مجلة الكوفة للعلوم القانونية والسياسية

ISSN

٢٠٧٠٩٨٣٨ (مطبوع)٣٠٠٦٧٦٧٧ (إلكتروني)

العدد الأول / المجلد الثامن عشر

تاريخ النشر / ٢٠/٣/٢٠٢٦

# دور الذكاء الصناعي في الوقاية من الجريمة

# The role of artificial intelligence in crime prevention

**الدكتور محمدعلى حاجي ده آبادي - استاذ في جامعة قم الحكومية**

**أسامة ستار حاجي - طالب دكتوراه قانون جنايى فى جامعة قم الحكومية**

**المستخلص:** تناولت هذه الدراسة تحليل الدور المتنامي للذكاء الصناعي في الوقاية من الجريمة ومكافحتها، من خلال استعراض تطبيقاته في التحليل الجنائي الاستباقي، ورصد الجرائم الإلكترونية، وتعزيز سلامة الفضاء العام في المدن الذكية، ومكافحة الجرائم المالية، ودعم التحقيقات الجنائية. وقد بيّن البحث بمنهج وصفي و تحليلي أن التحولات التقنية الكبرى أدت إلى توسّع نطاق الجريمة وتعقيد أساليبها، مما جعل الأدوات التقليدية غير كافية للكشف عنها أو منعها، في حين أتاح الذكاء الصناعي قدرات تحليلية عميقة تستند إلى معالجة البيانات الضخمة والخوارزميات التنبؤية التي تحدد أنماط السلوك الإجرامي وتوجه السلطات الأمنية إلى مناطق الخطر الفعلية. وأظهرت الدراسة أن الذكاء الصناعي أصبح الأداة الأكثر فاعلية في مواجهة الجرائم الإلكترونية، بفضل قدرته على تحليل حركة الشبكات في الزمن الحقيقي، وكشف الهجمات قبل وقوعها، والتعرف على الأنشطة الشاذة التي قد تؤدي إلى اختراق أو سرقة بيانات أو تخريب أنظمة. كما اتضح أن المدن الذكية تعتمد بصورة متزايدة على المراقبة الذكية، وتحليل الفيديو والسلوك، وإدارة الحشود، مما يعزز الوقاية ويرفع مستوى الأمن الحضري. وفي المجال المالي، أثبتت الأنظمة الذكية قدرتها على اكتشاف غسل الأموال والاحتيال والتلاعب المالي عبر تحليل البصمة المالية للعميل ورصد الانحرافات، في حين قدّم الذكاء الصناعي دعماً نوعياً للتحقيقات الجنائية من خلال تحليل الأدلة الرقمية، والصور، والفيديو، والبصمات الوراثية، وإعادة بناء مسرح الجريمة، وبالرغم من هذا التقدم، أبرزت الدراسة تحديات قانونية وأخلاقية تتعلق بالخصوصية، وتحقيق الشفافية الخوارزمية، وتحديد المسؤولية عن الأخطاء التقنية، مما يجعل الحاجة ملحة لوضع إطار تشريعي يوازن بين الفعالية الأمنية وحماية الحقوق. وتخلص الدراسة إلى أن الذكاء الصناعي يمثل مستقبل السياسة الجنائية الحديثة، شريطة ضبطه بنظم قانونية تضمن الاستخدام الرشيد والتوافق مع مبادئ العدالة.

**الكلمات المفتاحية: الذكاء الصناعي، الجريمة، الوقاية، التدابير الإحترازية، القانون العراقي.**

**Abstract:** This study analyzes the growing role of artificial intelligence (AI) in crime prevention and control, reviewing its applications in proactive criminal analysis, cybercrime detection, enhancing public safety in smart cities, combating financial crimes, and supporting criminal investigations. The research, employing a descriptive and analytical approach, demonstrates that major technological shifts have led to an expansion in the scope of crime and a more complex set of methods, rendering traditional tools insufficient for detection or prevention. Meanwhile, AI has provided in-depth analytical capabilities based on big data processing and predictive algorithms that identify patterns of criminal behavior and guide security authorities to actual danger zones. The study shows that AI has become the most effective tool in combating cybercrime.

Thanks to its ability to analyze network traffic in real time, detect attacks before they occur, and identify anomalous activities that could lead to data breaches, theft, or system sabotage, smart cities are increasingly relying on intelligent surveillance, video and behavioral analysis, and crowd management, thus enhancing prevention and raising the level of urban security. In the financial sector, intelligent systems have proven their ability to detect money laundering, fraud, and financial manipulation by analyzing a client's financial fingerprint and monitoring deviations, while artificial intelligence has provided significant support to criminal investigations through the analysis of digital evidence.

Images, videos, DNA fingerprinting, and crime scene reconstruction are among the advancements in artificial intelligence. Despite these advancements, the study highlights legal and ethical challenges related to privacy, achieving algorithmic transparency, and determining liability for technical errors. This underscores the urgent need for a legislative framework that balances security effectiveness with the protection of rights. The study concludes that artificial intelligence represents the future of modern criminal policy, provided it is regulated by legal systems that ensure its judicious use and compliance with the principles of justice.

**Keywords: Artificial intelligence, crime, prevention, Precautionary measures , Iraqi law.**

المقدمة

شهد المجتمع المعاصر تحولًا جذريًا في طبيعة المخاطر الإجرامية، بعد أن اتسعت مجالات النشاط الاقتصادي والمالي والرقمي، وصارت الجريمة أكثر تعقيدًا في أدواتها وأوسع أثرًا في نتائجها. ولم تعد وسائل مكافحة الجريمة التقليدية قادرة وحدها على مواجهة هذا الواقع الجديد، في ظل دخول الجريمة المعلوماتية، والجرائم العابرة للحدود، وجرائم غسل الأموال، وانتهاكات الخصوصية الرقمية، وتلاعب الخوارزميات، ضمن دائرة التهديدات التي تواجه الدول. وفي هذه البيئة المتغيرة برز الذكاء الصناعي بوصفه أحد أهم الأدوات التي يمكن أن تستند إليها السياسة الجنائية لتحقيق وقاية فعّالة، قادرة على الاستجابة السريعة للمتغيرات، وتحليل الأنماط الإجرامية، واكتشاف السلوك الخطِر قبل أن يتحول إلى فعل مجرّم، وقد أدى التقدم الهائل في قدرات الحوسبة وتحليل البيانات إلى انتقال الذكاء الصناعي من مجرد التقاط إشارات تقنية محدودة إلى مستوى أعمق تتداخل فيه الخوارزميات مع البيانات الضخمة، مما يسمح باستقراء السلوك الإجرامي، وتحديد مناطق الخطورة، وإعادة بناء خرائط التوقعات الأمنية. ولم يعد دور الذكاء الصناعي مقتصرًا على كشف الأدلة أو تحليل الصور، بل أصبح عنصرًا أساسيًا في نماذج التنبؤ بالجريمة (Predictive Policing)، وفي إدارة المدن الذكية، ومراقبة الشبكات الرقمية، وتحليل المعاملات المالية، وتحديد الأنماط الشاذة التي قد تنبئ بوجود نشاط إجرامي. وهذا التطور فتح الباب أمام مرحلة جديدة من السياسة الجنائية التي تعتمد على الاستباق بدلاً من الردّ، وعلى جعل الوقاية هدفًا أوليًا قبل المنع أو العقاب.

تنبع أهمية هذا الموضوع من أن الجريمة الحديثة لم تعد فردية أو بسيطة، بل أصبحت جزءًا من شبكات عنقودية مرتبطة بالاقتصاد، والتكنولوجيا، وحركة رؤوس الأموال، وشبكات التواصل، وهو ما يجعل اكتشافها أو منعها دون أدوات تحليلية عالية الدقة أمرًا شبه مستحيل. وهنا يظهر الدور المحوري للذكاء الصناعي في تحليل الأنماط الإحصائية، وتحديد الروابط الخفية بين الوقائع، والكشف عن السلوكيات المريبة التي لا تستطيع القدرات البشرية رصدها في الوقت المناسب. كما أن قدرته على معالجة ملايين البيانات خلال ثوانٍ تجعله أداة فريدة في منع الهجمات الإلكترونية، وتحليل عمليات الاحتيال المالي، ورصد التلاعب بالأسواق، وتعقب الأنشطة الرقمية التي تستهدف المؤسسات والأفراد، مع ذلك، فإن توظيف الذكاء الصناعي في الوقاية من الجريمة لا يخلو من تحديات قانونية وأخلاقية تتعلق بالخصوصية وحماية البيانات، ومبدأ التناسب، واحترام الضمانات الإجرائية. فالقانون الجنائي يقوم على حرية الفرد، ولا يمكن للأنظمة الذكية أن تتجاوز هذه القيم أو تتحول إلى وسيلة رقابية غير منضبطة. ومن هنا يصبح التنظيم التشريعي الدقيق شرطًا أساسيًا لضمان أن يكون الذكاء الصناعي أداة للعدالة، لا وسيلة للمساس بالحقوق.

