أدلة الإثبات المستمدة من الذكاء الاصطناعي في المسائل الجنائية

بين الاعتداد القضائي والضوابط القانونية

Evidence derived from AI in criminal matters Between Judicial Credibility and Legal Controls

ط. د حسين عبد المعطي عبد النبي

مستشار قانوني ومحكم معتمد – باحث في مرحلة الدكتوراه في القانون العام

(جمهورية مصر العربية)

hussienabdlmo3ty@gmail.com

د. خيري محمد شعبان

نائب رئيس مجلس الدولة – عضو هيئة تدريس منتدب في الجامعات المصرية

(جمهورية مصر العربية)

DOI: https://doi.org/10.70411/MJLS.4.1.2026346

تاريخ الاستلام: 08-12-2025 تاريخ المراجعة: 15-12-2025 تاريخ القبول: 15-12-2025

الملخص

يشهد العصر الرقمي تطورًا غير مسبوق في أدوات الإثبات الجنائي، مع تزايد الاعتماد على تقنيات الذكاء الاصطناعي (AI) في جمع الأدلة وتحليلها، مما يطرح إشكاليات جوهرية تتعلق بمشروعية هذه الأدلة، ومدى موثوقيتها، وحجيتها أمام القضاء. حيث تهدف الدراسة إلى تحليل الإطار القانوني والمعيار الناظم لاستخدام أدلة الذكاء الاصطناعي في المسائل الجنائية، من خلال مقارنة تحليلية بين الأنظمة القانونية في الدول العربية، ودول الاتحاد الأوروبي، واليابان.

إن الدراسة الماثلة تتناول نماذج متعددة لاستخدام الذكاء الاصطناعي في العمل الجنائي، مثل تقنيات التعرف على الوجوه، وتحليل البيانات الضخمة، وأنظمة التنبؤ بالسلوك الإجرامي، وتبحث مدى اتساق هذه التطبيقات مع المبادئ الدستورية، لا سيما مبدأ الشرعية الجنائية، وضمانات المحاكمة العادلة، وأخيرا وليس آخرًا حماية الخصوصية.

ومن الجدير بالذكر أنها كشفت عن تباين واضح في المواقف التشريعية والقضائية؛ ففي حين تتجه دول الاتحاد الأوروبي نحو تقييد استخدام هذه الأدلة ووضع أطر تشريعية صارمة لحماية الحقوق الأساسية، تعتمد منهجًا تكامليًا ومرنًا، يقوم على إدماج الأدلة الرقمية وتقنيات الذكاء الاصطناعي ضمن التشريعات العامة دون إصدار قانون موحد، مع إرساء ضوابط قضائية صارمة تكفل حماية الخصوصية وضمان مشروعية الدليل، مع غياب إطار قانوني موحّد أو معايير فنية ضابطة.

وخلصت الدراسة إلى أن القبول القضائي لأدلة الذكاء الاصطناعي يظل رهينًا بمدى موثوقية التقنية المستخدمة، وشفافية خوارزمياتها، ومدى احترامها لمبادئ العدالة الإجرائية. كما دعت الدراسة إلى ضرورة تطوير تشريعات وطنية واضحة، وإرساء معايير فنية وقانونية مشتركة، تضمن توازنًا فاعلا بين مقتضيات مكافحة الجريمة وحقوق الأفراد.

الكلمات المفتاحية: أدلة الإثبات الجنائي، التشريع الجنائي المقارن، المحاكمة العادلة، الخوارزميات العدلية، التحيز الخوارزمي، التقييم القضائي للتكنولوجيا.

Abstract

The digital age is witnessing an unprecedented development in criminal evidence tools, with increasing reliance on artificial intelligence (AI) technologies to collect and analyze evidence. This raises fundamental issues related to the legitimacy, reliability, and admissibility of this evidence before the courts. This study aims to analyze the legal and normative framework governing the use of AI evidence in criminal matters, through a comparative analytical comparison between the legal systems of Arab countries, the European Union, and Japan.

The study examines various models for the use of AI in criminal work, such as facial recognition technologies, big data analysis, and systems for predicting criminal behavior. It examines the consistency of these applications with constitutional principles, particularly the principle of criminal legality, fair trial guarantees, and privacy protection.

The study revealed a clear divergence in legislative and judicial positions. While European Union countries are moving toward restricting the use of such evidence and establishing strict legislative frameworks to protect fundamental rights, they are adopting an integrative and flexible approach based on integrating digital evidence and AI technologies into general legislation without issuing a unified law. This approach also establishes strict judicial controls to protect privacy and ensure the legitimacy of evidence, in the absence of a unified legal framework or controlling technical standards.

The study concluded that the judicial acceptance of AI evidence remains dependent on the reliability of the technology used, the transparency of its algorithms, and its adherence to the principles of procedural justice. The study also called for the development of clear national legislation and the establishment of common technical and legal standards that ensure an effective balance between the requirements of combating crime and the rights of individuals.

Keywords: criminal evidence, comparative criminal legislation, fair trial, forensic algorithms, algorithmic bias, judicial evaluation of technology.

المقدمة

يشكل الذكاء الاصطناعي أحد أبرز التحولات التقنية في العصر الحديث، إذ امتدت تطبيقاته إلى مختلف المجالات، من الاقتصاد والصحة إلى الأمن والقضاء. وفي ظل هذا التوسع، لم يكن المجال الجنائي بمعزل عن موجة التحول الرقمي، حيث بدأت تقنيات الذكاء الاصطناعي تفرض وجودها في مراحل مختلفة من العدالة الجنائية، بدءًا من التحقيق وجمع الأدلة، وصولًا إلى تحليلها وتقديمها أمام القضاء.

غير أن هذا التحول التقني، على الرغم من فوائده في تسريع الإجراءات وتحسين كفاءة العدالة، يثير تساؤلات قانونية عميقة تتعلق بمشروعية أدلة الذكاء الاصطناعي، ومدى موثوقيتها، وحجيتها أمام القضاء، خاصة في ظل الطبيعة "الصندوقية" لبعض الخوارزميات، وغموض أسس اتخاذ القرار داخلها، ما قد يُعرّض حقوق الأفراد، لا سيما الحق في المحاكمة العادلة والخصوصية، لانتهاكات خطيرة.

وعليه، تسعى هذه الدراسة إلى معالجة إشكالية محورية تتمثل في:

"مدى مشروعية وحجية أدلة الإثبات المستمدة من أنظمة الذكاء الاصطناعي في المسائل الجنائية، وما حدود القبول القضائي لها في ظل التباين بين الأنظمة القانونية المختلفة؟"

وللإجابة عن هذه الإشكالية، تعتمد الدراسة منهجًا تحليليًا مقارنًا بين ثلاثة أنظمة قانونية رئيسة: النظام العربي، ونظام الاتحاد الأوروبي (المتسم بالحذر التنظيمي والاهتمام بحقوق الإنسان)، والنظام الياباني. وذلك لهدف استجلاء الفروق في المواقف القانونية والقضائية تجاه هذه الأدلة، وتحليل مدى ملاءمتها مع الضمانات الدستورية والإجرائية في كل نظام.

ومن الجلي أن هذا الموضوع لا يكتفي بطرح أسئلة تقنية أو قانونية بحتة؛ بل يلامس جوهر التوازن المطلوب بين حماية المجتمع من الجريمة وضمان حقوق الأفراد في مواجهة أدوات قد تكون فاعلة، لكنها غير خالية من المخاطر القانونية والأخلاقية.

أهمية البحث

تكمن أهمية الدراسة من خلال تناولها قضية حديثة وجدلية تتعلق بحجية أدلة الذكاء الاصطناعي في المسائل الجنائية، في ظل التباين بين سرعة التطور التكنولوجي وبطء الاستجابة التشريعية. وتُسهم أيضًا في توضيح التحديات المرتبطة بالعدالة الخوارزمية والخصوصية الرقمية، مما يجعلها ذات قيمة لصنّاع القرار والباحثين، في سبيل وضع إطار قانوني يضمن الاستخدام المسؤول لهذه التقنيات.

أهداف البحث

تهدف الدراسة إلى وضع إطار قانوني منظم لاستخدام أدلة الذكاء الاصطناعي في المسائل الجنائية، مع التركيز على مدى توافقها مع المبادئ الدستورية والضمانات الإجرائية، والكشف عن أوجه القصور أو الغموض التشريعي في النظم القانونية العربية فيما يتعلق بحجية الأدلة المستمدة من تقنيات الذكاء الاصطناعي، وتحديد الثغرات التي قد تؤثر على حقوق المتهم وضمانات المحاكمة العادلة، ومقارنة المواقف القضائية والتشريعية بين الدول العربية والدول الأجنبية بشأن القبول أو الرفض لأدلة الذكاء الاصطناعي، واستجلاء الأسس القانونية والفلسفية التي تحكم هذه المواقف.

