التحديات الإجرائية المتعلقة بقبول الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي في المجال الجنائي

الباحثة/ غادة بنت أحمد بن سالم البلوي

حاصلة على درجة الماجستير في القانون الجنائي والعلوم الجنائية- جامعة نايف العربية للعلوم الأمنية

تحت إشراف،،،

أ.د. علي مصطفى الأمين جبر

(أستاذ مساعد القانون الجنائي بجامعة نايف العربية للعلوم الأمنية)

(ISSN: 2537- 0758)

التحديات الإجرائية المتعلقة بقبول الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي في المجال الجنائي

الباحثة/ غادة بنت أحمد بن سالم البلوي

الملخص:

تناولت هذه الدراسة التحديات الإجرائية المرتبطة بقبول الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي في المجال الجنائي. وتهدف الدراسة إلى توضيح الإطار المفاهيمي للأدلة الرقمية وتقنيات الذكاء الاصطناعي، مع تحليل الضوابط القانونية والإجرائية لجمعها، وتقييم دور الخبير الرقمي في تحقيق موثوقية الأدلة، ومن ثمَّ إبراز سلطة القاضي الجنائي في قبولها وتقديرها. واستخدمت الدراسة المنهج الوصفي والتحليلي، وتوصلت الدراسة إلى نتائج من أهمها أن الأدلة الرقمية المستخلصة بواسطة الذكاء الاصطناعي تُعد أداة فعالة في الإثبات الجنائي إذا ما تم جمعها وتحليلها وفق ضوابط قانونية صارمة تضمن أصالتها ومصداقيتها وكفاءتها، كما تبين أن الذكاء الاصطناعي يسهم في تحسين الأداء الجنائي، لا سيما في مجالات الوقاية من الجرائم وتحليل الأدلة، إلا أن استخدامه يتطلب إطارًا قانونيًا يحمي حقوق الأفراد ويصون خصوصياتهم. وأكدت الدراسة أهمية دور الخبير الرقمي كجهة فنية محايدة في تقديم تقارير تدعم العدالة، وسلطت الضوء على السلطة التقديرية للقاضي في قبول الأدلة الرقمية بناءً على معايير قانونية واضحة. وأوصت الدراسة بوضع نصوص في نظام الإجراءات الجزائية مختصة بتنظيم جمع الأدلة الرقمية باستخدام تقنيات الذكاء الاصطناعي، مع وضع إطار قانوني لتنظيم استخدام تقنيات الذكاء الاصطناعي في جمع الأدلة الرقمية، وتحديد المسؤوليات القانونية لكل الأطراف المعنية.

الكلمات المفتاحية: الأدلة الرقمية، الذكاء الاصطناعي، المشروعية القانونية، الإجراءات الجنائية، الخبير الرقمي، القاضي الجنائي.

Abstract:
This study examines the procedural challenges associated with the admissibility of digital evidence extracted using artificial intelligence (AI) technologies in criminal proceedings. The study aims to clarify the conceptual framework of digital evidence and AI technologies, analyze the legal and procedural safeguards for their collection, evaluate the role of digital forensic experts in ensuring the reliability of evidence, and highlight the discretionary authority of criminal judges in admitting and evaluating such evidence. The study adopts a descriptive and analytical methodology. It concludes that digital evidence extracted through AI technologies serves as an effective tool in criminal proof if collected and analyzed under strict legal standards ensuring its authenticity, credibility, and relevance. The findings also reveal that AI enhances criminal justice performance, particularly in crime prevention and evidence analysis. However, its use necessitates a legal framework that protects individual rights and preserves privacy. The study emphasizes the critical role of digital forensic experts as impartial entities in providing reports that support justice and highlights the discretionary power of judges to admit digital evidence based on clear legal standards. The study recommends establishing a specialized procedural framework to regulate the collection of digital evidence using AI technologies, raising awareness about the risks of misusing such technologies, and clearly defining the legal responsibilities of all stakeholders.

Keywords: Digital Evidence, Artificial Intelligence, Legal Admissibility, Criminal Procedures, Digital Forensic Expert, Criminal Judge**.**

(ISSN: 2537- 0758)

المقدمة

يعد قبولُ الأدلةِ الرقميةِ المستخلصةِ باستخدامِ تقنياتِ الذكاءِ الاصطناعي من القضايا القانونية المُعَقَّدة التي تطرحُ العديدَ من التحدياتِ الإجرائية، وتتضمن أولاً مشروعيةَ استخدام هذه التقنيات في استخلاص الأدلة الرقمية، وثانيًا مشروعيةَ الإجراءاتِ المتَّبَعةِ لجمعِ الأدلة، إذ يتطلب قبولُ هذه الأدلةِ الامتثالَ لإجراءاتٍ قانونيةٍ صارمةٍ تضمنُ عدمَ انتهاكِ حقوقِ الأفراد، وخصوصياتهم، كما أن مشروعيةَ استخدام تقنيات الذكاء الاصطناعي ترتبط ارتباطًا وثيقًا بضمان نزاهة الأدلة وعدم التلاعب بها، مما يجعلها أدلة قانونية يُعتد بها أمام المحاكم.

وعليه؛ تُعدُّ الشريعةُ الإسلاميةُ في طليعةِ الأنظمةِ التي أكدت على حماية خصوصية الأفراد من أي انتهاك، مشيرة إلى أن أي تدخل غير مشروع في هذه الخصوصية يُعد محظورًا، لذا؛ فإن الشريعة الإسلامية تشكّل أساسًا قويًّا لقياس مشروعية استخدام تقنيات الذكاء الاصطناعي لاستخلاص الأدلة الرقمية، بما يحقق التوازن بين الكشف عن الجرائم، وحماية حقوق الأفراد.

كما اعتمدت التشريعات؛ سواءً على الصعيد الدولي، أو المحلي، قوانين لحماية حقوق الأفراد من تأثيرات تقنيات الذكاء الاصطناعي، إذ نصّت التشريعات الدولية على معاييرَ لحمايةِ الخصوصية، في حين تبنَّت المملكة العربية السعودية قوانينَ مثل: نظام حماية البيانات الشخصية، ونظام مكافحة الجرائم المعلوماتية لضمان استخدام البيانات بطرق قانونية، وحماية الأفراد من انتهاك حرياتهم.

ويُعد نظامُ الإجراءاتِ الجزائيةِ السعودي من أبرزِ الأنظمةِ التي تضمنُ مشروعيةَ جمعِ الأدلةِ الرقمية، حيث يُشترط اتباعُ إجراءاتٍ قانونيةٍ محددةٍ بدقة لضمان قانونية الأدلة، مع التأكيد على أن أي مخالفة لهذه الإجراءات تؤدي إلى بطلان الدليل واستبعاده.

وأما ما يتعلقُ بالسُّلْطَةِ القضائيةِ، فإن القاضي يتمتعُ بسُلْطَةٍ تقديريةٍ واسعةٍ في قبولِ الأدلة الرقميةِ المستخلصةِ باستخدام الذكاء الاصطناعي، حيث يعتمد في قراره على تقييم مشروعية الإجراءات المُتَّبَعَة في جَمْعِ الأدِلَّة، وهذه السلطةُ تتيحُ له قبولَ الأدلةِ بشكلٍ كاملٍ، أو جزئيٍّ، أو رفضها بناءً على قناعاته الشخصية، ومدى التزامها بالضوابط القانونية.

مشكلة الدراسة:

لقد أصبحت تقنيات الذكاء الاصطناعي– في ضوء التطور التقني والعلمي السريع– تؤدي دورًا مهمًّا في استخلاص الأدلة الرقمية من مصادر عديدة، وبالرغم من أن هذه التقنيات تسهم في الكشف عن مرتكبي الجرائم، إلا أن مشروعية استخدامها تمثل منعطفًا حساسًا حول تأثيرها على حقوق الأفراد وخصوصياتهم، إلى جانب الإجراءات المتعلقة بكيفية الحصول على الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي تعكس مسألة بالغة الأهمية، إذ إن أي إخلال، أو تجاوز في الإجراءات المتبعة قد يؤدي إلى بطلان الدليل الرقمي وعدم قبوله أمام القضاء.

ومن هنا تبرز إشكاليةُ الدراسةِ في ضرورةِ توضيح كيفية ضمان مشروعية استخدام تقنيات الذكاء الاصطناعي لحماية حقوق الأفراد، وأهمية اتباع الإجراءات القانونية المتعلقة بالحصول على الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي، وأن أي إخلال بها قد يهدد مقبولية الأدلة الرقمية أمام القضاء، مما يدعو إلى **السؤال الرئيسي** التالي: **ما هي التحديات الإجرائية المتعلقة بقبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي؟**

تساؤلات الدراسة:

ينبثق من السؤال الرئيسي عدد من التساؤلات الفرعية الآتية:

- ما هو تعريف الأدلة الرقمية والذكاء الاصطناعي في السياق القانوني؟، وكيف تؤثر استخدام تقنيات الذكاء الاصطناعي في استخلاص الأدلة الرقمية على حقوق الأفراد في الخصوصية؟.
- ما هي الضوابط الإجرائية للحصول على الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي؟، وهل يمكن للقاضي أن يمارس سلطته القانونية في قبول وتقدير الأدلة المستخلصة باستخدام تقنيات الذكاء الاصطناعي؟.

أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

- فهم طبيعة الأدلة الرقمية والذكاء الاصطناعي.
- دراسة المشروعية القانونية لاستخدام تقنيات الذكاء الاصطناعي.

(ISSN: 2537- 0758)

- بيان ضوابط الحصول على الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي
- معرفة سلطة القاضي في قبول وتقدير الأدلة الرقمية المستخلصة من الذكاء الاصطناعي.

أهمية الدراسة:

تبرز أهميةُ الدراسةِ في فهمِ الإجراءاتِ القانونيةِ المُتَّبَعَة للحصول على الأدلَّةِ الرقميةِ المستخلصة باستخدام تقنيات الذكاء الاصطناعي، إلى جانب ضمان مشروعية استخدام هذه التقنيات بما يتماشى مع حقوق الأفراد وحماية حرياتهم، ومن ثم بيان مدى سلطة القاضي في تقدير هذه الأدلة، إذ تتجسد أهمية الدراسة في جانبيها العلمي والعملي والتي تتجلى فيما يلي:

الأهمية العلمية: تتمثل الأهمية العلمية لهذه الدراسة في استكشاف مشروعية استخدام تقنيات الذكاء الاصطناعي واستخلاص الأدلة الرقمية لضمان احترام حقوق الأفراد، وحمايتها من انتهاك الخصوصية، أو المراقبة غير القانونية، كما أنها تسهم في إثراء الفهم القانوني حول ضرورة اتباع الإجراءات القانونية اللازمة للحصول على الأدلة الرقمية المستخلصة بالذكاء الاصطناعي، واستنادًا إلى ذلك، يتبين أن الدراسة تسهم في تحقيق التوازن بين التكنولوجيا وحقوق الأفراد في مجال القضاء الجنائي، مما يجعل هذا الموضوع من أهم وأحدث القضايا في هذا المجال.

الأهمية العملية: تبرز الأهمية العملية للدراسة في تقديم حلول وإجراءات قانونية تسهم في ضمان استخدام تقنيات الذكاء الاصطناعي بشكل مشروع، وتحديد الضوابط الإجرائية لاستخلاص الأدلة الرقمية، كما أنها تساعد في زيادة الوعي بالقانون لدى المختصين في مجال الإثبات الجنائي، من قضاة، وأصحاب الحقوق في معرفة الضمانات الإجرائية اللازمة، للدفاع عن أنفسهم، كما تفيد المحامي في تقديم دفاع موكله مسترشدًا بالمعايير القانونية المتبعة.

منهج الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي والتحليلي، حيث تم جمع المعلومات والحقائق المتعلقة بالتحديات الإجرائية في قبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي، ومن خلال المنهج الوصفي تم تسليط الضوء على القواعد والأحكام

القانونية ومدى فاعليتها، وتطبيقها، أما المنهج التحليلي فقد استُخدم لفحص مدى كفاية هذه القواعد في مواجهة التحديات القانونية والإجرائية المعقدة، وذلك بهدف تقييم قدرتها في سياق قبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي.

خطة الدراسة:

تتضمن الدراسة مبحثين رئيسيين، ولكل مبحث مطلبان ثم الخاتمة وذلك على التالي:

المبحث الأول: ماهية الأدلة الرقمية المستخلصة من الذكاء الاصطناعي.

المطلب الأول: الإطار المفاهيمي للأدلة الرقمية والذكاء الاصطناعي.

المطلب الثاني: المشروعية القانونية لاستخدام تقنيات الذكاء الاصطناعي.

المبحث الثاني: حجية الأدلة الرقمية المستخلصة بواسطة الذكاء الاصطناعي.

المطلب الأول: ضوابط الحصول على الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي.

المطلب الثاني: سلطة القاضي الجنائي في قبول وتقدير الأدلة الرقمية المستخلصة بالذكاء الاصطناعي.

الخاتمة: وتتضمن أهم النتائج والتوصيات.

المبحث الأول
ماهية الأدلة الرقمية المستخلصة من الذكاء الاصطناعي

تمهيد:

مع التقدم الهائل في مجالات التكنولوجيا فقد أصبحت تقنيات الذكاء الاصطناعي تمثل واحدة من أهم الابتكارات وأكثرها تأثيرًا في مجال التحقيقات الجنائية والقانونية، حيث أصبح هناك ازدياد في الاعتماد على التكنولوجيا في شتى القطاعات والمجالات، فبرز الذكاء الاصطناعي كأداة قوية تساهم بشكل فعال في استخلاص، وجمع، وتحليل البيانات والمعلومات الرقمية بطرق دقيقة وفعالة.

وبفضل الله ثم بفضل قدرات الذكاء الاصطناعي المتقدمة في معالجة كميات هائلة من البيانات والمعلومات وتحليلها في وقت قياسي، أصبح بالإمكان اكتشاف روابط خفية بين الأدلة الرقمية المتعلقة بالجرائم، وعلى سبيل المثال لا الحصر، الدليل المستخلص

(ISSN: 2537- 0758)

من الكاميرات الرقمية، والذي يمكن أن يكشف عن تفاصيل دقيقة تتعلق بالجريمة الواقعة، أو الأصوات المنقحة والمحسنة باستخدام تقنيات الذكاء الاصطناعي، مما يمكّن الجهات المختصة من نسبها إلى المتهم، وهذه التقنيات تحلل تفاصيل يصعب على القدرات البشرية التقليدية الوصول إليها.

وتعد الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي من أبرز العوامل التي تعمل على تقديم رؤى متكاملة وعميقة حول الأنشطة والسلوكيات المختلفة للأفراد والأنظمة، مما يسهم بشكل كبير في تعزيز قدرات المحققين على كشف الجرائم، وتحليل الأنماط السلوكية، والتمكن من استخلاص نتائج دقيقة تستند إلى الأدلة الرقمية التي تمت معالجتها وتحليلها وفق أسس علمية متينة، وهذا يعني أن النتائج التي يتم التوصل إليها غير مبنية على تخمينات، أو افتراضات، بل تعتمد على أدلة رقمية تم جمعها وتحليلها بعناية، بحيث يمكن تقديمها أمام القضاء باعتبارها أدلة موثوقة يعتد بها.

واستنادًا على هذه الأهمية المتزايدة، فإنه سيتم في هذا المبحث تناول موضوع الأدلة الرقمية المستمدة من الذكاء الاصطناعي، وذلك من خلال تقسيمه إلى مطلبين رئيسيين:

نستعرض في **المطلب الأول:** الإطار المفاهيمي للأدلة الرقمية والذكاء الاصطناعي.

نتناول في **المطلب الثاني:** المشروعية القانونية لاستخدام تقنيات الذكاء الاصطناعي.

المطلب الأول
الإطار المفاهيمي للأدلة الرقمية والذكاء الاصطناعي

إن الأدلة الرقمية هي كل ما يستمد من بيانات تُنتج أو ترسل أو تُخزن أو تستقبل من وسائل رقمية، وتكون قابلة للاسترجاع، أو الحصول عليها بطريقة يمكن فهمها، حيث توفر هذه الأدلة معلومات وبيانات دقيقة تساهم في الكشف عن الجريمة، مما يجعلها ركيزة أساسية في الإثبات الجنائي، وفي هذا السياق يشكل الذكاء الاصطناعي تطورًا نوعيًا من خلال قدرته على تحليل البيانات الضخمة لدعم عمليات التحقيق والاستنتاج، وبناءً على ما تقدم سوف نتناول في هذا المطلب فرعين رئيسيين حيث يستعرض **الفرع الأول** طبيعة الأدلة الرقمية، ويركز **الفرع الثاني** على مفهوم الذكاء الاصطناعي.

الفرع الأول
طبيعة الأدلة الرقمية

يعد الدليل الرقمي ذو طبيعة رقمية ثنائية وهو أمر يحدث عن طريق نظام الثنائي الرقمي (٠) و(١)، وهو النموذج الذي يسجل جميع البيانات والمعلومات من رموز، وأشكال، وحروف، وألوان، وأصوات، وغيرها داخل الوسيلة الرقمية، فجميع مدخلات ومخرجات الوسائل الرقمية تتمثل في (٠) و(١) حيث يتم إدخالها كمعلومات في تلك الوسائل الرقمية ويتم تحويلها إلى النظام الرقمي، فإن الدليل بهذه الحالة يعتبر برمجية الأجهزة، سواءً كانت هواتف ذكية، أو حواسيب، أو من تقنيات الذكاء الاصطناعي، أو غيرها[١].

