الادلة الرقمية في الاجراءات الجنائية:
اشكاليات القبول والتوثيق

م.م عبد الرحمن حسين كريم
جامعة كركوك/ كلية الاداب

المقدمة

في ظل التطور التكنولوجي المتسارع، أصبحت الأدلة الرقمية تلعب دوراً محورياً في الإجراءات الجنائية، حيث تُشكل مصدراً رئيسياً لإثبات الجرائم في العصر الرقمي. ومع ذلك، فإن استخدام هذه الأدلة يثير تحديات كبيرة تتعلق بقبولها في المحاكم، وبتوثيقها، وصحتها، وحجيتها القانونية، خاصةً في ظل عدم وجود معايير موحدة تحكم عملية جمعها وتحليلها واعتمادها أمام القضاء.

وتكمن هذه الإشكاليات في طبيعة مصادر الأدلة الرقمية، مثل البيانات المستخرجة من الهواتف الذكية، والحواسيب، ومنصات التواصل الاجتماعي، مما يتطلب تكييف آليات قانونية وفنية تضمن سلامة هذه الأدلة وقانونية استخدامها وحجيتها في الإثبات.

مشكلة البحث

تكمن مشكلة البحث في التحديات القانونية والفنية المرتبطة بقبول الأدلة الرقمية وتوثيقها ومنحها الحجية القانونية ضمن الإجراءات الجنائية، في ظل غياب إطار قانوني موحد ومعايير واضحة تنظم كيفية جمع هذه الأدلة وتحليلها واعتمادها أمام الجهات القضائية، مما يثير إشكاليات جوهرية تتعلق بسلامة الإجراءات وضمانات المحاكمة العادلة.

1. **عدم وضوح المعايير القانونية** التي تحكم عملية جمع الأدلة الرقمية وتحليلها.
2. **ضعف الإطار التشريعي** في العديد من الدول، مما يؤدي إلى اختلاف التطبيقات القضائية.
3. **التحديات الفنية** المتعلقة باحتمال التلاعب بالأدلة الرقمية أو تلفها.

10.70126/aqj.v9i18.296

أهمية البحث

يأتي هذا البحث ليُسلط الضوء على أهمية الأدلة الرقمية في الإجراءات الجنائية، ويساهم في:

1. **تطوير الإطار التشريعي** لضمان قبول الأدلة الرقمية في المحاكم.
2. **تعزيز الثقة** في الأدلة الرقمية من خلال وضع معايير واضحة لجمعها وتحليلها.
3. **توفير حلول عملية** للتحديات الفنية والقانونية التي تواجه المحققين والقضاة.
4. **رفع مستوى الوعي** بأهمية التوثيق الدقيق للأدلة الرقمية لضمان حجيتها في الإثبات.

أهداف البحث

يهدف هذا البحث إلى:

1. **تحليل الإشكاليات القانونية والفنية** المتعلقة بقبول الأدلة الرقمية في الإجراءات الجنائية.
2. **دراسة المعايير الدولية** والمقارنة بين التشريعات المختلفة في مجال الأدلة الرقمية.
3. **تقديم توصيات** لتعزيز موثوقية الأدلة الرقمية وتوثيقها.
4. **تطوير إطار عمل** يضمن سلامة الأدلة الرقمية من مرحلة الجمع حتى العرض في المحكمة.

منهج البحث

يعتمد هذا البحث على **منهجية تحليلية** تشمل:

1. **المنهج الوصفي** :لوصف طبيعة الأدلة الرقمية وإشكالياتها في الإجراءات الجنائية.
2. **المنهج التحليلي** :لتحليل التشريعات الدولية والمحلية المتعلقة بالأدلة الرقمية.

المبحث الأول: الإطار النظري للأدلة الرقمية

تُعد الأدلة الرقمية من أبرز المستجدات في مجال الإثبات الجنائي والمدني، حيث أصبحت التكنولوجيا الحديثة مصدرًا رئيسيًا للمعلومات المتعلقة بالجرائم والمعاملات القانونية. ومع تطور الوسائل الرقمية، باتت هذه الأدلة تلعب دورًا حيويًا في كشف الحقائق وتعزيز العدالة. إلا أن استخدامها في المحاكم يستدعي فهماً عميقًا للإطار النظري الذي يحكمها، والذي يتضمن تعريفها، خصائصها، وأهميتها القانونية

المطلب الأول: مفهوم الأدلة الرقمية وأنواعها

مع التطور السريع في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في مختلف جوانب الحياة، أصبحت الأدلة الرقمية عنصرًا أساسيًا في العديد من القضايا القانونية والجنائية. وتشمل هذه الأدلة كل ما يمكن استخراجه من الأجهزة الإلكترونية أو الشبكات الرقمية، مثل البيانات المخزنة أو المرسلة. لفهم أهمية الأدلة الرقمية ودورها في تعزيز العدالة، يتطلب الأمر توضيح مفهومها الدقيق واستعراض أنواعها المختلفة التي تلعب دورًا محوريًا في التحقيقات والإجراءات القضائية.

الفرع الاول :تعريف الأدلة الرقمية

الأدلة الرقمية هي **البيانات والمعلومات التي يتم إنشاؤها أو تخزينها أو نقلها بواسطة الأجهزة الإلكترونية**، والتي يمكن استخدامها في الإجراءات القانونية والتحقيقات الجنائية. تُعرف الأدلة الرقمية بأنها "أي معلومات ذات قيمة إثباتية يتم الحصول عليها من مصادر رقمية" [1]. تشمل هذه الأدلة نطاقًا واسعًا من البيانات، مثل النصوص، والصور، والفيديوهات، وبيانات الاتصالات، وبيانات تحديد الموقع.

