

بسم الله الرحمن الرحيم



جامعة ميداو شن

كلية الإدارة

أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية
ومخاطر أمن البيانات

(الدور المعدّل 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)

إعداد الطالب /

خالد وليد عابد طوخي

الرقم الجامعي /

252000924

إشراف :

د. الفيصّل عبد الحميد محمد حسن

العام الجامعي :

1447هـ - 2026م

المحتويات

6	الإهداء :
8	الشكر والتقدير
9	المستخلص:
10	Abstract:
11	قائمة الجداول :
12	الفصل الأول: الإطار العام للدراسة
12	1.1 خلفية الدراسة :
13	1.2 الذكاء الاصطناعي الظلي بوصفه ظاهرة تنظيمية :
14	1.3 مشكلة الدراسة :
15	1.4 أسئلة الدراسة :
16	1.5 أهداف الدراسة:
17	1.6 أهمية الدراسة العلمية:
18	1.7 أهمية الدراسة التطبيقية:
19	1.8 حدود الدراسة:
20	1.9 متغيرات الدراسة:
21	1.10 فرضيات الدراسة:
21	1.11 مصطلحات الدراسة:
22	1.12 منطلقات الدراسة النظرية:
26	الفصل الثاني : الإطار النظري والدراسات السابقة
26	أولاً : الاطار النظري :
26	المبحث الأول: الذكاء الاصطناعي والذكاء الاصطناعي الظلي
26	2.1.1 مفهوم الذكاء الاصطناعي وتطوره في بيئات الأعمال:
27	2.1.2 الذكاء الاصطناعي التوليدي وطبيعة الاستخدام اليومي:
28	2.1.3 من الذكاء الاصطناعي الرسمي إلى الذكاء الاصطناعي الظلي:
29	2.1.4 أسباب انتشار الذكاء الاصطناعي الظلي:

- 2.1.5 أنماط استخدام الذكاء الاصطناعي الظلي في العمل: 30.....
- 2.1.6 المكاسب والقيود في الاستخدام غير الرسمي: 31.....
- المبحث الثاني: الكفاءة التشغيلية في سياق الذكاء الاصطناعي 32.....
- 2.2.1 مفهوم الكفاءة التشغيلية: 32.....
- 2.2.2 الذكاء الاصطناعي وأتمتة العمليات الروتينية: 33.....
- 2.2.3 الذكاء الاصطناعي ودعم القرار التشغيلي: 34.....
- 2.2.4 حدود الكفاءة التشغيلية الناتجة عن الذكاء الاصطناعي: 34.....
- المبحث الثالث: مخاطر أمن البيانات المرتبطة بالذكاء الاصطناعي الظلي 35.....
- 2.3.1 مفهوم أمن البيانات وأبعاده: 35.....
- 2.3.2 حساسية البيانات في بيئة العمل: 36.....
- 2.3.3 مخاطر إدخال البيانات في أدوات عامة: 37.....
- 2.3.4 مخاطر الخصوصية وحماية البيانات الشخصية: 37.....
- 2.3.5 مخاطر عدم الامتثال التنظيمي: 38.....
- المبحث الرابع: سياسات الحوكمة الرقمية وحوكمة الذكاء الاصطناعي 39.....
- 2.4.1 مفهوم الحوكمة الرقمية: 39.....
- 2.4.2 حوكمة الذكاء الاصطناعي: 40.....
- 2.4.3 إدارة مخاطر الذكاء الاصطناعي وفق NIST AI RMF: 40.....
- 2.4.4 معيار 42001ISO/IEC ونظام إدارة الذكاء الاصطناعي: 41.....
- 2.4.5 الضوابط الوطنية السعودية ذات الصلة: 42.....
- 2.4.6 سياسة استخدام الذكاء الاصطناعي داخل المؤسسة: 43.....
- 2.4.7 التدريب والتوعية والرقابة: 43.....
- المبحث الخامس: النظريات المفسرة والنموذج المفاهيمي 45.....
- 2.5.1 نظرية النظم الاجتماعية التقنية: 45.....
- 2.5.2 إطار التكنولوجيا والتنظيم والبيئة TOE: 45.....
- 2.5.3 نظرية الموارد والقدرات الديناميكية: 45.....
- 2.5.4 نموذج قبول التقنية وسلوك المستخدم: 45.....

46.....	2.5.5 مدخل إدارة المخاطر:
47.....	2.5.6 النموذج المفاهيمي المعدل للدراسة:
48.....	2.5.7 خلاصة الإطار النظري:
49.....	ثانياً : الدراسات السابقة :
49.....	أولاً : الدراسات العربية.....
50.....	ثانياً : الدراسات الأجنبية :
52.....	2.39 أوجه التشابه والاختلاف والاستفادة والفجوة البحثية:
53.....	الفصل الثالث: منهجية الدراسة وإجراءاتها
53.....	3.1 منهج الدراسة:
53.....	3.2 تصميم الدراسة:
54.....	3.3 مجتمع الدراسة:
54.....	3.4 عينة الدراسة:
55.....	3.5 أداة الدراسة:
55.....	3.6 مقياس الاستجابة:
56.....	3.7 بناء الاستبانة:
57.....	3.8 صدق أداة الدراسة:
57.....	3.9 ثبات أداة الدراسة:
57.....	3.10 إجراءات جمع البيانات:
58.....	3.11 أنواع البيانات:
58.....	3.12 أساليب التحليل الإحصائي:
59.....	3.13 ربط الفرضيات بالتحليل الإحصائي:
60.....	3.14 الاعتبارات الأخلاقية:
60.....	3.15 حدود المنهجية:
61.....	خاتمة الفصل :
62.....	الفصل الرابع :عرض النتائج وتحليلها ومناقشتها
62.....	4.1 خصائص عينة الدراسة:

- 4.2 اختبار ثبات أداة الدراسة: 63
- 4.3 المتوسطات الحسابية لمتغيرات الدراسة : 64
- 4.4 تحليل أبعاد استخدام الذكاء الاصطناعي الظلي : 65
- 4.5 تحليل أبعاد الكفاءة التشغيلية 66
- 4.6 تحليل أبعاد مخاطر أمن البيانات 67
- 4.7 تحليل الارتباط بين متغيرات الدراسة:..... 68
- 4.8 اختبار أثر الذكاء الاصطناعي الظلي على الكفاءة التشغيلية: 68
- 4.9 اختبار أثر الذكاء الاصطناعي الظلي على مخاطر أمن البيانات: 69
- 4.10 اختبار الدور المعدل لسياسات الحوكمة الرقمية: 70
- 4.11 ملخص اختبار الفرضيات: 71
- 4.12 مناقشة النتائج في ضوء الدراسات السابقة:..... 72
- خاتمة الفصل: 73
- الفصل الخامس: الاستنتاجات والتوصيات والنموذج المقترح 74
- 5.1 الاستنتاجات العامة للدراسة: 74
- 5.2 الاستنتاجات المتعلقة باستخدام الذكاء الاصطناعي الظلي: 74
- 5.3 الاستنتاجات المتعلقة بالكفاءة التشغيلية: 75
- 5.4 الاستنتاجات المتعلقة بمخاطر أمن البيانات:..... 75
- 5.5 الاستنتاجات المتعلقة بسياسات الحوكمة الرقمية: 76
- 5.6 التوصيات الموجهة للإدارة العليا: 76
- 5.7 التوصيات الموجهة لإدارات تقنية المعلومات:..... 77
- 5.8 التوصيات الموجهة لأمن المعلومات وحماية البيانات: 77
- 5.9 التوصيات الموجهة للموارد البشرية والتدريب: 78
- 5.10 النموذج المقترح لحوكمة الذكاء الاصطناعي الظلي: 78
- 5.11 خطة تنفيذ مرحلية مقترحة: 79
- 5.12 مصفوفة قرار استخدام الذكاء الاصطناعي حسب مستوى الخطر 80
- 5.13 مكونات سياسة حوكمة الذكاء الاصطناعي داخل المؤسسة: 81

81.....	5.14 مقترحات الدراسات المستقبلية:
82.....	5.15 الخاتمة العامة للدراسة :
83.....	قائمة المراجع والمصادر:
86.....	الملاحق
86.....	ملحق (1) : الاستبانة المقترحة للدراسة
90.....	ملحق (2) : ترميز متغيرات الدراسة
90.....	ملحق (3) : نموذج موافقة مستنيرة
90.....	ملحق (4) : سجل مخاطر مختصر لاستخدام الذكاء الاصطناعي الظلي
91.....	ملحق (5) : قائمة تحقق لاستخدام الذكاء الاصطناعي بأمان
92.....	ملحق (6): بنود مقترحة لسياسة حوكمة استخدام الذكاء الاصطناعي
92.....	ملحق (7) : سيناريوهات تطبيقية لتقييم مخاطر الذكاء الاصطناعي الظلي
94.....	ملحق (8) : قاموس مصطلحات مختصر

الإهداء :

إلى كل من كان سنداً في طريق العلم، وإلى اسرتي الكريمة التي منحني الباحث الدافعية والصبر،
وإلى الأساتذة الذين يؤمنون بأن المعرفة مسؤولية قبل أن تكون شهادة، وإلى كل عامل يسعى إلى
استخدام التقنية بطريقة تعزز قيمة العمل وتحمي حقوق الآخرين وبياناتهم.

الشكر والتقدير

أتقدم بخالص الشكر والتقدير إلى جامعة ميداو شن وكلية الإدارة على ما تقدمه من بيئة علمية داعمة للبحث الأكاديمي، كما يتقدم بالشكر إلى المشرف العلمي على ما قدمه من توجيه ومتابعة، وإلى كل من أسهم بفكرة أو ملاحظة أو دعم في إعداد هذه الدراسة. ويؤكد الباحث أن موضوع الدراسة يكتسب أهميته من سرعة التحول الرقمي واتساع استخدام أدوات الذكاء الاصطناعي في بيئات العمل، الأمر الذي يتطلب بحثاً علمياً متوازناً يجمع بين الاستفادة من الابتكار وحماية البيانات.

المستخلص:

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. ويقصد بالذكاء الاصطناعي الظلي استخدام الموظفين لأدوات أو تطبيقات ذكاء اصطناعي دون اعتماد رسمي أو إشراف مؤسسي مباشر، بما يشمل استخدام أدوات عامة أو حسابات شخصية أو إدخال بيانات مرتبطة بالعمل في منصات غير معتمدة. وتنبع أهمية الدراسة من كون هذه الظاهرة تحمل أثرًا مزدوجًا؛ فهي قد تسهم في تسريع إنجاز الأعمال وتحسين جودة المخرجات، لكنها في الوقت ذاته قد ترفع احتمالات تسرب البيانات ومخالفة سياسات الخصوصية والامتثال.

اعتمدت الدراسة على المنهج الوصفي التحليلي، واقترحت استبانة لقياس أربعة محاور رئيسة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، وسياسات الحوكمة الرقمية. كما قدمت الدراسة نموذجًا إحصائيًا تطبيقيًا يوضح آليات اختبار العلاقات المباشرة والتفاعلية بين المتغيرات باستخدام معاملات الارتباط والانحدار الخطي والانحدار الهرمي. وتشير نتائج النموذج التطبيقي إلى أن الاستخدام غير المنظم للذكاء الاصطناعي يرتبط إيجابيًا بالكفاءة التشغيلية، لكنه يرتبط كذلك بارتفاع مخاطر أمن البيانات، بينما تعمل سياسات الحوكمة الرقمية على تعظيم الأثر الإيجابي وتقليل الأثر السلبي. خلصت الدراسة إلى أن التعامل الفعال مع الذكاء الاصطناعي الظلي لا يكون بالمنع المطلق ولا بالإتاحة غير المقيدة، بل من خلال بناء إطار حوكمة رقمي يحدد الأدوات المعتمدة، ويصنف البيانات، ويضع ضوابط للإدخال والإخراج، ويوفر التدريب، وينشئ آليات رقابة وتدقيق مستمرة. وأوصت الدراسة بتطوير سياسة مؤسسية لاستخدام الذكاء الاصطناعي، وإنشاء سجل للمخاطر، وتوفير بدائل مؤسسية آمنة، ورفع مستوى الوعي لدى الموظفين، ودمج حوكمة الذكاء الاصطناعي ضمن منظومة أمن المعلومات والتحول الرقمي.

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

Abstract:

This study examines 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. Shadow AI refers to employees' use of artificial intelligence tools without formal approval or direct organizational oversight, including public AI applications, personal accounts, or unsanctioned platforms for work-related tasks.

The study adopts a descriptive analytical design and proposes a structured questionnaire covering shadow AI use, operational efficiency, data security risks, and digital governance policies. The applied statistical model demonstrates how direct and interaction effects can be tested through correlation, linear regression, and hierarchical regression. The proposed results indicate that shadow AI may improve operational efficiency, but it also increases data security risks when governance controls are weak.

The study concludes that organizations should not rely on complete prohibition or unrestricted use. Instead, they should develop balanced AI governance policies that classify data, approve safe tools, define user responsibilities, train employees, monitor usage, and integrate AI governance with data protection and information security management systems.

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

قائمة الجداول :

- جدول(1) : متغيرات الدراسة وأبعادها
- جدول(2) : التعريفات المنهجية والإجرائية
- جدول(3) : مقارنة الذكاء الاصطناعي الظلي بتقنية المعلومات الظلية
- جدول(4) : مصفوفة مخاطر أمن البيانات
- جدول(5) : الدراسات السابقة العربية والأجنبية
- جدول(6) : محاور الاستبانة وفقراتها
- جدول(7) : نتائج الثبات والصدق
- جدول(8) : المتوسطات والانحرافات المعيارية
- جدول(9) : مصفوفة الارتباط
- جدول(10) : اختبار الفرضيات المباشرة والتفاعلية
- جدول(11) : خطة تنفيذ حوكمة الذكاء الاصطناعي

قائمة الأشكال:

- شكل(1) : النموذج المفاهيمي المقترح للدراسة
- شكل(2) : دورة حوكمة استخدام الذكاء الاصطناعي في بيئة العمل
- شكل(3) : المتوسطات الحسابية لمتغيرات الدراسة
- شكل(4) : الأثر المعدل لسياسات الحوكمة الرقمية

الفصل الأول: الإطار العام للدراسة

تمهيد :

يعرض هذا الفصل الإطار العام للدراسة من خلال تحديد خلفيتها ومشكلتها وأسئلتها وأهدافها وأهميتها وحدودها ومصطلحاتها ومتغيراتها ونموذجها المفاهيمي. وتكمن أهمية هذا الفصل في أنه يوضح البناء المنهجي الذي تنتظم حوله بقية الفصول، ويحدد طبيعة العلاقة بين استخدام الذكاء الاصطناعي الظلي في بيئة العمل من جهة، وبين الكفاءة التشغيلية ومخاطر أمن البيانات من جهة أخرى، في ظل الدور المعدل لسياسات الحوكمة الرقمية.

وتسعى الدراسة إلى تقديم معالجة متوازنة لموضوع حديث لا تزال أدبياته العربية في طور التكوين، إذ إن معظم الكتابات المتاحة تناقش الذكاء الاصطناعي بوصفه أداة رسمية أو نظاماً مؤسسياً، بينما تكشف الممارسة الواقعية عن انتشار استخدامات فردية غير معتمدة قد تسبق السياسات المؤسسية. وبذلك فإن موضوع الذكاء الاصطناعي الظلي يتطلب معالجة تجمع بين الإدارة، وتقنية المعلومات، وأمن البيانات، والحوكمة الرقمية، والسلوك التنظيمي.

1.1 خلفية الدراسة :

يمثل خلفية الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في خلفية استخدام الذكاء الاصطناعي في بيئة العمل؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (هيئة الحكومة الرقمية، 2025؛ سدايا، 2023؛ OECD، 2024).

وتزداد أهمية خلفية الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات

المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن خلفية الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.2 الذكاء الاصطناعي الظلي بوصفه ظاهرة تنظيمية :

يمثل الذكاء الاصطناعي الظلي بوصفه ظاهرة تنظيمية أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطًا بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطًا بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في تحول الأدوات العامة إلى أدوات عمل غير رسمية؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (IBM، 2025؛ Microsoft & LinkedIn، 2024).

وتزداد أهمية الذكاء الاصطناعي الظلي بوصفه ظاهرة تنظيمية في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن الذكاء الاصطناعي الظلي بوصفه ظاهرة تنظيمية لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.3 مشكلة الدراسة :

يمثل مشكلة الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطًا بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطًا بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في تعارض المكاسب التشغيلية مع المخاطر الأمنية؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (IBM، 2025؛ Microsoft & LinkedIn، 2024) (الهيئة الوطنية للأمن السيبراني، 2018؛ سدايا، 2020؛ NIST، 2023).

وتزداد أهمية مشكلة الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن مشكلة الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر.

ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات. وبناءً على ذلك تتحدد 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؟

1.4 أسئلة الدراسة :

يمثل أسئلة الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في ترجمة المشكلة إلى أسئلة قابلة للاختبار؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (سدايا، 2020؛ ISO، 2023؛ ISACA، 2019؛ NIST، 2023).

وتزداد أهمية أسئلة الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن أسئلة الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجرداً، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها

لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

- ما مستوى استخدام الذكاء الاصطناعي الظلي في بيئة العمل؟
- ما أثر هذا الاستخدام على الكفاءة التشغيلية؟
- ما أثره على مخاطر أمن البيانات؟
- ما مستوى توافر سياسات الحوكمة الرقمية؟
- هل تعدل سياسات الحوكمة الرقمية العلاقة بين الذكاء الاصطناعي الظلي والكفاءة التشغيلية؟
- هل تعدل سياسات الحوكمة الرقمية العلاقة بين الذكاء الاصطناعي الظلي ومخاطر أمن البيانات؟

1.5 أهداف الدراسة:

يمثل أهداف الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في قياس العلاقات المباشرة والتفاعلية بين المتغيرات؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (Noy & Zhang، 2023؛ Brynjolfsson et al.، 2025؛ Dell'Acqua et al.، 2023).

وتزداد أهمية أهداف الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن أهداف الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

- بناء إطار نظري يوضح مفهوم الذكاء الاصطناعي الظلي وأسبابه وأنماطه.
- قياس أثر الاستخدام غير الرسمي لأدوات الذكاء الاصطناعي على مؤشرات الكفاءة التشغيلية.

- تحليل أثر هذا الاستخدام على مخاطر أمن البيانات والخصوصية والامتثال.
- اختبار الدور المعدّل لسياسات الحوكمة الرقمية في العلاقات محل الدراسة.
- اقتراح إطار عملي لحوكمة استخدام الذكاء الاصطناعي داخل المؤسسات.

1.6 أهمية الدراسة العلمية:

يمثل أهمية الدراسة العلمية أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في إثراء الأدبيات العربية في موضوع حديث؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (هيئة الحكومة الرقمية، 2025؛ سدايا، 2023؛ OECD، 2024).

وتزداد أهمية أهمية الدراسة العلمية في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات

المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن أهمية الدراسة العلمية لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.7 أهمية الدراسة التطبيقية:

يمثل أهمية الدراسة التطبيقية أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطًا بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطًا بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في توجيه القيادات وإدارات تقنية المعلومات نحو سياسات قابلة للتنفيذ؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (سدايا، 2023 ؛ هيئة الحكومة الرقمية، 2025 ؛ الهيئة الوطنية للأمن السيبراني، 2018).

وتزداد أهمية أهمية الدراسة التطبيقية في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن أهمية الدراسة التطبيقية لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.8 حدود الدراسة:

يمثل حدود الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطًا بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطًا بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في تحديد المجال الموضوعي والبشري والمكاني والزمني والمنهجي؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (سدايا، 2020؛ ISO؛ 2023، ISACA؛ 2019، NIST، 2023).

وتزداد أهمية حدود الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن حدود الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي،

والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.9 متغيرات الدراسة:

يمثل متغيرات الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في ضبط البناء المفاهيمي والقياسي للدراسة؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (Noy & Zhang، 2023؛ Brynjolfsson et al.، 2025؛ Dell'Acqua et al.، 2023؛ NIST، 2020؛ سدايا، 2018؛ NIST، 2020؛ Dell'Acqua et al.، 2023).

وتزداد أهمية متغيرات الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن متغيرات الدراسة لا يُفهم بوصفه مفهوماً نظرياً مجرداً، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.10 فرضيات الدراسة:

يمثل فرضيات الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في صياغة العلاقات المتوقعة بين المتغيرات؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصراً عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (Noy & Zhang، 2023، Brynjolfsson et al.، 2025، Dell'Acqua et al.، 2023).

وتزداد أهمية فرضيات الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءاً كبيراً من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن فرضيات الدراسة لا يُفهم بوصفه مفهوماً نظرياً مجرداً، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.11 مصطلحات الدراسة:

يمثل مصطلحات الدراسة أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطاً بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطاً بطريقة استخدام الأفراد

للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في تحديد المفاهيم المنهجية والإجرائية؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (IBM، 2025؛ Microsoft & LinkedIn، 2024) (سدايا، 2020؛ ISO، 2023؛ NIST، 2019؛ ISACA، 2023).

