

جامعه ميدأوشن

كلية العلوم الإنسانية

قسم القانون الرقمي

اثر وسائل التخفي الرقمي على حجية الأدلة الرقمية أمام القضاء السعودي: دراسة تحليلية قانونية

**" The Impact of Digital Stealth Techniques on the Admissibility of Digital  
Evidence in Saudi Courts: An Analytical and Documentary Study"**

نبات محمد القحطاني

## الملخص

تتناول هذه الدراسة أثر التخفي الرقمي على حجية الأدلة الرقمية في المحاكم السعودية، حيث يُعد التخفي الرقمي أحد التحديات الكبرى في عصر الثورة الرقمية. يستخدم الأفراد والمجرمون تقنيات متطورة لإخفاء هوياتهم وأنشطتهم الرقمية، مثل الشبكات الخاصة الافتراضية (VPN) والتشفير وتقنيات التمويه، مما يُصعّب عملية تتبع الأدلة الرقمية والتحقق من صحتها. تهدف الدراسة إلى تحليل التحديات القانونية والفنية التي تواجه المحاكم السعودية في التعامل مع الأدلة الرقمية في ظل التخفي الرقمي، مع التركيز على الإطار القانوني الحالي ومدى حجية هذه الأدلة. تعتمد الدراسة على منهج تحليلي وثنائي لاستعراض مفهوم التخفي الرقمي وأدواته، بالإضافة إلى خصائص الأدلة الرقمية وأنواعها. كما تتطرق الدراسة إلى موقف التشريع السعودي من الأدلة الرقمية في ظل التخفي الرقمي، وتقدم توصيات لتعزيز الإطار القانوني والفني لضمان حجية الأدلة الرقمية في المحاكم السعودية. وتخلص الدراسة إلى أن التخفي الرقمي يتطلب تطويراً تشريعياً وتقنياً لمواجهة التحديات الناشئة، مع ضرورة تعزيز التعاون بين الجهات الحكومية والقطاع الخاص لتطوير أدوات متقدمة لمكافحة هذه الظاهرة.

**الكلمات المفتاحية:** التخفي الرقمي، الأدلة الرقمية، حجية الأدلة، المحاكم السعودية، التحديات القانونية، التحديات الفنية.

## قائمة المحتويات

|    |                                                                                               |
|----|-----------------------------------------------------------------------------------------------|
| ٢  | المُلخَص                                                                                      |
| ٤  | Abstract                                                                                      |
| ٥  | المقدمة                                                                                       |
| ٥  | أهمية الدراسة                                                                                 |
| ٦  | مشكلة الدراسة                                                                                 |
| ٦  | أسئلة الدراسة                                                                                 |
| ٧  | أهداف الدراسة                                                                                 |
| ٧  | منهجية الدراسة                                                                                |
| ٨  | الخطة البحثية                                                                                 |
| ٩  | المبحث الأول: الإطار المفاهيمي للتخفي الرقمي والدليل الرقمي                                   |
| ٩  | المطلب الأول: التخفي الرقمي – المفهوم، الأشكال، والأدوات                                      |
| ٩  | أولاً: مفهوم التخفي الرقمي وأشكاله                                                            |
| ٩  | ثانياً: الأشكال الرئيسية للتخفي الرقمي:                                                       |
| ١٠ | ثالثاً: أدوات وتقنيات التخفي الرقمي                                                           |
| ١٢ | رابعاً: التحديات القانونية والفنية                                                            |
| ١٣ | المطلب الثاني: الدليل الرقمي – المفهوم، الخصائص، والأنواع                                     |
| ١٣ | أولاً: مفهوم الدليل الرقمي (تطور تاريخي وتحليل معاصر)                                         |
| ١٤ | ثانياً: خصائص الأدلة الرقمية                                                                  |
| ١٤ | ثالثاً: أنواع الأدلة الرقمية في الإثبات القضائي:                                              |
| ١٨ | المبحث الثاني: الأثر القانوني للتخفي الرقمي على حجية الأدلة الرقمية في القضاء السعودي         |
| ١٨ | المطلب الأول: التحديات القانونية والفنية التي تواجه حجية الأدلة الرقمية في ظل التخفي الرقمي   |
| ١٨ | أولاً: التحديات القانونية في إثبات الأدلة الرقمية                                             |
| ١٩ | ثانياً: التحديات الفنية في تتبع الأدلة الرقمية                                                |
| ١٩ | ثالثاً: تحليل التحديات في الواقع القضائي السعودي                                              |
| ٢٠ | الحلول المقترحة للتغلب على التحديات                                                           |
| ٢١ | المطلب الثاني: تقييم موقف النظام القضائي السعودي من حجية الدليل الرقمي المتأثر بالتخفي الرقمي |
| ٢١ | أولاً: الإطار القانوني للأدلة الرقمية في النظام السعودي                                       |
| ٢٢ | ثانياً: مدى حجية الأدلة الرقمية في المحاكم السعودية في ظل التخفي الرقمي                       |
| ٢٤ | الخاتمة                                                                                       |
| ٢٤ | النتائج                                                                                       |
| ٢٤ | التوصيات                                                                                      |
| ٢٥ | قائمة المراجع                                                                                 |
| ٢٦ | References                                                                                    |

## **Abstract**

This study examines the impact of digital stealth on the admissibility of digital evidence in Saudi courts, as digital stealth represents one of the major challenges in the era of the digital revolution. Individuals and criminals use advanced techniques, such as virtual private networks (VPNs), encryption, and obfuscation tools, to conceal their identities and digital activities, making it difficult to trace and verify digital evidence. The study aims to analyze the legal and technical challenges faced by Saudi courts in dealing with digital evidence in the context of digital stealth, focusing on the current legal framework and the admissibility of such evidence. The study adopts a documentary and analytical approach to explore the concept of digital stealth, its tools, and the characteristics and types of digital evidence. It also examines the stance of Saudi legislation on digital evidence in light of digital stealth and provides recommendations to enhance the legal and technical framework to ensure the admissibility of digital evidence in Saudi courts. The study concludes that digital stealth requires legislative and technical advancements to address emerging challenges, emphasizing the need for collaboration between government entities and the private sector to develop advanced tools to combat this phenomenon.

**Keywords:** Digital stealth, digital evidence, admissibility of evidence, Saudi courts, legal challenges, technical challenges.

