ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net

"الدور الوقائي للذكاء الإصطناعي في مواجهة الجرائم الإلكترونية"

"Preventive Role of Artificial Intelligence in Confronting Cybercrimes"

إعداد الباحثين:

د. سيد محمود ميرخليلي[1] – د. مهدي خاقاني إصفهاني[2] – سجاد الهماشي[3]

1- أستاذ بكلية القانون مجمع الفارابي بجامعة طهران، إيران.

2- أستاذ مساعد في القانون الجنائي بأكاديمية البحث والتطوير في العلوم الإنسانية (سمت)، طهران

3- باحث دكتوراه في القانون الجنائي بجامعة طهران، إيران.

Researchers:

Dr. Seyed Mahmoud Mirkhalili – Dr. Mahdi Khaghani Esfahani – Sajjad Al-Hamashi

Received: 26/03/2026 | Revised: 27/03/2026 | Accepted: 31/03/2026 | Published: 02/04/2026

Abstract:

With the development of artificial intelligence (AI) tools and the rise of cybercrime, including financial fraud, phishing, and hacking, it is essential that scientific research addresses how to combat these crimes using innovative tools that provide effective prevention. AI offers practical solutions for combating cybercrime; however, legal frameworks in many countries need to adapt to these advanced technologies. This research will analyze the ethical and legal challenges associated with using AI in combating cybercrime, such as privacy and the protection of personal data. The benefit of artificial intelligence's preventative role in combating cybercrime lies in a range of advantages that significantly contribute to improving cybersecurity and data protection. The main benefits of using AI in crime prevention can be summarized as follows: early threat detection, rapid and automated response to cyberattacks, prevention of unknown threats, big data analysis and pattern recognition, and improved accuracy and performance of cybersecurity systems. This research employs a descriptive-analytical approach within the field of crime prevention, a branch of criminology. The study concluded that the use of AI in non-punitive social prevention encompasses several measures, most notably the impact of raising public awareness about AI on preventing deception, and the effect of increasing specialized AI knowledge among government employees in deterring them from committing crimes. The use of AI in situational prevention focuses on identifying opportunities for cybercrime and making it more difficult to commit.

Keywords: Artificial intelligence, cybercrime, criminology, situational prevention, cybersecurity rights

ملخص البحث

مع تطور أدوات الذكاء الاصطناعي وزيادة الجرائم الإلكترونية التي تشمل الاحتيال المالي، التصيد الإلكتروني، والقرصنة، من الضروري أن يتعامل البحث العلمي مع كيفية مواجهة هذه الجرائم باستخدام أدوات مبتكرة توفر الوقاية الفعالة. الذكاء الإصطناعي يقدّم حلولًا عملية لمكافحة الجرائم الإلكترونية، ولكن مع ذلك، فإن التشريعات القانونية في العديد من الدول بحاجة إلى التكيف مع هذه الأدوات التكنولوجية المتطورة. البحث سيحلل التحديات الأخلاقية والقانونية المرتبطة باستخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، مثل الخصوصية وحماية البيانات الشخصية. الفائدة من الدور الوقائي للذكاء الاصطناعي في مواجهة الجرائم الإلكترونية تكمن في مجموعة من المزايا التي تساهم بشكل كبير في تحسين الأمن السيبراني وحماية البيانات. يمكن تلخيص الفوائد الرئيسية لإستخدام الذكاء الإصطناعي في الوقاية من الجرائم في النقاط التالية: الكشف المبكر عن التهديدات، الاستجابة السريعة والآلية للهجمات الإلكترونية، منع التهديدات المجهولة، تحليل البيانات الضخمة والكشف عن الأنماط، تحسين دقة وأداء أنظمة الأمان السيبراني. يعتمد البحث المنهج الوصفي التحليلي في نطاق علم الوقاية من الإجرام وهو أحد فروع علم الإجرام. توصّلت الداسة إلى أنّ استخدام

AJSP
المجلة العربية للنشر العلمي

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الذكاء الاصطناعي في الوقاية غير العقابية الإجتماعية تشمل عدة تدابير، أهمّها أثر زيادة الوعي العام حول الذكاء الاصطناعي على منع خداع الناس، وأثر زيادة المعرفة التخصصية لدى موظفي الحكومة بالذكاء الاصطناعي في ردعهم عن ارتكاب الجرائم. أما إستخدام الذكاء الاصطناعي في الوقاية الظرفية تركّز على تحديد فرص الجريمة الالكترونية وإيجاد الصعوبة في ارتكابها.

الكلمات الرئيسية: الذكاء الإصطناعي، الجرائم الإلكترونية، علم الإجرام، الوقاية الظرفية، حقوق الأمن السيبراني.

How to Cite This Article

ميرخليلي، س. م.، إصفهاني، م. خ.، والهماشي، س. (2026). الدور الوقائي للذكاء الاصطناعي في مواجهة الجرائم الإلكترونية. *المجلة العربية للنشر العلمي (AJSP)*، 9(90)، (565 -584).

AJSP | Vol. 9 | Issue 90 | DOI: https://doi.org/10.36571/ajsp.90 AJSP ORCID: https://orcid.org/0009-0005-8048-2082

المقدمة:

إنّ العصر الرقمي الحالي تواجه تحولات جذرية في طبيعة الجرائم وأنماطها، حيث أصبحت الجرائم الإلكترونية تشكل تهديداً متزايداً للأمن القومي والاقتصادي للأفراد والدول على حد سواء. في مواجهة هذا التحدي، برز الذكاء الاصطناعي كأحد أهم الأدوات الحديثة التي تعتمد عليها الحكومات والمؤسسات الأمنية في منع الجرائم قبل وقوعها. تهدف هذه الدراسة إلى تحليل متعمق للدور الوقائي للذكاء الاصطناعي في مجال مكافحة الجرائم، مع التركيز على آليات العمل والتطبيقات العملية والتحديات المصاحبة لهذا الاستخدام.

بخصوص الإطار النظري للوقاية من الجرائم باستخدام الذكاء الاصطناعي، يعتمد مفهوم الوقاية من الجرائم باستخدام الذكاء الاصطناعي على ثلاثة محاور رئيسية: التنبؤ، والرصد، والتحليل. تقوم أنظمة الذكاء الاصطناعي بتحليل كميات هائلة من البيانات من مصادر متنوعة، بما في ذلك سجلات الجرائم السابقة وبيانات المراقبة وأنماط السلوك البشري.[1] من خلال تقنيات التعلم الآلي، تتمكن هذه الأنظمة من تحديد الأنماط غير الطبيعية التي قد تشير إلى نية إجرامية، مما يتيح للسلطات المختصة اتخاذ إجراءات استباقية.

في مجال إنفاذ القانون التقليدي، تستخدم العديد من أجهزة الشرطة حول العالم أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي. هذه الأنظمة لا تقتصر على مجرد تسجيل الفيديو، بل تقوم بتحليل المشاهد في الوقت الفعلي للكشف عن السلوكيات المشبوهة أو التعرف على المشتبه بهم من خلال تقنيات التعرف على الوجوه.[2] كما يتم استخدام الذكاء الاصطناعي في تحسين توزيع الموارد الأمنية من خلال تحليل البيانات التاريخية للجرائم والتنبؤ بالمناطق الأكثر عرضة للجرائم في أوقات محددة.

بخصوص التحديات والمخاطر المرتبطة باستخدام الذكاء الاصطناعي فعلى الرغم من الفوائد الكبيرة التي يوفرها الذكاء الاصطناعي في مجال الوقاية من الجرائم، إلا أن هناك العديد من التحديات والمخاطر التي يجب أخذها في الاعتبار.[3] أحد أهم هذه التحديات هو

[1] عوضين، فايق، "استخدامات تقنيات الذكاء الاصطناعي بين المشروعية وعدم المشروعية". (المجلة الجنائية القومية 1، القاهرة: مجلة ربع سنوية تصدر عن المركز القومي للبحوث الاجتماعية والجنائية، مجلد 65 –مارس 2022م)، ص 133.

[2] تركي، منى كامل، "دور تكنولوجيا النانو في الكشف عن الجريمة، وحجّيّتها كدليل أمام القضاء". تقديم: مصطفى الفوركي، (مجلة القانون والأعمال الدولية، 33، سلسلة الأبحاث الجامعية والأكاديمية، 2020 م)، ص 83.

[3] دولي الخضر، ناصري نفيسة، دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، مجلة المؤشر للدراسات الاقتصادية، المجلد 2، العدد 2، 2018م، ص 34.

مسألة الخصوصية، حيث أن استخدام تقنيات المراقبة الذكية وتحليل البيانات الشخصية يثير تساؤلات حول حدود الرقابة وحقوق الأفراد في الخصوصية.

التحدي الآخر يتمثل في إمكانية التحيز في الخوارزميات، حيث أن أنظمة الذكاء الاصطناعي تعتمد على البيانات التاريخية التي قد تحتوي على تحيزات بشرية. هذا قد يؤدي إلى نتائج تمييزية ضد فئات معينة من المجتمع. بالإضافة إلى ذلك، هناك تحديات تقنية تتعلق بتكلفة تطوير وصيانة هذه الأنظمة، والحاجة إلى كوادر بشرية متخصصة قادرة على إدارتها وتفسير نتائجها.

من حيث التحديات، يجب مراعاة الأخلاقيات في استخدام تقنيات الذكاء الاصطناعي. ويجب أن يقترن استخدام الذكاء الاصطناعي باحترام الحقوق الأساسية للناس وأمنهم وسبل عيشهم وحماية المواطنين. لا ينبغي لأنظمة الرقابة والمراقبة أن تؤدي إلى السيطرة والهيمنة على المواطنين. إن استخدام هذه التكنولوجيا للحكومات المحتاجة هو إطار عمل تم تحديده لزيادة ثقة الجمهور، وتحسين مستويات معيشة الناس، وزيادة الخدمات الحكومية المقدمة للشعب وتسهيلها وتحسينها.[4] ولذلك، فإن استخدامها لا ينبغي أن يؤدي إلى انتهاك الخصوصية أو حقوق الإنسان الأساسية. ومن الضروري وضع حد أدنى من القوانين والأنظمة في هذا المجال على المستويين المحلي والدولي. ومن المهم أيضًا معالجة قضايا من المسؤول إذا تسببت أنظمة التشغيل الآلية في أضرار أو إصابات؟ وقد تقدمت بعض الدول بمقترحات مثل منح الشخصية الإلكترونية، ومنح الهوية، والتأمين، ولكن يبقى أن نرى ما هي التحديات والعواقب التي يفرضها كل من هذه المقترحات. تحاول بعض البلدان حاليًا إعطاء شخصيات للروبوتات. إذا قبلنا مثل هذه المسألة، فسوف تحدث ثورة وتحول كبير في الفكر القانوني التقليدي في تحديد الحقوق والمسؤوليات والواجبات. بخصوص العقوبات القانونية المقررة للمتجاوزين في إطار استخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، فهو يعني من يُسيء استخدام الذكاء الاصطناعي أو يستغله بطريقة تُخل بالأمن الرقمي أو تنتهك الحقوق.[5]

في إطار الدراسة المقارنة بين القانون العراقي والقانون القطري، إليك توضيحًا عامًّا للعقوبات، مع الإشارة إلى أن معظم الدول لا تزال تعمل على تطوير تشريعات واضحة ومباشرة بشأن الذكاء الاصطناعي تحديدًا، لذلك تُستمد العقوبات غالبًا من القوانين الخاصة بالجرائم الإلكترونية والبيانات الشخصية. يتجه مستقبل استخدام الذكاء الاصطناعي في الوقاية من الجرائم نحو مزيد من التطور والتكامل. من المتوقع أن تشهد السنوات القادمة تطوراً في تقنيات الذكاء الاصطناعي التفسيري، الذي لا يكتفي بالتنبؤ بالجرائم بل يقدم تفسيرات واضحة لقراراته، مما يزيد من الشفافية والثقة في هذه الأنظمة.[6]

[4] الأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، مجلة القانون والعلوم البيئية، المجلد2، العدد2، 2023م، ص 185.

