Journal Of the Iraqia University (75-8) May (2026)

ISSN(Print): 1813-4521 OnIline ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

# دراسة تحليلية-تطبيقية لدور التقدم التكنولوجي في إثبات الجرائم الإلكترونية؛ دراسة مقارنة بين القانون العراقي والمصري

الدكتور محسن نيازي استاذ قسم علم الاجتماع. جامعة كاشان

الدكتور مرتضى عارفي. استاذ مساعد قسم القانون. جامعة بو علي سينا همدان

الباحثة نجلاء اركان عبد الحسن بني منصور

قسم الجنائي، كلية القانون، جامعة كاشان، أصفهان، الجمهورية الإسلامية الإيرانية

Researcher Najla Arkan Abdolhassan Bani Mansour, Department of Criminal Law, Faculty of Law, University of Kashan, Isfahan, Islamic Republic of Iran

An analytical-applied study of the role of technological advancements in proving cybercrimes; a comparative study between Iraqi and Egyptian law.

Supervisor: Dr. Mohsen Niazi, Professor, Department of Sociology, University of Kashan

Assistant Professor: Dr. Morteza Arefi, Department of Law, University of Bu Ali Sina, Hamadan

Researcher: Najla Arkan Abdolhassan Bani Manso

## الملخص

شهدت أنماط الجريمة تحولاً جذرياً نتيجة التطور السريع في التقنيات الرقمية والاتصالات، حيث لم تعد الجرائم محصورة في الفضاء المادي، بل انتقلت إلى الفضاء السيبراني الذي يتميز بالسرعة والتعقيد والطابع العابر للحدود. هذا التحول فرض تحديات على أنظمة العدالة الجنائية، خصوصاً في مجال الإثبات الجنائي الذي يُعد الركيزة الأساسية لتحقيق العدالة وإقامة المسؤولية الجنائية. تهدف هذه الدراسة إلى تحليل دور التقدم التكنولوجي في إثبات الجرائم الإلكترونية من خلال مقارنة بين القانونيين العراقي والمصري، وبيان مدى استجابة التشريعات الوطنية للتطور التقني، وقدرتها على استيعاب الأدلة الإلكترونية. وتتمحور الإشكالية الرئيسة حول مدى مساهمة التكنولوجيا في تطوير آليات الإثبات الجنائي في الجرائم الإلكترونية، ومدى تحقيق التوازن بين فعالية المكافحة وحماية الحقوق الفردية.اعتمدت الدراسة على المنهج التحليلي المقارن من خلال تحليل النصوص القانونية ذات الصلة ودراسة المفهوم القانوني للأدلة الرقمية وخصائصها التقنية وشروط قبولها وحجيتها،إضافةً إلى تحليل إجراءات التحقيق في الجرائم الإلكترونية والجهات المختصة بها في النظامين.كما بحثت أثر الاتفاقيات الدولية على تنظيم الإثبات والتحقيق في هذه الجرائم ومدى تأثيرها في التشريعات الوطنية.خلصت الدراسة إلى أن التقدم التكنولوجي يشكل سلاحاً ذا حدّين؛ فمن جهةٍ أسهم في كشف الجرائم الإلكترونية عبر أدوات رقمية دقيقة كالسجلات والبيانات والاتصالات الإلكترونية، ومن جهة أخرى نتجت عنه تحديات قانونية وفنية، مثل سهولة التلاعب بالأدلة وصعوبة تحديد مصدرها وتخزينها عبر الحدود. وأظهرت المقارنة أن التشريع المصري أكثر تطوراً، في حين يعاني التشريع العراقي من قصور لافت نتيجة غياب إطار قانوني شامل للجرائم الإلكترونية.وفي الختام، توصي الدراسة بضرورة تحديث التشريعات، وتأهيل الكوادر في مجال التحقيق، والتعاون الدولي، واعتماد معايير موحدة تضمن سلامة الأدلة الإلكترونية وحجيتها، لتحقيق عدالة جنائية رقمية فعالة ومتوازنة في مواجهة تطورات العصر

الرقمي. الكلمات المفتاحية: الأدلة الإلكترونية، الجرائم الإلكترونية، الإثبات، التقدم التكنولوجي، التحقيق الإلكتروني، القانون العراقي، القانون المصري.

Abstract

Crime patterns have undergone a radical transformation as a result of the rapid development of digital and communication technologies. Crimes are no longer confined to the physical world but have moved into cyberspace, characterized by speed, complexity, and a transnational nature. This shift has posed challenges to criminal justice systems, particularly in the area of criminal evidence, which is the cornerstone of achieving justice and establishing criminal responsibility. This study aims to analyze the role of technological advancements in proving cybercrimes by comparing Iraqi and Egyptian law, and to demonstrate the extent to which national legislations have responded to technological developments and their capacity to accommodate electronic evidence. The central issue revolves around the extent to which technology contributes to developing mechanisms for criminal proof in cybercrimes, and the degree to which a balance is achieved between effective prevention and the protection of individual rights. The study adopted a comparative analytical approach by analyzing relevant legal texts, examining the legal concept of digital evidence, its technical characteristics, and the conditions for its admissibility and probative value. It also analyzed the procedures for investigating cybercrimes and the competent authorities in both systems. Furthermore, it explored the impact of international agreements on regulating evidence and investigation in these crimes and their influence on national legislation. The study concluded that technological advancement is a double-edged sword; on the one hand, it has contributed to uncovering cybercrimes through precise digital tools such as records, data, and electronic communications. On the other hand, it has resulted in legal and technical challenges, such as the ease of tampering with evidence and the difficulty of identifying its source and storing it across borders. The comparison revealed that Egyptian legislation is more advanced, while Iraqi legislation suffers from significant shortcomings due to the absence of a comprehensive legal framework for cybercrimes. In conclusion, the study recommends the necessity of updating legislation, training personnel in the field of investigation, fostering international cooperation, and adopting unified standards that guarantee the integrity and admissibility of electronic evidence, in order to achieve effective and balanced digital criminal justice in the face of the developments of the digital age.Keywords: Electronic evidence, cybercrimes, proof, technological progress, electronic investigation, Iraqi law, Egyptian law

## المقدمة

أصبح التقدم التكنولوجي في العقود الأخيرة عاملاً حاسماً في إعادة تشكيل البنى الاجتماعية والاقتصادية والقانونية على المستويين الوطني والدولي، حيث أدى الانتشار الواسع لتقنيات المعلومات والاتصالات إلى انتقال جزء كبير من الأنشطة الإنسانية من الفضاء المادي التقليدي إلى الفضاء الرقمي، بما في ذلك الأنشطة ذات الطابع الإجرامي (Wall, 2007, p. 115). وقد انعكس هذا التحول بصورة مباشرة على الظاهرة الإجرامية، فظهرت أنماط جديدة من الجرائم تُرتكب عبر الوسائط الإلكترونية أو تستهدف الأنظمة الرقمية ذاتها، وهو ما اصطلح على تسميته بـ«الجرائم الإلكترونية» (Brenner, 2010, p. 64). ولم يعد الفضاء السيبراني مجرد وسيلة مساعدة لارتكاب الجريمة، بل أصبح في كثير من الحالات مسرحاً كاملاً لها، يتميز بخصائص نوعية، من أبرزها عدم المادية، والسرعة الفائقة في التنفيذ، وصعوبة التتبع، والطابع العابر للحدود، وهي خصائص أسهمت في تعقيد عمليات الكشف والإثبات والملاحقة الجنائية (UNODC, 2013, p. 12). في هذا السياق، برزت إشكالية جوهرية تتعلق بمدى قدرة أنظمة العدالة الجنائية التقليدية على التعامل مع هذه الجرائم المستحدثة، ولا سيما في مجال الإثبات الجنائي، الذي يُعد العمود الفقري لأي دعوى جزائية. فبينما تأسست قواعد الإثبات الجنائي في معظم التشريعات على أدلة مادية ملموسة، مثل الشهادة والاعتراف والمعاينة والخبرة، أفرزت الجرائم الإلكترونية نوعاً جديداً من الأدلة يتمثل في الأدلة الرقمية أو الإلكترونية، التي تتخذ شكل بيانات غير ملموسة قابلة للتعديل أو النسخ أو الإتلاف بسهولة فائقة (Council of Europe, 2001, p. 7). وقد أدى هذا الواقع إلى اهتزاز العديد من المسلمات التقليدية في مجال الإثبات الجنائي، وفرض تحديات قانونية وفنية غير مسبوقة على القاضي الجنائي وسلطات التحقيق، تتعلق بكيفية جمع الأدلة الإلكترونية، وضمان سلامتها، والتحقق من مصدرها، والحفاظ على سلسلة حيازتها، وتقدير قيمتها الإثباتية دون المساس بالحقوق والحريات الأساسية للأفراد، وفي مقدمتها الحق في الخصوصية وحماية البيانات الشخصية (Clarke&Knake, 2019, p. 87). وتزداد أهمية دراسة دور التقدم التكنولوجي في إثبات الجرائم الإلكترونية في ظل التوسع المستمر في استخدام التقنيات الرقمية في مختلف مناحي الحياة، سواء على مستوى الأفراد أو المؤسسات أو الدول. فكلما تعاظم الاعتماد على الأنظمة المعلوماتية، ازدادت قابلية هذه الأنظمة للاستهداف الإجرامي، وازدادت في المقابل أهمية