في القانون العراقي، يُولي النظام القضائي أهمية خاصة لتحديد معايير جمع وحفظ وتحليل الأدلة الرقمية بما يضمن مصداقيتها وسلامتها. وتستلزم هذه المعايير أن تكون الأدلة الرقمية قد جُمعت بطريقة تحترم مبادئ السلسلة الإجرائية (Chain of Custody)، بحيث يتمكن القاضي أو المحكمة من التأكد من عدم تعرضها للتلاعب أو التغيير منذ لحظة جمعها[2].

إن الاعتماد المتزايد على التكنولوجيا في الحياة اليومية وفي عمليات الاتصال والتخزين الرقمي جعل من الأدلة الرقمية عنصرًا أساسيًا في إجراءات التحقيقات الجنائية، خاصةً في

[1] محمد أحمد علي. 2018، الأدلة الرقمية في الإجراءات الجنائية. دار النهضة العربية، القاهرة،. ص 55

[2] أحمد ،محمد علي،2020 ،الأدلة الرقمية في الإجراءات الجنائية، دار الثقافة للنشر والتوزيع، بغداد، ، ص. 9

10.70126/aqj.v9i18.296

قضايا الجرائم الإلكترونية والجرائم التي تستعمل التكنولوجيا كوسيلة تنفيذ أو إخفاء للجرائم. ومن هنا، يتوجب على الجهات القضائية والنيابية والفنية الالتزام بتطوير القدرات والخبرات اللازمة للتعامل مع هذه الأدلة بما يكفل تحقيق العدالة وحماية حقوق الأفراد في ظل التحديات التي تفرضها الطبيعة التقنية للأدلة الرقمية.

تتميز الأدلة الرقمية بأنها غير ملموسة وتعتمد بشكل كلي على التكنولوجيا في استخراجها وتحليلها، فإن الأدلة الرقمية تشكل تحديًا كبيرًا في الإثبات الجنائي بسبب طبيعتها غير الملموسة واعتمادها على التقنيات الحديثة[3].

الفرع الثاني : أنواع الأدلة الرقمية

تتنوع الأدلة الرقمية وفقًا لمصادرها وطبيعتها، ومن أبرز أنواعها:

1. **بيانات الهواتف الذكية:**

تُعد الهواتف الذكية من أهم مصادر الأدلة الرقمية في العصر الحديث. تحتوي الهواتف على كميات هائلة من البيانات، مثل الرسائل النصية، وسجلات المكالمات، وتسجيلات الصوت، وبيانات تحديد الموقع (GPS)، فإن الهواتف الذكية أصبحت "مستودعًا" للبيانات الشخصية التي يمكن استخدامها في التحقيقات الجنائية. على سبيل المثال، في قضايا الابتزاز الإلكتروني، يمكن لسجلات المكالمات والرسائل النصية أن تكون أدلة حاسمة[4].

2. **بيانات الحواسيب:**

تشمل البيانات المخزنة على أجهزة الكمبيوتر، مثل الملفات النصية، ورسائل البريد الإلكتروني، وسجلات الإنترنت. تُعتبر الحواسيب مصدرًا رئيسيًا للأدلة في جرائم مثل

[3] خالد، عبد الرحمن. 2020، التقنيات الحديثة في جمع الأدلة الرقمية. مركز الدراسات القضائية، الرياض،. ص 112

[4] محمد، فاطمة الزهراء. (2019). إشكاليات الأدلة الرقمية في التشريع المصري. مجلة القانون والاقتصاد، جامعة القاهرة، العدد 88، ص. 75–95.

القرصنة الإلكترونية، وانتحال الشخصية، والاحتيال المالي. على سبيل المثال، في قضايا الاحتيال عبر البريد الإلكتروني، يمكن لسجلات البريد الإلكتروني أن توفر أدلة قوية على هوية الجاني .[5]

3. **بيانات الشبكات:**

تشمل المعلومات المنقولة عبر الشبكات، مثل سجلات خوادم الإنترنت (Server Logs)، وبيانات المرور الشبكي (Network Traffic). تُستخدم هذه البيانات في التحقيقات المتعلقة بالجرائم الإلكترونية والاختراقات. على سبيل المثال، في قضايا الاختراق الإلكتروني، يمكن لسجلات الشبكة أن تكشف عن عنوان IP المستخدم في الهجوم.[6]

4. **السحابة الإلكترونية:(Cloud)**

مع تزايد استخدام خدمات التخزين السحابي، أصبحت السحابة مصدرًا مهمًا للأدلة الرقمية. تشمل البيانات المخزنة على السحابة ملفات، وصور، وفيديوهات، وبيانات تطبيقات ، فإن تحليل البيانات السحابية يتطلب تقنيات متقدمة بسبب طبيعتها الموزعة. على سبيل المثال، في قضايا انتهاك الخصوصية، يمكن لبيانات التطبيقات المخزنة على السحابة أن توفر أدلة على الأنشطة غير المشروعة[7].

المطلب الثاني: خصائص الأدلة الرقمية

أصبحت الأدلة الرقمية جزءًا لا غنى عنه في القضايا القانونية مع التقدم التكنولوجي وانتشار استخدام الأجهزة الرقمية. فهي تتضمن أي معلومات أو بيانات يتم تخزينها أو نقلها

[5] خليل، محمود عبد الكريم. (2020). التحقيق الجنائي في الجرائم الإلكترونية. دار الجامعة الجديدة، الإسكندرية.ص50

[6] يوسف، ندى حسن. (2021). "دور البيانات الرقمية في إثبات الجرائم المعلوماتية". المجلة العراقية للعلوم القانونية والسياسية، المجلد 10، العدد 2، ص. 113–130.

[7] علي حسن. الأدلة الإلكترونية في الجرائم المعلوماتية. دار الثقافة للنشر، عمان، 2017. ص 200–220, 175–190.