[5] سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة، جامعة عجمان، الإمارات العربية المتحدة، 2020م، ص 208.

[6] الحضيري، الحسن الطيب عبد السلام الأسمر، "الاثبات الجنائي بالوسائل العلمية الحديثة – دراسة مقارنة بين القانون الجنائي الليبي والفقه المعاصر". رسالة ماجستير، بقسم الشريعة والقانون، كلية الدراسات العليا، جامعة مولانا إبراهيم الإسلامية الحكومية مالانج، إشراف: د. محمد عبد الحميد، العام الجامعي 2016م، ص 132.

الفائدة من الدور الوقائي للذكاء الاصطناعي في مواجهة الجرائم الإلكترونية تكمن في مجموعة من المزايا التي تساهم بشكل كبير في تحسين الأمن السيبراني وحماية البيانات. يمكن تلخيص الفوائد الرئيسية في النقاط التالية:

1. الكشف المبكر عن التهديدات: الذكاء الاصطناعي يمكنه تحليل البيانات بشكل سريع وفعال للكشف عن الأنماط غير العادية أو السلوكيات المشبوهة. هذا يسمح بالكشف المبكر عن التهديدات الإلكترونية قبل أن تصبح هجمات كبيرة. أمثلة: استخدام تقنيات مثل التعلم الآلي (Machine Learning) لتحليل سجلات البيانات واكتشاف محاولات الاختراق أو الهجمات الموجهة بشكل مبكر.

2. الاستجابة السريعة والآلية للهجمات الإلكترونية: الذكاء الاصطناعي يمكنه اتخاذ إجراءات فورية للحد من الهجمات الإلكترونية، مثل إغلاق الثغرات الأمنية أو عزل الأنظمة المتضررة. هذه الاستجابة السريعة تقلل من الأضرار التي قد تحدث نتيجة للهجمات الإلكترونية.

3. منع التهديدات المجهولة: الذكاء الاصطناعي يمكن أن يتعرف على أنماط هجومية جديدة غير معروفة مسبقًا، مما يمكنه من منع الهجمات التي قد لا تكون برامج الحماية التقليدية قادرة على اكتشافها. يعتمد الذكاء الاصطناعي على الخوارزميات الذكية التي تحلل سلوك الأنظمة وتتعرف على التهديدات غير التقليدية.

4. تحليل البيانات الضخمة والكشف عن الأنماط: من خلال القدرة على تحليل كميات ضخمة من البيانات (Big Data)، يمكن للذكاء الاصطناعي أن يكشف عن الاتجاهات المتكررة أو السلوكيات الغير طبيعية التي قد تشير إلى محاولات اختراق أو أنشطة إجرامية. على سبيل المثال: استخدام تقنيات تحليل البيانات للكشف عن محاولات التصيد الاحتيالي (Phishing) أو الهجمات المتقدمة الموجهة (APT).

5. تحسين دقة وأداء أنظمة الأمان السيبراني. الذكاء الاصطناعي يمكن أن يحسن أداء الأنظمة الأمنية من خلال فحص البيانات وتحليلها في الوقت الفعلي، مما يجعل أنظمة الحماية أكثر دقة و كفاءة. تقنيات مثل أنظمة الكشف عن التسلل المدعومة بالذكاء الاصطناعي تعمل على تحسين معدل الكشف وتقليل نسبة الإيجابيات الكاذبة (False Positives)

6. هناك مجالات مختلفة للذكاء الاصطناعي في العمل الشرطي والأمني، وهذا غالباً يندرج تحت استراتيجية المدن الذكية، والتي من ضمن أهدافها استخدام التقنيات المتطورة مثل الذكاء الاصطناعي؛ لضمان أمن وسلامة السكان في المدينة، وتشمل تقنيات الذكاء الاصطناعي على كاميرات المراقبة الذكية التي لديها القدرة على تحليل الصور والفيديو لاكتشاف أماكن تواجد المشبوهين أو المطلوبين والأمور غير الطبيعية وتنبيه مركز التحكم مباشرةً، واستخدام تقنية تعلم الآلة في مجال الأمن الإلكتروني، واستخدام الطائرات الذكية بدون طيار (سمارت درونز) للمراقبة الجوية[7]، وكذلك تطبيقات "التنبؤ الشرطي، وتقوم بعض الجهات الشرطية الرائدة حالياً باستخدام الذكاء الاصطناعي وتقنياته المختلفة في محاربة الجريمة، من خلال الاعتماد على تقنياته الذكية في مجال التحقيق الجنائي للكشف عن العديد من الجرائم من أهمها الجرائم الإلكترنية.

7. إنّ تقنيات الذكاء الإصطناعي تساعد في سرعة الكشف عن الجرائم، من خلال تحليل كميات ضخمة من البيانات والإدلة والتعرف على المشتبه بهم بأقل وقت، كما يعزز الذكاء الإصطناعي من قدرة مأموري الضبط القضائي من القيام بالدور الوقائي لمنع وقوع الجرائم من خلال امكانية التنبؤ بها واتخاذ تدابير اللازمة لمنعها[8]. وإنما يشكل الذكاء الإصطناعي وسيلة لتعزيز الأدلة المقدمة من مأمور الضبط القضائي في مرحلة التحري والإستدلال مما ينعكس على قوة الإثبات الجنائي ويحقق العدالة. كما تعد تقنيات الذكاء الإصطناعي أداة مهمة في مكافحة الجرائم الإلكترونية والحد منها. وتعزز من استقرار النظام العام في الإماكن المزودة بها.

يفترض البحث أن تقنيات الذكاء الاصطناعي تمتلك قدرة عالية على الكشف المبكر عن الجرائم الإلكترونية للوقاية الظرفية والتقليل من فرص وقوعها، مما يجعل لها دورًا وقائيًا فعّالاً. وباستخدام الذكاء الاصطناعي، يقومون بتحديد أنماط السلوك غير العادية والمزعجة

وتصنيف وتتبع الأفراد الذين من المحتمل أن يرتكبوا أعمالاً إجرامية. وتقوم هذه البلدان بأنشطة استخراج البيانات في التحقيقات الجنائية وتحليل الجرائم الذكية على أساس المتغيرات الثلاثة للجريمة، بما في ذلك المتغير المكاني الزمني (إحداثيات الزمان والمكان للجريمة)، والخصائص السلوكية الطبيعية (مثل خصائص مسرح الجريمة، ونمط السلوك الإجرامي)، والخصائص الإجرامية (مثل الجنس والعمر والعرق، وما إلى ذلك). تستخدم برامج وأنظمة التحقيق الجغرافي نهجًا مختلفًا عن تقنيات رسم خرائط الجريمة التقليدية، وذلك باستخدام مواقع الجريمة السابقة وخوارزميات رياضية معقدة لتقدير احتمالية إقامة مجرم في مكان معين. تحتوي بعض البرامج على نظام تنبيه ومراقبة جغرافية يتم استخدامها للإبلاغ عن الجرائم وموقع الضحية وحالة الخطر الجرميّ.

2- الأهمية، مشكلة البحث وأهدافه

تكمن أهمية هذا البحث في كونه يتناول جانبًا مستقبليًا حيويًا يمس أمن الدول، ويطرح رؤية قانونية تحليلية مقارنة تسهم في سد الثغرات التشريعية وتعزيز سبل الوقاية الرقمية، مع احترام الخصوصية والحقوق الأساسية للأفراد في البيئة السيبرانية.

كما تتجلى أهمية هذه الدراسة في أن الذكاء الاصطناعي يصطدم بشكل مباشر بالحقوق الأساسية للإنسان إيجاباً وسلباً، وكأننا في هذا الصدد نحاول الموازنة ما بين حاجتنا المستمرة لتطوير تقنيات الذكاء الاصطناعي والحفاظ على حقوق الأفراد المنصوص عليها في القانون الدولي لحقوق الإنسان كحق الأفراد بعدم انتهاك خصوصيتهم. وعليه، فانه لابد للمجتمع الدولي أن ينظم عمل هذه التقنيات عن طريق مجموعة من القواعد والقوانين والأسس التي تضبط تطوير الذكاء الاصطناعي وطريقة عملهما بواءم احترام قواعد القانون الدولي لحقوق الإنسان، وهذا ما يطلق عليه بحوكمة الذكاء الاصطناعي من منظور حقوق الإنسان.

يشهد العالم اليوم تطورًا رقميًا غير مسبوق، نتج عنه تحوّل كبير في طبيعة التهديدات الأمنية، لا سيما مع تصاعد الجرائم الإلكترونية التي تستهدف الأفراد والمؤسسات والدول على حدّ سواء. لم تَعُد الجرائم الإلكترونية محصورة في القرصنة أو الاحتيال، بل توسعت لتشمل الإرهاب الرقمي، الابتزاز، انتهاك الخصوصية، وتخريب البنى التحتية الرقمية. وفي ظل هذا الواقع المتغيّر، برزت الحاجة إلى أدوات وتقنيات تواكب هذا التطور[9]، لا سيما تلك التي تعتمد على الذكاء الاصطناعي بوصفه أداة حديثة يمكن تسخيرها في تعزيز الأمن السيبراني. الذكاء الاصطناعي، بما يملكه من قدرة على معالجة كميات هائلة من البيانات، وتعلُّم الأنماط وتحليلها، والتنبؤ بالسلوك الإجرامي، بات يمثل أحد الركائز الأساسية في الوقاية من الجرائم الإلكترونية. إذ يمكن من خلال تقنياته رصد محاولات الاختراق مبكرًا، التعرف على السلوكيات الشاذة في الشبكات، تحليل البرمجيات الخبيثة، والتعامل مع التهديدات بشكل استباقي قبل تطورها إلى جرائم فعلية.

وفي هذا الإطار، يُثار التساؤل حول مدى مواكبة التشريعات الوطنية، لا سيما في الدول العربية، لهذا التطور التقني. ومن هنا تأتي أهمية البحث في "الدور الوقائي للذكاء الاصطناعي في مواجهة الجرائم الإلكترونية"، وذلك من خلال دراسة مقارنة بين القانون العراقي والقانون القطري، بهدف بيان كيفية تنظيم هذه الدول لاستخدام الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، ومدى استيعاب تشريعاتها للمخاطر والفرص التي تفرضها هذه التكنولوجيا.[10]

---

[7] تركي، المصدر السابق، ص 197.

[8] أوسندي أ.أوشوبا، ووليليام ويسلر الرابع، "مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل". (مؤسسة RAND كليفورنيا، الولايات المتحدة الأمريكية، 2017م)، ص 309.

[9] عمار ياسر زهير البابلي، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الأمن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد 1، 2021، ص 198.

[10] عبد الله أحمد مطر الفلاسي، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، دون دار نشر، دون سنة نشر، ص 91.

تنبع أهمية هذا الموضوع من كونه يدمج بين بعدين حيويين: التقني والقانوني، ويسلط الضوء على تحديات المرحلة القادمة، في ظل تنامي الاعتماد على الذكاء الاصطناعي في كافة مجالات الحياة، بما في ذلك الأمن ومكافحة الجريمة. كما تسعى هذه الدراسة إلى إثراء الفقه القانوني العربي بأدوات تحليلية تساعد على وضع تشريعات مرنة ومتطورة تستجيب لطبيعة العصر الرقمي.

وخلال العقود الأخيرة تطورًا هائلًا في مجالات التكنولوجيا والاتصالات، ونتيجة لذلك ظهرت أنماط جديدة من الجرائم عُرفت بالجرائم الإلكترونية. هذه الجرائم لا تقتصر على سرقة الأموال أو المعلومات، بل تمتد لتشمل تهديد الأمن القومي، وانتهاك الخصوصية، ونشر الشائعات، وابتزاز الأفراد.[11] في ظل هذا التطور المعقّد والمتسارع، لم تعد الوسائل التقليدية في مكافحة الجرائم كافية، مما استدعى الاستعانة بأدوات وتقنيات متقدمة، وفي مقدمتها الذكاء الاصطناعي.

