Artificial Intelligence Risks to Information Privacy and Security on the Future of Organizations: A Modern Vision

Saeed bin Ghurmallah bin Saeed Al Wasi[a], Dr. Ismail Mohammed Bahkali[b]
[a,b]Department of Information Science - Faculty of Arts and Humanities - King Abdulaziz University - Jeddah - Saudi Arabia
E-mail: s2011wasy@gmail.com
Ibahkali@kau.edu.sa

Abstract

This study aims to analyze and understand the risks of artificial intelligence on the privacy and security of information in the advanced digital environment, and what measures and strategies can be taken to maintain security and privacy in the face of these risks and challenges in the future. To achieve this goal, the researcher relied on the descriptive and analytical approach, it includes all organizations in the Kingdom of Saudi Arabia, regardless of their locations. The size of the study population was (80) employees, and it was a random sample of the study population, and the questionnaire was the tool for collecting information.

The current study reached a set of results, most notably:

- Providing specialized educational and training programs in the fields of artificial intelligence and related technology.
- Organizing and monitoring the economic and social impact.
- Providing an encouraging business climate for technology companies and startups working in the field of artificial intelligence.
- Cloud-based network security solutions.
- Behavior analysis and advanced threat classification.

In the light of the findings of the current study, it recommends the following:

• Identify how the increasing use of artificial intelligence impacts the privacy and security of information in these areas.
• Analyzing security threats related to hacking, data theft, and exploiting vulnerabilities in artificial intelligence systems.
• The need to develop new laws or amend existing laws.
• Study the techniques and tools available to protect data and information from security threats associated with artificial intelligence, such as encryption and cyber security.
• Liability for potential damages from the impact of artificial intelligence must be limited.

Key Words: Information Security, Artificial Intelligence (AI), Risks, Privacy, Digital Environment.

مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات عل مستقبل المنظمات :رؤية حديثة

الباحث/ سعيد بن غرم الله بن سعيد الواسي، د. إسماعيل محمد بهكلي

قسم علم المعلومات –كلية الآداب والعلوم الإنسانية – جامعة الملك عبد العزيز – جدة – المملكة العربية السعودية

مستخلص الدراسة

تهدف هذه الدراسة إلى التعرف على تحليل وفهم مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في البيئة الرقمية المتطورة، وما هي التدابير والاستراتيجيات التي يمكن اتخاذها للحفاظ على الأمن والخصوصية في وجه هذه المخاطر والتحديات على مستقبل المنظمات، ولتحقيق هذا الهدف فقد اعتمد الباحث على المنهج الوصفي التحليلي، يشمل كافة المنظمات بمحافظة جدة، على اختلاف اماكنهم. وقد بلغ حجم مجتمع الدراسة (**80**) موظفاً وكانت على عينة عشوائي من مجتمع الدراسة، وكانت الاستبانة هي الاداة لجمع المعلومات.

وتوصلت الدراسة الى مجموعة من النتائج ابرزها:

- توفير برامج تعليمية وتدريبية متخصصة في مجالات الذكاء الاصطناعي والتكنولوجيا المرتبطة.
- تنظيم ورصد الأثر الاقتصادي والاجتماعي.
- توفير مناخ أعمال مشجع لشركات التكنولوجيا والشركات الناشئة التي تعمل في مجال الذكاء الاصطناعي.
- حلول أمن الشبكات القائمة على السحابة.
- تحليل السلوك والتصنيف المتقدم للتهديدات.

في ضوء ما توصلت اليه الدراسة الحالية من نتائج فإنها توصي بالاتي:

- حدد كيف يؤثر الاستخدام المتزايد للذكاء الاصطناعي على خصوصية وأمن المعلومات في هذه المجالات.
- تحليل التهديدات الأمنية المتعلقة بالاختراقات وسرقة البيانات واستغلال الثغرات في أنظمة الذكاء الاصطناعي.
- الحاجة لتطوير قوانين جديدة أو تعديل القوانين الحالية.
- القيام بدراسة التقنيات والأدوات المتاحة لحماية البيانات والمعلومات من تهديدات الأمن المرتبطة بالذكاء الاصطناعي، مثل التشفير والأمن السيبراني.
- يجب تحديد المسؤولية عن الأضرار المحتملة من تأثير الذكاء الاصطناعي.

الكلمات المفتاحية: أمن المعلومات، الذكاء الاصطناعي، المخاطر، الخصوصية، البيئة الرقمية.

١. الإطار العام للدراسة

١,١ المقدمة

في هذا الفصل الاول الذي عنون بالاطار العام للدراسة سوف اتطرق فيه مقدمة البحث ثم مشكلة البحث واهمية البحث العملية والتطبيقية وتساؤلات البحث واسئلة البحث واهداف البحث ومنهجية البحث وحدود البحث ومصطلحات البحث والهيكل العام المقترح للبحث، ومبررات البحث.

خرج الذكاء الاصطناعي من أروقة المختبرات البحثية وصفحات روايات الخيال العلمي ليصبح جزءًا حيويًا لا يتجزأ من واقعنا اليومي. عندما نتحدث عن الذكاء الاصطناعي(**AI**) ، نشير إلى تقنيات وأنظمة تهدف إلى منح الحواسيب قدرات تفكير وتعلم تقترب من قدرات البشر. إن تقدم الذكاء الاصطناعي يعتبر تطورًا مثيرًا في عالم التكنولوجيا، وأصبح جزءًا أساسيًا من حياتنا اليومية، حيث يمكننا الاستفادة منه في تطبيقات تعتمد على التعلم الآلي والتحليل الذكي للبيانات الكبيرة.

ومع ذلك، يترتب على هذا التقدم الكبير في مجال الذكاء الاصطناعي مجموعة من المخاطر التي يجب أن ننظر فيها بعناية، تتعلق بشكل خاص بمجالات الأمن ومستقبل العمل والبشر. إحدى هذه المخاطر الأمنية تتمثل

في استخدام الذكاء الاصطناعي في هجمات سيبرانية متقدمة، حيث يمكن للمهاجمين الاستفادة من التكنولوجيا الذكية لتنفيذ هجمات تصعب على الأمن اكتشافها كما يمكن للذكاء الاصطناعي أيضًا تعلم سلوك المستخدمين عبر الإنترنت واستخدام هذه المعلومات في هجمات استهدافية.

بالإضافة إلى ذلك، هناك مخاوف تتعلق بتأثير الذكاء الاصطناعي على سوق العمل ومستقبل الوظائف. فقد قام الذكاء الاصطناعي بتغيير الطريقة التي ننفذ بها بعض المهام التقليدية، مما أدى إلى فقدان بعض الوظائف البشرية في بعض القطاعات. يتطلب ذلك تكييف المجتمع وتطوير مهارات جديدة لمواكبة هذا التغيير التكنولوجي.

على الرغم من هذه المخاطر، ينبغي أيضًا أن نفهم أن الذكاء الاصطناعي يمكن أن يسهم في خلق فرص جديدة ويعزز من فرص العمل والابتكار في العديد من الصناعات، مما يفتح أفاقًا واعدة للتنمية والنمو الاقتصادي.

فتعيش البشرية حاليًا في عصر من التقدم التكنولوجي الهائل، حيث أصبحت التكنولوجيا تحتل مكانة أساسية في مختلف جوانب حياتنا اليومية. ومن بين هذه التكنولوجيا التي تشكل تحولًا ثوريًا في العديد من الصناعات والقطاعات، يأتي دور الذكاء الاصطناعي بمكانة خاصة. *فالذكاء الاصطناعي* هو مجال يعتمد على استخدام الحواسيب والبرامج لتنفيذ مهام تتطلب تفكيرًا وتعلمًا ذاتيًا، وهو يعد من بين أهم التطورات التكنولوجية في العصر الحديث.

يتميز الذكاء الاصطناعي بقدرته على تحليل البيانات بسرعة هائلة واتخاذ قرارات دقيقة، وهو يُعَدُّ عنصرًا أساسيًا في تطوير التطبيقات والأنظمة التي تستند إلى البيانات والتحليلات. وعلى الرغم من الفوائد الكبيرة التي يمكن أن يقدمها الذكاء الاصطناعي في مجالات متعددة، إلا أنه يترتب عليه أيضًا تحديات ومخاطر جسيمة.

إحدى أبرز هذه المخاطر تتعلق بالخصوصية وأمن المعلومات. إذ يمكن للذكاء الاصطناعي جمع وتحليل كميات ضخمة من البيانات الشخصية، مما يشكل تهديدًا كبيرًا على خصوصية المستخدمين. بالإضافة إلى ذلك، قد تتعرض الأنظمة والتطبيقات التي تعتمد على الذكاء الاصطناعي لاختراقات أمنية قد تؤدي إلى تسريب المعلومات أو تعريض الأفراد والمؤسسات للمخاطر.

هذه الرسالة تهدف إلى دراسة وتحليل مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات. سنقوم بفحص الأساليب والتقنيات التي يمكن أن تُستخدم لحماية البيانات وضمان خصوصية المعلومات في ظل تطور الذكاء الاصطناعي. سنستعرض السيناريوهات المحتملة لاستخدام الذكاء الاصطناعي في انتهاك الخصوصية ونقدم استراتيجيات لمواجهة هذه المخاطر وتقديم حلول فعّالة.

باختصار، تعد هذه الرسالة محاولة لفهم وتقدير التأثيرات المتزايدة للذكاء الاصطناعي على خصوصية وأمن المعلومات، وما يمكن أن تعنيه هذه المخاطر بالنسبة للمجتمع والأفراد على مستقبل المنظمات. سنسعى إلى

تقديم توصيات واقتراحات تساهم في تعزيز الأمن الرقمي والحفاظ على الخصوصية في عالم متزايد التحول التكنولوجي.

تتناول هذه الدراسة معرفة **مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات**.

٢,١ مشكلة الدراسة

مع التقدم الهائل في مجال تكنولوجيا المعلومات وانتشار الذكاء الاصطناعي في مختلف جوانب حياتنا، تزايدت المخاطر المتعلقة بأمن وخصوصية المعلومات بشكل ملحوظ. يعد الذكاء الاصطناعي تحديًا كبيرًا في هذا السياق نظرًا لقدرته على تحليل ومعالجة البيانات بشكل أسرع وأكثر دقة من البشر، مما يتيح الفرص لتنفيذ هجمات سيبرانية متطورة واختراق أمن الأنظمة والشبكات.

أصبحت اليوم وظيفة المتخصصين في إدارة مصادر المعلومات ومراكزها وظيفة أساسية في الإدارات العصرية بالتخطيط للتكنولوجيا المعلوماتية في أية منظمة وذلك بجمع المعلومات وحفظها ومن ثم معالجتها بما يخدم أهداف المنظمة. وعليه، نجد أن وظيفة مدراء إدارة المعلومات المتخصصين في تحليل النظم والبرمجة وإدارة قاعدة البيانات آخذة في النمو في حيز المهام التنفيذية قصيرة المدى إلى حيز المهام الإستراتيجية طويلة المدى.

فالمتخصصين في إدارة مصادر المعلومات ومصادرها يدعمون المدراء التنفيذيين المستخدمين للحاسبات الآلية بخدمات عديد تفيدهم في انجاز مهامهم الإدارية كالتسويق والتحويل والتوظيف وبحوث العمليات فهم يوفرون ما يعرف بالخط الساخن (**Hot Line**) للموظفين لتوفير المساعدة لهم في كيفية أداء عملهم، وهم يوفرون أيضاً حصراً كاملاً لجميع استفسارات المشتغلين والمستخدمين لأجهزة الحاسبات الآلية بالمنظمة ويعلمون على حل مشاكلهم المتعلقة بالأجهزة الإلكترونية كما أنهم يدربون الموظفين حديثي التعيين على استخدام الكمبيوتر، ويقدمون أحدث الأجهزة والبرامج للموظفين الذين يحتاجونها في عملهم علاوة على إسداء النصح والمشورة لكل من يرغب في إيجاد الحلول المناسبة للمشاكل المتعلقة بالحاسبات الآلية التي يستخدمونها مثل تصميم أنظمة إدارة قواعد البيانات والجداول الإلكترونية والبرمجة، وتجميع التقارير وما إلي ذلك من الأعمال الإدارية التي يمكن أن تخضع لاستخدامات الكمبيوتر الحديثة.

يتعين على المجتمع الدولي والمؤسسات الخاصة والحكومات العمل على تقديم حلول فعالة لمعالجة هذه المخاطر والتحديات المتنامية. من المهم فهم كيف يمكن لتقنيات الذكاء الاصطناعي أن تكون عرضة للاستغلال من قبل الأطراف الخبيثة وكيف يمكن حماية البيانات الحساسة والخصوصية الشخصية للأفراد والمؤسسات.

من خلال ذلك، يُمكن صياغة التساؤل الرئيسي للدراسة كالآتي: **"كيف يمكن تحليل وفهم مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في البيئة الرقمية المتطورة، وما هي التدابير والاستراتيجيات التي يمكن اتخاذها للحفاظ على الأمن والخصوصية في وجه هذه المخاطر والتحديات على مستقبل المنظمات؟"**

٣,١ أهمية الدراسة

الأهمية النظرية

١. **التقدم العلمي والنظري:** يساهم هذا البحث في تطوير المعرفة والنظريات المتعلقة بمفهوم الأمن السيبراني وتأثير التطورات التكنولوجية مثل الذكاء الاصطناعي على هذا المفهوم.

٢. **التوعية العامة:** يساهم البحث في زيادة الوعي بين العامة والمحترفين بشأن مخاطر الذكاء الاصطناعي وأهمية الأمن السيبراني على مستقبل المنظمات.

٣. **توجيه السياسات والتشريعات:** يمكن استخدام نتائج البحث في توجيه وتطوير السياسات والتشريعات المتعلقة بأمن المعلومات والتكنولوجيا.

٤. **البحث والتطوير المستقبلي:** يمكن أن يمهد البحث الطريق للبحث والتطوير المستقبلي في مجال الأمن السيبراني وتطبيقات الذكاء الاصطناعي.

٥. **الفهم الأخلاقي والقانوني:** يساهم البحث في فهم القضايا الأخلاقية والقانونية المرتبطة بالذكاء الاصطناعي والأمن السيبراني.

الأهمية العملية

١. **حماية المعلومات والبيانات:** يساهم البحث في تطوير استراتيجيات لحماية المعلومات والبيانات الحساسة من التهديدات السيبرانية المتزايدة.

٢. **تحسين أمن الأعمال والشركات:** يمكن للبحث مساعدة الشركات والمؤسسات في تحسين أمن أنظمتها الرقمية وحماية مصالحها ومعلومات عملائها.

٣. **تطوير التكنولوجيا الآمنة:** يمكن أن يدفع البحث بتطوير تقنيات وأدوات ذكاء اصطناعي آمنة تسهم في تقليل المخاطر السيبرانية.

٤. **تعزيز الاستدامة الاقتصادية:** من خلال فهم تأثير الذكاء الاصطناعي على الأمن السيبراني، يمكن تعزيز الاستدامة الاقتصادية وتفادي الخسائر الاقتصادية الناجمة عن الهجمات السيبرانية.

٥. **تقديم التوجيهات العملية:** يمكن للبحث تزويد الشركات والمؤسسات بتوجيهات عملية للتعامل مع تحديات مخاطر الذكاء الاصطناعي على الأمن السيبراني على مستقبل المنظمات.

٤,١ أهداف الدراسة

الهدف الرئيسي من الدراسة هو **تحليل وفهم مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في البيئة الرقمية المتطورة، وما هي التدابير والاستراتيجيات التي يمكن اتخاذها للحفاظ على الأمن والخصوصية في وجه هذه المخاطر والتحديات على مستقبل المنظمات**. وسيتم تحقيق هذا الهدف الرئيس من خلال تحقيق الأهداف الفرعية التالية:

١. **تقييم تأثير الهجمات السيبرانية بواسطة الذكاء الاصطناعي على المؤسسات** عن طريق فهم كيفية تأثير هجمات الذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات، وكيفية التصدي لهذه التأثيرات.

٢. **تقديم استراتيجيات وتوجيهات للأمن السيبراني** من خلال تطوير استراتيجيات وتوجيهات فعالة لتعزيز أمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي.

٣. **فحص الأثر الاجتماعي والاقتصادي للاستخدام المتزايد للذكاء الاصطناعي** على تأثير تزايد استخدام الذكاء الاصطناعي على سوق العمل والمهن المختلفة وتقديم توصيات للمؤسسات والحكومات للتعامل مع التحديات والفرص الاقتصادية.

٤. **تطوير أدوات وتقنيات للكشف المبكر عن هجمات الذكاء الاصطناعي** عبر تطوير أدوات وتقنيات فعالة للكشف المبكر عن وتصدي للهجمات التي تستخدم تقنيات الذكاء الاصطناعي، مما يسهم في تقليل التأثيرات السلبية على الأمن الرقمي والخصوصية.

٥,١ أسئلة الدراسة

١. ما أخطار الذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات؟

٢. هل يمكن تطوير استراتيجيات وتوجيهات فعالة لتعزيز التدابير الوقائية وأمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي؟

٣. ما درجة الوعي والمعرفة بالأمن الرقمي في عصر التقدم التكنولوجي واستخدام الذكاء الاصطناعي في النظام التعليمي؟

٤. ما درجة الثقة والاعتماد على استخدام تقنيات الذكاء الاصطناعي؟

٦,١ فرضيات الدراسة

١. هناك علاقة ذات دلالة بين تقديم الاستراتيجيات الذكاء الصناعي والتقليل من التأثيرات السلبية لهجمات الذكاء الصناعي.
٢. هناك علاقة ذات دلالة بين ادوات تقنيات فعالية الكشف المبكر عن الهجمات والحفاظ على الامن الرقمي.
٣. هناك علاقة ذات دلالة بين تأثير هجمات الذكاء الصناعي ومساهمته في الابعاد الاجتماعية والاقتصادية لهذه التهديدات.
٤. هناك علاقة بين استخدام الذكاء الصناعي وتأهيل القوى العاملة لمواكبة التحولات التكنولوجية والاستفادة الفرص الاقتصادية.

٧,١ منهجية الدراسة

يتوجب على كل دراسة علمية اعتماد منهج علمي يهدف إلى إثبات فرضياتها، ويكمن نجاح هذا الإثبات في الانسجام بين المنهج العلمي المستخدم وفرضيات الدراسة. في هذا السياق، تم اعتماد المنهج الوصفي التحليلي لتحليل موضوع الدراسة.

٨,١ حدود الدراسة

يقتصر الباحث في دراسة على الحدود الآتية:

١. **الموضوعية:** معرفة مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات.
٢. **المكانية:** المؤسسات والشركات التي تعمل بالذكاء الاصطناعي.
٣. **الحدود الزمانية:** تم تطبيق البحث خلال الفصل الدراسي الأول من العام الدراسي **٢٠٢٤**.
٤. **الحدود اللغوية والبشرية:** الموظفين الذين يتحدثون باللغة العربية والانجليزية في المؤسسات والشركات التي تعمل بالذكاء الاصطناعي.

٩,١ مصطلحات الدراسة

١. **تعلم الآلة (Machine Learning)**: هذا المصطلح يشير إلى القدرة على الأنظمة الذكية على تعلم وتطوير أدائها من خلال التفاعل مع البيانات واستخدام الخوارزميات (سعد، ٢٠٢١).

التعريف الاجرائي: هو مجموعة من التقنيات التي تمكّن الأنظمة الحاسوبية من تعلم وتحسين أدائها من خلال التفاعل مع البيانات. في سياق دراسة مخاطر الذكاء الاصطناعي، يعتبر تعلم الآلة مصدرًا محتملًا للتسريبات أو استغلال البيانات الشخصية في حالة استخدامه بطرق غير مألوفة أو غير مراقبة.

٢. **الشبكات العصبية الاصطناعية (Artificial Neural Networks)**: هذه هي نماذج تشبه بنية الشبكة العصبية في الدماغ البشري وتستخدم في تطوير الذكاء الاصطناعي لمحاكاة القرارات البشرية (العزب، ٢٠٢٢).

التعريف الاجرائي: هي نموذج حاسوبي مستوحى من الشبكات العصبية البيولوجية في الدماغ. ومن الناحية الأمنية، يمكن أن تواجه الشبكات العصبية الاصطناعية تحديات متعلقة بالاختراقات أو الهجمات المستهدفة لاستهداف التحليلات العميقة واستغلال ثغرات الأمان في هذه الشبكات.

٣. **معالجة اللغة الطبيعية (Natural Language Processing – NLP)**: هذه التقنية تسمح للأنظمة الذكية بفهم وتفسير اللغة البشرية والتفاعل معها بشكل طبيعي (المالكي، ٢٠٢٣).

التعريف الاجرائي: تُعد هذه التقنية جزءًا أساسيًا في تحليل البيانات وفهم اللغة البشرية بشكل طبيعي. ومن الممكن أن يشكل استخدام معالجة اللغة الطبيعية في تطبيقات الذكاء الاصطناعي تحديات أمنية في حفظ خصوصية البيانات اللغوية أو تفاصيل الاتصالات الشخصية.

٤. **التصور الحاسوبي (Computer Vision)**: يشير هذا المصطلح إلى القدرة على تمكين الأنظمة الذكية من تحليل وفهم الصور والفيديوهات بطريقة مشابهة للإنسان (ابو زيد، ٢٠٢٢).

التعريف الاجرائي: يشكل التصور الحاسوبي جزءًا أساسيًا في تطوير العديد من التطبيقات، ولكنه يمكن أن يتسبب في تصور مخاطر متعلقة بأمن المعلومات فيما يتعلق بالنماذج الثلاثية الأبعاد التي قد تحتوي على معلومات تفصيلية قد تكون حساسة.

٥. **الأمن السيبراني (Cybersecurity)**: هو مجموعة من الممارسات والتدابير والتقنيات التي تستخدم لحماية أنظمة المعلومات والبيانات والأنشطة على الإنترنت من التهديدات والهجمات السيبرانية. يهدف الأمن السيبراني إلى الحفاظ على سرية المعلومات، وضمان توافر الخدمات الرقمية، والحماية من الاختراقات والاستيلاء على البيانات، وضمان سلامة الأنظمة الرقمية (حسين، ٢٠٢١).

التعريف الاجرائي: يعتبر الأمن السيبراني جوهريًا في الحفاظ على خصوصية المعلومات وسلامتها. في سياق الدراسة المعنية، يعد الأمن السيبراني الجانب الأساسي لمواجهة التحديات الأمنية المحتملة نتيجة لتطبيقات الذكاء الاصطناعي والتقنيات ذات الصلة.

١٠,١ الهيكل العام المقترح للدراسة

تتكون هذه الاطروحة من ستة فصول على النحو الآتي:

- **الفصل الأول**: الإطار العام لمشكلة الدراسة، ويتناول مقدمة الدراسة ومشكلتها وتساؤلاتها وأهدافها وأهميتها ومنهجها، ومصطلحاتها.
- **الفصل الثاني**: أدبيات الدراسة.
- **الفصل الثالث**: منهجية البحث.
- **الفصل الرابع**: تحليل البيانات.
- **الفصل الخامس**: مناقشة النتائج.
- **الفصل السادس**: الاستنتاجات والتوصيات والاستراتيجية المقترحة والخلاصة.

١١,١ مبررات الدراسة

تكمن أهم مبررات اختيار الباحث لموضوع الدراسة في الآتي:

- يتواكب الموضوع مع متطلبات العصر وهو عصر التقنية وعصر الحكومة الالكترونية أي عصر استخدام الرقمية.
- لدى رجوع الباحث للإنتاج الفكري العربي تبين له عدم وجود دراسات تناولت لموضع الدراسة الحالية.
- تم اختيار موضوع مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات لأنها تعبر عن مخاطر استخدام الذكاء الصناعي والأمن السيبراني والتهديدات التي تواجه الأمن السيبراني.

٢. الإطار النظري للدراسة والدراسات السابقة

الإطار النظري للدراسة

تمهيد

سيتناول هذا الاطار دراسة مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات. يتمحور حول فهم التأثيرات المحتملة للتقنيات الحديثة المتعلقة بالذكاء الاصطناعي والتطورات السريعة في هذا المجال على الخصوصية والأمن السيبراني، فيتمثل المتغير الأول في استخدام تقنيات تعلم الآلة والشبكات العصبية

الاصطناعية كأساس للتحليل بينما يشكل المتغير الثاني معالجة اللغة الطبيعية وأدوات التصور الحاسوبي اللازمة لفهم وتحليل البيانات، وبالإضافة إلى ذلك، يتم التركيز على تقييم الأمن السيبراني والتحديات التي قد تنشأ نتيجة استخدام التقنيات الذكاء الاصطناعي في مجالات مختلفة، وذلك من خلال دراسة المتغير الثالث المتمثل في الأمن السيبراني، **ويتكون من ثلاثة مباحث: المبحث الأول: مخاطر الذكاء الاصطناعي على الخصوصية والأمن، والمبحث الثاني: مخاطر الذكاء الاصطناعي لأمن المعلومات على مستقبل المنظمات، والمبحث الثالث: التخفيف من مخاطر الذكاء الاصطناعي.**

المبحث الأول: مخاطر الذكاء الاصطناعي على الخصوصية والأمن

يواجه الذكاء الاصطناعي (**AI**) عدة مخاطر للأمان والخصوصية، والتي يمكن أن تكون لها عواقب كبيرة على الأفراد والمؤسسات والمجتمع بشكل عام. وسأذكر في هذا المبحث بعض من أهم المخاطر المرتبطة بالذكاء الاصطناعي في سياق الأمن والخصوصية.

