جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
Est. 1978

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

The Use of Artificial Intelligence in Security and Surveillance: An Analysis of International Practices and Anticipation of Future Challenges

استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية

عبد الرحمن كامل
كلية الحقوق، جامعة القاضي عيّاض، المملكة المغربيَّة

Abdulrahman Kamel
Faculty of Law, Cadi Ayyad University, Kingdom of Morocco

Received on 13 Feb. 2025; accepted on 14 Apr. 2025; available online on 24 June 2025

Abstract

The study aimed to analyze the role of AI in enhancing security and surveillance by reviewing leading international practices, with a focus on the legal and ethical challenges facing its applications. The study addressed the issue of the balance between the use of AI to achieve effective security and respect for privacy and individual rights. The descriptive-analytical approach was used to analyze international experiences such as the United States, China, and the United Arab Emirates in security AI applications. The results found that AI contributes to improving the efficiency of security systems through the speed and accuracy of data analysis, but it faces challenges related to privacy violations and lack of cyberinfrastructure in some countries, and the study showed the importance of international cooperation to develop joint strategies. The most important recommendations included developing legislation regulating the use of AI, improving cyberinfrastructure, training security personnel, strengthening international cooperation and developing ethical standards.

Keywords: *security studies, artificial intelligence, security and surveillance, security applications, international practices, data security*

المستخلص

هدفت هذه الدراسة إلى تحليل دور الذكاء الاصطناعي في تعزيز الأمن والمراقبة من خلال استعراض الممارسات الدولية الرّائدة، مع التركيز على التحدّيات القانونية والأخلاقية التي تواجه تطبيقاته. وقد تمّ تناول مشكلة التوازن بين استخدام الذكاء الاصطناعي لتحقيق أمن فعّال واحترام الخُصوصية والحقوق الفردية. واعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل تجارب دولية؛ مثل: الولايات المتحدة الأمريكية والصين والإمارات في تطبيقات الذكاء الاصطناعي الأمني. وبيّنت النتائج أنّ الذكاء الاصطناعي يُسهم في تحسين كفاءة الأنظمة الأمنية من خلال سرعة تحليل البيانات ودقتها، لكنه يواجه تحديات تتعلّق بانتهاك الخُصوصية، وضعف البنية التحتية الإلكترونية في بعض الدول، كما أظهرت الدراسة أهمية التعاون الدولي لتطوير إستراتيجيات مشتركة. وشملت التوصيات الرئيسة وضع تشريعات تُنظِّم استخدام الذكاء الاصطناعي، وتحسين البنية التحتية الإلكترونية، وتدريب الكوادر الأمنية، بالإضافة إلى تعزيز التعاون الدولي وتطوير معايير أخلاقية.

الكلمات المفتاحية: الدراسات الأمنية، الذكاء الاصطناعي، الأمن والمراقبة، التطبيقات الأمنية، الممارسات الدولية، أمن البيانات

* Corresponding Author: *Abdulrahman Kamel*
Email: benkamel.immo@gmail.com

doi: 10.26735/CXSD7939

1. المقدمة

لقد أصبح الذكاء الاصطناعي في عصرنا الحالي أحد أكثر التقنيات تطوُّرًا وأهمية في مختلف المجالات، بما في ذلك الأمن والمراقبة، بسبب أنّ هذه التقنيات تُتيح القدرة على تحسين الكفاءة والفاعلية في عمليات المراقبة الأمنية، من خلال الأتمتة والتحليل المتقدم للبيانات، واتخاذ القرارات الذكية. وقد أحدثت هذه التكنولوجيا ثورة في كيفية رصد وتحليل الأنشطة، سواء أكانت في المدن الكبرى أو على الحدود أو في مواقع أخرى حيوية.

ويُعدُّ مجال الأمن والمراقبة من أهم المجالات التي استفادت بشكل كبير من تطبيقات الذكاء الاصطناعي، فالأنظمة الأمنية التقليدية تعتمد غالبًا على المراقبة البشرية، وهو ما يُشكل تحديات كبيرة في التعامل مع الكمّ الهائل من البيانات التي تحتاج إلى تحليل وتفسير، لكن بفضل هذه التقنيات أصبح بالإمكان تحليل كميات ضخمة من البيانات في وقت قياسي، والتنبُّؤ بالتهديدات الأمنية قبل وقوعها. وتتعدَّد التطبيقات في هذا المجال، ونجد من أبرزها أنظمة المراقبة بالفيديو المدعومة بالذكاء الاصطناعي التي تستطيع التعرُّف على الوجوه، وأيضًا تحليلات البيانات الضخمة لتحديد الاتجاهات الأمنية، وحتى مراقبة السّلوك في الأماكن العامة باستخدام كاميرات ذكية تراقب الحركة بشكل مستمر. كما أنَّ الذكاء الاصطناعي يسهم في تطوير الأنظمة الدفاعية؛ مثل: الطائرات المسيّرة التي يتم التحكم فيها بواسطة الخوارزميات الذَّكية لتنفيذ عمليات استطلاع ومراقبة في أماكن خطرة أو صعبة الوصول.

وبالرغم من هذه الفوائد، تبرز العديد من التحدّيات المستقبلية المتعلّقة باستخدام الذكاء الاصطناعي في الأمن والمراقبة، وعلى سبيل المثال: تُثير قضايا الخصوصية وحرّيات الأفراد مخاوف واسعة حول استخدام هذه التكنولوجيا بشكل مفرط أو دون رقابة. ويمكن أن تؤدي المراقبة الأمنية المستمرة إلى خرق الخصوصية الفردية، وتهديد حرية الأفراد. كما أنَّ هناك تحديات تقنية؛ مثل: دقة الخوارزميات في التنبّؤ بالمخاطر والتمييز بين الأنشطة الطبيعية والتهديدات الفعلية؛ ممَّا يفتح المجال للأخطاء، أو للاستخدام السيئ لهذه الأنظمة.

ومن ثمَّ من المهم إجراء تحليل لمختلف الممارسات الدولية في هذا المجال والنظر في التحدّيات المستقبلية التي قد تظهر نتيجة للتطوّرات التقنية السّريعة، ودراسة سُبل التغلّب عليها.

مشكلة الدراسة

بالرغم من التطوّر السّريع في استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة، فإنّ هذا الاستخدام يُثير تحدّيات مُعقّدة تتعلّق بالتوازن بين تعزيز الأمن، وضمان حماية الحقوق والحرّيات الأساسية، وما زال المجتمع الدولي يواجه نقصًا في القوانين والسياسات الموحَّدة لتنظيم هذه التقنيات، وهو ما أدَّى إلى تفاوت في الممارسات الدولية، وظهور تحديات جديدة مثل: إساءة الاستخدام، والتحيُّز في الخوارزميات والمخاطر الأخلاقية. ومن ثمَّ تتمثَّل المشكلة البحثية للدراسة في السؤال الرئيس الآتي:

كيف يُمكن تحقيق التوازن بين الاستفادة من الذكاء الاصطناعي في تعزيز الأمن والمراقبة وضمان احترام الحقوق والحرّيات الأساسية؟

تساؤلات الدراسة

تسعى الدراسة للإجابة عن التساؤلات الآتية:

- كيف يُستخدَم الذكاء الاصطناعي لتعزيز الأمن والمراقبة في السّياقات الدولية؟
- ما أبرز الممارسات الدولية الرّائدة في استخدام الذكاء الاصطناعي في الأمن والمراقبة؟
- ما التحدّيات القانونية والأخلاقية والتقنية المرتبطة باستخدام الذكاء الاصطناعي في الأمن والمراقبة؟
- كيف يُمكن استشراف المخاطر المستقبلية المرتبطة بهذه التكنولوجيا؟

أهمية الدراسة

لهذه الدراسة أهميتان: أولًا: أهمية نظرية تتمثَّل في الإسهام في سدِّ الفجوة المعرفية حول موضوع التوازن بين استخدام الذكاء الاصطناعي للأمن، وضمان حماية الحقوق الأساسية مع تحليل الممارسات الدولية. وثانيًا: أهمية تطبيقية تتمثَّل في النتائج والتوصيات العملية التي تتضمّنها، والتي تهدف من خلالها إلى دعم صانع القرار في تطوير سياسات وتنظيمات تتماشى مع التحديات المستقبلية. وبشكل أشمل، تسهم الدراسة في إثراء الأدبيات المتعلقة بالتقنيات الحديثة في قطاع الأمن، في ظل تزايد استخدام الذكاء الاصطناعي في مختلف المجالات الأمنية.