في السياق العراقي، فإن الوضع القانوني المرتبط بالجرائم الإلكترونية لا يزال يعاني من فراغ تشريعي واضح. حتى عام 2024 لم يصدر قانون شامل ومخصص للجرائم الإلكترونية، على الرغم من المحاولات المتكررة لتمرير مشاريع قوانين في هذا المجال. الجهود الحالية تكتفي باستخدام النصوص العامة في قانون العقوبات العراقي رقم 111 لسنة 1969، إلى جانب بعض التعليمات الإدارية، ما يجعل من الصعب ملاحقة مرتكبي هذه الجرائم بفعالية، خاصة في ظل تعقيد الأدلة الرقمية وحداثة أساليب الجريمة. علاوة على ذلك، فإن البنية التحتية التقنية لدى الجهات الأمنية ما زالت محدودة، وغالبًا ما تفتقر الكوادر إلى التدريب الكافي في التعامل مع أدوات التحليل الإلكتروني أو تقنيات الذكاء الاصطناعي، ما يجعل العراق بحاجة ماسة إلى إصلاحات قانونية ومؤسسية لتحديث منظومة مكافحة الجريمة الإلكترونية.

على العكس من ذلك، تبنّت دولة قطر منهجًا أكثر تطورًا وشمولية في التعامل مع الجرائم الإلكترونية. فقد صدر في عام 2014 قانون مكافحة الجرائم الإلكترونية رقم 14، الذي يُعد من التشريعات الحديثة في المنطقة، ويمثل خطوة متقدمة في تغطية الجوانب القانونية المرتبطة بالجرائم الرقمية. هذا القانون يُجرّم عددًا واسعًا من الأفعال الإلكترونية مثل اختراق الشبكات، سرقة البيانات، التزوير الرقمي، ونشر البرمجيات الخبيثة، ويضع عقوبات رادعة تصل إلى السجن والغرامات المالية الكبيرة. بالإضافة إلى ذلك، سنت قطر قانونًا لحماية البيانات الشخصية ينظم كيفية جمع البيانات واستخدامها، ويمنح الأفراد حق السيطرة على معلوماتهم الإلكترونية.

ينبغي تحديد احتياجات الشرطة للذكاء الاصطناعي وتصنيفها بطريقة منظمة ومشاركتها لتسهيل تطوير المشاريع المستقبلية؛ ينبغي تحديد مبادرات الذكاء الاصطناعي الجديدة أو الجارية بوعي من قبل وكالات إنفاذ القانون في الدولة؛ ينبغي إعداد نصوص قانونية أخلاقية لجمع وتحليل البيانات اللازمة لإنفاذ القانون[12]؛ ينبغي استكشاف الفرص وتقنيات إدارة الخصوصية وقضايا المساءلة المتعلقة باستخدام الذكاء الاصطناعي؛ ينبغي إجراء دراسة للجرائم الجديدة والناشئة التي تنطوي على الاستخدام الخبيث للذكاء الاصطناعي والروبوتات؛ المناقشة القادمة حول الوعي. ينبغي تطوير الوعي بشكل أكبر بقضايا الذكاء الاصطناعي والروبوتات داخل الشرطة من خلال تحسين التدريب وتبادل المعلومات؛ يجب مراقبة مشهد تكنولوجيا الذكاء الاصطناعي والروبوتات باستمرار؛ الموضوع القادم هو الاجتماعات والتنسيق. ينبغي تشكيل اجتماعات ومنتديات نقاش متخصصة بشكل نشط من خلال اجتماعات سنوية في مجال الذكاء الاصطناعي للشرطة والمنظمات المماثلة. وينبغي إقامة تعاون دولي بين وكالات إنفاذ القانون وغيرها من أصحاب المصلحة ذوي الصلة؛ ينبغي عقد وتنظيم المزيد من الفعاليات مثل الدورات التدريبية وورش العمل والدورات المختلفة للتحليل لمهام الشرطة في مجال

[11] سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة، جامعة عجمان، الإمارات العربية المتحدة، 2020م، ص 143.

[12] Osoba، O.A. and W. Welser IV. (2017). *The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica*، CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE237.html.

التنبؤ بالجريمة[13]؛ والموضوع التالي يتعلق بالمعرفة وتبادل المعلومات. ينبغي تشجيع وتعزيز العلاقات بين الشرطة والأوساط الأكاديمية وشركاء الصناعة المجتمعية؛ ويجب تطوير مجال التعاون المتبادل والعمل المشترك والمشاركة.

بخصوص **مزايا الذكاء الصناعي في الميدان القانوني والقضائي، إنّ استخدام الذكاء الصناعي له مزايا عديدة في القانون والقضاء نذكر منها: أ) انه مساعد افتراضي للقضاة والمدعين والمحامين ففي امركا والدول المتقدمة ادت اتمتة القوانين والقضايا والقرارات الى جعلها كنزا للمعلومات يلجا اليه القضاة عند عرض واقعة معينة امامه بسبب الية البرامج المعتمدة في تغذية الذكاء الصناعي للربورتات التي امتلكت القدرة الهائلة على الجمع بين الضروف المتشابهة في القضايا المتماثلة والخروج بنتائج تعرض على القضاة الذين يعتمدون هذا النظام ففي احدى التجارب التي اجرية في الولايات المتحدة الامركية تمكنت هذه الربورتات خلال فترة قصيرة من الخروج بنتائج معينة من خلال المطابقة بين 750000الف قضية حسمها القضاء واصدر فيها قراراته وهذه النتائج استشارية وليست الزامية وهي تمكن القاضي من اجراء التحليل الدقيق لضروف الواقعة المعروضة امامه وادلتها وصولا الى اصدار حكم عادل فيها[14] .ب) ان استخدام الذكاء الصناعي يسرع من اجرأت التقاضي ويختزل الجهد والوقت والنفقات المطلوبة لحسم الدعوى وهذا بدوره ينعكس ايجابا على عملية الترافع امام المحاكم ويسهم في ضمان استقرار القضاء. ج) الغاية من اعتماد الذكاء الصناعي تتمثل في ايجاد نظام متكامل للمعلومات القانونية والقضائية يمكن القضاة والمحامين اللجوء اليها والافادة منها في اسرع وقت ممكن لان الرجوع لهذه المعلومات يستغرق وقتا طويلا مما يؤدي الى تكرار تاجيل القضايا المنظورة امام القضاء وتراكم الدعاوى من جهة واطالت امد النزاع وما له من اثار سلبية لايحمد عقباها من جهة اخرى وهو ما تعاني منه الانظمة القضائية التي لم تعتمد الذكاء الصناعي في جميع مفاصل العملية القضائية ومنها النظام القضائي لدينا في العراق.** ويتجلى **الذكاء الصناعي** في أداء الجهاز الإداري للقضاء وفي أداء القضاة والمحامين والمحضرين. إن وجود الذكاء الاصطناعي يمكن أن يقضي على العديد من الوظائف غير الضرورية وينقل الموارد البشرية المتخصصة والتقدير القضائي نحو قدر أكبر من الكفاءة والسرعة والدقة، مما سيؤدي في نهاية المطاف إلى زيادة رضا المترددين على النظام القضائي وتحقيق عدالة أفضل.

تتركز مشكلة الدراسة في استخدام تقنيات الذكاء الإصطناعي والإستفادة منها في مكافحة الجريمة منعًا وكشفاً كأحد الوسائل الحديثة في أداء مهام حفظ الأمن ومكافحة الجرائم، والتنبؤ بأماكن حدوثها بناءً على بيانات لأماكن تجمع المجرمين وتتبعهم، وهو ما يندرج تحت إستراتيجية المدن الذكية التي من أهم أهدافها استخدام التقنيات المتطورة لحماية استقرارها؛ لضمان سلامة أشخاصها وأمن ممتلكاتها؛ فضال عن استعانة أجهزة إنفاذ القانون، إلا أن مكافحة الجرائم الواقعة على الأشخاص والأموال وجدت تحديات تواجه كشفها وملاحقة مترتكبيها.

يؤدي الذكاء الإصطناعي دورا بارزا في الحد من الجرائم، وخاصة الجرائم الماسة بحق الإنسان في الحياة وسلامته البدنية، بإعتبارها أهم المصالح العليا التي قرر المشرع الجنائي حمايتها، فيمكن الإستعانة بتطبيقات الذكاء الإصطناعي في كشف هذا النوع من الجرائم وملاحقة مرتكبيها، مما يعزز الحد منها[15]. يلجأ مأمورو الضبط القضائي إلى الإستعانة بتقنيات الذكاء الإصطناعي من خلال تفريغ

[13]Narain، K.، Swami، A.، Srivastava، A.، and Swami، S. (2019). Evolution and control of artificial superintelligence (ASI): a management perspective. *Journal of Advances in Management Research*، 16(5), 698-714. https://doi.org/10.1108/JAMR-01-2019-0006

[14] Mpinga، E.، Bukonda N.، Qailouli S.، and Chastonay P. (2022). Artificial Intelligence and Human Rights: Are There Signs of an Emerging Discipline? A Systematic Review. *Journal of Multidisciplinary Healthcare*، 15، 235-246. https://doi.org/10.2147/JMDH.S315314

[15] Abdel Razek، R. (2021). The Effect of Artificial Intelligence on Electronic Crime. *The Scientific Journal of King Faisal University.* Humanities and Management Sciences، 22(1)، 430-437.

كاميرات المراقبة وتحليلها، بفحص كل الأماكن أو المحلات أو الشوارع المحيطة بمسرح الجريمة وحركة جميع الأشخاص في مسرح الجريمة او في محيطه والتعرف عليهم؛ بهدف التوصل للمشتبه بهم، واخضاعهم للتحقيق، فهناك برامج يمكنها تحليل كل هذه المعلومات والصور بدقة وخلال وقت قصير جدا، بموضوعية وبعيدًا عن الأهواء الشخصية، كما يمكن من خلال هذه التقنيات اتخاذ التدابير الوقائية لمنع وقوع الجرائم الماسة بالحق في الحياة، من خلال مراقبة ودراسة طبيعة المناطق الأكثر خطورة، والتنبؤ بوقوع الجريمة ووضع الحلول لتجنب وقوعها وتقليل المخاطر بصورة كبيرة.

وقد أسهمت تقنيات الذكاء الإصطناعي في كشف جرائم السرقة من خلال كاميرات المراقبة للحد من ارتكاب الجرائم، حيث باتت كاميرات المراقبة بأنواعها المختلفة سواء في المنازل أو الشوارع العامة أو الكشف عن مرتكبيها[16]، بالإضافة إلى ما في الحد من ارتكاب الجرائم وأيضاً الموجودة داخل المحال تلعب دوراً يشكّله وجودها من رادع لكل من تسوّل له نفسه بتجاوز القوانين أو المساس بالمحظورات على اقتراف جرم أو إلحاق ضرر.

إن تقنيات الذكاء الإصطناعي أصبحت ضرورة لأصحاب المؤسسات والشركات والمحال التجارية للمتابعة والإشراف والرقابة على حسن سير العمل في منشآتهم من الإحتيال التقليدي والإحتيال الإلكتروني أحد أنواع الخداع والحيل ما تحدث هذه الجرائم في غرف الدردشة أو عبر البريد الإلكتروني أو التي تتم على شبكة الإنترنت، وغالباً إلى الإحتيال على العملاء والمستخدمين عن طريق سرقة الأموال على المنتديات أو مواقع الويب، ويهدف عادةً بهدف التجسس أو انتحال الشخصية أو المعلومات وغيرها من الأغراض الأخرى، وتكون هجمات الإحتيال عادةً الحصول على معلومات حسابهم في مركز حساس.

