



إشكالية إثبات أصالة الأدلة الرقمية في قضايا التزيف العميق: نحو إطار إجرائي مقترح للتشريع الإماراتي

محمد حسن خليفة بن سرور الكتبي

الأستاذ الدكتور وان عبد الفتاح بن وان إسماعي

الملخص

يتناول هذا البحث إشكالية إثبات أصالة الأدلة الرقمية في ظل الانتشار المتسارع لتقنيات الذكاء الاصطناعي والتزيف العميق، وما تثيره هذه التقنيات من تحديات أمام قواعد الإثبات التقليدية، ولا سيما فيما يتعلق بمصدر الدليل وسلامته وإمكانية نسبته إلى صاحبه. وتتمثل مشكلة البحث في مدى كفاية القواعد التشريعية والإجرائية الإماراتية القائمة للتحقق من أصالة الأدلة الرقمية المتأثرة بالتزيف العميق، ومدى الحاجة إلى تطوير إطار إجرائي متخصص يضمن موثوقيتها وقابليتها للتحقق القضائي. واعتمد البحث على المنهج الوصفي التحليلي والمقارن والاستنباطي، من خلال تحليل التشريعات الإماراتية ذات الصلة، وبخاصة المرسوم بقانون اتحادي رقم (35) لسنة 2022 بشأن الإثبات، والرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة، ومقارنتها ببعض القواعد القانونية في النظامين الفرنسي والأمريكي. وتوصل البحث إلى أن القواعد الإماراتية توفر أساساً عاماً للاعتراف بالدليل الإلكتروني، إلا أنها لا تتضمن تنظيمًا تفصيليًا للأدلة الاصطناعية الناتجة عن التزيف العميق، ولا بروتوكولاً موحدًا لسلسلة حفظها والتحقق من أصالتها. كما خلص إلى ضرورة تعزيز دور الخبرة الفنية واعتماد إجراءات متخصصة تشمل التوثيق الأولي، وحفظ الأصل، وإنشاء البصمة الرقمية، وفحص البيانات الوصفية، وتوثيق سلسلة المنشأ والسلامة، وإجراء فحص فني متعدد الأدوات. ويقترح البحث إطاراً إجرائياً متكاملاً يمكن أن يساهم في تطوير التشريع والممارسة القضائية الإماراتية وتحقيق التوازن بين التطور التقني وضمانات العدالة القضائية.

الكلمات المفتاحية: التزيف العميق، الأدلة الرقمية، أصالة الدليل، الذكاء الاصطناعي، سلسلة حفظ الدليل، الخبرة الفنية، الإثبات الإلكتروني، التشريع الإماراتي.



The Problem of Establishing the Authenticity of Digital Evidence in Deepfakes: Towards a Proposed Procedural Framework for UAE Legislation

Mohammed Hassan Khalifa Bin Surour Al-Ketbi

Prof. Dr. Wan Abdul Fattah Bin Wan Ismaili

ABSTRACT

This research addresses the problem of establishing the authenticity of digital evidence in light of the rapid spread of artificial intelligence and deepfakes technologies, and the challenges these technologies pose to traditional rules of evidence, particularly regarding the source, integrity, and attributability of evidence. The research problem lies in the adequacy of existing UAE legislative and procedural rules for verifying the authenticity of digital evidence affected by deepfakes, and the need to develop a specialized procedural framework that ensures its reliability and judicial verifiability. The research employs a descriptive, analytical, comparative, and deductive approach, analyzing relevant UAE legislation, especially Federal Law No. (35) of 2022 on Evidence and Federal Law No. (46) of 2021 on Electronic Transactions and Trust Services, and comparing them with legal rules in the French and American legal systems. The research concluded that while UAE regulations provide a general basis for recognizing electronic evidence, they lack detailed provisions for addressing artificial evidence resulting from deepfakes, as well as a unified protocol for its preservation and authentication. It further concluded that it is necessary to strengthen the role of expert testimony and adopt specialized procedures encompassing initial documentation, preservation of the original, digital fingerprinting, metadata examination, chain of origin and integrity verification, and multi-tool forensic examination. The research proposes a comprehensive procedural framework that can contribute to the development of UAE legislation and judicial practice, achieving a balance between technological advancements and the guarantees of judicial fairness.

Keywords: Deepfakes, Digital Evidence, Evidence Authenticity, Artificial Intelligence, Evidence Preservation Chain, Expert Testimony, Electronic Evidence, UAE Legislation.



1. المقدمة

أحدث التطور المتسارع في تقنيات الذكاء الاصطناعي تحولاً جوهرياً في طبيعة المحتوى الرقمي وطرق إنتاجه وتداوله، وأصبح بالإمكان إنشاء صور وتسجيلات صوتية ومقاطع مرئية تحاكي الواقع بدرجة عالية من الدقة، دون أن يكون لها بالضرورة أصل واقعي مطابق لما توحي به ظاهرياً. وفي مقدمة هذه التطبيقات تبرز تقنيات التزييف العميق (Deepfake) التي تعتمد على تقنيات التعلم العميق والذكاء الاصطناعي التوليدي لإنتاج أو تعديل محتوى رقمي يمكن أن ينسب ظاهرياً إلى أشخاص أو وقائع لم تحدث أصلاً. وقد أدى هذا التطور إلى إعادة طرح عدد من المسائل القانونية التقليدية المتعلقة بمفهوم الدليل وأصالته وسلامته وقابليته للاعتماد القضائي (Chesney & Citron, 2019; Maras & Alexandrou, 2019; Dixon, 2021).

ولا تتمثل خطورة التزييف العميق في قدرته على إنتاج محتوى كاذب فحسب، وإنما تمتد إلى قدرته على إضعاف الثقة في المحتوى الرقمي الصحيح؛ إذ إن مجرد إمكانية إنتاج محتوى اصطناعي شديد الواقعية قد تجعل الدليل الرقمي الحقيقي عرضة للتشكيك، حتى في الحالات التي لا يكون فيها أي تلاعب قد وقع بالفعل. ومن ثم، فإن الإشكالية القانونية لم تعد محصورة في السؤال التقليدي المتعلق بما إذا كان الدليل الرقمي جائزاً من حيث المبدأ، وإنما أصبحت تتمحور حول مدى إمكانية إثبات مصدره، وسلامة بنيته الرقمية، وعدم تعرضه للتعديل، وإمكانية تتبع تاريخه منذ لحظة الحصول عليه وحتى تقديمه أمام المحكمة (Rini, 2020; Vaccari & Chadwick, 2020; Hydera et al., 2024). ويؤكد هذا الاتجاه أن التزييف العميق لا يهدد قيمة الدليل المزيف وحده، بل قد يؤدي إلى ما يمكن وصفه بأزمة الثقة في الدليل الرقمي بصورة عامة.

وتكتسب هذه الإشكالية أهمية خاصة في المجال القضائي؛ لأن النظام القانوني يقوم في جوهره على قدرة المحكمة على تكوين قناعة تستند إلى أدلة يمكن التحقق من وجودها ومصدرها وسلامتها. وإذا كان الدليل التقليدي يرتبط عادة بمصدر مادي يمكن تتبع حيازته وانتقاله بين الأشخاص والجهات المختصة، فإن الدليل الرقمي يختلف من حيث قابليته للنسخ والتعديل وإعادة الإنتاج، بينما تزداد المسألة تعقيداً عندما يكون المحتوى نفسه قد أنشئ أو غُذِل باستخدام تقنيات الذكاء الاصطناعي. ولذلك أصبحت مسألة أصالة الدليل الرقمي (Digital Evidence Authenticity) تمثل أحد أهم التحديات المعاصرة لقانون الإثبات (Casey, 2020; Çelebi & Liu, 2022).