أهداف الدراسة

تهدف هذه الدراسة إلى الآتي:

- تحليل كيفية استخدام الذكاء الاصطناعي لتعزيز الأمن والمراقبة.
- استعراض الممارسات الدولية الرَّائدة واستخلاص الدروس المستفادة.
- تحديد التحديات الأخلاقية والقانونية والتقنية التي تواجه استخدام الذكاء الاصطناعي في الأمن والمراقبة.

- اقتراح حلول للتخفيف من المخاطر المستقبلية المرتبطة بهذه التكنولوجيا.

مفاهيم الدراسة

تتضمّن المفاهيم الأساسية التي تتناولها الدراسة: الذكاء الاصطناعي، الأمن، المراقبة، التحدّيات المستقبلية، وسيتمُّ تعريفها إجرائيًّا كخطوة منهجية، وفيما يلي عرض لمدلول كلٍّ منها:

- **الذكاء الاصطناعي**

يُشير الذكاء الاصطناعي إلى قدرة الأنظمة الحاسوبية على محاكاة العمليات الذهنية البشرية، مثل: التفكير والتعلُّم واتخاذ القرارات. وفي سياق الأمن والمراقبة، تُستخدم هذه التقنيات في معالجة وتحليل كميات ضخمة من البيانات بشكل آلي لاكتشاف الأنماط والتهديدات الأمنية، واتخاذ إجراءات استباقية (Russell and Norvig, 2016, p. 6).

- **الأمن**

يُشير الأمن إلى مجموعة التدابير والسياسات المعتمدة لحماية الأفراد والممتلكات والمعلومات من التهديدات المختلفة؛ مثل: الهجمات السيبرانية والإرهاب والجريمة، وفي سياق الدراسة يتضمَّن الأمن الوطني والحماية من الهجمات الإلكترونية وأمن المعلومات، والحفاظ على استقرار المجتمع والدولة باستخدام تقنيات حديثة؛ مثل: الذكاء الاصطناعي (Bertino and Sandhu, 2005, p. 20-21).

- **المراقبة**

المراقبة هي عملية جمع البيانات بشكل دوري أو مستمر لمتابعة وتحليل الأنشطة أو السُّلوكيات؛ بهدف تحقيق مستوى عالٍ من الأمن. وتتضمّن المراقبة في السّياق الأمني استخدام التكنولوجيا، مثل: كاميرات المراقبة وأجهزة الاستشعار وتحليل البيانات الضخمة، لمراقبة الأفراد وتحديد التهديدات والحفاظ على النظام العام (Zuboff, 2019, p. 105).

- **التحدّيات المستقبلية**

تُشير التحديات المستقبلية في هذه الدراسة إلى العقبات أو المشكلات المحتملة التي قد تواجه الدول أو المؤسّسات في استخدام تقنيات الذكاء الاصطناعي في مجالات الأمن والمراقبة، وتشمل هذه التحدّيات التوازن بين ضمان الأمن واحترام الخصوصية، وتعزيز دقة الأنظمة الذكية ومواجهة التهديدات السّيبرانية الجديدة، إضافةً إلى قضايا القوانين والتنظيمات المتعلقة باستخدام الذكاء الاصطناعي في المراقبة.

2. الدراسات السّابقة

هدفت دراسة (العموش والعبدولي، 2023) إلى تحديد تقنيات الذكاء الاصطناعي المتاحة وربطها بعلم الجريمة للاستفادة منها في تحليل الجرائم وأنماطها، كما هدفت إلى إبراز أهمية هذه التقنيات في تقليل الوقت اللازم لتحليل الجرائم وتتبُّع مواقعها. وتمّ التوصل إلى أنَّ هذه التقنيات خاصة التعلُّم الآلي تُساعد في تتبُّع الجرائم وتقليل وقت تحليلها، كما توصلت إلى أنَّ نُذرة الموارد البشرية المؤهلة والتحديات المتعلِّقة بجمع البيانات، يعدان أكبر عائق في استخدام الذكاء الاصطناعي في التحليل الجُرمي في العالم العربي. وأخيرًا أوصت الدراسة بضرورة تعزيز التعاون بين الدول العربية من خلال إنشاء رابطة شرطية عربية لتبادل المعرفة والخبرات.

تناولت دراسة (أبو منصور، 2020) تطوّر تقنيات الذكاء الاصطناعي التي تُعدُّ إحدى ركائز الثورة الصناعية الرابعة، مع التركيز على تطبيقاتها في المجالات الأمنية والعسكرية، كما استعرضت الأبعاد الأمنية لتلك التقنيات؛ مثل: الروبوتات والطائرات المسيَّرة ونُظم القيادة والسّيطرة، بالإضافة إلى إبراز الفرص التي توفرها هذه التقنيات؛ مثل: تحسين سرعة اتخاذ القرار والتنبؤ بالتهديدات وتقليل المخاطر. وأوصت الدراسة بإنشاء مراكز بحثية متخصصة في الأمن والذكاء الاصطناعي، وتقنين استخدام هذه التقنيات لتجنُّب المخاطر الأخلاقية والقانونية، وأخيرًا تعزيز التعاون الدولي لضمان الاستخدام المسؤول.

استعرضت دراسة (البابلي، 2024) استخدام الذكاء الاصطناعي لتعزيز الأمن والاستخبارات من خلال تحليل البيانات الضخمة وتوظيف الخوارزميات الذَّكية، كما سلَّطت الضوء على كيفية استفادة الأجهزة الأمنية من الذكاء الاصطناعي للتنبُّؤ بالجرائم والإرهاب عبر تحليل البيانات الجغرافية وسجلات الاتصالات والمحتوى الإلكتروني. وناقشت التوازن بين الاستفادة من هذه التقنيات والالتزام بالمعايير الأخلاقية والخصوصية، وخَلُصت إلى أنَّ الاستخدام الأمثل لها يُمكن أن يُعزِّز الأمن السيبراني ويسهم في مواجهة التهديدات الإرهابية بكفاءة عالية، مع توفير رؤى استباقية لتحليل التحديات المستقبلية.

هدفت دراسة (الصويلح، 2023) إلى التعرُّف على مصادر الشّائعات والحروب النفسية عبر الإنترنت، واستعراض آليات استخدام الذكاء الاصطناعي لمكافحتها وتحليلها، بالإضافة إلى تطوير إستراتيجيات أجهزة الإعلام الأمني لتعزيز الوعي ضد المخاطر. وتمَّ التوصل إلى أنَّ الشّائعات تُمثِّل أداة قوية في التأثير على الرأي العام، ولها مخاطر

كبيرة على الأمن القومي، كما أظهرت الدراسة أنَّ تقنيات الذكاء الاصطناعي؛ مثل: التعلُّم الآلي والشبكات العصبية الاصطناعية، تُعدُّ أدوات فعَّالة في تصنيف الأخبار الزائفة والكشف عن الشَّائعات. ومن أهم توصيات الدراسة زيادة التعاون بين الحكومات وشركات التكنولوجيا لمكافحة الحروب النفسية الإلكترونية.

هدفت دراسة (Jada and others, 2024) إلى إجراء مراجعة منهجية للأدبيات لتقييم تأثير التقنيات القائمة على الذكاء الاصطناعي في الأمن السّيبراني المؤسّسي، وتحديد فاعليتها مقارنةً بأساليب الأمن السيبراني التقليدية، وذلك باستخدام مخطط تدفق PRISMA لتوجيه عملية المراجعة، حيث تمَّ تضمين المقالات التي راجعها النظراء من 2018 إلى 2023 من EBSCO Host وGoogle Scholar وScience Direct وProQuest وSCOPUS وتمَّ تجميع 73 مقالة. وكشفت النتائج أنّ الذكاء الاصطناعي يُمكن أن يؤثر على الأمن السيبراني طوال دورة حياته بالكامل؛ ممّا يؤدي إلى فوائد مثل: الأتمتة وذكاء التهديدات وتحسين الدفاع السيبراني. وفي المقابل، فإنه يجلب تحديات؛ مثل: الهجمات المعادية والحاجة إلى بيانات عالية الجودة، وهو ما قد يؤدي إلى عدم كفاءته، كما تؤكد هذه النتائج التأثير الإيجابي للذكاء الاصطناعي على الأمن السيبراني، وتعزيز الفاعليَّة والمرونة.