قضايا الخصوصية للبيانات

تعتبر قضايا الخصوصية للبيانات مسألة هامة بالفعل في سياق أنظمة الذكاء الاصطناعي. إليك بعض النقاط الرئيسية التي يجب النظر فيها: (الأسد، ٢٠٢٣)

١. **جمع وتخزين البيانات:** تتطلب أنظمة الذكاء الاصطناعي، ولا سيما نماذج التعلم الآلي، كميات كبيرة من البيانات للتدريب بشكل فعال. يمكن أن تتضمن هذه البيانات معلومات شخصية وحساسة عن الأفراد. تظهر المخاوف عندما تقوم المؤسسات بجمع هذه البيانات وتخزينها دون الحصول على موافقة مناسبة أو وضع تدابير أمنية يمكن أن يؤدي الوصول غير المصرح به إلى انتهاكات للخصوصية.
٢. **تعميم البيانات وعدم التعريف:** حتى عندما تتم جمع البيانات بموافقة، هناك خطر أن يتم التعرف على الأفراد من البيانات المزعومة معممة أو غير معرَّفة. وهذا يبرز أهمية تقنيات وتدابير الحماية المناسبة لحماية هويات الأفراد.
٣. **أمن البيانات:** أمن البيانات أمر بالغ الأهمية. يمكن أن يتعرض البيانات للهجمات السيبرانية أو انتهاكات البيانات عندما تتم المعالجة أو التخزين بشكل غير آمن. يجب تصميم أنظمة الذكاء الاصطناعي بميزات أمن قوية لمنع هذه المخاطر.
٤. **موافقة مستنيرة:** يجب على الأفراد أن يتم إعلامهم بجمع البيانات واستخدامها. تعتبر سياسات الخصوصية الشفافة ونماذج الموافقة أمرًا أساسيًا لضمان فهم الأشخاص لكيفية استخدام بياناتهم. ويتضمن ذلك كيفية تحليل أنظمة الذكاء الاصطناعي للبيانات واتخاذ توقعات بناءً على تلك البيانات.

٥. **سياسات الاحتفاظ بالبيانات**: يجب على المؤسسات وضع سياسات واضحة للاحتفاظ بالبيانات. يزيد تخزين البيانات بشكل غير محدود من مخاطر انتهاكات البيانات. يجب حذف البيانات أو تعميمها بمجرد عدم حاجتها للغرض المقصود.

٦. **الامتثال التنظيمي**: العديد من المناطق لديها تنظيمات حماية البيانات مثل **GDPR** في أوروبا أو **CCPA** في كاليفورنيا. الالتزام بهذه التنظيمات ليس مطلوبًا قانونيًا فقط ولكن أيضًا ممارسة جيدة لحماية الخصوصية.

٧. **الاعتبارات الأخلاقية**: يمكن أن تكون انتهاكات الخصوصية لها تبعات أخلاقية خطيرة. يجب على مطوري الذكاء الاصطناعي والمؤسسات أن ينظروا في التداعيات الأخلاقية الأوسع لاستخدام بيانات أنظمتهم.

٨. **تطوير الذكاء الاصطناعي المسؤول**: يجب على المطورين اعتماد ممارسات الذكاء الاصطناعي المسؤولة، بما في ذلك تصميم الخصوصية من البداية في تطوير نظام الذكاء الاصطناعي.

٩. **التدقيق والمساءلة**: من المهم وجود آليات لتتبع وتدقيق استخدام البيانات، ضمان المساءلة في حالة سوء استخدام البيانات.

١٠. **تقليل البيانات**: جمع فقط البيانات اللازمة للمهمة المحددة، بدلاً من المعلومات الزائدة. يمكن أن يقلل ذلك من احتمال انتهاكات الخصوصية.

١١. **تحكم المستخدم**: يجب أن يكون للمستخدمين السيطرة على بياناتهم. يجب أن يكون لديهم القدرة على الوصول إلى بياناتهم وتصحيحها أو حذفها، بالإضافة إلى إمكانية الانسحاب من جمع البيانات.

١٢. **مشاركة البيانات مع أطراف ثالثة**: إذا تم مشاركة البيانات مع أطراف ثالثة، يجب التأكد من الالتزام بنفس معايير الخصوصية لمنع تسرب البيانات.

التعامل مع مخاوف الخصوصية ليس مسؤولية قانونية فقط ولكن أيضًا مسألة بناء الثقة مع المستخدمين والحفاظ على استخدام أخلاقي لأنظمة الذكاء الاصطناعي. ستكون المؤسسات التي تعطي الأولوية للخصوصية على ما يرام مجهزة بشكل أفضل للتعامل مع هذه المخاوف وتجنب انتهاكات محتملة.

سرقة البيانات والوصول غير المصرح به

تعتبر سرقة البيانات والوصول غير المصرح به مخاوف أمنية كبيرة، ويمكن أن تزيد الهجمات مدعومة بالذكاء الاصطناعي من هذا التهديد. فيما يلي نقاط رئيسية يجب مراعاتها: (نوار، ٢٠٢٣)

١. **هجمات معززة بالذكاء الاصطناعي**: يمكن للمهاجمين استخدام تقنيات الذكاء الاصطناعي لتعزيز استراتيجياتهم. على سبيل المثال، يمكن استخدام الذكاء الاصطناعي لتأمين الهجمات، وإنشاء رسائل احتيال متطورة بشكل تلقائي، أو استغلال الثغرات بطريقة مستهدفة وفعالة بشكل أكبر.

٢. **هندسة اجتماعية**: يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات لصقل هجمات الهندسة الاجتماعية بشكل مقنع للغاية. يمكن للمهاجمين استخدام الذكاء الاصطناعي لتقمص الهويات الموثوق بها أو المؤسسات لخداع المستخدمين وإفشاء معلومات حساسة أو منح وصولًا غير مصرح به.

٣. **تسريب البيانات**: يمكن استخدام الذكاء الاصطناعي لتسريب البيانات الحساسة من الأنظمة المخترقة بشكل أكثر تمويهًا. يمكن للذكاء الاصطناعي تعلم أنماط النشاط الشبكي العادي لتجنب الكشف وتجنب تنبيهات الأمان.

٤. **البيانات المصادقة**: يمكن للذكاء الاصطناعي أتمتة هجمات بيانات المصادقة، حيث يستخدم المهاجمون مجموعات مسروقة من اسم المستخدم وكلمة المرور من موقع واحد للوصول غير المصرح به إلى حسابات متعددة على مواقع أخرى. وهذا يمكن أن يؤدي إلى اختراقات حساب واسعة الانتشار.

٥. **استغلال الثغرات صفر اليوم**: يمكن للذكاء الاصطناعي التعرف على واستغلال الثغرات الأمنية المجهولة مسبقًا (ثغرات صفر اليوم) بشكل أسرع من القراصنة البشر. وهذا يشكل تهديدًا كبيرًا للبرمجيات والأنظمة التي لم يتم تصحيحها بعد.

٦. **البرمجيات الخبيثة المعززة بالذكاء الاصطناعي**: يمكن استخدام الذكاء الاصطناعي لإنشاء وتطوير برمجيات خبيثة أصعب اكتشافها وإزالتها. يمكن أن تكيف سلوكها استجابة لتدابير الأمن، مما يجعلها تهديدًا مستمرًا.

٧. **التعلم الآلي للدفاع**: على الجانب الدفاعي، يمكن استخدام الذكاء الاصطناعي لاكتشاف والرد على هذه التهديدات بكفاءة أكبر. يمكن لأدوات الأمن المدعومة بالذكاء الاصطناعي تحليل مجموعات ضخمة من البيانات في الوقت الحقيقي للكشف عن التغييرات غير المعتادة والتهديدات المحتملة.

٨. **تحليل السلوك**: يمكن لأنظمة الذكاء الاصطناعي تحليل سلوك المستخدمين والأجهزة للكشف عن أنشطة غير عادية أو مشبوهة، مما يشير إمكانيات وصول غير مصرح به أو سرقة بيانات.

٩. **المراقبة المستمرة**: المراقبة والتدقيق المستمر للأنظمة والشبكات ضروريين لاكتشاف الوصول غير المصرح به أو سرقة البيانات بسرعة والاستجابة لهما على الفور.

١٠. **ضوابط الوصول**: يجب تنفيذ ضوابط وصول صارمة، والمصادقة متعددة العوامل، ومبدأ أقل الامتياز لتقليل الضرر المحتمل الناجم عن وصول غير مصرح به.

١١. **إدارة التصحيح**: تقوم بتحديث وتصحيح البرامج والأنظمة بانتظام لإصلاح الثغرات المعروفة وتقليل سطح الهجوم.

١٢. **تدريب المستخدمين**: من خلال توعية الموظفين والمستخدمين بمخاطر الاحتيال والهندسة الاجتماعية وغيرها من هجمات الذكاء الاصطناعي المعززة. يمكن أن يساعد التدريب الأشخاص في التعرف على الأنشطة المشبوهة والإبلا غ عنها.

١٣. **خطة استجابة للحوادث**: عبر تطوير خطة استجابة للحوادث قوية تحدد كيفية التصرف في حالة الوصول غير المصرح به أو سرقة البيانات. يجب أن تتضمن هذه الخطة خطوات للتحقيق والاحتواء والاستعادة.

تهديدات الهجمات المدعومة بالذكاء الاصطناعي تزداد تفاقمًا، ويجب على المؤسسات الاستثمار في تدابير أمن مدعومة بالذكاء الاصطناعي للبقاء في مقدمة التهديدات المتطورة. التعاون بين مجتمع الأمن السيبراني وأجهزة إنفاذ القانون والهيئات التنظيمية أمر حاسم أيضًا للتقليل من هذه المخاطر وحماية البيانات الحساسة.

الهجمات العدائية

الهجمات العدائية هي مشكلة كبيرة في مجال الذكاء الاصطناعي، ولا سيما في سياق نماذج التعلم الآلي والتعلم العميق. تتضمن هذه الهجمات التلاعب بالبيانات الداخلة بطرق دقيقة لخداع أو التأثير على أنظمة الذكاء الاصطناعي. فيما يلي بعض النقاط الرئيسية التي يجب النظر فيها: (عبد الهادي، ٢٠٢٣)

١. **تلاعب بالبيانات الداخلة**: تشمل الهجمات العدائية عادة إجراء تغييرات صغيرة وغير ملحوظة على البيانات الداخلة، مثل الصور والصوت والنص، بهدف جعل نظام الذكاء الاصطناعي يتخذ قرارات غير صحيحة أو غير متوقعة.

٢. **أنواع الهجمات العدائية**

- **الصندوق الأبيض**: يمتلك المهاجمون معرفة كاملة بنموذج الذكاء الاصطناعي ومعلماته.
- **الصندوق الأسود**: يمتلك المهاجمون معرفة محدودة أو عدم معرفة عن نموذج الذكاء الاصطناعي وعملياته الداخلية.
- **القابلية للنقل**: يمكن أن تعمل الأمثلة العدائية المصممة لنموذج ذكاء اصطناعي واحد أيضًا ضد نموذج مختلف ولكن مشابه.

٣. **تأثيرها على أنظمة الذكاء الاصطناعي**

- يمكن أن تؤدي الهجمات العدائية إلى توقعات خاطئة، وتصنيفات خاطئة، أو أنماط سلوك غير متوقعة في أنظمة الذكاء الاصطناعي.
- يمكن أن تعرض هذه الهجمات أمن الأنظمة التي تعتمد على الذكاء الاصطناعي لاتخاذ القرارات، مثل السيارات الذاتية القيادة وأنظمة الأمن وتشخيص الرعاية الصحية.

٤. **الدفاع ضد الهجمات العدائية**

- يقوم الباحثون بتطوير آليات دفاع متنوعة، مثل التدريب العدائي، لجعل نماذج الذكاء الاصطناعي أكثر متانة أمام مثل هذه الهجمات.
- يمكن أن يجعل إدخال التبعية وعدم اليقين في نماذج الذكاء الاصطناعي من الصعب على المهاجمين إنشاء أمثلة عدائية فعالة.

٥. **هجمات التجاوز والتسميم**: يمكن تصنيف الهجمات العدائية إلى هجمات التجاوز (جعل نظام الذكاء الاصطناعي يصنف البيانات بشكل خاطئ) وهجمات التسميم (تلويث البيانات التدريبية للتلاعب في سلوك النموذج).

٦. **اعتبارات أخلاقية**: تثير الهجمات العدائية أسئلة أخلاقية حول موثوقية أنظمة الذكاء الاصطناعي، خصوصًا في التطبيقات التي تكون فيها السلامة والأمن أمورًا حرجة، مثل السيارات الذاتية القيادة والرعاية الصحية.

٧. **البحث المستمر**: ميدان الهجمات العدائية والدفاع عنها متطور باستمرار، ويعمل الباحثون على متابعة ومواجهة طرق الهجوم المتزايدة تعقيدًا.

٨. **اختبار المتانة**: من المهم أن تقوم المؤسسات بإجراء اختبارات المتانة لتقييم مدى عرضة أنظمة الذكاء الاصطناعي للهجمات العدائية واتخاذ تدابير للتخفيف من هذه المخاطر.

٩. **التنظيم والمعايير**: نظرًا لأن الهجمات العدائية تشكل مخاطر للسلامة والأمن، قد تقوم الهيئات التنظيمية ومنظمات المعايير الصناعية بتطوير إرشادات ولوائح لضمان أن نظم الذكاء الاصطناعي تكون مقاومة لهذه الهجمات.

١٠. **توعية المستخدمين**: توعية المستخدمين والمطورين بالضعف المحتمل لنظم الذكاء الاصطناعي أمام الهجمات العدائية يمكن أن تساهم في بناء الوعي والتخفيف من المخاطر.

الهجمات العدائية تمثل تحديًا كبيرًا في مجتمع الذكاء الاصطناعي، ومعالجتها تتطلب مزيجًا من البحث والتطوير وأفضل الممارسات لجعل أنظمة الذكاء الاصطناعي أكثر مقاومة للتلاعب والخداع.

تكنولوجيا الذكاء الاصطناعي "ديب فيك (Deep Fake)"

قد لفتت انتباها كبيرًا بفضل إمكانيتها في إنشاء محتوى وسائط متعددة واقعية ولكن مفبركة تمامًا. فيما يلي بعض النقاط الرئيسية التي يجب مراعاتها فيما يتعلق بمخاطر وآثار تكنولوجيا الديب فيك: (علي، ٢٠٢٢)

١. **التقمص والتلاعب**

- يمكن استخدام تقنية الذكاء الاصطناعي لإنشاء تمثيلات مقنعة للأفراد، بما في ذلك السياسيين والمشاهير أو الأشخاص العاديين. يمكن استخدام هذه التمثيلات لأغراض خبيثة متنوعة، مثل نشر معلومات كاذبة، وابتزاز، أو سرقة الهوية.
- يمكن لتقنيات الذكاء الاصطناعي الصوتية أن تعدل تسجيلات الصوت لتجعل شخصًا ما يبدو وكأنه يقول أشياء لم يقلها أبدًا، مما يزيد من درجة الخداع.

٢. **فقدان الثقة والسمعة**

- يمكن لتقنيات الذكاء الاصطناعي أن تقلل من الثقة والمصداقية في وسائط الإعلام والمعلومات. يمكن أن يصبح الناس متشككين في أصالة مقاطع الفيديو والصوت، مما يمكن أن يكون له تأثيرات واسعة في الصحافة والأدلة القانونية والحوار العام.
- قد يتعرض الأفراد والمؤسسات لأضرار في سمعتهم إذا تم إنشاء محتوى الذكاء الاصطناعي لنسب بيانات أو أفعال كاذبة إليهم.

٣. **إمكانية السوء**

- يمكن أن تسيء استخدام تكنولوجيا الذكاء الاصطناعي للتحرش والتنمر عبر الإنترنت، وحملات نشر المعلومات الكاذبة، مما يمكن أن يحث على العنف، ويضر بالعلاقات، وينقض الثقة العامة.

٤. **قضايا قانونية وأخلاقية**

- إن إنشاء وتوزيع محتوى الذكاء الاصطناعي يثير أسئلة قانونية وأخلاقية هامة. قد تحتاج القوانين المتعلقة بالتشهير والخصوصية والملكية الفكرية إلى التكيف لمعالجة هذه القضايا.
- يعد الاعتبارات الأخلاقية المتعلقة بالموافقة والاستخدام المسؤول للمحتوى الذي تولده تقنيات الذكاء الاصطناعي أمورًا حيوية (الفار، ٢٠٢٣).

٥. **الكشف والتحقق**

- مع تقدم تكنولوجيا الذكاء الاصطناعي ، يزداد الحاجة إلى وسائل كشف وتحقق قوية. يقوم الباحثون والشركات التكنولوجية بتطوير أدوات للكشف عن محتوى الذكاء الاصطناعي.

- تُبحث تقنيات البلوك شين والوسم الرقمي لمساعدة في تحديد أصالة محتوى الوسائط المتعددة.

٦. **ثقافة الإعلام والتعليم**

- تعتبر تثقيف الجمهور حول وجود وخطورة تكنولوجيا الذكاء الاصطناعي أمرًا أساسيًا. يمكن لبرامج تعليم الإعلام مساعدة الأفراد في التعرف على المحتوى الكاذب المحتمل (الفار، ٢٠٢٣).

٧. **رقابة المحتوى والتنظيم**

- تركز منصات وسائل التواصل الاجتماعي ومواقع مشاركة المحتوى بشكل متزايد على رقابة المحتوى للكشف عن محتوى الذكاء الاصطناعي وإزالته. قد تقوم الحكومات والهيئات التنظيمية أيضًا بتطوير إرشادات وتنظيمات في هذا الصدد.

٨. **الاستخدام المسؤول للذكاء الاصطناعي**

- يجب على المطورين وممارسي الذكاء الاصطناعي اعتماد ممارسات الذكاء الاصطناعي المسؤول والنظر في الآثار الأخلاقية لعملهم. التأكد من استخدام تكنولوجيات الذكاء الاصطناعي بمسؤولية أمر حيوي لتقليل الأذى (الفار، ٢٠٢٣).

٩. **البحث والابتكار**

- هناك حاجة مستمرة إلى البحث لتحسين كشف محتوى الذكاء الاصطناعي وتطوير تقنيات الذكاء الاصطناعي المتقدمة أكثر لإنشاء وتلاعب محتوى الوسائط، والذي يمكن استخدامه لأغراض تقنية جنائية وترفيهية.

تكنولوجيا الذكاء الاصطناعي هي أداة قوية لها إمكانيات إيجابية وسلبية. يتطلب التعامل مع المخاطر والتحديات المتعلقة بالذكاء الاصطناعي نهجًا متعدد التخصصات يشمل تطوير التكنولوجيا والتنظيم والتعليم والاعتبارات الأخلاقية.

الذكاء الاصطناعي الخبيث

الذكاء الاصطناعي الخبيث، المعروف أيضًا بتهديدات الأمن المدعومة بالذكاء الاصطناعي، يشكل تحديًا كبيرًا للأمن السيبراني. يمكن للمهاجمين استخدام الذكاء الاصطناعي لأتمتة وتعزيز قدرات هجماتهم العدائية، مما يجعل

الدفاع عن تهديدات الأمن السيبراني أكثر تحدياً. فيما يلي بعض النقاط الرئيسية التي يجب النظر فيها: (المومني، ٢٠١٩)

١. **الهجمات المُتمَتَّعة بالأتمتة:** يمكن للذكاء الاصطناعي أن يقوم بأتمتة مراحل متعددة من هجمات السيبراني، مثل استطلاع الأمن، والاختراق، وسرقة البيانات. وهذا يزيد من سرعة ونطاق الهجمات.

٢. **الهجمات المستهدفة:** يمكن للذكاء الاصطناعي أن يساعد المهاجمين في التعرف على الضعف في الأنظمة أو المؤسسات الخاصة بأهداف معينة. يمكن لخوارزميات التعلم الآلي تحليل الأثر الرقمي للهدف للبحث عن الضعف (أحمد، ٢٠٢١).

٣. **الصيد الاحتيالي والهندسة الاجتماعية:** يمكن للذكاء الاصطناعي أن يقوم بإنشاء رسائل صيد احتيالية وتكتيكات هندسة اجتماعية أكثر إقناعًا عبر تحليل مجموعات كبيرة من البيانات لإعداد رسائل شخصية ومضللة (النسور، ٢٠٢٢).

٤. **استغلال الثغرات الصفرية:** يمكن للذكاء الاصطناعي اكتشاف واستغلال الثغرات التي لم يتم اكتشافها مسبقًا (الثغرات الصفرية) بسرعة أكبر من القراصنة البشر، مما يجعله أداة قوية لاختراق الأنظمة.

٥. **تطوير البرامج الخبيثة:** يمكن للمهاجمين استخدام الذكاء الاصطناعي لإنشاء وتطوير برامج خبيثة أصعب في الكشف عنها وإزالتها. يمكن للبرمجيات الخبيثة المدعومة بالذكاء الاصطناعي التكيف مع سلوك الأمان (النسور، ٢٠٢٢).

٦. **تجنب الكشف:** يمكن استخدام الذكاء الاصطناعي لتحليل تدابير الأمن وتطوير تكتيكات لتجنب الكشف. على سبيل المثال، يمكنه تحديد الثغرات في أنظمة اكتشاف الاختراق وتجنب الكشف.

٧. **سرقة البيانات والتشفير:** يمكن استخدام الذكاء الاصطناعي لسرقة البيانات الحساسة من الأنظمة المخترقة بشكل أكثر تلطيفًا. يمكن للذكاء الاصطناعي تعلم أنماط النشاط الشبكي العادية لتجنب الكشف.

٨. **برامج فدية وابتزاز:** يمكن للمهاجمين استخدام الذكاء الاصطناعي لشن هجمات فدية أكثر فعالية وانتشارًا، عن طريق تشفير البيانات والمطالبة بفدية مقابل مفاتيح الفك (العمر، ٢٠٢٢).

٩. **الدفاع باستخدام الذكاء الاصطناعي:** استخدام الذكاء الاصطناعي في الدفاع ضروري. يمكن لأدوات الأمن المدعومة بالذكاء الاصطناعي تحليل مجموعات ضخمة من البيانات في الوقت الحقيقي للكشف عن التشوهات والتهديدات المحتملة، مما يساعد في اكتشاف والرد على الهجمات الخبيثة المدعومة بالذكاء الاصطناعي (المجالي، ٢٠٢٣).

١٠. **قوى العمل للأمن السيبراني**: يجب تدريب وتجهيز قوى العمل في مجال الأمن السيبراني للتعامل مع التهديدات المدعومة بالذكاء الاصطناعي. تظل الخبرة البشرية أمرًا حاسمًا في مواجهة هذه التحديات (العمر، ٢٠٢٢).

١١. **سياسات الأمن والتنظيم**: قد تحتاج الحكومات والهيئات التنظيمية إلى وضع إرشادات ولوائح لضمان استخدام الذكاء الاصطناعي بشكل مسؤول في مجال الأمن السيبراني وللإبلاغ عن انتهاكات الأمان (المجالي، ٢٠٢٣).

١٢. **التعاون ومشاركة المعلومات**: التعاون بين المؤسسات ومشاركة المعلومات حول التهديدات الناشئة ضروريان للبقاء في الأمام في مواجهة الذكاء الاصطناعي الخبيث (الأسدي، ٢٠٢٢).

١٣. **اعتبارات أخلاقية**: الآثار الأخلاقية لاستخدام الذكاء الاصطناعي لأغراض خبيثة ذات أهمية كبيرة. قد يتعين على المهاجمين أن يتحملوا مسؤولية عواقب أفعالهم (المجالي، ٢٠٢٣).

معالجة الذكاء الاصطناعي الخبيث تتطلب مزيجًا من آليات الدفاع المدعومة بالذكاء الاصطناعي وتطوير السياسات والتعليم والتعاون داخل مجتمع الأمن السيبراني. مع استمرار تقدم تكنولوجيا الذكاء الاصطناعي، تتطور استراتيجيات وتكتيكات الجهات الخبيثة أيضًا، مما يجعل من مواجهة هذه التهديدات بشكل استباقي تحدًا مستمرًا.

التحيز والتمييز

التحيز والتمييز في أنظمة الذكاء الاصطناعي هما قضيتان حرجتان يمكن أن تكون لهما عواقب وخيمة ومنتشرة. فيما يلي نقاط رئيسية يجب مراعاتها: (الأسدي، ٢٠٢٢)

١. التحيز في بيانات التدريب

- تتعلم خوارزميات الذكاء الاصطناعي من البيانات التاريخية، وإذا كانت هذه البيانات تحتوي على تحيزات أو تعكس تحيزات اجتماعية موجودة، يمكن لنظام الذكاء الاصطناعي أن يواصل وحتى يكبر هذه التحيزات.
- على سبيل المثال، يمكن أن تؤدي البيانات المتحيزة في عمليات التوظيف إلى تفضيل أنظمة الذكاء الاصطناعي لفئات معينة، مما يؤدي إلى التمييز في مكان العمل.

٢. نتائج غير عادلة

- يمكن أن تؤدي أنظمة الذكاء الاصطناعي التي تواصل التحيز إلى معاملة غير عادلة في مجموعة متنوعة من المجالات، بما في ذلك التوظيف والإقراض وإنفاذ القانون والرعاية الصحية، وغيرها.

- يمكن أن يتجلى التمييز في عدم المساواة في الفرص، والوصول إلى الخدمات، والعواقب القانونية، مما يؤثر بشكل غير متساو على الفئات المهمشة والممثلة بشكل غير كاف.

٣. **المساءلة الخوارزمية**

من الضروري ضمان المساءلة الخوارزمية. يجب أن تكون المؤسسات التي تستخدم الذكاء الاصطناعي مسؤولة عن نتائج خوارزمياتها والعمل بنشاط على تقليل التحيز (الحجاج، ٢٠٢٢).

٤. **العدالة والأخلاق**

تطوير أنظمة الذكاء الاصطناعي مع العدالة والأخلاق في الاعتبار أمر حاسم. وهذا يشمل النظر في التأثيرات المحتملة على مجموعات مختلفة ومعالجة أي تحيز قد يظهر.

٥. **مجموعات تدريب بيانات متنوعة**

يمكن أن تساهم مجموعات التدريب المتنوعة والممثلة في تقليل التحيز. قد يتضمن ذلك جمع واستخدام البيانات من مصادر وفئات متنوعة (Nadimpalli, 2017).

٦. **تقنيات تقليل التحيز**

يعمل الباحثون على تطوير تقنيات لتقليل التحيز في أنظمة الذكاء الاصطناعي، مثل إعادة عينات البيانات لتحقيق توازن التمثيل، واستخدام خوارزميات تأهل العدالة، وأساليب معالجة ما بعد المعالجة (Cheatham, 2019).

