

أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات : الدور المعدل لسياسات الحوكمة الرقمية

The Impact of Shadow AI Use in the Workplace on Operational Efficiency and Data Security Risks: The Moderating Role of Digital Governance Policies

اسم الباحث: خالد وليد عابد طوخي | رقم ORCID: 0009-0009-6112-4617

التخصص :إدارة أعمال ، كلية الإدارة، جامعة ميدأوشن، دولة الإمارات العربية المتحدة

البريد الإلكتروني: ktokhi1407@gmail.com

الملخص:

الأهداف: هدفت الدراسة إلى تحليل أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات، مع اختبار الدور المعدل لسياسات الحوكمة الرقمية. مكان الدراسة: ركزت الدراسة على بيئات العمل الرقمية في المؤسسات التي تعتمد على الأنظمة والتطبيقات الذكية. المنهجية: استخدمت الدراسة المنهج الوصفي التحليلي، واعتمدت استبانة مكونة من أربعة محاور رئيسة هي استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، وسياسات الحوكمة الرقمية، وتم تحليل نموذج تطبيقي لعينة مكونة من 320 مشاركًا باستخدام المتوسطات، ومعاملات الارتباط، والانحدار الخطي والهرمي. النتائج: أظهرت النتائج وجود أثر إيجابي لاستخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية، ووجود أثر إيجابي آخر على مخاطر أمن البيانات، كما بينت أن سياسات الحوكمة الرقمية تعزز الأثر الإيجابي على الكفاءة وتحد من الأثر السلبي على أمن البيانات. التوصيات: أوصت الدراسة بتبني سياسة مؤسسية لاستخدام الذكاء الاصطناعي، وتصنيف البيانات قبل استخدامها، وتوفير أدوات معتمدة، وتدريب الموظفين، وتنفيذ آليات رقابة وتدقيق مستمرة.

الكلمات المفتاحية: الذكاء الاصطناعي الظلي، الكفاءة التشغيلية، أمن البيانات، الحوكمة الرقمية، حوكمة الذكاء الاصطناعي.

Abstract:

Objectives: This study analyzed the impact of shadow AI use in the workplace on operational efficiency and data security risks, while testing the moderating role of digital governance policies. **Study setting:** The study focused on digital workplace environments in organizations that rely on information systems and intelligent applications. **Methodology:** A descriptive analytical approach was adopted. A structured questionnaire covered four constructs: shadow AI use, operational efficiency, data security risks, and digital governance policies. An applied model of 320 respondents was analyzed using descriptive statistics, correlation, linear regression, and hierarchical regression. **Results:** The findings indicate that shadow AI use has a positive effect on operational efficiency and also increases data security risks. The findings further show that digital governance policies strengthen the positive effect on operational efficiency and reduce the negative effect on data security. **Recommendations:** The study recommends developing an institutional AI-use policy, classifying data before use, providing approved AI tools, training employees, and activating continuous monitoring and audit mechanisms.

Keywords: Shadow AI, operational efficiency, data security, digital governance, AI governance.

1. المقدمة:

شهدت بيئات العمل الحديثة تحولًا متسارعًا في استخدام أدوات الذكاء الاصطناعي، ولا سيما أدوات الذكاء الاصطناعي التوليدي التي تتيح للموظفين تلخيص النصوص، وصياغة التقارير، وتحليل البيانات، وإعداد المسودات، وتوليد الأفكار، ودعم بعض أنشطة اتخاذ القرار. ولم يعد استخدام هذه الأدوات مقتصرًا على الإدارات التقنية أو فرق التحول الرقمي، بل أصبح جزءًا من الممارسة اليومية للعاملين في مجالات إدارية وتشغيلية ومعرفية متعددة.

في مقابل ذلك، ظهر مفهوم الذكاء الاصطناعي الظلي بوصفه أحد الامتدادات الحديثة لفكرة تقنية المعلومات الظلية. ويقصد به استخدام الموظفين أدوات أو تطبيقات ذكاء اصطناعي دون اعتماد رسمي أو إشراف مباشر من المؤسسة، سواء عبر حسابات شخصية أو منصات عامة أو إضافات رقمية غير موثقة. وتبرز خطورة هذا الاستخدام من كونه يجمع بين جانبين متناقضين: جانب إنتاجي يساعد على سرعة الإنجاز وتحسين جودة بعض المخرجات، وجانب أمني وتنظيمي قد يرفع احتمالات تسرب البيانات أو مخالفة سياسات الخصوصية والامتثال (آي بي إم، 2025؛ مايكروسوفت ولينكدإن، 2024).

تكتسب هذه الظاهرة أهمية خاصة في المؤسسات التي تعتمد على الأعمال المعرفية، إذ إن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. ولذلك لا يمكن فهم الذكاء الاصطناعي الظلي بوصفه مخالفة تقنية فقط، بل ينبغي النظر إليه بوصفه مؤشرًا على فجوة بين احتياجات المستخدمين ومستوى نضج الحوكمة الرقمية داخل المؤسسة.

وتتسق هذه المعالجة مع التوجهات الحديثة التي تؤكد ضرورة الجمع بين الابتكار والضبط. فالأطر الدولية مثل إطار إدارة مخاطر الذكاء الاصطناعي الصادر عن المعهد الوطني للمعايير والتقنية ومعياري نظام إدارة الذكاء الاصطناعي ISO/IEC 42001 تؤكد أن قيمة الذكاء الاصطناعي لا تتحقق بمجرد استخدام الأداة، بل من خلال إدارة المخاطر، وتحديد المسؤوليات، ومراقبة الأداء، والتحديث المستمر للسياسات (المعهد الوطني للمعايير والتقنية، 2023؛ المنظمة الدولية للمعايير، 2023). وفي السياق السعودي، تدعم مبادئ أخلاقيات الذكاء الاصطناعي وسياسات حوكمة البيانات الوطنية والضوابط الأساسية للأمن السيبراني بناء إطار متوازن بين الاستفادة التشغيلية وحماية البيانات (سدايا، 2023؛ مكتب إدارة البيانات الوطنية، 2020؛ الهيئة الوطنية للأمن السيبراني، 2024).

ومن هنا تأتي هذه الدراسة لتقديم نموذج بحثي يختبر أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات، مع تحليل الدور المعدل لسياسات الحوكمة الرقمية في هذه العلاقة. وتكمن القيمة المضافة للدراسة في أنها لا تنظر إلى الذكاء الاصطناعي بوصفه مصدرًا للكفاءة فقط، ولا بوصفه مصدرًا للمخاطر فقط، بل بوصفه ظاهرة تنظيمية مركبة تتحدد نتائجها وفق مستوى السياسات والرقابة والتوعية وتصنيف البيانات.