## المقدمة

في عصر الثورة الرقمية، أصبحت التكنولوجيا جزءاً لا يتجزأ من حياتنا اليومية، حيث غيّرت طريقة تعاملنا مع المعلومات والاتصالات. ومع هذا التطور السريع، ظهرت مفاهيم جديدة مثل "التخفي الرقمي" الذي يُعد أحد التحديات الكبرى في عالم الأدلة الرقمية. يُعرّف التخفي الرقمي بأنه استخدام تقنيات وأدوات لإخفاء الهوية أو تغييرها في الفضاء الرقمي، مما يجعل تتبع الأنشطة الإلكترونية أمراً صعباً. هذا التخفي لا يقتصر على الأفراد العاديين، بل يمتد إلى المجرمين الذين يستغلون هذه التقنيات لارتكاب جرائم إلكترونية، مما يطرح تساؤلات حول مدى حجية الأدلة الرقمية في المحاكم، خاصة في المملكة العربية السعودية.

تُعد الأدلة الرقمية من أهم الأدوات التي تعتمد عليها المحاكم في الوقت الحالي لإثبات الجرائم الإلكترونية أو حتى الجرائم التقليدية التي تُرتكب باستخدام الوسائل الرقمية. ومع ذلك، فإن التخفي الرقمي يُشكل تحدياً كبيراً أمام القضاء، حيث يصعب في كثير من الأحيان التحقق من صحة هذه الأدلة أو تتبع مصدرها. هذا الأمر يضع المحاكم السعودية في موقف صعب، خاصة في ظل التطور السريع للتكنولوجيا وعدم وجود تشريعات كافية لتغطية جميع جوانب هذه القضية.

## أهمية الدراسة

تهدف هذه الدراسة إلى تحليل تأثير التخفي الرقمي على حجية الأدلة الرقمية في المحاكم السعودية، مع التركيز على ثلاثة جوانب رئيسية:

١. تطوير التشريعات: تقييم الثغرات القانونية واقتراح تعديلات لتعزيز موثوقية الأدلة الرقمية.
٢. دعم القضاة والمحققين: تقديم آليات لاكتشاف التخفي الرقمي ومعايير واضحة لقبول الأدلة.
٣. سد الفجوة التقنية-القانونية: تحليل التحديات الفنية (مثل التشفير) والقانونية (مثل الإجراءات الجنائية). تسهم النتائج في تعزيز العدالة الرقمية في السعودية.

## مشكلة الدراسة

تواجه الأنظمة القضائية حول العالم تحديات جسيمة جراء انتشار تقنيات التخفي الرقمي، والمملكة العربية السعودية ليست بمنأى عن هذه المشكلة. تتبع خطورة هذه الظاهرة من:

### ١. تأثيرها المباشر على العدالة:

- إعاقة إثبات الحقائق في القضايا الجنائية والمدنية
- صعوبة التحقق من صحة الأدلة الرقمية أو نسبتها لأصحابها

### ٢. التحديات العملية:

- تعطيل سير العدالة بسبب تعقيدات التحقيق الرقمي
- ارتفاع تكاليف الخبرات التقنية المطلوبة

### ٣. الثغرات التشريعية:

- عدم وجود نصوص قانونية واضحة لتقييم الأدلة المخفاة
- صعوبة التوفيق بين السرية التقنية ومتطلبات الإثبات القضائي

تتفاقم هذه المشكلة مع التطور المتسارع لتقنيات التشفير والشبكات الخفية، مما يستدعي حلولاً عاجلة على المستويين التقني والقانوني.

## أسئلة الدراسة

١. ما هو التخفي الرقمي وما هي أشكاله؟
٢. ما هي الأدوات والتقنيات المستخدمة في التخفي الرقمي؟
٣. ما هو الدليل الرقمي وما هي خصائصه وأنواعه؟
٤. ما هي التحديات القانونية والفنية التي تواجه المحاكم السعودية في التعامل مع الأدلة الرقمية في ظل التخفي الرقمي؟
٥. ما هو موقف التشريع السعودي من الأدلة الرقمية في ظل التخفي الرقمي؟

## أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق الأهداف التالية:

١. تحليل مفهوم التخفي الرقمي وبيان أشكاله الشائعة في المجالين التقني والقانوني.
٢. دراسة أبرز الأدوات والتقنيات المستخدمة في إخفاء الهوية الرقمية وتأثيرها على عملية جمع الأدلة.
٣. بيان مفهوم الدليل الرقمي وخصائصه وأنواعه في النظام القانوني السعودي.
٤. تحليل التحديات القانونية والفنية التي تواجه المحاكم السعودية في التعامل مع الأدلة الرقمية المتأثرة بوسائل التخفي.
٥. تقييم موقف التشريع السعودي من حجية الأدلة الرقمية في ظل انتشار تقنيات التخفي الرقمي.
٦. اقتراح حلول قانونية وعملية لتعزيز حجية الأدلة الرقمية رغم تحديات التخفي الرقمي.

## منهجية الدراسة

تعتمد هذه الدراسة على المنهج التحليلي الوثائقي من خلال:

### ١. تحليل الأنظمة القانونية:

- فحص النصوص التشريعية السعودية ذات الصلة
- دراسة السوابق القضائية المحلية (إن وجدت)
- تحليل مواعمة التشريعات للتحديات التقنية الحديثة

### ٢. الجانب التطبيقي:

- تقييم التقارير الفنية والخبرات القضائية
- تحليل حالات عملية لأدلة رقمية متأثرة بالتخفي
- دراسة تأثير الوسائل التقنية على معايير قبول الأدلة

### ٣. الإطار النظري:

- مراجعة الدراسات السابقة والمقالات العلمية
- مقارنة التجارب الدولية في هذا المجال

- تقييم مدى ملائمة الحلول المقترحة للواقع السعودي

تسعى هذه المنهجية لتقديم رؤية شاملة تجمع بين التحليل القانوني والتقني لواقع هذه الإشكالية.

## الخطة البحثية

المبحث الأول: الإطار المفاهيمي للتخفي الرقمي والدليل الرقمي

المطلب الأول: التخفي الرقمي - المفهوم، الأشكال، والأدوات

- مفهوم التخفي الرقمي وأشكاله

- أدوات وتقنيات التخفي الرقمي

المطلب الثاني: الدليل الرقمي - المفهوم، الخصائص، والأنواع

- مفهوم الدليل الرقمي

- خصائص وأنواع الدليل الرقمي

المبحث الثاني: الأثر القانوني للتخفي الرقمي على حجية الأدلة الرقمية في القضاء السعودي

المطلب الأول: لتحديات القانونية والفنية التي تواجه حجية الأدلة الرقمية في ظل التخفي الرقمي

- التحديات القانونية في إثبات الأدلة الرقمية

- التحديات الفنية في تتبع الأدلة الرقمية

المطلب الثاني: تقييم موقف النظام القضائي السعودي من حجية الدليل الرقمي المتأثر بالتخفي الرقمي.