٧. **الشفافية والقابلية للشرح**

جعل أنظمة الذكاء الاصطناعي أكثر شفافية وقابلة للشرح يمكن أن يساعد في تحديد ومعالجة التحيز. يجب على المستخدمين أن يتعرفوا على كيفية اتخاذ القرارات (Nadimpalli, 2017).

٨. **إطارات تنظيمية**

تقوم الحكومات بتنفيذ أو النظر في لوائح تتعلق بالذكاء الاصطناعي والتحيز. قد تتطلب هذه التنظيمات من المؤسسات أن تثبت العدالة في عمليات اتخاذ القرارات التي تعتمد على الذكاء الاصطناعي (Cheatham, 2019).

٩. **تدقيقات التحيز**

إجراء تدقيقات للتحيز في أنظمة الذكاء الاصطناعي أمر مهم. يتضمن ذلك تقييم النواتج وتحديد أي اختلافات أو أنماط تمييزية (النسور، ٢٠٢٢).

١٠. **المراقبة المستمرة**

يمكن أن يتطور التحيز في أنظمة الذكاء الاصطناعي مع مرور الوقت، وبالتالي، المراقبة المستمرة ضرورية لتحديد وتصحيح مصادر التحيز الجديدة (المجالي، ٢٠٢٣).

١١. **تعليقات المستخدم والتعويض**

توفير آليات للمستخدمين للإبلاغ عن التحيز المشتبه فيه في أنظمة الذكاء الاصطناعي والتعويض عنه يمكن أن يساعد في تحسين العدالة (النسور، ٢٠٢٢).

١٢. **التنوع في تطوير الذكاء الاصطناعي**

تعزيز التنوع في فرق تطوير الذكاء الاصطناعي يمكن أن يؤدي إلى وجهات نظر أكثر شمولًا وقد يقلل من التحيزات غير المقصودة في تصميم أنظمة الذكاء الاصطناعي (أحمد، ٢٠٢١).

١٣. **التعليم والوعي**

توعية المستخدمين والمطورين واتخاذ القرار حول مخاطر وتحديات التحيز في الذكاء الاصطناعي أمر حيوي. يمكن أن يؤدي الوعي الأكبر إلى ممارسات أفضل (المومني، ٢٠١٩).

معالجة التحيز والتمييز في الذكاء الاصطناعي هي عملية مستمرة تتطلب التعاون بين أصحاب التقنيات وصناع السياسات وأخلاقيين والمجتمع بشكل عام. من خلال اعتماد نهج نشط وأخلاقي، يمكن تطوير أنظمة الذكاء الاصطناعي التي تعزز العدالة والمساواة بدلاً من استمرار التحيزات الاجتماعية.

الهجمات السيبرانية الذاتية

الهجمات السيبرانية الذاتية، التي يقودها أنظمة الذكاء الاصطناعي، هي قضية متزايدة القلق في ميدان الأمن السيبراني. تشمل هذه الهجمات أدوات وخوارزميات تعتمد على الذكاء الاصطناعي يمكنها أتمتة وتنفيذ هجمات سيبرانية على نطاق وسرعة تتجاوز قدرات البشر، مما يجعل من الصعب الدفاع عن هذه التهديدات. فيما يلي نقاط رئيسية يجب مراعاتها: (المومني، ٢٠١٩)

١. **الهجمات المُؤتمتة**: يمكن للذكاء الاصطناعي أتمتة مراحل مختلفة من هجمة سيبرانية، بما في ذلك عمليات الاستطلاع، والاختراق، وسرقة البيانات، وحتى اتخاذ القرارات أثناء الهجوم، كما يمكن للأنظمة الذاتية أن تفحص الثغرات واستهدافها عبر مجموعة واسعة من الأهداف المحتملة بسرعة.
٢. **الحجم والسرعة**: يمكن للهجمات التي تعتمد على الذكاء الاصطناعي التوسع وتنفيذ هجمات بحجم ضخم، مستهدفة العديد من الأنظمة والأجهزة بشكل متزامن، كما يمكن أن تجاوز سرعة الهجمات الذاتية الدفاعات التقليدية للأمن السيبراني، مما يترك للمؤسسات وقتًا قليلًا للرد.

٣. **تكتيكات تكيفية:** يمكن للأنظمة الذاتية أن تتكيف وتتعلم من كل هجوم، مما يجعلها أكثر تطورًا وفعالية مع مرور الوقت، كما يمكن لخوارزميات الذكاء الاصطناعي تحديد واستغلال الثغرات الجديدة، مما يجعل من الصعب مواكبة التهديدات المتطورة.

٤. **هجمات مُستهدفة ومستمرة:** يمكن للأنظمة الذاتية أن تنفذ هجمات مُستهدفة بشكل كبير ضد منظمات معينة، أو صناعات، أو حتى أفراد، كما يمكن أن تشارك أيضًا في هجمات مستمرة، حيث تقوم بشكل مستمر بفحص الضحايا للبحث عن نقاط الضعف وشن الهجمات عندما تتاح الفرصة.

٥. **هجمات منع الخدمة:** يمكن استخدام الذكاء الاصطناعي لتنظيم هجمات قوية منع الخدمة الموزعة (**DDoS**) التي تعطل الشبكات والخدمات.

٦. **سرقة البيانات والتجسس:** (النسور، ٢٠٢٢)

- يمكن للأنظمة الذاتية أن تتمتع بالقدرة على أتمتة سرقة البيانات، حيث تقوم بسحب المعلومات الحساسة من الشبكات أو الأجهزة المخترقة.
- يمكن للجهات الممولة من الدولة استخدام الذكاء الاصطناعي في التجسس السيبراني، حيث تستهدف الحكومات والشركات والبنية التحتية الحيوية.

٧. **تحديات الكشف والدفاع:** كشف والدفاع ضد الهجمات الذاتية هو تحدي كبير. قد تكون الآليات التقليدية القائمة على القواعد والتوقيعات غير كافية، ويتعين استخدام أدوات الأمن التي تعتمد على الذكاء الاصطناعي للكشف عن التغيرات غير المألوفة وتحليل كميات ضخمة من البيانات والرد على التهديدات في الوقت الحقيقي (المجالي، ٢٠٢٣).

٨. **التعلم الآلي للدفاع:** الذكاء الاصطناعي ضروري لتطوير أنظمة أمن متكيفة يمكنها التعلم والرد على التهديدات المتطورة (Yigitcanlar, 2020).

٩. **التعاون ومشاركة المعلومات:** الجهود التعاونية ومشاركة المعلومات بين المؤسسات وخبراء الأمن السيبراني ضرورية لمواكبة الهجمات السيبرانية الذاتية (Müller, 2016).

١٠. **التنظيم والسياسة:** قد تحتاج الحكومات والهيئات التنظيمية إلى وضع إرشادات ولوائح للتعامل مع الهجمات السيبرانية الذاتية واستخدام الذكاء الاصطناعي في الأمن السيبراني (Scherer, 2015).

١١. **استخدام الذكاء الاصطناعي بشكل مسؤول:** الترويج لاستخدام التكنولوجيا بشكل مسؤول مهم. يجب على المطورين والمؤسسات النظر في الآثار الأخلاقية لعملهم والأفضلية للأمن السيبراني.

ارتفاع الهجمات السيبرانية الذاتية يؤكد على ضرورة اتباع نهج متكامل ونشط في مجال الأمن السيبراني، يجمع بين آليات الدفاع المتقدمة التي تعتمد على الذكاء الاصطناعي والتعاون والتنظيم وممارسات تطوير الذكاء الاصطناعي المسؤولة للتخفيف من تطور المشهد التهديدي (الحجاج، ٢٠٢٢).

فقدان السيطرة

فقدان السيطرة في أنظمة الذكاء الاصطناعي المستقلة، مثل السيارات ذاتية القيادة والطائرات بدون طيار، يشكل مخاطر أمن وخصوصية يجب معالجتها. فيما يلي بعض النقاط الرئيسية التي يجب النظر فيها: (الحجاج، ٢٠٢٢)

١. **مخاطر الأمن السيبراني**: تكون أنظمة الذكاء الاصطناعي المستقلة متصلة بالإنترنت وشبكات أخرى، مما يجعلها عرضة للهجمات السيبرانية. إذا تم اختراق هذه الأنظمة، يمكن استخدامها لأغراض خبيثة، بما في ذلك الوصول غير المصرح به، سرقة البيانات، أو تسبب الأذى الجسدي.
٢. **اختراق وبرامج ضارة**: يمكن للمهاجمين اختراق أنظمة الذكاء الاصطناعي المستقلة والسيطرة على عملياتها. على سبيل المثال، يمكن للجهات الخبيثة السيطرة على سيارة ذاتية القيادة، مما يشكل خطرًا على ركابها والمشاة، ويمكن استخدام برامج ضارة مصممة للطائرات بدون طيار لاعتراض البيانات، وتعطيل العمليات، أو السيطرة على وظائف الطائرة.
٣. **اهتمامات الخصوصية**: غالبًا ما تقوم الأنظمة المستقلة بجمع وإرسال البيانات، بما في ذلك معلومات الموقع وبيانات الاستشعار. يمكن أن يؤدي الوصول غير المصرح به إلى انتهاكات للخصوصية وتتبع حركة الأفراد.
٤. **مخاطر السلامة**: يمكن أن تعرض الأنظمة المستقلة المخترقة، خصوصًا في التطبيقات الحرجة مثل السيارات ذاتية القيادة أو الروبوتات الطبية، سلامة المستخدمين والجمهور للخطر.
٥. **المرونة والاحتياطي**: ضمان المرونة والاحتياطي للأنظمة المستقلة أمر حاسم. يجب أن تتوفر لديها إجراءات وآليات احتياطية للتخفيف من تأثير الاختراقات الأمنية.
٦. **الاتصال الآمن**: تشفير عمليات نقل البيانات وضمان التواصل الآمن بين الأنظمة المستقلة ومراكز التحكم يمكن أن يساعد في حماية ضد اعتراض البيانات والتلاعب بها.
٧. **المصادقة ومراقبة الوصول**: تنفيذ آليات المصادقة القوية ومراقبة الوصول يمكن أن يساعد في منع الوصول غير المصرح به إلى الأنظمة المستقلة.
٨. **تحديثات البرامج الآمنة**: يجب أن تتلقى الأنظمة المستقلة تحديثات برامج آمنة ومحدثة بانتظام لسد الثغرات والدفاع ضد التهديدات السيبرانية.

٩. **الأطُر الأخلاقية والقانونية:** إنشاء أطُر أخلاقية وقانونية لاستخدام الأنظمة المستقلة المدعومة بالذكاء الاصطناعي أمر ضروري. ويتضمن ذلك المسؤولية والمسائلة في حالة حدوث انتهاكات للأمن أو سوء الاستخدام (Scherer, 2015).

١٠. **التنظيم والمعايير:** قد تحتاج الحكومات وهيئات الصناعة إلى وضع لوائح ومعايير لأمن الأنظمة المستقلة المدعومة بالذكاء الاصطناعي، لضمان موقف أمان ثابت وقوي (Osoba, 2017).

١١. **وعي المستخدم والتدريب:** يجب أن يتلقى المستخدمون ومشغلو الأنظمة المستقلة تدريبًا حول أفضل الممارسات الأمنية لمنع الهجمات والاستجابة للحوادث الأمنية (Raso, 2018).

١٢. **خطط استجابة للحوادث:** وجود خطط استجابة للحوادث محددة بشكل جيد أمر حاسم. يجب أن توضح هذه الخطط الخطوات التي يجب اتخاذها في حالة حدوث اختراق للأمن أو فقدان السيطرة.

١٣. **تقييم الأمان المستمر:** تقييم الأمن بانتظام للأنظمة المستقلة أمر أساسي. ويشمل ذلك اختبار الثغرات واختبار الاختراق والمراقبة المستمرة (Osoba, 2017).

معالجة فقدان السيطرة في أنظمة الذكاء الاصطناعي المستقلة تتطلب مزيجًا من الحواجز التكنولوجية والتنظيم والتعليم والاستخدام المسؤول، ومن الضروري التخفيف من المخاطر المرتبطة بانتهاكات الأمن المحتملة والوصول غير المصرح به إلى هذه الأنظمة.

نقص التنظيمات والمعايير الكافية

نقص التنظيمات والمعايير في ميدان الذكاء الاصطناعي يشكل تحديات كبيرة ويمكن أن ينتج عنه فجوات في حماية الأمن والخصوصية. فيما يلي بعض النقاط الرئيسية التي يجب النظر فيها: (Raso, 2018)

١. **تقنية متطورة:** تتقدم تقنية الذكاء الاصطناعي بسرعة، والتنظيمات الحالية قد تجد صعوبة في مجاراة المشهد المتغير باستمرار، مما يترك القضايا الحرجة دون عناوين.

٢. **رقابة متشعبة:** تكون التنظيمات والمعايير للذكاء الاصطناعي متشعبة، حيث تمتلك الأقاليم والمؤسسات المختلفة قوانينها الخاصة، مما يؤدي إلى عدم تنسيق في معالجة مخاوف الأمن والخصوصية.

٣. **اهتمامات الخصوصية:** تنتج التنظيمات الناقصة في حماية خصوصية الأفراد، مما يتيح لجمع البيانات الشخصية واستخدامها ومشاركتها بشكل غير لائق.

٤. **ثغرات الأمن:** تفشل التنظيمات الضعيفة أو التي لم تُحدث منذ فترة طويلة في المطالبة باتخاذ إجراءات أمن كافية لأنظمة الذكاء الاصطناعي، مما يترك ثغرات يمكن استغلالها من قبل الجهات الخبيثة.

٥. **اعتبارات أخلاقية:** لا تتم معالجة الاعتبارات الأخلاقية، مثل تلك المتعلقة بالتحيز والعدالة والشفافية والمساءلة، بشكل كافٍ في الأطُر التنظيمية، مما يمكن أن يؤدي إلى انتهاكات أخلاقية محتملة.

٦. **المسؤولية والمسائلة:** تكون هناك قواعد واضحة بشأن المسؤولية والمسائلة في حالة حدوث حوادث أو حوادث متعلقة بالذكاء الاصطناعي غائبة، مما يجعل من الصعب تحميل المسؤولية عندما تحدث أمور خاطئة.

٧. **قضايا عابرة للحدود:** يعمل الذكاء الاصطناعي عبر الحدود، ونقص التنظيمات الدولية الموحدة يمكن أن يخلق تحديات في معالجة مخاوف الأمن والخصوصية على نطاق عالمي.

٨. **حجب تنظيمي:** لا تناسب التطبيقات وحالات الاستخدام الجديدة للذكاء الاصطناعي تمامًا في فئات التنظيم الحالية، مما يؤدي إلى حجب تنظيمي.

٩. **حماية البيانات:** يضر نقص التنظيمات بجهود حماية البيانات، خصوصًا في الحالات حيث يتم استخدام البيانات الشخصية في تدريب أنظمة الذكاء الاصطناعي.

١٠. **حماية المستهلك:** تترك التنظيمات الضعيفة المستهلكين ومستخدمي أنظمة الذكاء الاصطناعي بحماية غير كافية ضد الممارسات الخادعة أو الضارة للذكاء الاصطناعي.

١١. **الابتكار والاستثمار:** تقم التنظيمات الزائدة القيد أو الغامضة بمثل هذا النوع من القيود بقمع الابتكار وردع الاستثمار في تطوير الذكاء الاصطناعي.

١٢. **التعليم والوعي:** يفتقر العديد من أصحاب المصلحة، بما في ذلك صناع السياسات، إلى فهم عميق لتكنولوجيا الذكاء الاصطناعي، مما يمكن أن يعيق تطوير التنظيمات الفعالة.

١٣. **تحقيق التوازن بين المصالح:** تطوير التنظيمات التي تجمع بين تعزيز الابتكار وحماية مصالح الأمن والخصوصية هو مهمة معقدة.

معالجة تحديات نقص التنظيمات والمعايير في مجال الذكاء الاصطناعي تتطلب نهجًا متعدد الجوانب. يشمل ذلك التعاون المستمر بين الحكومات والصناعة والخبراء، والتركيز على الاعتبارات الأخلاقية، والالتزام بضبط التنظيمات وفقًا لتطور المشهد في مجال الذكاء الاصطناعي مع ضمان معالجة مخاوف الأمن والخصوصية بشكل كاف.

المبحث الثاني: مخاطر الذكاء الاصطناعي لأمن المعلومات على مستقبل المنظمات

يقدم الذكاء الاصطناعي (**AI**) العديد من الفوائد والفرص، ولكنه يمثل أيضًا العديد من المخاطر والتحديات لأمن المعلومات على مستقبل المنظمات. وفي هذا المبحث سأقوم بذكر بعض المخاطر الرئيسية المرتبطة بالذكاء الاصطناعي وأمن المعلومات (الحجاج، ٢٠٢٢).

التشغيل الآلي للعمليات الروبوتية (RPA)

أمن نظام الأتمتة العمليات الروبوتية (**RPA**) أمر بالغ الأهمية. هنا بعض نقاط الضعف التي يجب أخذها في الاعتبار لضمان أمن الأتمتة العمليات الروبوتية:

١. **الوصول غير المصرح به:** الجهات الضارة يمكنها محاولة استغلال الضعف في أنظمة **RPA** للوصول غير المصرح به إلى الأنظمة والبيانات. لحماية ذلك، يجب تنفيذ إجراءات صارمة لمراقبة وإدارة وصول المستخدمين وضمان أن يتم تقديم الصلاحيات بشكل صحيح (Osoba, 2017).

٢. **الثغرات الأمنية في البرمجيات:** تحتوي البرمجيات المستخدمة في أنظمة **RPA** على ثغرات أمنية. هذه الثغرات يمكن أن تكون نقطة هجوم للمهاجمين. يجب تحديث ومراقبة البرمجيات بانتظام وتنفيذ إجراءات إصلاح فوري لأي ثغرات تم اكتشافها (الحجاج، ٢٠٢٢).

٣. **تهيئة غير آمنة:** تكون تهيئة أنظمة **RPA** المفتوحة للهجمات إذا لم يتم ضبطها بشكل صحيح. يجب ضمان أن تكون الإعدادات آمنة وتتبع أفضل الممارسات لتأمين النظام (أحمد، ٢٠٢١).

٤. **تحديث البرمجيات:** الإصدارات القديمة من البرمجيات قد تحمل ثغرات أمنية معروفة. يجب تحديث جميع البرمجيات المستخدمة في أنظمة **RPA** بانتظام للحفاظ على الأمن (المومني، ٢٠١٩).

٥. **القضايا المتعلقة بالمصدر المفتوح:** إذا كانت أنظمة **RPA** تستخدم مكونات مصدر مفتوح، يجب مراقبتها بعناية والتحقق من أمانها. البرمجيات مفتوحة المصدر يمكن أن تحتوي على ثغرات أمنية يمكن استغلالها (النسور، ٢٠٢٢).

٦. **حقوق الوصول:** يجب تقييم منح الوصول بعناية وضمان أن يتم منح الصلاحيات بناءً على الحاجة والحد الأدنى الضروري لأداء المهام المحددة. الوصول غير المبرر يزيد من خطر الاختراق (العمر، ٢٠٢٢).

٧. **التحقق من الهوية والمصادقة:** يجب توظيف تقنيات قوية للتحقق من هوية المستخدمين وضمان أن الوصول يقتصر على الأشخاص المصرح لهم فقط (المجالي، ٢٠٢٣).

٨. **مراقبة الأنشطة:** ينبغي تسجيل ومراقبة الأنشطة التي تتم عبر أنظمة **RPA** هذا يمكن أن يساعد في كشف أي أنشطة غير مصرح بها (الأسدي، ٢٠٢٢).

٩. **التدريب والتوعية:** يجب توفير التدريب والتوعية للموظفين حول مخاطر الأمن المحتملة وكيفية التصرف في حالة الاكتشاف.

١٠. **استراتيجية الاستجابة للحوادث:** يجب وضع استراتيجية استجابة للحوادث للتعامل مع الهجمات المحتملة واستعادة الأنظمة بسرعة في حالة وقوع اختراق.

توفير أمان قوي لأنظمة **RPA** يتطلب تنفيذ مجموعة من إجراءات الأمن ومراقبة مستمرة لضمان حماية الأنظمة والبيانات من التهديدات المحتملة.

الذكاء الاصطناعي في المصادقة

استخدام الذكاء الاصطناعي في أنظمة المصادقة البيومترية والسلوكية يمكن أن يكون مزيدًا من التطور التكنولوجي ولكنه يثير أيضًا مخاوف أمنية مهمة. القضية الرئيسية تكمن في قدرة الذكاء الاصطناعي على تقليد سمات بيومترية أو سلوكية معينة بهدف الوصول غير المصرح به أو الانتحال. هذا يمكن أن يؤدي إلى تعرض الأنظمة والبيانات لمخاطر محتملة. لمواجهة هذه التحديات، يمكن اتباع بعض الإجراءات: (المومني، ٢٠١٩)

١. **الاستدلال المتعدد**: دمج أنظمة المصادقة البيومترية والسلوكية مع أنظمة مصادقة أخرى مثل كلمات المرور أو رموز التحقق لزيادة الأمن وتعزيز الصعوبة في الوصول غير المصرح به.
٢. **مراقبة السلوك**: استخدام الذكاء الاصطناعي لمراقبة سلوك المستخدمين بشكل مستمر لاكتشاف أي تغييرات غير مألوفة تشير إلى انتحال الشخصية.
٣. **الكشف عن التزوير**: تطوير أنظمة الذكاء الاصطناعي للكشف عن محاولات التزوير باستخدام تقنيات مثل تحليل الأنماط والتعرف على الصور.
٤. **تحليل السلوك الديناميكي**: استخدام الذكاء الاصطناعي لتحليل السلوك الديناميكي للمستخدم، مثل طريقة المشي أو نمط الكتابة، والتحقق من صحته بشكل مستمر.
٥. **التحقق المتعدد العوامل**: استخدام أنظمة التحقق المتعدد العوامل لزيادة الأمن، حيث يتعين على المستخدم تقديم أكثر من عامل للوصول.
٦. **التعلم الآلي**: استخدام تقنيات التعلم الآلي لتحسين قدرة النظام على التعرف على الانتحال والمحاولات غير المصرح بها بناءً على السلوك والبيانات البيومترية.

هذه الإجراءات تهدف إلى تعزيز الأمان في أنظمة المصادقة البيومترية والسلوكية والتقليل من مخاطر الانتحال وانتحال الشخصية. ومع ذلك، يجب أن يكون التوازن دائمًا بين الأمن وسهولة الاستخدام، حيث يجب أن تكون الأنظمة فعالة من الناحية الأمنية وفي الوقت نفسه سهلة الاستخدام للمستخدمين.

التصيد المعزز بالذكاء الاصطناعي

هو تقنية تستخدم الذكاء الاصطناعي لتصميم وتنفيذ هجمات تصيُّد البيانات(**Phishing**) بشكل أكثر تطورًا وفعالية. يمكن أن يشمل التصيد المعزز بالذكاء الاصطناعي العناصر التالية: (Cheatham, 2019)

١. **إنشاء رسائل مقنعة:** باستخدام تقنيات التوليد النصي وتوليد اللغة الطبيعية (**NLP**)، يمكن للذكاء الاصطناعي إنشاء رسائل بريد إلكتروني أو رسائل نصية تبدو مقنعة بشكل مذهل. هذه الرسائل يمكن أن تحتوي على تفاصيل شخصية مزيفة وروابط ضارة.

٢. **استهداف مستهدف:** بفضل التحليل الذكي للبيانات العامة والتواصل الاجتماعي، يمكن للمهاجمين تحديد الأفراد أو المؤسسات المستهدفة بشكل أفضل. هذا يزيد من نجاح الهجمات وقدرتها على الوصول إلى الأهداف المرغوبة.

٣. **اختزال النصوص:** للذكاء الاصطناعي طرق لتخصيص الرسائل للأفراد بناءً على المعلومات المتاحة عنهم. يتيح ذلك للرسائل أن تبدو أكثر مصداقية وتخصيصًا.

٤. **تجنب الكشف:** باستخدام تقنيات متقدمة، يمكن للمهاجمين تجنب الكشف عن هويتهم ومصادر الهجوم. يمكن استخدام خوادم بروكسي وتقنيات أخرى لإخفاء أثرهم.

٥. **استغلال ثغرات نفسية:** للذكاء الاصطناعي إمكانية لتحليل سلوك الأفراد واستخدام معلومات نفسية لجعل الرسائل أكثر إغراءً بالنسبة للمتلقين.

للتصدي لهذه الهجمات، يجب على المؤسسات والأفراد اتخاذ الإجراءات الوقائية من بينها: (الحجاج، ٢٠٢٢)

- **التعليم والتوعية:** تعليم الموظفين والأفراد حول مخاطر التصيُّد وكيفية التعرف على الهجمات.
- **استخدام أدوات أمن البريد الإلكتروني:** تنفيذ حلول أمن البريد الإلكتروني التي تمكن من اكتشاف ومنع رسائل التصيُّد.
- **التحقق من الهوية:** استخدام تقنيات التحقق من الهوية مثل مصادقة العاملين بعاملين (**MFA**) للحماية من هجمات التصيُّد.
- **التحديث الدوري:** تحديث البرمجيات والأنظمة بانتظام لسد الثغرات الأمنية المعروفة.
- **مراقبة الأنشطة الشبكية:** مراقبة الأنشطة الشبكية للكشف عن نشاط مشبوه واستجابة سريعة.
- **التبليغ عن الهجمات:** تبليغ عن أي هجوم تصيُّد يتم اكتشافه للسلطات المعنية ولمزودي الخدمات الأمنية.

التصيُّد المعزز بالذكاء الاصطناعي يمثل تهديدًا متزايدًا، ولذلك يجب أن تكون استراتيجيات الأمن جاهزة لمكافحته.

مخاطر سلسلة التوريد

هي قضية هامة تتعلق بأنظمة الذكاء الاصطناعي وغالباً ما تشمل مشكلات مثل المكونات الملوثة أو البرامج المخترقة. إليك بعض النقاط المهمة حول هذه المخاطر: (الحجاج، ٢٠٢٢)

١. **المكونات الملوثة:** تحمل المكونات المستخدمة في تطوير نظام الذكاء الاصطناعي ثغرات أمنية غير مكتشفة أو برمجيات ملوثة. يمكن أن تُضاف هذه المكونات الملوثة إلى سلسلة التوريد بدون علم المستخدم النهائي.