فإن البيئة التي يتواجد بها الدليل الرقمي هي البيئة الرقمية أو الفضاء السيبراني، وعلى سبيل المثال لو تم الاحتفاظ بصور أو مقاطع مستمدة من كاميرات المراقبة، أو بملفات تحتوي على أرقام دخول سرية للمواقع فإنه يعد دليل رقمي، فبالرغم من تنوع واختلاف هيئات الدليل الرقمي، وأشكاله؛ إلا أن طبيعته واحدة، وهي علاقته الوثيقة بتكنولوجيا المعلومات، وأنه يتكون من رقمي (٠) و(١)، علمًا أن هذه الطبيعة تؤثر على حجم الملف وتكوينه[٢].

ويجدر التنويه إلى أن تنوع أشكال وأنواع الأدلة الرقمية لا يعني أن جميعها تم الحصول عليه من مصدر واحد، بل هناك العديد من الوسائل المختلفة التي يُستخلص منها الدليل الرقمي، ومن بين هذه الوسائل تقنية الذكاء الاصطناعي، وهي الوسيلة الرقمية محل الدراسة.

---

(١) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦م، ص٢٢.

(٢) عمر محمد أبو بكر ابن يونس، الإجراءات الجنائية عبر الإنترنت، في ترجمة المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا للدليل الالكتروني في التحقيقات الجنائية، بدون دار نشر، ٢٠٠٤م، ص٩٩٥.

(ISSN: 2537- 0758)

أولًا: **تعريف الأدلة لغة واصطلاحاً**:

- **الأدلة لغة:** جمع دليل، ويقال دلَّه على الطريق؛ أي علّمه على الطريق، وهو المرشد الذي يستدل به(٣).
- **الأدلة اصطلاحًا:** هو ما يستدعي الإلمام به كنتيجة؛ وذلك لأن إدراكه مرتبط بالعلم بشيء آخر يؤدي إليه أو يؤثر عليه(٤).

ثانياً: **تعريف الرقمية لغة واصطلاحاً**.

- **الرقمية لغةً:** اسم مؤنث يعود إلى الرقم، والرقميّة مصدرها من الرَّقم، وهو في اللغة من رقمت الشيء أي ميزته بعلامة عن غيره(٥)، ولغة رقمية: لغة مبرمجة وفق قواعد محددة خصيصًا ليتم استخدامها في تشغيل الحاسبات الإلكترونية(٦).
- **الرقمية اصطلاحًا:** الرقمية هو مصطلح يشير إلى الطرق التي تخزن وتنقل البيانات والمعلومات مثل: المعلومات الصوتية، أو الكتابية، أو الفيديو عن طريق جهاز الكمبيوتر والشبكة الإلكترونية، من خلال أجهزة رقمية تقوم بتحويل تلك المعلومات والبيانات إلى أرقام وتخزنها بالذاكرة، مما يسهل معالجة البيانات ونقلها(٧).

---

(٣) جمال الدين بن مكرم ابن منظور، لسان العرب، دار إحياء التراث، بيروت، ١٩٨٨م، ص٢٤٨.

(٤) السيد محمد حسن الشريف، "النظرية العامة للإثبات الجنائي"، رسالة دكتوراة، جامعة القاهرة، مصر، ٢٠٠٢م، ص١٢٩.

(٥) أحمد محمد علي الفيومي، المصباح المنير في غريب الشرح الكبير، المكتبة العلمية، بيروت، (٢٣٦/١) مادة: "رقم".

(٦) أحمد مختار عبد الحميد عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة،١٤٢٩هـ، (٢/ ٩٣٠).

(٧) سعد علي تركي الجلعود، الدليل الرقمي وأثره في الإثبات: دراسة فقهية تطبيقية مقارنة بالنظام السعودي، مجلة العلوم الشرعية، المنظومة، ٢٠٢٤م ص٨٨، تم الوصول إليه في ٢٠٢٤/٩/١٢، (http://search.mandumah.com/Record/1449220)

ثالثاً: تعريف الأدلة الرقمية.

يقصد بالأدلة الرقمية هي الأدلة التي تم أخذها من الأجهزة الإلكترونية، على هيئة مجالات كهربائية أو مغناطيسية، ويمكن تجميعها وتحليلها عبر برامج خاصة، لتقديمها كدليل إثبات امام القضاء(٨).

كما تم تعريف الدليل الرقمي بأنه: "عبارة عن معلومات مخزنة في جهاز الحاسب الآلي، يتم جمعها وتحليلها من خلال برامج خاصة لإثبات الجرائم التي وقعت"(٩).

واتجه رأي إلى تعريف الدليل الرقمي بأنه الدليل الذي يتضمن جميع البيانات الرقمية التي يمكن أن تثبت وقوع جريمة، أو تثبت وجود صلة بين الجريمة الواقعة والجاني، أو تربط بين الجريمة والمجني عليه(١٠).

وقد عرَّف المنظم السعودي الدليل الرقمي في نظام الاثبات بأنه: "يعد دليلاً رقميًّا كل دليل مستمد من أي بيانات تنشأ أو تصدر أو تسلم أو تحفظ أو تبلغ بوسيلة رقمية، وتكون قابلة للاسترجاع أو الحصول عليها بصورة يمكن فهمها"(١١).

ويشمل الدليل الرقمي وفقًا لذات النظام على :"السجل الرقمي والمحرر الرقمي، والمحرَّر الرقمي، والتوقيع الرقمي، والمراسلات الرقمية بما فيها البريد الرقمي، ووسائل الاتصال، والوسائط الرقمية، وأي دليل رقمي آخر"(١٢).

ويتضح من خلال هذا التعريف أن المنظم السعودي قد وسع من مفهوم الأدلة الرقمية وانتقل تعريفه من نطاق أجهز الكمبيوتر إلى مجال أوسع، بحيث لم تعد الأدلة الرقمية مقتصرة على ما يستخرج من الحاسب الآلي فقط، بل توسع بقوله "بوسيلة

---

(٨) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت– رسالة ماجستير– ، جامعة الشرق الأوسط للدراسات العليا، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١١م، ص٢٣٠.

(٩) عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠م، ص٦١.

(10) Eoghan Casey, "Digital Evidence and Computer Crime", 3rd Edition, London, Academic Press, 2011, P 33

(١١) نظام الاثبات م/٥٣ بالمرسوم الملكي رقم (م/٤٣) وتاريخ ٢٦/ ٥/ ١٤٤٣هـ.

(١٢) نظام الاثبات م/ ٥٤ بالمرسوم الملكي رقم (م/٤٣) وتاريخ ٢٦/ ٥/ ١٤٤٣هـ.

(ISSN: 2537- 0758)

رقمية"، والوسائل الرقمية ليست محصورة بأجهزة الكمبيوتر، فقد تشمل تقنيات الذكاء الاصطناعي، والهواتف النقالة، والكاميرات الرقمية، وغيرها.

وبناءً على ما سبق، نرى أن تعريف الدليل الرقمي المستخلص من الذكاء الاصطناعي هو: دليل يحتوي على بيانات أو معلومات متوفرة بوسائل رقمية تستخرج من خلال تقنية الذكاء الاصطناعي، سواء كان ذلك الدليل نص مكتوب، أو مرسوم، أو صوت، أو صور، أو فيديو...الخ، والتي يستطيع جمعها وتحليلها عن طريق المختصين بذلك باستخدام تقنيات الذكاء الاصطناعي لتقديمها كدليل إثبات أمام القضاء.

رابعاً: تصنيفات الأدلة الرقمية.

أصبحت الأدلة الرقمية التي تعتمد عليها المحاكم تتزايد وتتنوع، وتشمل الصور والمقاطع الرقمية، والملفات الصوتية المسجلة، ومحتويات ذاكرة الكمبيوتر، ورسائل البريد الالكتروني، والتواريخ المأخوذة من تطبيقات المراسلة الفورية، وغيرها من الأدلة المستمدة من الوسائل الرقمية، **ويمكن تصنيف الأدلة الرقمية كما يلي**[١٣]:

أ- بحسب شكل الدليل: مثل الصور، والفيديوهات، والتسجيلات الصوتية، والنصوص المكتوبة عن طريق وسيلة رقمية، والكوكيز، وسجلات المخدم،

ب- بحسب المصدر الذي تم استخلاص الدليل منه: كتقنيات الذكاء الاصطناعي، والحاسب، والهاتف الخلوي، والشبكات.

ج- بحسب طبيعة البيانات: هل هي ملفات تم حذفها ثم استرجاعها، أم أنها ملفات موجودة أصلًا.

وفيما يتعلق بأماكن البحث عن الدليل الرقمي، يمكن القول إن من أهمها ما يلي[١٤]:

---

(١٣) ميادة مصطفى محمد المحروقي، ذاتية الضوابط الإجرائية للأدلة الرقمية في الأنظمة القانونية ذات الأصل اللاتيني والأنجلو أمريكي، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، كلية الحقوق، الإسكندرية، ٢٠١٩م، ص١٠.

(١٤) محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد ٢١، العدد ٨١، ٢٠١٢م، ص٤٩.

١- **جهاز الحاسب وملحقاته:** يتم استخراج الأدلة الرقمية من جهاز الحاسب مثل تاريخ تصفح الإنترنت، أو مفاتيح سجلات النظام في ويندوز، أو سجلات (Logs)، أو الملفات المحذوفة، بالإضافة إلى الملحقات التي ترتبط بسجلات (log files) والتي تتضمن معلومات ضخمة وتحديدًا بالاستخدام الشخصي للحاسب.

٢- **الأجهزة المحلقة بالحاسوب المتعلقة بالجريمة:** مثل كاميرات المراقبة، والماسحات الضوئية، والطابعات.

٣- **الهواتف الخلوية:** يمكن استخراج الدليل من خلال سجل الرسائل، أو التطبيقات، أو المكالمات.

٤- **الشبكات:** يمكن تحليل البيانات المرسلة عبر الشبكة باستخدام برامج مثل (wire shark).

وفي رأينا أن التصنيف حسب المصدر الذي تم استخراج الدليل الرقمي منه، هو الأنسب في سياق دراستنا، إذ يشمل تقنيات الذكاء الاصطناعي التي تتعامل مع البيانات بشكل خاص، ومن المهم أن يتم تصنيف الأدلة الرقمية المستخلصة عبر هذه التقنيات تحت هذا التصنيف، ومن ذلك على سبيل المثال في حالات بصمات الصوت المستخلصة باستخدام الذكاء الاصطناعي.

أما من جانب أماكن البحث عن الدليل الرقمي فإننا نرى أن الأدلة الرقمية يمكن استخراجها من مصادر مختلفة ومتنوعة، كالحواسيب، والهواتف الخلوية، والكاميرات الرقمية، وغيرها مما سبق ذكرها، كل من هذه الأماكن أو المصادر توفر أدلة قد تكون حاسمة في التحقيقات، مما يلزم التعامل معها بدقة لضمان صحة استخراج الأدلة الرقمية.

خامساً: آليات التعامل مع الأدلة الرقمية.

تعد الأدلة الرقمية من الأدلة العلمية غير الملموسة، وغير المرئية، حيث تختلف عن أي دليل مادي ملموس مثل الأسلحة أو الوثائق الملموسة، فهو يتكون من مجالات مغناطيسية أو كهربائية، وعند جمع وتوثيق الدليل الرقمي، يتم تحويل البيانات من طبيعتها الرقمية (مثل: الصور، والفيديوهات، أو النصوص المخزنة في الحاسوب)، إلى معلومات، ولكن هذا التحويل لا يعني أن الدليل أصبح ماديًا، بل هو ببساطة عملية نقل

(ISSN: 2537- 0758)

هذه البيانات من شكل رقمي إلى شكل يمكن للإنسان فهمه والتعامل معه، وذلك لاستخدامه كدليل إثبات في المحكمة[١٥].

ومن المبادئ التي اعتمدها المؤتمر الدولي المعني بجرائم التكنولوجيا في عام ١٩٩٩ للحفاظ على مقبولية الأدلة الرقمية تتمثل في النقاط التالية[١٦]:

١- **سلامة الدليل:** يلزم اتباع الإجراءات القانونية للحصول على الدليل الرقمي دون تغيير محتواه، لأن أي تغيير في الأدلة الرقمية قد يؤثر على مصداقيتها.

٢- **الإجراءات القانونية:** ينبغي أن يكون الشخص الذي يتولى جمع الأدلة الرقمية، قد تم تكليفه قانونيًا من جهة قضائية، أو من خلال إذن رسمي تطبيقًا للقانون.

٣- **توثيق الأنشطة ذات الصلة بالأدلة:** ضرورة توثيق كل الخطوات التي تم تنفيذها على الأدلة الرقمية، ابتداءً من مصادرتها إلى تخزينها ونقلها، مع ضرورة حفظ هذه الوثائق وتوفيرها للمراجعة مستقبلًا لضمان الشفافية.

٤- **المسؤولية:** كل جهة أو شخص يقوم بإجراء على الأدلة الرقمية، سواءً كان الوصول إليها أو جمعها أو نقلها، يجب أن يتحمل المسؤولية عن ذلك الإجراء وان يلتزم بالمبادئ المذكورة لضمان الحفاظ على شرعية الدليل.

ونرى أن هذا المؤتمر يبرز أهمية الحفاظ على مصداقية الأدلة الرقمية في التحقيقات الجنائية، فإن المبادئ التوجيهية التي اعتمدها المؤتمر تؤكد ضرورة أن تبقى الأدلة الرقمية كما هي دون تأثير أثناء الحصول عليها، بالإضافة إلى أهمية توثيق جميع الإجراءات المتعلقة بمصادرتها أو نقلها، ومن خلال هذه المبادئ، يظهر أن التعامل السليم ضمن إجراءات قانونية صحيحة هو أساس لاستدامة قوة الأدلة الرقمية أمام المحاكم.

وعليه، فإن الأهمية الرئيسية للأدلة الرقمية تكمن في وجوب استيفاء مجموعة من الضوابط، وأهمها هو أن يتم تحصيل تلك الأدلة وفق إجراءات سليمة ووسائل مشروعة،

---

(١٥) علي محمود علي حموده، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، دبي، ٢٦-٢٨ أبريل ٢٠٠٣.

(١٦) ميادة مصطفى المحروقي، مرجع سابق، ص١٣.

فإن مخالفتها قد يؤدي إلى بطلان تلك الأدلة حتى وإن كانت الأدلة نفسها صحيحة، وهذا هو نواة دراستنا.

الفرع الثاني
مفهوم الذكاء الاصطناعي

بالرغم من الزيادة في الاعتماد على تطبيقات الذكاء الاصطناعي في أغلب الأمور، إلا أنه يواجه صعوبة في وضع تعريف عام له، وذلك بسبب التطورات والتغييرات ورفع مستوى أدائه بتوافر كمية من المعلومات والبيانات المتحصل عليها، والتي تعتبر المحرك الأساسي لتطبيقات الذكاء الاصطناعي.

أولًا: **تعريف الذكاء الاصطناعي**.

يوجد العديد من الجهود لتعريف الذكاء الاصطناعي ومنها: "أنه علم حديث نسبيًّا من علوم الحاسب، يهدف إلى ابتكار وتصميم أنظمة الحاسبات الذكية التي تحاكي أسلوب الذكاء البشري نفسه، لتتمكن من تلك الأنظمة من أداء المهام بدلًا من الإنسان ومحاكاة وظائفه، وقدراته، باستخدام خواصه الكيفية، وعلاقتها المنطقية، والحسابية"[١٧].

كما تم تعريف الذكاء الاصطناعي بأنه: "فرع من فروع علوم الكمبيوتر يهتم بدراسة أنظمة الكمبيوتر وتكوينها، والتي تظهر بعض أشكال الذكاء، وتلك الأنظمة لديها القدرة على استخلاص استنتاجات مفيدة حول مشكلة معينة، كما يمكن لهذه الأنظمة فهم الإدراك الحي والقدرات الأخرى التي تحتاج إلى ذكاء إذا تم تنفيذها من قبل البشر"[١٨].

وجاء القول أيضًا على أن الذكاء الاصطناعي هو العلم الذي يهدف إلى تمكين الآلات من القيام بالمهام التي تستدعي الذكاء البشري لتنفيذها، أو أنه العلم الذي يحاول

---

(١٧) عبد الرزاق مختار محمود، تطبيقات الذكاء الاصطناعي، مدخل لتطوير التعليم في ظل جائحة فيروس كورونا، المؤسسة الدولية لآفاق المستقبل، المجلة الدولية للبحوث في العلوم التربوية، المجلد ٣، العدد٤، ٢٠٢٠م، ص١٨٤.

(١٨) شيخ هجيره، دور الذكاء الاصطناعي في إدارة علاقة الزبون الالكتروني للقرض الشعب الجزائري CPA، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد ١٠، العدد ٢، جامعة حسيبة بن بوعلي، الشلف، ٢٠١٨م، ص١٨.