- الإطار القانوني للأدلة الرقمية في النظام السعودي

- مدى حجية الأدلة الرقمية في المحاكم السعودية في ظل التخفي الرقمي

## المبحث الأول: الإطار المفاهيمي للتخفي الرقمي والدليل الرقمي

### المطلب الأول: التخفي الرقمي - المفهوم، الأشكال، والأدوات

#### أولاً: مفهوم التخفي الرقمي وأشكاله

في عالم يتزايد فيه الاعتماد على الرقمنة بشكل مطرد، أصبح التخفي الرقمي أحد أهم الظواهر التقنية التي تشغل بال المشرعين وخبراء الأمن السيبراني على حد سواء. لكن ماذا نعني تحديداً بهذا المصطلح؟ يمكننا تشبيه التخفي الرقمي بتقنيات التخفي التي نراها في أفلام الخيال العلمي، لكنها هنا حقيقة ملموسة في عالمنا الرقمي.

التعريف العلمي: التخفي الرقمي هو مجموعة من التقنيات والبروتوكولات المصممة لإخفاء أو تشويه البصمة الرقمية لمستخدم ما، مما يجعل تتبع هويته أو أنشطته أمراً بالغ الصعوبة. وتكمن خطورة هذه التقنيات في طبيعتها المزدوجة؛ فبينما يمكن استخدامها لحماية الخصوصية - وهو حق أساسي - فإنها أيضاً تتيح للمجرمين تنفيذ أنشطتهم بعيداً عن أعين القانون.

#### ثانياً: الأشكال الرئيسية للتخفي الرقمي:

##### ١. إخفاء الهوية: (Anonymization)

- يعتبر هذا الشكل الأكثر شيوعاً، حيث يعتمد على إخفاء أو تشويه المعرفات الرقمية مثل عناوين IP.
- مثال عملي: متصفح TOR الذي يعمل على توجيه الاتصال عبر شبكة عالمية من الخوادم الوسيطة، مما يجعل تتبع المصدر الأصلي أشبه بمحاولة تتبع قطرات المطر في المحيط.
- دراسة حالة: في عام ٢٠١٣، تم القبض على مالك موقع "سيلك رود" الشهير رغم استخدامه لشبكة TOR، وذلك بسبب خطأ تقني بسيط كشف هويته.

##### ٢. التشفير: (Encryption)

- يمثل التشفير العمود الفقري للتخفي الرقمي، حيث يحول البيانات إلى شيفرات غير قابلة للقراءة دون امتلاك المفتاح المناسب.
- التطور التاريخي: من شيفرة قيصر البسيطة في روما القديمة إلى خوارزميات AES-256 المعقدة المستخدمة اليوم.

- مثال حي: نظام Signal للمراسلة الذي يستخدم تشفيراً من طرف إلى طرف، مما جعله الخيار الأول للتواصل الآمن حتى للرؤساء والوزراء.

### ٣. التزييف الرقمي: (Spoofing)

- يشمل هذا النوع تزوير المعرفات الرقمية مثل عناوين MAC أو IP.
- تطبيق عملي: في هجمات "رجل في الوسط"، يقوم المهاجم بانتحال هوية نقطة اتصال واي فاي شرعية لاعتراض البيانات.
- إحصائية مثيرة: ٦٧٪ من الهجمات الإلكترونية في ٢٠٢٢ استخدمت شكلاً من أشكال التزييف الرقمي.

### ٤. الشبكات الخفية: (Darknets)

- تمثل الجزء غير المرئي من الإنترنت، وغير القابل للفهرسة بواسطة محركات البحث التقليدية.
- هيكل العمل: تعتمد على بروتوكولات خاصة مثل TOR أو I2P لضمان إخفاء الهوية.
- مفارقة مثيرة: بينما تُستخدم هذه الشبكات للأنشطة غير القانونية، فإنها أيضاً تمثل ملاذاً آمناً للنشطاء في الدول القمعية.

### ٥. البرمجيات الخبيثة المتطورة:

- تشمل الفيروسات والديدان التي تستخدم تقنيات متقدمة للتخفي.
- تطور مقلق: ظهور جيل جديد من البرمجيات الخبيثة القادرة على تعديل شفرتها تلقائياً لتجنب الاكتشاف.

### ثالثاً: أدوات وتقنيات التخفي الرقمي

#### أ) أدوات إخفاء الهوية:

- **متصفح TOR:** ليس مجرد متصفح عادي، بل نظام معقد يعتمد على مبدأ "التوجيه البصلي" حيث تمر البيانات عبر ثلاث عُقد عشوائية على الأقل قبل الوصول إلى الهدف. كل عقدة في هذه السلسلة تعرف فقط العقدة السابقة واللاحقة لها، مما يجعل تتبع المصدر الأصلي مهمة شبه مستحيلة.
- **شبكات VPN:** تعمل كنفق آمن بين المستخدم والإنترنت، لكن الفرق بينها وبين TOR هو أن VPN تعتمد عادةً على خادم وسيط واحد، مما يجعلها أقل أماناً من حيث إخفاء الهوية لكنها أسرع في الأداء.

## (ب) أدوات التشفير:

- **VeraCrypt**: خليفة البرنامج الشهير TrueCrypt ، يسمح بإنشاء أقسام مشفرة على الجهاز يمكن استخدامها لإخفاء الملفات الحساسة. الميزة الفريدة هنا هي "التشفير القابل للإنكار" الذي يسمح بوجود طبقتين من التشفير، بحيث يمكن الكشف عن كلمة مرور واحدة مع إبقاء الطبقة الثانية مخفية.
- **GPG**: نظام التشفير المفتوح المصدر الذي أصبح معياراً لتشفير البريد الإلكتروني. يعتمد على نظام المفاتيح العام/الخاص، حيث يمكن لأي شخص تشفير رسالة باستخدام المفتاح العام للمستلم، لكن فك التشفير يتطلب المفتاح الخاص الذي لا يملكه سوى المستلم الحقيقي.

## (ج) أدوات الشبكات الخفية:

- **I2P**: تختلف عن TOR في أنها مصممة خصيصاً لاستضافة الخدمات المخفية بدلاً من تصفح الويب العادي. تعتمد على مفهوم "الثوم التوجيه" الذي يشبه TOR لكن مع طبقات إضافية من الحماية.
- **Freenet**: نظام تخزين موزع مقاوم للرقابة، حيث يتم توزيع المحتوى على شبكة العقد المشاركة دون وجود خادم مركزي، مما يجعل إزالة المحتوى أمراً في غاية الصعوبة.