إشكالية البحث

يُثير استخدام الذكاء الاصطناعي في الإثبات الجنائي إشكالية قانونية تتعلق بمشروعية الأدلة الناتجة عن خوارزميات غير بشرية، في ظل غموض آلية عملها، وغياب الشفافية والحياد أحيانًا. وتتفاقم هذه الإشكالية مع غياب التشريعات الواضحة في الدول العربية، مقارنة ببعض الدول الغربية التي بدأت بوضع أطر قانونية متقدمة.

وتتمثل إشكالية الدراسة في الإجابة عن التساؤل الآتي:

ما مدى حجية ومشروعية أدلة الإثبات المستمدة من أنظمة الذكاء الاصطناعي في المسائل الجنائية؟ وما حدود القبول أو الرفض القضائي لها في ظل التباين التشريعي والقضائي؟

ويتفرع عن هذا التساؤل الرئيس عدد من التساؤلات الفرعية، من أبرزها:

1. ما مدى توافق أدلة الذكاء الاصطناعي مع المبادئ الأساسية للمحاكمة العادلة، خصوصًا مبدأ المواجهة وحق الدفاع؟
2. هل تفي هذه الأدلة بمتطلبات الشفافية والموثوقية القانونية؟
3. كيف تعاملت المحاكم في النظم المقارنة مع هذا النوع من الأدلة؟
4. وما السبل التشريعية الكفيلة بإيجاد توازن بين فاعلية أدوات الذكاء الاصطناعي، وضمان حقوق المتهمين؟

منهجية البحث

تعتمد هذه الدراسة المنهج التحليلي المقارن، بتحليل النصوص القانونية والقضائية المتعلقة بأدلة الذكاء الاصطناعي في المسائل الجنائية، ومقارنتها بين الدول العربية، والاتحاد الأوروبي، واليابان. ويُستخدم المنهج التحليلي لتفكيك المفاهيم ومدى توافقها مع مبادئ الشرعية والدفاع والخصوصية، بينما يُوظف المنهج المقارن لرصد أوجه التشابه والاختلاف بين النظم القانونية واستخلاص توصيات لتطوير التشريعات العربية.

المبحث الأول

أدلة الذكاء الاصطناعي في المجال الجنائي

في ظل التحولات المتسارعة التي يشهدها العالم الرقمي، بات الذكاء الاصطناعي من أبرز الأدوات التي غيّرت ملامح العدالة الجنائية، سواء أكان على مستوى التحري الجنائي أم تحليل الأدلة أم حتى تقديم التوصيات القضائية[1]. ولم تعد أجهزة العدالة الجنائية تعتمد فقط الوسائل التقليدية في الإثبات؛ بل أصبحت تتجه نحو تقنيات حديثة تستند إلى خوارزميات معقدة، قادرة على معالجة كميات ضخمة من البيانات واستخلاص مؤشرات جنائية يُعوّل عليها في اتخاذ قرارات مصيرية، كالتوقيف، الإدانة، أو التبرئة[2].

يسهم الذكاء الاصطناعي في توفير أدلة رقمية دقيقة، والتي تعمل على تقديم رؤى متكاملة وعميقة للسلوكيات والأنشطة، ما يسهم بشكل كبير في تعزيز قدرات المحققين على كشف الجرائم، وتحليل الأنماط السلوكية، وتتميز هذه الأدلة بكونها مستندة إلى تحليل علمي منهجي للبيانات، بعيدًا عن التخمين، ما يجعلها أدوات موثوقة يُمكن اعتمادها أمام القضاء.

غير أن هذه الأدلة المستمدة من أنظمة الذكاء الاصطناعي تطرح إشكاليات قانونية ومفاهيمية غير مسبوقة، تمس جوهر مبادئ الشرعية الجنائية وضمانات المحاكمة العادلة، لا سيما حين تكون مبنية على أنظمة "غير شفافة"، يصعب تفسير نتائجها أو مساءلة مصدرها[3]. الأمر الذي يستدعي فحصًا دقيقًا لطبيعتها القانونية، وحدود قبولها، والمعايير التي ينبغي أن تستند إليها في تقييم مشروعيتها القضائية[4].

1. Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York University Press.
2. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Journal of Law and Information Technology, 27(2), 91–121. accessed 2 May 2025 : https://doi.org/10.1093/ijlit/eaz002.
3. European Union Agency for Fundamental Rights (FRA). (2020). Getting the future right – Artificial intelligence and fundamental rights. Publications Office of the European Union. accessed 2 May 2025 : https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights.
4. Sulyok, M. (2021). The evidentiary value of AI-based data in criminal proceedings: A European perspective. New Journal of European Criminal Law, 12(4), 473–489. accessed 2 May 2025 : https://doi.org/10.1177/20322844211044777.

المطلب الأول

المفهوم القانوني والتقني لأدلة الذكاء الاصطناعي

يمثل الذكاء الاصطناعي طفرة تقنية في مجال العدالة الجنائية، حيث يُستخدم في استخراج أنماط معينة من البيانات الضخمة، والتنبؤ بسلوك إجرامي، والتعرف على الوجوه، وتحليل الصوت، والتنقل، وحتى توقع النتائج القضائية. وتُعرّف أدلة الذكاء الاصطناعي بأنها المعلومات أو المخرجات الناتجة عن تحليل البيانات باستخدام أنظمة ذكية تعتمد خوارزميات تعلم الآلة (Machine Learning) أو الذكاء المعرفي (Cognitive AI)، ويتم توظيفها كوسيلة إثبات في الإجراءات الجنائية[1].

أن الأدلة الرقمية هي كل ما يُستمد 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.

تعريف الأدلة الرقمية: بأنها الأدلة التي تم أخذها من الأجهزة الإلكترونية، على هيئة مجالات كهربائية أو مغناطيسية، ويمكن تجميعها وتحليلها عبر برامج خاصة، لتقديمها كدليل إثبات أمام القضاء[2].

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[3].

واتجه رأي أول 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[4].

---

1. Brkan, M. (2019). Do algorithms rule the world ? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Journal of Law and Information Technology, 27(2), 91–121. accessed 3 May 2025 : https://doi.org/10.1093/ijlit/eaz002.

2. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت– رسالة ماجستير–، جامعة الشرق الأوسط للدراسات العليا، دار الثقافة للنشر والتوزيع، عمان، (2011) ، ص230.

3. عائشة بن قارة مصطفي، حجية الدليل الإلكتروني في مجال الأثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، (2010)، ص61.

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

واتجه رأي آخر إلى أن هذه الأدلة قد تكون صورًا وفيديوهات ونتائج تحليل صوتي، أو توقعات سلوكية ناتجة عن تحليل بيانات ضخمة، تُعالج باستخدام خوارزميات لا تعمل دائمًا على أساس قواعد صريحة يمكن تفسيرها؛ بل تعتمد ما يُعرف بالصندوق الأسود(Black Box Algorithms) ، ما يصعب فهم الأساس الذي قامت عليه النتائج أو مدى دقتها[1].

وبناءً على ما سبق فإن الأدلة الرقمية: هي دليل يحتوي على بيانات أو معلومات متوفرة بوسائل رقمية تستخرج من تقنيات الذكاء الاصطناعي، سواء أكانت صورًا وفيديوهات، أم نتائج تحليل صوتي، أم توقعات سلوكية ناتجة عن تحليل بيانات ضخمة، تُعالج باستخدام خوارزميات، والتي يستطيع جمعها وتحليلها عن طريق المتخصصين بذلك باستخدام تقنيات الذكاء الاصطناعي لتقديمها كدليل إثبات أمام القضاء.

أما من الناحية القانونية، فإن هذه الأدلة ما تزال تفتقر إلى تعريف موحد أو تنظيم صريح في معظم الأنظمة القانونية، الأمر الذي يطرح تساؤلات حول مدى وصفها دليلًا جنائيًا مشروعًا، ومدى قبولها في ضوء قواعد الإثبات التقليدية التي تقوم على وضوح المصدر، وإمكان المناقشة، وحق الدفاع[2]. وقد حذّرت تقارير أوروبية من خطورة استخدام هذه الأنظمة دون إطار قانوني يضمن الشفافية والمساءلة، لا سيما في ظل المخاطر المتعلقة بالتحيز الخوارزمي وانتهاك الخصوصية[3].

وعلى الرغم من أهمية هذه الأدلة، إلا أننا نرى أن استخدامها دون اتّباع معايير الشفافية قد يؤدي إلى نتائج قضائية غير منضبطة، وبالأخص في حالات الاعتماد على خوارزميات غير خاضعة للتدقيق القضائي.

---

1. Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York University Press.
2. Sulyok, M. (2021). The evidentiary value of AI-based data in criminal proceedings: A European perspective. New Journal of European Criminal Law, 12(4), 473–489. accessed 3 May 2025 : https://doi.org/10.1177/20322844211044777.
3. European Union Agency for Fundamental Rights (FRA). (2020). Getting the future right – Artificial intelligence and fundamental rights. accessed 3 May 2025 : https://fra.europa.eu/.