3- التأصيل التاريخي والدراسات السابقه

في التأصيل التاريخي لفكرة الوقاية من الجرائم السيبرانية عبر الذكاء الاصطناعي، يلزم أولًا إرجاع المفهوم إلى جذوره في السياسة الجنائية الوقائية التقليدية: انتقال التركيز من "الردع اللاحق" إلى "التحييد السابق" عبر إدارة المخاطر وتقليل فرص الإجرام. نظريًا، استندت الوقاية إلى مدرسة "الوقاية الوضعية من الجريمة" ونظرية "الأنشطة الروتينية" التي تُعيد ضبط البيئة لتقليل الحوافز وإتاحة الكشف المبكر.[17] عند انتقال الظاهرة إلى الفضاء الرقمي في تسعينيات القرن العشرين وبدايات الألفية، تَجَسّد ذلك في نظم كشف التسلّل القائمة على التوقيعات، وجدران النار، وفلترة الرسائل غير المرغوب فيها، وهي أدوات خوارزمية لكنها غير "ذكية" بالمعنى الحديث. في المستوى القانوني، مَهّدَتْ الاتفاقات الدولية والتشريعات الوطنية الخاصة بالجريمة المعلوماتية لإضفاء المشروعية على تدابير الرصد الاستباقي المشروط بمبادئ الضرورة والتناسب وحماية الحياة الخاصة، وبالتوازي تَرسَّخَت مقاربة "الحوكمة المعتمدة على المخاطر" في معايير أمن المعلومات والالتزام المؤسسي، بما أرسى أرضيةً معياريةً لقبول أدوات وقائية مؤتمتة ما دامت ترتبط بهدف مشروع وتخضع لرقابة لاحقة فعّالة.

تناولت معظم الدراسات الإنسانية العربية المتعلقة بالذكاء الاصطناعي دراسة الموضوع من منظور تقني، أما بالنسبة لدراسة التنظيم القانوني لتطوير الذكاء الاصطناعي؛ فهي محدودة. فعلى الرغم من التزايد المضطرد لاستخدام تقنيات الذكاء الصناعي في سائر المجالات إلا أن المناقشات الأكاديمية القانونية المتعلقة بتأثير الذكاء الاصطناعي على حقوق الإنسان لا تزال قليلة. إذ نجد بأن بعض القانونيين قد عنوا بتحليل الذكاء الاصطناعي من وجهة نظر وطنية في حدود التشريعات الداخلية المنظمة لتطوير هذه التقنيات وتطبيقها.

[16] Dahshan, Y. (2020). Criminal Responsibility for Artificial Intelligence Crimes. *Sharia and Law Journal*, 34(82), p. 143.

[17] خليفة، محمد محمد طه (2018). الذكاء الاصطناعي في ميزان التشريع. *مجلة دبي القانونية*، (28)، ص 133.

بينما اتجه بعضهم الآخر لتحليل التحديات والإشكاليات القانونية المترتبة على تطوير هذه التقنيات وعلاقتها بالمسؤولية المدنية (Mujahid, 2021) والمسؤولية الجزائية (Dahshan, 2020) والملكية الفكرية (Saeed, 2021)، فبالإضافة لتزايد التشريعات الوطنية التي بدأت بتنظيم عمل هذه التقنيات على المستوى الوطني فإن تنظيم عملية تطوير هذه التقنيات وعملها أصبحت محط عناية إقليمية ودولية أيضا (Al-Khalidi, 2021; Dahiyat, 2019). ولكون تبعات استخدام تقنيات الذكاء الاصطناعي أصبحت أمراً لا يمكن تجاهله أو حتى محاولة التقليل من أهمية تأثيره على البشرية كلها وعلى الفرد بشكل خاص، فإننا في دراستنا هذه سنركز على تنظيم تطوير تقنيات الذكاء الاصطناعي وحوكمتها ضمن إطار القانون الدولي لحقوق الإنسان. أي أننا لن نكتفي بذكر تأثير الذكاء الاصطناعي على حقوق الإنسان (Hassan, 2021) بل سنتوجه إلى تحليل واقتراح منظومة حوكمة قانونية تنظم عمل الذكاء الاصطناعي وفقاً لقواعد القانون الدولي لحقوق الإنسان.

على الرغم من أهمية الدور الوقائي للذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، إلا أن الموضوع لم يلق الاهتمام الكافي من الباحثين في العراق و قطر، وقد يعود ذلك لصعوبة قياس تدابير الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، ولعل ابرز الدراسات التي عالجت هذا الموضوع:

1- دراسة هادي فاروق عباس (2022) «استخدام الذكاء الإصطناعي في تنفي العقوبات الجنائية في النظام السعودي». هدف الدارسة إلى توضيح الذكاء الإصطناعي المتمثل في المراقبة الإلكترونية ومناقشة الضوابط القانونية لإستخدام الذكاء الإصطناعي المتمثل في المراقبة الإلكترونية، وتحليل ذاتية الذكاء الإصطناعي المتمثل في المراقبة الإلكترونية عما يتشابه معه. وتوصلت الدراسة إلى اتفاق المشرع الإماراتي مع المنظم السعودي في مناسبة السوار الإلكتروني كنموذج للذكاء الإصطناعي في تنفيذ العقوبات، والأهمية الكبرى لإستخدامات الذكاء الإصطناعي في تنفيذ العقوبات، وأن تطبيقات الذكاء الإصطناعي تساعد في تنفيذ العقوبات وإعادة التوازن بين الصالح العام من ناحية وصالح المجني عليه من ناحية أخرى.

2- دراسة سجى أحمد موسى (2022) «دور كيانات الذكاء الإصطناعي في التنبؤ والكشف عن الجريمة» وتهدف الدراسة التعريف بمصطلح كيانات الذكاء الإصطناعي والإعتماد على هذه الكيانات وربطها مع التطور في تقنية المعلومات والبيانات الضخمة ووسائل الإتصال والوقوف على أبرز المستجدات التقنية الحديثة. وتوصلت الدراسة إلى إن المستجدات التقنية الحديثة لها تأثير كبير وسيع على خدمة الأمن والصالح العام في المجتمع وحفظ الأمن وذلك بالكشف المبكر عن الجريمة والتنبؤ بها بواسطة كيانات الذكاء الإصطناعي.

3- دراسة محمد نورالدين سيد (2021) «التحديات الأمنية لإستخدام الذكاء الإصطناعي والأنظمة الرقمية في العمل وسبل ومواجهتها». وتهدف هذه الدراسة إلى التعرف على الذكاء الإصطناعي وأهم أنواعه وذكر تطبيقاتها والأنظمة التقنية المستخدمة في الأعمال المدنية ومعلوماتها وكذا تحديد الإيجابيات والسلبيات التي تعيق هذه التقنيات خاصة عند استعمالها في الهيئات والمؤسسات الأمنية. وقد استخدمت الدراسة المنهج الوصفي التحليلي والإستنباطي. وتوصلت الدراسة إلى نتائج من أبرزها أهمية وجود شراكة بين أجهزة أنفاذ القانون وإدارات مكافحة الجرائم السيبرانية وبين الشركات العاملة في تكنولوجيا الذكاء الإصطناعي وشركات القطاع الخاص التي تستعمل هذه التقنية للتعاون في تحصيل الأدلة التقنية.

4- دراسة حسن أحمد المؤمني (2019) «أهمية الذكاء الإصطناعي في مستقبل العمل الشرطي» وتهدف الدراسة إلى تحليل دور وأهمية التقنيات الحديثة كالبيانات الكبرى قيام الأجهزة الشرطية بجمع العديد من الأدلة ومراقبة الجريمة من خلال التحليل المسبق للبيانات المتوفرة مع الأخذ بعين الإعتبار ما يتصل بالتبعات الأمنية والنظامية والإنسانية. وتوصلت الدراسة إلى أن الذكاء الإصطناعي له أهمية كبرى في مستقبل العمل الشرطي حيث يساهم بشكل كبير اختصار الكثير من الإجراءات الطويلة والمعقدة، وتفسير مختلف البيانات والمعلومات كما يتميز بالسرعة في ملاحقة الجناة واكتشافهم في وقت قصير من خلال تقنيات الذكاء الإصطناعي المتطورة.

4- المبادى الفكرية والمصطلحات الرئيسية

بناء على المقدمة المذكورة أعلاه سنقوم الآن بعرض المفاهيم والمصطلحات والنظريات المهمة المتعلقة بموضوع الرسالة في هذا القسم من الفصل الأول، وذلك لتوفير الأساس لإدخال المحتوى الرئيسي في الفصل التالي من الرسالة. الدور الوقائي للذكاء الاصطناعي يختلف عن العناوين الأخرى لأنه يدمج بين التكنولوجيا و القانون بشكل عملي، ويبحث في كيف يمكن للذكاء الاصطناعي أن يكون أداة فعّالة في منع الجرائم بدلاً من التعامل مع الآثار السلبية بعد وقوعها. هذا البحث سيُساهم بشكل مباشر في فهم كيفية دمج التكنولوجيا ضمن الأنظمة القانونية لمواجهة التحديات المستقبلية في الجرائم الإلكترونية.

4-1- حقوق الأمن السيبراني

للأمن السيبراني أهمية كبيرة لكل مجتمع ولكل دولة، فالأمن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية والصور والملفات والفيديوهات والحسابات الشخصية وكلمات المرور والحسابات البنكية. وعلى مستوى المجتمع، من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي والبيانات المجمعة والخصوصيات للمجتمع. منظور القانون الجنائي للأمن السيبراني يركز على تجريم الأنشطة الضارة التي تتم عبر الإنترنت أو باستخدام التكنولوجيا الرقمية، مثل الاختراقات، والتهديدات، والابتزاز الإلكتروني، والاحتيال الرقمي. يهدف القانون الجنائي في هذا السياق إلى حماية الأفراد والمؤسسات والبيانات والمعلومات من الجرائم السيبرانية وتعزيز الأمن في الفضاء السيبراني.[18]

أهم جوانب الأمن السيبراني من منظور القانون الجنائي، تشكل: 1- تجريم الجرائم السيبرانية: يحدد القانون الجنائي أنواع الجرائم السيبرانية ويعاقب عليها، مثل اختراق الأنظمة، وسرقة البيانات، ونشر البرمجيات الخبيثة، والابتزاز الإلكتروني، والتشهير عبر الإنترنت. 2- حماية البيانات والمعلومات: يهدف القانون إلى حماية البيانات الشخصية والمالية والمعلومات الحساسة من الوصول غير المصرح به والاستخدام غير القانوني. 3- تعزيز الأمن السيبراني للمؤسسات: يشمل القانون السيبراني جوانب تنظيمية وإجرائية لضمان أمن المؤسسات والمنظمات في الفضاء السيبراني، من خلال وضع سياسات وإجراءات أمنية فعالة. التعاون الدولي: تتطلب الجرائم السيبرانية تعاونًا دوليًا لتبادل المعلومات والخبرات وتنسيق الجهود لمكافحة الجريمة السيبرانية عبر الحدود. وأما التحديات التي تواجه القانون الجنائي في مجال الأمن السيبراني تشكل: التطور السريع للتكنولوجيا: يتطلب القانون تحديثًا مستمرًا لمواكبة التطورات السريعة في التكنولوجيا والجرائم السيبرانية الجديدة. صعوبة تحديد مرتكبي الجرائم: يصعب تحديد مرتكبي الجرائم السيبرانية في كثير من الحالات بسبب طبيعة الفضاء السيبراني والقدرة على إخفاء الهوية. التحديات القانونية: قد تواجه القوانين السيبرانية تحديات تتعلق بتفسيرها وتطبيقها في مختلف السياقات القانونية.

أمثلة على الجرائم السيبرانية التي يعاقب عليها القانون الجنائي: الابتزاز الإلكتروني: استخدام التهديد بنشر معلومات خاصة أو صور أو مقاطع فيديو لابتزاز الضحية ماليًا. التجسس الإلكتروني: الوصول غير المصرح به إلى أنظمة الكمبيوتر أو المعلومات الشخصية أو الحساسة. سرقة الهوية: انتحال صفة شخص آخر للحصول على معلومات أو أموال أو خدمات[19]. الاحتيال الإلكتروني:

[18] مقناني، وسيم. وشبيلة، محمد.(2019). دور البيانات الضخمة في دعم التنمية المستدامة بالدول العربية. *مجلة دراسات وتكنولوجيا المعلومات*، 1(4)، ص 65.