وتزداد أهمية مصطلحات الدراسة في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن مصطلحات الدراسة لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

1.12 منطلقات الدراسة النظرية:

يمثل منطلقات الدراسة النظرية أحد المحاور الجوهرية في هذه الدراسة، لأن التحول الرقمي لم يعد مرتبطًا بمجرد اقتناء الأنظمة التقنية، بل أصبح مرتبطًا بطريقة استخدام الأفراد للتقنيات داخل مسارات العمل اليومية. ويظهر ذلك بوضوح في النظر إلى التقنية ضمن نظام اجتماعي وتنظيمي؛ إذ تتداخل اعتبارات السرعة والإنتاجية مع اعتبارات الحماية والامتثال والرقابة، الأمر الذي يجعل النظر إلى التقنية بمعزل عن السياق التنظيمي قاصرًا عن

تفسير نتائجها الفعلية. ومن ثم فإن تحليل هذا المحور يتطلب الجمع بين المنظور الإداري الذي يهتم بالأداء والكفاءة، والمنظور التقني الذي يهتم بالبيانات والأمن، والمنظور الحوكمي الذي يحدد حدود الاستخدام المقبول والمسؤول (سدايا، 2020؛ ISO؛ 2023، ISACA؛ 2019، NIST، 2023).

وتزداد أهمية منطلقات الدراسة النظرية في بيئات العمل التي تعتمد على الأعمال المعرفية، لأن جزءًا كبيرًا من قيمة العمل ينتج من معالجة النصوص والتقارير والبيانات والمراسلات والقرارات. وفي مثل هذه البيئات قد يلجأ الموظف إلى أدوات رقمية خارج المنظومة الرسمية عندما يشعر بأن الأدوات المتاحة لا تكفي لإنجاز العمل بالسرعة أو الجودة المطلوبة. وهذا السلوك لا يعني بالضرورة وجود نية مخالفة، لكنه يكشف عن فجوة بين احتياجات المستخدمين وسياسات المؤسسة، وهي فجوة يمكن أن تتحول إلى مصدر قيمة أو مصدر خطر بحسب مستوى النضج المؤسسي والرقابة والتوعية.

وبالنسبة للدراسة الحالية، فإن منطلقات الدراسة النظرية لا يُفهم بوصفه مفهومًا نظريًا مجردًا، بل بوصفه ممارسة يومية قابلة للقياس من خلال فقرات الاستبانة ومؤشرات الأداء والمخاطر. ولذلك سيتم ربط هذا المحور بمتغيرات الدراسة الثلاثة: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، مع اختبار الكيفية التي يمكن من خلالها لسياسات الحوكمة الرقمية أن تضبط العلاقة بين هذه المتغيرات. ويعكس هذا الربط طبيعة الموضوع المركبة التي تجمع بين الابتكار والضبط، وبين المرونة التشغيلية وحماية البيانات.

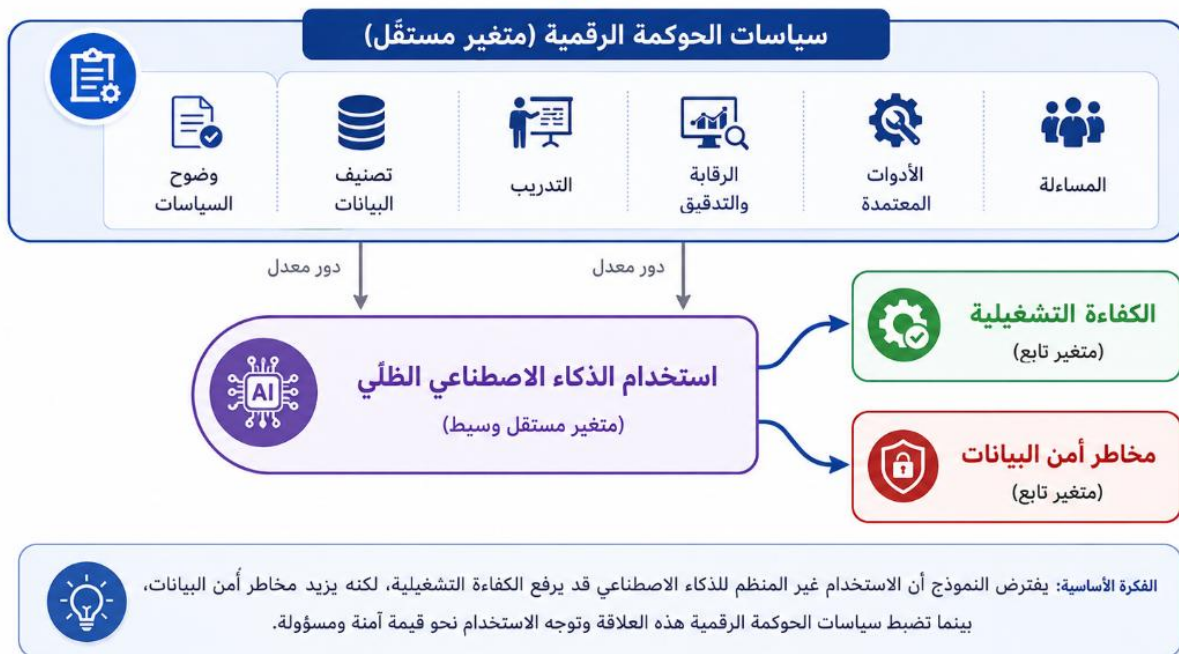
جدول (1) : متغيرات الدراسة وأبعادها

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، الاعتماد على 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.

النموذج المفاهيمي المقترح للدراسة



شكل (1) : النموذج المفاهيمي المقترح للدراسة .

*المصدر: إعداد الباحث.

جدول (2) : التعريفات المنهجية والإجرائية لمصطلحات الدراسة

المصطلح	التعريف المنهجي	التعريف الإجرائي
الذكاء الاصطناعي الظلي	استخدام أدوات ذكاء اصطناعي دون موافقة رسمية أو رقابة مؤسسية مباشرة.	درجة موافقة أفراد العينة على فقرات استخدام الأدوات غير المعتمدة والحسابات الشخصية وإدخال بيانات العمل في أدوات عامة.
الكفاءة التشغيلية	قدرة المؤسسة أو الموظف على إنجاز الأعمال بأقل وقت وجهد وتكلفة مع جودة مناسبة.	درجة موافقة أفراد العينة على فقرات سرعة الإنجاز وجودة المخرجات وخفض الجهد وتحسين تدفق العمل.
مخاطر أمن البيانات	احتمالية تعرض البيانات لتهديدات تمس السرية أو السلامة أو التوافر أو الخصوصية.	درجة موافقة أفراد العينة على فقرات التسرب، إدخال بيانات حساسة، ضعف الرقابة، صعوبة التتبع، وعدم الامتثال.
سياسات الحوكمة الرقمية	مجموعة السياسات والضوابط التي تنظم استخدام التقنيات الرقمية والذكاء الاصطناعي.	درجة موافقة أفراد العينة على فقرات وضوح السياسات وتصنيف البيانات والأدوات المعتمدة والتدريب والرقابة.

*المصدر : إعداد الباحث بالاستناد إلى أدبيات الدراسة.

الفصل الثاني : الإطار النظري والدراسات السابقة أولاً: الإطار النظري :

يمثل الإطار النظري في هذه الدراسة حلقة الربط بين الظاهرة التقنية الحديثة، وهي استخدام الذكاء الاصطناعي الظلي في بيئة العمل، وبين النتائج التنظيمية المترتبة عليها، وفي مقدمتها الكفاءة التشغيلية ومخاطر أمن البيانات. ويعتمد هذا الفصل على مقارنة تكاملية لا تنظر إلى الذكاء الاصطناعي باعتباره أداة تقنية مجردة، بل باعتباره ممارسة اجتماعية وتنظيمية تتأثر بسلوك المستخدمين، ونضج السياسات، وحساسية البيانات، ومستوى الرقابة المؤسسية. ولذلك جرى تنظيم الفصل في خمسة مباحث رئيسية، تجمع بين التعريف والتحليل والمقارنة والتفسير النظري.

تستند المعالجة النظرية إلى مصادر عربية وسعودية رسمية مثل تقرير هيئة الحكومة الرقمية حول الذكاء الاصطناعي التوليدي، ومبادئ أخلاقيات الذكاء الاصطناعي الصادرة عن سدايا، وسياسات حوكمة البيانات الوطنية، والضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، إضافة إلى أطر دولية مثل إطار إدارة مخاطر الذكاء الاصطناعي NIST AI RMF ومعياري ISO/IEC 42001، ودراسات ميدانية وتجريبية حديثة حول أثر الذكاء الاصطناعي في بيئة العمل (هيئة الحكومة الرقمية، 2025؛ سدايا، 2023؛ الهيئة الوطنية للأمن السيبراني، 2024؛ المعهد الوطني للمعايير والتقنية، 2023؛ المنظمة الدولية للمعايير، 2023).

المبحث الأول: الذكاء الاصطناعي والذكاء الاصطناعي الظلي

2.1.1 مفهوم الذكاء الاصطناعي وتطوره في بيئات الأعمال:

لم يعد الذكاء الاصطناعي في بيئات الأعمال مجرد نظام تقني محدود بوظائف محددة، بل أصبح منظومة أدوات وخوارزميات قادرة على إنتاج نصوص، وتلخيص وثائق، وتحليل بيانات، وتوليد أفكار، والمساعدة في البرمجة، ودعم القرار. وقد أدى هذا التحول إلى انتقال الذكاء الاصطناعي من مستوى الاستخدام المتخصص داخل إدارات تقنية المعلومات إلى مستوى الاستخدام اليومي بواسطة الموظفين في وحدات الأعمال المختلفة. وتؤكد هيئة الحكومة الرقمية أن الذكاء الاصطناعي التوليدي أصبح قادرًا على إنتاج مخرجات متنوعة تشمل

النصوص والصور والأكواد والملخصات، وهو ما يفتح مجالات واسعة لتحسين الخدمات والأعمال الرقمية (هيئة الحكومة الرقمية، 2025).

تزداد أهمية هذا التحول في الأعمال المعرفية التي تعتمد على المراسلات والتقارير والبيانات والتحليل، لأن قيمة العمل فيها لا ترتبط فقط بعدد المهام المنجزة، بل ترتبط أيضاً بجودة المعالجة وسرعة الاستجابة ودقة القرار. ولهذا أصبح الذكاء الاصطناعي مورداً تشغيلياً يمكن أن يعزز الإنتاجية، لكنه في الوقت نفسه قد يفتح مسارات جديدة للمخاطر إذا استخدم خارج الضوابط المؤسسية أو دون وعي بحساسية البيانات (سدايا، 2023؛ نوي وزانغ، 2023).

جدول (1-2) : تمييز مفاهيمي بين الذكاء الاصطناعي العام والتوليدي والظلي

المفهوم	المعنى الرئيس	دلالته في الدراسة الحالية
الذكاء الاصطناعي	أنظمة قادرة على أداء مهام تتطلب عادةً قدرات بشرية مثل التحليل والتنبؤ والتصنيف والتوصية.	يمثل الإطار التقني العام الذي تنتهي إليه أدوات الدراسة.
الذكاء الاصطناعي التوليدي	نماذج قادرة على إنشاء محتوى جديد مثل النصوص والملخصات والأكواد والصور بناءً على مدخلات المستخدم.	أكثر أنواع الذكاء الاصطناعي ارتباطاً بالاستخدام اليومي للموظفين.
الذكاء الاصطناعي الظلي	استخدام أدوات ذكاء اصطناعي دون اعتماد أو إشراف رسمي من جهة العمل.	المتغير المستقل في الدراسة، ويقاس من خلال الاستخدام غير المعتمد والحسابات الشخصية وإدخال بيانات العمل.

*المصدر: إعداد الباحث بالاستناد إلى (هيئة الحكومة الرقمية، 2025؛ أي بي إم، 2025).

2.1.2 الذكاء الاصطناعي التوليدي وطبيعة الاستخدام اليومي:

تنبع خصوصية الذكاء الاصطناعي التوليدي من سهولة الوصول إليه وقلة حاجته إلى خبرة تقنية عميقة، إذ يستطيع الموظف استخدامه من خلال محادثة نصية أو واجهة بسيطة لإنجاز أعمال متكررة أو معرفية. ويختلف هذا عن كثير من أنظمة الذكاء الاصطناعي التقليدية

التي تتطلب تكاملاً تقنياً معقداً أو فرقاً متخصصة. لذلك أصبح الذكاء الاصطناعي التوليدي قريباً من الموظف العادي، وقادراً على التأثير في روتين العمل اليومي داخل المؤسسات (هيئة الحكومة الرقمية، 2025؛ مايكروسوفت ولينكدإن، 2024).

1. تلخيص المراسلات والاجتماعات والتقارير الطويلة.
2. صياغة مسودات للخطابات والعروض والسياسات الداخلية.
3. تحليل أولي للبيانات والجداول واستخراج الأنماط العامة.
4. اقتراح أفكار لحل المشكلات التشغيلية أو تحسين الإجراءات.
5. مساعدة فرق التقنية في كتابة أكواد أو تفسير أخطاء برمجية.
6. إعداد محتوى تدريبي أو معرفي للموظفين والعملاء.

حيث أنه من الملاحظ كلما زادت سهولة الوصول إلى الأداة وارتفعت فائدتها المدركة، زاد احتمال استخدامها خارج القنوات الرسمية، خصوصاً إذا كانت المؤسسة لا توفر بدائل آمنة أو سياسات واضحة للاستخدام.

2.1.3 من الذكاء الاصطناعي الرسمي إلى الذكاء الاصطناعي الظلي:

يتحول استخدام الذكاء الاصطناعي من استخدام رسمي إلى استخدام ظلي عندما تكون الأداة خارج قائمة الأدوات المعتمدة، أو عندما تُستخدم بحساب شخصي، أو عندما لا تعلم الإدارة المختصة بطبيعة البيانات المدخلة فيها. وتعرف أي بي إم الذكاء الاصطناعي الظلي بأنه استخدام غير معتمد لأداة أو تطبيق ذكاء اصطناعي من قبل الموظفين أو المستخدمين النهائيين دون موافقة أو إشراف رسمي من إدارة تقنية المعلومات (أي بي إم، 2025).

شكل (2-2): مسار التحول من الاستخدام الرسمي إلى الاستخدام الظلي

احتياج تشغيلي ضغط وقت أو مهمة معرفية	◀	بحث عن أداة عامة سهلة الوصول	◀	استخدام غير مصرح حساب شخصي أو منصة عامة	◀	نتيجة مزدوجة كفاءة محتملة ومخاطر بيانات
---	---	------------------------------	---	---	---	---

*المصدر: إعداد الباحث بالاستناد إلى (أي بي إم، 2025؛ مايكروسوفت ولينكدإن، 2024).

جدول (2-2): مقارنة بين الاستخدام الرسمي والظلي للذكاء الاصطناعي

وجه المقارنة	الاستخدام الرسمي	الاستخدام الظلي
اعتماد الأداة	أداة معتمدة من المؤسسة أو موثقة في سياسة داخلية.	أداة يختارها الموظف دون اعتماد رسمي.
إدارة البيانات	توجد ضوابط لإدخال البيانات وتخزينها ومراجعتها.	قد تُدخل بيانات العمل في منصة عامة أو حساب شخصي.
المساءلة	المسؤوليات محددة بين المستخدم والإدارة التقنية والحوكمة.	المسؤولية غير واضحة وقد تظهر بعد وقوع حادثة.
المكاسب	استفادة مؤسسية قابلة للقياس والتعميم.	مكاسب فردية سريعة لكنها غير مرئية للمؤسسة.
المخاطر	مخاطر مضبوطة نسبياً عبر التصنيف والرقابة.	مخاطر أعلى في الخصوصية والسرية والامتثال.

*المصدر: إعداد الباحث بالاستناد إلى (أي بي إم، 2025؛ المعهد الوطني للمعايير والتقنية، 2023).

2.1.4 أسباب انتشار الذكاء الاصطناعي الظلي:

لا ينتشر الذكاء الاصطناعي الظلي بالضرورة نتيجة رغبة في مخالفة السياسات، بل غالباً نتيجة وجود فجوة بين احتياجات العمل اليومية والبدائل المؤسسية المتاحة. وقد أظهر تقرير مايكروسوفت ولينكدإن لعام 2024 أن نسبة مرتفعة من مستخدمي الذكاء الاصطناعي يجلبون أدواتهم الخاصة إلى العمل، وهو ما يعكس توجهاً عالمياً نحو BYOAI أو إحضار أدوات الذكاء الاصطناعي الشخصية إلى بيئة العمل (مايكروسوفت ولينكدإن، 2024).

جدول (3-2): دوافع انتشار الذكاء الاصطناعي الظلي وآثارها

الدافع	تفسيره العملي	الأثر المحتمل
ضغط الوقت	الحاجة إلى إنجاز سريع لتقارير أو مراسلات أو تحليلات.	تحسن سرعة الإنجاز مع احتمال تجاوز الضوابط.
ضعف البدائل الرسمية	عدم توفر أداة مؤسسية سهلة أو فعالة.	زيادة الاعتماد على أدوات عامة خارج السيطرة.
سهولة الوصول	الأدوات متاحة عبر المتصفح أو الهاتف وبحسابات شخصية.	انخفاض حاجز الاستخدام وارتفاع احتمالات الاستخدام غير المرئي.
ثقافة الإنجاز الفردي	الموظف يقيس النجاح بسرعة الإنتاج لا بالامتثال فقط.	تحسن مخرجات فردية مع ضعف التوثيق والمراجعة.
تأخر السياسات	غياب قواعد واضحة لما يجوز أو لا يجوز إدخاله في الأداة.	عدم اتساق الممارسات وارتفاع مخاطر أمن البيانات.

المصدر: إعداد الباحث بالاستناد إلى (مايكروسوفت ولينكدان، 2024؛ سدايا، 2023).

2.1.5 أنماط استخدام الذكاء الاصطناعي الظلي في العمل:

يمكن قياس الذكاء الاصطناعي الظلي من خلال أنماط استخدام قابلة للملاحظة داخل بيئة العمل، وليس فقط من خلال وجود الأداة ذاتها. فالمعيار الأهم هو علاقة الاستخدام بالبيانات والمهام الرسمية، ومدى معرفة المؤسسة بهذا الاستخدام. وبناءً على ذلك يمكن تصنيف الأنماط العملية كما في الجدول الآتي:

جدول (4-2): أنماط استخدام الذكاء الاصطناعي الظلي في بيئة العمل

النمط	مثال تطبيقي	المخاطر المصاحبة	الإجراء الحوكمي المناسب
تلخيص مستندات العمل	رفع تقرير داخلي أو محضر اجتماع إلى أداة عامة للتلخيص.	احتمال كشف بيانات داخلية أو شخصية.	منع رفع الوثائق الحساسة وتوفير أداة مؤسسية آمنة.

صياغة المراسلات	كتابة ردود أو خطابات تتضمن بيانات عمل.	إفشاء معلومات أو تبني صياغات غير دقيقة.	إلزام المراجعة البشرية وتصنيف نوع المراسلات.
تحليل بيانات العملاء	نسخ جدول يتضمن بيانات عملاء أو موظفين لتحليله.	مخاطر خصوصية وامتثال وتسرب.	إخفاء الهوية ومنع إدخال البيانات الشخصية.
المساعدة في البرمجة	إدخال كود أو مفاتيح أو رسائل خطأ من نظام داخلي.	مخاطر ملكية فكرية أو أمن تطبيقات.	سياسة واضحة للأكواد والبيئات التجريبية.
إعداد عروض وتقارير	استخدام أداة عامة لبناء عرض أو تقرير إداري.	مخرجات غير موثقة أو تحيز في التحليل.	توثيق المصدر والمراجعة المتخصصة قبل الاعتماد.

*المصدر: إعداد الباحث بالاستناد إلى (أي بي إم، 2025؛ سدايا، 2024؛ الهيئة الوطنية للأمن السيبراني، 2024).

2.1.6 المكاسب والقيود في الاستخدام غير الرسمي:

قد يحقق الاستخدام غير الرسمي مكاسب تشغيلية حقيقية، خاصة في المهام المعرفية الروتينية، لكنه يظل مكسبًا غير مكتمل إذا لم يخضع لضوابط مؤسسية. وقد أثبتت دراسات تجريبية حديثة أن أدوات الذكاء الاصطناعي التوليدي يمكن أن تقلل وقت إنجاز بعض المهام وتحسن جودة المخرجات، لكنها في الوقت نفسه قد تؤدي إلى نتائج غير دقيقة عندما تستخدم خارج حدودها المناسبة أو دون مراجعة بشرية كافية (نوي وزانغ، 2023؛ ديل أكوا وآخرون، 2023). ويمكن اختصارها بالآتي:

- المكسب التشغيلي الرئيس: تقليل الوقت والجهد في المهام المتكررة والمعرفية.
- القيد المعرفي: احتمالية إنتاج إجابات غير دقيقة أو غير موثقة أو متحيزة.
- القيد المهني: ضعف قدرة الموظف على تفسير المخرجات أو التحقق من مصادرها.
- القيد الأمني: احتمال إدخال بيانات غير مسموح بها في أدوات عامة.
- القيد الحوكمي: صعوبة تتبع الاستخدام عندما يتم بحسابات شخصية أو خارج الأنظمة الرسمية.