المطلب الثاني

الطبيعة القانونية للأدلة الرقمية وحدودها في إطار الشرعية الجنائية

أولًا: الطبيعة القانونية للأدلة الرقمية:

تُعد الأدلة الرقمية من وسائل الإثبات الحديثة في النظام القانوني، وتكتسب أهمية متزايدة في كل من القضايا الجنائية والمدنية. وتشمل هذه الأدلة المعلومات المستخرجة من الأجهزة الإلكترونية مثل الحواسيب، الهواتف الذكية، الخوادم، أو أي أجهزة أخرى تحتوي بيانات يمكن استخدامها في التحقيقات أو المحاكمات القانونية. ومع التقدم التكنولوجي المتسارع وتزايد الاعتماد على البيانات الرقمية في مختلف مجالات الحياة، أصبحت الأدلة الرقمية أداة محورية في إثبات أو دحض الوقائع الجنائية[1].

يُعد الدليل الرقمي ذا طبيعة رقمية ثنائية رقمية، حيث يتم تمثيله من خلال النظام الثنائي (0) و(1)، وهو النظام الذي تُسجل به البيانات والمعلومات كافة من رموز وأشكال، وحروف، وألوان، وأصوات، وغيرها داخل الوسيلة الرقمية، فجميع مدخلات ومخرجات الوسائل الرقمية تتمثل في (0)و(1) حيث يتم إدخالها كمعلومات في تلك الوسائل الرقمية، ويتم تحويلها إلى النظام الرقمي، فإن الدليل بهذه الحالة يعد برمجية الأجهزة، سواء أكانت هواتف ذكية، أم حواسيب، أم من تقنيات الذكاء الاصطناعي، أم غيرها[2].

وتتواجد هذه الأدلة ضمن ما يُعرف بالبيئة الرقمية أو الفضاء السيبراني؛ فعلى سبيل المثال، إذا تم الاحتفاظ بصور أو مقاطع فيديو مستمدة من كاميرات المراقبة، أو بملفات تحتوي على أرقام دخول سرية للمواقع فإنه يعد دليلًا رقميًا، فعلى الرغم من تنوع واختلاف هيئات الدليل الرقمي، وأشكاله؛ إلا أن طبيعته واحدة، وهي علاقته الوثيقة بتكنولوجيا المعلومات، وأنه يتكون من رقمي (0) و(1)، علمًا أن هذه الطبيعة تؤثر على حجم الملف وتكوينه[3].

---

1. Chan, J., & Lee, K. (2019). Digital evidence in the modern legal system : Challenges and opportunities. International Journal of Legal Technology, 22(4), 213-230. accessed 3 May 2025 : https://doi.org/10.1016/j.ijlt.2019.04.003.

2. محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، (2006)، ص22.

3. عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الإنترنت، في ترجمة المرشد الفيدرالي الاميركي لتفتيش وضبط الحواسيب وصولاً للدليل الإلكتروني في التحقيقات الجنائية، بدون دار نشر، (2004)، ص 995.

وفي ظل التطور التكنولوجي المتسارع، أصبحت الأدلة الرقمية عنصرًا أساسيًا في منظومة الإثبات الجنائي والمدني، وتشمل طيفًا واسعًا من الوسائط كالسجلات الإلكترونية، والبصمات الرقمية، وبيانات التواصل الاجتماعي. ويعكس هذا التنوع التحول في وسائل الإثبات التقليدية، وما يطرحه من فرص وتحديات للعدالة الحديثة.

ثانيًا: حدود قبول أدلة الذكاء الاصطناعي في إطار الشرعية الجنائية:

تُثير أدلة الذكاء الاصطناعي في المجال الجنائي إشكاليات معقدة تتعلق بمبدأ الشرعية الجنائية، الذي يقضي بأنه "لا جريمة ولا عقوبة ولا إجراء إلا بنص"، الأمر الذي يستوجب أن تستند وسائل الإثبات إلى إطار قانوني مشروع وواضح. فعلى الرغم من التطور التقني الهائل في أدوات الذكاء الاصطناعي، إلا أن قبولها كدليل إثبات أمام القضاء يظل مشروطًا بتحقق مجموعة من الضمانات القانونية والحقوقية.

وتتمثل أولى هذه الضمانات في مدى مشروعية جمع الدليل، بحيث يتم ذلك وفقًا لنصوص القانون، وبما لا يمس حقوق الدفاع أو ينتهك الخصوصية، تطبيقًا لمبدأ "حجية الدليل ترتبط بمشروعية وسيلة الحصول عليه"[1].

كما يتعين أن تكون الخوارزميات المستخدمة في تحليل البيانات قابلة للتفسير والمراجعة القضائية، وألا تشكل ما يُعرف ب "الصندوق الأسود" الذي يُعجز القاضي أو الدفاع عن فهم آلية عمله، حيث يُعد ذلك إخلالًا بمبدأ المواجهة وشفافية الإجراءات المنصوص عليها ضمن ضمانات المحاكمة العادلة[2].

كما يواجه اعتماد الأدلة المستمدة من الذكاء الاصطناعي تحديًا إضافيًا يتمثل في احتمال وجود تحيز خوارزمي، الأمر الذي قد يُفضي إلى نتائج غير دقيقة أو غير عادلة تمس حق المتهم في المساواة وعدم التمييز.

لذلك، تشترط بعض النظم القانونية، مثل الاتحاد الأوروبي، أن تخضع أدوات الذكاء الاصطناعي لتقييمات أولية للامتثال القانوني قبل استخدامها في الإجراءات الجنائية[3].

---

1. محمود الخطيب، الحماية الجنائية للبيانات الرقمية: دراسة مقارنة، دار الجامعة الجديدة، (2022)، ص174.

2. Surden, H. (2019). Artificial intelligence and law: An overview. Georgia State University Law Review, 35(4), 1305–1338.accessed 4 May 2025 : https://readingroom.law.gsu.edu/gsulr/vol35/iss4/4.

3. European Commission. (2021). *Proposal for a Regulation laying down harmonized rules* onartificial intelligence (Artificial Intelligence Act). Retrieved from : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 accessed 4 May 2025.

تتطلب مشروعية استخدام تقنيات الذكاء الاصطناعي تنظيمًا قانونيًا دقيقًا يحدد ضوابط استخدامها، لتفادي انتهاك حرية الأفراد وخصوصيتهم، وتحقيق التوازن بين الأمن العام وحماية الحقوق. وتعتمد هذه الأنظمة تحليل بيانات ضخمة، كثير منها ذات طابع شخصي، ما يثير تساؤلات حول مدى احترامها للحقوق الدستورية. وقد أكدت المحكمة الأوروبية لحقوق الإنسان على ضرورة أن يتم جمع البيانات واستخدامها في إطار قانوني واضح يوازن بين الأمن والحقوق الفردية[1]. وأي استخدام خارج هذا الإطار قد يؤدي إلى بطلان الدليل، خاصة وأن بعض أدوات الذكاء الاصطناعي قد تنتج قرارات منحازة بسبب تغذية بيانات غير متوازنة، ما يشكل خرقًا لمبدأ المساواة ويُضعف حجية الدليل[2].

يُثير استخدام الذكاء الاصطناعي في مجال الإثبات الجنائي تحديات خطيرة، تتعلق بشرعية الدليل ومشروعيته، خصوصًا في ضوء مبدأ الشرعية الجنائية الذي يقتضي وجود نصوص قانونية واضحة، ووسائل إثبات مشروعة، وإجراءات شفافة قابلة للمراجعة والطعن. وبناءً عليه، لا يمكن قبول الأدلة المستمدة من تقنيات الذكاء الاصطناعي إلا في ظل إطار قانوني صارم، يضمن احترام الحقوق الأساسية، وشفافية الخوارزميات، والمشروعية الإجرائية في جمع البيانات وتحليلها.

المطلب الثالث

الإشكاليات العملية والحقوقية المرتبطة بالأدلة الرقمية

أدى التطور التكنولوجي المتسارع في مجال الذكاء الاصطناعي إلى إثارة إشكاليات قانونية وحقوقية معقدة تتعلق بإمكان قبول الأدلة الناتجة عن هذه التقنيات أمام المحاكم الجنائية. وتنبع هذه الإشكاليات في التعارض المحتمل بين الخصائص التقنية للذكاء الاصطناعي من جهة، ومبادئ العدالة الجنائية وحقوق المتهم من جهة أخرى.

أولًا: غموض مصدر الدليل وعدم إمكان التحقق

تُعد صعوبة التحقق من مصدر وطريقة توليد الدليل المستخلص من الذكاء الاصطناعي، خاصة عندما تعتمد الخوارزميات بيانات ضخمة غير موثقة أو مستمدة مصادر غير واضحة أو مشكوك في

1. European Court of Human Rights (ECtHR). (2018). Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15.
2. Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.

موثوقيتها. ويؤدي ذلك إلى تعارض جوهري مع قواعد الإثبات التقليدية التي تشترط وضوح الدليل وإمكان التحقق من صحته ومصدره أمام المحكمة، تحقيقًا لمبدأ الشفافية وضمانات المحاكمة العادلة[1].

