفادي أي تساؤلات بشأن مصداقيتها في المستقبل. (الجسمي، 2017، ص10).

3. **جمع الأدلة الرقمية بإستخدام أدوات متخصصة:**

يجب إستخدام أدوات وتقنيات متخصصة في جمع الأدلة الرقمية، مثل برامج النسخ الإحتياطي وأدوات تحليل البيانات. ومن الضروري أن تتضمن عملية جمع الأدلة الرقمية إستخدام تقنيات تكنولوجية معترف بها دوليًا لضمان عدم فقدان أو تغيير البيانات أثناء العملية. (القاضي، 2022، ص188).

4. **الحفاظ على سلسلة الحيازة:**

تشير سلسلة الحيازة إلى توثيق كافة الأفراد الذين يتعاملون مع الأدلة الرقمية منذ لحظة جمعها وحتى تقديمها في المحكمة، مما يضمن عدم تعرضها لأي عبث. ويساهم الحفاظ على سلسلة الحيازة في تأكيد أن الأدلة المعروضة أمام المحكمة هي نفسها التي تم جمعها من مسرح الجريمة، دون أي تغيير أو تلاعب. (القاضي، 2011، ص54).

5. **التخزين الآمن للأدلة الرقمية:**

يجب تخزين الأدلة الرقمية بطرق آمنة بإستخدام تقنيات متطورة تضمن حمايتها من الإختراق أو التلاعب. ويتطلب ذلك الإعتماد على بروتوكولات أمان صارمة وأنظمة تخزين مؤمنة، لضمان عدم الوصول غير المصرح به إلى البيانات والحفاظ على سلامتها. (أحمد ، 2002، ص67).

6. **تحليل الأدلة الرقمية في بيئة محايدة:**

ينبغي أن يتم تحليل الأدلة الرقمية في بيئة مختبرية آمنة ومحايدة، مع الإعتماد على أدوات تحليل متقدمة لضمان دقة النتائج. وإن إجراء التحليل في بيئة محايدة يسهم في التأكد من صحة الأدلة وسلامتها، مما يزيد من موثوقيتها عند تقديمها أمام المحاكم. (عبد العال، 2021، ص698-699).

7. **إعداد تقرير فني شامل:**

ينبغي إعداد تقرير فني مفصل يشمل جميع المعلومات المتعلقة بعملية جمع وتحليل الأدلة الرقمية، بالإضافة إلى الخطوات المتخذة لضمان سلامتها. وهذا التقرير يعتبر وثيقة رسمية محورية تُساعد في تقديم الأدلة الرقمية بشكل سليم أمام القضاء، مما يقلل من إحتمالية التشكيك في مصداقيتها. (بهنوس، 2017، ص185).

وعلى الرغم من التطور التكنولوجي في وقتنا الحاضر إلا أنه تواجه إجراءات ضبط الأدلة الرقمية مجموعة من التحديات، وهذه التحديات مشتركة بين القانون الفلسطيني والأردني والمصري، وتأخد هذه التحديات عدة صور منها:

1. **التحكم في الأدلة والتلاعب بها:**

نظراً للطبيعة الرقمية للأدلة، فإنها قد تكون عرضة للتلاعب إذا لم يتم تأمينها بشكل فعال. وتتمثل التحديات الرئيسية في حماية الأدلة من التغيير أو العبث أثناء مراحل جمعها وتحليلها، خصوصًا في ظل التطور المستمر في تقنيات الجرائم الإلكترونية. (يونس، 2008، ص43).

2. **نقص الخبرة التقنية:**

يتطلب جمع الأدلة الرقمية وتحليلها مهارات تقنية عالية التخصص، وهي قد لا تتوافر دائمًا لدى بعض الهيئات القضائية أو فرق التحقيق. ويمكن أن يؤدي نقص الخبرة التقنية إلى تحديات في التعامل السليم مع الأدلة الرقمية، مما قد يؤثر سلبًا على مدى قبولها في المحاكم. (يوسف، 2016، ص328).

3. **التحديات القانونية الدولية:**

تختلف التشريعات المنظمة لضبط الأدلة الرقمية بين الدول، مما يزيد من تعقيد القضايا المتعلقة بالجرائم الإلكترونية العابرة للحدود. وهذه التباينات القانونية تفرض تحديات إضافية على التحقيقات، وتؤثر بشكل مباشر على مدى قبول الأدلة الرقمية في المحاكم. (الشهري، 2022، ص273–276).

ويرى الباحث ومن خلال دراسة الضبط الإجرائي للأدلة الرقمية، أن ضبط الأدلة الرقمية في الجرائم يشكل تحديًا كبيرًا في مجال التحقيقات الجنائية، نظرًا للطبيعة التقنية المعقدة لهذه الأدلة التي تتطلب إستخدام أدوات وتقنيات متخصصة لضمان جمعها وتحليلها بصورة سليمة. ومن هنا تبرز أهمية الإطار القانوني الذي ينظم هذه العملية في التشريعات الوطنية والدولية، بهدف ضمان سلامة الأدلة الرقمية وقبولها في المحاكم.و من خلال دراسة التشريعات الفلسطينية والأردنية والمصرية، يلاحظ الباحث أن المشرعين في هذه الدول قد وضعوا قواعد قانونية واضحة تحدد كيفية جمع الأدلة الرقمية وتوثيقها وحمايتها من العبث أو التلاعب، مع التأكيد على ضرورة التوازن بين ضمان الأمن السيبراني وحماية حقوق الأفراد. ويشير الباحث إلى أن هذه التشريعات تشترط إستخدام تقنيات حديثة ومتطورة في عملية جمع الأدلة الرقمية، مثل إستخدام برامج تحليل البيانات الجنائية الرقمية وأدوات إستعادة البيانات المحذوفة. وكما تقتضي هذه القوانين توثيق كافة الإجراءات المتخذة

أثناء عملية الضبط، بما في ذلك تسجيل توقيت جمع الأدلة، والأدوات المستخدمة، وأية تغييرات تطرأ على الأجهزة أو البيانات أثناء التحليل. ويعتبر هذا التوثيق خطوة أساسية لضمان مصداقية الأدلة أمام المحكمة وحمايتها من الشكوك.

كما يبرز الباحث أهمية الحصول على إذن قانوني من الجهات القضائية المختصة لجمع الأدلة الرقمية، وذلك بما يتماشى مع حقوق الخصوصية وحماية الأفراد. ورغم تعقيد هذه الإجراءات، فإن هدفها يكمن في منع انتهاك الخصوصية أو جمع الأدلة بطرق قد تؤدي إلى المساس بالحقوق الدستورية للأفراد، مما يعكس التوازن بين مكافحة الجرائم الرقمية وإحترام الحقوق الشخصية. ومع ذلك، يلاحظ الباحث أن هذه المتطلبات قد تؤدي إلى تأخير جمع الأدلة في بعض الحالات، مما قد يوفر فرصة للمجرمين لإتلاف أو تعديل الأدلة قبل الحصول على الإذن القضائي. ومن جهة أخرى، يلفت الباحث إلى التحديات التي تواجه التشريعات الفلسطينية والأردنية والمصرية في تطبيق إجراءات جمع الأدلة الرقمية بفعالية. من أبرز هذه التحديات تطور الأدوات والتقنيات المستخدمة في الجرائم جميعها بشكل عام والجرائم الإلكترونية بشكل خاص وسرعة تغيير برمجيات الجريمة الرقمية. وفي العديد من الحالات، يصعب على فرق التحقيق مواكبة هذا التطور التكنولوجي، مما يعرض الأدلة الرقمية لخطر الضياع أو التلاعب قبل أن تتمكن الأجهزة الأمنية من جمعها وتحليلها. وإضافة إلى ذلك، يواجه المحققون صعوبة في التعامل مع الجرائم التي تتم عبر الإنترنت بين دول متعددة، ما يعقد من عملية التحقيق ويجعل تحديد الولاية القضائية المناسبة أمرًا معقدًا. وفي هذا السياق، يرى الباحث أن الحلول تكمن في تعزيز التعاون بين الدول في مواجهة الجرائم، من خلال تبادل المعلومات والخبرات حول أفضل الممارسات في جمع وتحليل الأدلة الرقمية. كما يوصي الباحث بتطوير البنية التحتية التقنية للمؤسسات القضائية والأمنية، وتوفير التدريب المستمر للمحققين على أحدث الأدوات والتقنيات المستخدمة في هذا المجال. وكما يشدد الباحث على

أهمية إستخدام تقنيات الذكاء الإصطناعي والأنظمة الذكية في تحليل الأدلة الرقمية، ما قد يسهم في تسريع عملية التحقيق وزيادة دقتها، خاصة في الحالات التي تتطلب فحص كميات ضخمة من البيانات الرقمية. وأخيرًا، يلاحظ الباحث أنه رغم التقدم الذي أحرزته التشريعات في الدول المعنية في مجال جمع الأدلة الرقمية، إلا أن النجاح في مواجهة الجرائم يتطلب تضافر جهود جميع الأطراف المعنية، بما في ذلك المؤسسات القضائية، والأجهزة الأمنية، وشركات التكنولوجيا، والمجتمع الدولي، لضمان فعالية هذه القوانين في مكافحة الجرائم.

## الفصل الثاني: حجية الأدلة الرقمية في الإثبات الجنائي

مع تطور التكنولوجيا وإنتشار الجرائم الإلكترونية، أصبحت الأدلة الرقمية إحدى الوسائل الأساسية في إثبات الجرائم وتقديم مرتكبيها للعدالة. وأن قبول هذه الأدلة أمام القضاء الجنائي يثير تساؤلات عديدة تتعلق بشروطها القانونية ومشروعيتها، لا سيما في ظل طبيعتها الخاصة التي تجعلها عرضة للتلاعب والتزييف. ولذا، يتناول هذا الفصل حجية الأدلة الرقمية في الإثبات الجنائي من خلال دراسة مقبوليتها كوسيلة إثبات وفق القوانين المقارنة، وتحليل الشروط القانونية التي تضمن قبولها. وكما يناقش هذا الفصل مشروعية الأدلة الرقمية في الإثبات الجنائي والتحديات التي تواجه مشرعية هذه الأدلة، مسلطًا الضوء على الإشكالات المتعلقة بجمعها وتقديمها أمام القضاء بما يتماشى مع مبادئ العدالة الجنائية.

### المبحث الأول: مقبولية الأدلة الرقمية في الإثبات الجنائي

تشكل الأدلة الرقمية عنصرًا أساسيًا في إثبات الجرائم في العصر الحديث، إلا أن قبولها في المحاكم يتطلب إستيفاء مجموعة من الشروط لضمان نزاهتها ومصداقيتها. ومن الضروري تحديد هذه الشروط لضمان جمع الأدلة وتحليلها وفق المعايير القانونية، مما يحافظ على حقوق المتهمين ويعزز مبدأ العدالة. ويركز هذا المبحث على دراسة الشروط اللازمة لقبول الأدلة الرقمية أمام القضاء، مثل سلامة إجراءات الضبط، وموثوقية المصدر، وإحترام حقوق الخصوصية. وسيتم أيضًا إستعراض وتحليل هذه الشروط في إطار التشريعات الأردنية والمصرية لتحديد مدى توافقها مع المعايير الدولية، بالإضافة إلى بيان أوجه القصور والتحديات التي قد تعترض سبيل قبول الأدلة الرقمية في المحاكم.

## المطلب الأول: الشروط القانونية لقبول الأدلة الرقمية أمام القضاء الجنائي

لقبول الأدلة الرقمية أمام القضاء الجنائي، يجب توافر شروط قانونية صارمة تضمن مشروعيتها وسلامتها. وتشمل هذه الشروط جمع الأدلة بطريقة مشروعة تتماشى مع القوانين، مع ضمان عدم المساس بالخصوصية أو انتهاك الحقوق الفردية. ويناقش هذا المطلب المعايير التي تضعها القوانين الوطنية والمقارنة لقبول الأدلة الرقمية، بدءًا من مراحل جمعها وتحليلها، وصولًا إلى تقديمها أمام المحاكم. وكما يبرز أهمية الإلتزام بسلسلة الحيازة لضمان سلامة الأدلة ومصداقيتها.

### الفرع الأول: المعايير القانونية لضمان قبول الأدلة الرقمية في القانون الفلسطيني

يشترط القانون أن يتم جمع الأدلة الرقمية بطريقة مشروعة، بحيث تكون خالية من التلاعب أو الإنتهاكات. ويُركز هذا الفرع على كيفية تحقيق هذه الشروط في المراحل الأولية لجمع الأدلة الرقمية. ولضمان أن تكون الأدلة الرقمية في التشريع الفلسطيني حجة قوية في الإثبات الجنائي أمام القضاء الجنائي، يجب توافر عدة شروط قانونية فيها، من أبرزها:

#### 1. سلامة الأدلة:

يجب أن تكون الأدلة الرقمية متوافقة مع معايير السلامة، وخالية من أي تلاعب، مما يستدعي إتباع إجراءات دقيقة لجمعها وتوثيقها وتخزينها. ويتطلب الحفاظ على سلامة هذه الأدلة إثبات عدم حدوث أي تغيير أو تلاعب بها منذ لحظة جمعها وحتى تقديمها إلى المحكمة، وبالإضافة إلى ذلك، يجب إستخدام أدوات وتقنيات موثوقة في عملية جمع وتحليل الأدلة الرقمية لضمان دقتها ومصداقيتها، يتضمن ذلك

الإعتماد على برامج تحليل معترف بها من قبل الجهات القانونية لضمان صحة النتائج المستخلصة. (عرفة، 2018، ص483).

