

خطة بحث بعنوان

الإثبات الجنائي في الجرائم الإلكترونية: دراسة مقارنة بين
القانون السعودي والقانون المصري

Digital Forensics in Cyber Crimes: A Comparative Study
between Saudi Law and Egyptian Law

إعداد الطالب/

محمد بن عوضه علي الأسمرى

الرقم الأكاديمي: 251001789

العام الجامعي

2025

يشهد العالم اليوم تحولاً رقمياً غير مسبوق، حيث تتغلغل التكنولوجيا في شتى مناحي الحياة، مما أفرز أنماطاً جديدة من السلوك الإجرامي لم تكن معهودة من قبل. وفي خضم هذا التطور، برزت الجرائم الإلكترونية كأحد أخطر التحديات التي تواجه المجتمعات والحكومات على حد سواء (Alqahtani, 2023, p. 34). تتسم هذه الجرائم بطبيعتها العابرة للحدود وصعوبة تتبع مرتكبيها، مما يستلزم تطوير آليات قانونية وتقنية فعالة لمواجهتها والحد من أثارها السلبية على الأفراد والمؤسسات والدول. وفي هذا السياق، يكتسب الإثبات الجنائي أهمية قصوى، فهو الأداة الأساسية التي تعتمد عليها العدالة الجنائية في كشف الحقيقة وتحديد المسؤولية الجنائية في هذه النوعية المستجدة من الجرائم.

إن الدور المحوري للإثبات الجنائي يتجلى بوضوح في سياق مكافحة الجرائم الإلكترونية، حيث يمثل حجر الزاوية في بناء القناعة لدى القاضي بثبوت الواقعة الإجرامية ونسبة ارتكابها إلى المتهم (مصطفى، 2021، ص. 15). فبدون أدلة قوية وموثوقة، يصبح من الصعب إنزال العقاب العادل على مرتكبي هذه الجرائم، مما قد يؤدي إلى إفلاتهم من العقاب وتشجيعهم على ارتكاب المزيد منها. وتزايد أهمية الإثبات الجنائي في ظل الطبيعة الرقمية المعقدة للأدلة الإلكترونية، والتي تتطلب خبرات فنية وقانونية متخصصة في جمعها وتحليلها وتقديمها أمام المحاكم (Baggili et al., 2022, pp. 45-48).

وعلى الجانب الآخر، تمثل الجرائم الإلكترونية تحدياً فريداً لأنظمة الإثبات الجنائي التقليدية. فالأدلة في هذه الجرائم غالباً ما تكون في شكل بيانات رقمية قابلة للتغيير أو الحذف بسهولة، وقد تكون مخزنة في أماكن بعيدة أو حتى عابرة للحدود القضائية للدولة (Kshetri & Voas, 2020, p. 112). وهذا التعقيد يفرض على الأنظمة القانونية ضرورة التكيف وتطوير قواعد وإجراءات إثبات جديدة تتلاءم مع طبيعة هذه الجرائم وتضمن تحقيق العدالة دون المساس بالحقوق والحريات الأساسية للأفراد.

من هذا المنطلق، تتضح العلاقة الوثيقة بين الإثبات الجنائي والجرائم الإلكترونية، حيث يشكل الأول الأداة الرئيسية لمواجهة التحديات التي تفرضها الثانية. ففاعلية القوانين التي تجرم الأفعال الإلكترونية تتوقف إلى حد كبير على وجود آليات إثبات قوية تمكن من تطبيق هذه القوانين على أرض

الواقع. وبالمثل، فإن تطور أساليب ارتكاب الجرائم الإلكترونية يستلزم تطوراً مستمراً في أدوات وتقنيات الإثبات الجنائي لمواكبة هذه التغيرات وضمان عدم إفلات المجرمين من العقاب.

في هذا السياق، تبرز أهمية دراسة الأنظمة القانونية في دول مختلفة لفهم كيفية تعاملها مع هذه الإشكالية. تعد المملكة العربية السعودية وجمهورية مصر العربية من الدول التي بذلت جهوداً تشريعية وقضائية لمكافحة الجرائم الإلكترونية وتطوير آليات الإثبات فيها. ففي المملكة العربية السعودية، صدر نظام مكافحة جرائم المعلوماتية الذي تضمن العديد من الأحكام المتعلقة بالإثبات في هذا النوع من الجرائم (Saudi Anti-Cyber Crime Law, 2007). وبالمثل، أصدرت جمهورية مصر العربية قانون مكافحة جرائم تقنية المعلومات الذي تناول جوانب الإثبات المتعلقة بهذه الجرائم (Egyptian Cybercrime Law No. 175 of 2018).

تهدف هذه الدراسة إلى إجراء تحليل مقارنة بين النظامين القانونيين السعودي والمصري فيما يتعلق بالإثبات الجنائي في الجرائم الإلكترونية. من خلال هذا التحليل، تسعى الدراسة إلى تحديد أوجه التشابه والاختلاف بين النظامين في تعاملهما مع الأدلة الرقمية وإجراءات جمعها وتقديمها أمام المحاكم، بالإضافة إلى تقييم مدى فعالية هذه الأنظمة في مواجهة التحديات التي تفرضها طبيعة الجرائم الإلكترونية. كما تطمح الدراسة إلى تقديم توصيات عملية تساهم في تطوير وتعزيز الأطر القانونية والإجرائية المتعلقة بالإثبات الجنائي في الجرائم الإلكترونية في كلا البلدين.

إن تناول هذا الموضوع بالبحث والدراسة يكتسب أهمية خاصة في الوقت الراهن نظراً للترديد المستمر في حجم وتطور الجرائم الإلكترونية، وتأثيرها المتنامي على مختلف جوانب الحياة. كما أن المقارنة بين تجربتي المملكة العربية السعودية وجمهورية مصر العربية، وهما دولتان عربيتان لهما أنظمة قانونية متأثرة بتقاليد قانونية مشتركة وفي نفس الوقت تواجهان تحديات مماثلة في مجال مكافحة الجريمة الإلكترونية، يمكن أن يقدم رؤية قيمة للمشرعين والممارسين القانونيين في كلا البلدين وفي المنطقة العربية بشكل عام. من خلال هذه الدراسة، نأمل في إلقاء الضوء على أفضل الممارسات والتحديات القائمة، والمساهمة في تعزيز القدرة على مكافحة الجرائم الإلكترونية وتحقيق العدالة في هذا المجال الحيوي.

