

الأدلة الرقمية في المحاكمات الجزائية

حجيتها وحدود مشروعيتها

وثام المصري

أستاذ — القانون الجنائي

w.almasri@kilaw.edu.kw

Abstract

This article examines the probative value and legitimacy of digital evidence in criminal proceedings under Kuwaiti law. As cybercrime has become increasingly prevalent, traditional evidentiary instruments — including testimonial, documentary, and real evidence — have proven insufficient as sole bases for criminal adjudication. The study maps Kuwait's normative framework governing digital evidence, with particular attention to Article 39 of the Constitution, which guarantees the confidentiality of communications, and Law No. 63 of 2015 on Combating Information Technology Crimes, which establishes the statutory foundation for the admissibility of electronically-sourced proof.

The analysis engages with the Court of Cassation's ruling in Case No. 355/2019 as a landmark judicial recognition of digital evidence, conditioned upon the integrity of its provenance and the absence of procedural defect. The article identifies three structural challenges: the anonymization of offenders through virtual private networks, the authentication difficulties posed by AI-generated synthetic media, and institutional deficiencies in forensic digital capacity. The study concludes with de lege ferenda recommendations, including dedicated digital evidence legislation, the establishment of specialized forensic units, and reinforced bilateral cooperation frameworks to address the transboundary character of cybercrime.

الكلمات المفتاحية: الأدلة الرقمية · الإثبات الجنائي · الجرائم الإلكترونية · القانون الكويتي
· مشروعية الأدلة

الأدلة الرقمية في المحاكمات الجزائية

حجبتها وحدود مشروعيتها

وثام المصري

أستاذ القانون الجنائي

كلية القانون الكويتية العالمية (KILAW) — دولة الكويت

w.almasri@kilaw.edu.kw

استلم: يناير 2026 • قبل: مارس 2026

Abstract

تناول هذه الدراسة حجية الأدلة الرقمية وحدود مشروعيتها في المحاكمات الجزائية في ضوء النظام القانوني الكويتي. وفي ظل تنامي ظاهرة الجرائم الإلكترونية، باتت وسائل الإثبات التقليدية من شهادة ومستندات ومعاينة قاصرة وحدها عن تحقيق العدالة الجنائية. وتستند الدراسة إلى المادة (39) من الدستور الكويتي، وقانون مكافحة جرائم تقنية المعلومات رقم (63) لسنة 2015، وحكم محكمة التمييز في الطعن رقم (355/2019). وتتناول ثلاثة تحديات رئيسية: إخفاء هوية الجاني عبر الشبكات الافتراضية، وإشكاليات توثيق الوسائط المنشأة بالذكاء الاصطناعي، والقصور المؤسسي في الطاقة الجنائية الرقمية. وتخلص إلى جملة من التوصيات التشريعية والمؤسسية. الكلمات المفتاحية — الأدلة الرقمية؛ الإثبات الجنائي؛ الجرائم الإلكترونية؛ القانون الكويتي؛ مشروعية الأدلة.

1. الأجهزة الإلكترونية: حواسيب، هواتف ذكية، أجهزة تخزين — وتشمل الملفات والرسائل وسجلات التصفح.
2. الشبكات والأنظمة المعلوماتية: عناوين الإنترنت (IP)، سجلات الدخول والخروج، والبيانات المتبادلة عبر البريد الإلكتروني ووسائل التواصل.
3. الأدلة السمعية والبصرية الرقمية: تسجيلات صوتية أو مرئية من كاميرات أو تطبيقات ذكية، شريطة الحصول عليها بطريقة مشروعة لا تمس الخصوصية أو الحقوق الدستورية.

III. الأساس القانوني في النظام الكويتي

لم يضع المشرع الكويتي تعريفاً محدداً للأدلة الرقمية، إلا أن النصوص القانونية القائمة تؤكد اتجاهها واضحاً نحو الاعتراف بها كوسيلة مشروعة. وقد نصت المادة (39) من الدستور الكويتي [3] على أن: «حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبتها أو إفشاء سريتها إلا في الحالات التي يبينها القانون وبالإجراءات المنصوص عليها فيه». كما أكدت المادتان (78) و(87) من قانون الإجراءات والمحاكمات الجزائية على حرمة المساكن والمراسلات، وعدم جواز دخولها أو تفتيشها إلا في الأحوال التي حددها القانون، مما يُرسخ مبدأ حماية الخصوصية الرقمية.