وتشير الأدبيات القانونية والتقنية إلى أن تحديد أصالة الأدلة المرئية والمسموعة في عصر الذكاء الاصطناعي لم يعد ممكناً دائماً بالاعتماد على الملاحظة البشرية أو الوسائل التقليدية وحدها؛ إذ يمكن للتقنيات الحديثة أن تنتج محتوى يصعب على غير المتخصصين، بل وفي بعض الحالات على المتخصصين، اكتشاف مظاهر التلاعب فيه دون استخدام أدوات الفحص الجنائي الرقمي المتقدمة (Maras & Alexandrou, 2019; Amerini & Caldelli, 2025). وقد دفعت هذه التطورات إلى إعادة النظر في المعايير التقليدية لقبول الأدلة الرقمية، ولا سيما معيار الأصالة وسلامة المصدر وإمكانية التحقق الفني منه.

وفي السياق الإماراتي، يمثل هذا الموضوع أهمية خاصة بالنظر إلى التطور التشريعي الذي شهدته الدولة في مجال تنظيم المعاملات الإلكترونية والإثبات الرقمي. فقد تبني المشرع الإماراتي مفهوماً واسعاً للمستند والبيانات الإلكترونية، وأقر من حيث الأصل الحجية القانونية للمحررات الإلكترونية متى توافرت شروط الموثوقية والسلامة وإمكانية نسبتها إلى مصدرها. كما عزز المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة هذا الاتجاه من خلال الاعتراف بالحجية القانونية للمستند الإلكتروني متى استوفى الشروط القانونية المقررة.

إلا أن الاعتراف التشريعي بالدليل الإلكتروني لا يعني بالضرورة أن الإطار القانوني القائم قادر على التعامل مع جميع صور الأدلة التي أفرزتها تقنيات الذكاء الاصطناعي. فالقواعد العامة التي تشترط سلامة الدليل وإمكانية نسبته إلى مصدره وضمان عدم العبث به وضعت في سياق قانوني كانت فيه طبيعة التلاعب الرقمي أقل تعقيداً مما هي عليه اليوم. أما في حالة التزييف العميق، فقد يبدو المحتوى سليماً من الناحية التقنية، في حين يكون غير حقيقي من حيث مصدره أو مضمونه، الأمر الذي يجعل مجرد التحقق من سلامة الملف أو نسبته الظاهرية غير كافٍ لإثبات حقيقته الموضوعية (الخولي، 2021؛ الشمري، 2025؛ Maras & Alexandrou, 2019).

وتكشف الدراسة الأصلية التي ينطلق منها هذا البحث عن وجود فجوة تشريعية وإجرائية تتمثل في عدم وجود تنظيم متخصص ومتكامل للأدلة الاصطناعية الناتجة عن الذكاء الاصطناعي، فضلاً عن عدم تحديد إجراءات تقنية ملزمة للتحقق من أصالة هذه الأدلة. كما أظهرت الدراسة أن قانون الإثبات الإماراتي يمنح المحكمة إمكانية



الاستعانة بالخبرة الفنية، إلا أن اللجوء إلى الخبير لا يرتبط بصورة إلزامية بكل حالة يثار فيها شك جدي حول أصالة دليل رقمي، وهو ما قد يؤدي إلى تفاوت في الممارسة القضائية.

وترداد أهمية هذه المسألة عند الانتقال من مجرد قبول الدليل الرقمي إلى البحث في سلسلة حفظه (Chain of Custody). فسلسلة الحفظ تمثل الإطار الذي يسمح بتتبع الدليل منذ لحظة جمعه أو الحصول عليه، مروراً بمراحل نقله وتخزينه وفحصه وتحليله، وصولاً إلى تقديمه أمام المحكمة. وفي الأدلة الرقمية، لا تقتصر وظيفة هذه السلسلة على إثبات الحيازة المادية، وإنما تمتد إلى توثيق كل عملية وصول أو نقل أو معالجة أو تحليل قد تؤثر في سلامة الدليل. ولذلك فإن أي انقطاع أو غموض في سلسلة الحفظ قد يثير شكوكاً بشأن أصالة الدليل أو سلامته (Casey, 2020; Hydera et al., 2024).

وتظهر المشكلة بصورة أكثر تعقيداً في حالة الأدلة الاصطناعية؛ لأن بعض هذه الأدلة قد لا يكون له أصل مادي تقليدي يمكن تتبع حيازته، وإنما قد يكون قد أنشئ أصلاً بواسطة نظام ذكاء اصطناعي. ومن ثم، فإن مفهوم سلسلة الحفظ التقليدية يحتاج إلى إعادة صياغة بحيث يتحول من مجرد تتبع الحيازة إلى تتبع منشأ الدليل وتاريخ إنشائه وتعديلاته وانتقاله ومعالجته. وقد خلصت الدراسة محل التحليل إلى أن سلسلة حفظ الدليل لم تتطور تشريعياً بالقدر الذي يتناسب مع طبيعة الأدلة الاصطناعية، وأن غياب معايير تقنية واضحة لتوثيق هذه السلسلة قد يؤدي إلى تفاوت في التطبيق وإلى مخاطر تتعلق بالاعتماد على أدلة غير موثوقة.

ومن منظور مقارن، تكشف التجارب القانونية الأجنبية عن اتجاه متزايد نحو تعزيز متطلبات المصادقة على الأدلة الرقمية وإخضاع الخبرة الفنية لمعايير أكثر صرامة. ففي النظام الأمريكي، تقرر القاعدة (901) من القواعد الفيدرالية للإثبات على مقدم الدليل تقديم أساس كافٍ يدعم كونه ما يدعيه، في حين تسمح القاعدة (702) بالاستعانة بالخبرة الفنية عندما تكون ذات أساس علمي موثوق. كما تمنح القاعدة (403) المحكمة إمكانية استبعاد الدليل إذا كانت آثاره المضللة أو الضارة تفوق قيمته الإثباتية.

أما في فرنسا، فقد اعترف القانون المدني بالحجية القانونية للكتابة الإلكترونية، مع اشتراط ضمان سلامة الدليل الإلكتروني وظروف حفظه. إلا أن الدراسة المقارنة تشير إلى أن النظام الفرنسي، رغم تقدمه في تنظيم الدليل الإلكتروني، لا يتضمن تنظيمًا تشريعيًا متخصصًا ومتكاملاً للأدلة الناتجة عن التزيف العميق، مما يجعل الخبرة والممارسة القضائية توديان دوراً مهماً في التحقق من سلامة المحتوى الرقمي.

وعليه، فإن المشكلة التي يطرحها هذا البحث لا تتعلق بضرورة رفض الأدلة الرقمية أو افتراض عدم حجيتها بسبب إمكانية تعرضها للتزيف العميق، وإنما تتعلق بضرورة إعادة بناء معيار إثبات الأصالة بحيث يجمع بين المتطلبات القانونية والضمانات التقنية. فالتحدي الحقيقي أمام المشرع والقاضي لا يكمن في اختيار موقف ثنائي بين قبول الدليل أو استبعاده، وإنما في بناء آلية موضوعية تسمح بتحديد درجة موثوقيته استناداً إلى مصدره وسلامته وسلسلة حفظه ونتائج الفحص الفني.

ومن هذا المنطلق، يسعى البحث إلى الانتقال من المعالجة العامة لحجية الأدلة الرقمية إلى معالجة أكثر تخصصاً تتمثل في إثبات أصالة الأدلة الرقمية المتأثرة بالتزيف العميق، مع تقديم إطار إجرائي مقترح يمكن أن يسهم في تطوير التشريع الإماراتي وتحقيق التوازن بين الاستفادة من التطور التكنولوجي وضمانات العدالة القضائية.