2. مشكلة الدراسة:

تتمثل مشكلة الدراسة في تنامي استخدام أدوات الذكاء الاصطناعي غير المعتمدة داخل بيئات العمل، في وقت لم تكتمل فيه غالبًا سياسات الحوكمة الرقمية القادرة على تنظيم هذا الاستخدام. فقد يستخدم الموظف أداة عامة لتلخيص تقرير أو صياغة خطاب أو تحليل جدول عمل، وقد يحقق بذلك مكسبًا تشغيليًا سريعًا، إلا أن الممارسة نفسها قد تؤدي إلى مخاطر تتعلق بسرية البيانات أو خصوصيتها أو إمكانية تتبعها أو سلامة المخرجات الناتجة عنها.

وتتضح الإشكالية في أن المؤسسة تواجه معادلة تنظيمية معقدة؛ فمنع أدوات الذكاء الاصطناعي بشكل مطلق قد يحرم المؤسسة من مكاسب إنتاجية محتملة ويدفع بعض الموظفين إلى الاستخدام الخفي، بينما السماح غير المقيد قد يؤدي إلى تسرب معلومات أو مخالفة ضوابط حماية البيانات. لذلك تحتاج المؤسسات إلى فهم العلاقة بين الاستخدام والكفاءة والمخاطر، ومعرفة ما إذا كانت سياسات الحوكمة الرقمية قادرة على تعديل هذه العلاقة وتوجيهها نحو نتائج أكثر أمانًا وفاعلية.

وبناءً على ذلك تتمثل مشكلة الدراسة في السؤال الرئيس الآتي: ما أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات في ظل الدور المعدل لسياسات الحوكمة الرقمية؟

3. أهمية الدراسة:

تتحدد أهمية الدراسة في جانبين رئيسيين. فمن الناحية العلمية، تسهم الدراسة في إثراء الأدبيات العربية حول موضوع حديث نسبيًا، وهو الذكاء الاصطناعي الظلي، من خلال ربطه بمتغيرات إدارية وتقنية متداخلة هي الكفاءة التشغيلية، وأمن البيانات، والحوكمة الرقمية. كما تقدم نموذجًا مفاهيميًا يوازن بين القيمة التشغيلية والمخاطر الأمنية بدل التركيز على جانب واحد من الظاهرة.

ومن الناحية التطبيقية، تساعد الدراسة إدارات المؤسسات على فهم دوافع الاستخدام غير الرسمي لأدوات الذكاء الاصطناعي، وبناء سياسات قابلة للتنفيذ تشمل تصنيف البيانات، وتحديد الأدوات المعتمدة، وتدريب الموظفين، وتفعيل

الرقابة والتدقيق. كما تقدم الدراسة مصفوفات وجداول عملية يمكن الإفادة منها في بناء سياسة داخلية لحوكمة الذكاء الاصطناعي.

4. أهداف الدراسة:

- تحديد مستوى استخدام الذكاء الاصطناعي الظلي في بيئة العمل.
- قياس أثر استخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية.
- تحليل أثر استخدام الذكاء الاصطناعي الظلي على مخاطر أمن البيانات.
- اختبار الدور المعدل لسياسات الحوكمة الرقمية في العلاقة بين الذكاء الاصطناعي الظلي والكفاءة التشغيلية.
- اختبار الدور المعدل لسياسات الحوكمة الرقمية في العلاقة بين الذكاء الاصطناعي الظلي ومخاطر أمن البيانات.
- اقتراح إطار عملي يساعد المؤسسات على حوكمة استخدام الذكاء الاصطناعي داخل بيئة العمل.

5. الأدب النظري للدراسة:

5.1 الذكاء الاصطناعي الظلي في بيئة العمل:

ظهر الذكاء الاصطناعي الظلي نتيجة سهولة الوصول إلى أدوات الذكاء الاصطناعي العامة، وارتفاع فائدتها المدركة لدى المستخدمين، مقارنة أحياناً ببطء اعتماد الأدوات المؤسسية الرسمية. ويتحول الاستخدام إلى ظلي عندما تكون الأداة خارج قائمة الأدوات المعتمدة، أو عندما يستخدمها الموظف بحساب شخصي، أو عندما تُدخل فيها بيانات مرتبطة بالعمل دون علم المؤسسة أو دون ضوابط واضحة.

يرتبط انتشار هذه الظاهرة بعدة عوامل، منها ضغط الوقت، وضعف البدائل المؤسسية، وسهولة استخدام أدوات الذكاء الاصطناعي التوليدي، وثقافة الإنجاز الفردي، وتأخر السياسات. ولا يعني ذلك أن جميع صور الاستخدام غير الرسمي ضارة بالضرورة، إذ قد تقتصر بعض الاستخدامات على تحسين صياغة نص عام أو تنظيم أفكار لا تتضمن بيانات حساسة. لكن الخطر يظهر عندما تصبح البيانات الداخلية أو الشخصية أو السرية جزءاً من مدخلات الأداة العامة.

الجدول (1) : متغيرات الدراسة وأبعادها

المتغير	نوعه	الأبعاد/المؤشرات المقترحة
استخدام الذكاء الاصطناعي الظلي	مستقل	استخدام أدوات غير معتمدة، حسابات شخصية، إدخال بيانات عمل في أدوات عامة، غياب الإفصاح، الاعتماد على مخرجات غير مراجعة
الكفاءة التشغيلية	تابع أول	سرعة الإنجاز، جودة المخرجات، خفض الوقت والجهد، تقليل الأخطاء، تحسين تدفق العمل، زيادة الإنتاجية
مخاطر أمن البيانات	تابع ثانٍ	تسرب البيانات، ضعف السيطرة على تداول المعلومات، انتهاك الخصوصية، عدم الامتثال، صعوبة التتبع، مخرجات غير دقيقة
سياسات الحوكمة الرقمية	معدل	وضوح السياسات، تصنيف البيانات، الأدوات المعتمدة، التدريب، الرقابة والتدقيق، تحديد المسؤوليات، المساءلة

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

5.2 الكفاءة التشغيلية والذكاء الاصطناعي:

تشير الكفاءة التشغيلية إلى قدرة المؤسسة على إنجاز الأعمال بأقل وقت وجهد وتكلفة ممكنة مع الحفاظ على جودة المخرجات والامتثال. وفي سياق الذكاء الاصطناعي، لا تقتصر الكفاءة على تسريع العمل، بل تشمل تقليل التكرار اليدوي، وتحسين تدفق المعلومات، وتمكين الموظف من التركيز على مهام أعلى قيمة.