تسعى هذه الدراسة إلى تحليل دور الذكاء الصناعي في الوقاية من الجريمة في إطار قانوني متوازن، يدمج بين فوائد التقنية الحديثة وضرورات احترام الحقوق، وصولًا إلى رسم ملامح سياسة جنائية جديدة تستجيب لواقع متغير، وتحقق الأمن دون المساس بجوهر الحرية.

أولًا: الذكاء الصناعي بوصفه أداة تحليل جنائي استباقي: أفرزت التطورات التقنية المتسارعة الحاجة إلى أدوات تتجاوز القدرة البشرية التقليدية في رصد الظواهر وتحليلها والتنبؤ بمآلاتها، خاصة في المجال الجنائي الذي يعتمد بصورة جوهرية على فهم الأنماط السلوكية وتوقع المخاطر. وقد أدّى ظهور الذكاء الصناعي إلى إحداث نقلة نوعية في إمكانات التحليل الجنائي، لأنه قادر على التعامل مع كميات من المعلومات لا يمكن للإنسان معالجتها في الظروف الاعتيادية، فضلاً عن امتلاكه القدرة على تحديد الروابط الخفية بين الوقائع، والتقاط الإشارات الضعيفة التي لا تُرى في التحليل البشري المباشر. وهذا جعله اليوم في صميم السياسات الجنائية الحديثة بوصفه أداة تحليل استباقي تهدف إلى منع الجريمة قبل وقوعها، لا مجرد معالجتها بعد تحققها.[١]

كما تكمن أهم خصائص الذكاء الصناعي في المجال الجنائي في قدرته على استشراف التهديدات من خلال تحليل البيانات الضخمة التي تنتجها المؤسسات الأمنية والهيئات الحكومية والقطاعات الخاصة. وهذه البيانات قد تشمل سجلات الجرائم السابقة، وبلاغات المواطنين، وحركة المركبات، وكاميرات المراقبة، والمعاملات المالية، والمراسلات الإلكترونية، والسجلات الإدارية، وخرائط توزيع الجريمة بحسب الزمان والمكان، فضلاً عن البيانات الاجتماعية والسلوكية. وعند ربط هذه المعلومات عبر خوارزميات متقدمة—خصوصًا خوارزميات التعلم العميق والشبكات العصبية—يصبح النظام قادرًا على استخراج أنماط دقيقة تُنبئ بأن سلوكًا إجراميًا محددًا قد يتحقق في المستقبل القريب.[٢]

يظهر دور الذكاء الصناعي الاستباقي بوضوح في ما يُعرف بـ التنبؤ بالجريمة (Predictive Policing)، الذي يعتمد على تحليل الوقائع السابقة لبناء نماذج إحصائية تتوقع احتمالية وقوع الجريمة في منطقة معينة، وفي وقت معين، وعلى يد فئة معينة. وتساعد هذه النماذج أجهزة الشرطة على توزيع الموارد البشرية والإمكانيات الميدانية بصورة أكثر فاعلية، بحيث يتركّز الوجود الأمني في المناطق ذات الخطورة الأعلى، وهو ما يرفع معدلات الوقاية ويقلل الوقت اللازم للتدخل. وقد أثبتت التجارب العملية في دول عديدة أن استخدام الذكاء الصناعي في التنبؤ بالجريمة أدى إلى الانخفاض النسبي في بعض الجرائم مثل السرقات، والاعتداءات، والجرائم المرتبطة بالعنف، خاصة عندما يُستخدم النظام بالتكامل مع قواعد البيانات الجنائية.[٣]

وما يعزز الدور الاستباقي للذكاء الصناعي هو قدرته على تحليل السلوك الفردي والجماعي من خلال مراقبة التغيرات الطارئة على الأنماط اليومية للأفراد أو المجموعات، مثل الحركة غير المعتادة في مناطق معينة، أو التفاعل الرقمي المريب، أو الأنشطة المالية التي تشير إلى مخاطر غسل الأموال، أو الارتباطات الاتصالية التي توحي بتكوين شبكات إجرامية. وتصبح هذه القدرة أكثر قيمة حين يتعلق الأمر بالجرائم المنظمة التي تعمل ضمن شبكات معقدة ومتكررة النمط، وقد أتاح الذكاء الصناعي إمكانية دمج التحليل المكاني–الزماني بالجريمة، إذ يتم تحليل المكان والوقت الذي تتكرر فيه الجرائم على شكل "بؤر حرجة" (Hotspots). ومن خلال هذه النماذج، يمكن للنظام التنبؤ بمناطق الخطر المستقبلية، مما يسمح للأجهزة

الأمنية باتخاذ إجراءات احترازية قبل وقوع الجريمة، كتفعيل الرقابة، أو تعزيز الإنارة، أو إعادة توزيع الدوريات، أو مراقبة الأسواق ذات النشاط المشبوه.[٤]

من جانب آخر، يتضمن التحليل الجنائي الاستباقي للذكاء الصناعي القدرة على تقييم المخاطر الفردية للأشخاص ذوي السوابق أو المشتبه بهم عبر ربط بياناتهم الشخصية بنشاطهم الاجتماعي والاقتصادي والرقمي. وتساعد هذه القدرة على توقع احتمالية العود إلى الجريمة (Recidivism)، وهو ما يُعد عنصراً مهمًا للنيابات العامة والسلطات القضائية عند تقدير خطورة المتهمين. ومع ذلك، يظل استخدام هذه البيانات محاطًا بقيود قانونية صارمة لضمان عدم المساس بالحقوق الأساسية، ويمتد الدور الاستباقي للذكاء الصناعي ليشمل منع الجرائم الإلكترونية التي باتت من أكثر الجرائم تطورًا وتخفّيًا. فالأنظمة الذكية قادرة على مراقبة الشبكات الرقمية وتحليل سلوك المستخدمين ورصد الأنماط غير السوية التي تشير إلى محاولات اختراق أو نشر برامج خبيثة أو سرقة بيانات. ويتميز الذكاء الصناعي بأنه يرصد هذه الأنشطة في ثوان معدودة، وهو ما يمنع الضرر قبل حدوثه، بعكس الأساليب التقليدية التي غالبًا ما ترصد الجريمة بعد تحققها.[٥]

كما تبرز أهمية الذكاء الصناعي كذلك في تحليل الاتصالات الرقمية بين الأشخاص الذين يُحتمل تورطهم في الجرائم المنظمة. وقد أثبتت الخوارزميات الذكية فعاليتها في رصد الأنماط الاتصالية المشبوهة، واستنتاج العلاقة بين أفراد الشبكات الإجرامية—حتى وإن لم تكن العلاقة مباشرة—من خلال تحليل البيانات المهيكلة وغير المهيكلة، بما فيها الرسائل، والمكالمات، ووسائط التواصل الاجتماعي.

أما في المجال المالي، فيُعد الذكاء الصناعي اليوم أداة لا يمكن الاستغناء عنها في التحليل الوقائي للمعاملات المصرفية. إذ تستطيع الأنظمة الذكية تتبع التحويلات المالية التي يشوبها الشك، والتمييز بين المعاملات المشروعة وتلك التي تنتمي إلى غسل الأموال أو تمويل الإرهاب. وتُعد المصارف والمؤسسات المالية الأكثر استعمالًا لهذه التقنيات لأنها تتعامل مع ملايين المعاملات يوميًا، ويستحيل على الإنسان مراقبتها جميعًا دون دعم تقني، وعلى الرغم من الفوائد الواسعة التي يقدمها الذكاء الصناعي في التحليل الجنائي الاستباقي، إلا أن استخدامه يثير تحديات قانونية وأخلاقية تتعلق بحدود جمع البيانات، وحماية الخصوصية، ومدى شفافية الخوارزميات، وإمكانية وقوع التحيّز في التحليل. فالذكاء الصناعي يعتمد على البيانات، وإذا كانت هذه البيانات ناقصة أو متحيّزة، فإن المخرجات ستكون بدورها متحيّزة. وهذا قد يؤدي إلى قرارات أمنية غير عادلة أو إلى استهداف فئات اجتماعية معينة بصورة خاطئة. ومن هنا تظهر الحاجة إلى أطر قانونية دقيقة توازن بين الاستفادة من الذكاء الصناعي في منع الجريمة وبين احترام الحقوق الأساسية للمواطنين.[٦]

إذن اعتماد الأجهزة الأمنية المفرط على الذكاء الصناعي دون رقابة قد يؤدي إلى نتائج غير مقبولة، مثل اتخاذ قرارات تقوم على تقديرات خوارزمية بلا تحقق بشري، وهو ما يهدد مبدأ الشرعية الإجرائية. ولذلك يتجه الفكر الجنائي المعاصر إلى تأكيد أن الذكاء الصناعي لا يجب أن يحل محل العنصر البشري، بل ينبغي أن يكون أداة دعم، وأن تبقى سلطة التقدير

النهائي بيد القاضي أو المحقق أو ضابط الأمن. فأن الذكاء الصناعي أصبح يمثل ركيزة أساسية في الوقاية من الجريمة، لأنه لا يكتفي بتحليل ما وقع من أفعال، بل يسعى إلى استكشاف المستقبل المحتمل للجريمة، وتوجيه أجهزة الدولة إلى مناطق الخطر، ورصد المؤشرات التي تسبق الجريمة بوقت كافٍ لردعها. وهذا التحول يحمل دلالة عميقة على تطور السياسة الجنائية، إذ لم تعد تعتمد على رد الفعل، بل تبنت مبدأ الاستباق، بناءً على التحليل الذكي والمعطيات الرقمية.

