مجلة القرار للبحوث العلمية المحكّمة | العدد 21، المجلد 7، السنة الثانية | أيلول (سبتمبر) 2025 | ربيع الأول 1447
ISSN 3006-7294

إثبات الجرائم الرقمية في ضوء الأدلة المستخرجة آليًا عبر الذكاء الاصطناعي

إعداد: الباحث / محمد مصطفى عدنان الشافعي | الجمهورية اللبنانية

طالب دكتوراه في الحقوق – القانون الخاص | الجامعة الإسلامية في لبنان

E-mail: mohamadcheifie@gmail.com | https://orcid.org/0009-0002-3168-1622
https://doi.org/10.70758/elqarar/7.21.24

تاريخ الاستلام: 2025/8/30	تاريخ القبول: 2025/9/9	تاريخ النشر: 2025/9/15

للاقتباس: الشافعي، محمد مصطفى عدنان، إثبات الجرائم الرقمية في ضوء الأدلة المستخرجة آليًا عبر الذكاء الاصطناعي، مجلة القرار للبحوث العلمية المُحكّمة، المجلد السابع، العدد 21، السنة الثانية، 2025، ص–ص 528–545. https://doi.org/10.70758/elqarar/7.21.24

المُلخّص

يُشكّل هذا البحث دراسة قانونية معمّقة في مدى مشروعية توظيف الذكاء الاصطناعي في استخراج الأدلة الرقمية ودوره في مكافحة الجريمة المعلوماتية، مع التركيز على التحديات القانونية في مجال الإثبات الجنائي. وقد بيّنت الدراسة أنَّ هذه الأدلة ليست مجرد بياناتٍ خام، بل نواتج تحليل خوارزمي معقّد يتطلب ضمانات خاصة تتعلق بالشرعية والموثوقية وقابلية التفسير. وتناول البحث شروط قبول هذه الأدلة أمام القضاء، مشدداً على ضرورة احترام الشفافية والضمانات الدستورية، لا سيما ما يتعلق بالخصوصية والمحاكمة العادلة، مع التأكيد على أهمية توفير آليات دفاعية فعالة للطعن في مشروعيتها. وخلص إلى ضرورة تبني إطار تشريعي متوازن يحكم هذا المجال المستحدث، بما يضمن فعالية العدالة الجنائية دون المساس بالحقوق الأساسية.

الكلمات المفتاحية: الذكاء الاصطناعي، الأدلة الرقمية، الإثبات الجنائي، الجرائم الإلكترونية، الخصوصية الرقمية، المشروعية، الطعن في الأدلة، المحاكمة العادلة.

ElQarar Journal for Peer-Reviewed Scientific Research | Issue 21, Vol 7, Year 2 | September 2025 | Rabi al-Awwal 1447
ISSN 7294-3006

Proving Digital Crimes in Light of Automatically Extracted Evidence via Artificial Intelligence

Author: Researcher / Mohammad Moustafa Adnan Al-Shafii | Lebanese Republic

PHD Candidate in Public Law / Criminal Procedure Law- Islamic University of Lebanon

E-mail: mohamadcheifie@gmail.com | https://orcid.org/0009-0002-3168-1622
https://doi.org/10.70758/elqarar/7.21.24

Received : 30/8/2025	**Accepted :** 9/9/2025	**Published :** 15/9/2025

Cite this article as: *Al-Shafii, Mohammad Moustafa Adnan, Proving Digital Crimes in Light of Automatically Extracted Evidence via Artificial Intelligence*, *ElQarar Journal for Peer-Reviewed Scientific Research, vol 7, issue 21, Second year, 2025, pp. 528-545. https://doi.org/10.70758/elqarar/7.21.24*

Abstract

This research constitutes an in-depth legal study on the legitimacy of employing artificial intelligence in the extraction of digital evidence and its role in combating cybercrime, with a particular focus on the legal challenges surrounding criminal evidence. The study demonstrates that such evidence is not merely raw data, but rather the product of complex algorithmic analysis that necessitates specific safeguards related to legality, reliability, and interpretability. It examines the conditions under which this type of evidence may be admitted in court, emphasizing the need to uphold transparency and constitutional guarantees, particularly those concerning privacy and the right to a fair trial. The research underscores the importance of providing effective defense mechanisms to challenge the legitimacy of such evidence and concludes by calling for the adoption of a balanced legislative framework to regulate this emerging field in a manner that ensures the effectiveness .of criminal justice without infringing upon fundamental rights

Keywords: Artificial Intelligence, Digital Evidence, Criminal Evidence, Cybercrime, .Digital Privacy, Legality, Evidence Challenge, Fair Trial

المقدمة

تُعد الجريمة الرقمية من أبرز إفرازات الطفرة التكنولوجية المعاصرة، حيث شهدت البنية الإجرامية تحوّلاً نوعياً، تجلّى في استغلال الفضاء الرقمي والأنظمة المعلوماتية المتقدمة كوسائل رئيسية لارتكاب أنماط مستحدثة من الجرائم، وفي مقدّمتها الاحتيال الإلكتروني، وتبييض الأموال، وتمويل الإرهاب عبر الوسائط السيبرانية. وقد اتسمت هذه الجرائم بقدرٍ عالٍ من التعقيد والذكاء، مما جعلها تتجاوز النطاق التقليدي لإمكانات أجهزة إنفاذ القانون في الرصد والملاحقة. أمام هذا الواقع، فرضت الظاهرة الإجرامية الرقمية تحدياً بنيوياً على المنظومة القانونية، التي بات لزاماً عليها تحديث أدواتها وآلياتها الإجرائية لمواكبة هذا التحوّل النوعي. وفي طليعة تلك الأدوات يبرز اللجوء إلى تقنيات الذكاء الاصطناعي في تحليل البيانات الضخمة، ورصد الأنماط السلوكية المشبوهة، وتتبع الأنشطة الرقمية ذات الطابع الإجرامي، مما مكّن من كشف أدلة رقمية كانت لتظل عصيّة أو خفيّة لولا هذه الوسائل. إلا أنَّ إدراج الذكاء الاصطناعي في ميدان جمع الأدلة يطرح إشكاليات قانونية دقيقة، يتصدرها مدى مشروعية الحصول على هذه الأدلة عبر وسائل آلية، وحدود احترام الحق في الخصوصية، وضمانات حماية الحرية الفردية من الانتهاك أو التعسف.