ثانيًا: خطر التحيّز والتمييز الخوارزمي

إذ إنّ التحيّز الكامن في البيانات المستخدمة لتدريب النماذج الخوارزمية قد يؤدي إلى نتائج تمييزية وغير عادلة، مما يسبب تمييزًا ضد فئات معينة على أساس العرق، أو الجنس، أو غيرها من الصفات الاجتماعية. ويؤثر هذا التحيّز بشكل مباشر على نزاهة العملية القضائية تهديدًا لمبدأي العدالة والمساواة أمام القانون، ما يفرض ضرورة تحسين جودة البيانات المستخدمة في هذه النماذج، وتصميم خوارزميات أكثر حيادية لضمان عدالة الإجراءات القانونية[2].

ثالثًا: التهديد لخصوصية الأفراد

توفر تقنيات الذكاء الاصطناعي إمكانات واسعة في مجال مراقبة وتحليل البيانات بشكل متطور ومستحدث، إلا أن إساءة استخدام هذه التقنيات أدت 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، ما يمثل انتهاكًا صارخًا للخصوصية الشخصية[3].

رابعًا: المساءلة والمسؤولية القانونية

عندما تعتمد جهات التحقيق أو القضاء أداة ذكاء اصطناعي لاستنتاج معلومات جنائية أو تقييم درجة الخطورة الإجرامية، فإن سؤال المسؤولية عن الخطأ أو الانحراف في النتائج يبقى معلقًا: هل المسؤول هو المبرمج؟ أم الجهة المستخدمة؟ أم الجهة القضائية التي اعتمدت الدليل؟ وهذا الغموض يخلق فراغًا تشريعيًا يجب معالجته لضمان المحاسبة والشفافية[4].

---

1. Borgesius, F. Z. (2018). Discrimination, Artificial Intelligence, and Algorithmic Decision-Making. Council of Europe Report.

2. اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي" المؤتمر العام، الدورة 41، باريس، (نوفمبر 2021) وهي توصية تهدف إلى وضع إطار أخلاقي شامل لاستخدام تقنيات الذكاء الاصطناعي، مع التركيز على تعزيز حقوق الإنسان، وحماية البيئة، وتشجيع التنوع الثقافي.

3. Solove, D. J. (2021). Understanding Privacy (2nd ed.). Harvard University Press.

4. Cath, C., et al. (2018). Artificial Intelligence and the 'Good Society' : The US, EU, and UK Approach. Science and Engineering Ethics, 24(2), 505-528.

خامسًا: ضعف قابلية المناقشة والمواجهة

وفقًا لمبدأ المواجهة، يجب أن يتمتع المتهم ومحاميه الحق الكامل في مناقشة وتفنيد الأدلة المقدمة ضده. إلا أن تعقيد أنظمة الذكاء الاصطناعي وصعوبة فهم الخوارزميات المستخدمة يشكلان عائقًا أمام ممارسة هذا الحق، ما يمسّ جوهر المحاكمة العادلة[1].

كما يُثير استخدام الذكاء الاصطناعي في الإثبات الجنائي تحديات قانونية وحقوقية، أبرزها مدى توافقه مع مبدأ الشرعية الجنائية، في ظل غياب نصوص واضحة وصعوبة فهم نتائج الخوارزميات. كما يطرح مخاوف من التحيّز الخوارزمي والمسؤولية عن نتائجه، ما يستدعي تأطيرًا تشريعيًا يوازن بين التطور التقني وضمانات العدالة.

1. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, Explainable, and Accountable AI for Robotics. Science Robotics, 2(6), eaan6080.

المبحث الثاني

موقف التشريعات المقارنة من أدلة الذكاء الاصطناعي في المسائل الجنائية

شهدت السنوات الأخيرة تطورًا ملحوظًا في توظيف تقنيات الذكاء الاصطناعي ضمن المنظومات العدلية، وخصوصًا في المجال الجنائي. وعلى الرغم مما توفره هذه التقنيات من إمكانات واعدة في مجالات التحليل الجنائي والتنبؤ بالجريمة، إلا أن مواقف التشريعات المقارنة تجاه استخدامها كأدلة إثبات لا تزال متفاوتة، تبعًا لاختلاف التطور التشريعي والتقني بين الدول.

وفي هذا السياق، يُثير اعتماد أدلة الذكاء الاصطناعي عدة تساؤلات حول مدى مشروعية استخدامها، وضمان توافقها مع المبادئ الدستورية، وعلى رأسها مبدأ الشرعية الجنائية، وحقوق الدفاع، والحق في محاكمة عادلة.

يتم استعراض وتحليل موقف ثلاث تجارب قانونية في هذا المجال، وهي: تجربة الاتحاد الأوربي، واليابان، وتجارب بعض الدول العربية.

المطلب الأول

الإطار القانوني العربي

على الرغم مما تشهده الدول العربية من تطور متسارع في مجالات الذكاء الاصطناعي وتطبيقاته، ما يزال الإطار القانوني لاستخدامها في المسائل الجنائية محدودًا، حيث تفتقر معظم الأنظمة إلى تشريعات خاصة تنظم اعتماد الذكاء الاصطناعي كدليل جنائي. ومع ذلك، يمكن الاستناد إلى بعض القواعد العامة في قوانين حماية البيانات ومكافحة الجرائم الإلكترونية كإطار غير مباشر، شريطة احترام مبادئ الشرعية وضمانات الدفاع وحقوق الإنسان.

أولًا: جمهورية مصر العربية

على الرغم من أن مصر قد شرعت في إدخال مفاهيم جديدة تتعلق بالتحول الرقمي في مجالات متعددة، إلا أن التعامل مع الأدلة الرقمية ما يزال في كثير من الأحيان يتم من خلال قواعد الإثبات التقليدية.

فقد صدر قانون مكافحة جرائم تقنية المعلومات (قانون رقم 175 لسنة 2018)، ويشمل البيانات الرقمية التي يتم جمعها عبر الإنترنت أو باستخدام تقنيات متقدمة مثل الذكاء الاصطناعي. وتنص بعض

مواد القانون على ضرورة اتّباع ضوابط دقيقة فيما يتعلق بكيفية جمع ومعالجة البيانات الشخصية، ما يضمن احترام حق الأفراد في الخصوصية وحمايتهم من الاستخدام غير المشروع لهذه البيانات[1].

ويحدد قانون الإجراءات الجنائية المصري (قانون رقم 150 لسنة 1950) مبادئ أساسية فيما يتعلق بكيفية جمع الأدلة في القضايا الجنائية، حيث يشترط أن يكون الدليل الذي يُعتمد قد تم جمعه بطريقة قانونية وبموافقة الجهات القضائية المتخصصة. ولكن لا توجد نصوص صريحة توضح كيفية استخدام أو قبول الأدلة المستخلصة باستخدام تقنيات الذكاء الاصطناعي، ما يجعل الموضوع غامضًا ويعتمد التفسير القضائي في إطار القوانين العامة[2].

ومع تطور البيئة الرقمية وتعقّد التعامل مع البيانات الشخصية، جاء قانون حماية البيانات الشخصية رقم 151 لسنة 2020 ليساهم في ترسيخ أسس قانونية جديدة لحماية المعطيات الرقمية. وعلى الرغم من أن القانون لا يتناول الأدلة الرقمية بشكل صريح، إلا أن أحكامه تُشكّل إطارًا تنظيميًا مهمًا يُؤثر على مشروعية جمع ومعالجة وتقديم هذه الأدلة أمام الجهات القضائية. فقد نص القانون على ضرورة الحصول على موافقة صريحة من الشخص المعني قبل جمع بياناته أو معالجتها، كما حدّد مجموعة من الحقوق للأفراد تشمل: الحق في معرفة كيفية استخدام بياناتهم، والحق في تعديلها أو محوها، وهو ما يُعد عاملًا حاسمًا في تحديد مدى قانونية الدليل الرقمي إذا تَمثَّل في بيانات شخصية جُمعت أو استُعملت دون إذن[3].

كما أقر القانون إنشاء هيئة حماية البيانات الشخصية كمؤسسة رقابية مستقلة تختص بالإشراف على الالتزام بتطبيق قواعد حماية البيانات، ومنح التراخيص، وتلقي الشكاوى. وتكتسب هذه الهيئة أهمية خاصة في دعم الثقة في الدليل الرقمي، لا سيما في ظل تزايد الحاجة إلى تقييم مشروعية مصادر البيانات التي تُقدَّم كأدلة رقمية في المسائل المدنية أو الجنائية.

---

[1]. قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الجريدة الرسمية، العدد 32 مكرر (أ)، 14 أغسطس 2018.

[2]. قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، الجريدة الرسمية، العدد 8 مكرر، 2 فبراير 1950.

[3]. جمهورية مصر العربية، قانون حماية البيانات الشخصية رقم 151 لسنة 2020 .الجريدة الرسمية، العدد 32 مكرر (ب)، في 15 يوليو 2020.