A. قانون رقم (63) لسنة 2015

أصدر المشرع الكويتي قانون مكافحة جرائم تقنية المعلومات [4]، الذي وضع إطاراً تشريعياً خاصاً بالجرائم الإلكترونية. ونصت المادة (13) منه على تجريم الدخول غير المشروع إلى الأنظمة أو العبث بالبيانات الرقمية، وقد ساهم في ترسيخ القواعد التي تنظم مشروعية الدليل الرقمي وشروط قبوله.

B. موقف القضاء الكويتي

أكد حكم محكمة التمييز رقم (355/2019 جزائي) [5] اعتماد الأدلة الرقمية متى كانت سليمة في مصدرها وخالية من العيوب الفنية أو الإجرائية التي تمس سلامتها. ويُعد هذا الحكم من أوائل التطبيقات القضائية التي اعترفت صراحةً بحجية الأدلة الرقمية في الإثبات الجنائي الكويتي.

I. المقدمة

أحدثت الثورة الرقمية تحولاً جذرياً في شتى مجالات الحياة، فلم يعد تأثيرها مقتصرًا على الجوانب الاقتصادية والاجتماعية، بل امتد ليشمل المجالات السياسية والقانونية. وقد أفرز هذا التحول ما يُعرف بـ«الدبلوماسية الرقمية» التي تعتمد على الوسائط التقنية الحديثة كأداة للتواصل والتفاوض ونشر المواقف الرسمية للدول، مما يعكس عمق التحوّل الذي يشهده العالم. وفي إطار هذا التطور التقني، كان لقطاع العدالة نصيب بارز، إذ انتقل ميدان الإثبات من الأدلة التقليدية إلى الأدلة الرقمية التي أصبحت تمثل أداة رئيسة في كشف الحقيقة وإثبات الوقائع الجنائية. فلم تعد الشهادة والمعاينة والخبرة وغيرها كافية وحدها لتحقيق العدالة، في ظل تزايد الجرائم التي تتخذ من الفضاء الإلكتروني ميداناً لها.

وتكمن أهمية هذا البحث في تسليط الضوء على حجية الأدلة الرقمية وحدود مشروعيتها في المحاكمات الجزائية من خلال دراسة تستند إلى الواقع القانوني الكويتي، مع بيان الإشكاليات الفنية والقانونية التي تواجه جهات التحقيق والقضاء في التعامل مع هذا النوع من الأدلة.

II. مفهوم الأدلة الرقمية وأنواعها

تُعد الأدلة الرقمية من أبرز مخرجات التطور التكنولوجي. ويُقصد بها [1] كلُّ بيان أو معلومة ذات طابع إلكتروني يتم الحصول عليها أو حفظها أو نقلها أو معالجتها باستخدام الأجهزة والأنظمة التقنية، بحيث يمكن الاستدلال بها على واقعة قانونية محل نزاع أو تحقيق.

وتتميّز الأدلة الرقمية عن التقليدية في أنها بيانات غير ملبوسة تُخزّن داخل وسائط إلكترونية أو شبكات معلوماتية [2]، مما يجعلها أكثر عرضةً للتغيير أو التلاعب، ويستلزم إجراءات فنية وقانونية دقيقة في جمعها وتحليلها لضمان سلامتها أمام القضاء.

A. أنواع الأدلة الرقمية

يمكن تصنيف الأدلة الرقمية إلى ثلاثة أنواع رئيسية:

IV. حدود المشروعية والتحديات.

يُشترط لسلامة الدليل الرقمي أن يُجمع بطرق مشروعة لا تمس الحقوق والحريات، وأن يُقدّم أمام القضاء بعد التحقق من سلامته الفنية ومصادقته. وأي دليل يُحصل عليه بطريقة غير قانونية — كمراقبة المراسلات الإلكترونية دون أمر قضائي — يُعدّ باطلاً ولا يجوز التعويل عليه، وفقاً للمادتين (2) و(3) من قانون رقم (63) لسنة 2015.