ومن هذا المنطلق، يكتسب هذا البحث أهميته كونه يسعى إلى تحليل الإطار القانوني الناظم لحجية الأدلة الرقمية المستخرجة بواسطة تقنيات الذكاء الاصطناعي في سياق مكافحة الجريمة الرقمية، مع التركيز على طبيعتها وخصائصها، وضبط المحددات القانونية لمشروعيتها وإمكان الاستناد إليها في الإثبات الجنائي. كما يتناول البحث الوقوف على التحديات التي تفرضها هذه الأدلة على البنية التقليدية لقواعد الإثبات، وبلورة مقاربة قانونية متوازنة تجمع بين مقتضيات الأمن الرقمي، ومتطلبات صيانة الحقوق الدستورية الأصيلة.

وانطلاقًا من ذلك، يطرح البحث **الإشكالية** التالية: «إلى أي مدى يمكن اعتماد الأدلة المستخرجة آليًا عبر الذكاء الاصطناعي في إثبات الجرائم الرقمية، في ظل التحديات القانونية والإجرائية المرتبطة بمشروعيتها وحجيتها؟» لمعالجة هذه الإشكالية، يعتمد البحث **المنهجين الوصفي والتحليلي**، من خلال **تقسيمه** إلى مبحثين رئيسيين. يتناول المبحث الأول الطبيعة القانونية للأدلة الرقمية المستخرجة آليًا، مع بيان خصائصها ومشروعية جمعها. في حين يخصص المبحث الثاني لتحليل حجية هذه الأدلة في الإثبات الجنائي، والمعايير والضمانات التي تحكم قبولها والطعن فيها. ويُختتم البحث بخاتمة تتضمن أهم النتائج والتوصيات المقترحة.

المبحث الأول:

الطبيعة القانونية للأدلة الرقمية المستخرجة عبر الذكاء الاصطناعي

في ظل الطفرات المتسارعة التي يشهدها حقل الذكاء الاصطناعي، أضحت الأدلة الرقمية المستخرجة بوسائل آلية أحد الأعمدة الرئيسية في منظومة التحقيق الجنائي لمجابهة الجريمة الإلكترونية. ولم تعد هذه الأدلة مجرد وثائق رقمية تقليدية أو معطيات جامدة، بل أضحت ثمرة معالجات تحليلية عميقة، تتكئ على تقنيات التعلم الآلي واكتشاف الأنماط السلوكية، ما يضفي عليها قدرة فائقة في الكشف عن الارتباطات الخفية والسلوكيات الإجرامية المضمرة، التي قد تستعصي على وسائل التحري التقليدية.

من هنا، يهدف هذا المبحث إلى دراسة الطبيعة القانونية لهذه الأدلة من زاويتين مترابطتين. أولًا، من خلال بيان مفهومها وخصائصها التقنية والقانونية، وما يميزها عن الأدلة التقليدية. وثانيًا، من خلال تحليل المشروعية والضوابط القانونية التي تحكم جمعها ومعالجتها في إطار الإجراءات الجنائية.

المطلب الأول: تعريف الأدلة الرقمية المستخرجة آليًا وخصائصها

تُوصَف الأدلة الرقمية المستخرجة بوسائط الذكاء الاصطناعي بأنها معطيات تُجمع أو تُولَّد أو تُحلَّل بواسطة آليات خوارزمية متقدمة، بغرض استجلاء وقائع جنائية أو تأكيدها، وذلك من خلال عمليات معالجة فائقة الكثافة للبيانات تعتمد على التحليل النمطي أو الاستدلال التنبؤي. وتمتاز هذه الأدلة بطبيعة تركيبية معقّدة تجعلها تتجاوز المفهوم التقليدي للأدلة الرقمية، إذ إنها لا تُستخلص يدوياً أو بطريقة مباشرة، بل تُستنتج استنتاجاً استقرائياً عبر منظومات ذكية قادرة على ربط المؤشرات، واستنتاج السلوكيات، ورسم الأنماط الإجرامية الكامنة في كتل البيانات الهائلة[1].

وتنفرد هذه الفئة من الأدلة الرقمية بخصائص تميزها جوهريًا عن نظيرتها التقليدية، إذ إنها لا تقتصر على مجرد البيانات الخام أو المعطيات الأولية، بل تمتد لتشمل المخرجات الاستنتاجية الناتجة عن المعالجة الذكية، والتي غالبًا ما تكون تعبيرًا عن أنماط سلوكية مركّبة أو توقعات مبنية على نماذج تحليل خوارزمية فائقة التعقيد. ومن النماذج التطبيقية البارزة لهذه الأدلة، ما شهده التحقيق في احدى القضايا، حيث تم إخضاع حوالي ستمائة ألف رسالة بريد إلكتروني لتحليل دقيق عبر تقنيات التعلم الآلي، مما أفضى إلى استخلاص أنماط احتيالية معقدة وكشف الشبكات الخفية

(1) S. Russell & P. Norvig, Artificial Intelligence: A Modern Approach, 4th edition, Pearson, 2021, p 1032–1036.

التي جمعت بين أطراف القضية، في سابقة عززت مشروعية استخدام الذكاء الاصطناعي كأداة استدلال جنائي عالية الكفاءة[1].

وفي السياق عينه، تنكبّ وحدات مكافحة الجريمة الإلكترونية في عدد من الدول، من بينها دولة الإمارات العربية المتحدة وجمهورية مصر العربية والجمهورية اللبنانية، على تطوير منظومات ذكاء اصطناعي متقدمة تُعنى بتحليل الرسائل النصية والمحتوى المنشور عبر منصات التواصل الاجتماعي، بغية رصد أنماط التصيّد الاحتيالي واستراتيجيات التجنيد الإرهابي، وذلك في إطار مقاربة تقنية وقائية تتوسّل بالخوارزميات الاستباقية لرصد المؤشرات الرقمية ذات الطابع الإجرامي قبل تفاقم آثارها.

تتفرّد هذه الأدلة بجملة من السمات التقنية والقانونية التي تضفي عليها طابعًا استثنائيًا في منظومة الإثبات الجنائي. ويأتي في طليعة تلك السمات، أولا: اعتمادها على آليات جمع ومعالجة تلقائية لا تخضع للتدخل البشري المباشر، إذ ترتكز على خوارزميات التعلم العميق القادرة على استنباط أنماط سلوكية بالغة التعقيد، يعزّ على الوسائل اليدوية التقليدية بلوغها أو الإحاطة بها. إلا أن هذا الطابع الذكائي، وإن مكّنها من إنتاج استدلالات بالغة العمق، فإنه في المقابل يُفضي إلى إشكاليات جوهرية، تتعلق بمدى إمكانية تفسير تلك المخرجات أو إخضاعها للتحقّق القضائي بشفافية تامة تضمن سلامة النتائج وتُعزّز حجّيتها القانونية[2].