ثانيًا: دور الذكاء الصناعي في رصد الجرائم الإلكترونية

أصبحت الجرائم الإلكترونية اليوم أحد أعقد التحديات التي تواجه الدولة الحديثة، نظرًا لطبيعتها اللامركزية، وسرعة ارتكابها، واتساع نطاق ضررها، وقدرة مرتكبيها على التخفي خلف شبكات معقدة من الأدوات التقنية. وتُعدّ هذه الجرائم بطبيعتها عابرة للحدود، وتستهدف الأفراد والمؤسسات والقطاعات المالية والمعلوماتية، مما يجعل مواجهتها بالوسائل التقليدية أمرًا غير ممكن. وفي هذا السياق برز الذكاء الصناعي كآلية رئيسية لرصد الأنشطة غير المشروعة في الفضاء الرقمي، لأنه يمتلك قدرات تحليل وسرعة معالجة تتجاوز بكثير إمكانات العنصر البشري، ويستطيع مراقبة شبكات المعلومات بصورة مستمرة ودقيقة، ويعتمد الذكاء الصناعي في رصد الجرائم الرقمية على مجموعة من الخوارزميات التي تمكّنه من تحليل البيانات الضخمة المرتبطة بحركة الشبكات، واتصالات المستخدمين، وتدفقات المعلومات، والسلوك الرقمي للأجهزة والبرمجيات. وتستند هذه الخوارزميات إلى نماذج التعلم الآلي والتعلم العميق، التي تتغذى على بيانات ضخمة من عمليات سابقة، تُستخدم لاحقًا لبناء تصورات دقيقة عن السلوك الطبيعي للشبكة والتمييز بينه وبين السلوك الشاذ الذي قد يمثل تهديدًا أو هجومًا إلكترونيًا وشيكًا.[٧]

تتمثل إحدى أهم وظائف الذكاء الصناعي في هذا المجال في الكشف المبكر عن الهجمات السيبرانية، إذ يستطيع النظام التعرف على عمليات غير معتادة في الشبكة، مثل محاولات الدخول المتكررة إلى خادم معين، أو انتقال بيانات كبيرة الحجم إلى جهة مجهولة، أو استخدام بروتوكولات اتصال مشفرة بصورة غير مبررة، أو تشغيل برمجيات غير مألوفة في سير عمل المؤسسة. وتساعد هذه المؤشرات على اكتشاف الهجمات قبل وقوع الضرر، سواء كانت هجمات اختراق، أو تسلل خبيث، أو نشر برمجيات فدية، أو محاولات تعطيل أنظمة المعلومات، ويُعدّ الذكاء الصناعي كذلك عنصرًا أساسيًا في مكافحة جرائم سرقة البيانات، التي تُعدّ من أخطر الجرائم الرقمية وأكثرها انتشارًا. فأنظمة التحليل الذكي قادرة على مراقبة حركة البيانات داخل المؤسسة، وتحديد مواقع الوصول الحساسة، ومطابقة العمليات الجارية مع "البصمة الرقمية" الطبيعية للمستخدمين. فإذا أظهرت البيانات سلوكًا غير متوقع — مثل الوصول في وقت غير معتاد، أو طلب ملفات ليست ضمن اختصاص الموظف، أو تحويل نسخ ضخمة من الملفات — يتدخل النظام فوريًا ويصدر إنذارًا أو يوقف العملية تلقائيًا.[٨]

كما يمتد دور الذكاء الصناعي إلى رصد الجرائم المالية الرقمية، وهي الجرائم التي تستهدف أنظمة المدفوعات، وبطاقات الائتمان، والتحويلات الإلكترونية. وتساعد الخوارزميات على

قراءة الأنماط المالية غير الطبيعية، مثل التحويلات المتكررة صغيرة القيمة التي تهدف إلى إخفاء نشاط كبير، أو استخدام البطاقات في مواقع جغرافية متعددة خلال وقت قصير، أو تغير سلوك العميل المالي بصورة مفاجئة. وتتيح هذه القدرة للقطاع المصرفي الاستجابة السريعة للاحتيال، وإيقاف العمليات المشبوهة قبل اكتمالها، وتبرز أهمية الذكاء الصناعي كذلك في مواجهة الهجمات المعقدة متعددة الطبقات ( Advanced Persistent Threats – APTs)، وهي هجمات طويلة الأمد تنفذها جهات محترفة بقصد السيطرة التدريجية على أنظمة المؤسسات. ويتميز الذكاء الصناعي بقدرته على كشف هذه الأنشطة الخفية عبر تحليل السلوك المتراكم بمرور الوقت، إذ يراقب النظام التحركات الصغيرة التي قد لا تُرى مباشرة، لكنه عند جمعها يصبح قادرًا على تحديد نمط الهجوم بدقة.[٩]

ويسهم الذكاء الصناعي أيضًا في تحليل البرمجيات الخبيثة عبر التعرف على "البصمة السلوكية" للبرامج، وليس فقط خواصها البرمجية التقليدية. فالهجمات الحديثة غالبًا ما تُغيّر مظهرها الخارجي، إلا أنها تظل تحمل سلوكًا داخليًا ثابتًا، مثل إنشاء اتصالات خارجية غير مصرّح بها، أو إعادة كتابة الملفات، أو محاولة تعطيل أنظمة الحماية. ومن خلال هذا التحليل، يستطيع الذكاء الصناعي رصد البرامج الضارة حتى قبل التعرف عليها من قواعد البيانات التقليدية، ولا يتوقف دور الذكاء الصناعي عند الكشف التقني، بل يتعداه إلى رصد الأنشطة الإجرامية في الفضاء الاجتماعي الرقمي، مثل الجرائم المتعلقة بالابتزاز الإلكتروني، والتحريض، والتجنيد عبر الإنترنت، والاحتيال عبر مواقع التواصل. وتعمل الخوارزميات هنا على تحليل المحتوى، والتعرف على الكلمات المفتاحية، وبناء شبكات ارتباطية بين المستخدمين، وتحديد الحسابات التي تبدي سلوكًا عدوانيًا أو احتياليًا. وقد أثبتت هذه التقنيات قدرتها على كشف العديد من عمليات الابتزاز والتحرش والاتجار عبر الإنترنت قبل تطورها.[١٠]

كما تتجلى القوة الوقائية للذكاء الصناعي في العديد من الدول التي تبنّت أنظمة المراقبة الذكية لحركة البيانات، والتي تعمل على مدار الساعة، وترسل تقارير فورية إلى وحدات الاستجابة السريعة. وقد ساعد هذا النوع من الأنظمة على تقليل معدل الهجمات الرقمية، وزيادة سرعة الاستجابة، والحد من الخسائر المالية والمعلوماتية، غير أن دور الذكاء الصناعي في رصد الجرائم الإلكترونية يثير تحديات قانونية لا يمكن تجاهلها، أهمها:

أولًا: حماية الخصوصية

فالقدرة على مراقبة البيانات وتحليلها قد تمس الحياة الخاصة للأفراد، وهو ما يوجب وضع حدود تشريعية تحدد متى وكيف ولِمَ يجوز استخدام التحليل الذكي.

ثانيًا: الشرعية والرقابة

الأنظمة الذكية قد تتخذ قرارات آلية تؤدي إلى تدخل غير مبرر في حرية الأفراد أو في نشاط المؤسسات، مما يستلزم رقابة قضائية وإدارية واضحة تضمن احترام مبدأ الشرعية.

ثالثًا: التحيّز

إذا كانت البيانات المستخدمة في تدريب النظام غير متوازنة، فإن الخوارزميات قد تتضمن تحيزًا يؤدي إلى استهداف مجموعات معينة بصورة غير عادلة، وهو أمر يتعارض مع مبادئ العدالة الجنائية.