2.1 مشكلة البحث

تتمثل المشكلة البحثية في أن التطور التقني في مجال الذكاء الاصطناعي التوليدي أدى إلى ظهور أدلة رقمية يمكن أن تكون عالية الواقعية من الناحية الشكلية، ولكنها مصطنعة من حيث المصدر أو المحتوى، الأمر الذي يضع قواعد الإثبات التقليدية أمام تحدٍ يتعلق بإثبات الأصالة وليس بمجرد إثبات وجود الدليل.

وترداد هذه المشكلة حدة في التشريع الإماراتي؛ فعلى الرغم من أن المشرع أقر الحجية القانونية للمحركات والبيانات الإلكترونية وربطها بمفاهيم السلامة والموثوقية وإمكانية النسبة إلى صاحبها، فإن التنظيم القائم لا يضع - وفق ما تكشفه الدراسة الأصلية - إجراءات فنية تفصيلية وملزمة للتحقق من هذه الشروط عندما يكون الدليل محل نزاع ناتجاً عن تقنية التزيف العميق.

كما أن ترك الاستعانة بالخبرة الفنية للسلطة التقديرية للمحكمة قد لا يكون كافياً في الحالات التي تعتمد فيها الدعوى بصورة جوهرية على تسجيل صوتي أو صورة أو مقطع فيديو يثار بشأنه احتمال التلاعب بواسطة الذكاء الاصطناعي. وتظهر هذه الإشكالية بصورة واضحة في المقارنة التي أجرتها الدراسة بين التشريع



الإماراتي والأنظمة المقارنة، حيث لا تزال القواعد القائمة في هذه الأنظمة تعتمد بدرجات مختلفة على مفاهيم تقليدية للأصالة والمصادقة، رغم التطور الكبير في وسائل إنتاج الأدلة الاصطناعية. وبناءً على ذلك، تتمحور المشكلة الرئيسية للبحث حول السؤال الآتي:

إلى أي مدى تكفي القواعد التشريعية والإجرائية القائمة في دولة الإمارات العربية المتحدة لإثبات أصالة الأدلة الرقمية في قضايا التزيف العميق، وما المتطلبات اللازمة لبناء إطار إداري متكامل يضمن سلامة الدليل وقابليته للتحقق القضائي؟

3.1 أسئلة البحث

ينفرد عن السؤال الرئيس عدد من الأسئلة الفرعية:

1. ما المقصود بأصالة الدليل الرقمي، وما خصوصيتها في ظل تقنيات التزيف العميق؟
2. ما مدى كفاية القواعد الإماراتية الحالية في ضمان سلامة ومصدر الدليل الرقمي؟
3. إلى أي مدى يمكن تطبيق مفهوم سلسلة حفظ الدليل التقليدية على الأدلة الاصطناعية؟
4. ما دور الخبرة الفنية والتحليل الجنائي الرقمي في إثبات أصالة الدليل؟
5. كيف عالجت التشريعات والممارسات القضائية المقارنة مسألة مصادقة الأدلة الرقمية؟
6. ما أوجه القصور التشريعي والإداري في النظام الإماراتي؟
7. ما العناصر التي ينبغي أن يتضمنها إطار إداري إماراتي خاص بالتحقق من أصالة الأدلة الرقمية المتأثرة بالتزيف العميق؟

4.1 أهداف البحث

يهدف البحث إلى تحقيق مجموعة مترابطة من الأهداف، تتمثل في:

- أولاً، تحليل مفهوم أصالة الدليل الرقمي في ضوء التحولات التي أحدثتها تقنيات الذكاء الاصطناعي والتزيف العميق.
- ثانياً، تقييم مدى كفاية الإطار التشريعي الإماراتي في التعامل مع الأدلة الرقمية التي يثار بشأنها احتمال التلاعب أو الإنشاء الاصطناعي.
- ثالثاً، تحليل مفهوم سلسلة حفظ الدليل الرقمي وبيان مدى ملاءمته للأدلة التي يتم إنتاجها أو تعديلها بواسطة الذكاء الاصطناعي.
- رابعاً، تحديد الدور القانوني والفني للخبير المتخصص في التحقق من أصالة الأدلة الرقمية.
- خامساً، إجراء مقارنة تحليلية مع عدد من النظم القانونية، وبخاصة النموذجان الفرنسي والأمريكي.
- سادساً، اقتراح إطار إداري متكامل للتحقق من أصالة الدليل الرقمي يمكن أن يشكل أساساً لتطوير التشريع والممارسة القضائية في دولة الإمارات.

5.1 أهمية البحث

تتبع الأهمية العلمية للبحث من أنه يعالج منطقة تقاطع بين قانون الإثبات، والذكاء الاصطناعي، والأدلة الرقمية، والطب الشرعي الرقمي. وعلى الرغم من تزايد الدراسات التي تناولت المسؤولية القانونية عن التزيف العميق أو خطورته على المجتمع، فإن الحاجة لا تزال قائمة إلى تطوير معالجة تركز بصورة مباشرة على إثبات أصالة الدليل والإجراءات التي ينبغي اتباعها قبل اعتماده قضائياً (أبو سيف، 2025؛ مكتوف وعاشور، 2025؛ الشمري، 2025). كما تستمد الدراسة أهميتها من كونها لا تتعامل مع التزيف العميق باعتباره مجرد جريمة إلكترونية، وإنما باعتباره تحدياً لنظرية الإثبات ذاتها. وقد أشارت الأدبيات إلى أن الخطر لا يقتصر على إنتاج أدلة مزيفة، وإنما يشمل إمكانية التشكيك في الأدلة الصحيحة، وهو ما يمكن أن يؤثر في الثقة بالقضاء وفي اليقين القضائي (Chukwuebuka, 2025; Maras & Alexandrou, 2019).

أما من الناحية التطبيقية، فتتمثل أهمية البحث في تقديم إطار إداري يمكن أن يساعد المشرع والقضاء والنيابة العامة والخبراء في التعامل مع الأدلة الرقمية محل الشك. ويكتسب ذلك أهمية خاصة في ضوء ما خلصت إليه الدراسة الأصلية من ضرورة تطوير آليات تحقق موحدة ومعتمدة قضائياً، وتعزيز التعاون بين المؤسسات القانونية والفنية.



6.1 منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي لتحليل القواعد القانونية الإماراتية المنظمة للإثبات الإلكتروني، ولا سيما الأحكام المتعلقة بسلامة الدليل وإمكانية نسبته وموثوقيته، وتحليل مدى قابليتها للتطبيق على الأدلة الرقمية المتأثرة بالتزيف العميق. كما يوظف البحث المنهج المقارن من خلال تحليل بعض القواعد والممارسات القانونية في النظامين الفرنسي والأمريكي، مع التركيز على معايير الأصالة والمصادقة والخبرة الفنية وسلسلة حفظ الدليل.

ويستعين البحث كذلك بالمنهج الاستنباطي القانوني، من خلال الانتقال من المبادئ العامة التي تحكم حجية الأدلة الرقمية إلى تطبيقها على حالة خاصة تتمثل في الأدلة التي يحتمل أن تكون قد أنشئت أو عُُدلت بواسطة تقنيات الذكاء الاصطناعي. وقد اعتمدت الدراسة الأصلية نفسها على هذه المناهج بصورة متكاملة، حيث وظفت المنهج الاستنباطي والوصفي التحليلي والمقارن لدراسة حجية الأدلة الرقمية والتزيف العميق في التشريع الإماراتي.