ثانيًا، تُجسِّد هذه الأدلة طابعًا احتماليًا محضًا، إذ لا تُفضي في الغالب إلى نتائج يقينية قاطعة، بل تطرح تقديرات تستند إلى مستويات متفاوتة من الاحتمال، وهو ما يثير إشكالًا قانونيًا دقيقًا بشأن مدى اتساقها مع معيار «اليقين القضائي» اللازم لإسناد الإدانة الجنائية. فعلى سبيل المثال، قد يُقدِّم نظام ذكاء اصطناعي تحليلاً لسلسلة تحويلات مالية، مُصدِرًا إنذارًا بوجود احتمال مرتفع لارتكاب جريمة غسل أموال؛ غير أنّ هذا الاستنتاج، وبطبيعته الاحتمالية، يظل قاصرًا عن بلوغ مرتبة الدليل القاطع، ولا يستقيم اعتماده بمفرده دون أن يُعضَّد بأدلة إضافية ترسّخ قوته الإثباتية وتسدّ ما يشوبه من فجوات الشك[3].

ثالثًا، يرتكز هذا النمط من الأدلة على معالجة كميات ضخمة من البيانات الشخصية، الأمر الذي يُثير إشكاليات قانونية وأخلاقية بالغة الحساسية، لا سيّما في ما يتصل بصيانة الحق في الخصوصية. وتتعاظم هذه الإشكالية عندما تُجمع تلك البيانات دون الحصول على موافقة

(1) Shapiro, A. K., Predictive Policing and Artificial Intelligence. Yale Law & Policy Review, 37(2), 2019, p 228.

(2) Pasquale, F., The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015, p 71–72.

(3) Dignum, V., Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way, Springer, 2019, p 83–85.

صريحة من أصحابها، أو تُستقى من مصادر مفتوحة بطريقة قد تفتقر إلى المشروعية أو لا تُراعي الضمانات الواجبة لحماية الحقوق الفردية. فعلى سبيل المثال، قد تُمكّن تقنيات التعرف على الوجوه، المدعّمة بخوارزميات الذكاء الاصطناعي، من تتبّع مشتبه بهم عبر كاميرات المراقبة العامة، غير أنّ غياب إطار تشريعي صارم يُنظّم هذه الممارسة قد يُفضي إلى تحولها من أداة تحرٍّ مشروع إلى وسيلة مراقبة جماعية تنطوي على مساس خطير بالحريات الأساسية(1).

وقد أرست بعض السوابق القضائية مبدأً قاطعًا بضرورة إحاطة هذا الصنف من الأدلة بضوابط معيارية دقيقة، تضمن اتساقها مع مبادئ العدالة وضمانات المحاكمة العادلة. ولعل من أبرز ما كرّسته محكمة العدل الأوروبية، في إحدى أحكامها المفصلية، تأكيدها الحاسم على لزوم تقييد استخدام الأدلة الناتجة عن تقنيات الذكاء الاصطناعي بإطار قانوني واضح ومحكم، يوازن بين مقتضيات الأمن العام ومتطلبات حماية الحقوق الأساسية، وفي مقدمتها الحق في الخصوصية وسلامة الإجراءات القضائية(2)، قضت المحكمة ببطلان التوجيه الأوروبي الذي يفرض تخزين بيانات الاتصالات على نحو جماعي ودون قيود مُحكمة، مُعتبرةً أن هذا الإجراء يُشكّل مساسًا خطيرًا وجسيمًا بجوهر الحق في الخصوصية، وينطوي على خرقٍ صريح للحدود الدستورية التي تؤطّر مبدأ التناسب بين مقتضيات الأمن العام وضمانات الحقوق الفردية المصانة(3).

خصائص مجتمعة تضفي على الأدلة الرقمية المستخرجة آليًا عبر تقنيات الذكاء الاصطناعي طابعًا هجينًا بالغ التعقيد، إذ تجمع بين القدرة التقنية المتقدمة التي تُعزّز من نجاعة التحقيق الجنائي، وبين إشكاليات قانونية وأخلاقية متجذّرة تُحتم إخضاعها لإطار تنظيمي صارم يتّسم بالدقة والشفافية.

وفي ضوء ما تقدّم من تحديد لمفهوم هذه الأدلة وبيان خصائصها التقنية والوظيفية المميّزة، تبرز إلى السطح إشكالية أكثر تعقيدًا وأشدّ حساسية، تتمثل في مشروعية إجراءات جمعها والقيود القانونية الناظمة لها، وهي الإشكالية التي ستكون محلّ المعالجة في المطلب التالي.

المطلب الثاني: المشروعية والضوابط القانونية لجمع الأدلة الرقمية المستخرجة آليًا عبر الذكاء الاصطناعي

يُثير جمع الأدلة الرقمية عبر وسائط الذكاء الاصطناعي إشكاليات قانونية شائكة تتصل بمدى مشروعية هذه الممارسات، والضوابط الإجرائية التي ينبغي أن تؤطرها في نطاق العدالة الجنائية. فقد أضحت التحقيقات المعاصرة تعتمد، بوجه متزايد، على تقنيات التحليل الآلي للبيانات

(1) شحاتة، أسامة، الذكاء الاصطناعي والقانون، دار المنهل اللبناني، بيروت، لبنان، 2021، ص 77.

(2) Court of Justice of the European Union, Case C-293/12 Digital Rights Ireland Ltd v Minister for Communications, 2014.

(3) Court of Justice of the European Union, 2014.

الضخمة، التي قد تنطوي على معلومات ذات طابع بالغة الحساسية، جُمعت من مصادر تمس صميم الحياة الخاصة، كالاتصالات الشخصية، والمعاملات المالية، وسجلات التصفح الإلكتروني، والمواقع الجغرافية الدقيقة عبر أجهزة التتبع الذكي. ويُعد مبدأ المشروعية حجر الزاوية في بنية الإجراءات الجنائية، بما يفرض أن تخضع عملية جمع الأدلة لقواعد قانونية مُحددة وواضحة، تكفل صيانة الحقوق والحريات الفردية، وفي صدارتها الحق في الخصوصية، كما ورد في المواثيق الدولية الملزمة، وعلى رأسها المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية، التي تحظر أي تدخل تعسفي أو غير مشروع في الحياة الخاصة للأفراد، وتؤكد ضرورة حماية الكرامة الإنسانية من أي اعتداء مؤسسي مموّه بغلاف تقني أو تنظيمي[1].