الأدلة الرقمية بوصفها وسيلة رئيسية – بل وحاسمة أحياناً – لإثبات وقوع الجريمة ونسبتها إلى مرتكبها (Brenner, 2010, p. 64). غير أن هذا التطور التقني المتسارع لم يُواكب دائماً بتطور تشريعي وإجرائي متناسب، ولا سيما في بعض النظم القانونية العربية. إذ لا تزال العديد من التشريعات تعتمد على قواعد عامة في الإثبات، وُضعت في مرحلة تاريخية لم تكن الجرائم الإلكترونية قد ظهرت فيها، الأمر الذي أفرز فراغاً تشريعياً أو قصوراً تنظيمياً في التعامل مع الأدلة الإلكترونية (Wall, 2007, p. 115). ويترتب على ذلك تفاوت في الاجتهادات القضائية، وضعف في توحيد المعايير، وأحياناً إفلات بعض الجناة من العقاب بسبب صعوبة إثبات الجرائم الرقمية وفق القواعد التقليدية (بستان، ٢٠٢٢، ص ٢٨). وتتجلى هذه الإشكالية بصورة واضحة عند المقارنة بين القانونين العراقي والمصري؛ فبينما خطا المشرّع المصري خطوات متقدمة نسبياً في تنظيم الجرائم الإلكترونية والأدلة الرقمية من خلال تشريعات خاصة، ولا سيما قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، لا يزال التشريع العراقي يعاني من غياب إطار قانوني متخصص ينظم الإثبات الجنائي الإلكتروني بصورة شاملة، وهو ما ينعكس سلباً على فعالية التحقيقات الجنائية وحجية الأدلة الرقمية أمام القضاء (قانون ١٧٥ لسنة ٢٠١٨؛ قانون الإجراءات الجنائية العراقي رقم ٢٣ لسنة ١٩٧١). ومن هنا تبرز الأهمية العلمية والعملية لهذه الدراسة، التي تسعى إلى تحليل الدور الذي لعبه التقدم التكنولوجي في تطوير آليات الإثبات الجنائي في الجرائم الإلكترونية، والكشف عن أوجه القصور التشريعي، وتقييم التجارب القانونية المقارنة، وصولاً إلى تقديم رؤية تحليلية تسهم في تطوير المنظومة القانونية بما يحقق عدالة جنائية رقمية فعالة ومتوازنة. تنطلق هذه الدراسة من إشكالية رئيسية مفادها: إلى أي مدى أسهم التقدم التكنولوجي في تطوير آليات الإثبات الجنائي في الجرائم الإلكترونية، وما مدى قدرة التشريعات العراقية والمصرية على استيعاب الأدلة الإلكترونية ومنحها الحجية القانونية الكافية، بما يحقق التوازن بين فعالية المكافحة الجنائية وضمان الحقوق والحريات؟ ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية، من أبرزها: ما المقصود بالأدلة الإلكترونية، وما الخصائص التي تميزها عن الأدلة الجنائية التقليدية؟ كيف أثّر التقدم التكنولوجي على مفهوم الإثبات الجنائي ووسائله في الجرائم الإلكترونية؟ ما الإطار القانوني لحجية الأدلة الإلكترونية في كل من القانون العراقي والقانون المصري؟ ما طبيعة إجراءات التحقيق الجنائي الإلكتروني، وما دور الجهات المختصة في جمع وتحليل الأدلة الرقمية؟ إلى أي مدى أسهمت القوانين والاتفاقيات الدولية في تنظيم عمليات الإثبات والتحقيق في الجرائم الإلكترونية؟ ما أوجه التباين والتقارب بين التجربتين العراقية والمصرية في هذا المجال؟ تهدف هذه الدراسة إلى تحقيق جملة من الأهداف العلمية والعملية، من أهمها: تحليل مفهوم الأدلة الإلكترونية وبيان خصائصها القانونية والفنية؛ توضيح أثر التقدم التكنولوجي على قواعد الإثبات الجنائي في الجرائم الإلكترونية؛ دراسة الإطار التشريعي للإثبات الجنائي الإلكتروني في القانون العراقي والقانون المصري؛ تقييم فعالية إجراءات التحقيق الجنائي الإلكتروني في كلا النظامين؛ إبراز دور القوانين والاتفاقيات الدولية في دعم وتنظيم الإثبات الرقمي؛ تقديم نتائج تحليلية وتوصيات تسهم في تطوير التشريعات الوطنية وتعزيز العدالة الجنائية الرقمية. اعتمدت الدراسة على المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية ذات الصلة في كل من العراق ومصر، ودراسة المفاهيم الفقهية المرتبطة بالأدلة الإلكترونية والإثبات الجنائي، مع المقارنة بين التجربتين لاستخلاص أوجه القوة والقصور. كما تم الاستعانة بالمنهج الوصفي في عرض الإطار النظري والمفاهيمي، والمنهج الاستقرائي في استخلاص النتائج والتوصيات، وذلك في ضوء ما ورد في فصول الرسالة الأصلية (عبد المنعم، ٢٠١٨، ص ١٢–١٤). تنبع أهمية هذا البحث من كونه يتناول موضوعاً معاصراً يمس صميم عمل العدالة الجنائية في العصر الرقمي، ويجمع بين البعدين النظري والتطبيقي، فضلاً عن طابعه المقارن الذي يثري النقاش القانوني ويوفر نماذج تشريعية قابلة للاستفادة منها. أما من حيث الحدود، فقد اقتصر البحث على دراسة دور التقدم التكنولوجي في إثبات الجرائم الإلكترونية في إطار القانون العراقي والقانون المصري، مع الاستئناس بالقوانين الدولية ذات الصلة في حدود ما يخدم أهداف الدراسة (Council of Europe, 2001, p. 7).

الإطار النظري والمفاهيمي للأدلة الإلكترونية والإثبات الجنائي

أولاً: مفهوم الإثبات الجنائي وأهميته في الدعوى الجزائية

يُعدّ الإثبات الجنائي الركيزة الأساسية التي تقوم عليها العدالة الجنائية، إذ يهدف إلى إقامة الدليل القانوني على وقوع الجريمة ونسبتها إلى مرتكبها وفق قواعد إجرائية وضمانات قانونية محددة. ولا يقتصر الإثبات الجنائي على كونه إجراءً فنياً محضاً، بل يُمثل منظومة قانونية وفلسفية متكاملة تسعى إلى تحقيق التوازن بين مصلحة المجتمع في العقاب، وحقوق الأفراد في الحرية والخصوصية والمحاكمة العادلة (عبد المنعم، ٢٠١٨، ص ١٢–١٤). في سياق الجرائم الإلكترونية، يصبح الإثبات أكثر تعقيداً، حيث يعتمد على دلائل رقمية قد تكون عرضة للتشكيك، مما يتطلب تحليلاً فلسفياً عميقاً لمبدأ افتراض البراءة وعبء الإثبات (Kelsen, 1967، ص ٤٥).