تستكشف دراسة (Mu and others, 2024) تطبيق تكنولوجيا الذكاء الاصطناعي في ضمان أمن العملات الرقمية، فمع ارتفاع نسبة تداولها، أصبح ضمان أمنها مصدر قلق بالغ الأهمية. وترى الدراسة إمكانية استخدام تقنيات الذكاء الاصطناعي، مثل: التعلُّم الآلي والتعلُّم العميق لتحديد التهديدات الأمنية في أنظمة العملات الرقمية ومنعها. بالإضافة إلى ذلك، تبحث الدراسة في كيفية تعزيز الذكاء الاصطناعي للتدابير الأمنية والتحكم في المخاطر على منصَّات تداول العملات الرقمية؛ ممّا يوفر رؤى حول أنظمة التنبيه بالمخاطر في الوقت الفعلي. ويتمثَّل الهدف النهائي في توفير أدوات نظرية جديدة لإدارة الاستقرار المالي في عملية استبدال العملة الرقمية بـ M0. ويُقدّم هذا المشروع محتوى البحث في الأجزاء الأربعة التي تشمل التصور العام ومسار التسليم والتكنولوجيا الأساسية وفقاعة العملة الافتراضية.

تناولت دراسة (Majed, 2024) موضوع بصمة الدماغ التي تُعدُّ إحدى التقنيات الحديثة التي تعتمد على الذكاء الاصطناعي في مجال قانون الأدلة الجنائية؛ حيث يمكن الحصول على معلومات الدماغ بدقة وموثوقية في الإجراءات الجنائية دون اللجوء إلى إجراءات أو أسئلة معقَّدة ومتعدّدة، ولا تُسبِّب إحراجًا للشخص أو حتى انتهاكًا لكرامته الإنسانية، كما أنها تُعطي نتائج فورية ودقيقة. كما تُعتبر تقنية BF من التقنيات المتقدّمة المتعلّقة بالأدلة العلمية العصبية، التي تعتمد بشكل كبير على الذكاء الاصطناعي، والتي يُمكن أيضًا من خلالها التعرّف على ما إذا كان المشتبه به أو المجرم لديه معلومات عن الجريمة أم لا. ويتم ذلك من خلال تصوير الدماغ بالرنين المغناطيسي (EEG) وفحص الإشارات الصادرة عنه، والتي تسمى p300. وتؤكد الدراسة أنه لا يُثبت اختبار تخطيط الدماغ بالموجات فوق الصوتية الإدانة أو البراءة، ولكنه يوفر معلومات بشأن ما هو مخزون في ذاكرة الشخص عن الجريمة، ويُمكن للقاضي استخدام هذه المعلومات عند الحكم في القضية المعروضة أمامه.

هدفت دراسة (Maheswari and others, 2023) إلى تقديم نظرة عامَّة حول أهمية وكيفية توظيف تقنيات الذكاء الاصطناعي في المراقبة بالفيديو ومعالجة الصور في التجربة الهندية. حيث تقدَّم المراقبة بالفيديو مجموعة واسعة من التطبيقات للحدِّ من الخسائر البيئية والاقتصادية، وهي من أكثر الوسائل فاعلية لضمان الأمن. كما ركزت الدراسة على أدوار المراقبة الذَّكية بالفيديو من حيث الكشف عن الأفعال الإجرامية ووصف مسرح الجريمة والكشف عن الوجوه وإحصاء الحشود، وما شابه ذلك؛ إذ تعتمد معظم عمليات المراقبة المدعومة بالذكاء الاصطناعي على الشَّبكات العصبية العميقة وتقنيات التعلُّم العميق باستخدام تحليل إطارات الفيديو كصور.

التعليق على الدراسات السابقة

قدَّمت الدراسات السابقة رؤى متعدِّدة حول كيفية تأثير الذكاء الاصطناعي في إستراتيجيات الأمن، لكنها ركزت بشكل رئيس على مجالات محدّدة مثل: الأمن السيبراني ومكافحة الإرهاب، كما تناولت بعض الدراسات التحديات الأخلاقية والتقنية المتعلقة باستخدام هذه التقنيات، ولكن لم تتطرّق بشكل كافٍ إلى تأثيرها الشّامل على جميع مجالات الأمن الوطني. ومن هنا فإنَّ هذه الدراسة تُقدّم إضافة نوعية من خلال دراسة تأثير الذكاء الاصطناعي على الإستراتيجيات الأمنية عامةً، مع التركيز على التحليل الشَّامل للأدوات الحديثة والتحديات الأخلاقية والقانونية.

3. منهج الدراسة

للإجابة عن المشكلة البحثية وتساؤلاتها الفرعية، تمَّ اعتماد المنهج الوصفي التحليلي الذي يُستخدم في دراسة الوضع الراهن للظواهر من حيث الخصائص والأشكال والعلاقات والعوامل المؤثرة، كما أنه يُتيح

التنبُّؤ بمستقبل هذه الظواهر والأحداث (المحمودي، 2015، ص 47)، وتم تطبيقه عبر تحليل الأدوات والتقنيات الحديثة للذكاء الاصطناعي والتعلُّم الآلي والبيانات الضخمة في مجال الأمن والمراقبة، وأيضًا مناقشة التحديات الأخلاقية والقانونية المرتبطة بتطبيق هذه التقنيات في صنع القرار الأمني. إضافة إلى ذلك سيتم أيضًا تطبيق المنهج المقارن لدراسة الممارسات الدولية واستخلاص أوجه التشابه والاختلاف بينها.

3. 1 أدوات جمع البيانات والمعلومات

تمَّ جمع بيانات ومعلومات الدراسة بالاعتماد على المراجعة الوثائقية عبر تحليل الدراسات الأكاديمية والتقارير الأمنية والمقالات التحليلية المتعلّقة بتطبيقات الذكاء الاصطناعي في الأمن والمراقبة.

حدود الدراسة

اعتمدت الدراسة على مجموعة من الحدود تتمثَّل في الآتي:

- **الحدود الموضوعية:** تقتصر الدراسة على تطبيقات الذكاء الاصطناعي في القطاع الأمني دون التطرُّق إلى تطبيقاته في القطاعات الأخرى.
- **الحدود الجغرافية:** تُركِّز الدراسة على تطبيقات الذكاء الاصطناعي في الأمن الوطني والدولي، مع الاهتمام بالدول التي بدأت بالفعل في دمج هذه التقنيات في إستراتيجياتها الأمنية، مثل: الصين، الولايات المتحدة الأمريكية، بريطانيا، فرنسا، دولة الإمارات.

4. الإطار النظري للدراسة

اعتمدت الدراسة على نظرية الخصوصية وحماية البيانات التي تركِّز على حق الأفراد في حماية معلوماتهم الشَّخصية. وفي السِّياق الأمني، يُثير استخدام الذكاء الاصطناعي في المراقبة قضايا تتعلَّق بجمع البيانات الشَّخصية وتحليلها، ومن ثمَّ فإنَّ حماية الخصوصية تُصبح محورية.

وسيتمّ تطبيق هذه النظرية في الدراسة من خلال استكشاف كيفية تحقيق التوازن بين استخدام الذكاء الاصطناعي في الأمن والمراقبة وحماية الخُصوصية، مع دراسة جوانب التشريعات والسِّياسات المتعلّقة بهذا المجال.

4. 1 الممارسات الدولية لاستخدام الذكاء الاصطناعي في الأمن والمراقبة والدروس المستفادة

يتناول هذا المحور من الدراسة أبرز تطبيقات استخدام الذكاء الاصطناعي عبر مجموعة من الدول المختلفة في مجالات الأمن والمراقبة، ومن خلاله سيتم استعراض الابتكارات الرئيسة في هذه المجالات، إضافةً إلى التحديات التي تواجه تطبيق هذه التقنيات، وسُبُل معالجتها من خلال إستراتيجيات مبتكرة. ويعكس التنوّع في التطبيق والتحدّيات لدى الدول المختلفة، تبنيها للذكاء الاصطناعي في سياقاتها الأمنية المحلية، كما يُسلّط هذا المحور الضوء على كيفية توافق هذه التقنيات مع البيئة السياسية والاجتماعية لكل دولة.