وهذا ويشير الباحث إلى أن أعمال الخبرة الفنية من جهة مختصة بها في المجالات التقنية والرقمية من أهم الأدوات لتحقق من هذا الشرط القانوني بحيث يتم الإستعانة بالخبراء من أجل التحققق من سلامة الأدلة الرقمية وعدم تعرضها لأي تلاعب يؤدي إلى تغير صورتها الحقيقية، وبالتالي تكون مشاركة الخبراء الفنيين الذين يمتلكون المعرفة التقنية الكافية للتحقق من صحة الأدلة بشكل عام، يمثل الاهتمام بالسلامة جانبًا محوريًا في تعزيز مصداقية الأدلة الرقمية أمام المحكمة. وكذلك يمكن إعتبار النص القانوني رقم 4/52 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته الذي نص " لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات." وبهذا يكون المشرع الفلسطيني نص على أهمية الإستعانة بأهل الخبرة في المجال التقني تجنباَ من الوقوع في أي خلل عند جمع هذه الأدلة أو من أجل التأكد من من سلامة هذه الأدلة.

2. **أصالة الأدلة:**

يجب أن تتمتع الأدلة الرقمية بصفة الأصالة، مما يعني أنه لم يتم إجراء أي تغييرات أو تعديلات عليها منذ جمعها. وترتبط الأصالة بكون الأدلة المقدمة تمثل النسخة الأصلية التي تم الحصول عليها دون أي تدخل، وهو شرط أساسي لضمان قبولها أمام المحكمة. ولذلك من الضروري أن تبقى الأدلة الرقمية في حالتها الأصلية دون أي تعديل منذ لحظة جمعها. ويتطلب ذلك إستخدام تقنيات مثل التشفير والتوثيق

الرقمي لضمان صحة البيانات. وكما يجب أيضًا تقديم شهادات من المحققين تؤكد عدم تغيير البيانات. (بهنوس، 2017، ص185).

ويشير الباحث إلى أن صفة الأصالة لدليل تُعد عنصرًا جوهريًا لضمان موثوقية الأدلة الرقمية ومقبوليتها أمام القضاء. ويتطلب الحفاظ على هذه الأصالة إعتماد تقنيات دقيقة، مثل التشفير والتوثيق الرقمي، التي تتيح تتبع أي محاولة للتلاعب أو التعديل. وبالإضافة إلى ذلك، تُعتبر الشهادات المقدمة من المحققين عنصرًا داعمًا يعزز الثقة في سلامة الأدلة الرقمية أمام المحكمة. ومع ذلك، تواجه الأصالة تحديات كبيرة، لا سيما في ظل التطور التكنولوجي الذي يُسهِّل التلاعب بالبيانات، مما يجعل من الضروري تحديث الأدوات القانونية والتقنية بشكل مستمر لمجابهة هذه التحديات وضمان فعالية الأدلة الرقمية. وكذلك يمكن إعتبار النص القانوني رقم 55 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته الذي نص "على الجهات المختصة إتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها." وبهذا يكون المشرع الفلسطيني نص على أهمية الحفاظ على أصالة الدليل بنسخته الأصلية لحين صدور قرار من الجهات الفضائية.

### 3. مصداقية الأدلة:

يتعين أن تتمتع الأدلة الرقمية بمستوى عالٍ من الموثوقية، وأن تكون مصداقيتها واضحة تماما، لتحقيق ذلك، يجب إستخدام تقنيات معترف بها لجمع الأدلة وتحليلها، مما يسهل عملية التحقق من صحتها،

تعتمد مصداقية هذه الأدلة بشكل كبير على الأساليب المستخدمة في جمعها والتحقق منها، مما يؤثر بشكل مباشر على إمكانية قبولها في المحاكم. ويتضمن التوثيق توثيق جميع التفاصيل المتعلقة بعملية جمع وتحليل الأدلة، بما في ذلك الوقت والتاريخ والمكان والأفراد المشاركين. وكما يتطلب أيضًا إعداد تقارير شاملة توضح كيفية جمع الأدلة والتقنيات المستخدمة في هذه العملية. (الحمداني، 2016، ص37).

يرى الباحث أن مصداقية الأدلة الرقمية تعتمد على دقة الإجراءات المتبعة في جمعها وتحليلها. وإجراءات جمع الأدلة يجب أن تكون موثوقة وتتسم بالدقة لضمان قابلية الأدلة للقبول أمام المحكمة. ولذا، يُعتبر توثيق جميع مراحل جمع الأدلة وتحليلها أمرًا بالغ الأهمية لضمان مصداقيتها، حيث تسهم التفاصيل الدقيقة مثل توقيت جمع الأدلة والموقع والأشخاص المشاركين في تعزيز تلك المصداقية.

**4. سلسلة الحيازة:**

تشير سلسلة الحيازة إلى توثيق شامل لجميع الإجراءات المتعلقة بجمع الأدلة وتخزينها وتحليلها، وذلك لضمان عدم تعرضها لأي تدخل أو تلاعب. ويجب أن تكون هذه السلسلة واضحة ودقيقة لضمان أن الأدلة المقدمة أمام المحكمة هي ذاتها التي تم جمعها من موقع الجريمة. وكما وينبغي جمع الأدلة الرقمية وفقًا للإجراءات القانونية المعتمدة لضمان قبولها أمام المحكمة. ويتضمن ذلك الحصول على الأذونات المطلوبة من السلطات القضائية، بالإضافة إلى توثيق كل مرحلة من مراحل عملية جمع الأدلة بشكل دقيق. (عبد العال، 2021، ص685-686).

ويرى الباحث أن سلسلة الحيازة تمثل أحد العناصر الجوهرية التي تؤكد سلامة الأدلة وتدعم مصداقيتها. وفي حالة الأدلة الرقمية، يجب توثيق جميع الخطوات التي مرّت بها الأدلة، بدءًا من جمعها،

مرورًا بتخزينها، وصولًا إلى تحليلها. وهذا التوثيق يساعد على تجنب أي تلاعب أو تبديل، ويثبت أن الأدلة المقدمة أمام المحكمة هي الأدلة الأصلية التي تم جمعها من موقع الجريمة، مما يعزز إمكانية قبولها في القضاء الجنائي. وكذلك يمكن إعتبار نصوص المواد 52 و 53 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته ومفادهما أنه يتم تفتيش الأشخاص والأماكن بناءا على إذن من النيابة العامة وبهذا يكون المشرع الفلسطيني نص على ضرورة الحصول على إذن مسبق من النيابة العامة حفاضا على صحة الإجراء وتفاديا لتعرض لإجراءات الطعن.

**5. الإمتثال للمعايير الفنية والتقنية:**

يجب أن تجرى عملية جمع وتحليل الأدلة الرقمية بإستخدام أدوات وتقنيات معترف بها على المستوى الدولي، وذلك لضمان دقتها وموثوقيتها. وإن الإلتزام بالمعايير الفنية يسهم في تقليل إحتمالية رفض الأدلة الرقمية نتيجة أي أخطاء تقنية أو إجرائية. (أبو عامر، 2009، ص730).

يؤكد الباحث أن الإلتزام بالمعايير الفنية والتقنية الدولية يعد من الشروط الأساسية لقبول الأدلة الرقمية في المحاكم. والإعتماد على أدوات وتقنيات معترف بها دوليًا يقلل من إحتمال رفض الأدلة بسبب الأخطاء التقنية أو الإجرائية. ويساهم الإلتزام بهذه المعايير في ضمان دقة الأدلة الرقمية وموثوقيتها، مما يعزز فرص قبولها كأدلة قانونية في المحاكم. وكذلك يمكن إعتبار النص القانوني رقم 62 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته الذي نص "1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل

المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والإتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. 2. يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون." وبهذا يكون المشرع الفلسطيني نص على أهمية تيسير التعاون الدولي في المجالات التقنية والفنية والإمتثال لها وفقا لإتفاقيات دولية وطبقا لمبدأ المعاملة بالمثل.

**الفرع الثاني: الشروط القانونية لضمان قبول الأدلة الرقمية في القانون الأردني والمصري**

يناقش هذا الفرع أهمية جميع مراحل التعامل مع الأدلة لضمان قبولها أمام القضاء بالنسبة للقانون الأردني والمصري، وبالتالي فإنه وبالنسبة لشروط قبول الأدلة الرقمية في التشريع الأردني، يتطلب قبول الأدلة الرقمية تلبية الشروط التالية:

- **تسلسل الحفظ** :يجب ضمان الحفاظ على سلسلة الحفظ الشاملة للأدلة الرقمية، مع توثيق كافة الخطوات منذ لحظة جمعها وحتى تقديمها في المحكمة. ويشمل ذلك تسجيل جميع الإجراءات المرتبطة بالأدلة، بما في ذلك النقل والتخزين والتحليل. (القاضي، 2022، ص195-196).

يرى الباحث أن تسلسل الحفظ يشكل جزءًا أساسيًا من قبول الأدلة الرقمية في النظام القضائي الأردني. وتوثيق جميع الخطوات منذ جمع الأدلة وحتى تقديمها أمام المحكمة يضمن الحفاظ على سلامتها ويمنع أي تحريف أو تلاعب. ويُعتبر هذا التسلسل أداة مهمة لتوثيق مصداقية الأدلة الرقمية، مما يتيح للمحكمة التأكد من أنها لم تتعرض لأي تدخل غير قانوني. وكذلك يمكن إعتبار نص المادة

32 فقرة أ من قانون الجرائم الإلكترونية رقم 17 لسنة 2023 الأردني ومفادهما أنه يتم تفتيش الأشخاص والأماكن والدخول إليها يكون بناءا على إذن من المدعي العام أو المحكمة المختصة وبهذا يكون المشرع الأردني نص على ضرورة الحصول على إذن مسبق من الجهات القضائية حفاضا على صحة الإجراء وتفاديا لتعرض لإجراءات الطعن.

- **الإجراءات القانونية** :يجب جمع الأدلة الرقمية وفقًا للإجراءات القانونية السارية، والتي تشمل الحصول على إذن من الجهة القضائية المختصة عند الحاجة. ويتطلب القانون الأردني أيضًا توثيق كافة الخطوات المتبعة أثناء عملية جمع الأدلة، وذلك لضمان سلامتها وحمايتها من أي تلاعب. (عبد العال، 2021، ص685).

يؤكد الباحث على ضرورة التزام إجراءات جمع الأدلة الرقمية بالقوانين المعمول بها في الأردن. ويتطلب ذلك الحصول على الأذونات القانونية اللازمة من الجهات القضائية، مما يضمن أن الأدلة قد تم جمعها بطريقة قانونية وموافقة للأطر التشريعية المعتمدة. ويشير الباحث إلى أن توثيق كافة الخطوات المتبعة أثناء جمع الأدلة يضمن عدم تعرض الأدلة لأي تدخل يؤثر على مشروعيتها أمام المحكمة. وكذلك يمكن إعتبار نص المادة 32 فقرة ب من قانون الجرائم الإلكترونية رقم 17 لسنة 2023 الأردني ومفادهما أنه يتم تنظيم محضر بواقعة تفتيش الأشخاص والأماكن والدخول إليها وبهذا يكون المشرع الأردني نص على ضرورة تنظيم محضر بواقعة تفتيش الأشخاص والأماكن والدخول إليها حفاضا على صحة الإجراء وتفاديا لتعرض لإجراءات الطعن.

- **تحليل موثوق** :يجب إستخدام أدوات وتقنيات موثوقة لتحليل الأدلة الرقمية، مع ضرورة التأكيد على صحة نتائج هذا التحليل وعدم تعرضها لأي شكل من أشكال التلاعب. ويتطلب ذلك أيضًا إعداد

تقارير مفصلة توضح كيفية إجراء عملية التحليل والتقنيات المعتمدة في هذا السياق. (الحوامدة، 2021، ص909).

يشير الباحث إلى ضرورة إستخدام أدوات وتقنيات معترف بها لتحليل الأدلة الرقمية في النظام القضائي الأردني. والتحليل الموثوق للأدلة يمكن المحكمة من التأكد من صحتها وسلامتها. وكما أن إعداد تقارير مفصلة توضح كيفية إجراء التحليل والتقنيات المستخدمة يعزز المصداقية العلمية للأدلة ويجعلها أكثر قبولًا أمام المحكمة.

أما بالنسبة لشروط قبول الأدلة الرقمية في التشريع المصري، تشمل الشروط الرئيسية لقبول الأدلة الرقمية:

- **الإثبات على الأصالة** :يجب تقديم الأدلة الرقمية مع إثبات أصالتها ووجود ضمانات بعدم تعرضها لأي تلاعب. ويتطلب ذلك إعتماد تقنيات للتحقق من الهوية الرقمية، فضلاً عن توثيق سلسلة الحيازة لضمان سلامة الأدلة. (أبو عامر، 1971، ص120).

يرى الباحث أن إثبات الأصالة هو جزء أساسي لضمان قبول الأدلة الرقمية. وفي هذا السياق، يضع الباحث أهمية خاصة لتقنيات التحقق من الهوية الرقمية وضمان أن الأدلة لم تتعرض للتلاعب أو التعديل. وهذا يساهم في ضمان أن الأدلة المقدمة أمام المحكمة هي النسخ الأصلية التي تم جمعها بشكل قانوني.

- **توافق الإجراءات** :يجب أن تتوافق إجراءات جمع الأدلة الرقمية مع المعايير القانونية السارية، بما في ذلك الحصول على الأذونات اللازمة من الجهات القضائية المختصة وتوثيق كافة الخطوات المتبعة في هذه العملية. (عبد العال، 2021، ص685-686).