٢. **البرمجيات المخترقة:** يتم اختراق البرامج المستخدمة في تطوير وتشغيل الذكاء الاصطناعي، مما يجعلها عرضة للهجمات. يمكن أن يتم تضمين برمجيات مخترقة في التحديثات أو التحسينات البرمجية التي تأتي من مصادر غير موثوقة.

٣. **القيود الجغرافية:** تكون هناك مشكلات في سلسلة التوريد تتعلق بالقيود الجغرافية، حيث يتم إنتاج المكونات أو البرمجيات في مناطق تخضع لتشريعات أمن مختلفة أو تحت قيود تصدير.

٤. **التحقق من الأمن في سلسلة التوريد:** من الضروري تنفيذ ممارسات التحقق من الأمن في سلسلة التوريد للتحقق من نوعية المكونات والبرمجيات المستخدمة. يجب على الشركات التحقق من مصدر المكونات والتحقق من أمانها قبل استخدامها.

٥. **التوثيق والمراقبة:** يجب على الشركات والمنظمات أن تقوم بتوثيق مكونات سلسلة التوريد ومراقبتها بعناية للكشف عن أي مشاكل أمنية محتملة.

٦. **التعاون مع الموردين:** التواصل والتعاون مع الموردين لفهم وتقليل المخاطر في سلسلة التوريد يمكن أن يكونا مهمين لضمان الأمن.

تجنب هذه المخاطر يتطلب مراعاة أمن سلسلة التوريد كجزء أساسي من استراتيجية الأمن وتنفيذ سياسات صارمة للتحقق من الأمن ومراقبة الجودة في جميع مكونات الذكاء الاصطناعي.

التحديات التنظيمية

تمثل جزءًا مهمًا من التحديات التي تواجه المؤسسات والحكومات في العصر الرقمي. إليك بعض التحديات التنظيمية الرئيسية: (Yigitcanlar, 2020)

١. **تطوير التشريعات واللوائح:** يتطلب التنظيم الفعال للذكاء الاصطناعي وأمن المعلومات وضع قوانين ولوائح تنظم استخدام وتطوير التقنيات المتقدمة. هذا يشمل قوانين حماية البيانات وتنظيم استخدام البيانات الحساسة ومسائل أخرى.

٢. **تحقيق التوازن بين الأمن والابتكار:** تحتاج المؤسسات إلى التوازن بين تعزيز الأمن وتشجيع الابتكار. تطبيق أمن فعال للذكاء الاصطناعي يجب أن يكون جزءًا من العمليات الأساسية دون أن يكون عقبة أمام التقدم التكنولوجي.

٣. **مراجعة الأخلاقيات والتأثير الاجتماعي**: تحتاج اللوائح إلى تضمين مبادئ أخلاقية لاستخدام الذكاء الاصطناعي بشكل مسؤول، بما في ذلك معالجة مسائل مثل التمييز والخصوصية والتأثير على الوظائف والمجتمع.

٤. **التعاون الدولي**: التحديات التنظيمية تمتد عبر الحدود، ولذلك يجب تعزيز التعاون الدولي لتطوير معايير ولوائح دولية تساعد في توجيه التقدم التكنولوجي وتحقيق الأمن.

٥. **توجيه الاستثمار**: تحتاج الحكومات والمؤسسات إلى توجيه الاستثمار في الأمن والأبحاث ذات الصلة بالذكاء الاصطناعي. هذا يشمل دعم البحث والتطوير وتوجيه الاموال نحو تعزيز الأمن التكنولوجي.

٦. **تحفيز الامتثال**: يجب على الحكومات والمنظمات تشجيع الامتثال باللوائح وتنفيذه. يجب أيضًا تحفيز الشركات والمؤسسات على تطوير سياسات داخلية تعزز من أمن الذكاء الاصطناعي.

٧. **تعليم وتوعية**: تعزيز التوعية وتوجيه التعليم حول أمن الذكاء الاصطناعي هو جزء مهم من التحديات التنظيمية. يتعين على الموظفين والجمهور الفهم الجيد للمخاطر وكيفية تجنبها.

تحقيق التوازن بين الابتكار والأمن يمكن أن يكون تحديًا صعبًا، ولكنه ضروري لضمان استفادة مجتمعاتنا من فوائد التقنيات المتقدمة دون تعريض الأمن والخصوصية للتهديد.

المبحث الثالث: التخفيف من مخاطر الذكاء الاصطناعي

للتخفيف من هذه المخاطر، من الأمور الحاسمة اعتماد ممارسات أمن قوية وتطوير الذكاء الاصطناعي بشكل أخلاقي واتخاذ إجراءات لحماية الخصوصية. وتشمل ذلك: (Scherer, 2015)

- **حماية البيانات**: تنفيذ تشفير البيانات القوي وضوابط الوصول وتقنيات التعمية لحماية المعلومات الحساسة.
- **الفحوصات والاختبارات الدورية**: اختبار أنظمة الذكاء الاصطناعي بشكل مستمر للبحث عن الثغرات وإجراء فحوصات أمان لتحديد ومعالجة الضعف.
- **تطوير الذكاء الاصطناعي بشكل أخلاقي**: التأكد من تدريب نماذج الذكاء الاصطناعي على مجموعات بيانات متنوعة وممثلة، وتقييم ومعالجة التحيز في خوارزميات الذكاء الاصطناعي بانتظام.
- **إرشادات الأخلاق في الذكاء الاصطناعي**: التمسك بإرشادات ومعايير أخلاقية عند تطوير ونشر أنظمة الذكاء الاصطناعي، مع مراعاة التأثير على الخصوصية والأمن.
- **التوعية بالأمن السيبراني**: تثقيف المستخدمين والمنظمات حول التهديدات المتعلقة بالذكاء الاصطناعي وتشجيع أفضل الممارسات للأمن والخصوصية.

- **التشريع والتنظيم**: يجب على الحكومات والمنظمات العمل سوياً لتطوير وفرض التشريعات التي تعالج مخاوف الأمن والخصوصية المتعلقة بالذكاء الاصطناعي.

معالجة تخفيف المخاطر الناتجة من الذكاء الاصطناعي

تعتبر معالجة هذه المخاطر هي تحدٍ مستمر، وتتطلب جهداً تعاونياً من الحكومات والشركات والباحثين والأفراد لضمان تطوير التقنيات الذكية بشكل مسؤول وآمن.

بالإضافة إلى تقديم لمحة عن التحديات المقبلة، فإن الأمثلة والتصنيفات المذكورة أعلاه مفيدة لتحديد المخاطر وترتيب أولوياتها وأسبابها الجذرية. إذا فهمت الأماكن التي قد تكون فيها المخاطر كامنة، أو غير مفهومة، أو ببساطة غير محددة، فلديك فرصة أفضل للقبض عليها قبل أن تلحق بك.

ولكنك ستحتاج إلى جهد مركز على مستوى المؤسسة للانتقال من فهرسة المخاطر إلى استئصالها. وتساعد تجارب اثنين من البنوك الرائدة في توضيح الوضوح والاتساع والدقة الدقيقة المطلوبة الأول، يعمل على تطبيق التحليلات المتقدمة وقدرات الذكاء الاصطناعي لتحسين مركز الاتصال، واتخاذ قرارات الرهن العقاري، وإدارة العلاقات، ومبادرات إدارة الخزانة. والثانية هي شركة عالمية رائدة تسعى إلى تطبيق نموذج التعلم الآلي على قراراتها المتعلقة بائتمان العملاء.

استخدم منهج لتحديد المخاطر الأكثر أهمية

بدأ المدير التنفيذي للعمليات في البنك الأوروبي بجمع قادة من قطاع الأعمال وتكنولوجيا المعلومات والأمن وإدارة المخاطر لتقييم المخاطر الكبرى وتحديد أولوياتها. تضمنت المدخلات نظرة واضحة على المخاطر الحالية التي تواجهها الشركة وكيف يمكن أن تتفاقم بسبب جهود التحليلات القائمة على الذكاء الاصطناعي قيد النظر، والمخاطر الجديدة التي يمكن أن تخلقها عوامل تمكين الذكاء الاصطناعي، أو الذكاء الاصطناعي نفسه، وكان بعضها واضحاً، ولكن البعض الآخر أقل من ذلك، ان أحد الأشياء التي اقتربت بشكل غير متوقع من أعلى القائمة كان تقديم توصيات منتجات سيئة أو متحيزة للمستهلكين. يمكن أن تؤدي مثل هذه التوصيات المعيبة إلى قدر كبير من الضرر بما في ذلك خسائر المستهلكين ورد الفعل العنيف والغرامات التنظيمية.

إن ما حققه قادة البنك من خلال هذه العملية المنظمة لتحديد المخاطر هو الوضوح بشأن السيناريوهات الأكثر إثارة للقلق، وهو ما سمح لهم بتحديد أولويات المخاطر المشمولة، والتعرف على الضوابط التي كانت مفقودة، وتنظيم الوقت والموارد وفقا لذلك. ومن الطبيعي أن تختلف هذه السيناريوهات والمخاطر ذات الأولوية حسب الصناعة والشركة، قد تعطي الشركة المصنعة للأغذية الأولوية لسيناريوهات المنتجات الملوثة. قد يكون مطور البرامج قلقًا بشكل خاص بشأن الكشف عن كود البرنامج، قد تركز منظمة الرعاية الصحية على قضايا مثل التشخيص الخاطئ للمريض أو التسبب في ضرر للمرضى عن غير قصد، يعد الحصول على مجموعة متنوعة من المديرين الذين يركزون على تحديد السيناريوهات الإشكالية وتصنيفها طريقة جيدة لتحفيز الطاقة الإبداعية

وتقليل خطر إغفال المتخصصين الضيقين أو التفكير ضيق الأفق لنقاط الضعف الرئيسية، لا ينبغي للمؤسسات أن تبدأ من الصفر بهذه الجهود على مدى السنوات القليلة الماضية، أصبح تحديد المخاطر فنًا متطورًا، ويمكن نشره مباشرة في سياق الذكاء الاصطناعي.

الاتساع: إنشاء ضوابط قوية على مستوى المؤسسة

من الأمور الحاسمة أيضًا تطبيق الضوابط على مستوى الشركة لتوجيه تطوير واستخدام أنظمة الذكاء الاصطناعي، وضمان الرقابة المناسبة، ووضع سياسات وإجراءات قوية وتدريب العمال وخطط الطوارئ. وبدون بذل جهود واسعة النطاق، فإن احتمالات فشل عوامل الخطر مثل تلك التي تم وصفها سابقًا قد تتلاشى.

وانطلاقاً من القلق إزاء المخاطر المحتملة الناجمة عن توصيات المنتجات الرديئة أو المتحيزة، بدأ البنك الأوروبي في تبني مجموعة قوية من مبادئ العمل التي تهدف إلى تفصيل كيف وأين يمكن استخدام الآلات لاتخاذ القرارات التي تؤثر على الصحة المالية للعميل. حدد المديرون المواقف التي يحتاج فيها الإنسان (على سبيل المثال، مدير العلاقات أو مسؤول القروض) إلى أن يكون قبل تسليم التوصية إلى العميل. سيوفر هؤلاء العمال شبكة أمنية لتحديد ما إذا كان العميل يعاني من ظروف خاصة، مثل وفاة أحد أفراد الأسرة أو صعوبات مالية، قد تجعل التوصية في وقت غير مناسب أو غير مناسبة.

كما أجرت لجنة الإشراف في البنك تحليلاً للفجوات، فحددت المجالات في إطار إدارة المخاطر الحالي في البنك والتي تحتاج إلى تعميق، أو إعادة تعريف، أو توسيع.

وتضمن الحوكمة الشاملة والمتسقة في البنك التعريف المناسب للسياسات والإجراءات، وضوابط محددة لنماذج الذكاء الاصطناعي، والمبادئ الأساسية (المدعومة بالأدوات) لتوجيه تطوير النماذج، والفصل بين الواجبات والرقابة الكافية على سبيل المثال، تضمن أدوات تطوير النماذج قيام علماء البيانات بتسجيل رمز النموذج وبيانات التدريب والمعلمات المختارة باستمرار طوال دورة حياة التطوير.

كما تم اعتماد المكتبات القياسية لقابلية الشرح، وإعداد تقارير أداء النماذج، ومراقبة البيانات والنماذج في الإنتاج. أثبت إطار الحوكمة أنه لا يقدر بثمن بالنسبة لجهود تطوير الذكاء الاصطناعي الداخلية ولتقييم ومراقبة أدوات الذكاء الاصطناعي التابعة لجهات خارجية مثل نموذج الاحتيال **SaaS** الذي اعتمده البنك.

بالإضافة إلى ذلك، تتطلب سياسات البنوك من جميع أصحاب المصلحة، بما في ذلك مديري الأعمال الرعاة، إجراء تخطيط السيناريو وإنشاء خطة احتياطية في حالة انحراف أداء نموذج الذكاء الاصطناعي، أو تحول مدخلات البيانات بشكل غير متوقع، أو حدوث تغييرات مفاجئة، مثل الكوارث الطبيعية، في بيئة خارجية. يتم تضمين هذه الخطط الاحتياطية في عملية مراجعة المخاطر المنتظمة للبنك، مما يمنح لجنة المخاطر التابعة لمجلس الإدارة رؤية واضحة للخطوات التي يتم اتخاذها للتخفيف من المخاطر المرتبطة بالتحليلات والمتعلقة بالذكاء الاصطناعي.

كما يحتل تدريب العمال وتوعيتهم مكانة بارزة في جهود البنك لتخفيف المخاطر. يتلقى جميع الموظفين المتأثرين اتصالات شاملة حول مكان استخدام الذكاء الاصطناعي وكيفية عمل إطار حوكمة البنك والتكنولوجيا الآلية وأدوات التطوير معًا. بالإضافة إلى ذلك، يتلقى رعاة الأعمال وفرق المخاطر وموظفي التحليلات تدريبًا مستهدفًا حول دورهم في تحديد المخاطر وتقليلها.

تعد مراقبة التحليلات المعتمدة على الذكاء الاصطناعي جهدًا مستمرًا، وليست نشاطًا منفردًا. على هذا النحو، تقوم مجموعات الرقابة التابعة للبنك، بما في ذلك لجان المخاطر التابعة لمجلس الإدارة، بمراجعة البرنامج بانتظام للبقاء على اطلاع على المخاطر الجديدة التي قد تنشأ نتيجة للتغييرات التنظيمية، والتحولات الصناعية، والتفسيرات القانونية (مثل السوابق القضائية الناشئة في القانون العام لحماية البيانات)، توقعات المستهلكين المتطورة، والتكنولوجيا المتغيرة بسرعة.

الفروق الدقيقة: تعزيز ضوابط محددة اعتمادا على طبيعة المخاطر

على الرغم من أهمية الضوابط على مستوى المؤسسة، إلا أنها نادرًا ما تكون كافية لمواجهة كل المخاطر المحتملة، غالبًا ما تكون هناك حاجة إلى مستوى آخر من الدقة والفروق الدقيقة، وستعتمد الضوابط المطلوبة على عوامل مثل مدى تعقيد الخوارزميات، ومتطلبات البيانات الخاصة بها، وطبيعة التفاعل بين الإنسان والآلة (أو من آلة إلى آلة)، واحتمالية حدوث ذلك للاستغلال من قبل الجهات الفاعلة السيئة، ومدى دمج الذكاء الاصطناعي في العمليات التجارية. الضوابط المفاهيمية، بدءًا من ميثاق حالة الاستخدام، تكون ضرورية في بعض الأحيان وكذلك الأمر بالنسبة لضوابط البيانات والتحليلات المحددة، بما في ذلك متطلبات الشفافية، فضلاً عن ضوابط التغذية الراجعة والمراقبة، مثل تحليل الأداء للكشف عن التدهور أو التحيز.

يلقي مثالنا الثاني ضوءًا قيمًا على تطبيق الضوابط الدقيقة، أرادت هذه المؤسسة رؤية كيفية اتخاذ نموذج التعلم الآلي للقرارات المتعلقة بعملية معينة تواجه العملاء، وبعد النظر بعناية في متطلبات الشفافية، قررت المؤسسة التخفيف من المخاطر عن طريق الحد من أنواع خوارزميات التعلم الآلي التي تستخدمها. إن عدم السماح ببعض النماذج النموذجية التي كانت مفرطة في التعقيد والغموض مكّن المؤسسة من تحقيق التوازن الذي كانت مريحة له. وفقدت بعض القدرة التنبؤية، الأمر الذي كان له تكاليف اقتصادية. لكن شفافية النماذج المستخدمة أعطت الموظفين ثقة أكبر في القرارات التي اتخذوها. كما سهّلت النماذج الأبسط فحص البيانات والنماذج نفسها بحثًا عن أي تحيزات قد تنشأ عن سلوك المستخدم أو التغييرات في متغيرات البيانات أو تصنيفاتها.

وكما يوحي هذا المثال، ستحتاج المؤسسات إلى مزيج من الضوابط الخاصة بالمخاطر، وأفضل طريقة لتطبيقها هي إنشاء بروتوكولات تضمن وجودها ومتابعتها طوال عملية تطوير الذكاء الاصطناعي. قامت كثير من المؤسسات التجارية بتنفيذ هذه البروتوكولات التي قدمناها بتنفيذ هذه البروتوكولات، فضلاً عن الضوابط على مستوى المؤسسة، جزئياً على الأقل، من خلال البنية التحتية الحالية للمخاطر. لا يزال بإمكان الشركات التي

تفتقر إلى منظمة مركزية للمخاطر استخدام تقنيات إدارة مخاطر الذكاء الاصطناعي هذه في العمل باستخدام عمليات قوية لإدارة المخاطر.

ما يمكن أن تفعله المنظمات للتخفيف من مخاطر الذكاء الاصطناعي

أ. وضع مبادئ للتوجيه: مجموعة من المبادئ الأخلاقية التي تتبناها وتدعمها القيادة توفر نجمة الشمال للمنظمة. ومع ذلك، فإن المبادئ في حد ذاتها ليست كافية لتضمين ممارسات الذكاء الاصطناعي المسؤولة. يحتاج أصحاب المصلحة إلى النظر في المبادئ في سياق عملهم اليومي لتصميم السياسات والممارسات التي يمكن للشركة بأكملها أن تلتزم بها.

ب. خذ بعين الاعتبار ملكية الحوكمة: لحسن الحظ، يهتم العديد من القادة داخل المؤسسات بتأسيس ممارسات حوكمة الذكاء الاصطناعي والبيانات. ومع ذلك، بدون تحديد مالك لهذه الإدارة، فمن المرجح أن تجد المنظمة نفسها أمام مشكلة مختلفة ممارسات منفصلة قد تتعارض مع بعضها البعض. حدد الفرق التي يجب عليها تصميم مناهج الحوكمة، والاتفاق على المالك وعملية تحديد التحديثات للسياسات الحالية بالإضافة إلى تنفيذ عمليات موحدة للتطوير والمراقبة، مع بوابات مرحلة محددة للإشارة إلى المكان الذي يلزم الحصول على الموافقات والمراجعات للمضي قدمًا، يجب أن ترتبط هذه العملية بآليات إدارة البيانات والخصوصية الحالية بالإضافة إلى دورة حياة تطوير البرمجيات.

ج. كسر الصوامع: بالمواءمة بين مجموعات أصحاب المصلحة الضرورية لربط الفرق لأغراض تبادل الأفكار والممارسات الرائدة بإنشاء قوائم جرد مشتركة للذكاء الاصطناعي والبيانات الخاصة بعملية الحوكمة، واستخدم هذا التمرين كفرصة للنظر في التغييرات الهيكلية أو عمليات إعادة التنظيم التي يمكن أن تمكن الشركة من العمل بشكل أفضل.

د. راقب المناخ التنظيمي سريع التغير: لا يقتصر الأمر على العملاء والمستثمرين والموظفين الذين يطالبون بممارسات مسؤولة ينتبه المنظمون ويقترحون التشريعات على مستوى الولاية والجهة التنظيمية والوطنية وفوق الوطنية. وتنبع بعض التنظيمات من الجهود الموسعة لحماية البيانات والخصوصية، وبعضها من جهات تنظيمية محددة في مجالات حالات الاستخدام الضيقة (مثل الخدمات المصرفية)، وبعضها من رغبة أكثر عمومية في تحسين المساءلة (مثل قانون الذكاء الاصطناعي في الاتحاد الأوروبي). تعد مواكبة هذه اللوائح أمرًا أساسيًا لتحديد أنشطة الامتثال المستقبلية.

الدراسات السابقة

تمهيد

يشهد العصر الحالي تطوراً متسارعاً في مجال التكنولوجيا، ولاسيما في مجال الذكاء الاصطناعي الذي يشكل تحولًا هامًا في عدة مجالات من الحياة اليومية والصناعية والحكومية. وقد أصبحت هذه التطورات تحدياً كبيراً يواجه العديد من الدول والمجتمعات على مستوى العالم. تجلى هذا التحدي في تناول **13** من الدراسات العربية والاجنبية التي أسهمت في تحديد وتحليل المخاطر والتحديات التي تنطوي على استخدام التكنولوجيا والذكاء الاصطناعي وأثرها على العديد من الجوانب الحياتية.

بدايةً، يتضح من الدراسات العربية والأجنبية الحديثة أهمية دراسة تأثير الذكاء الاصطناعي على مختلف الجوانب الاجتماعية والقانونية والأخلاقية. في الدراسات العربية، قدمت دراسات متعددة تحليلات حول الموضوع. قامت دراسة الأسد (٢٠٢٣) بتسليط الضوء على الفرص والمخاطر التي يمكن أن يحملها الذكاء الاصطناعي في الدول العربية، في حين قدمت دراسة نوار (٢٠٢٣) مراجعة للحماية المدنية لحقوق الإنسان في مواجهة تحديات الذكاء الاصطناعي. علاوة على ذلك، اهتمت دراسة عبد الهادي (٢٠٢٣) بالحماية القانونية للمحتويات المرئية على الإنترنت، فيما استعرضت دراسة علي (٢٠٢٢) تأثير تقنيات الذكاء الاصطناعي على المراجعة الداخلية في المؤسسات، ومن جهة أخرى، في الدراسات الأجنبية، قامت دراسة Sobrino-García (٢٠٢١) بتحليل المخاطر والتحديات التي يواجهها الإدارة العامة في إسبانيا نتيجة استخدام تقنيات الذكاء الاصطناعي. كما قامت دراسة McLean وآخرون (٢٠٢٣) بمراجعة منهجية للمخاطر المرتبطة بالذكاء الاصطناعي العام، ويبرز من هذه الدراسات الحاجة الماسة لفهم تأثيرات الذكاء الاصطناعي على العديد من الجوانب الاجتماعية والقانونية والأخلاقية. يتبين أن المجال يستدعي البحث المستمر والتفاعل مع التطورات السريعة في هذا المجال لتطوير سياسات وأطر أخلاقية وقانونية ملائمة للتصدي للتحديات المستقبلية المحتملة، وسنقدم هذه الدراسات بشيء من التفصيل.

اولاً: الدراسات العربية

١. دراسة الأسد، الأسد صالح. (٢٠٢٣). الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية. *مجلة إضافات اقتصادية*

تهدف هذه الدراسة إلى التعرف على الفرص والتحديات المترتبة على استخدام تقنيات وأنظمة الذكاء الاصطناعي، وفهم انتشار وتقدم التكنولوجيا الذكية الاصطناعية بسرعة متزايدة، وتقديم لمحة حول وضع الدول العربية في مجال الذكاء الاصطناعي ومستوى تطبيقها، واعتمدت الدراسة منهجًا تحليليًا لفحص الفرص والتحديات المتعلقة بتقنيات الذكاء الاصطناعي. تم استخدام عينة متنوعة تضم مشاركين من مجموعات مختلفة لضمان تنوع وشمولية وجهات النظر، وأظهرت الدراسة أن التطور السريع للذكاء الاصطناعي يتيح فرصًا كبيرة للاستفادة منه في مختلف المجالات. ومع ذلك، يتطلب الاستفادة الأمثل من هذه التقنيات ومواجهة التحديات

والمخاطر الناجمة عنها اتخاذ إجراءات واحتياطات مناسبة، وأما فيما يتعلق بالدول العربية، فإن الدراسة كشفت عن تباين في مستوى التقدم واعتماد التكنولوجيا الذكية الاصطناعية. بينما تسجل بعض الدول تقدماً وجهودًا جيدة في هذا السياق، فإن بعض الدول الأخرى لا تزال تواجه تحديات في تطوير استراتيجيات وتنفيذها بشكل فعال، وبشكل عام تسلط هذه الدراسة الضوء على أهمية فهم الفرص والتحديات المرتبطة بالذكاء الاصطناعي وتعزز من الحاجة إلى تطوير استراتيجيات وسياسات مناسبة لضمان استفادة مستدامة ومسؤولة من هذه التقنيات في الدول العربية.

٢. دراسة نوار، اسماء عاطف عبد السلام عثمان (٢٠٢٣). الحماية المدنية لحقوق الإنسان الطبيعية من مخاطر الذكاء الاصطناعي للروبوت. *مجلة بنها للعلوم الإنسانية*

تهدف هذه الدراسة إلى فهم الأثر البيئي لتطور التكنولوجيا الحديثة، وخاصة الذكاء الاصطناعي، على المجتمع والأفراد. وتهدف أيضًا إلى دراسة التحديات والفرص التي يمكن أن تنشأ نتيجة لاستخدام الروبوتات ذات الذكاء الاصطناعي، واعتمدت الدراسة منهج تحليلي لفحص تأثير التكنولوجيا الحديثة على المجتمع. تم اختيار عينة متنوعة تتضمن أفرادًا من مجموعات مختلفة لاستكمال وجهات نظر متعددة حول موضوع الدراسة، وأظهرت الدراسة أن التطور السريع في مجال التكنولوجيا الحديثة، بما في ذلك الذكاء الاصطناعي، قد أحدث تحولات كبيرة في العالم الرقمي والاجتماعي. وبينما توفر هذه التقنيات فرصًا مذهلة، فإنها تثير أيضًا تحديات وقضايا أخلاقية جديدة، وتشير النتائج إلى أهمية وجود ضوابط إجرائية وأخلاقية لحماية حقوق الإنسان الطبيعية في ظل هذا التطور التكنولوجي. يجب على المجتمع والأفراد النظر في كيفية استخدام هذه التقنيات بشكل مسؤول وآمن للمساهمة في تحسين الحياة وحماية الحقوق الأساسية للإنسان.