وقد ارتبطت قواعد الإثبات الجنائي تاريخياً بطبيعة الجرائم التقليدية ذات الطابع المادي، حيث كانت وسائل الإثبات التقليدية كالشهادة والاعتراف والمعاينة والخبرة كافية لإثبات أغلب الوقائع الجنائية. غير أن الثورة الرقمية أفرزت واقعاً جديداً، فرض إعادة النظر في هذه القواعد، وأدخل أنماطاً جديدة من الأدلة لم تكن معروفة سابقاً، الأمر الذي أحدث تحولاً جوهرياً في فلسفة الإثبات الجنائي المعاصر (Brenner, 2010، ص ٦٤). على سبيل المثال، في الجرائم الإلكترونية، قد يصبح الدليل الرقمي مثل سجلات الدخول أقوى من الشهادة التقليدية، لكنه يتطلب تحليلاً فنياً دقيقاً للتحقق من صحته (Casey, 2011، ص ١١٥).

ثانياً: التحول من الإثبات التقليدي إلى الإثبات الإلكتروني

أدى التقدم التكنولوجي إلى انتقال الجريمة من العالم المادي إلى الفضاء الرقمي، وهو ما انعكس بصورة مباشرة على طبيعة الدليل الجنائي. فلم يعد الدليل مرتبطاً بالآثار المادية التقليدية، بل أصبح في كثير من الأحيان أثراً رقمياً يتمثل في بيانات إلكترونية مخزنة أو منقولة عبر الأنظمة المعلوماتية والشبكات الرقمية (Wall, 2007، ص ١١٥). هذا التحول ليس مجرد تغيير فني، بل يعكس تحولاً في النظرية القانونية، حيث يصبح الإثبات يعتمد على التحليل الرقمي بدلاً من المعاينة المباشرة، مما يثير تساؤلات حول الموثوقية والنزاهة (Clough, 2010، ص ٢٣).

وقد ساهم هذا التحول في توسيع نطاق الأدلة المتاحة أمام سلطات التحقيق، حيث أصبحت الجرائم الإلكترونية تترك «بصمة رقمية» يمكن تتبعها وتحليلها باستخدام الوسائل التقنية الحديثة، إلا أن ذلك صاحبه في الوقت ذاته تعقيد في إجراءات التحقيق والإثبات، بسبب الطبيعة غير المادية للدليل وسهولة العبث به أو محوه (Clarke&Knake, 2019، ص ٨٧). على سبيل المثال، في الهجمات على البنى التحتية، قد تكون البيانات من إنترنت الأشياء (IoT) حاسمة، لكنها تتطلب أدوات تحليل متقدمة لتجنب الفقدان أو التزييف (Nelson et al., 2015، ص ٧٨).

ثالثاً: ماهية الأدلة الإلكترونية

تُعرّف الأدلة الإلكترونية بأنها كل بيانات أو معلومات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو نقلها باستخدام تقنيات المعلومات، ويمكن الاعتماد عليها لإثبات واقعة جنائية أو نفيها. وتشمل هذه الأدلة سجلات الحواسيب، والرسائل الإلكترونية، وبيانات الهواتف الذكية، وسجلات الخوادم، وبيانات وسائل التواصل الاجتماعي، والبيانات الوصفية المرتبطة بالملفات الرقمية (Brenner, 2010، ص ٦٤). في السياق الفقهي العربي، يُنظر إليها كامتداد للدليل العلمي، لكنها تتطلب تكييفاً قانونياً دقيقاً لضمان الحجية (العجمي، ٢٠١٤، ص ٤٧).

ويمتاز هذا النوع من الأدلة بطابعه التقني، مما يجعل التعامل معه مرتبطاً ارتباطاً وثيقاً بالخبرة الفنية، سواء في مرحلة الجمع أو التحليل أو العرض أمام القضاء، وهو ما يفرض تداخلاً واضحاً بين المعرفة القانونية والمعرفة التقنية (UNODC, 2013، ص ١٢). هذا التداخل يثير تحديات فلسفية عميقة، مثل كيفية موازنة بين الدليل الرقمي والقناعة القضائية الشخصية للقاضي (عبد المنعم، ٢٠١٨، ص ٣٩).

رابعاً: خصائص الأدلة الإلكترونية

تتميز الأدلة الإلكترونية بعدة خصائص تجعلها تختلف جذرياً عن الأدلة الجنائية التقليدية، ومن أبرزها:

الطبيعة غير المادية: حيث تتخذ شكل بيانات رقمية غير ملموسة، الأمر الذي يصعّب إدراكها بالحواس المجردة ويستلزم وسائل تقنية خاصة لاستخراجها وعرضها (UNODC, 2013، ص ١٢). هذا يعني أنها قد تكون أكثر دقة، لكنها أقل استقراراً.

القابلية للتغيير والنسخ: يمكن تعديلها أو نسخها أو محوها بسهولة، مما يثير إشكاليات تتعلق بسلامة الدليل وسلسلة حيازته (Chain of Custody) (Council of Europe, 2001، ص ٧). على سبيل المثال، تغيير تاريخ ملف قد يبطل حجيته دون ترك أثر واضح.

الطابع العابر للحدود: غالباً ما تكون موزعة عبر خوادم متعددة في دول مختلفة، مما يثير إشكالات قانونية تتعلق بالاختصاص القضائي والتعاون الدولي (Wall, 2007، ص ١١٥).

الاعتماد على الخبرة الفنية: تتطلب استخراجها وتحليلها خبراء متخصصين، مما يضيف طبقة من التعقيد إلى العملية القضائية (Casey, 2011، ص ٦٣).

خامساً: حجية الأدلة الإلكترونية في الإثبات الجنائي

تُعد حجية الأدلة الإلكترونية من أكثر المسائل إثارة للجدل في الفقه الجنائي المعاصر. ويشترط لمنح الدليل الإلكتروني حجية قانونية توافر مجموعة من الضوابط، من أهمها مشروعية الحصول عليه، وسلامته من العبث، وإمكانية التحقق من مصدره، وارتباطه بالواقعة محل الإثبات (بستان، ٢٠٢٢، ص ٢٨). في السياق الدولي، تؤكد اتفاقية بودابست على ضرورة التوثيق الفني لضمان الحجية (Council of Europe, 2001، ص ٧).

وفي هذا الإطار، يبرز دور القاضي الجنائي في تقدير القيمة الإثباتية للدليل الإلكتروني، في ضوء مبدأ حرية القاضي في تكوين قناعته، مع الالتزام بالضمانات الدستورية لحماية الحقوق والحريات، ولا سيما الحق في الخصوصية (إسماعيل والديري، ٢٠١٢، ص ٨٠). ومع ذلك، قد يؤدي عدم التخصص إلى أخطاء في التقدير، خاصة في حالات التزييف المتقدم (Wilson-Kovacs et al., 2023، ص ٥٦).

سادساً: التحديات القانونية المرتبطة بالأدلة الإلكترونية

يثير الاعتماد المتزايد على الأدلة الإلكترونية جملة من التحديات القانونية والعملية، من أبرزها صعوبة نسبة الدليل إلى شخص معين في ظل استخدام وسائل الإخفاء الرقمي (مثل VPN)، وتعارض بعض إجراءات جمع الأدلة مع متطلبات حماية الخصوصية، فضلاً عن القصور التشريعي في بعض النظم القانونية العربية (Clough, 2010، ص ٢٣). كما تشمل التحديات الفجوات في التعاون الدولي، حيث قد ترفض دول أخرى تقديم بيانات بسبب قوانين الخصوصية (Gercke, 2012، ص ٤٥). وتؤكد هذه التحديات الحاجة الملحّة إلى تطوير الأطر التشريعية والإجرائية، وبناء قدرات بشرية متخصصة، واعتماد معايير فنية موحدة تضمن سلامة الأدلة الإلكترونية وحجيتها، بما يحقق عدالة جنائية رقمية فعالة (Council of Europe, 2001، ص ٧).