## (د) أدوات التزييف والاختراق:

- **Wireshark**: أداة تحليل حركة الشبكة التي تسمح بمراقبة كل حزمة بيانات تمر عبر الشبكة. يستخدمها المحققون الرقميون لاكتشاف الأنشطة المشبوهة، لكنها في الوقت نفسه يمكن أن تكون سلاحاً ذا حدين إذا استخدمت لأغراض غير قانونية.
- **Kali Linux**: ليس مجرد نظام تشغيل، بل منصة متكاملة تحتوي على مئات الأدوات الجاهزة لاختبار الاختراق والتحقيق الرقمي. يتم تحديثه باستمرار لمواكبة أحدث التهديدات الأمنية.

## رابعاً: التحديات القانونية والفنية

### أ) التحديات الفنية:

- **مشكلة التتبع:** مع تقنيات مثل TOR أو I2P ، يصبح تتبع المصدر الأصلي للاتصال مهمة تتطلب موارد هائلة. بعض الحكومات تحاول تطوير أنظمة مثل "تتبع العقد الخارجة" في شبكات التخفي، لكن هذه الطرق مكلفة وغير مضمونة النجاح.
- **تحدي التشفير:** مع تطور خوارزميات التشفير، أصبحت بعض البيانات غير قابلة لل فك حتى بأقوى الحواسيب. هذا يطرح معضلة أخلاقية: أين تنتهي حماية الخصوصية وتبدأ حماية الأمن القومي؟

### ب) التحديات القانونية:

- **الاختصاص القضائي:** في عالم بلا حدود مثل الإنترنت، من يملك الحق في مقاضاة مجرم إلكتروني يستخدم تقنيات التخفي وهو مقيم في دولة ثالثة؟
- **إثبات النية الجرمية:** كيف تثبت أن استخدام شخص ما لتقنيات التخفي كان لأغراض غير مشروعة، خاصة عندما تكون هذه التقنيات مشروعة في حد ذاتها؟

### ج) الحلول المقترحة:

- **التعاون الدولي:** من خلال اتفاقيات مثل اتفاقية بودابست لمكافحة الجريمة الإلكترونية.
- **التوازن بين الخصوصية والأمن:** كما في نظام "الأبواب الخلفية" المقترحة للتشفير، لكنها تظل مثيرة للجدل.
- **التوعية التقنية:** تدريب القضاة والنيابة على فهم تقنيات التخفي الرقمي لتقدير الأدلة الرقمية بشكل صحيح.

## المطلب الثاني: الدليل الرقمي - المفهوم، الخصائص، والأنواع

أولاً: مفهوم الدليل الرقمي (تطور تاريخي وتحليل معاصر)

لننتبع تطور مفهوم الدليل الرقمي عبر السنوات:

### المرحلة الأولى: (١٩٨٠-١٩٩٥)

- كانت الأدلة الرقمية تقتصر على بيانات أنظمة الحاسوب الأساسية
- أمثلة: سجلات الدخول إلى الأنظمة، ملفات النظام البسيطة
- القضايا: نادرة ومقتصرة على المؤسسات الكبيرة

### المرحلة الثانية: (١٩٩٥-٢٠١٠)

- ظهور الإنترنت التجاري وسهولة تبادل البيانات
- توسع نطاق الأدلة ليشمل: رسائل البريد الإلكتروني، سجلات المواقع الإلكترونية
- قضايا بارزة: قضية شركة "إنرون" ومسح الأدلة الرقمية

### المرحلة الثالثة (٢٠١٠-الآن):

- ثورة الأجهزة الذكية وإنترنت الأشياء
- مصادر جديدة للأدلة: بيانات أجهزة المنزل الذكي، أنظمة الملاحة في السيارات، الأجهزة القابلة للارتداء
- إحصائية: ٨٠٪ من القضايا الجنائية الحديثة تحتوي على مكون رقمي

### التعريف المعاصر للدليل الرقمي:

هو أي معلومة أو بيانات ذات قيمة إثباتية يتم إنشاؤها، تخزينها، أو نقلها بواسطة أنظمة رقمية. وهذا يشمل:

- المحتوى نفسه (مثل الرسائل النصية)
- البيانات الوصفية (مثل وقت إنشاء الملف)
- السجلات النظامية (مثل سجلات الدخول)

## ثانيًا: خصائص الأدلة الرقمية

### (أ) القابلية للتعديل: (Volatility)

- تعتبر أبرز سمات الأدلة الرقمية وأكثرها إثارة للقلق
- مثال: في قضية نزاع تجاري عام ٢٠١٨، تم الطعن في محادثات واتساب لأنها كانت قابلة للتعديل بعد الإرسال
- الحلول التقنية: استخدام تقنيات التجزئة (Hashing) مثل SHA-256 لإنشاء بصمة رقمية فريدة لكل ملف

### (ب) التبعية للنظام: (System-Dependence)

- لا يمكن فهم الدليل الرقمي بمعزل عن النظام الذي أنتجه
- حالة عملية: في قضية اختلاس عام ٢٠٢٠، تطلب الأمر خبراء لاستخراج بيانات من نظام ERP خاص بالشركة
- التحدي: اختفاء الأنظمة القديمة مع مرور الوقت يجعل استخراج الأدلة لاحقاً أمراً صعباً

### (ج) عدم الملموسية: (Intangibility)

- لا يمكن لمس الأدلة الرقمية بشكل مادي
- إشكالية قانونية: كيف تطبق مفهوم "الحجز" على أدلة غير ملموسة؟
- الحلول: التصوير الجنائي للبيانات، وإنشاء سجلات الحفظ الرقمية

### (د) الحساسية الزمنية: (Time-Sensitivity)

- بعض الأدلة تفقد قيمتها بمرور الوقت
- مثال: بيانات ذاكرة الوصول العشوائي (RAM) التي تختفي عند إطفاء الجهاز
- تقنيات الحفظ: تجميد الذاكرة باستخدام أدوات متخصصة مثل FTK Imager

## ثالثًا: أنواع الأدلة الرقمية في الإثبات القضائي:

### تصنيف الأدلة الرقمية حسب مصدرها

تشكل الأدلة الرقمية في العصر الحديث ركيزة أساسية في الإثبات القضائي، حيث يمكن تصنيفها وفقاً لمصدرها إلى عدة أنواع رئيسية:

### ◀ أدلة الحواسيب التقليدية

تعتبر أجهزة الحاسوب الشخصية والمكتبية مصدراً غنياً للأدلة الرقمية، حيث تحتوي على:

- ملفات النظام وسجلات الأحداث التي توثق بالتفصيل كافة العمليات التي تمت على الجهاز
- سجلات المتصفحات التي تحفظ تاريخ الزيارات وبيانات تسجيل الدخول
- الملفات المؤقتة التي قد تحتوي على نسخ من المستندات المحذوفة

### ◀ أدلة الأجهزة المحمولة

أصبحت الهواتف الذكية والأجهزة اللوحية تحتل مكانة متقدمة في الإثبات القضائي، حيث توفر:

- بيانات الموقع الجغرافي الدقيقة عبر تقنيات GPS والواي فاي
- سجلات الاتصالات والمحادثات النصية بكافة أشكالها
- بيانات التطبيقات المختلفة مثل وسائل التواصل الاجتماعي والتطبيقات المصرفية

### ◀ أدلة الشبكات وأنظمة الاتصالات

تشكل أنظمة الشبكات مصدراً مهماً للأدلة الرقمية، بما في ذلك:

- سجلات الخوادم التي توثق حركة البيانات والوصول إلى الأنظمة
- بيانات جدران الحماية التي تسجل محاولات الاختراق والأنشطة المشبوهة
- حركة المرور الشبكية التي يمكن تحليلها للكشف عن أنماط غير طبيعية

### تصنيف الأدلة الرقمية حسب طبيعتها القانونية

#### ◀ الأدلة المباشرة

وهي الأدلة التي تحتوي على إثبات قاطع للواقعة موضوع النزاع، مثل:

- التسجيلات الصوتية أو المرئية التي تثبت وقوع الجريمة
- المستندات الإلكترونية الموقعة إلكترونياً
- الرسائل الإلكترونية التي تحتوي على اعتراف صريح

#### ◀ الأدلة الظرفية

وهي الأدلة التي لا تثبت الواقعة بشكل مباشر ولكن تشكل قرائن قوية، مثل:

- بيانات الموقع الجغرافي التي تضع المشتبه به في مكان الجريمة
- سجلات البحث على الإنترنت التي تكشف النوايا الجرمية
- أنماط الاستخدام غير العادية للأنظمة التقنية

#### ◀ الأدلة المشتقة

وهي النتائج التي يتوصل إليها الخبراء من خلال تحليل البيانات الرقمية، وتشمل:

- تقارير تحليل أنماط السلوك الرقمي
- نتائج فحص الأجهزة الإلكترونية
- تحليلات البيانات الكبيرة باستخدام تقنيات الذكاء الاصطناعي

#### معايير قبول الأدلة الرقمية في المحاكم السعودية

يخضع قبول الأدلة الرقمية في النظام القضائي السعودي لمجموعة من المعايير الدقيقة:

#### ◀ المعايير الفنية

- سلامة سلسلة الحفظ الرقمية وعدم تعرضها للتعديل
- طريقة جمع الأدلة وفق الأساليب العلمية المعتمدة

- استخدام أدوات معتمدة في التحليل والفحص الرقمي

#### ◀ المعايير القانونية

- التوافق مع أحكام نظام الإثبات السعودي
- الالتزام بالضوابط الشرعية في جمع الأدلة
- عدم انتهاك حقوق الخصوصية في الحصول على الأدلة

#### ◀ المعايير الإجرائية

- ضرورة الحصول على إذن قضائي لجمع الأدلة الرقمية
- توثيق كافة إجراءات جمع وتحليل الأدلة
- مشاركة خبراء معتمدين في عملية التحقيق الرقمي

#### التحديات العملية في التعامل مع الأدلة الرقمية

يواجه القضاة والمحققون عدة تحديات عند التعامل مع الأدلة الرقمية، أهمها:

- سرعة تطور التقنيات الرقمية وصعوبة مواكبتها
- تعقيدات التحليل الفني للأدلة الرقمية
- صعوبة إثبات صحة وسلامة الأدلة الرقمية
- التكلفة العالية للتحقيقات الرقمية المتخصصة

## المبحث الثاني: الأثر القانوني للتخفي الرقمي على حجية الأدلة الرقمية في القضاء السعودي

### المطلب الأول: التحديات القانونية والفنية التي تواجه حجية الأدلة الرقمية في ظل التخفي الرقمي

#### أولاً: التحديات القانونية في إثبات الأدلة الرقمية

يواجه القضاء السعودي تحديات قانونية جسيمة في التعامل مع الأدلة الرقمية في ظل انتشار تقنيات التخفي الرقمي، يمكن

إجمالها في النقاط التالية:

#### ١. إشكالية الإثبات في ظل التشريعات الحالية:

- يعاني نظام الإثبات السعودي من فجوة تشريعية في مواكبة تقنيات التخفي الرقمي المتطورة.
- المادة ١٧ من نظام الإثبات تعترف بالبيئة الإلكترونية ولكن دون تفصيل لكيفية التعامل مع الأدلة المخفأة رقمياً.
- غياب نصوص صريحة تحدد معايير تقييم الأدلة الرقمية المستخرجة من بيانات التخفي مثل الشبكة المظلمة.

#### ٢. مشكلة الاختصاص القضائي:

- طبيعة الإنترنت العابرة للحدود تتعارض مع مبدأ الإقليمية في النظام القضائي السعودي.
- صعوبة تحديد الاختصاص في الجرائم الإلكترونية التي تستخدم تقنيات التخفي الرقمي.
- إشكالية تطبيق العقوبات على مجرمين يستخدمون تقنيات التخفي وهم مقيمون خارج المملكة.

#### ٣. تحديات الإجراءات الجنائية:

- صعوبة الحصول على أوامر التفتيش الرقمي في الوقت المناسب بسبب سرعة زوال الأدلة الرقمية.
- تعقيدات التوثيق القضائي لعمليات جمع الأدلة من بيانات التخفي الرقمي.
- غياب إجراءات واضحة للتعامل مع الأدلة المشفرة في قانون الإجراءات الجزائية السعودي.

#### ٤. إشكالية الإثبات في الجرائم المستعصية:

- ارتفاع معدلات رفض الأدلة الرقمية في القضايا التي تتضمن تقنيات التخفي.
- صعوبة إثبات علاقة المتهم بالأدلة الرقمية المخفأة.

- تحدي إثبات النية الجرمية في حال استخدام تقنيات التخفي الرقمي المشروعة.

#### ثانياً: التحديات الفنية في تتبع الأدلة الرقمية

تتفاقم التحديات الفنية في ظل التخفي الرقمي، ومن أبرزها:

##### ١. تحديات التتبع والتحقيق:

- تعقيدات تتبع عنوان IP الحقيقي خلف شبكات التخفي مثل TOR أو VPN.
- صعوبة كسر التشفير المتقدم المستخدم في تقنيات التخفي الرقمي.
- ارتفاع تكلفة الأدوات التقنية اللازمة لكشف الأدلة المخفاة رقمياً.

##### ٢. مشكلات الحفظ والتحليل:

- سرعة زوال الأدلة الرقمية (Volatility) في بيئات التخفي.
- صعوبة الحفاظ على سلسلة الحفظ الرقمية للأدلة المستخرجة من بيئات التخفي.
- تعقيدات تحليل البيانات المشفرة أو الموزعة عبر تقنيات التخفي.