رابعًا: الإسناد القانوني للمسؤولية

عندما ترتكب الأنظمة خطأً تقنيًا يؤدي إلى إغفال جريمة أو تعطيل خدمة أو المساس بحقوق أحد الأفراد، تصبح مسألة تحديد المسؤولية القانونية إشكالية تحتاج إلى إطار تشريعي واضح.[١١]

مع ذلك، فإن هذه التحديات لا تُنقص من القيمة الجوهرية للذكاء الصناعي، بل تدعو إلى تنظيمه وتقييده بقواعد تضمن الفعالية دون المساس بالحقوق الدستورية. ومن خلال هذا التنظيم يصبح الذكاء الصناعي أداة متقدمة في حماية الأمن الرقمي ورصد الجرائم الإلكترونية قبل وقوعها، مما يعزز الأمن الوطني ويحمي المؤسسات من الهجمات المتزايدة.

ثالثًا: الذكاء الصناعي كوسيلة لحماية الفضاء العام ومنع الجريمة في المدن الذكية

أدى التحول الحضري المتسارع، وازدياد الكثافة السكانية، واتساع النشاط الاقتصادي والخدمي داخل المدن، إلى بروز تحديات جدية تتعلق بسلامة الفضاء العام وإدارة المخاطر الأمنية. ومع ظهور المدن الذكية التي تعتمد على بنية رقمية متطورة، أصبحت الحاجة ملحة إلى أدوات قادرة على مراقبة هذه الفضاءات ورصد السلوكيات الخطرة والتدخل قبل وقوع الجريمة. وفي هذا السياق، اكتسب الذكاء الصناعي موقعًا مركزيًا بوصفه آلية فعّالة في تحليل المشهد الحضري، واستشراف التهديدات، وتوفير مستوى أعلى من الأمن الوقائي، ويستند دور الذكاء الصناعي في المدن الذكية إلى دمج مجموعة واسعة من التقنيات، أهمها: كاميرات المراقبة عالية الدقة، وأجهزة الاستشعار، والاتصالات اللاسلكية، والخرائط الذكية، وأنظمة تحليل الصور والفيديو، وبرمجيات التعرف على الأنماط السلوكية. وتعمل هذه التقنيات بطريقة متكاملة، بحيث تشكل شبكة تراقب الفضاء العام بصورة مستمرة، وتوفر للسلطات الأمنية معلومات فورية حول أي نشاط يبدو شاذًا أو محفوفًا بالمخاطر. وما يميز الذكاء الصناعي هنا هو عدم اعتماده على الرصد البصري البشري فقط، بل على تحليل آلي دقيق يمكنه التعامل مع ملايين اللقطات في اللحظة نفسها.[١٢]

وتُعد أنظمة المراقبة البصرية الذكية من أبرز تطبيقات الذكاء الصناعي في مجال السلامة العامة. إذ تعمل خوارزميات تحليل الفيديو على تحديد الأفعال أو الحركات التي تُعد غير طبيعية مقارنة بالسلوك المعتاد في المكان، مثل عدوانية مفاجئة، أو تجمعات غير مبررة، أو دخول شخص إلى منطقة محظورة، أو ترك حقيبة في مكان مزدحم. وفي حال اكتشاف أي من هذه المؤشرات، يرسل النظام إشعارًا مباشرًا إلى غرفة العمليات لاتخاذ الإجراء المناسب. وتتميز هذه الأنظمة بقدرتها على التعلم المستمر من البيانات، مما يسمح لها بتحسين دقتها

بمرور الوقت، هنا يبرز الدور الوقائي الذكّي في التعرف على الوجوه ولوحات المركبات، إذ تتيح هذه التقنية إمكانية تتبع الأشخاص المطلوبين، أو المركبات المشبوهة، أو الأنشطة المرتبطة بشبكات إجرامية. ويُستخدم هذا النوع من الأنظمة في المطارات، والمنافذ الحدودية، والمناطق التجارية الحيوية، ومحطات النقل العام، حيث يمكن للذكاء الصناعي مطابقة الوجوه مع قواعد البيانات الجنائية خلال ثوانٍ معدودة، دون الإخلال بانسيابية الحركة. كما تساعد هذه الأنظمة في تحديد مسار الشخص أو المركبة، الأمر الذي يعزز قدرة السلطات على منع الجريمة أو ضبط مرتكبيها بسرعة.[١٣]

كما تشهد المدن الذكية توسعًا كبيرًا في أنظمة التحليل السلوكي الذكية، وهي أنظمة تعتمد على تتبع أنماط حركة الأفراد والتجمعات داخل الفضاء العام. ومن خلال هذه التقنية يمكن للنظام رصد مؤشرات على احتمال وقوع جريمة، مثل النزاع الجماعي، أو محاولات السرقة، أو الاقتراب غير الطبيعي من مداخل المباني أو المنشآت الحساسة. وتتمتع هذه الأنظمة بقدرتها على تحديد "المستويات الحرجة" في الأماكن العامة، أي النقاط التي تتكرر فيها السلوكيات الشاذة أو الأنشطة المشبوهة، مما يساعد السلطات على تعزيز الوجود الأمني في تلك المناطق.

ويبرز دور الذكاء الصناعي كذلك في إدارة الحشود ومنع الكوارث، إذ تعتمد المدن الذكية على أنظمة قادرة على تتبع حجم الكتل البشرية، ونمط تحركها، وسرعة انتقالها، مع تقديم توقعات فورية حول احتمالية حدوث تدافع أو ازدحام خطير. وتستخدم هذه التقنيات في الملاعب، والمراكز التجارية، والاحتفالات الكبرى، والمواسم الدينية. وقد أثبتت التجارب أن دمج الذكاء الصناعي في مراقبة الحشود يقلل من احتمالات وقوع إصابات أو وفيات ناتجة عن الازدحام، ويتيح للجهات الأمنية التدخل المبكر وتنظيم المسارات، ومن التطبيقات المتقدمة كذلك استخدام الذكاء الصناعي في إدارة المرور ومنع الجرائم المرتبطة بالمركبات. فمن خلال تحليل بيانات الطرق، يمكن للنظام تحديد الأنماط التي ترتبط بتجمعات المركبات المشبوهة، أو مراقبة المركبات المسروقة، أو كشف السلوكيات غير الطبيعية مثل القيادة العشوائية أو السير في اتجاهات غير مبررة. وتساعد هذه القدرة في منع الجرائم المتعلقة بالمطاردة، والنقل غير القانوني، والتهريب، والفرار من مسرح الحادث.[١٤]

كما يمتد أثر الذكاء الصناعي إلى تحليل البنية الحضرية ورصد المخاطر المكانية التي قد تشكل بيئة مناسبة للجريمة. إذ تستطيع أنظمة التخطيط الذكي تحديد الأماكن المعتمة أو المهجورة التي تزداد فيها احتمالات الاعتداء، كما يمكنها قياس تأثير غياب الإنارة أو كاميرات المراقبة على ارتفاع معدلات الجريمة.[١٥] ويساعد هذا التحليل السلطات البلدية في اتخاذ قرارات تخطيطية تحدّ من الفراغات الخطرة، وتحسن جودة الحيز العام، ولا يقتصر دور الذكاء الصناعي على الجانب الأمني، بل يشمل جانبًا اجتماعيًا مهمًا يتمثل في تحليل الظروف الاجتماعية–الاقتصادية التي تؤثر في توزيع الجريمة داخل المدينة. ومن خلال مقارنة البيانات السكانية بمعدلات الجريمة والازدحام ونشاط الأسواق، يمكن للسلطات وضع خطط شاملة لمعالجة الأسباب الجذرية للجريمة، بدل الاكتفاء بالاستجابة الأمنية.

ومع هذه الفوائد الواسعة، يبرز سؤال جوهري يتعلق بالحقوق والحريات. فأنظمة المراقبة الذكية في المدن تثير إشكالات تتعلق بـ:

- الحق في الخصوصية
- حدود استخدام الصور والبيانات
- إمكانية التعسف في مراقبة المواطنين
- التحيز الإلكتروني في عمليات التعرف على الوجوه
- عدم وضوح المسؤولية القانونية عن الأخطاء التقنية[١٦]

لهذا يُخشى أن يؤدي الاستخدام غير المنضبط للذكاء الصناعي في الفضاء العام إلى تحويل المدن إلى "مجتمعات مراقبة" تمس جوهر الحياة الخاصة. ولهذا تتجه التشريعات الحديثة إلى وضع قواعد تضمن أن تكون المراقبة الذكية محدودة بالضرورة الأمنية، وأن تخضع لرقابة قضائية وإدارية تضمن عدم إساءة استخدامها، فتبرز الحاجة كذلك إلى ضمان أن تكون الخوارزميات المستخدمة شفافة وخالية من التحيز، وأن تُخضع لعمليات تدقيق دوري تكشف مصادر الخطأ أو الاختلال. وينبغي أن تكون أي بيانات تُجمع عبر أنظمة المدن الذكية محمية بقواعد صارمة لمنع تسريبها أو استخدامها خارج الإطار القانوني. مع ذلك، فإن هذه التحديات لا تنقص من أهمية الذكاء الصناعي في تعزيز سلامة المدن، بل تدفع نحو تبني نموذج متوازن يجمع بين الفعالية الأمنية والضمانات القانونية. فالتكنولوجيا عندما تُدار ضمن إطار قانوني رشيد، تصبح أداة لدعم الحقوق لا لتهديدها. ومن خلال هذا التوازن، تتشكل مدن آمنة، قادرة على مواجهة المخاطر، وتقديم خدمات حضارية متقدمة، وتحقيق الأمن دون المساس بحقوق الأفراد وحرياتهم.