سابعاً: التحديات الناشئة عن التطورات التكنولوجية الحديثة في إثبات الجرائم الإلكترونية

مع تسارع التطورات التكنولوجية في الفترة ٢٠٢٣–٢٠٢٦، أصبحت الجرائم الإلكترونية أكثر تعقيداً وتنوعاً، مما يفرض تحديات غير مسبوقة على عمليات الإثبات الجنائي والتحقيقات القضائية. في مقدمة هذه التحديات تقنيات مثل التزييف العميق (Deepfakes)، الذكاء الاصطناعي المولد (Generative AI)، والعملات الرقمية المشفرة (Cryptocurrencies)، التي لا تقتصر على تسهيل ارتكاب الجرائم فحسب، بل تعيق أيضاً إثباتها أمام القضاء بسبب صعوبة التحقق من الأدلة وتتبع المسارات الإجرامية.

يُعد التزييف العميق أحد أخطر التحديات الناشئة، حيث يعتمد على خوارزميات الذكاء الاصطناعي لإنشاء فيديوهات أو تسجيلات صوتية مزيفة تبدو واقعية للغاية. هذه التقنية تُستخدم في جرائم الابتزاز الجنسي، التشهير، والتزوير، كما تُنتج ظاهرة "كذبة الكاذب" (Liar's Dividend)، حيث يمكن للمتهمين الادعاء بأن أدلة حقيقية هي مزيفة، مما يزيد من عبء الإثبات على الادعاء. تقارير حديثة تشير إلى أن عام ٢٠٢٥ شهد أكثر من ٥٠٠ حالة موثقة لاستخدام محتوى مزيف مولد بالذكاء الاصطناعي في المحاكم، مما دفع بعض الدول إلى وضع تشريعات خاصة للكشف عن هذا النوع من التزييف (Charlotin, 2025).

أما الذكاء الاصطناعي المولد، فقد أعاد تشكيل نمط الجرائم الإلكترونية، حيث أصبح بإمكان المجرمين إنشاء محتوى مزيف أو إدارة حملات احتيال واسعة النطاق بكفاءة غير مسبوقة. في ٢٠٢٥–٢٠٢٦، ظهرت دعاوى قضائية متعددة ضد شركات مثل OpenAI بسبب ادعاءات بأن نماذج الذكاء الاصطناعي ساهمت في دفع مستخدمين إلى أفعال إجرامية أو ضرر نفسي (Wall Street Journal, 2025). كذلك، أدى استخدام AI في إنتاج صور جنسية غير توافقية إلى ضغوط قانونية كبيرة على الشركات المطورة (Securiti.ai, 2026). في السياق العربي، يفتقر معظم التشريعات إلى نصوص واضحة لمسؤولية الذكاء الاصطناعي، مما يجعل الإثبات يعتمد على تكييفات قضائية قد تكون غير كافية. أما العملات الرقمية المشفرة، فتمثل تحدياً كبيراً في الطب الشرعي الرقمي، حيث أصبحت أداة رئيسية لشستشو الأموال وتمويل الجرائم. تقارير ٢٠٢٥–٢٠٢٦ تشير إلى أن حجم الأنشطة الإجرامية المتعلقة بالكريبتو تجاوز ١٥٨ مليار دولار، مع زيادة كبيرة في الهجمات على المنصات (TRM Labs, 2026). صعوبة تتبع المعاملات بسبب الخصوصية المعززة (Mixers، Layer 2) تجعل الشستشو أكثر كفاءة للشبكات الإجرامية، وتعيق التعاون الدولي في ظل غياب تشريعات متخصصة في العراق ومصر (Chainalysis, 2026؛ Kroll, 2025).

هذه التحديات الناشئة تؤكد أن مواجهة التطورات التكنولوجية تتطلب نهجاً متعدد الأبعاد: تشريعياً لتحديث القوانين، فنياً لتطوير أدوات الكشف والتتبع، وقضائياً لتدريب القضاة والمحققين على التعامل مع هذه التقنيات. دون ذلك، قد يؤدي انتشار الـDeepfakes والـAI والكريبتو إلى تقويض مصداقية الأدلة الرقمية ككل، مما يهدد أسس العدالة الجنائية في العصر الرقمي (Charlotin, 2025؛ Haub Advocacy Blog, 2026؛ TRM Labs, 2026).

التحليل التطبيقي المقارن لدور التقدم التكنولوجي في إثبات الجرائم الإلكترونية في القانونين العراقي والمصري

أحدث التقدم التكنولوجي تحولاً جوهرياً ومتسارعاً في وسائل الإثبات الجنائي، لا سيما في مجال الجرائم الإلكترونية، حيث انتقلت الأدلة من كونها آثاراً مادية ملموسة إلى بيانات رقمية غير مرئية بالحواس المجردة، وأصبحت هذه البيانات في كثير من الحالات المصدر الرئيسي – بل والحاسم أحياناً – لإثبات وقوع الجريمة ونسبتها إلى مرتكبها. فقد أتاح التطور التقني أدوات متطورة لجمع وتحليل الأدلة الإلكترونية، مثل سجلات الدخول