10.70126/aqj.v9i18.296

عبر الوسائل الإلكترونية. ويُعد فهم مفهوم الأدلة الرقمية وأنواعها خطوة أساسية لتقدير دورها وأهميتها في العمليات القضائية، خاصة في ظل تنامي الاعتماد على التكنولوجيا في مختلف جوانب الحياة.

الفرع الاول :الطبيعة غير الملموسة للأدلة الرقمية

تُعدُّ الطبيعة غير الملموسة للأدلة الرقمية من السمات الجوهرية التي تميز هذا النوع من الأدلة عن الأدلة التقليدية في الإجراءات القانونية، خاصةً في سياق القانون العراقي. تكمن أهمية هذه الخاصية في تأثيرها المباشر على كيفية جمع الأدلة، حفظها، تحليلها وتقديمها أمام الجهات القضائية. وفيما يلي تفصيل موسع لهذه الطبيعة مع استعراض التحديات القانونية والإجرائية والمراجع ذات الصلة:[8]

1.السمات والخصائص

أ. **الغياب الفيزيائي:**

تختلف الأدلة الرقمية عن الأدلة المادية، إذ أنها لا تتميز بالحضور الفيزيائي؛ فهي تتواجد على شكل بيانات ومعلومات مخزنة إلكترونيًا على أجهزة الحاسوب، الهواتف الذكية، الخوادم أو غيرها من الوسائط الرقمية. هذا الغياب الفيزيائي يجعل عملية إثبات صحتها وسلامتها أكثر تعقيدًا، حيث يتطلب ذلك استخدام تقنيات وأساليب فنية دقيقة لضمان عدم تعديلها أو التلاعب بها.

ب. **الاعتماد على التكنولوجيا:**

تعتمد الأدلة الرقمية بشكل كامل على التكنولوجيا في استخراجها وتحليلها، ما يستلزم وجود مختصين يمتلكون معرفة تقنية عالية لإثبات سلامة البيانات. على سبيل المثال، فإن عملية استخراج سجل المكالمات أو بيانات

[8] قانون الجرائم الإلكترونية العراقي رقم 28 لسنة 2015. (2015). الجمهورية العراقية: الهيئة التشريعية.

تحديد الموقع تعتمد على برامج وأنظمة تحليل متطورة لا يمكن التحقق من صحتها إلا من خلال آليات تقنية دقيقة.

ت. **قابلية التلاعب والتغيير:**

نظرًا لطبيعتها الإلكترونية، يمكن تعديل أو تغيير الأدلة الرقمية بسهولة إذا لم تُتّبع سلسلة الحفظ (Chain of Custody) والإجراءات الفنية اللازمة. هذا يفرض على الجهات القضائية في العراق تطبيق معايير صارمة لجمع وتخزين الأدلة الرقمية، بحيث تكون هناك توثيق كامل لكل خطوة من خطوات التعامل معها، بدءًا من نقطة جمعها مرورًا بنقلها وتحليلها، وصولاً إلى تقديمها في المحكمة.

2.التحديات القانونية والإجرائية

أ. **سلسلة الحفظ والإثبات:**

يُعتبر الحفاظ على سلسلة الحفظ من أهم المتطلبات في التعامل مع الأدلة الرقمية، إذ يجب توثيق كافة العمليات التي تتعرض لها الأدلة منذ لحظة جمعها وحتى تقديمها أمام المحكمة. في القانون العراقي، تُعتبر سلسلة الحفظ الدليل الأساسي على سلامة الأدلة وعدم تعرضها للتلاعب. وقد أكدت العديد من الدراسات القانونية مثل "دور سلسلة الحفظ في إثبات الأدلة الرقمية" على أهمية اتباع معايير دقيقة في هذا الشأن[9].

ب. **التعريف القانوني والتصنيف:**

لم يصدر بعد في العراق قانون متخصص يعالج الأدلة الرقمية بشكل شامل، إلا أن بعض النصوص العامة تُشير إليها ضمن السياق الإجرائي. كما أدرجت بعض المسودات التشريعية، مثل **مشروع قانون مكافحة الجرائم الإلكترونية**)مسودة رقم 28 لسنة 2015)، تعريفات عامة للأدلة الرقمية ومصادرها، دون أن يتم إقرار القانون حتى الآن. وتفتقر هذه التعريفات إلى التفصيل الكافي بشأن طبيعة

[9] خليل، محمود عبد الكريم. (2020). التحقيق الجنائي في الجرائم الإلكترونية. دار الجامعة الجديدة، الإسكندرية.

10.70126/aqj.v9i18.296

البيانات الرقمية، وقيمتها الإثباتية، وتصنيفها الإجرائي[10].

ت. **الاعتماد على الخبرات الفنية:**

نظرًا لتعقيد الأدلة الرقمية وطبيعتها غير الملموسة، فإن تقديمها أمام المحكمة يتطلب دعم خبراء تقنيين قادرين على شرح الإجراءات الفنية المتبعة في جمعها وتحليلها. وقد أشار عدد من القضاة العراقيين في أحكامهم إلى ضرورة الاستعانة بخبراء في علوم المعلومات والتكنولوجيا لضمان قبول الأدلة الرقمية كأدلة قانونية صحيحة. يُعتبر هذا الجانب تحديًا إضافيًا خاصةً في ظل النقص النسبي في الكوادر المتخصصة في هذا المجال داخل النظام القضائي العراقي[11].

ث. **التعامل مع النسخ والتكرار:**

بما أن الأدلة الرقمية يمكن نسخها وتكرارها بشكل غير محدود، فإن القضاء العراقي يواجه تحديات في تحديد النسخة الأصلية وصلاحية استخدامها كدليل إثباتي. لذلك، تعتمد الإجراءات القانونية على بروتوكولات رقمية دقيقة لضمان توثيق النسخ واستخدامها بطريقة تضمن سلامة المعلومات وعدم تحريفها[12].