يشير الباحث إلى أن الإجراءات المتعلقة بجمع الأدلة الرقمية في مصر يجب أن تتوافق مع المعايير القانونية السارية، بما في ذلك ضرورة الحصول على الأذونات من السلطات القضائية المختصة. وهذا ما أكدت عليه نص المادة 6 قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات ومفادها أن جهة التحقيق المختصة تمنح مأموري الضبط القضائي الإذن اللازم، ولذلك يعزز الباحث ضرورة توثيق كافة الخطوات المتبعة أثناء جمع الأدلة، حيث أن ذلك يضمن مصداقية الأدلة أمام المحكمة ويمنع أي تدخل قد يؤدي إلى التشكيك في صحتها.

- **تطبيق التقنيات المتقدمة** :يشترط القانون المصري إستخدام تقنيات حديثة لجمع وتحليل الأدلة الرقمية، لضمان دقتها وسلامتها من التلاعب. ويتضمن ذلك الإستعانة بأدوات تحليل متطورة وتوثيق جميع الإجراءات بشكل دقيق. (بوكرة، 2017، ص507).

يؤكد الباحث على أهمية إستخدام التقنيات المتقدمة في جمع وتحليل الأدلة الرقمية في النظام القضائي المصري. وإستخدام هذه التقنيات يضمن أن الأدلة الرقمية ستظل سليمة ودقيقة، مما يعزز فرص قبولها في المحكمة. ويشير الباحث إلى أن توثيق جميع الإجراءات بشكل دقيق يعد ضروريًا لضمان سلامة الأدلة وحمايتها من التلاعب.

ويرى الباحث ومن خلال دراسة الشروط القانونية لقبول الأدلة الرقمية أمام القضاء الجنائي أن سلامة الأدلة الرقمية تمثل الركيزة الأساسية لضمان قبولها أمام القضاء الجنائي، حيث تعد الحفاظ على سلامتها من التلاعب أو التعديل أمرًا بالغ الأهمية لضمان مصداقيتها وقوتها في الإثبات. ويشير الباحث إلى أن سلامة الأدلة تتطلب إتباع إجراءات دقيقة ومنهجية منذ لحظة جمعها وحتى تقديمها أمام الجهات القضائية، وتشمل هذه الإجراءات جمع الأدلة بطرق معتمدة، توثيقها بأسلوب واضح ومفصل، وتخزينها في بيئات آمنة ومحمية

من التلاعب. وكما أن إستخدام تقنيات وأدوات معترف بها دوليًا يسهم بشكل كبير في تقليل فرص التشكيك في هذه الأدلة، ويعزز من موثوقيتها أمام المحاكم. وفي هذا الإطار، يقارن الباحث بين القوانين الفلسطينية والأردنية والمصرية من حيث تناولها لموضوع سلامة الأدلة الرقمية. ويرى أن القانون الفلسطيني يولي أهمية لسلامة الأدلة وأصالته ومصداقيته وضمان سلسلة الحيازة. وفي المقابل، يتميز القانون الأردني بتقديم متطلبات تفصيلية وإجراءات واضحة تهدف إلى ضمان سلامة الأدلة الرقمية في جميع مراحل التعامل معها. وأما القانون المصري، فقد تفوق بإستخدامه تقنيات متقدمة لضمان مصداقية الأدلة، مما يعزز موقفها أمام القضاء الجنائي ويقلل من إحتمالية رفضها.

أما فيما يتعلق بأصالة الأدلة الرقمية، يشدد الباحث على أنها تمثل أحد الشروط الجوهرية لقبول الأدلة، حيث تعني الأصالة بقاء الأدلة بحالتها الأصلية دون أن تتعرض لأي تعديل أو تلاعب منذ لحظة جمعها وحتى عرضها أمام المحكمة. ولتحقيق هذا الشرط، يوصي الباحث بإستخدام تقنيات حديثة مثل التشفير، والتي تُعد أدوات فعالة لضمان حماية الأدلة الرقمية من التغيير غير المشروع. ويرى الباحث أن التشريعات الفلسطينية بحاجة إلى تعزيز هذا الجانب من خلال إعتماد تقنيات أكثر تطورًا، بينما يظهر القانون الأردني في صورة متقدمة حيث يوفر إطارًا قانونيًا أكثر وضوحًا وتفصيلًا لضمان أصالة الأدلة. وعلى الجانب الآخر، يتميز القانون المصري بصرامته في هذا المجال، حيث يعتمد على تقنيات حديثة لضمان إستيفاء الأدلة لمعايير الأصالة بشكل كامل. وكذلك الأمر فيما يخص مصداقية الأدلة الرقمية، يرى الباحث أنها تعتمد على جودة الإجراءات والأساليب المستخدمة في جمع وتحليل الأدلة. وإن إتباع ممارسات معترف بها دوليًا، مثل توثيق جميع المراحل التي تمر بها الأدلة وإعداد تقارير شاملة حول عمليات الجمع والتحليل، يعزز بشكل كبير من مصداقية الأدلة ويقلل من فرص رفضها أمام القضاء. ويشير الباحث إلى أن القوانين الفلسطينية والأردنية

والمصرية تتفق جميعها على أهمية مصداقية الأدلة الرقمية، ولكنها تختلف في تفاصيل الإجراءات اللازمة لتحقيق ذلك. فعلى سبيل المثال، يركز التشريع الفلسطيني على التوثيق العام دون الدخول في تفاصيل دقيقة، بينما يتميز التشريع الأردني بتقديم إرشادات تفصيلية حول كيفية جمع وتحليل الأدلة الرقمية. وفي المقابل، يتفوق التشريع المصري بإستخدامه تقنيات حديثة تسهم في تعزيز موثوقية الأدلة وضمان سلامتها. وفيما يتعلق بسلسلة الحيازة، يرى الباحث أنها تمثل أحد المعايير الأساسية لضمان قبول الأدلة الرقمية أمام المحاكم. تعني سلسلة الحيازة توثيق جميع المراحل التي تمر بها الأدلة منذ جمعها وحتى عرضها على المحكمة، بما في ذلك مراحل الحفظ والنقل والتحليل. ويؤكد الباحث على أن الإلتزام بالإجراءات القانونية السليمة، مثل الحصول على الأذونات القضائية اللازمة وتوثيق العمليات بشكل دقيق، يساهم في تعزيز موثوقية الأدلة الرقمية. ويقارن الباحث بين القوانين الثلاثة، حيث يرى أن القانون الفلسطيني يفتقر إلى التفاصيل الدقيقة التي يوفرها القانون الأردني فيما يتعلق بسلسلة الحيازة. وأما القانون المصري، فيتميز بتبنيه إجراءات صارمة توثق جميع الخطوات بإستخدام تقنيات متقدمة، مما يعزز من قبول الأدلة الرقمية أمام القضاء.

وأخيرًا، يلفت الباحث النظر إلى أهمية الإمتثال للمعايير الفنية والتقنية العالمية كشرط أساسي لقبول الأدلة الرقمية. ويرى أن استخدام أدوات وتقنيات معتمدة دوليًا لا يسهم فقط في تعزيز دقة الأدلة، بل يقلل أيضًا من إحتمالية رفضها نتيجة أخطاء إجرائية. ويشير الباحث إلى أن القانون الفلسطيني بحاجة إلى تحسينات في هذا الجانب، حيث يجب عليه اعتماد تقنيات حديثة وممارسات معترف بها عالميًا. وفي المقابل، يوازن القانون الأردني بين التقنية والإجراءات القانونية، مما يضمن قبول الأدلة الرقمية بشكل أفضل. وأما القانون المصري، فيعتمد بشكل كبير على التقنيات الحديثة كمعيار رئيسي لقبول الأدلة الرقمية، مما يجعله أكثر تقدمًا في هذا الجانب مقارنة بالقوانين الأخرى. ويخلص الباحث إلى أن الشروط القانونية المتعلقة بقبول الأدلة الرقمية تُعد

متطلبات أساسية لضمان حُجيتها أمام القضاء الجنائي. وعلى الرغم من إتفاق القوانين الفلسطينية والأردنية والمصرية على أهمية هذه الشروط، إلا أنها تختلف في درجة تفصيل الإجراءات ومستوى التقنية المستخدمة.

**المطلب الثاني: تحديات قبول الأدلة الرقمية أمام القضاء الجنائي**

رغم أهمية الأدلة الرقمية، فإنها تواجه تحديات عديدة تؤثر على قبولها أمام القضاء الجنائي. وتشمل هذه التحديات الجانب القانوني المتمثل في غياب التشريعات الواضحة والموحدة دوليا، بالإضافة إلى الصعوبات التقنية مثل قابلية التلاعب. ويناقش هذا المطلب أبرز التحديات التي تواجه القضاة في تقييم الأدلة الرقمية، وكما يُبرز دور التكنولوجيا المتطورة في تجاوز بعض هذه التحديات. وعلى الرغم من أهمية الأدلة الرقمية في الإثبات الجنائي، إلا أن هناك العديد من التحديات التي تواجه قبولها في المحاكم الجنائية، وأن هذه التحديات مشتركة بين التشريع الفلسطيني والأردني والمصري، وهذه التحديات هي تحديات قانونية وتقنية.

**الفرع الأول: التحديات القانونية المتعلقة بقبول الأدلة الرقمية**

في ظل التطور السريع لتكنولوجيا المعلومات والإتصالات، أصبحت الأدلة الرقمية من العناصر الحيوية في الإجراءات الجنائية، حيث تلعب دورًا أساسيًا في إثبات الجرائم وكشف الحقائق. ولكن، في الوقت نفسه، تطرح هذه الأدلة العديد من التحديات القانونية التي تؤثر بشكل مباشر على قبولها أمام القضاء. وإن أبرز هذه التحديات يكمن في غياب المعايير القانونية الموحدة دوليًا، مما يخلق حالة من التضارب بين الأنظمة القانونية المختلفة حول كيفية قبول وتقييم هذه الأدلة. وكما أن التفاعل بين القوانين المحلية وحقوق الأفراد في الخصوصية يشكل تحديًا مستمرًا، حيث يتطلب تحقيق العدالة موازنة دقيقة بين الحفاظ على الحقوق الفردية وضرورات

التحقيق الجنائي. ولذلك، تبرز الحاجة الملحة لإيجاد حلول قانونية تتناسب مع متطلبات العصر الرقمي، وتضمن قبول الأدلة الرقمية في المحاكم بطريقة مشروعة وآمنة.

**أولا: عدم وضوح المعايير القانونية**

تختلف المعايير القانونية المتعلقة بقبول الأدلة الرقمية من دولة إلى أخرى، مما يخلق تحديات في توحيد الإجراءات والمعايير المطلوبة لضمان قبولها في المحاكم. وكما أن غياب معايير موحدة ومعترف بها دوليًا يجعل من الصعب تحقيق الإتساق في التعامل مع الأدلة الرقمية عبر الحدود. (عرفة، 2018، ص713-717).

ويعتبر غياب المعايير القانونية الموحدة لدول العالم بشأن قبول الأدلة الرقمية من أكبر التحديات، حيث تختلف القوانين المحلية من دولة لأخرى. وفي غياب المعايير الواضحة، يصبح من الصعب التنسيق بين مختلف الأنظمة القانونية عبر الحدود، مما يخلق فجوات في تطبيق القانون ويؤثر سلبًا على قبول الأدلة الرقمية، مما يعزز الحاجة إلى وضع إطار قانوني دولي موحد لتوجيه عمليات جمع وتقديم الأدلة الرقمية.

**ثانيا: الخصوصية وحماية البيانات**

قد يتسبب جمع الأدلة الرقمية في بعض الأحيان في تعارض مع حقوق الخصوصية وحماية البيانات الشخصية، مما يتطلب ضرورة إيجاد توازن دقيق بين حقوق الأفراد ومتطلبات تحقيق العدالة. وإن الحفاظ

على هذا التوازن بين حقوق الخصوصية وإحتياجات الإثبات الجنائي يعتبر تحديا قانونيا مستمرا. (عبد العال، 2021، ص706-709).

ومن أبرز التحديات القانونية التي تقيد قبول الأدلة الرقمية في القضايا الجنائية هي مسألة حماية الخصوصية. وفي العديد من الحالات، يمكن أن يتداخل جمع الأدلة الرقمية مع حقوق الأفراد في الخصوصية وحماية بياناتهم الشخصية، الأمر الذي يتطلب توازنًا دقيقًا بين احترام حقوق الأفراد وضرورات التحقيق الجنائي. وإذ أن أي تجاوز للخصوصية في جمع الأدلة قد يؤدي إلى تشكيك في قانونية تلك الأدلة.

**الفرع الثاني: التحديات التقنية المتعلقة بقبول الأدلة الرقمية**

تعد الأدلة الرقمية من أكثر الأدلة تعرضًا للتحديات التقنية التي قد تؤثر على قبولها أمام القضاء الجنائي. وفي حين أن هذه الأدلة تتميز بالسهولة في جمعها وتحليلها، إلا أن تزايد تعقيدها وإستخدام التقنيات الحديثة في تخزينها يجعلها عرضة للتلاعب والتزوير. ومن هذا المنطلق، تبرز أهمية ضمان سلامة الأدلة الرقمية وحمايتها من التلاعب أثناء جمعها وتحليلها. وبالإضافة إلى ذلك، تتطلب هذه الأدلة تقنيات متقدمة وأدوات متخصصة لضمان دقتها ومصداقيتها، وهو ما قد يشكل عبئًا على بعض الأنظمة القضائية التي تفتقر إلى الموارد اللازمة لهذا الغرض. وإن التحديات التقنية لا تقتصر فقط على حماية الأدلة، بل تمتد أيضًا إلى صعوبة إستخراج البيانات وتحليلها بطريقة تضمن صحتها أمام المحكمة.

**أولا: التلاعب والتزوير**

يعتبر التلاعب والتزوير في الأدلة الرقمية من التحديات الرئيسية التي تواجه قبولها في المحاكم. وإذ إن الخصائص الرقمية لهذه الأدلة تجعلها عرضة للتلاعب والتزوير، مما يستدعي إتخاذ إجراءات دقيقة لضمان صحتها وأصالتها. (عبد العال، 2021، ص706-708).