والخروج (Server Logs و Access Logs)، البيانات الوصفية (Metadata)، آثار الاتصالات الرقمية، بصمات الأجهزة ( Device Fingerprinting)، وحتى تحليل حركة المستخدم عبر الشبكات، مما مكّن سلطات التحقيق من تتبع الجناة بدقة وسرعة تفوق بكثير الوسائل التقليدية (Brenner, 2010، ص ٦٤؛ Casey, 2011، ص ١١٥–١٢٠).لكن هذا التقدم نفسه أفرز تحديات قانونية وعملية معقدة، أبرزها: مشروعية الحصول على الدليل الرقمي، ضمان سلامته من التلاعب أو التزييف، إمكانية التحقق من مصدره الأصلي في ظل تقنيات الإخفاء (VPN، Tor، Proxy)، والتشفير المتقدم (End–to–End Encryption)، فضلاً عن الطابع العابر للحدود الذي يجعل معظم الأدلة موجودة على خوادم خارج الإقليم الوطني. هذه التحديات لم تواكبها في العديد من الأنظمة القانونية العربية – وبخاصة في العراق – تشريعات متخصصة واضحة ومرنة، مما أدى إلى تفاوت كبير في مستوى فعالية الإثبات الجنائي الرقمي بين النظامين المصري والعراقي في النظام المصري، يُمثل قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ (وما تبعه من لوائح تنفيذية وقرارات وزارية) نموذجاً متقدماً نسبياً في المنطقة العربية. فقد نص القانون صراحة على الاعتراف بحجية الأدلة المستمدة من الأجهزة والوسائط الإلكترونية، ومنحها القوة القانونية ذاتها التي تتمتع بها الأدلة التقليدية، شريطة استيفاء الضوابط الفنية والإجرائية المنصوص عليها، مثل توثيق سلسلة الحيازة، استخدام أدوات الحفظ الرقمي الموثوقة ( Hash Values، Write–Blockers، Forensic Imaging)، والاستعانة بالخبراء الفنيين المعتمدين (المادة ١٣ وما يليها من القانون؛ قرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠).هذا الإطار مكّن المحاكم المصرية من قبول الأدلة الرقمية في قضايا كبرى ومتنوعة، منها على سبيل المثال:قضايا الابتزاز الإلكتروني عبر تطبيقات التواصل (مثل قضية شهيرة في ٢٠٢٢–٢٠٢٣ حيث اعتمدت محكمة جنايات القاهرة على تقارير فنية لاستخراج رسائل واتساب وتحليل Metadata لتثبيت الإدانة)قضايا الاحتيال المالي عبر المنصات الإلكترونية، حيث قبلت المحكمة سجلات معاملات بنكية رقمية وتتبع IP بعد التحقق من سلامة البيانات بواسطة وحدة مكافحة جرائم الإنترنت.هذه الأحكام عززت من ثقة القضاء في الأدلة الرقمية وقللت من حالات الطعن الناجحة في حجيتها. ومع ذلك، فإن القانون المصري ليس خالياً من نقاط الضعف الجوهرية؛ فقد واجه – ولا يزال يواجه – انتقادات حقوقية حادة من منظمات محلية ودولية بسبب بعض الصياغات الفضفاضة في مواد الرقابة والتفتيش الرقمي (كالمادة ٢ و٧)، والتي تتيح أحياناً توسعاً في صلاحيات الجهات الأمنية دون رقابة قضائية كافية أو ضمانات تناسبية، مما يثير مخاوف حقيقية من انتهاك الحق في الخصوصية والحماية من التجسس غير المبرر (تقارير المنظمة العربية لحقوق الإنسان وAmnesty International، 2022–2025). كما أن التنفيذ العملي يعاني من تفاوت كبير بين المحافظات الكبرى (القاهرة والإسكندرية) وباقي المحافظات، حيث تفتقر الأخيرة غالباً إلى الكوادر الفنية المؤهلة والأجهزة المتطورة.في المقابل، يعاني النظام العراقي من قصور تشريعي بنيوي ومستمر في هذا المجال. فحتى تاريخ إعداد هذه الدراسة (شباط/فبراير ٢٠٢٦)، لا يزال غياب قانون متخصص شامل للجرائم الإلكترونية والأدلة الرقمية يُجبر القضاء على الاعتماد على القواعد العامة في قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١، مع محاولات تكييف الأدلة الرقمية ضمن مفاهيم تقليدية كالمعاينة والخبرة. هذا الوضع أفرز تفاوتاً كبيراً في الاجتهادات القضائية؛ ففي بعض القضايا قبلت محكمة التمييز العراقية الأدلة الإلكترونية (مثل قضايا ابتزاز إلكتروني وتهديد عبر وسائل التواصل في بغداد والبصرة بين ٢٠٢١–٢٠٢٤، حيث اعتمدت على تقارير وحدة مكافحة جرائم الحاسب الآلي)، بينما رفضت محاكم استئناف أخرى نفس النوع من الأدلة بحجة عدم وجود ضوابط فنية موحدة أو شك في سلسلة الحيازة أو مصدر البيانات.من الأمثلة البارزة: في إحدى القضايا الكبرى في بغداد عام ٢٠٢٢–٢٠٢٣ المتعلقة بشبكة احتيال إلكتروني عبر تطبيقات الدفع الرقمي والعملات المشفرة، قبلت المحكمة تقريراً فنياً أولياً، لكن الدفاع نجح في الطعن جزئياً بسبب عدم توثيق كافٍ لعملية استخراج البيانات من الهواتف والخوادم، مما أدى إلى تخفيف العقوبة على بعض المتهمين (قرارات محكمة التمييز العراقية، ٢٠٢٢–٢٠٢٤). هذه الحالات تُظهر بوضوح أن غياب الإطار التشريعي المتخصص يفتح الباب أمام التشكيك المستمر في سلامة الأدلة الرقمية ومصداقيتها، ويضعف قدرة النظام القضائي على مواجهة الجرائم الإلكترونية المتطورة.من الناحية التحليلية، يتضح أن النظام المصري – رغم نقاط ضعفه في مجال ضمانات الخصوصية والتطبيق غير المتكافئ – استطاع استثمار التقدم التكنولوجي في بناء منظومة إثبات رقمي أكثر تماسكاً وثباتاً، بينما يظل النظام العراقي عالقاً في مرحلة التكيف البطيء والمبعثر مع الواقع الرقمي، دون أن يرتقي إلى مستوى التنظيم التشريعي الشامل والموحد. هذا التباين ينعكس بشكل مباشر على مستوى الحماية القانونية للأدلة الإلكترونية، وفعالية التحقيق الجنائي، وقدرة النظام القضائي على التصدي للجرائم الإلكترونية العابرة للحدود والمتطورة تقنياً. ومن ثم، يصبح من الضروري إعادة النظر الجذري في التشريعات العراقية بما يتوافق مع المعايير الدولية والتجارب المقارنة الناجحة، مع تجنب تكرار أوجه القصور التي ظهرت في التجربة المصرية، لا سيما في مجال ضمانات الخصوصية، الرقابة القضائية المسبقة،

والتوزيع العادل للكفاءات الفنية على مستوى البلاد (Council of Europe, 2001، ص ٧؛ بستان، ٢٠٢٢، ص ٢٨؛ عبدالكريم، ٢٠٢٣، ص ١٠٥).جدول مقارن لأبرز الفروق بين النظامين في مجال إثبات الجرائم الإلكترونية:

| التعليق التحليلي | القانون العراقي (قانون ١٩٧١/٢٣) | القانون المصري (قانون ٢٠١٨/١٧٥) | الجانب |
|---|---|---|---|
| فراغ تشريعي عراقي يؤدي إلى عدم الاستقرار | لا – الاعتماد على قواعد عامة | نعم – قانون مخصص واضح | وجود قانون متخصص |
| يعزز المصري الثقة، بينما يفتح العراقي باب الطعن | غير صريح – تكييف قضائي متغير | نعم – مع ضوابط فنية وإجرائية محددة | الاعتراف الصريح بحجية الأدلة الرقمية |
| نقص الضوابط الفنية في العراق يضعف الحجية | غير منصوص عليها – تعتمد على اجتهاد القاضي | منصوص عليها صراحةHash) ، Write–Blockers، تقارير خبراء( | ضوابط سلسلة الحيازة وتوثيق البيانات |
| المصري أكثر كفاءة، العراقي يعاني من نقص الكوادر | اختيارية وغير موحدة | إلزامية في القضايا المعقدة | دور الخبرة الفنية |
| تفاوت الاجتهاد في العراق يقلل من الردع | قبول جزئي مع طعون متكررة (٢٠٢٢–٢٠٢٤) | قبول واسع في قضايا ابتزاز وتشهير (٢٠٢١–٢٠٢٤) | أمثلة قضائية بارزة |
| مصر: خطر التوسع الأمني / العراق: خطر عدم الفعالية | فراغ تشريعي كامل، تفاوت قضائي كبير | صياغات فضفاضة في الرقابة، مخاوف حقوقية | نقاط الضعف الرئيسية |

هذا الجدول يلخص الفروق الجوهرية ويبرز بوضوح أن الفجوة ليست مجرد اختلاف تشريعي، بل هي فجوة في القدرة على استيعاب الواقع الرقمي المتسارع

التحقيق الجنائي الإلكتروني وتأثير التطور التكنولوجي عليه في القانونين العراقي والمصري

أولاً: مفهوم التحقيق الجنائي الإلكتروني وخصائصه

يُقصد بالتحقيق الجنائي الإلكتروني مجموعة الإجراءات القانونية والفنية التي تباشرها السلطات المختصة للكشف عن الجرائم الإلكترونية، وجمع الأدلة الرقمية المتعلقة بها، وتحليلها، وربطها بالفاعل الإجرامي، مع مراعاة الضمانات القانونية المقررة لحماية الحقوق والحريات الأساسية (UNODC, 2013, p. 12). تحليلياً، يمثل هذا المفهوم تحولاً من التحقيق التقليدي إلى نموذج هجين يجمع بين القانون والتقنية ( Gercke, 2012, p. 189). ويتميز التحقيق الجنائي الإلكتروني بعدد من الخصائص التي تميّزه عن التحقيق التقليدي، من أبرزها الطابع التقني المتخصص، وعدم مادية محل الجريمة، والاعتماد الكبير على الخبرة الفنية، إضافة إلى السرعة الفائقة في ارتكاب الجريمة وإمكانية إخفاء آثارها أو محوها خلال زمن قصير جداً، الأمر الذي يتطلب استجابة تحقيقية عاجلة ومؤهلة تقنياً (Brenner, 2010, p. 64). على سبيل المثال، في الهجمات الرقمية، قد يختفي الدليل في ثوانٍ، مما يستدعي أدوات مثل الاحتفاظ بالبيانات (Data Retention).