تُعدُّ الطبيعة غير الملموسة للأدلة الرقمية من السمات الجوهرية التي تفرض تحديات قانونية وإجرائية معقدة في نظام العدالة العراقي. يتطلب التعامل مع هذه الأدلة اتباع إجراءات تقنية وقانونية دقيقة لضمان سلامتها وعدم تعرضها للتلاعب، كما يستلزم ذلك اعتماد خبراء مختصين وتوثيق كامل لسلسلة الحفظ. تُظهر التشريعات العراقية الحديثة، خاصة قانون الجرائم

[10] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.p50

[11] قانون أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971، المواد (143–150).

[12] المجلة العراقية للعلوم القانونية. (2017). دور سلسلة الحفظ في إثبات الأدلة الرقمية. المجلة العراقية للعلوم القانونية, (2), 45–62.

الإلكترونية، الجهود المبذولة في هذا الاتجاه، إلا أنه لا يزال هناك حاجة لتعزيز البنية التحتية القانونية والتقنية لمواكبة التطورات التكنولوجية المتسارعة.

تعمل هذه الإجراءات على تعزيز موثوقية الأدلة الرقمية أمام الجهات القضائية وضمان تحقيق العدالة في القضايا التي تستند إلى هذه الأدلة، مما يُعد خطوة أساسية في مكافحة الجرائم الإلكترونية وحماية حقوق الأفراد في العصر الرقمي.[13]

الفرع الثاني :قابلية التعديل والتلف

تُعدُّ قابلية التعديل والتلف من أبرز التحديات التي تواجه الأدلة الرقمية في النظام القانوني العراقي. وتتمثل هذه التحديات في إمكانية تغيير البيانات أو تلفها بسهولة، مما يؤثر سلبًا على قيمتها الإثباتية في الإجراءات القانونية. وفيما يلي تفصيل لهذه النقاط مع ذكر الإجراءات الفنية والتدابير الوقائية المتبعة في القانون العراقي[14]:

1.قابلية التعديل والتلف للأدلة الرقمية

أ. **سهولة التعديل:**

تُظهر الأدلة الرقمية بطبيعتها قابلية عالية للتعديل؛ حيث يمكن لأي شخص لديه إمكانية الوصول إلى النظام تعديل الملفات الإلكترونية أو حذفها أو حتى استبدالها بنسخ مُعدلة. على سبيل المثال، في قضايا تزوير المستندات الإلكترونية، يمكن تغيير البيانات الأصلية بشكل غير ملحوظ إذا لم يتم اتخاذ الإجراءات الوقائية المناسبة. هذا يضع تحديات كبيرة أمام الجهات القضائية في إثبات سلامة الأدلة ومصداقيتها.

ب. **قابلية التلف:**

بالإضافة إلى التعديل، فإن الأدلة الرقمية عرضة للتلف نتيجة لعوامل متعددة مثل الأعطال الفنية، البرمجيات الخبيثة، أو حتى

[13] سامي محمود. تحليل الأدلة الرقمية في جرائم الإنترنت. مركز البحوث القانونية، بيروت، 2021. ص 88-105, 200-215.

[14] قانون الجرائم الإلكترونية العراقي رقم 28 لسنة 2015. (2015). الجمهورية العراقية: الهيئة التشريعية.ص52

10.70126/aqj.v9i18.296

عمليات النقل غير الصحيحة للبيانات. يُعد تلف البيانات من المشكلات الحرجة التي قد تُفقد المعلومات أو تُضعف دقتها، مما يؤثر على إمكانية استخدامها كأدلة قانونية.

2.الإجراءات الوقائية والتقنيات المستخدمة

أ. **استخدام تقنيات التجزئة:(Hashing)**

لضمان عدم تعديل البيانات أثناء عملية جمعها ونقلها وتحليلها، يُعتمد في القانون العراقي على تقنيات التجزئة، والتي تقوم بتحويل البيانات إلى سلسلة رقمية ثابتة (توقيع رقمي). عند كل عملية نقل أو نسخ للملفات، يُعاد حساب قيمة التجزئة؛ فإذا كانت القيمة متطابقة، فهذا يدل على عدم حدوث أي تعديل. تُعد هذه التقنية حجر الزاوية في الحفاظ على سلامة الأدلة الرقمية.

ب. **تطبيق سلسلة الحفظ (Chain of Custody):**

يعتبر الحفاظ على سلسلة الحفظ من أهم الإجراءات الوقائية في التعامل مع الأدلة الرقمية، حيث يتم توثيق كافة خطوات التعامل مع البيانات منذ لحظة جمعها وحتى تقديمها في المحكمة. يساهم ذلك في إثبات عدم تعرض البيانات للتعديل أو التلف، ويضمن قبولها كأدلة قانونية.

ت. **استخدام أدوات التوثيق والفحص الرقمي:**

يجب على المحققين استخدام أدوات وبرمجيات متخصصة لتوثيق البيانات والتأكد من سلامتها قبل وأثناء عملية التحليل. تُسهم هذه الأدوات في اكتشاف أي تعديلات قد تكون حدثت، وتوفير تقارير فنية تدعم الإجراءات القضائية.[15]

3.التطبيقات العملية والتحديات في قضايا الفساد الإلكتروني

[15] المجلة العراقية للعلوم القانونية. (2017). دور سلسلة الحفظ في إثبات الأدلة الرقمية. المجلة العراقية للعلوم القانونية, (2), 45–62.ص45

في قضايا تتعلق بتزوير المستندات الإلكترونية، تُظهر التجارب القضائية أن تعديل الملفات الأصلية يمكن أن يتم بسهولة إذا لم تُتخذ الإجراءات الفنية اللازمة. ولذلك، يؤكد النظام القانوني العراقي على ضرورة[16]:

أ. الالتزام التام بإجراءات سلسلة الحفظ لضمان توثيق كل عملية تعامل مع البيانات.