ويشكل التلاعب والتزوير في الأدلة الرقمية تحديًا حيويًا أمام قبولها في المحاكم، حيث أن الخصائص الرقمية مثل سهولة النسخ والتعديل تجعل الأدلة الرقمية عرضة للزوال أو التغيير. وفي هذه الحالة، يتطلب الأمر تقنيات متقدمة وأدوات تحليل متخصصة لضمان صحة الأدلة وأصالتها، وهو ما يفرض على الأجهزة القضائية والمحققين إتباع إجراءات صارمة لضمان التحقق من صدق الأدلة الرقمية قبل قبولها في المحاكمة.

**ثانيا: التحديات التقنية**

تتطلب الأدلة الرقمية إستخدام تقنيات متقدمة لجمعها وتحليلها، وهو ما قد يكون غير متوفر في بعض الأنظمة القضائية أو لدى فرق التحقيق. وتتضمن التحديات التقنية نقص الموارد البشرية والتقنية اللازمة للتعامل بشكل فعال مع هذه الأدلة. (الشهري، 2022، ص273-277).

تواجه بعض الأنظمة القضائية صعوبة في جمع وتحليل الأدلة الرقمية بسبب نقص التكنولوجيا المتطورة والكوادر البشرية المدربة. وبينما قد تكون بعض الأدلة الرقمية معقدة وتتطلب مهارات عالية وموارد

تقنية كبيرة، فإن العديد من الدول قد لا تتمكن من توفير هذه الأدوات أو المتخصصين المدربين، مما يشكل عقبة كبيرة أمام قبول الأدلة الرقمية في المحكمة ويؤثر على جودة التحقيقات.

ويتضح مما سبق أن قبول الأدلة الرقمية في المحاكم الجنائية يواجه تحديات معقدة تتنوع بين الجوانب القانونية والتقنية، مما يستوجب التعامل معها بجدية لضمان تحقيق العدالة الجنائية دون الإضرار بحقوق الأفراد. ومن هذا المنطلق، يرى الباحث أن غياب التشريعات الواضحة والموحدة دوليًا يشكل عقبة رئيسية أمام الإعتراف بالأدلة الرقمية، خاصة في ظل تباين القوانين المحلية بين الدول المختلفة، الأمر الذي يؤدي إلى تضارب في الأحكام وخلق ثغرات قانونية قد تؤثر سلبًا على سير العدالة. ولذا، فإن الحاجة الملحة لوضع إطار قانوني موحد يكون متوافقًا مع التطورات التقنية المتسارعة باتت ضرورية لضمان مشروعية هذه الأدلة وحجيتها أمام القضاء.

وفيما يتعلق بالتحديات القانونية، فإن مسألة عدم وضوح المعايير القانونية المعتمدة لقبول الأدلة الرقمية تعتبر من أبرز العقبات التي تؤثر على مدى حجيتها أمام المحاكم. ويرى الباحث أن عدم وجود إطار قانوني واضح يؤدي إلى تفاوت المعايير بين النظم القانونية المختلفة، مما يضعف من إمكانية التعاون القضائي الدولي في القضايا ذات البعد العابر للحدود. ومن هنا، ينبغي على الدول العمل على مواءمة تشريعاتها الوطنية مع المعايير الدولية لضمان تكامل الأدلة الرقمية ضمن منظومة الإثبات الجنائي.

وكما أن مسألة حماية الخصوصية تعد تحديًا قانونيًا معقدًا، إذ أن جمع الأدلة الرقمية قد يتعارض في بعض الحالات مع حقوق الأفراد في الخصوصية وحماية بياناتهم الشخصية، مما يقتضي ضرورة التوازن بين تحقيق العدالة وضمان إحترام الحريات الشخصية. وأما فيما يخص التحديات التقنية، فإن الأدلة الرقمية تتميز

بكونها عرضة للتلاعب والتزوير، مما يستوجب وجود آليات تقنية متطورة للتحقق من مصداقيتها. ويرى الباحث أن التقدم التكنولوجي أتاح أدوات فعالة لضمان سلامة الأدلة الرقمية، مثل تقنيات التشفير والتحقق الرقمي، إلا أن هذه الوسائل لا تزال غير متاحة في بعض الأنظمة القضائية التي تعاني من نقص الموارد الفنية والبشرية المتخصصة في هذا المجال. ولذا، فإن تعزيز القدرات التقنية للمؤسسات القضائية والأجهزة الأمنية يُعدّ خطوة ضرورية لضمان التعامل الأمثل مع الأدلة الرقمية ومنع التلاعب بها.

وإضافةً إلى ذلك، يبرز التحدي المتمثل في عدم توفر الكفاءات المتخصصة في التعامل مع الأدلة الرقمية، إذ أن تحليل هذه الأدلة يحتاج إلى خبراء مؤهلين قادرين على فحصها والتحقق من صحتها وفقًا للمعايير التقنية والقانونية المناسبة. وفي هذا السياق، يرى الباحث أن من الضروري تطوير برامج تدريبية للقضاة والمحامين وخبراء الأدلة الجنائية لتمكينهم من التعامل مع الأدلة الرقمية بكفاءة، بالإضافة إلى تزويد المختبرات الجنائية بأحدث التقنيات التي تضمن دقة وموثوقية عمليات التحليل الرقمي. وفي ضوء هذه التحديات، يوصي الباحث بضرورة تطوير تشريعات وطنية تتوافق مع المعايير الدولية بشأن الأدلة الرقمية، وإيجاد حلول قانونية وتقنية لضمان حجية هذه الأدلة أمام القضاء. وكما يؤكد الباحث على أهمية توفير البنية التحتية التقنية اللازمة لتمكين المؤسسات العدلية من التعامل مع الأدلة الرقمية بكفاءة، بالإضافة إلى تعزيز التعاون الدولي في مجال الأدلة الجنائية الرقمية لضمان تحقيق العدالة الجنائية في القضايا ذات الطابع العابر للحدود. وبذلك، يمكن مواجهة التحديات القانونية والتقنية التي تعترض قبول الأدلة الرقمية، مما يسهم في تعزيز دورها كوسيلة إثبات فعالة في القضاء الجنائي.

## المبحث الثاني: مشروعية الأدلة الرقمية في الإثبات الجنائي

تُعتبر الأدلة الرقمية إحدى الأدوات الحديثة التي تلعب دورًا محوريًا في الكشف عن الجرائم وإثباتها في ظل التطور الرقمي المتسارع. ومع تقدم التكنولوجيا، أصبح من الضروري دراسة مدى مشروعية هذه الأدلة عند إستخدامها في الإجراءات القضائية. ويستعرض هذا المبحث القواعد القانونية التي تنظم إستخدام الأدلة الرقمية في الإثبات الجنائي، مع تسليط الضوء على مدى توافقها مع المبادئ القانونية الأساسية، مثل حقوق المتهم، حماية الخصوصية، وضمانات المحاكمة العادلة. وكما سيتم تقديم دراسة مقارنة بين الأنظمة القانونية المختلفة، مع التركيز على القانونين الأردني والمصري، لتوضيح أوجه التشابه والإختلاف في تنظيم مشروعية الأدلة الرقمية وكيفية تكيف تلك الأنظمة مع التطورات التكنولوجية لضمان تحقيق التوازن بين العدالة الجنائية وحماية حقوق الأفراد.

### المطلب الأول: إطار مشروعية الأدلة الرقمية في الإثبات الجنائي

إن مجرد وجود دليل جنائي يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، إذ يجب أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائي تتوقف على مسألتين رئيستين، الأولى المشروعية، والثانية اليقينية في دلالته على الوقائع المراد إثباتها. (الهيتي، 2010، ص22).

تشير حجية الأدلة الرقمية إلى مدى قبولها وإعتبارها أدلة قانونية معترف بها أمام المحاكم، بحيث يمكن الإعتماد عليها لإثبات أو نفي الوقائع في القضايا الجنائية. وتعتمد هذه الحجية بشكل رئيسي على إلتزام الأدلة الرقمية بالشروط القانونية والإجرائية اللازمة لضمان صحتها وسلامتها من أي تلاعب أو تزوير. (محمودي، 2017، ص918-919).

لذلك يعتبر قبول الأدلة الرقمية في المحاكم مسألة معقدة تتعلق بطبيعة هذه الأدلة ومدى قدرتها على إقناع القاضي أو المحكمة بصحة الوقائع المعروضة، على الرغم من أن الأدلة الرقمية لا تختلف في حجيتها عن الأدلة التقليدية، فإنها تتطلب الإلتزام بمعايير وإجراءات تضمن سلامتها، مثل الحفاظ على سلسلة الحيازة والتأكد من أصالة الأدلة ومصداقيتها. (الجبلي، 2009، ص29).

لحسن تطبيق مبدأ الشرعية الجنائية على الجرائم يتوجب على القاضي إحترام مبدأ الشرعية الإجرائية، أو ما يعرف بشرعية الدليل الجنائي، فلا يسوغ له بناء حكمه على دليل جنائي غير شرعي، أو تحصل عليه المحقق بطرق غير شرعية، حتى يكتسي الدليل القضائي الحجية القانونية في إسناد واقعة الإتهام إلى المتهم أو نفيها عنه، بالإضافة إلى أنه يدخل في مشروعية الدليل الرقمي مسألة تكوين قناعة القاضي بقرار الإدانة للمتهم بناءاً على هذه الأدلة سيما وأنها تم الحصول عليها من الوسائل الإلكترونية المشروعة ومبنية على إجرءات قانونية سليمة. (الجسمي، 2017، ص33 ؛ سلامة، 1981، ص732).

وإنطلاقاً من مبدأ ضرورة أن يكون القضاء نزيهاً فإنه يتوجب عليه أن يبني أحكامه وقراراته على أدلة مشروعة، إذ يشترط في الدليل الجنائي عموماً لقبوله كدليل إثبات أن يتم الحصول عليه بطرق مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون، كما أن الحديث عن مدى مشروعية الدليل الرقمي يجرنا حتماً للحديث عن مدى مشروعية طرق ووسائل الحصول عليه، مثل اللجوء إلى ممارسة إجراءات التفتيش في مختلف الوسائط التقنية، بالإضافة إلى أن هذا الإجراء ينبغي أن يمارس من سلطة التحقيق المختصة، وهي النيابة العامة. (سرور، 1981، ص506).

**الفرع الأول: أقسام حجية الأدلة الرقمية في الأنظمة الإجرائية**

فقد أختلفت الآراء حول مسألة مدى إمكانية الأخذ بالدليل الرقمي على إطلاقه أو أنه يعتمد نسبياً بمعنى هل القاضي حر في الأخذ بما يشاء من الأدلة الرقمية؟ أم أنه مقيد فيما قيده المشرع بالنص عن هذه الأدلة؟ وذلك نظراً لوجود عدة إختلافات بين النظم الإجرائية للإثبات الجنائي، فمنها ما يأخذ بنظام الإثبات الحر، ومنها ما يأخذ بنظام الإثبات المقيد، ومنها ما يأخذ بالنظامين معاً، وسوف نحاول التطرق إلى هذه الأنظمة الإجرائية بإختصار على النحو التالي:

**1- الحجية في نظام الإثبات المقيد:** يقوم نظام الإثبات المقيد على مبدأ أساسي في أن المشرع الجنائي يحدد سلفاً الوسائل والطرق التي يعتمدها في إقامة الدليل الجنائي على مرتكبي الجرائم، فوفقاً لهذا الإتجاه فإن المشرع هو الذي يحدد الأدلة التي يجوز للقاضي اللجوء إليها ويقدر قيمتها الإقناعية، بحيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من توافر الشروط التي حددها القانون، فلا سبيل للإستناد على دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، كما لا دور للقاضي في تقدير القيمة الإستدلالية للدليل، حيث أن القانون يقيد القاضي بقائمة الأدلة التي حددت قيمتها الإثباتية. (أحمد، 1997، ص22).

**2- الحجية في نظام الإثبات الحر:** يسود نظام الإثبات الحر في القوانين الإجرائية اللاتينية بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المعروضة عليه ولا يلزمه القانون بأدلة معينة للإستناد عليها في تكوين قناعته الشخصية، وإن حجية الدليل الرقمي المتحصل من مختلف وسائله لا تثير أي صعوبات متعلقة بمدى حرية تقديم الأدلة لإثبات الجريمة، ولا بمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة بإعتبارها أدلة إثبات في المواد الجنائية أم لا، بل إن العنصر الأساسي وفق هذا المذهب

هو مدى حرية قاضي الموضوع في تقدير هذه الأدلة، ومدى قبول هذه الأدلة، كدليل قائم بذاته وكافٍ لإثبات الإدانة أو البراءة (أحمد، 1997، ص23)، فالقاضي في هذا النظام يتمتع بدور إيجابي في مجال الإثبات وبالمقابل تقييد دور المشرع، وعليه ففي هذا الإتجاه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود على إعتبار أن المشرع لم يعهد إليه مهمة تحديد قائمة أدلة الإثبات، فمسألة قبول الأدلة لا ينال منها سوى مدى إقتناع القاضي بها (أحمد، 1998، ص95).