مشكلة الدراسة

تواجه القطاعات القانونية والقضائية في مختلف دول العالم تحديات جمة في سبيل مكافحة الجرائم الإلكترونية، ولا يستثنى من ذلك النظامان القانونيان السعودي والمصري. فمع التطور التقني المتسارع، أصبحت الجرائم الإلكترونية أكثر تعقيداً وتنوعاً، مما يطرح صعوبات كبيرة في مجال الإثبات الجنائي. إن طبيعة الأدلة الرقمية، التي قد تكون عابرة للحدود، سهولة التغيير أو الإتلاف، ومخزنة في أجهزة أو أنظمة متعددة، تجعل من عملية جمعها والحفاظ عليها وتقديمها كدليل مقبول أمام المحاكم أمراً بالغ الصعوبة (Baggili et al., 2022, pp. 45-48). فالتحديات التقنية، مثل تشفير البيانات وإخفاء الهوية عبر الإنترنت، تعيق جهود المحققين في الوصول إلى الأدلة اللازمة لكشف الحقيقة وملاحقة المجرمين.

في سياق البيئة القانونية في المملكة العربية السعودية وجمهورية مصر العربية، يلاحظ الباحث وجود حاجة متزايدة لفهم معمق وشامل لكيفية تعامل النظامين القانونيين مع هذه التحديات. فبالرغم من وجود تشريعات تجرم الأفعال الإلكترونية، مثل نظام مكافحة جرائم المعلوماتية في السعودية وقانون مكافحة جرائم تقنية المعلومات في مصر (Saudi Anti-Cyber Crime Law, 2007; Egyptian Cybercrime Law No. 175 of 2018)، إلا أن تطبيق هذه القوانين على أرض الواقع يواجه صعوبات تتعلق بالإثبات. فعلى سبيل المثال، قد يواجه المحققون صعوبة في تحديد مصدر الهجوم الإلكتروني أو تتبع مسار الأموال المتحصلة من الجرائم الإلكترونية، خاصة في ظل استخدام تقنيات إخفاء الهوية والشبكات الافتراضية الخاصة (VPNs). كما أن حجية الأدلة الرقمية المستمدة من مصادر خارجية أو عبر الحدود قد تثير إشكاليات قانونية تتعلق بالسيادة والاختصاص القضائي.

وقد أشارت بعض الدراسات والمؤتمرات إلى هذه التحديات بشكل عام في المنطقة العربية. فعلى سبيل المثال، أكدت دراسة لـ Kamal and Ibrahim (2023) على أن هناك حاجة لمزيد من التنسيق والتعاون بين الدول العربية في مجال مكافحة الجرائم الإلكترونية، بما في ذلك تبادل الأدلة والمعلومات. كما أن الصعوبات المتعلقة بجمع الأدلة الرقمية وتقديمها أمام المحاكم كانت من بين الموضوعات التي تم تناولها في العديد من الفعاليات والمؤتمرات المتخصصة في الأمن السيبراني والقانون في الشرق الأوسط. ومع ذلك، لا يزال هناك نقص ملحوظ في الدراسات الأكاديمية التي تقدم تحليلاً مقارناً معمقاً

وشاملاً لكيفية تعامل النظامين القانونيين السعودي والمصري تحديداً مع مسألة الإثبات الجنائي في الجرائم الإلكترونية.

تبرز هنا الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها. فبالرغم من أهمية الموضوع والتحديات التي يواجهها كلا البلدين، لا يوجد حتى الآن دراسة أكاديمية مستفيضة تقارن بين النظامين القانونيين السعودي والمصري في مجال الإثبات الجنائي للجرائم الإلكترونية. هذه الفجوة تستدعي الوقوف عندها بالبحث والدراسة، خاصة في ظل التطورات القانونية والتقنية المتسارعة. تسعى الدراسة الحالية إلى سد هذه الفجوة من خلال تقديم تحليل مقارنة معمق لأطر الإثبات الجنائي في الجرائم الإلكترونية في كل من المملكة العربية السعودية وجمهورية مصر العربية. وتهدف الدراسة بشكل خاص إلى التعرف على أوجه التشابه والاختلاف في القواعد والإجراءات المتعلقة بجمع الأدلة الرقمية، وشروط قبولها أمام المحاكم، والتحديات التي تواجه القضاة والممارسين القانونيين في هذا المجال. من خلال هذا التحليل المقارن، تأمل الدراسة في تقديم رؤى وتوصيات قيمة تساهم في تعزيز فعالية جهود مكافحة الجرائم الإلكترونية في كلا البلدين.

أهمية الدراسة

تستمد هذه الدراسة أهميتها من عدة جوانب نظرية وعملية، فهي تسعى أولاً إلى إثراء الأدبيات القانونية المتعلقة بالإثبات الجنائي في سياق الجرائم الإلكترونية، وهو مجال لا يزال يشهد تطورات متسارعة ويحتاج إلى مزيد من البحث والتحليل، خاصة في البيئة القانونية العربية. من الناحية النظرية، تقدم الدراسة تحليلاً مقارناً معمقاً بين النظامين القانونيين السعودي والمصري، مما يساهم في فهم أعمق لأوجه التشابه والاختلاف في تعاملهما مع هذا النوع المستجد من الجرائم. كما أنها تسلط الضوء على التحديات القانونية والفنية التي تواجه عملية الإثبات في الجرائم الإلكترونية، وتقدم إطاراً نظرياً يمكن الاستفادة منه في تطوير هذا المجال.

أما من الناحية العملية، فتكمن أهمية الدراسة في قدرتها على تقديم توصيات عملية ومفيدة للمشرعين والقضاة والممارسين القانونيين في المملكة العربية السعودية وجمهورية مصر العربية. من خلال تحديد نقاط القوة والضعف في كل نظام قانوني، يمكن للدراسة أن تساهم في اقتراح تعديلات تشريعية أو تطوير إجراءات قضائية تهدف إلى تعزيز فعالية مكافحة الجرائم الإلكترونية. على سبيل المثال، قد تقدم الدراسة

توصيات بشأن كيفية تحديث قوانين الإثبات لتشمل بشكل واضح الأدلة الرقمية بأنواعها المختلفة، أو كيفية وضع ضوابط قانونية لعملية جمع الأدلة الرقمية عبر الحدود، أو كيفية تدريب القضاة والمحامين على التعامل مع هذه النوعية من الأدلة.

بالإضافة إلى ذلك، تكمن القيمة المضافة لهذه الدراسة في طبيعتها المقارنة التي تجمع بين تجربتين قانونيتين عربيتين هامتين. هذه المقارنة يمكن أن توفر رؤى قيمة ليس فقط للمملكة العربية السعودية وجمهورية مصر العربية، بل أيضاً للدول العربية الأخرى التي تواجه تحديات مماثلة في مجال مكافحة الجرائم الإلكترونية. إن فهم الكيفية التي يتعامل بها نظامان قانونيان مختلفان مع نفس المشكلة يمكن أن يساعد في تبادل الخبرات وأفضل الممارسات، ويساهم في تطوير منظومة قانونية عربية أكثر فعالية في مواجهة الجريمة الإلكترونية. كما أن الدراسة قد تفتح آفاقاً لبحوث مستقبلية أكثر تخصصاً وتعمقاً في جوانب محددة من موضوع الإثبات الجنائي في الجرائم الإلكترونية في المنطقة العربية.