أمّا في التشريع الفرنسي، فقد تولّى المشرّع تنظيم استخدام الوسائل التقنية المتقدّمة في ميدان التحقيق الجنائي ضمن أحكام قانون الإجراءات الجنائية الفرنسي، حيث أرسى إطارًا قانونيًا محكمًا يُقيّد اللجوء إلى أدوات المراقبة الإلكترونية، لا سيّما حين يتعلّق الأمر بجمع بيانات ذات طابع بالغة الحساسية. وقد اشترط القانون صراحةً صدور إذن قضائي مُسبق كشرط جوهري لاكتساب تلك الإجراءات مشروعية قانونية، بما يضمن الخضوع للرقابة القضائية المسبقة ويحول دون المساس غير المشروع بالحقوق الأساسية للأفراد[2].

في المقابل، لا تزال جملة من الأنظمة القانونية، لا سيما في بعض الدول العربية، تُواجه تحديات بنيوية على المستوى التشريعي في ما يتصل بتنظيم جمع الأدلة المستخرجة آليًا. إذ تعاني التشريعات الجنائية في هذه السياقات من قصور ظاهر في النصوص القانونية التي تُنظّم صراحةً استخدام تقنيات الذكاء الاصطناعي في سياق التحقيقات الجنائية، وهو ما أفضى إلى نشوء فراغ تشريعي يُمكن أن يُستغل، في غياب رقابة قضائية صارمة، لجمع بيانات شخصية ذات طابع حساس خارج الأطر الضابطة، بما يُهدد بانتهاك مبدأ المشروعية ويُعرّض الحقوق الأساسية للأفراد لخطر التجاوز غير المشروع[3].

ومن أبرز الضوابط القانونية التي يتعيّن استحضارها لضمان مشروعية جمع الأدلة الرقمية بالوسائل الآلية، يبرز أولا، مبدأ التناسب بوصفه حجر الزاوية في ضبط حدود التدخل في الحياة الخاصة. ويُحتّم هذا المبدأ ضرورة إحداث توازن دقيق بين جسامة الجريمة موضوع التحقيق من جهة، وبين مستوى التوغّل في خصوصية الأفراد من جهة أخرى. فلا يُعقل – قانونًا ولا عدلًا – تبرير اللجوء إلى أدوات تحليلية شاملة أو تقنيات مراقبة فائقة الاتساع في سياق تحقيقات تتعلق بجرائم بسيطة أو محدودة الأثر، وهو ما أكّدته لجنة البندقية في رأيها الصادر بشأن الرقابة

(1) United Nations, 1966, Article 17.

(2) Code de procédure pénale, Article 706-95.

(3) البدوي، عبد المجيد، الذكاء الاصطناعي والتحقيق الجنائي، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020، ص 143.

الإلكترونية الواسعة، باعتباره انحرافًا عن مقتضيات التناسب ومساسًا غير مبرّر بالحقوق الجوهرية للأفراد. ثانيًا، ينبني مبدأ الضرورة على القاعدة الجوهرية التي تلزم حصر جمع البيانات في حدود ما لا بدّ منه لتحقيق الغاية القانونية المشروعة، مع استبعاد اللجوء إلى وسائل ذات أثر تدخلي فائق متى توفرت بدائل أقل إلحاحًا. ثالثًا، يجب أن تكون عمليات جمع البيانات محكومة برقابة قضائية مشددة وفعالة، تتطلب الحصول على إذن قضائي مسبق مستند إلى مبررات قانونية واضحة، بما يضمن توفير ضمانة حقيقية ضد التعسف والتجاوز[1].

إن انعدام هذه الضوابط من شأنه أن يفتح الباب واسعًا أمام انتهاكات خطيرة تطال الحقوق والحريات الأساسية، بل ويُقوّض مرتكزات العدالة الجنائية برمّتها، بما يُخلّ بمبدأ المشروعية ويُفقد الإجراءات القضائية نزاهتها ومشروعيتها. ومن ثم، تبرز الحاجة الملحّة إلى صياغة أطر تشريعية دقيقة ومحكمة، تُكرّس شرعية جمع الأدلة الرقمية المستخرجة بوسائل آلية، وتُرسّخ قواعد صريحة تُنظّم استخدام تقنيات الذكاء الاصطناعي في الحقل الجنائي، على نحو يوفّق بين مقتضيات الفعالية في مكافحة الجريمة وضمانات صون الحقوق الفردية والحريات الدستورية.

وفي ضوء هذه التحديات الإجرائية والتقييدات القانونية الناظمة لمشروعية جمع هذا النوع من الأدلة، يثور تساؤل محوري لا يقل شأنًا، يتعلق بمدى حجية هذه الأدلة في الإثبات الجنائي، وما يحيط بقبولها من معايير وضمانات قانونية، وهو ما سيشكّل محور المبحث الثاني.

(1) Conseil Constitutionnel, Décision n° 2015-713 DC, 23 juillet 2015.

المبحث الثاني:

حجية الأدلة المستخرجة آليًا في الإثبات الجنائي

عقب الوقوف على الطبيعة القانونية للأدلة الرقمية المستخرجة بوسائط الذكاء الاصطناعي، وبيان خصائصها التقنية والضوابط المعيارية التي تحكم مشروعيتها، تبرز إشكالية محورية ذات ثقل بالغ في نطاق العدالة الجنائية، تتمثّل في مدى حجّية هذه الأدلة في ميدان الإثبات. فمع التصاعد المضطرد في توظيف تقنيات الذكاء الاصطناعي لتحليل البيانات والتنبؤ بالأنماط السلوكية الإجرامية، ظهرت أدلة رقمية تتسم بدرجة فائقة من التعقيد[1]، مُستمدّة من خوارزميات عميقة، قد تعجز الكوادر القضائية التقليدية عن الإحاطة بمنطق اشتغالها أو تفسير بنيتها الحسابية على نحو شفاف. ويفرض هذا الواقع جملة من التحديات القانونية والإجرائية الدقيقة، ترتبط بالمعايير المعتمدة لقبول هذه الأدلة أمام المحاكم، وشروط صلاحيتها كوسيلة للإدانة الجنائية، فضلاً عن حدود قابليتها للطعن والمنازعة. كما يُثير تساؤلات جوهرية حول مدى موثوقيتها، ونزاهة بنيتها التحليلية، وإمكان إخضاعها للمراجعة القضائية الدقيقة، وكل ذلك في ضوء الضمانات المكفولة لمحاكمة عادلة، وكفالة غير منقوصة لحقوق الدفاع.