[19] Abdel Razek، R. (2021). The Effect of Artificial Intelligence on Electronic Crime. *The Scientific Journal of King Faisal University.* Humanities and Management Sciences، 22(1), p. 430.

استخدام الإنترنت لتضليل الأفراد أو المؤسسات للحصول على أموال أو معلومات. أهمية الأمن السيبراني من منظور القانون الجنائي: الحفاظ على الأمن القومي: حماية البنية التحتية الحيوية للدولة من الهجمات السيبرانية. حماية الاقتصاد: حماية الشركات والمؤسسات من الخسائر المالية الناجمة عن الجرائم السيبرانية. حماية الخصوصية: ضمان حماية المعلومات الشخصية للأفراد من الاستخدام غير القانوني. الحفاظ على الثقة في الفضاء السيبراني: تعزيز الثقة في استخدام الإنترنت والأدوات الرقمية من خلال توفير بيئة آمنة.

4-2- الذكاء الإصطناعي كآليّة جرائم ضد حقوق الإنسان

يعد الذكاء الاصطناعي شكلاً من أشكال التكنولوجيا التي سعت البشرية منذ القدم للوصول إليها. فتخيلات البشر بتطوير آليات لها قدرة على التحليل، واتخاذ التصرفات الذاتية يعود إلى مئات السنين، وخلال القرن الواحد والعشرين انتقلنا من الخيال إلى الواقع[20]، وذلك بتطوير تقنيات قادرة على أداء أعمال بشكل ذاتي إلا أنها لا تزال في مراحلها الأولى. وكأي تطور في المجتمع الإنساني، فان هذه التقنيات التي تعمل بشكل مباشر وغير مباشر مع الأفراد لها إيجابياتها وسلبياتها، أي أنها توفر للبشر فرص جديده لتحسين حياتهم، وتمكينهم من الحصول على حياة كريمة بالحفاظ على حقوقهم الأساسية، وبالمقابل فإنها بحداثتها قد تشكل تحديات ومخاطر على حقوق الأفراد، وحرياتهم العامة أيضا.

وعلى الرغم من أهمية الذكاء الاصطناعي في عالم التكنولوجيا إلا أنه لا يوجد تعريف جامع مانع متفق عليه للذكاء الاصطناعي، إذ يعد الذكاء الاصطناعي مجالًا أكثر من كونه مفهوما يمكن تعريفه بسهولة (Andersen, 2018, p.8). فقد تعددت التعريفات المعتمدة للذكاء الاصطناعي تبعا للتخصص الذي تطورت فيه، فالذكاء الاصطناعي مستمد من مجالات أخرى غير علوم الكمبيوتر؛ كعلم النفس، وعلم الأعصاب، والعلوم المعرفية، والفلسفة، واللغويات، والاحتمالية، والمنطق، وعليه يمكن تقسيم الذكاء الاصطناعي كمجال معرفي إلى العديد من الحقول الفرعية المتقاطعة بشكل كبير، مثل التعلم الآلي والروبوتات، ومن ثم الشبكات العصبية والرؤية، وأيضًا معالجة اللغة الطبيعية ومعالجة الكلام.

يرى البعض أن التأثير السلبي للذكاء الاصطناعي على المجتمع البشري سيحدث تغييراً اجتماعياً ضخما يعطل الطريقة التي نعيش بها في المجتمع البشري تدريجياً. فمع التطور التدريجي للذكاء الاصطناعي، لن تكون هناك حاجة للجهود البشرية بحيث أنه يمكن القيام بكل شيء تقريبا ميكانيكيًا، ومن هنا يتخوف العديد من الأشخاص بأن البشر سيصبحون أكثر كسلا، ويتدهورون في النهاية إلى المرحلة التي يعودون فيها إلى شكلهم البدائي، فهم يتصورون بأن التواصل البشري سيتضاءل تدريجيًا حيث سيحل الذكاء الاصطناعي محل الحاجة للقاء الناس وجها لوجه لتبادل الأفكار؛ أي أن الذكاء الاصطناعي سيحد من التواصل البشري بين الناس بحيث لن تكون هناك حاجة للتجمع الشخصي للتواصل مما سيشوه العلاقات الاجتماعية البشرية بشكلها الحالي (Tai, 2020, p.341). ومن ناحية أخرى، ومع ازدياد وسائل التواصل الاجتماعي الافتراضي عوضا عن التواصل البشري، فإن مخاطر الاعتداء على حق الأفراد بالخصوصية، ولاسيما فيما يتعلق بالمعلومات الحساسة ستزداد بشكل مضطرد.[21]

بل ويذهب بعضهم إلى تقييم مخاطر الذكاء الاصطناعي في مواجهة الاقتصاد العالمي، كخطر استبدال العمالة البشرية بالآلات – وهو أمر واقعي كحال العديد من خطوط الصناعة لتجميع السيارات التي تعمل بالآلات والروبوتات – مما أجبر العمال التقليديين على

[20] Al-Khalidi، E. (2021). Governance of the use of artificial intelligence in judicial work: a legal reading of the European Ethical Charter on the Use of Artificial Intelligence (AI) in Judicial Systems and Their Environment (CEPEJ). *Journal of Sharia Research and Studies: Abdel Fattah Mahmoud Idris*، 10 (116)، 155.

[21] الاتحاد الأوربي، قواعد اخلاقيات الذكاء الاصطناعي، مجموعة القواعد والارشادات حول الكيفية التي يجب اتباعها من قبل الشركات والحكومات عند تطوير تطبيقات الذكاء الاصطناعي، الصادرة في ابريل 2019.

فقدان وظائفهم الذي سيتسبب بأزمة بطالة عالمية قد تمس الاقتصاد العالمي بشكل واسع (Osoba & Welser, 2017, p.2). وهذا سينشئ تفاوتاً في الثروة حيث سيحصل مستثمرو الذكاء الاصطناعي على الحصة الأكبر من الأرباح، وستتسع الفجوة بين الأغنياء والفقراء (Tai, 2020, p.340). فاتساع الفجوة الاقتصادية بين الأفراد سيتسبب بشكل مباشر وغير مباشر بانتهاكات واسعة لحقوق الإنسان، فالهشاشة على سبيل المثل ترتبط ارتباطاً وثيقاً بالفقر، فإذا ما اعتبرنا بأن الأشخاص الهشين هم أكثر عرضة لمخاطر انتهاك حقوقهم، فإننا سنوسع من دائرة الأفراد الأكثر عرضة للخطر بمجرد ازدياد الفقر، وعليه سيؤثر سلباً في الأمن الإنساني بمختلف نواحيه. وقد ركزت المبادئ التوجيهية بشأن الفقر المدقع وحقوق الإنسان على أنه لكل إنسان الحق في الغذاء والتغذية الكافيين، والحق بالسكن اللائق وغيرها من مظاهر حق الإنسان في الحياة والسلامة الجسدية، وذلك لضمان حياة كريمة للأفراد التي هي ركيزة منظومة حقوق الإنسان (OHCHR, 2012a, p.15).

هنالك أيضاً تخوف من بعض المخاطر المتصورة بشكل مستقبلي في حال تم التوصل فعلاً إلى تطوير النوع الفائق من الذكاء الاصطناعي بظهور مشكلات جديدة ليس فقط بالمعنى الاجتماعي، ولكن أيضًا في الذكاء الاصطناعي نفسه بحيث يصبح الذكاء الاصطناعي الذي يتم تدريبه وتعليمه على كيفية تشغيل مهمة معينة إلى خلق مشاكل وعواقب غير متوقعة في حال إدراك هذا الذكاء إلى إمكانيته في تجاوز تحكم البشر به، كأن تتجاهل الخوارزميات – التي تعمل في الأصل وفقًا لمسار خاص بها – الأوامر التي صممت من أجلها وتتصرف بشكل تلقائي مما قد يتسبب في تصرفات خطيرة أو متحيزة عنصريًا أو أن تتوجه ذاتياً نحو إيذاء أشخاص معينين أو أشياء بقصد أو دون قصد[22]. وهنا تظهر إشكالية الخوارزميات المتعلقة بالتعلم الذاتي التي يتم تصميمها لتحليل البيانات الضخمة للوصول الى فئات محددة من الأفراد دون غيرهم كأن يتم الإعلان عن وظائف معينه لفئات محددة من الأفراد، واستبعاد أخرى على أساس الجنس أو اللون أو الدين مثلا، وهذا كله فيه تكريس للتمييز وعدم المساواة.[23]

وقد ظهرت العديد من الإشكاليات القانونية المتعلقة بالذكاء الاصطناعي لتلامس مجموعة متنوعة من القضايا، بعض هذه الإشكاليات تعتبر واسعة التطبيق بينما يعد بعضها الآخر تحديات تمس قضايا محددة للغاية بطبيعتها. وعليه تمت دراسة هذه الإشكاليات القانونية بشكلها الشمولي كتلك المتعلقة بالشخصية القانونية، والملكية الفكرية، وحماية العمل والعامل، والبيانات الضخمة، والأمن السيبراني، والمسؤولية عن الأضرار والمساءلة والمراقبة، التي تم تناولها بحسب التخصص كتلك التي تتمركز في المواضيع المتعلقة بالرعاية الصحية أو الدفاع والحماية الأمنية. أما بالنسبة للقضايا القانونية ضيقة النطاق والخاصة بعمل الذكاء الاصطناعي؛ فقد تناولتها دراسات أكثر تعمقاً لتحليل الإشكاليات المتعلقة بالمرونة والإنصاف في صنع القرار، التحيز والتمييز، والقضايا المتعلقة بحق الخصوصية وحماية البيانات الحساسة.

وقد أدت هذه الإشكاليات القانونية إلى تجريم العديد من الأفعال المرتبطة بالذكاء الاصطناعي، فعلى سبيل المثال، قد يتم إساءة استخدام تقنية الذكاء الاصطناعي واستغلالها على نحو غير مشروع وذلك بقصد الإضرار بمصالح الأفراد والهيئات المختلفة وحتى الدول، فقد ساهم التطور التقني المستمر للذكاء الاصطناعي في استحداث أنماط وأشكال جديدة من الجرائم الإلكترونية أو ما يسمى بالجرائم المعلوماتية. تتنوع جرائم الذكاء الاصطناعي وتتعدد، وكل يوم يظهر نوع وتصنيف جديد لتلك الجرائم. بالإمكان تصنيف هذه الجرائم إلى تلك الماسة بالاعتداء على سلامة البيانات والمعلومات، ومن صورها التلاعب بالنظام المعلوماتي وإتلاف المعلومات، والجرائم الواقعة على البرامج، ومن صورها جريمة الاعتداء على البرامج التطبيقية أو على برامج الحاسب الآلي، والجرائم المعلوماتية الموجهة

[22] مبادرة IEEE العالمية حول أخلاق أنظمة الحكم الذاتي والذكاء، اخلاقيات التصميم: رؤية لأولويات رفاهية الانسان مع أنظمة التحكم الذكية والذاتية، الإصدار 2، 2017.

[23] يحيى الدهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات، 2019م، ص 54.

ضد الأشخاص أو الأموال أو الحكومات وغيرها من الجرائم.

جميع ما ذكر يؤثر بشكل أو بآخر في حقوق الأفراد وحرياتهم الأساسية ابتداءً من انتهاك حق الأفراد بالحياة الكريمة وحقهم بالغذاء الكافي والحصول على المياه الصالحة بعيدا عن الفقر المدقع، مروراً بحقهم في الحفاظ على خصوصيتهم وحقهم بالمساواة وعدم التمييز والانحياز باستخدام الخوارزميات، وانتهاءً بحق الأفراد في الحفاظ على أسلوب الحياة الذي يختارونه[24]. وبغض النظر عن تعددية الإشكاليات القانونية المتعلقة بالذكاء الاصطناعي، يعتقد البعض بأن المشكلة الأساسية تتمثل في أن تعقيد تقنيات الذكاء الاصطناعي يعني استحالة التعرف إلى المحركات التي تجعل تقنيات الذكاء الاصطناعي تؤدي المهام المنوطة بها تحديداً، فليس بإمكان الفرد تفنيد التفاصيل الدقيقة لهذه التقنيات أي التعرف عن كثب على مكوناتها والأجزاء التي تتحكم فيها وهي قيد التشغيل.