أسئلة الدراسة

تسعى الدراسة الحالية للإجابة عن السؤال البحثي الرئيسي التالي:

السؤال الرئيسي: ما هي أوجه التشابه والاختلاف بين النظامين القانونيين السعودي والمصري في مجال الإثبات الجنائي للجرائم الإلكترونية؟

ويتفرع عن هذا السؤال الرئيسي الأسئلة الفرعية التالية:

1. ما هي المصادر القانونية التي تنظم الإثبات الجنائي في الجرائم الإلكترونية في النظام القانوني السعودي؟
2. ما هي المصادر القانونية التي تنظم الإثبات الجنائي في الجرائم الإلكترونية في النظام القانوني المصري؟
3. ما هي أوجه التشابه والاختلاف بين النظامين السعودي والمصري في تعريف الأدلة الرقمية وأنواعها وشروط قبولها أمام القضاء؟

4. ما مدى فعالية الإجراءات القانونية المتبعة في كل من النظامين في جمع الأدلة الرقمية والمحافظة عليها وضمان سلامتها؟

5. ما هي التحديات التي تواجه تطبيق قوانين الإثبات الجنائي في الجرائم الإلكترونية في كل من المملكة العربية السعودية وجمهورية مصر العربية؟

6. ما هي المقترحات والتوصيات التي يمكن أن تساهم في تطوير الأطر القانونية والإجرائية للإثبات الجنائي في الجرائم الإلكترونية في كلا البلدين؟

أهداف الدراسة

يهدف هذا البحث بشكل رئيس إلى:

الهدف الرئيسي: إجراء دراسة مقارنة بين النظام القانوني السعودي والنظام القانوني المصري في مجال الإثبات الجنائي للجرائم الإلكترونية بهدف تحديد أوجه التشابه والاختلاف وتقييم الفعالية واقتراح سبل التطوير.

ينبثق عن هذا الهدف الرئيسي الأهداف الفرعية التالية:

1. التعرف على الإطار القانوني المنظم للإثبات الجنائي في الجرائم الإلكترونية في النظام القانوني السعودي.

2. التعرف على الإطار القانوني المنظم للإثبات الجنائي في الجرائم الإلكترونية في النظام القانوني المصري.

3. تحديد أوجه التشابه والاختلاف بين النظامين القانونيين السعودي والمصري في مجال تعريف الأدلة الرقمية وشروط قبولها.

4. تقييم فعالية الإجراءات القانونية المتبعة في كل من النظامين في جمع الأدلة الرقمية والمحافظة عليها وتقديمها أمام المحاكم.

5. اقتراح توصيات عملية وقابلة للتطبيق لتطوير الأطر القانونية والإجرائية للإثبات الجنائي في الجرائم الإلكترونية في المملكة العربية السعودية وجمهورية مصر العربية.

مصطلحات الدراسة

الجريمة الإلكترونية (Cybercrime)

• **الجريمة الإلكترونية هي:** الأفعال الإجرامية التي تُرتكب باستخدام الأجهزة الإلكترونية أو عبر الإنترنت، بهدف الإضرار بالأفراد أو المؤسسات أو الدول. وتشمل هذه الجرائم الاختيال الإلكتروني¹، والاختراق، وسرقة الهوية، والتجسس الإلكتروني، والابتزاز الرقمي، ونشر البرمجيات الخبيثة (مقتبس من عناوين رسائل ماجستير ودكتوراه حول الجرائم الإلكترونية 2025).

• **وتعرف أيضاً بأنها:** أي فعل ينتهك القانون، ويتم ارتكابه باستخدام تكنولوجيا المعلومات والاتصالات، إما لاستهداف الشبكات أو الأنظمة أو البيانات أو مواقع الويب و/أو التكنولوجيا أو لتسهيل ارتكاب جريمة (Brenner, 2002; Wall, 2007; Wilson, & Goodman 2008; ITU, 2012; Maras, 2014; Maras, 2016).

• **كما تعرف بأنها:** هي الدخول غير المصرح به إلى أنظمة الحاسوب أو الشبكات أو البيانات، أو إتلاف أو تعديل أو تدمير المعلومات أو البرامج أو الأجهزة، أو استخدام الحاسوب أو الإنترنت لارتكاب الاختيال أو السرقة أو التشهير أو أي فعل غير قانوني آخر (قاموس مصطلحات الأمن السيبراني، لم يتم العثور على مصدر محدد باللغة العربية منشور بين 2020-2025 في نتائج البحث، لذا تم الاعتماد على تعريف شائع ومفهوم).

التعريف الإجرائي للجريمة الإلكترونية في الدراسة الحالية: يُقصد بالجريمة الإلكترونية في هذه الدراسة أي فعل مجرم بموجب القوانين ذات الصلة في المملكة العربية السعودية وجمهورية مصر العربية، والذي يتم باستخدام وسيلة إلكترونية أو عبر شبكة الإنترنت، ويتطلب إثباته اتباع إجراءات خاصة بالأدلة الرقمية.

الإثبات الرقمي (Digital Evidence)

- **التعريف الاصطلاحي:** هو أي معلومة تتم معالجتها بواسطة وسيط إلكتروني تدعم أو تدحض فرضية حول حالة القطع الأثرية الرقمية أو الأحداث الرقمية، ذات صلة محتملة بقيمة إثباتية لتحقيق جنائي (Stoykova, 2022).
- **التعريف الإجرائي للإثبات الرقمي في الدراسة الحالية:** يشير إلى أي بيانات أو معلومات ذات طبيعة إلكترونية يتم الحصول عليها من الأجهزة أو الأنظمة الرقمية، وتكون ذات صلة بواقعة جريمة إلكترونية قيد التحقيق في المملكة العربية السعودية أو جمهورية مصر العربية، ويمكن استخدامها لإثبات ارتكاب تلك الجريمة.

إجراءات جمع الأدلة الرقمية (Procedures for Collecting Digital Evidence)

- **التعريف الاصطلاحي:** هي العلم الذي يختص بالحصول على الأدلة من الحواسيب والأجهزة المحمولة وأجهزة التخزين الإلكترونية الرقمية الأخرى، والحفاظ عليها وتوثيقها. يجب أن يتم كل ذلك بطريقة مصممة للحفاظ على القيمة الإثباتية للأدلة وضمان مقبوليتها في الإجراءات القانونية (Computer Forensics definition from ResearchGate).
- **التعريف الإجرائي لإجراءات جمع الأدلة الرقمية في الدراسة الحالية:** تشمل كافة الخطوات والوسائل القانونية والتقنية التي تتبعها السلطات المختصة في المملكة العربية السعودية وجمهورية مصر العربية لضبط وتفتيش وتحريز الأدلة الرقمية المتعلقة بالجرائم الإلكترونية، بما يضمن سلامتها وقبولها في الإجراءات القضائية.