7.1 الدراسات السابقة والفجوة البحثية

تناولت الدراسات السابقة موضوع الأدلة الرقمية والتزيف العميق من زوايا متعددة. فقد ركز أبو العز (2023) على دور التقنيات العلمية الحديثة في الإثبات الجنائي، مؤكداً أهمية الوسائل التقنية في دعم تكوين القناعة القضائية في الجرائم المستحدثة. كما تناول لطفي (2021) الأدلة الجنائية الحديثة ودورها في إثبات الجرائم الإلكترونية، مع التركيز على الأدلة التقنية وتحليل البيانات الرقمية.

وفي السياق العربي، تناولت المعمرية (2024) حجية الدليل الرقمي في الإثبات الجزائي، وأبرزت مشكلة غياب المعايير التقنية الدقيقة للتحقق من مصداقية الأدلة الرقمية. كما بحث المعموري (2025) حجية استخدام الذكاء الاصطناعي في الإثبات الجنائي، وأكدت ضرورة إخضاع مخرجات الذكاء الاصطناعي للرقابة القضائية والفحص الفني.

كما تناولت محمود (2026) الأدلة المتحصلة بواسطة الذكاء الاصطناعي وحجيتها في قانون الإثبات العراقي، وأبرزت إشكالية مصدر الدليل التقني وإمكانية الطعن في دقته أو التلاعب به، والحاجة إلى الخبرة الفنية المتخصصة.

أما مكتوف وعاشور (2025) فقد ركزا على جريمة التزيف العميق وتكييفها القانوني والتحديات الإجرائية التي تثيرها في البيئة الرقمية، بينما تناولت دراسات أخرى التزيف العميق من منظور المسؤولية الجزائية والتهديد الذي يشكله على الأفراد والمجتمع.

وعلى المستوى الأجنبي، قدمت دراسة Maras and Alexandrou (2019) معالجة مباشرة لإشكالية تحديد أصالة الأدلة المرئية في عصر الذكاء الاصطناعي، بينما ركز Delfino (2023) على دور القاضي في التعامل مع الأدلة المرتبطة بالتزيف العميق والحاجة إلى تطوير وظيفة المحكمة في التحقق من أصالتها. كما ناقش Dixon (2021) مستقبل قانون الإثبات في ظل الذكاء الاصطناعي والتزيف العميق، في حين تناول Pfeifferkorn (2021) التحديات القانونية والمعايير الإثباتية المتعلقة بالتزيف العميق أمام القضاء. وتبحث دراسات أحدث في الأدلة الاصطناعية من منظور الخبرة الفنية والتحقق الجنائي الرقمي (Amerini & Caldelli, 2025; Hydera et al., 2024; Hydera et al., 2025). وعلى الرغم من أهمية هذه الدراسات، فإن الفجوة التي يسعى البحث الحالي إلى معالجتها تتمثل في عدم الجمع بصورة مركزة بين ثلاثة عناصر مترابطة: أصالة الدليل الرقمي، وسلسلة حفظه، والإطار الإجرائي اللازم للتحقق من الأدلة المتأثرة بالتزيف العميق في التشريع الإماراتي. وهذه الإضافة تجعل البحث مختلفاً عن الدراسة الأصلية، رغم استفادته المباشرة من مادتها العلمية.

2. الإطار القانوني لإثبات أصالة الدليل الرقمي في التشريع الإماراتي

2.1 الاعتراف التشريعي بالدليل الرقمي

شهد التشريع الإماراتي خلال السنوات الأخيرة تطوراً ملحوظاً في الاعتراف بالأدلة الإلكترونية وإدماجها ضمن منظومة الإثبات القانونية. ويأتي المرسوم بقانون اتحادي رقم (35) لسنة 2022 بشأن الإثبات في المعاملات المدنية والتجارية في مقدمة التشريعات التي عززت هذا الاتجاه، إلى جانب المرسوم بقانون اتحادي رقم (46)



لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة. ويقوم هذا التوجه على عدم التمييز بين الدليل التقليدي والدليل الإلكتروني لمجرد اختلاف الوسيط الذي يحتويه، وإنما على مدى توافر شروط الموثوقية والسلامة وإمكانية نسبة الدليل إلى مصدره.

ويعكس هذا الاتجاه انتقال المشرع الإماراتي من المفهوم الشكلي للإثبات إلى مفهوم أكثر مرونة يقوم على الوظيفة الإثباتية للدليل؛ فالعبارة ليست بكون المعلومات مثبتة على ورق أو محفوظة إلكترونياً، وإنما بقدرتها على التعبير عن واقعة قانونية وإمكانية التحقق من سلامتها ومصدرها. ويعد هذا الاتجاه متوافقاً مع التطور العام في قوانين الإثبات الحديثة التي اتجهت إلى الاعتراف بالمحركات والبيانات الإلكترونية متى توافرت الضمانات اللازمة لحمايتها من التعديل أو التلاعب (الزهراني، 2023؛ نور الدين، 2023).

وقد أشار الملف محل الدراسة إلى أن المادة (8) من قانون الإثبات الإماراتي تشترط بالنسبة للمحرر الإلكتروني أن تكون المعلومات الواردة فيه محفوظة في ظروف تضمن عدم تغييرها، وأن يكون من الممكن التحقق من مصدرها ونسبتها إلى صاحبها. وبشكل ذلك أساساً قانونياً مهماً لمفهوم أصالة الدليل الرقمي، حتى وإن لم يستخدم المشرع مصطلح "الأصالة" بالمفهوم التقني المتداول في الأدبيات الجنائية الرقمية.

غير أن هذا التنظيم، على الرغم من أهميته، يواجه تحدياً جوهرياً عند تطبيقه على محتوى التزييف العميق. فالمشكلة في الدليل المزيف بواسطة الذكاء الاصطناعي ليست بالضرورة في سلامة الملف ذاته أو قابليته للتخزين والاسترجاع، وإنما في العلاقة بين المحتوى والواقع. فقد يكون الملف محفوظاً بطريقة سليمة ولم يتعرض لأي تعديل منذ لحظة ضبطه، ومع ذلك يكون المحتوى الذي يتضمنه مصطنعاً بالكامل. وهنا يظهر الفرق بين سلامة الملف وصدق المحتوى.

وتؤكد الأدبيات أن هذا التمييز أصبح ضرورياً في عصر التزييف العميق؛ إذ إن التقنيات الحديثة تستطيع إنتاج محتوى يستوفي ظاهرياً متطلبات السلامة التقنية، بينما يكون غير حقيقي في جوهره (Maras & Alexandrou, 2019; Dixon, 2021). وبالتالي فإن إثبات سلامة الملف وحده لم يعد كافياً لضمان أصالة المحتوى.

2.2 شروط الأصالة في مواجهة التزييف العميق

يمكن تحديد أصالة الدليل الرقمي من خلال مجموعة مترابطة من العناصر، أهمها: المصدر، وسلامة المحتوى، وسلامة البيانات الوصفية، وسلسلة الحفظ، وإمكانية إعادة الفحص، وموثوقية الوسيلة التقنية المستخدمة للتحقق منه.

ويكتسب عنصر المصدر أهمية خاصة؛ لأن الدليل الرقمي قد ينسب ظاهرياً إلى شخص معين دون أن يكون صادرًا عنه بالفعل. وهذه الإشكالية تظهر بصورة واضحة في التزييف العميق الصوتي والمرئي، حيث يمكن محاكاة الصوت أو الصورة أو الحركات بطريقة تجعل النسبة الظاهرية غير كافية لإثبات النسبة الحقيقية. وقد أشارت الدراسة إلى أن شرط إمكانية نسبة الدليل إلى صاحبه، رغم أهميته في التشريع الإماراتي، يواجه تحدياً كبيراً عندما يمكن لتقنيات التزييف العميق إنشاء محتوى ينسب ظاهرياً إلى شخص لم يصدر عنه.