انطلاقا من إدراكنا لعلاقة الذكاء الاصطناعي بحقوق الإنسان، وتقييمنا لأهم الإشكاليات التي تضعها هذه التقنية على الأفراد وحقوقهم بشكل عام، فإنه لابد من إيجاد منظومة عامة لحوكمة عمل تقنية الذكاء الاصطناعي وتنظيم تطويرها على المستويين الدولي والوطني بما يواءم احترام القانون الدولي لحقوق الإنسان. فالتشريعات الدولية المعنية بحقوق الإنسان لا تخلو من القواعد العامة التي بالإمكان اللجوء إليها لتنظيم عمل تقنية الذكاء الاصطناعي على مختلف صورها برؤية محورها احترام هذه الحقوق وحفظها من الانتهاك.

5- دور الذكاء الإصطناعي في الوقاية الظرفية من الجرائم

الذكاء الاصطناعي هو المجال الذي يهدف إلى تمكين الآلات من محاكاة الذكاء البشري. على الرغم من وجود عدة تعاريفٍ للذكاء الاصطناعي، إلا أننا يمكننا تعريفه بشكلٍ بسيطٍ على أنه تقنيةٌ تمكّن الآلات من محاكاة قدرات البشر العقلية معتمدةً على تكامل علوم الكمبيوتر وتحليل البيانات لأداء مهامٍ معقدةٍ واتخاذ قراراتٍ باستخدام خوارزمياتٍ متقدمةٍ تعمل بسرعةٍ ودقةٍ عاليةٍ. في المجال القانوني، يمكن أن يساعد الذكاء الاصطناعي في تعزيز الكفاءة وخفض التكاليف من خلال أتمتة المهام الروتينية وتبسيط سير العمل. على سبيل المثال، يمكن أن يساعد الذكاء الاصطناعي في البحث القانوني وصياغة رسائل البريد الإلكتروني[25].

يلعب الذكاء الاصطناعي دوراً متنامياً في منظومة الوقاية الظرفية من الجرائم، باعتباره أداة قادرة على تحليل كمّيات هائلة من البيانات بشكل آني وتوقّعي، ومن ثمّ المساعدة في تقليص فرص ارتكاب الجريمة قبل وقوعها. في هذا الإطار، يمكن القول إنّ الذكاء الاصطناعي يعيد تعريف مفهوم "التقليل من الفرص" الذي يعد جوهر الوقاية الظرفية. فمثلاً، خوارزميات التنبؤ الإحصائي القائمة على التعلّم الآلي تستطيع رصد أنماط غير اعتيادية في تحركات الأشخاص أو المركبات داخل الفضاءات الحضرية، ومن ثمّ إصدار إنذارات استباقية تسمح للشرطة أو السلطات الأمنية بتكثيف التواجد الوقائي في مناطق بعينها، وهو ما يقلّص من احتمالية حدوث السلوك الإجرامي عبر الردع العلني ورفع الكلفة المتوقعة على الجاني[26].

كما يُسهم الذكاء الاصطناعي في تعزيز قدرات المراقبة والرصد، وهو أحد أهم عناصر الوقاية الظرفية. الأنظمة المبنية على "الرؤية الحاسوبية" قادرة على التعرف التلقائي على السلوكيات المشبوهة مثل ترك حقيبة في مكان عام أو محاولة التسلل إلى منشأة محمية. هذه القدرات تتجاوز الإمكانات البشرية التقليدية من حيث سرعة الاستجابة ودقة الملاحظة، مما يعني أن الذكاء الاصطناعي يعزز

[24] همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت، دراسة في قواعد القانون المدني الأوروبي الخاص بالروبوتات، مجلة جيل الأبحاث القانونية، العدد 21، ص 51.

[25] فايق عوضين، استخدامات تقنيات الذكاء الاصطناعي بين المشروعية وعدم المشروعية، المجلة الجنائية القومية، العدد 65، مارس 2022، ص 76.

[26] عماد عبد الستار، تطبيق السلاسل الزمنية في التنبؤ بأعداد المترددين على مكتبة كلية الآداب، جامعة كفر الشيخ، المجلة الدولية لعلوم المكتبات والمعلومات، مج8، ع4، 2021، ص 63.

وظيفة "الحارس الميكانيكي" الذي يراقب باستمرار ويُقلّص من فجوات الحماية. هنا يصبح تدخل الإنسان أكثر فاعلية لأنه يستند إلى معلومات دقيقة في الوقت الحقيقي، بدلاً من التشتت في المراقبة العامة الواسعة.

إلى جانب المراقبة، يوفر الذكاء الاصطناعي إمكانات متقدمة في إدارة المخاطر البيئية التي تغذي الجريمة. على سبيل المثال، عبر دمج بيانات الإضاءة الحضرية، الكثافة السكانية، مستويات الضوضاء، وأنماط التنقل، يمكن للأنظمة الذكية تحديد "النقاط السوداء" أو أماكن تمركز السلوكيات الانحرافية. وبناءً على ذلك، يمكن توجيه تدخلات هندسية أو تنظيمية مثل زيادة الإضاءة، تحسين تصميم الشوارع، أو تعزيز الوجود الأمني. هذه المقاربة تُترجم عملياً مبادئ نظريات الوقاية الظرفية مثل "الأنشطة الروتينية" و"الفرصة الإجرامية"، حيث يصبح الذكاء الاصطناعي بمثابة أداة لرسم خريطة الفرص وتقييدها[27].

ولا يقتصر دور الذكاء الاصطناعي على المجال الأمني الصرف، بل يمتد إلى تحليل الجرائم الاقتصادية والرقمية أيضاً. في قطاع التمويل، تعمل الخوارزميات على كشف المعاملات غير العادية والأنماط التي قد تشير إلى غسل أموال أو تمويل إرهاب، ما يقطع خطوط الإمداد المالي للشبكات الإجرامية قبل أن تتحول إلى وقائع ملموسة. وفي الفضاء السيبراني، يُستخدم الذكاء الاصطناعي لرصد محاولات الاختراق أو الاحتيال الإلكتروني، وبالتالي يُغلق "النوافذ" التي قد يستغلها المجرمون. كل ذلك يُعَد امتداداً لمفهوم الوقاية الظرفية في بيئة رقمية حيث الفرص الإجرامية آخذة في التزايد.

لكن إدماج الذكاء الاصطناعي في الوقاية الظرفية ليس خالياً من التحديات. فالاعتماد المفرط على الخوارزميات قد يثير إشكالات تتعلق بالتحيز والعدالة، إذ يمكن أن تُعيد الأنظمة إنتاج أنماط تمييزية متأصلة في البيانات التي تدربت عليها. كذلك فإن المراقبة الجماعية المدعومة بالذكاء الاصطناعي تطرح أسئلة حقوقية جدية حول الخصوصية وحماية البيانات الشخصية[28]. من منظور علم الإجرام، فإن تجاوز هذه المخاطر يتطلب إطاراً قانونياً وأخلاقياً واضحاً يضمن أن يظل الذكاء الاصطناعي أداة لتعزيز الوقاية الظرفية لا وسيلة لإضعاف شرعية النظام القانوني أو ثقة المواطنين.

في المحصلة، يمكن القول إن الذكاء الاصطناعي يمثل نقلة نوعية في مجال الوقاية الظرفية من الجرائم، إذ يوفر أدوات للتنبؤ، المراقبة، والتحكم البيئي تتجاوز الإمكانات البشرية التقليدية. غير أن الفعالية الحقيقية لهذه الأدوات تظل مشروطة بمدى قدرتها على التوازن بين الفاعلية الأمنية من جهة، وضمانات حقوق الإنسان والعدالة من جهة أخرى. بذلك، يصبح الذكاء الاصطناعي عنصراً تكاملياً في سياسات الوقاية من الجريمة، لكنه لا يغني عن الإصلاح المؤسسي، المشاركة المجتمعية، والرقابة القانونية المستقلة.

تطوّرت التدابير الوقائية الظرفية ضد الجرائم التكنولوجية على نحوٍ تراكمي يبدأ من منطق "تقليل الفرص" الذي صاغته مدرسة الوقاية الظرفية في علم الإجرام، وينتقل إلى فضاء التقنية حيث تُترجم مبادئها الخمسة (زيادة الجهد، زيادة المخاطر، تقليل العوائد، تقليل الاستفزازات، وإزالة الأعذار) إلى حلول هندسية وتنظيمية. في الموجة الأولى (عصر الحوسبة المؤسسية والشبكات المحلية)، ظهرت ضوابط الدخول والاعتماد، الفصل بين الصلاحيات، سجلات التتبع، والنسخ الاحتياطي، بوصفها وسائل تمنع تحقق الركن المادي لجرائم الاختلاس المعلوماتي أو الدخول غير المشروع عبر جعل الفعل أكثر كلفة وأعلى خطراً على الفاعل. وقد منح القانون الجنائي والسياسة الجنائية لهذه التدابير مشروعيةً بوصفها أدوات "وقائية قبلية" لا تمسّ قرينة البراءة متى التزمت الضرورة والتناسب، مع توظيف المسؤولية الجنائية للشخص المعنوي والحوافز الجزائية (كالتخفيف عند توافر برامج امتثال فعّالة) لدفع الفاعلين الاقتصاديين نحو تبنّيها.[29] ومع

[27] سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة، الجزائر، 2016، ص 133.
[28] أكرم بوليقرينات، حرمة الحياة الخاصة بين الحماية القانونية والشريعة" مجلة النوازل الفقهية القانونية، 1، 2017، ص 73.
[29] وسام، عواس، "مشروعية وسائل البحث الجنائي الحديثة". رسالة ماجستير، بقسم القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 2013- 2014 م، إشرف: د. لنوار عبد الرحيم، وعبد الله أوهايبة، ص 166.

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net
ISSN: 2663-5798 || Arab Journal for Scientific Publishing

ذلك، زامن هذا الطورَ توتّرٌ مفاهيمي بين الوقاية المشروعة والرقابة الشاملة، ما فرض وضع حدود إجرائية وموضوعية تحول دون تحوّل أدوات الحماية إلى وسائل مساسٍ غير مبرّر بالخصوصية والسرية المهنية.

في الموجة الثانية (انتشار الإنترنت والتجريم المعلوماتي الخاص)، انتقلت الوقاية الظرفية من أسوار التنظيم الداخلي إلى تخطيط البنية الشبكية ذاتها: الجدران النارية، التقسيم الشبكي وتقليل الثقة، أنظمة كشف/منع التسلل، التشفير وإدارة المفاتيح، وأنظمة التصفية والتبيّن (للتصيّد والبرمجيات الخبيثة). على المستوى القانوني، ارتبط هذا التحوّل بترسيخ "واجب العناية" و"حكومة المخاطر" على مزوّدي الخدمة والبنى التحتية الحيوية، وبتشريعات تُجرّم الأفعال على نحوٍ تقنيّ الدقة (الدخول غير المصرّح، الاعتراض غير المشروع، إتلاف البيانات)، وتسمح في المقابل بحيازة أدلة رقمية عبر سلاسل حفظٍ موثوقة. هنا تغدو التدابير الظرفية جزءاً من المنع البنيوي للجريمة: تقليل سطح الهجوم، تقليص الوقت اللازم للكشف، وزيادة احتمال التعرّف على الفاعل. غير أنّ الفرضية الشائعة بأن "المزيد من التقانة يعني جريمة أقل" لا تصمد دائماً؛ فهناك أثر الإزاحة (تحوّل الجناة إلى أهداف أو أدوات أخرى) وأثر التعويض (رفع الجناة لمهاراتهم)، مما يستلزم تداخلاً بين الوقاية الظرفية والتدابير الاجتماعية والقانونية (التجريم، الردع القضائي، والعدالة الإصلاحية) بدل الركون إلى الحلول التقنية وحدها.