رابعًا: دور الذكاء الصناعي في مكافحة الجرائم المالية

القطاع المالي الحديث من أكثر القطاعات عرضة للجرائم في ظل التطور الرقمي، واتساع حجم المعاملات، وتنوع الأدوات المصرفية، وتداخل الأنظمة الإلكترونية عبر الحدود. ومع تنامي جرائم غسل الأموال، وتمويل الإرهاب، والاحتيال المصرفي، والتلاعب بالأسواق، بات من الضروري أن تعتمد المؤسسات المالية على تقنيات قادرة على قراءة السلوك المالي قراءة دقيقة، وتحديد الأنماط المريبة، وتحليل العمليات في وقتها الفعلي. وهنا يتجلى دور الذكاء الصناعي بوصفه أداة مركزية في تعزيز الرقابة المالية، وإغلاق الثغرات التي يستغلها الجناة، وإتاحة مستوى أعلى من الوقاية الاستباقية.[١٧]

تتميز الجرائم المالية بطابعها الخفي، وصعوبة اكتشافها عبر الوسائل التقليدية المعتمدة على التدقيق اليدوي أو التحليل البشري البطيء. وقد أدت السرعة الهائلة للمعاملات الإلكترونية إلى جعل التدقيق التقليدي عاجزًا عن متابعة ملايين العمليات اليومية. وهذا ما دفع المؤسسات المصرفية والجهات الرقابية إلى تبني الذكاء الصناعي بوصفه وسيلة للكشف اللحظي عن الأنشطة المالية المشبوهة، عبر تحليل البيانات المتدفقة باستخدام خوارزميات التعلم الآلي التي تتعرف على "البصمة المالية" لكل مستخدم، وتحدد ما إذا كانت العملية تقع ضمن

السلوك الطبيعي أو تشكل انحرافًا يستوجب التحقيق، وتكمن القوة الأساسية للذكاء الصناعي في هذا المجال في قدرته على التعلم من البيانات. فكل عميل لديه نمط مالي معيّن من حيث أوقات السحب والإيداع، وحجم العمليات، ونوعية المستفيدين، وطبيعة النشاط التجاري. وعندما تُدرب الأنظمة الذكية على تاريخ تعاملات العميل، تصبح قادرة على مقارنة العملية الجديدة بالنمط المعتاد. فإذا ظهرت عملية غير مبررة—مثل تحويل كبير إلى حساب خارجي، أو عمليات متكررة صغيرة القيمة تهدف إلى تمويه حركة الأموال، أو استخدام بطاقة في موقعين جغرافيين متباعدين خلال وقت قصير—يتدخل النظام تلقائيًا ويرسل إشعارًا إلى وحدة الامتثال، أو يوقف العملية حتى يتم التحقق منها.[١٨]

تبرز هذه القدرة في مكافحة غسل الأموال، وهو أخطر الجرائم الاقتصادية وأكثرها تعقيدًا. فالجناة عادةً ما يلجأون إلى تفتيت الأموال، أو توزيعها على حسابات متعددة، أو إدخالها في سلسلة طويلة من التحويلات بقصد إخفاء مصدرها. وتستطيع خوارزميات الذكاء الصناعي رصد هذه الأنماط العبثية، ومطابقتها مع قواعد البيانات الجنائية الدولية، وتحديد "التحركات الخطرة" التي تُعد من مؤشرات غسل الأموال. وقد أصبحت كثير من المصارف تعتمد على هذه الأنظمة للامتثال للمعايير الدولية الخاصة بـ مكافحة غسل الأموال وتمويل الإرهاب (AML/CFT). بالإضافة إلى ذلك، يُعد الذكاء الصناعي وسيلة فعالة لمواجهة الاحتيال المصرفي، سواء في بطاقات الائتمان، أو الخدمات الإلكترونية، أو المحافظ الرقمية. فعند استخدام بطاقة معينة، يسجل الذكاء الصناعي الوقت والمكان ونوع العملية والقيمة، ويقارنها مع السلوك الطبيعي لصاحب البطاقة. فإذا حدث استخدام للبطاقة في مكان بعيد غير مألوف، أو ظهرت محاولات متعددة لعمليات غير مكتملة، أو تم إدخال البطاقة في جهاز غير موثوق، يرسل النظام تحذيرًا فوريًا أو يوقف البطاقة تلقائيًا. وقد أدت هذه الأنظمة إلى تقليل الخسائر المالية التي يتحملها القطاع المصرفي، ورفع مستوى الأمان للمستخدمين.[١٩]

كما يتجاوز الدور الوقائي للذكاء الصناعي كشف العمليات المشبوهة إلى المشاركة في تحليل الأسواق المالية لمنع التلاعب بالأسعار أو التداول بناءً على معلومات داخلية ( Insider Trading). وتستطيع الخوارزميات تحليل حركة الأسهم والمؤشرات خلال أجزاء من الثانية، والتعرف على العمليات غير الطبيعية التي تشير إلى محاولة التأثير على السوق من خلال ضغوط صناعية أو تداولات جماعية مشبوهة. وتسمح هذه القدرة للجهات الرقابية—كالهيئات المالية والبورصات—بمتابعة الأسواق بصورة دقيقة واتخاذ الإجراءات السريعة ضد أي نشاط يخالف قواعد المنافسة العادلة، ويبرز كذلك دور الذكاء الصناعي في مكافحة الاحتيال عبر الشركات (Corporate Fraud)، بما في ذلك التلاعب بالحسابات، أو إخفاء الديون، أو استخدام الفواتير الوهمية، أو تضخيم الأصول. وتعمل الأنظمة الذكية هنا على تحليل السجلات المالية، ومقارنة البيانات التاريخية، واكتشاف التناقضات التي يصعب رصدها يدويًا، مثل اختلاف حركة المخزون عن حركة المبيعات، أو تضخم الأرباح بصورة غير منطقية، أو ظهور معاملات غير واضحة بين الأقسام الداخلية للمؤسسة. وقد بدأت بعض الدول في اعتماد الذكاء الصناعي كجزء من عمليات التدقيق المالي الرسمية، لزيادة الشفافية ومنع التلاعب المحاسبي.[٢٠]

ويمتد دور الذكاء الصناعي كذلك إلى رصد الجرائم المالية الرقمية المرتبطة بالعملات المشفرة (Cryptocurrencies)، التي أصبحت بيئة خصبة لعمليات غسل الأموال وتمويل الأنشطة غير القانونية. ويُعد تحليل "سلاسل البلوك تشين" من أبرز تطبيقات الذكاء الصناعي، لأنه قادر على تتبع عمليات التحويل المشفرة، وربط المحافظ الإلكترونية ببعضها، وتحديد الشبكات التي تقوم بتحويلات مريبة أو تتعامل مع منصات غير منظمة لذلك من الجوانب المهمة في هذا الإطار استخدام الذكاء الصناعي في التحليل النصي ( Text Mining) لعقود الصفقات المالية، حيث يستطيع النظام قراءة آلاف المستندات خلال ثوانٍ، والكشف عن البنود التي تُعد من مؤشرات الاحتيال، مثل فروقات الأسعار غير المبررة، أو الشروط التي تخالف قواعد الامتثال، أو الصياغات التي تشير إلى نية التهرب الضريبي. وهذا النوع من التحليل أصبح جزءًا أساسيًا من أدوات المحققين الماليين والمدققين الخارجيين.[٢١]

رغم الدور الحيوي لهذه التقنيات، إلا أن استخدامها يثير تحديات قانونية مهمة. فالإفراط في جمع البيانات قد يؤدي إلى المساس بخصوصية العملاء، خاصة إذا لم تكن هناك قواعد صارمة لحماية البيانات. كما أن الخوارزميات قد ترتكب أخطاء حسابية تؤدي إلى تصنيف معاملة مشروعة بوصفها مشبوهة، وهو ما يسبب ضررًا للعميل ويطرح سؤالًا حول المسؤولية القانونية، ويصبح الأمر أكثر تعقيدًا عندما تعتمد المؤسسات المالية على خوارزميات "الصندوق الأسود" التي لا يمكن معرفة طريقة اتخاذها للقرار، مما يستلزم وجود إطار تشريعي يضمن الشفافية الخوارزمية وإمكانية الطعن في نتائج الأنظمة الذكية.