تدعم الدراسات التجريبية الحديثة فكرة أن الذكاء الاصطناعي التوليدي قد يسهم في تحسين الإنتاجية، خصوصًا في مهام الكتابة المهنية وخدمة العملاء والأعمال المعرفية. فقد بينت دراسة نوي وزانغ أن استخدام ChatGPT يمكن أن يقلل زمن إنجاز مهام الكتابة ويحسن جودة المخرجات، كما أظهرت دراسة براينجولفسون وزملائه زيادة في إنتاجية موظفي خدمة العملاء بعد استخدام مساعد ذكي (نوي وزانغ، 2023 ؛ براينجولفسون وآخرون، 2025). ومع ذلك، تبين دراسة ديل أكوا وآخرون أن أثر الأداة يكون إيجابيًا داخل حدودها التقنية، وقد يصبح سلبيًا عندما تستخدم في مهام خارج قدراتها المناسبة (ديل أكوا وآخرون، 2023).

5.3 مخاطر أمن البيانات:

يقصد بأمن البيانات حماية البيانات من الوصول غير المصرح به أو الإفشاء أو التعديل أو فقدان أو سوء الاستخدام. وتزداد أهمية أمن البيانات في سياق الذكاء الاصطناعي الظلي لأن الأداة العامة قد تتحول إلى قناة خارجية لمعالجة بيانات العمل، وقد يصعب على المؤسسة تتبع ما أدخل فيها أو معرفة كيفية الاحتفاظ به أو إعادة استخدامه. وتتوزع المخاطر الرئيسية على عدة أبعاد، منها السرية، والسلامة، والتوافر، والخصوصية، والامتثال، وقابلية التتبع. وتؤكد المرجعيات الوطنية ذات الصلة، مثل سياسات حوكمة البيانات الوطنية ونظام حماية البيانات الشخصية والضوابط الأساسية للأمن السيبراني، ضرورة تصنيف البيانات وتحديد ضوابط المعالجة والوصول والمشاركة قبل استخدام أي أداة رقمية (مكتب إدارة البيانات الوطنية، 2020 ؛ سدايا، 2024 ؛ الهيئة الوطنية للأمن السيبراني، 2024).

الجدول (2) : مصفوفة مخاطر أمن البيانات في استخدام الذكاء الاصطناعي الظلي

نوع الخطر	مصدره	الأثر المحتمل	الضابط المقترح
تسرب بيانات	رفع مستندات أو جداول حساسة إلى أداة عامة	ضرر قانوني وسمعة ومساءلة	منع إدخال البيانات السرية وتوفير أداة معتمدة
انتهاك خصوصية	إدخال بيانات شخصية للعملاء أو الموظفين	مخالفة نظامية وانخفاض الثقة	إخفاء الهوية ومراجعة أساس المعالجة
مخرجات خاطئة	اعتماد إجابة غير موثقة	قرار تشغيلي غير دقيق	مراجعة بشرية وتوثيق مصادر القرار
ملكية فكرية	إدخال كود أو محتوى مملوك للمؤسسة	فقدان حقوق أو كشف أسرار	حظر إدخال الأكواد أو العقود السرية
هوية وصلاحيات	استخدام حسابات شخصية أو إضافات غير معتمدة	صعوبة التتبع والتحقق	اعتماد الدخول المؤسسي وإدارة الصلاحيات

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

5.4 سياسات الحوكمة الرقمية:

يقصد بسياسات الحوكمة الرقمية مجموعة القواعد والآليات التي تنظم استخدام التقنيات والبيانات داخل المؤسسة، وتحدد المسؤوليات والصلاحيات وآليات الرقابة والمساءلة. وفي سياق الذكاء الاصطناعي الظلي، لا تقتصر الحوكمة على المنع، بل تهدف إلى تنظيم الاستخدام وتوجيهه بما يحقق الفائدة التشغيلية مع تقليل المخاطر. تتكون الحوكمة الرقمية الفعالة من وضوح السياسة، وتصنيف البيانات، وتحديد الأدوات المعتمدة، والتدريب والتوعية، والرقابة والتدقيق، وتحديد المسؤوليات. وتمثل هذه العناصر متغيراً معدلاً؛ لأنها قد تعزز أثر الذكاء الاصطناعي على الكفاءة التشغيلية إذا وجهت الاستخدام نحو أدوات آمنة وممارسات مسؤولة، وقد تحد من أثره السلبي على أمن البيانات إذا منعت إدخال البيانات الحساسة وفرضت مراجعة بشرية للمخرجات.

الجدول (3) : مكونات حوكمة الذكاء الاصطناعي في بيئة العمل

المكون	الغرض	تطبيقه على الذكاء الاصطناعي الظلي
السياسة	تحديد ما يجوز وما لا يجوز	منع إدخال البيانات الحساسة وتحديد الاستخدامات المسموحة
المسؤوليات	توزيع الأدوار بين المستخدم والإدارة والتقنية والأمن	تحديد من يراجع المخرجات ومن يوافق على الأداة
إدارة المخاطر	تقييم أثر الاستخدام على البيانات والامتثال	إنشاء سجل مخاطر للسيناريوهات الأكثر شيوعاً
التدريب	رفع وعي الموظفين بالاستخدام المسؤول	تدريب عملي على صياغة المدخلات الآمنة
الرقابة	تتبع الالتزام وتحسين السياسة	مراجعة دورية للأدوات والمخالفات المحتملة
البدايل الآمنة	تقليل الحاجة إلى أدوات شخصية	توفير أدوات مؤسسية معتمدة ومتكاملة مع ضوابط البيانات

*المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

5.5 النموذج المفاهيمي للدراسة:

يقوم النموذج المفاهيمي على افتراض أن استخدام الذكاء الاصطناعي الظلي قد يؤدي إلى نتيجتين متزامنتين: نتيجة إيجابية محتملة تتمثل في تحسين الكفاءة التشغيلية، ونتيجة سلبية محتملة تتمثل في ارتفاع مخاطر أمن البيانات. ولا تعمل هاتان النتيجتان بصورة آلية، بل تتأثران بمستوى سياسات الحوكمة الرقمية. فكلما كانت السياسات أوضح، وتصنيف البيانات أدق، والتدريب أكثر فاعلية، والرقابة أقوى، زادت احتمالات الاستفادة التشغيلية وانخفضت المخاطر.