لذلك، يسعى هذا المبحث إلى دراسة هذه الإشكالية في بُعدين متكاملين: أولًا، من خلال تحليل المعايير الفنية والقانونية التي تحكم قبول هذه الأدلة واعتبارها موثوقة في الإثبات الجنائي. وثانيًا، من خلال بحث حدود الطعن في مشروعيتها وقيمتها الإثباتية، بما يضمن حماية حقوق المتهم وتحقيق التوازن الضروري بين فعالية العدالة الجنائية وصيانة الحقوق والحريات الأساسية.

المطلب الأول: المعايير الفنية والقانونية لقبول الأدلة الرقمية المستخرجة آليًا في الإثبات الجنائي

يُشكّل قبول الأدلة الرقمية المستخرجة آليًا عبر تقنيات الذكاء الاصطناعي أمام القضاء تحديًا مركّبًا بالغ الدقة، يستوجب إرساء معايير معيارية مُحكَمة تكفل احترام مقتضيات المحاكمة العادلة وصون الضمانات الجوهرية لحقوق الدفاع. فخصوصية هذه الأدلة، المرتبطة بكونها نتاج خوارزميات تحليلية معقّدة، تُلقي على عاتق المشرّع والقاضي عبء وضع ضوابط قانونية واضحة ومحددة توازن بين فعالية أدوات مكافحة الجريمة، من جهة، والحفاظ على نزاهة الإجراءات القضائية، من جهة أخرى.

(1) Cath, C, Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges, Philosophical Transactions of the Royal Society A, 2018, p 79–81.

ويُعد معيار الموثوقية التقنية في صدارة هذه الضوابط، إذ يُشترط إمكان التحقّق من سلامة البنية الخوارزمية المعتمدة في جمع البيانات وتحليلها، مع ضمان خلوّها من العيوب البنيوية أو الانحرافات الناتجة عن انحيازات كامنة في البيانات التدريبية، والتي قد تنسف دقة النتائج المستخرجة وتُفضي إلى أحكام غير عادلة. وفي هذا السياق، أرست المحاكم الأمريكية معيار Daubert لقبول الأدلة العلمية، والذي يُلزم القاضي بالتثبت من أن المنهجية المعتمدة قد خضعت لاختبارات علمية مُعترف بها، وحازت على قبول معتبر لدى الأوساط العلمية المتخصصة، وتتمتع بنسبة خطأ معروفة ومحددة يمكن تقويمها[1].

وانطلاقًا من هذا التصور، شرعت بعض الهيئات القضائية في الولايات المتحدة في اشتراط إخضاع الخوارزميات الأمنية المعتمدة في تحليل البيانات الجنائية لتقييم مستقلّ ومحايد، يُعنى بالتثبت من شفافية بنيتها التقنية ونزاهة منطقها التحليلي، وتفادي ما قد يشوبها من تحيّزات ضمنية أو عيوب خفية. وقد شكّل الحكم الصادر في قضية State v. Loomis محطة فارقة في هذا السياق، حيث نبّه صراحة إلى المخاطر الجسيمة التي قد تنجم عن الارتهان غير المدروس لتقنيات التنبؤ بالخطر الجنائي، دون تمكين الجهات القضائية والدفاع من النفاذ إلى الأسس الفنية التي تقوم عليها تلك الأنظمة، الأمر الذي من شأنه أن يفتقر إلى الحد الأدنى من مقومات العدالة الإجرائية ويُقوّض حق المتهم في محاكمة منصفة[2].

في منظومة التشريع الأوروبي، يشترط النظام العام لحماية البيانات (GDPR) أن تخضع القرارات الآلية التي يترتب عليها أثر قانوني أو تأثير جوهري في مراكز الأفراد القانونية، لقدر معياري من الشفافية، يكفل الاطلاع على منطق اتخاذها. كما يُلزم بوجود آليات مراجعة بشرية فاعلة، تُتيح للمعنيّين الاعتراض والفحص، اتّقاءً لمخاطر الانفراد الخوارزمي بالقرار دون رقابة بشرية ضامنة لمبادئ العدالة الإجرائية والتوازن الحقوقي[3]. كما بادرت المفوضية الأوروبية إلى إصدار مسودة «قانون الذكاء الاصطناعي» (AI Act)، الذي يرسي معايير صارمة تنظّم تشغيل «أنظمة الذكاء الاصطناعي عالية الخطورة»، فارضًا التزامات دقيقة تتعلّق بتوثيق بيانات التدريب، والتحقق من آليات اختبار النماذج، بغية الحد من الانحيازات الكامنة وضمان نزاهة المخرجات، في إطار تشريعي يوازن بين التطور التقني وحماية الحقوق الأساسية[4].

أمّا في السياق الفرنسي، فقد أوجب المشرّع إخضاع الأدلة الإلكترونية لنظام توثيق صارم، يكفل سلامة سلسلة الحفظ (chaîne de conservation)، ويُؤمِّن قابليتها للتحقق القضائي، على نحو ما نصّت عليه المادة 1-56 من قانون الإجراءات الجنائية الفرنسي. وتُعدّ هذه القاعدة شرطًا

(1) Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, 1993.
(2) Wisconsin Supreme Court, 2016.
(3) Regulation (EU) 2016/679, Article 22.
(4) European Commission, 2021, Proposal for an AI Act.

جوهريًا للحيلولة دون التلاعب أو التعديل غير المشروع في البيانات الرقمية خلال مراحل الجمع أو المعالجة الآلية. وعلاوة على شرط الموثوقية التقنية، فإن القبول القضائي لهذا النمط من الأدلة يقتضي التقيّد بمبدأ المشروعية في إجراءات جمعها، وذلك من خلال احترام الضمانات الإجرائية والدستورية، وفي مقدّمتها ضرورة الحصول على إذن قضائي مسبق عند التعامل مع بيانات ذات طابع حسّاس. وفي هذا الإطار، نصّت بعض التشريعات العربية، ومنها القانون الاتحادي الإماراتي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، على اشتراط صدور إذن عن النيابة العامة لاعتراض أو مراقبة الاتصالات الإلكترونية، تحقيقًا للتوازن بين مقتضيات الأمن الرقمي وصيانة الحقوق الدستورية المكفولة للأفراد[1].