يُضاف إلى ذلك أن فعالية الذكاء الصناعي تعتمد على جودة البيانات. فإذا كانت البيانات المدخلة متحيزة أو ناقصة، ستنتج خوارزميات مشوهة غير دقيقة. ولهذا تؤكد الجهات الرقابية العالمية ضرورة تدقيق البيانات، والتحقق من خلوها من الأخطاء، وإخضاع الأنظمة الذكية للاختبار الدوري للتأكد من سلامة مخرجاتها. فإن الذكاء الصناعي أصبح أحد أهم الأدوات في مكافحة الجرائم المالية، لأنه يرفع مستوى الحماية، ويقلل المخاطر، ويمنح المؤسسات القدرة على مواجهة الهجمات المالية المتزايدة التعقيد. ومع ذلك، فإن توظيفه يحتاج إلى إطار قانوني متكامل يكفل الشفافية، ويحمي حقوق العملاء، ويضمن أن تكون القرارات المالية المستندة إلى الذكاء الصناعي منسجمة مع مبادئ العدالة والشرعية.

خامسًا: استخدام الذكاء الصناعي في التحقيقات الجنائية

أدى التقدم الهائل في قدرات الذكاء الصناعي وتقنيات التحليل الرقمي إلى إعادة تشكيل منهجية التحقيق الجنائي بصورة غير مسبوقة. فلم تعد الأدلة الجنائية مقتصرة على البصمات أو الشهود أو الأدوات التقليدية، بل أصبحت اليوم تشمل كمًّا هائلًا من البيانات الرقمية والسلوكية والبصرية التي تحتاج إلى تحليل دقيق يتجاوز القدرات البشرية. ومع تنامي هذه المعطيات، أصبح الذكاء الصناعي أداة جوهرية في دعم التحقيقات الجنائية، لأنه قادر على معالجة البيانات بسرعة فائقة، وتحديد العلاقات الخفية بين الوقائع، واستخلاص القرائن التي

يصعب الوصول إليها بالطرق التقليدية. وهذا الدور لم يعد مجرد تقنية مساعدة، بل تحول إلى عنصر مركزي في استراتيجية الدولة لمكافحة الجريمة.[٢٢]

تتمثل إحدى أهم وظائف الذكاء الصناعي في تحليل الأدلة الرقمية. فالجرائم المعاصرة تُخلّف وراءها آثارًا كمية ونوعية ضخمة تشمل الاتصالات الهاتفية، والبريد الإلكتروني، والسجلات المتبادلة على تطبيقات التواصل، ومعلومات المواقع، وسجلات الدخول إلى الأنظمة، والمحتوى المنشور على الشبكات الاجتماعية. وتعد هذه البيانات ذات قيمة تحقيقية عالية لأنها تحمل أنماطًا دقيقة من السلوك الرقمي الذي يمكن أن يثبت علاقة المشتبه به بالجريمة أو ينفيها. ويستطيع الذكاء الصناعي تحليل هذه البيانات بطريقة منهجية، وفصل المعلومات الرئيسية عن الضوضاء المعرفية، ثم تقديم تصور متكامل لمسار الحركة، أو تسلسل الأحداث، أو شبكة العلاقات بين الأفراد، ويبرز دور الذكاء الصناعي كذلك في تحليل الصور والفيديو التي أصبحت جزءًا من المشهد الجنائي الحديث، مع الانتشار الواسع لكاميرات المراقبة والهواتف الذكية. وتسمح الخوارزميات المتقدمة باستخراج تفاصيل دقيقة من المقاطع المصورة، مثل التعرف على الوجوه، وقراءة لوحات المركبات، وتحليل الحركة، وتحديد الزمن والموقع بدقة. كما يمكن للأنظمة الذكية تحسين جودة الفيديوهات المتضررة أو المعتمة، مما يتيح استخدام مواد كانت في السابق غير صالحة كدليل. وقد أدت هذه التقنيات إلى كشف آلاف الجرائم في دول متعددة، لأنها جعلت من إمكانية تزوير الأدلة المصورة أمرًا أكثر صعوبة.[٢٣]

ويشمل الدور التحليلي للذكاء الصناعي أيضًا التعرف على الأصوات وتحليلها، إذ يمكن للنظام مقارنة طبقة الصوت ونمط الكلام مع قاعدة بيانات واسعة، لتحديد هوية المتحدث أو مطابقة التسجيلات الصوتية مع المتهمين. وتُستخدم هذه الأدوات في الجرائم التي تتضمن اتصالات هاتفية أو رسائل صوتية، خاصة في قضايا الابتزاز والتهديد والإرهاب. كما يمكن للذكاء الصناعي تحليل اللهجات وتحديد المنطقة الجغرافية للمتحدث، مما يسهم في تضييق نطاق البحث الجنائي. أما في ميدان الأدلة المادية، فيسهم الذكاء الصناعي في تحليل البصمات الوراثية (DNA) من خلال الخوارزميات التي تُسرع مطابقة البصمات الجينية بين قاعدة البيانات والعينات المرفوعة. وتعمل هذه التقنية على تقليل الوقت اللازم للبحث، وتحديد العلاقات البيولوجية، ومعرفة احتمالات التطابق بدقة رياضية. ويدخل ضمن هذا المجال ما يسمى "التحليل الجيني التنبؤي" الذي يمكنه التعرف على بعض السمات البيولوجية بناءً على العينة الجينية، وهو مجال يتطلب تنظيمًا قانونيًا دقيقًا بسبب حساسيته.[٢٤]

ويمتد دور الذكاء الصناعي إلى تتبع الأموال الرقمية في الجرائم الاقتصادية المعقدة، حيث يمكن للنظام تحليل حركة الأموال، وربط المعاملات المتفرقة، وإعادة بناء الشبكات المالية التي يستخدمها الجناة لإخفاء أموالهم. ويُعد هذا الدور بالغ الأهمية في قضايا غسل الأموال وتمويل الإرهاب، لأن الذكاء الصناعي يستطيع كشف أنماط لا تُرى مباشرةً في التقارير المالية التقليدية، ومن التطبيقات المتقدمة في التحقيق الجنائي استخدام الذكاء الصناعي في إعادة بناء مسرح الجريمة عبر نماذج ثلاثية الأبعاد تساعد المحققين على فهم موقع الجريمة، واتجاه حركة الجاني، واحتمالية استخدام أدوات معينة، ومدى تطابق أقوال الشهود مع

المعطيات الفيزيائية. وتتيح هذه النماذج المحاكاة الدقيقة للحوادث، سواء كانت حوادث قتل أو سرقة أو اعتداء، مما يرفع مستوى الدقة في تقدير الوقائع.[٢٥]

لذلك تبرز فائدة الذكاء الصناعي كذلك في التحليل النصي والاستدلال اللغوي. فالخوارزميات الحديثة قادرة على تحليل الرسائل المكتوبة، واكتشاف نبرة التهديد، أو الأسلوب الاحتيالي، أو البرمجيات الخبيثة المضمنة في النصوص، أو العلاقات بين الرسائل التي تبدو غير مرتبطة. ويستفيد المحققون من هذه القدرة في تتبع العصابات الإلكترونية أو الجماعات المتطرفة التي تعتمد على الاتصالات السرية، ومع اتساع نطاق هذا الدور، برز الذكاء الصناعي كأداة مهمة في تصنيف المشتبه بهم وتقدير الخطورة الإجرامية. إذ تستطيع الخوارزميات ربط السوابق، والبيانات السلوكية، والمعلومات الاجتماعية لتقدير مدى خطورة الشخص أو احتمال ارتكابه للجريمة مرة أخرى. غير أن هذا التقدير، على الرغم من فائدته، يحتاج إلى ضوابط قانونية صارمة، لأن القراءة الخوارزمية قد تتأثر بالبيانات المعيبة أو التحيزات الحسابية.[٢٦]

ومع كل هذه الإمكانات، تبرز تحديات قانونية تحتاج إلى معالجة. فالاستخدام غير المنضبط للذكاء الصناعي في التحقيق قد يؤدي إلى انتهاك الخصوصية إذا تُرك بدون حدود واضحة للبيانات التي يمكن جمعها أو تحليلها. كما قد يؤدي إلى المساس بمبدأ البراءة إذا اعتمدت الجهات الأمنية بشكل كامل على نتائج الخوارزميات دون تحقق بشري. وهناك أيضًا تحدي "الصندوق الأسود"، حيث يصعب أحيانًا معرفة الأساس الذي بُني عليه القرار الخوارزمي، مما قد يعرّض حجية الأدلة للطعن أمام القضاء.