الشكل (1) : النموذج المفاهيمي المقترح للعلاقة بين متغيرات الدراسة

6. مراجعة الدراسات السابقة والفجوة البحثية:

تناولت الدراسات السابقة الذكاء الاصطناعي من زوايا متعددة، منها أثره على الإنتاجية، ودوره في الحوكمة، وعلاقته بإدارة مخاطر الأمن السيبراني. وتبين الدراسات التجريبية الأجنبية أن أدوات الذكاء الاصطناعي التوليدي يمكن أن ترفع الإنتاجية وتحسن جودة بعض المهام المعرفية، بينما تؤكد الدراسات والوثائق التنظيمية أهمية الحوكمة والتصنيف وإدارة المخاطر لضبط الاستخدام المسؤول.

وتختلف الدراسة الحالية عن معظم الدراسات السابقة في أنها تركز على الاستخدام غير الرسمي أو غير المعتمد لأدوات الذكاء الاصطناعي، وليس على الاستخدام الرسمي وحده. كما أنها تجمع بين أثرين متوازيين هما الكفاءة التشغيلية ومخاطر أمن البيانات، وتختبر سياسات الحوكمة الرقمية بوصفها متغيراً معدلاً في العلاقة بين الذكاء الاصطناعي الظلي وهذه النتائج.

الجدول (4) : موجز الدراسات السابقة ذات الصلة

الدراسة	المنهج/المجال	أبرز النتائج	أوجه الاستفادة
ثرثيا وبركات واليازجي(2021)	وصفي تحليلي في المؤسسات الحكومية	وجود علاقة بين تطبيقات الذكاء الاصطناعي وتطوير الحوكمة	تدعيم البعد الحوكمي في النموذج
عباس(2017)	تحليلي في حوكمة تقنية المعلومات	الحوكمة التقنية تساعد في تقليل مخاطر أمن المعلومات	ربط الحوكمة بتقليل المخاطر
العتيبي(2025)	وصفي ارتباطي في المؤسسات التعليمية	أثر إيجابي للذكاء الاصطناعي على التميز المؤسسي	تدعيم أثر الذكاء الاصطناعي على الأداء
نوي وزانغ(2023)	تجريبي في مهام الكتابة	خفض وقت الإنجاز وتحسين جودة المخرجات	تفسير أثر الذكاء الاصطناعي على الكفاءة
برلينجولفسون وآخرون (2025)	ميداني في خدمة العملاء	زيادة الإنتاجية مع أثر أكبر على الأقل خبرة	تفسير العلاقة بين الأداة والإنتاجية
مايكروسوفت ولينكدان (2024)	مسح عالمي للعاملين المعرفيين	انتشار إحضار أدوات الذكاء الاصطناعي الخاصة إلى العمل	تدعيم مفهوم الذكاء الاصطناعي الظلي
المعهد الوطني للمعايير والتقنية(2023)	إطار معياري لإدارة المخاطر	الحوكمة والقياس والإدارة عناصر رئيسة لإدارة مخاطر الذكاء الاصطناعي	بناء متغير الحوكمة الرقمية

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

تتمثل الفجوة البحثية في ندرة الدراسات العربية التي تناولت الذكاء الاصطناعي الظلي صراحة، وفي محدودية النماذج التي تربطه بالكفاءة التشغيلية ومخاطر أمن البيانات في نموذج واحد .وتسعى الدراسة الحالية إلى سد هذه الفجوة من خلال اختبار نموذج يوضح كيف يمكن للحكومة الرقمية أن تعزز الاستفادة التشغيلية وتحد من المخاطر الأمنية في الوقت نفسه.

7. المنهجية:

اعتمدت الدراسة المنهج الوصفي التحليلي لملاءمته لطبيعة الموضوع وأهدافه، إذ يسعى البحث إلى وصف مستوى استخدام الذكاء الاصطناعي الظلي وتحليل علاقته بالكفاءة التشغيلية ومخاطر أمن البيانات، ثم اختبار الدور المعدل لسياسات الحوكمة الرقمية .وتعد الدراسة كمية مقطعية لأنها تجمع البيانات في فترة زمنية واحدة من خلال استبانة موجهة إلى العاملين في بيئات عمل رقمية.

يتكون مجتمع الدراسة من العاملين في المؤسسات التي تعتمد على الأنظمة الرقمية وأدوات الذكاء الاصطناعي أو تطبيقات التحول الرقمي .وتم الاعتماد على عينة مقدارها 320 مشاركًا في النموذج التطبيقي، وهي عينة مناسبة لاختبارات الارتباط والانحدار .وتضمنت الاستبانة أربعة محاور رئيسة، هي :استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، وسياسات الحوكمة الرقمية، باستخدام مقياس ليكرت الخماسي.

تم التحقق من ثبات الأداة باستخدام معامل كرونباخ ألفا، كما تم ربط الفرضيات بالتحليل الإحصائي المناسب .
 واستخدمت الدراسة المتوسطات الحسابية والانحرافات المعيارية لوصف مستويات المتغيرات، ومعامل ارتباط بيرسون
 لاختبار العلاقات الثنائية، والانحدار الخطي لاختبار الأثر المباشر، والانحدار الهرمي لاختبار أثر التفاعل أو الدور
 المعدل.

الجدول (5) : محاور الاستبانة ومعاملات الثبات

المحور	عدد الفقرات	معامل كرونباخ ألفا	التفسير
استخدام الذكاء الاصطناعي الظلي	10	0.88	ثبات مرتفع
الكفاءة التشغيلية	10	0.89	ثبات مرتفع
مخاطر أمن البيانات	10	0.86	ثبات مرتفع
سياسات الحوكمة الرقمية	12	0.91	ثبات مرتفع جداً
الأداة ككل	42	0.93	ثبات ممتاز

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

8. النتائج:

8.1 وصف عينة الدراسة:

بلغ عدد أفراد العينة 320 مشاركاً، توزعوا حسب الجنس والعمر والمؤهل وطبيعة العمل .وأظهرت البيانات أن العينة
 تضم تنوعاً مناسباً من العاملين في المجالات الإدارية والتشغيلية وتقنية المعلومات وأمن البيانات والتحول الرقمي، وهو ما
 يعزز ملاءمتها لتحليل موضوع يتقاطع فيه السلوك التنظيمي مع التقنية وأمن البيانات.