على الرغم من غياب التشريعات التفصيلية في هذا المجال، فإن هناك حاجة ملحة لتطوير إطار قانوني خاص في مصر يتناول كيفية استخدام الذكاء الاصطناعي في المجال الجنائي، مع مراعاة الضمانات القانونية وحقوق المتهم، لضمان التوازن بين الاستفادة من التكنولوجيا وحماية الحقوق الأساسية.

ثانيًا: المملكة العربية السعودية

شهدت المملكة العربية السعودية خلال العقد الأخير تطورًا تشريعيًا وتقنيًا كبيرًا في مجال العدالة الرقمية، فقد تبنّت المملكة سياسة تشريعية تهدف إلى مأسسة التحول الرقمي وضمان أمن المعلومات وتكريس حجية الأدلة المستخرجة عبر الوسائل التقنية، بما يحقق التوازن بين الفاعلية القضائية وحماية الحقوق.

فقد أصدرت المملكة نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم م/17 بتاريخ 8 ربيع الأول 1428هـ (2007م)، والذي يعد أول تنظيم قانوني يتناول الجرائم الإلكترونية والدليل الرقمي في سياقها الجنائي. وقد نص في المادة 11 على تجريم إنشاء أو إرسال أو إعادة إرسال بيانات أو معلومات تتعلق بالحياة الخاصة عن طريق الشبكة المعلوماتية دون موافقة، ما يفتح الباب للاعتراف بالدليل الرقمي كوسيلة إثبات ضد هذه الجرائم[1].

كما أقرّ النظام مشروعية جمع وتحليل الأدلة الرقمية بواسطة الجهات المتخصصة، شرط الالتزام بالإجراءات النظامية، ما عزز استخدام وسائل التقنية الحديثة في التحقيق والإثبات.

وقد أصدر المجلس الأعلى للقضاء، بالتعاون مع وزارة العدل، عددًا من التوجيهات لتفعيل الأدلة الرقمية في القضايا المدنية والجنائية، وأكدت اللوائح التنفيذية لنظام الإثبات الصادر في 2021م على أن[2]: "الكتابة الإلكترونية والمراسلات الرقمية والمستخرجات التقنية تعد من وسائل الإثبات متى توفرت فيها الشروط المقررة نظامًا" (المادة 16 من نظام الإثبات).

---

[1]. المملكة العربية السعودية (2007) *نظام مكافحة جرائم المعلوماتية*، المرسوم الملكي رقم م/17 بتاريخ 8 ربيع الأول 1428هـ. الجريدة الرسمية.

[2]. المملكة العربية السعودية (2021) نظام الإثبات الجديد، المرسوم الملكي رقم (م/43) بتاريخ 1443/5/26هـ.

وقد أتاح النظام الجديد للإثبات الاعتراف بوسائل مثل الرسائل النصية، البريد الإلكتروني، تسجيلات الصوت والصورة، والتوقيع الإلكتروني، بوصفها أدلة مكتملة الحجية إذا ثبتت صحتها، وذلك على غرار ما هو معمول به في الأنظمة القضائية الحديثة.

وقد أنشأت وزارة العدل منصة "ناجز" و"بوابة تراضي" و"المحكمة الرقمية" لتكريس التحول الرقمي القضائي، وهو ما عزز إمكان تقديم الأدلة الرقمية وتداولها إلكترونيًا، ما جعل المملكة واحدة من الدول العربية الرائدة في تبني الإثبات الإلكتروني رسميًا[1].

ثالثًا: الإمارات العربية المتحدة

تعد دولة الإمارات العربية المتحدة من أوائل الدول العربية التي خطت خطوات تشريعية جادة نحو تقنين الأدلة الرقمية ودمجها في منظومتها العدلية، في إطار توجه إستراتيجي نحو التحول الرقمي الشامل. وقد اعتمدت الدولة منهجًا تشريعيًا ومؤسسيًا متقدمًا يكرّس حجية الأدلة المستمدة من الوسائط الإلكترونية في المجالات المدنية والجنائية والتجارية[2].

وقد نص قانون الإثبات في المعاملات المدنية والتجارية رقم (10) لسنة 1992، والمعدل بالقانون رقم (35) لسنة 2022، على قبول الكتابة الإلكترونية، والمستندات الرقمية، والتوقيع الإلكتروني كوسائل إثبات مقبولة قانونًا، ووفق المادة (20 مكررًا) من القانون المعدل: تُعد البيانات والمحررات الإلكترونية، والوسائل التقنية الحديثة، من وسائل الإثبات متى توافرت فيها شروط الموثوقية، وسلامة البيانات".

كما تضمن القانون اعترافًا صريحًا بحجية الصور والتسجيلات الصوتية، والمراسلات عبر البريد الإلكتروني، وتطبيقات المراسلة، مثل: "واتساب، وإيمو، وسناب شات"، في حال تم التحقق من مصدرها وصحتها الفنية.

وفي العام 2012، أصدرت الإمارات القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات[3]، وهو من القوانين الرائدة في المنطقة، وقد تضمن عدة نصوص تعالج مسألة الأدلة

---

[1]. السهلي، "دور المنصات العدلية الرقمية في تطوير نظام الإثبات الإلكتروني في السعودية ."المجلة السعودية للقانون والتقنية، 5(2)، (2023)، 33-55.

[2]. العبيدلي، ع. العدالة الرقمية في الإمارات: من البنية التقنية إلى فاعلية الإثبات الإلكتروني، مجلة الشريعة والقانون، جامعة الإمارات، 56(1)، (2022)، 33-62.

[3]. دولة الإمارات العربية المتحدة .(2012) القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وزارة العدل.

الرقمية من حيث الجمع، والمعالجة، والحجية. وقد أقرّ القانون للجهات القضائية والضبط القضائي الحق في استخدام الوسائل الرقمية في الكشف عن الجريمة، وجمع الأدلة الرقمية، وضمان صحتها وسلامتها القانونية، ما يشكل دعمًا مباشرًا لحجية هذا النوع من الأدلة.

وعززت الدولة هذا التوجه بإصدار القانون الاتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية والتوقيعات الرقمية، والذي نص على أن للتوقيع الرقمي الحجية القانونية ذاتها للتوقيع الخطي إذا توافرت فيه المعايير الفنية المحددة[1].

تُعد الإمارات من الدول السباقة في رقمنة القضاء، حيث أنشأت وزارة العدل ودوائر القضاء في الإمارات– مثل أبو ظبي ودبي والشارقة– محاكم رقمية متكاملة، تتيح تقديم المرافعات، وتبادل المستندات، وتقديم الأدلة الرقمية من خلال منصات إلكترونية مؤمنة. وتشمل تلك المنصات "بوابة العدالة"، و"المحكمة الذكية"، و"خدمة التقاضي عن بُعد."

وقد أكدت محكمة النقض بدبي في أحكامها على جواز استخدام الرسائل النصية، والمكالمات المسجلة، ومراسلات البريد الإلكتروني، بوصفها أدلة إثبات شريطة إثبات صدورها من صاحبها، وعدم الطعن في صحتها[2].

ويرى الباحثان من التجارب السابقة أن الدول العربية قد اتخذت خطوات متفاوتة في تنظيم الأدلة الرقمية، تعكس تباينًا في الرؤية القانونية، ومدى النضج التشريعي، والاستجابة للتحولات الرقمية المتسارعة.

---

[1]. دولة الإمارات العربية المتحدة .(2021) .القانون الاتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية والتوقيعات الرقمية .الجريدة الرسمية.

[2]. خليفة، م. حجية المحررات الإلكترونية في القانون الإماراتي: دراسة تحليلية مقارنة .مجلة القانون الإماراتي المعاصر، 12(2)، (2023)، 77–101.

المطلب الثاني

تجربة الاتحاد الأوربي

يتبنى الاتحاد الأوروبي نهجًا حذرًا ومنضبطًا تجاه استخدام الذكاء الاصطناعي، يرتكز على مبدأي "الثقة والشفافية"، خاصة في المجالات الحساسة مثل العدالة الجنائية. وتؤمن المفوضية الأوروبية بأن أدوات الذكاء الاصطناعي يجب أن تُستخدم لتعزيز الكفاءة ودقة العدالة، ولكن دون المساس بحقوق الإنسان الأساسية أو سيادة القانون، ولهذا تبلورت مجموعة من المبادئ والقواعد القانونية المنظمة لهذا المجال، تتكامل بين قوانين حماية البيانات والخصوصية والشفافية، بالإضافة إلى مقترحات تشريعية صريحة متعلقة بالذكاء الاصطناعي[1].

أولًا: اللائحة العامة لحماية البيانات(GDPR)

تُعد اللائحة العامة لحماية البيانات رقم 679/2016 حجر الأساس في الإطار القانوني الأوروبي، حيث تفرض قيودًا مشددة على المعالجة الآلية للبيانات الشخصية، خاصة في الحالات التي ينتج عنها "اتخاذ قرارات قانونية" أو ذات تأثير جوهري على الأفراد[2].