المبحث الثاني: الكفاءة التشغيلية في سياق الذكاء الاصطناعي

2.2.1 مفهوم الكفاءة التشغيلية:

تشير الكفاءة التشغيلية إلى قدرة المؤسسة على إنتاج المخرجات المطلوبة بأقل وقت وجهد وتكلفة ممكنة، مع الحفاظ على مستوى مقبول من الجودة والامتثال. وفي سياق الذكاء الاصطناعي، لا تقتصر الكفاءة على تسريع العمل، بل تشمل تحسين تدفق الإجراءات، وتقليل الأخطاء، وتمكين الموظف من التركيز على أعمال أعلى قيمة. وتؤكد هيئة الحكومة الرقمية أن الذكاء الاصطناعي التوليدي يمكن أن يسهم في رفع الإنتاجية وتحسين استخدام الموارد في أعمال الحكومة الرقمية، خصوصًا في التلخيص، وإنشاء المحتوى، ودعم تطوير البرمجيات (هيئة الحكومة الرقمية، 2025).

لكن الكفاءة التشغيلية الناتجة عن الذكاء الاصطناعي لا ينبغي أن تُفهم بمعزل عن المخاطر؛ فقد تكون السرعة الظاهرة مصحوبة بمخاطر جودة أو خصوصية أو امتثال إذا لم تُراجع المخرجات أو إذا استُخدمت بيانات لا يجوز مشاركتها. لذلك تتبنى الدراسة الحالية مفهومًا متوازنًا للكفاءة التشغيلية يربط بين الإنتاجية من جهة، والالتزام والضبط من جهة أخرى (سدايا، 2023؛ المعهد الوطني للمعايير والتقنية، 2023).

جدول (2-5): مؤشرات الكفاءة التشغيلية في الدراسة الحالية

المؤشر	التفسير	مثال قياس في الاستبانة
سرعة الإنجاز	تقليل الزمن اللازم لإنهاء المهمة.	يساعد الذكاء الاصطناعي على إنجاز المهام في وقت أقصر.
جودة المخرجات	تحسين الصياغة والتنظيم والدقة النسبية.	تحسن أدوات الذكاء الاصطناعي جودة التقارير والمراسلات.
تقليل الجهد	خفض العمل اليدوي المتكرر.	تقلل الأدوات الذكية الجهد المبذول في المهام الروتينية.
خفض الأخطاء	تقليل أخطاء التنسيق والحساب واللغة عند المراجعة المناسبة.	يساعد الذكاء الاصطناعي على تقليل الأخطاء التشغيلية.
تحسين تدفق العمل	تسريع انتقال المعلومات بين المراحل.	يسهم الاستخدام المنظم في تسهيل متابعة الإجراءات.
استثمار الموارد	توجيه وقت الموظف إلى مهام تحليلية أو إبداعية أعلى قيمة.	يساعد الذكاء الاصطناعي على استثمار الوقت في مهام أكثر أهمية.

*المصدر: إعداد الباحث بالاستناد إلى (هيئة الحكومة الرقمية، 2025؛ نوي وزانغ، 2023؛ براينجولفسون وآخرون، 2025).

2.2.2 الذكاء الاصطناعي وأتمتة العمليات الروتينية:

تعد أتمتة العمليات الروتينية أحد أهم مسارات التأثير في الكفاءة التشغيلية، لأن كثيراً من الأعمال الإدارية اليومية تتكون من مهام متكررة مثل فرز الرسائل، وتلخيص المحاضر، وإعداد مسودات الردود، وتجهيز تقارير دورية. وعندما يستخدم الموظف أداة ذكاء اصطناعي لإنجاز هذه المهام، فإن المكسب يظهر في تقليل الوقت وتحسين الاستجابة. إلا أن هذا المكسب يظل مشروطاً بكون البيانات المستخدمة غير حساسة أو مصرحاً بمعالجتها، وبوجود مراجعة بشرية للمخرجات قبل اعتمادها (هيئة الحكومة الرقمية، 2025؛ سدايا، 2024).

وتتمثل الأتمتة بالآتي :

1. أتمتة القراءة الأولية: تلخيص الوثائق الطويلة واستخراج النقاط الرئيسة.
2. أتمتة الكتابة الأولية: إعداد مسودات تقارير وخطابات قبل المراجعة.
3. أتمتة التنظيم: تحويل ملاحظات الاجتماعات إلى مهام أو قوائم متابعة.
4. أتمتة التحليل البسيط: قراءة جداول غير حساسة واستخراج مؤشرات عامة.
5. أتمتة الدعم المعرفي: تقديم مقترحات أو بدائل للقرارات التشغيلية.

جدول (2-6): علاقة أدوات الذكاء الاصطناعي بأبعاد الكفاءة التشغيلية

نوع الاستخدام	الأثر على الوقت	الأثر على الجودة	شرط السلامة
تلخيص تقرير داخلي غير حساس	مرتفع	متوسط إلى مرتفع	إزالة المعلومات السرية والشخصية.
صياغة خطاب رسمي	متوسط	مرتفع بعد المراجعة	اعتماد مراجعة إدارية ولغوية.
تحليل جدول مؤشرات تشغيلية	مرتفع	متوسط	التأكد من عدم وجود بيانات شخصية أو سرية.
إعداد أفكار تحسين إجراءات	متوسط	متغير	التحقق من ملاءمة المقترحات للسياسات الداخلية.
كتابة أكواد أو حلول تقنية	متوسط إلى مرتفع	متغير	عدم مشاركة مفاتيح أو أكواد سرية أو بنية داخلية حساسة.

*المصدر: إعداد الباحث بالاستناد إلى (هيئة الحكومة الرقمية، 2025؛ ديل أكوا وآخرون، 2023).

2.2.3 الذكاء الاصطناعي ودعم القرار التشغيلي:

يدعم الذكاء الاصطناعي القرار التشغيلي من خلال تنظيم المعلومات وتقديم ملخصات ومقارنات وتوصيات أولية. ومع ذلك فإن القرار النهائي يجب أن يبقى قرارًا بشريًا مؤسسيًا، لأن مخرجات الذكاء الاصطناعي قد تكون غير مكتملة أو منحازة أو غير محدثة. وتؤكد مبادئ أخلاقيات الذكاء الاصطناعي الصادرة عن سدايا أهمية المساءلة والشفافية والعدالة والموثوقية في تطوير واستخدام الأنظمة الذكية، وهي مبادئ ضرورية عند توظيف الذكاء الاصطناعي في قرارات تشغيلية (سدايا، 2023).

قاعدة حوكمة مقترحة
لا يعتمد أي قرار تشغيلي أو إداري جوهري على مخرجات أداة ذكاء اصطناعي عامة دون مراجعة بشرية موثقة، وتحديد مصدر البيانات، والتحقق من توافق الاستخدام مع سياسات البيانات والخصوصية.

2.2.4 حدود الكفاءة التشغيلية الناتجة عن الذكاء الاصطناعي:

تظهر حدود الكفاءة عندما يُستخدم الذكاء الاصطناعي في مهمة تتجاوز قدرته أو لا تتوافر له بيانات كافية عنها. وقد بينت دراسة ديل أكوا وزملائه أن أثر الذكاء الاصطناعي يكون إيجابيًا عندما تقع المهمة داخل حدود قدرة الأداة، لكنه قد يكون سلبيًا عندما يستخدم في مهام خارج تلك الحدود. وهذا يعني أن الكفاءة ليست أثرًا تلقائيًا للأداة، بل نتيجة لتوافق المهمة مع قدرة الأداة وخبرة المستخدم ونظام الرقابة (ديل أكوا وآخرون، 2023).

وتتمثل هذه الحدود بما يلي :

1. نوع المهمة: المهام الروتينية والنصية أكثر قابلية للتحسين من المهام التي تتطلب حكمًا مهنيًا عميقًا.
2. خبرة المستخدم: المستخدم الخبير يستطيع صياغة المدخلات ومراجعة المخرجات بصورة أفضل.
3. جودة البيانات: إدخال بيانات ناقصة أو خاطئة يؤدي إلى مخرجات ضعيفة مهما كانت الأداة متقدمة.
4. مستوى الحوكمة: وجود سياسة واضحة يقلل الاستخدام العشوائي ويزيد الاستفادة الآمنة.
5. المراجعة البشرية: شرط أساسي لتحويل المخرجات من مساعدة أولية إلى قرار أو منتج نهائي.

المبحث الثالث: مخاطر أمن البيانات المرتبطة بالذكاء الاصطناعي الظلي

2.3.1 مفهوم أمن البيانات وأبعاده:

يقصد بأمن البيانات حماية البيانات من الوصول غير المصرح به أو الإفشاء أو التعديل أو فقدان أو سوء الاستخدام. ويقوم أمن البيانات عادةً على ثلاثة أبعاد رئيسة هي السرية، والسلامة، والتوافر، وتضاف إليها في بيئات الذكاء الاصطناعي أبعاد الخصوصية والامتثال وقابلية التتبع. وفي المملكة العربية السعودية، ترتبط حماية البيانات بضوابط الأمن السيبراني وحوكمة البيانات ونظام حماية البيانات الشخصية ولوائحه التنفيذية (الهيئة الوطنية للأمن السيبراني، 2024؛ سدايا، 2024؛ مكتب إدارة البيانات الوطنية، 2020).

جدول (2-7): أبعاد أمن البيانات في سياق الذكاء الاصطناعي الظلي

البعد	المعنى	الخطر عند استخدام أدوات عامة
السرية	منع الإفشاء غير المصرح به.	رفع مستندات أو بيانات داخلية إلى منصة غير معتمدة.
السلامة	الحفاظ على دقة البيانات وعدم تغييرها بطريقة غير مصرح بها.	اعتماد تحليل أو ملخص غير دقيق يؤثر في القرار.
التوافر	إتاحة البيانات والأنظمة عند الحاجة.	فقدان السيطرة على نسخة البيانات أو اعتماد خدمة خارجية غير مضمونة.
الخصوصية	حماية البيانات الشخصية وحقوق أصحابها.	إدخال بيانات عملاء أو موظفين في أداة لا تخضع لسياسات المؤسسة.
الامتثال	الالتزام بالسياسات والأنظمة والمعايير.	مخالفة سياسات المؤسسة أو المتطلبات الوطنية لحماية البيانات.
قابلية التتبع	معرفة من استخدم البيانات ومتى ولماذا.	صعوبة توثيق الاستخدام عند الاعتماد على حسابات شخصية.

*المصدر: إعداد الباحث بالاستناد إلى (الهيئة الوطنية للأمن السيبراني، 2024؛ سدايا، 2024؛ المعهد الوطني للمعايير والتقنية، 2023).

2.3.2 حساسية البيانات في بيئة العمل:

تبدأ إدارة مخاطر الذكاء الاصطناعي الظلي من فهم حساسية البيانات. فالبيانات ليست على مستوى واحد من الخطورة؛ فهناك بيانات عامة يمكن مشاركتها، وبيانات داخلية ينبغي ضبط تداولها، وبيانات سرية أو شخصية أو حساسة لا يجوز إدخالها في أدوات عامة. وتؤكد سياسات حوكمة البيانات الوطنية أهمية تصنيف البيانات وفق قيمتها وحساسيتها وأثر الإفصاح عنها، لأن التصنيف يمثل الأساس العملي لتحديد ضوابط الاستخدام والتخزين والمشاركة (مكتب إدارة البيانات الوطنية، 2020؛ سدايا، 2024).

جدول (2-8): تصنيف البيانات وضوابط إدخالها في أدوات الذكاء الاصطناعي

مستوى البيانات	أمثلة	حكم إدخالها في أداة عامة	الإجراء الآمن
عامة	معلومات منشورة للجمهور أو مواد تدريبية عامة.	مسموح غالبًا بعد التحقق من الملكية الفكرية.	استخدامها دون بيانات داخلية أو شخصية.
داخلية	إجراءات عمل أو مؤشرات غير منشورة.	مقيد ويتطلب سياسة واضحة.	إزالة التفاصيل الحساسة أو استخدام أداة مؤسسية.
سرية	عقود، خطط استراتيجية، تقارير مالية داخلية.	غير مسموح في الأدوات العامة.	استخدام بيئة مؤسسية معتمدة وضوابط وصول.
شخصية	بيانات العملاء أو الموظفين أو المتقدمين.	غير مسموح غالبًا دون أساس نظامي وضوابط.	إخفاء الهوية أو طلب موافقة/أساس نظامي عند اللزوم.
حساسة	بيانات صحية أو مالية أو أمنية أو بيانات اعتماد.	محظور في الأدوات العامة.	منع الإدخال والاحتفاظ والمعالجة خارج الأنظمة الرسمية.

*المصدر: إعداد الباحث بالاستناد إلى (مكتب إدارة البيانات الوطنية، 2020؛ سدايا، 2024).

2.3.3 مخاطر إدخال البيانات في أدوات عامة:

تمثل عملية إدخال البيانات في أدوات عامة إحدى أخطر نقاط الذكاء الاصطناعي الظلي؛ لأن الموظف قد ينظر إلى الأداة بوصفها مساعدًا شخصيًا، بينما تتعامل المؤسسة معها بوصفها قناة خارجية لمعالجة البيانات. وتكمن الخطورة في أن البيانات قد تُحفظ أو تُستخدم لتحسين النماذج أو تنتقل خارج نطاق سيطرة المؤسسة وفق شروط الخدمة الخاصة بالأداة. لذلك لا بد من التفريق بين استخدام الأداة لتوليد أفكار عامة، وبين استخدامها لمعالجة بيانات عمل فعلية (أي بي إم، 2025؛ سدايا، 2024).

وتتمثل هذه المخاطر بالآتي :

1. خطر الإفشاء: ظهور بيانات داخلية أو شخصية خارج نطاق المؤسسة.
2. خطر الاحتفاظ: بقاء المدخلات في سجلات المنصة أو حساب المستخدم.
3. خطر النقل: انتقال البيانات إلى خوادم أو جهات خارجية لا تخضع لسياسات المؤسسة.
4. خطر إعادة الاستخدام: احتمال استخدام المدخلات في تحسين الخدمة أو تدريب النماذج بحسب شروط المنصة.
5. خطر غياب السجل: صعوبة إثبات ما أدخله الموظف ومتى ولأي غرض.

2.3.4 مخاطر الخصوصية وحماية البيانات الشخصية:

ترتبط مخاطر الخصوصية مباشرة باستخدام الذكاء الاصطناعي الظلي عندما تتضمن المدخلات أسماء أو أرقام هويات أو بيانات اتصال أو سجلات معاملات أو أي بيانات يمكن أن تعرّف فردًا بشكل مباشر أو غير مباشر. ويطبق نظام حماية البيانات الشخصية في المملكة على عمليات معالجة البيانات الشخصية، كما توضح لائحته التنفيذية التزامات المتحكم والمعالج وحقوق أصحاب البيانات. وبناءً على ذلك فإن إدخال بيانات شخصية في أداة عامة دون أساس نظامي أو ضوابط مناسبة قد يشكل مخالفة امتثال ومخاطرة أمنية في الوقت نفسه (سدايا، 2024؛ نظام حماية البيانات الشخصية، 2021).

ولو طبقنا ذلك على الدراسة الحالية نلاحظ أنها لا تقيس "وجود تسرب فعلي" بالضرورة، بل تقيس مستوى مخاطر أمن البيانات كما يدركها العاملون، من خلال ممارسات مثل إدخال بيانات حساسة، وصعوبة التتبع، وضعف الرقابة، واحتمال مخالفة سياسات المؤسسة.

2.3.5 مخاطر عدم الامتثال التنظيمي:

قد يحقق الموظف مكسبًا سريعًا باستخدام أداة غير معتمدة، لكنه قد يعرض المؤسسة لمخاطر عدم امتثال إذا كان الاستخدام مخالفًا لسياسة أمن المعلومات، أو سياسة تصنيف البيانات، أو متطلبات حماية البيانات الشخصية، أو الضوابط الوطنية للأمن السيبراني. وتؤكد الضوابط الأساسية للأمن السيبراني على أهمية حوكمة الأمن السيبراني وإدارة المخاطر وحماية الأنظمة والبيانات، وهي مبادئ تتصل مباشرة بإدارة استخدام الذكاء الاصطناعي في بيئة العمل (الهيئة الوطنية للأمن السيبراني، 2024؛ سدايا، 2024).

جدول (2-9): مصفوفة مخاطر أمن البيانات في استخدام الذكاء الاصطناعي الظلي

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

*المصدر: إعداد الباحث بالاستناد إلى (الهيئة الوطنية للأمن السيبراني، 2024؛ أي بي إم، 2025؛ سدايا، 2024).

المبحث الرابع: سياسات الحوكمة الرقمية وحوكمة الذكاء الاصطناعي

2.4.1 مفهوم الحوكمة الرقمية:

يقصد بالحوكمة الرقمية مجموعة السياسات والآليات والهياكل التي تضبط استخدام التقنيات والبيانات داخل المؤسسة، وتحدد المسؤوليات والصلاحيات وآليات الرقابة والمساءلة. وفي سياق الذكاء الاصطناعي الظلي، لا تقتصر الحوكمة الرقمية على منع الاستخدام، بل تهدف إلى تنظيمه وتوجيهه بما يحقق الفائدة التشغيلية مع تقليل المخاطر. فالمنع المطلق قد يدفع الموظفين إلى إخفاء الاستخدام، بينما التنظيم الذكي يوفر بدائل آمنة ويجعل الاستخدام قابلاً للتتبع والتقييم (سدايا، 2023؛ المعهد الوطني للمعايير والتقنية، 2023).

تتكون الحوكمة الرقمية الفعالة في هذه الدراسة من عدة عناصر مترابطة: وضوح السياسة، تصنيف البيانات، تحديد الأدوات المعتمدة، التدريب والتوعية، الرقابة والتدقيق، وتحديد المسؤوليات والمساءلة. وتؤدي هذه العناصر دوراً معديلاً في العلاقة بين استخدام الذكاء الاصطناعي الظلي والنتائج التابعة؛ إذ قد تعزز أثره الإيجابي على الكفاءة التشغيلية وتخفف أثره السلبي على أمن البيانات.

شكل (2-3): دورة الحوكمة الرقمية للاستخدام الآمن للذكاء الاصطناعي



*المصدر: إعداد الباحث بالاستناد إلى (المعهد الوطني للمعايير والتقنية، 2023؛ المنظمة الدولية للمعايير، 2023؛ سدايا، 2023).

2.4.2 حوكمة الذكاء الاصطناعي :

حوكمة الذكاء الاصطناعي هي الإطار الذي يحدد كيف تُصمم أنظمة الذكاء الاصطناعي وتُستخدم وتُراقب وتُراجع داخل المؤسسة. وهي تختلف عن الحوكمة الرقمية العامة لأنها تتعامل مع مخاطر خاصة مثل التحيز، وعدم الدقة، وضعف التفسير، واعتماد المستخدم على المخرجات دون تحقق. وتشير مبادئ أخلاقيات الذكاء الاصطناعي إلى ضرورة مراعاة الإنصاف والخصوصية والأمن والشفافية والمساءلة والموثوقية، وهي مبادئ ضرورية عند تنظيم استخدام أدوات الذكاء الاصطناعي في بيئة العمل (سدايا، 2023).

جدول (2-10): مكونات حوكمة الذكاء الاصطناعي في الدراسة الحالية

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 شيوعًا.
التدريب	رفع وعي الموظفين باستخدام المسؤول.	تدريب عملي على صياغة المدخلات الآمنة وعدم مشاركة البيانات السرية.
الرقابة	تتبع الالتزام وتحسين السياسة.	مراجعة دورية للأدوات المستخدمة والمخالفات المحتملة.
البدائل الآمنة	تقليل الحاجة إلى أدوات شخصية.	توفير أدوات مؤسسية معتمدة ومتكاملة مع ضوابط البيانات.

*المصدر: إعداد الباحث بالاستناد إلى (سدايا، 2023؛ المعهد الوطني للمعايير والتقنية، 2023؛ المنظمة الدولية للمعايير، 2023).

2.4.3 إدارة مخاطر الذكاء الاصطناعي وفق NIST AI RMF :

يوفر إطار إدارة مخاطر الذكاء الاصطناعي الصادر عن المعهد الوطني للمعايير والتقنية NIST AI RMF نموذجًا مهمًا لفهم المخاطر المرتبطة بالذكاء الاصطناعي وإدارتها طوال دورة الحياة. ويرتكز الإطار على وظائف رئيسة يمكن توظيفها في هذه الدراسة: الحوكمة، ورسم السياق، والقياس، والإدارة. وتبرز أهمية هذا الإطار في أنه يتعامل مع الذكاء الاصطناعي بوصفه نظامًا اجتماعيًا تقنيًا يتأثر بالمستخدمين والبيانات والسياق التنظيمي وليس بالنموذج التقني فقط (المعهد الوطني للمعايير والتقنية، 2023).