٣.دراسة عبد الهادي، محمود. (٢٠٢٣). الحماية القانونية من مخاطر أدوات الذكاء الاصطناعي المستخدمة في تصفية المحتويات المرئية عبر شبكة الانترنت، *مجلة البحوث الفقهية والقانونية*، ٤١(٤١), ٨٣-١٢٧

تهدف هذه الدراسة إلى تقديم تقييم شامل لتأثير تكنولوجيا الذكاء الاصطناعي على تصفية وترشيح المحتوى المرئي على منصات العرض الرقمي عبر الإنترنت. وتركز الدراسة على فهم الفوائد والمخاطر المرتبطة بهذا الاستخدام وكيفية التعامل مع التحديات القانونية والمسائل المتعلقة بالمسؤولية، واعتمدت الدراسة منهجًا تحليليًا لاستقصاء تأثير تكنولوجيا الذكاء الاصطناعي على تصفية المحتوى المرئي. تم استخدام عينة متنوعة تشمل مالكي ومشغلي ومطوري منصات العرض الرقمي، بالإضافة إلى مستخدمي هذه المنصات، بهدف فهم وجهات نظر متعددة، وأظهرت الدراسة أن تكنولوجيا الذكاء الاصطناعي توفر فرصًا كبيرة في تحسين تصفية وترشيح المحتوى المرئي على المنصات الرقمية. ومع ذلك، تثير هذه التقنية أيضًا قضايا قانونية وأخلاقية حول المسؤولية

والحماية لمستخدمي هذه المنصات، وتقترح الدراسة تبني نظام مسئولية يسهم في تحقيق التوازن بين مالكي المنصات ومستخدميها، حيث تكون المسؤولية مشتركة بناءً على حجم الضرر والمسؤولية الأقوى تكون مسؤولة عن تعويض الأطراف المتضررة. هذا يعكس الحاجة إلى تطوير إطار قانوني وأخلاقي مناسب للتعامل مع مسائل الذكاء الاصطناعي في هذا السياق.

٤. دراسة علي، منذر محمد. (٢٠٢٢). أثر تفعيل تقنيات الذكاء الاصطناعي علي تعزيز أنشطة المراجعة الداخلية. *مجلة الإسكندرية للبحوث المحاسبية*, ٦(٣), ١-٤٠

تهدف هذه الدراسة إلى استكشاف العلاقة بين تقنيات الذكاء الاصطناعي وأنشطة المراجعة الداخلية. يتمثل الهدف الرئيسي في فهم كيفية تأثير تكنولوجيا الذكاء الاصطناعي على عملية المراجعة الداخلية وما إذا كانت هذه التقنيات تحسن أو تؤثر على كفاءة وفعالية المراجعة الداخلية، واعتمدت الدراسة منهجية البحث المسحي لجمع البيانات الأولية. تم توزيع استبيان على عينة تشمل مراجعين داخليين، ومحاسبين، وأعضاء هيئة التدريس، ومدراء ماليين. تم تحليل البيانات باستخدام الإحصاءات والبرمجيات الإحصائية، وأظهرت نتائج الدراسة أن تقنيات الذكاء الاصطناعي تعزز وتحسن أنشطة المراجعة الداخلية. تمثل هذه التقنيات فرصًا لتوفير الوقت وزيادة دقة التحليل وتحسين فهم العمليات التجارية. كما أشارت الشركات الكبرى إلى استخدامها بنجاح في تقييم المخاطر وتخطيط العمليات وتحليل المعاملات، توصي الدراسة بأهمية استخدام تقنيات الذكاء الاصطناعي في مجال المراجعة الداخلية والاستفادة منها لتحسين الكفاءة والفعالية. يُشجع على دمج التطبيقات الذكية في العمليات المحاسبية والمراجعة لتحقيق توفير في التكاليف وتعزيز الرصد المستمر للعمليات. وتُشدد الدراسة على أهمية استمرار تطوير تلك التقنيات لمواكبة التحديات الناشئة والتغيرات البيئية.

٥. دراسة الفار، مايسة، داود، ومينا إسحق توفيلس. (٢٠٢٣). أخلاقيات الذكاء الاصطناعي: مناقشة المخاطر المحتملة والمعضلات الأخلاقية المرتبطة بها في الفن والتصميم. *مجلة التراث والتصميم*

تهدف الدراسة الحالية إلى استكشاف المخاطر المحتملة والمشكلات الأخلاقية المرتبطة بتطوير وتنفيذ تكنولوجيا الذكاء الاصطناعي (**AI**)، وتقديم اقتراحات للتعامل مع هذه التعقيدات. تتضمن المواضيع التي تم التركيز عليها تأثير الذكاء الاصطناعي على مجالات الفن والتصميم، وقدرته على الحفاظ على التحيزات والتمييز الحاليين أو تفاقمهما. كما تتعرض الدراسة للمسائل الأخلاقية المتعلقة باستخدام الذكاء الاصطناعي في إنتاج المحتوى. بالإضافة إلى ذلك، تركز الدراسة على دور المصممين والمطورين في ضمان امتثال التكنولوجيا للمعايير الأخلاقية كدليل توجيهي لاستخدام الذكاء الاصطناعي، وتمثل الدراسة منهجاً نوعياً، حيث تستخدم المقابلات وتحليل المحتوى كأساليب لجمع البيانات. تم اختيار عينة متنوعة من المشاركين لتضمين وجهات نظر متعددة وأصوات متنوعة، وأظهرت النتائج أن الذكاء الاصطناعي يمكن أن يحمل مخاطر كبيرة وتحديات أخلاقية في مجالات الفن

والتصميم. تم تحديد تأثير الذكاء الاصطناعي على الحفاظ على الميزات والتحيزات الحالية، وكذلك تسليط الضوء على الاعتبارات الأخلاقية لاستخدام هذه التقنية في إنتاج المحتوى. تؤكد النتائج أيضًا على أهمية التعاون متعدد التخصصات والحوار المستمر لضمان تقدم واستخدام الذكاء الاصطناعي بشكل مسؤول.

ثانياً: الدراسات الأجنبية

٦. **Sobrino-García, I. (2021). Artificial intelligence risks and challenges in the Spanish public administration: An exploratory analysis through expert judgements. Administrative Sciences, 11(3), 102.**

يهدف البحث إلى تحديد المخاطر المرتبطة باستخدام الذكاء الاصطناعي في الإدارة العامة الإسبانية ومدى قدرة الآليات القانونية على حل هذه المشكلات. نجيب على هذه الأسئلة من خلال تبني نهج بحثي نوعي، من خلال إجراء مقابلات شبه منظمة مع عدة خبراء في هذا المجال. على الرغم من الفوائد التي قد يتضمنها هذا التكنولوجيا، يمكننا التأكيد من خلال هذا البحث أن استخدام الذكاء الاصطناعي يمكن أن يولد مشاكل متعددة مثل عدم الشفافية وعدم اليقين القانوني والتحيز أو انتهاكات حماية البيانات الشخصية. ولم تكن الآليات الموفرة بالفعل من قبل القانون الإسباني كافية لتجنب هذه المخاطر لأنها لم تكن مصممة لمواجهة استخدام الذكاء الاصطناعي في الإدارة العامة. بالإضافة إلى ذلك، يجب إنشاء تعريف قانوني موحد للذكاء الاصطناعي.

٧. **McLean, S., Read, G. J., Thompson, J., Baber, C., Stanton, N. A., & Salmon, P. M. (2023). The risks associated with Artificial General Intelligence: A systematic review. Journal of Experimental & Theoretical Artificial Intelligence, 35(5), 649-663.**

يُقدم الذكاء الاصطناعي العام (**AGI**) فوائد هائلة للبشرية، ولكنه يشكل أيضًا تهديدًا كبيرًا. كان هدف هذا الاستعراض الأدبي هو تلخيص البحوث التي قام بها الخبراء حول المخاطر المرتبطة بالذكاء الاصطناعي العام. تم اتباع إرشادات إعداد التقارير المفضلة للاستعراضات الأدبية والتحليلات الوصفية(**PRISMA**) تم اختيار ستة عشر مقالًا للإدراج في هذا الاستعراض. تم تصنيف الأنواع المشمولة في الاستعراض بوصفها مناقشات فلسفية، وتطبيقات لتقنيات النمذجة، وتقييم الأطر والعمليات الحالية المتعلقة بالذكاء الاصطناعي العام. حدد الاستعراض مجموعة من المخاطر المتعلقة بالذكاء الاصطناعي العام، مثل إمكانية خروج الذكاء الاصطناعي العام

عن سيطرة أصحابه/مديريه البشريين، أو تحديد أهداف غير آمنة وتنفيذها، أو تطوير الذكاء الاصطناعي العام بطرق غير آمنة، أو تطور الذكاء الاصطناعي العام ذو الأخلاق والقيم السلبية. وأشار الاستعراض أيضًا إلى الإدارة غير الكافية للذكاء الاصطناعي العام والمخاطر الوجودية. وتم التأكيد على العديد من القيود الموجودة في قاعدة أدبيات الذكاء الاصطناعي العام، بما في ذلك العدد المحدود من المقالات المراجعة من قبل الخبراء والتركيز على تقنيات النمذجة المتعلقة بمخاطر الذكاء الاصطناعي العام. وأشير أيضًا إلى نقص في البحوث المحددة حول المجالات التي يمكن تنفيذ الذكاء الاصطناعي العام فيها، ونقص في التعاريف الموحدة للذكاء الاصطناعي العام ونقص في وجود تصنيف موحد لمصطلحات **AGI** يجب تقديم توصيات لمعالجة المشكلات المحددة المرتبطة بأبحاث مخاطر الذكاء الاصطناعي العام لتوجيه تصميمه وتنفيذه وإدارته.

٨. **Manheim, K., & Kaplan, L. (2019)**

تم نشر "مؤشر الديمقراطية" سنويًا من قبل مجلة "**The Economist**" في عام **٢٠١٧**، أفاد المؤشر بأن نصف دول العالم حصلت على درجات أقل من العام السابق. وتضمنت هذه الدول الولايات المتحدة، التي تم تخفيض تصنيفها من "ديمقراطية كاملة" إلى "ديمقراطية معيبة". العامل الرئيسي وراء ذلك كان "تآكل الثقة في الحكومة والمؤسسات العامة". لعب التدخل الروسي وتلاعب الناخبين من قبل كامبريدج أناليتيكا في الانتخابات الرئاسية عام **٢٠١٦** دورًا كبيرًا في هذا الإحباط العام.

سيستمر توجه مثل هذه التهديدات، نتيجة للنمو المتزايد في استخدام أدوات الذكاء الاصطناعي (**AI**) للتلاعب بالشروط المسبقة والآليات للديمقراطية. بالمثل، يُعتبر تهديد الذكاء الاصطناعي للخصوصية القرارية والمعلوماتية مدمرًا أيضًا. الذكاء الاصطناعي هو المحرك وراء تحليلات البيانات الكبيرة وإنترنت الأشياء. بينما يُمنح بعض الفوائد للمستهلك، إلا أن وظيفتهم الرئيسية حاليًا هي التقاط المعلومات الشخصية، وإنشاء ملامح سلوكية تفصيلية، وبيع السلع والأجندات. الخصوصية والتعريف غير المعروف والحكم الذاتي هي الخسائر الرئيسية لقدرة الذكاء الاصطناعي على التلاعب بالخيارات في القرارات الاقتصادية والسياسية.

الطريق إلى الأمام يتطلب مزيدًا من الاهتمام بهذه المخاطر على الصعيد الوطني، ووضع لوائح تنظيمية مصاحبة. في حالة عدم وجود ذلك، ستهيمن الشركات التكنولوجية، التي تستثمر بشكل كبير في الذكاء الاصطناعي وتحقيق أرباح منه، ليس فقط على الحوار العام، ولكن أيضًا على مستقبل قيمنا الأساسية ومؤسساتنا الديمقراطية.

٩. **Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021)**

الهدف من هذا البحث هو تقديم استعراض شامل لأمن السيبراني فيما يتعلق بتقنيات الذكاء الاصطناعي والتحليل العميق للهجمات المعادية ضدها، وتم تحليل ودراسة الهجمات المعادية ضد تطبيقات الذكاء الاصطناعي وأمانها من خلال استخدام مجموعة متنوعة من النماذج والتقنيات الحديثة في هذا المجال، وتم استخدام أساليب البحث النوعي والكمي لتحليل وتقييم الهجمات المعادية ضد تطبيقات الذكاء الاصطناعي، مع التركيز على دراسة النماذج الرياضية الحديثة والتحليل الأمني، وأظهرت النتائج التحليلية للبحث استعراضاً شاملاً للهجمات المعادية المحتملة ضد تطبيقات الذكاء الاصطناعي وتأثيرها على أمن البيانات والتحديات المستقبلية المحتملة في هذا المجال، وزيادة اعتماد الذكاء الاصطناعي تمثل فرصة لحل العديد من التحديات الاجتماعية والاقتصادية والبيئية؛ ومع ذلك، لا يمكن أن يحدث ذلك من دون تأمين التقنيات الممكّنة بالذكاء الاصطناعي. في السنوات الأخيرة، أصبح معظم النماذج الذكاء الاصطناعي عرضة لتقنيات القرصنة المتقدمة والمعقدة. هذا التحدي دفع بجهود البحث الموجّهة نحو الذكاء الاصطناعي المعادي، بهدف تطوير نماذج التعلم الآلي والتعلم العميق القوية والمقاومة لأنواع مختلفة من السيناريوهات المعادية. في هذه الورقة، نقدم استعراضًا شاملاً لأمن السيبراني يُظهر الهجمات المعادية ضد تطبيقات الذكاء الاصطناعي، بما في ذلك جوانب مثل المعرفة والقدرات المعادية، وطرق توليد الأمثلة المعادية ونماذج الدفاع السيبراني الموجودة. نشرح النماذج الرياضية للذكاء الاصطناعي، وخصوصاً الأصناف الجديدة من التعلم التعزيزي والتعلم الموحّد لنبين كيف ستستغل سيناريوهات الهجوم نقاط الضعف في نماذج الذكاء الاصطناعي. نقترح أيضًا إطارًا منهجيًا لعرض تقنيات الهجوم على تطبيقات الذكاء الاصطناعي، ونستعرض الدفاعات السيبرانية التي ستحمي تلك التطبيقات من تلك الهجمات. نسلط أيضًا الضوء على أهمية فهم أهداف العدو وقدراتهم المعادية، خاصة الهجمات الأخيرة ضد تطبيقات الصناعة، لتطوير دفاعات متكيفة تقيم لتأمين تطبيقات الذكاء الاصطناعي. وأخيرًا، نصف التحديات الرئيسية واتجاهات البحث المستقبلية في مجال أمن وخصوصية التقنيات الذكاء الاصطناعي.

١٠. Villegas-Ch, W., & García-Ortiz, J. (2023)

يهدف هذا البحث إلى تقديم إطار عمل شامل لمعالجة التحديات الرئيسية في مجال أمن البيانات والخصوصية في نظم الذكاء الاصطناعي. يسعى البحث لتحليل البحوث السابقة والتطورات في هذا المجال، وتحديد الفجوات والمجالات غير المستكشَفة التي تتطلب اهتمامًا لتعزيز الأطر الحالية وتعزيز الأمن والخصوصية في الذكاء الاصطناعي، والتوسع السريع للذكاء الاصطناعي يشكل تحديات كبيرة في مجال أمان البيانات والخصوصية. يقترح هذا المقال نهجاً شاملاً لتطوير إطار عمل لمعالجة هذه المسائل. أولاً، يتم استعراض الأبحاث السابقة حول الأمن والخصوصية في الذكاء الاصطناعي، مما يسلط الضوء على التقدمات والقيود الحالية. بالإضافة إلى ذلك، يتم تحديد المجالات البحثية المفتوحة والفجوات التي تحتاج إلى اهتمام لتحسين الأطر الحالية، وفيما يتعلق بتطوير الإطار العمل، يتناول العمل حماية البيانات في الذكاء الاصطناعي، مشيرًا إلى أهمية حماية البيانات المستخدمة

في نماذج الذكاء الاصطناعي وشرح السياسات والممارسات لضمان أمانها، وكذلك النهج المتبع للحفاظ على سلامة هذه البيانات. بالإضافة إلى ذلك، يتم فحص أمن الذكاء الاصطناعي، من خلال تحليل الضعف والمخاطر المتواجدة في أنظمة الذكاء الاصطناعي وتقديم أمثلة على الهجمات المحتملة والتلاعبات الخبيثة، إلى جانب الأطر الأمنية للتخفيف من هذه المخاطر.

١١. **Nick Ruijs.(2022) Ethics & AI: A Systematic Review on Ethical Concerns and Related Strategies for Designing with AI in Healthcare Industrial Design Department, Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands**

في الحياة الحديثة، عزز تطبيق الذكاء الاصطناعي (AI) تنفيذ الخوارزميات القائمة على البيانات في المجالات عالية المخاطر، مثل الرعاية الصحية. ومع ذلك، فقد أصبح من الصعب بشكل متزايد على البشر فهم عمل ومنطق هذه الخوارزميات المعقدة والمبهمة. ولكي يدعم الذكاء الاصطناعي القرارات الأساسية في هذه المجالات، لا بد من معالجة قضايا أخلاقية محددة لمنع التفسير الخاطئ للذكاء الاصطناعي، والذي قد يكون له عواقب وخيمة على البشر. ومع ذلك، لم يتم نشر سوى القليل من الأبحاث حول المبادئ التوجيهية التي تعالج بشكل منهجي القضايا الأخلاقية عند تطبيق تقنيات الذكاء الاصطناعي في الرعاية الصحية. في هذه المراجعة المنهجية للأدبيات، كنا نهدف إلى تقديم لمحة عامة عن الاهتمامات الأخلاقية والاستراتيجيات ذات الصلة التي تم تحديدها حاليًا عند تطبيق الذكاء الاصطناعي في الرعاية الصحية. كشفت المراجعة، التي اتبعت إرشادات **PRISMA**، عن **١٢** قضية أخلاقية رئيسية: العدالة والإنصاف، والحرية والاستقلالية، والخصوصية، والشفافية، وسلامة المرضى والأمن السيبراني، والثقة، والإحسان، والمسؤولية، والتضامن، والاستدامة، والكرامة، والصراعات. بالإضافة إلى هذه القضايا الأخلاقية الرئيسية الـ **١٢**، قمنا باستخلاص **١٩** قضية أخلاقية فرعية والاستراتيجيات المرتبطة بها من الأدبيات.

١٢. **JamesRuff .(2020). Using artificial intelligence at work may harm your job performance, Australia Academe, University Etoua**

قد يؤدي استخدام الذكاء الاصطناعي في العمل إلى الإضرار بأدائك الوظيفي، إذا تم استخدامه لمهام خارج نطاق قدراته، حسبما وجدت دراسة أميركية جديدة.

وبحسب موقع «بيزنس إنسايدر»، فقد أجريت الدراسة بواسطة باحثين من مجموعة بوسطن الاستشارية وجامعة هارفارد، وكلية وارتون لإدارة الأعمال، ومعهد ماساتشوستس للتكنولوجيا، لمعرفة كيف يؤثر الذكاء الاصطناعي على إنتاجية الموظفين الإداريين وجودة عملهم.

وشملت الدراسة **٧٥٨** استشارياً في مجموعة بوسطن تم تقسيمهم إلى **٣** مجموعات قبل طلب مهام معينة منهم. وطُلب من المجموعة الأولى عدم استخدام الذكاء الاصطناعي أثناء أداء المهام، فيما سُمح للثانية استخدام برنامج الذكاء الاصطناعي «تشات جي بي تي»، وطُلب من المجموعة الثالثة استخدام «تشات جي بي تي» جنبا إلى جنب مع مشاهدة مقاطع فيديو وقراءة وثائق تعليمية حول الاستراتيجيات السريعة التي يمكن أداء المهام بها.

وصنف الباحثون بعض المهام المطلوبة من المشاركين على أنها «داخل نطاق قدرات» الذكاء الاصطناعي، وتضمنت تبادل الأفكار والمعلومات حول مفاهيم معينة أو وضع خطة عمل محتملة لمشروع ما، فيما صنفوا مهام أخرى على أنها «خارج نطاق قدرات» هذه التقنية، حيث تتطلب عقلا وتفكيرا بشريا لأدائها.

على سبيل المثال، طُلب من المستشارين المكلفين ببعض المهام تقديم توصيات إلى الرئيس التنفيذي لشركة افتراضية باستخدام البيانات المالية الداخلية للشركة واعتمادا على مقابلات مع أشخاص مطلعين في الشركة، وهي معلومات لم يتمكن الذكاء الاصطناعي من الوصول إليها.

١٣. **Yueen Li*, Jin Gu and Liyang Wang. (2020). Research on Artificial Intelligence Ethics in the Field of Art Design. Shandong Jianzhu University, Faculty of Industrial Design, room JY324, Fengming St.,Jinan, China.**

هدفت الدراسة الى تحليل المعضلات الأخلاقية التي يواجها الذكاء الاصطناعي في مجال التصميم الفني، يتم استخدام أسلوب التحليل المنهجي لتقديم أساليب ونماذج أبحاث أخلاقيات الفن في ظل ظروف الذكاء الاصطناعي، ويتم تعديل تنفيذ المعايير الأخلاقية للذكاء الاصطناعي لدراسة مبادئ أخلاقية جديدة.

نتائج الدراسات السابقة

والسعي لتحقيق أقصى قدر من الفعالية العملية لأخلاقيات الذكاء الاصطناعي؛ إنشاء معيار موثوق للإبداع الفني في ظل ظروف الذكاء الاصطناعي. وعلى أساس التأكيد على البحث التقني، يعد أكبر بحث ممكن في مجال تحقيق العلوم الإنسانية. ومن البحث والتصميم عالي المستوى لأخلاقيات الذكاء الاصطناعي، وتعزيز تحسين معيشة الناس ورفاهيتهم، وتعزيز التنمية الصحية للصناعة، وفهم مبادرة جولة جديدة من الثورة التكنولوجية.

توصيات الدراسات السابقة

اغتنام فترة فرص التطوير الاستراتيجي للذكاء الاصطناعي، وتسريع وتيرة الأخلاق البحث والابتكار، وبناء ميزة تنافسية في تطوير الذكاء الاصطناعي، وبناء مجتمع ذكي في أسرع وقت ممكن، واستخدام التكنولوجيا لصالح الجميع.

التعقيب عن الدراسات السابقة

اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) مع دراسة الباحث في تناولها لمخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في المستقبل. اما الدراسة الاجنبية فقد اتفقت دراسة الطالب او الباحث مع دراسة Salmon, P. M. (2023) Sobrino-García, I. (2021 مع دراسة الباحث فيتناولها مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في المستقبل .

اما فيما يخص المنهج فقد اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) ودراسة Salmon, P. M. (2023) Sobrino-García, I. (2021 مع دراسة الباحث في استخدامها للمنهج الوصفي التحليلي .

كما اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) ودراسة Salmon, P. M. (2023) Sobrino-García, I. (2021 مع دراسة الباحث في الاداء حيث اعتبرت الاستبانة اداة لكل الدراسات السابقة.

اما فيما يخص الاهداف فقد اتفقت كل من دراسة عبد الهادي (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة الاسد(٢٠٢٣) ودراسة الفار (٢٠٢٣) في اتفاقها مع دراسة الباحث مخاطر استخدم الذكاء الاصطناعي.

اما دراسة علي و Sobrino-García, I. (2021 ودراسة McLean (٢٠٢٣) على انها لم تتناول مخاطر الذكاء الاصطناعي وانما تناولت فوائد الذكاء الاصطناعي.

اما فيما يخص النتائج فقد اتفقت اغلب الدراسات مع دراسة الباحث في أن التطور السريع للذكاء الاصطناعي يتيح فرصًا كبيرة للاستفادة منه في مختلف المجالات ،ولكن يجب الحد من مخاطر الذكاء الاصطناعي.

التعقيب عن الدراسات السابقة

اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) مع دراسة الباحث في تناولها لمخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في المستقبل. اما الدراسة الاجنبية فقد اتفقت دراسة الطالب او الباحث مع دراسة

Sobrino-García, I. (2021 Salmon, P. M. (2023) مع دراسة الباحث فيتناولها مخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات في المستقبل .

اما فيما يخص المنهج فقد اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) ودراسة Salmon, P. M. (2023) Sobrino-García, I. (2021 مع دراسة الباحث في استخدامها للمنهج الوصفي التحليلي .

كما اتفقت كل من دراسة الاسد (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة عبد الهادي (٢٠٢٣) ودراسة الفار(٢٠٢٣) ودراسة علي (٢٠٢٢) ودراسة Sobrino-García, Salmon, P. M. (2023) I. (2021 مع دراسة الباحث في الاداء حيث اعتبرت الاستبانة اداة لكل الدراسات السابقة.

اما فيما يخص الاهداف فقد اتفقت كل من دراسة عبد الهادي (٢٠٢٣) ودراسة نورا (٢٠٢٣) ودراسة الاسد(٢٠٢٣) ودراسة الفار (٢٠٢٣) في اتفاقها مع دراسة الباحث مخاطر استخدم الذكاء الاصطناعي.

اما دراسة علي و Sobrino-García, I. (2021 ودراسة McLean (٢٠٢٣) على انها لم تتناول مخاطر الذكاء الاصطناعي وانما تناولت فوائد الذكاء الاصطناعي.

اما فيما يخص النتائج فقد اتفقت اغلب الدراسات مع دراسة الباحث في أن التطور السريع للذكاء الاصطناعي يتيح فرصًا كبيرة للاستفادة منه في مختلف المجالات ،ولكن يجب الحد من مخاطر الذكاء الاصطناعي.