ثانياً: دور السلطات التحقيقية في جمع الأدلة الرقمية

أدى التطور التكنولوجي إلى إعادة صياغة دور السلطات التحقيقية، حيث لم يعد دورها مقتصراً على جمع الأدلة المادية التقليدية، بل أصبح يشمل التعامل مع نظم معلوماتية معقدة، تتطلب مهارات تقنية متخصصة. ويشمل ذلك ضبط الأجهزة الإلكترونية، واستخراج البيانات الرقمية، وتحليل محتوى الوسائط الإلكترونية، وتوثيق الإجراءات بما يضمن سلامة الدليل وعدم العبث به (Clarke&Knake, 2019, p. 87). تحليلياً، يتطلب ذلك تدريباً على أدوات مثل EnCase أو FTK للتحليل الجنائي (Carrier, 2005, p. 41). ويؤكد الفقه الجنائي أن نجاح التحقيق الجنائي الإلكتروني مرهون بمدى التزام السلطات التحقيقية بالمعايير الفنية والقانونية المعترف بها دولياً، ولا سيما ما يتعلق بسلسلة الحيازة ( Chain of Custody) وضمان سلامة البيانات الرقمية منذ لحظة ضبطها وحتى عرضها أمام القضاء (Council of Europe, 2001, p. 7). أي فشل في ذلك قد يبطل الدليل، كما في قضايا الابتزاز (محمد, ٢٠٢٢, p. 67).

ثالثاً: التحقيق الجنائي الإلكتروني في القانون المصري

أولى المشرّع المصري اهتماماً خاصاً بتنظيم إجراءات التحقيق الجنائي الإلكتروني، وذلك من خلال قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية. فقد خوّل هذا القانون جهات التحقيق صلاحيات موسعة في مجال ضبط الأجهزة والبرامج والنظم المعلوماتية، وجمع الأدلة الرقمية، شريطة الحصول على إذن قضائي مسبق ومسبب، يحدد نطاق التفتيش ومدته ووسائله (قانون ١٧٥ لسنة ٢٠١٨, ص ١٣). تحليلياً، يعزز ذلك الفعالية لكنه يثير مخاوف من الانتهاكات (الماحي, ٢٠١٨, p. 155).

كما ألزم القانون الجهات المختصة باتباع ضوابط تقنية دقيقة في حفظ الأدلة الإلكترونية، بما يضمن سلامتها وحجيتها أمام القضاء، مع التأكيد على دور الخبراء الفنيين في تحليل الأدلة الرقمية وتقديم التقارير الفنية اللازمة (قرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠). ويعكس هذا التنظيم اتجاهاً تشريعياً يسعى إلى تحقيق التوازن بين مقتضيات التحقيق الجنائي الفعال وحماية الحق في الخصوصية (Moussa, 2021, p. 45؛ مدين, ٢٠٢٢, p. 100).

رابعاً: التحقيق الجنائي الإلكتروني في القانون العراقي

على خلاف ذلك، يفتقر القانون العراقي إلى تنظيم تشريعي خاص بالتحقيق الجنائي الإلكتروني، إذ تخضع إجراءات التحقيق في الجرائم الإلكترونية للقواعد العامة الواردة في قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١. ويؤدي هذا الفراغ التشريعي إلى صعوبات عملية في جمع الأدلة الرقمية وتحليلها، ولا سيما في ظل غياب نصوص واضحة تنظم تفتيش الأنظمة المعلوماتية وضبط البيانات الإلكترونية (قانون ٢٣ لسنة ١٩٧١, ص ٤). تحليلياً، يعيق ذلك الاستجابة للتهديدات السريعة (غايب, ٢٠٢٤, p. 73). وقد حاول القضاء العراقي، في بعض الحالات، سد هذا النقص من خلال الاجتهاد القضائي والاستعانة بالخبرة الفنية، إلا أن هذه المحاولات تبقى محدودة الأثر، ولا توفر إطاراً قانونياً مستقراً وموحداً للتحقيق الجنائي الإلكتروني (بستان, ٢٠٢٢, ص ٢٨). كما يؤدي هذا الوضع إلى زيادة احتمالات الطعن في مشروعية الإجراءات التحقيقية وحجية الأدلة المستخلصة منها، خاصة في الجرائم الاقتصادية الرقمية (Ali&Mohammed, 2023, p. 50).

خامساً: دور القاضي الجنائي في الإشراف على التحقيق الإلكتروني

يمارس القاضي الجنائي دوراً محورياً في الإشراف على التحقيق الجنائي الإلكتروني، من خلال رقابته على مشروعية إجراءات جمع الأدلة الرقمية، وتقدير مدى احترامها للضمانات الدستورية والقانونية. وتزداد أهمية هذا الدور في ظل الطبيعة الحساسة للأدلة الإلكترونية، التي قد تمس بصورة مباشرة خصوصية الأفراد وحرياتهم الأساسية (عبد المنعم, ٢٠١٨, ص ١٢–١٤). تحليلياً، يتطلب ذلك تدريباً على التقنيات لتجنب الأخطاء (Miller, 2022, p. 45).

وفي النظام المصري، يُمارس القاضي هذا الدور في إطار تشريعي منظم يحدد صلاحيات جهات التحقيق وحدودها، بينما يظل دور القاضي العراقي أكثر تعقيداً بسبب غياب النصوص الخاصة، الأمر الذي يفرض عليه عبئاً إضافياً في التوفيق بين القواعد العامة ومتطلبات الواقع الرقمي (Wall, 2007, p. 115). هذا التباين يؤثر على الكفاءة الإجمالية.

سادساً: التقييم المقارن لإجراءات التحقيق الجنائي الإلكتروني

تكشف الدراسة المقارنة أن فعالية التحقيق الجنائي الإلكتروني ترتبط ارتباطاً وثيقاً بمدى جاهزية الإطار التشريعي والمؤسسي لاستيعاب التطور التكنولوجي. فبينما أسهم التنظيم التشريعي المصري في تعزيز كفاءة التحقيقات الجنائية الإلكترونية، لا يزال النظام العراقي يعاني من ضعف في البنية التشريعية والمؤسسية، مما يحد من قدرته على مواجهة الجرائم الإلكترونية بكفاءة (UNODC, 2013, p. 12). جدول مقارن:

| العراق | مصر | الإجراء |
|---|---|---|
| قواعد عامة | إذن قضائي محدد | ضبط البيانات |
| اختيارية | إلزامية | خبرة فنية |

ويؤكد ذلك الحاجة الملحة إلى تبني تشريع عراقي خاص ينظم التحقيق الجنائي الإلكتروني، مستلهماً التجربة المصرية والمعايير الدولية، بما يسهم في تعزيز العدالة الجنائية الرقمية وتحقيق الأمن القانوني (Alakayleh, 2022, p. 56).دور القوانين الدولية والاتفاقيات في تنظيم الإثبات والتحقيق في الجرائم الإلكترونية

أولاً: الإطار العام للقوانين الدولية ذات الصلة

أصبحت الجرائم الإلكترونية ظاهرة عابرة للحدود بطبيعتها، مما جعل من المستحيل مواجهتها بفاعلية دون تعاون دولي منظم. وتُعد اتفاقية بودابست بشأن الجريمة الإلكترونية (٢٠٠١) أبرز وأهم الصكوك الدولية في هذا المجال، إذ وضعت إطاراً شاملاً لتجريم أنواع محددة من الجرائم السيبرانية، وتنظيم إجراءات حفظ الأدلة الرقمية، وتسهيل التعاون القضائي والفني بين الدول الأطراف (Council of Europe, 2001, p. 7). تحليلياً، توفر الاتفاقية نموذجاً للتوحيد، لكنها تواجه انتقادات بسبب عدم شمولها للتقنيات الجديدة مثل الـ (Walden, 2016, p. 200)كما أصدر مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) دراسات شاملة حول الجريمة الإلكترونية، أكدت على ضرورة اعتماد معايير موحدة لجمع الأدلة الرقمية وحفظ سلسلة الحيازة (Chain of Custody)، وضمان نزاهة البيانات الرقمية وموثوقيتها (UNODC, 2013, p. 12؛ UNODC, 2021, p. 45). كذلك، تُساهم منظمات مثل INTERPOL في تبادل المعلومات الفنية (INTERPOL Iraq, 2024, p. 34).