جدول (2-11): توظيف وظائف NIST AI RMF في ضبط الذكاء الاصطناعي الظلي

وظيفة الإطار	معناها	تطبيقها في الدراسة
الحكومة Govern	وضع المسؤوليات والسياسات والثقافة المؤسسية.	بناء سياسة استخدام الذكاء الاصطناعي وتحديد المساءلة.
رسم السياق Map	فهم السياق والبيانات والأطراف المتأثرة.	تصنيف المهام والبيانات قبل السماح بالاستخدام.
القياس Measure	قياس المخاطر والموثوقية والجودة.	تقييم أثر الاستخدام على الكفاءة والمخاطر.
الإدارة Manage	اختيار المعالجات والضوابط والتحسين.	توفير بدائل أمنة وتدريب ورقابة دورية.

*المصدر: إعداد الباحث بالاستناد إلى (المعهد الوطني للمعايير والتقنية، 2023).

2.4.4 معيار ISO/IEC 42001 ونظام إدارة الذكاء الاصطناعي:

يمثل معيار ISO/IEC 42001 أحد المعايير الدولية المهمة في حوكمة الذكاء الاصطناعي؛ لأنه يضع متطلبات لإنشاء وتنفيذ وصيانة وتحسين نظام إدارة الذكاء الاصطناعي داخل المؤسسة. وتبرز قيمته للدراسة الحالية في أنه يترجم الحوكمة إلى نظام إداري يتضمن سياسات وأهدافاً وعمليات ومسؤوليات، وهو ما يساعد المؤسسات على الانتقال من الاستجابة العشوائية لاستخدامات الذكاء الاصطناعي إلى إدارة منظمة للمخاطر والفرص (المنظمة الدولية للمعايير، 2023).

وفي المقابل، يرتبط معيار ISO/IEC 27001 بنظام إدارة أمن المعلومات، وهو مهم لأن مخاطر الذكاء الاصطناعي الظلي لا تنفصل عن أمن المعلومات. فالأداة قد تكون ذكية من حيث الإنتاجية، لكنها تصبح مصدر خطر إذا أدخلت إليها بيانات لا يسمح النظام الأمني بإخراجها من بيئة المؤسسة. ولذلك ينبغي أن تتكامل حوكمة الذكاء الاصطناعي مع حوكمة أمن المعلومات وليس أن تعمل بمعزل عنها (المنظمة الدولية للمعايير، 2023؛ الهيئة الوطنية للأمن السيبراني، 2024).

2.4.5 الضوابط الوطنية السعودية ذات الصلة:

ينبغي أن تُبنى سياسة استخدام الذكاء الاصطناعي في المؤسسات السعودية على تكامل عدة مرجعيات وطنية؛ فمبادئ أخلاقيات الذكاء الاصطناعي تقدم مبادئ عامة للاستخدام المسؤول، وسياسات حوكمة البيانات الوطنية تقدم أساساً لتصنيف البيانات وتحديد ضوابطها، ونظام حماية البيانات الشخصية يحدد التزامات المعالجة عند التعامل مع بيانات الأفراد، والضوابط الأساسية للأمن السيبراني تضع متطلبات حماية الأصول المعلوماتية والتقنية (سدايا، 2023؛ مكتب إدارة البيانات الوطنية، 2020؛ سدايا، 2024؛ الهيئة الوطنية للأمن السيبراني، 2024).

جدول (2-12): مرجعيات وطنية داعمة لحوكمة الذكاء الاصطناعي في بيئة العمل

المرجعية	مجالها	علاقتها بالذكاء الاصطناعي الظلي
مبادئ أخلاقيات الذكاء الاصطناعي	الاستخدام المسؤول والشفافية والمساءلة.	تحدد المبادئ التي يجب أن تحكم استخدام الأدوات الذكية.
سياسات حوكمة البيانات الوطنية	تصنيف البيانات وحوكمتها وإدارتها.	تحدد ما يمكن إدخاله في الأدوات وما يجب منعه أو إخفاؤه.
نظام حماية البيانات الشخصية ولائحته التنفيذية	حقوق أصحاب البيانات والتزامات المتحكم والمعالج.	يضبط استخدام البيانات الشخصية في أي أداة أو منصة.
الضوابط الأساسية للأمن السيبراني	إدارة المخاطر وحماية الأصول التقنية والمعلوماتية.	تربط استخدام الأدوات بضوابط الأمن والوصول والتتبع.
تقرير الذكاء الاصطناعي التوليدي في أعمال الحكومة الرقمية	استخدامات الذكاء الاصطناعي التوليدي في الحكومة الرقمية.	يوضح فرص الاستخدام المؤسسي المنظم وأثره على الكفاءة.

*المصدر: إعداد الباحث بالاستناد إلى المصادر الوطنية الرسمية ذات الصلة.

2.4.6 سياسة استخدام الذكاء الاصطناعي داخل المؤسسة:

تحتاج المؤسسات إلى سياسة استخدام ذكاء اصطناعي لا تكون عامة جدًا بحيث تفقد قيمتها، ولا تفصيلية جدًا بحيث يصعب تطبيقها. ويقترح الإطار النظري الحالي أن تتضمن السياسة عناصر عملية واضحة قابلة للفهم والقياس، بحيث يعرف الموظف ما الأداة المسموح بها، وما البيانات الممنوعة، ومتى يجب الإفصاح عن استخدام الذكاء الاصطناعي، ومن يراجع المخرجات.

جدول (2-13): بنود مقترحة لسياسة استخدام الذكاء الاصطناعي في المؤسسة

البند	السؤال الذي يجيب عنه	مثال تطبيقي
نطاق السياسة	من المخاطب بالسياسة؟	كل موظف أو متعاقد يستخدم أدوات ذكاء اصطناعي في مهام العمل.
الأدوات المعتمدة	ما الأدوات المسموح بها؟	قائمة أدوات مؤسسية أو خدمات وافقت عليها تقنية المعلومات.
البيانات الممنوعة	ما الذي لا يجوز إدخاله؟	البيانات السرية والشخصية والحساسة والعقود والأكواد الداخلية.
الإفصاح والتوثيق	متى يجب الإفصاح؟	عند استخدام الأداة لإنتاج تقرير أو توصية أو تحليل مؤثر.
المراجعة البشرية	من يراجع المخرجات؟	الموظف المختص أو المدير أو الفريق القانوني/الأمني بحسب نوع المخرجات.
العقوبات والمعالجة	ماذا يحدث عند المخالفة؟	إجراءات تصحيح وتدريب وربما مساءلة حسب خطورة المخالفة.

*المصدر: إعداد الباحث بالاستناد إلى (سدايا، 2023؛ المعهد الوطني للمعايير والتقنية، 2023؛ المنظمة الدولية للمعايير، 2023).

2.4.7 التدريب والتوعية والرقابة:

لا تكفي السياسة المكتوبة وحدها لضبط سلوك الموظفين، لأن كثيرًا من المخالفات التقنية تحدث بسبب ضعف الوعي أو غموض الحدود بين البيانات المسموح بها والممنوعة. ولذلك يعد التدريب والتوعية عنصرًا حاكمًا في الحد من الذكاء الاصطناعي الظلي. وينبغي أن

- يكون التدريب عمليًا قائمًا على سيناريوهات حقيقية، مثل: هل يجوز رفع محضر اجتماع؟ هل يجوز إدخال أسماء عملاء؟ هل يجوز تلخيص عقد؟ وما البديل الآمن في كل حالة؟
- وانطلاقًا مما سبق، يمكن تلخيص أبرز الأدوار التي تؤديها منظومة التدريب والتوعية والرقابة في الحد من استخدام الذكاء الاصطناعي الظلي وتعزيز الامتثال للسياسات التنظيمية فيما يأتي:
- (1) التدريب يوضح للموظف حدود الاستخدام المسموح والممنوع.
 - (2) التوعية تقلل المخالفات غير المقصودة الناتجة عن الجهل بحساسية البيانات.
 - (3) الرقابة تكتشف أنماط الاستخدام غير المعتمد وتساعد في تحسين السياسة.
 - (4) التدقيق يربط بين الاستخدام الفعلي وسجل المخاطر والحوادث المحتملة.
 - (5) التحديث الدوري يضمن بقاء السياسة مناسبة مع تطور أدوات الذكاء الاصطناعي.

المبحث الخامس: النظريات المفسرة والنموذج المفاهيمي

2.5.1 نظرية النظم الاجتماعية التقنية:

تعد نظرية النظم الاجتماعية التقنية مدخلًا ملائمًا لهذه الدراسة لأنها تفسر الأداء والمخاطر بوصفها نتاجًا لتفاعل التقنية مع الإنسان والتنظيم. فالذكاء الاصطناعي الظلي لا ينتج فقط عن خصائص الأداة، بل عن حاجة الموظف، وضغط الوقت، وغياب البدائل، وثقافة المؤسسة، ومستوى الحوكمة. لذلك فإن الأثر على الكفاءة التشغيلية أو أمن البيانات لا يمكن تفسيره من خلال الأداة وحدها، بل من خلال النظام الاجتماعي التقني المحيط بها (المعهد الوطني للمعايير والتقنية، 2023).

2.5.2 إطار التكنولوجيا والتنظيم والبيئة TOE:

يساعد إطار التكنولوجيا والتنظيم والبيئة TOE في تفسير تبني التقنيات داخل المؤسسات من خلال ثلاثة أبعاد: البعد التقني، والبعد التنظيمي، والبعد البيئي. وفي هذه الدراسة يظهر البعد التقني في سهولة أدوات الذكاء الاصطناعي التوليدي وفائدتها، ويظهر البعد التنظيمي في السياسات والحوكمة والتدريب، ويظهر البعد البيئي في متطلبات الامتثال والتنافسية والتحول الرقمي. ومن ثم يفسر الإطار لماذا قد يستخدم الموظفون أدوات غير معتمدة عندما تتفوق سهولة الأداة على نضج الضبط المؤسسي.

2.5.3 نظرية الموارد والقدرات الديناميكية:

تنظر نظرية الموارد والقدرات الديناميكية إلى التقنية والبيانات والمهارات والحوكمة بوصفها قدرات مؤسسية يمكن أن تحقق ميزة إذا أُديرَت بفاعلية. ووفق هذا المدخل، فإن الذكاء الاصطناعي لا يصبح مصدر كفاءة إلا عندما تمتلك المؤسسة قدرة على استكشاف فرصه، ودمجه في العمليات، وإعادة تشكيل السياسات والمهارات والضوابط بما يناسبه. أما إذا تُرك الاستخدام فرديًا وغير مرئي فقد تتحول القدرة التقنية إلى مصدر خطر بدلًا من مصدر قيمة.

2.5.4 نموذج قبول التقنية وسلوك المستخدم:

يفسر نموذج قبول التقنية اتجاه الموظفين إلى استخدام الأدوات التي يدركون أنها سهلة ومفيدة. وبناءً عليه، فإن انتشار الذكاء الاصطناعي الظلي يرتبط غالبًا بالفائدة المدركة وسهولة الاستخدام، لا بقرار مؤسسي رسمي. فإذا رأى الموظف أن الأداة العامة أسرع وأسهل من الأدوات الرسمية، فقد يلجأ إليها رغم غياب الاعتماد. ومن هنا تتضح أهمية تقديم بدائل مؤسسية

سهلة وأمنة لا تقل فاعلية عن الأدوات العامة (مايكروسوفت ولينكدان، 2024؛ أي بي إم، 2025).

2.5.5 مدخل إدارة المخاطر:

ينطلق مدخل إدارة المخاطر من أن الهدف ليس إلغاء المخاطر تمامًا، بل تحديدها وتحليلها وترتيبها ومعالجتها ومراقبتها. وهذا المدخل مناسب للذكاء الاصطناعي الظلي لأن الاستخدام غير الرسمي لن يختفي بمجرد المنع، بل يحتاج إلى تحويله من ممارسة غير مرئية إلى ممارسة قابلة للرصد والمعالجة. ولذلك تقترح الدراسة أن تُدار مخاطر الذكاء الاصطناعي الظلي من خلال سجل مخاطر يتضمن نوع الاستخدام، ونوع البيانات، واحتمال الخطر، وأثره، والضابط المناسب (الهيئة الوطنية للأمن السيبراني، 2024؛ المعهد الوطني للمعايير والتقنية، 2023).

جدول (2-14): النظريات المفسرة وعلاقتها بمتغيرات الدراسة

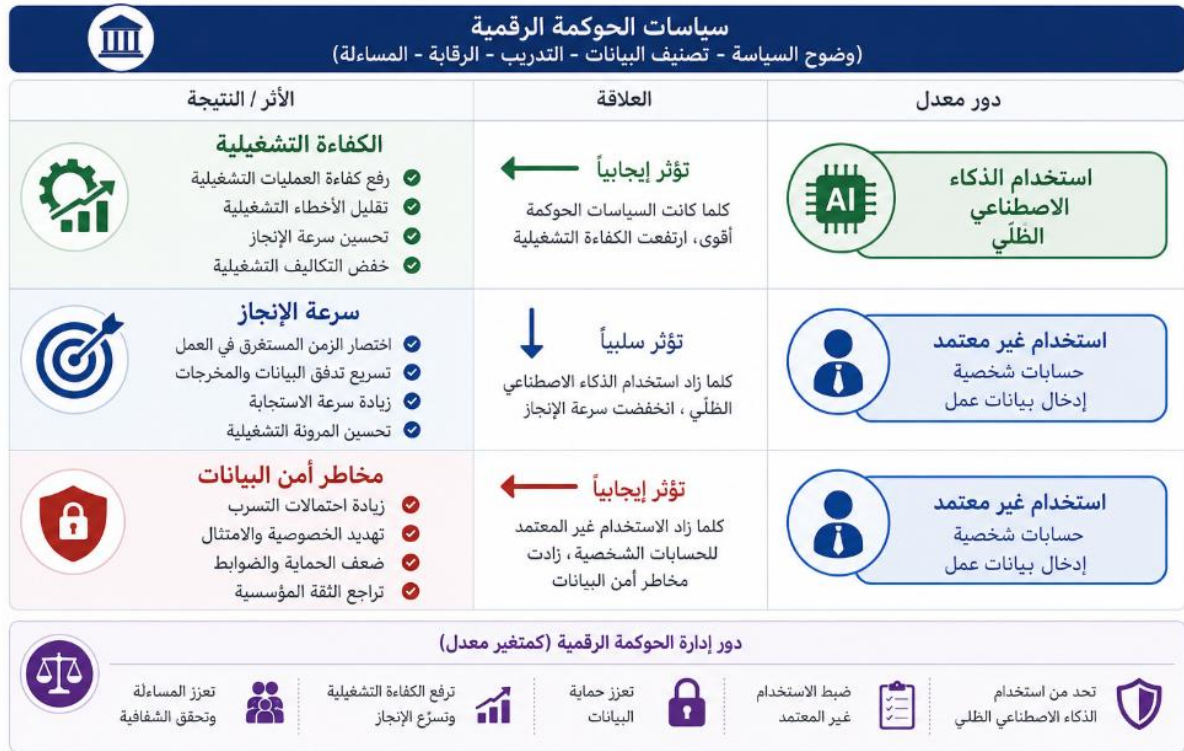
النظرية / المدخل	ما الذي يفسره؟	ارتباطه بمتغيرات الدراسة
النظم الاجتماعية التقنية	تفاعل التقنية مع الإنسان والتنظيم.	يفسر لماذا يختلف أثر الذكاء الاصطناعي الظلي حسب الثقافة والسياسات والمهارات.
TOE	أثر العوامل التقنية والتنظيمية والبينية في التبني.	يفسر دوافع استخدام أدوات غير معتمدة في ظل ضغط بيئي وضعف تنظيمي.
الموارد والقدرات الديناميكية	تحويل التقنية والبيانات إلى قدرة مؤسسية.	يفسر كيف تعزز الحوكمة تحويل الذكاء الاصطناعي إلى كفاءة مستدامة.
قبول التقنية	سلوك المستخدم بناءً على الفائدة والسهولة.	يفسر ميل الموظف إلى استخدام أدوات شخصية سهلة وسريعة.
إدارة المخاطر	تحديد المخاطر ومعالجتها ورقابتها.	يفسر دور الحوكمة في خفض مخاطر أمن البيانات.

المصدر: إعداد الباحث بالاستناد إلى الأدبيات النظرية وأطر الحوكمة والمخاطر.

2.5.6 النموذج المفاهيمي المعدل 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.

شكل (2-4): النموذج المفاهيمي المعدل للعلاقة بين متغيرات الدراسة



*المصدر: إعداد الباحث بالاستناد إلى متغيرات الدراسة وأطر الحوكمة الرقمية.

جدول (2-15): ترجمة النموذج المفاهيمي إلى علاقات بحثية قابلة للاختبار

العلاقة	التفسير النظري	الدلالة المنهجية
الذكاء الاصطناعي الظلي ← الكفاءة التشغيلية	قد يحسن السرعة والجودة وتقليل الجهد في المهام المعرفية.	تختبر بانحدار أثر المتغير المستقل على الكفاءة.
الذكاء الاصطناعي الظلي ← مخاطر أمن البيانات	قد يرفع مخاطر التسرب والخصوصية والامتثال بسبب الاستخدام غير المعتمد.	تختبر بانحدار أثر المتغير المستقل على المخاطر.
الحكومة الرقمية × الذكاء الاصطناعي الظلي ← الكفاءة	السياسات قد تحول الاستخدام إلى ممارسة آمنة ومنتجة.	تختبر بأثر التفاعل أو الانحدار الهرمي.
الحكومة الرقمية × الذكاء الاصطناعي الظلي ← المخاطر	السياسات والتصنيف والرقابة تخفف الأثر السلبي على البيانات.	تختبر بأثر التفاعل بين المتغير المستقل والمعدل.

المصدر: إعداد الباحث بالاستناد إلى النموذج المفاهيمي للدراسة.

2.5.7 خلاصة الإطار النظري:

يخلص الإطار النظري إلى أن الذكاء الاصطناعي الظلي ظاهرة مركبة تجمع بين فرصة تشغيلية ومخاطر أمنية. فمن ناحية، يمكن أن يرفع الكفاءة التشغيلية من خلال تسريع إنجاز الأعمال المعرفية وتقليل الجهد وتحسين جودة المخرجات. ومن ناحية أخرى، قد يرفع مخاطر أمن البيانات إذا تضمن إدخال بيانات حساسة أو شخصية في أدوات عامة أو استخدام حسابات شخصية غير قابلة للتتبع. لذلك يمثل متغير سياسات الحكومة الرقمية عنصراً حاسماً في تفسير العلاقة بين الاستخدام والنتائج؛ فهو لا يمنع الابتكار، بل يضبطه ويجعله مسؤولاً وقابلًا للقياس.

وبناءً على ما سبق، فإن الدراسة الحالية لا تنظر إلى الذكاء الاصطناعي الظلي بوصفه ممارسة خاطئة دائماً أو مفيدة دائماً، بل بوصفه ممارسة تتوقف نتائجها على سياق الاستخدام ومستوى الوعي ونضج الحكومة. وهذا التوازن هو ما يميز النموذج البحثي المقترح، لأنه يجمع بين سؤال الكفاءة وسؤال المخاطر وسؤال الحكومة في نموذج واحد.