٣. الإجراءات المنهجية للدراسة

تمهيد

سيوضح هذا الفصل المنهج المستخدم في الدراسة، وأدواته، ومن ثم تحديد مجتمع الدراسة ووصف خصائص عينة الدراسة، كما سيتطرق لبناء أداة الدراسة والإجراءات التي تم إتباعها للتحقق من صدقها وثباتها كما سيبين أيضاً آلية تطبيق الدراسة ميدانياً ،والأساليب الإحصائية التي سيتم استخدامها في معالجة بيانات الدراسة والإجابة على تساؤلاتها.

١,٣ منهج الدراسة

مناهج البحث العلمي تتمثَّل في إجراءات مُنظمة، وبصورة تجعل الباحثين قادرين على وضع تصورات وشروح لمشكلة أو موضوع علمي، واختيار الموضوع العلمي منذ البداية المحدد الرئيسي لنوعية المناهج التي يمكن استخدامها في البحث، فكلما كانت المعلومات الرقمية شحيحة كان ذلك دافع نحو اختيار المنهج الوصفي كمحور أساسي لتفصيل الدراسية، وفي الحالة الرغبة بتتبع موضوع من خلال الخلفية التاريخية له، كان ذلك أدعى لاختيار المنهج التاريخي، وفي حالة الرغبة في دراسة مشكلة بأسلوب متعمق؛ فإن هناك حاجة لاختيار المنهج التحليلي، وفي حالة رغبة الباحث بتناول موضوعًا علميًا تطبيقيًا، ويحتاج للتجريب؛ فيمكن اختيار المنهج التجريبي، والشائع هو اختيار أكثر من منهج علمي في الوقت ذاته (المزجاجي،٢٠١٥).

لابد لكل دراسة علمية من منهج علمي يتبعه الباحث لإثبات فرضيات دراسته، وذلك من خلال الانسجام الذي يخلقه المنهج العلمي المستخدم بين فرضيات الدراسة وعملية إثباتها ميدانيا، وقد تم الاعتماد في تحليل موضوع لدراسة على المنهج الوصفي التحليلي. حيث يقوم المنهج الوصفي التحليلي على جمع المعلومات والبيانات وتصنيفها وتدوينها ومحاولة تفسيرها وتحليلها من أجل قياس ومعرفة تأثير العوامل على أحداث الظاهرة محل الدراسة.

من أجل أن يتم تحقيق أهداف الدراسة سيتم استخدام منهجين، المنهج الأول وهو المنهج الاستقرائي الذي من خلاله سيغطي الجانب النظري وذلك من خلال استقراء الأدبيات العربية والأجنبية، والرسائل العلمية، والأبحاث المحكمة، والكتب وبعض مواقع الإنترنت ذات الصلة بالموضوع، وسيغطي الجانب العملي بتطبيق المنهج الوصفي الاستدلالي، للتعرف على أثر الرفع المالي على ربحية السهم في البنوك التجارية الوطنية السعودية (المزجاجي،٢٠١٥).

٢,٣ مجتمع الدراسة

مجموعة من المؤسسات بمحافظة جدة وتم اختيار عينة قوامها (٨٠) مفردة من خلال اختيار عينة عشوائية بسيطة.

٣,٣ عينة الدراسة

عينة البحث هي جزء من مجتمع الدراسة يتم اختياره بطريقة منهجية أو عشوائية لتمثيل مجتمع الدراسة، ويتم فحص عينة الدراسة لتعميم النتائج على باقي المجتمع.

كيفية تحديد حجم عينة الدراسة يجب أولاً تحديد مجتمع البحث الذي يتم دراسته، ثم الرجوع للدراسات السابقة التي تناولت نفس الموضوع وذلك لتحديد رقم تقريبي للعينة، ثم يقوم الباحث بتحديد ما إذا كان

مجتمع البحث متجانساً، حيث انه وفي حالة التجانس لا يشترط الحصول على عينة كبيرة فجزء صغير يستطيع أن يمثل المجتمع بالكامل. ويختلف حجم العينة على حسب نوع البحث سواء وصفي أو تحليلي أو خلافه (المزجاجي،٢٠١٥).

بناءً على كُبر مجتمع الدراسة وصعوبة التواصل مع عينه فعليه سوف أحدد عينة بسيطة لأن جميع عناصر العينة موظفي الشركات والمؤسسات بناءً على المعادلة الإحصائية الخاصة بتحديد حجم العينة: هي **80** موظفاً على اختلاف المؤسسات والشركات بشكل عشوائي.

٤,٣ أدوات جمع البيانات ومقاييس الدراسة

لأجل التحقق من فرضية البحث وتحقيق اهدافه تم اعداد استمارة استبيان شملت معظم الاسئلة والمتغيرات التي يرى الباحثين أهميتها وخدمتها لأهداف البحث، وقد أخضعت هذه الاستبانة الى التقييم من قبل عدد من السادة المحكمين، إذ أخذ الباحثين بنظر الاعتبار ملاحظات ومقترحات السادة المحكمين، وبالتالي أصبحت الاستبانة بشكلها النهائي. وتكونت الاستبانة من **١٠** اسئلة وتم توزيعهم بشكل عشوائي.

وقد تم أعداد الاستبانة بحيث يقوم المجيب بوضع إشارة (√) أمام كل فقرة من الفقرات الخاصة بالمحور، إذ يوجد مقابل كل فقرة أعمدة، تعكس خمسة مستويات للإجابة أو للموافقة عليه ، ويمثل كل مستوى وزناً معينا تصاعديا يتدرج من **١** إلى **٥** وفقا لمقياس ليكرت الخماسي، وحيث أن جميع البنود كانت إيجابية في الاستبانة.

٥,٣ أنواع البيانات ومصادرها

مصادر المعلومات الأولية

مصدر المعلومات الأولي يوفر معلومات مباشرة ومعلومات عن تجربة عن حدث أو شخص أو كائن أو عمل فني؛ فالمصادر الأولية معاصرة لما يصفونه، فهي مواد أصلية لم يتم تفسيرها أو تلخيصها أو تقييمها من قبل طرف ثانٍ. وفيما يلي بعض الأمثلة لمصادر المعلومات الأولية:

- المذكرات الشخصية
- التجارب الشخصية
- القصائد
- المراسلات الشخصية

- اللوحات
- المقابلات الشخصية
- التقارير السنوية لمنظمة أو وكالة
- براءات الاختراع
- سجلات المحكمة

مصادر المعلومات الثانوية

يقوم مصدر المعلومات الثانوي بتحليل أو تفسير أو مناقشة المعلومات المتعلقة بمصدر المعلومات الأولي، وتأتي المصادر الثانوية بعد ما تصفه، حيث يتم إنتاجها في مرحلة ما بعد ظهور مصدر المعلومات الأولي؛ وعادةً ما تحتوي الأوراق العلمية التي يكتبها الطلاب الأكاديميين على مصادر ثانوية في الغالب. وفيما يلي بعض الأمثلة لمصادر المعلومات الثانوية:

- الكتب الدراسية (الجامعية / المدرسية)
- كتب التراجم (كتب تتناول سير حياة المشاهير من الناس عبر العصور المختلفة)
- مقالات المجلات العلمية
- مراجعات الكتب **Book Reviews**
- الكتب التاريخ

١. البيانات الأولية

سيتم جمع البيانات الأولية من خلال استبيان منظم يجيب عليه عينة من الموظفين في المؤسسات والشركات بشكل عشوائي في المملكة العربية السعودية.

٢. البيانات الثانوية

سيتم جمع البيانات الثانوية من أحدث مراجعة للأدبيات المتعلقة بمخاطر الذكاء الاصطناعي على خصوصية وأمن المعلومات على مستقبل المنظمات من الكتب والصحف.

٦,٣ المقاييس والاختبارات الاحصائية

سيتم استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (**SPSS**) من أجل تحليل البيانات التي تم الحصول عليها لتحقيق أهداف الدراسة والإجابة على التساؤلات في ضوء طبيعة متغيرات الدراسة وأساليب القياس وأغراض التحليل، وسيتم استخدام الأساليب الإحصائية التالية:

- معامل بيرسون للارتباط لحساب الاتساق الداخلي
- معامل ألفا كرونباخ لحساب الثبات
- التكرارات والنسب المئوية لوصف المتغيرات الأولية
- المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للإجابة على تساؤلات الدراسة.

كما تم استخدام برنامج (**Excel**) لعمل الرسومات البيانية.

٤ . تحليل النتائج

تمهيد

سوف يقوم الباحث بالإجراء الاحصائي هو احد العناصر المهمة في البحث العلمي، الإحصاء هو العلم الذي يعمل على استعمال الأسلوب العلمي في طرائق جمع البيانات وتحليلها بهدف الحصول على استنتاجات وقراءات مناسبة وأيضا هو علم يبحث في طرائق جمع وعرض وتفسير وتحليل الحقائق والبيانات الخاصة بالظواهر العلمية والفنية التي تقاس عدديا والتي تتمثل في المشاهدات او الحالات المختلفة، وكذلك يبحث في تلخيص الحقائق بهذه المشاهدات او الحالات بصورة يسهل بها معرفه الاتجاهات والعلاقات التي ترتبط بعضها بالبعض.

١,٤ التحقق من الصدق والثبات لأداة جمع البيانات

صدق أداة الدراسة

للتحقق من صدق الاتساق الداخلي (صدق البناء الداخلي) للاستبانة فقد تم استخدام طريقة معامل بيرسون للارتباط (**Pearson Correlation**)، وذلك كما في الجدول التالي:

جدول رقم (٤–١) صدق الاتساق الداخلي لأداة الدراسة بطريقة معامل ارتباط بيرسون

المحـــور	رقم العبارة	معامل الارتباط بالمحور	الدلالة الإحصائية
خطر الذكاء الاصطناعي	١	.800**	0.000
	٢	.722**	0.000
	٣	.764**	0.000
الأمن والتدابير الوقائية	٤	.785**	0.000
	٥	.778**	0.000
	٦	.841**	0.000
الوعي والتعليم	٧	.831**	0.000
	٨	.675**	0.000
الثقة والاعتماد	٩	.850**	0.000
	١٠	.811**	0.000

(**) الارتباط دال عند مستوى (٠,٠١)

الجدول السابق (**٤–١**) يوضح نتائج التحقق من صدق البناء الداخلي لأداة الدراسة، وذلك من خلال حساب معاملات الارتباط لبيرسون بين كل عبارة ودرجة المحور الذي تتبع له. يتضح أن جميع معاملات الارتباط لبيرسون بين كل عبارة ودرجة المحور الذي تتبع له تراوحت بين (**٠,٦٧٥** – **٠,٨٥٠**) وجميعها قيم موجبة وذات دلالة إحصائية عند مستوى معنوية (**٠,٠١**) وبالتالي فإن الأداة تمتاز بصدق الاتساق الداخلي (البناء الداخلي) في محاورها.

ثبات أداة الدراسة

تم استخدام معامل ألفا كرونباخ بهدف التحقق من درجة ثبات الاستبانة، وذلك من خلال الجدول التالي:

جدول رقم (٤–٢) معاملات ثبات أداة الدراسة بطريقة ألفا كرونباخ

المحاور	عدد العبارات	معامل الثبات
خطر الذكاء الاصطناعي	٣	٠,٦٢٣
الأمن والتدابير الوقائية	٣	٠,٦٩٠
الوعي والتعليم	٢	٠,٥٥٣
الثقة والاعتماد	٢	٠,٥٤٩
الاستبانة ككل	١٠	٠,٧١٧

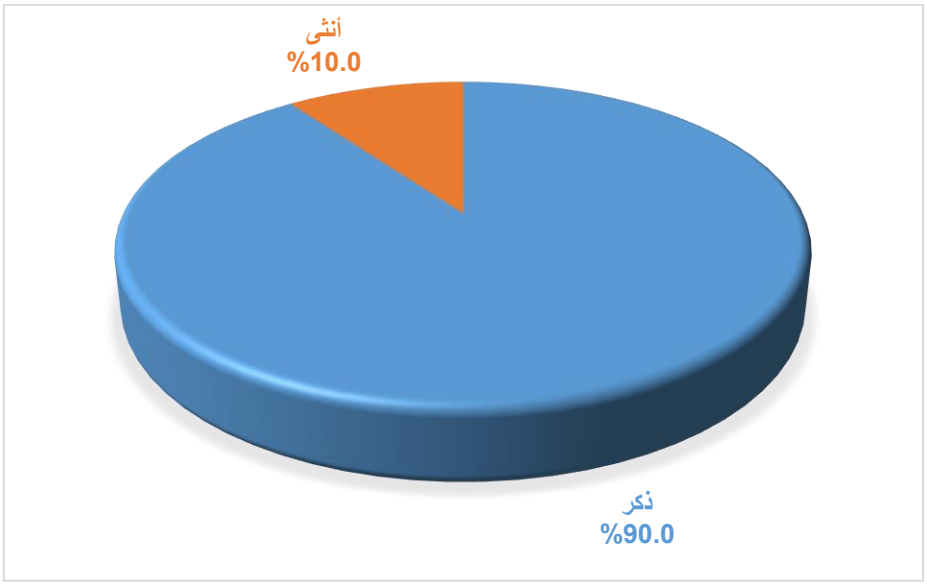
من خلال الجدول (٤–٢) السابق نجد أن قيم معاملات الثبات للمحاور جاءت متوسطة ومقبولة، حيث تراوحت بين (٠,٦٩٠ – ٠,٥٤٩)، وللاستبانة ككل الذي يتكون من (١٠ عبارات) بلغت (٠,٧١٧)، وتعتبر هذه القيمة مقبولة للباحث وتفي بتحقق الثبات لأداة الدراسة.

٢,٤ وصف عينة الدراسة

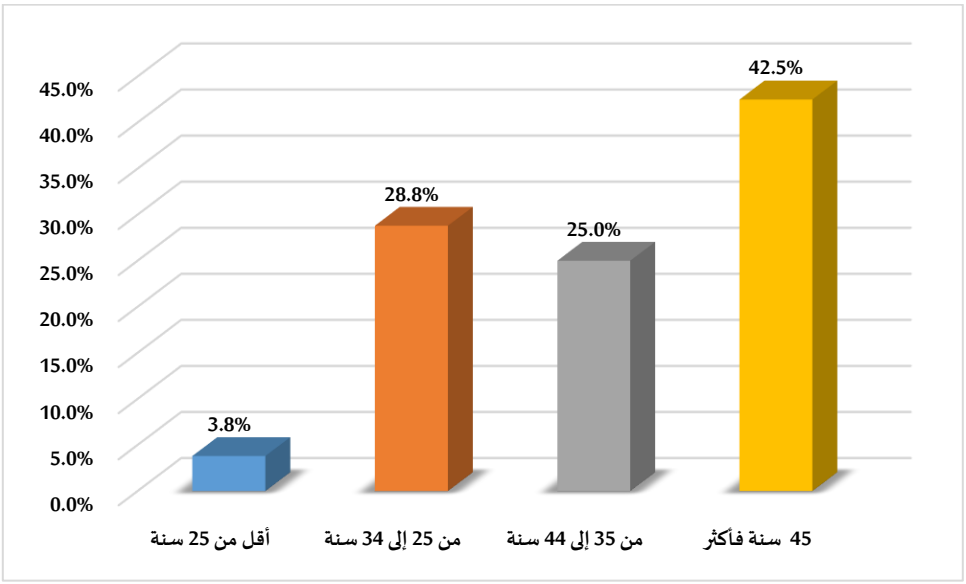
جدول رقم (٤–٣) توزيع عينة الدراسة وفقاً لمتغير الجنس

الجنس	العدد	النسبة
ذكر	72	% 90.0
أنثى	8	% 10.0
المجموع	80	% 100.0

من خلال الجدول (٤–٣) السابق يتضح أن غالبية أفراد عينة الدراسة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي بنسبة ٩٠,٠ % هم ذكور، بينما بلغت نسبة الإناث ١٠,٠ % فقط من إجمالي أفراد العينة. والشكل البياني التالي يوضح هذه النسب:



شكل بياني رقم (٤-١) توزيع أفراد العينة تبعاً لمتغير الجنس



شكل بياني رقم (٤-٢) توزيع أفراد العينة تبعاً لمتغير العمر

جدول رقم (٤-٤) توزيع عينة الدراسة وفقاً لمتغير العمر

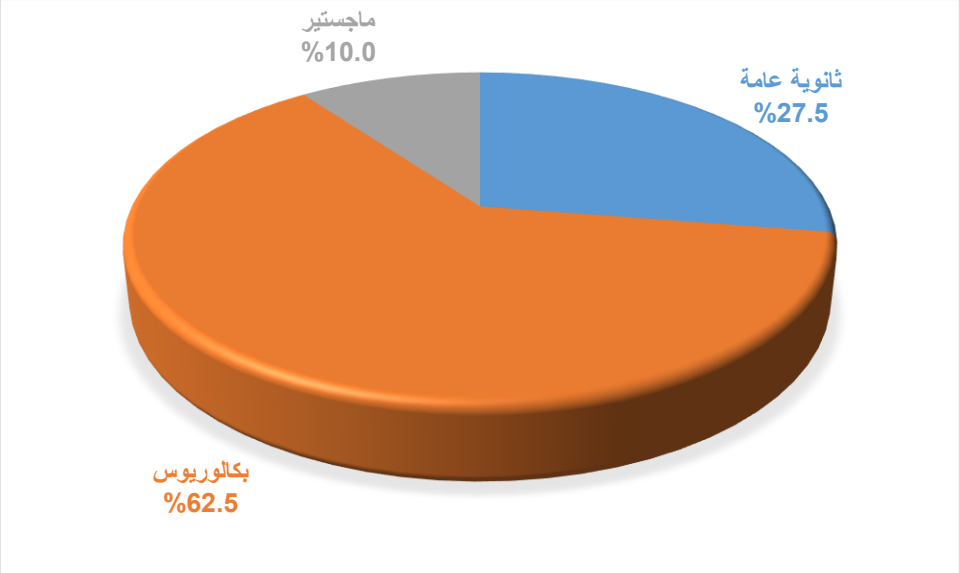
الفئات العمرية	العدد	النسبة
أقل من 25 سنة	3	% 3.8
من 25 إلى 34 سنة	23	% 28.8
من 35 إلى 44 سنة	20	% 25.0
45 سنة فأكثر	34	% 42.5
المجموع	80	% 100.0

من خلال الجدول (٤-٤) السابق يتضح أن نسبة **٤٢,٥ %** من أفراد العينة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي في الفئة العمرية (**٤٥** سنة فأكثر)، وأن نسبة **٢٨,٨ %** في الفئة العمرية (من **٢٥** إلى **٣٤** سنة)، وأن نسبة **٢٥,٠ %** في الفئة العمرية (من **٣٥** إلى **٤٥** سنة)، وأن نسبة **٣,٨ %** فقط في الفئة العمرية (أقل من **٢٥** سنة). والشكل البياني التالي يوضح هذه النسب:

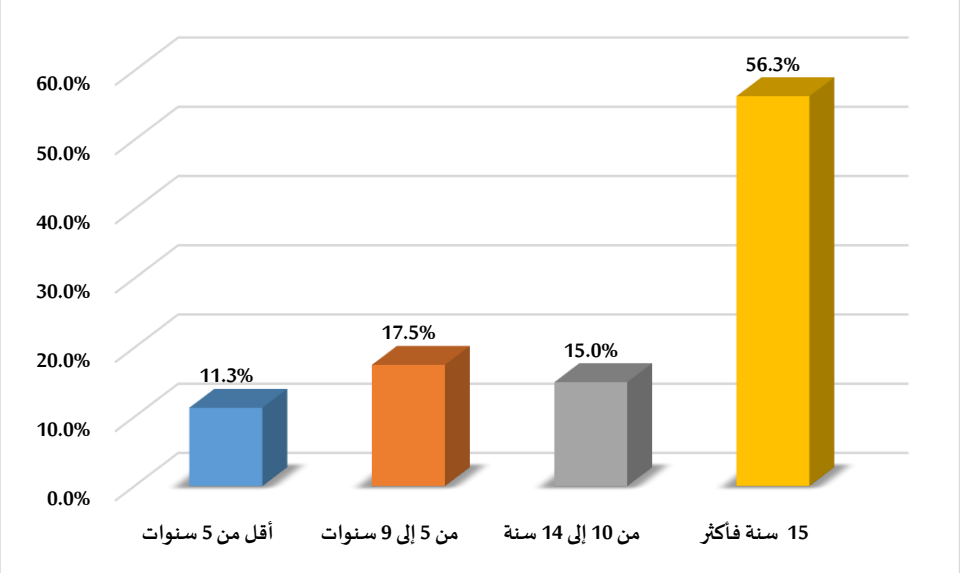
جدول رقم (٤-٥) توزيع عينة الدراسة وفقاً لمتغير المؤهل العلمي

المؤهل العلمي	العدد	النسبة
ثانوية عامة	22	% 27.5
بكالوريوس	50	% 62.5
ماجستير	8	% 10.0
المجموع	80	%100.0

من خلال الجدول (٤-٥) السابق يتضح أن غالبية أفراد العينة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي بنسبة **٦٢,٥ %** مؤهلهم العلمي (بكالوريوس)، وأن نسبة **٢٧,٥ %** مؤهلهم العلمي (ثانوية عامة)، وأن نسبة **١٠,٠ %** فقط مؤهلهم العلمي (ماجستير). والشكل البياني التالي يوضح هذه النسب:



شكل بياني رقم (٤-٣) توزيع أفراد العينة تبعاً لمتغير المؤهل العلمي



شكل بياني رقم (٤-٤) توزيع أفراد العينة تبعاً لمتغير سنوات الخبرة

جدول رقم (٤-٦) توزيع عينة الدراسة وفقاً لمتغير سنوات الخبرة

سنوات الخبرة	العدد	النسبة
أقل من 5 سنوات	9	% 11.3
من 5 إلى 9 سنوات	14	% 17.5
من 10 إلى 14 سنة	12	% 15.0
15سنة فأكثر	45	% 56.3
المجموع	80	%100.0

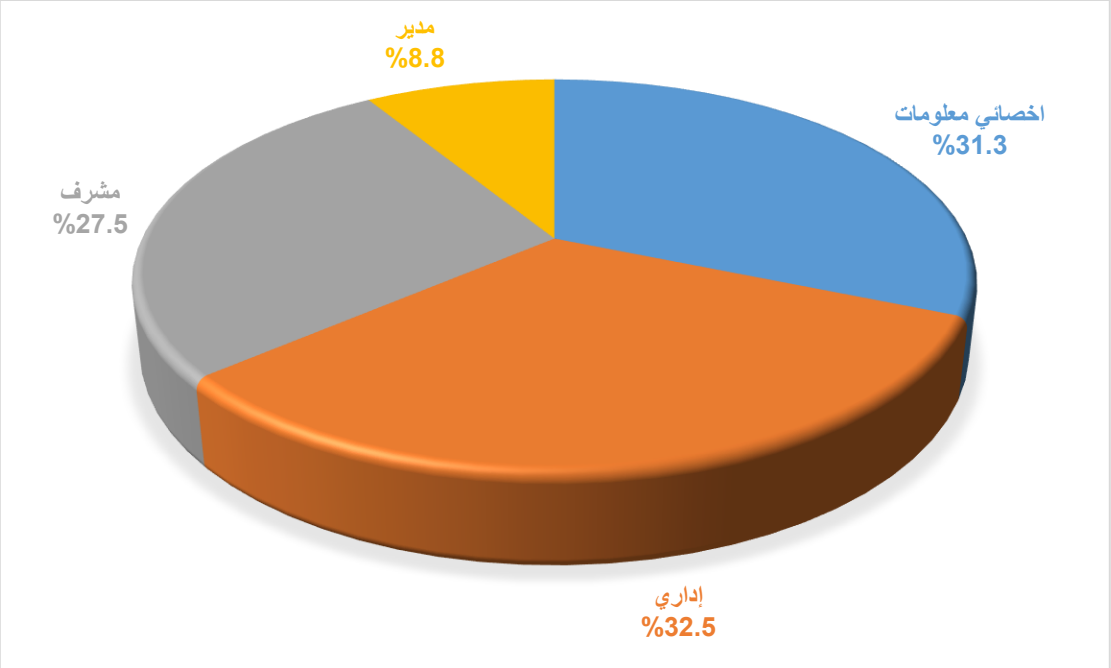
من خلال الجدول (٤-٦) السابق يتضح أن نسبة **٥٦,٣ %** من أفراد العينة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي تبلغ خبرتهم (**١٥** سنة فأكثر)، وأن نسبة **١٧,٥ %** تبلغ خبرتهم (من **٥** إلى **٩** سنوات)، وأن نسبة **١٥,٠ %** تبلغ خبرتهم (من **١٠** إلى **١٤** سنة)، وأن نسبة **١١,٣ %** تبلغ خبرتهم (أقل من **٥** سنوات). والشكل البياني التالي يوضح هذه النسب:

جدول رقم (٤-٧) توزيع عينة الدراسة وفقاً لمتغير الوظيفة الحالية

الوظيفة الحالية	العدد	النسبة
اخصائي معلومات	25	% 31.3
إداري	26	% 32.5
مشرف	22	% 27.5

مدير	7	% 8.8
المجموع	80	%100.0

من خلال الجدول (٤-٧) السابق يتضح أن نسبة **٣٢,٥ %** من أفراد العينة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي في وظيفة (إداري)، وأن نسبة **٣١,٣ %** في وظيفة (أخصائي معلومات)، وأن نسبة **٢٧,٥ %** في وظيفة (مشرف)، وأن نسبة **٨,٨ %** في وظيفة (مدير). والشكل البياني التالي يوضح هذه النسب:



شكل بياني رقم (٤-٥) توزيع أفراد العينة تبعاً لمتغير الوظيفة الحالية

٣,٤ تحليل أسئلة الدراسة

للإجابة على تساؤلات الدراسة، قام الباحث بتحليل عبارات محاور أداة الدراسة وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية للإجابات على كل عبارة من عبارات محاور الاستبانة، وذلك كما يلي:

التساؤل الأول: ما أخطار الذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات؟

للإجابة على هذا التساؤل، فقد قام الباحث بإجراء التحليل الإحصائي لعبارات المحور الأول وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد العينة على كل عبارة بالمحور الأول، وجاءت النتائج كما في الجدول التالي:

جدول رقم (٤-٨) أخطار الذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات مرتبة تنازلياً من وجهة نظر أفراد العينة

م	العبارات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	المستوى	الترتيب
١	هل تعتقد أن الذكاء الاصطناعي يمكن أن يشكل تهديدًا على خصوصية المعلومات على مستقبل المنظمات؟	4.00	1.01	80.0 %	موافق	٢
٢	هل سبق لك أن تعرضت لانتهاك خصوصية معلوماتك عبر الإنترنت؟	3.14	1.23	62.8 %	محايد	٣
٣	هل تعتقد أن الذكاء الاصطناعي يمكن أن يزيد من خطر انتهاك الخصوصية عبر الإنترنت؟	4.06	0.97	81.2 %	موافق	١
	المتوسط الحسابي لكامل المحور	3.73	1.07	74.6 %	موافق	

الجدول رقم (٤-٨) عبارة عن التحليل الإحصائي لعبارات المحور الأول: خطر الذكاء الاصطناعي، وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد عينة الدراسة على عبارات المحور. بلغ المتوسط العام للمحور (٣,٧٣) ويقع ضمن الفئة الثانية (٣,٤٠ -< ٤,٢٠) من مقياس ليكرت الخماسي ويشير إلى اتجاه الرأي العام نحو مستوى (موافق) وبنسبة مئوية كلية بلغت (٧٤,٦٪). بلغ

الانحراف المعياري لكامل المحور (**١,٠٧**) ويشير إلى مدى تجانس الإجابات نحو عبارات المحور، وبالتالي فإن غالبية أفراد عينة الدراسة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي يوافقون بنسبة **٧٤,٦٪** على وجود أخطار للذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات.