الموجة الثالثة (الحوسبة السحابية، الأجهزة الذكية، والذكاء الاصطناعي) أعادت تعريف الوقاية الظرفية بوسائل أكثر ديناميكية: المصادقة المتعدّدة العوامل، انعدام الثقة الافتراضي، العزل الدقيق للأحمال، إدارة الثغرات المؤتمتة، تقنيات الخداع والفخاخ العسلية[30]، والاستجابة الممكّنة بالخوارزميات. قانوناً، أُدمجت هذه الأدوات في عقود الخدمة كالتزامات أداء، وفي معايير اعتمادٍ وتصديقٍ تُنتِج "قرينة امتثال" نسبية يمكن أن تؤثر في التكييف الجنائي وفي تقدير الجزاء على الكيانات المقصِّرة. لكن إدخال الذكاء الاصطناعي للكشف الشذوذي وفرز المخاطر يطرح إشكالات تفسيرية وإثباتية: كيف يُدقَّق نموذجٌ غير قابلٍ للتفسير؟ متى تُعدّ إنذاراته "أسباباً معقولة" لاتخاذ إجراء ماسّ بالحقوق (حجب حساب، تجميد معاملة)؟ وما حدود تفويض القرار الآلي في بيئات إنفاذٍ جنائي؟ الإجابة الرشيدة التي تتوافق مع مبدأ الشرعية تقتضي ربط أي تدبيرٍ وقائيٍّ ذكيٍّ بمتطلبات الشفافية القابلة للتدقيق، والتقييم الدوري لأثر الحقوق، وإشرافٍ بشري فعّال، مع عدم تحويل مقدّمي الخدمة إلى "شرطةٍ خاصة" بلا ضوابط؛ وإلا انزلقت الوقاية إلى خصخصةٍ غير خاضعة للمساءلة لوظائف الضبط الجنائي.

أخيراً، تكشف القراءة التاريخية النقدية أنّ فاعلية الوقاية الظرفية ضد الجرائم التكنولوجية مشروطةٌ بحوكمةٍ قانونيةٍ متعددة المستويات: (1) مستوى معياري يحدّد الغاية المشروعة ويُقيّد الوسيلة بمبادئ الضرورة والتناسب وعدم التمييز ؛ (2) مستوى مؤسسي يُحدّد المسؤوليات ويتيح المساءلة (مدنية وجنائية) ويكافئ الامتثال الحقيقي لا "مسرح الامتثال"؛ (3) مستوى إجرائي/إثباتي يضمن سلامة الدليل الرقمي، وقابلية إعادة الاختبار، والحفاظ على سلاسل الحيازة؛ و(4) مستوى تعاوني عابر للحدود لتبادل الاستخبارات الفنية دون المساس بالحقوق الأساسية. وبقدر ما تُصمَّم التدابير الظرفية على أنها "بُنى ثقة" (تصميم آمن منذ البدء، خصوصية منذ البدء، أقلّ امتياز، شفافية)، وتتقاطع مع أدوات غير تقنية (التثقيف، الحوافز الاقتصادية، سياسات الادعاء القائمة على المخاطر)، بقدر ما تُحدث "انتشار فوائد" يتجاوز الإزاحة ويقلّص فرص الإجرام فعلياً. أما الاعتقاد بإمكان بلوغ "مناعةٍ رقميةٍ كاملة" فمتوهَّم؛ المعيار الواقعي في علم القانون الجنائي هو خفض المخاطر النظامية بطريقة قابلة للقياس، وحفظ الشرعية الدستورية، وتجنب إنتاج مخاطرٍ جديدةٍ على الحرّيات باسم الوقاية.

[30] جميل، أحمد عادل و عثمان، عثمان حسين .(2012) *إمكانية استخدام تقنيات الذكاء الصناعي في ضبط جودة التدقيق الداخلي، دراسة ميدانية في الشركات المساهمة العامة الأردنية*] .ورقة بحثية]. المؤتمر العلمي السنوي الحادي عشر بعنوان "ذكاء الأعمال واقتصاد المعرفة" 2012. جامعة الزيتونة الأردنية، كلية الاقتصاد والعلوم الإدارية، عمان، الأردن، ص 187.

6- عمليات الذكاء الاصطناعي لتحديد المناطق المعرضة للجريمة والكشف عن الجريمة

أدّى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إحداث تحوّل عميق في أدوات تحليل الظاهرة الإجرامية، بحيث لم تعد الجريمة تُفهم باعتبارها واقعة فردية معزولة، بل بوصفها ظاهرة مكانية وزمانية واجتماعية يمكن دراستها والتنبؤ بها استنادًا إلى معطيات رقمية دقيقة. وقد أتاح هذا التحول إمكانات غير مسبوقة لتحديد المناطق الأكثر عرضة لوقوع الجرائم والكشف المبكر عنها، وهو ما أسهم في إعادة توجيه السياسة الجنائية من منطق التدخل اللاحق إلى منطق الوقاية والاستباق.

تعتمد عمليات الذكاء الاصطناعي في هذا المجال على جمع وتحليل كميات ضخمة من البيانات الجنائية والتكميلية، تشمل سجلات الجرائم السابقة، والبيانات المكانية، والمؤشرات الاجتماعية والاقتصادية، وأنماط الحركة والسلوك داخل الفضاءين المادي والرقمي. ومن خلال تقنيات التعلم الآلي، يتم تحليل هذه البيانات للكشف عن علاقات خفية بين المكان والزمن ونوع الجريمة، بما يسمح بتحديد مناطق تتسم بارتفاع احتمالية النشاط الإجرامي أو قابليته للتصاعد في المستقبل القريب.

ويُعدّ التحليل المكاني أحد الركائز الأساسية لهذه العمليات، حيث تُدمج البيانات الجنائية مع نظم معلومات جغرافية ذكية قادرة على إنتاج خرائط ديناميكية للمخاطر الإجرامية. ولا يقتصر هذا التحليل على تحديد مواقع الجرائم التي وقعت بالفعل، بل يتجاوز ذلك إلى رصد التحولات التدريجية في البيئة المحيطة، مثل تغير أنماط الاستخدام الحضري، أو تراجع الخدمات، أو ضعف البنية الأمنية، وهي عوامل تُسهم في خلق بيئة مواتية للجريمة. ومن منظور القانون الجنائي، يمثل هذا النهج أداة وقائية تتيح التدخل في مرحلة مبكرة دون المساس بمبدأ الشرعية الجنائية.

ولا تقتصر عمليات الذكاء الاصطناعي على توصيف المناطق المعرّضة للجريمة، بل تمتد إلى التنبؤ بتطور المخاطر الإجرامية. فالنماذج التنبؤية تعتمد على تحليل الاتجاهات السابقة وربطها بالمعطيات الراهنة، بما يسمح باستشراف احتمالات تكرار الجريمة في مناطق معينة أو انتقالها إلى مناطق مجاورة. ويكتسب هذا التنبؤ أهمية خاصة في توجيه الموارد الأمنية والقضائية توجيهًا عقلانيًا، قائمًا على تقدير المخاطر بدل الاعتماد على الانتشار العشوائي أو ردود الفعل المتأخرة.

وفي إطار الكشف عن الجريمة، تؤدي تقنيات الذكاء الاصطناعي دورًا محوريًا في رصد السلوكيات غير الطبيعية داخل المناطق عالية الخطورة. فكل نشاط إجرامي، سواء كان تقليديًا أو إلكترونيًا، يترك آثارًا رقمية أو سلوكية يمكن تحليلها آليًا، مثل أنماط حركة غير معتادة، أو تكرار نشاط مالي مشبوه، أو استخدام غير مألوف للبنية التحتية الرقمية. ويتيح الذكاء الاصطناعي الكشف عن هذه المؤشرات في الزمن شبه الحقيقي، مما يقلّص الفاصل الزمني بين وقوع الجريمة واكتشافها.

ومن الزاوية الجنائية، يُعدّ تقليص هذا الفاصل الزمني عنصرًا حاسمًا في تعزيز فعالية العدالة الجنائية، إذ يزيد من فرص ضبط الجريمة في مراحلها الأولى، ويحدّ من توسع آثارها، ويُضعف قدرة الجناة على الإفلات من المساءلة. كما يُسهم الكشف المبكر في حماية الضحايا المحتملين، وهو ما يعكس البعد الإنساني للسياسة الجنائية الوقائية.

وتكتسب عمليات الذكاء الاصطناعي أهمية خاصة في الكشف عن الجرائم المعقدة والمنظمة، التي تتسم بالتخفي والتشظي المكاني. فالجرائم المنظمة لا ترتبط دائمًا بمكان واحد، بل تعتمد على شبكة من الأنشطة المتداخلة. ويتيح الذكاء الاصطناعي تحليل هذه الشبكات عبر ربط البيانات المتفرقة، وكشف العلاقات بين الأشخاص والأماكن والوسائط، بما يسمح بفهم البنية الإجرامية الكامنة وراء الأفعال الظاهرة. ومن ثم، لا يقتصر الكشف على الفعل الإجرامي ذاته، بل يمتد إلى النظام الذي يُنتجه ويعيد إنتاجه.

كما يُسهم الذكاء الاصطناعي في تحليل العوامل الاجتماعية والاقتصادية المرتبطة بتمركز الجريمة في مناطق معينة، مثل الفقر، والبطالة، والهشاشة العمرانية، والحرمان الرقمي. ويُعدّ هذا التحليل أساسًا لتكامل السياسة الجنائية مع السياسات الاجتماعية والتنموية، بما يحقق مقاربة شمولية لمكافحة الجريمة لا تقتصر على المعالجة الأمنية أو العقابية.

ومن منظور الإجراءات الجنائية، يوفّر الذكاء الاصطناعي أدوات متقدمة لدعم التحقيق في المناطق المعرّضة للجريمة، من خلال تحليل الأدلة الرقمية، ومقاطع المراقبة، وسجلات الاتصالات، بما يُسرّع عملية الكشف ويُقلل من الاعتماد على التقدير البشري الفردي. غير أن هذا الدور يظل مشروطًا باحترام الضمانات القانونية، ولا سيما ما يتعلق بحماية الخصوصية، وشرعية جمع الأدلة، وإمكانية الطعن في النتائج المستخلصة آليًا.

وتنعكس هذه العمليات على السياسة الجنائية في صورة انتقال واضح نحو العدالة الوقائية، حيث يُعاد تعريف وظيفة أجهزة إنفاذ القانون من مجرد ملاحقة الجريمة إلى إدارتها استباقيًا. ويُسهم هذا التحول في تعزيز مبدأ التناسب في التدخل الجنائي، إذ يتم توجيه الجهد نحو المناطق الأكثر احتياجًا للحماية، بدل تعميم التدخل على المجتمع بأسره.

غير أن استخدام الذكاء الاصطناعي في تحديد المناطق المعرّضة للجريمة والكشف عنها يثير إشكالات قانونية دقيقة، أبرزها خطر الوصم المكاني، أي ربط مناطق معينة بالجريمة على نحو دائم، بما قد يؤدي إلى تمييز غير مشروع ضد سكانها. كما تبرز مخاطر التحيز الخوارزمي الناتج عن بيانات غير متوازنة أو تاريخية، وهو ما قد ينعكس سلبًا على العدالة والمساواة أمام القانون. ومن ثم، يتطلب هذا الاستخدام إطارًا قانونيًا وأخلاقيًا صارمًا يضمن المراجعة الدورية للنماذج، وشفافية المعايير، وخضوع القرارات المدعومة بالذكاء الاصطناعي للرقابة القضائية.