4. 2 تحليل الممارسات الدولية الرَّائدة في استخدام الذكاء الاصطناعي للأمن والمراقبة

يتمثَّل التحليل الفعَّال للمُمارسات الدولية الرائدة في استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة، في دراسة التجارب التي تبنَّت هذه التقنيات لتعزيز فاعليَّة وكفاءة أنظمتها الأمنية. وتعكس هذه الممارسات التقدُّم الكبير في مجالات؛ مثل: المراقبة الجماعية ومكافحة الإرهاب وتحليل البيانات الاستخباراتية، فضلًا عن استخدام الطائرات المسيَّرة وأنظمة التعرُّف على الوجه. ومن خلال استعراض هذه الممارسات يُمكن استخلاص الدروس المستفادة وتحديد الابتكارات التي أسهمت في تطوير الأمن العام.

يُظهر الجدول التالي كيف تطوّر استخدام تقنيات الذكاء الاصطناعي في عدَّة مُمارسات دولية وإقليمية في مجالات الأمن والمراقبة، مع تباين واضح في التطبيقات والابتكارات والتحدّيات والإستراتيجيات المتّبعة. إذ تسعى كل دولة إلى الاستفادة من هذه التقنيات في سياقات أمنية محلّية خاصّة بها، مع التركيز على ابتكارات تُواكب احتياجاتها السياسية والاجتماعية.

كما يتبيَّن من خلال الجدول أيضًا أنَّ الولايات المتحدة الأمريكية تُركِّز بشكل كبير على تحليل البيانات الاستخباراتية والأنظمة الذاتية مثل: الطائرات المسيّرة، وهي تسعى لمواكبة التحدّيات المرتبطة بالخصوصية وحقوق الإنسان عبر شراكات بين القطاعين العام والخاص، كما تُظهر هذه التجربة التوازن بين التطوّر التكنولوجي والاستثمارات الضخمة في البحث والتطوير لمواجهة التهديدات المتزايدة (McKew, 2019, p. 46-47) . في حين تذهب الصين إلى المراقبة الجماعية باستخدام تقنيات مثل: التعرُّف على المشاعر، وهو ما يُثير قضايا أخلاقية كبيرة على المستوى الدولي، وتتركز الإستراتيجيات الصينية حول تطوير البنية التحتية التقنية وتوسيع تطبيقات الأمن الداخلي، وهو ما يعكس التوجه نحو السّيطرة الكاملة في مراقبة مواطنيها (Chen & Li, 2021, p. 524). وقد تعرّضت هذه الممارسات لانتقادات حادّة من المجتمع الدولي؛ حيث عُدت انتهاكًا للحريات الفردية، وهو ما دفع بعض الشركات التكنولوجية إلى إعادة النظر في استخدام هذه التقنيات. أمّا بريطانيا فإنها تُركز على

جدول 1 تطبيقات الذكاء الاصطناعي في مجالات الأمن والمراقبة

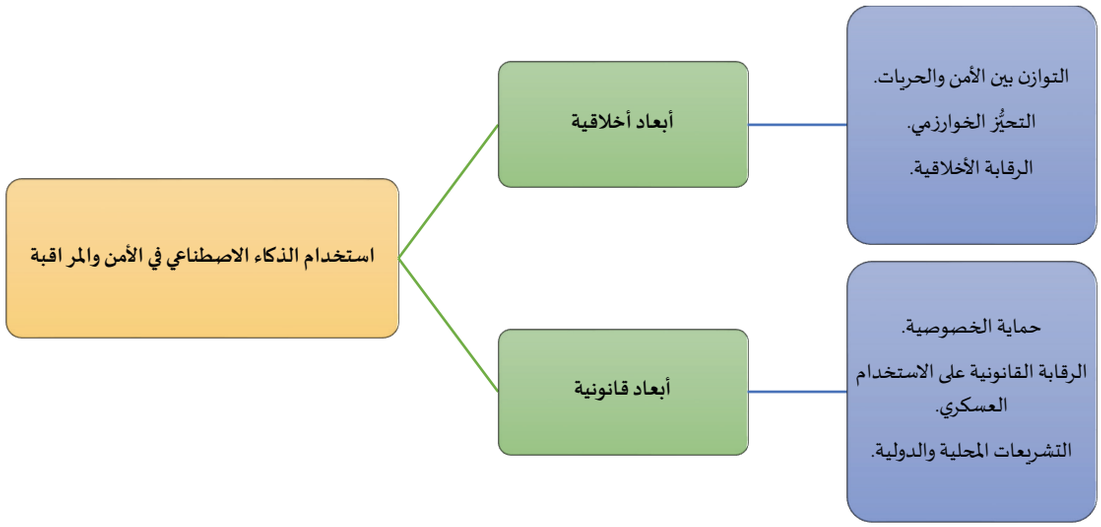
Table 1 Artificial intelligence applications in the fields of security and surveillance

الدول	مجالات التطبيق	أبرز الابتكارات	التحدّيات	الإستراتيجيات
أمريكا	- تحليل البيانات الاستخباراتية. - المراقبة والكشف عن التهديدات. - الأنظمة الذاتية (الطائرات المسيّرة).	- أنظمة تحليل التهديدات في الوقت المناسب. - الطائرات المسيَّرة العسكرية. - نظام التعرّف على الوجه.	- قضايا الخصوصية وحقوق الإنسان. - الاعتماد المفرط على التكنولوجيا.	- شراكات بين القطاعين العام والخاص. - استثمارات ضخمة في البحث والتطوير.
الصين	- المراقبة الجماعية. - مكافحة الجرائم الإلكترونية. - التنبّؤ بالسلوك الإجرامي.	- شبكة المراقبة باستخدام الذكاء الاصطناعي. - تقنية التعرّف على المشاعر.	- قضايا أخلاقيات الاستخدام. - انتقادات دولية بشأن الخصوصية.	- تطوير البنية التحتية التقنية. - توسيع نطاق تطبيقات الأمن الداخلي.
بريطانيا	- مكافحة الإرهاب. - حماية البنية التحتية. - تحليل البيانات الجنائية.	- أنظمة التعرّف على الوجه في الأماكن العامَّة. - أنظمة التنبُّؤ بالجرائم.	- قضايا الثقة بين المواطنين والدولة. - نقص الكفاءات التقنية.	- التعاون مع الجامعات والمؤسسات الأكاديمية. - إشراك المجتمع المدني في تطوير السياسات.
فرنسا	- مكافحة الإرهاب. - حماية الأماكن العامة. - إدارة الأزمات والكوارث.	- تطبيقات تحليل الحشود والجماهير. - الروبوتات المخصّصة للبحث والإنقاذ.	- ارتفاع تكاليف التطوير. - تحديات التنسيق بين المؤسسات الأمنية.	- تعزيز التعاون الأوروبي. - إطلاق مبادرات وطنية للذكاء الاصطناعي.
دولة الإمارت	- إدارة المدن الذكية. - المراقبة وحفظ الأمن. - التنبُّؤ بالجرائم.	- منصّة «عين الشرطة» للتنبّؤ بالجريمة. - استخدام الروبوتات في الدوريات الأمنية.	- القضايا المتعلقة بحوكمة البيانات. - التدريب على الأنظمة الجديدة.	- دعم رؤية 2030 الوطنية. - الاستثمار في التكنولوجيا الذكية عبر شراكات عالمية.