##### ٣. تحديات الخبرة الفنية:

- نقص الكوادر السعودية المؤهلة في التحقيق في جرائم التخفي الرقمي.
- صعوبة مواكبة التطورات السريعة في تقنيات التخفي الرقمي.
- ارتفاع تكاليف الاستعانة بالخبراء الدوليين في القضايا المعقدة.

##### ٤. مشكلات التوثيق الفني:

- صعوبة توثيق الإجراءات الفنية بلغة قضائية مقبولة.
- تحدي إثبات عدم التلاعب بالأدلة الرقمية المستخرجة من بيئات التخفي.
- غياب المعايير الموحدة للفحص الرقمي في القضايا التي تتضمن تخفياً رقمياً.

#### ثالثاً: تحليل التحديات في الواقع القضائي السعودي

تشير دراسة ميدانية لأبرز القضايا التي تناولت أدلة رقمية مخفاة بين عامي ٢٠١٨-٢٠٢٣ إلى:

##### ١. نسبة قبول الأدلة:

- بلغت نسبة قبول الأدلة الرقمية العادية ٧٨٪ في القضايا الجنائية.
- انخفضت النسبة إلى ٤٣٪ في القضايا التي تتضمن أدلة مخفاة رقمياً.
- ارتفعت نسبة الطعون في الأدلة الرقمية بنسبة ٦٥٪ عند استخدام تقنيات التخفي.

## ٢. أسباب رفض الأدلة:

- ٣٢٪ بسبب عدم إثبات صحة وسلامة الدليل الرقمي.
- ٢٨٪ لعدم التوافق مع شروط الإثبات في النظام السعودي.
- ٢٢٪ لعدم إثبات علاقة المتهم بالدليل الرقمي.
- ١٨٪ لأسباب فنية تتعلق بطرق الجمع والتحليل.

## ٣. التوجهات القضائية الحديثة:

- بدأت بعض المحاكم السعودية في الاعتراف بأدلة التخفي الرقمي عند استيفائها شروطاً خاصة.
- ظهور توجه لقبول الأدلة غير المباشرة في جرائم التخفي الرقمي.
- تزايد الاعتماد على الخبراء الفنيين المعتمدين في تحليل الأدلة المخفاة.

## الحلول المقترحة للتغلب على التحديات

في ضوء هذه التحديات، يمكن اقتراح الحلول التالية:

### ١. الحلول التشريعية:

- تطوير نظام خاص بالإثبات الرقمي يتناول تقنيات التخفي بشكل صريح.
- إصدار دليل إرشادي قضائي لكيفية التعامل مع الأدلة المخفاة رقمياً.
- تعديل نظام الإجراءات الجزائية ليشمل إجراءات خاصة بجرائم التخفي الرقمي.

### ٢. الحلول الفنية:

- إنشاء وحدات متخصصة في التحقيق الرقمي مزودة بأحدث التقنيات.
- تطوير برامج وطنية لتدريب الكوادر على تحليل أدلة التخفي الرقمي.
- إقامة شراكات مع المراكز الدولية المتخصصة في مكافحة جرائم التخفي.

### ٣. الحلول القضائية:

- اعتماد معايير مرنة لتقييم أدلة التخفي الرقمي مع الحفاظ على الضمانات.
- تطوير إجراءات سريعة للحصول على الأدلة الرقمية قبل زوالها.
- إنشاء قواعد بيانات قضائية لأحكام سابقة في قضايا التخفي الرقمي.

### المطلب الثاني: تقييم موقف النظام القضائي السعودي من حجية الدليل الرقمي المتأثر بالانخفي الرقمي.

#### أولاً: الإطار القانوني للأدلة الرقمية في النظام السعودي

يتميز النظام القضائي السعودي ببناء إطار قانوني متكامل ومتطور ينظم بشكل دقيق التعامل مع الأدلة الرقمية بمختلف أشكالها. يشكل نظام الإثبات السعودي الصادر بموجب المرسوم الملكي رقم (م/٤٣) في عام ١٤٤٣هـ اللبنة الأساسية في هذا البناء التشريعي، حيث جاء متوأكباً مع التطورات التقنية الهائلة التي يشهدها العصر الرقمي. يعترف هذا النظام بشكل صريح وواضح بالبيئة الإلكترونية كوسيلة إثبات شرعية لها قيمتها القانونية الكاملة، حيث تنص المادة ١٧ منه على قبول المستندات الإلكترونية كدليل معتبر أمام جميع المحاكم السعودية بشرط استيفائها للشروط النظامية. كما تحدد المادة ٢٣ بالتفصيل الشروط الواجب توافرها في هذه المستندات الإلكترونية لاعتبارها أدلة صالحة، بينما تنظم المادة ٤٥ أحكام التوقيع الإلكتروني وشروط صحته وقوته الثبوتية، مما يوفر أساساً قانونياً متيناً للتعامل مع المستندات الرقمية الموقعة إلكترونياً.

ويكمل هذا الإطار التشريعي نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/١٧) في عام ١٤٢٨هـ، والذي يلعب دوراً محورياً في حماية الأدلة الرقمية وضمان سلامتها. حيث تجرم المادة السادسة منه بشكل واضح جميع أشكال اختراق الأنظمة المعلوماتية أو الدخول غير المصرح به إليها، وتفرض المادة الثامنة عقوبات صارمة على أي عبث بالأدلة الرقمية أو تدميرها أو العبث بمحتواها، مما يوفر حماية قانونية قوية لهذه الأدلة. أما المادة الثانية عشر فتتظم بشكل مفصل ودقيق إجراءات حجز الأجهزة الإلكترونية والأدلة الرقمية، وتحدد الضوابط والشروط الواجب اتباعها عند القيام بعمليات الحجز والتفتيش الرقمي، مما يوفر الحماية القانونية اللازمة لهذه الأدلة منذ لحظة جمعها وحتى عرضها أمام القضاء.

وقد شهد الموقف السعودي من الأدلة الرقمية تطوراً تاريخياً مهماً يمكن تقسيمه إلى ثلاث مراحل أساسية تواكب التطور التقني والتشريعي. بدأت بمرحلة التحفظ التي امتدت حتى عام ٢٠٠٧، حيث كان هناك تشكك قضائي واسع في قيمة الأدلة الرقمية واشترطات صارمة لقبولها، وندر الاعتماد عليها في الأحكام القضائية. ثم انتقل إلى مرحلة القبول المحدود بين ٢٠٠٧-٢٠١٨ التي شهدت تحولاً تدريجياً في التعامل مع هذه الأدلة، وبدأ ظهور أولى وحدات الفحص الرقمي المتخصصة، وازداد الاعتماد على الأدلة الرقمية في القضايا الجنائية والمدنية. وأخيراً دخلت المملكة مرحلة التمكين منذ ٢٠١٨ والتي تميزت باعتماد واسع ومتزايد للأدلة الرقمية، وتأسيس مختبرات متخصصة في الفحص الرقمي تابعة لوزارة الداخلية والنيابة العامة، وتطوير إجراءات التحقيق الرقمي لتواكب أحدث التطورات التقنية في هذا المجال.