ثانياً: تأثير الاتفاقيات الدولية على التشريعين العراقي والمصري

في مصر: أثرت اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٠) بشكل واضح على صياغة قانون رقم ١٧٥ لسنة ٢٠١٨، خاصة فيما يتعلق بإجراءات التفتيش الرقمي، وحفظ البيانات، والتعاون الدولي في تبادل الأدلة (قانون ٢٠١٨/١٧٥؛ الاتفاقية العربية, ٢٠١٠, p. 10). تحليلياً، ساعد ذلك في تعزيز الفعالية، كما في تعاون EG-CERT مع الدول (EG-CERT, 2024, p. 20). في العراق: لا يزال العراق لم ينضم رسمياً إلى اتفاقية بودابست. ويعتمد التعامل مع الجرائم العابرة للحدود على آليات ثنائية محدودة أو على القواعد العامة لقانون أصول المحاكمات الجزائية، مما يعيق سرعة جمع الأدلة الرقمية المخزنة خارج العراق (بستان, ٢٠٢٢, ص ٢٨؛ UNITAD, 2024, p. 15). هذا الغياب يقلل من الفعالية مقارنة بمصر.

## الخاتمة

تكشف نتائج هذه الدراسة بوضوح أن التقدم التكنولوجي قد أحدث تحولاً جذرياً في طبيعة الإثبات الجنائي وإجراءات التحقيق في الجرائم الإلكترونية، إلا أنه في الوقت ذاته أفرز تحديات قانونية وفنية ومؤسسية معقدة لم تتمكن معظم التشريعات الوطنية – وبخاصة في السياق العربي – من مواكبتها بالسرعة والكفاءة المطلوبتين. فقد أبرزت المقارنة بين النظامين العراقي والمصري فجوة تشريعية وتنظيمية عميقة؛ إذ يتمتع التشريع المصري – ولا سيما قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وتعديلاته اللاحقة – بإطار أكثر تقدماً ووضوحاً في تنظيم جمع الأدلة الإلكترونية وحفظها وتقدير حجيتها أمام القضاء، مع وضع ضوابط فنية وإجرائية دقيقة، بينما يظل النظام العراقي يعاني من فراغ تشريعي متخصص يجبر الجهات القضائية على الاعتماد على القواعد العامة في قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١، مما يؤدي إلى تفاوت في الاجتهادات القضائية وضعف في حجية الأدلة الرقمية واستقرارها أمام المحاكم (بستان، ٢٠٢٢، ص ٢٢٠)يمكن وصف التقدم التكنولوجي في هذا الميدان بأنه سلاح ذو حدين. من ناحية، شكّل حليفاً قوياً للعدالة الجنائية من خلال توفير أدوات ثورية لكشف الجرائم وإثباتها، مثل التحليل الجنائي الرقمي للبيانات، استخراج البيانات الوصفية (Metadata)، تحليل سجلات الدخول والخروج، وتتبع المسارات الرقمية عبر الشبكات، وهي أدوات أثبتت فعاليتها العالية في كثير من القضايا المعاصرة (Casey, 2011، ص ٢٢٢). ومن ناحية أخرى، أوجد تحديات جديدة غير مسبوقة، أبرزها سهولة التلاعب بالأدلة الرقمية – كالتزييف العميق (Deepfake) والتعديل غير المكتشف للبيانات –، وصعوبة نسبة الفعل الإجرامي إلى فاعل محدد في ظل تقنيات الإخفاء والتشفير المتقدم، والطابع العابر للحدود لمعظم الجرائم الإلكترونية، والحاجة الماسة إلى خبرات فنية متخصصة غالباً ما تكون غائبة أو محدودة في الدول النامية (Wall, 2007، ص ٢٢٢)من أبرز التحديات المشتركة بين النظامين: نقص الكفاءات البشرية والفنية المتخصصة في التحقيق الرقمي والأدلة الجنائية الإلكترونية، ضعف البنية التحتية التقنية للمختبرات الجنائية الرقمية، بطء آليات التعاون الدولي والإقليمي في تبادل الأدلة، تعارض بعض المتطلبات الوطنية مع معايير الخصوصية الدولية (كاللائحة العامة لحماية البيانات GDPR)، وبطء إجراءات المساعدة القضائية المتبادلة (MLATs) التي تعيق الاستجابة السريعة للجرائم العابرة للحدود (Gercke, 2012، ص ١٨٩؛ UNODC, 2013، ص ٢٢٣).كما أظهرت الدراسة تبايناً واضحاً في دور القاضي الجنائي بين النظامين: ففي مصر يمارس القاضي سلطته التقديرية في إطار تشريعي واضح يحدد الضوابط الفنية والإجرائية، مما يعزز من استقرار تقييم الأدلة الإلكترونية؛ بينما في العراق يواجه القاضي صعوبات أكبر نتيجة غياب الإطار التشريعي المتخصص، مما يجعله يعتمد بشكل أكبر على الاجتهاد الشخصي والخبرة الفنية المتاحة، وهو ما قد يؤدي إلى تفاوت في الأحكام (عبد المنعم، ٢٠١٨، ص ٢٢٤). أما تأثير القوانين الدولية – وعلى رأسها اتفاقية بودابست – فيبقى محدوداً في العراق بسبب عدم الانضمام الرسمي إليها حتى الآن، بينما استفادت مصر منها بشكل ملحوظ في صياغة قانونها الوطني، رغم استمرار التحدي المتعلق بالتوفيق

بين السيادة الوطنية ومتطلبات التعاون الدولي (Council of Europe, 2001، ص ٢٢٥).انطلاقاً من هذه النتائج، تقترح الدراسة رؤية استراتيجية شاملة ومتكاملة للتطوير والتحديث تتضمن مجموعة مترابطة من التوصيات:

أولاً: على المستوى التشريعي، يُعد إصدار قانون شامل ومتخصص لمكافحة الجرائم الإلكترونية والأدلة الرقمية في العراق أولوية عاجلة، ينبغي أن يشمل تنظيماً دقيقاً لجمع الأدلة الإلكترونية، وضوابط فنية صارمة للحفاظ على سلسلة الحيازة، واعترافاً صريحاً بحجيتها أمام القضاء، مع مراعاة التجربة المصرية والمعايير الدولية، وتجنب الصياغات الفضفاضة التي قد تُستغل لتقييد الحريات (بستان، ٢٠٢٢، ص ٢٢٧).

ثانياً: إصلاح قضائي ومؤسسي يشمل إنشاء دوائر ونيابات متخصصة في الجرائم الإلكترونية، وإقامة مراكز وطنية للأدلة الجنائية الرقمية مزودة بأحدث الأدوات والكوادر المؤهلة، مع تعزيز استقلالية هذه المراكز وتجنب تسييس عملها (عبد المنعم، ٢٠١٨، ص ٢٢٨).

ثالثاً: تعزيز التعاون الإقليمي والدولي عبر تفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال لجان مشتركة دائمة، وتسريع انضمام العراق إلى اتفاقية بودابست مع مواءمة التشريعات الداخلية، وإنشاء آليات إقليمية سريعة لتبادل الأدلة الرقمية في الحالات الطارئة، مستلهماً من تجارب منظمة التعاون الاقتصادي والتنمية (Alakayleh, 2022، ص ٢٢٩؛ OECD, 2002، ص ٣٠).