كذلك، تستلزم المعايير القانونية المعتمدة لقبول الأدلة الرقمية توافر قابلية المراجعة القضائية، بما يعني أن الخوارزميات المستعملة في استخراج تلك الأدلة يجب أن تكون شفافة من حيث البنية، قابلة للفحص، ومفسَّرة تفسيرًا يُمكّن القاضي وجهات الدفاع من الوقوف على أسسها التقنية والاعتراض عليها عند الاقتضاء. إذ إن غياب هذه الإمكانية من شأنه أن يُحول تلك الأدلة إلى ما يشبه «صندوقًا أسودًا» عصيًّا على المساءلة، يَحُول دون الطعن في نتائجه، ويُقوّض جوهر الحق في الدفاع المشروع. وفي هذا السياق، أكدت جمعية المحامين الأمريكية (ABA) في تقريرها الصادر سنة 2018، على ضرورة تمكين أطراف الخصومة الجنائية من الوصول إلى معلومات كافية حول طبيعة أنظمة الذكاء الاصطناعي الموظّفة في سياق التحقيقات، بما يسمح بمساءلة منهجيتها، واختبار درجة موثوقيتها، ودرء مخاطر الانزلاق نحو عدالة مُعتِمة تفتقر لأبسط ضمانات التمحيص القضائي الرشيد[2].

أخيرًا، يُعدّ شرط تحقيق التوازن بين الضرورة والتناسب ركيزة لا غنى عنها في إضفاء المشروعية القانونية على الأدلة المستخرجة بواسطة تقنيات الذكاء الاصطناعي، إذ يتعيّن أن يكون توظيف هذه الوسائل محصورًا في حدود الأهداف المشروعة، ومتناسبًا مع جسامة الفعل الجرمي المرتكب. ولا يُقبل، بأي وجه، التسويغ بجمع بيانات ضخمة وتحليلها آليًا بناءً على اشتباه غير مؤسس، لما ينطوي عليه ذلك من تهديد بنيوي خطير بتحويل أدوات الذكاء الاصطناعي إلى منظومة رقابة شمولية تهدر الخصوصيات وتقوّض الحريات العامة من أساسها. وفي هذا الإطار، حذّرت اللجنة البرلمانية البريطانية المعنية بالذكاء الاصطناعي من مغبة الانزلاق إلى هذا المنحدر، مشددة على ضرورة سنّ قواعد قانونية دقيقة ومحددة، تكبح جماح الرقابة المفرطة، وتضمن انضباط استخدام الأدوات الذكية بضوابط التناسب والعدالة الإجرائية[3].

(1) قانون مكافحة جرائم تقنية المعلومات الإماراتي، المادة 48.

(2) American Bar Association, 2018, Report on AI in Criminal Justice.

(3) UK House of Lords, AI in the UK: Ready, Willing and Able? House of Lords Select Committee on Artificial Intelligence, 2018, p 15.

في ضوء تلك الضوابط الفنية والمعايير القانونية التي تؤطر مشروعية قبول الأدلة الرقمية المستخرجة آليًا، تتجلّى إشكالية قانونية على قدرٍ بالغ من الأهمية، تتمثّل في الحدود الفاصلة لإمكانية الطعن في مشروعية هذه الأدلة وقوتها الحجّية داخل البنية القضائية. وهي الإشكالية التي ستُشكّل محور المعالجة في المطلب التالي.

المطلب الثاني: حدود الطعن في مشروعية الأدلة الرقمية المستخرجة آليًا وحجيتها في الإثبات الجنائي

إن الطبيعة المركّبة للأدلة الرقمية المستخرجة آليًا عبر تقنيات الذكاء الاصطناعي تُثير تحدّيًا قضائيًا دقيقًا يتمحور حول مدى قابليتها للطعن، سواء من جهة مشروعيتها أو من جهة قيمتها الإثباتية ضمن المسار الجنائي. فعلى الرغم من ما تتيحه هذه الأدلة من قدرات تقنية فائقة في تفكيك البنى المعقّدة للجرائم الرقمية، إلا أنّها لا تخلو من مخاطر قانونية قد تمس جوهر الضمانات المكفولة للمتهم، وفي مقدّمتها حق الدفاع والحق في المحاكمة العادلة، ما يستوجب من الأنظمة القانونية إرساء قواعد محكمة تُحدّد نطاق الطعن في تلك الأدلة، وتوازن بين اعتبارات الفعالية الجنائية وحماية الحقوق الأساسية. وفي هذا السياق، يُمثّل تمكين المتهم من ممارسة حق الدفاع في مواجهة الأدلة الرقمية الآلية حجر الأساس في صرح أي منظومة إجرائية عادلة. فرغم ما تنطوي عليه الخوارزميات التحليلية من دقة تقنية متقدمة، فإن مقتضيات العدالة الإجرائية تقتضي إتاحة الفرصة كاملة للمتهم ودفاعه للاطلاع على منهجية جمع البيانات وآليات تحليلها، والطعن في مصداقية النتائج المستخرجة منها. وقد شدّدت اللجنة الوطنية للمحامين في إسبانيا، في تقريرها الصادر سنة 2020، على ضرورة ضمان إمكانية مراجعة النماذج الخوارزمية المُستخدمة في التحقيقات الجنائية، مؤكدةً أن حرمان الدفاع من هذا الحق يُعدّ انتهاكًا جسيمًا لمبدأ المواجهة، بما يخلّ بالتوازن الإجرائي ويقوّض أركان المحاكمة العادلة[1].

ثانيًا، تُعد قابلية الأنظمة الذكية للخضوع للفحص القضائي شرطًا جوهريًا لاكتساب مشروعيتها كوسيلة إثبات، إذ لا يمكن إسناد الحجية القانونية لأي أداة تقنية ما لم تكن قابلة للتحقّق من قِبل السلطة القضائية المختصة. وفي هذا الإطار، تشترط قواعد الإجراءات الجنائية الألمانية، المنصوص عليها في § 100a من قانون الإجراءات الجنائية، أن تكون الوسائل التقنية المعتمدة في الإثبات خاضعة لإمكان المراجعة القضائية، بما يشمل الحفاظ على تسلسل البيانات الزمني، وإمكانية التثبت من طرق جمعها ومعالجتها. ويُعدّ ذلك ضمانة أساسية تُمكّن القاضي من بسط رقابته على مشروعية الدليل، ومدى التزامه بالضوابط الإجرائية المكفولة. ثالثًا، تثير إشكالية «الصندوق الأسود» في الخوارزميات المخاوف الأعمق والأكثر تعقيدًا في هذا المضمار، إذ إن اعتماد الجهات الأمنية على أنظمة معقدة مغلقة المصدر في استخراج الأدلة الرقمية يحول، في كثير من الحالات،

(1) Consejo General de la Abogacía Española, 2020.