ثانياً : الدراسات السابقة :

أولاً: الدراسات العربية

جدول (5) : ملخص الدراسات العربية ذات الصلة

الباحث/السنة	العنوان	الهدف	المنهج	العينة/ال مجال	أبرز النتائج	أبرز التوصيات
ثريا وبركات واليازجي (2021)	دور الذكاء الاصطناعي في تطوير الحوكمة في المؤسسات الحكومية	التعرف على دور الذكاء الاصطناعي في تطوير الحوكمة	وصفي تحليلي/اس تبانة	20 موظفًا	وجود علاقة دالة بين النظم الخبرة وتطوير الحوكمة	تعزيز توظيف الذكاء الاصطناعي في العمل الحكومي
عباس(2017)	حوكمة تكنولوجيا المعلومات كتوجه استراتيجي لتخفيض مخاطر أمن المعلومات	بيان دور حوكمة تقنية المعلومات في تقليل المخاطر	تحليلي	أدبيات ومفاهيم	الحوكمة التقنية تساعد في تقليل مخاطر أمن المعلومات	تبني الحوكمة كخيار استراتيجي لحماية المعلومات
العتيبي(2025)	أثر تطبيق استراتيجيات الذكاء الاصطناعي على التميز المؤسسي	قياس أثر استراتيجيات الذكاء الاصطناعي على التميز المؤسسي	وصفي ارتباطي/ ستبانة	211 إداريًا وإدارية	أثر إيجابي للذكاء الاصطناعي على التميز المؤسسي	نشر ثقافة الابتكار والتحول الرقمي
الراحلة (2025)	دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني	توضيح دور الذكاء الاصطناعي في إدارة مخاطر الأمن السيبراني	تحليلي	أطر وسيناريوه ات	يدعم الذكاء الاصطناعي الاكتشاف والاستجابة والامتثال	تطوير أطر حوكمة وامتثال

تطوير سياسات وضوابط للاستخدام الآمن	يسهم في الإنتاجية وخفض التكاليف وتسريع البرمجيات	خبراء وقيادات ومصادر ثانوية	تحليلي/اس تشرافي	تقييم أثر وتحديات الذكاء الاصطناعي التوليدي في الحكومة الرقمية	الذكاء الاصطناعي التوليدي في أعمال الحكومة الرقمية	هيئة الحكومة الرقمية (2025)
توسيع الاستثمار في تطبيقات الذكاء الاصطناعي المدروسة	أثر إيجابي على الكفاءة وخفض التكاليف	شركة أكاكوس للعمليات النفطية	دراسة حالة	تحليل مساهمة تطبيقات الذكاء الاصطناعي في الكفاءة التشغيلية	ممارسة تطبيقات الذكاء الاصطناعي وتحسين الكفاءة التشغيلية وتقليل التكاليف	بن حليم (2025)
اعتماد تدريجي مدعوم بالحكومة والتأهيل	ارتباط الذكاء الاصطناعي بالكفاءة والاستدامة التشغيلية	أدبيات ومصادر ثانوية	وصفي تحليلي	تحليل علاقة الذكاء الاصطناعي بالأداء التشغيلي في الموانئ	أثر الذكاء الاصطناعي في تحول الأداء التشغيلي في الموانئ البحرية	النعال (2026)

المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة.

ثانياً: الدراسات الأجنبية :

جدول (6) : ملخص الدراسات الأجنبية ذات الصلة

أبرز التوصيات	أبرز النتائج	العينة/المجال	المنهج	الهدف	العنوان	الباحث/السنة
دراسة الأثر حسب نوع المهمة والخبرة	خفض وقت الإنجاز ورفع جودة المخرجات	444مهنياً	تجريبي	قياس أثر ChatGPT على إنتاجية مهام الكتابة	Experimental Evidence on the Productivity Effects of Generative AI	Noy & Zhang (2023)

زيادة الإنتاجية بنحو 15% مع أثر أكبر على الأقل خبرة	5172 موظف دعم	ميداني كمي	قياس أثر مساعد ذكي في خدمة العملاء	Generative AI at Work	Brynjolfsson et al. (2025)
تحسن الأداء داخل حدود التقنية وانخفاضه خارجها	758 مستشارًا	تجربة ميدانية	تحليل أثر GPT-4 على الأعمال المعرفية	Navigating the Jagged Technological Frontier	Dell'Acqua et al. (2023)
انتشار BYOAI واستخدام الأدوات الخاصة	31000 عامل معرفي	مسح عالمي	تحليل واقع استخدام الذكاء الاصطناعي في العمل	Work Trend Index	Microsoft & LinkedIn (2024)
إطار حوكمة مرن يضبط المخاطر دون منع الابتكار	الاستخدام غير الرسمي يتجاوز قدرة المؤسسات على الرقابة	45 دراسة و 345 مهنيًا	مراجعة ومسح	BYOAI in the Workplace	Anthuvan et al. (2025)
دمج إدارة المخاطر في دورة حياة AI	تركيز على الحوكمة والقياس والإدارة والمراجعة	منظمات تستخدم أو تطور AI	إطار معياري	تقديم إطار لإدارة مخاطر الذكاء الاصطناعي	AI Risk Management Framework NIST (2023)

المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة.

2.39 أوجه التشابه والاختلاف والاستفادة والفجوة البحثية:

تشابه الدراسة الحالية مع الدراسات السابقة في اهتمامها بأثر الذكاء الاصطناعي على الأداء والكفاءة والحوكمة والمخاطر. فهي تلتقي مع الدراسات التجريبية الأجنبية في تأكيد إمكانية رفع الإنتاجية وتحسين جودة المخرجات عند استخدام أدوات الذكاء الاصطناعي في مهام معرفية محددة، كما تلتقي مع الدراسات العربية والرسمية في إبراز أهمية الحوكمة وضبط المخاطر الرقمية. غير أن الدراسة الحالية تختلف في تركيزها على الاستخدام غير الرسمي أو غير المعتمد، وليس على الذكاء الاصطناعي الرسمي وحده.

وتتمثل أوجه الاختلاف الأساسية في أن هذه الدراسة تجمع بين أثرين متوازيين: أثر إيجابي محتمل على الكفاءة التشغيلية، وأثر سلبي محتمل على مخاطر أمن البيانات. كما أنها لا تدرس سياسات الحوكمة الرقمية كمتغير مستقل فقط، بل تختبرها كمتغير معدل يغير قوة واتجاه العلاقة بين الاستخدام الظلي والنتائج التشغيلية والأمنية. وهذا يجعل النموذج المقترح أكثر قدرة على تفسير الواقع العملي الذي قد يجمع بين القيمة والخطر في الوقت ذاته.

أما الفجوة البحثية فتظهر في ندرة الدراسات العربية التي تناولت مفهوم الذكاء الاصطناعي الظلي صراحة، وفي محدودية النماذج التي تربطه بالكفاءة التشغيلية ومخاطر أمن البيانات في نموذج واحد. ومن ثم تسعى الدراسة الحالية إلى تقديم إضافة نظرية وتطبيقية من خلال بناء نموذج يفسر كيف يمكن للمؤسسة أن تستفيد من الاستخدام الذكي للأدوات الحديثة، مع تقليل مخاطر إدخال البيانات الحساسة أو الاعتماد على مخرجات غير موثوقة أو مخالفة السياسات.

الفصل الثالث: منهجية الدراسة وإجراءاتها

تمهيد:

يتناول هذا الفصل الإجراءات المنهجية التي تعتمد عليها الدراسة في اختبار أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات، مع قياس الدور المعدل لسياسات الحوكمة الرقمية. ويعرض الفصل منهج الدراسة، وتصميمها، ومجتمعها وعينتها، وأداة جمع البيانات، وطرق التحقق من صدق الأداة وثباتها، وأساليب التحليل الإحصائي، إضافة إلى الاعتبارات الأخلاقية المرتبطة بجمع البيانات من المشاركين. وتكتسب منهجية هذه الدراسة أهمية خاصة بسبب حساسية موضوعها؛ إذ يتناول البحث استخدام أدوات ذكاء اصطناعي قد لا تكون معتمدة رسميًا داخل بيئة العمل. لذلك روعي في تصميم الأداة أن تكون العبارات موضوعية ومحيدة، وأن تقيس الظاهرة دون اتهام المشاركين أو دفعهم إلى الإفصاح عن معلومات سرية تخص جهات عملهم.

3.1 منهج الدراسة:

تعتمد الدراسة على المنهج الوصفي التحليلي، لملاءمته لطبيعة الموضوع وأهدافه؛ إذ يسعى البحث إلى وصف مستوى استخدام الذكاء الاصطناعي الظلي في بيئة العمل، وتحليل علاقته بكل من الكفاءة التشغيلية ومخاطر أمن البيانات، ثم اختبار أثر سياسات الحوكمة الرقمية بوصفها متغيرًا معدلاً في هذه العلاقة.

ويُعد هذا المنهج مناسباً للدراسات الإدارية والتطبيقية التي تهدف إلى قياس اتجاهات أفراد العينة وتحليل العلاقات بين المتغيرات باستخدام أساليب إحصائية منظمة. كما أنه لا يقتصر على وصف الظاهرة، بل يمتد إلى تفسير العلاقات بين أبعادها بما يساعد في بناء نتائج قابلة للمناقشة والتطبيق.

3.2 تصميم الدراسة:

تتبع الدراسة تصميمًا كمياً مقطوعياً؛ حيث يتم جمع البيانات من أفراد العينة في فترة زمنية واحدة باستخدام الاستبانة. ويُناسب هذا التصميم طبيعة الدراسة التي تهدف إلى قياس اتجاهات العاملين نحو استخدام الذكاء الاصطناعي الظلي، ومدى انعكاسه على الكفاءة التشغيلية ومخاطر أمن البيانات.

كما يمكن وصف الدراسة بأنها ارتباطية تفسيرية؛ لأنها لا تكتفي بقياس مستوى المتغيرات، بل تختبر طبيعة العلاقات والأثر بين المتغير المستقل والمتغيرات التابعة، مع اختبار الدور المعدل لسياسات الحوكمة الرقمية.

3.3 مجتمع الدراسة:

يتكون مجتمع الدراسة من العاملين في المؤسسات التي تعتمد في أعمالها على الأنظمة الرقمية أو أدوات الذكاء الاصطناعي أو تطبيقات التحول الرقمي. ويشمل ذلك العاملين في الإدارات الإدارية، والتشغيلية، وتقنية المعلومات، وأمن المعلومات، والتحول الرقمي، وخدمة العملاء، وغيرها من الإدارات ذات الصلة.

ويمكن تطبيق الدراسة ميدانيًا على إحدى الفئات الآتية، بحسب نطاق الرسالة وإمكانات الباحث:

1. العاملون في المؤسسات الحكومية ذات الطابع الرقمي.
 2. العاملون في البنوك والمؤسسات المالية.
 3. العاملون في شركات الاتصالات أو التقنية.
 4. العاملون في الجامعات أو المؤسسات التعليمية.
 5. العاملون في الشركات الخدمية التي تعتمد على الأنظمة الرقمية.
- ويُفضل أن يحدد الباحث في النسخة النهائية جهة أو قطاعًا واضحًا حتى تكون نتائج الدراسة أكثر دقة وقابلية للتفسير.

3.4 عينة الدراسة:

تعتمد الدراسة على عينة من العاملين الذين لديهم تعامل مباشر أو غير مباشر مع الأدوات الرقمية أو تطبيقات الذكاء الاصطناعي في بيئة العمل. ويمكن اختيار العينة بإحدى الطريقتين:

1. العينة العشوائية الطبقية إذا توافرت قوائم رسمية بالعاملين موزعة بحسب الإدارات أو المستويات الوظيفية.
2. العينة القصدية إذا كان الباحث يستهدف فئة محددة ممن يستخدمون الأدوات الرقمية أو يتعاملون مع البيانات والأنظمة التقنية.

ويقترح أن يتراوح حجم العينة بين 250 و300 مفردة كحد مناسب للتحليل الإحصائي باستخدام الارتباط والانحدار، مع إمكانية زيادة العدد إذا أراد الباحث استخدام نمذجة المعادلات الهيكلية.

3.5 أداة الدراسة:

تعتمد الدراسة على الاستبانة بوصفها الأداة الرئيسة لجمع البيانات، وذلك لملاءمتها لطبيعة المنهج الكمي، وقدرتها على الوصول إلى عدد مناسب من أفراد العينة خلال فترة زمنية محددة.

وتتكون الاستبانة من خمسة أقسام رئيسة:

جدول (1-3): محاور الاستبانة المقترحة

القسم	المحتوى	الغرض من القياس
القسم الأول	البيانات العامة	وصف خصائص أفراد العينة
القسم الثاني	استخدام الذكاء الاصطناعي الظلي	قياس درجة استخدام أدوات غير معتمدة أو غير مصرح بها
القسم الثالث	الكفاءة التشغيلية	قياس السرعة، الجودة، تقليل الوقت، وتحسين تدفق العمل
القسم الرابع	مخاطر أمن البيانات	قياس مخاطر التسرب، الخصوصية، الامتثال، وصعوبة التتبع
القسم الخامس	سياسات الحوكمة الرقمية	قياس وضوح السياسات، التدريب، الرقابة، وتصنيف البيانات

المصدر: إعداد الباحث.

3.6 مقياس الاستجابة:

تعتمد الاستبانة على مقياس ليكرت الخماسي، لأنه من أكثر المقاييس استخدامًا في الدراسات الإدارية والاجتماعية، ويتيح قياس درجة موافقة أفراد العينة على فقرات الأداة.

جدول (2-3): مقياس ليكرت الخماسي

الدرجة	درجة الموافقة
5	أوافق بشدة
4	أوافق
3	محايد
2	لا أوافق
1	لا أوافق بشدة

ولتفسير المتوسطات الحسابية، يمكن اعتماد المعيار الآتي:

المتوسط الحسابي	مستوى التقدير
1.00 – 1.80	منخفض جدًا
1.81 – 2.60	منخفض
2.61 – 3.40	متوسط
3.41 – 4.20	مرتفع
4.21 – 5.00	مرتفع جدًا

المصدر: إعداد الباحث.

3.7 بناء الاستبانة:

تم بناء الاستبانة في ضوء مشكلة الدراسة وأهدافها وفرضياتها، وبالاستفادة من الأدبيات ذات الصلة بالذكاء الاصطناعي في بيئة العمل، وأمن البيانات، والحوكمة الرقمية. وقد روعي في صياغة الفقرات ما يأتي:

1. أن تكون العبارات واضحة ومباشرة.
2. أن تقيس كل فقرة بُعدًا محددًا من أبعاد الدراسة.
3. أن تتجنب العبارات الاتهامية أو الحساسة.
4. ألا تطلب من المشاركون الإفصاح عن بيانات سرية تخص جهة عمله.
5. أن تكون الفقرات مناسبة للموظفين غير المتخصصين تقنيًا.

3.8 صدق أداة الدراسة:

للتحقق من صدق الأداة، تعتمد الدراسة على أكثر من إجراء، وذلك على النحو الآتي:

3.8.1 الصدق الظاهري:

يتم التأكد من أن فقرات الاستبانة واضحة من حيث اللغة والصياغة، وأنها مناسبة للمبحوثين، ولا تحمل غموضاً أو لبساً في المعنى.

3.8.2 صدق المحتوى:

تُعرض الاستبانة على مجموعة من المحكمين المتخصصين في الإدارة، وتقنية المعلومات، وأمن البيانات، والذكاء الاصطناعي، للتحقق من مناسبة الفقرات لأبعاد الدراسة. وبعد استلام ملاحظات المحكمين، يتم تعديل الفقرات بالحذف أو الإضافة أو إعادة الصياغة وفق ما تقتضيه الملاحظات العلمية.

3.8.3 الصدق البنائي:

بعد جمع البيانات، يمكن التحقق من الصدق البنائي باستخدام معاملات الارتباط بين الفقرات والمحاور التي تنتمي إليها، أو من خلال التحليل العاملي إذا كان حجم العينة مناسباً.

3.9 ثبات أداة الدراسة:

يُقاس ثبات الأداة باستخدام معامل كرونباخ ألفا للتحقق من الاتساق الداخلي لفقرات كل محور من محاور الاستبانة. ويُعد معامل الثبات مقبولاً إذا بلغ 0.70 فأكثر، بينما تشير القيم الأعلى إلى درجة أفضل من الاتساق الداخلي.

ويمكن إجراء دراسة استطلاعية أولية على عينة محدودة تتراوح بين 30 و50 مشاركاً قبل التطبيق النهائي، بهدف التأكد من وضوح الفقرات وثبات الأداة وإجراء التعديلات اللازمة.

3.10 إجراءات جمع البيانات:

تمر عملية جمع البيانات بعدة خطوات منظمة، تتمثل في الآتي:

1. إعداد الاستبانة في صورتها الأولية.
2. عرض الاستبانة على المحكمين.
3. تعديل الأداة بناءً على ملاحظات التحكيم.

4. تطبيق الاستبانة استطلاعياً للتأكد من وضوحها وثباتها.
5. توزيع الاستبانة إلكترونياً على أفراد العينة.
6. توضيح هدف الدراسة للمشاركين قبل الإجابة.
7. استبعاد الاستجابات غير المكتملة أو غير الصالحة للتحليل.
8. ترميز البيانات وإدخالها في البرنامج الإحصائي.
9. إجراء التحليلات الإحصائية المناسبة لاختبار الفرضيات.

3.11 أنواع البيانات:

تعتمد الدراسة على نوعين من البيانات:

أولاً: البيانات الأولية:

وهي البيانات التي يجمعها الباحث مباشرة من أفراد العينة باستخدام الاستبانة، وتشمل استجاباتهم حول استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، وسياسات الحوكمة الرقمية.

ثانياً: البيانات الثانوية:

وتتمثل في الكتب، والدراسات السابقة، والتقارير الرسمية، والمعايير ذات الصلة بموضوع الدراسة، مثل أدبيات الذكاء الاصطناعي، وأمن المعلومات، وحوكمة البيانات، وحوكمة الذكاء الاصطناعي.

3.12 أساليب التحليل الإحصائي:

تستخدم الدراسة برنامجاً إحصائياً مثل SPSS، ويمكن دعم التحليل ببرامج أخرى مثل AMOS أو SmartPLS إذا اقتضت طبيعة التحليل ذلك. وتشمل الأساليب الإحصائية المقترحة ما يأتي:

جدول (3-3): أساليب التحليل الإحصائي المقترحة

الأسلوب الإحصائي	الغرض من التحليل
التكرارات والنسب المئوية	وصف خصائص العينة
المتوسطات الحسابية والانحرافات المعيارية	تحديد مستوى المتغيرات
معامل ارتباط بيرسون	قياس العلاقة بين المتغيرات

الأسلوب الإحصائي	الغرض من التحليل
الانحدار الخطي البسيط أو المتعدد	اختبار أثر الذكاء الاصطناعي الظلي على الكفاءة التشغيلية
الانحدار الخطي البسيط أو المتعدد	اختبار أثر الذكاء الاصطناعي الظلي على مخاطر أمن البيانات
الانحدار الهرمي وتحليل أثر التفاعل	اختبار الدور المعدل للحكومة الرقمية
اختبار (T) وتحليل التباين الأحادي ANOVA	اختبار الفروق بين أفراد العينة

المصدر: إعداد الباحث.

3.13 ربط الفرضيات بالتحليل الإحصائي:

جدول (3-4): ربط فرضيات الدراسة بالاختبارات الإحصائية

الاختبار المناسب	مضمون الفرضية	الفرضية
الانحدار الخطي	أثر الذكاء الاصطناعي الظلي على الكفاءة التشغيلية	H1
الانحدار الخطي	أثر الذكاء الاصطناعي الظلي على مخاطر أمن البيانات	H2
الانحدار الهرمي	الدور المعدل للحكومة الرقمية في العلاقة بين الذكاء الاصطناعي الظلي والكفاءة التشغيلية	H3
الانحدار الهرمي	الدور المعدل للحكومة الرقمية في العلاقة بين الذكاء الاصطناعي الظلي ومخاطر أمن البيانات	H4
T-test / ANOVA	الفروق في استجابات العينة وفق المتغيرات الديموغرافية	H5

المصدر: إعداد الباحث.

3.14 الاعتبارات الأخلاقية:

- نظرًا لحساسية موضوع الدراسة وارتباطه بممارسات استخدام أدوات الذكاء الاصطناعي في بيئة العمل، تلتزم الدراسة بعدد من الضوابط الأخلاقية، وهي:
1. توضيح هدف الدراسة للمشاركين قبل الإجابة عن الاستبانة.
 2. التأكيد على أن المشاركة اختيارية.
 3. عدم جمع أسماء المشاركين أو بيانات تعريفية مباشرة.
 4. عدم طلب أي مستندات أو بيانات سرية تخص المؤسسات.
 5. استخدام البيانات لأغراض البحث العلمي فقط.
 6. حفظ البيانات بطريقة آمنة.
 7. عرض النتائج بصورة إجمالية دون الإشارة إلى أفراد أو جهات بعينها.
 8. إتاحة حق الانسحاب من المشاركة دون أي أثر سلبي.

3.15 حدود المنهجية:

- رغم ملاءمة المنهج الوصفي التحليلي لطبيعة الدراسة، إلا أن هناك بعض الحدود المنهجية التي ينبغي الإشارة إليها، ومنها:
1. اعتماد الدراسة على الاستبانة يجعل النتائج مرتبطة بأراء المشاركين وتقديراتهم الذاتية.
 2. التصميم المقطعي يقيس الظاهرة في فترة زمنية محددة، ولا يتابع تغيرها عبر الزمن.
 3. قد يتحفظ بعض المشاركين عند الإجابة بسبب حساسية موضوع الذكاء الاصطناعي الظلي.
 4. لا تقيس الدراسة الاستخدام الفعلي للأدوات التقنية من خلال سجلات النظام، بل تقيسه من خلال استجابات أفراد العينة.
- ومع ذلك، فإن هذه الحدود لا تقلل من قيمة الدراسة، لكنها تساعد في تفسير النتائج بدقة وتحديد مجال تعميمها.

خاتمة الفصل :

عرض هذا الفصل المنهجية التي تعتمد عليها الدراسة في اختبار العلاقة بين استخدام الذكاء الاصطناعي الظلي والكفاءة التشغيلية ومخاطر أمن البيانات، مع تحليل الدور المعدل لسياسات الحوكمة الرقمية. وقد تم تحديد المنهج الوصفي التحليلي، وتصميم الدراسة، ومجتمعها وعينتها، وأداة جمع البيانات، وإجراءات الصدق والثبات، وأساليب التحليل الإحصائي، والاعتبارات الأخلاقية. ويمثل هذا الفصل الأساس الإجرائي الذي سيتم من خلاله الانتقال إلى جمع البيانات وتحليلها وعرض نتائج الدراسة في الفصل اللاحق.