(ISSN: 2537- 0758)

نقل الذكاء البشري إلى الأجهزة، ويكون ذلك من خلال تزويد الآلات ببرامج وقدرات تشبه ذكاء البشر، حتى يمكنه على القيام بعمليات ذكية[١٩].

وثمة تعريف آخر بأن الذكاء الاصطناعي هو: "الذكاء الذي يصنعه الإنسان أو يصنعه في آلة أو كمبيوتر، فهو الذي يصدر عن الإنسان في الأصل ثم يمنحه للآلة أو للحاسوب، وبالتالي فإن الذكاء الاصطناعي هو علم يتم تحديد على أساس هدفه، وهو جعل الآلات تقوم بأشياء تحتاج إلى الذكاء"[٢٠].

وفي ضوء التعريفات السابقة يتبين لنا أنهم اتفقوا على أن الذكاء الاصطناعي هو العلم الذي يتفحص سلوك البشر ويحاكي ذكاء الانسان، وقدراته، والإنسان ذاته هو الذي يمنح الآلة ذلك الذكاء من خلال تطوير البرمجيات بشكل يومي.

ثانياً: أهداف تقنية الذكاء الاصطناعي.

يمكننا تلخيص أهم أهداف تقنية الذكاء الاصطناعي على وجه العموم[٢١]:

١- تحليل وفهم طبيعة الذكاء البشري عبر فك شفرات الدماغ، بهدف محاكاته وجعل الأجهزة أكثر ذكاءً وكفاءة.

٢- إتاحة القدرة للآلات على معالجة المعلومات والبيانات بطريقة تشبه الأسلوب البشري في حل المشكلات، بمعنى التنفيذ المتزامن للعمليات، وهذه الطريقة الأكثر تشابهًا مع أسلوب البشر في حل المشكلات.

ومن وجهة نظرنا نرى أن لكل من العقل البشري والذكاء الاصطناعي نقاط قوة ونقاط ضعف، فإن العقل البشري يتمتع بقدرات فريدة في الإبداع والتفاعل الاجتماعي، بينما الذكاء الاصطناعي يبرع في معالجة البيانات وتحليلها، فإن الذكاء الاصطناعي قد

---

(١٩) عبد الله سعيد عبد الله الوالي، المسؤولية المدنية عن أضرار تطبيقات الذكاء الاصطناعي في القانون الإماراتي، دار النهضة العلمية، دبي، ٢٠٢١م، ص٢٩، وص٢١.

(٢٠) سعد الغالب ياسين، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمّان، ٢٠١٢م، ص١١٤.

(٢١) عايض علي القحطاني، دور الذكاء الاصطناعي في تحقيق التنمية المستدامة في إطار رؤية المملكة العربية السعودية ٢٠٣٠، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، المجلد ٣، القاهرة، ٢٠٢٢م، ص١٠٨ وما بعدها.

اكتسب خصائص الذكاء البشري، والتي كانت مقتصرة على البشر كالتفكير، والتخاطب والتعلم والإبداع، بل وقد حقق نجاحات مذهلة في تحقيق هذه الأهداف إلى الآن، ولكن على الرغم من مزايا تقنية الذكاء الاصطناعي ومحاكاته لقدرات البشر، إلا أنه لن يتفوق على الذكاء البشري الذي أنشأه وطور مهاراته وقدراته.

ثالثاً: مجالات استخدام الذكاء الاصطناعي.

- مجال الأمن والسلامة العامة.

قامت وزارة الداخلية بتبني تقنيات الأنظمة الأمنية الذكية المعتمدة على الذكاء الاصطناعي بهدف تحسين كفاءة المهام الأمنية للأفراد داخل المجتمع، وضبط المخالفات المرورية والأمنية في مختلف مدن ومحافظات المملكة، كما تسهم هذه التقنيات بحماية الممتلكات والأشخاص، وتحسّن من جودة الحياة لكل المواطنين، والمقيمين، والزائرين[٢٢].

- مجال الأبحاث:

تعمل الهيئة السعودية للبيانات والذكاء الاصطناعي "سدايا" على تطوير المشاريع البحثية الوطنية، وتعزيز استراتيجية البحث والابتكار في مجال الذكاء الاصطناعي لدعم الأولويات الوطنية وتحقيق أهدف رؤية المملكة ٢٠٣٠، ومن أبرز مشاريعها مركز الأبحاث المشترك للذكاء الاصطناعي الذي تأسس عام ٢٠٢٢، ويهدف إلى تعزيز مكانة المملكة كمركز عالمي في الاقتصاد المعتمد على البيانات، من خلال الابتكار والتطوير في مختلف فروع الذكاء الاصطناعي بما يتماشى مع احتياجات المملكة ومجالاتها الاستراتيجية[٢٣].

---

(٢٢) وزارة الداخلية المملكة تستعرض أنظمة الذكاء الاصطناعي للأمن العام في معرض سيتي سكيب العالمي بالرياض https://safiu.moi.gov.sa/wps/vanityurl/ar/home: تم الوصول إليه في ٣١/ ١٠/ ٢٠٢٤م.

(٢٣) وزارة الداخلية وسدايا تطلق عدداً من المعسكرات التدريبة في علوم البيانات والذكاء الاصطناعي: https://www.spa.gov.sa/N2013946 تم الوصول إليه في ٢٠٢٤/١١/١م.

(ISSN: 2537- 0758)

- **مجال الصحة:**

تم تأسيس المركز الاصطناعي للصحة في المملكة العربية السعودية عام ٢٠٢١، وذلك لتحقيق التفوق في القطاع الصحي، من خلال تطوير وتنفيذ استراتيجيات البيانات والذكاء الاصطناعي، ويهدف المركز أيضًا إلى تحسين ترتيب المملكة في المؤشرات الدولية المتعلقة بالبيانات والذكاء الاصطناعي، بالإضافة إلى تعزيز استخدام تقنيات الذكاء الاصطناعي والحوسبة السحابية في قطاع الصحة[٢٤].

- **مجال الوقاية من الجريمة:**

تساهم تطبيقات الذكاء الاصطناعي بشكل كبير في مجال الوقاية من الجرائم، حيث يعتمد على تحليل البيانات الضخمة والتعرف على الأنماط لتحديد الأنشطة المشبوهة قبل حدوثها، ومن أبرز الأمثلة على تطبيقات الذكاء الاصطناعي المعتمدة في المملكة العربية السعودية هي استخدام تقنيات التحليل الذكي للقطات المأخوذة من كاميرات المراقبة، وذلك لرصد سلوكيات غير عادية قد تشير إلى احتمالية وقوع هجمات أو سرقات أو غيرها من الجرائم، إذ تساعد هذه التقنيات في اتخاذ تدابير وقائية للحد من وقوع الجرائم بشكل مسبق[٢٥].

وفي تصورنا نرى أن الأدلة الرقمية تستخلص من مجموعة متنوعة من المصادر الذكية، وتتميز بطابعها التقني الذي يختلف اختلافًا جذريًا عن الأدلة التقليدية، مما يجعل هذا الأخير غير كافي لإثبات الجرائم الحديثة، فما الذي يحول دون استخدام تقنيات الذكاء الاصطناعي في استخراج وتحليل هذه الأدلة لطالما كانت تساعد الجهات المختصة على سرعة التطور في مواجهة الجرائم المستحدثة.

---

(٢٤) البراء جمعان محمد الشهري، "استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة"، المجلة العربية للنشر العلمي، رماح، ٢٠٢٤م، ص٨١.

(٢٥) البراء جمعان محمد الشهري، مرجع سابق، ص٨١ وما بعدها.

المطلب الثاني

المشروعية القانونية لاستخدام تقنيات الذكاء الاصطناعي

تعد تقنيات الذكاء الاصطناعي من الوسائل المبتكرة في استخلاص الأدلة الرقمية، حيث تقدم أساليب متقدمة لمعالجة البيانات وتحليلها، ويشمل دور هذه التقنيات قدرتها على استخراج معلومات دقيقة من كميات ضخمة من البيانات، ومع تطور استخدام هذه التقنيات، تبرز الأهمية إلى ضمان مشروعية تطبيقها في إطار النظام في المملكة العربية السعودية وذلك حرصًا على عدم انتهاك حقوق الأفراد والمجتمع، وبناءً على ما تقدم سوف نتناول في هذا المطلب فرعين رئيسيين حيث يستعرض **الفرع الأول** أنواع تقنيات الذكاء الاصطناعي المستخدمة في توليد وتحليل الأدلة الرقمية، ويتناول **الفرع الثاني** مشروعية استخدام تقنيات الذكاء الاصطناعي.

الفرع الأول

أنواع تقنيات الذكاء الاصطناعي المستخدمة في توليد وتحليل الأدلة الرقمية

يتناول هذا الفرع أنواع تقنيات الذكاء الاصطناعي في توليد وتحليل الأدلة الرقمية، وينقسم إلى محورين أساسيين: الأول يختص بتقنيات الذكاء الاصطناعي المستخدمة في توليد الأدلة الرقمية، بينما يركز الثاني على تقنيات الذكاء الاصطناعي المستخدمة في تحليل الأدلة الرقمية.

أولًا: **تقنيات الذكاء الاصطناعي المستخدمة في توليد الأدلة الرقمية**:

يقصد بتقنيات الذكاء الاصطناعي المستخدمة في توليد الأدلة الرقمية هي الأجهزة أو الأنظمة التي تعد مصدرًا لتوليد أو جمع الأدلة الرقمية الناتجة عن تفاعلات أو أنشطة رقمية معينة يجعلها قابلها للتتبع، ويسعنا أن نذكر منها على سبيل المثال لا على سبيل الحصر:

١ – طائرات بدون طيار:

الطائرة بدون طيار، أو كما تسمى في الاستخدام الشائع "الدرونز"، هي طائرات تعمل بشكل ذاتي دون الحاجة إلى طاقم بشري، وفي مجال الأدلة الرقمية تعد هذه الطائرات أداة حيوية في جمع البيانات من أماكن يصعب الوصول إليها، مثل موقع الجريمة، أو الكوارث، أو المرتفعات وغيرها، حيث يمكنها التقاط صور وفيديوهات من

(ISSN: 2537- 0758)

زوايا مختلفة ذات جودة عالية لتوثيق المشاهد، وتحليلها لاحقًا بواسطة تقنيات الذكاء الاصطناعي[٢٦].

تستخدم الطائرات بدون طيار لأغراض متنوعة، بما في ذلك تأمين البنية التحتية، ومراقبة الحدود، كما يمكن أن تُوظف في عمليات الشرطة لرصد الأنشطة غير القانونية داخل الأراضي الوطنية، وقد أصبح من الواضح اهتمام المملكة العربية السعودية بتطوير هذه التقنية، حيث استخدمتها في عدة مجالات، مثل مراقبة البيئة، والحفاظ على المحميات، ومتابعة حقول النفط والغاز[٢٧].

٢- كاميرات المراقبة الأمنية:

عرف المنظم السعودي كاميرات المراقبة الأمنية بأنها: "أجهزة ثابتة أو متحركة، معدة لالتقاط الصور المتحركة وفقاً لأحكام النظام، ولا تشمل الكاميرات التي يضعها الأفراد داخل الوحدات والمجمعات السكنية الخاصة"[٢٨].

وتُعتبر كاميرات المراقبة الأمنية واحدة من أهم مصادر الأدلة الرقمية، حيث تساهم في توثيق الأحداث وتفاصيلها من خلال تسجيلات مرئية وصوتية تُخزن لفترات طويلة، مما يسهل الوصول إلى هذه التسجيلات لمراجعة الأحداث والتفاصيل عند الحاجة[٢٩].

٣- أجهزة تتبع المركبات (GPS):

يعتمد نظام تحديد المواقع العالمي (GPS) على إرسال إشارات من الأقمار الصناعية التي تحتوي على معلومات حول الموقع الجغرافي الدقيق، ويتم استقبال هذه الإشارات بواسطة أجهزة تدعم تقنية (GPS) الموجودة على الأرض، مثل تلك المثبتة في المركبات أو الأجهزة الأخرى التي تدعم هذه التقنية، إذ تعد البيانات التي تم الحصول

---

(٢٦) هشام عمر أحمد الشافعي، "التنظيم القانوني للطائرات المسيرة بدون طيار (الدرونز)"، مجلة الفكر الشرطي، المجلد رقم ٢٨، العدد ١١٠، الشارقة، ٢٠١٩م، ص١٩٨.

(٢٧) البراء جمعان محمد الشهري، مرجع سابق، ص٨٣.

(٢٨) نظام استخدام كاميرات المراقبة الأمنية م/ ١، مرسوم ملكي رقم (م/٣٤) وتاريخ ٧/٣/١٤٤٤هـ.

(٢٩) تقنيات آرلو، (٢٠٢١). كاميرات الأمان الذكية باستخدام الذكاء الاصطناعي والوصول عن بعد. تقنيات آرلو. تم الوصول إليه في ١١/ ١٠/ ٢٠٢٤م، (https://www.arlo.com).

عليها كالموقع الجغرافي ووقت الحركة دليلًا رقميًا يمكن استخدامه لتحديد مواقع الأشخاص، أو المركبات، في وقت ارتكاب الجريمة[٣٠].

٤- تقنية سلسلة الكتل (Blockchain).

تقنية البلوك تشين هي نظام رقمي يعتمد على سلسلة من الكتل (Blocks) تحتوي على بيانات مشفرة تُخزن وتُوزع عبر شبكة من الحواسيب، مما يضمن الأمان والشفافية ويمنع التلاعب، إذ تُستخدم هذه التقنية لتوثيق المعاملات الرقمية والعقود الذكية بشكل غير قابل للتغيير، مما يجعلها مصدرًا موثوقًا لتوليد الأدلة الرقمية، فعلى سبيل المثال، في قضايا الملكية الفكرية، يمكن استخدام البلوك تشين لتوثيق تاريخ نشر العمل الرقمي، بحيث يتم تسجيل توقيت الإيداع أو النشر في الشبكة، وبالتالي يمكن إثبات أسبقية العمل بشكل قانوني دون إمكانية التلاعب[٣١].

٥- الهواتف الذكية:

يعتبر الهاتف الذكي واحدًا من أكثر الأجهزة استخدامًا في عصرنا الحالي، وهو جهاز الكتروني محمول يستخدم تقنيات متقدمة مثل الاتصال عبر الشبكات اللاسلكية، والتصوير، والتسجيل الصوتي.

ويعد مصدرًا مهما للأدلة الرقمية، إذ يحتوي على العديد من البيانات القابلة للاستخراج مثل: المحادثات عبر التطبيقات المختلفة، والرسائل النصية، ورسائل البريد الالكتروني، والمكالمات الصوتية، والتسجيلات، وغيرها، كذلك يمكن للهاتف الذكي التقاط الصور والفيديوهات باستخدام الكاميرا، كما أنه مزود بتقنية (GPS) التي تتيح

---

(٣٠) تامر محمد صالح، التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة كلية الحقوق، المنصورة، ٢٠٢١م، ص٧٢٠.

(٣١) تقرير "تبني تقنية سلسلة الكتل" الصادر عن المركز الوطني السعودي للتقنية (CST) في عام ٢٠٢٢م. تم الوصول إلى التقرير بتاريخ ١٢/٨/ ٢٠٢٤م عبر الرابط: https://www.cst.gov.sa/ar/Digitalknowledge/Documents/Blockchainadoptionar.pdf

(ISSN: 2537- 0758)

تحديد المواقع الجغرافية بدقة، حيث تكمن أهمية هذه البيانات في كشف بعض الجرائم كالابتزاز أو التهديد باستخدام التسجيلات الصوتية[٣٢].

٦- أجهزة الحاسب الآلي:

يعد الحاسب الآلي مصدرًا رئيسيًا لتوليد الأدلة الرقمية، فعندما يتم استخدامه كأداة للجريمة، مثل الاحتيال الالكتروني أو اختراق الأنظمة، فإنه ينتج بيانات رقمية كالسجلات الأنشطة الشبكية، وملفات البرمجيات الخبيثة، أما إذا كان الحاسب هدفًا للجريمة، مثل العبث في الأنظمة، أو سرقة البيانات، فإن السجلات الرقمية تصبح أدلة على الأنشطة غير المشروعة[٣٣].

وبرأينا أن التقنيات التي تم ذكرها تعد من المصادر الأساسية للأدلة الرقمية، حيث تساهم في جمع وتوثيق الأحداث والأنشطة على شكل بيانات رقمية، كالصور والفيديوهات، وكذلك معلومات المواقع الجغرافية، والملفات، هذه البيانات تساعد بشكل كبير في تسريع عملية التحقيقات الجنائية.

ثانياً: تقنيات الذكاء الاصطناعي المستخدمة في تحليل الأدلة الرقمية:

يأتي هذا القسم بعد مرحلة جمع الأدلة الرقمية من مصدرها الأساسي، حيث يتم تحليل الأدلة باستخدام تقنيات الذكاء الاصطناعي، **وهي كالتالي:**

١- تقنيات تحليل البيانات الضخمة (Big data Anaytics).