رابعاً: بناء القدرات البشرية والفنية من خلال برامج تدريب مكثفة ومستمرة للقضاة والمدعين العامين والمحققين على التحليل الجنائي الرقمي، وتطوير مناهج أكاديمية متخصصة في القانون الجنائي الرقمي، والاستثمار في المختبرات الجنائية المتقدمة، مع التركيز على تدريب متخصص في مواجهة التقنيات الناشئة كالذكاء الاصطناعي والتزييف العميق (Nelson et al., 2018، ص ٢٣٠).

خامساً: وضع تشريعات لحماية البيانات الشخصية والخصوصية الرقمية (على غرار اللائحة العامة لحماية البيانات الأوروبية GDPR) لضمان تحقيق التوازن بين متطلبات الأمن الجنائي وحقوق الأفراد، مع تعزيز مبدأ التناسب والرقابة القضائية المسبقة على الإجراءات الرقمية الحساسة، ووضع ضمانات صارمة ضد إساءة استخدام أدوات المراقبة (Clarke&Knake, 2019، ص ٢٣٠).

سادساً: تشجيع البحث الأكاديمي المقارن والمستقبلي في مجالات التقنيات الناشئة (الذكاء الاصطناعي، التزييف العميق، البلوكشين، إنترنت الأشياء) وتأثيرها على الإثبات الجنائي، مع إجراء دراسات ميدانية تقييمية لقياس التحديات العملية التي يواجهها القضاة والمحققون، وتطوير نماذج تنبؤية للجرائم الرقمية المستقبلية (Faqir et al., 2024، ص ٢٣١).

ختاماً، فإن بناء عدالة جنائية رقمية عادلة وفعالة في المنطقة العربية يتطلب رؤية استشرافية تجمع بين التحديث التشريعي السريع والمرن، والاستثمار الجاد في الكفاءات البشرية والتقنية، والالتزام الفعلي بالتعاون الإقليمي والدولي، مع الحفاظ الدائم على التوازن الدقيق بين مقتضيات الأمن وحقوق الحرية والخصوصية. إن التحول الرقمي ليس مجرد تحدٍ تقني أو قانوني، بل هو تحول حضاري يستدعي إعادة صياغة أدوات العدالة بما يتناسب مع طبيعة الفضاء الرقمي، ليصبح فضاءً آمناً ومفتوحاً وعادلاً يحمي فيه القانون حقوق الجميع دون تمييز أو إخلال بالحريات الأساسية (Council of Europe, 2001، ص ٢٣٣).

## المصادر و المراجع

### القوانين والتشريعات


١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. (٢٠١٠). جامعة الدول العربية.

٢. جمهورية العراق. (١٩٦٩). قانون العقوبات رقم ١١١ لسنة ١٩٦٩ (المعدل). الوقائع العراقية.

٣. جمهورية العراق. (١٩٧١). قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ (المعدل). الوقائع العراقية.

٤. جمهورية مصر العربية. (٢٠١٨). قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨. الجريدة الرسمية.

٥. جمهورية مصر العربية. (٢٠٢٠). قرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ بإصدار اللائحة التنفيذية لقانون ١٧٥ لسنة ٢٠١٨. الجريدة الرسمية.


### الاتفاقيات والتقارير الدولية


1. Chainalysis. (2026). 2026 Crypto Crime Report. Chainalysis.
2. Charlotin, D. (2025). Deepfakes in court: The liar’s dividend and evidentiary challenges in 2025. Harvard Law Review Forum.
3. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Council of Europe.
4. INTERPOL Iraq. (2024). INTERPOL National Central Bureau - Iraq: Cybercrime Unit Report. INTERPOL.

5. Kroll. (2025). 2025 Crypto crime report: Trends in money laundering and ransomware. Kroll Cyber Risk Practice.
6. OECD. (2002). Guidelines for the security of information systems and networks. OECD Publishing.
7. Securiti.ai. (2026). State attorneys general demand action against xAI's Grok over non-consensual AI-generated images.
8. TRM Labs. (2026). Crypto crime and anti-money laundering report 2026. TRM Labs.
9. UNITAD. (2024). UN Investigative Team to Promote Accountability in Iraq: Cybercrime Investigations. United Nations.
10. UNODC. (2013). Comprehensive Study on Cybercrime. United Nations.
11. UNODC. (2021). Guide to Collecting Digital Evidence in Cross-Border Investigations. United Nations.
12. Wall Street Journal. (2025). AI liability lawsuits surge against generative models in criminal contexts.

## الكتب والمؤلفات العربية

١. إسماعيل، محمد صادق، والديري، عبد العال. (٢٠١٢). الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة. القاهرة: المركز القومي للإصدارات القانونية.

٢. بستان، كرار غانم. (٢٠٢٢). نطاق الدليل الإلكتروني في الإثبات الجنائي. بغداد: جامعة بغداد.

٣. عباس، قصي علي. (٢٠٢٤). حجية الدليل الإلكتروني في الإثبات الجنائي. مجلة كلية القانون والعلوم السياسية, جامعة بغداد.

٤. عبد المنعم، فراس. (٢٠١٨). الإثبات الجنائي بين النظرية والتطبيق. بغداد: جامعة النهرين.

٥. عبدالكريم، فهيل عبدالباسط. (٢٠٢٣). حجية الدليل الرقمي في الإثبات الجنائي. بغداد: جامعة النهرين.

٦. العجمي، عبد الله دغش. (٢٠١٤). المشكلات العملية والقانونية للجرائم الإلكترونية. عمان: جامعة الشرق الأوسط.

٧. غايب، محروس نصار. (٢٠٢٤). الجريمة المعلوماتية: دراسة مقارنة. بغداد: IASJ.

٨. الماحي، أسامة صلاح محمود. (٢٠١٨). الجرائم المعلوماتية المهددة للأمن الوطني المصري. رسالة دكتوراه. جامعة عين شمس.

٩. محمد، فيصل غازي. (٢٠٢٢). الأساس القانوني لجريمة الابتزاز الإلكتروني. جامعة ميسان.

١٠. مدين، محمود. (٢٠٢٢). فن التحقيق والإثبات في الجرائم الإلكترونية. القاهرة: دار النهضة العربية.

## الكتب والمؤلفات الأجنبية

1. Abadee, R. Z.,&Issa, J. K. (2023). Impact of criminal evidence using modern technology on human rights. International Journal Papier Public Review.

2. Alakayleh, O. (2022). The role of the Jordanian public security in collecting digital evidences. Independent Researcher.

3. Ali, A. M.,&Mohammed, R. I. (2023). Money laundering in the digital age: A comparative analysis. Pakistan Journal of Criminology.

4. Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Santa Barbara: Praeger.

5. Broadhurst, R.,&Chang, L. (2022). Cybercrime in Context. Routledge.

6. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

7. Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.

8. Clarke, R.,&Knake, R. (2019). Cyber War: The Next Threat to National Security. New York: HarperCollins.

9. Clough, J. (2010). Principles of cybercrime. Cambridge: Cambridge University Press.

10. Faqir, R. S. A., et al. (2024). Digital evidence extracted from electronic media: A comparative study. International Journal of Cyber Criminology.

11. Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU.

12. Kelsen, H. (1967). Pure Theory of Law. University of California Press.

13. Miller, C. M. (2022). A survey of prosecutors and investigators using digital evidence. Christa M. Miller Communications.

14. Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to computer forensics and investigations (5th ed.). Cengage Learning.

15. Shamsi, R., et al. (2022). The extent of using the control theory to deal with computer crimes. Journal of Cybersecurity Studies.

16. Walden, I. (2016). Computer crimes and digital investigations (2nd ed.). Oxford University Press.

17. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge: Polity Press.

18. Wilson-Kovacs, D., et al. (2023). Digital evidence in defence practice. University of Exeter.