تم ترتيب العبارات تنازلياً وفقاً لقيمة المتوسط الحسابي لتشير إلى أبرز تلك الأخطار، حيث جاءت في المرتبة الأولى أن أفراد العينة يوافقون على أن الذكاء الاصطناعي يمكن أن يزيد من خطر انتهاك الخصوصية عبر الإنترنت حيث بلغ المتوسط الحسابي (**٤,٠٦**) بمستوى استجابة (موافق)، ثم جاءت في المرتبة الثانية أن أفراد العين يوافقون على أن الذكاء الاصطناعي يمكن أن يشكل تهديدًا على خصوصية المعلومات على مستقبل المنظمات، حيث بلغ المتوسط الحسابي (**٤,٠٠**) ويشير إلى مستوى استجابة (موافق)، ثم جاءت في المرتبة الثالثة (سبق لك أن تعرضت لانتهاك خصوصية معلوماتك عبر الإنترنت) بأقل متوسط حسابي بلغ (**٣,١٤**) ويشير إلى مستوى استجابة (محايد).

التساؤل الثاني: هل يمكن تطوير استراتيجيات وتوجيهات فعالة لتعزيز التدابير الوقائية وأمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي؟

للإجابة على هذا التساؤل، فقد قام الباحث بإجراء التحليل الإحصائي لعبارات المحور الثاني وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد العينة على كل عبارة بالمحور الثاني، وجاءت النتائج كما في الجدول التالي:

جدول رقم (٤–٩) الأمن والتدابير الوقائية مرتبة تنازلياً من وجهة نظر أفراد العينة

م	العبارات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	المستوى	الترتيب
٤	هل تعتقد أن هناك حاجة ملحة لتطوير قوانين ولوائح جديدة لحماية الخصوصية في عصر الذكاء الاصطناعي؟	4.43	0.67	88.6 %	موافق بشدة	٢
٥	هل تقوم باتخاذ تدابير إضافية لحماية خصوصية معلوماتك عبر الإنترنت (مثل	4.25	0.93	85.0 %	موافق بشدة	٣

	استخدام برامج حماية خصوصية أو تغيير كلمات المرور بانتظام)؟					
٦	**هل ترى أن التوعية بمخاطر الذكاء الاصطناعي على خصوصية المعلومات من خلال الحملات التعليمية تلعب دورًا مهمًا في تعزيز الأمن الرقمي؟**	**4.49**	**0.64**	**89.8 %**	**موافق بشدة**	**١**
	المتوسط الحسابي لكامل المحور	**4.39**	**0.75**	**87.8 %**	**موافق بشدة**	

الجدول رقم (**٤–٩**) عبارة عن التحليل الإحصائي لعبارات المحور الثاني: الأمن والتدابير الوقائية، وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد عينة الدراسة على عبارات المحور.

بلغ المتوسط العام للمحور (**٤,٣٩**) ويقع ضمن الفئة الأولى (**٤,٢٠ – ٥,٠**) من مقياس ليكرت الخماسي ويشير إلى اتجاه الرأي العام نحو مستوى (موافق بشدة) وبنسبة مئوية كلية بلغت (**٨٧,٨ %**). بلغ الانحراف المعياري لكامل المحور (**٠,٧٥**) وتشير إلى مدى تجانس الإجابات نحو عبارات المحور، وبالتالي فإن غالبية أفراد عينة الدراسة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي يوافقون بشدة بنسبة **٨٧,٨ %** على أنه يمكن تطوير استراتيجيات وتوجيهات فعالة لتعزيز التدابير الوقائية وأمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي.

تم ترتيب العبارات تنازلياً وفقاً لقيمة المتوسط الحسابي لتشير إلى أبرز طرق الأمن والتدابير الوقائية، حيث جاءت في المرتبة الأولى أن أفراد العينة يوافقون بشدة على (التوعية بمخاطر الذكاء الاصطناعي على خصوصية المعلومات من خلال الحملات التعليمية تلعب دورًا مهمًا في تعزيز الأمن الرقمي) والتي بلغ متوسطها الحسابي (**٤,٤٩**) ويشير إلى مستوى استجابة (موافق بشدة)، ثم جاءت في المرتبة الثانية أن أفراد العينة يوافقون بشدة على أن (هناك حاجة ملحة لتطوير قوانين ولوائح جديدة لحماية الخصوصية في عصر الذكاء الاصطناعي) بمتوسط حسابي بلغ (**٤,٤٣**) ومستوى استجابة (موافق بشدة)، ثم جاءت في المرتبة الثالثة أن أفراد العينة يوافقون بشدة على أنه يتم اتخاذ تدابير إضافية لحماية خصوصية معلوماتك عبر الإنترنت (مثل استخدام برامج حماية خصوصية

أو تغيير كلمات المرور بانتظام) حيث بلغ متوسطها الحسابي (**٤,٢٥**) ويشير إلى مستوى استجابة (موافق بشدة).

التساؤل الثالث: ما درجة الوعي والمعرفة بالأمن الرقمي في عصر التقدم التكنولوجي واستخدام الذكاء الاصطناعي في النظام التعليمي؟

للإجابة على هذا التساؤل، فقد قام الباحث بإجراء التحليل الإحصائي لعبارات المحور الثالث وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد العينة على كل عبارة بالمحور الثالث، وجاءت النتائج كما في الجدول التالي:

جدول رقم (٤–١٠) درجة الوعي والمعرفة بالأمن الرقمي في عصر التقدم التكنولوجي واستخدام الذكاء الاصطناعي في النظام التعليمي مرتبة تنازلياً من وجهة نظر أفراد العينة

م	العبارات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	المستوى	الترتيب
٧	هل تشعر أن لديك معرفة كافية حول كيفية حماية خصوصية معلوماتك في عصر الذكاء الاصطناعي؟	3.54	0.84	70.8 %	موافق	٢
٨	هل تعتقد أن هناك حاجة إلى تعزيز التوعية حول الأمن الرقمي وحماية الخصوصية في النظام التعليمي؟	3.65	0.73	73.0 %	موافق	١
٩	المتوسط الحسابي لكامل المحور	3.60	0.79	72.0 %	موافق	

الجدول رقم (٤–١٠) عبارة عن التحليل الإحصائي لعبارات المحور الثالث: الوعي والتعليم، وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد عينة الدراسة على عبارات المحور. بلغ المتوسط العام للمحور (٣,٦٠) ويقع ضمن الفئة الثانية (٣,٤٠ –< ٤,٢٠) من مقياس ليكرت الخماسي ويشير إلى اتجاه الرأي العام نحو مستوى (موافق) وبنسبة مئوية كلية بلغت (٧٢,٠ %). بلغ الانحراف المعياري لكامل المحور (٠,٧٩) ويشير إلى مدى تجانس الإجابات نحو عبارات المحور، وبالتالي فإن غالبية أفراد عينة الدراسة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي يوافقون بنسبة ٧٢,٠ % على درجة الوعي والمعرفة بالأمن الرقمي في عصر التقدم التكنولوجي واستخدام الذكاء الاصطناعي في النظام التعليمي.

تم ترتيب العبارات تنازلياً وفقاً لقيمة المتوسط الحسابي، حيث جاءت في المرتبة الأولى أن أفراد العينة يوافقون على (أن هناك حاجة إلى تعزيز التوعية حول الأمن الرقمي وحماية الخصوصية في النظام التعليمي) حيث بلغ متوسطها الحسابي (٣,٦٥) ويشير إلى مستوى استجابة (موافق)، ثم جاءت في المرتبة الثانية أن أفراد العينة يوافقون على أن لديهم معرفة كافية حول كيفية حماية خصوصية معلوماتك في عصر الذكاء الاصطناعي والتي بلغ متوسطها الحسابي (٣,٥٤) ويشير إلى مستوى استجابة (موافق).

التساؤل الرابع: ما درجة الثقة والاعتماد على استخدام تقنيات الذكاء الاصطناعي؟

للإجابة على هذا التساؤل، فقد قام الباحث بإجراء التحليل الإحصائي لعبارات المحور الرابع وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد العينة على كل عبارة بالمحور الرابع، وجاءت النتائج كما في الجدول التالي:

جدول رقم (٤–١١) درجة الثقة والاعتماد على استخدام تقنيات الذكاء الاصطناعي مرتبة تنازلياً من وجهة نظر أفراد العينة

م	العبارات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	المستوى	الترتيب
٩	هل تعتقد أن يجب أن يكون هناك مزيد من الشفافية من قبل الشركات التي تستخدم	4.31	0.79	86.2 %	موافق بشدة	٢

	التكنولوجيا الذكية لجمع ومعالجة المعلومات الشخصية؟					
١٠	**هل تعتقد أن الحكومات يجب أن تلعب دورًا أكبر في تنظيم استخدام التكنولوجيا الذكية وحماية خصوصية المواطنين؟**	**4.53**	**0.71**	**90.6 %**	**موافق بشدة**	**١**
١١	**المتوسط الحسابي لكامل المحور**	**4.42**	**0.75**	**88.4 %**	**موافق بشدة**	

الجدول رقم (**٤–١١**) عبارة عن التحليل الإحصائي لعبارات المحور الرابع: الثقة والاعتماد، وذلك بحساب المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد عينة الدراسة على عبارات المحور. بلغ المتوسط العام للمحور (**٤,٤٢**) ويقع ضمن الفئة الأولى (**٤,٢٠ – ٥,٠**) من مقياس ليكرت الخماسي ويشير إلى اتجاه الرأي العام نحو مستوى (موافق بشدة) وبنسبة مئوية كلية بلغت (**٨٨,٤ %**). بلغ الانحراف المعياري لكامل المحور (**٠,٧٥**) وتشير إلى مدى تجانس الإجابات نحو عبارات المحور، وبالتالي فإن غالبية أفراد عينة الدراسة من موظفي الشركات والمؤسسات التي تعمل بالذكاء الاصطناعي يوافقون بشدة بنسبة **٨٨,٤ %** على درجة الثقة والاعتماد على استخدام تقنيات الذكاء الاصطناعي.

تم ترتيب العبارات تنازلياً وفقاً لقيمة المتوسط الحسابي لتشير إلى أبرز مقومات الثقة والاعتماد، حيث جاءت في المرتبة الأولى أن أفراد العينة يوافقون بشدة على (أن الحكومات يجب أن تلعب دورًا أكبر في تنظيم استخدام التكنولوجيا الذكية وحماية خصوصية المواطنين) حيث بلغ متوسطها الحسابي (**٤,٥٣**) ويشير إلى مستوى استجابة (موافق بشدة)، ثم جاءت في المرتبة الثانية أن أفراد العينة يوافقون بشدة على (وجوب أن يكون هناك مزيد من الشفافية من قبل الشركات التي تستخدم التكنولوجيا الذكية لجمع ومعالجة المعلومات الشخصية) حيث بلغ متوسطها الحسابي (**٤,٣١**) ويشير إلى مستوى استجابة (موافق بشدة).

نتائج الاستبيان

يعتبر تحليل النتائج ومناقشته خطوة أساسية في البحث العلمي، حيث يُعنى هذا الفصل بتقديم التفسيرات والتحليلات العميقة للبيانات التي تم جمعها وتحصيلها من خلال الاستبيان المنجز. تم استخدام الاستبيان كأداة رئيسية لفهم وتحليل وجهات النظر والآراء والمعلومات التي قد تكون مفيدة لفهم وتحليل الظواهر المرتبطة بالموضوع المدروس.

تم اختيار عينة مكونة من **٨٠** موظفًا من مختلف المؤسسات والشركات في المملكة العربية السعودية باستخدام الطريقة العشوائية البسيطة. يتضح من الجدول الديموغرافي الذي سيُعرض في هذا الفصل العديد من السمات البيانية للمشاركين في الدراسة، مثل العمر والجنس والتخصص العلمي أو القطاع الصناعي الذي يعملون فيه.

سيتم في هذا الفصل استعراض النتائج التي تم جمعها من الاستبيان والتركيز على تحليلات محددة تُظهر الاتجاهات والمعرفة المكتسبة. كما سيتم إجراء مناقشة دقيقة وتحليل شامل لهذه النتائج بهدف فهم القضايا الرئيسية المرتبطة بالبحث وتفسيرها واستنتاجاتها.

الفصل الحالي يمثل الخطوة التالية الهامة لفهم البيانات المجمعة والتوصل إلى استنتاجات وافية تُسهم في تعميق الفهم للموضوع المدروس وتقديم الإضافة إلى المعرفة الحالية.

جدول رقم (٤–١٢) استبانة الأسئلة الأولية

المتغير	مستوى التغير	التكرار	النسبة المئوية
الجنس	ذكر	٧٢	% ٩٠,٠
	أنثى	٨	% ١٠,٠
العمر	أقل من ٢٥ سنة	٣	% ٣,٨
	من ٢٥ إلى ٣٤ سنة	٢٣	% ٢٨,٨
	من ٣٥ إلى ٤٤ سنة	٢٠	% ٢٥,٠
	٤٥ سنة فأكثر	٣٤	% ٤٢,٥
المؤهل العلمي	ثانوية عامة	٢٢	% ٢٧,٥
	بكالوريوس	٥٠	% ٦٢,٥

	ماجستير	٨	% ١٠,٠
	دكتوراه	٠	% ٠,٠
سنوات الخبرة	أقل من ٥ سنوات	٩	% ١١,٣
	من ٥ إلى ٩ سنوات	١٤	% ١٧,٥
	من ١٠ إلى ١٤ سنة	١٢	% ١٥,٠
	15سنةً فأكثر	٤٥	% ٥٦,٣
الوظيفة الحالية	اخصائي معلومات	٢٥	% ٣١,٣
	اداري	٢٦	% ٣٢,٥
	مشرف	٢٢	% ٢٧,٥
	مدير	٧	% ٨,٨

جدول رقم (٤–١٣) استبانة الأسئلة الثانوية

خطر الذكاء الاصطناعي							
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري
هل تعتقد أن الذكاء الاصطناعي يمكن أن يشكل تهديدًا على خصوصية المعلومات على مستقبل المنظمات؟	33.8 %	45.0 %	%12.5	%5.0	%3.8	4.00	1.01

هل سبق لك أن تعرضت لانتهاك خصوصية معلوماتك عبر الإنترنت؟	%13.8	%32.5	%16.3	28.8 %	%8.8	3.14	1.23
هل تعتقد أن الذكاء الاصطناعي يمكن أن يزيد من خطر انتهاك الخصوصية عبر الإنترنت؟	%38.8	%38.8	%13.8	%7.5	%1.3	4.06	0.97
الأمن والتدابير الوقائية							
هل تعتقد أن هناك حاجة ملحة لتطوير قوانين ولوائح جديدة لحماية الخصوصية في عصر الذكاء الاصطناعي؟	%52.5	%37.5	10.0 %	%0.0	%0.0	4.43	0.67
هل تقوم باتخاذ تدابير إضافية لحماية خصوصية معلوماتك عبر الإنترنت (مثل استخدام برامج حماية خصوصية أو تغيير كلمات المرور بانتظام)؟	%48.8	%35.5	%11.3	%2.5	%2.5	4.25	0.93
هل ترى أن التوعية بمخاطر الذكاء الاصطناعي على خصوصية المعلومات من خلال الحملات التعليمية تلعب دورًا مهمًا في تعزيز الأمن الرقمي؟	%56.3	%36.3	% 7.5	%0.0	%0.0	4.49	0.64

الوعي والتعليم							
هل تشعر أن لديك معرفة كافية حول كيفية حماية خصوصية معلوماتك في عصر الذكاء الاصطناعي؟	**%11.3**	**41.3 %**	**%38.8**	**%7.5**	**%1.3**	**3.54**	**0.84**
هل تعتقد أن هناك حاجة إلى تعزيز التوعية حول الأمن الرقمي وحماية الخصوصية في النظام التعليمي؟	**%62.5**	**30.0 %**	**% 7.5**	**%0.0**	**%0.0**	**3.65**	**0.73**
الثقة والاعتماد							
هل تعتقد أن يجب أن يكون هناك مزيد من الشفافية من قبل الشركات التي تستخدم التكنولوجيا الذكية لجمع ومعالجة المعلومات الشخصية؟	**%48.8**	**%36.3**	**%12.5**	**%2.5**	**%0.0**	**4.31**	**0.79**
هل تعتقد أن الحكومات يجب أن تلعب دورًا أكبر في تنظيم استخدام التكنولوجيا الذكية وحماية خصوصية المواطنين؟	**%63.8**	**%26.3**	**% 8.8**	**%1.3**	**%0.0**	**4.53**	**0.71**

الاجابة على السؤال الاول: ما هو تأثير هجمات الذكاء الاصطناعي على الأمن الرقمي والخصوصية للمؤسسات والشركات، وكيفية التصدي لهذه التأثيرات؟

٧٨,٨ % من المشاركين يرون أن الذكاء الاصطناعي يمكن أن يشكل تهديدًا على خصوصية المعلومات على مستقبل المنظمات. هذا يشير إلى قلق معتبر بين الأفراد حيال تلك القضية.

٤٦,٣ % من المشاركين أبلغوا أنهم سبق لهم أن تعرضوا لانتهاك خصوصية معلوماتهم عبر الإنترنت. هذا يشير إلى أن هناك عددًا كبيرًا من الأفراد قد تأثروا بشكل مباشر بمشكلة انتهاك الخصوصية.

٧٧,٦ % من المشاركين يعتقدون أن الذكاء الاصطناعي قد يزيد من خطر انتهاك الخصوصية عبر الإنترنت. هذا يشير إلى مخاوف مشتركة حيال تصاعد تلك المشكلة مع تطور التكنولوجيا واستخدام الذكاء الاصطناعي. بناءً على هذه النتائج، يبدو أن هناك حاجة ملحة إلى اتخاذ إجراءات إضافية لحماية الخصوصية وتعزيز الأمن عبر الإنترنت في مستقبل يشهد تقدمًا سريعًا في مجال الذكاء الاصطناعي.

الاجابة على السؤال الثاني: هل يمكن تطوير استراتيجيات وتوجيهات فعالة لتعزيز أمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي؟

٩٠,٠ % من المشاركين يرون أن هناك حاجة ملحة لتطوير قوانين ولوائح جديدة لحماية الخصوصية في عصر الذكاء الاصطناعي. هذا يشير إلى دعم قوي لتحسين الإطار القانوني للحفاظ على الخصوصية.

٨٣,٨ % من المشاركين يؤكدون على أنهم يقومون باتخاذ تدابير إضافية لحماية خصوصية معلوماتهم عبر الإنترنت، مثل استخدام برامج حماية خصوصية أو تغيير كلمات المرور بانتظام. هذا يشير إلى الوعي المتزايد بأهمية الأمن الرقمي والعمل الفعلي على تعزيزه.

٩٢,٦ % من المشاركين يرون أن التوعية بمخاطر الذكاء الاصطناعي على خصوصية المعلومات من خلال الحملات التعليمية تلعب دورًا مهمًا في تعزيز الأمن الرقمي. هذا يشير إلى دعم قوي للتثقيف والتوعية بمخاطر الاستخدام غير الآمن للتكنولوجيا.

بناءً على هذه النتائج، يمكن القول إن هناك حاجة إلى تطوير القوانين واللوائح لحماية الخصوصية في عصر الذكاء الاصطناعي، وأيضًا هناك وعي ملحوظ حيال أهمية الأمن الرقمي والعمل الفعلي على تعزيزه. كما تشير النتائج إلى دعم قوي لجهود التوعية بمخاطر الذكاء الاصطناعي وأهمية التثقيف في هذا السياق.

الاجابة على السؤال الثالث: ما هو تأثير تزايد استخدام الذكاء الاصطناعي على سوق العمل والمهن المختلفة وتقديم توصيات للمؤسسات والحكومات للتعامل مع التحديات والفرص الاقتصادية؟

٥٢,٦ % من المشاركين يشعرون أن لديهم معرفة كافية حول كيفية حماية خصوصية معلوماتهم في عصر الذكاء الاصطناعي. هذا يشير إلى وعي جيد بأساليب الحماية.

٩٢,٥ % من المشاركين يعتقدون أن هناك حاجة ملحة إلى تعزيز التوعية حول الأمن الرقمي وحماية الخصوصية في النظام التعليمي. هذا يشير إلى أن هناك فرصة لتحسين التوعية والتثقيف بشكل أفضل في المؤسسات التعليمية.

بناءً على هذه النتائج، يمكن القول إن هناك مستوى معين من الوعي بأمن البيانات وكيفية حمايتها في عصر الذكاء الاصطناعي. ومع ذلك، هناك فرصة لتحسين التوعية والتثقيف بشكل أوسع في النظام التعليمي لضمان تزويد الأفراد بالمعرفة والمهارات الضرورية لحماية خصوصيتهم.

الإجابة على السؤال الرابع: ما هي الأدوات والتقنيات الفعالة للكشف المبكر عن المخاطر والتصدي للهجمات التي تستخدم تقنيات الذكاء الاصطناعي؟

٨٥,١ % من المشاركين يعتقدون أن يجب أن يكون هناك مزيد من الشفافية من قبل الشركات التي تستخدم التكنولوجيا الذكية لجمع ومعالجة المعلومات الشخصية. يُظهر هذا توجهًا واعيًا نحو زيادة الشفافية في الممارسات التكنولوجية.

٩٠,١ % من المشاركين يعتقدون أن الحكومات يجب أن تلعب دورًا أكبر في تنظيم استخدام التكنولوجيا الذكية وحماية خصوصية المواطنين. هذا يشير إلى دعوة لزيادة دور الحكومات في تنظيم التكنولوجيا وتعزيز الحماية.

بناءً على هذه النتائج، يُظهر المشاركون تفهمًا لأهمية الشفافية من قبل الشركات وأيضًا الدور المناسب للحكومات في تنظيم وحماية الخصوصية في عصر التكنولوجيا الذكية. يمكن أن تساعد هذه الرؤى في توجيه السياسات والممارسات المستقبلية للتكنولوجيا.

٥. مناقشة النتائج

تمهيد

في هذا الفصل، سنتطرق إلى مناقشة النتائج المتعلقة بأسئلة الدراسة وفروضها الرئيسية. يهدف الفصل إلى استعراض النتائج التي تم الحصول عليها من خلال الاستبيان أو الدراسة والتحليل المفصّل لهذه النتائج بناءً على الأسئلة الأساسية والفروض التي وضعت لهذا البحث.

سنبدأ بمناقشة النتائج المتعلقة بأسئلة الدراسة الرئيسية، حيث سيتم تحليل البيانات والتركيز على الاستجابات المتعلقة بكل سؤال من أسئلة الدراسة. سيتم استعراض الاتجاهات والمعلومات التي تم الحصول عليها وتحليلها بشكل مفصّل لفهم مدى تأثيرها وعلاقتها بموضوع البحث.

ثم سنتحول إلى مناقشة النتائج المتعلقة بفروض الدراسة وتحليلها. سيتم استعراض البيانات التي تم جمعها وتقييم كيفية تطابقها مع الفروض المفروضة في بداية البحث. سيتم التركيز على تحليل مدى تأييد أو تفنيده لهذه الفروض من خلال البيانات التي تم جمعها.

تهدف هذه المناقشة إلى فهم النتائج بشكل أعمق واستنتاجات أكثر دقة لتحليل الأسئلة والفروض المطروحة في إطار البحث. سيتم التركيز على القضايا الرئيسية والاستنتاجات الأساسية التي يمكن استخلاصها من هذه النتائج بما يسهم في تعزيز المعرفة وفهم الموضوع المدروس.

مناقشة النتائج

يمكن تطوير استراتيجيات وتوجيهات فعالة لتعزيز أمن المعلومات وخصوصيتها في ظل التقدم التكنولوجي واستخدام الذكاء الاصطناعي كتقنيات التعلم الآلي لتحليل البيانات واكتشاف الأنماط والسلوكيات غير المعتادة التي تشير إلى هجمات محتملة، كما يمكن لهذا التحليل المتقدم مساعدة الشركات في التعرف على التهديدات قبل أن تحدث أضرارًا كبيرة، وتوجيه الاستثمار نحو تطوير نظم الحماية المتقدمة واعتراض واستجابة الهجمات السيبرانية. يمكن لهذا التوجيه تعزيز قدرة الشركة على التصدي للهجمات والدفاع عن بنيتها التحتية، وتحسين الحماية من الهجمات على البريد الإلكتروني.