حجية الأدلة الرقمية (Admissibility of Digital Evidence)

- **التعريف الاصطلاحي:** إن فقه التحقيقات في الأدلة الرقمية هو نظرية وفلسفة دراسة القانون والمبادئ التي يستند إليها القانون. لكي تظهر الأدلة الرقمية في المحكمة وتكون مقبولة قانونًا، يجب أن تكون الأدلة أصلية ودقيقة وكاملة ومقنعة لهيئة المحلفين (Digital Forensics Investigation Jurisprudence definition from ResearchGate, 2024).

- **التعريف الإجرائي لحجية الأدلة الرقمية في الدراسة الحالية:** تعني مدى قبول المحاكم الجنائية في المملكة العربية السعودية وجمهورية مصر العربية للأدلة الرقمية المقدمة في قضايا الجرائم الإلكترونية، وذلك بناءً على استيفائها للشروط والمعايير القانونية المنصوص عليها في قوانين الإثبات والإجراءات الجنائية في كلا البلدين.

النظام القانوني السعودي (Saudi Legal System)

- هو مجموعة القواعد والمبادئ القانونية المستمدة أساساً من الشريعة الإسلامية، بالإضافة إلى الأنظمة واللوائح التي تصدرها الدولة لتنظيم مختلف جوانب الحياة في المملكة العربية السعودية. ويهدف إلى تحقيق العدل والأمن وحماية الحقوق والحريات وفقاً للشريعة السمحة.

النظام القانوني المصري (Egyptian Legal System)

- **التعريف الاصطلاحي:** هو نظام قانوني يعتمد على مزيج من مبادئ القانون المدني المستوحاة من القانون الروماني والقانون الفرنسي، بالإضافة إلى مبادئ الشريعة الإسلامية التي تعد مصدراً رئيسياً للتشريع بموجب الدستور المصري. ويهدف إلى تنظيم العلاقات القانونية المختلفة في المجتمع المصري وتحقيق العدالة.

تمهيد

يستعرض هذا الجزء مجموعة من الدراسات السابقة التي تناولت موضوع الإثبات الجنائي في الجرائم الإلكترونية والأدلة الرقمية وحجيتها، والتي تم إجراؤها على مستويات مختلفة محلية وإقليمية ودولية خلال الفترة من عام 2011 إلى عام 2024. ويهدف هذا الاستعراض إلى توفير خلفية علمية وواقعية للدراسة الحالية، وتسلط الضوء على الجهود البحثية السابقة في هذا المجال، وتحديد الفجوات التي تسعى الدراسة الحالية إلى معالجتها. فيما يلي ملخص موجز لأهم هذه الدراسات:

1. دراسة "المعلم، والكربي" (2024)، التي أجريت في المملكة العربية السعودية، بعنوان: "تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي (دراسة تحليلية)". هدفت الدراسة إلى تحليل تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي. اعتمدت الدراسة على المنهج التحليلي، وتناولت مفهوم الإثبات وأهميته ومذاهبه، ثم الأدلة الرقمية، وحجيتها، وتأثير التقنية عليها في النظام السعودي. وقد توصلت الدراسة إلى أن للتقنية دور مهم في تحسين وسائل الإثبات الرقمية، وأوصت بأهمية مواكبة التطورات التقنية في مجال الإثبات.

2. دراسة "أبو العلا" (2024)، التي أجريت في مصر، بعنوان: "المواجهة الجنائية لمخاطر تقنية الديب فيك DEEP FAKES وأثرها على حجية الأدلة الرقمية في الإثبات الجنائي: دراسة تحليلية مقارنة". هدفت الدراسة إلى بحث التحديات التي تفرضها تقنية التزييف العميق (Deepfakes) على حجية الأدلة الرقمية في الإثبات الجنائي في مصر من خلال دراسة تحليلية مقارنة. وقد توصلت إلى أن تقنية الديب فيك تمثل تهديداً كبيراً لموثوقية الأدلة الرقمية وقابليتها للإثبات. ودعت إلى تطوير آليات قانونية وتقنية لمواجهة هذه المخاطر والتحقق من صحة الأدلة الرقمية.

3. دراسة "Alasaf & Aljadani" (2023)، التي أجريت في المملكة العربية السعودية، بعنوان: "Digital Evidence in Saudi Law: A Comparative Study – ماهية

الدليل الرقمي في النظام السعودي: دراسة مقارنة". هدفت الدراسة إلى بحث ماهية الدليل الرقمي في النظام القانوني السعودي من خلال دراسة مقارنة. تناولت الدراسة مشروعية الدليل الرقمي وفقاً لمذاهب الإثبات المختلفة، مبينة أنه في الأنظمة التي تتبع نظام الإثبات المقيد لا يمكن التعويل على الأدلة الرقمية ما لم يتم تنظيمها وفق نصوص قانونية. وقد أشارت الدراسة إلى أن الأدلة الرقمية تحتاج إلى تنظيم قانوني واضح لقبولها في نظام الإثبات المقيد.

4. دراسة "تمارا فخري" (2022)، التي أجريت في العراق، بعنوان: "حجية الدليل الرقمي في الإثبات الجنائي". هدفت الدراسة إلى التعرف على حجية الدليل الرقمي في الإثبات الجنائي في التشريع العراقي. اعتمدت الدراسة على المنهج الوصفي التحليلي. وقد خلصت الدراسة إلى أن الأدلة الرقمية أصبحت ذات أهمية كبيرة في الإثبات الجنائي، خاصة في ظل التطور التكنولوجي وتزايد الجرائم الإلكترونية، وأن التشريع العراقي خطا خطوات مهمة في الاعتراف بها. ودعت الدراسة إلى ضرورة تحديث التشريعات بما يواكب التطور التقني في مجال الأدلة الرقمية وتوفير آليات واضحة للتعامل معها في الإجراءات الجنائية.

5. دراسة "شرف الدين" (2021)، التي أجريت في الجزائر، بعنوان: "إجراءات جمع الأدلة الرقمية طبقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات". هدفت هذه الدراسة إلى التعرف على الإجراءات القانونية لجمع الأدلة الرقمية في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل نصوص الاتفاقية. تناولت الدراسة أنواع الأدلة الرقمية وإجراءات جمعها مثل المعلومات المخزنة وبيانات الحركة واعتراض معلومات المحتوى، بالإضافة إلى الأحكام القانونية المنظمة لهذه الإجراءات في الاتفاقية.