ومن ثم، فإن مفهوم الأصالة في الأدلة الرقمية الحديثة ينبغي ألا يقتصر على سؤال: من صاحب الملف؟ وإنما ينبغي أن يتوسع ليشمل أسئلة أخرى، من قبيل: كيف أنشئ الملف؟ ومتى أنشئ؟ وهل كان محتواه موجوداً قبل عملية المعالجة؟ وما البرامج التي استخدمت في إنتاجه أو تعديله؟ وهل توجد نسخة أصلية يمكن الرجوع إليها؟ وهل تتوافق البيانات الوصفية مع الادعاءات المتعلقة بمصدره وتاريخه؟

ويؤكد Casey (2020) أن القيمة الإثباتية للدليل الرقمي ترتبط ارتباطاً وثيقاً بسلامة إجراءات جمعه وحفظه وتحليله، لأن أي خلل في هذه المراحل قد يؤثر في إمكانية الاعتماد عليه أمام المحكمة. كما أن تطوير تقنيات التزييف العميق يجعل الاعتماد على الملاحظة البشرية وحدها غير كافٍ للتحقق من أصالة المحتوى (Casey, 2020; Amerini & Caldelli, 2025).



3.2 سلسلة حفظ الدليل الرقمي وأثرها في إثبات الأصالة

1.3.2 مفهوم سلسلة الحفظ

تمثل سلسلة حفظ الدليل أحد أهم الضمانات الإجرائية التي تسمح بإثبات أن الدليل الذي يقدم إلى المحكمة هو ذاته الدليل الذي تم الحصول عليه في مرحلة جمع الأدلة، وأنه لم يتعرض لتغيير أو استبدال أو معالجة غير موثقة خلال مراحل انتقاله وفحصه.

ولا ينبغي فهم سلسلة الحفظ باعتبارها مجرد سجل إداري لحيازة الدليل، بل بوصفها آلية إثباتية متكاملة توثق تاريخ الدليل الرقمي منذ لحظة اكتشافه وحتى تقديمه للقضاء. ويتضمن ذلك تحديد الشخص أو الجهة التي حصلت عليه، وتوقيت الحصول عليه، وطريقة الاستخراج، والوسيلة المستخدمة للحفظ، والجهات التي تعاملت معه، وأي إجراءات فنية أجريت عليه.

وتكتسب هذه المسألة أهمية خاصة في الأدلة الرقمية؛ لأن الملف الإلكتروني يمكن نسخه مرات متعددة دون أن تظهر عليه بالضرورة علامات التغيير المادي التي يمكن ملاحظتها في الأدلة التقليدية. ولهذا يعتمد الفحص الجنائي الرقمي على إجراءات متخصصة للحفاظ على النسخة الأصلية وإنشاء نسخ عمل يمكن فحصها دون المساس بالأصل. (Casey, 2011; Casey, 2020)

وقد أكدت الدراسة محل البحث أن التشريع الإماراتي لا يتضمن تنظيمًا تفصيليًا وصريحًا لسلسلة حفظ الدليل الرقمي، رغم أن اشتراط سلامة المحرر الإلكتروني وإمكانية نسبته وظروف حفظه يمكن أن يشكل أساساً قانونياً غير مباشر لهذا المفهوم.

1.3.2 قصور المفهوم التقليدي لسلسلة الحفظ

تواجه سلسلة الحفظ التقليدية تحدياً جديداً يتمثل في الأدلة التي لا تنتقل بين الأشخاص بالمعنى التقليدي، وإنما تنشأ مباشرة بواسطة أنظمة الذكاء الاصطناعي.

ففي حالة تسجيل فيديو تقليدي، يمكن تحديد الجهاز الذي سجل الفيديو، ومكان التسجيل، وتاريخ التسجيل، والأشخاص الذين حصلوا على الملف بعد ذلك. أما إذا كان الفيديو قد أنشئ بالكامل بواسطة نموذج ذكاء اصطناعي، فإن السؤال يصبح أكثر تعقيداً: من هو "مصدر" الدليل؟ هل هو المستخدم الذي أدخل الأوامر؟ أم البرنامج الذي أنشأه؟ أم البيانات التي درب عليها النموذج؟ أم الجهاز الذي حفظ النتيجة؟

وهذا ما يجعل سلسلة الحفظ التقليدية بحاجة إلى إعادة تعريف. وقد أظهرت الدراسة أن مفهوم سلسلة الحيازة يصبح غير كافٍ في حالة الأدلة التي يتم إنشاؤها بالكامل بواسطة الذكاء الاصطناعي، لأنها قد لا تمر أصلاً بالمرحلة التقليدية للحيازة والنقل.

ومن هنا يمكن اقتراح الانتقال من مفهوم Chain of Custody إلى مفهوم أكثر شمولاً يمكن تسميته:

سلسلة منشأ وسلامة الدليل الرقمي. (Digital Evidence Provenance and Integrity Chain)

ويشمل هذا المفهوم ليس فقط الأشخاص الذين حازوا الدليل، وإنما كذلك البيئة التقنية التي أنشئ فيها الدليل، والبرمجيات والأدوات المستخدمة في معالجته، والبيانات الوصفية المرتبطة به، وعمليات النقل والتخزين والتحليل.

4.2 دور الخبرة الفنية في إثبات أصالة الدليل

لا يمكن التعامل مع التزيف العميق باعتباره مسألة قانونية بحتة؛ إذ إن إثبات وجود التلاعب غالباً ما يتطلب معرفة تقنية متخصصة تتجاوز المعرفة القانونية للقاضي.

ويؤدي الخبير الفني دوراً محورياً في تحليل البيانات الوصفية، وفحص بنية الملف، وتحليل الأنماط الصوتية أو المرئية، والتحقق من وجود مؤشرات على المعالجة الاصطناعية. كما يمكن استخدام أدوات متقدمة للكشف عن عدم الاتساق في الصور أو الفيديوهات أو التسجيلات الصوتية.

وتؤكد الدراسات التقنية الحديثة أن التطور المتسارع في أدوات التزيف العميق يجعل عملية الكشف أكثر تعقيداً، وأن تقنيات الكشف نفسها تحتاج إلى التطوير المستمر لمواكبة تقنيات الإنشاء والتلاعب (Amerini &

Caldelli, 2025; Hydera et al., 2024; Hydera et al., 2024).



وقد أشارت الدراسة إلى أن قانون الإثبات الإماراتي يسمح للمحكمة بالاستعانة بالخبرة الفنية، إلا أن اللجوء إليها يظل في الأصل خاضعاً لتقدير المحكمة. وتتمثل الإشكالية في أن بعض الأدلة قد تكون ذات طبيعة تقنية لا يستطيع القاضي تقييمها بصورة دقيقة اعتماداً على الخبرة القضائية العامة وحدها.

وتبرز المقارنة الأمريكية أهمية هذه المسألة بصورة واضحة، إذ تربط القاعدة الفيدرالية رقم (702) قبول شهادة الخبير بموثوقية الأساس العلمي والمنهجي الذي تستند إليه. كما أن القاعدة (901) تضع متطلبات لإثبات أصالة الدليل قبل اعتماده.

وقد ذهب Thomson (2024) إلى ضرورة تعزيز الدور الرقابي للقاضي باعتباره "حارس بوابة" للأدلة الرقمية، بحيث لا يقتصر دوره على استقبال تقرير الخبير، وإنما يمتد إلى التأكد من أن المنهجية التي استخدمت للتحقق من الدليل تتمتع بدرجة مناسبة من الموثوقية (Thomson, 2024).