ترتبط هذه التحديات بسؤال جوهري يتعلق بـ المسؤولية القانونية عن الأخطاء الخوارزمية. فإذا قامت الأنظمة بتحليل خاطئ أدّى إلى اتهام بريء أو تجاهل متهم حقيقي، فمن يتحمل المسؤولية؟ المبرمج؟ الشركة المصممة؟ الجهة الأمنية؟ أم الخوارزمية ذاتها؟ وهذه الأسئلة تحتاج إلى إطار قانوني حديث يحدد نطاق المسؤولية ويضع الضمانات اللازمة لحماية حقوق المتهمين.[٢٧] وبالرغم من هذه الإشكالات، فإن التطبيقات العملية أثبتت أن الذكاء الصناعي أصبح جزءًا لا يتجزأ من منظومة التحقيق الجنائي الحديثة، لأنه يرفع مستوى الدقة، ويقلل الوقت، ويكشف الجرائم المعقدة التي كانت في الماضي تحتاج إلى شهور من التحليل. ومن خلال قواعد قانونية واضحة، ورقابة قضائية فعالة، يمكن للذكاء الصناعي أن يتحول إلى ركيزة أساسية في البحث الجنائي، دون أن يمس الحقوق والحريات.

**الخاتمة:**

تثبت التحولات التقنية التي شهدها العالم خلال العقدين الأخيرين أن الذكاء الصناعي لم يعد مجرد خيار تقني مساعد، بل أصبح ضرورة أمنية وقانونية ترتبط ارتباطًا مباشرًا بقدرة الدولة على حماية النظام الاجتماعي والاقتصادي والرقمي. وقد بيّن التحليل أن الذكاء الصناعي يقدم للسياسة الجنائية ما لم تستطع الأدوات التقليدية تحقيقه، من حيث قدرته على التنبؤ بالجريمة وتحليل أنماطها، ورصد السلوكيات غير الطبيعية، وإدارة الفضاء العام،

وتأمين شبكات المعلومات، وتعقب الجرائم المالية، ودعم التحقيقات الجنائية عبر أدوات دقيقة لم تكن متاحة في الماضي. واتضح أن البنية التحليلية للذكاء الصناعي تمنح الأجهزة الأمنية والجهات القضائية قدرة استباقية حقيقية، تُحول الوقاية إلى ممارسة عملية قابلة للقياس، لا مجرد هدف تشريعي. فخوارزميات التعلم العميق وتطبيقات تحليل الفيديو والمعاملات المالية والبصمات الرقمية أصبحت قادرة على استنتاج الروابط الخفية بين الوقائع، وإعادة بناء سلوك الجناة، وتحديد المناطق أو الأوقات الأكثر عرضة للجريمة، مما يعزز فعالية التدخل الأمني ويقلل الفجوة الزمنية بين ظهور التهديد واتخاذ القرار، وفي الوقت ذاته، برزت تحديات قانونية وأخلاقية تستدعي تأسيس إطار تشريعي متوازن يضمن ألا تتحول الأنظمة الذكية إلى وسيلة لمراقبة الأفراد دون ضوابط، أو إلى أداة تتخذ قرارات غير شفافة تمس الحقوق والحريات. فالذكاء الصناعي—على الرغم من دقته—لا يخلو من احتمالات الخطأ أو التحيز، ما يفرض ضرورة إخضاعه لرقابة قضائية وإدارية صارمة، وتقييد استخدامه بمبادئ الشرعية، والتناسب، والخصوصية، وحق الدفاع، وضمان الشفافية الخوارزمية. لذلك يظهر أن الذكاء الصناعي يمثل مرحلة جديدة من التطور الجنائي المعاصر، مرحلة تتكامل فيها القدرات التقنية مع الأهداف القانونية، بحيث تظل التكنولوجيا في خدمة العدالة، وتظل العدالة محصّنة بضمانات القانون. وإذا ما تمكّن المشرّع من تنظيم هذا التوازن، فإن الذكاء الصناعي سيشكل إحدى أكثر الأدوات فاعلية في تعزيز الأمن ومنع الجريمة وصون النظام العام.

النتائج:

١. تبيّن أن الذكاء الصناعي يمثّل حجر الأساس في التحليل الجنائي الاستباقي، لأنه قادر على رصد الأنماط السلوكية الكامنة وراء الجريمة بدقة تفوق التحليل البشري. وأسهم في تحويل الوقاية إلى ممارسة عملية تقوم على التنبؤ لا ردّ الفعل، مما وسّع من قدرة الأجهزة الأمنية على منع الجريمة قبل وقوعها.
٢. أظهرت الدراسة أن التنبؤ بالجريمة عبر الذكاء الصناعي يعتمد على تحليل البيانات الضخمة وربطها بالسياق المكاني والزماني، وهو ما مكّن المؤسسات الأمنية من تحديد "البؤر الحرجة" وتوزيع الموارد على أساس علمي، الأمر الذي يعزز حماية المجتمع ويحد من العشوائية في التدخل الأمني.
٣. اتضح أن الذكاء الصناعي أصبح أدق الوسائل في رصد الجرائم الإلكترونية، لأنه قادر على مراقبة الشبكات في الزمن الحقيقي، واكتشاف الهجمات قبل تنفيذها، والتعرف على الأنماط الشاذة في حركة البيانات. وأسهم في تخفيض معدلات الاختراق، ورفع جاهزية المؤسسات الرقمية.
٤. أثبتت الأنظمة الذكية فعاليتها في كشف سرقة البيانات، وهجمات الفدية، وتخريب الأنظمة، لأنها تعتمد على التحليل السلوكي للبرمجيات وليس فقط على التعرف التقليدي للأكواد الضارة، وهو ما جعلها أداة رئيسية في الدفاع الرقمي الوطني.
٥. أظهرت الدراسة أن سلامة الفضاء العام أصبحت تعتمد على الذكاء الصناعي بوصفه آلية لرصد السلوكيات الخطرة في المدن الذكية، من خلال كاميرات المراقبة الذكية، وتحليل

الحركة، والتعرف على الوجوه، وإدارة الحشود، مما رفع من مستوى الوقاية ومنع كثيرًا من الجرائم قبل اكتسابها طابعًا فعليًا.

٦. اتضح أن الذكاء الصناعي قادر على إدارة المرور بصورة تمنع الجرائم المرتبطة بالمركبات، مثل السرقة أو النقل المحظور أو التخفي، عبر تحليل تدفق الحركة، والتعرف على لوحات المركبات، وتحديد المركبات المشتبه بها في ثوانٍ معدودة.

٧. كشفت الدراسة عن قدرة الذكاء الصناعي على تحليل البنية الحضرية للمدن، وتحديد المواقع التي تشكل بيئة خصبة للجريمة، مما يساعد البلديات والأجهزة الأمنية على تعديل التصميم العمراني وفق متطلبات السلامة.

٨. بيّنت النتائج أن الذكاء الصناعي أصبح عنصرًا محوريًا في مكافحة الجرائم المالية، لأنه يحلل ملايين المعاملات في لحظات، ويكشف الأنماط الشاذة المرتبطة بغسل الأموال وتمويل الإرهاب والاحتيال المصرفي.

٩. أظهرت التحليلات أن الأنظمة الذكية تستطيع بناء "البصمة المالية" لكل عميل، مما يساعد المؤسسات المالية على اكتشاف الانحرافات الدقيقة في السلوك المالي، وإيقاف المعاملات المشبوهة فورًا، وهو ما أدى إلى تقليل الخسائر المالية وتعزيز الامتثال للمعايير الدولية.

١٠. اتضح أن الذكاء الصناعي يسهم بفعالية في كشف التلاعب بالأسواق المالية والجرائم المرتبطة بالبورصات، بفضل قدرته على تحليل التقلبات السريعة وربطها بأنماط تاريخية ومؤشرات خطر.

١١. أثبتت الدراسة أن الذكاء الصناعي أصبح جزءًا أساسيًا من التحقيقات الجنائية الحديثة، سواء في تحليل الأدلة الرقمية، أو الصور، أو الفيديو، أو الأصوات، أو البصمات الوراثية، مما زاد من دقة التحقيق وقلل من احتمالات الخطأ البشري.

١٢. أظهرت الأنظمة الذكية قدرة متميزة على تحليل محتوى التواصل الاجتماعي، واستخراج المؤشرات الدالة على الجرائم، مثل الابتزاز والتحريض والاتجار الرقمي، وهو ما عزز دورها في مواجهة الجرائم المنظمة والإرهاب الإلكتروني.

١٣. بيّنت الدراسة أن استخدام الخوارزميات في تصنيف المشتبه بهم وتقدير الخطورة ضرورة عملية، لكنها تحتاج إلى ضوابط قانونية تكفل الشفافية والحد من التحيز وتجنب المساس بمبدأ البراءة.

١٤. أظهرت النتائج أن الاعتماد على الذكاء الصناعي في التحقيقات يثير تحديات تتعلق بالخصوصية، وحق الدفاع، وحماية البيانات، مما يستوجب إطارًا تشريعيًا يحدد بدقة نطاق المعلومات التي يجوز جمعها وأسلوب استخدامها وفقًا لمبدأ الشرعية الإجرائية.