ب. استخدام تقنيات التجزئة كأداة للتحقق من سلامة الأدلة الرقمية.

ت. الاعتماد على خبراء مختصين في تحليل الأدلة الرقمية لتفسير النتائج وتقديمها للمحاكم كأدلة موثوقة.

الفرع الثالث الاعتماد على التكنولوجيا في التحليل

يتطلب تحليل الأدلة الرقمية **اعتمادًا كبيرًا على التكنولوجيا**، حيث يتم استخدام برامج وأدوات متخصصة لاستخراج البيانات وتحليلها، فإن التطور السريع في التكنولوجيا يجعل من الضروري تحديث هذه الأدوات باستمرار لمواكبة التغييرات في أنظمة التشغيل وتقنيات التخزين.

على سبيل المثال، في قضية تتعلق بجرائم الإنترنت، يمكن أن تتطلب الأدلة الرقمية استخدام برامج متخصصة لفك تشفير البيانات أو استعادة الملفات المحذوفة. بدون هذه الأدوات، قد يكون من المستحيل الوصول إلى الأدلة اللازمة للإثبات[17].

المبحث الثاني: الإشكاليات القانونية للأدلة الرقمية

على الرغم من أهمية الأدلة الرقمية في كشف الحقائق وتعزيز العدالة، إلا أنها تثير العديد من الإشكاليات القانونية. يتعلق ذلك بطبيعتها التقنية، وطرق جمعها، ومدى قبولها أمام المحاكم. وفي هذا المبحث، سيتم استعراض أبرز الإشكاليات القانونية التي تواجه الأدلة

[16] الحسن، ع. (2018). الإثبات الرقمي في القوانين الحديثة. بغداد: دار النشر القانونية.ص50

[17] عثمان، آمال عبد الرحيم. (2021). "الإثبات الإلكتروني في المسائل الجنائية". دار الجامعة الجديدة، الإسكندرية. ص 175-320.

10.70126/aqj.v9i18.296

الرقمية، مع التركيز على التحديات المرتبطة بمعايير القبول وسلامة الإجراءات القانونية.

المطلب الأول: إشكاليات القبول في المحاكم

تُعتبر الأدلة الرقمية من أهم الوسائل الحديثة المستخدمة في إثبات الجرائم والقضايا القانونية، إلا أن قبولها في المحاكم يواجه تحديات عديدة. تنبع هذه الإشكاليات من طبيعتها التقنية التي تستلزم معايير دقيقة لضمان سلامتها ومصداقيتها

الفرع الاول معايير قبول الأدلة الرقمية

تخضع الأدلة الرقمية لمعايير صارمة لقبولها في المحاكم، حيث يجب أن تتوفر فيها عدة شروط لضمان موثوقيتها وقيمتها الإثباتية، فإن أهم معايير قبول الأدلة الرقمية تشمل[18]:

1. **السلامة والأصالة:**

يجب أن تكون الأدلة الرقمية سليمة ولم يتم التلاعب بها. يتم التحقق من ذلك من خلال استخدام تقنيات التجزئة (Hashing) التي تضمن عدم تغيير البيانات أثناء عملية التحليل.

2. **سلسلة حفظ الأدلة (Chain of Custody):**

يجب توثيق كل خطوة من خطوات جمع الأدلة الرقمية وتحليلها، بدءًا من اكتشافها وحتى عرضها في المحكمة. فإن أي خلل في سلسلة الحفظ قد يؤدي إلى رفض الأدلة.

3. **الارتباط بالجريمة:**

يجب أن تكون الأدلة الرقمية ذات صلة مباشرة بالجريمة قيد التحقيق. على سبيل المثال، في قضايا الاحتيال الإلكتروني، يجب أن تكون رسائل البريد الإلكتروني أو سجلات المعاملات مرتبطة بالمتهم.

[18] Inci Turk, & Eric Cole. (2013). Digital Forensics: An Introduction to Computer Forensics. Jones & Bartlett Learning.p20

الفرع الثاني :التحديات المتعلقة بالإثبات الجنائي

تواجه الأدلة الرقمية عدة تحديات في الإثبات الجنائي، مما يجعل قبولها في المحاكم أمرًا معقدًا، فإن أبرز هذه التحديات تشمل[19]:

1. **التلاعب بالأدلة:**

يمكن التلاعب بالأدلة الرقمية بسهولة، مما يضعف قيمتها الإثباتية. على سبيل المثال، يمكن تعديل ملفات الوسائط أو حذفها دون ترك أثر واضح.

2. **عدم وجود تشريعات واضحة:**

في العديد من الدول، لا تزال التشريعات المتعلقة بالأدلة الرقمية غير واضحة أو غير كافية، مما يؤدي إلى اختلاف التطبيقات القضائية.

3. **التحديات الفنية:**

يتطلب تحليل الأدلة الرقمية مهارات فنية عالية، وقد لا تتوفر هذه المهارات لدى جميع المحققين أو القضاة.

المطلب الثاني: الإطار التشريعي للأدلة الرقمية

مع التطور الكبير في استخدام التكنولوجيا، أصبح من الضروري وجود إطار تشريعي ينظم التعامل مع الأدلة الرقمية في الأنظمة القانونية. يهدف هذا الإطار إلى وضع القواعد التي تضمن جمع الأدلة الرقمية وحفظها وتقديمها بطريقة قانونية تحقق العدالة.

الفرع الاول التشريعات الوطنية والدولية

تختلف التشريعات المتعلقة بالأدلة الرقمية من دولة إلى أخرى، ولكن هناك بعض الجهود الدولية لتوحيد هذه التشريعات ، فإن أبرز التشريعات الوطنية والدولية تشمل[20]:

1. **التشريعات الوطنية:**

أ. في مصر، ينظم قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

[19] United Nations Office on Drugs and Crime (UNODC). Model Law on Computer Crime, 2013.