وفي السياق نفسه، يرى Delfino (2023) أن انتشار التزييف العميق يفرض إعادة التفكير في الدور التقليدي للقاضي عند تقييم الأدلة الرقمية، لأن التحدي لم يعد متعلقاً بوجود دليل تقني فقط، وإنما بقدرة المحكمة على التمييز بين المحتوى الحقيقي والمحتوى الاصطناعي (Delfino, 2023).

5.2 عبء إثبات أصالة الدليل في قضايا التزييف العميق

تثير الأدلة الناتجة عن التزييف العميق مشكلة خاصة فيما يتعلق بعبء الإثبات. فالقواعد العامة تفترض عادة أن الطرف الذي يتمسك بالدليل يقدم الأساس الذي يسمح بقبوله، بينما يتحمل الطرف الذي يطعن في صحته عبء إثبات ما يدعيه بحسب طبيعة الدعوى والقواعد الإجرائية المطبقة.

إلا أن تطبيق هذه القاعدة بصورة جامدة على التزييف العميق قد يؤدي إلى نتائج غير متوازنة. فإذا قدم أحد الخصوم مقطعاً مرئياً يبدو واقعياً، ثم ادعى الخصم الآخر أنه مصطنع باستخدام الذكاء الاصطناعي، فقد يتطلب إثبات التزييف أدوات تقنية متقدمة وخبرة متخصصة وتكلفة مالية قد لا تكون متاحة للطرف الذي يطعن في الدليل.

وقد أشارت الدراسة الأصلية إلى أن توزيع عبء الإثبات التقليدي قد يمثل عبئاً تقنياً ومالياً كبيراً على الطرف الذي يدعي زيف الدليل، واقترحت إمكان نقل عبء الإثبات في الحالات التي يتمكن فيها الخصم من إثارة شك معقول حول أصالة الدليل.

ولا يعني هذا الاقتراح إهدار القواعد العامة لعبء الإثبات، وإنما يعني إعادة تفسيرها بما يتناسب مع الطبيعة الخاصة للدليل الاصطناعي. فمتى أثار الطرف المعارض شكاً فنياً جدياً ومعقولاً بشأن أصالة الدليل، ينبغي ألا يبقى عبء إثبات العكس بالكامل على عاتقه، وإنما ينبغي أن يطلب من الطرف المتمسك بالدليل تقديم الأساس الفني الذي يثبت مصدره وسلامته.

ويتفق هذا الاتجاه مع الهدف العام المتمثل في تحقيق التوازن بين حرية الإثبات وحماية الخصوم من الأدلة المصطنعة، دون تحويل مجرد الادعاء بالتزييف العميق إلى وسيلة لتعطيل العدالة.

6.2 التزييف العميق ومبدأ الافتناع القضائي

يقوم القضاء في العديد من الأنظمة القانونية على منح القاضي سلطة تقديرية واسعة في وزن الأدلة وتكوين اقتناعه القضائي. وتتيح هذه السلطة للقاضي تقييم الأدلة مجتمعة بدلاً من إخضاعها لنظام آلي جامد.

إلا أن التزييف العميق يكشف حدود هذا النموذج؛ لأن القاضي قد يستطيع تقييم مضمون التسجيل أو الفيديو وسياقه، ولكنه قد لا يستطيع بنفسه تحديد ما إذا كان الملف قد تعرض لتعديل بواسطة خوارزمية ذكاء اصطناعي. وهنا تظهر الحاجة إلى التمييز بين السلطة القانونية للقاضي والقدرة التقنية على التحقق. فالقاضي يظل صاحب الاختصاص في تقدير القيمة الإثباتية للدليل، لكن ذلك لا يعني أن عليه أن يقوم بنفسه بالتحليل التقني للملف.

وتشير الدراسة إلى أن القضاء الإماراتي، رغم مرونته في قبول الأدلة الرقمية، يعتمد بدرجة كبيرة على الاقتناع القضائي دون وجود معايير تقنية تفصيلية، وهو ما قد يؤدي إلى اختلاف النتائج في القضايا التي تتضمن أدلة رقمية معقدة.

ويؤكد Delfino (2023) أن تطور تقنيات التزييف العميق يستدعي توسيع الدور الرقابي للقاضي قبل السماح للدليل التقني بالوصول إلى مرحلة الاعتماد النهائي، بينما يرى Thomson (2024) ضرورة تعزيز دور المحكمة في فحص أساس الدليل قبل السماح له بالتأثير في تكوين القناعة القضائية.



وعليه، فإن المطلوب ليس تقليص السلطة التقديرية للقاضي، وإنما تدعيمها بأدوات فنية وإجرائية تمكنه من ممارسة هذه السلطة على أساس علمي موثوق.

7.2 الدراسة المقارنة: الإمارات وفرنسا والولايات المتحدة

1.7.2 النموذج الإماراتي

يمتاز النموذج الإماراتي بالاعتراف الواسع بالأدلة الإلكترونية وربط حجيتها بمفاهيم السلامة والموثوقية وإمكانية النسبة. إلا أن التشريع لا يتضمن تنظيمًا تفصيليًا خاصًا بالتزيف العميق أو الأدلة التي يتم إنشاؤها بواسطة الذكاء الاصطناعي. وتتمثل أهم نقاط القوة في مرونة الإطار القانوني وإمكانية الاستفادة من الخبرة الفنية، بينما تتمثل نقطة الضعف الرئيسية في غياب بروتوكول إجرائي موحد للتحقق من أصالة الدليل الاصطناعي.

2.7.2 النموذج الفرنسي

يستند النظام الفرنسي إلى مبدأ الاعتراف بالحجية القانونية للكتابة الإلكترونية متى أمكن التعرف على مصدرها وضمان سلامتها. وتعد المادة (1366) من القانون المدني الفرنسي أساسًا مهمًا في هذا المجال. غير أن هذا النموذج، رغم تقدمه، لا يقدم إطارًا متخصصًا للتزيف العميق، كما أن إجراءات الفحص الفني لا تزال تعتمد بدرجة كبيرة على الخبرة والممارسة القضائية. وقد أشارت الدراسة إلى أن أي خلل في ظروف حفظ الدليل يمكن أن يؤثر في حجته، وأن الخبرة الفنية تلعب دورًا مهمًا في تحديد مدى تعرض الدليل للتعديل.

3.7.2 النموذج الأمريكي

يقدم النظام الأمريكي نموذجًا أكثر تفصيلًا في مجال مصادقة الأدلة، ولا سيما من خلال القاعدة (901) التي تتطلب أساسًا كافيًا لإثبات أن الدليل هو ما يدعي مقدمه أنه كذلك، إلى جانب القاعدة (702) الخاصة بالخبرة العلمية والفنية. كما أن الاتجاه القضائي الأمريكي يولي أهمية متزايدة لدور القاضي باعتباره "حارس بوابة" في التعامل مع الأدلة التقنية، خاصة في الحالات التي يمكن أن يؤدي فيها الاعتماد على دليل غير موثوق إلى التأثير بصورة جوهرية في نتيجة الدعوى. (Delfino, 2023; Thomson, 2024) ومع ذلك، لا يخلو النموذج الأمريكي نفسه من الصعوبات؛ إذ إن التزيف العميق يمثل تحديًا لمفهوم المصادقة التقليدي القائم على إثبات أن الدليل يمثل ما يدعي مقدمه أنه يمثل، خصوصًا عندما يمكن إنتاج الدليل دون وجود مصدر واقعي أصلي. وقد خلصت الدراسة إلى أن النماذج الإماراتية والفرنسية والأمريكية تشترك، رغم اختلافاتها، في الاعتماد على قواعد إثبات عامة لم تُصمم أصلاً للتعامل مع المحتوى الاصطناعي المتقدم.