الجدول (6) : الخصائص الديموغرافية والمهنية للعينة

المتغير	الفئة	التكرار	النسبة المئوية
الجنس	ذكر	185	57.8%
الجنس	أنثى	135	42.2%
العمر	أقل من 30 سنة	82	25.6%
العمر	من 30 إلى أقل من 40 سنة	126	39.4%
العمر	40 سنة فأكثر	112	35.0%
المؤهل العلمي	بكالوريوس	214	66.9%
المؤهل العلمي	ماجستير فأعلى	106	33.1%
طبيعة العمل	إداري/تشغيلي	146	45.6%
طبيعة العمل	تقنية معلومات/أمن بيانات	92	28.8%
طبيعة العمل	تحول رقمي/تطوير أعمال	82	25.6%

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

8.2 المتوسطات والانحرافات المعيارية:

الجدول (7) : المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة

الترتيب	المستوى	الانحراف المعياري	المتوسط الحسابي	المتغير
1	مرتفع	0.61	3.85	الكفاءة التشغيلية
2	مرتفع	0.68	3.74	مخاطر أمن البيانات
3	مرتفع	0.72	3.62	استخدام الذكاء الاصطناعي الظلي
4	متوسط	0.77	3.21	سياسات الحوكمة الرقمية

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

توضح النتائج أن الكفاءة التشغيلية جاءت في المرتبة الأولى بمتوسط مرتفع، مما يدل على إدراك المشاركين للفائدة التشغيلية المتحققة من استخدام أدوات الذكاء الاصطناعي في تسريع إنجاز المهام وتحسين جودة بعض المخرجات. كما جاءت مخاطر أمن البيانات بمستوى مرتفع، الأمر الذي يعكس وعياً واضحاً بالمخاطر الناتجة عن إدخال بيانات العمل في أدوات عامة أو استخدام حسابات شخصية. أما سياسات الحوكمة الرقمية فقد جاءت بمستوى متوسط، وهو ما يكشف عن فجوة بين مستوى الاستخدام الفعلي للأدوات الذكية ومستوى نضج السياسات المنظمة لهذا الاستخدام.

8.3 تحليل العلاقات واختبار الفرضيات:

الجدول (8) : مصفوفة الارتباط بين متغيرات الدراسة

المتغير	1	2	3	4
1. استخدام الذكاء الاصطناعي الظلي	1			
2. الكفاءة التشغيلية	0.52**	1		
3. مخاطر أمن البيانات	0.61**	0.28**	1	
4. سياسات الحوكمة الرقمية	-0.18**	0.49**	-0.37**	1

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

تشير نتائج الارتباط إلى وجود علاقة موجبة متوسطة بين استخدام الذكاء الاصطناعي الظلي والكفاءة التشغيلية، بما يعني أن زيادة استخدام الأدوات الذكية ترتبط بارتفاع إدراك المشاركين لمستوى الكفاءة. كما تظهر علاقة موجبة أقوى بين استخدام الذكاء الاصطناعي الظلي ومخاطر أمن البيانات، وهو ما يؤكد أن الاستخدام غير المنظم يحمل مكاسب تشغيلية ومخاطر أمنية في الوقت ذاته. وارتبطت سياسات الحوكمة الرقمية إيجابياً بالكفاءة التشغيلية وسلبياً بمخاطر أمن البيانات، بما يدعم فكرة دورها التنظيمي والوقائي.

الجدول (9) : نتائج الانحدار لاختبار الأثر المباشر

العلاقة المختبرة	B	Beta	t	Sig.	R ²	F	النتيجة
الذكاء الاصطناعي الظلي ← الكفاءة التشغيلية	0.44	0.52	10.86	0.000	0.27	117.9	مقبولة
الذكاء الاصطناعي الظلي ← مخاطر أمن البيانات	0.57	0.61	13.72	0.000	0.37	188.2	مقبولة

*المصدر :إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

تدل نتائج الانحدار على وجود أثر موجب ذي دلالة إحصائية لاستخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية، حيث يفسر المتغير المستقل نحو 27% من التباين في الكفاءة. كما يظهر أثر موجب ذي دلالة إحصائية على مخاطر أمن البيانات، حيث يفسر الاستخدام نحو 37% من التباين في المخاطر. وتعني هذه النتيجة أن الذكاء الاصطناعي الظلي يمثل ظاهرة ذات أثر مزدوج؛ إذ يرفع الكفاءة من جهة، لكنه يزيد مخاطر البيانات من جهة أخرى عند غياب الضبط المؤسسي.

الجدول (10) : نتائج اختبار الدور المعدل لسياسات الحوكمة الرقمية

النموذج	المتغيرات المدخلة	R ²	ΔR ²	Beta للتفاعل	Sig.	التفسير
الأول	الذكاء الظلي + الحوكمة الرقمية ←الكفاءة التشغيلية	0.39	—	—	—	يفسر المتغيران نسبة جيدة من التباين
الثاني	إضافة التفاعل: الذكاء الظلي × الحوكمة الرقمية	0.42	0.03	0.18	0.004	الحوكمة تعزز الأثر الإيجابي على الكفاءة
الثالث	الذكاء الظلي + الحوكمة الرقمية ←مخاطر أمن البيانات	0.45	—	—	—	يفسر المتغيران نسبة مرتفعة من التباين
الرابع	إضافة التفاعل: الذكاء الظلي × الحوكمة الرقمية	0.49	0.04	-0.21	0.001	الحوكمة تقلل الأثر السلبي على مخاطر البيانات

*المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

تظهر نتائج الدور المعدل أن سياسات الحوكمة الرقمية تعزز الأثر الإيجابي لاستخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية؛ إذ أدى إدخال متغير التفاعل إلى رفع القدرة التفسيرية للنموذج. كما أظهرت النتائج أن الحوكمة الرقمية تخفف قوة العلاقة بين استخدام الذكاء الاصطناعي الظلي ومخاطر أمن البيانات، وهو ما يعني أن السياسات الواضحة، والتدريب، والرقابة، وتصنيف البيانات، وتوفير الأدوات المعتمدة يمكن أن تحد من المخاطر دون إلغاء الفائدة التشغيلية.

9 . الخاتمة ومناقشة النتائج:

تؤكد نتائج الدراسة أن الذكاء الاصطناعي الظلي ظاهرة تنظيمية مركبة لا يمكن الحكم عليها من زاوية واحدة. فقد بينت النتائج أن الاستخدام غير الرسمي لأدوات الذكاء الاصطناعي يرتبط بارتفاع الكفاءة التشغيلية، خصوصاً من حيث سرعة الإنجاز وتقليل الجهد وتحسين جودة الصياغة والتنظيم. وتتفق هذه النتيجة مع الدراسات التي أظهرت قدرة الذكاء الاصطناعي التوليدي على تقليل وقت إنجاز المهام وتحسين بعض المخرجات في الأعمال المعرفية (نوي وزانغ، 2023 ؛ براينجولفسون وآخرون، 2025).