استخدام الذكاء الاصطناعي لتحليل البريد الإلكتروني واكتشاف الرسائل المشبوهة والتصيّد الاصطناعي. بفضل هذه التقنيات، يمكن تقليل فرص نجاح هجمات البريد الإلكتروني والحفاظ على سلامة الاتصالات، وتشفير البيانات في حالة النقل والتخزين لضمان أمن المعلومات. هذا يساهم في حماية البيانات من الوصول غير المصرح به وضمان سرية المعلومات المهمة، ووضع سياسات صارمة للخصوصية والحفاظ على الامتثال للتشريعات المحلية والعالمية مثل **GDPR** و**CCPA**. هذا يسهم في حماية البيانات الشخصية والامتثال للقوانين، كما يتم تقييد الوصول إلى البيانات والأنظمة الحساسة بوجه منع الوصول غير المصرح به. هذا يسهم في تقليل فرص الوصول غير المصرح به وحماية البيانات، وتوجيه الموظفين والمستخدمين النهائيين في مجال الأمن والخصوصية وتوفير تدريب دوري لزيادة الوعي بالتهديدات السيبرانية. يمكن لهذا التوعية والتدريب تقليل خطر الهجمات بسبب الأخطاء البشرية.

كما اتضح من دراسة Manheim, K., & Kaplan, L (٢٠١٩) ودراسة Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021) أن تأثير هجمات الذكاء الاصطناعي على الأمان الرقمي والخصوصية للمؤسسات والشركات يعتمد على الطرق والأساليب المستخدمة وقدرة الشركات على التصدي لهذه التحديات. يتعرض الأمن الرقمي والخصوصية للمؤسسات لتهديدات متنوعة نتيجة استخدام الذكاء الاصطناعي في عمليات الاختراق والاحتيال والتجسس السيبراني، فتستخدم هذه الهجمات التقنيات الذكية للتلاعب بالضحايا واستخراج معلومات حساسة، ويمكن تدريب الموظفين على التعرف على البريد الإلكتروني والرسائل المشبوهة، واستخدام أنظمة مكافحة البرمجيات الضارة وحماية البريد الإلكتروني لتصفية الهجمات، كما ذكر في دراسة كلا من "الأسد، الأسد صالح" (٢٠٢٣) ودراسة "نوار، اسماء عاطف عبد السلام عثمان (٢٠٢٣)" أن استخدام التكنولوجيا الذكية، بما في ذلك الذكاء

الاصطناعي، يحمل إمكانيات كبيرة للتطوير الاقتصادي والتحسين في الدول العربية، وهو ما يتماشى مع نتائج الدراسة الحالية التي أشارت إلى ضرورة توجيه الاستثمار نحو تقنيات الحماية للمؤسسات في مواجهة التحديات السيبرانية، كما اشارت دراسة: عبد الهادي، محمود (٢٠٢٣)، ودراسة علي، منذر محمد (٢٠٢٢) أن الذكاء الاصطناعي يستخدم لاختراق أنظمة الأمن والدخول غير المصرح به، ويجب تحسين أمن البيانات والشبكات باستخدام أنظمة اعتراض واستجابة (**IDS/IPS**) والحماية المتقدمة للهجمات، كما تستخدم الذكاء الاصطناعي لاكتشاف الثغرات في العمليات المالية والمعاملات، ويمكن بناء نماذج تعرف على الاحتيال باستخدام الذكاء الاصطناعي والتحليل الاحصائي لتحديد الاحتيال بشكل فعال، كما يمكن للذكاء الاصطناعي تسهيل سرقة البيانات الشخصية والحساسة، ويجب تشديد حماية البيانات باستخدام تشفير البيانات، وإعداد سياسات الخصوصية الصارمة، والامتثال للتشريعات الخاصة بالخصوصية مثل**GDPR** و **CCPA**، كما يستخدم الروبوتات والطائرات بدون طيار مهمات تجسس أو تدمير، ويمكن استخدام تكنولوجيا الاعتراض والكشف عن الأجسام غير المرغوب فيها لمنع هجمات الطائرات بدون طيار، وتأمين المناطق الحساسة، كما يمكن للذكاء الاصطناعي استخدام البيانات الكبيرة للكشف عن أنماط معينة في السلوك والتوجهات، وتقوم الشركات بحماية بيانات العملاء والمعلومات الحساسة من الاستخدام غير المصرح به وضمان الامتثال للقوانين، ومن خلال نسبة العينة في الاتفاق على تأثير تزايد استخدام الذكاء الاصطناعي على سوق العمل والمهن المختلفة وتقديم توصيات للمؤسسات والحكومات للتعامل مع التحديات والفرص الاقتصادية، وتزايد استخدام الذكاء الاصطناعي يشكل تأثيرًا كبيرًا على سوق العمل والمهن المختلفة. إليك نظرة عامة على هذا التأثير وتوصيات للمؤسسات والحكومات للتعامل مع هذه التحديات والاستفادة من الفرص الاقتصادية، وهذه نفس النتائج التي اشارت اليها دراسة كلا من "الفار، مايسة، داود، ومينا إسحق توفيلس (٢٠٢٣)" ودراسة "Oseni (٢٠٢١)".

٦. النتائج والتوصيات

تمهيد

تعتبر نتائج الدراسة هي عملية كتابة الإجابات عن الفرضيات والتساؤلات التي عرضها الباحث في مضمون البحث، وكذلك كتابة اكتشافات ما رآه الباحث من خلال إعداده البحث ثم بعد عرض النتائج الخاصة بالبحث يكمن التوصل الى اهم النتائج التي توصل اليها الباحث خلال بحثه.

١,٦ النتائج

التأثير على سوق العمل

١. **تغيير متطلبات المهارات:** يجعل تطور التكنولوجيا واستخدام الذكاء الاصطناعي الأتمتة والتحليل البياني جزءًا أساسيًا من العديد من الصناعات. هذا يعني أن الطلب على المهارات الرقمية والتحليلية سيزيد.

٢. **التحديات في مجال العمل:** قد يؤدي الاستخدام المتزايد للذكاء الاصطناعي إلى التشغيل آلي لبعض الوظائف، مما يخلق تحديات لبعض القطاعات والعمال. يجب أن تتخذ السياسات للتعامل مع التحديات الاقتصادية والاجتماعية المحتملة.

٣. **إمكانية إنشاء وظائف جديدة:** توفر تقنيات الذكاء الاصطناعي أيضًا فرصًا لإنشاء وظائف جديدة في مجالات مثل تطوير البرمجيات وإدارة البيانات وتصميم النظم.

توصيات للمؤسسات

١. **استثمار في التدريب وتطوير الموارد البشرية:** تعزيز المهارات الرقمية للموظفين الحاليين وتطوير قاعدة مهارات قوية في مجالات الذكاء الاصطناعي والتحليل البياني. هذا يمكن أن يساعد في تجهيز الموظفين للتعامل مع التكنولوجيا الجديدة.

٢. **التكامل بين البشر والذكاء الاصطناعي:** يجب أن تسعى المؤسسات لاستخدام الذكاء الاصطناعي كأداة داعمة للبشر بدلاً من بديل لهم. يمكن للذكاء الاصطناعي تعزيز أداء العمل واتخاذ القرارات الاستراتيجية.

٣. **التمويل والاستثمار في الابتكار:** يمكن للمؤسسات البحث عن فرص للاستثمار في مجالات الذكاء الاصطناعي والابتكار التقني. هذا يمكن أن يساعد في تعزيز التنافسية وتطوير منتجات وخدمات جديدة.

توصيات للحكومات

١. **إعداد التعليم والتدريب:** توفير برامج تعليمية وتدريبية متخصصة في مجالات الذكاء الاصطناعي والتكنولوجيا المرتبطة. يمكن أن تتعاون الحكومات مع المؤسسات التعليمية والصناعة لتحقيق ذلك.

٢. **تنظيم ورصد الأثر الاقتصادي والاجتماعي:** يجب على الحكومات مراقبة الأثر الاقتصادي والاجتماعي للاستخدام المتزايد للذكاء الاصطناعي والتحرك بناءً على البيانات والأدلة.

٣. **تشجيع الابتكار:** توفير مناخ أعمال مشجع لشركات التكنولوجيا والشركات الناشئة التي تعمل في مجال الذكاء الاصطناعي. قد تشمل ذلك التحفيزات الضريبية والتمويل العام.

هناك العديد من الأدوات والتقنيات الفعالة للكشف المبكر عن المخاطر والتصدي للهجمات التي تستخدم تقنيات الذكاء الاصطناعي. تتضمن بعض هذه الأدوات والتقنيات:

١. **أنظمة اكتشاف التسلل (IDS)**: تعتمد هذه الأنظمة على تحليل حركة البيانات وسلوك المستخدمين للكشف عن أنماط غير عادية. يمكن تكييفها لاكتشاف هجمات تستخدم تقنيات الذكاء الاصطناعي مثل هجمات الاختراق الذكي.

٢. **التحليل السلوكي وتحليل السياق**: يمكن استخدام التحليل السلوكي للتعرف على سلوك مستخدمي النظام والكشف عن أي تغييرات غير معتادة في سلوكهم. تعتمد تلك التقنيات على مراقبة السلوك بدقة وتحليل السياق لاكتشاف هجمات متقدمة.

٣. **التعلم الآلي والذكاء الصناعي**: يمكن استخدام تقنيات التعلم الآلي والذكاء الصناعي لتحليل البيانات بشكل آلي والكشف عن أنماط غير عادية أو هجمات محتملة. يمكن تدريب نماذج الذكاء الصناعي على معرفة السلوك الطبيعي والكشف عن الانحرافات.

٤. **التحليل المتقدم للتهديدات (ATA)**: تستخدم تقنيات **ATA** لتحليل البيانات من مصادر متعددة للكشف عن هجمات متقدمة تستخدم تقنيات الذكاء الاصطناعي. تتضمن هذه الأدوات تقنيات تحليل السلوك والتصنيف المتقدم للتهديدات.

٥. **حلول أمن الشبكات القائمة على السحابة**: تقدم بعض الشركات حلول أمن الشبكات القائمة على السحابة التي تستخدم الذكاء الاصطناعي للكشف عن هجمات الشبكات والتهديدات الأمنية.

٦. **تحليل السياق والمعرفة الأمنية**: تقنيات تحليل السياق والمعرفة الأمنية تعتمد على فهم أفضل للسياق والتاريخ الأمني للنظام للكشف عن تهديدات مستدامة.

٧. **التعاون بين الشبكات ومشاركة المعلومات**: يمكن أن تكون مشاركة المعلومات حول التهديدات والهجمات بين مؤسسات مختلفة والتعاون بينها أداة فعالة للكشف المبكر عن هجمات تستخدم تقنيات الذكاء الاصطناعي.

٨. **الاستراتيجيات الدفاعية متعددة الطبقات**: يجب تنفيذ استراتيجيات دفاعية متعددة الطبقات تتضمن تدابير تكنولوجية وإجرائية لضمان تغطية واستجابة شاملة للتهديدات.

٩. **تحليل الضرر والاستجابة السريعة**: يجب وضع استراتيجيات لتحليل الضرر بعد الهجوم والاستجابة السريعة لاحتواء التهديد واستعادة النظام.

١٠. **التدريب والتوعية الأمنية**: تعتبر التدريب والتوعية الأمنية للموظفين والمستخدمين جزءًا مهمًا في الكشف المبكر عن التهديدات، حيث يمكنهم التعرف على علامات التهديد واتخاذ الإجراءات المناسبة.

يجب أن تتعدد الأدوات والتقنيات المستخدمة لتوفير نهج متعدد الطبقات للأمن، ويجب أن تكون هذه الأدوات متكاملة مع بعضها البعض لضمان الكشف المبكر عن التهديدات والحماية منها.

٢,٦ التوصيات

- **تقييم مختلف تطبيقات الذكاء الاصطناعي**: دراسة مختلف التطبيقات والمجالات التي تستخدم فيها تقنيات الذكاء الاصطناعي، مثل الصحة والتعليم والأعمال والأمن. حدد كيف يؤثر الاستخدام المتزايد للذكاء الاصطناعي على خصوصية وأمن المعلومات في هذه المجالات.
- **تحليل التهديدات الأمنية**: دراسة التهديدات الأمنية التي يمكن أن تنشأ نتيجة استخدام تقنيات الذكاء الاصطناعي. هذا يشمل الاعتبارات المتعلقة بالاختراقات وسرقة البيانات واستغلال الثغرات في أنظمة الذكاء الاصطناعي.
- **التشريعات واللوائح القانونية**: دراسة التأثيرات المحتملة للتشريعات واللوائح القانونية المتعلقة بالخصوصية وأمن المعلومات على استخدام تقنيات الذكاء الاصطناعي. هل هناك حاجة لتطوير قوانين جديدة أو تعديل القوانين الحالية؟ يجب تطوير القوانين لتواكب التكنولوجيا الحديثة
- **تقنيات الحماية والتشفير**: دراسة التقنيات والأدوات المتاحة لحماية البيانات والمعلومات من تهديدات الأمن المرتبطة بالذكاء الاصطناعي، مثل التشفير والأمن السيبراني.
- **المسؤولية القانونية والأخلاقية**: استكشف مسائل المسؤولية القانونية والأخلاقية المتعلقة بالاستخدام والتطوير والنشر لتقنيات الذكاء الاصطناعي. هل يجب تحديد المسؤولية عن الأضرار المحتملة؟
- **تأثير الذكاء الاصطناعي على الخصوصية الفردية**: دراسة تأثير تقنيات الذكاء الاصطناعي على الخصوصية الفردية وكيف يمكن تعزيز الوعي بأهمية حماية البيانات الشخصية.
- **التحديات التقنية**: التحديات التقنية المرتبطة بحفظ خصوصية المعلومات في عصر الذكاء الاصطناعي، مثل تحليل البيانات الكبيرة والتشفير الكمي.

٣,٦ الخاتمة

إن تطبيقات الذكاء الاصطناعي تفرض تحديات كبيرة على حقوق الإنسان، مشيرة إلى أن "استخدام التكنولوجيا

في آليات صنع القرار في القطاع العام تشكل تحديا لحقوق المواطنين في بعض الآحيان".

أن التعامل بمسؤولة مع الذكاء الاصطناعي ليست على "عاتق الحكومات والأفراد فقط، بل تقع في المرتبة الأولى على عاتق الشركات التي تطور هذه التكنولوجيا، وعليهم الموازنة بين التطوير وحماية حقوق الإنسان." ينبغي تشجيع الابتكارات التكنولوجية التي تركز على تعزيز حقوق الإنسان والتنمية المستدامة ودعم تمثيل المجتمع المدني والمنظمات غير الحكومية في المناقشات حول استخدام الذكاء الاصطناعي وحقوق الإنسان."ان المخاوف من أن استخدام تقنيات الذكاء الاصطناعي من البعض يكون "أمرا مجهولا، وهو ما يجعل من الصعب معرفة أين؟ وكيف تستخدم هذه الأنظمة؟"، ولهذا يجب أن يتم التعامل دوليا مع هذا الأمر بشكل شفاف ومعلن. كما يجب اتخاذ إجراءات لمكافحة انتشار "برامج التجسس التجاري" من خلال تعميق التعاون الدولي، ووضع مبادئ توجيهية حول استخدام الحكومات لتكنولوجيا المراقبة، إضافة تعزيز المبادرات لتعزيز الأمن السيبراني للمجتمعات الأكثر عرضة للخطر، أو المعرضين للقمع العابر للحدود.

أن التكنولوجيا الحديثة مثل أنظمة الذكاء الاصطناعي والتقنيات الحيوية لها فوائد قد تكون مغيرة للواقع بشكل كبير، ولهذا يجب ضمان ألا تكون الابتكارات والتقدم على حساب القيم الديمقراطية وحقوق الإنسان. يجب وضع خارطة طريق لتحقيق هذه الأهداف من خلال مشاريع قوانين الذكاء الاصطناعي وأطر العمل لإدارة مخاطر هذه التقنية.

المراجع العربية

١. ابو زيد، ا. ا.، & احمد الشورى. (٢٠٢٢). الذكاء الاصطناعي وجودة الحكم. مجلة كلية الاقتصاد والعلوم السياسية, ٢٣(٤), ١٤٥-١٧٦.

٢. حسين أبو منصور. (٢٠٢١). الذكاء الاصطناعي وأبعاده الأمنية. أوراق السياسات الأمنية, ٠١-١٨.

٣. وفاء فواز المالكي. (٢٠٢٣). دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي (مراجعة الأدبيات). مجلة العلوم التربوية والنفسية, ٧(٥), ٩٣-١٠٧.

٤. Al Debaisi, A. A. (٢٠٢٣). صحافة الذكاء الاصطناعي والتحديات المهنية والأخلاقية. مجلة الجامعة الإسلامية للبحوث الإنسانية, ٣١(٣).

٥. العزب، م.، محمد، & النشار. (٢٠٢٢). الذكاء الاصطناعي وانعكاساته في التعليم. المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب, ٢(٢), ١٣-٣٠.

٦. سعد احمد محمد، م.، & محمد. (٢٠٢١). دور التأمين في مواجهة المخاطر الناشئة عن الذكاء الاصطناعي وتكنولوجيا المعلومات" دراسة تحليلية. 112(543), 459-504.

٧. الأسد، & الأسد صالح. (٢٠٢٣). الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية. مجلة إضافات اقتصادية, ٧(١), ١٦٥-١٨٤.

٨. عبد الهادي، م.، & محمود. (٢٠٢٣). الحماية القانونية من مخاطر أدوات الذكاء الاصطناعي المستخدمة في تصفية المحتويات المرئية عبر شبكة الانترنت، مجلة البحوث الفقهية والقانونية, ٤١(٤١), ٨٣-١٢٧.

٩. علي، منذر محمد، عبدالله، عمرو صلاح، خطاب، & جمال سعد. (٢٠٢٢). أثر تفعيل تقنيات الذكاء الاصطناعي علي تعزيز أنشطة المراجعة الداخلية. مجلة الإسكندرية للبحوث المحاسبية, ٦(٣), ١-٤٠.

١٠. باحث الدكتوراه فلاح ساهي خلف. (٢٠٢٣). التوجه الموضوعي للمسؤولية المدنية عن أنشطة الذكاء الاصطناعي. مجلة الباحث للعلوم القانونية, ٤(١).

١١. الأسد، الأسد صالح. (٢٠٢٣). الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية. مجلة إضافات اقتصادية.

١٢. نوار، اسماء عاطف عبد السلام عثمان (٢٠٢٣). الحماية المدنية لحقوق الإنسان الطبيعية من مخاطر الذكاء الاصطناعي للروبوت. مجلة بنها للعلوم الإنسانية.

١٣. عبد الهادي، محمود. (٢٠٢٣). الحماية القانونية من مخاطر أدوات الذكاء الاصطناعي المستخدمة في تصفية المحتويات المرئية عبر شبكة الانترنت، مجلة البحوث الفقهية والقانونية, ٤١(٤١), ٨٣-١٢٧.

١٤. علي، منذر محمد. (٢٠٢٢). أثر تفعيل تقنيات الذكاء الاصطناعي علي تعزيز أنشطة المراجعة الداخلية. مجلة الإسكندرية للبحوث المحاسبية, ٦(٣), ١-٤٠.

١٥. الفار، مايسة، داود، ومينا إسحق توفيلس. (٢٠٢٣). أخلاقيات الذكاء الاصطناعي: مناقشة المخاطر المحتملة والمعضلات الأخلاقية المرتبطة بها في الفن والتصميم. مجلة التراث والتصميم.

١٦. حسن، إبراهيم محمد. (٢٠١٨). "الذكاء الاصطناعي وانعكاساته على أداء المنظمة". مجلة الإدارة والاقتصاد.

١٧. المومني، حسن أحمد. (٢٠١٩). "أهمية وأثر الذكاء الاصطناعي في مستقبل العمل". المؤتمر السنوي الخامس والعشرين لجمعية المكتبات المتخصصة، فرع الخليج العربي.

١٨. أحمد، أبو بكر سلطان. (٢٠٢١). أخلاقيات الذكاء الاصطناعي. مجلة القافلة، مج٧٠, ع٤ ، ٨٢ – ٨٩.

١٩. النسور، مرح فراس محمد، وبقيلة، بسام خليل عطا الله. (٢٠٢٢). أثر الذكاء الاصطناعي في التدقيق المبني على المخاطر: الدور الوسيط لجودة التدقيق في البنوك التجارية الأردنية .جامعة العلوم الإسلامية العالمية، عمان.
https://search.mandumah.com/Record/1334614

٢٠. العمر، رناد مجدي حسن، والعكور، سامر محمد حسين. (٢٠٢٢). أثر الذكاء الاصطناعي في الحد من مخاطر المحاسبة السحابية للشركات الصناعية الأردنية، جامعة العلوم الإسلامية العالمية، عمان.
https://search.mandumah.com/Record/1328680

٢١. المجالي، محمد صلاح، وحميدات، محمد محمود أحمد. (٢٠٢٣). أثر استخدام تقنيات الذكاء الاصطناعي في تخفيض مخاطر التدقيق الخارجي في الأردن: الدور المعدل لجدارة المدقق. جامعة البلقاء التطبيقية، السلط.
https://search.mandumah.com/Record/1385061

٢٢. الأسدي، محي الدين فهمي، وأبو الهيجاء، محمد فوزي. (٢٠٢٢). أثر الذكاء الاصطناعي على إدارة المخاطر المؤسسية في البنوك التجارية الأردنية: الدور المعدل – كفاءة نظام الرقابة الداخلي جامعة جرش، جرش.
https://search.mandumah.com/Record/1357539

٢٣. الحجاج، إبراهيم حسن سالم، والعكور، سامر محمد حسين. (٢٠٢٢). أثر فاعلية التدقيق الداخلي في الحد من مخاطر الذكاء الاصطناعي في الشركات الصناعية المدرجة في بورصة عمان. جامعة العلوم الإسلامية العالمية، عمان.
https://search.mandumah.com/Record/1263908/Description

المراجع الإنجليزية

١. Nadimpalli, M. (2017). Artificial intelligence risks and benefits. International Journal of Innovative Research in Science, Engineering and Technology, 6(6).
٢. Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2(38), 1-9.
٣. Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. Yale JL & Tech., 21, 106.
٤. Parnas, D. L. (2017). The real risks of artificial intelligence. Communications of the ACM, 60(10), 27-31.
٥. Yigitcanlar, T., Desouza, K. C., Butler, L., & Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. Energies, 13(6), 1473.
٦. Müller, V. C. (Ed.). (2016). Risks of artificial intelligence. CRC Press.
٧. Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. Harv. JL & Tech., 29, 353.
٨. Osoba, O. A., Welser IV, W., & Welser, W. (2017). An intelligence in our image: The risks of bias and errors in artificial intelligence. Rand Corporation.
٩. Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. Berkman Klein Center Research Publication, (2018-6).
١٠. Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, *21*, 106.
١١. Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. arXiv preprint arXiv:2102.04661.

١٢. Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. Electronics, 12(18), 3786.

١٣. *AI, Data Analysis and Algorithms: Campaign*. Fair Trials. (2023, November 7). https://www.fairtrials.org/campaigns/ai-algorithms-data/?gad_source=1&gclid

الملاحق

بعنوان (مخاطر الذكاء الاصطناعي على خصوصية أمن المعلومات على مستقبل المنظمات)

أ. مقدمة الاستبيان

السلام عليكم ورحمة الله وبركاته

انا طالب ماجستير اقوم بدراسة حول مخاطر الذكاء الاصطناعي على خصوصية أمن المعلومات على مستقبل المنظمات، علما بأن المعلومات سرية، ولن تستخدم إلا لأغراض البحث العلمي، تتكون أسئلة البحث من عشر أسئلة.

ب. الأسئلة العامة

الجنس

- **ذكر**
- **أنثى**

العمر

- **أقل من ٢٥ سنة**
- **من ٢٥ إلى ٣٤ سنة**
- **من ٣٥ إلى ٤٤ سنة**
- **٤٥ سنة فأكثر**

المؤهل العلمي

- **ثانوية عامة**
- **بكالوريوس**
- **ماجستير**

- دكتوراة

سنوات الخبرة

- أقل من ٥ سنوات
- من ٥ إلى ٩ سنوات
- من ١٠ إلى ١٤ سنة
- ١٥ سنةً فأكثر

الوظيفة الحالية

- اخصائي معلومات
- اداري
- مشرف
- مدير

ج. الأسئلة الرئيسية

خطر الذكاء الاصطناعي							
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري

هل تعتقد أن الذكاء الاصطناعي يمكن أن يشكل تهديدًا على خصوصية المعلومات على مستقبل المنظمات؟							
هل سبق لك أن تعرضت لانتهاك خصوصية معلوماتك عبر الإنترنت؟							
هل تعتقد أن الذكاء الاصطناعي يمكن أن يزيد من خطر انتهاك الخصوصية عبر الإنترنت؟							
الأمن والتدابير الوقائية							
هل تعتقد أن هناك حاجة ملحة لتطوير قوانين ولوائح جديدة لحماية الخصوصية في عصر الذكاء الاصطناعي؟							
هل تقوم باتخاذ تدابير إضافية لحماية خصوصية معلوماتك عبر الإنترنت (مثل استخدام برامج حماية خصوصية أو تغيير كلمات المرور بانتظام)؟							
هل ترى أن التوعية بمخاطر الذكاء الاصطناعي على خصوصية المعلومات من خلال الحملات التعليمية تلعب دورًا مهمًا في تعزيز الأمن الرقمي؟							
الوعي والتعليم							

هل تشعر أن لديك معرفة كافية حول كيفية حماية خصوصية معلوماتك في عصر الذكاء الاصطناعي؟							
هل تعتقد أن هناك حاجة إلى تعزيز التوعية حول الأمن الرقمي وحماية الخصوصية في النظام التعليمي؟							
الثقة والاعتماد							
هل تعتقد أن يجب أن يكون هناك مزيد من الشفافية من قبل الشركات التي تستخدم التكنولوجيا الذكية لجمع ومعالجة المعلومات الشخصية؟							
هل تعتقد أن الحكومات يجب أن تلعب دورًا أكبر في تنظيم استخدام التكنولوجيا الذكية وحماية خصوصية المواطنين؟							