**3- الحجية في نظام الإثبات المختلط:** يقوم النظام المختلط على أساس الجمع بين خصائص النظام المقيد ونظام الإثبات الحر، إذ يعتمد أساساً أن القانون يحدد أدلة معينة لإثبات وقائع دون بعضها الآخر، وقد يحدد قبول الدليل بشروط معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقدير الأدلة القانونية على غرار القانون الفلسطيني فقد نصت المادة (1/206) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته على أنه"1. تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات. 2..."، مشيراً إلى ما ورد في تفسير محكمة النقض الفلسطينية بأنه: "أما عن أسباب الطعن في مجملها نجد أنها بنيت على أن المحكمة أخطأت في تطبيق القانون وعدم بناء حكمها على الخبرة الفنية. ولما كانت البينة من طرق الإثبات الجزائي في الدعوى أن المادة 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته تفيد المادة 206 فقرة 1 "تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات.". وخاصة وأن الأدلة في الدعوى الجزائية تخضع لمبدأ القناعة الوجدانية للمحكمة، ومحكمة الإستئناف كمحكمة موضوع لها صلاحية وزن البينة حيث أن القاعدة في الأحكام الجزائية وجوب إشتمالها على الأدلة والأسباب الموجبة للتجريم أي إستظهار أركان الجريمة وعناصرها وفقاً للتعريف الذي نص عليه القانون، ولمحكمة الموضوع الصلاحية في الأخذ بما تقتنع به من البينة المقدمة والخبرة من

عداد البينات وهي مسألة موضوعية يترخص قاضي الموضوع بتقديرها وما دام أن محكمة الموضوع لم ترى جدوى بإحداث خبرة خلاف من ثم سماع شهادته كخبير في الدعوى وهو موظف البنك بكر العمري فإنها تكون قد إستعملت خيارها في هذه المسألة ما دام أنها ثبتت حكمها على الوقائع الثابتة في الدعوى والمستمدة من الأدلة المقدمة إليها والتي عالجت هذه الواقعة محكمة الإستئناف أيضاً كما أن هذا لم يكن مدار طعن أمام محكمة الإستئناف مما يجعل من هذه الأسباب أسباباً جديدة لا يستقيم طرحها أمام محكمة النقض مما يستوجب ردها، حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 77 لسنة 2016 بتاريخ 2016/04/04. وقضت محكمة النقض الفلسطينية في حكم اخر بأنه: "ترى هذه المحكمة أن المحكمة الإستئناف حينما عدلت حكم محكمة أول درجة وأدانت الطاعن بالتهمة الأولى المسندة إليه قد أعملت وظيفتها الأساسية وهي إعادة النظر في الحكم المستأنف من الناحيتين القانونية والموضوعية وأعملت صلاحيتها في الرقابة على محكمة أول درجة في تقدير الشهود وأنزلت صحيح حكم القانون والسوابق القضائية بالنسبة للبينة التي ساقتها النيابة العامة ذلك أنه من المقرر قانوناً في المواد الجزائية جواز إثباتها بكافة طرق الإثبات المقررة ما لم ينص القانون على غير ذلك المادة (206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001م وتعديلاته) وأن من ضمن هذه الطرق حسبما نصت عليه المواد 106 ،108 ،109 من قانون البينات رقم 4 لسنة 2001م القرائن القضائية كما أن ما أستقر عليه قضاء هذه المحكمة من أن البينة الظرفية كافية لإثبات التهمة قبل فاعلها الأمر الذي يكون معه النعي على الحكم المطعون فيه بمخالفته للقانون على غير أساس متعيناً رفضه أما عن النعي على الحكم بإجحافه بحقوق الطاعن فإن هذا النعي مردود كذلك لكون هذا السبب ليس من الأسباب الموجبة للطعن بالنقض طبقاً لنص المادة 251 من قانون الإجراءات الجنائية الأمر الذي يتعين

معه رفض الطعن."، حكم محكمة النقض الفلسطينية المنعقدة في غزة في الدعوى الجزائية رقم 205 لسنة 2003 بتاريخ 2005/10/25.

وأن ما أخذ به المشرع الفلسطيني في إثبات المسائل الجنائية هو نظام الإثبات الحر وهذا واضح في نص المادة 206 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م وتعديلاته والتي نصت على إقامة الدعوى الجزائية بكافة طرق الإثبات"1- تقام البينة في الدعاوى الجزائية بجميع طرق الاثبات إلا إذا نص القانون على طريقة معينة للإثبات 2- إذا لم تقم البينة على المتهم قضت المحكمة ببراءته."، بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المعروضة عليه ولا يلزمه القانون بأدلة معينة للإستناد عليها في تكوين قناعته الشخصية.

وكذلك الأمر القانون الأردني يعطي للقاضي الحرية في تقدير الأدلة القانونية، وهذا واضح في نص في المادة 3/2/147 من قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م وتعديلاته "2- تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته الشخصية. 3- إذا نص القانون على طريقة معينة للإثبات وجب التقيد بهذه الطريقة."، وبالتالي فإن المشرع الأردني أخذ في نظام الإثبات الحر في إثبات المسائل الجنائية، بحيث يتمتع القاضي بالحرية الكاملة في هذا النظام في إثبات الوقائع المعروضة أمامه.

وأما بالنسبة للقانون المصري كذلك الأمر نجد أنه يعتمد على مبدأ حرية الإثبات في المواد الجنائية، مع إعطاء القاضي دورًا جوهريًا في تقييم الأدلة، بما يتوافق مع قناعته الشخصية، وهذا واضح في نص المادة 302 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950م وتعديلاته "يحكم القاضي في الدعوى

حسب العقيدة التي تكونت لديه بكامل حريته ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة. وكل قول يثبت أنه صدر من أحد المتهمين أو الشهود تحت وطأة الإكراه أو التهديد به يهدر ولا يعول عليه."، وبذلك يكون المشرع المصري أخذ في نظام الإثبات الحر في إثبات المسائل الجنائية.

وتشير مشروعية الأدلة الرقمية إلى مدى قانونية إستخدام هذه الأدلة كوسائل إثبات أمام المحاكم في القضايا الجنائية. وتستند هذه المشروعية إلى مدى توافق إجراءات جمع الأدلة وتحليلها وتقديمها مع القوانين واللوائح والأنظمة المعمول بها. ولضمان مشروعية الأدلة الرقمية، يجب أن يتم جمعها بطرق قانونية ودون اللجوء إلى وسائل غير مشروعة مثل الإختراق أو التجسس دون إذن قضائي، مما يضمن قبولها كأدلة موثوقة في العملية القضائية. (سلامة، 1981، ص732).

تهدف مشروعية الأدلة إلى حماية حقوق الأفراد وضمان نزاهة الإجراءات القانونية. تعد الأدلة الرقمية غير مشروعة إذا تم جمعها بطرق تنتهك حقوق الخصوصية أو تتعارض مع المبادئ الأساسية للعدالة، مما يسلط الضوء على أهمية الإلتزام بالمعايير القانونية في عملية جمع وإستخدام الأدلة في القضايا الجنائية. (الطوالبة، 2009، ص11).

تعد مشروعية الأدلة الرقمية في فلسطين أساسًا ضروريًا لضمان قبول هذه الأدلة في المحاكمات الجنائية. ويتم تنظيم هذه المشروعية من خلال مجموعة من القوانين واللوائح التي تهدف إلى تحقيق العدالة وحماية حقوق الأفراد. ويتطلب ذلك الإلتزام بالمعايير القانونية أثناء جمع وتحليل الأدلة الرقمية، إلى جانب توفير الضمانات اللازمة لضمان نزاهة الإجراءات وحق الدفاع.

وقد أشار قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م وتعديلاته في أحد نصوصه عن موضوع البصمات والصور مما يعني ذلك قبول الأدلة الرقمية في القضاء الجنائي أمام القاضي الجزائي سيما وأن البصمات والصور من أنواع الأدلة الرقمية، حيث نصت المادة 219 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م وتعديلاته "تقبل في معرض البينة بصمات الأصابع وبصمات راحة اليد وباطن القدم أثناء إجراءات التحقيق أو المحاكمة، ويجوز قبول الصور الشمسية في معرض البينة للتعرف على صاحبها وذلك لمعرفة هوية المتهم ومن له علاقة بالجريمة."، وبالرجوع إلى نصوص القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته نجد من ضمن نصوصه أنه نص على قبول الأدلة الرقمية في الإثبات الجنائي أمام القاضي الجزائي، وهذا واضح في نصوص المواد 57 و 58 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته حيث نصت المادة 57 منه أنه "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات."، وكذلك الأمر نصت المادة 58 منه "تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي."، بالإضافة إلى ما نصت عليه القوانين الفلسطينية حديثاً عن حجية الدليل الإلكتروني بالإثبات وهو نص المادة 44 من القرار بقانون رقم 17 لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة "1. يكون الدليل الإلكتروني رسميًا إذا توافرت فيه شروط السندات الرسمية، ويكون له ذات الحجية المقرر للسند الرسمي. 2. يكون الدليل الإلكتروني عرفيًا إذا توافرت فيه شروط السند العرفي أو السندات غير الموقع عليها، ويكون له ذات الحجية المقرر للسند العرفي والسندات غير الموقع عليها. 3. تعتبر السجلات الإلكترونية التي

يستخدمها التاجر في تنظيم عملياته المالية وقيوده المحاسبية بمثابة دفاتر تجارية. 4. يكون للمستخرج الورقي من الدليل الإلكتروني الحجية المقررة للدليل نفسه بالقدر الذي يكون فيه المستخرج مطابقًا للأصل."، وهذا كله يأكد المشرع الفلسطيني على حجية الأدلة الرقمية في الإثبات الجنائي أمام القاضي الجزائي في التشريع الجنائي الفلسطيني في ظل تبني المشرع الفلسطيني نظام الإثبات الحر في المسائل الجنائية.

**الفرع الثاني: الإجراءات القانونية لحجية الأدلة الرقمية في القانون الفلسطيني والأردني والمصري**

القانون الفلسطيني للجرائم الإلكترونية وهو القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته ينظم بشكل رئيسي كيفية التعامل مع الأدلة الرقمية. وينص على أن الأدلة الرقمية تكون مشروعة إذا تم جمعها وتحليلها وفقًا لإجراءات قانونية واضحة:

- **الموافقة القانونية** :يعتبر قانون الجرائم الإلكترونية الفلسطيني الأدلة الرقمية جزءًا من الأدلة القانونية المعترف بها، بشرط أن تُجمع وتُحلل وفق الإجراءات القانونية السليمة. يتطلب ذلك من الجهات المعنية الحصول على إذن قضائي، مثل أمر التفتيش، والذي يتضمن تقديم طلب يوضح تفاصيل الأدلة المستهدفة والسبب المبرر لجمعها. ويعتبر هذا الإجراء ضروريًا لضمان أن عملية جمع الأدلة تتماشى مع القوانين المعمول بها، مما يعزز من مشروعية الأدلة ويحمي حقوق الأفراد. (الجاسم، 2021، ص181).

- **الإجراءات المحددة** :يشترط القانون الفلسطيني عند جمع الأدلة الرقمية الحصول على إذن من المحكمة أو السلطات القضائية المختصة. وينبغي أن تتم عملية جمع الأدلة بطريقة تحافظ على سلامتها وأصالتها، مع أهمية توثيق جميع الإجراءات المتبعة لضمان قبولها في المحاكم. وتشمل هذه الإجراءات إستخدام أدوات متخصصة، مثل برامج الإسترداد والتحليل، التي تضمن عدم تغيير البيانات الأصلية.

كما يتعين على المحققين الإلتزام بإجراءات دقيقة للحفاظ على سلامة البيانات، وتوثيق كل خطوة في عملية جمع وتحليل الأدلة لضمان موثوقيتها. (الفيل، 2012، ص54).

- **حماية الحقوق** :تسعى القوانين الفلسطينية إلى حماية الحقوق الفردية، بما في ذلك الحق في الخصوصية وحماية البيانات. ويتعين على المحققين ضمان أن عملية جمع الأدلة تتماشى مع الحدود القانونية المقررة، مما يستدعي الإلتزام بالتفويضات القانونية وتجنب أي ممارسات قد تُعتبر إنتهاكًا لحقوق الأفراد. (الحمداني، 2016، ص38–39).

أما بالنسبة لمشروعية الأدلة الرقمية في القانون الأردني، نجد أن القانون الأردني يعترف بالأدلة الرقمية كأدلة قانونية شريطة أن يتم جمعها وفقًا للمعايير القانونية وهذا واضح عندما نص المشرع الأردني في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023م نصت المادة 36 منه "أ–يكون للأدلة المقدمة أو المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الشبكة المعلوماتية أو التقنية المعلومات أو نظام أو برنامج الحاسوب أو مزود الخدمة حجية الإثبات أمام الجهات القضائية. ب– تكون للبيانات والمعلومات التي يتم الحصول عليها من الجهات الرسمية من دول أخرى حجية الإثبات أمام الجهات القضائية الأردنية."، وبهذا يأكد المشرع الأردني على حجية الأدلة الرقمية في الإثبات الجنائي أمام القاضي الجزائي في التشريع الجنائي الأردني في ظل تبني المشرع الأردني نظام الإثبات الحر في المسائل الجنائية.

وبالمقابل نجد أن قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023م يحدد كيفية جمع الأدلة الرقمية وإستخدامها في المحاكم وفقًا لإجراءات قانونية واضحة:

- **الإعتراف بالأدلة الرقمية** :يعترف القانون الأردني بالأدلة الرقمية كأدلة قانونية معتمدة معترف بها، شريطة جمعها وتحليلها وفق الإجراءات القانونية السليمة. ويتوجب على المحققين إستخدام أدوات

وتقنيات موثوقة لضمان دقة وسلامة البيانات، مما يعزز من مصداقية الأدلة المقدمة أمام المحكمة. (عبد العال، 2021، ص700).