دون تمكين الدفاع من النفاذ إلى تلك الأنظمة أو فهم آليات عملها، وهو ما يُقوّض مبدأ الشفافية ويُضعف القدرة على الطعن. وفي تقرير صادر عن المفوضية الكندية للخصوصية، تم التحذير من المخاطر الكامنة في هذا الغموض الحسابي، مشيرًا إلى أنّ عدم الإفصاح عن منطق القرارات الآلية قد يُفضي إلى تكريس تمييز خفي أو أخطاء منهجية، الأمر الذي استدعى الدعوة إلى إقرار التزامات قانونية صريحة تُوجب الإفصاح عن البنية المنطقية للأنظمة الذكية عند استخدامها في الإجراءات ذات الأثر القانوني[1].

رابعًا، تمثّل قابلية الطعن في مشروعية إجراءات جمع البيانات الأصلية بُعدًا قانونيًا بالغ الأثر، يُلقي بظلاله على القيمة الإثباتية للأدلة الرقمية المستخرجة لاحقًا، حتى وإن بدت نتائج المعالجة الآلية سليمة من الناحية التقنية. ذلك أن انتهاك المشروعية عند نقطة الانطلاق – أي أثناء جمع البيانات – يستتبع، تبعًا للقاعدة الأصولية المعروفة بـ»ثمرة الشجرة المسمومة»، إبطال النتائج المترتبة عليها. وقد كُرِّس هذا المبدأ في الفقه القضائي الأمريكي ضمن حكم المحكمة العليا في قضية (Silverthorne Lumber Co. v. United States (251 U.S. 385, 1920، حيث قضى بعدم جواز استخدام الأدلة المستخلصة من مصادر غير مشروعة، ولو أعيدت معالجتها لاحقًا باستخدام تقنيات متقدمة. خامسًا، يُعدّ التحقق من خلوّ مخرجات الذكاء الاصطناعي من التحيّز والتمييز معيارًا جوهريًا في ضبط مشروعية تلك الأدلة. فقد نبّهت دراسة صادرة عن جامعة أكسفورد إلى أنّ أنظمة التنبؤ الجنائي، إذا استُند في تدريبها إلى بيانات تاريخية مشوبة بانحيازات إثنية أو اجتماعية موروثة، قد تُفضي إلى قرارات تمييزية مُنهجة، تُعيد إنتاج تلك الأنماط الإقصائية في ثوب رقمي خفي، الأمر الذي يهدّد مبدأ المساواة أمام القانون، ويقوّض ثقة الجمهور في عدالة الأنظمة الذكية الموظّفة في الحقل الجنائي[2]. وهو ما يفتح الباب على مصراعيه للطعن في نتائج التحليل الآلي متى تبيّن أنّ مخرجاته مشوبة بانحياز أو تفتقر إلى الحياد الموضوعي، الأمر الذي يُحتّم على السلطة القضائية إخضاع الخوارزميات المستخدمة وبيانات التدريب المُعتمدة لفحص دقيق واستقصاء علمي معمّق. سادسًا، يُعدّ الحق في طلب استبعاد الأدلة ضمانة إجرائية مركزية لا غنى عنها في صون توازن المحاكمة الجنائية. ففي النظام القضائي الفرنسي، كرّس الاجتهاد القضائي مبدأ بطلان الإجراءات التي تفتقر إلى الشرعية أو تنتهك الضمانات الجوهرية للمتهم، بما في ذلك الأدلة الإلكترونية التي جُمعت أو عولجت على نحو غير مشروع أو بشكل يفتقر إلى التناسب مع الحق المستهدف بالحماية. وبمقتضى هذا المبدأ، يُتاح لجهة الدفاع التماس استبعاد الأدلة المستخرجة بوسائل آلية، متى ثبت أنّها نُفذت على خلاف مقتضيات القانون أو تعارضت مع الحقوق الأساسية المكفولة دستوريًا[3].

(1) Office of the Privacy Commissioner of Canada, 2021.

(2) Crawford, K., & Calo, R., There is a Blind Spot in AI Research, Nature, 2016, p 178.

(3) Cour de cassation, chambre criminelle, n° 16-82.066, 11 janvier 2017.

تهدف هذه القواعد والضمانات، في مجموعها، إلى إرساء توازن محكم بين مقتضيات الفعالية في مكافحة الجريمة الرقمية من جهة، وبين صيانة حقوق الدفاع وحماية الحرية الفردية من جهة مقابلة، في ظل التنامي المتسارع لأدوات التحقيق التقنية. وهي بذلك تُلقي على عاتق المشرّع والسلطة القضائية مسؤولية بلورة معايير قانونية متطورة وواضحة، تُراعي الخصوصية البنيوية للأدلة الرقمية المستخرجة آليًا، دون أن تُفرّط في المبادئ المؤسسة للعدالة الجنائية. وفي ضوء ما تقدّم من حدود قانونية تؤطر مشروعية هذه الأدلة وقابليتها للطعن وحجّيتها ضمن منظومة الإثبات، تتجلّى الحاجة الملحّة إلى تشييد إطار قانوني متوازن، يُحقّق الانسجام بين فعالية الملاحقة الجنائية في الفضاء الرقمي، وضمانات الدفاع والحقوق الإنسانية الأصيلة. وهي الخلاصة التي سيتناولها هذا البحث في خاتمته، مقرونة بأبرز ما انتهى إليه من نتائج وتوصيات مُقترحة.

الخاتمة

تُعد مسألة توظيف تقنيات الذكاء الاصطناعي في المجال الجنائي من أعقد التحديات التي تفرضها التحوّلات التكنولوجية المتسارعة على البُنى القانونية المعاصرة، بالنظر لما ينطوي عليه هذا التوظيف من إمكانات تحليلية فائقة، تقابلها في الوقت ذاته إشكاليات قانونية وأخلاقية شديدة التشعّب. فقد مكّنت هذه التقنيات أجهزة إنفاذ القانون من تفكيك أنماط إجرامية مموّهة، عبر تحليل كميات هائلة من البيانات الرقمية، والوصول إلى أدلة كانت مستعصية في ظل الوسائل التقليدية. غير أنّ هذه القدرات المتقدمة لا تأتي بمعزل عن أثمان قانونية باهظة، في مقدّمتها ضرورة صون الحقوق الأساسية، وعلى رأسها الحق في الخصوصية والمحاكمة العادلة. ذلك أن الأدلة الرقمية المستخرجة آليًا عبر خوارزميات الذكاء الاصطناعي تتسم بتعقيدها البِنيوي، وغموض منهجياتها، الأمر الذي يثير تساؤلات جوهرية حول مشروعية إجراءات جمعها، وإمكانية التدقيق في آلية تحليلها، ومدى صلاحيتها كوسائل إثبات ضمن منظومة العدالة الجنائية. وقد سعى هذا البحث إلى معالجة هذه الإشكالية المركّبة من خلال تحليل الطبيعة القانونية لهذه الأدلة، واستجلاء الشروط الفنية والقانونية التي تضبط مشروعيتها، والمعايير الضامنة لقبولها قضائيًا. كما تناول بالدراسة حدود الطعن فيها، والضمانات الإجرائية التي تكفل حق الدفاع، وصولًا إلى رسم معالم مقاربة قانونية متوازنة تُوفّق بين ضرورات مكافحة الجريمة الرقمية، ومقتضيات احترام الحقوق الدستورية للمواطنين.