المصدر: الجدول من إعداد الباحث

مكافحة الإرهاب وحماية البنية التحتية مع استخدام أنظمة التعرُّف على الوجه والأنظمة التنبُّئية للجرائم (Amoore, 2020, p. 108-109). وبالرغم من فاعلية هذه الأنظمة في تعزيز الأمن العام فإن هناك تحديات تتعلق بالدقة والإنصاف، حيث وُجد أنه لديها معدّلات خطأ أعلى عند تحليلها لوجوه الأفراد غير البيض، وهو ما أثار عدَّة انتقادات حقوقية في العديد من تطبيقاتها؛ ممّا أدى إلى فرض قيود قانونية على استخدامها. وتسعى فرنسا إلى تطوير تقنيات لمكافحة الإرهاب وحماية الأماكن العامّة، مع استخدام الروبوتات في البحث والإنقاذ وتحليل الحشود الجماهيرية، لكنها تواجه ارتفاع تكاليف التطوير وصعوبة التنسيق بين المؤسَّسات الأمنية المتعدّدة، وتتمثّل إستراتيجياتها في تعزيز التعاون الأوروبي وإطلاق المبادرات الوطنية الخاصة بالذكاء الاصطناعي(Lemoine, C., & Dupont, 2021, p. 211) . وأخيرًا تبرز تجربة الإمارات العربية المتحدة كمثال على إدارة المدن الذكية والتنبُّؤ بالجرائم عبر تقنيات مثل: منصّة «عين الشرطة» التي تُتيح للمواطنين والمقيمين الإبلاغ الاستباقي عن أي خطر أمني كيفما كان، وتواجه هذه التجربة تحدّيات مثل: حوكمة البيانات، لكنها تسعى إلى دعم رؤية 2030 الوطنية عبر تعزيز الاستثمار في التكنولوجيا الذّكية وعقد شراكات عالمية (الديسي، 2018، ص. 105-106)، ونُضيف في هذا السّياق أنّ الذكاء الاصطناعي يُستخدم في تأمين المنشآت والهيئات الحيوية من خلال أنظمة المراقبة الذكية التي تعتمد على تحليل الصور والفيديوهات الحيَّة، وقد أسهم تطوير هذه الأنظمة الذكية للكشف عن التهديدات الأمنية في المطارات والمباني الحكومية في الرفع من مستوى الأمان بدولة الإمارات؛ حيث حلَّت في المركز الثاني عالميًا ضمن أكثر الدول أمانًا في العالم وفق تقرير عن تصوّرات الأمان صادر عام 2023م.

ويتبيَّن من كل ما سبق أنَّ الولايات المتحدة الأمريكية تتبنّى إستراتيجيات تعتمد بشكل كبير على الابتكار التكنولوجي واستخدام الأنظمة الذاتية مثل: الطائرات المسيّرة، لكنها تتعامل مع تحديات تتعلَّق بالخصوصية والاعتماد المفرط على التكنولوجيا. في حين تركز الصين ودولة الإمارات بشكل أكبر على المراقبة الجماعية واستخدام الذكاء الاصطناعي في الحفاظ على النظام العام، وهو ما يعكس اختلافات ثقافية وسياسية في مقاربة الأمن. أمَّا بريطانيا وفرنسا فتسعيان لتحقيق التوازن بين التكنولوجيا وحقوق الإنسان والتركيز على التعاون الدولي لمواجهة التحديات الأمنية.



شكل 1 الأبعاد القانونية والأخلاقية لاستخدام الذكاء الاصطناعي في الأمن والمراقبة

Figure 1 *Legal and ethical dimensions of using artificial intelligence in security and surveillance*

4 . 3 الأبعاد القانونية والأخلاقية في الممارسات الدولية

تُعدُّ الأبعاد القانونية والأخلاقية من القضايا الحيوية التي تبرز في تطبيقات الذكاء الاصطناعي في مجالات الأمن والمراقبة، ومع توسيع استخدام هذه التقنيات عالميًّا تَظهَر تحديات كبيرة تتعلّق بحماية حقوق الأفراد وضمان احترام الخصوصية في ظل التطوّرات السّريعة التي قد تتجاوز أحيانًا الأطر القانونية القائمة.

- **الأبعاد القانونية**

حماية الخصوصية: تعتمد تطبيقات المراقبة باستخدام الذكاء الاصطناعي بشكل كبير على جمع وتحليل البيانات الشخصية، على سبيل المثال: يتم في الصين استخدام شبكة المراقبة الجماعية وأنظمة التعرُّف على الوجه لمراقبة ملايين الأفراد في توقيت واحد، بينما يتمّ التسويق لهذه الأداة على أنها تسهم في تعزيز الأمن، في حين أنها تُثير قضايا قانونية تتعلق بانتهاك قوانين حماية البيانات وحقوق الخصوصية في ظل غياب رقابة شفَّافة على هذه التقنيات (Chen, 2021, p. 83-84). وفي مقابل هذا الوضع، تعتمد اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي على تقييد استخدام البيانات الشخصية (Parker and Taylor, 2021, p. 152)، وهو ما يُعوق نشر أنظمة مُشابهة لتلك المستخدَمة في الصين.

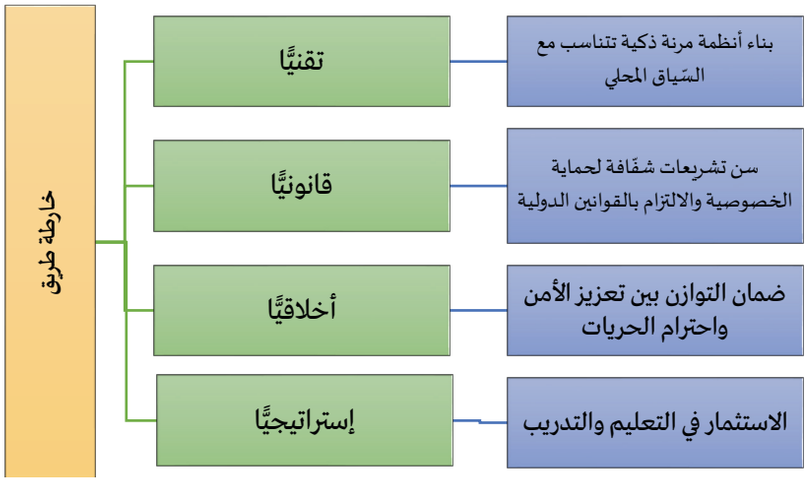
الرقابة القانونية على الاستخدام العسكري: يُثير استخدام الطائرات المسيَّرة والأنظمة الذاتية في العمليات العسكرية جدلًا حول شرعية هذه التطبيقات، وفي الولايات المتحدة الأمريكية تُستخدم الطائرات المسيَّرة لاستهداف مواقع جغرافية بعيدة دون إشراف قضائي واضح (Parker & Hill, 2020, p. 122). وهو ما أثار قضايا تتعلَّق بالقانون الدولي الإنساني، حيث طالت انتقادات واسعة لاستخدام الطائرات المسيّرة الأمريكية في منطقة الشرق الأوسط التي أدى بعضها إلى مقتل مدنيين، وهو ما يُعدُّ انتهاكًا لقوانين الحرب التي تتطلّب التمييز بين الأهداف العسكرية والمدنية.

التشريعات المحلية والدولية: تواجه القوانين المتعلِّقة بتصدير التقنيات الأمنية تحديات كبيرة، خصوصًا في الولايات المتحدة الأمريكية؛ حيث يتمُّ تطوير أنظمة مراقبة متقدِّمة، لكنها تخضع لتقييدات دولية؛ لضمان عدم استخدامها في انتهاكات حقوق الإنسان في مناطق النزاع (Green, 2021, p. 95-96).

- **الأبعاد الأخلاقية**

التوازن بين الأمن والحريات: تستغل العديد من الحكومات؛ مثل: الصين ودولة الإمارات الذكاء الاصطناعي لتعزيز الأمن الداخلي ومكافحة الجريمة (Zhang & Wang, 2020, p. 236). ومع ذلك فإنَّ المراقبة المفرطة تُهدِّد الحرّيات الفردية، مثل: حرية التعبير والتجمُّع، وتُثير إشكالات حول مدى أخلاقية هذه التدابير، مثال على ذلك ما حدث في الصين، حيث تمّ انتقاد تقنية التعرُّف على المشاعر التي تُستخدم لتقييم ولاء المواطنين للدولة ومراقبة سلوكياتهم، ممّا يُعدُّ تدخلًا صارخًا في خصوصياتهم.