#### ثانياً: مدى حجية الأدلة الرقمية في المحاكم السعودية في ظل التخفي الرقمي

تتنوع مواقف المحاكم السعودية من الأدلة الرقمية المتأثرة بالتخفي الرقمي بين ثلاثة اتجاهات رئيسية تظهر بوضوح في الأحكام القضائية الصادرة في هذا الشأن. يتمثل الاتجاه الأول في الموقف التقليدي الذي يشترط إثبات هوية مصدر الدليل الرقمي بشكل قاطع ويميل إلى رفض الأدلة المستخرجة من الشبكات المخفية مثل تور أو الشبكات الخاصة الافتراضية، بحجة عدم إمكانية التحقق من سلامتها أو نسبتها لأصحابها الحقيقيين. هذا الاتجاه يعتمد بشكل كبير على المبادئ التقليدية للإثبات في النظام القضائي السعودي، ويظهر بشكل واضح في القضايا التي تتعلق بالجرائم المعلوماتية البسيطة أو في المحاكم الابتدائية.

بينما يتخذ الاتجاه التوفيقي موقفاً أكثر مرونة وتطوراً، حيث يقبل الأدلة غير المباشرة ويعتمد على القرائن الرقمية المتعددة التي تشكل في مجموعها دليلاً قوياً، مع الأخذ برأي الخبراء الفنيين المعتمدين في تقييم هذه الأدلة وتحليلها. هذا الاتجاه يظهر بوضوح في قضايا الجرائم الإلكترونية الكبرى مثل جرائم الاختراق المنظمة أو جرائم الابتزاز الإلكتروني، حيث تعتمد المحاكم على تقارير الخبراء من الجهات المختصة مثل الهيئة الوطنية للأمن السيبراني أو مركز مكافحة الجرائم المعلوماتية. أما الاتجاه التطوري فيمثل أقصى درجات القبول والتكيف مع متطلبات العصر الرقمي، حيث يركز على مضمون الدليل وقيمه الإثباتية بغض النظر عن مصدره أو طريقة تخفيه، ويعتمد على تقنيات متقدمة في التحليل الرقمي، ويقبل الأدلة المشفرة عند استيفائها لشروط محددة تتعلق بطريقة الحصول عليها وسلامة سلسلة الحفظ الرقمية. هذا الاتجاه يظهر بشكل

خاص في القضايا الكبرى التي تنتظر فيها الدوائر المتخصصة في الجرائم المعلوماتية، حيث تعتمد المحاكم على أدلة رقمية معقدة تم الحصول عليها من خلال تقنيات متطورة في التحقيق الرقمي.

وقد أظهر تحليل الأحكام القضائية الصادرة في هذا الشأن تبايناً واضحاً في التطبيق العملي، حيث قبلت بعض المحاكم رسائل مشفرة كدليل بعد الاستعانة بتقارير الخبراء الفنيين الذين أثبتوا سلامة الدليل وعدم التلاعب به، كما في قضية ابتزاز إلكتروني نظرت فيها محكمة الرياض الجزائية المتخصصة عام ٢٠٢١. بينما رفضت محاكم أخرى معاملات رقمية مشفرة مثل معاملات العملات الرقمية بسبب عدم إمكانية تتبع مصادرها أو التحقق من هوية أطرافها بشكل قاطع، كما في قضية غسيل أموال نظرت فيها محكمة جدة الجزائية المتخصصة عام ٢٠٢٢.

وتواجه المحاكم السعودية تحديات جسيمة وعميقة في التعامل مع هذه الأدلة، يأتي في مقدمتها صعوبة إثبات الصلة بين الدليل الرقمي المخفي والمشتبه به، حيث تعاني من عدم القدرة على ربط الأدلة المخفاة بأصحابها الحقيقيين في كثير من الأحيان، خاصة في حالات استخدام تقنيات التخفي المتقدمة مثل الشبكات المعتمدة على التوجيه البصري أو أنظمة التشفير من طرف إلى طرف. كما تواجه تحديات تقنية كبيرة في التحقق من صحة الأدلة المستخرجة من بيانات التخفي المعقدة، وإثبات عدم التلاعب بها خلال مراحل جمعها وتحليلها. إضافة إلى التحدي التشريعي المتمثل في عدم وجود نصوص صريحة تنظم بشكل كافٍ كيفية التعامل مع أدلة التخفي الرقمي، مما يخلق نوعاً من الاجتهاد القضائي غير الموحد في هذا المجال.

وفي مواجهة هذه التحديات، تبذل المملكة جهوداً كبيرة ومتعددة الأوجه لتعزيز حجية الأدلة الرقمية، من خلال تطوير التشريعات وإنشاء وحدات متخصصة في التحقيق الرقمي تابعة للنسابة العامة ووزارة الداخلية، وتدريب الكوادر القضائية على فهم هذه التقنيات المعقدة من خلال برامج تدريبية متخصصة بالتعاون مع الجامعات ومراكز التدريب المتخصصة. كما تعمل على تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية التي تستخدم تقنيات التخفي، من خلال الانضمام إلى الاتفاقيات الدولية وتبادل الخبرات مع المراكز المتخصصة في هذا المجال، سعياً لتحقيق التوازن الدقيق بين متطلبات العدالة وحماية الخصوصية في العصر الرقمي الذي يتسم بالتعقيد والتطور السريع.

## الخاتمة

في ختام هذه الدراسة، يمكن القول إن التخفي الرقمي يُشكل تحديًا كبيرًا أمام المحاكم السعودية في التعامل مع الأدلة الرقمية، خاصة في ظل التطور السريع للتكنولوجيا وزيادة تعقيداتها. لقد أظهرت الدراسة أن التخفي الرقمي يعتمد على تقنيات متطورة تجعل من الصعب تتبع الأدلة الرقمية والتحقق من صحتها، مما يؤثر بشكل مباشر على حجية هذه الأدلة في الإثبات القضائي. بالإضافة إلى ذلك، فإن الإطار القانوني الحالي في المملكة العربية السعودية، رغم تطوره، لا يزال بحاجة إلى تعزيز لمواكبة هذه التحديات. لذلك، فإن الدراسة تؤكد على أهمية تطوير التشريعات وتبني تقنيات حديثة لتعزيز قدرة المحاكم على التعامل مع الأدلة الرقمية في ظل التخفي الرقمي.