- **التقنيات والأدوات** :يتعين على المحققين إستخدام أدوات وتقنيات متقدمة لجمع الأدلة الرقمية، بما في ذلك برامج التحليل الرقمي والأجهزة المتخصصة. وكما يشترط القانون توظيف تقنيات حماية مثل التشفير، لضمان سلامة الأدلة وحمايتها من التلاعب أو التعديل. (عرفة، 2018، ص485).
- **الموافقة القانونية** :يجب أن يتم جمع الأدلة الرقمية بناءً على إذن قضائي، مع ضرورة توثيق كافة الخطوات المتبعة خلال عملية جمع وتحليل هذه الأدلة. يشمل ذلك تقديم طلبات للحصول على أذونات تفتيش أو إذن لجمع البيانات من مصادر محددة. (بهنوس، 2017، ص179).
- **توثيق الإجراءات** :يشترط القانون توثيق جميع العمليات المرتبطة بجمع الأدلة الرقمية، بما في ذلك تسجيل كل خطوة من خطوات الجمع والتحليل والتخزين. ويجب على المحققين إعداد تقارير دقيقة توضح كيفية التعامل مع هذه الأدلة بشكل شامل. (الحمداني، 2016، ص38).
- **الإمتثال للإجراءات** :يتطلب القانون الأردني الحفاظ على سلسلة الحيازة للأدلة الرقمية بدءًا من لحظة جمعها وحتى عرضها أمام المحكمة. ويشمل ذلك توثيق جميع الخطوات المتبعة لضمان عدم تعرض الأدلة لأي تلاعب أو تغيير. (الحمداني، 2016، ص39).

أما بالنسبة لمشروعية الأدلة الرقمية في القانون المصري، نجد أن القانون المصري يعترف بالأدلة الرقمية كأدلة قانونية شريطة أن يتم جمعها وفقًا للمعايير القانونية عندما نص المشرع المصري في قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات نصت المادة 11 منه "يكون للأدلة المستمدة أو

المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو نظام المعلوماتي أو برامج الحاسب، أو أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت الشروط الفنية الواردة في باللائحة التنفيذية."، وأن هذه الشروط واردة في نص المادة 9 من قرار رئيس الوزراء 1699 لسنة 2020 باللائحة التنفيذية للقانون رقم 175 لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات حيث نصت المادة 9 من اللائحة التنفيذية "تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائى إذا توافرت فيها الشروط والضوابط الآتية:

1 – أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التى تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات ، أو أى تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات ، أو أنظمة المعلومات أو البرامج أو الدعامات الالكترونية وغيرها. ومنها على الأخص تقنيةDigital Images Hash ، Write Blocker، وغيرها من التقنيات المماثلة. 2 – أن تكون الأدلة الرقمية ذات صلة بالواقعة وفى إطار الموضوع المطلوب إثباته أو نفيه ، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة. 3 – أن يتم جمع الدليل الرقمى واستخراجه وحفظه وتحريزه بمعرفة مأمورى الضبط القضائى المخول لهم التعامل في هذه النوعية من الأدلة ، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة ، على أن يبين في محاضر الضبط ، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التى تم استخدامها ، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمى بمحضر الضبط أو تقرير الفحص الفنى ، مع ضمان استمرار الحفاظ على الأصل دون عبث به. 4 – في حالة تعذر فحص نسخة الدليل الرقمى وعدم إمكانية التحفظ على الأجهزة محل الفحص لأى سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص

والتحليل. 5 – أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته ."، وبهذا يأكد المشرع المصري على حجية الأدلة الرقمية في الإثبات الجنائي أمام القاضي الجزائي في التشريع الجنائي المصري في ظل تبني المشرع المصري نظام الإثبات الحر في المسائل الجنائية.

وينص قانون مكافحة الجرائم الإلكترونية المصري وهو قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات على أن الأدلة الرقمية يمكن أن تُستخدم في المحاكم بشرط أن تُجمع وتحلل وفقًا للإجراءات القانونية المعتمدة:

- **التشريعات واللوائح** :يعترف القانون المصري بالأدلة الرقمية كأدلة قانونية، شريطة أن يتم جمعها وتحليلها وفقًا للإجراءات القانونية المنصوص عليها. وكما يُلزم القانون بإستخدام تقنيات وأدوات متخصصة لضمان سلامة هذه الأدلة وموثوقيتها. (الطوالبة، 2009، ص9).
- **إجراءات جمع الأدلة** :يتطلب القانون المصري جمع الأدلة الرقمية الحصول على إذن قضائي عند الضرورة، مع الإلتزام بإستخدام تقنيات تضمن سلامة البيانات ودقتها. (قنديل، 2018، ص149).
- **حماية البيانات** :يتطلب القانون إستخدام تقنيات مثل التشفير والنسخ الإحتياطي لضمان حماية الأدلة الرقمية من التلاعب. وكما يفرض القانون الإلتزام بإجراءات دقيقة للحفاظ على سلامة البيانات وسلامتها خلال مراحل جمعها وتحليلها. (المنصوري، 2018، ص73).

- **توثيق سلسلة الحفظ** :يجب توثيق كافة مراحل جمع وتحليل الأدلة الرقمية بدقة، ويتضمن ذلك إعداد تقارير فنية توضح الأساليب المستخدمة في التعامل مع هذه الأدلة وطرق ضمان سلامتها. (الصغير، 2002، ص111-115).

وبالتالي تعتبر الأدلة الرقمية ذات قيمة كبيرة في مجال الإثبات الجنائي نظرًا لدورها الحيوي في كشف الحقائق وتحقيق العدالة. فهي تساهم في تسريع سير التحقيقات وكشف ملابسات الجرائم، بفضل قدرتها على تقديم معلومات دقيقة وفورية تتعلق بالجناة، وتحركاتهم، ووسائل تواصلهم. وتجعل هذه الخصائص الأدلة الرقمية أداة لا غنى عنها للمحققين في جهودهم لكشف الجرائم وتعزيز كفاءة العملية القضائية. (البشري، 2002، ص102).

كما وتتميز الأدلة الرقمية بدقتها العالية وموثوقيتها، مما يعزز فعالية التحقيقات الجنائية ويساهم في توجيه الإتهامات بدقة بناءً على حقائق مثبتة. وتعتبر هذه الموثوقية عنصرًا أساسيًا في الإجراءات القضائية، حيث تساعد في بناء قضايا قوية وتقديم أدلة لا تقبل الجدل في المحاكم. وفي هذا الإطار، تم التأكيد على أن الإستخدام الفعال للأدلة الرقمية يسهم بشكل كبير في تعزيز قدرة المحققين على فهم الجريمة وتوجيه التحقيقات نحو الجناة الحقيقيين. وكما يضمن تقديم أدلة قوية وممكن الدفاع عنها في المحاكم. ويبرز هذا التأكيد الأهمية الإستراتيجية للأدلة الرقمية في تحقيق العدالة والحفاظ على نزاهة الإجراءات القانونية. (أحمد ، 2020، ص1082).

في النظام القانوني الفلسطيني وفق ما نص عليه القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته تعتبر الأدلة الرقمية من الأساليب الحديثة التي

نشأت نتيجة للتطور التكنولوجي. وتشمل هذه الأدلة المعلومات المخزنة أو المنقولة إلكترونيًا، والتي يمكن إستخدامها لتحديد مرتكبي الجرائم أو لتوثيق الحوادث. وتعتمد حجية هذه الأدلة على الإلتزام بالإجراءات القانونية أثناء جمعها وتحليلها، لضمان عدم إنتهاك حقوق الأفراد، خاصة فيما يتعلق بالخصوصية، وبدأت الأدلة الرقمية تلعب دورًا متزايدًا في قضايا الجرائم المرتبطة بالإنترنت بشكل خاص وباقي الجرائم بشكل عام. ومع ذلك، تظل الحاجة ملحة لوضع إطار تشريعي واضح يُحدد كيفية قبول الأدلة الرقمية وفق المعايير الدولية.

أما في القانون الأردني، تم معالجة الأدلة الرقمية بشكل أكثر وضوحًا من خلال التعديلات على قانون أصول المحاكمات الجزائية وقانون الجرائم الإلكترونية الجديد رقم 17 لسنة 2023م. والذي نص على قبول الأدلة الرقمية شرط جمعها بشكل قانوني، حيث تُعد الأردن من الدول الرائدة في تنظيم الجرائم الإلكترونية وإدماج الأدلة الرقمية في القضايا الجنائية. ويجب أن تُجمع الأدلة الرقمية بموجب أمر قضائي لضمان حماية حقوق الأفراد وعدم إنتهاك خصوصيتهم. وفي قضايا الجرائم الإلكترونية مثل الإحتيال والتزوير الإلكتروني، تُعتبر الأدلة الرقمية ضرورية للإثبات، وتُعتمد بشكل رئيسي على الخبراء الذين يتحققون من صحتها وسلامة الإجراءات.

أما في القانون المصري وفق ما نص عليه قانون رقم 175 لسنة 2018م في شأن مكافحة الجرائم التقنية تستخدم الأدلة الرقمية بشكل أساسي في القضايا المرتبطة بالتكنولوجيا، مثل الإحتيال الإلكتروني والقرصنة، وتُعتبر حاسمة في إدانة المتهمين. وكما يشدد القانون المصري على أهمية وجود خبراء معتمدين لتحليل الأدلة الرقمية والتأكد من صحتها وسلامتها. ومع ذلك، يواجه النظام المصري تحديات تتعلق بالبنية التحتية اللازمة لتحليل الأدلة الرقمية وضمان إستخدامها بشكل قانوني.

وتظهر المقارنة بين التشريعات الفلسطينية والأردنية والمصرية أن الأدلة الرقمية تلعب دورًا مهمًا ومتزايدًا في الإثبات الجنائي، لكن هناك تفاوت في مستوى التنظيم والتشريع. وبينما يفتقر القانون الفلسطيني إلى إطار تشريعي واضح للأدلة الرقمية لكنه تناول موضوع الأدلة الرقمية بشكل غير مباشر في نصوص القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته عندما نص ضمن نصوص وخاصة المادة 57 منه أنه يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات من أدلة الإثبات وبما أن الأدلة الرقمية ناتج عن وسائل تكنولوجيا المعلومات فهي من أدلة الإثبات، فإن الأردن ومصر قد أتخذتا خطوات متقدمة بنصوص صريحة في تنظيم هذه الأدلة وقبولها في المحاكم وإعتبارها من أدلة الإثبات، وهذا ما نصت عليه المادة 36 من قانون الجرائم الإلكترونية الإردني رقم 17 لسنة 2023م بأنه يعتبر الدليل المستمد والمستخرج من الأجهزة وشبكات الإلكترونية من أدلة الإثبات أمام الجهات القضائية، والمادة 11 من قانون رقم 175 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الإليكترونية، أو النظام من برامج الحاسب، أو من أى وسيلة تقنية من أدلة الإثبات الجنائي.

ويرى الباحث مما سبق ذكره ومن خلال إستعراض إطار مشروعية الأدلة الرقمية في الإثبات الجنائي أن مبدأ مشروعية الأدلة الرقمية في الإثبات الجنائي يُعد من الركائز الأساسية لضمان نزاهة الإجراءات القانونية وحماية حقوق الأفراد في أي نظام قضائي، خاصةً في ظل التقدم التكنولوجي السريع الذي يشهده العالم اليوم. ويتضح من هذا المبدأ أن التوازن بين إستخدام الأدلة الرقمية وإحترام حقوق الإنسان، ولا سيما الحق في الخصوصية، هو أمر بالغ الأهمية، إذ يتعين على الأنظمة القضائية أن تضع في إعتبارها عدم المساس بهذه الحقوق أثناء إستخدام الأدلة الرقمية. ويعتبر مبدأ مشروعية الأدلة الرقمية من المبادئ التي لا يمكن التفريط

فيها، حيث إن القاضي في أي محكمة جنائية يجب أن يعتمد على الأدلة التي تم جمعها وفقًا للإجراءات القانونية السليمة، بحيث يتم التأكد من أن هذه الأدلة لم تُحصل بطرق تنتهك حقوق الأفراد، مثل التجسس أو الوصول غير المصرح به إلى البيانات الشخصية. ولذا فإن مشروعية الأدلة الرقمية تستدعي إحترام المعايير القانونية الصارمة التي تُحدَّد بوضوح في التشريعات المحلية والدولية، ما يعزز مصداقية الأدلة ويصون حقوق الأفراد.

وبناءً عليه، لا تقتصر مشروعية الأدلة الرقمية على جانب قانوني صرف، بل تشمل أيضًا بعدًا أخلاقيًا يتجسد في التأكد من أن الأدلة تم جمعها وفق معايير تلتزم بمبادئ العدالة وحماية حقوق الإنسان. وهذا التوجه يتماشى مع متطلبات العدالة الجنائية، ويعكس تزاوجًا بين القيم القانونية والأخلاقية في سياق القضايا الجنائية.

## المطلب الثاني: شروط مشروعية الأدلة الرقمية في الإثبات الجنائي

تعتبر الأدلة الرقمية من الوسائل الحديثة التي تلعب دورًا متزايد الأهمية في مجال الإثبات الجنائي، حيث باتت تشكل أساسًا في إثبات العديد من الجرائم المرتبطة بالتكنولوجيا. ولضمان مشروعية هذه الأدلة أمام القضاء، يتوجب الإلتزام بجملة من الشروط والقواعد القانونية التي تضمن حماية الحقوق الفردية وتحقق العدالة. وفي هذا السياق، يشترك كل من القانون الفلسطيني والأردني والمصري في وضع شروط أساسية لمشروعية الأدلة الرقمية، مع وجود تحديات تواجه هذه المشروعية وتؤثر على قبول الأدلة أمام المحاكم. وبناءً على ذلك، ينقسم هذا المطلب إلى فرعين: الأول يتناول الشروط القانونية لمشروعية الأدلة الرقمية، والثاني يناقش التحديات التي تعترض مشروعية هذه الأدلة.