التحيُّز الخوارزمي: تتميّز أنظمة الذكاء الاصطناعي بعدم الحياد التام، فالبيانات المستخدمة في تدريبها قد تحمل انحيازات تؤدِّي إلى نتائج غير عادلة. على سبيل المثال في بريطانيا، أظهرت بعض الدراسات أنَّ أنظمة التنبُّؤ قد تُظهر تحيّزًا ضدَّ الأقليات العرقية، ممّا يُفاقم مشاكل الثقة بين الدولة والمواطنين، كما أثارت تجربة نظام التعرُّف



شكل 2 خارطة الطريق للدروس المستفادة

Figure 2 *Roadmap of lessons learned*

على الوجه في الأماكن العامة اعتراضات من جمعيات مدنية، حيث أظهرت الخوارزميات معدلات خطأ أعلى عند تحليل صور أفراد من خلفيات غير بيضاء (Shahid, 2020, p. 48).

الرقابة الأخلاقية: تواجه الدول التي تستخدم الذكاء الاصطناعي للأغراض الأمنية تحديًا في وضع معايير أخلاقية تُوازن بين حماية الأمن واحترام كرامة الأفراد. على سبيل المثال: تستخدم دولة الإمارات روبوتات ذكية في تسيير الدوريات الأمنية (وكالة أنباء الإمارات، 2024)، وهو ما يُثير إشكالات حول كيفية تعامل هذه الروبوتات مع المواطنين والمقيمين دون تدخل بشري، خصوصًا في الحالات الحرجة.

وعامة، يُعدُّ استخدام الذكاء الاصطناعي في الأمن والمراقبة سلاحًا ذا حدّين، وعلى الرغم من مساهمته في تعزيز الأمن ومكافحة الجرائم، سواء التقليدية أو الإلكترونية، فإنه يتطلَّب وضع أُطُر قانونية وأخلاقية صارمة، تشمل حماية الخصوصية ومنع الانحياز وتعزيز الشَّفافية؛ لضمان استخدام هذه التقنيات بطريقة تُحقّق الأمن دون المساس بالحقوق الأساسية للأفراد.

4. 4 استخلاص الدروس المستفادة من الممارسات الدولية

أظهرت تجارب الدول الرائدة في استخدام الذكاء الاصطناعي للأمن والمراقبة، أنَّ النجاح يعتمد على التكامل بين التطوّر التقني والأُطُر القانونية والاعتبارات الأخلاقية مع اعتماد إستراتيجيات طويلة الأمد.

- **التطوّر التقني والبنية التحتية الإلكترونية**

يُعدُّ الاستثمار في بنية تحتية تقنية قوية أساس الاستخدام الناجح لأدوات الذكاء الاصطناعي، فقد تفوَّقت الصين باستخدام شبكة مراقبة متقدِّمة مدعومة بأنظمة التعرُّف على الوجه والمشاعر، بينما استخدمت دولة الإمارات تقنيات المدن الذكية لتعزيز الأمن. ومع ذلك يجب تحقيق التوازن بين التكنولوجيا والموارد البشرية؛ لضمان الكفاءة واستدراك الأخطاء، مثل ما أثبتته التجربة الأمريكية التي تعتمد أنظمة تحليلية دقيقة مدعومة بفرق بشرية متخصِّصة.

- **التشريعات المرنة والشَّفافية**

تؤكد تجارب أمريكا والصين الحاجة إلى تشريعات محلية تراعي الخصوصية، وتنسجم مع القوانين الدولية، بينما تُظهر بريطانيا أهمية الشَّفافية لتعزيز الثقة بين المواطنين والدولة، من خلال إشراك المجتمع المدني في وضع السياسات وضمان الامتثال للمعايير الأخلاقية.

- **التوازن بين الأمن والحريات**

يُثير الاستخدام المكثَّف لتقنيات المراقبة كما في تجربة الصين، قضايا تتعلق بانتهاك الخصوصية والحريات الفردية، وفي المقابل يبرز في بريطانيا وفرنسا أهمية إشراك المجتمع والجامعات لتطوير أنظمة تُراعي القبول المجتمعي، وتحترم الحقوق الأساسية.

- **إستراتيجيات التعليم والتعاون**

يُعزِّز نقص الكفاءات التقنية كما في بريطانيا أهمية الاستثمار في التدريب والتعاون مع الجامعات والمؤسَّسات التقنية، ومن جهة أخرى يُظهر النموذج الأمريكي فائدة الشَّراكات بين القطاعين العام والخاص

لتسريع الابتكار، بينما تؤكد فرنسا أهمية التعاون الإقليمي والدولي لضمان الاستخدام الأمثل للتقنيات.

خلاصة القول، أظهرت الممارسات الدولية في استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة، أنَّ النجاح يعتمد على عدّة عوامل مترابطة، تتمثّل في التطوّر التقني المدعوم ببنية تحتية تقنية قوية، والتشريعات القانونية المرنة والشَّفافة التي تحترم الحقوق والحريات، بالإضافة إلى التوازن بين الأمن والحريات الفردية، وأخيرًا أهمية التعليم والتعاون بين القطاعين العام والخاص، كما أنَّ اتباع إستراتيجيات شاملة ومتوازنة يُسهم في تحقيق نتائج فعَّالة ومستدامة في استخدام هذه التقنيات المتقدّمة بشكل يحترم القيم الإنسانية، ويُعزّز الأمن العام للدول.

4. 5 استشراف التحديات المستقبلية لاستخدام الذكاء الاصطناعي في الأمن والمراقبة

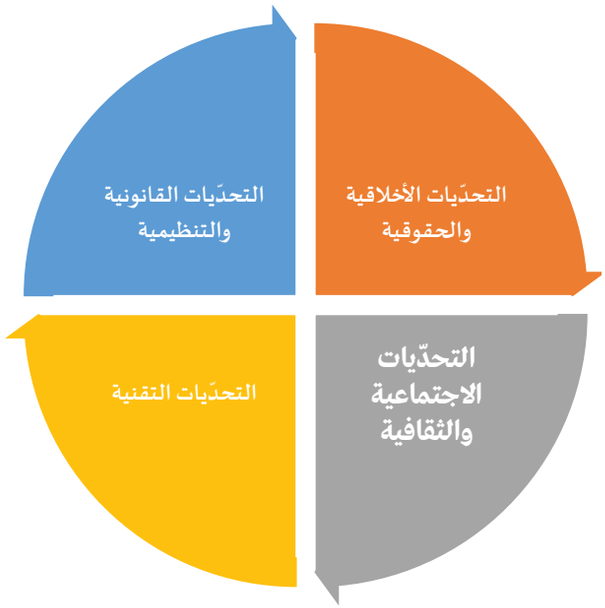
بالرغم من الفرص الكبيرة التي توفرها تقنيات الذكاء الاصطناعي في تعزيز قُدرات الأمن والمراقبة، فإن هناك عددًا من التحديات الكبيرة التي قد تواجه استخدامها في المستقبل، وتتنوّع بين القضايا القانونية والأخلاقية والتقنية والاجتماعية والسياسية، وستكون لها تَبِعات واسعة على كيفية استخدام هذه التقنيات في المجتمع. وفي هذا الإطار من المهم تحليل هذه التحدّيات بشكل مُوسّع، لضمان الاستخدام الأمثل للذكاء الاصطناعي في مجالات الأمن، مع الحفاظ على حقوق الأفراد والاستقرار المجتمعي.

التحديات القانونية والتنظيمية

يواجه استخدام الذكاء الاصطناعي في المجال الأمني تحديات مستقبلية على المستويات القانونية والتنظيمية، تتمثّل في غياب التشريعات القانونية الموحّدة وفي الرقابة على تصدير التقنيات.