8.2 الإطار الإجرائي المقترح لإثبات أصالة الأدلة الرقمية

استنادًا إلى التحليل السابق، يقترح البحث إطارًا إجرائيًا يتكون من عشر مراحل مترابطة:

المرحلة الأولى: التوثيق الأولي

يجب توثيق لحظة ضبط الدليل، ومكان الحصول عليه، والجهاز أو الوسيط الذي استخرج منه، والجهة القائمة بالإجراء.

المرحلة الثانية: المحافظة على الأصل

ينبغي الحفاظ على النسخة الأصلية من الدليل دون إجراء أي معالجة عليها، وإنشاء نسخة عمل للفحص والتحليل.

المرحلة الثالثة: إنشاء البصمة الرقمية

يجب إنشاء قيمة Hash للنسخة الأصلية لإثبات عدم تغييرها أثناء مراحل الفحص.

المرحلة الرابعة: توثيق البيانات الوصفية

ينبغي استخراج البيانات الوصفية Metadata وتوثيقها، بما في ذلك تاريخ الإنشاء والجهاز والبرنامج ومعلومات التعديل المتاحة.



المرحلة الخامسة: توثيق سلسلة الحفظ

ينبغي تسجيل كل شخص أو جهة تعاملت مع الدليل، وكل عملية نقل أو تخزين أو فحص تمت عليه.

المرحلة السادسة: الفحص الفني الأولي

عند وجود مؤشرات معقولة على التزيف العميق، ينبغي إجراء فحص فني متخصص بدل الاكتفاء بالفحص البصري أو السمعي.

المرحلة السابعة: الفحص متعدد الأدوات

لا ينبغي الاعتماد على أداة واحدة للكشف عن التزيف، وإنما استخدام أكثر من منهج أو تقنية متى كان ذلك ممكناً، لأن تقنيات الكشف نفسها قد تكون عرضة للأخطاء أو التطور المضاد.

المرحلة الثامنة: تقرير الخبير

ينبغي أن يتضمن التقرير الفني منهجية الفحص، والأدوات المستخدمة، ودرجة موثوقيتها، والنتائج، والقيود التي واجهت عملية الفحص.

المرحلة التاسعة: تمكين الخصوم من الطعن

يجب تمكين الطرف الآخر من الاطلاع على الأساس الفني الذي بني عليه التقرير، ومن الاستعانة بخبير مقابل عند الحاجة.

المرحلة العاشرة: التقدير القضائي النهائي

بعد اكتمال الإجراءات، يبقى للقاضي تقدير القيمة الإثباتية للدليل في ضوء مجموع الأدلة، دون أن يكون تقرير الخبير ملزماً له.

وتتوافق هذه الآلية مع ما خلصت إليه الدراسة الأصلية من ضرورة اعتماد بروتوكول وطني موحد لفحص الأدلة الرقمية، وتنظيم الخبرة المتخصصة، وتوثيق سلسلة حفظ الدليل.

3. النتائج

توصل البحث إلى مجموعة من النتائج، أهمها:

أولاً: إن الإطار التشريعي الإماراتي يعترف بالدليل الإلكتروني ويمنحه حجية قانونية متى استوفى شروط السلامة والموثوقية وإمكانية النسبة، إلا أن هذه القواعد العامة لا تتضمن تنظيمًا تفصيليًا للأدلة الناتجة عن تقنيات التزيف العميق.

ثانيًا: إن مفهوم أصالة الدليل الرقمي أصبح أكثر تعقيداً نتيجة تقنيات الذكاء الاصطناعي، ولم يعد كافيًا التحقق من سلامة الملف أو مصدره الظاهري، بل يجب التحقق من العلاقة بين المحتوى والواقعة التي يدعي الدليل إثباتها. ثالثًا: إن سلسلة حفظ الدليل تمثل ضماناً أساسية في إثبات سلامة الأدلة الرقمية، إلا أن مفهومها التقليدي يواجه تحدياً في الأدلة التي يتم إنشاؤها مباشرة بواسطة الذكاء الاصطناعي.

رابعاً: إن غياب بروتوكول موحد لسلسلة حفظ الأدلة الرقمية قد يؤدي إلى تفاوت في الممارسة القضائية ويزيد احتمالية الاعتماد على أدلة غير موثوقة.

خامساً: إن الخبرة الفنية ينبغي أن تتجاوز مجرد كونها وسيلة اختيارية في الحالات التقنية المعقدة، وأن تكون إلزامية متى أثبتت شبهة جدية ومدعومة فنياً بشأن أصالة الدليل.

سادساً: إن القواعد الأمريكية المتعلقة بمصادقة الدليل والخبرة تقدم نموذجاً مفيداً يمكن الاستفادة منه، وإن كان لا يخلو هو الآخر من تحديات في مواجهة الأدلة الاصطناعية.

4. التوصيات

في ضوء النتائج السابقة، يوصي البحث بما يلي:

أ. إدخال تنظيم تشريعي صريح للأدلة الرقمية المتأثرة بتقنيات الذكاء الاصطناعي والتزيف العميق ضمن قانون الإثبات الإماراتي أو تشريع مكمل.

ب. اعتماد تعريف قانوني للدليل الاصطناعي يميز بين الدليل الرقمي التقليدي والدليل الذي تم إنشاؤه أو تعديله بواسطة الذكاء الاصطناعي.

ت. إقرار بروتوكول وطني موحد لسلسلة حفظ الدليل الرقمي يتضمن جميع مراحل جمع الدليل وحفظه ونقله وتحليله.



- ث. إلزام الجهات المختصة بإنشاء بصمة رقمية للنسخة الأصلية وتوثيقها منذ لحظة ضبط الدليل .
ج. إلزام الجهات القضائية بإجراء فحص فني متخصص عندما تثار شبهة جدية بشأن استخدام التزييف العميق .
ح. إنشاء سجل أو نظام اعتماد متخصص لخبراء الأدلة الرقمية والذكاء الاصطناعي مع اشتراط التدريب المستمر .
خ. وضع معايير قانونية لقبول تقارير كشف التزييف العميق بحيث لا تعتمد المحكمة على نتيجة أداة تقنية واحدة دون تقييم منهجيتها ودرجة موثوقيتها .