### الفرع الأول: الشروط القانونية لمشروعية الأدلة الرقمية

تُعد الشروط القانونية لمشروعية الأدلة الرقمية عنصرًا أساسيًا لضمان قبولها كأدلة معترف بها أمام المحاكم. وإذ تتطلب هذه الشروط الإلتزام بمجموعة من الضوابط التي تشمل الحصول على إذن قضائي مسبق، واحترام الخصوصية الفردية، وسلامة الإجراءات أثناء جمع وتحليل الأدلة، بالإضافة إلى الإمتثال للقوانين المحلية والدولية، مع التحقق من مصدر الأدلة لضمان مشروعيتها. ويشترك القانون الفلسطيني والأردني والمصري في التأكيد على هذه الشروط كمعيار لضمان نزاهة الأدلة الرقمية ومشروعيتها أمام القضاء. وهذه الشروط هي:

1. **الحصول على إذن قانوني:**

يتوجب جمع الأدلة الرقمية فقط بعد الحصول على إذن مسبق من الجهات القضائية المختصة، مثل النيابة العامة أو المحكمة. ويعتبر الحصول على هذا الإذن القانوني شرطًا أساسيًا لضمان مشروعية الأدلة الرقمية، حيث يهدف إلى حماية حقوق الأفراد ومنع إستخدام أساليب غير قانونية في عملية جمع هذه الأدلة. (حسين، 2012، ص113).

2. **عدم إنتهاك الخصوصية:**

يعد إحترام حق الخصوصية من المبادئ الأساسية التي يجب الإلتزام بها عند جمع الأدلة الرقمية. وينبغي أن تتم عملية جمع الأدلة بطرق لا تنتهك حقوق الأفراد في الخصوصية، إذ إن أي دليل يجمع بطرق تتعارض مع هذه الحقوق قد يُعتبر غير مقبول قانونيا. (الحمداني، 2016، ص4-7).

3. **سلامة الإجراءات:**

يجب أن يتم جمع الأدلة الرقمية وتحليلها وفقًا لإجراءات قانونية واضحة ودقيقة. ويتطلب ذلك توثيق جميع الخطوات المتبعة لضمان عدم تعرض الأدلة للتلاعب أو التعديل. وإن سلامة الإجراءات تقتضي توثيقًا شاملًا لكل مراحل الأدلة الرقمية، بدءًا من جمعها وحتى تقديمها أمام المحكمة، وذلك لضمان عدم وجود أي شك في صحتها. (فرغلي و المسماري ، 2007، ص15).

4. **الإمتثال للقوانين المحلية والدولية:**

يجب أن يتم جمع الأدلة الرقمية وفقًا للقوانين الوطنية والدولية المعنية بحماية البيانات والخصوصية، مع الحفاظ على حقوق الأفراد. وإن الإلتزام بهذه القوانين يعزز مشروعية الأدلة الرقمية ويقلل من إحتمالية رفضها في المحاكم. (أبو عامر، 1971، ص120).

5. **التحقق من مصدر الأدلة:**

يعد التأكد من قانونية مصدر الأدلة الرقمية أمرًا بالغ الأهمية، إذ يجب أن تكون هذه الأدلة قد جُمعت بطرق قانونية، دون اللجوء إلى ممارسات غير مشروعة مثل القرصنة أو الإحتيال. وتعتبر الشرعية القانونية لمصدر الأدلة عنصرًا رئيسيًا في تقييم مشروعيتها، حيث يمكن رفض الأدلة التي تُجمع بوسائل غير قانونية خلال الإجراءات القضائية. (أحمد ، 2020، ص1107-1108).

**الفرع الثاني: التحديات التي تواجه مشروعية الأدلة الرقمية**

على الرغم من أهمية الأدلة الرقمية ودورها الفاعل في إثبات الجرائم، إلا أن مشروعية هذه الأدلة تواجه العديد من التحديات. تتعلق هذه التحديات بمدى التوافق بين استخدام الأدلة الرقمية وحماية حقوق الإنسان، ونقص التشريعات المحدثة لمواكبة التطور التكنولوجي، بالإضافة إلى الصعوبات التقنية المتعلقة بالتحقق من صحة الأدلة ومصدرها. وعلى الرغم من أهمية الأدلة الرقمية في الإثبات الجنائي أمام القضاء الجنائي، إلا أن هناك العديد من التحديات تواجه مشروعية هذه الأدلة، وأن هذه التحديات مشتركة بين القانون الفلسطيني والأردني والمصري، وهذه التحديات هي:

1. **تعارض الأدلة الرقمية مع حقوق الإنسان:**

يمكن أن يؤدي جمع الأدلة الرقمية إلى حدوث تعارض مع بعض الحقوق الأساسية للإنسان، مثل الحق في الخصوصية وحرية التعبير. وغالبًا ما تنشأ التحديات المتعلقة بمشروعية الأدلة الرقمية نتيجة للتداخل بين إستخدام هذه الأدلة وحماية حقوق الإنسان. (الحمداني، 2016، ص37).

2. **غياب التشريعات المحدثة:**

تعاني العديد من الدول من نقص في التشريعات القانونية التي تعالج قضايا مشروعية الأدلة الرقمية. وفي ظل التطور السريع في مجال الجرائم الإلكترونية، يواجه تحديث القوانين والتشريعات بطئًا ملحوظًا، مما يؤدي إلى ظهور فجوات قانونية تؤثر سلبًا على مشروعية هذه الأدلة. (البشري، 2002، ص91).

3. **التحديات التقنية في التحقق من الأدلة:**

تتطلب الأدلة الرقمية تقنيات متقدمة للتحقق من صحتها ومصدرها، وهو ما قد لا يكون متاحًا دائمًا. وتشمل التحديات التقنية صعوبة التأكد من مصداقية الأدلة الرقمية ومدى توافقها مع المعايير القانونية، مما قد يؤثر سلبًا على مشروعية هذه الأدلة في المحاكم. (البشري، 2002، ص123-126).

4. **الإختلافات بين النظم القانونية:**

تتباين الأنظمة القانونية من دولة لأخرى، مما يؤدي إلى إختلاف معايير قبول الأدلة الرقمية ومشروعيتها. وهذا التنوع بين الأنظمة القانونية يساهم في خلق تحديات تتعلق بمشروعية الأدلة الرقمية وإمكانية قبولها في المحاكم. (القاضي، 2022، ص207).

ويرى الباحث ومن خلال دراسة مشروعية الأدلة الرقمية في الإثبات الجنائي إن موضوع مشروعية الأدلة الرقمية في الإثبات الجنائي يمثل أحد القضايا الأكثر حساسية وأهمية في عصرنا الحالي، حيث يشهد العالم تقدمًا تكنولوجيًا غير مسبوق، مما جعل من الأدلة الرقمية أداة حاسمة في محاكمة القضايا الجنائية. ويشمل هذا الموضوع عدة إشتراطات قانونية تهدف إلى ضمان مصداقية الأدلة الرقمية وتوفير العدالة، وذلك من خلال حماية الحقوق الأساسية للأفراد وإتباع الإجراءات القانونية السليمة. ويستعرض الباحث في هذا السياق الشروط اللازمة لضمان مشروعية الأدلة الرقمية، مع مقارنة بين التشريعات الفلسطينية والأردنية والمصرية، ويؤكد على أهمية هذه الشروط في حماية حقوق الأفراد وضمان نزاهة الأنظمة القضائية، وكذلك تجنب الطعن في صحة الأدلة.

أولاً، يُعد الحصول على إذن قانوني من الجهات القضائية المختصة، مثل النيابة العامة أو المحكمة، الخطوة الأولى في مشروعية جمع الأدلة الرقمية. ويتفق القانون الفلسطيني مع القانونين الأردني والمصري في ضرورة الحصول على إذن مسبق قبل جمع الأدلة الرقمية، وهو ما يضمن أن عملية جمع الأدلة تتم في إطار قانوني يحترم حقوق الأفراد. وهذا الشرط يعد ضروريًا لضمان عدم حدوث انتهاك لحقوق الخصوصية أو أي تجاوزات قد تؤثر على مصداقية الأدلة.

الشرط الثاني يتناول إحترام الخصوصية، حيث يتعين أن تخضع عملية جمع الأدلة الرقمية لمعايير قانونية وأخلاقية صارمة. ففي التشريعات الفلسطينية والأردنية والمصرية، يُشترط أن يتم جمع الأدلة الرقمية فقط بموجب إذن قضائي مسبق، وهو ما يعزز إحترام الخصوصية ويحول دون إساءة إستخدام هذه الأدلة. ويشمل هذا المبدأ حماية الحقوق الشخصية للأفراد، ويمنع أن تُستخدم الأدلة الرقمية كأداة للضغط أو التعدي على الحريات الفردية.

أما الشرط الثالث، فيتمثل في سلامة الإجراءات، وهو أمر أساسي لضمان مشروعية الأدلة الرقمية. ومن الضروري أن تتم عملية جمع الأدلة وتحليلها وفقًا لإجراءات دقيقة وموثقة بشكل يسهل التحقق منها في المستقبل. ويشدد الباحث على أهمية هذا الشرط، حيث أنه يوفر ضمانات قانونية ضد التلاعب أو التعديل في الأدلة. والإجراءات القانونية المنصوص عليها تشكل إطارًا يتيح مراجعة كل خطوة من خطوات جمع الأدلة، مما يعزز فرص قبول الأدلة في المحاكم في حالة الطعن في صحتها.

الإمتثال للقوانين المحلية والدولية يمثل أحد الشروط الأساسية الأخرى لمشروعية الأدلة الرقمية. وتتطلب هذه القوانين أن تلتزم الدول المعنية بالقوانين الدولية الخاصة بحماية البيانات الشخصية وحقوق الخصوصية، مثل اتفاقية حماية البيانات الشخصية، وهو ما يعزز مشروعية الأدلة الرقمية ويزيد من قبولها في المحاكم المحلية والدولية. ومع ذلك، يلاحظ الباحث أن بعض هذه القوانين ما زالت بحاجة إلى تحديثات لتواكب التطور التكنولوجي السريع.

أما الشرط الأخير الذي يناقشه الباحث فهو التحقق من مصدر الأدلة، حيث يعد هذا الأمر محوريًا في تحديد مشروعية الأدلة الرقمية. ومن الضروري أن يتم التأكد من أن الأدلة قد تم جمعها بطرق قانونية وشرعية لضمان قبولها أمام المحكمة. ويشدد الباحث على أهمية التحقق الدقيق من مصدر الأدلة، لأن الأدلة التي يتم الحصول عليها من مصادر غير قانونية، مثل القرصنة، يتم رفضها تلقائيًا في النظام القضائي.

إلى جانب هذه الشروط، يتناول الباحث التحديات الكبيرة التي قد تواجه مشروعية الأدلة الرقمية، خصوصًا في ما يتعلق بتعارضها مع حقوق الإنسان، مثل الحق في الخصوصية وحرية التعبير. وكما أن غياب التشريعات المحدثة في بعض البلدان يشكل عائقًا كبيرًا في التكيف مع التطورات التكنولوجية السريعة، مما يزيد من تعقيد

القضايا المرتبطة بالجرائم الإلكترونية. وأما التحديات التقنية المتعلقة بالتحقق من صحة الأدلة الرقمية، فهي تعكس نقصًا في الأدوات التكنولوجية المتطورة التي تتيح فحص الأدلة بسهولة وموثوقية، مما يعرقل قبول هذه الأدلة في بعض الحالات. وأخيرًا، تختلف طرق قبول الأدلة الرقمية بين النظم القانونية المختلفة، مما يؤدي إلى إشكالات في تطبيق هذه الأدلة وتفسيرها بشكل موحد.

إستنادًا لكل هذه التفاصيل السابقة، يمكن للباحث أن يخلص إلى أن مشروعية الأدلة الرقمية في الإثبات الجنائي تتطلب تطورًا مستمرًا في التشريعات، مع ضرورة تحديث القوانين لتواكب التغيرات التكنولوجية السريعة. وبالإضافة إلى ذلك، يعد تدريب المختصين في جمع وتحليل الأدلة الرقمية أمرًا بالغ الأهمية لضمان مصداقيتها وقبولها في المحاكم.

## النتائج والتوصيات:

حاولنا في هذه الدراسة تبيان الأدلة الرقمية وحجيتها في الإثبات الجنائي الفلسطيني دراسة مقارنة مع القانون الأردني والمصري على ضوء أحكام القرار بقانون رقم 10 لسنة 2018 م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته وقانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م دراسة مقاررنة مع القوانين الأردنية والمصرية ذات العلاقة من خلال فصلين ناقشنا في الأول ماهية الأدلة الرقمية في الإثبات الجنائي وتعريفها وخصائصها وأنواعها ومصادرها وتناولنا في الفصل الثاني حجية الأدلة الرقمية في الإثبات الجنائي عن طريق بحث مقبولية الأدلة الرقمية في الإثبات الجنائي ودراسة مشروعية الأدلة الرقمية في الإثبات الجنائي. ولئن كانت خاتمة هذه الدراسة هي إبراز لأهم النتائج التي توصلت إليها، وبيان لأهم المقترحات التي يمكن التوصية بها، فقد توصلت في هذه الدراسة إلى عدد من النتائج والتوصيات والتي يمكن إجمال أهمها فيما يأتي:

**النتائج:**

1. تبين لنا أن الأدلة الرقمية أصبحت ضرورة ملحة في التحقيقات الجنائية لتتبع الجرائم الإلكترونية والتقليدية، لكنها تواجه تحديات تقنية في التشريعات الفلسطينية والأردنية والمصرية.
2. غياب تعريف واضح وشروط موحدة لقبول الأدلة الرقمية أدى إلى تفاوت في تفسيرها وقبولها أمام المحاكم الفلسطينية.
3. إن كل من التشريع الفلسطيني الأردني والمصري تناولا تنظيمًا واضحًا للأدلة الرقمية.
4. الأدلة الرقمية تعد عنصرًا حيويًا في الجرائم العابرة للحدود لتتبع الجناة وتعقب الأنشطة الإجرامية.