6. دراسة "Mili Kanoujiya" (2021)، التي أجريت في الهند، بعنوان: "A STUDY OF DIGITAL EVIDENCES WITH RESPECT TO CYBER FORENSICS". هدفت الدراسة إلى بحث - "دراسة للأدلة الرقمية فيما يتعلق بالطب الشرعي السيبراني". تناولت الدراسة مفهوم الأدلة الرقمية،

وأهميتها، وعلاقتها بالأدلة الجنائية الإلكترونية، ودور الأدلة الجنائية الإلكترونية في جمع الأدلة وتقديمها أمام المحاكم. وقد أكدت الدراسة على أهمية الأدلة الرقمية في التحقيقات الجنائية الإلكترونية. ودعت الدراسة إلى فهم أفضل للأدلة الرقمية وكيفية التعامل معها في الإجراءات القانونية.

7. دراسة "Kumar and Sharma" (2021)، التي أجريت في الهند، بعنوان: "Digital Evidence Admissibility in Indian Courts: Bridging Legal Gaps in the Age of Cybercrime" - "قبول الأدلة الرقمية في المحاكم الهندية: سد الفجوات القانونية في عصر الجرائم الإلكترونية". هدفت الدراسة إلى تحليل التحديات الإجرائية التي تواجه إثبات الجرائم الإلكترونية في المحاكم الهندية. وقد توصلت الدراسة إلى أن 73% من قضايا الجرائم الإلكترونية التي تم تحليلها واجهت تحديات تتعلق بقبول الأدلة الرقمية بسبب إجراءات الجمع أو المصادقة غير السليمة. كما تبين أن النزاعات حول الوصول إلى البيانات كانت العامل المهيمن في الطعن في الأدلة الرقمية في 62% من الحالات، وأن إجراءات جمع الأدلة كانت غير كافية في 47% من الحالات، مما يسلط الضوء على فجوات إجرائية كبيرة.

8. دراسة "UNODC" "United Nations Office on Drugs and Crime"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة". (2014)، التي أجريت على مستوى دولي، بعنوان: "Cybercrime Module 6 Key Issues: Digital Evidence Admissibility" - "الوحدة 6 من الجرائم الإلكترونية: القضايا الرئيسية - قبول الأدلة الرقمية". يهدف هذا المورد إلى تناول الجوانب العملية لتحقيقات الجرائم الإلكترونية والأدلة الجنائية الرقمية، مع التركيز على قبول الأدلة الرقمية. ويؤكد هذا المورد على أهمية المعايير والبروتوكولات في مختبرات الأدلة الجنائية الرقمية لضمان الكفاءة في التعامل مع الأدلة وتحليلها وإنتاج نتائج موثوقة. كما يسلط الضوء على دور الاعتماد في تحسين الجودة وضمان استخدام أساليب موثوقة ومعدات وبرامج مناسبة وموظفين مؤهلين للوصول إلى استنتاجات معقولة.

9. دراسة "Faqi Hussein" (2011)، مصر، بعنوان: "Computer Evidence and its Authenticity in Criminal Evidence: A Comparative Study" - "الأدلة الإلكترونية وموثوقيتها في الأدلة الجنائية: دراسة مقارنة". هدفت الدراسة إلى إجراء دراسة مقارنة حول الأدلة الحاسوبية وأصالتها في الإثبات الجنائي. تناولت الدراسة مفهوم الأدلة الرقمية وأهميتها في الأنظمة القانونية الحديثة، وتحديات إثبات أصالتها.

تعقيب عام على الدراسات السابقة

تتعدد الدراسات السابقة التي تناولت موضوع الإثبات الجنائي في الجرائم الإلكترونية والأدلة الرقمية. من خلال استعراضها، تظهر مجموعة من جوانب الاتفاق والاختلاف بين هذه الدراسات، بالإضافة إلى الفجوات البحثية التي تسعى الدراسة الحالية لمملئها.

جوانب الاتفاق

1. **أهمية الأدلة الرقمية:** تناولت جميع الدراسات المعروضة أهمية الأدلة الرقمية في سياق الإثبات الجنائي. وقد أكدت الدراسات المختلفة، سواء كانت على مستوى محلي أو دولي، على الدور الحاسم الذي تؤديه التكنولوجيا في توثيق الأدلة وتحسين الإجراءات القضائية.

2. **التحديات المتعلقة بالحجية:** اتفقت الدراسات على وجود تحديات تتعلق بحجية الأدلة الرقمية، بما في ذلك تأثير تقنيات جديدة مثل الـديب فيك، وقضايا قبول الأدلة في المحاكم بسبب التفاوتات في الإجراءات القانونية بين الأنظمة المختلفة.

3. **الحاجة إلى تحديث التشريعات:** دعت العديد من الدراسات إلى ضرورة مواكبة التشريعات للتطورات التقنية المتسارعة في مجال الجرائم الإلكترونية، مما يعكس الفهم المتزايد لأهمية تطويع القوانين بما يتلاءم مع العصر الرقمي.

جوانب الاختلاف

1. **التركيز الجغرافي:** تتميز الدراسات بتنوعها الجغرافي، حيث تناولت بعض الدراسات السياق السعودي، وأخرى المصرية، بالإضافة إلى دراسات من دول عربية كالـعراق والـجزائر، وأيضاً دراسات من الـهند. هذا الاختلاف في السياق القانوني والثقافي يمكن أن يؤدي إلى تباين النتائج والتوصيات.

2. **المنهجيات المستخدمة:** تنوعت الأساليب البحثية بين الدراسات، حيث استخدمت بعض الدراسات المنهج الوصفي التحليلي، في حين اعتمدت الأخرى على المنهج المقارن. هذا التنوع يعكس اختلافاً في طريقة معالجة المشكلة والبحث عن الحلول.

الفجوة البحثية

رغم وجود العديد من الدراسات، إلا أن هناك فجوة ملحوظة في تناول موضوع **التقنيات الحديثة وتأثيرها على الإجراءات الجنائية**، مثل تأثير التقنيات الجديدة على مصداقية الأدلة الرقمية. فبينما تناولت بعض الدراسات مسألة الديب فيك، لا تزال هناك حاجة لدراسات تتناول التطورات التقنية الحديثة وتفاعلاتها مع الأنظمة القضائية المختلفة بشكل شامل.

توجد أيضًا حاجة أكبر لدراسات مقارنة أوسع تشمل عدة دول بشكل متزامن، لتحديد كيفية تعامل مختلف الأنظمة القانونية مع نفس التحديات المتعلقة بالأدلة الرقمية.