1. تنص المادة 22 من اللائحة على أنه لا يجوز أن يكون الفرد موضوعًا لقرار يعتمد فقط المعالجة الآلية، بما في ذلك التوصيف الآلي(profiling) إلا في حالات محددة مثل الحصول على موافقة صريحة أو وجود سند قانوني واضح.

2. تنطبق هذه المادة مباشرة على القرارات التي تتخذها أنظمة الذكاء الاصطناعي في المجال الجنائي، مثل تقييم الخطورة، أو تحديد احتمالية التورط في الجريمة، وهي أمثلة تدخل في نطاق "التصنيف الآلي".

تفرض اللائحة الأوروبية قيودًا صارمة على قبول مخرجات الذكاء الاصطناعي كأدلة، خاصة عند غياب الإشراف البشري أو ضمانات العدالة. ويسعى الاتحاد الأوروبي إلى تنظيم استخدام الذكاء

---

[1]. وفقًا للمفوضية الأوروبية (2021)، يتبنى الاتحاد الأوروبي نهجًا متوازنًا في تنظيم الذكاء الاصطناعي، حيث يهدف إلى تعزيز الشفافية والثقة في أدوات الذكاء الاصطناعي مع ضمان حماية حقوق الإنسان وخصوصية الأفراد. ويشمل ذلك تشريعات مثل قانون الذكاء الاصطناعي المقترح (AI Act) الذي يحدد القواعد القانونية اللازمة لضمان توافق هذه الأدوات مع مبادئ حقوق الإنسان ويفرض الشفافية في استخدام الخوارزميات لتجنب التمييز أو التحيز.

[2]. European Parliament and Council. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

الاصطناعي جنائيًا من خلال إطار قانوني يضمن الالتزام بالقيم الأوروبية، واحترام حقوق الإنسان، وتقييم المخاطر في الحالات الحساسة، بما يضمن حماية الحريات والعدالة[1].

بالإضافة إلى ذلك، تضع الوثيقة إطارًا للتعاون بين الدول الأعضاء والمنظمات الأوروبية لهدف ضمان تكامل وتوحيد الجهود في تتبع ومراقبة استخدام الذكاء الاصطناعي في المسائل الجنائية، مع تعزيز الشفافية والمسؤولية من خلال توفير آليات فاعلة لإشراك المجتمع المدني والمتخصصين القانونيين في تقييم المخاطر المتعلقة بتقنيات الذكاء الاصطناعي، وكذلك في تحديث التشريعات ذات الصلة [2].

أعلنت المفوضية الأوروبية في 2021 عن أول إطار قانوني شامل لتنظيم الذكاء الاصطناعي في العالم، وهو ما يُعرف باسم "قانون الذكاء الاصطناعي"، وقد تم اعتماده بشكل مبدئي في 2023، ويُنتظر دخوله حيز التنفيذ قريبًا[3].

1. يُقسم القانون تطبيقات الذكاء الاصطناعي إلى أربع فئات وفقًا لمستوى الخطورة :غير مقبول، مرتفع، محدود، ضئيل.

2. تُعد تطبيقات الذكاء الاصطناعي في مجال إنفاذ القانون والإجراءات الجنائية من الفئة "عالية الخطورة (High-Risk)"، وبالتالي يجب أن:

- تكون خاضعة لإشراف بشري فاعل.
- تضمن الشفافية وقابلية التفسير.
- تحترم الحقوق الأساسية للأفراد بما في ذلك الحق في محاكمة عادلة والدفاع.

وتُلزم اللائحة الجهات المطورة والمستخدمة لهذه الأنظمة بتقديم وثائق تقنية تفصيلية، وخضوعها لتدقيق قانوني وتقني قبل استخدامها في البيئة الجنائية. وبالتالي، تهدف تجربة الاتحاد الأوروبي إلى تحقيق توازن دقيق بين الاستفادة من قدرات الذكاء الاصطناعي في تعزيز كفاءة القضاء وحماية الأمن

1. Council of the European Union, Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption 6177/19, 2019.
2. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).
3. European Commission. (2023). Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.

العام، وبين حماية حقوق الأفراد وحرياتهم، من خلال إطار تنظيمي قوي يعتمد مبادئ الشفافية، والمساءلة، والحقوق الأساسية.

المطلب الثالث

تجربة اليابان

تعد اليابان واحدة من أكثر الدول تقدمًا في مجال التكنولوجيات الرقمية، وقد انعكس هذا التقدم على تنظيمها القانوني للأدلة الرقمية في سياق الإجراءات القضائية. ويتميز النموذج الياباني بتكامله بين القواعد القانونية الراسخة والتحديثات التقنية، بما يضمن فاعلية الإثبات الرقمي دون الإخلال بضمانات الخصومة وحماية الحقوق الفردية.

أولًا: الإطار التشريعي للأدلة الرقمية في اليابان

1. قانون الإجراءات الجنائية الياباني وتعديلاته

على الرغم من أن قانون الإجراءات الجنائية الياباني (Code of Criminal Procedure) لم يتضمن عند صدوره نصوصًا صريحة بشأن الأدلة الرقمية، إلا أن التعديلات التي أُدخلت عليه خلال العقدين الأخيرين مكّنت المحاكم والنيابة العامة من استخدام البيانات الرقمية كوسائل إثبات، شريطة مراعاة مبادئ العدالة الإجرائية. حيث أجاز القانون تفتيش الأجهزة الإلكترونية، كالحواسيب والهواتف، والتحفظ على البيانات الرقمية المحفوظة فيها، بشرط الحصول على إذن قضائي مسبق واحترام حقوق الدفاع[1].

وقد نصّت المادة 218 من قانون الإجراءات الجنائية على جواز إصدار أوامر تفتيش تشمل الوسائط الإلكترونية، بشرط أن يكون جمع البيانات ضروريًا للتحقيق، وأن يُراعى في ذلك مبدأ التناسب بين الإجراء المتخذ وحق الفرد في الخصوصية.

2. قانون تنظيم الجرائم المعلوماتية والأدلة الإلكترونية (2004)

صدر في العام 2004 قانون خاص ينظم الجوانب المتعلقة بالجرائم الرقمية وجمع الأدلة ذات الصلة، ويُعرف بـ "قانون الأدلة الإلكترونية والجرائم المعلوماتية"، وقد تضمن هذا القانون عدة أحكام مهمة أبرزها[2] :

- تعريف السجلات الإلكترونية وتحديد شروط اعتمادها كدليل إثبات.

1. Japanese Ministry of Justice. (2019). Code of Criminal Procedure. Retrieved from https://www.japaneselawtranslation.go.jp. accessed 5 May 2025.
2. Cabinet Secretariat of Japan. (2004). Act on Prohibition of Unauthorized Computer Access. Retrieved from https://www.nisc.go.jp . accessed 5 May 2025.

- وضع إطار قانوني لجمع الأدلة الرقمية من مزودي الخدمة والإنترنت.
- تجريم الأفعال التي تؤثر على سلامة الأدلة الرقمية، مثل التلاعب أو الإتلاف أو التزوير.

كما فرض القانون التزامات على المؤسسات التقنية بحفظ البيانات لفترات معينة تتيح استخدامها لاحقًا في التحقيقات أو المحاكمات.

3. قانون حماية المعلومات الشخصية (APPI)

يمثل قانون حماية المعلومات محورًا أساسيًا في التوازن بين حماية الخصوصية واستخدام الأدلة الرقمية. ويضع القانون قيودًا واضحة على استخدام البيانات الشخصية في سياق الإثبات، بما في ذلك ضرورة وجود أساس قانوني أو إذن قضائي للنفاذ إلى البيانات الحساسة، ليتماشى مع المعايير الدولية مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR) ويتضمن هذا القانون أحكامًا تحدد[1]:

- كيفية التعامل مع البيانات الرقمية التي تحتوي معلومات شخصية.
- قيود مشاركة هذه البيانات مع السلطات، حتى لأغراض قضائية، إلا بموجب أوامر قانونية.
- ضمان أمن البيانات المُجمعة، سواء أكان في أثناء النقل أم التخزين أم التحليل.

ويُلزم القانون السلطات القضائية والأمنية باستخدام أدلة رقمية دون المساس بمبادئ الشفافية، وعدم استخدام البيانات خارج حدود الغرض المشروع.

4. قانون التوقيع الإلكتروني والخدمات الرقمية(2000)

نظرًا لأهمية إثبات صحة المستندات والرسائل الإلكترونية، تبنّت اليابان منذ العام 2000 قانون التوقيع الإلكتروني، والذي يعترف قانونيًا بالتوقيعات الإلكترونية إذا استوفت شروط التحقق التقني، وعدّ الوثائق الإلكترونية، بما فيها العقود، صالحة قانونًا كأدلة في حال مطابقتها لمتطلبات التوثيق الإلكتروني[2].

وعلي الرغم من صدور العديد من التشريعات وما يظهره من مرونة متقدمة في الاستجابة لتطور الأدلة الرقمية، لم تصدر اليابان بعد قانونًا موحدًا وشاملًا للأدلة الرقمية.