[20] عوض، محمد محي الدين. (2020). "قواعد الإثبات في المواد الجنائية". منشأة المعارف، الإسكندرية. ص 280.

10.70126/aqj.v9i18.296

استخدام الأدلة الرقمية في الإثبات الجنائي.

ب. في المملكة العربية السعودية، صدر نظام مكافحة الجرائم المعلوماتية في عام 2007، والذي يتناول جمع الأدلة الرقمية وتحليلها.

ت. في العراق، تم اعتماد تشريعات تهدف إلى مكافحة الجرائم الإلكترونية وتنظيم استخدام الأدلة الرقمية في سياق الإجراءات القضائية، وقد جاءت هذه التشريعات استجابة للتحديات المتزايدة في عصر المعلومات والتكنولوجيا. ومن أهم ملامح هذه التشريعات:

ث. تنظيم الأدلة الرقمية: ينظم القانون العراقي الإجراءات الخاصة بجمع وتحليل الأدلة الرقمية، مما يضمن استخدامها بشكل قانوني في الإثبات الجنائي.

ج. حماية البيانات والأمن السيبراني: يتناول التشريع أيضاً حماية البيانات الشخصية وتأمين نظم المعلومات من الاختراقات والهجمات الإلكترونية.

ح. التعاون الدولي: يسهم القانون في تعزيز التعاون مع الجهات القضائية والأمنية الدولية لمكافحة الجرائم الإلكترونية العابرة للحدود.

خ. التحديث المستمر: نظراً للتطور السريع في مجال التكنولوجيا والجرائم الرقمية، يشهد الإطار التشريعي العراقي تحديثات دورية تواكب المستجدات التقنية وتطور أساليب الجرائم.

2. **التشريعات الدولية:**

أ. اتفاقية بودابست: وهي أول معاهدة دولية تتناول الجرائم الإلكترونية، وتشمل أحكامًا حول جمع الأدلة الرقمية.

ب. اللائحة العامة لحماية البيانات (GDPR)في الاتحاد الأوروبي: والتي تنظم استخدام البيانات الشخصية، بما في ذلك الأدلة الرقمية.

الفرع الثاني :الفجوات التشريعية وعدم الوضوح

رغم الجهود التشريعية، لا تزال هناك فجوات كبيرة في الإطار القانوني للأدلة الرقمية.فإن أبرز هذه الفجوات تشمل[21]:

1. **عدم وجود معايير موحدة:**

تختلف معايير قبول الأدلة الرقمية من دولة إلى أخرى، مما يؤدي إلى صعوبات في التعاون الدولي في التحقيقات الجنائية.

2. **عدم وضوح الإجراءات:**

في العديد من الدول، لا تزال الإجراءات المتعلقة بجمع الأدلة الرقمية غير واضحة، مما يؤدي إلى اختلاف التطبيقات القضائية.

3. **التحديات التكنولوجية:**

مع التطور السريع في التكنولوجيا، يصبح من الصعب على التشريعات مواكبة التغييرات، مما يؤدي إلى وجود فجوات تشريعية.

المبحث الثالث: التجارب الدولية والمقارنة التشريعية

يشهد العالم تباينًا كبيرًا في التعامل مع الأدلة الرقمية بين مختلف الدول، حيث تعتمد كل دولة على إطار تشريعي وتنظيمي يتناسب مع نظامها القانوني ومستوى تقدمها التقني. ومن خلال دراسة التجارب الدولية والمقارنة التشريعية، يمكن التعرف على أفضل الممارسات القانونية في جمع وتحليل الأدلة الرقمية وقبولها في المحاكم. يهدف هذا المبحث إلى تسليط الضوء على تجارب دولية مختلفة ومقارنتها لتقديم رؤية شاملة تسهم في تطوير التشريعات الوطنية.

المطلب الأول: التجربة الأوروبية في التعامل مع الأدلة الرقمية

تمثل التجربة الأوروبية نموذجًا متقدمًا في تنظيم التعامل مع الأدلة الرقمية، حيث تتبنى دول الاتحاد الأوروبي تشريعات متطورة تتماشى

القحطاني، معجب معدي. (2021). "الإثبات الجنائي بالقرائن المعاصرة". مكتبة القانون والاقتصاد، الرياض. ص 195 [21].

10.70126/aqj.v9i18.296

مع التطور التكنولوجي وتحمي حقوق الأفراد. وفي هذا المطلب، سيتم استعراض أبرز ملامح التجربة الأوروبية، مع التركيز على الإطار القانوني والتشريعي الذي ينظم الأدلة الرقمية ودورها في تحقيق العدالة.

الفرع الاول إطار العمل العام لحماية البيانات (GDPR)

يُعتبر **اللائحة العامة لحماية البيانات (GDPR)**التي دخلت حيز التنفيذ في مايو 2018 أحد أهم التشريعات الأوروبية التي تنظم استخدام البيانات الشخصية، بما في ذلك الأدلة الرقمية. وفقًا لـ (محمد أحمد علي، 2018، ص 150)، فإن GDPR يهدف إلى حماية خصوصية الأفراد وضمان استخدام بياناتهم بشكل قانوني وشفاف.

من أهم مبادئ GDPR التي تؤثر على الأدلة الرقمية[22]:

1. **الموافقة المسبقة** :يجب الحصول على موافقة الأفراد قبل جمع بياناتهم الشخصية.
2. **الحد الأدنى من البيانات** :يجب جمع الحد الأدنى من البيانات اللازمة للتحقيق.
3. **حقوق الأفراد** :للأفراد الحق في الوصول إلى بياناتهم وطلب حذفها.