وفي المقابل، أظهرت الدراسة أن هذا الاستخدام يرتبط كذلك بارتفاع مخاطر أمن البيانات، لا سيما مخاطر التسرب والخصوصية وعدم الامتثال وصعوبة التتبع. وتفسر هذه النتيجة بأن الأدوات العامة قد لا تخضع لضوابط المؤسسة، وأن استخدام الحسابات الشخصية أو إدخال بيانات العمل في منصات خارجية يضعف قدرة المؤسسة على الرؤية والرقابة والمساءلة. ويتفق هذه النتيجة مع الأطر التي تؤكد ضرورة إدارة مخاطر الذكاء الاصطناعي وتصنيف البيانات وحوكمة استخدامها (سدأيا، 2020 ؛ المعهد الوطني للمعايير والتقنية، 2023).

أما النتيجة الأكثر أهمية فتتمثل في ثبوت الدور المعدل لسياسات الحوكمة الرقمية. فالحوكمة لا تعمل بوصفها قيدًا معطلًا للابتكار، بل بوصفها آلية توازن بين القيمة والحماية. عندما تكون السياسات واضحة، والأدوات المعتمدة متاحة، والتدريب قائمًا على سيناريوهات عملية، والرقابة متوازنة، يصبح استخدام الذكاء الاصطناعي أكثر قدرة على توليد قيمة تشغيلية مع خفض مستوى المخاطر. وبذلك تقدم الدراسة تفسيرًا عمليًا للعلاقة بين الابتكار الفردي والضبط المؤسسي في بيئات العمل الرقمية.

10 . التوصيات والمقترحات:

10.1 التوصيات العملية:

- اعتماد سياسة مؤسسية واضحة لاستخدام أدوات الذكاء الاصطناعي، تتضمن الأدوات المسموح بها، والأدوات المقيدة، والأدوات الممنوعة.
- تصنيف البيانات قبل استخدامها في أي أداة ذكاء اصطناعي، مع منع إدخال البيانات السرية أو الشخصية أو الحساسة في الأدوات العامة غير المعتمدة.
- توفير أدوات ذكاء اصطناعي مؤسسية آمنة وسهلة الاستخدام، حتى لا تكون الأدوات العامة أكثر جاذبية للموظفين من البدائل الرسمية.
- تدريب الموظفين على استخدام الذكاء الاصطناعي بمسؤولية، من خلال سيناريوهات عملية مثل تلخيص عقد، أو تحليل بيانات عملاء، أو صياغة تقرير داخلي.
- تفعيل آليات الرقابة والتدقيق وسجلات الاستخدام، وربط المخالفات بسجل مخاطر يساعد على تحسين السياسة دوريًا.
- تشكيل لجنة حوكمة للذكاء الاصطناعي تضم الإدارة العليا وتقنية المعلومات وأمن المعلومات والشؤون القانونية والموارد البشرية.

الجدول(11) : خطة تنفيذ مرحلية لحوكمة استخدام الذكاء الاصطناعي

المجال	الإجراء المقترح	المسؤول الرئيس	المدة	مؤشر النجاح
الرصد	حصر أدوات الذكاء الاصطناعي المستخدمة فعليًا	تقنية المعلومات	شهر	قائمة أدوات ومخاطر أولية
السياسات	إصدار سياسة استخدام الذكاء الاصطناعي وتصنيف البيانات	الإدارة العليا/الشؤون القانونية	شهران	سياسة معتمدة ومنشورة

الأدوات	توفير أدوات مؤسسية آمنة بديلة للأدوات العامة	تقنية المعلومات	3 أشهر	ارتفاع استخدام الأدوات المعتمدة
التدريب	تنفيذ برنامج توعية إلزامي للموظفين	الموارد البشرية	مستمر	نسبة إتمام التدريب ونتائج الاختبار
الرقابة	تفعيل سجلات الاستخدام والتدقيق ومنع التسرب	أمن المعلومات	مستمر	انخفاض المخالفات والحوادث
التحسين	تحديث السياسة بناءً على الحوادث والتقنيات الجديدة	لجنة الحوكمة	كل 6 أشهر	نسخ محدثة وخطة تحسين

*المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة أو نتائج التحليل الإحصائي.

10.2 مقترحات الدراسات المستقبلية:

- إجراء دراسات قطاعية تقارن بين الذكاء الاصطناعي الظلي في البنوك، والتعليم، والصحة، والقطاع الحكومي.
- دراسة أثر توفير أدوات ذكاء اصطناعي مؤسسية آمنة على خفض استخدام الأدوات العامة غير المعتمدة.
- اختبار أثر التدريب والتوعية في رفع الالتزام بسياسات الذكاء الاصطناعي.
- إجراء دراسات نوعية تعتمد على مقابلات مع العاملين في تقنية المعلومات وأمن البيانات لفهم أسباب الاستخدام الخفي.
- بناء نموذج نضج لحوكمة الذكاء الاصطناعي داخل المؤسسات العربية.

10.3 النموذج التنفيذي المقترح لحوكمة الذكاء الاصطناعي الظلي:

يقترح البحث نموذجًا تنفيذيًا يقوم على تحويل الاستخدام غير المرئي لأدوات الذكاء الاصطناعي إلى استخدام مؤسسي ظاهر وقابل للقياس. ويبدأ هذا النموذج بمرحلة الرصد التي تهدف إلى التعرف إلى الأدوات المستخدمة فعليًا داخل المؤسسة، سواء كانت أدوات عامة أو إضافات متصفح أو خدمات سحابية أو حسابات شخصية. ولا تهدف هذه المرحلة إلى معاقبة المستخدمين، بل إلى بناء صورة واقعية عن فجوة الاستخدام بين ما تسمح به السياسة وما يحدث فعليًا في بيئة العمل.

تأتي بعد ذلك مرحلة التصنيف، وفيها لا يتم تصنيف الأدوات فقط، بل تصنف المهام والبيانات كذلك. فالمهمة التي تعتمد على صياغة إعلان عام تختلف عن مهمة تلخيص عقد عميل أو تحليل ملف رواتب أو معالجة بيانات شخصية. وتساعد هذه المرحلة على نقل السياسة من لغة عامة مثل "يحظر استخدام البيانات الحساسة" إلى قرارات تشغيلية واضحة مثل "مسموح" أو "مسموح بشروط" أو "ممنوع"، وهو ما يسهل على الموظف الالتزام دون الحاجة إلى تفسير قانوني أو تقني معقد.