المراجع

1. أبو العز، عصام. (2023). دور التقنيات العلمية الحديثة في الإثبات الجنائي للجرائم المستحدثة. دار النهضة العربية.
2. أبو سيف، محمود حسين سيد. (2025). التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوروبي. مجلة العلوم القانونية والاقتصادية، 67(1)، 16-42.
3. البدرابي، عبد المنعم. (1966). نظرية الإثبات في المواد المدنية والتجارية. دار النهضة العربية.
4. البواب، سباتا عصام سليم. (2024). مدى حجية الأدلة الجزائية في إثبات جرائم مواقع التواصل الاجتماعي في القانون الأردني [رسالة ماجستير غير منشورة]. جامعة الإسراء الخاصة.
5. بوسحرة، ليليا، وبودريالة، عبد القادر. (2023). التزييف العميق والدعاية الرقمية في عصر التمكين الرقمي: قراءة في النماذج والرهانات. مجلة مصداقية، 5(1)، 94.
6. تحفة، أسماء. (2020). مقارنة بين حجية الدليل الجنائي والدليل العلمي في ضوء استخدام الوسائل التكنولوجية الحديثة. مجلة القانون الجنائي المعاصر، 6، 55-59.
7. الخولي، أحمد. (2021). الدليل الإلكتروني وحجبه في الإثبات. دار النهضة العربية.
8. الدناصور، عزمي، والشواربي، عبد الحميد. (1985). الإثبات في المواد المدنية والتجارية. دار النهضة العربية.
9. الزهراني، عبد الرحمن بن أحمد. (2023). الإثبات الجنائي بالوسائل الإلكترونية في ضوء التطور الرقمي.
10. الصويلح، سعد بن محمد. (2023). دور أنظمة الذكاء الاصطناعي في مكافحة الشائعات الإلكترونية. مجلة الدراسات الأمنية، 169، 201-210.
11. الشمري، فهد بن ناصر. (2025). حجية الأدلة الرقمية في ظل تقنيات الذكاء الاصطناعي والتزييف العميق: دراسة مقارنة. المجلة العربية للفقهاء والقضاء، 17(1)، 89-126.
12. عبود، وليد فرمان. (2024). التحديات التي تواجه الإثبات الرقمي في الجرائم الإلكترونية. مجلة العلوم القانونية الحديثة، 6(4)، 255-312.
13. عبد اللطيف، محمد حسنين. (1972). مبادئ الإثبات في القانون المدني. دار النهضة العربية.
14. عبد الله، حسن محمود. (2023). تقنيات التحقيق الجنائي الرقمي وأثرها في الإثبات .
15. المعاينة، معن نايل محمود. (2024). استراتيجيات الأمن السيبراني ودورها في حماية الأدلة الرقمية . مجلة العلوم الإنسانية والتطبيقية، 15(2)، 294.
16. المعمريّة، منار بن حمد بن سليمان. (2024). حجية الدليل الرقمي في الإثبات الجزائي في التشريع العماني: دراسة مقارنة [رسالة ماجستير غير منشورة]. جامعة السلطان قابوس.
17. المعموري، سلمى غضبان حسين. (2025). حجية استخدام الذكاء الاصطناعي في الإثبات الجنائي: دراسة مقارنة [أطروحة دكتوراه غير منشورة]. جامعة بغداد.
18. محمود، رنا صادق. (2026). الأدلة المتحصلة بواسطة الذكاء الاصطناعي وحجيتها في الإثبات: دراسة في قانون الإثبات العراقي. مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية، 3(2)، 180-197.
19. مكتوف، محمود، وعاشور، عبد الرحمن. (2025). جريمة التزييف العميق: التكيف القانوني والتحديات الإجرائية في البيئة الرقمية. مجلة العلوم القانونية، 12، 55-159.



مجلة الفنون والأدب وعلوم الإنسانية والاجتماع

Journal of Arts, Literature, Humanities and Social Sciences

Website: www.jalhss.com Email: editor@jalhss.com

Volume (133) October 2026 | العدد (133) أكتوبر 2026



20. مكطوف، صابر بن جاسم، وعاشور، أميل جبار. (2025). المسؤولية الجزائية عن جرائم التزييف العميق: دراسة مقارنة [رسالة ماجستير غير منشورة]. جامعة ميسان.
21. الناعي، محمد عبد الرحيم عبد الفتاح. (2019). حجية الدليل العلمي في الإثبات الجنائي: دراسة مقارنة [رسالة ماجستير غير منشورة]. الجامعة المستنصرية.
22. النجدي، يوسف بن علي. (2023). أثر التطور التكنولوجي على قواعد الإثبات التقليدية. مجلة القانون والتكنولوجيا، 4(1)، 23-51.
23. نور الدين، محمد عبد الكريم. (2023). حجية الدليل الإلكتروني في الإثبات الجنائي. مجلة الفقه والقانون، 11(2)، 59.
24. زيدان، محمود زكي. (2025). المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييف العميق: دراسة مقارنة. دار الفكر والقانون.
25. سليمان، أحمد عبد الرحمن. (2025). التحديات القانونية لاستخدام الذكاء الاصطناعي في القضاء. مجلة الدراسات القضائية، 9(2)، 69.
26. Amerini, I., & Caldelli, R. (2025). Deepfake media forensics: Status and future challenges. *Journal of Imaging*, 11(3), 73.
27. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.). Academic Press.
28. Casey, E. (2020). *Digital evidence and computer crime: Forensic science, computers and the Internet* (4th ed.). Academic Press.
29. Cassia, M., Guarnera, L., Casu, M., Zangara, I., & Battiato, S. (2025). Deepfake forensic analysis and legal implications of synthetic media manipulation. *arXiv Research Paper*.
30. Çelebi, N., & Liu, Q. (2022). A survey of deepfake detection for trial courts. *International Journal of Digital Evidence and Forensics*, 14(2), 85–110.
31. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107.
32. Chukwuebuka, D. (2025). Is truth and integrity of justice on trial in the age of artificial intelligence (AI)? Re-assessing digital evidence in the context of AI-generated evidence such as deepfakes. *International Review of Law and Jurisprudence*, 7(1).
33. Delfino, R. A. (2023). Deepfakes on trial: A call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *Hastings Law Journal*, 74(2), 293–366.
34. Delmas-Marty, M. (2018). *Evidence and criminal procedure in comparative law*. Cambridge University Press.
35. Dixon, H. B. (2021). Deepfakes, artificial intelligence, and the future of evidence. *Judicature*, 105(2).
36. Dixon, J. (2024). The “deepfake defense”: An evidentiary conundrum. *Judges' Journal*, 63(2).
37. Grossman, M. R., & Grimm, P. W. (2025). Judicial approaches to acknowledged and unacknowledged AI-generated evidence. *Columbia Science and Technology Law Review*, 26(2).
38. Hydera, I., Sultan, A., Al-Kuwari, S., Al-Mutawa, N., et al. (2024). Digital evidence integrity and deepfake detection in modern judicial systems. *Digital Investigation*, 48, 101–119.



39. Hydera, M., Kikuchi, M., & Ozono, T. (2024). Empirical assessment of deepfake detection: Advancing judicial evidence verification through artificial intelligence. *IEEE Access*, 12, 151188–151203.
40. Losey, R. (2024). The problem of deepfakes and AI-generated evidence: Is it time to revise the rules of evidence? *EDRM Journal*.
41. Ma'arif, A. (2025). Social, legal, and ethical implications of AI-generated deepfake content. *Journal of Information Ethics*.
42. Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *International Journal of Evidence & Proof*, 23(3), 255–262. <https://doi.org/10.1177/1365712718807226>
43. Pfefferkorn, R. (2021). "Deepfakes" in the courtroom: Legal challenges and evidentiary standards. Silicon Flatirons Center, University of Colorado Law School.
44. Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework. *Computer Law & Security Review*.
45. Sandoval, M. P. (2024). Threat of deepfakes to the criminal justice system. *International Journal of Cybersecurity*.
46. Sandoval, M.-P., de Almeida Fiuza, M., Solas, J., & Rodríguez, L. (2022). Deepfakes and the criminal justice system: A systematic review of threats and challenges. *Criminology*.
47. Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13(1).
48. Singh, R. (2025). Deepfake evidence and criminal trials. *Journal of Law and Emerging Technologies*.
49. Singh, S., & Dhiman, S. (2025). Cybercrime and computer forensics in the age of AI. *arXiv Research Paper*.
50. Stojkovski, N. F. (2024). Threats of deepfakes to the criminal justice system: A systematic review. *Journal of Digital Forensics*, 1(1), 163.
51. Thomson, L. (2024). Deepfakes on trial: A call to expand the trial judge's gatekeeping. *Harvard Journal of Law & Technology*, 38(1), 115–182.
52. Thomson, S. (2023). Deepfakes and the future of evidence law. *Journal of Digital Forensics and Legal Studies*, 12(3).
53. Veale, M., & Borgesius, F. Z. (2021). *Demystifying the draft EU Artificial Intelligence Act*. Hart Publishing.
54. Zuckerman, A. (2013). *Zuckerman on civil procedure: Principles of practice* (3rd ed.). Sweet & Maxwell.