غياب التشريعات القانونية الموحَّدة

من أكبر التحديات المستقبلية التي قد تواجه الدول في استخدامها للذكاء الاصطناعي في مجالات الأمن والمراقبة هو غياب التشريعات القانونية الموحَّدة، بينما تُمثّل بعض الدول مثل: الاتحاد الأوروبي نموذجًا في تنظيم استخدام البيانات وحمايتها مثل: قانون اللائحة العامة لحماية البيانات (GDPR) (Floridi, 2019, p. 99-100)، فإنَّ باقي الدول تفتقر إلى إطار قانوني موحَّد يُنظّم استخدام هذه التقنيات في المراقبة. وفي هذا السّياق تُثير تقنيات؛ مثل: التعرُّف على الوجه والمراقبة الجماعية قضايا حسَّاسة جدًّا تتعلّق بالخصوصية وحماية



شكل 3 التحدّيات المستقبلية لاستخدام الذكاء الاصطناعي في الأمن والمراقبة

Figure 3 *Future challenges of using artificial intelligence in security and surveillance*

البيانات، وفي غياب قوانين واضحة قد تَحدُث إساءة استخدام لهذه الأنظمة، وهو ما سيؤدي إلى انتهاك حقوق وحريات الأفراد.

التحديات في الرقابة عبر الحدود وتصدير التقنيات

تُعدُّ قضية تصدير تقنيات المراقبة من أبرز التحديات القانونية، على سبيل المثال: قد تواجه الولايات المتحدة الأمريكية التي تستخدم أدوات متقدّمة مثل: الطائرات المسيّرة أو شبكات المراقبة باستخدام الذكاء الاصطناعي، صعوبة في تصديرها بسبب القيود القانونية الدولية التي تحظر تصدير تقنيات قد تُستخدم في انتهاك حقوق الإنسان، كما يحدث في بعض الدول التي قد تستخدمها في تعزيز الأنظمة السياسية الاستبدادية (Lyon, 2021, p. 126-127).

التحديات الأخلاقية والحقوقية

تتجلَّى التحديات الأخلاقية والحقوقية في الاستخدام الأمني للذكاء الاصطناعي في كل من التحيُّز الخوارزمي، وانتهاك الخصوصية وحرية الأفراد.

التحيُّز الخوارزمي

يُعدُّ التحيُّز الخوارزمي من أبرز التحدّيات التي قد تواجه استخدام الذكاء الاصطناعي في الأمن والمراقبة، لأن هذا الذكاء يعتمد بشكل

كبير على نتائج البيانات المدخلة التي قد تحتوي على تحيُّزات اجتماعية أو ثقافية أو إثنية أو حتى دينية، والتي يُمكنها أن تنعكس على نتائج المراقبة الأمنية أو التحقيقات الجنائية، وهو ما يؤدّي إلى استهداف فئات معيَّنة من الأشخاص بشكل غير عادل (Sandvig, 2020, p. 28-29). وسيتعيّن مُستقبلًا على الدول والشركات التكنولوجية التي تُطوّر تقنيات الذّكاء الاصطناعي تبنّي آليات دقيقة للتأكد من نزاهة الخوارزميات، كما يجب استخدام بيانات متنوّعة ومتوازنة في تدريب الأنظمة لتقليل التحيُّزات الخوارزمية وضمان العدالة الاجتماعية.

انتهاك الخصوصية وحرية الأفراد

من أبرز القضايا التي قد تُثار في المستقبل هي انتهاك الخصوصية، لأنَّ الذكاء الاصطناعي يمكنه التسبُّب في جمع ومراقبة كمّيات ضخمة من البيانات الشخصية، بما في ذلك الأنشطة اليومية للأفراد في الأماكن العامة، وهو ما قد يؤدي إلى مراقبة مستمرة لهم في حياتهم الخاصة. وفي ظل هذه التحدّيات ستزداد الحاجة إلى حماية الخصوصية، وتطبيق إجراءات رقابة صارمة لضمان أنّ المراقبة الأمنية تتمّ في حدود القوانين التي تضمن حقوق وحريات الأفراد.

التحدّيات التقنية

تشمل التحدّيات التقنية لاستخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة كلًّا من الهجمات السّيبرانية على الأنظمة الذكية، وصعوبات تفسير قرارات هذا الذكاء.

الهجمات السّيبرانية على الأنظمة الذكية

كلما زادت الاعتمادية على الذكاء الاصطناعي في الأنظمة الأمنية زادت معها التهديدات السّيبرانية التي أصبحت أكثر تطوّرًا، وبإمكانها أن تستهدف الأنظمة المعتمدة على هذه التقنيات، مثل: الطائرات المسيَّرة أو أنظمة التعرُّف على الوجه (Bada and Sasse, 2020, p. 106). وسيُصبح من الضروري في المستقبل تطوير تقنيات أمنية تعتمد على الذكاء الاصطناعي لمكافحة الهجمات السّيبرانية، مع ضمان تحسين القدرة على استشراف المخاطر والتهديدات ومعالجتها.

صعوبة تفسير قرارات الذكاء الاصطناعي

من أكبر التحديات التقنية هي غموض قرارات الذكاء الاصطناعي، حيث يكون من الصعب أحيانًا تفسير لماذا تتخذ الأنظمة قرارات معيَّنة، خاصة في مجالات حسَّاسة مثل: التنبُّؤ بالجرائم أو تحليل البيانات الجنائية (Barocas, Hardt, and Narayanan, 2019, p. 114).

ومن ثمَّ يتعيَّن على الحكومات ومؤسَّسات إنفاذ القانون على وجه الخصوص تطوير تقنيات تفسيرية للذكاء الاصطناعي تجعل قراراته شفَّافة وواضحة، ويَسهُل فهمها من قبل الأشخاص المتأثّرين بها.

التحدّيات الاجتماعية والثقافية

تتمثّل التحديات الاجتماعية والثقافية في تأثير المراقبة الجماعية على العلاقات الاجتماعية، وفي التحوّلات في سوق العمل الأمني.

تأثير المراقبة الجماعية على العلاقات الاجتماعية

من المتوقع أن يكون لتوسيع استخدام تقنيات المراقبة تأثير كبير على العلاقات الاجتماعية بين الأفراد، وقد يؤدي الاستخدام الواسع لها إلى زيادة القلق الاجتماعي بشأن مراقبة سلوك الأفراد في الأماكن العامة (السكسيوي، 2020). ويفرض هذا الوضع ضرورة تطوير إستراتيجيات توعوية تؤكد التوازن بين الأمن والحرية، وأن يتمّ احترام حقوق الأفراد في التعبير والمشاركة المجتمعية.

التحولات في سوق العمل الأمني

قد تُغيِّر تقنيات الذكاء الاصطناعي في الأمن طبيعة بعض الوظائف الأمنية، مثل: تقليص الحاجة إلى الأفراد في الدوريات الأمنية أو المراقبة البشرية في الأماكن العامَّة، وهو ما قد يُسبّب تحوّلات في سوق العمل الأمني ينتج عنها التخلي عن وظائف تقليدية (Cunningham and Montagu, 2020, p.36-37). ولمواجهة هذا التحدّي يتعيّن على المؤسّسات الأمنية تطوير برامج تدريب وتقديم فرص تعليمية لإعادة تأهيل القوى العاملة في المجال الأمني لمواكبة التحوُّلات التكنولوجية.

وختامًا يعكس استشراف التحدّيات المستقبلية لاستخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة الحاجة إلى مقاربة متكاملة، تأخذ في الاعتبار التحديات القانونية والأخلاقية والتقنية والاجتماعية. ومن أجل ضمان أنَّ هذه التقنيات تخدم المجتمع بشكل عادل وآمن يجب أن تتوافر تشريعات تنظيمية واضحة مع التزام واضح بحماية الحقوق والحريات الأساسية للأفراد، مثل: الخصوصية وحرية التعبير. وفي نفس الوقت يتطلّب مواكبة التطوّر التكنولوجي المستمر، تطوير آليات أمان متقدّمة وتفسيرٍ أفضل لقرارات الذكاء الاصطناعي.

5. النتائج والتوصيات

5. 1 النتائج

انطلاقًا ممَّا سبق، تكشف النتائج الآتية عن أهمّ القضايا التي تواجهها المؤسّسات الأمنية فيما يتعلّق بالخصوصية والتشريعات القانونية والتحيُّز في الأنظمة، فضلًا عن التهديدات المستقبلية.