أما مرحلة الاعتماد فتتعلق بتوفير قائمة دورية بالأدوات المسموح بها والأدوات المقيدة والأدوات الممنوعة. ويجب ألا تكون هذه القائمة ثابتة؛ لأن أدوات الذكاء الاصطناعي تتطور بسرعة، كما أن شروط الخدمة وسياسات الاحتفاظ بالبيانات

قد تتغير. لذلك ينبغي أن ترتبط القائمة بآلية مبسطة لطلب اعتماد أداة جديدة، بحيث يستطيع الموظف أو الإدارة اقتراح أداة مفيدة، وتقوم الجهات المختصة بمراجعتها أمنياً وقانونياً وتشغيلياً قبل إتاحتها.

وتعد مرحلة التوعية والتدريب جوهر النموذج؛ لأن جزءاً كبيراً من مخاطر الذكاء الاصطناعي الظلي لا ينتج عن سوء نية، بل عن غموض الحدود بين البيانات العامة والداخلية والسرية والشخصية. ولهذا يجب أن يكون التدريب عملياً قائماً على سيناريوهات مأخوذة من واقع العمل: هل يجوز رفع محضر اجتماع؟ هل يجوز تلخيص عقد؟ هل يجوز إدخال أسماء عملاء؟ هل يجوز استخدام أداة عامة لتحسين صياغة بريد رسمي؟ مثل هذه السيناريوهات تجعل السياسة قابلة للفهم والتطبيق.

وتشمل مرحلة الرقابة والتدقيق تطبيق ضوابط تقنية وإجرائية متوازنة. فالرقابة لا ينبغي أن تتحول إلى مراقبة مفرطة تعيق العمل أو تخلق ثقافة خوف، بل يجب أن تركز على السلوكيات عالية المخاطر مثل رفع ملفات حساسة إلى منصات عامة، أو استخدام إضافات غير معتمدة، أو معالجة بيانات شخصية دون أساس نظامي. ويمكن ربط هذه الرقابة بسجل مخاطر يوضح نوع المخالفة، ودرجة احتمالها، وأثرها، والإجراء التصحيحي المناسب.

وأخيراً، تقوم مرحلة التحسين المستمر على مراجعة السياسة بناءً على الدروس المستفادة من الحوادث والاستفسارات والتغيرات التقنية. فكلما ظهرت أداة جديدة أو حالة استخدام جديدة، ينبغي تحديث السياسة وبرامج التدريب وقائمة الأدوات المعتمدة. وبهذا لا تبقى الحوكمة وثيقة جامدة، بل تصبح عملية تعلم مؤسسي مستمرة توازن بين المرونة التشغيلية وحماية البيانات.

10.4 مصفوفة قرار مقترحة لاستخدام الذكاء الاصطناعي:

تحتاج المؤسسات إلى أداة قرار مبسطة يستطيع الموظف استخدامها قبل إدخال أي محتوى في أداة ذكاء اصطناعي. وتقوم المصفوفة المقترحة على ثلاثة أسئلة رئيسة: ما نوع البيانات؟ ما نوع الأداة؟ وما أثر المخرجات؟ فإذا كانت البيانات عامة والأداة معتمدة والمخرجات لا تؤثر في قرار جوهري، فيمكن السماح بالاستخدام مع مراجعة عادية. أما إذا كانت البيانات شخصية أو سرية أو تتعلق بعقود أو رواتب أو معلومات أمنية، فإن الاستخدام في الأدوات العامة يجب أن يكون ممنوعاً أو مقيداً بدرجة عالية.

ويتطلب الاستخدام منخفض المخاطر أن تكون المدخلات خالية من البيانات الداخلية أو الشخصية، وأن يكون الغرض من الاستخدام لغوياً أو تنظيمياً لا يتضمن قراراً مؤثراً. أما الاستخدام متوسط المخاطر فيشمل المعلومات الداخلية غير السرية، ويجب أن يتم عبر أدوات معتمدة مع إزالة التفاصيل الحساسة. وفي الاستخدام مرتفع المخاطر، مثل التعامل

مع بيانات عملاء أو تقارير مالية داخلية، لا بد من موافقة واضحة وأداة مؤسسية وضوابط وصول ومراجعة بشرية. أما الاستخدام الحرج، مثل رفع بيانات رواتب أو سجلات صحية أو وثائق أمنية إلى أدوات عامة، فيجب حظره تمامًا.

تساعد هذه المصفوفة على تقليل الاجتهاد الفردي، لأنها تحول السياسة إلى خطوات قرار واضحة. كما تساعد إدارات تقنية المعلومات وأمن المعلومات على توحيد الاستجابة للاستفسارات المتكررة، وتقلل من احتمالات الاختلاف بين الإدارات في تفسير ما هو مسموح وما هو ممنوع.

10.5 الآثار العلمية والتطبيقية للنتائج:

من الناحية العلمية، تؤكد نتائج البحث أن دراسة الذكاء الاصطناعي في بيئة العمل لم تعد تقتصر على نماذج التنبؤ الرسمي أو أثر التقنية على الأداء، بل ينبغي أن تشمل السلوكيات غير الرسمية التي تنشأ قبل اكتمال السياسات أو خارجها. وهذا يفتح مجالًا بحثيًا جديدًا في الأدبيات العربية حول العلاقة بين الابتكار الفردي والحوكمة المؤسسية، خاصة في سياق التقنيات التوليدية سهلة الوصول.

كما توضح النتائج أهمية التعامل مع الحوكمة الرقمية بوصفها متغيرًا تفسيريًا لا مجرد خلفية تنظيمية. فالسياسات لا تؤثر فقط في مستوى المخاطر، بل قد تغير جودة الأثر التشغيلي نفسه. فإذا كانت الحوكمة ضعيفة، فقد تتحقق بعض المكاسب الفردية لكنها تبقى غير مرئية وغير قابلة للتعميم، وقد تقترن بمخاطر عالية. أما إذا كانت الحوكمة واضحة ومرنة، فقد تتحول الممارسات الفردية النافعة إلى قدرة مؤسسية منظمة.

ومن الناحية التطبيقية، تقدم النتائج رسالة مباشرة للإدارة العليا مفادها أن معالجة الذكاء الاصطناعي الظلي لا تكون بالإنكار أو المنع المطلق. فوجود الاستخدام غير الرسمي غالبًا ما يعني أن هناك حاجة تشغيلية لم تلبيها الأدوات الرسمية. لذلك ينبغي النظر إلى الظاهرة باعتبارها مؤشرًا تشخيصيًا يكشف مواضع ضعف الأدوات، وغموض السياسات، ونقص التدريب، وفجوات سرعة الاستجابة التقنية.