تحليل البيانات الضخمة هو عملية فحص مجموعات كبيرة من البيانات لاكتشاف الأنماط المخفية، الارتباطات، والاتجاهات التي تساعد المؤسسات في اتخاذ قرارات استراتيجية، حيث يتم استخدام تقنيات التحليل المتقدمة مثل النماذج التنبؤية

---

(٣٢) أسماء جابر علي مهران، "فحص انعكاسات الجريمة المشهودة التي تم ضبطها بوساطة كاميرا المراقبة أو الهواتف الذكية أو البث المباشر على نمذجة السلوك الاجرامي وتقليد الجريمة من قبل مجرمي التقليد"، مجلة كلية الآداب، العدد ٧١، جامعة بني سويف، بني سويف، ٢٠٢٤م، ص٢٨٨ وما بعدها.

(٣٣) صالح بن محمد المسند، عبد الرحمن بن راشد المهيني، جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد ١٥، العدد ٢٩، الرياض، ٢٠٠٠م، ص١٧٨.

والخوارزميات الإحصائية لتفسير البيانات، وهذه العملية تُستخدم في العديد من المجالات مثل الرعاية الصحية، حيث يتم تحليل سجلات المرضى والمطالبات الطبية، مقارنة بالطرق التقليدية توفر تحليلات البيانات الضخمة حلًا للتعامل مع البيانات المعقدة والكبيرة(٣٤).

٢- تقنية التعرف على الأنماط (Pattern Recognition).

تقنية التعرف على الأنماط تعتبر من تقنيات الذكاء الاصطناعي المستخدمة في تحليل البيانات، حيث تهدف إلى تحديد الهياكل المتكررة، أو التسلسلات التي يمكن أن تكون ذات دلالة، وهذه التقنية تُستخدم لاستخراج الأنماط غير الظاهرة من البيانات الرقمية، سواء كانت نصوصًا، أو صورًا، أو فيديوهات، ويتم تطبيق هذه التقنية لتحليل كميات ضخمة من البيانات واستخلاص الأنماط المتكررة التي قد تشير إلى سلوك إجرامي أو تواطؤ، حيث تُعد هذه الأنماط أساسية في التحقيقات الجنائية، إذ تساهم في بناء الأدلة بشكل دقيق وموثوق لدعم القضايا القانونية(٣٥).

٣- تقنيات تحليل الصوت.

تحليل الأصوات باستخدام الذكاء الاصطناعي أصبح جزءًا مهمًّا في مجال التحقيق الجنائي، حيث يمكن استخراج الأدلة الصوتية من مصادر مختلفة ومن ثم تحليلها لتقديم معلومات دقيقة، ويُعد (جهاز أوراس) من أفضل تقنيات الذكاء الاصطناعي المستخدمة في تحليل البصمة الصوتية، حيث يشتمل على وحدة إدخال للأصوات، وتتم عملية القياس من خلال ترشيح الإشارات الصوتية للحصول على طيف مسطح لترددات الأصوات البشرية، وتتمثل وظيفة المرشح في هذه الحالة في القيام بدور معاكس لوظيفة النقل السمعي للجهاز الصوتي المتحدث، مما يساعد في عزل الصفات المميزة للصوت، وقد أظهرت التجارب العلمية التي أُجريت باستخدام هذا الجهاز أن نسبة الخطأ لا تتجاوز ١%(٣٦) .

---

(٣٤) لمزيد من المعلومات حول تقنيات تحليل البيانات الضخمة، يمكنك الرجوع إلى المقال عبر الرابط: https://2u.pw/vn6UVczN تم الوصول إليه في ٨/ ١٢/ ٢٠٢٤م.

(٣٥) تقنية التعرف على الأنماط: دليل شامل لفهم أنواعها وتطبيقاتها، أرقام، ١٤ يونيو ٢٠٢٤، تم الوصول إليه في ١٠/ ١٢/ ٢٠٢٤م، https://2u.pw/5IyhSsEe.

(٣٦) عادل عيسى الطوسي، بصمة الصوت سماتها واستخداماتها، المجلة العربية للدراسات الأمنية والتدريب، العدد١١، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ١٩٩٧م، ص٧٨، وانظر

(ISSN: 2537- 0758)

٤- التعلم الآلي (Machine Learning).

التعلم الآلي هو تقنية تستخدم لتحليل البيانات من خلال خوارزميات تتعلم من البيانات السابقة لتقديم توقعات، أو قرارات بناءً على الأنماط التي تكتشفها، إذ يُستخدم لتحليل البيانات المُعلمة مثل النصوص أو الأرقام، ويعتمد على الإنسان في تحديد الخصائص المهمة للبيانات، ومن أمثلة ذلك: أن يتم استخدامه لتحليل الأنماط في البيانات المالية، أو تصنيف البريد الإلكتروني(٣٧).

٥-التعلم العميق (Deep Learning).

يعد التعلم العميق فرع من التعلم الآلي إذ يستخدم الشبكات العصبية الاصطناعية متعددة الطبقات لتحليل البيانات المعقدة مثل الصور والفيديوهات، والصوت، يمكنه التعرف على الأنماط دون الحاجة لتدخل بشري، ويُستخدم لتحليل الصور، أو النصوص، أو حتى التعرف على الكلام.

ومن بين التقنيات التي تعتمد على التعلم العميق لتحليل الوجوه في الصور والفيديوهات هي تقنية (Gaussian Face)، وتستخدم هذه التقنية لاستخراج ملامح الوجه من الصور أو الفيديوهات بدقة، مما يساهم في التعرف على الأشخاص حتى مع تغير الزوايا والإضاءة(٣٨).

٦- تقنية معالجة اللغة الطبيعية (NLP).

تعد معالجة اللغة الطبيعية إحدى تقنيات الذكاء الاصطناعي التي تهدف إلى تحليل النصوص المكتوبة واستخلاص المعاني منها، كما تشمل الفهم اللغوي، ومعالجة البيانات، واستخراج المعلومات من البيانات النصية التي تم استخلاصها من مصادر

الى محمود جمال الدين الشاذلي، الأدلة الجنائية في ظل التطور التكنولوجي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٤م، ص٣٦٧.

(37) IBM, Machine Learning versus Deep Learning، تم الوصول إليه في ٩/ ١٢/ ٢٠٢٤م -https://www.ibm.com/topics/machine-learning

(٣٨) خلدون غسان سعيد، "تقنيات متطورة للتعرف على الوجوه". صحيفة الشرق الأوسط، ١١ فبراير ٢٠٢٠، جدة، تم الوصول إليه في ٣/ ١٢/ ٢٠٢٤م، https://tinyurl.com/2n7bxues.

متنوعة مثل الهواتف الذكية بما في ذلك المحادثات عبر تطبيق "واتساب"، وغيرها من المصادر – سبق ذكرها–، إذ يمكن لهذه التقنية اكتشاف النوايا وراء النصوص المكتوبة مثل المؤشرات الخفية المتعلقة بنشاطات مشبوهة(٣٩).

٧- تحليل بصمة العين:

تُؤخذ بصمة العين باستخدام مجموعة من التقنيات، من بينها تقنية "المسح الحدقي" تُعتبر تقنية متقدمة تُستخدم لإظهار الملامح الفريدة لحدقة العين لكل فرد، حيث يقوم الجهاز بتصوير العين بشكل فيديو، مما يمكّن من استخراج الميزات الدقيقة للحدقة، تُخزن هذه الميزات لاحقًا وتحول إلى شفرة رقمية، ثم يتم مقارنتها مع البصمات المخزنة للأشخاص المشتبه بهم، مما يتيح التعرف السريع على الأفراد(٤٠).

ومن وجهة نظرنا نرى أن تقنيات الذكاء الاصطناعي المستخدمة في استخراج وتحليل الأدلة الرقمية تعد من التقنيات الفعالة في التنبؤ بالجرائم والوقاية منها، ورغم الفوائد العديدة لهذه التقنيات في حماية الأمن العام وتحقيق العدالة، إلا أنه من المهم أن نأخذ بعين الاعتبار الجوانب المتعلقة بانتهاك الخصوصية، فيجب الحفاظ على هذه البيانات الشخصية وضمان احترام حقوق الإنسان لتفادي استخدام هذه التقنيات بطريقة تهدد الحريات الفردية، وعليه، يمكن القول إن التوازن بين الابتكار والتطور التكنولوجي وحماية حقوق الإنسان هو المفتاح الأساسي لنجاح تطبيقات الذكاء الاصطناعي في المجال الأمني.

الفرع الثاني
مشروعية استخدام تقنيات الذكاء الاصطناعي

إن مشروعية استخدام تقنيات الذكاء الاصطناعي تتطلب أن يحدد القانون تنظيم استخدامها بموجب نص قانوني واضح، إذ أن استخدام هذه التقنيات قد تؤدي إلى

(٣٩) عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، القاهرة، ٢٠١٩م، ص١٧٤.

(٤٠) محمد لطفي عبد الفتاح، البصمة الوراثية فرع من التكنولوجية الحيوية ودورها في الإثبات الجنائي "دراسة علمية قانونية" الحلقة الثانية، مجلة جامعة ابن يوسف، جمعية إحياء جامعة ابن يوسف، المجلد ١٤، العدد ١٥، ٢٠١٤م، ص١١٤.

(ISSN: 2537- 0758)

المساس بشكل مباشر بحرية الأفراد وحقهم في الخصوصية، وتؤكد الشريعة الإسلامية على حماية هذه الحقوق، محذرة من التجسس أو التعدي على الحياة الخاصة، مما يجعل من الضروري تحقيق التوازن بين استخدام هذه التقنيات لتعزيز الأمن العام واحترام حقوق الأفراد، مع تحديد الضوابط التي تنظم استخدامها بما يتوافق مع الشريعة الإسلامية والقانون.

أولًا: مخاطر استخدام تقنيات الذكاء الاصطناعي:

إن تقنيات الذكاء الاصطناعي توفر فرصًا واسعة لمراقبة وتحليل البيانات بشكل متطور ومستحدث، إلا أن سوء استخدام هذه التقنيات إلى انتهاك حقوق الأفراد والمجتمعات، مثل تتبع أماكن تواجد الأشخاص بطريقة غير قانونية، أو التنصت على المحادثات الخاصة، وعلى سبيل المثال قد يتم تتبع موقع الأشخاص عبر نظام (GPS) دون إذن منهم، أو استخدام الهواتف الذكية للتجسس على المكالمات أو الرسائل النصية، مما يمثل انتهاكًا صارخًا للخصوصية الشخصية.

إذ يمكن لهذه التقنيات من جمع بيانات شخصية حساسة دون موافقة الأفراد، سواء عن طريق اختراق الأجهزة أو استغلال أنظمة المراقبة في الأماكن العامة والخاصة، وقد حرصت الشريعة الإسلامية على حماية خصوصية الأفراد، حيث حرم الإسلام التجسس والتعدي على الآخرين كما جاء في قوله تعالى "وَلَا تَجَسَّسُوا.."[٤١].

وتطبيقًا لذلك يتدخل نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية لمعاقبة من استخدم هذه التقنيات بشكل غير قانوني، مثل: التنصت، أو التجسس على الأفراد، فقد نصت المادة الثالثة على أنه: يُعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تتجاوز ثلاثة ملايين، أو بإحدى هاتين العقوبتين، كل من استعمل الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، أو وسائل التقنية الأخرى في التجسس، أو التنصت على بيانات إلكترونية، أو وسائل الاتصال الخاصة بالأفراد دون إذن قانوني، أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها[٤٢].

([٤١]) سورة الحجرات، آية (١٢).

([٤٢]) نظام مكافحة الجرائم المعلوماتية، م/٣، مرسوم ملكي رقم م/١٧ بتاريخ ٨/ ٣/ ١٤٢٨.

ونصت المادة الثامنة من نظام استخدام كاميرات المراقبة الأمنية على أن: "تتولى الهيئة السعودية للبيانات والذكاء الاصطناعي- باستخدام تقنيات البيانات والذكاء الاصطناعي- تطوير أنظمة معالجة وتحليل بث وتسجيلات كاميرات المراقبة الأمنية، وتمكين الوزارة ورئاسة أمن الدولة- بحسب الأحوال- من استخدامها والاستفادة منها وفقاً للأنظمة ذات الصلة؛ وذلك بما لا يتعارض مع الأنظمة ذات العلاقة"[٤٣].

وتشير المادة أن الهيئة السعودية للبيانات والذكاء الاصطناعي هي المسؤولة عن تطوير الأنظمة التي تعالج تسجيلات كاميرات المراقبة، كما يتم استخدام هذه الأنظمة من قبل الجهات الأمنية مثل الوزارة ورئاسة أمن الدولة لكن وفقًا للأنظمة ذات الصلة، وتركز هذه المادة على كاميرات المراقبة المثبتة في الأماكن العامة، دون أن تشمل الأماكن الخاصة كالمنازل، إذ تهدف المادة إلى ضمان الاستخدام الآمن والقانوني للبيانات، بما يحقق حماية الخصوصية ويحول دون إساءة استعمال هذه التقنيات.

ويأتي نظام حماية البيانات الشخصية أيضًا كوسيلة أخرى لحماية حقوق الأفراد، فقد نصت المادة الرابعة على وجوب علم الأفراد بالسبب القانوني لجمع بيانات الأفراد والهدف منها[٤٤]، إذ إن حماية الخصوصية لا تعني فقط حق الأفراد في أن يعرفوا ماهي البيانات التي تم جمعها عنهم، بل يشمل أيضًا تأكيد أن هذه البيانات لا تُجمع ولا تستخدم إلا بموافقة قانونية واضحة وبغرض معين.

ثانياً: التنظيم الشكلي لاستخدام تقنيات الذكاء الاصطناعي:

يتعلق التنظيم الشكلي بوضع القوانين التي تحدد حدود استخدام هذه التقنيات بشكل عام، أي أنه يحدد الأماكن المسموح بها، وبيان الأهداف التي تستخدم لأجلها، ويتضمن أيضًا وجوب إعلام الأفراد بوجود هذه التقنيات قيد الاستخدام، هذا النوع من التنظيم يسعى إلى وضع ضوابط عامة تكفل حقوق الأفراد، وتحافظ على خصوصياتهم.

([٤٣]) نظام استخدام كاميرات المراقبة الأمنية مرسوم ملكي رقم (م/٨) وتاريخ ٧/٣/١٤٤٤هـ.

([٤٤]) عدلت المادة الرابعة من نظام الحماية البيانات الشخصية وذلك بموجب المرسوم الملكي رقم (م/١٤٨) وتاريخ ٥/٩/١٤٤٤هـ، لتكون بالنص الآتي: "يكون لصاحب البيانات الشخصية- وفقاً للأحكام الواردة في النظام وما تحدده اللوائح- الحقوق الآتية:١-الحق في العلم، ويشمل ذلك إحاطته علماً بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها.

(ISSN: 2537- 0758)

١ – التنظيم الدولي لاستخدام تقنيات الذكاء الاصطناعي:

يعد تنظيم استخدام تقنيات الذكاء الاصطناعي على المستوى الدولي أمرًا بالغ الأهمية، لحماية القيم الإنسانية والمبادئ الأخلاقية، ومن المنظمات الدولية التي شكلت إطارًا مرجعيًا بشأن أخلاقيات الذكاء الاصطناعي هي توصية "اليونسكو"، إذ تهدف إلى تحقيق التوازن بين الابتكار والتقيد بالقيم الإنسانية، والعدالة، وحماية الخصوصية، كما تدعو هذه التوصية إلى الدول الأعضاء إلى تطبيق المبادئ الواردة فيها، **ومن أبرزها**[٤٥]:

- حماية الخصوصية والبيانات الشخصية مع الاخذ بعين الاعتبار المخاطر المحتملة المتعلقة باستخدام تقنيات الذكاء الاصطناعي في جمع البيانات وتحليلها.
- تعزيز التعاون بين الدول والمنظمات الدولية لضمان الاستخدام المتوازن لتقنيات الذكاء الاصطناعي، مع التأكيد على دور الدول في تطوير الأطر القانونية والتنظيمية اللازمة.
- ضرورة النظر في التأثيرات البيئية لهذه التقنيات والعمل على تقليل الأضرار البيئية المرتبطة بها.

وفي إطار التنظيم الدولي لاستخدام تقنيات الذكاء الاصطناعي، جاء تقرير الأمم المتحدة بشأن "الحق في الخصوصية في العصر الرقمي"، الذي تناول تأثير تقنيات الذكاء الاصطناعي على الخصوصية وحقوق الأفراد الرقمية، حيث أشار التقرير إلى ضرورة وجود ضمانات قانونية تحمي البيانات الشخصية للأفراد في ظل الاستخدام المتزايد لتقنيات الذكاء الاصطناعي مثل: حق الأفراد بمعرفة كيفية جمع واستخدام بياناتهم والموافقة عليها، كما ناقش أهمية اتخاذ تدابير تشريعية وتشغيلية للتأكد من أن هذه التقنيات لا تنتهك حقوق الأفراد في الخصوصية، أو الإضرار بحقوقهم الأساسية، وشدد التقرير على حتمية مراقبة السياسات وتحديثها بشكل دوري موفقًا للتطورات التقنية لضمان حماية الأفراد من المخاطر المرتبطة باستخدام هذه التقنيات[٤٦].

---

(٤٥) اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي "المؤتمر العام، الدورة ٤١، باريس، نوفمبر ٢٠٢١"، وهي توصية تهدف إلى وضع إطار أخلاقي شامل لاستخدام تقنيات الذكاء الاصطناعي، مع التركيز على تعزيز حقوق الإنسان، وحماية البيئة، وتشجيع التنوع الثقافي.

(٤٦) مجلس حقوق الإنسان التابع للأمم المتحدة، قرار الحق في الخصوصية في العصر الرقمي، A/HRC/RES/42/15,. https://undocs.org/A/HRC/RES/42/15 م٢٠١٩

كما أقرت اللائحة العامة لحماية البيانات **(GDPR)** من قبل الإتحاد الأوروبي، بوجوب تنظيم الوصول إلى البيانات الشخصية بطريقة تحترم خصوصية الأفراد، حيث يشترط توفير الأذونات اللازمة لجمع البيانات ومعالجتها، كما يتم تحديد معايير واضحة تتعلق بكيفية استخدام البيانات، بالإضافة إلى ضرورة تأمينها من الوصول غير المصرح به، بما يتماشى مع المبادئ الأساسية للحماية والشفافية(٤٧).

ومن المهم الإشارة أن قانون الذكاء الاصطناعي للاتحاد الأوروبي **(AI Act)**، الذي دخل حيز التنفيذ في ١ أغسطس ٢٠٢٤، إذ يُعد من أحدث التشريعات التي تهدف إلى تنظيم تقنيات الذكاء الاصطناعي داخل الاتحاد الأوروبي، حيث يُركز القانون على ضمان تطور هذه الأنظمة واستخدامها بطريقة مسؤولة وآمنة، مع اعتماد نهج قائم على المخاطر لتصنيف الأنظمة بناءً على درجة المخاطر التي تشكلها، كما يسعى القانون إلى تحقيق التوازن بين تشجيع الابتكار وحماية حقوق الأفراد وضمان سلامتهم، مع توافقه مع قوانين حماية البيانات الأوروبية، لضمان الحفاظ على الخصوصية وأمن البيانات الشخصية(٤٨).

٢- التنظيم المملكة العربية السعودية لاستخدام تقنيات الذكاء الاصطناعي:

تعد مسالة تحديد الأماكن المسموح بها قانونيًا لاستخدام تقنيات الذكاء الاصطناعي ذات أهمية قصوى لضمان تحقيق التوازن بين استخدام هذه التقنيات للأمن العام وحماية خصوصية الأفراد، يأتي هذا التحديد كجزء من الضوابط القانونية التي تهدف إلى تنظيم الاستخدام العادل لهذه التقنيات.

وتطبيقًا لذلك، أقرت المملكة العربية السعودي بنظام استخدام كاميرات المراقبة الأمنية، حيث تطرق هذا النظام إلى تقسيم الأماكن التي يسمح أو يحظر فيها تركيب الكاميرات، وهي كالتالي(٤٩):

---

(٤٧) الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، تشريع قانوني أوروبي صادر عن الاتحاد الأوروبي لعام ٢٠١٦م، https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

(٤٨) الاتحاد الأوروبي، قانون الذكاء الاصطناعي (AI Act)، تم الوصول إليه في ٢٠٢٤/١٢/١٠م، https://eur-lex.europa.eu/legal-content/AR/TXT/?uri=CELEX%3A52021PC0206.

(٤٩) نظام استخدام كاميرات المراقبة الأمنية مرسوم ملكي رقم (م/٣٤) وتاريخ ٧/٣/١٤٤٤هـ.

(ISSN: 2537- 0758)

أ) الأماكن العامة (المسموح بها):

المرافق السياحية، مثل: الفنادق، والمباني السكنية المشتركة (باستثناء داخل الوحدات السكنية الخاصة)، والمنشآت الصحية، مثل: المستشفيات والعيادات، المجمعات التجارية، ومراكز الأسواق، إذ يشترط في هذه الأماكن وضع لوحات تشير إلى وجود كاميرات، والالتزام بتخزين التسجيلات بشكل آمن لمدة محددة.

ب) الأماكن الخاصة (المحظورة):

دورات المياه، وغرف تبديل الملابس في المجمعات والمرافق، وغرف الكشف الطبي، وغرف التنويم والعلاج الطبيعي، كذلك غرف العمليات الجراحية، وداخل الوحدات السكنية الخاصة في مرافق الإيواء.

ووفقًا للوائح الهيئة العامة للطيران المدني السعودي يتم تشغيل الطائرات المسيرة بعد تسجيلها بموجب تصاريح رسمية والالتزام بمعايير الأمن والسلامة، وتشدد الأنظمة على عدم استخدام هذه الطائرات في المناطق المحظورة، أو الأماكن الخاصة إلا بإذن قانوني مسبق(٥٠).

ونؤكد أن الشريعة الإسلامية قد أولت اهتمامًا بالغًا بحماية خصوصية الأفراد من التجسس والتنصت، مما يعكس تأكيدها على ضرورة حماية الحياة الخاصة، واستنادًا إلى ذلك، اتخذت المملكة العربية السعودية خطوات حاسمة من خلال تحديد الضوابط القانونية لاستخدام تقنيات الذكاء الاصطناعي، بما يضمن عدم انتهاك خصوصية الأفراد وحرياتهم.

ويتوافق ذلك مع المبادئ التوجيهية الدولية التي أقرتها العديد من المنظمات، مثل اليونسكو والأمم المتحدة، التي أكدت على ضرورة وضع ضمانات قانونية لحماية خصوصية الأفراد في ظل التوسع في استخدام تقنيات الذكاء الاصطناعي.

---

(٥٠) واس، "الطيران المدني تطلق خدماتها الإلكترونية لتصريح طائرات الدرونز"، سبق، ١١ يناير ٢٠١٩، تم الوصول إليه في ٦/١١/ ٢٠٢٤م، https://sabq.org/saudia/zhtdwn.

المبحث الثاني
حجية الأدلة الرقمية المستخلصة بواسطة الذكاء الاصطناعي

تمهيد:

تعد إجراءات جمع الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي من العمليات المعقدة، التي تتطلب التزامًا دقيقًا بالإجراءات القانونية لضمان مشروعيتها، وقبولها في المحكمة، وتشمل هذه الإجراءات المعاينة، والتفتيش، وضبط الأدلة الرقمية، بالإضافة إلى دور الخبير الرقمي في تحليل الأدلة وتقديم تقارير فنية موثوقة تعكس دقة النتائج المستخلصة[٥١].

إضافة إلى ذلك، فإن للقاضي سلطة تقديرية في قبول الأدلة الرقمية المستخلصة بالذكاء الاصطناعي، حيث يمكنه مدى مصداقية الأدلة وفقًا لما يراه مناسبًا، مستندًا إلى قناعته الشخصية ومعرفته بالأبعاد القانونية والإجرائية المتعلقة بالأدلة الرقمية، وبناءً على ما تقدم، **سيتم تقسيم هذا المبحث إلى مطلبين:**

يتناول **المطلب الأول:** ضوابط الحصول على الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي.

بينما يستعرض **المطلب الثاني:** سلطة القاضي في قبول وتقدير الأدلة الرقمية المستخلصة بالذكاء الاصطناعي.

المطلب الأول
ضوابط الحصول على الأدلة الرقمية
المستخلصة باستخدام تقنيات الذكاء الاصطناعي

لقد أصبح من الضروري- مع تزايد الاعتماد على الأدلة الرقمية في الإجراءات الجنائية- وضع ضوابط إجرائية صارمة تضمن الحصول على تلك الأدلة دون المساس بحقوق وحريات الأفراد، وعليه فإن هذا المطلب ينقسم إلى فرعين رئيسيين، فيتناول **الفرع الأول** إجراءات ضبط الأدلة الرقمية، ويركز **الفرع الثاني** على دور الخبير الرقمي ومدى تأثير رأيه في القضية، وسنوضح كلاً منهما بالتفصيل كما يلي:

([٥١]) أشرف شمس الدين، شرح قانون الإجراءات الجنائية، القسم الأول، دار النهضة العربية، القاهرة، ٢٠١٢م، ص٤٤٤.

(ISSN: 2537- 0758)

الفرع الأول
إجراءات ضبط الأدلة الرقمية

تعد إجراءات ضبط الأدلة الرقمية من الخطوات الأساسية في التحقيقات، حيث تشمل على الحصول على إذن من النيابة العامة، ومعاينة وتفتيش البيئة الرقمية، بالإضافة إلى ضبط الأدلة المتحصل عليها.

أولًا: **الحصول على إذن من النيابة العامة**:

يتطلب قبل القيام بأي إجراء لجمع الأدلة الرقمية أن يتم الحصول على إذن من النيابة العامة لضمان مشروعية الإجراءات، سواء كان في البيئة التقليدية أو الرقمية، حيث يجب على مأمور الضبط الجنائي تقديم طلب للنيابة العامة مرفقًا بأدلة معقولة تدعم الحاجة للتفتيش والضبط.

إذ يشمل الطلب تفاصيل المكان أو الشخص المستهدف، لضمان تحديد نطاق التفتيش وعدم تجاوزه. بعد مراجعة الأدلة، تقرر النيابة العامة منح الإذن أو رفضه، وفي حال الموافقة، يتم تحديد نطاق التفتيش ضمن حدود معينة، هذا الإجراء ينطبق على التفتيش في البيئة الرقمية كما في التقليدية.

ووفقًا للمادة ٤٨ من نظام الإجراءات الجزائية السعودي، يجب أن يتضمن الإذن بالتفتيش النص على التفتيش أو بيان الضرورة الملحة التي تبرر التفتيش دون إذن، إذ يسمح باتخاذ إجراءات فورية في حالات التلبس أو المواقف الطارئة [٥٢].

ثانياً: **معاينة البيئة الرقمية**:

إن المعاينة– بصفة عامة– تعني "المشاهدة الفاحصة لمكان الجريمة والآثار التي خلفتها، وحالة الأشخاص الذين لهم صلة بها، ويثبت المحقق خلال المعاينة ما يشاهده من آثار"[٥٣].

([٥٢]) الفقرة الثانية من المادة ٤٨ من نظام الإجراءات الجزائية بالمرسوم الملكي رقم (م/٢) بتاريخ ٢٢/ ١/ ١٤٣٥هـ.

([٥٣]) أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٨م، ص٢٢٢.

واستنادًا إلى ذلك، فقد ذهب فريق من فقهاء القانون إلى القول بأن إجراء المعاينة التي يتم اتخاذها لجمع الأدلة التقليدية تتخذ كذلك في جمع الأدلة الرقمية، وفي إطار الأدلة الرقمية؛ فإن المعاينة تستهدف البيئة الرقمية(٥٤).

إن إجراء المعاينة في البيئة الرقمية يتقيد بعدة ضوابط وترتيبات فنية يجب مراعاتها، نظرًا لطبيعة الأدلة الرقمية التي تتميز بكونها غير ملموسة، **يمكن ذكرها فيما يلي(٥٥):**

١- مراجعة الخطة وتنبيه الفريق: التأكد من التحضير الفني والعلمي لتأمين الأدلة الرقمية.

٢- توثيق الأجهزة وإعدادات النظام: تصوير الأجهزة الإلكترونية مع تحديد التاريخ والوقت.

٣- فحص التوصيلات والكابلات: مراقبة وإثبات حالة الكابلات المتصلة بمكونات النظام لتحليلها لاحقًا.

٤- عدم نقل المواد المعلوماتية قبل إجراء اختبارات: يجب التأكد من خلو المحيط الخارجي للأجهزة من أي مجال مغناطيسي قد يتسبب في محو البيانات المحفوظة.

٥- التحفظ على المواد المادية المهملة: مثل الأوراق الممزقة، الأوراق الكربونية المستعملة، الأقراص غير السليمة، وفحصها جيدًا لرفع أي بصمات أو أدلة مرتبطة بالجريمة.

٦- التحفظ على مستندات الإدخال والمخرجات الورقية: مثل الوثائق المتعلقة بالجريمة الصادرة من البيئة الرقمية.

٧- مراعاة مبدأ المشروعية القانونية: يجب الالتزام بالقوانين المعمول بها في جميع خطوات المعاينة لضمان عدم الإخلال بالإجراءات القانونية.

٨- الكفاءة العلمية والخبرة الفنية: ضرورة حصر إجراء المعاينة على المحققين والباحثين ذوي الخبرة والكفاءة العلمية.

---

(٥٤) مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ٢٠٠٨م، ص١٧١.

(٥٥) عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠١م، ص٢٨٣.

(ISSN: 2537- 0758)

ووفقًا لنظام الإجراءات الجزائية السعودي فإنه يلزم رجل الضبط الجنائي بإبلاغ النيابة العامة فور انتقاله إلى مكان وقوع الجريمة، كما يقع على عاتقه عند الانتقال إجراء معاينة دقيقة لمسرح الجريمة لضبط الأدلة وحمايتها من التلف أو الضياع، بالإضافة إلى ذلك يجب عليه الاستماع إلى أقوال الأشخاص الحاضرين أو أي شخص قد تكون لديه معلومات حول الحادثة المرتكبة، وتوثيق جميع هذه الإفادات بشكل رسمي ضمن الضبوط اللازمة[٥٦].

ثالثاً: تفتيش البيئة الرقمية:

بالرغم من أن حرمة حياة الإنسان تمثل جزءًا أساسيًا من الحقوق التي تحميها التشريعات الوطنية والدولية، إلا أن أغلب التشريعات أجازت التفتيش لضبط ما يفيد في استجلاء الحقيقة عن الجريمة التي ارتكبت، وهو ما يعد تقييدًا لحرية الأفراد.

ويعرف التفتيش في مجال تكنولوجيا المعلومات بأنه الدخول إلى أنظمة المعالجة الآلية للبيانات للتنقيب والبحث في البرامج التي تم استخدامها، والبيانات المحفوظة، مما يسهم في الكشف عن تفاصيل الجريمة الواقعة وتحديد مرتكبيها[٥٧].

وأما ما يخص المبادئ القانونية، فإن التفتيش في البيئة الرقمية يخضع لنفس المبادئ التي تحكم التفتيش التقليدي، حيث يتم اتخاذ إجراءات قانونية مشابهة للحصول على الأدلة الرقمية ومصادرتها، تمامًا كما في التفتيش التقليدي، فضلًا على أن المتطلبات القانونية للحصول على إذن قانوني لإجراء البحث والتفتيش تظل نفسها، سواء كانت أدلة مادية ملموسة، أو رقمية غير ملموسة[٥٨].

([٥٦]) نظام الإجراءات الجزائية م/٣١ بالمرسوم الملكي رقم (م/٢) بتاريخ ٢٢/ ١/ ١٤٣٥هـ.

([٥٧]) أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، ٢٠١٢م، ص١٩٨.

([٥٨]) المادة ١٩ من الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) ٢٠٠١م، تم اعتمادها من لجنة وزراء مجلس أوروبا مجموعة المعاهدات الأوروبية – رقم ١٨٥، تسعى هذه الاتفاقية بشكل أساسي إلى:

– تنسيق الأحكام الجنائية التقليدية لتناسب خصوصيات الجرائم الإلكترونية.

– إنشاء نظام يتميز بالسرعة والفعالية للتعاون الدولي.

والجدير بالذكر أن نظام الإجراءات الجزائية السعودي يحتوي على عدة قواعد لتنظيم إجراء التفتيش التقليدي من قبل مأمور الضبط الجنائي، ولكن لم ينص صراحة على التفتيش في البيئة الرقمية، ومع ذلك، يتم تطبيق نفس المبادئ القانونية المتبعة في التفتيش التقليدي على التفتيش الرقمي، وفي هذا الجانب سوف نتطرق إلى القواعد الجوهرية التي يلزم اتباعها عند إجراء التفتيش في البيئة الرقمية[٥٩]:

القاعدة الأول: أسباب التفتيش الرقمي: أقرت المادة (٤٢) من النظام أنه لا يجوز تفتيش المسكن إلا في الأحوال المنصوص عليها نظامًا، وبأمر مسبب من النيابة العامة، وإذا رفض صاحب المسكن قيام التفتيش جاز لرجل الضبط الجنائي أن يتخذ الوسائل اللازمة المشروعة، كما أوجبت المادة (٥٥) أنه لا يجوز تفتيش غير المتهم، أو مسكن غير مسكنه، إلا إذا كانت هناك دلائل قوية تفيد في التحقيق، وأيضا جاء في المادة (٥٦) أن للرسائل البريدية والبرقية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة، فلا يجوز الاطلاع عليها أو مراقبتها إلا بأمر مسبَّب ولمدة محددة، وفقًا لما ينص عليه هذا النظام.

وتجدر الإشارة إلى أن التفتيش عملًا من أعمال التحقيق، ويجب أن يكون بناءً على ارتباط الشخص بالجريمة أو حيازته أشياء تتعلق بها، وذلك وفقًا للمادة (٨٠) من نفس النظام.

واستنادًا إلى ذلك، نرى أن تفتيش البيئة الرقمية يمكن أن يكون مشابهًا لتفتيش المسكن، إذ تتضمن الأجهزة الرقمية معلومات شخصية حساسة تحتاج إلى نفس الحماية القانونية.

القاعدة الثانية: الغرض من التفتيش الرقمي: حددت المادة (٤٦) من النظام أن يكون الغرض من التفتيش هو البحث عما يفيد في كشف حقيقة الجريمة المرتكبة، وفي المقابل تطبق المادة (٤٦) في البيئة الرقمية من خلال تحديد الغرض من التفتيش الرقمي في البحث عن الأدلة التي تكشف الجريمة الواقعة، وفي هذا السياق، يتيح النظام للنائب العام وفقًا للمادة (٥٧) إصدار أوامر بمراقبة المحادثات والرسائل الإلكترونية، بما يخدم المصلحة من التحقيق.

---

(٥٩) نظام الإجراءات الجزائية مرسوم ملكي رقم (م/٢) بتاريخ ٢٢/ ١/ ١٤٣٥هـ.

(ISSN: 2537- 0758)

القاعدة الثالثة: حالات التلبس بالجريمة: قررت المادة (٤٤) الأحوال التي تجيز فيها التفتيش لرجال الضبط الجنائي وهي حالتين: حالة التلبس بالجريمة، والأحوال التي تجيز القبض.

القاعدة الرابعة: توثيق إجراءات التفتيش الرقمي: أوجبت المادة (٤٨) من النظام البيانات التي يتضمنها محضر التفتيش، وأهمها اسم من أجرى التفتيش، ووظيفته، وتوقيعه، وتاريخ التفتيش، وساعته، ونص الإذن الصادر بإجراء التفتيش، أو بيان الضرورة الملحة التي اقتضت التفتيش بغير إذن، أسماء الأشخاص الذين حضروا التفتيش وتوقيعاتهم، وصف الموجودات التي ضبطت وصفًا دقيقًا، وإثبات جميع الإجراءات التي اتخذت أثناء التفتيش والإجراءات المتخذة بالنسبة إلى الأشياء المضبوطة، وكذلك ينبغي أن يطبق نفس المبدأ في البيئة الرقمية.

رابعاً: ضبط الأدلة الرقمية:

إن النتيجة المرجوة عن إجراء المعاينة والتفتيش هي ضبط الأدلة التي تم الحصول عليها من خلال هذه الإجراءات، وحتى تتناسب القوانين الإجرائية التقليدية البيئة الرقمية يجب استخدام المصطلحات الحاسوبية الحديثة مع الاحتفاظ باللغة التقليدية في الإجراءات الجنائية؛ فكلمة البحث والمصادرة يعادلها باللغة التقنية النفاذ والضبط[٦٠].

إذ ينبغي تطبيق المادة (٥٧) من نظام الإجراءات الجزائية في البيئة الرقمية بنفس المبادئ القانونية، مع مراعاة الاختلافات التقنية المتعلقة بالبيانات الإلكترونية وطرق الوصول إليها، إذ أقرت المادة أنه يمكن للنائب العام إصدار أمر ضبط الرسائل الإلكترونية، والإذن بمراقبة المحادثات عبر تطبيقات رقمية مختلفة–من ضمنها تقنية الذكاء الاصطناعي– سواء كانت نصية أو صوتية، إذا كان ذلك يخدم مصلحة التحقيق في جريمة معينة، ويجب أن يكون الامر مسببًا ويحد فترة الضبط أو المراقبة، بحيث لا تزيد على عشرة أيام مع إمكانية التجديد حسب الحاجة والتطورات في التحقيق[٦١].

---

(٦٠) ميادة مصطفى محمد المحروقي، مرجع سابق، ص٩٠.

(٦١) م/٧٥ من نظام الإجراءات الجزائي السعودي الصادر بتاريخ ٢٢/ ١/ ١٤٣٥هـ ينص على "لرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل والخطابات والمطبوعات والطرود، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها، متى كان لذلك فائدة في ظهور الحقيقة في

أما بالنسبة لضبط الأدلة الرقمية دون إذن مسبق، فقد أجاز النظام القضائي الأمريكي ذلك في حالات استثنائية، مثل وجود خطر من تلف الأدلة، ومع ذلك؛ أكدت المحكمة العليا الأمريكية على أنه في حال عدم وجود مبررات قوية تقتضي الوصول إلى البيانات فورًا، يُفضل إصدار إذن قضائي، حيث يمكن للخبير الرقمي استخراج معلومات دقيقة وذات صلة من الجهاز، والتي لا يمكن الوصول إليها من خلال بحث تم إجراؤه بشكل متسرع، مما قد يؤدي إلى فقدان بيانات هامة يصعب استعادتها(٦٢).

ونرى أن جمع الأدلة الرقمية يتطلب اتباع إجراءات دقيقة في المعاينة، والتفتيش، والضبط، لضمان الحفاظ على سلامة الأدلة وحمايتها من التلف أو التلاعب، إلى جانب توثيق كافة الإجراءات المتخذة.

الفرع الثاني
دور الخبير الرقمي

يعرّف الخبير الرقمي بأنه: الشخص المختص في الانظمة الإلكترونية، والذي يمكنه الإدلاء برأيه الفني في الأمور التي تتعلق بالوسائل التقنية المستحدثة، بشرط أن يكون لديه المؤهل العلمي، ومعه الخبرات العلمية التي تتطلبها هذه المهمة(٦٣).

ولعل من مهام الخبير الرقمي وضع وتنفيذ استراتيجيات التحوّل الرقمي، وضمان مواءمتها مع الاستراتيجية العامة للوزارة .بناء وتصميم وصيانة البنية التحتية لتقنية المعلومات في الوزارة.

واستنادً إلى التعريف السابق، لا بد من الإشارة إلى مدى أهمية رأي الخبير الرقمي في القضية، والمهام التي يضطلع بها الخبير الرقمي في مجاله، والمعايير التي يجب

جريمة وقعت، على أن يكون الأمر أو الإذن مسبَّبًا ومحددًا بمدة لا تزيد على عشرة أيام قابلة للتجديد وفقًا لمقتضيات التحقيق".

(62) United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995); David, 756 F. Supp. 1392; Morales-Ortiz, 376 F. Supp. 2d 1142 n.2.

(٦٣) محمود عبد الغني جاد المولى، دور الدليل الالكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية،٢٠١٩م، ص١٧٥-١٧٦.

(ISSN: 2537- 0758)

الالتزام بها، بالإضافة إلى سمات الخبير الرقمي، وذلك وفقًا لنظام الإثبات، ونظام الإجراءات الجزائية، وهي كالتالي(٦٤):

أولًا: أهمية الخبير الرقمي:

يعد الخبير الرقمي جهة فنية معتمدة تُسند إليها مسؤولية جوهرية في التحقيقات الجنائية، خاصةً في التعامل مع الأدلة الرقمية التي تتطلب مهارة تقنية على تحليل البيانات المعقدة، ويكتسب رأيه أهمية قانونية بالغة كونه أداة حاسمة يعتمد عليها القاضي في تقييم موثوقية الأدلة ودقتها.

١- **أهمية رأي الخبير الرقمي:** تشير المادة (١١٠) من النظام إلى أهمية رأي الخبير في القضايا التي تحتاج المحكمة إلى رأي متخصص للفصل فيها.

٢- **تأثير تقرير الخبير الرقمي:** توضح المادة (١٢١) من ذات النظام إلى أن تقرير الخبير قد يؤثر على سير القضية، ولكن المحكمة غير ملزمة بالأخذ به إذا تبين وجود قصور أو خطأ به.

٣- **استناد المحكمة على تقرير الخبير الرقمي:** نصت المادة (١٢٤) من النظام على أنه: "يجوز للمحكمة الاستناد إلى تقرير خبير مقدم في دعوى أخرى عوضاً عن الاستعانة بخبير في الدعوى، وذلك دون إخلال بحق الخصوم في مناقشة ما ورد في ذلك التقرير"، إذ تبرز إمكانية اعتماد المحكمة على تقرير الخبير، مما يدل على الثقة بأهمية رأي الخبير.

ثانياً: سمات الخبير الرقمي:

تعد سمات الخبير هي الصفات التي يتميز بها لضمان قدرته على تقديم رأي فني دقيق وموثوق به في القضايا المتعلقة بالأدلة الرقمية، **ومن أهمها:**

- **التخصص الفني:** تشترط المادة (٧٦) من نظام الإجراءات الجزائية بأن يكون الخبير الرقمي متخصصًا في المجال الذي يتعامل فيه مع الأدلة الرقمية، كالصور والفيديوهات، ليتمكن من تقديم رأي فني دقيق.

---

(٦٤) نظام الإثبات مرسوم ملكي رقم (م/٤٣) وتاريخ ٢٦/٥/١٤٤٣هـ، نظام الإجراءات الجزائية مرسوم ملكي رقم (م/٢) بتاريخ ٢٢/ ١/ ١٤٣٥هـ.

- **الخبرة العملية:** تضع المادة (٧٦) من نظام ذاته شرطًا بأن يكون الخبير الرقمي ذو خبرة كافية في فحص الأدلة الرقمية وتحليلها.
- **الحيادية والاستقلالية:** تنص المادة (١١٣) من نظام الإثبات على وجوب حيادية الخبير الرقمي وعدم تحيزه لأطراف القضية، وعليه أن يفصح على العلاقات التي تربطه بالخصوم لضمان تقييمه للأدلة الرقمية.

ثالثاً: واجبات الخبير الرقمي:

إن واجبات الخبير الرقمي تتعلق بالوظيفة الأساسية التي يؤديها، مثل: تقديم رأي فني، وإعداد التقرير، وهي تتضمن مجموعة من المهام التي يجب الالتزام بها وفقًا للنظام السعودي، ويمكن ذكرها على النحو التالي:

١- واجبات الخبير الرقمي وفقًا لنظام الإجراءات الجزائية[٦٥]:

- إعداد التقرير: أوجبت المادة (٧٧) من نظام الإجراءات الجزائية على أن يقدم الخبير الرقمي تقريره كتابة في الموعد الذي حدده المحقق، ويتضمن ملخصًا للأعمال التي أداها، بما في ذلك الإجراءات الفنية المتخذة والنتائج التي توصل إليها.

- تقديم رأي فني: أقرت للمادة (٧٦) من نظام الإجراءات الجزائية على أنه يُستعان بالخبير الرقمي لإبداء رأيه الفني في الأمور المتعلقة بالأدلة الرقمية كالفيديوهات والصور، يشمل ذلك تحليلها واستخلاص النتيجة، وهي الاستنتاجات الفنية التي يتوصل إليها الخبير بناءً على فحص الأدلة الرقمية، وعلى سبيل المثال قد يتبين للخبير ما إذا كانت الصورة قد تعرضت للتلاعب باستخدام برامج، أو ما إذا كان الفيديو قد تم تحريفه.

كما يجب على الخبير الرقمي إرفاق التقرير الذي أعده مع ملف الدعوى ليكون جزءًا من الإجراءات القضائية، بالإضافة إلى إبلاغ الأطراف المعنية بإيداع رأيه للمحكمة خلال ٢٤ ساعة من إتمام المهمة، وذلك بهدف حفاظًا على سرية المعاملة التي قام بها[٦٦].

([٦٥]) نظام الإجراءات الجزائية مرسوم ملكي رقم (م/٢) بتاريخ ٢٢/ ١/ ١٤٣٥هـ.

([٦٦]) زكي محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، مكتبة الملك فهد الوطنية للنشر، الرياض، ١٤٣١هـ، ص٢٢٣.

(ISSN: 2537- 0758)

٢- واجبات الخبير الرقمي وفقًا لنظام الإثبات[٦٧]:

- الإفصاح عن المصالح والعلاقات: أوجبت المادة (١١٣) من النظام على ضرورة إفصاح الخبير الرقمي عن أي مصلحة أو علاقة تربطه بأطراف القضية قبل بدء مهمته، إذ يؤدي عدم الإفصاح إلى التشكيك في مصداقية التقرير الفني، ويجعل الأدلة الرقمية غير موثوقة بسبب احتمال التحيز.

- التقيد بالمهلة الزمنية: أقرت المادة (١١٨) من ذات النظام بوجوب التزام الخبير الرقمي بالموعد المحدد لإنجاز مهمته وتقديم التقرير الفني بما لا يتجاوز (خمسة) أيام، حيث تكمن مخاطر التأخير في تدهور مصداقية الأدلة الرقمية والمماطلة في سير الدعوى.

رابعاً: المعايير التي يجب على الخبير الرقمي الالتزام بها[٦٨]:

تركز المعايير على الجوانب التقنية المتعلقة بكيفية التعامل مع الأدلة الرقمية، إذ يجب على الخبير الرقمي الالتزام بها لضمان سلامة الأدلة الرقمية ودقة الإجراءات الفنية، **وهي كالتالي:**

١- **الاستحواذ:** يقوم الخبير هذه المرحلة بإنشاء نسخة مطابقة للمعلومات الموجودة بمحل الدليل.

٢- **التوثيق:** تسجيل خطوات جمع وتحليل الأدلة بدقة لضمان مصداقيتها.

٣- **حماية الأدلة الرقمية:** يتم الحفاظ على سلامة الأدلة من خلال العمل على النسخة بدلًا من الأصل، ومن ثم تحليل المعلومات لتوضيح ملابسات القضية[٦٩].

٤- **إعداد تقرير المعمل الجنائي الرقمي:** يتضمن التقرير النهائي للمعمل الجنائي الرقمي كافة المعلومات المتعلقة بالقضية، بما في ذلك الملفات المكتشفة وتحليلها

([٦٧]) نظام الإثبات مرسوم ملكي رقم (م/٤٣) وتاريخ ٢٦/٥/١٤٤٣هـ.

([٦٨]) ميادة المحروقي، مرجع سابق، ص٢٠ وما بعدها.

([٦٩]) أزهري عبد الرحمن، نسرين بشير عثمان، "جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فاعلية"، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، الرياض، ٢٠١٥م، ص١٥.

والأدوات المستخدمة، وجميع التفاصيل عن الجهاز الذي يحتوي على الدليل، ويقسم التقرير إلى: ١- ملخص القضية، ٢- طرق الفحص والتحليل، ٣- النتائج.

لذا؛ برأينا أن دور الخبير الرقمي يتمثل في تحليل الأدلة الرقمية مثل الرسائل، أو الصور، أو البيانات، أو غيرها من الأدلة الرقمية- سبق ذكرها-، باستخدام تقنية الذكاء الاصطناعي، لاستخراج الأنماط التي قد يصعب اكتشافها بالطرق التقليدية، إذ يمكن للخبير وبمساعدة تقنيات الذكاء الاصطناعي تأكيد أو نفي أقوال الأطراف لتقديم صورة أكثر شمولية وتكاملًا عن الاحداث الواقعة، ومن ثم مقارنتها مع أقوال الخصوم، أو الشهود، لتعزيز فهم القاضي للأحداث الواقعة.

ومع ذلك، نرى بأن التحديات الإجرائية الكبرى تكمن في التوازن بين ضرورة جمع الأدلة الرقمية لكشف الجريمة ومعرفة مرتكبها، وحماية الخصوصية للأفراد، مما يستدعي الالتزام الصارم بالقوانين المتعلقة بإجراءات الحصول على الأدلة الرقمية وكذلك الالتزام بالضمانات الإجرائية وعدم انتهاك الخصوصية، لضمان قبولها أمام المحاكم.

المطلب الثاني

سلطة القاضي في قبول وتقدير الأدلة الرقمية المستخلصة بالذكاء الاصطناعي

يعتبر قبول الدليل الرقمي الخطوة الأولى التي يقوم بها القاضي قبل أن يتطرق إلى تقييمه ومناقشته، بحيث يركز القاضي بهذه المرحلة على التأكد من مشروعية الدليل أي أنه قد تم الحصول على الدليل الرقمي وفقًا للأنظمة والإجراءات الصحيحة، وإلا لن ينتج للدليل الرقمي أي أثر قانوني إذا تم ضبطه بطرق غير مشروعة، بل قد يعتبر باطلًا.

واستخدام الذكاء الاصطناعي لاستخلاص الأدلة الرقمية يعتمد كذلك على هذه المشروعية؛ فإذا كانت إجراءات جمع الأدلة الرقمية سليمة، يمكن للقاضي الاعتماد على تقرير التحليل الصادر عن الذكاء الاصطناعي لتلك الأدلة، أما إذا كانت إجراءات الحصول على الدليل رقمي غير قانونية، فإن ذلك يؤدي إلى بطلانه بالكامل، بغض النظر عن دقة التحليل المقدم.

وعليه فإن هذا المطلب ينقسم إلى فرعين رئيسيين، يستعرض **الفرع الأول** المعايير القانونية لقبول الأدلة الرقمية المستخلصة بالذكاء الاصطناعي، بينما يتناول **الفرع الثاني** صلاحيات القاضي في تقدير الأدلة الرقمية المستخلصة بالذكاء الاصطناعي.

(ISSN: 2537- 0758)

الفرع الأول

المعايير القانونية لقبول الأدلة الرقمية المستخلصة بالذكاء الاصطناعي

يعتمد قبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي أمام القضاء على توافر شروط قانونية معينة لضمان صحتها، بالإضافة إلى مشروعية الإجراءات المتبعة في جمعها، فإن الإخلال بأي من هذين العنصرين قد يؤدي إلى استبعاد الدليل الرقمي وعدم قبوله في المحكمة.

أولًا: شروط صحة الأدلة الرقمية:

تتمثل شروط صحة الأدلة الرقمية في ضمان أصالته، ومصداقيته، وكفاءته، بما يضمن قبولها كوسيلة قانونية معتمدة في الإثبات، وهذه الشروط تتحدد في النقاط التالية:

الشرط الأول: أصالة الدليل الرقمي:

يعد شرط أصالة الدليل الرقمي المستخلص من الذكاء الاصطناعي هو النسخة الأصلية من البيانات التي تم جمعها، دون تعديل أو تلاعب من لحظة الاستخراج، إذ يركز هذا الشرط على ضمان أن البيانات والمعلومات المستخلصة بواسطة تقنيات الذكاء الاصطناعي لم تتعرض لأي تحريفات أو تغييرات أثناء عملية المعالجة، لذلك من المهم التأكد من التقنيات التي تعمل على استخلاص هذه الأدلة الرقمية، بأنها عملت بشكل سليم، وأن تلك الأدلة التي قدمت للمحكمة هي النسخة الأصلية التي تعكس الحقيقة[٧٠].

الشرط الثاني: مصداقية الدليل الرقمي:

تشير المصداقية إلى مدى صحة أو مصداقية الدليل المستخلص من الذكاء الاصطناعي بناءً على المصدر الذي أُخذ منه، والإجراءات المتبعة في جمعه ومعالجته، فإذا كان الإجراء صحيحًا وواضحًا، فإن الدليل يكون أكثر مصداقية، كما أن المصداقية تتعلق بالموثوقية والقدرة على الوثوق بالدليل كوسيلة قانونية[٧١].

---

(٧٠) سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي "دراسة في القانونين الإنجليزي والأمريكي"، المجلة الدولية للقانون، دار جامعة حمد بن خليفة للنشر، الدوحة، ٢٠١٧م، ص١٤.

(٧١) سامي حمدان الرواشدة، مرجع سابق، ص١٤.

وعليه، فإن الاختلاف الرئيسي بين الأصالة والمصداقية والكفاءة، يكمن في أن الأصالة تتعلق بسلامة الدليل وحمايته من التلاعب أو التعديل، بينما تشير المصداقية إلى مدى قابلية الاعتماد عليه كدليل قانوني يمكن الاستناد إليها في القضية، أما الكفاءة فتركز على صلة الدليل في القضية، ويعني ذلك أنه يجب أن يكون للدليل الرقمي المستخلص التأثير في زيادة احتمالية صحة الوقائع المطروحة أمام المحكمة.

الشرط الثالث: كفاءة الدليل الرقمي.

يشترط لقبول الأدلة الرقمية المستخلصة من الذكاء الاصطناعي أن تكون ذات كفاءة علمية، وذات صلة بالقضية المطروحة، إذ يجب أن يمتلك الدليل الرقمي المستخلص الصلاحية العلمية اللازمة التي تجعله ذا قيمة إثباتية، بحيث يكون قادرًا على التأثير في مجريات القضية وإظهار الحقيقة. وقد بيّنت المادة ١٠٤ من قانون الإثبات الفيدرالي أن الأدلة تكون لها صلة إذا كان يساعد في تقريب الحقيقة أو زيادة احتمالية حدوثها في غياب الأدلة الأخرى، وتؤدي النتيجة إلى استنتاج يعتمد على الإجراءات المتخذة[٧٢].

وقد وضعت المحاكم الأمريكية بعض العوامل التي يجب اعتمادها لقياس مدى كفاءة الأدلة الرقمية كأدلة علمية صالحة في الإثبات، **وتشمل هذه العوامل**[٧٣]:

١- سلامة عمل التقنية المستخدمة في استخراج الدليل منه، وإذا كان هناك جزء معين في هذه التقنية لا يعمل بشكل سليم، فيجب ألّا يؤثر الجزء المعطل على استخلاص الدليل، أو محتوى الدليل الرقمي المستخلص.

([٧٢]) القواعد الفيدرالية للأدلة- المادة الرابعة: الصلة وحدودها: القاعدة ٤٠١- اختبار الأدلة ذات الصلة

يكون الدليل ذا صلة إذا:

١- كان له أي ميل لجعل حقيقة معينة أكثر أو أقل احتمالاً مما كانت عليه بدون هذا الدليل؛ و

٢- كانت الحقيقة ذات أهمية في تحديد نتيجة الإجراء.

https://www.law.cornell.edu/rules

([٧٣]) نزار أولاد مومن، الإثبات في الميدان الجنائي من خلال الدليل المعلوماتي ، مجلة الفقه والقانون، الناشر صلاح الدين دكداك، العدد ٧١، ٢٠١٨م، ص٤٩.

(ISSN: 2537- 0758)

٢- يجب التحقق من دقة الدليل الرقمي، إذ يجب ألا يكون هناك سبب منطقي للاعتقاد بأن الدليل الرقمي قد يتضمن خطأ في عملية استخلاصه.

٣- في حال تم تسجيل أو تخزين الدليل الرقمي من قبل شخص ليس طرفًا في القضية أثناء أداء أعماله الاعتيادية، يجب التحقق من عدم قيامه بذلك لصالح أطراف الدعوى.

تطرقت الدراسة إلى الشروط الجوهرية لصحة الدليل المستخلص من الذكاء الاصطناعي، لكن يثور تساؤل حول هذه الشروط: هل يمكن أن يتوافر في الدليل الرقمي المستخلص الأصالة والمصداقية، بينما يفتقد الكفاءة؟

بناءً على السؤال المطروح، يمكننا القول إنه في الواقع قد يحدث ذلك، فالدليل الرقمي قد يكون صحيحًا من الناحية التقنية؛ أي أنه لم يتم التلاعب به، ويكون موثوقًا في محتواه؛ أي أنه يعكس الواقع بشكل سليم، وقد تم جمعه وفق إجراءات صحيحة، لكن لا يعني ذلك أنه ذي صلة بالقضية المطروحة أمام المحكمة.

على سبيل المثال، نفترض أنه تم استخدام جهاز أوراس-سبق ذكره- لتحليل ملف صوتي تم ضبطه في مكان الجريمة، ثم تبين آنذاك أن الملف الصوتي أصيل؛ أي أنه لم يتم تعديله أو التلاعب به، وأُثبت بأن الصوت غير مزور.

لكن عند تقديم الملف الصوتي في المحكمة، تبين أنه لا يوجد ما يربط الصوت بالقضية، إنما كانت مجرد محادثات عادية لا تتعلق بالقضية المطروحة، فبهذه الحالة، بالرغم كون الدليل المستخلص صحيحًا من حيث الأصالة والمصداقية، إلا أنه يخلو من الكفاءة، لأنه لا يساعد في إثبات أو نفي الحقيقة، مما يجعله غير مناسب لاستخدامه كدليل إثبات في هذه القضية.

ثانياً: تأثير مشروعية الإجراءات على قبول الأدلة الرقمية:

في الواقع ليست كل الأدلة الرقمية تعتبر ذات قيمة قانونية أمام القاضي، مهما كانت قوية أو مفيدة في كشف الحقيقة، وبمعنى آخر أن الدليل لا يكون مقبولًا فقط لأنه قد كشف الجريمة أو قدم معلومات هامة، بل يجب أيضًا أن يكون مشروعًا وقانونيًا، والأصل في قبول القاضي المختص للأدلة الرقمية هو أن يكون ذلك الأخير قد تم الحصول عليه بطريقة موافقة للقواعد القانونية المعمول بها، حتى لو كان يكشف عن

معلومة حاسمة في القضية، وبحال تم ضبط الأدلة الرقمية بطريقة تخالف النظام، فإنه يفقد قيمته القانونية أمام القاضي الجنائي ولا يمكن استخدامه لإثبات الاتهامات(٧٤).

ويعني ذلك قبل أن يبدأ القاضي الجنائي في تقييم مدى قوة الدليل الرقمي المستمد من تقنية الذكاء الاصطناعي أو تأثيره على القضية، يجب أن يتأكد أولًا من أن الدليل الرقمي المستخلص قد تم الحصول عليه بطرق مشروعة تتوافق مع القوانين والإجراءات المعمول بها، وعلى سبيل المثال إذا كان الدليل الرقمي المستخلص قد تم الحصول عليه عن طريق تفتيش غير مشروع كعدم وجود إذن مسبق، فلن تقبل المحكمة هذا الدليل، حتى لو كان يدل على معلومات هامة وحاسمة.

وتطبيقًا لذلك هي قضية –Mapp v. Ohio–، حيث تم تفتيش منزل ماب دون موافقتها ودون الحصول على إذن قضائي، وأسفر التفتيش على أدلة أُدينت ماب بناءً عليها، لكن مع ذلك، قررت المحكمة العليا أن الأدلة التي جُمعت بطريقة غير قانونية يجب استبعادها(٧٥).

الشاهد في هذه القضية أنه إذا كان التفتيش غير مصرح به، فإن أي دليل لاحق يتم جمعه استنادًا إلى هذا التفتيش يُستبعد من المحكمة، بغض النظر عما إذا كان هذا الدليل يكشف عن معلومات حاسمة في القضية، وذلك وفقًا لمبدأ "استبعاد الأدلة المتحصلة بطرق غير مشروعة".

وفي رأينا أن هذا المبدأ ينطبق أيضًا على الأدلة الرقمية المستخلصة باستخدام تقنيات الذكاء الاصطناعي، فإذا تم جمع هذه الأدلة من خلال وسائل غير قانونية، أو دون الالتزام بالإجراءات القانونية المعتمدة، فإنها تعتبر غير مقبولة في المحكمة.

وبناءً على ذلك، فإن أساس قبول القاضي الجنائي للدليل الرقمي المستخلص يعتمد على تحقق شرط المشروعية، أي أن يكون الدليل الرقمي متوافقًا مع الأنظمة والقوانين المعمول بها، والمشروعية هنا تعرف بأنها التقيد بأحكام القانون واحترامها، والهدف

---

(٧٤) سهى إبراهيم عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، جامعة القدس، كلية الحقوق، القدس، ٢٠١٤م، ص١٧.

(75) Mapp v. Ohio, 367 U.S. 643 (1961).
https://www.oyez.org/cases/1960/236.

(ISSN: 2537- 0758)

الأساسي من المشروعية هو ضمان حرية الأفراد وحقوقهم من تعسف السلطات، وهو الحفاظ على النظام الاجتماعي للدولة من خلال فرض القانون بشكل عادل ومنصف سواء على الأفراد أو السلطات، وبالتالي يصبح هناك توازن بين حماية النظام الاجتماعي ومنح الأفراد حماية متساوية من أي تعسف(٧٦).

كما نرى أن قبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي يتطلب توافر ثلاثة شروط أساسية وهي الأصالة (عدم التلاعب بالدليل)، والمصداقية (جمعه وفق إجراءات قانونية موثوقة)، والكفاءة (صلته بالقضية)، بالإضافة إلى ذلك، يجب أن تكون الإجراءات المتبعة في جمع الأدلة مشروعة وفقًا للأنظمة المعمول بها، حيث أن أي دليل تم جمعه بطرق غير قانونية يُستبعد من المحكمة، لذا؛ يجب على القاضي التأكد من مشروعية جمع الأدلة الرقمية وتوافر هذه الشروط لضمان قبولها كدليل قانوني صالح.

الفرع الثاني

سلطة القاضي في تقييم الأدلة الرقمية المستخلصة بالذكاء الاصطناعي

يتناول هذا الفرع دور القاضي في تقييم الأدلة الرقمية المستخلصة بواسطة تقنيات الذكاء الاصطناعي، من خلال موقفه من تقرير الخبير الرقمي، وكيفية تأثر قناعاته بتلك الأدلة، إذ تتمثل سلطته في قبول، أو رفض هذه الأدلة بناءً على تقييمه الشخصي.

أولًا: موقف القاضي من تقرير الخبير الرقمي:

يمتلك القاضي سلطة تقديرية في التعامل مع تقرير الخبير، سواء بقبوله كاملًا أو جزئيًا، أو رفضه، وفيما يلي أهم الجوانب التي تحدد موقف القاضي تجاه تقرير الخبير:

١- سلطة القاضي في تقدير تقرير الخبير الرقمي:

وفقًا للمادة (١٢١) من نظام الإثبات، لا يقيد رأي الخبير المحكمة، إذ يمكن للقاضي رفض التقرير كليًا، أو جزئيًا، شريطة أن يوضح أسباب ذلك في حكمه، مما يعكس أهمية الرقابة القضائية على عمل الخبير الرقمي(٧٧).

---

(٧٦) سلامة محمد المنصوري، تطبيق مبدأ الاقتناع القضائي على الدليل الالكتروني ، رسالة ماجستير، جامعة الإمارات العربية المتحدة، كلية القانون، قسم القانون العام، أبو ظبي، ٢٠١٨م، ص٥٩.

(٧٧) نظام الإثبات مرسوم ملكي رقم (م/٤٣) وتاريخ ٢٦/٥/١٤٤٣هـ.

وبحال اتفق الخصوم على قبول نتيجة تقرير الخبير الرقمي، يعمل القاضي بهذا الاتفاق ما لم يخالف النظام العام، وهو ما يؤكد دور القاضي في مراجعة التقرير حتى مع وجود اتفاق الأطراف، وإذا ثبت للمحكمة وجود عيب أو إهمال أدى إلى بطلان التقرير، فإن التقرير يفقد قيمته القانونية، وتأمر بعدم الأخذ به.

وفيما يتعلق بمناقشة الخبير الرقمي، نصت المادة (١٢١) من نظام الإثبات على القاضي من تلقاء نفسه، أو بناءً على طلب أحد الخصوم، وفي أي مرحلة تكون عليها الدعوى، أن يأمر باستدعاء الخبير ومناقشته في تقريره شفاهًا، أو كتابةً، ولها أن توجه إليه ما تراه من الأسئلة.

٢- العيوب التي تؤدي إلى بطلان تقرير الخبير الرقمي:

إذا أعد التقرير شخص غير مخوّل كخبير، مثل من شُطب اسمه من قائمة الخبراء، أو زوَّر مؤهلاته، أو بحال لم يباشر الخبير المنتدب شخصيًّا للمهمة الموكلة إليه، واعتمد على مساعديه، كذلك يعد مخالفًا إذا قام بأعمال الخبرة خبيرٌ غيرُ مُعَيَّنٍ من المحكمة، أو مُتَّفَقٌ عليه بين الخصوم[٧٨].

٣- سلطة القاضي بالأخذ بتقرير الخبير الرقمي.

عندما الحكم ببطلان تقرير الخبير بسبب وجود عيب مؤثر، أو مخالفة للإجراءات، لا يمكن للقاضي الاستناد إليه كدليل في القضية، وإلا كان حكمه معيبًا.

كما يجوز للقاضي متى ما كانت الدعوى تتطلب رأيًا فنيًا جديدًا إصدار أمر بإجراء خبرة أخرى، سواء عن طريق ندب خبير آخر، أو تشكيل لجنة من الخبراء، والهدف من ذلك هو الوصول إلى تقرير يعالج النقاط الفنية المعقدة التي لم يغطيها التقرير السابق بشكل صحيح.

ورغم ذلك، إذا كانت بيانات التقرير الباطل صحيحة وتتفق مع الوقائع، والمستندات المتاحة، يجوز للقاضي الاستناد إلى تلك الأجزاء دون الحاجة إلى خبرة جديدة، بشرط أن تكون تلك البيانات واضحة وغير متأثرة بالعيوب[٧٩].

---

(٧٨) بو فاتح أحمد، سلطة القاضي المدني إزاء تقرير الخبرة القضائية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية الحقوق، جامعة عمار ثليجي، الأغواط، المجلد ٨، ٢٠١٩م، ص١٠، وانظر إلى: معتصم خالد محمود حيف، الخبرة القضائية في القضايا الحقوقية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٤م، ص١٣٩.

(٧٩) معتصم خالد محمود حيف، مرجع سابق، ص١٤٠.

(ISSN: 2537- 0758)

ثانياً: مبدأ اقتناع القاضي بالأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي:

إن القاضي يواجه تحديات معقدة عن النظر في الأدلة الرقمية المستخلصة من الذكاء الاصطناعي، ومن أبزر هذه التحديات هي الموازنة بين مصلحة المجتمع في تحقيق الردع العام، ومصلحة الأفراد في الحفاظ على حقوقهم وحرياتهم، ورغم ذلك، فإن القاضي يتمتع بسلطة تقديرية كاملة في رفض أو قبول الدليل الرقمي المستخلص بناءً على اقتناعه الشخصي، ويعتمد القاضي في هذا الاقتناع على أساس العقل والمنطق، مع مراعاة الخصوصية العلمية للأدلة الرقمية المستخلصة من الذكاء الاصطناعي، والتي تتطلب خبرات دقيقة وارتباطها بالتقنيات الحديثة، لهذا السبب؛ يمكن للقاضي أن يستعين بالخبراء المختصين في هذا المجال، حيث يساعد هؤلاء الخبراء في توضيح الأمور التقنية المعقدة التي قد لا يكون القاضي متمكنًا منها(٨٠).

كما أن مسألة اقتناع القاضي في الحكم الجنائي يعتمد على الأدلة المطروحة أمامه لتكوين هذه القناعة، لكن ليس بالضرورة أن تكون كل الأدلة التي يعتمد عليها القاضي حاسمة أو قاطعة في كل جزئية من القضية، حيث أن الأدلة تكون عادةً متساندة، بمعنى أن كل دليل يُكمل الآخر، ولا يتم النظر إلى كل دليل بشكل منفصل عن الأدلة الأخرى، فالقاضي يُقيّم كل الأدلة بشكل جماعي، ولا يناقش كل دليل على حدة، بل يراها في مجموعتها حتى يكوّن عقيدته ويحكم بناءً عليها.