الفصل الرابع: عرض النتائج وتحليلها ومناقشتها

تمهيد:

يعرض هذا الفصل نتائج التحليل الإحصائي للبيانات المرتبطة بمتغيرات الدراسة، والمتمثلة في: استخدام الذكاء الاصطناعي الظلي، والكفاءة التشغيلية، ومخاطر أمن البيانات، وسياسات الحوكمة الرقمية. ويبدأ الفصل بوصف خصائص العينة، ثم التحقق من ثبات أداة الدراسة، ثم عرض المتوسطات الحسابية والانحرافات المعيارية، وتحليل علاقات الارتباط والانحدار، واختبار الدور المعدل لسياسات الحوكمة الرقمية. كما يتضمن الفصل مناقشة النتائج في ضوء الإطار النظري والدراسات السابقة.

ويجب التنبيه إلى أن النتائج الواردة في هذا الفصل تمثل نموذجًا تحليليًا تطبيقيًا يصلح للبناء عليه عند إدخال البيانات الميدانية الفعلية، مع إمكانية تعديل القيم والجداول وفقًا لما تسفر عنه الاستبانات بعد جمعها وتحليلها.

4.1 خصائص عينة الدراسة:

يوضح الجدول الآتي الخصائص الديموغرافية والمهنية لأفراد العينة في النموذج التطبيقي. وقد بلغ عدد أفراد العينة 320 مشاركًا، وهو حجم مناسب لإجراء التحليلات الإحصائية الأساسية مثل المتوسطات، ومعاملات الارتباط، وتحليل الانحدار.

جدول (1-4): 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%

المتغير	الفئة	التكرار	النسبة المئوية
طبيعة العمل	تقنية معلومات / أمن بيانات	92	28.8%
طبيعة العمل	تحول رقمي / تطوير أعمال	82	25.6%

المصدر: إعداد الباحث.

يتضح من الجدول أن العينة تضم تنوعاً مناسباً من حيث الجنس والعمر والمؤهل وطبيعة العمل، وهو ما يعزز ملاءمة البيانات لتحليل موضوع الدراسة؛ إذ إن استخدام الذكاء الاصطناعي الظلي لا يرتبط بفئة وظيفية واحدة، بل قد يظهر في الوظائف الإدارية والتشغيلية والتقنية على حد سواء. كما أن تمثيل العاملين في تقنية المعلومات وأمن البيانات والتحول الرقمي يمنح النتائج بعداً مهماً، لأن هذه الفئات أكثر قرباً من قضايا الحوكمة والمخاطر الرقمية.

4.2 اختبار ثبات أداة الدراسة :

تم التحقق من ثبات أداة الدراسة باستخدام معامل كرونباخ ألفا، وذلك لقياس الاتساق الداخلي لفقرات الاستبانة. ويُعد معامل الثبات مقبولاً إذا تجاوز 0.70، بينما تشير القيم الأعلى إلى درجة أفضل من الاعتمادية.

جدول (4-2): معاملات الثبات لمحاور الاستبانة

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.

تشير القيم السابقة إلى أن أداة الدراسة تتمتع بدرجة عالية من الثبات، مما يعني أن فقرات كل محور تقيس المفهوم نفسه بدرجة جيدة من الاتساق الداخلي. كما أن ارتفاع معامل الثبات للأداة ككل إلى 0.93 يدل على صلاحية الاستبانة للاستخدام في القياس الإحصائي، مع مراعاة استكمال إجراءات الصدق الظاهري وصدق المحتوى من خلال التحكيم العلمي.

4.3 المتوسطات الحسابية لمتغيرات الدراسة :

تم استخدام المتوسطات الحسابية والانحرافات المعيارية لتحديد مستوى إدراك أفراد العينة لمتغيرات الدراسة. ويعرض الجدول الآتي النتائج العامة لكل متغير.

جدول (4-3): 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.

توضح النتائج أن الكفاءة التشغيلية جاءت في المرتبة الأولى بمتوسط حسابي مرتفع، مما يشير إلى أن المشاركين يدركون وجود أثر إيجابي لاستخدام أدوات الذكاء الاصطناعي في تحسين سرعة الإنجاز وجودة المخرجات وتقليل الوقت والجهد. وجاءت مخاطر أمن البيانات في المرتبة الثانية بمستوى مرتفع، وهو ما يعكس وعياً واضحاً بالمخاطر التي قد تنتج عن استخدام أدوات غير معتمدة أو إدخال بيانات العمل في منصات عامة.

أما استخدام الذكاء الاصطناعي الظلي فقد جاء بمستوى مرتفع، مما يدل على أن الظاهرة ليست هامشية أو محدودة، بل تمثل ممارسة قائمة داخل بيئة العمل الحديثة. في المقابل، جاءت سياسات الحوكمة الرقمية بمستوى متوسط، وهو ما يكشف عن فجوة بين مستوى الاستخدام الفعلي للأدوات الذكية ومستوى نضج السياسات المنظمة لهذا الاستخدام. وتعد هذه النتيجة محورية؛ لأنها تفسر سبب اجتماع الفائدة التشغيلية مع ارتفاع المخاطر الأمنية في الوقت نفسه.

4.4 تحليل أبعاد استخدام الذكاء الاصطناعي الظلي :

جدول (4-4): متوسطات أبعاد استخدام الذكاء الاصطناعي الظلي

البعد	المتوسط	المستوى	قراءة النتيجة
استخدام أدوات غير معتمدة	3.78	مرتفع	يشير إلى انتشار استخدام أدوات عامة خارج الاعتماد الرسمي
استخدام حسابات شخصية	3.44	مرتفع	يعكس وجود ممارسات فردية تحتاج إلى ضبط وتوعية
إدخال بيانات عمل في أدوات عامة	3.28	متوسط	يدل على خطر قائم، لكنه يتفاوت حسب نوع البيانات
غياب الإفصاح عن الاستخدام	3.66	مرتفع	يؤكد وجود فجوة بين الممارسة والسياسات الرسمية
الاعتماد على مخرجات غير مراجعة	3.39	متوسط	يتطلب تعزيز المراجعة البشرية والمسؤولية المهنية

المصدر: إعداد الباحث.

يتضح أن أعلى أبعاد الذكاء الاصطناعي الظلي يتمثل في استخدام أدوات غير معتمدة، وهو ما يعكس سهولة الوصول إلى أدوات الذكاء الاصطناعي العامة مقارنة بالأدوات المؤسسية. كما أن ارتفاع بُعد غياب الإفصاح عن الاستخدام يشير إلى أن جزءاً من الممارسة يتم خارج الرؤية الإدارية والتقنية للمؤسسة، مما يضعف قدرة الإدارات المعنية على تقدير مستوى المخاطر الحقيقي.

وتُظهر النتيجة الخاصة بإدخال بيانات العمل في أدوات عامة أن الخطر قائم، حتى وإن لم يكن في أعلى مستوياته. وهذا يعني أن المؤسسة لا تحتاج فقط إلى منع الاستخدام الخطر، بل إلى توضيح الفروق بين البيانات العامة والداخلية والسرية والحساسة، بما يتوافق مع مبادئ حوكمة البيانات وتصنيفها (سدايا، 2020؛ الهيئة الوطنية للأمن السيبراني، 2018).

4.5 تحليل أبعاد الكفاءة التشغيلية

جدول (4-5): متوسطات أبعاد الكفاءة التشغيلية

البعد	المتوسط	المستوى	قراءة النتيجة
سرعة إنجاز المهام	4.08	مرتفع	أكثر مؤشرات الكفاءة تأثرًا بالأدوات الذكية
تحسين جودة المخرجات	3.91	مرتفع	يرتبط بالتلخيص والتنظيم والصياغة
تقليل الجهد والوقت	3.97	مرتفع	يعكس دور الأتمتة في الأعمال الروتينية
تقليل الأخطاء التشغيلية	3.52	مرتفع	يتطلب مراجعة بشرية لتجنب أخطاء جديدة
تحسين تدفق العمل	3.76	مرتفع	يعكس أثر الأدوات في ترتيب الأولويات وتسريع الاتصالات

تشير النتائج إلى أن أثر الذكاء الاصطناعي يظهر بوضوح في سرعة إنجاز المهام وتقليل الجهد والوقت، وهي نتيجة منطقية في بيئات العمل المعرفية التي تعتمد على الكتابة والتحليل والتلخيص وإعداد التقارير. وتتسق هذه النتيجة مع الدراسات التي بينت أثر الذكاء الاصطناعي التوليدي في رفع الإنتاجية وتحسين جودة بعض المهام المعرفية (نوي وزانغ، 2023؛ براينجولفسون وآخرون، 2025).

ومع ذلك، فإن انخفاض متوسط تقليل الأخطاء التشغيلية نسبيًا مقارنة بسرعة الإنجاز يشير إلى أن الذكاء الاصطناعي لا يضمن الدقة تلقائيًا؛ إذ قد يختصر الوقت، لكنه يحتاج إلى مراجعة بشرية، خصوصًا في التقارير المهمة أو القرارات ذات الأثر الإداري.

4.6 تحليل أبعاد مخاطر أمن البيانات

جدول (4-6): متوسطات أبعاد مخاطر أمن البيانات

البعد	المتوسط	المستوى	قراءة النتيجة
احتمال تسرب البيانات	3.88	مرتفع	أعلى المخاطر المدركة لدى المشاركين
إدخال بيانات حساسة	3.62	مرتفع	يشير إلى حاجة فورية لتصنيف البيانات
ضعف السيطرة على تداول المعلومات	3.80	مرتفع	يعكس مشكلة الرؤية والرقابة
مخاطر الخصوصية	3.77	مرتفع	ترتبط بالبيانات الشخصية وحقوق أصحابها
مخاطر عدم الامتثال	3.65	مرتفع	تتطلب سياسات وإجراءات واضحة ومعلنة

المصدر: إعداد الباحث.

تدل هذه النتائج على أن المشاركين يدركون أن الاستخدام غير المنظم لأدوات الذكاء الاصطناعي لا يمثل مجرد ممارسة تقنية، بل يرتبط بمخاطر أمنية وتنظيمية حقيقية. فقد جاء احتمال تسرب البيانات في المرتبة الأولى، وهو ما يعكس حساسية إدخال بيانات العمل في أدوات عامة قد لا تخضع لسيطرة المؤسسة.

كما تشير النتائج إلى أن مخاطر الخصوصية وعدم الامتثال حاضرة بوضوح، لا سيما في البيئات التي تتعامل مع بيانات العملاء أو الموظفين أو العقود أو المعلومات المالية. وتنسجم هذه النتيجة مع التوجهات الوطنية والدولية التي تؤكد ضرورة حوكمة البيانات، وتصنيفها، وإدارة مخاطر الذكاء الاصطناعي، وتحديد المسؤوليات بوضوح (سدايا، 2023؛ الهيئة الوطنية للأمن السيبراني، 2018؛ المعهد الوطني للمعايير والتقنية، 2023).

4.7 تحليل الارتباط بين متغيرات الدراسة:

تم استخدام معامل ارتباط بيرسون لقياس طبيعة العلاقة بين متغيرات الدراسة. ويوضح الجدول الآتي مصفوفة الارتباط.

جدول (4-7): 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

دالة عند مستوى 0.01.

تظهر النتائج وجود علاقة ارتباط موجبة بين استخدام الذكاء الاصطناعي الظلي والكفاءة التشغيلية بلغت 0.52، وهي علاقة متوسطة موجبة، مما يعني أن زيادة استخدام هذه الأدوات ترتبط بارتفاع إدراك المشاركين لمستوى الكفاءة التشغيلية.

كما تظهر النتائج علاقة موجبة أقوى بين استخدام الذكاء الاصطناعي الظلي ومخاطر أمن البيانات بلغت 0.61، وهي نتيجة مهمة؛ إذ تؤكد أن الاستخدام غير المنظم لا ينتج مكاسب تشغيلية فقط، بل يرتبط أيضاً بارتفاع مستوى المخاطر الأمنية.

أما سياسات الحوكمة الرقمية فقد ارتبطت إيجابياً بالكفاءة التشغيلية، وسلبياً بمخاطر أمن البيانات. وتعني هذه النتيجة أن وجود سياسات واضحة وتدريب ورقابة وتصنيف بيانات يمكن أن يساهم في رفع الكفاءة من جهة، وتقليل المخاطر من جهة أخرى.

4.8 اختبار أثر الذكاء الاصطناعي الظلي على الكفاءة التشغيلية:

لاختبار أثر استخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية، تم استخدام تحليل الانحدار الخطي البسيط، كما يوضح الجدول الآتي.

جدول (4-8): نتائج الانحدار لأثر الذكاء الاصطناعي الظلي على الكفاءة التشغيلية

المتغير المستقل	B	Beta	t	Sig.	R ²	F
استخدام الذكاء الاصطناعي الظلي	0.44	0.52	10.86	0.000	0.27	117.9

تشير النتائج إلى وجود أثر موجب ذي دلالة إحصائية لاستخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية، حيث بلغت قيمة $Beta = 0.52$ ، وهي قيمة تعكس أثرًا متوسطًا يميل إلى القوة. كما بلغت قيمة معامل التفسير $R^2 = 0.27$ ، أي أن استخدام الذكاء الاصطناعي الظلي يفسر نحو 27% من التباين في الكفاءة التشغيلية.

وتعني هذه النتيجة أن الموظفين قد يحققون مكاسب تشغيلية ملموسة من خلال استخدام أدوات الذكاء الاصطناعي، خصوصًا في المهام التي تتطلب سرعة في المعالجة أو تنظيمًا للمعلومات أو تحسينًا للصياغة أو إعدادًا أوليًا للتقارير. وبذلك تُقبل الفرضية التي تنص على وجود أثر ذي دلالة إحصائية لاستخدام الذكاء الاصطناعي الظلي على الكفاءة التشغيلية.

4.9 اختبار أثر الذكاء الاصطناعي الظلي على مخاطر أمن البيانات:

تم استخدام تحليل الانحدار الخطي البسيط لاختبار أثر استخدام الذكاء الاصطناعي الظلي على مخاطر أمن البيانات، كما يوضح الجدول الآتي.

جدول (4-9): نتائج الانحدار لأثر الذكاء الاصطناعي الظلي على مخاطر أمن البيانات

المتغير المستقل	B	Beta	t	Sig.	R ²	F
استخدام الذكاء الاصطناعي الظلي	0.57	0.61	13.72	0.000	0.37	188.2

توضح النتائج وجود أثر موجب ذي دلالة إحصائية لاستخدام الذكاء الاصطناعي الظلي على مخاطر أمن البيانات، حيث بلغت قيمة $Beta = 0.61$ ، وهي قيمة مرتفعة نسبيًا. كما بلغت قيمة معامل التفسير $R^2 = 0.37$ ، أي أن استخدام الذكاء الاصطناعي الظلي يفسر نحو 37% من التباين في مخاطر أمن البيانات.

وتدل هذه النتيجة على أن زيادة الاستخدام غير المنظم لأدوات الذكاء الاصطناعي تقترن بارتفاع مستوى المخاطر، خصوصًا عندما يتم استخدام حسابات شخصية، أو إدخال بيانات عمل في أدوات عامة، أو الاعتماد على مخرجات غير موثقة. وبناءً على ذلك، تُقبل الفرضية التي تنص على وجود أثر ذي دلالة إحصائية لاستخدام الذكاء الاصطناعي الظلي على مخاطر أمن البيانات.

4.10 اختبار الدور المعدل لسياسات الحوكمة الرقمية:

لاختبار الدور المعدل لسياسات الحوكمة الرقمية، تم إدخال متغير التفاعل بين استخدام الذكاء الاصطناعي الظلي وسياسات الحوكمة الرقمية، وذلك لمعرفة ما إذا كانت الحوكمة تغير قوة العلاقة أو اتجاهها.

جدول (4-10): نتائج اختبار الدور المعدل لسياسات الحوكمة الرقمية

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

تشير النتائج إلى أن سياسات الحوكمة الرقمية تؤدي دورًا معدلاً في العلاقة بين استخدام الذكاء الاصطناعي الظلي والكفاءة التشغيلية؛ إذ إن إدخال متغير التفاعل رفع القدرة التفسيرية للنموذج من 0.39 إلى 0.42، وكانت قيمة التفاعل موجبة ودالة إحصائيًا. وهذا يعني أن وجود سياسات واضحة وتدريب ورقابة وأدوات معتمدة لا يلغي الفائدة التشغيلية، بل قد يجعلها أكثر انتظامًا واستدامة.

كما تشير النتائج إلى أن الحوكمة الرقمية تعدل العلاقة بين استخدام الذكاء الاصطناعي الظلي ومخاطر أمن البيانات باتجاه سلبي؛ إذ إن قيمة Beta للتفاعل بلغت -0.21،

وهي دالة إحصائيًا. ويدل ذلك على أن قوة العلاقة بين الذكاء الاصطناعي الظلي ومخاطر أمن البيانات تنخفض عندما ترتفع درجة تطبيق سياسات الحوكمة الرقمية. وبناءً على ذلك، تُقبل الفرضيتان المتعلقةتان بالدور المعدّل لسياسات الحوكمة الرقمية.

4.11 ملخص اختبار الفرضيات:

جدول (4-11): ملخص نتائج اختبار الفرضيات

رقم الفرضية	نص الفرضية المختصر	النتيجة	مستوى الدعم
H1	يوجد أثر للذكاء الاصطناعي الظلي على الكفاءة التشغيلية	مقبولة	مدعومة إحصائيًا
H2	يوجد أثر للذكاء الاصطناعي الظلي على مخاطر أمن البيانات	مقبولة	مدعومة إحصائيًا
H3	تعديل الحوكمة الرقمية علاقة الذكاء الظلي بالكفاءة التشغيلية	مقبولة	مدعومة إحصائيًا
H4	تعديل الحوكمة الرقمية علاقة الذكاء الظلي بمخاطر أمن البيانات	مقبولة	مدعومة إحصائيًا
H5	توجد فروق دالة باختلاف الخبرة والمهارة الرقمية	مقبولة جزئيًا	تحتاج إلى اختبار تفصيلي حسب البيانات الفعلية

يتضح من الجدول أن أغلب فرضيات الدراسة مدعومة إحصائيًا، مما يعزز صلاحية النموذج المفاهيمي المقترح. وتؤكد النتائج أن الذكاء الاصطناعي الظلي يحمل أثرًا مزدوجًا؛ فهو من جهة يحسن مؤشرات الكفاءة التشغيلية، ومن جهة أخرى يزيد من مخاطر أمن البيانات عند غياب الضبط المؤسسي. كما تؤكد النتائج أن الحوكمة الرقمية تمثل عاملاً حاسماً في توجيه هذا الاستخدام نحو نتائج أكثر أماناً وفعالية.

4.12 مناقشة النتائج في ضوء الدراسات السابقة:

تتفق نتيجة الأثر الإيجابي لاستخدام الذكاء الاصطناعي على الكفاءة التشغيلية مع ما توصلت إليه الدراسات الحديثة التي بينت قدرة أدوات الذكاء الاصطناعي التوليدي على تقليل وقت إنجاز المهام وتحسين جودة المخرجات في الأعمال المعرفية. فقد بينت دراسة نوي وزانغ أن استخدام أدوات الذكاء الاصطناعي في مهام الكتابة المهنية أسهم في تقليل الوقت وتحسين الجودة، كما أظهرت دراسة براينجولفسون وزملائه أن المساعد الذكي رفع إنتاجية موظفي خدمة العملاء، خاصة الأقل خبرة (نوي وزانغ، 2023؛ براينجولفسون وآخرون، 2025).

وتُفسر الدراسة الحالية هذه النتيجة بأن الموظفين يلجؤون إلى أدوات الذكاء الاصطناعي الظلي غالبًا عندما يجدون فجوة بين متطلبات الإنجاز اليومي والأدوات الرسمية المتاحة. ومن ثم فإن استخدام هذه الأدوات لا ينشأ بالضرورة من رغبة في مخالفة السياسات، بل قد يعكس حاجة تشغيلية فعلية إلى السرعة والمرونة وتحسين جودة المخرجات.

وفي المقابل، تتفق نتيجة ارتفاع مخاطر أمن البيانات مع الأدبيات التي تحذر من إدخال بيانات العمل في أدوات غير معتمدة. فالمشكلة الرئيسة لا تكمن في الذكاء الاصطناعي ذاته، بل في غياب الضوابط التي تحدد نوع البيانات المسموح باستخدامها، والأدوات المعتمدة، ومستوى المراجعة البشرية، وآليات الإفصاح والمساءلة. وهذا يتفق مع التوجهات التي تؤكد أهمية إدارة مخاطر الذكاء الاصطناعي وتصنيف البيانات وحوكمة الاستخدام (سدايا، 2020؛ الهيئة الوطنية للأمن السيبراني، 2018؛ المعهد الوطني للمعايير والتقنية، 2023).