1. Personal Information Protection Commission (PPC). (2020). Amendments to the Act on the Protection of Personal Information. Retrieved from https://www.ppc.go.jp.
2. Japanese Ministry of Economy, Trade and Industry (METI). (2000). Law Concerning Electronic and Certification Business. Retrieved from https://www.meti.go.jp.

ثانيًا: التطبيقات القضائية واعتراف المحاكم اليابانية بالأدلة الرقمية

لقد شهدت المحاكم اليابانية تطورًا ملحوظًا في تعاملها مع الأدلة الرقمية، حيث انتقلت من موقف التحفظ المشوب بالحذر إلى مرحلة الاعتراف الواضح والمنظم بها، في إطار احترام المبادئ الإجرائية الأساسية، وخاصة مبدأ شرعية الدليل، وحماية الخصوصية.

1. اعترفت المحاكم اليابانية بالأدلة الرقمية

هنالك امثلة كثيرة على اعتراف المحاكم اليابانية بالادلة الرقمية، ومن هذه الأمثلة، رسائل البريد الإلكتروني، وسجلات الاتصال، والتسجيلات من كاميرات المراقبة، شريطة أن تكون قد جُمعت بوسائل قانونية، ومن خلال إذن قضائي. وقد شددت المحكمة العليا اليابانية في عدة أحكام على ضرورة إثبات "صحة المصدر" و"سلامة الدليل من التلاعب"، وهو ما يُعرف بمبدأ "الموثوقية الجوهرية" للأدلة الرقمية[1].

وفي أحد الأحكام البارزة، أصدرت المحكمة العليا اليابانية قرارًا في العام 2017 يتعلق بقانونية استخدام بيانات تحديد المواقع (GPS) التي حصلت عليها الشرطة دون إذن مسبق، وأقرت بأن هذا السلوك يمثل انتهاكًا للخصوصية، ولا يجوز استخدام هذه الأدلة أمام المحكمة. وقد رسّخ هذا الحكم مبدأ ضرورة الإذن القضائي المسبق للحصول على الأدلة الرقمية ذات الطبيعة الخاصة[2].

وهذا الحكم أسس لقاعدة قانونية تقضي بوجوب حصول الشرطة على إذن قبل تتبع الأفراد عبر تقنيات رقمية، بما يعكس احترام اليابان للحقوق الدستورية، حتى في مواجهة الجريمة الرقمية.

2. التعامل مع البيانات المستخرجة من وسائل التواصل الاجتماعي

أظهرت المحاكم اليابانية مرونة مدروسة في التعامل مع الأدلة الرقمية المستخرجة من منصات التواصل الاجتماعي مثل "تويتر" و"فيسبوك"، وذلك ضمن ضوابط قانونية تراعي الخصوصية والعدالة. فقد قضت محاكم يابانية بإمكان قبول المنشورات والتعليقات والرسائل كأدلة رقمية في كل من القضايا الجنائية والمدنية، بشرط أن تكون قد جُمعت بطريقة مشروعة. ويُعد الإذن القضائي أو كون المنشورات متاحة

1. Hirano, Y. (2021). Digital Evidence and Procedural Challenges in Japanese Criminal Law. Journal of Japanese Law, 46(2), 45–67.

2. Supreme Court of Japan. (2017). *GPS Surveillance Case*, Judgment No. 平成29(あ)第442号.

للعامة دون إعدادات خصوصية مشددة من أبرز المعايير الحاسمة في تحديد مدى قانونية هذا النوع من الأدلة[1].

ومن أبرز الأحكام في هذا السياق، حكم محكمة طوكيو الصادر في العام 2019، الذي قبل منشورًا على موقع "تويتر" كدليل إثبات في جريمة تهديد، وذلك بعد أن قدم الادعاء العام ما يثبت فنيًا أن الحساب المستخدم في النشر تابع للمتهم، من خلال تتبع عنوان الـIP ، وتحليل بيانات الجهاز، وربطها بمعرفات الاستخدام.

3. اعتماد التوقيعات والوثائق الرقمية أمام القضاء

قد انعكس الإطار التشريعي على ممارسات المحاكم اليابانية، حيث أقرت عدة أحكام قضائية بأهمية التوقيع الرقمي في الإثبات. فعلى سبيل المثال، قضت محكمة أوساكا العليا في العام 2005[2] بوصف عقد إلكتروني موقع توقيعًا رقميًا صادرٍ عن شركة مدرجة، دليلًا كافيًا على الإيجاب والقبول في علاقة تعاقدية، وذلك بعد التحقق من صحة التوقيع عبر الهيئة المصدّقة المعتمدة.

كما أكدت المحكمة العليا في اليابان في أحد أحكامها الصادرة في العام 2011 أن التوقيع الرقمي إذا استوفى المتطلبات التقنية والقانونية المحددة قانونًا، فإنه يتمتع بالحجية ذاتها التي يملكها التوقيع التقليدي[3].

ثالثًا: موقف القضاء من تعارض الأدلة الرقمية مع حرمة الحياة الخاصة

اتبعت المحاكم اليابانية نهجًا متوازنًا في التعامل مع تعارض الأدلة الرقمية وحرمة الحياة الخاصة، حيث شددت المحكمة العليا على ضرورة جمع البيانات الرقمية وفق ضوابط صارمة تضمن التوازن بين متطلبات العدالة الجنائية وحقوق الأفراد الدستورية، والحق في الخصوصية.

وقد شكل الحكم الشهير الصادر عن المحكمة العليا اليابانية في قضية تتبع نظام تحديد المواقع GPSللعام 2017 محطة حاسمة في هذا المجال، حيث قضت المحكمة بعدم مشروعية استخدام أجهزة التتبع الإلكتروني دون أمر قضائي، واصفة أن هذا الإجراء يشكل "تدخلًا جسيمًا في الحياة الخاصة"،

1. Tokyo District Court. (2019). Twitter Threat Case, Judgment No. 平成31(わ)第278号. Reported in: Mainichi Shimbun, March 12, 2019.
2. Osaka High Court. (2005). Electronic Contract Case, Judgment No. 平成17(ネ)第1056号. Published in: Hanrei Jiho, 1890, 33–37.
3. Supreme Court of Japan. (2011). Digital Signature Validity Case, Judgment No. 平成23(オ)第415号.

وينتهك المادة 35 من الدستور الياباني التي تكفل حرمة المساكن والأماكن الخاصة. وبذلك أرست المحكمة مبدأ قضائيًا مفاده أن الأدلة الرقمية المستخرجة من مصادر خاصة دون إذن قضائي تعد باطلة وغير قابلة للاستخدام أمام القضاء، إلا في حالات الضرورة القصوى وبضوابط قانونية واضحة[1].

وفي قضايا أخرى، كقضية جمع رسائل البريد الإلكتروني أو البيانات من الهواتف المحمولة، شددت المحاكم اليابانية على ضرورة تحقيق التناسب بين الهدف من جمع البيانات ووسائل جمعها، ومدى تأثيرها على خصوصية الأفراد.

فتُظهر تجربة اليابان في تنظيم الأدلة الرقمية أنها تعكس توازنًا بين التقدم التقني وصون الحقوق، إذ أقرت التشريعات حجية البيانات والتوقيعات الرقمية بضوابط قانونية، وأكدت المحاكم، خصوصًا المحكمة العليا، ضرورة احترام الخصوصية وعدم جمع الأدلة دون إذن قضائي.

[1]. Supreme Court of Japan. (2017). *GPS Surveillance Case*, Judgment No. 平成29(あ)第442号.

الخاتمة

شهدت العقود الأخيرة تطورًا هائلًا في تقنيات الذكاء الاصطناعي، وهو ما انعكس بوضوح على منظومة العدالة الجنائية، ولا سيما في مجال جمع وتحليل الأدلة. وعلى الرغم مما توفره هذه الأنظمة من سرعة ودقة وقدرة على التعامل مع البيانات الضخمة، إلا أن استخدامها في الإثبات الجنائي يطرح إشكاليات قانونية معقدة تتعلق بمبدأ العدالة، وحقوق الدفاع، وشفافية مصادر الإثبات. وقد تباينت المواقف القضائية في قبول هذه الأدلة، حيث قبلتها بعض المحاكم ضمن ضوابط صارمة، بينما رفضتها أخرى لافتقارها للموثوقية أو لانتهاكها الضمانات الإجرائية. ومن هنا، يبرز التحدي الحقيقي في كيفية المواءمة بين الابتكار التكنولوجي ومتطلبات العدالة الجنائية.