A. إخفاء الهوية الرقمية

تبرز صعوبة تحديد هوية مرتكب الجريمة الإلكترونية بسبب لجوء الجناة إلى الشبكات الافتراضية الخاصة (VPN) [6]، وهي أنظمة تُخفي هوية المستخدم وموقعه الجغرافي عند الاتصال بالإنترنت، مما يُعسر تتبع مصدر الجريمة أو تحديد الفاعل الحقيقي.

B. تحديات الذكاء الاصطناعي

ظهرت أنظمة متطورة مثل Sora 2 [7] التي تولّد مقاطع فيديو واقعية من نصوص أو صور، مما يُثير تساؤلات قانونية حول مدى حجيتها كدليل أمام القضاء، خاصة في ظل صعوبة التمييز بين المحتوى الحقيقي والمُنشأ رقمياً.

C. القصور المؤسسي والتعاون الدولي

يُضاف إلى ذلك نقص الكوادر الفنية المتخصصة، وضرورة تطوير آليات التعاون بين جهات التحقيق وإدارة الجرائم الإلكترونية. كما يُمثل التعاون الدولي [8] ركيزة محورية في مكافحة الجرائم العابرة للحدود، وفق اتفاقية بودابست لعام 2001 ومذكرات التفاهم.

V. النتائج والتوصيات

A. النتائج

أظهرت الدراسة أن الأدلة الرقمية باتت أحد أهم وسائل الإثبات في القضايا الجزائية. وتبين أن المشرّع الكويتي وإن لم يضع تعريفاً محدداً لها، فإن أحكام قانون رقم (63) لسنة 2015 والقواعد العامة أرسّت الإطار القانوني الذي يضمن مشروعيّتها وشروط قبولها أمام القضاء.

B. التوصيات

1. وضع تشريع خاص بالأدلة الرقمية يبيّن ماهيتها وضوابط جمعها وشروط قبولها أمام القضاء.
2. تحديث النصوص القانونية القائمة لتواكب التطورات التقنية المستجدة في مجال الإثبات الرقمي.
3. إنشاء وحدات فنية متخصصة ضمن جهات التحقيق تتولى فحص وتحليل الأدلة الرقمية وإعداد تقارير فنية موثوقة.
4. تعزيز التنسيق المؤسسي بين الجهات الأمنية والفنية لضمان سرعة التعامل مع الجرائم الرقمية وحفظ سلامة الأدلة.
5. تفعيل التعاون الدولي والإقليمي في مجال مكافحة الجرائم الإلكترونية وتبادل المعلومات وفق الاتفاقيات الثنائية.
6. تطوير أدوات تقنية متقدمة للكشف عن التلاعب بالأدلة الرقمية وضمان موثوقيتها أمام القضاء.

VI. الخاتمة

يتبين أن الأدلة الرقمية تمثل نقلة نوعية في منظومة الإثبات الجزائي، إذ أوجدت واقعاً قانونياً جديداً يستلزم تطوير التشريعات لمواكبة الثورة التقنية وضمان تحقيق العدالة. ومن ثمّ فإن تنظيم هذا النوع من الأدلة بتشريع خاص يُعدّ ضرورةً تشريعية وعملية، تُوازن بين حماية الحقوق والحريات وصون العدالة الجنائية في العصر الرقمي.

References

- [1] ع. أحمد، الأدلة الرقمية في الإثبات الجنائي. دار النهضة العربية، القاهرة، 2019.
- [2] ح. محمود، التحقيق الجنائي الرقمي. دار الجامعة الجديدة، الإسكندرية، 2020.
- [3] دستور دولة الكويت، المادة (39).
- [4] قانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات. الجريدة الرسمية «الكويت اليوم»، العدد (1248)، 12 يوليو 2015.
- [5] محكمة التمييز الكويتية، الدائرة الجزائية. الطعن رقم (482/2018) جزائي، جلسة 15 مايو 2019.
- [6] VPN: اختصار Virtual Private Network (شبكة افتراضية خاصة).
- [7] Sora 2: نموذج ذكاء اصطناعي أصدرته OpenAI عام 2025.
- [8] اتفاقية بودابست لعام 2001 بشأن الجريمة الإلكترونية. مجلس أوروبا، معاهدة رقم (185).