الفرع الثاني التطبيقات القضائية في دول الاتحاد الأوروبي

تطبق دول الاتحاد الأوروبي تشريعات GDPRبشكل صارم، مما يؤثر على كيفية جمع الأدلة الرقمية واستخدامها في الإجراءات الجنائية، فإن المحاكم الأوروبية ترفض الأدلة الرقمية التي يتم الحصول عليها بشكل غير قانوني أو دون احترام مبادئ.GDPR

[22] المري، علي حسن. (2019). "الأدلة الإلكترونية في المحاكم الجزائية". المكتب الجامعي الحديث، الإسكندرية. ص85

على سبيل المثال، في قضية شهيرة في ألمانيا عام 2019، تم رفض أدلة رقمية تم الحصول عليها من هاتف متهم دون موافقته، حيث اعتبرت المحكمة أن ذلك ينتهك مبادئ GDPR.

المطلب الثاني: التجربة الأمريكية في مجال الأدلة الرقمية

تعد التجربة الأمريكية في مجال الأدلة الرقمية من أبرز التجارب العالمية التي أسهمت في تطوير وتنظيم استخدام الأدلة الرقمية في النظام القضائي. فقد بدأت الولايات المتحدة في تبني الأدلة الرقمية كمجال مهم في التحقيقات الجنائية والمحاكمات القانونية منذ عدة عقود، مما جعلها رائدة في هذا المجال. تتمثل هذه التجربة في تطوير قوانين وتشريعات تواكب التقدم التكنولوجي، بالإضافة إلى تأسيس معايير وتقنيات متقدمة في جمع وتحليل الأدلة الرقمية. وتعتبر هذه التجربة نموذجًا يحتذى به للعديد من الدول التي تسعى إلى تحسين استخدام الأدلة الرقمية في مجالات التحقيقات والمقاضاة.

الفرع الاول قانون الأدلة الرقمية في الولايات المتحدة

في الولايات المتحدة، يتم تنظيم الأدلة الرقمية من خلال عدة قوانين فيدرالية وقوانين ولايات، فإن أبرز هذه القوانين تشمل[23]:

1. **قانون الخصوصية الإلكترونية (ECPA):**

ينظم جمع الأدلة الرقمية من الاتصالات الإلكترونية، مثل البريد الإلكتروني والرسائل النصية.

2. **قانون باتريوت:(Patriot Act)**

يمنح سلطات أمنية واسعة لمراقبة الاتصالات وجمع الأدلة الرقمية في قضايا الإرهاب.

3. **قواعد الأدلة الفيدرالية (Federal Rules of Evidence):**

[23] مصطفى، محمود محمود. (2020). "الإثبات في المواد الجنائية". دار النهضة العربية، القاهرة. ص 350

10.70126/aqj.v9i18.296

تحدد معايير قبول الأدلة الرقمية في المحاكم الفيدرالية.

الفرع الثاني دراسات حالات قضائية

تعتبر الولايات المتحدة من أكثر الدول تقدمًا في استخدام الأدلة الرقمية في الإجراءات الجنائية، فإن هناك العديد من الحالات القضائية التي تم فيها استخدام الأدلة الرقمية بشكل فعال[24]:

1. **قضية الولايات المتحدة ضد Microsoft (2018):**

رفضت المحكمة العليا الأمريكية طلب الحكومة بالوصول إلى بيانات مخزنة على خوادم Microsoft في أيرلندا، مما أثار نقاشًا حول حدود السلطة القضائية في جمع الأدلة الرقمية عبر الحدود.

2. **قضية Apple ضد FBI (2016):**

رفضت Apple طلب FBI بفك تشفير هاتف أحد المشتبه بهم في هجوم إرهابي، مما أثار جدلًا حول التوازن بين الخصوصية والأمن القومي.

الخاتمة والاستنتاجات والتوصيات

الخاتمة

في ظل التطورات المتسارعة في مجال التكنولوجيا الرقمية، أصبحت الأدلة الرقمية تلعب دورًا رئيسيًا في الإجراءات الجنائية، حيث تساهم في كشف الجرائم الإلكترونية وضمان تحقيق العدالة. ومع ذلك، لا تزال هناك تحديات قانونية وتقنية تعيق الاستخدام الأمثل لهذه الأدلة، مثل عدم وضوح التشريعات، وضعف الإطار القانوني، وصعوبة إثبات صحة الأدلة الرقمية في بعض الحالات. يتطلب التعامل مع هذه التحديات تطوير أنظمة قانونية متكاملة تستوعب التطورات التقنية وتحمي الحقوق القانونية للأفراد.

[24] الجبوري، سليمان خالد. (2018). "حجية الأدلة الإلكترونية في الإثبات الجنائي". دار الفكر الجامعي، الإسكندرية. ص 75-190.

الاستنتاجات

1. **أهمية الأدلة الرقمية** :أصبحت الأدلة الرقمية عنصرًا أساسيًا في التحقيقات الجنائية، خاصة في الجرائم السيبرانية والجرائم المتعلقة بالأنظمة المعلوماتية.

2. **الفجوات التشريعية** :لا تزال التشريعات العراقية والعربية بحاجة إلى تحديثات مستمرة لمواكبة التطورات التكنولوجية وضمان القبول القانوني للأدلة الرقمية.

3. **التحديات الفنية** :تتطلب الأدلة الرقمية إجراءات متقدمة لحفظها وضمان عدم التلاعب بها، مثل استخدام تقنيات التجزئة (Hashing) وسلسلة الحفظ(Chain of Custody)).

4. **الحاجة إلى تعاون دولي** :نظرًا لأن الجرائم الإلكترونية غالبًا ما تتجاوز الحدود الوطنية، يجب تعزيز التعاون الدولي لضمان تتبع الأدلة الرقمية وتحقيق العدالة الجنائية.

5. **ضرورة تطوير المهارات القضائية** :

يحتاج القضاة والمحققون إلى تدريب مستمر في مجال الأدلة الرقمية لفهم طبيعتها وإجراءات قبولها في المحاكم.