١٥. خلصت الدراسة إلى أن الذكاء الصناعي يمثل مستقبل السياسة الجنائية الحديثة، بشرط أن يُستخدم ضمن منظومة قانونية متوازنة تضمن احترام الحقوق والحريات، وتوفر رقابة فعّالة، وتخضع الخوارزميات لمعايير الشفافية والمسؤولية القانونية.

## الهوامش:

[١] البنا، محمد عبد الفتاح. أمن المعلومات والجرائم الرقمية. القاهرة: دار النهضة العربية، ٢٠١٧: ص ٢١

[٢] الخالدي، ناصر. الذكاء الاصطناعي والقانون. دبي: جامعة الإمارات، ٢٠٢١: ص ٣٨

[٣] الفرج، عبد الله. القانون والتكنولوجيا الحديثة. الكويت: جامعة الكويت، ٢٠١٦: ص ٩١
[٤] الجبور، عبد الكريم. المسؤولية الجنائية للأشخاص المعنوية. عمان: دار الثقافة للنشر، ٢٠١٨: ص ١٢
[٥] الكامل، مصطفى. المدن الذكية وإدارة الأمن. القاهرة: دار الفجر، ٢٠٢٠: ص ١٣٨
[٦] حسن، عبد القادر. تحليل البيانات في العمل الأمني. القاهرة: مركز الدراسات الأمنية، ٢٠٢٠:
[٧] سالم، رعد. أطر الأمن السيبراني ومعيار NIST. بغداد: دار البيان، ٢٠٢٢: ص ١٤٥
[٨] فاضل، عبد الباقي. جرائم الرشوة في ظل الثورة الرقمية. بغداد: مطبعة العدالة، ٢٠٢١: ص ٢٣١
[٩] مبارك، زهير. القانون الجنائي للأعمال. بيروت: منشورات الحلبي، ٢٠١٨: ص ٨١
[١٠] سعد، نجلاء. حماية الملكية الفكرية في البيئة الرقمية. القاهرة: دار الفكر القانوني، ٢٠١٩: ص ١٣٩
[١١] علي، عبد الجبار. المسؤولية الجنائية للشركات في الجرائم التقنية. بغداد: دار السنهوري، ٢٠٢٠: ص ١٧٦
[١٢] ناصر، أحمد خالد. السياسة الجنائية الحديثة. بغداد: دار الصفوة، ٢٠٢٠: ص ١٣
[١٣] جاسم، عبد الكريم. المسؤولية المدنية والجنائية في الأنظمة التقنية. بغداد: جامعة بغداد، ٢٠١٩: ص ١٣٦
[١٤] القريوتي، صلاح. الجريمة المنظمة والفساد التقني. بيروت: دار الراتب، ٢٠١٧: ص ٤١
[١٥] الخفاجي، إسماعيل. الحماية الجنائية للفضاء الرقمي. بغداد: دار الثقافة القانونية، ٢٠٢٢: ص ٢٦٢
[١٦] الطائي، فهد كاظم. مقدمة في الذكاء الاصطناعي. بغداد: دار الحكمة، ٢٠١٨: ص ٦٩-٧١ (بتلخيص)
[١٧] دروبي، خالد. التزوير الرقمي واستعمال المحررات الإلكترونية. بغداد: دار الحكمة، ٢٠٢١: ص ١٣١
[١٨] صادق، حسين. التحقيق المالي الجنائي. بغداد: مركز العدالة، ٢٠١٩: ص ٦٤
[١٩] كاظم، محمود. حماية البيانات التجارية والأسرار المهنية. عمان: دار الثقافة، ٢٠٢١: ص ٨٧
[٢٠] طاهر، سمير. الحماية الجنائية للمال العام. بغداد: دار الأمل، ٢٠١٩: ص ٢٣١
[٢١] المياحي، سامر. مكافحة غسل الأموال وفق التقنيات الحديثة. بغداد: دار الدليل، ٢٠٢١: ص ٣٩
[٢٢] القيسي، فاروق عبد الوهاب. الجرائم الإلكترونية وأمن المعلومات. عمان: دار وائل، ٢٠١٦: ص ٢
[٢٣] المدني، محمود. الأدلة الرقمية في التحقيق الجنائي. الرياض: دار النهضة، ٢٠١٩: ص ١٩٨
[٢٤] أنظر: الشواف، ميسون. التقنيات الحديثة في جمع الأدلة الجنائية. بيروت: دار النهضة، ٢٠٢٢: ص ١٢٩-١٣١ (بتلخيص و تصرف)
[٢٥] الطائي، حيدر عبد الأمير. جرائم الاختراق العلمي والرقمي. النجف: منشورات المواكب، ٢٠١٩: ص ٩٧
[٢٦] الدليمي، عبد الله حسين. السياسة الجنائية في مواجهة الجريمة الحديثة. بغداد: دار القضاء، ٢٠٢١: ص ٦٧
[٢٧] الزحيلي، وهبة. أثر التطور العلمي على التشريعات الجنائية. دمشق: دار الفكر، ٢٠١٢: ص ١٣٥.

## المصادر:

١. البنا، محمد عبد الفتاح. أمن المعلومات والجرائم الرقمية. القاهرة: دار النهضة العربية، ٢٠١٧.
٢. الخالدي، ناصر. الذكاء الاصطناعي والقانون. دبي: جامعة الإمارات، ٢٠٢١.
٣. الفرج، عبد الله. القانون والتكنولوجيا الحديثة. الكويت: جامعة الكويت، ٢٠١٦.
٤. الجبور، عبد الكريم. المسؤولية الجنائية للأشخاص المعنوية. عمّان: دار الثقافة للنشر، ٢٠١٨.
٥. الكامل، مصطفى. المدن الذكية وإدارة الأمن. القاهرة: دار الفجر، ٢٠٢٠.
٦. حسن، عبد القادر. تحليل البيانات في العمل الأمني. القاهرة: مركز الدراسات الأمنية، ٢٠٢٠.
٧. سالم، رعد. أطر الأمن السيبراني ومعيار NIST.بغداد: دار البيان، ٢٠٢٢.
٨. فاضل، عبد الباقي. جرائم الرشوة في ظل الثورة الرقمية. بغداد: مطبعة العدالة، ٢٠٢١.
٩. مبارك، زهير. القانون الجنائي للأعمال. بيروت: منشورات الحلبي، ٢٠١٨.
١٠. سعد، نجلاء. حماية الملكية الفكرية في البيئة الرقمية. القاهرة: دار الفكر القانوني، ٢٠١٩.
١١. علي، عبد الجبار. المسؤولية الجنائية للشركات في الجرائم التقنية. بغداد: دار السنهوري، ٢٠٢٠.
١٢. ناصر، أحمد خالد. السياسة الجنائية الحديثة. بغداد: دار الصفوة، ٢٠٢٠.
١٣. جاسم، عبد الكريم. المسؤولية المدنية والجنائية في الأنظمة التقنية. بغداد: جامعة بغداد، ٢٠١٩.
١٤. القريوتي، صلاح. الجريمة المنظمة والفساد التقني. بيروت: دار الراتب، ٢٠١٧.
١٥. الخفاجي، إسماعيل. الحماية الجنائية للفضاء الرقمي. بغداد: دار الثقافة القانونية، ٢٠٢٢.

١٦. الطائي، فهد كاظم. مقدمة في الذكاء الاصطناعي. بغداد: دار الحكمة، ٢٠١٨.
١٧. دروبي، خالد. التزوير الرقمي واستعمال المحررات الإلكترونية. بغداد: دار الحكمة، ٢٠٢١.
١٨. صادق، حسين. التحقيق المالي الجنائي. بغداد: مركز العدالة، ٢٠١٩.
١٩. كاظم، محمود. حماية البيانات التجارية والأسرار المهنية. عمّان: دار الثقافة، ٢٠٢١.
٢٠. طاهر، سمير. الحماية الجنائية للمال العام. بغداد: دار الأمل، ٢٠١٩.
٢١. المياحي، سامر. مكافحة غسل الأموال وفق التقنيات الحديثة. بغداد: دار الدليل، ٢٠٢١.
٢٢. القيسي، فاروق عبد الوهاب. الجرائم الإلكترونية وأمن المعلومات. عمّان: دار وائل، ٢٠١٦.
٢٣. المدني، محمود. الأدلة الرقمية في التحقيق الجنائي. الرياض: دار النهضة، ٢٠١٩.
٢٤. الشواف، ميسون. التقنيات الحديثة في جمع الأدلة الجنائية. بيروت: دار النهضة، ٢٠٢٢.
٢٥. الطائي، حيدر عبد الأمير. جرائم الاختراق العلمي والرقمي. النجف: منشورات المواكب، ٢٠١٩.
٢٦. الدليمي، عبد الله حسين. السياسة الجنائية في مواجهة الجريمة الحديثة. بغداد: دار القضاء، ٢٠٢١.
٢٧. الزحيلي، وهبة. أثر التطور العلمي على التشريعات الجنائية. دمشق: دار الفكر، ٢٠١٢.