5. إن كل من التشريعات الفلسطينية والأردنية والمصرية تؤكد على حجية الأدلة الرقمية في الإثبات الجنائي.
6. الأدلة الرقمية وبالرغم من قيمتها العالية، تحتاج إلى إجراءات صارمة لضمان مشروعيتها وعدم إنتهاك الخصوصية.
7. هناك حاجة ماسة لتأهيل الكوادر القضائية والأمنية للتعامل مع الخصائص الفريدة والتحديات المرتبطة بالأدلة الرقمية.

**التوصيات:**

وبعد بيان نتائج الدراسة فإننا نورد بعض التوصيات بالإضافة لما ورد ضمن الدراسة والتي نقترح أن يتم الأخذ بها من قبل المشرع الفلسطيني:

1. أن يقوم المشرع الفلسطيني بمواكبة إصدار قوانين شاملة وواضحة ومترابطة ومتكاملة تُعنى بتنظيم الأدلة الرقمية، مع وضع تعريف قانوني واضح للأدلة الرقمية مع تحديد شروط مشروعيتها وقبولها أمام المحاكم، بما يتماشى مع التطورات التقنية الحديثة.
2. نقترح أن يتم تطوير الوحدات المتخصصة بالأدلة الرقمية ضمن الهيئات القضائية والأمنية الفلسطينية، تضم خبراء في مجالات التحليل الرقمي والجرائم الإلكترونية لدعم التحقيقات بشكل فعّال.
3. نقترح أن يتم توفير برامج تدريبية مستمرة للقضاة وأعضاء النيابة العامة حول التعامل مع الأدلة الرقمية، بدءًا من جمعها وتحليلها وصولًا إلى تقديمها كدليل إثبات أمام المحاكم.
4. نوصي جهات تطبيق القانون بتحسين البنية التحتية التقنية في فلسطين، بما يتيح جمع الأدلة الرقمية وحفظها وتحليلها بطرق تضمن مصداقيتها وسلامتها.

5. نوصي بتعزيز الضمانات القانونية لحماية الخصوصية أثناء عمليات جمع الأدلة الرقمية وتحليلها، مع وضع قيود صارمة على استخدامها بما يحقق التوازن بين تحقيق العدالة وحماية الحقوق الفردية.
6. نوصي بإنشاء آليات تعاون قانوني بين فلسطين والدول المقارنة لتبادل الخبرات في مجال الأدلة الرقمية، مع التركيز على وضع معايير موحدة لقبول الأدلة الرقمية وتطوير تشريعات جنائية مشتركة تعالج التحديات التقنية والقانونية، للإستفادة من تجاربهم في تحسين الأطر القانونية والإجرائية.

## المراجع


أولاً: المصادر

القانون الأساسي المعدل لسنة 2003م.

قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م وتعديلاته.

القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته.

قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م وتعديلاته.

قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023م.

قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950م وتعديلاته.

قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018م.

ثانياً: المعاجم

الإمام محمد بن مكرم بن منظور، لسان العرب.

ثالثاً: الكتب

المناعسة، أ. ، و الزعبي، ج، (2014)، *جرائم نظم تقنية المعلومات الإلكترونية "دراسة مقارنة"* ، (ط 1)، دار الثقافة للنشر والتوزيع، عمان.

عليان، ر. ، الدبسي، م، (2003)، *وسائل الإتصال وتكنولوجيا التعليم*، ط 2، دار صفاء للنشر والتوزيع، عمان.

العبادي، م، (2010)، *القناعة الوجدانية للقاضي الجزائي ورقابة القضاء عليها* ، دار الفكر، عمان.

الشريف، م، (2002)، *النظرية العامة للإثبات الجنائي*، دار النهضة العربية، القاهرة.

المناعسة، أ. ، والزعبي، ج، (2014)، *جرائم تقنية المعلومات "دراسة مقارنة"* ، ط1، دار الثقافة للنشر والتوزيع، عمان.

عوض، م، (1971)، *قانون الإجراءات الجنائية السوداني معلقا عليه*، المطبعة العالمية، القاهرة.

إبراهيم، خ، (2010)، *فن التحقيق الجنائي في الجرائم الإلكترونية*، ط1، دار الفكر الجامعي، الإسكندرية.

أبو القاسم، أ، (2013)، *الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص*، الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية.

عزت، ف، (2010)، *الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية*، ط1، دار الفكر القانوني للنشر والتوزيع، الإسكندرية.

حنفي، ح، (2017)، *الدليل الإلكتروني ودوره في المجال الجنائي*، ط1، دار النهضة العربية، القاهرة.

الصغير، ج، (2002)، *أدلة الإثبات الجنائي والتكنولوجيا الحديثة*، دار النهضة العربية، القاهرة.

أحمد، أ، (1994)، *الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص*، الجزء الأول، أكادمية نايف للعلوم الأمنية، الرياض.

القاضي، ر، (2011)، *مكافحة الجرائم المعلوماتية في التشريعات المقارنة والمواثيق الدولية*، ط1، دار النهضة العربية، القاهرة.

الطحاوي، أ، (2015)، *الأدلة الإلكترونية ودورها في الإثبات الجنائي دراسة مقارنة*، دار النهضة العربية، القاهرة.

الهيتي، م، (2010)، *التحقيق الجنائي والأدلة الجرمية*، ط 1، دار المناهج للنشر والتوزيع، عمان.

أبو عامر، م، (2009)، *الإجرءات الجنائية*، دار الجامعة الجديدة، الإسكندرية.

سلامة، م، (1981)، *الإجرءات الجنائية معلقاً عليه الفقة والقضاء*، دار الفكر العربي، القاهرة.

سرور، أ، (1981)، *الوسيط في قانون الإجراءات الجنائية*، ط4، المجلد الأول، دار النهضة العربية، القاهرة.

أحمد، ه، (1997)، *حجية المخرجات الكمبيوترية*، ط1، دار النهضة العربية، القاهرة.

أحمد، ه، (1998)، *تنفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي "دراسة مقارنة"*، دار النهضة العربية، القاهرة.

الفيل، ع، (2012)، *إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية*، دراسة مقارنة، ط 1، المكتب الجامعي الحديث، بغداد.

قنديل، أ، (2018)، *الوسائل الإلكترونية ودورها في الإثبات الجنائي*، دراسة مقارنة، ط1، دار الجامعة الجديدة للنشر، الإسكندرية.

حسين، س، (2012)، *الأدلة المتحصلة من الحاسب وحجيتها في الإثبات الجنائي*، دار الكتب القانونية، مصر.

فرغلي، ع. ، المسماري، م، (2007)، *الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية*، (د.ط)، جامعة نايف العربية للعلوم الأمنية، الرياض.

يوسف، أ، (2009)، *الجرائم المعلوماتية على شبكة الإنترنت*، دار المطبوعات الجامعية، الإسكندرية.
أحمد، ه، (2000)، *إلتزام الشاهد بالإعلام في الجريمة المعلوماتية "دراسة مقارنة"*، دار النهضة العربية، القاهرة.
أحمد، ه، (2002)، *الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001*، دار النهضة العربية، القاهرة.
بن يونس، ع، (2008)، *الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية*، دار النهضة العربية، القاهرة.

رابعاً: الرسائل الجامعية

دراوشة، ح، (2015)، *مدى مشروعية الأدلة المستمدة من الوسائل العلمية الحديثة في الإثبات الجزائي – دراسة مقارنة –*، كلية الشريعة والقانون، جامعة العلوم الإسلامية العالمية، الأردن.
العجارمة، ن، (2019)، *حجية التسجيلات الصوتية والمرئية في الإثبات الجنائي*، جامعة الشرق الأوسط، الأردن.
العازمني، ف، (2012)، *"الإجراءات الجنائية المعلوماتية"*، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، جمهورية مصر العربية.
الحسيني، أ، (2013)، *الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية*، رسالة دكتوراه، جامعة عين شمس، جمهورية مصر العربية.
فرغلي وآخر، ع، (2007)، *الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية – دراسة تطبيقية مقارنة –*، جامعة نايف العربية للعلوم الأمنية، الرياض.
الجبلي، ط، (2009)، *الدليل الرقمي في مجال الإثبات الجنائي*، أكادمية الدراسات العليا، طرابلس.
بوكرة، رش، (2017)، *الحماية الجزائية للتعاملات الإلكترونية*، رسالة دكتوراه، كلية الحقوق، جامعة الجيلاني اليابس، الجزائر.
المنصوري، س، (2018)، *تطبيق مبدأ الإقتناع القضائي على الدليل الإلكتروني*، كلية الحقوق، قسم القانون العام، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة.

خامساً: البحوث

جيتس، ب، (1998)، المعلوماتية بعد الإنترنت – طريق المستقبل (ع. رضوان، مترجم)، *مجلة عالم المعرفة، (231)*، الكويت.

الحمداني، م، (2016)، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، *مجلة الحقوق، (18)*، جامعة النهرين، بغداد.

البشري، م، (2002)، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، *المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد33*، جامعة نايف العربية للعلوم الأمنية، الرياض.

أرحومة، م، (2009)، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، *أكادمية الدراسات العليا*، طرابلس.

العربي، م، (2016)، دور الدليل الرقمي في الإثبات الجنائي، *مجلة البحوث القانونية*، جامعة مصراته، ليبيا.

بهنوس، آ، (2017)، الدليل الرقمي في الإجراءات الجنائية، *المجلة الأكاديمية للبحث القانوني*، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، الجزائر.

عبد العال، أ، (2021)، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية "دراسة تحليلية مقارنة"، *مجلة البحوث القانونية والإقتصادية*، كلية الحقوق، جامعة المنصورة، مصر.

نجيب، ه، (2014)، حجية الدليل الإلكتروني في الإثبات الجنائي، *المجلة الجنائية القومية*، المركز القومي للبحوث الإجتماعية والجنائية، القاهرة.

القاضي، ر، (2022)، الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم 175 لسن 2018 ولائحته التنفيذية والتشريعات المقارنة والمواثيق الدولية، *مجلة القانون والتكنولوجيا*، مصر.

أحمد، ع، (2020)، الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية "دراسة فقهية مقارنة"، *المجلة العلمية*، كلية الشريعة والقانون بأسيوط، جامعة الأزهر، مصر.

الجاسم، ي، (2021)، حجية الأدلة الرقمية في النظام القضائي الإسلامي، *مجلة البحوث الفقهية الإسلامية*، تركيا.

محمودي، ن، (2017)، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، *مجلة الباحث الدراسات الأكاديمية*، الجزائر.

عرفة، م، (2018)، مدى حجية الأدلة الإلكترونية الرقمية في الإثبات في المواد الجنائية "دراسة تحليلية تطبيقية مقارنة"، *مجلة كلية الحقوق للبحوث القانونية والإقتصادية*، كلية الحقوق، جامعة الإسكندرية، مصر.

الحوامدة، ل، (2021)، حجية الأدلة الرقمية في الإثبات الجنائي "دراسة تحليلية مقارنة"، *مجلة البحوث الفقهية والقانونية*، كلية الشريعة والقانون، جامعة الأزهر، مصر.

أبو عامر، م، (1971)، القيود القضائية على حرية القاضي الجنائي في الإقناع، *مجلة القانون والإقتصاد*، جامعة القاهرة، مصر.

الشهري، أ، (2022)، حجية الدليل الرقمي في النظام السعودي والفقة الإسلامي "دراسة مقارنة في ضوء نظام الإثبات"، *مجلة كلية الدراسات الإسلامية والعربية للبنات بكفر الشيخ*، جامعة الأزهر، مصر.

الجسمي، خ، (2017)، الإثبات الجنائي بالأدلة الرقمية، *مجلة القانون المغربي*، دار السلام للطباعة والنشر، المغرب.

الطوالبة، ع، (2009)، مشروعية الدليل الإلكتروني المستمد من الدليل التفتيش الجنائي "دراسة مقارنة"، *مركز الإعلام الأمني*، البحرين.

المعمري، م، (2018)، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، *مجلة كلية القانون الكويتية العالمية*، الكويت.

# The Digital Evidence and the Authenticity to Prove It in Palestinian Criminal Proceedings (A Comparative Study)

**wael ahmad saif eid**
**Dr. Abdullatif Rabaia**
**Dr. issam al'atrash**
**Dr. mohammad shtayeh**

## Abstract

The main objective of this study is to distinguish digital evidence and its validity in certainty and the Palestinian comparative study with Jordanian and Palestinian law. The researcher used in writing this study the clear descriptive analytical lesson and the comparative approach. This research reached a set of the most prominent of which is the absence of a unified definition and conditions for accepting digital evidence, meaning a difference in its trial and acceptance before the Palestinian court. Both Palestinian, Jordanian and Egyptian laws emphasize the validity of digital evidence in proof, and it has been proven that the Palestinian legislator should keep pace with the issuance of comprehensive, clear, integrated and comprehensive laws concerned with digital evidence, with setting a definition of digital evidence with specifying the conditions of its project and acceptance before the courts, including a clear definition with technology, in addition to legal guarantees to protect privacy during the collection and analysis of digital evidence, with a good position for effective effectiveness including the balance between achieving justice and protecting rights.

Keywords: Digital Evidence, Electronic Evidence, Traditional Evidence, Law.