أولاً: النتائج

1. الذكاء الاصطناعي أصبح أداة مركزية في التحقيقات الجنائية الحديثة، خاصة في تحليل البيانات الإلكترونية والتنبؤ بالسلوك الإجرامي.
2. غياب الإطار القانوني الموحد لاستخدام الأدلة المستمدة من الذكاء الاصطناعي أدى إلى تضارب في الأحكام القضائية بين القبول والرفض.
3. طبيعة بعض الخوارزميات بوصفها "صندوقًا أسود "تمثل تحديًا لمبدأ الشفافية القضائية وتضعف إمكان الطعن في الأدلة.
4. الممارسات القضائية المقارنة، مثل التجربة الأميركية التي أظهرت أهمية وجود رقابة قضائية مسبقة على استخدام هذه الأنظمة.
5. استخدام الذكاء الاصطناعي قد يهدد مبدأ المحاكمة العادلة إذا لم تُضبط آليات عمله قانونيًا وتكنولوجيًا.
6. الحاجة إلى حوكمة قانونية رقمية، بيّنت الدراسة ضرورة وجود أطر تشريعية مرنة وفاعلة تواكب التطور السريع في تقنيات الذكاء الاصطناعي، وتراعي التوازن بين الابتكار وضمان الحقوق الأساسية.

ثانياً: التوصيات

1. سن تشريعات خاصة تنظم استخدام أنظمة الذكاء الاصطناعي في الإجراءات الجنائية، تضمن حماية الخصوصية وحقوق المتهم.
2. إلزام الجهات القضائية والأمنية بالكشف عن كيفية عمل الأنظمة الخوارزمية المستخدمة في التحليل الجنائي.
3. وضع ضوابط قضائية واضحة لقبول هذه الأدلة، بما في ذلك تقييم مدى موثوقيتها وقابليتها للتفسير البشري والطعن القانوني.
4. تدريب القضاة وأعضاء النيابة العامة على الجوانب التقنية لأنظمة الذكاء الاصطناعي لفهم طبيعة الأدلة المولدة منها كي يتحقق الأمن القانوني.
5. التعاون الدولي لوضع معايير موحدة للأدلة الرقمية المستندة إلى الذكاء الاصطناعي، خاصة في ظل تزايد الجرائم العابرة للحدود من خلال إبرام اتفاقيات دولية في هذا الشأن.
6. إصدار مدونات سلوك مهنية رقمية تنظم استخدام الذكاء الاصطناعي في المجال القانوني، وتراعي المبادئ الأخلاقية لمهنة المحاماة والقضاء.

بيان تضارب المصالح

يقر جميع المؤلفين أنه ليس لديهم أي تضارب في المصالح.

قائمة المصادر والمراجع

أولًا: القوانين والاتفاقيات الدولية

1. الدستور المصري للعام 2014، الجريدة الرسمية، العدد 22 مكرر (ب)، 18 يناير 2014.
2. قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، الجريدة الرسمية، العدد 8 مكرر، 2 فبراير 1950.
3. قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الجريدة الرسمية، العدد 32 مكرر (أ)، 14 أغسطس 2018.
4. اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي" المؤتمر العام، الدورة 41، باريس، نوفمبر 2021" وهي توصية، تهدف إلى وضع إطار أخلاقي شامل لاستخدام تقنيات الذكاء الاصطناعي، مع التركيز على تعزيز حقوق الانسان، وحماية البيئة، وتشجيع التنوع الثقافي.

ثانيًا: الكتب العربية

1. 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، (2004).
2. عائشة بن قارة مصطفي، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، (2010).
3. محمود الخطيب، الحماية الجنائية للبيانات الرقمية: دراسة مقارنة، دار الجامعة الجديدة، (2020).
4. محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، (2006).

ثالثًا: الرسائل العلمية

1. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت– رسالة ماجستير–، جامعة الشرق الأوسط للدراسات العليا، دار الثقافة للنشر والتوزيع، عمان، (2011).

رابعًا: الدوريات (المجلات العلمية)

2. الشمري، س. ن، مشروعية الأدلة الرقمية في الإجراءات الجنائية: دراسة مقارنة. مجلة العلوم القانونية، 33(1)، (2020).
3. العتيبي، م. خ، الضمانات القانونية للمتهم في مواجهة أنظمة الذكاء الاصطناعي المستخدمة في التحقيقات الجنائية. المجلة السعودية للقانون، 12(3)، (2020).

خامسًا:المراجع الأجنبية

1. Artificial Intelligence in Criminal Justice: A Review of the Use of Artificial Intelligence in Criminal Justice System» (2020) by the National Institute of Justice (NIJ). URL: https://nij.ojp.gov/ library/publications/artificial-intelligence-criminal-justice.
2. AI in Law Enforcement: The Power, Risks, and Ethics of Using AI for Criminal Justice. (2021) by the Future of Life Institute. URL: https://futureoflife.org/ai-law-enforcement-power risksethics-using-ai-criminal-justice.
3. Artificial Intelligence in Criminal Justice: Addressing Ethical Concerns. (2019) by the Brennan Centre for Justice. URL: https://www.brennancenter.org/our-work/research reports/artificialintelligence-criminal-justice-addressing-ethical-concerns.
4. Borgesius, F. Z. (2018). *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*. Council of Europe Report.
5. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Journal of Law and Information Technology. accessed 2 May 2025: https://doi.org/10.1093/ijlit/eaz002
6. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology, 27*(2), accessed 3 May 2025: https://doi.org/10.1093/ijlit/eaz002
7. Chan, J., & Lee, K. (2019). *Digital evidence in the modern legal system: Challenges and opportunities*. International Journal of Legal Technology, 22(4), https://doi.org/10.1016/j.ijlt.2019.04.003
8. Cath, C., et al. (2018). *Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach*. Science and Engineering Ethics, 24(2).
9. Council of the European Union, *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption*, 2019.
10. Cabinet Secretariat of Japan. (2004). *Act on Prohibition of Unauthorized Computer Access*. Retrieved from https://www.nisc.go.jp . accessed 5 May 2025
11. Donohue, L. K. (2016). *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*. Oxford University Press.
12. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).
13. European Commission. (2023). *Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act)*, COM (2021) 206 final.
14. European Union Agency for Fundamental Rights (FRA). (2020). *Getting the future*
15. *right – Artificial intelligence and fundamental rights*.: https://fra.europa.eu/
16. European Commission. (2021). *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 accessed 4 May 2025.

17. European Parliament and Council. (2016). *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679.
18. Eoghan Casey. (2011). "Digital Evidence and Computer Crime", 3rd Edition, London, Academic Press.
19. Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
20. European Union Agency for Fundamental Rights (FRA). (2020). *Getting the future right – Artificial intelligence and fundamental rights*. Publications Office of the European Union. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights accessed 2 May 2025.
21. European Court of Human Rights (ECtHR). (2018). *Big Brother Watch and Others v. the United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15.
22. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.
23. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.
24. Hirano, Y. (2021). *Digital Evidence and Procedural Challenges in Japanese Criminal Law*. *Journal of Japanese Law*, 46(2).
25. Japanese Ministry of Justice. (2019). *Code of Criminal Procedure*. Retrieved from https://www.japaneselawtranslation.go.jp accessed 5 May 2025
26. Japanese Ministry of Economy, Trade and Industry (METI). (2000). *Law Concerning Electronic Signatures and Certification Business*. Retrieved from https://www.meti.go.jp
27. Osaka High Court. (2005). *Electronic Contract Case*, Judgment No. 平成17(ネ)第1056号. Published in: Hanrei Jiho, 1890.
28. Personal Information Protection Commission (PPC). (2020). *Amendments to the Act on the Protection of Personal Information*. Retrieved from https://www.ppc.go.jp
29. Sulyok, M. (2021). The evidentiary value of AI-based data in criminal proceedings: A European perspective. *New Journal of European Criminal Law, 12*(4) https://doi.org/10.1177/20322844211044777 accessed 3 May 2025.
30. Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, 35(4), 1305–1338. https://readingroom.law.gsu.edu/gsulr/vol35/iss4/4 accessed 4 May 2025.
31. Supreme Court of Japan. (2017). *GPS Surveillance Case*, Judgment No. 平成29(あ)第442号.
32. Supreme Court of Japan. (2011). *Digital Signature Validity Case*, Judgment No. 平成23(オ)第415号.
33. Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Harvard University Press.
34. Sulyok, M. (2021). The evidentiary value of AI-based data in criminal proceedings: A European perspective. *New Journal of European Criminal Law, 12*(4),. https://doi.org/10.1177/20322844211044777 accessed 2 May 2025.

35. The Use of Artificial Intelligence in Criminal Investigations and Prosecutions. (2020) by the Council of Europe. URL: https://rm.coe.int/the-use-of-artificial-intelligence-in-criminal investigations and - prosec/1680a84a92.
36. Tokyo District Court. (2019). *Twitter Threat Case*, Judgment No. 平成31(わ)第278号. Reported in: Mainichi Shimbun, March 12, 2019.
37. Tomiyama, H. (2021). *Judicial Oversight on Digital Evidence Collection in Japan*. Tokyo Law Review, 48(1).
38. U.S. Congress. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272. Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162
39. U.S. Congress. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272. https://www.congress.gov/bill/107th-congress/house-bill/3162.
40. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Transparent, Explainable, and Accountable AI for Robotics*. Science Robotics, 2(6), eaan6080.

This work is licensed under a

Creative Commons Attribution NonCommercial 4.0

International license.