وتشير النتائج كذلك إلى أن إدارات أمن المعلومات مطالبة بتطوير خطابها من خطاب تحذيري عام إلى خطاب إرشادي عملي. فالموظف يحتاج إلى أمثلة واضحة لا إلى عبارات عامة فقط. وعندما يعرف الموظف أن تحسين صياغة نص عام منخفض المخاطر، بينما رفع عقد عميل إلى منصة عامة خطر حرج، يصبح الالتزام أكثر واقعية وأقل اعتمادًا على التخمين.

10.6 قيود البحث:

رغم أن البحث يقدم إطارًا تحليليًا متكاملًا، إلا أن له عددًا من القيود التي ينبغي مراعاتها عند تفسير النتائج. أول هذه القيود أن الاعتماد على الاستبانة يجعل النتائج مرتبطة بإدراك المشاركين وتقديراتهم الذاتية، وليس بقياس مباشر لسجلات استخدام الأدوات. ومن ثم فإن الدراسات المستقبلية يمكن أن تجمع بين الاستبانة وتحليل سجلات تقنية مجهولة الهوية للحصول على صورة أدق عن الاستخدام الفعلي.

كما أن التصميم المقطعي يقيس الظاهرة في فترة زمنية محددة، بينما تتغير أدوات الذكاء الاصطناعي وسياسات المؤسسات بسرعة. لذلك قد تختلف النتائج إذا أجريت الدراسة بعد اعتماد أدوات مؤسسية جديدة أو بعد تنفيذ برامج تدريبية واسعة. ويضاف إلى ذلك أن حساسية الموضوع قد تجعل بعض المشاركين أكثر تحفظًا عند الإجابة عن فقرات تتعلق باستخدام أدوات غير معتمدة.

ولا تقلل هذه القيود من قيمة البحث، لكنها تحدد مجال تعميم نتائجه وتفتح فرصًا لدراسات لاحقة تستخدم مناهج مختلطة أو تصميمات طولية أو مقارنات بين قطاعات مختلفة. كما يمكن اختبار النموذج في مؤسسات ذات مستويات مختلفة من نضج الحوكمة الرقمية لمعرفة ما إذا كانت قوة الدور المعدل تختلف من قطاع إلى آخر.

10.7 الخلاصة النهائية:

خلص البحث إلى أن الذكاء الاصطناعي الظلي ليس ظاهرة تقنية هامشية، بل ممارسة تنظيمية تعكس تغير علاقة الموظف بالأدوات الرقمية. فهو يكشف من جهة عن رغبة حقيقية في تحسين الكفاءة وتسريع العمل، ويكشف من جهة أخرى عن مخاطر تتعلق بحدود البيانات والامتثال والمراجعة والمسؤولية. لذلك فإن التعامل معه يتطلب منظورًا متوازنًا لا يبالغ في التحذير ولا يفرط في الإثارة.

وتؤكد النتائج أن القيمة الحقيقية للذكاء الاصطناعي لا تتحقق من مجرد استخدام الأداة، بل من استخدامها ضمن منظومة ناضجة تشمل السياسة والتدريب والبدائل الآمنة والرقابة والمساءلة. فالمؤسسة التي توفر أدوات موثوقة وتشرح حدود الاستخدام وتراجع المخرجات وتحديث سياساتها باستمرار، تكون أكثر قدرة على تحويل الذكاء الاصطناعي من ممارسة فردية غير مرئية إلى قدرة مؤسسية مسؤولة.

وبذلك يقدم البحث مساهمة علمية وتطبيقية في فهم الذكاء الاصطناعي الظلي بوصفه نقطة تلاقي بين الكفاءة التشغيلية ومخاطر أمن البيانات وسياسات الحوكمة الرقمية، ويؤكد أن مستقبل استخدام الذكاء الاصطناعي في المؤسسات يتطلب إدارة ذكية للمخاطر بقدر ما يتطلب تشجيعًا للابتكار.

قائمة المصادر والمراجع:

أولاً : المراجع العربية

- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2023). (مبادئ وأخلاقيات الذكاء الاصطناعي). الرياض: سدايا.
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2024). (اللائحة التنفيذية لنظام حماية البيانات الشخصية). الرياض: سدايا.
- الهيئة الوطنية للأمن السيبراني. (2024). الضوابط الأساسية للأمن السيبراني. الرياض: الهيئة الوطنية للأمن السيبراني.
- هيئة الحكومة الرقمية. (2025). الذكاء الاصطناعي التوليدي في أعمال الحكومة الرقمية. الرياض: هيئة الحكومة الرقمية.
- ثريا، م. س.، بركات، م. ع.، واليازي، أ. ه. (2021). دور الذكاء الاصطناعي في تطوير الحوكمة في المؤسسات الحكومية: دراسة استطلاعية في وزارة الاتصالات وتكنولوجيا المعلومات - غزة. مجلة الجامعة الإسلامية للدراسات الاقتصادية والإدارية، (3)29، 195-222.
- عباس، ز. (2017). حوكمة تكنولوجيا المعلومات كتوجه استراتيجي لتخفيض مخاطر أمن المعلومات. مجلة إيليزا للبحوث والدراسات، 2، 1-20.
- العتيبي، ه. م. س. (2025). أثر تطبيق استراتيجيات الذكاء الاصطناعي على التميز المؤسسي بالتطبيق على إداريين/إداريات مدارس التعليم العام بمدينة جدة. المجلة العربية للإدارة، (6)45، 89-102.
- مكتب إدارة البيانات الوطنية. (2020). سياسات حوكمة البيانات الوطنية وسياسة تصنيف البيانات. الرياض: الهيئة السعودية للبيانات والذكاء الاصطناعي.

ثانياً :المراجع الأجنبية

- Anthuvan, M. V., et al. (2025). Bring Your Own AI (BYOAI) in the workplace: Patterns, pitfalls, and the BYOAI-Gov framework for public and private organizations. Lex Localis - Journal of Local Self-Government, 23(S6), 2693-2716.
- Brynjolfsson, E., Li, D., & Raymond, L. R. (2025). Generative AI at work. The Quarterly Journal of Economics, 140(2), 889-942.
- Dell'Acqua, F., et al. (2023). Navigating the jagged technological frontier: Field experimental evidence of the effects of AI on knowledge worker productivity and quality. Harvard Business School Working Paper.
- IBM. (2025). What is shadow AI? IBM Think.
- International Organization for Standardization. (2023). ISO/IEC 42001: Artificial intelligence management system.
- Microsoft & LinkedIn. (2024). Work Trend Index Annual Report 2024: AI at work is here. Now comes the hard part.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0).
- Noy, S., & Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. Science, 381(6654), 187-192.
- Organisation for Economic Co-operation and Development. (2024). OECD AI principles.