مميزات الدراسة الحالية

تسعى الدراسة الحالية لمعالجة الفجوات البحثية المذكورة من خلال:

1. **تحليل شامل للتحديات:** تهدف الدراسة إلى تقديم تحليل شامل لتأثير التقنيات الحديثة على الإثبات الجنائي، مع التركيز على التقنيات الناشئة مثل الذكاء الاصطناعي، والبيانات الكبيرة، وكيفية تأثيرها على موثوقية الأدلة الرقمية.
 2. **تقديم توصيات عملية:** تهدف الدراسة إلى تقديم توصيات عملية قابلة للتطبيق على صعيد التشريعات والإجراءات القانونية، مما يساعد في تحسين فعالية النظام القضائي في مواجهة التحديات المرتبطة بالجرائم الإلكترونية.
 3. **استجابة للتغيرات السريعة:** تستجيب الدراسة للتغيرات السريعة في عالم التكنولوجيا، مما يجعلها ذات أهمية عالية للممارسين القانونيين وصناع القرار على حد سواء.
- وبصفة عامة، يكشف استعراض الدراسات السابقة عن صورة معقدة وغنية بالمعلومات حول موضوع الإثبات الجنائي والجرائم الإلكترونية، مما يبرز الحاجة لمزيد من البحث والتطوير في هذا المجال الحيوي.

المنطلقات النظرية للدراسة:

تمهيد:

يهدف هذا الجزء إلى إرساء الأساس النظري المتين الذي تستند إليه الدراسة الحالية في تحليلها المقارن للإثبات الجنائي في الجرائم الإلكترونية بين النظامين القانونيين السعودي والمصري. سنسعى من خلال هذا المبحث إلى تحديد وتعريف المفاهيم الرئيسية المتعلقة بالجرائم الإلكترونية والإثبات الجنائي، واستكشاف الخصائص الفريدة التي تميز الجرائم الإلكترونية وتؤثر على عملية الإثبات. كما سنتناول أهم التحديات التي تواجه جهود إثبات هذه النوعية من الجرائم في البيئة الرقمية المعاصرة.

أولاً: الجرائم الإلكترونية ماهيتها وخصائصها

تُعد الجرائم الإلكترونية من أبرز التحديات الأمنية والقانونية التي نشأت مع التطور الهائل في تكنولوجيا المعلومات والاتصالات.

• تعريف الجرائم الإلكترونية وأنواعها: يُمكن تعريف الجرائم الإلكترونية بأنها أية أفعال مجرمة

يتم ارتكابها باستخدام الحواسيب أو شبكاتها أو الأجهزة الإلكترونية الأخرى، أو عبر الإنترنت.

يشمل هذا التعريف طيفاً واسعاً من الأنشطة غير القانونية التي تستغل التكنولوجيا كوسيلة أو

هدفاً. تتنوع أنواع الجرائم الإلكترونية بشكل كبير لتشمل، على سبيل المثال لا الحصر:

○ جرائم الاحتيال المالي عبر الإنترنت، مثل سرقة أرقام بطاقات الائتمان والتصيد الاحتيالي.

○ جرائم الاعتداء على البيانات والمعلومات، مثل الاختراق وسرقة البيانات الحساسة ونشر البرمجيات الخبيثة.

○ جرائم المحتوى غير القانوني، مثل نشر مواد إباحية للأطفال أو التحريض على الكراهية والعنف.

○ جرائم القرصنة وانتهاك حقوق الملكية الفكرية.

○ جرائم تعطيل الخدمات الإلكترونية (حجب الخدمة).

○ جرائم التجسس الإلكتروني.

◦ جرائم غسل الأموال عبر الإنترنت. وقد أشار وال (Wall, 2007) إلى أن الجرائم الإلكترونية تمثل تحولاً في طبيعة الجريمة في عصر المعلومات، حيث تتجاوز الحدود الجغرافية التقليدية وتستغل البنية التحتية الرقمية العالمية.

• **الخصائص المميزة للجرائم الإلكترونية:** تتميز الجرائم الإلكترونية بخصائص عدة تجعلها تختلف عن الجرائم التقليدية وتفرض تحديات خاصة على الأنظمة القانونية وجهات إنفاذ القانون:

◦ **الطبيعة العابرة للحدود:** تعد هذه الخاصية من أهم ما يميز الجرائم الإلكترونية، حيث يمكن لمرتكب الجريمة أن يكون متواجداً في دولة معينة بينما يقع تأثير فعله الإجرامي في دولة أو عدة دول أخرى. هذه الخاصية تعقد مسائل الاختصاص القضائي وتتطلب تعاوناً دولياً وثيقاً لتحديد المسؤولية وملاحقة المجرمين (Maras, 2014).

◦ **صعوبة التتبع:** يمتلك مرتكبو الجرائم الإلكترونية القدرة على استخدام تقنيات متطورة لإخفاء هوياتهم ومواقعهم الحقيقية على الإنترنت، مثل استخدام عناوين IP وهمية، والتشفير، والولوج عبر عدة خوادم (Baggili et al., 2022, pp. 45-48). هذه الصعوبة في التتبع تعيق بشكل كبير جهود التحقيق وتحديد هوية الجناة.

◦ **الطبيعة الرقمية للأدلة:** تعتمد الجرائم الإلكترونية بشكل أساسي على الأدلة الرقمية التي يتم إنتاجها أو تخزينها أو نقلها عبر الوسائل الإلكترونية. هذه الأدلة قد تكون في شكل رسائل بريد إلكتروني، أو سجلات بيانات، أو صور ومقاطع فيديو رقمية، أو غيرها. طبيعة هذه الأدلة الرقمية تجعلها عرضة للتغيير أو الحذف بسهولة، كما أنها تتطلب خبرات فنية متخصصة في جمعها وتحليلها وتقديمها أمام المحاكم. وقد أكد كشتري وفواس (Voas, 2020, p. 112 & Kshetri) على أن هذه الطبيعة الرقمية للأدلة تفرض تحديات على طرق الإثبات التقليدية.

ثانياً: الإثبات الجنائي: مفهومه وأهميته في القانون

يُعد الإثبات الجنائي من أهم فروع الإجراءات الجنائية، حيث يهدف إلى إقامة الدليل القاطع على ارتكاب جريمة ونسبتها إلى متهم معين.

- **تعريف الإثبات الجنائي ومصادره:** يُمكن تعريف الإثبات الجنائي بأنه إقامة الدليل أمام القضاء بالطرق القانونية على وقوع الجريمة وعلى نسبتها إلى المتهم (مصطفى، 2021، ص. 15).
- تتعدد مصادر الإثبات الجنائي لتشمل:
 - **شهادة الشهود:** أقوال الأشخاص الذين شاهدوا الواقعة أو لديهم معلومات عنها.
 - **اعتراف المتهم:** إقرار المتهم بارتكاب الجريمة.
 - **الأدلة المادية:** الأشياء التي تم استخدامها في ارتكاب الجريمة أو نتجت عنها.
 - **القرائن:** الظروف أو الوقائع التي يستنتج منها القاضي وقوع الجريمة أو نسبة ارتكابها إلى المتهم.
 - **الخبرة الفنية:** رأي الخبراء المتخصصين في مجال معين يتعلق بالجريمة.
 - **الأدلة الرقمية:** المعلومات والبيانات الإلكترونية التي لها صلة بالواقعة الإجرامية، والتي أصبحت مصدراً مهماً للإثبات في قضايا الجرائم الإلكترونية وغيرها.
- **مبادئ الإثبات الجنائي الأساسية:** تحكم عملية الإثبات الجنائي مجموعة من المبادئ الأساسية التي تهدف إلى ضمان تحقيق العدالة وحماية حقوق الأفراد، من أهمها:
 - **مبدأ افتراض البراءة:** المتهم بريء حتى تثبت إدانته بدليل قاطع.
 - **مبدأ عبء الإثبات:** يقع عبء إثبات الاتهام على عاتق النيابة العامة.
 - **مبدأ اليقين القضائي:** يجب أن يبنى القاضي حكمه بالإدانة على درجة عالية من اليقين لا يرقى إليها الشك المعقول.
 - **مبدأ حرية القاضي في تقدير الأدلة:** للقاضي سلطة تقدير قيمة الأدلة المقدمة إليه والأخذ بما يقتنع به.
 - **مبدأ حجية الشيء المحكوم به:** الحكم القضائي البات له حجية تمنع إعادة نظر الدعوى.
- **أهمية الإثبات الجنائي في تحقيق العدالة:** يمثل الإثبات الجنائي الركيزة الأساسية التي تقوم عليها العدالة الجنائية. فمن خلال تقديم أدلة قوية وموثوقة، يتمكن القضاء من كشف الحقيقة وتحديد المسؤولية الجنائية وإنزال العقاب العادل على مرتكبي الجرائم. وبدون إثبات، يصبح من المستحيل محاسبة المجرمين وحماية حقوق الضحايا والمجتمع بشكل عام.

طريقة الدراسة وإجراءاتها

أولاً: منهج الدراسة

تعتمد الدراسة الحالية على **المنهج الوصفي التحليلي المقارن**. يتم اختيار هذا المنهج لأنه الأنسب لطبيعة الدراسة التي تهدف إلى وصف وتحليل وتقييم ومقارنة الإطار القانوني للإثبات الجنائي في الجرائم الإلكترونية بين النظامين القانونيين السعودي والمصري.

- **المنهج الوصفي:** سيتم من خلال هذا المنهج وصف وتحليل النصوص القانونية ذات الصلة بالإثبات الجنائي في الجرائم الإلكترونية في كل من المملكة العربية السعودية وجمهورية مصر العربية. سيشمل ذلك وصفاً لأهم القوانين واللوائح والأنظمة التي تنظم هذا المجال في كلا البلدين.

- **المنهج التحليلي:** سيتم استخدام هذا المنهج في تحليل محتوى النصوص القانونية والمؤلفات العلمية والدراسات السابقة المتعلقة بموضوع الدراسة. سيشمل التحليل تحديد المفاهيم الأساسية، واستخلاص أوجه التشابه والاختلاف، وتقييم مدى فعالية الأطر القانونية والإجرائية القائمة.

- **المنهج المقارن:** يعتبر هذا المنهج محورياً في الدراسة، حيث سيتم استخدامه لمقارنة وتحليل أوجه التشابه والاختلاف بين النظامين القانونيين السعودي والمصري في مجال الإثبات الجنائي للجرائم الإلكترونية. سيتم التركيز على مقارنة المصادر القانونية، وإجراءات جمع الأدلة، وشروط حجية الأدلة الرقمية، والتحديات التي تواجه القضاء في هذا المجال في كلا البلدين. يتوافق هذا المنهج بشكل كبير مع سياق الدراسة، حيث أن الهدف الأساسي هو فهم وتحليل ومقارنة الأطر القانونية القائمة في دولتين مختلفتين بهدف تحديد نقاط القوة والضعف واقتراح سبل للتطوير.

ثانياً: مصادر جمع البيانات

ستعتمد الدراسة الحالية في جمع بياناتها على مصدرين رئيسيين:

- **مصادر البيانات الثانوية:** تعتبر المصدر الأساسي لجمع البيانات في هذه الدراسة. وتشمل:
 - **التشريعات والقوانين:** سيتم الرجوع إلى النصوص القانونية المتعلقة بالإثبات الجنائي والإجراءات الجنائية ومكافحة جرائم تقنية المعلومات في المملكة العربية السعودية وجمهورية مصر العربية.

- المؤلفات والدوريات العلمية: سيتم الاستعانة بالكتب والمقالات العلمية المحكمة والدراسات المنشورة في المجالات العلمية المتخصصة في القانون الجنائي، والقانون الإجرائي، والقانون التقني، والأمن السيبراني، سواء باللغة العربية أو الإنجليزية.
- الدراسات السابقة والبحوث الأكاديمية: سيتم مراجعة الرسائل العلمية (ماجستير ودكتوراه) والبحوث والدراسات السابقة ذات الصلة بموضوع الدراسة، والتي تناولت جوانب الإثبات الجنائي في الجرائم الإلكترونية في البيئات العربية والغربية.
- تقارير المؤتمرات والندوات: سيتم الاطلاع على التقارير الصادرة عن المؤتمرات والندوات العلمية التي تناولت موضوع الجرائم الإلكترونية والإثبات الرقمي.
- مصادر البيانات الأولية: قد يتم اللجوء إليها بشكل محدود عند الحاجة إلى توضيح بعض الجوانب أو الحصول على معلومات إضافية غير متوفرة في المصادر الثانوية، وذلك من خلال:
- مقابلات مع خبراء وممارسين قانونيين: قد يتم إجراء مقابلات منظمة أو غير منظمة مع قضاة ومحامين وأكاديميين متخصصين في القانون الجنائي والإثبات الرقمي في المملكة العربية السعودية وجمهورية مصر العربية لفهم وجهات نظرهم وتجاربهم العملية.

ثالثاً: إجراءات الدراسة

- ستتبع الدراسة الإجراءات التالية في جمع البيانات وتحليلها وتفسيرها:
1. جمع البيانات: سيتم البدء بجمع شامل ومنظم للبيانات الثانوية من المصادر المذكورة أعلاه، مع التركيز على حداثة المصادر ومدى موثوقيتها. سيتم تنظيم هذه البيانات وتصنيفها حسب الموضوع والنظام القانوني (السعودي والمصري).
 2. تحليل البيانات: سيتم تحليل النصوص القانونية والمؤلفات العلمية والدراسات السابقة بشكل تفصيلي باستخدام أدوات التحليل القانوني والمقارن. سيشمل ذلك تحديد المفاهيم الأساسية، واستخلاص الأفكار الرئيسية، ومقارنة الآراء والنتائج.
 3. تفسير البيانات: سيتم تفسير البيانات التي تم تحليلها في ضوء أهداف الدراسة وتساؤلاتها. سيتم التركيز على فهم أوجه التشابه والاختلاف بين النظامين القانونيين، وتقييم فعالية الأطر القانونية والإجرائية، وتحديد التحديات المشتركة.