وترتيبًا على ما سبق، نرى أن القاضي يتمتع بسلطة تقديرية واسعة في التعامل مع تقرير الخبير الرقمي، حيث يمكنه قبوله كاملًا، أو جزئيًا، أو رفضه بناءً على قناعته الشخصية، مع ضرورة توضيح أسباب الرفض في حكمه، كما أن القاضي يتمتع بسلطة فحص دقة الإجراءات التي تمت أثناء إعداد التقرير، ويمكنه رفض التقرير إذا شابته عيوب مؤثرة، أو مخالفة للإجراءات القانونية.

بالإضافة إلى أن القاضي يمكنه إصدار أمر بإجراء خبرة جديدة إذا كان التقرير غير كافٍ، أو لم يعالج النقاط الفنية بشكل صحيح، لكن في حال كانت بعض البيانات الواردة في التقرير الباطل صحيحة وتتوافق مع الواقع، يجوز للقاضي أن يعتمد على تلك

(٨٠) ميادة مصطفى المحروقي، مرجع سابق، ص١١١.

الأجزاء دون الحاجة لإجراء خبرة جديدة، شريطة أن تكون تلك البيانات غير متأثرة بالعيوب.

أما بالنسبة للأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي، فإن القاضي يعتمد في قبوله، أو رفضه على اقتناعه الشخصي المبني على العقل والمنطق، مع مراعاة الخصوصية العلمية لهذه الأدلة، وقد يستعين القاضي بالخبراء لفهم الجوانب التقنية المعقدة التي قد تكون خارجه عن نطاق خبراته.

الخاتمة

بعون الله وتوفيقه تم الانتهاء من هذه الدراسة، حيث تبين لنا من خلالها أن التحديات الإجرائية في قبول الأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي تتمثل في عدة جوانب رئيسية: فهم تقنيات الذكاء الاصطناعي المستخدمة لاستخلاص الأدلة الرقمية، ومشروعية استخدام هذه التقنيات وفقًا للمعايير القانونية، والالتزام بالإجراءات الجزائية لضمان قبول الأدلة في المحاكم، كما تبرز أهمية دور الخبير الرقمي في تقديم تقارير محايدة، مع التأكيد على سلطة القاضي في قبول الأدلة بناءً على تقييمه لتقرير الخبير، و استنادًا إلى ما تقدم، فقد خلصت الدراسة إلى عدد من النتائج التي تم الاستناد إليها في وضع التوصيات اللازمة:

أولًا: **النتائج**:

- تظهر الدراسة أن الأدلة الرقمية، بما في ذلك المستخلصة باستخدام تقنيات الذكاء الاصطناعي، تُعتبر أدلة قانونية معترف بها، شريطة أن يتم جمعها وتحليلها وفقًا للإجراءات القانونية الدقيقة التي تكفل سلامتها وحجيتها أمام القضاء.
- تفيد الدراسة إلى أن الذكاء الاصطناعي يعد وسيلة قوية تساعد في تحسين الأداء في عدة مجالات مثل: الأمن العام، والصحة، والوقاية من الجريمة، ويتميز بقدرته على معالجة البيانات واستخلاص الأدلة الرقمية.
- توضح الدراسة أن هناك نوعين رئيسيين من التقنيات المستخدمة في جمع وتحليل الأدلة الرقمية، الأول يشمل تقنيات الذكاء الاصطناعي التي تُعد مصدرًا لتوليد الأدلة الرقمية، أما الثاني فيتعلق بتقنيات الذكاء الاصطناعي التي تستخدم لتحليل هذه الأدلة.

(ISSN: 2537- 0758)

- تفيد الدراسة إلى أن مشروعية استخدام تقنيات الذكاء الاصطناعي تتطلب تأطيرًا قانونيًّا واضحًا يحافظ على حقوق الأفراد وحماية خصوصياتهم، وهنا يتم تحديد الضوابط القانونية لاستخدام هذه التقنيات في الأماكن العامة والخاصة، مع التزم الأنظمة المحلية والدولية بحماية الخصوصية وحقوق الأفراد من الانتهاك.
- تشير الدراسة إلى أن إجراءات جمع الأدلة الرقمية، يجب أن تتماشى وفقًا للأنظمة المعمول بها، مع مراعاة الخصائص الفنية للأدلة الرقمية.
- تبين الدراسة أهمية الخبير الرقمي في التحقيقات الجنائية المتعلقة بالأدلة الرقمية، حيث يعد عنصرًا أساسيًا في تحليل الأدلة الرقمية بدقة وحيادية باستخدام تقنيات الذكاء الاصطناعي، مع ضرورة الالتزام بالأنظمة والصلاحيات.
- تفيد الدراسة إلى أن قبول القاضي للأدلة الرقمية المستخلصة باستخدام الذكاء الاصطناعي يتوقف على تحقق مشروعية إجراءات جمعِها.
- يتمتع القاضي بسلطة تقديرية واسعة في التعامل مع تقرير الخبير الرقمي، إذ يمكنه قبوله كاملًا، أو جزئيًا، أو رفضه بناءً على قناعاته الشخصية، مع ضرورة توضيح أسباب ذلك في حكمه.

ثانياً: **التوصيات**:

نظرًا لأهمية تطوير تقنيات الذكاء الاصطناعي لاستخلاص الأدلة الرقمية في تعزيز العدالة الجنائية، والتصدي للجرائم التقنية التي تشكل تهديدًا للأمن، والاستقرار، **توصي الدراسة بما يلي:-**

- نوصي بإضافة نصوص في نظام الإجراءات الجزائية متخصصة لتنظيم، وجمع، وتأمين الأدلة الرقمية، لضمان مشروعية الإجراءات المتبعة وحماية حقوق الأفراد، مع تحقيق التوازن بين تطبيق القانون، واحترام الخصوصية.
- وضع إطار قانوني لتنظيم استخدام تقنيات الذكاء الاصطناعي في جمع الأدلة الرقمية بشكل آمن، مع ضمان حماية الخصوصية، مع ضمان اتخاذ إجراءات تقنية تحمي من التلاعب بالبيانات وتؤكد على دقتها.
- نوصي بتحديد المسؤولية الجنائية بوضوح بين الأطراف المعنية في استخدام تقنيات الذكاء الاصطناعي في جمع الأدلة الرقمية، لضمان المحاسبة في حالة حدوث جريمة، أو انتهاك لحقوق الأفراد.

قائمة المراجع

أولاً: **القرآن الكريم**.

ثانياً: **معاجم اللغة**.

- أحمد محمد علي الفيومي، المصباح المنير في غريب الشرح الكبير، المكتبة العلمية، بيروت، ١٩٨٨م.
- أحمد مختارعبد الحميد عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، ١٤٢٩هـ.
- جمال الدين بن مكرم ابن منظور، لسان العرب، دار إحياء التراث، بيروت، ١٩٨٨م.

ثالثاً: **الكتب القانونية**.

- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٨م.
- أسماء السيد محمد، كريمة محمود محمد، تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا التعليم، المجموعة العربية للتدريب والنشر، القاهرة، ٢٠٢٠م.
- أشرف شمس الدين، شرح قانون الإجراءات الجنائية، القسم الأول، دار النهضة العربية، القاهرة، ٢٠١٢م.
- زكي محمد شناق، الوجيز في نظام الإجراءات الجزائية السعودي، مكتبة الملك فهد الوطنية للنشر، الرياض، ١٤٣١هـ.
- سعد الغالب ياسين، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمّان، ٢٠١٢م.
- سهى إبراهيم عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، جامعة القدس، كلية الحقوق، القدس، ٢٠١٤م.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠م.
- عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، القاهرة، ٢٠١٩م.
- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٧م.
- عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠١م.

(ISSN: 2537- 0758)

- عبد الله سعيد عبد الله الوالي، المسؤولية المدنية عن أضرار تطبيقات الذكاء الاصطناعي في القانون الإماراتي، دار النهضة العلمية، دبي، ٢٠٢١م.
- عمر محمد أبو بكر ابن يونس، الإجراءات الجنائية عبر الانترنت، في ترجمة المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا للدليل الإلكتروني في التحقيقات الجنائية، بدون دار نشر، ٢٠٠٤م.
- محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م.
- مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ٢٠٠٨م.
- معتصم خالد محمود حيف، الخبرة القضائية في القضايا الحقوقية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٤م.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦م.

رابعاً: الرسائل العلمية (الدكتوراه، الماجستير).

- رسائل الدكتوراه:

- أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، ٢٠١٢م.
- عمر محمد أبو بكر ابن يونس، الإجراءات الجنائية عبر الانترنت، رسالة دكتوراه، ترجمة المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا للدليل الإلكتروني في التحقيقات الجنائية، بدون دار نشر، ٢٠٠٤م.
- مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، رسالة دكتوراه، مطابع الشرطة، القاهرة، ٢٠٠٨م.

- رسائل الماجستير:

- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١١م.
- سلامة محمد المنصوري، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، رسالة ماجستير، جامعة الإمارات العربية المتحدة، كلية القانون، أبو ظبي، ٢٠١٨م.

خامساً: المجلات والمقالات العلمية.

- أسماء جابر علي مهران، فحص انعكاسات الجريمة المشهودة التي تم ضبطها بوساطة كاميرا المراقبة أو الهواتف الذكية أو البث المباشر على نمذجة السلوك الإجرامي، مجلة كلية الآداب، العدد ٧١، جامعة بني سويف، بني سويف، ٢٠٢٤م.
- بو فاتح أحمد، سلطة القاضي المدني إزاء تقرير الخبرة القضائية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية الحقوق، جامعة عمار ثليجي، الأغواط، المجلد ٨، ٢٠١٩م.
- البراء جمعان محمد الشهري، استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة، المجلة العربية للنشر العلمي، رماح، ٢٠٢٤م.
- تامر محمد صالح، التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، كلية الحقوق، المنصورة، ٢٠٢١م.
- جاسم خربيط خلف، التفتيش في الجرائم المعلوماتية، مجلة الخليج العربي، مركز دراسات الخليج العربي، جامعة البصرة، المجلد٤١، العدد ٣-٤، ٢٠١٣م.
- سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي، المجلة الدولية للقانون، دار جامعة حمد بن خليفة للنشر، الدوحة، ٢٠١٧م.
- سعد علي تركي الجلعود، الدليل الرقمي وأثره في الإثبات: دراسة فقهية تطبيقية مقارنة بالنظام السعودي، مجلة العلوم الشرعية، المنظومة، ٢٠٢٤م.
- شيخ هجيره، "دور الذكاء الاصطناعي في إدارة علاقة الزبون الإلكتروني للقرض الشعب الجزائري CPA"، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد١٠، العدد٢، جامعة حسيبة بن بوعلي، الشلف، ٢٠١٨م.
- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني، جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م.
- عادل عيسى الطوسي، بصمة الصوت سماتها واستخداماتها، المجلة العربية للدراسات الأمنية والتدريب، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ١٩٩٧م.

(ISSN: 2537- 0758)

- عايض علي القحطاني، دور الذكاء الاصطناعي في تحقيق التنمية المستدامة في إطار رؤية المملكة العربية السعودية ٢٠٣٠، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، المجلد٣، القاهرة، ٢٠٢٢م.
- عبد الرزاق مختار محمود، تطبيقات الذكاء الاصطناعي، مدخل لتطوير التعليم في ظل جائحة فيروس كورونا، المجلة الدولية للبحوث في العلوم التربوية، المجلة الدولية للبحوث، ٢٠٢٠م.
- محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد ٢١، العدد ٨١، ٢٠١٢م.
- محمد لطفي عبد الفتاح، البصمة الوراثية فرع من التكنولوجية الحيوية ودورها في الإثبات الجنائي "دراسة علمية قانونية" الحلقة الثانية، مجلة جامعة ابن يوسف، جمعية إحياء جامعة ابن يوسف، المجلد١٤، العدد١٥، ٢٠١٤م.
- ميادة مصطفى محمد المحروقي، ذاتية الضوابط الإجرائية للأدلة الرقمية في الأنظمة القانونية ذات الأصل اللاتيني والأنجلو أمريكي، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، كلية الحقوق، الإسكندرية، ٢٠١٩م.
- نزار أولاد مومن، الإثبات في الميدان الجنائي من خلال الدليل المعلوماتي، مجلة الفقه والقانون، الناشر صلاح الدين دكداك، العدد ٧١، ٢٠١٨م.
- هشام عمر أحمد الشافعي، التنظيم القانوني للطائرات المسيرة بدون طيار (الدرونز)، مجلة الفكر الشرطي، مجلد ٢٨، العدد ١١٠، الشارقة، ٢٠١٩م.

سادساً: التشريعات القانونية.

- الاتحاد الأوروبي، قانون الذكاء الاصطناعي (AI Act)، الرابط: https://eur-lex.europa.eu/legal-content/AR/TXT/?uri=CELEX%3A52021PC0206
- الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، تشريع قانوني أوروبي صادر عن الاتحاد الأوروبي لعام ٢٠١٦، الرابط: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

سابعاً: المؤتمرات.

- أزهري عبد الرحمن، نسرين بشير عثمان، "جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فاعلية"، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، الرياض، ٢٠١٥م.
- علي محمود علي حموده، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، دبي، ٢٦-٢٨ أبريل ٢٠٠٣.
- اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي، المؤتمر العام، الدورة ٤١، باريس، نوفمبر ٢٠٢١م.

ثامناً: القرارات الدولية.

- مجلس حقوق الإنسان التابع للأمم المتحدة. قرار الحق في الخصوصية في العصر الرقمي، A/HRC/RES/42/15، ٢٠١٩ . https://undocs.org/A/HRC/RES/42/15

تاسعاً: الاتفاقيات الدولية.

- الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) ٢٠٠١م، المعتمدة من لجنة وزراء مجلس أوروبا مجموعة المعاهدات الأوروبية – رقم١٨٥.

عاشراً: المواقع الإلكترونية.

- تقنيات آرلو، كاميرات الأمان الذكية باستخدام الذكاء الاصطناعي والوصول عن بعد، https://www.arlo.com.
- تقرير "تبني تقنية سلسلة الكتل" الصادر عن المركز الوطني السعودي للتقنية (CST) في عام ٢٠٢٢م. تم الوصول إلى التقرير بتاريخ ٨/١٢/ ٢٠٢٤م عبر الرابط: https://www.cst.gov.sa/ar/Digitalknowledge/Documents/Blockchainadoptionar.pdf
- تقنية التعرف على الأنماط: دليل شامل لفهم أنواعها وتطبيقاتها، أرقام، ١٤ يونيو ٢٠٢٤، https://2u.pw/5IyhSsEe.
- تقنيات تحليل البيانات الضخمة، https://2u.pw/vn6UVczN

(ISSN: 2537- 0758)

- خلدون غسان سعيد، "تقنيات متطورة للتعرف على الوجوه". صحيفة الشرق الأوسط، ١١ فبراير ٢٠٢٠، جدة، https://tinyurl.com/2n7bxues.
- الطيران المدني تطلق خدماتها الإلكترونية لتصريح طائرات الدرونز، سبق، ١١ يناير ٢٠١٩، https://sabq.org/saudia/zhtdwn.
- القواعد الفيدرالية للأدلة– المادة الرابعة: الصلة وحدودها: القاعدة ٤٠١، https://www.law.cornell.edu/rules.
- وزارة الداخلية المملكة تستعرض أنظمة الذكاء الاصطناعي للأمن العام في معرض سيتي سكيب العالمي بالرياض: https://safiu.moi.gov.sa/wps/vanityurl/ar/home.
- وزارة الداخلية وسدايا تطلق عددًا من المعسكرات التدريبية في علوم البيانات والذكاء الاصطناعي"، https://www.spa.gov.sa/N2013946.
- IBM, Machine Learning versus Deep Learning,
- https://www.ibm.com/topics/machine-learning
- - Mapp v. Ohio, 367 U.S. 643 (1961), https://www.oyez.org/cases/1960/236 .

الحادي عشر: **الأنظمة والقوانين**.

- نظام الإثبات، مرسوم ملكي رقم (م/٤٣) وتاريخ ١٤٤٣/٥/٢٦هـ.
- نظام الإجراءات الجزائية، مرسوم ملكي رقم (م/٢) بتاريخ ١٤٣٥/١/٢٢هـ.
- نظام حماية البيانات الشخصية، مرسوم ملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.
- نظام استخدام كاميرات المراقبة الأمنية، مرسوم ملكي رقم (م/٣٤) وتاريخ ١٤٤٤/٣/٧هـ.
- نظام مكافحة الجرائم المعلوماتية، مرسوم ملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ.

الثاني عشر: **المراجع الأجنبية**.

- الكتب.

- Eoghan Casey, Digital Evidence and Computer Crime, 3rd Edition, London, Academic Press, 2011.

- القضايا.

- -United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995); David, 756 F. Supp. 1392; Morales-Ortiz, 376 F. Supp. 2d 1142 n.2.