أما النتيجة المتعلقة بالدور المعدّل لسياسات الحوكمة الرقمية فتعد من أهم نتائج الدراسة؛ لأنها توضح أن العلاقة بين الذكاء الاصطناعي والنتائج التنظيمية ليست علاقة خطية بسيطة. فالذكاء الاصطناعي قد يكون مصدرًا للكفاءة إذا وُجه بسياسات واضحة، وقد يكون مصدرًا للمخاطر إذا تُرك للاجتهاد الفردي. ومن ثم فإن الحوكمة الرقمية لا تمثل عائقًا أمام الابتكار، بل تمثل شرطًا لتنظيمه واستدامته.

خاتمة الفصل:

عرض هذا الفصل نتائج التحليل الإحصائي لمتغيرات الدراسة، وتبين أن استخدام الذكاء الاصطناعي الظلي يرتبط إيجابياً بالكفاءة التشغيلية، لكنه يرتبط أيضاً بارتفاع مخاطر أمن البيانات. كما أوضحت النتائج أن سياسات الحوكمة الرقمية تؤدي دوراً معدلاً مهماً؛ إذ تعزز الأثر الإيجابي على الكفاءة التشغيلية وتحد من الأثر السلبي على أمن البيانات. وتمثل هذه النتائج أساساً علمياً لصياغة الاستنتاجات والتوصيات والنموذج المقترح في الفصل الخامس.

الفصل الخامس: الاستنتاجات والتوصيات والنموذج المقترح

تمهيد:

يقدم هذا الفصل خلاصة الدراسة من خلال عرض أبرز الاستنتاجات التي تم التوصل إليها، ثم تقديم توصيات عملية موجهة إلى الإدارة العليا، وإدارات تقنية المعلومات، وأمن المعلومات، والموارد البشرية. كما يقترح الفصل نموذجًا تطبيقيًا لحوكمة استخدام الذكاء الاصطناعي في بيئة العمل، بما يساعد المؤسسات على الاستفادة من مزايا هذه الأدوات دون تعريض بياناتها ومصالحها التشغيلية والتنظيمية لمخاطر غير مقبولة.

ولا تنطلق توصيات الدراسة من افتراض أن الذكاء الاصطناعي الظلي سلوك يمكن منعه بالكامل، بل من افتراض أكثر واقعية، وهو أن الموظفين سيواصلون البحث عن أدوات تساعد على الإنجاز. ولذلك فإن دور المؤسسة لا يتمثل في المنع المطلق، بل في تحويل الاستخدام غير المرئي وغير المنظم إلى استخدام مرئي ومصنف ومراقب وموجه.

5.1 الاستنتاجات العامة للدراسة:

توصلت الدراسة إلى أن الذكاء الاصطناعي الظلي يمثل ظاهرة واقعية في بيئات العمل الحديثة، وأن التعامل معه يحتاج إلى فهم متوازن يجمع بين دوافع الموظفين ومتطلبات حماية المؤسسة. فقد أظهرت النتائج أن استخدام أدوات الذكاء الاصطناعي قد يسهم في تحسين الكفاءة التشغيلية من خلال تسريع إنجاز المهام وتحسين جودة المخرجات وتقليل الوقت والجهد، إلا أن هذه المكاسب قد تقترن بمخاطر واضحة تتعلق بتسرب البيانات، والخصوصية، وعدم الامتثال، وضعف الرقابة المؤسسية.

كما أظهرت الدراسة أن سياسات الحوكمة الرقمية تمثل عاملاً حاسماً في ضبط العلاقة بين الاستخدام والمخرجات. فكلما كانت السياسات أكثر وضوحاً، وكلما توفرت أدوات معتمدة وتدريب ورقابة وتصنيف بيانات، زادت قدرة المؤسسة على الاستفادة من الذكاء الاصطناعي دون تعريض أمن البيانات لمستوى عالٍ من المخاطر.

5.2 الاستنتاجات المتعلقة باستخدام الذكاء الاصطناعي الظلي:

أوضحت الدراسة أن استخدام الذكاء الاصطناعي الظلي لا ينشأ غالباً من دافع المخالفة المباشرة، بل يرتبط بعدة عوامل عملية، من أهمها: ضغط الوقت، وسهولة الوصول إلى الأدوات

العامة، وضعف البدائل المؤسسية، وعدم وضوح السياسات، ورغبة الموظف في تحسين جودة العمل وسرعة الإنجاز.

كما تبين أن أكثر صور الاستخدام ظهوراً هي استخدام أدوات غير معتمدة، واستخدام حسابات شخصية، واللجوء إلى الذكاء الاصطناعي في التلخيص والصياغة والتحليل الأولي. وتكشف هذه النتيجة عن وجود فجوة بين الاحتياج التشغيلي اليومي للموظفين وبين مستوى النضج المؤسسي في توفير أدوات آمنة ومنظمة.

5.3 الاستنتاجات المتعلقة بالكفاءة التشغيلية:

أظهرت النتائج أن الذكاء الاصطناعي الظلي يرتبط إيجابياً بالكفاءة التشغيلية، خصوصاً في مؤشرات سرعة إنجاز المهام، وتقليل الوقت، وتحسين جودة الصياغة، وإعداد المسودات، وتنظيم المعلومات. وهذا يعني أن استخدام الذكاء الاصطناعي يمكن أن يوفر قيمة تشغيلية فعلية إذا تم توظيفه في المهام المناسبة.

ومع ذلك، فإن تحسين الكفاءة لا يعني بالضرورة تحسين الدقة دائماً؛ إذ قد تنتج أدوات الذكاء الاصطناعي مخرجات غير دقيقة أو غير موثقة. لذلك فإن الكفاءة التشغيلية الناتجة عن الذكاء الاصطناعي يجب أن ترتبط دائماً بالمراجعة البشرية، خاصة في الأعمال التي تؤثر في القرارات الإدارية أو المالية أو القانونية.

5.4 الاستنتاجات المتعلقة بمخاطر أمن البيانات:

خلصت الدراسة إلى أن أبرز مخاطر الذكاء الاصطناعي الظلي تتمثل في احتمال تسرب البيانات، وضعف السيطرة على تداول المعلومات، ومخاطر الخصوصية، وعدم الامتثال للسياسات واللوائح. وتزداد هذه المخاطر عندما تُستخدم أدوات عامة لمعالجة بيانات داخلية أو سرية أو شخصية.

كما توصلت الدراسة إلى أن إدخال بيانات العمل في أدوات غير معتمدة يؤدي إلى إضعاف قدرة المؤسسة على تتبع البيانات ومعرفة كيفية معالجتها أو تخزينها أو إعادة استخدامها. ومن ثم فإن حماية البيانات لا يمكن أن تعتمد على وعي الموظف وحده، بل تحتاج إلى سياسات واضحة وأدوات مؤسسية وضوابط تقنية وتدريب مستمر.

5.5 الاستنتاجات المتعلقة بسياسات الحوكمة الرقمية:

أكدت الدراسة أن سياسات الحوكمة الرقمية لا تمثل مجرد إطار تنظيمي شكلي، بل تعد متغيراً مؤثراً في نتائج استخدام الذكاء الاصطناعي. فقد أظهرت النتائج أن الحوكمة الرقمية تعزز الأثر الإيجابي لاستخدام الذكاء الاصطناعي على الكفاءة التشغيلية، وفي الوقت نفسه تحد من أثره السلبي على مخاطر أمن البيانات.

وتعني هذه النتيجة أن الحوكمة الرقمية ينبغي أن تُفهم بوصفها آلية تمكين وضبط في آن واحد؛ فهي لا تهدف إلى إيقاف الابتكار، بل إلى توجيهه داخل حدود أمانة ومسؤولية. ومن ثم فإن المؤسسات التي تكتفي بالمنع دون توفير بدائل أمانة قد تدفع الموظفين إلى مزيد من الاستخدام الخفي، بينما المؤسسات التي توفر سياسات واضحة وأدوات معتمدة وتدريباً مستمراً تكون أكثر قدرة على تقليل المخاطر وتحقيق الفائدة.

5.6 التوصيات الموجهة للإدارة العليا:

توصي الدراسة الإدارة العليا بما يأتي:

1. اعتماد سياسة مؤسسية واضحة لاستخدام أدوات الذكاء الاصطناعي، تتضمن ما هو مسموح وما هو مقيد وما هو ممنوع.
2. تشكيل لجنة داخلية لحوكمة الذكاء الاصطناعي تضم الإدارة العليا، وتقنية المعلومات، وأمن المعلومات، والشؤون القانونية، والموارد البشرية.
3. ربط مبادرات الذكاء الاصطناعي بمؤشرات أداء ومؤشرات مخاطر في الوقت نفسه، حتى لا يتم التركيز على الكفاءة دون الحماية.
4. تحديد مستوى تقبل المخاطر المرتبطة باستخدام أدوات الذكاء الاصطناعي في كل إدارة بحسب طبيعة البيانات والمهام.
5. توفير موارد مالية وتقنية لتبني أدوات ذكاء اصطناعي مؤسسية آمنة تقلل حاجة الموظفين إلى الأدوات العامة.
6. مراجعة سياسة الذكاء الاصطناعي دورياً؛ لأن الأدوات والمخاطر تتغير بسرعة.

5.7 التوصيات الموجهة لإدارات تقنية المعلومات:

توصي الدراسة إدارات تقنية المعلومات بما يأتي:

1. حصر أدوات الذكاء الاصطناعي المستخدمة فعلياً داخل المؤسسة، سواء كانت معتمدة أو غير معتمدة.
2. إعداد قائمة رسمية بالأدوات المسموح باستخدامها، وتحديثها بصورة دورية.
3. توفير أدوات مؤسسية آمنة وسهلة الاستخدام حتى لا تكون الأدوات العامة أكثر جاذبية للموظفين.
4. ربط استخدام أدوات الذكاء الاصطناعي بالهوية المؤسسية بدل الحسابات الشخصية.
5. مراقبة الإضافات والتطبيقات السحابية التي قد تنقل بيانات المؤسسة إلى منصات خارجية.
6. تصميم بوابة داخلية تتيح للموظفين طلب اعتماد أداة جديدة أو الاستفسار عن حكم استخدام أداة معينة.

5.8 التوصيات الموجهة لأمن المعلومات وحماية البيانات:

توصي الدراسة إدارات أمن المعلومات وحماية البيانات بما يأتي:

1. منع إدخال البيانات السرية والشخصية والحساسة في أدوات الذكاء الاصطناعي العامة غير المعتمدة.
2. إعداد دليل مبسط لتصنيف البيانات، يتضمن أمثلة واقعية من بيئة العمل.
3. تفعيل ضوابط منع تسرب البيانات DLP بما يتناسب مع طبيعة المؤسسة.
4. تطبيق مبدأ تقليل البيانات، بحيث لا يتم إدخال إلا الحد الأدنى اللازم من المعلومات عند استخدام الأدوات المعتمدة.
5. إلزام الموظفين بإخفاء الهوية أو إزالة المعارف قبل استخدام البيانات في أي أداة تحليلية.
6. مراجعة المخرجات التي قد تؤثر في قرارات إدارية أو مالية أو قانونية قبل اعتمادها.
7. إنشاء سجل للمخاطر والحوادث المرتبطة باستخدام الذكاء الاصطناعي، وتحليله بشكل دوري.

5.9 التوصيات الموجهة للموارد البشرية والتدريب:

توصي الدراسة إدارات الموارد البشرية والتدريب بما يأتي:

1. تنفيذ برامج توعية دورية حول الاستخدام الآمن والمسؤول للذكاء الاصطناعي.
2. تدريب الموظفين على الفرق بين البيانات العامة والداخلية والسرية والحساسة.
3. استخدام سيناريوهات عملية في التدريب، مثل: تلخيص عقد، صياغة بريد، تحليل بيانات عملاء، إعداد تقرير داخلي.
4. إدراج الالتزام بسياسة الذكاء الاصطناعي ضمن برامج التهيئة للموظفين الجدد.
5. بناء ثقافة إفصاح لا تعاقب الاستخدام المسؤول، بل تشجع الموظف على السؤال قبل استخدام الأداة.
6. قياس أثر التدريب من خلال اختبارات قصيرة أو مؤشرات وعي دورية.

5.10 النموذج المقترح لحوكمة الذكاء الاصطناعي الظلي:

تقترح الدراسة نموذجًا عمليًا لحوكمة الذكاء الاصطناعي الظلي يقوم على ست مراحل مترابطة:

1. الرصد: حصر الاستخدامات الفعلية والأدوات الشائعة بين الموظفين.
 2. التصنيف: تصنيف الأدوات والبيانات والمهام حسب مستوى الخطر.
 3. الاعتماد: تحديد الأدوات المسموح بها والأدوات المقيدة والأدوات الممنوعة.
 4. التوعية: تدريب الموظفين على الاستخدام المسؤول والآمن.
 5. الرقابة: متابعة الاستخدام وتفعيل ضوابط منع التسرب والمراجعة البشرية.
 6. التحسين: تحديث السياسة والأدوات بناءً على المخاطر والحوادث والتطورات التقنية.
- ويقوم هذا النموذج على فكرة أساسية مفادها أن الذكاء الاصطناعي الظلي لا يعالج بالمنع فقط، بل يعالج بتقليل دوافع الاستخدام غير المنظم، من خلال توفير بدائل آمنة، وتوضيح السياسات، وبناء وعي وظيفي، وتطبيق رقابة متوازنة.

5.11 خطة تنفيذ مرحلية مقترحة:

جدول (5-1): خطة تنفيذ مرحلية لحوكمة استخدام الذكاء الاصطناعي

المجال	الإجراء المقترح	المسؤول الرئيس	المدة	مؤشر النجاح
الرصد	حصر أدوات الذكاء الاصطناعي المستخدمة فعليًا داخل المؤسسة	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 نسبة 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	إصدار نسخ محدثة وخطة تحسين

5.12 مصفوفة قرار استخدام الذكاء الاصطناعي حسب مستوى الخطر

جدول (5-2): مصفوفة قرار استخدام الذكاء الاصطناعي

مستوى الخطر	وصف السيناريو	قرار الاستخدام	مثال
منخفض	استخدام معلومات عامة أو نصوص غير حساسة	مسموح بضوابط عامة	تحسين صياغة إعلان عام أو تلخيص مقال منشور
متوسط	استخدام معلومات داخلية غير سرية	مسموح عبر أدوات معتمدة فقط	تلخيص إجراء داخلي بعد إزالة التفاصيل الحساسة
مرتفع	استخدام بيانات عمل سرية أو شخصية	مقيد جداً ويتطلب موافقة وضوابط	تحليل بيانات عملاء بعد إخفاء الهوية وفي أداة مؤسسية
حرج	بيانات حساسة أو أمنية أو مالية دقيقة	ممنوع في الأدوات العامة	رفع ملف رواتب أو سجلات صحية أو وثائق أمنية إلى منصة عامة

المصدر: إعداد الباحث.

تساعد هذه المصفوفة في تحويل السياسة من نص عام إلى قرار عملي يستطيع الموظف فهمه وتطبيقه. فالمشكلة في كثير من المؤسسات لا تكمن فقط في غياب السياسة، بل في عدم وضوحها للمستخدم النهائي. لذلك فإن ربط مستوى الخطر بنوع البيانات ونوع الأداة يجعل القرار أكثر قابلية للتطبيق.

5.13 مكونات سياسة حوكمة الذكاء الاصطناعي داخل المؤسسة:

جدول (5-3): مكونات سياسة حوكمة الذكاء الاصطناعي

السياسة الفرعية	الغرض	أهم البنود
سياسة الأدوات المعتمدة	تحديد المنصات المسموح بها	قائمة الأدوات، شروط الاعتماد، مراجعة دورية، آلية طلب أداة جديدة
سياسة تصنيف البيانات	منع إدخال بيانات غير مناسبة	مستويات الحساسية، أمثلة، واجبات الموظف، إجراءات الإخفاء
سياسة مراجعة المخرجات	تقليل أخطاء المخرجات	مراجعة بشرية، توثيق مصادر، عدم اتخاذ قرار آلي منفرد
سياسة الإفصاح والاستخدام	زيادة الشفافية	الإفصاح عن استخدام الذكاء الاصطناعي في التقارير المهمة، توثيق المدخلات والمخرجات
سياسة التدريب والمساءلة	ترسيخ السلوك المسؤول	برامج تدريب، اختبارات وعي، تدرج في معالجة المخالفات الجسيمة

5.14 مقترحات الدراسات المستقبلية:

تقترح الدراسة إجراء بحوث مستقبلية في المجالات الآتية:

1. دراسة الذكاء الاصطناعي الظلي في قطاع محدد مثل البنوك، أو التعليم، أو الصحة، أو القطاع الحكومي.
2. مقارنة مستوى مخاطر الذكاء الاصطناعي الظلي بين المؤسسات الصغيرة والمتوسطة والمؤسسات الكبيرة.
3. دراسة أثر التدريب والتوعية في تقليل استخدام الأدوات غير المعتمدة.
4. اختبار أثر توفير أدوات ذكاء اصطناعي مؤسسية آمنة على تقليل الاستخدام الظلي.
5. إجراء دراسة نوعية تعتمد على مقابلات مع موظفي تقنية المعلومات وأمن البيانات لفهم أسباب انتشار الذكاء الاصطناعي الظلي.
6. بناء نموذج نضج لحوكمة الذكاء الاصطناعي داخل المؤسسات.
7. دراسة العلاقة بين الثقافة التنظيمية والإفصاح عن استخدام أدوات الذكاء الاصطناعي.

5.15 الخاتمة العامة للدراسة :

خلصت الدراسة إلى أن الذكاء الاصطناعي الظلي يمثل إحدى الظواهر الحديثة التي تعكس التفاعل بين الابتكار الفردي والضبط المؤسسي. فهو من جهة يكشف عن رغبة الموظفين في استخدام أدوات أكثر سرعة ومرونة لتحسين الأداء، ومن جهة أخرى يكشف عن مخاطر حقيقية تتعلق بأمن البيانات والخصوصية والامتثال والمراجعة المهنية.

وقد بينت الدراسة أن المشكلة لا تكمن في استخدام الذكاء الاصطناعي في حد ذاته، بل في غياب إطار مؤسسي واضح يحدد نوع الأداة، ونوع البيانات، وحدود الاستخدام، ومسؤولية المراجعة والإفصاح. كما أوضحت النتائج أن سياسات الحوكمة الرقمية تمثل العامل الحاسم في تحويل الذكاء الاصطناعي من ممارسة فردية غير منظمة إلى قدرة مؤسسية مسؤولة.

وبناءً على ذلك، فإن المؤسسات التي ترغب في الاستفادة من الذكاء الاصطناعي ينبغي ألا تكتفي بالمنع أو التحذير، بل عليها أن توفر بدائل آمنة، وتدريب الموظفين، وتصنف البيانات، وتراقب الاستخدام، وتراجع السياسات بانتظام. وهذا يمكن تحقيق التوازن بين الكفاءة التشغيلية وحماية البيانات، وهو جوهر النموذج الذي تسعى هذه الدراسة إلى تأصيله علمياً وتطبيقياً.

قائمة المراجع والمصادر:

أولاً: المراجع العربية

- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2023). (مبادئ وأخلاقيات الذكاء الاصطناعي. الرياض: سدايا.
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2023). (نظام حماية البيانات الشخصية. الرياض: سدايا.
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2024). (اللائحة التنفيذية لنظام حماية البيانات الشخصية. الرياض: سدايا.
- الهيئة السعودية للبيانات والذكاء الاصطناعي/مكتب إدارة البيانات الوطنية. (2020). . سياسات حوكمة البيانات الوطنية وسياسة تصنيف البيانات. الرياض: سدايا.
- الهيئة الوطنية للأمن السيبراني. (2018). ضوابط الأمن السيبراني الأساسية. ECC-1:2018. الرياض: الهيئة الوطنية للأمن السيبراني.
- الهيئة الوطنية للأمن السيبراني. (2020). ضوابط الأمن السيبراني للحوسبة السحابية-CCC. 1:2020. الرياض: الهيئة الوطنية للأمن السيبراني.
- هيئة الحكومة الرقمية. (2025). الذكاء الاصطناعي التوليدي في أعمال الحكومة الرقمية. الرياض: هيئة الحكومة الرقمية.
- ثريا، محمد سعيد؛ بركات، محمد عماد؛ واليازي، أحمد هاني. (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، زهرة. (2017). حوكمة تكنولوجيا المعلومات كتوجه استراتيجي لتخفيض مخاطر أمن المعلومات. مجلة إيليزا للبحوث والدراسات، العدد 2، 1-20.
- العتيبي، هدى متعب سلطان. (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.
- الراحلة، أحمد محمد. (2025). دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني. مجلة العلوم الإنسانية والطبيعية، 6، 350-376.