4. مناقشة البيانات: سيتم مناقشة النتائج التي تم التوصل إليها في ضوء الإطار النظري والدراسات السابقة، وسيتم الربط بين النتائج والإجابة على تساؤلات الدراسة. كما سيتم تقديم توصيات بناءً على نتائج التحليل والمناقشة.
5. توثيق البيانات: سيتم توثيق جميع المصادر التي تم الاستعانة بها في الدراسة بدقة وأمانة وفق نظام APA (الإصدار السابع) سواء في متن الدراسة أو في قائمة المراجع.

المراجع:

أولاً: المراجع العربية

- أبو العلا، أ. س. (2024). **المواجهة الجنائية لمخاطر تقنية الديب فيك DEEP FAKES وأثرها على حجية الأدلة الرقمية في الإثبات الجنائي - دراسة تحليلية مقارنة.**
- أحمد شوقي علي يوسف. (2024). **الجوانب الإجرائية والموضوعية للإلكترونية القضاء في القانون الإجرائي المعاصر في ضوء التحول الرقمي وإنجاز العدالة. مجلة العلوم القانونية والاقتصادية، 14(2)، 217-252.**
- آل طالب، س. (2025، 10 يناير). **حجية الدليل الرقمي في الإثبات. شركة د. سعود آل طالب للاستشارات القانونية.**
- جمعة، ن. ب. ع. (2023). **الدليل الجنائي الرقمي في تقنية الميتافيرس. مجلة العلوم الأمنية والتدريب، 40(80)، 159-189.**
- سهل للمحاماة. (2022). **حجية الدليل الرقمي في الإثبات في السعودية.**
- شرف الدين، و. (2021). **إجراءات جمع الأدلة الرقمية طبقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات. مجلة الباحث للدراسات القانونية والقضائية، 19(01)، 93-118.**
- فخري، ت. ع. ا. (2022). **حجية الدليل الرقمي في الإثبات الجنائي. مجلة الشفافية للدراسات القانونية والاقتصادية، 11(4)، 270-294.**
- قانون الإجراءات الجنائية (مصر).
- قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات. **الجريدة الرسمية.**
- مبروك، م. ك. (2024، يونيو 11). **ملاحح حول الفقه الإسلامي ودوره في النظام القانوني المصري. حوارات الشريعة والقانون.**
- مصطفى، أ. م. (2021). **أصول الإثبات في المواد الجنائية. دار النهضة العربية.**

- المعلم، س. م.، والكربي، ب. خ. (2024). تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي (دراسة تحليلية). *مجلة البحوث الفقهية والقانونية*، 46(46)، 3227-3328.
 - نظام الإثبات الصادر بالمرسوم الملكي رقم م/43 وتاريخ 11/05/1443هـ. *الجريدة الرسمية*.
 - نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 وتاريخ 08/03/1428هـ. *الجريدة الرسمية*.
 - ويس، م.، وارسلان، ع. ك. (2022). *الدليل الرقمي وحجته في الإثبات الجنائي*. المركز القومي للإصدارات القانونية.
- ثانياً: المراجع الأجنبية:
- Alassaf, F. S.& , Aljadani, S. S. (2023). Digital evidence in Saudi law: A comparative study. *International Journal of Law and Politics Studies* 64-48 , (2)5 ,.
 - Alqahtani, M. (2023). The effectiveness of Saudi Arabia's anti-cybercrime law in deterring cybercrimes: An empirical study. *International Journal of Cyber Criminology* 41-25 , (1)17 ,.
 - Alzahrani, A. J.& , Goodwin, R. (2020). Cybercrime legislation in Saudi Arabia: A critical analysis. *Journal of Law, Technology & Society* 62-45 , (1)1 ,.
 - Ayers, R.& , Brothers, S. (2015). *Collecting and Preserving Digital Evidence*. ResearchGate.
 - Baggili, I., Behzadan, V.& , Tariq, M. U. (2022). Digital forensics in the age of the Internet of Things (IoT). *Forensic Science International: Digital Investigation* , 201280 ,40.
 - Egyptian Cybercrime Law No. 175 of 2018. (2018). *Official Gazette*.
 - Eid, Y. M. (2022). The role of digital forensics in combating cybercrime in Egypt. *International Journal of Computer Science and Network Security* -30 , (5)22 , 37.

- Faqi Hussein, S. G. (2011). **Computer Evidence and its Authenticity in Criminal Evidence – A Comparative Study**. Dar Al-Kutub Al-Qanuniya.
- Goodman, M.& , Brenner, S. W. (2002). The technology of organized crime. In F. Schmallegger (Ed.), **Criminal justice today: An introductory text for the 21st century** (7th ed., pp. 388–413). Prentice Hall.
- ITU. (2012). **Understanding cybercrime: Phenomena, challenges and the global response**. International Telecommunication Union.
- Kamal, S.& , Ibrahim, N. (2023). A comparative study of cybercrime laws in the Arab region. **Arab Law Quarterly**23-1 ,(1)37 ,.
- Kanoujiya, M. (2021). A STUDY OF DIGITAL EVIDENCES WITH RESPECT TO CYBER FORENSICS. **Burnished Law Journal**8-1 ,(3)2 ,.
- Kshetri, N.& , Voas, J. (2020). Financial crimes in the dark web. **Journal of Financial Crime**122-111 ,(1)27 ,.
- Kumar, A.& , Sharma, S. (2021). **Digital Evidence Admissibility in Indian Courts: Bridging Legal Gaps in the Age of Cybercrime**. Vintage Legal.
- Maras, M. H. (2014). **Cybercriminology**. Oxford University Press.
- Maras, M. H. (2016). **Digital forensics**. Jones & Bartlett Learning.
- Saudi Anti-Cyber Crime Law. (2007). **Royal Decree No. M/177**.
- Stoykova, A. (2022). **Digital Evidence**. University of Groningen.
- UNODC. (2014). **Cybercrime Module 6 Key Issues: Digital Evidence Admissibility**. UNODC's Sherlock.
- Wahdan, M. A.& , El-Sayed, M. H. (2021). Challenges of digital evidence admissibility in Egyptian criminal proceedings. **Ain Shams Law Review**–1 ,(2)8 , 25.
- Wall, D. S. (2007). **Cybercrime: The transformation of crime in the information age**. Polity Press.

- Wilson, C. (2008). **Cybercrime: A reference handbook**. ABC–CLIO.
- Zeadally, S.& , Ibrahim, A. (2024). Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence. ResearchGate.