وخلاصة القول، إن عمليات الذكاء الاصطناعي في تحديد المناطق المعرّضة للجريمة والكشف عنها تمثل تطورًا نوعيًا في أدوات السياسة الجنائية المعاصرة، إذ تتيح قراءة علمية دقيقة للفضاء المكاني والسلوكي للجريمة، وتعزز من فعالية الوقاية والكشف المبكر، وتسهم في ترشيد التدخل الجنائي. غير أن نجاح هذا الدور مرهون بإدماجه ضمن منظومة قانونية متوازنة، تضمن أن تظل التكنولوجيا في خدمة العدالة الجنائية، لا بديلًا عنها أو مصدرًا للمساس بحقوق الإنسان وحرياته الأساسية.

النتائج

إنّ استخدام الذكاء الصناعي له مزايا عديدة في القانون والقضاء نذكر منها: أ) انه مساعد افتراضي للقضاة والمدعين والمحامين ففي امركا والدول المتقدمة ادت اتمتة القوانين والقضايا والقرارات الى جعلها كنزا للمعلومات يلجا اليه القضاة عند عرض واقعة معينة امامه بسبب الية البرامج المعتمدة في تغذية الذكاء الصناعي للربورتات التي امتلكت القدرة الهائلة على الجمع بين الضروف المتشابهة في القضايا المتماثلة والخروج بنتائج تعرض على القضاة الذين يعتمدون هذا النظام ففي احدى التجارب التي اجرية في الولايات المتحدة الامركية تمكنت هذه الربورتات خلال فترة قصيرة من الخروج بنتائج معينة من خلال المطابقة بين 750000الف قضية حسمها القضاء واصدر فيها قراراته وهذه النتائج استشارية وليست الزامية وهي تمكن القاضي من اجراء التحليل الدقيق لضروف الواقعة المعروضة امامه وادلتها وصولا الى اصدار حكم عادل فيها .ب) ان استخدام الذكاء الصناعي يسرع من اجرأت التقاضي ويختزل الجهد والوقت والنفقات المطلوبة لحسم الدعوى وهذا بدوره ينعكس ايجابا على عملية الترافع امام المحاكم ويسهم في ضمان استقرار القضاء. ج) الغاية من اعتماد الذكاء الصناعي تتمثل قي ايجاد نظام متكامل للمعلومات القانونية والقضائية يمكن القضاة والمحامين اللجوء اليها والافادة منها في اسرع وقت ممكن لان الرجوع لهذه المعلومات يستغرق وقتا طويلا مما يؤدي الى تكرار تاجيل القضايا المنظورة امام القضاء وتراكم الدعاوى من جهة واطالت امد النزاع وما له من اثار سلبية لايحمد عقباها من جهة اخرى وهو ما تعاني منه الانظمة القضائية التي لم

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net
ISSN: 2663-5798 || Arab Journal for Scientific Publishing

تعتمد الذكاء الصناعي في جميع مفاصل العملية القضائية ومنها النظام القضائي لدينا في العراق. ويتجلى **الذكاء الصناعي** في أداء الجهاز الإداري للقضاء وفي أداء القضاة والمحامين والمحضرين. إن وجود الذكاء الاصطناعي يمكن أن يقضي على العديد من الوظائف غير الضرورية وينقل الموارد البشرية المتخصصة والتقدير القضائي نحو قدر أكبر من الكفاءة والسرعة والدقة، مما سيؤدي في نهاية المطاف إلى زيادة رضا المترددين على النظام القضائي وتحقيق عدالة أفضل.

هدفت الدراسة البحث عن النقاط الآتية: 1) تحديد الآليات الوقائية التي يوفرها الذكاء الاصطناعي في مجال الأمن السيبراني، 2) تصميم تدابير مراقبة دقيقة، وإدارة البيانات بشكل صحيح، وتطوير القوانين والأطر الأخلاقية المناسبة لكيفية منع الجريمة من خلال الذكاء الاصطناعي، 3) تقييم الموقف التشريعي لبعض الدول العربي منها العراق تجاه تنظيم استخدام الذكاء الاصطناعي في الوقاية من الجرائم الإلكترونية، 4) كشف أوجه النقص أو القصور القانوني في كلا النظامين فيما يتعلق باستخدام الذكاء الاصطناعي، 5) اقتراح تعديلات أو إضافات قانونية تعزز من قدرة الدولتين على الاستفادة من الذكاء الاصطناعي في إطار قانوني يحفظ الحقوق ويمنع الانتهاكات.

أصبحت الذكاء الاصطناعي ذات أهمية متزايدة في التحقيقات الجنائية والوقاية من الجريمة للتحليل واتخاذ القرار والمعالجة، ومكّن من الوصول السريع والفعال إلى المعلومات الموجودة، بما في ذلك سجلات بصمات الأصابع، واختبارات الحمض النووي، والتعرف على وجوه المشتبه بهم، وتخزين المعلومات ونقلها، وتحليل البيانات في الخوارزميات، مما يساهم بشكل كبير في أداء الشرطة واتخاذ القرار في مجال الوقاية من الجريمة والتخطيط الحضري والتعامل مع المجرمين. إن تطبيق الذكاء الاصطناعي بشكل عام من شأنه أن يخلق تطورات هائلة ومرغوبة في النظام القضائي للدول والتحقيقات الجنائية. في ظل تزايد الصراعات والمشاكل التي تواجه البشر في مجتمعات اليوم بسبب متطلبات أنماط الحياة الحديثة، سواء على مستوى القضايا القانونية أو المهنية أو الجنائية، فإن العاملين في النظام القضائي من البشر لا يستطيعون الاستجابة للحجم الهائل من الإحالات واتخاذ القرارات المبنية على البيانات الوفيرة المتاحة اليوم.

القانون العراقي لا يتضمن حتى الآن تشريعًا خاصًا ومباشرًا ينظم استخدام الذكاء الاصطناعي، لكن يمكن تطبيق العقوبات في حال إساءة استخدام الذكاء الاصطناعي تحت مظلة: قانون مكافحة الجرائم المعلوماتية العراقي (مسودة): ما زال مشروعًا لم يُقر نهائيًا، لكنه يتضمن عقوبات تصل إلى السجن والغرامة بحق من يرتكب جرائم باستخدام الوسائل التقنية الحديثة مثل: اختراق الأنظمة، انتهاك الخصوصية، نشر البرمجيات الخبيثة، التجسس الإلكتروني. يُطبّق في حال ترتبت نتيجة عن استخدام الذكاء الاصطناعي تمس الأمن العام، أو تُشكّل انتهاكًا لحقوق الأفراد، خاصة إذا اقترن الفعل بنتائج جرمية واقعية (نصب، احتيال، تشهير... إلخ).

المصادر

الاتحاد الأوربي، قواعد اخلاقيات الذكاء الاصطناعي، مجموعة القواعد والارشادات حول الكيفية التي يجب اتباعها من قبل الشركات والحكومات عند تطوير تطبيقات الذكاء الاصطناعي، الصادرة في ابريل 2019.

الأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، مجلة القانون والعلوم البيئية، المجلد2، العدد2، 2023م.

أكرم بوليقرينات، حرمة الحياة الخاصة بين الحماية القانونية والشريعة" مجلة النوازل الفقهية القانونية، 1، 2017.

أوسندي أ.أوشوبا، ووليليام ويسلر الرابع، "مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل". (مؤسسة RAND كليفورنيا، الولايات المتحدة الأمريكية، 2017م).

تركي، منى كامل، "دور تكنولوجيا النانو في الكشف عن الجريمة، وحجّيّتها كدليل أمام القضاء". تقديم: مصطفي الفوركي، (مجلة القانون والأعمال الدولية، 33، سلسلة الأبحاث الجامعية والأكاديمية، 2020م).

جميل، أحمد عادل و عثمان، عثمان حسين .(2012) *إمكانية استخدام تقنيات الذكاء الصناعي في ضبط جودة التدقيق الداخلي، دراسة ميدانية في الشركات المساهمة العامة الأردنية*] .ورقة بحثية]. المؤتمر العلمي السنوي الحادي عشر بعنوان "ذكاء الأعمال واقتصاد المعرفة" 2012. جامعة الزيتونة الأردنية، كلية الاقتصاد والعلوم الإدارية، عمان، الأردن.

الحضيري، الحسن الطيب عبد السلام الأسمر، "الاثبات الجنائي بالوسائل العلمية الحديثة – دراسة مقارنة بين القانون الجنائي الليبي والفقه المعاصر". رسالة ماجستير، بقسم الشريعة والقانون، كلية الدراسات العليا، جامعة مولانا إبراهيم الإسلامية الحكومية مالانج، إشراف: د. محمد عبد الحميد، العام الجامعي 2016م.

خليفة، محمد محمد طه (2018). الذكاء الاصطناعي في ميزان التشريع .*مجلة دبي القانونية*، (28).

دولي الخضر، ناصري نفيسة، دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، مجلة المؤشر للدراسات الاقتصادية، المجلد 2، العدد 2، 2018م

سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة، الجزائر، 2016.

سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة، جامعة عجمان، الإمارات العربية المتحدة، 2020م.

عبدالله أحمد مطر الفلاسي، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، دون دار نشر، دون سنة نشر.

عماد عبد الستار، تطبيق السلاسل الزمنية في التنبؤ بأعداد المترددين على مكتبة كلية الآداب، جامعة كفر الشيخ، المجلة الدولية لعلوم المكتبات والمعلومات، مج8، ع4، 2021.

عمار ياسر زهير البابلي، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الأمن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد 1، 2021م.

عوضين، فايق، "استخدامات تقنيات الذكاء الاصطناعي بين المشروعية وعدم المشروعية". (المجلة الجنائية القومية 1، القاهرة: مجلة ربع سنوية تصدر عن المركز القومي للبحوث الاجتماعية والجنائية، مجلد 65 –مارس 2022م).

مبادرة IEEE العالمية حول أخلاق أنظمة الحكم الذاتي والذكاء، اخلاقيات التصميم: رؤية لأولويات رفاهية الانسان مع أنظمة التحكم الذكية والذاتية، الإصدار 2،2017.

مقناني، وسيم. وشبيلة، محمد.(2019). دور البيانات الضخمة في دعم التنمية المستدامة بالدول العربية. *مجلة دراسات وتكنولوجيا المعلومات*، 1(4).

همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت، دراسة في قواعد القانون المدني الأوروبي الخاص بالروبوتات، مجلة جيل الأبحاث القانونية، العدد 21.

وسام، عواس، "مشروعية وسائل البحث الجنائي الحديثة". رسالة ماجستير، بقسم القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 2013– 2014 م، إشرف: د. لنوار عبد الرحيم، وعبد الله أوهايبة.

يحيى الدهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات، 2019م.

Abdel Razek، R. (2021). The Effect of Artificial Intelligence on Electronic Crime. *The Scientific Journal of King Faisal University.* Humanities and Management Sciences، 22(1).

Al-Khalidi، E. (2021). Governance of the use of artificial intelligence in judicial work: a legal reading of the European Ethical Charter on the Use of Artificial Intelligence (AI) in Judicial Systems and Their Environment (CEPEJ). *Journal of Sharia Research and Studies: Abdel Fattah Mahmoud Idris*، 10 (116).

Dahshan, Y. (2020). Criminal Responsibility for Artificial Intelligence Crimes. *Sharia and Law Journal*, 34(82).

Mpinga، E.، Bukonda N.، Qailouli S.، and Chastonay P. (2022). Artificial Intelligence and Human Rights: Are There Signs of an Emerging Discipline? A Systematic Review. *Journal of Multidisciplinary Healthcare*، 15، 235-246. https://doi.org/10.2147/JMDH.S315314

Narain، K.، Swami، A.، Srivastava، A.، and Swami، S. (2019). Evolution and control of artificial superintelligence (ASI): a management perspective. *Journal of Advances in Management Research*، 16(5), 698-714. https://doi.org/10.1108/JAMR-01-2019-0006

Osoba, O.A. and W. Welser IV. (2017). *The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica*، CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE237.html.

حقوق الطبع والنشر © 2026 محفوظة لـ: المجلة العربية للنشر العلمي(AJSP)