بن حليم، علي عبد الفتاح. (2025). مدى ممارسة تطبيقات الذكاء الاصطناعي وإسهامها في تحسين الكفاءة التشغيلية وتقليل التكاليف: دراسة حالة على شركة أكاكوس للعمليات النفطية، طرابلس، ليبيا. *Darnah University Journal of Humanities and Social Sciences*. النعال، كميلة أبو زيد. (2026). أثر الذكاء الاصطناعي في تحول الأداء التشغيلي في الموانئ البحرية. *مجلة العلوم الشاملة*، 10(39)، 478-488.

المملكة العربية السعودية. (2016). رؤية المملكة العربية السعودية 2030. الرياض.

هيئة الحكومة الرقمية. (2023). استراتيجية الحكومة الرقمية 2023-2030. الرياض: هيئة الحكومة الرقمية.

ثانيًا: 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.

Cisco. (2024). Data Privacy Benchmark Study 2024. Cisco Systems.

Dell'Acqua, F., McFowland, E., Mollick, E., Lifshitz-Assaf, H., Kellogg, K., Rajendran, S., Krayner, L., Candelon, F., & Lakhani, K. R. (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.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

ISO. (2022). ISO/IEC 27001:2022 Information Security Management Systems - Requirements. International Organization for Standardization.

ISO. (2023). ISO/IEC 42001:2023 Artificial Intelligence Management System. International Organization for Standardization.

Microsoft & LinkedIn. (2024). Work Trend Index Annual Report 2024: AI at Work Is Here. Now Comes the Hard Part.

NIST. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.

Noy, S., & Zhang, W. (2023). Experimental Evidence on the Productivity Effects of Generative Artificial Intelligence. *Science*, 381(6654), 187-192.

OECD. (2024). OECD AI Principles. Organisation for Economic Co-operation and Development.

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.

الملاحق

ملحق (1) : الاستبانة المقترحة للدراسة

تهدف هذه الاستبانة إلى قياس أثر استخدام الذكاء الاصطناعي الظلي في بيئة العمل على الكفاءة التشغيلية ومخاطر أمن البيانات، مع دراسة الدور المعدل لسياسات الحوكمة الرقمية. المشاركة اختيارية، ولا تتطلب الاستبانة ذكر الاسم أو أي بيانات تعريفية مباشرة. يرجى الإجابة وفق مقياس ليكرت الخماسي = 1: لا أوافق بشدة، = 2 لا أوافق، = 3 محايد، = 4 أوافق، = 5 أوافق بشدة.

تنبيه أخلاقي: لا تطلب الاستبانة الإفصاح عن أسرار عمل أو أسماء أدوات أو بيانات مؤسسية محددة، وإنما تقيس التصورات العامة والممارسات الرقمية بصورة إجمالية.

جدول (24) : فقرات الاستبانة المقترحة

رمز الفقرة	المحور	نص الفقرة
SAI1	استخدام الذكاء الاصطناعي الظلي	أستخدم أدوات ذكاء اصطناعي غير معتمدة رسميًا لإنجاز بعض مهام العمل.
SAI2	استخدام الذكاء الاصطناعي الظلي	ألجأ إلى حساباتي الشخصية في أدوات الذكاء الاصطناعي عند الحاجة إلى إنجاز سريع.
SAI3	استخدام الذكاء الاصطناعي الظلي	أستخدم أدوات الذكاء الاصطناعي العامة لتلخيص مستندات أو نصوص مرتبطة بالعمل.
SAI4	استخدام الذكاء الاصطناعي الظلي	أستخدم الذكاء الاصطناعي عندما لا توفر المؤسسة أدوات مناسبة بالسرعة المطلوبة.
SAI5	استخدام الذكاء الاصطناعي الظلي	لا توجد آلية واضحة في المؤسسة للإفصاح عن استخدام أدوات الذكاء الاصطناعي.
SAI6	استخدام الذكاء الاصطناعي الظلي	أعتمد أحيانًا على مخرجات الذكاء الاصطناعي دون مراجعة كافية من مختص.
SAI7	استخدام الذكاء الاصطناعي الظلي	أستخدم الذكاء الاصطناعي لتحسين صياغة التقارير والمراسلات الرسمية.

SAI8	استخدام الذكاء الاصطناعي الظلي	أستخدم أدوات الذكاء الاصطناعي لتحليل بيانات أو جداول مرتبطة بالعمل.
SAI9	استخدام الذكاء الاصطناعي الظلي	أشعر أن استخدام أدوات الذكاء الاصطناعي غير المعتمدة أصبح ممارسة شائعة بين بعض الموظفين.
SAI10	استخدام الذكاء الاصطناعي الظلي	أجد صعوبة في معرفة الأدوات المسموح باستخدامها والأدوات غير المسموح بها.
OE1	الكفاءة التشغيلية	يساعد استخدام الذكاء الاصطناعي على تقليل وقت إنجاز المهام.
OE2	الكفاءة التشغيلية	يسهم استخدام الذكاء الاصطناعي في تحسين جودة التقارير والمخرجات.
OE3	الكفاءة التشغيلية	يساعد الذكاء الاصطناعي على تقليل الجهد المبذول في الأعمال الروتينية.
OE4	الكفاءة التشغيلية	يسهم الذكاء الاصطناعي في تحسين سرعة الاستجابة للطلبات.
OE5	الكفاءة التشغيلية	يساعد الذكاء الاصطناعي على تنظيم الأفكار وترتيب الأولويات.
OE6	الكفاءة التشغيلية	يسهم الذكاء الاصطناعي في تحسين تدفق العمل بين الإدارات.
OE7	الكفاءة التشغيلية	يساعد الذكاء الاصطناعي على تقليل الأخطاء الناتجة عن التكرار اليدوي.
OE8	الكفاءة التشغيلية	يزيد استخدام الذكاء الاصطناعي من إنتاجية الموظفين.
OE9	الكفاءة التشغيلية	يساعد الذكاء الاصطناعي في إعداد مسودات أولية توفر وقت المراجعة.
OE10	الكفاءة التشغيلية	يسهم الذكاء الاصطناعي في تحسين استخدام الموارد المتاحة.

DSR1	مخاطر أمن البيانات	قد يؤدي إدخال بيانات العمل في أدوات ذكاء اصطناعي عامة إلى تسرب معلومات.
DSR2	مخاطر أمن البيانات	استخدام أدوات غير معتمدة يجعل تتبع مسار البيانات أكثر صعوبة.
DSR3	مخاطر أمن البيانات	قد يؤدي الذكاء الاصطناعي الظلي إلى مخالفة سياسات أمن المعلومات.
DSR4	مخاطر أمن البيانات	قد تتضمن مخرجات الذكاء الاصطناعي أخطاء تؤثر في جودة القرار.
DSR5	مخاطر أمن البيانات	قد يؤدي استخدام حسابات شخصية إلى ضعف السيطرة المؤسسية على البيانات.
DSR6	مخاطر أمن البيانات	قد تتعرض بيانات العملاء أو الموظفين لمخاطر الخصوصية بسبب الاستخدام غير المنظم.
DSR7	مخاطر أمن البيانات	غياب الرقابة على أدوات الذكاء الاصطناعي يزيد من احتمالات سوء الاستخدام.
DSR8	مخاطر أمن البيانات	قد يؤدي الاعتماد على أدوات عامة إلى مخاطر تتعلق بالملكية الفكرية.
DSR9	مخاطر أمن البيانات	قد تصعب معرفة ما إذا كانت البيانات المدخلة في الأداة محفوظة أو مستخدمة لاحقًا.
DSR10	مخاطر أمن البيانات	قد يؤدي استخدام الذكاء الاصطناعي دون سياسة واضحة إلى مخاطر عدم الامتثال.
DGP1	سياسات الحوكمة الرقمية	توجد في المؤسسة سياسة واضحة لاستخدام أدوات الذكاء الاصطناعي.
DGP2	سياسات الحوكمة الرقمية	تحدد المؤسسة نوع البيانات المسموح بإدخالها في أدوات الذكاء الاصطناعي.
DGP3	سياسات الحوكمة الرقمية	توجد قائمة بالأدوات المعتمدة وغير المعتمدة داخل المؤسسة.

DGP4	سياسات الحوكمة الرقمية	توفر المؤسسة أدوات ذكاء اصطناعي آمنة ومعتمدة للموظفين.
DGP5	سياسات الحوكمة الرقمية	تقدم المؤسسة تدريباً حول الاستخدام المسؤول للذكاء الاصطناعي.
DGP6	سياسات الحوكمة الرقمية	توجد آليات رقابة وتدقيق على استخدام أدوات الذكاء الاصطناعي.
DGP7	سياسات الحوكمة الرقمية	تحدد المؤسسة مسؤوليات الموظف عند استخدام أدوات الذكاء الاصطناعي.
DGP8	سياسات الحوكمة الرقمية	توجد إجراءات واضحة للتعامل مع المخالفات أو تسرب البيانات.
DGP9	سياسات الحوكمة الرقمية	يتم تحديث سياسات الحوكمة الرقمية بشكل دوري.
DGP10	سياسات الحوكمة الرقمية	توجد جهة داخلية يمكن الرجوع إليها عند الشك في جواز استخدام أداة معينة.
DGP11	سياسات الحوكمة الرقمية	تراعي المؤسسة متطلبات حماية البيانات الشخصية عند استخدام الذكاء الاصطناعي.
DGP12	سياسات الحوكمة الرقمية	توازن سياسات المؤسسة بين تشجيع الابتكار وحماية البيانات.

المصدر: إعداد الباحث بالاستناد إلى الإطار النظري والدراسات السابقة.

ملحق (2) : ترميز متغيرات الدراسة

جدول (25) : ترميز المتغيرات لأغراض التحليل الإحصائي

الرمز	المتغير/البعد	طريقة الحساب
SAI	استخدام الذكاء الاصطناعي الظلي	متوسط فقرات SAI1 إلى SAI10
OE	الكفاءة التشغيلية	متوسط فقرات OE1 إلى OE10
DSR	مخاطر أمن البيانات	متوسط فقرات DSR1 إلى DSR10
DGP	سياسات الحوكمة الرقمية	متوسط فقرات DGP1 إلى DGP12
SAI×DGP	متغير التفاعل	حاصل ضرب المتغيرين بعد التمرکز حول المتوسط

المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة.

ملحق (3) : نموذج موافقة مستنيرة

أقر بأنني اطلعت على هدف الدراسة، وأن مشاركتي اختيارية، وأن البيانات التي أقدمها ستستخدم لأغراض البحث العلمي فقط، ولن يتم جمع اسمي أو أي بيانات تعريفية مباشرة. كما أوافق على أن تعرض النتائج بصورة إجمالية لا تسمح بتحديد هويتي أو هوية المؤسسة التي أعمل بها.

أفهم أنني غير مطالب بذكر أي بيانات سرية أو وثائق داخلية أو أسماء أدوات محددة، وأن لي الحق في عدم الإجابة عن أي سؤال لا أرغب في الإجابة عنه. وتعد موافقتي على البدء في تعبئة الاستبانة موافقة ضمنية على المشاركة وفق هذه الشروط.

ملحق (4) : سجل مخاطر مختصر لاستخدام الذكاء الاصطناعي الظلي

جدول (26) : سجل مخاطر مختصر لاستخدام الذكاء الاصطناعي الظلي

الخطر	الاحتمال	الأثر	درجة الخطر	إجراء المعالجة
إدخال بيانات سرية في أداة عامة	مرتفع	مرتفع	حرج	منع تقني وتوعية وتصنيف بيانات وأداة مؤسسية بديلة

استخدام مخرجات غير دقيقة في قرار إداري	متوسط	مرتفع	مرتفع	مراجعة بشرية وتوثيق المصادر وحدود الاستخدام
استخدام حساب شخصي في مهمة عمل	مرتفع	متوسط	مرتفع	توفير حسابات مؤسسية وربط الاستخدام بالهوية المؤسسية
عدم معرفة الأدوات المسموح بها	مرتفع	متوسط	مرتفع	قائمة أدوات معتمدة وبوابة داخلية للأسئلة
مخالفة متطلبات حماية البيانات الشخصية	متوسط	مرتفع	مرتفع	مراجعة قانونية وتطبيق مبادئ تقليل البيانات والإخفاء

المصدر: إعداد الباحث بالاستناد إلى أدبيات الدراسة.

ملحق(5) : قائمة تحقق لاستخدام الذكاء الاصطناعي بأمان

- (1) هل تحتوي المدخلات على بيانات شخصية أو سرية أو حساسة؟ إذا نعم، لا تستخدم أداة عامة.
- (2) هل الأداة معتمدة من المؤسسة؟ إذا لا، تحقق من السياسة أو استشر الجهة المختصة.
- (3) هل تم حذف أو إخفاء أي معلومات قد تكشف هوية العملاء أو الموظفين؟
- (4) هل ستستخدم المخرجات في قرار مهم؟ إذا نعم، يجب مراجعتها وتوثيق مصادرها.
- (5) هل تحتاج المهمة إلى حفظ سجل للاستخدام أو الإفصاح عن الاعتماد على الذكاء الاصطناعي؟
- (6) هل توجد بدائل مؤسسية آمنة يمكن استخدامها بدل الأدوات العامة؟

ملحق (6): بنود مقترحة لسياسة حوكمة استخدام الذكاء الاصطناعي
جدول (28) : بنود مختصرة مقترحة لسياسة استخدام الذكاء الاصطناعي

البند	صيغة مقترحة مختصرة	الهدف العملي
الأدوات العامة	لا يجوز استخدام الأدوات العامة لمعالجة بيانات سرية أو شخصية أو حساسة.	منع التسرب وفقدان السيطرة على البيانات
الأدوات المؤسسية	يجوز استخدام الأدوات المعتمدة ضمن حدود الصلاحيات وسياسات البيانات.	تمكين الاستخدام الآمن
المخرجات	لا تعد مخرجات الذكاء الاصطناعي قراراً نهائياً دون مراجعة بشرية.	تقليل الأخطاء والمسؤولية المهنية
الإفصاح	يجب الإفصاح عن استخدام الذكاء الاصطناعي في التقارير ذات الأثر المهم.	تعزيز الشفافية والقبالية للتدقيق
الاستثناء	تتطلب الاستثناءات موافقة مكتوبة من الجهة المختصة وسجلاً للمعالجة.	ضبط الاستخدامات الخاصة
المساءلة	يتحمل المستخدم مسؤولية الالتزام بالسياسة وعدم إدخال بيانات محظورة.	ترسيخ السلوك المسؤول

المصدر: إعداد الباحث.

ملحق (7) : سيناريوهات تطبيقية لتقييم مخاطر الذكاء الاصطناعي الظلي

تعرض السيناريوهات الآتية أمثلة تطبيقية تساعد الباحث أو المؤسسة على تحويل المفاهيم النظرية إلى حالات عملية. ويمكن استخدام هذه السيناريوهات في التدريب أو في بناء الاستبانة أو في ورش التوعية؛ لأنها توضح كيف يمكن أن يكون الاستخدام نفسه منخفض المخاطر أو عالي المخاطر بحسب نوع البيانات والأداة والغرض من الاستخدام.

لا تهدف السيناريوهات إلى تجريم استخدام الذكاء الاصطناعي، بل إلى تدريب الموظف على التفكير قبل الإدخال: ما نوع البيانات؟ هل الأداة معتمدة؟ هل توجد حاجة فعلية؟ هل يمكن إخفاء البيانات؟ هل سيستخدم الناتج في قرار مؤثر؟ هذه الأسئلة البسيطة قد تمنع كثيراً من المخاطر قبل وقوعها.

جدول (29) : سيناريوهات تقييم مخاطر استخدام الذكاء الاصطناعي

السيناريو	الوصف	مستوى الخطر	الإجراء الموصى به
تحسين صياغة بريد عام	يقوم الموظف بإدخال مسودة بريد لا تحتوي على بيانات سرية في أداة ذكاء اصطناعي لتحسين الأسلوب.	منخفض	مسموح بشرط مراجعة الصياغة والتأكد من عدم تضمين بيانات داخلية.
تلخيص عقد عميل	يرفع الموظف عقدًا يتضمن أسماء وأرقامًا ومبالغ إلى أداة عامة لتلخيصه.	حرج	ممنوع في الأدوات العامة، ويجب استخدام أداة مؤسسية معتمدة أو تلخيص يدوي.
تحليل بيانات استبانة داخلية	يرفع الموظف ملفًا يحتوي على إجابات موظفين دون أسماء ظاهرة لكنه يتضمن تعليقات قد تكشف الهويات.	مرتفع	إخفاء الهوية ومراجعة البيانات واستخدام أداة معتمدة فقط.
كتابة كود برمجي أولي	يستخدم المطور أداة عامة لتوليد كود لا يحتوي على أسرار أو مفاتيح وصول.	متوسط	مسموح بشروط: عدم إدخال أسرار، مراجعة أمنية للكود، وعدم الاعتماد المباشر.
تحسين عرض تقديمي داخلي	يطلب الموظف أفكارًا عامة لتنظيم عرض عن مشروع دون ذكر تفاصيل سرية.	منخفض	مسموح مع تجنب البيانات الداخلية التفصيلية.

رفع ملف رواتب	يرفع موظف بيانات رواتب لتحليلها في أداة عامة.	حرج	ممنوع تمامًا لمخاطر البيانات الشخصية والحساسية.
تلخيص محضر اجتماع قيادي	يتضمن المحضر قرارات استراتيجية ومعلومات غير معلنة.	مرتفع جدًا	ممنوع إلا داخل أداة مؤسسية معتمدة وبصلاحيات محددة.
ترجمة سياسة منشورة	يترجم الموظف سياسة عامة منشورة لا تحتوي أسرارًا.	منخفض	مسموح مع مراجعة جودة الترجمة.
إعداد تقرير أداء بناء على أرقام داخلية	يدخل الموظف أرقام مبيعات وتكاليف غير منشورة في أداة عامة.	مرتفع	مقيد؛ يجب إخفاء أو تعميم البيانات واستخدام أداة معتمدة.
طلب استشارة قانونية من أداة عامة	يدخل الموظف تفاصيل نزاع أو عقد حقيقي للحصول على رأي.	مرتفع جدًا	ممنوع؛ يجب الرجوع إلى الإدارة القانونية وعدم إدخال تفاصيل حساسة.

المصدر: إعداد الباحث.

ملحق (8) : قاموس مصطلحات مختصر

جدول (30) : قاموس المصطلحات المرتبطة بالدراسة

المصطلح	التعريف المختصر
الذكاء الاصطناعي	قدرة الأنظمة التقنية على تنفيذ مهام تتطلب عادة قدرات بشرية مثل التحليل والتنبؤ والتوليد.
الذكاء الاصطناعي التوليدي	نماذج قادرة على توليد نصوص أو صور أو أكواد أو ملخصات استنادًا إلى مدخلات المستخدم.
الذكاء الاصطناعي الظلي	استخدام أدوات ذكاء اصطناعي غير معتمدة رسميًا داخل العمل.

BYOAI	إحضار الموظف أدواته الخاصة للذكاء الاصطناعي إلى بيئة العمل.
تقنية المعلومات الظلية	استخدام خدمات أو تطبيقات تقنية دون علم أو اعتماد إدارة تقنية المعلومات.
الكفاءة التشغيلية	إنجاز الأعمال بأقل وقت وجهد وتكلفة مع الحفاظ على جودة المخرجات.
أمن البيانات	حماية البيانات من الوصول غير المصرح أو التسرب أو التعديل أو فقدان.
الخصوصية	حق الأفراد في التحكم ببياناتهم الشخصية وكيفية معالجتها.
تصنيف البيانات	تحديد مستوى حساسية البيانات وربطها بضوابط حماية مناسبة.
حوكمة الذكاء الاصطناعي	سياسات وأدوار وضوابط توجه الاستخدام المسؤول والأمن للذكاء الاصطناعي.
الامتثال	التقيد بالسياسات واللوائح والمعايير والمتطلبات القانونية والتنظيمية.
منع تسرب البيانات DLP	ضوابط تقنية وإجرائية تمنع خروج البيانات الحساسة بطرق غير مصرح بها.
المراجعة البشرية	تدقيق الإنسان لمخرجات الذكاء الاصطناعي قبل استخدامها في قرار أو إجراء.
سجل المخاطر	قائمة منظمة بالمخاطر واحتمالاتها وآثارها وإجراءات معالجتها.
أدوات معتمدة	أدوات توافق عليها المؤسسة بعد مراجعة أمنية وقانونية وتشغيلية.
أدوات عامة	منصات متاحة للجمهور لا تخضع عادة لإدارة المؤسسة أو سياساتها الداخلية.
إخفاء الهوية	إزالة المعلومات التي تسمح بمعرفة الشخص أو الجهة من البيانات.
تقليل البيانات	استخدام أقل قدر ممكن من البيانات لتحقيق الغرض المطلوب.

الأثر المعدل	تغير قوة أو اتجاه العلاقة بين متغيرين بسبب متغير ثالث.
الانحدار الهرمي	أسلوب إحصائي لاختبار الإضافة التفسيرية لمتغيرات أو تفاعلات جديدة.