التوصيات

1. **تطوير التشريعات** :إصدار قوانين جديدة أو تحديث القوانين الحالية لتنظيم جمع وتحليل الأدلة الرقمية وضمان حجيتها في المحاكم.

2. **تعزيز سلسلة الحفظ** :وضع بروتوكولات واضحة لحفظ الأدلة الرقمية، بدءًا من جمعها حتى تقديمها في المحكمة، مع توثيق كل خطوة لضمان عدم التلاعب بها.

3. **تدريب المختصين** :توفير دورات تدريبية للقضاة، المحققين، والخبراء التقنيين حول كيفية التعامل مع الأدلة الرقمية وضمان سلامتها.

4. **استخدام التكنولوجيا الحديثة** :تبني أحدث التقنيات في مجال التحليل الرقمي، مثل الذكاء الاصطناعي وأدوات تحليل البيانات الكبيرة، لضمان دقة الأدلة الرقمية وسلامتها.

5. **تعزيز التعاون الدولي** :توقيع اتفاقيات تعاون مع الجهات الدولية لضمان تبادل المعلومات والتجارب في مجال الأدلة الرقمية، خاصة في الجرائم العابرة للحدود.

6. **إطلاق مبادرات توعية** :رفع الوعي لدى العاملين في المجال القانوني والمواطنين بأهمية الأدلة الرقمية وكيفية حمايتها من التلاعب أو التلف.

يؤكد البحث على ضرورة تبني منهجية متكاملة تجمع بين الأطر القانونية الحديثة والتقنيات

10.70126/aqj.v9i18.296

المتقدمة لضمان قبول الأدلة الرقمية في المحاكم

وتحقيق العدالة الجنائية بكفاءة وشفافية.

المصادر

أولًا: الكتب والأبحاث

1. أحمد، محمد علي. (2020). *الأدلة الرقمية في الإجراءات الجنائية* .دار الثقافة للنشر والتوزيع، بغداد.
2. الحسن، ع. (2018). *الإثبات الرقمي في القوانين الحديثة* .بغداد: دار النشر القانونية.
3. الجبوري، سليمان خالد. (2018). *حجية الأدلة الإلكترونية في الإثبات الجنائي* .دار الفكر الجامعي، الإسكندرية.
4. الخليل، محمود عبد الكريم. (2020). *التحقيق الجنائي في الجرائم الإلكترونية* .دار الجامعة الجديدة، الإسكندرية.
5. القحطاني، معجب معدي. (2021). *الإثبات الجنائي بالقرائن المعاصرة* .مكتبة القانون والاقتصاد، الرياض.
6. المري، علي حسن. (2019). *الأدلة الإلكترونية في المحاكم الجزائية* .المكتب الجامعي الحديث، الإسكندرية.
7. محمد، أحمد علي. (2018). *الأدلة الرقمية في الإجراءات الجنائية* .دار النهضة العربية، القاهرة.
8. مصطفى، محمود محمود. (2020). *الإثبات في المواد الجنائية* .دار النهضة العربية، القاهرة.
9. عثمان، آمال عبد الرحيم. (2021). *الإثبات الإلكتروني في المسائل الجنائية* .دار الجامعة الجديدة، الإسكندرية.
10. علي، حسن. (2017). *الأدلة الإلكترونية في الجرائم المعلوماتية* .دار الثقافة للنشر، عمان.

10.70126/aqj.v9i18.296

11. عوض، محمد محي الدين. (2020). *قواعد الإثبات في المواد الجنائية* .منشأة المعارف، الإسكندرية.

12. خالد، عبد الرحمن. (2020). *التقنيات الحديثة في جمع الأدلة الرقمية* .مركز الدراسات القضائية، الرياض.

13. سامي، محمود. (2021). *تحليل الأدلة الرقمية في جرائم الإنترنت* .مركز البحوث القانونية، بيروت.

ثانيًا: المراجع القانونية والتشريعات

14. قانون أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971.

15. قانون الجرائم الإلكترونية العراقي رقم 28 لسنة 2015. (2015). *الجمهورية العراقية: الهيئة التشريعية*.

ثالثًا: المجلات العلمية المحكمة

16. المجلة العراقية للعلوم القانونية. (2017). *دور سلسلة الحفظ في إثبات الأدلة الرقمية*.

17. محمد، فاطمة الزهراء. (2019). *إشكاليات الأدلة الرقمية في التشريع المصري* .*مجلة القانون والاقتصاد، جامعة القاهرة*.

18. يوسف، ندى حسن. (2021). *دور البيانات الرقمية في إثبات الجرائم المعلوماتية* .*المجلة العراقية للعلوم القانونية والسياسية*.

المراجع الأجنبية

1. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.
2. Inci Turk, & Cole, E. (2013). *Digital Forensics: An Introduction to Computer Forensics*. Jones & Bartlett Learning.
3. United Nations Office on Drugs and Crime (UNODC). (2013). *Model Law on Computer Crime*.

10.70126/aqj.v9i18.296

المستخلص

في ظل التطور التكنولوجي المتسارع، أصبحت الأدلة الرقمية تلعب دورًا رئيسيًا في الإجراءات الجنائية، حيث تشكل مصدرًا هامًا للإثبات.

ومع ذلك، تواجه الأدلة الرقمية تحديات كبيرة تتعلق بالقبول والتوثيق في المحاكم، بسبب غياب التشريعات الموحدة وصعوبة التعامل مع طبيعتها التقنية. يناقش هذا البحث مفهوم الأدلة الرقمية وخصائصها، إلى جانب الإشكاليات القانونية والفنية التي تواجهها، مثل سلسلة حفظ الأدلة وإمكانية التلاعب بها. كما يقدم البحث تحليلًا للتجارب الدولية، مع التركيز على الإطار الأوروبي والأمريكي، ويوصي بتطوير تشريعات ومعايير تضمن سلامة الأدلة الرقمية وقبولها أمام القضاء.