وفي ضوء هذا التحليل النظري والتطبيقي للإطار القانوني المنظّم للأدلة الرقمية المستخرجة آليًا عبر الذكاء الاصطناعي، توصّل البحث إلى النتائج الآتية:

1. توصّل البحث إلى أنّ الأدلة الرقمية الناتجة عن تقنيات الذكاء الاصطناعي تتميّز بقدرة تقنية فائقة في رصد أنماط الجريمة الرقمية المعقّدة، إلا أنها تستبطن طابعًا احتماليًا وتعقيدًا خوارزميًا يستوجب تأطيرًا قانونيًا دقيقًا ومحكمًا.
2. أظهر التحليل أن قبول هذه الأدلة في مجال الإثبات الجنائي مشروط باحترام مجموعة من المعايير الفنية والقانونية، وفي طليعتها: الموثوقية، الشفافية، قابلية الفحص القضائي، ومشروعية جمع البيانات الأصلية.
3. بيّنت الدراسة أن ضمانات الدفاع، ولا سيما الحق في الطعن، تُمثّل ركيزة لا غنى عنها لضمان عدالة المحاكمة، وهو ما يستلزم تمكين الدفاع من فحص وتفنيد مخرجات الأنظمة الذكية داخل بيئة قضائية تتسم بالوضوح والانفتاح الإجرائي.

وبناءً على ما سبق، يوصي البحث بجملة من التدابير التشريعية والمؤسسية التي من شأنها

إرساء توازن موضوعي بين مقتضيات الأمن الرقمي ومتطلبات حماية الحقوق الأساسية، وأهمها:

1. ضرورة إرساء إطار تشريعي وطني متكامل يُعرّف الأدلة الرقمية المستخرجة آليًا تعريفًا دقيقًا، ويُحدّد ضوابط جمعها وشروط استخدامها ضمن الإجراءات الجنائية.
2. إلزام السلطات الأمنية والقضائية بالشفافية التقنية، من خلال ضمان إمكانية إخضاع الخوارزميات للفحص والمراجعة، وتكوين الفاعلين القضائيين في المجال التقني لرفع قدرتهم على فهم آليات عمل هذه النظم.
3. تعزيز أطر التعاون الدولي في ميدان مكافحة الجريمة الرقمية، عبر اتفاقات ومعايير قانونية موحّدة تنظم تبادل البيانات والتحقيقات، وتراعي في الوقت ذاته الضمانات الحقوقية المعترف بها دوليًا.

وفي ضوء ما انتهى إليه هذا البحث، يبقى موضوع الأدلة الرقمية المستخرجة آليًا مجالًا خصبًا لمزيد من الاشتغال العلمي والنقاش التشريعي، لا سيما في ما يتعلّق بمسؤولية مطوّري الخوارزميات عن نتائجها، وتحديد القواعد الناظمة لإثبات الأدلة المستخرجة من الأنظمة التنبؤية، فضلًا عن تحليل أُطر التعاون القضائي الدولي في مكافحة الجرائم ذات الطابع العابر للحدود. وهي قضايا باتت تفرض نفسها بوصفها محاور بحثية مستجدة، تستلزم انخراطًا أكاديميًا وتشريعيًا جادًّا، يكفل مواءمة القانون مع الطفرات التقنية التي يفرضها عصر الذكاء الاصطناعي.

قائمة المراجع والمصادر

• مراجع باللغة العربية

1. البدوي، عبد المجيد، الذكاء الاصطناعي والتحقيق الجنائي، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020.

2. شحاتة، أسامة، الذكاء الاصطناعي والقانون، دار المنهل اللبناني، بيروت، لبنان، 2021.

• مراجع بالإنجليزية

1. American Bar Association, Report on Artificial Intelligence in Criminal Justice. American Bar Associatio, 2018.

2. Cath, C, Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges, Philosophical Transactions of the Royal Society A, 2018.

3. Crawford, K., & Calo, R., There is a Blind Spot in AI Research, Nature, 2016.

4. Dignum, V., Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way, Springer, 2019.

5. European Commission, Proposal for a Regulation on Artificial Intelligence (AI Act), 2021.

6. Office of the Privacy Commissioner of Canada, A Regulatory Framework for AI: Recommendations for PIPEDA Reform, Government of Canada, 2021.

7. Pasquale, F., The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.

8. Russell, S., & Norvig, P., Artificial Intelligence: A Modern Approach, 4th edition, Pearson, 2021.

9. Shapiro, A. K., Predictive Policing and Artificial Intelligence. Yale Law & Policy Review, 37(2), 2019.

10. UK House of Lords, AI in the UK: Ready, Willing and Able? House of Lords Select Committee on Artificial Intelligence, 2018.

11. UNODC, Compendium on AI and Criminal Justice, United Nations Office on Drugs and Crime, 2021.

• قوانين وتشريعات

1. Conseil Constitutionnel, Décision n° 2015-713 DC du 23 juillet 2015.

2. European Data Protection Board (EDPB), Guidelines 10/2020 on Restrictions under

Article 23 GDPR, 2020.

3. European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), 2016.

4. France. (n.d.). Code de procédure pénale, Articles 56-1 et 706-95.

5. Germany. (n.d.). Strafprozessordnung (StPO), § 100a.

6. United Arab Emirates. (2012). Federal Law No. 5 of 2012 on Combating Cybercrimes, as amended.

7. Venice Commission, Opinion on Mass Surveillance, CDL-AD, 2015.

• مراجع قانونية وأحكام قضائية

1. Cour de cassation, chambre criminelle, Arrêt n° 16-82.066, January 11, 2017.

2. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 1993.

3. European Court of Human Rights, Uzun v. Germany, Application no. 35623/05, 2010.

4. Court of Justice of the European Union, Case C-293/12 Digital Rights Ireland Ltd v Minister for Communications, 2014.

5. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 1920.

6. State v. Loomis, 881 N.W.2d 749 (Wisconsin Supreme Court, 2016.