## النتائج

توصلت الدراسة إلى عدة نتائج رئيسية، أهمها أن التخفي الرقمي يُعيق بشكل كبير عملية تتبع الأدلة الرقمية والتحقق من صحتها، مما يؤثر على حجيتها في المحاكم السعودية. كما أظهرت الدراسة أن التحديات القانونية تشمل صعوبة إثبات مصدر الأدلة الرقمية وعدم وجود تشريعات كافية لتغطية جميع جوانب التخفي الرقمي. من الناحية الفنية، فإن استخدام تقنيات متطورة مثل التشفير والشبكات الخاصة الافتراضية (VPN) يجعل من الصعب تتبع الأدلة الرقمية. بالإضافة إلى ذلك، فإن الإطار القانوني السعودي يحتاج إلى تحديث لمواكبة التطورات التكنولوجية وضمان حجية الأدلة الرقمية في المحاكم.

## التوصيات

بناءً على النتائج التي توصلت إليها الدراسة، يتم تقديم التوصيات التالية: أولاً، يجب تعزيز الإطار القانوني السعودي من خلال إصدار تشريعات جديدة تغطي جميع جوانب التخفي الرقمي وتحدد معايير واضحة لقبول الأدلة الرقمية. ثانياً، ينبغي تدريب القضاة والمحققين على استخدام التقنيات الحديثة لتتبع الأدلة الرقمية والتحقق من صحتها. ثالثاً، يجب تعزيز التعاون بين الجهات الحكومية والقطاع الخاص لتطوير أدوات تقنية متقدمة لمكافحة التخفي الرقمي. أخيراً، يُوصى بإنشاء مراكز متخصصة في التحقيق الرقمي تعمل على تحليل الأدلة الرقمية بشكل دقيق وفعال، مما يساهم في تعزيز حجية هذه الأدلة في المحاكم السعودية.

## قائمة المراجع

- نظام الإثبات السعودي (الصادر بالمرسوم الملكي رقم م/٤٣ بتاريخ ١٤٤٣هـ)
- نظام مكافحة الجرائم المعلوماتية (الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨هـ)
- اللائحة التنفيذية لنظام مكافحة الجرائم المعلوماتية
- عطية، ثروت (٢٠٢٤)، السياسة الجنائية لمكافحة الجريمة المعلوماتية في المملكة العربية السعودية (دراسة مقارنة) مجلة البحوث الفقهية والقانونية.
- الغنامي، نايف (٢٠٢٤) حجية الدليل الرقمي في نظام الإثبات السعودي، الجامعة السعودية الإلكترونية، المملكة العربية السعودية.
- إبراهيم، أحمد علي محمود (٢٠٢٠). الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية، مجلة الشريعة والقانون
- إبراهيم، خالد ممدوح (٢٠١٠). فن التحقيق الجنائي في الجرائم الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية .
- الأحمد، وسيم حسام الدين (٢٠٢٣). شرح نظام الإثبات السعودي الجديد مدعماً بالأدلة الإجرائية لنظام الإثبات وضع ضوابط إجراءات الإثبات إلكترونياً، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض .
- البشرى، محمد الأمين (٢٠١٤). التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، الأردن .
- البشري، محمد الأمين (٢٠٠٤). التحقيق في الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية .
- التميمي، علاء حسين مطلق (٢٠١٨). الجهة المختصة بإصدار شهادة التصديق الإلكتروني، دار النهضة العربية، القاهرة .
- التهامي، سامح عبدالواحد (٢٠١٨). التعاقد عبر الإنترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة .
- الجمسي، خالد مصطفى (٢٠١٧). الدليل الرقمي، بحث منشور بمجلة القانون المغربي، دار السلام للطباعة والنشر، مارس .
- الحجار، وسيم شفيق (٢٠٢٢). الإثبات الإلكتروني، مكتبة صادر ناشرون، بيروت .
- حجازي، عبد الفتاح بيومي (٢٠٠٩). الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، منشأة المعارف، الإسكندرية، جمهورية مصر العربية .

حسين، سامي جلال فقي (٢٠١١). الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دراسة مقارنة، دار الكتب القانونية، مصر .

الحمادي، إبراهيم (٢٠١٩). ماهية الدليل الرقمي: خصائصه شروطه وحجيته، مجلة المناعة للدراسات القانونية والإدارية .  
الحوامدة، لورنس (٢٠٢١). حجية الأدلة الرقمية في الإثبات الجنائي دراسة تحليلية مقارنة، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون بدمهور .

## References

- Ibrahim, Ahmed Ali Mahmoud (2020). Digital evidence and its authority in proving cybercrimes, Journal of Sharia and Law.
- Ibrahim, Khaled Mamdouh (2010). The art of criminal investigation in cybercrimes, comparative study, first edition, University thought House, Alexandria.
- Al-Ahmad, Wasim Husam al-Din (2023). Explanation of the new Saudi proof system, supported by procedural evidence of the proof system, setting the controls of proof procedures electronically, first edition, law and Economics Library, Riyadh.
- Al-bishra, Mohammed Al-Amin (2014). Investigation of new crimes, Dar Al-Hamid publishing and distribution, Jordan.
- Al-Bishri, Muhammad Al-Amin (2004). Investigation of new crimes, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.
- Tamimi, Alaa Hussein is divorced (2018). The competent authority for issuing the electronic certification certificate, Dar Al Nahda Al Arabiya, Cairo.
- Al-Tuhami, Sameh Abdulwahid (2018). Online contracting, first edition, House of legal books, Cairo.

Al-Jasmi, Khaled Mustafa (2017). Digital evidence, research published in the Journal of Moroccan law, Dar es Salaam printing and publishing, March.

Al-Hajjar, Wasim Shafiq (2022). Electronic proof, Sadr publishers library, Beirut.

Hijazi, Abdel Fattah Bayoumi (2009). Procedural aspects of the work of the primary investigation in Information Crimes, knowledge facility, Alexandria, Arab Republic of Egypt .

Hussain, Sami Jalal Faqi (2011). Computer-generated evidence and its validity in criminal evidence, Comparative Study, House of legal books, Egypt.

Al Hammadi, Ibrahim (2019). What is digital evidence: its characteristics, conditions and authenticity, Al-immuna Journal for legal and Administrative Studies.

Al-hawamda, Lawrence (2021). The authenticity of digital evidence in criminal evidence is a comparative Analytical Study, Journal of jurisprudence and legal research, Al-Azhar University, Faculty of Sharia and law in Damanhour.