- يُعزّز التقدّم التكنولوجي في استخدام الذكاء الاصطناعي من فاعليّة المراقبة والأمن، لكنه يُثير عدّة إشكالات بشأن الخصوصية.
- تتعلّق التحديات القانونية بالغياب الواضح للتشريعات لحماية الحقوق الفردية أمام استخدام الذكاء الاصطناعي في المراقبة.
- قد يؤدي التحيُّز الخوارزمي في الأنظمة إلى قرارات غير عادلة أو تمييزية في سياقات أمنية متعدّدة.
- يختلف التوسّع العالمي في استخدامات الذكاء الاصطناعي بين الدول، مع تركيز كل من الصين والإمارات على بنية تحتية إلكترونية متطوّرة.
- تشمل التهديدات المستقبلية الهجمات السّيبرانية على الأنظمة الذكية في الأمن والمراقبة؛ ممّا يُهدّد استقرارها.
- يتطلّب التوازن بين الأمن والحرّيات تشريعات مرنة تضمن الاستخدام الآمن للتكنولوجيا دون المساس بالحقوق الإنسانية.

5. 2 التوصيات

استنادًا إلى نتائج الدراسة، يتطلّب الاستخدام الأمني للذكاء الاصطناعي تبنّي إستراتيجيات تكنولوجية وقانونية متكاملة، لضمان تحقيق الأمن دون المساس بالحقوق والحريات الفردية، وفي هذا السّياق يمكن تطبيق التوصيات الآتية:

- حماية الخصوصية: وضع سياسات صارمة لحماية البيانات الشخصية وضمان الامتثال للمعايير الدولية، مع مراقبة تأثير أنظمة الذكاء الاصطناعي على الحرّيات الفردية.
- تطوير التشريعات: تحديث القوانين الوطنية بما يضمن التوازن بين متطلبات الأمن وحماية الحقوق الأساسية، مع الاستفادة من التجارب الدولية في تنظيم استخدام تقنيات المراقبة.
- مكافحة التحيُّز الخوارزمي: تطوير آليات لمراجعة وتحليل الخوارزميات المستخدمة في أنظمة الأمن والمراقبة للحدّ من القرارات التمييزية، خاصةً فيما يتعلق بالتعرّف على الوجه وتحليل سلوكيات الأفراد.
- تعزيز الأمن السّيبراني: تحسين بنية الأمن المعلوماتي لمواجهة الهجمات السّيبرانية التي تستهدف البنية التحتية الأمنية، مع تعزيز تقنيات الكشف المبكر عن التهديدات الأمنية.
- تدريب العاملين في الأمن: توفير برامج تدريبية متخصّصة في الذكاء الاصطناعي لرجال الأمن والمسؤولين عن نظم المراقبة لضمان الاستخدام الفعّال والمسؤول لهذه التقنيات.
- تقييم الأثر الاجتماعي: إجراء دراسات دورية لتقييم تأثير الذكاء الاصطناعي على المجتمع وحقوق الإنسان، خاصّة فيما يتعلق باستخدامه في المراقبة المفرطة، والتعرُّف على الوجه والتنبُّؤ بالسُّلوكيات الإجرامية.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

البابلي، عمَّار ياسر ، (2024). فرص استخدام الخوارزميَّات في تعزيز الاستخبارات الأمنية، أوراق السياسات الأمنية، المجلد 4، العدد 1، جامعة نايف العربية للعلوم الأمنية.

الديسي، حمدان خالد، (2018). تجربة مؤسسة شرطة دبي في توفير الأمن من خلال الخدمات الذكية: دراسة تحليلية لنظام الحوكمة والإدارة، أطروحة ماجستير، إشراف عبد الفتاح ياغي، كلية العلوم الانسانية والاجتماعية بجامعة الإمارات العربية المتحدة.

الصويلح، سعد مفلح حمود، (2023). دور أنظمة الذكاء الاصطناعي في مكافحة الشائعات الإلكترونية، المجلة العربية للدراسات الأمنية، المجلد 39، العدد 1.

العموش، أحمد فلاح والعبدولي، شيخة خميس (2023). أهمية أنظمة الذكاء الاصطناعي في تحليل الجرائم وأنماطها، مجلة الآداب، ملحق ع 145.

المحمودي، محمد سرحان علي ، (2015). مناهج البحث العلمي، دار الكتب، صنعاء.

أبو منصور، حسين يوسف، (2020). الذكاء الاصطناعي وأبعاده الأمنية، مجلة أوراق السياسات الأمنية، المجلد 1، العدد 1، جامعة نايف العربية للعلوم الأمنية.

المنشورات الإلكترونية

روبوتات ذكية بشرطة أبو ظبي للتخفيف المروري وتحديد المخالفات، وكالة أنباء الإمارات، 17 مارس 2024، تاريخ الدخول: 20 نوفمبر 2024. https://2u.pw/PErXQhYI

السكسيوي، أحمد، (2020/04/20) ، تفاهة المجتمعات الرقمية: أفول القيم وتكريس المراقبة التجسسية، الجزيرة نت، شوهد في: 2024/11/22 ، في: https://2u.pw/Ki6fAFRY

المراجع الأجنبية

Amoore, L, (2020). Cloud Computing and Predictive Crime: Surveillance in the UK. Journal of Technology and Politics, Volume 24, Issue 2.

Bada, M, & Sasse, M. A., (2020). Cyber Threats in the Age of AI: The Growing Risk of Cyber-attacks on Autonomous Systems. Journal of Cybersecurity, Volume 9, Issue 2.

Barocas, S., Hardt, M, and Narayanan, A., (2019). Fairness and Machine Learning. Cambridge University Press.

Bertino, Elisa and R. Sandhu, (2005). Database Security: Concepts, Approaches, and Challenges. Springer.

Chen, L, (2021). Facial Recognition Technology in China: Security vs Privacy Debate. Journal of Chinese Law and Technology, Volume 32, Issue 2.

Chen, L, & Li, X, (2021). China's Surveillance State: Technology, Society, and the Law. The Journal of Technology in Society, Volume 33, Issue 4.

Cunningham, M, & Montagu, D, (2020). AI in Security: How Artificial Intelligence is Transforming Security Operations. Security Management Journal, Volume 25, Issue 3.

Floridi, Luciano, (2019). The Fourth Industrial Revolution, Oxford University Press.

Green, H, (2021). Export Restrictions on Surveillance Technology in Israel: Navigating Human Rights and International Law. International Law Review, Volume 44, Issue 1.

Jada, Irshaad and others, (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review, Data and Information Management, Volume 8, Issue 2.

Lemoine, C, and Dupont, P, (2021). Artificial Intelligence and Security: France's National and European Initiatives. International Journal of Security and Technology, Volume 32, Issue 4.

Lyon, D., (2021). Surveillance Society: Monitoring Everyday Life. Polity Press.

Maheswari, Uma P and others, (2023). Artificial Intelligence in Video Surveillance In book: Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT, IGI Global.

Majed, Shar Fouad, (2024). Artificial Intelligence Technology in the Field of Modern Forensic Evidence: Brain Fingerprinting as a Model, Pakistan Journal of Criminology, Vol 16, No 03, July- September.

McKew, M., (2019). Artificial Intelligence and the Future of National Security. The Brookings Institution.

Mu, Jie and others, (2024). Application of Artificial Intelligence Technology in the Field of Digital Currency Security, Procedia Computer Science, Volume 243.

Parker, A, & Taylor, M., (2021). GDPR and Its Implications for Surveillance Technology in Europe. Journal of International Data Protection, Volume 33, Issue 2.

Parker, R, & Hill, J, (2020). Drone Warfare and International Law: Civilian Casualties and Legal Violations in the Middle East. Journal of International Humanitarian Law, Volume 34, Issue 2.

Russell, S, and Norvig, (2016). Artificial Intelligence: A Modern Approach (3rd ed.). Pearson.

Sandvig, C, (2020). Algorithmic Bias Detectable in Predictive Policing Technologies: An Investigation into Discriminatory Impacts in Surveillance Systems. Journal of Critical Surveillance Studies, Volume 8, Issue 1.

Shahid, S, (2020). The Problem of Racial Bias in Predictive Policing and Facial Recognition in the UK. Journal of Racial and Ethnic Studies, Volume 18, Issue 1.

Zhang, Y, & Wang, F, (2020). Emotion Recognition Technology in China: Implications for Privacy and Human Rights. Journal of Technology and Society, Volume 52, Issue 4.

Zuboff, Shoshana , (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs.

Zuboff, Shoshana , (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs.