

إستراتيجيات الحوكمة الرقمية للذكاء الاصطناعي المستدام في حماية البيانات الشخصية: دراسة تحليلية مقارنة لآليات الامتثال بين اللائحة العامة لحماية البيانات الأوروبية (GDPR) ونظام حماية البيانات الشخصية السعودي (PDPL)

أطروحة مقدمة استكمالاً للحصول على درجة الدكتوراه
تخصص (تقنية المعلومات)

إعداد الباحث:

عبد السلام محمد العتيبي

الرقم الأكاديمي: 2403001847

العام الجامعي

2026م

الفصل الثاني

الإطار النظري والدراسات السابقة

• مقدمة

أولاً: الإطار النظري للدراسة

- تمهيد
- المحور الأول: الذكاء الاصطناعي المستدام
- المحور الثاني: حماية البيانات الشخصية
- المحور الثالث: استراتيجيات الحوكمة الرقمية للذكاء الاصطناعي
- المحور الرابع: التحليل المقارن لآليات الامتثال بين (GDPR) و (PDPL)
- خاتمة الإطار النظري للدراسة

ثانياً: الدراسات السابقة

- تمهيد
- المحور الأول: الدراسات المرتبطة بالمتغير المستقل (الذكاء الاصطناعي المستدام)
- المحور الثاني: الدراسات المرتبطة بالمتغير التابع (حماية البيانات الشخصية)
- المحور الثالث: الدراسات التي جمعت بين المتغيرين (الذكاء الاصطناعي المستدام وحماية البيانات الشخصية)
- المحور الرابع: الدراسات المرتبطة بالمقارنة بين (GDPR) و (PDPL)
- تعقيب تحليلي عام على الدراسات السابقة

الفصل الثاني

الإطار النظري والدراسات السابقة

مقدمة:

يتناول هذا الفصل الإطار النظري للدراسة من خلال تفكيك المتغيرات الرئيسية ومناقشة الأبعاد التقنية والقانونية المرتبطة بالذكاء الاصطناعي المستدام وحماية البيانات الشخصية. ويهدف الفصل إلى بناء قاعدة معرفية رصينة تستند إلى الأدبيات الحديثة لتفسير العلاقة بين التطور التقني وأطر الحوكمة، مما يُمهّد الطريق لتحليل الفجوات بين التشريعات والواقع العملي في الفصول التالية.

أولاً: الإطار النظري للدراسة

تمهيد:

يستعرض هذا القسم الأسس المفاهيمية للذكاء الاصطناعي المستدام، بدءاً من جذوره التاريخية وتطوره التقني، وصولاً إلى هيكلية المعمارية. كما يُفصل طبيعة الحوكمة الرقمية ومتطلبات الامتثال القانوني، مع التركيز على التقاطعات الحرجة بين الأداء التقني للأنظمة الذكية والمتطلبات التشريعية لحماية البيانات الشخصية.

المحور الأول: الذكاء الاصطناعي المستدام

يُشكل هذا المحور المكون التقني والمعرفي للدراسة، إذ يُعالج الجذور التاريخية، والبنية الهندسية، والأخلاقيات، والابتكار الأخضر، والاقتصاديات المرتبطة بالأنظمة الذكية، تمهيداً لربطها بآليات الحوكمة الرقمية وحماية البيانات. ويُعد الذكاء الاصطناعي المستدام مفهوماً متعدد

الأبعاد يتجاوز الأداء التقني ليشمل الاعتبارات البيئية والاجتماعية والأخلاقية، وهو ما يستوجب تحليلاً منهجياً لمكوناته.

1.1. التطور المفاهيمي والجذور التاريخية للأنظمة الذكية

تُعد الأسس الفلسفية والرياضية للذكاء الآلي منطلقاً لفهم مسار تطوره، إذ أرست إسهامات آلان تورنغ في نظرية الحوسبة وجون فون نيومان في معمارية البرامج المخزنة الأسس المنطقية الأولى، ثم تبعها مؤتمر دارتموث (1956) الذي صاغ مصطلح الذكاء الاصطناعي بوصفه مجالاً بحثياً مستقلاً (Mittal & Sharda, 2023).

كما مرت الأنظمة الذكية بـ (3) أجيال نوعية؛ إذ تمثل الجيل الأول في الأنظمة الخبيرة القائمة على القواعد المنطقية الصورية، ثم انتقل التطور إلى الجيل الثاني القائم على التعلم الإحصائي الذي يستخلص الأنماط من البيانات، وأخيراً برز الجيل الثالث المتمثل في التعلم العميق والنماذج التوليدية التي تعتمد على الشبكات العصبية متعددة الطبقات والاهتمام الذاتي (Taeihagh, 2025).

ويُصنف الباحثون النماذج المعاصرة وظيفياً إلى أنظمة تحليلية للتنبؤ والتصنيف، وأخرى توليدية لإنتاج المحتوى، وتفاعلية للروبوتات المحادثة، ومستقلة لاتخاذ القرارات؛ مما يُبرز تنوع مجالات التطبيق وتعقيدها التقني (السعيد، 2023). وتتكامل هذه الأنظمة مع تقنيات الثورة الصناعية الرابعة كإنترنت الأشياء والحوسبة السحابية؛ إذ يُمكن التحليل اللحظي للبيانات المولدة من أجهزة الاستشعار؛ مما يُحسن كفاءة العمليات الصناعية والخدمية (Truby, 2020).

ويتمثل الفرق الجوهرى بين النماذج التقليدية والحديثة في قدرة النماذج التوليدية على إنتاج بيانات جديدة تحاكي توزيع البيانات الأصلية؛ مما يُحدث تحولاً في مجالات الإبداع والتصميم، لكنه يُثير تحديات تتعلق بملكية المعلومات وسلامتها (منور وبلعيدى، 2025). وقد استحدثت الأدبيات الأكاديمية مفاهيم كالذكاء الاصطناعي المسؤول والموثوق والقابل للتفسير؛ مما يُشير إلى انتقال مجال البحث من التركيز على الأداء التقني إلى دمج الاعتبارات الأخلاقية والقانونية في دورة التطوير (Arrieta et al., 2020).

ويُوضح الجدول (2.1) التصنيف التفصيلي للأجيال الثلاثة للذكاء الاصطناعي، مُبيناً الخصائص الأساسية لكل جيل:

جدول (2.1): تصنيف أجيال الذكاء الاصطناعي وخصائصها الرئيسية

الجيل	الفترة التقريبية	الأسس التقنية	الخصائص الرئيسية	التطبيقات النموذجية
الجيل الأول (القائم على القواعد)	(1950s) - (s1980)	المنطق الصوري، الأنظمة الخبيرة، البرمجة المنطقية	تعتمد على قواعد محددة سلفاً، تفسيرية عالية، محدودة القدرة على التعلم	التشخيص الطبي، تحليل البيانات المالية، نظم دعم القرار
الجيل الثاني (التعلم الإحصائي)	(1990s) - (s2010)	آلات المتجهات الداعمة، الغابات العشوائية، الشبكات العصبية الضحلة	تستخرج الأنماط من البيانات، تحتاج إلى هندسة ملامح يدوية، أداء جيد في المهام المحددة	التصنيف، الانحدار، التعرف على الأنماط، التنبؤ
الجيل الثالث (التعلم العميق والتوليدي)	(s2010) - حتى الآن	الشبكات العصبية العميقة، المحولات، نماذج الانتشار	تعلم ذاتي للسمات، قدرة توليدية عالية، معالجة بيانات ضخمة، تحديات في التفسيرية	معالجة اللغات الطبيعية، توليد الصور، المركبات الذاتية، الأنظمة التوصية

(المصدر: إعداد الباحث بالاعتماد على (Mittal & Sharda, 2023; Taeihagh, 2025; Arrieta et al., 2020).

يكشف الجدول (2.1) عن علاقة عكسية بين التقدم التقني وقابلية التفسير؛ إذ كلما تقدمنا في الأجيال زادت القدرات ولكن قلت الشفافية؛ مما يُشكل معضلة تنظيمية تفرض على الحوكمة الرقمية إيجاد آليات للتعامل مع الأنظمة المعقدة دون التضحية بالابتكار.

وبناءً على ما سبق، يرى الباحث أن التصنيف الجيلي للأنظمة الذكية لا يمثل مجرد تسلسل زمني، بل يعكس تحولاً في النماذج الذهنية للتصميم؛ إذ أصبحت الأنظمة الحديثة أقل شفافية وأكثر صعوبة في التفسير، وهو ما يستدعي تطوير أطر حوكمة قادرة على تتبع سلوكها وضمان امتثالها.

1.2. البنية الهندسية والمعمارية للأنظمة الذكية

تتكون الأنظمة الذكية من (6) طبقات معمارية متكاملة؛ كما يوضحها الشكل الآتي:



شكل (2.1): البنية الهندسية والمعمارية للأنظمة الذكية

يتضح من الشكل أعلاه أن البنية الهندسية والمعمارية للأنظمة الذكية تبدأ بطبقة جمع البيانات وتنقيتها من الأخطاء والقيم الشاذة، ثم طبقة تخزين البيانات وإدارتها عبر نظم قواعد البيانات الموزعة، تليها طبقة معالجة البيانات الأولية وتهيئتها، ثم طبقة بناء النماذج وتدريبها باستخدام خوارزميات التعلم، وبعدها طبقة تقييم الأداء والتحقق من المخرجات، وأخيراً طبقة النشر والمراقبة المستمرة التي تكشف الانحرافات في بيئة التشغيل (Batool et al., 2025). وتُعد البيانات الضخمة المورد الحيوي لهذه المعمارية؛ إذ تؤثر جودة البيانات وكميتها وتنوعها في أداء الخوارزميات بشكل جوهري، وتتطلب إدارة دقيقة لضمان سلامتها (هلال وآخرون، 2022).

كما تشمل منهجيات التعلم الآلي مدارس متعددة؛ منها التعلم الخاضع للإشراف وغير الخاضع للإشراف، والتعلم المعزز، والشبكات العصبية التلافيفية والمتكررة، والمحاولات التي تدعم النماذج اللغوية الضخمة (Bouderhem, 2024). وتعتمد معالجة اللغات الطبيعية على تقنيات التضمين (Embedding)، وآليات الانتباه (Attention) التي تُمكن النماذج من إدراك السياق وإنتاج نصوص متسقة؛ وهو ما مكن من تطوير روبوتات محادثة متقدمة وأنظمة ترجمة فورية (صميدة، 2025).

وتُعد الحوسبة السحابية أساساً لاستضافة هذه الأنظمة؛ إذ توفر مرونة عالية في التوسع وتخفيض التكاليف الرأسمالية، لكنها تُثير تحديات تتعلق بسيادة البيانات وخصوصيتها واعتمادها على شبكات الاتصال (Corrêa et al., 2023). ويتطلب التفاعل بين الإنسان والآلة في النظم

المستدامة تصميم واجهات بديهية تتيح للمستخدمين فهماً كافياً لعمل النظام وآليات التحكم فيه، مع توفير تغذية راجعة واضحة عن أدائه وقراراته (Stahl et al., 2021).

وفي ضوء ذلك، يؤكد الباحث أن البنية الهندسية لا تمثل مجرد تسلسل تقني، بل هي انعكاس للخيارات التصميمية التي تحدد قابلية النظام للتدقيق والمراجعة، وهذا يُشكل أحد المحاور التي تربط الأداء التقني بمتطلبات الامتثال في الحوكمة الرقمية؛ إذ ينبغي أن تكون المعمارية مرنة وقابلة لإعادة التهيئة لتواكب التغيرات في متطلبات العمل والتشريعات.

3. أخلاقيات النظم الذكية والمسؤولية التقنية والمهنية

تستند الأخلاقيات الرقمية إلى مجموعة من المبادئ العالمية التي أقرتها الهيئات الدولية كاليونسكو ومنظمة التعاون الاقتصادي والتنمية، وتشمل: احترام الكرامة الإنسانية، والعدالة، والشفافية، والمساءلة، وعدم الإضرار؛ إذ تُشكل هذه المبادئ إطاراً مرجعياً لتوجيه عملية التطوير (Corrêa et al., 2023). ويُعد التحيز الخوارزمي من أبرز التحديات الأخلاقية؛ إذ تنعكس التحيزات المضمنة في بيانات التدريب -كالتحيزات العرقية والجنسية- على مخرجات النماذج، مما يؤدي إلى ممارسات تمييزية في التوظيف والإقراض والعدالة الجنائية (Barthwal et al., 2025).

وتُعالج هذه المشكلة برمجياً عبر تقنيات إعادة توازن البيانات، وتعديل دوال الخسارة، وفرض قيود رياضية على الإنصاف أثناء التدريب، إلى جانب استخدام أدوات قياس كمية للعدالة (السعيد، 2023). كما تُعزز الشفافية من خلال توثيق مسارات اتخاذ القرار وتوفير تفسيرات مفهومة للمستخدمين والجهات الرقابية، وهو أمر بالغ الأهمية في التطبيقات عالية المخاطر كالقرارات الطبية والمالية (عبد، 2025).

وتتوزع المسؤولية القانونية والتقنية عن الأخطاء الآلية بين المطورين ومشغلي الأنظمة والجهات المستخدمة، مما يستدعي أطراً تنظيمية تحدد نسب التقصير وآليات التعويض، وهو مجال لا يزال يحتاج إلى مزيدٍ من التطوير (فلاق، 2025). وتشمل المعايير المهنية لتصميم الأنظمة المستقلة إجراء تقييمات الأثر الأخلاقي قبل النشر، وتوفير آليات للرقابة البشرية

(Human-in-the-loop)، واعتماد ممارسات الهندسة البرمجية الآمنة التي تدمج اختبارات المتانة والأمن في دورة التطوير (صالح، 2025).

وبناءً على ما سبق، يُشير الباحث إلى أن الأخلاقيات لا تُمثل طبقة إضافية فوق الأنظمة التقنية، بل هي جزء جوهري من هندستها؛ إذ يجب أن تُصمم الخوارزميات مع مراعاة القيم المجتمعية منذ البداية، وهذا يستلزم وجود أطر حوكمة داخلية وخارجية تضمن الالتزام بهذه المبادئ؛ مما يُحقق التكامل بين البعد الأخلاقي والبعد التنظيمي في هذه الدراسة.

4. الابتكار الأخضر وتطوير الخوارزميات منخفضة العبء

تتجه الجهود البحثية إلى تصميم خوارزميات رشيقة وموفرة للموارد للحد من الاستهلاك الطاقوي الهائل للعمليات الحسابية، وذلك من خلال تقنيات: التقطير (Distillation) التي تُنتج نموذجاً صغيراً يحاكي أداء النموذج الكبير، والتكميم (Quantization) الذي يُخفض دقة الأوزان الحسابية، وتقليم الشبكات (Pruning) الذي يزيل الوصلات العصبية غير المؤثرة (Burnaev et al., 2023). وتُعد إعادة تدوير البيانات وتحسين كفاءة التخزين الرقمي من الاستراتيجيات المهمة؛ حيث يُمكن الاستفادة من مخرجات النماذج السابقة كبيانات تدريب للنماذج اللاحقة مع ضمان تجنب التحيز التراكمي عبر تقنيات توزيع مناسبة (طاهر، 2024).

وتنهض منهجية الابتكار المسؤول على دمج اعتبارات الاستدامة في كل مرحلة من دورة حياة البرمجيات الذكية، بحيث تُصبح الاستدامة معياراً هندسياً أساسياً (Sætra, 2023). وتسهم الاستدامة التقنية في تعزيز التنافسية المؤسسية عبر خفض التكاليف التشغيلية للطاقة والتبريد وتحسين السمعة البيئية، وهو ما يُشكل ميزة في الأسواق التي تتبنى معايير ESG (Gkiotsalitis & Cats, 2022).

وتُعالج الحلول البرمجية ظاهرة الهلوسة في النماذج التوليدية -أي توليد معلومات غير صحيحة- عبر آليات التحقق الواقعي (Grounding)، والاسترجاع المعزز (RAG) التي تربط المخرجات بمصادر موثوقة؛ مما يُقلل معدل الأخطاء ويُعزز مصداقية النظام (Taeihagh, 2025). وتتضمن استراتيجيات تقليل الاستهلاك الطاقوي أيضاً تحسين كفاءة مراكز البيانات عبر

استخدام مصادر الطاقة المتجددة وتقنيات التبريد المتطورة؛ مما يُخفض البصمة الكربونية الإجمالية.

وعليه، يرى الباحث أن الابتكار الأخضر في الذكاء الاصطناعي لا يُعد خياراً أخلاقياً منعزلاً، بل ضرورة اقتصادية وتشغيلية ملحة؛ إذ أن تكاليف الطاقة تشكل نسبة متزايدة من ميزانيات المؤسسات التقنية، وتتزايد الضغوط التنظيمية لخفض الانبعاثات، مما يجعل تطوير خوارزميات منخفضة العبء استثماراً استراتيجياً يعود بفوائد مزدوجة على الكفاءة التشغيلية والامتثال البيئي، وهذه الفائدة تُعد وسيلة لتعزيز أطر الحوكمة المستدامة التي تسعى الدراسة إلى تحليلها.

5. اقتصاديات الذكاء الاصطناعي المستدام وعائد الاستثمار

يستلزم بناء وصيانة النظم المستدامة تحليلاً دقيقاً للتكاليف التشغيلية التي تشمل تكاليف البنية التحتية السحابية، واستهلاك الطاقة الكهربائية، وتخزين البيانات الضخمة، وتطوير النماذج وتدريبها، والصيانة المستمرة وتحديث الأنظمة (Burnaev et al., 2023). ويُقاس العائد على الاستثمار (ROI) في التقنيات الخضراء عبر خفض فواتير الطاقة، وتقليل تكاليف الامتثال القانوني بتجنب الغرامات، وتحقيق مكاسب السمعة المؤسسية التي تترجم إلى زيادة حصة السوق وثقة المستثمرين (السعيد، 2024).

ويؤثر التشغيل الآلي الذكي على سوق العمل بإحلال بعض المهام الروتينية، مع إيجاد فرص جديدة في تطوير الخوارزميات وحوكمة البيانات والأخلاقيات الرقمية؛ مما يستلزم إعادة تأهيل القوى العاملة بمهارات متقدمة (Truby, 2020). وتسهم الاستدامة في خفض التكاليف طويلة الأمد عبر تحسين كفاءة الموارد وتقليل النفايات الرقمية، وتجنب الغرامات الناتجة عن مخالفة التشريعات البيئية والرقمية (فلاق، 2025). وتشمل استراتيجيات التمويل لدعم الابتكارات المسؤولة المنح الحكومية، والصناديق الاستثمارية المتخصصة في التقنيات النظيفة، والشراكات بين القطاعين العام والخاص (صميده، 2025).

واتساقاً مع ما تقدم، يؤكد الباحث أن الجدوى الاقتصادية للذكاء الاصطناعي المستدام تتجاوز خفض التكاليف المباشرة؛ لتشمل تعزيز القدرة التنافسية، وتحسين إدارة المخاطر، وفتح أسواق

جديدة، مما يجعل الاستثمار في هذا المجال استراتيجياً؛ ولذا ينبغي على المؤسسات تبني رؤية متكاملة تربط الأداء التقني بالأثر البيئي والعائد المالي، ويتقاطع هذا الطرح مباشرة مع متغير الحوكمة الرقمية في الدراسة.

6. المهددات السيبرانية والمخاطر المرتبطة بالأنظمة المستقلة

تتعرض أنظمة الذكاء الاصطناعي لهجمات سيبرانية نوعية تستهدف مراحل التدريب والتشغيل والاستدلال؛ ومن أبرزها: هجمات التسميم (Poisoning) التي تُدخل بيانات خبيثة إلى مجموعة التدريب بهدف تشويه النموذج، وهجمات الاستدلال العكسي (Model Inversion) التي تستخرج بيانات التدريب الحساسة من النموذج المدرب عبر تحليل مخرجاته، وهجمات التعارض (Adversarial Attacks) التي تُضيف تشويهاً دقيقاً للمدخلات لتضليل النموذج وجعله يصنفها خطأً (El Mestari et al., 2024). ويُشكل التلاعب ببيانات التدريب خطراً كبيراً على سلامة المخرجات؛ خاصة في التطبيقات الأمنية والمالية؛ إذ قد يؤدي إلى قبول قرارات خاطئة أو رفض قرارات صحيحة (الررفافي، 2025).

كما تُهدد الخصوصية الفردية في بيئات الذكاء الاصطناعي من خلال إعادة تحديد الهوية عبر دمج قواعد بيانات متعددة، مما يجعل تقنيات إزالة الهوية التقليدية غير كافية (Ploug, 2023). وتنتج عن القرارات الآلية المستقلة آثار جانبية غير متوقعة، كتفاقم التحيزات الاجتماعية أو إحداث أضرار مادية في الأنظمة الفيزيائية السيبرانية؛ مما يُبرز أهمية نمذجة السيناريوهات المتطرفة واختبار المتانة في بيئات محاكاة متنوعة (Kaminski & Malgieri, 2021).

وتُعد نقاط الضعف البرمجية في معمارية الأنظمة الذكية مدخلاً رئيسياً للهجمات؛ حيث قد تحتوي المكتبات والأطر المستخدمة على ثغرات أمنية غير مكتشفة، أو قد يُساء تكوين الإعدادات الأمنية؛ مما يستدعي تطبيق ممارسات التطوير الآمن (Secure SDLC) كمراجعات الكود، واختبارات الاختراق، وتحليل نقاط الضعف الثابت والديناميكي (Kuner et al., 2021). ويُستخدم الذكاء الاصطناعي أيضاً بشكل عدائي في تطوير هجمات سيبرانية متطورة كالتصيد الذكي المدعوم بتوليد نصوص مخصصة ومقنعة، والبرمجيات الخبيثة التكيفية؛ مما يستدعي تطوير أنظمة دفاع تعتمد على الذكاء الاصطناعي نفسه لكشف الأنماط الشاذة (Ye & Zhang, 2024).

وفي هذا السياق، يرى الباحث أن إدارة المخاطر السيبرانية للأنظمة الذكية تتطلب نهجاً استباقياً متعدد الطبقات يشمل حماية البيانات، وتأمين الخوارزميات، ومراقبة الأداء، وتدريب الكوادر، ووضع خطط استجابة للحوادث والتعافي منها؛ وهو ما يتوافق مع متطلبات الأمن السيبراني في التشريعات الحديثة (PDPL)، و(GDPR)، ويتصل هذا الطرح ارتباطاً وثيقاً بمتغير الحوكمة الرقمية في الدراسة. ويُوضح الشكل (2.2) تصنيف الهجمات السيبرانية على أنظمة الذكاء الاصطناعي وفقاً لمرحلة الاستهداف والطبقة المعمارية:



شكل (2.2): تصنيف الهجمات السيبرانية على أنظمة الذكاء الاصطناعي وطبقات استهدافها

يُبرز الشكل (2.2) تعدد جبهات الهجوم على الأنظمة الذكية، مما يعني أن الحوكمة الأمنية لا يمكن أن تقتصر على نقطة دخول واحدة، بل تستلزم تأميناً شاملاً لكل طبقات المعمارية، وهذا يفرض تصميم أطر رقابية متكاملة تغطي دورة الحياة الكاملة للنظام.

في ضوء ما سبق، يرى الباحث أن تعقيد الهجمات السيبرانية وتنوعها يستدعي تحولاً في الفكر الأمني من الحماية التفاعلية إلى المنظومة الاستباقية المتكاملة، حيث تتطلب إدارة المخاطر السيبرانية للأنظمة الذكية ربطاً وثيقاً بين الأمن التقني والحوكمة الرقمية، مع إدراك أن حماية الخصوصية وسلامة القرارات الآلية تمثلان ركيزتين متلازميتين لا يمكن فصلهما، مما يُعزز أهمية بناء أطر تنظيمية متكاملة تغطي دورة حياة النظام بأكملها.

7. معايير الجودة والتميز والامتثال في البرمجيات الذكية

تُعد مؤشرات قياس الأداء النوعي أدوات أساسية لتقييم جودة نماذج الذكاء الاصطناعي، ومن أبرزها الدقة (Accuracy) التي تقيس نسبة التنبؤات الصحيحة، والاسترجاع (Recall) الذي يُحدد

قدرة النموذج على اكتشاف الحالات الإيجابية، ودرجة (F1) التي تجمع بين الدقة والاسترجاع، ومنحنى الخصائص التشغيلية (ROC-AUC) الذي يُقِيم أداء النموذج في التمييز بين الفئات (Pamuk et al., 2024). وتشمل اختبارات المتانة والقوة (Robustness Testing) تعريض النماذج لمدخلات متطرفة أو مشوشة أو معدلة خصيصاً لتحدي أدائها، وقياس قدرتها على الحفاظ على الدقة في ظل هذه الظروف، وهو أمر ضروري للأنظمة المستخدمة في بيئات غير مستقرة كأنظمة التعرف على الوجه في ظروف إضاءة مختلفة أو أنظمة القيادة الذاتية في طقس سيئ (Lukács & Váradi, 2023).

وتُطبق معايير الأمان والجودة العالمية، مثل: (ISO/IEC 25010) التي تُركز على جودة البرمجيات من حيث الوظيفية والموثوقية والكفاءة وقابلية الصيانة، و(ISO/IEC 27001) المتخصصة في أنظمة إدارة أمن المعلومات، و(ISO/IEC 42001) الخاصة بنظام إدارة الذكاء الاصطناعي، مما يُوفر أطراً مرجعية لضمان امتثال الأنظمة للمتطلبات الدولية ويُسهل عمليات التدقيق والاعتماد (van der Schyff et al., 2024).

وتُعد آليات التدقيق التقني المستمر، كمراقبة أداء النماذج بعد النشر واكتشاف الانحراف (Concept Drift) الذي يحدث عندما تتغير العلاقات الإحصائية بين المدخلات والمخرجات بمرور الوقت، ضرورة للحفاظ على جودة المخرجات، إذ تتيح إعادة تدريب النماذج أو تعديلها بشكل دوري لاستيعاب التغيرات (Lazcoz & De Hert, 2023).

جدول (2.2): معايير الجودة والامتثال الدولية لأنظمة الذكاء الاصطناعي

المعيار	النطاق	المجال الرئيسي	المتطلبات الأساسية
ISO/IEC 25010	جودة البرمجيات	الوظيفية، الموثوقية، الكفاءة، قابلية الصيانة	تقييم شامل لجودة المنتج البرمجي وفق أبعاد متعددة
ISO/IEC 27001	أمن المعلومات	إدارة أمن المعلومات	تطبيق ضوابط أمنية، إدارة المخاطر، التحسين المستمر
ISO/IEC 42001	الذكاء الاصطناعي	نظام إدارة الذكاء الاصطناعي	تطوير واستخدام مسؤول، إدارة المخاطر، الشفافية
ISO 24029	قابلية تفسير النماذج	تقييم قابلية التفسير	تقييم مدى فهم قرارات النموذج وتوثيقها

(المصدر: إعداد الباحث بالاعتماد على: Pamuk et al., 2024; van der Schyff et al., 2024).

يُلاحظ من الجدول تعدد أطر الجودة المعيارية وتداخلها، مما يُشير إلى أن الامتثال الكامل يتطلب تنسيقاً بين هذه المعايير، وهذا يُشكل تحدياً للمؤسسات، ولكنه في الوقت نفسه يُوفر مرونة في اختيار المسار المناسب لحوكمة أنظمتها وفق سياقها التشغيلي.

وبناءً على ذلك، يرى الباحث أن ضمان جودة البرمجيات الذكية يتطلب نهجاً منهجياً يدمج اختبارات الأداء والمتانة والأمان والامتثال في جميع مراحل التطوير، مع الاستعانة بأطر معيارية معترف بها دولياً، كما ينبغي أن تكون عمليات التدقيق والمراقبة مستمرة وليست حدثاً لمرة واحدة، لأن الأنظمة الذكية تتطور وتتفاعل مع بيئات متغيرة، مما يستوجب تقييماً دورياً وتصحيحاً مستمراً، وهذا ما يُعزز فعالية أطر الحوكمة الرقمية.

8. الذكاء الاصطناعي الموثوق والقابلية للتفسير الخوارزمي

تُعد قابلية التفسير (Explainability) سمة جوهرية للأنظمة الموثوقة، وتعني قدرة النظام على تقديم تفسيرات مفهومة لقراراته للمستخدمين والمطورين والجهات الرقابية، بحيث تُفهم العوامل المؤدية إلى نتيجة معينة والوزن النسبي لكل عامل، مما يُمكن من التحقق من صحة القرارات وكشف الأخطاء أو التحيزات (Arrieta et al., 2020).

وتبرز معضلة الصندوق الأسود بشكل خاص في النماذج المعقدة كالشبكات العصبية العميقة والمحولات، إذ يصعب تتبع خطوات اتخاذ القرار داخلها بسبب عدد الطبقات الهائل والتفاعلات غير الخطية بين العصبونات، مما يُضعف الثقة في مخرجاتها ويُعيق تحقيق الشفافية المطلوبة قانونياً (Cheong, 2024). ولمواجهة ذلك، تُستخدم تقنيات التفسير المحلية، مثل: (LIME و SHAP) التي تُقارب سلوك النموذج محلياً حول نقطة محددة لتقدير تأثير كل متغير، والتقنيات العالمية مثل: (Decision Trees surrogate) التي تُبني نموذجاً بسيطاً يحاكي النموذج المعقد على المستوى الكلي، مما يُسهل فهم آليته العامة (Gonçalves & Correia, 2026).

وتُعد الموثوقية أمراً بالغ الأهمية في الأنظمة ذات الحساسية العالية كالرعاية الصحية والقيادة الذاتية والطيران، حيث يتطلب أي خطأ محتملاً تدقيقاً دقيقاً وتصميماً مقاوماً للفشل، إلى جانب آليات للكشف المبكر عن الانحرافات وتصحيحها (Bouderhem, 2024). ويرتبط التفسير التقني

بعمليات الامتثال القانوني بشكل مباشر، إذ تنص تشريعات مثل (GDPR) على حق الأفراد في الحصول على تفسير للقرارات الآلية التي تمسهم (المادة 22)، وكذلك يُشترط في أنظمة الذكاء الاصطناعي عالية المخاطر بموجب قانون الذكاء الاصطناعي الأوروبي توفير وثائق تقنية شاملة (Noë et al., 2025).

وقد تناولت الأدبيات الحديثة هذا الحق في التفسير من عدة زوايا؛ إذ قدمت دراسة (Kumkar & Roth-Isigkeit, 2021) منهجاً قائماً على المعايير لتفسير متطلبات التفسير بموجب اللائحة، داعية إلى تفسير تقييدي للأحكام ذات الصلة، بينما حلت أطروحة (Dirutigliano, 2023) العلاقة بين التكنولوجيا الحديثة والمفاهيم القانونية للتفسير والشفافية، مقدمة إطاراً تفسيرياً لهذا الحق وتوصيات لتطويره في مواجهة أنظمة الذكاء الاصطناعي غير الشفافة.

كما ناقش (Tzimas, 2023) الشفافية الخوارزمية والقابلية للتفسير في القانون الأوروبي، مستكشفاً سبل الانتصاف القانونية التي تضمن الشفافية والمساءلة في مواجهة تأثير الصندوق الأسود للخوارزميات. وتجدر الإشارة إلى أن التفسيرية ليست غاية في حد ذاتها، بل وسيلة لتحقيق أهداف أوسع كالمساءلة والعدالة والسلامة، ولذا ينبغي موازنة مستوى التفسير مع احتياجات الفئات المختلفة من المستخدمين ومستوى المخاطر المرتبط بالتطبيق (الموح، 2024).

وفي ضوء ما سبق، يرى الباحث أن تحقيق التوازن بين الأداء العالي للنماذج وقابليتها للتفسير يُعد تحدياً مستمراً، إذ غالباً ما تُضحي النماذج الأكثر تعقيداً بقابلية التفسير مقابل دقة أعلى، مما يستلزم مقايضات تصميمية واعية، واستثماراً في أدوات التدقيق والتوثيق لضمان الامتثال التنظيمي دون إعاقة الابتكار، وهو ما يُشكل جوهر التحدي الذي تواجهه أطر الحوكمة الرقمية.

9. التوجهات المستقبلية والآفاق القادمة للتقنيات الذكية

يُتوقع أن يُحدث الذكاء الاصطناعي العام (AGI)، والفائق (ASI) تحولاً جذرياً في القدرات التقنية، إذ ستكون هذه الأنظمة قادرة على أداء أي مهمة معرفية يمكن للبشر أدائها، بل وتجاوزهم في العديد من المجالات، مما يُثير مخاوف جدية تتعلق بالسيطرة البشرية على مثل هذه الأنظمة،

والسلامة الوجودية، والأخلاقيات، وهو ما يستدعي وضع أطر حوكمة دولية قوية وضمانات أمنية قبل الوصول إلى هذه المرحلة (Taeihagh, 2025).

ويُعد الاندماج الاستراتيجي بين الحوسبة الكمية والذكاء الاصطناعي من أبرز الآفاق المستقبلية، إذ ستتيح الحواسيب الكمية معالجة مسائل معقدة في زمن قياسي بفضل مبادئ التراكب والتشابك الكمي، مما يُعزز قدرات النماذج في مجالات كالتشفير والمحاكاة الجزيئية وتحسين الخوارزميات (Majeed & Hwang, 2024). وتتجه الأبحاث نحو تطوير نظم ذكية ذاتية الإصلاح والتطوير المستقل، أي أنظمة قادرة على اكتشاف أخطائها البرمجية أو المنطقية وتصحيحها دون تدخل بشري، وهو ما يُعد نقلة في مجال الهندسة البرمجية، لكنه يفرض تحديات تنظيمية جديدة تتعلق بالمساءلة والسلامة والرقابة (Hulok, 2025).

وتؤدي الأنظمة المدمجة (Embedded Systems) دوراً محورياً في قيادة التحولات الرقمية الكبرى، خاصة في المدن الذكية التي تعتمد على أجهزة استشعار موزعة، والمركبات ذاتية القيادة التي تتطلب معالجة لحظية، والرعاية الصحية عن بعد التي تستخدم أجهزة قابلة للارتداء (Patel & Kumar, 2025). ويُعد الاستشراف الاستراتيجي لاستدامة البنى التحتية التقنية أمراً ضرورياً لتجنب التقادم التكنولوجي وضمان استمرارية الخدمات، ويشمل وضع خطط لتحديث الأجهزة والبرمجيات بشكل دوري، وتطوير معايير للتوافق مع الأنظمة الجديدة، وتقييم المخاطر المستقبلية المرتبطة بالتغيرات التقنية والبيئية (Tjondronegoro, 2024).

وتقوم الرؤية المستقبلية لاستدامة التقنية على تحقيق توازن بين الابتكار وحماية الحقوق والبيئة، وهو ما يستدعي تطوير أطر حوكمة مرنة تتكيف مع تسارع التغيرات التقنية، وإشراك جميع أصحاب المصلحة في عمليات صنع القرار، واعتماد مبادئ التصميم التكيفي (Zhong et al., 2025).

وبناءً على ما تقدم، يرى الباحث أن التوجهات المستقبلية للتقنيات الذكية تتطلب نهجاً استباقياً يجمع بين البحث العلمي، والاستثمار في البنى التحتية، وتطوير الكوادر البشرية، ووضع تشريعات مرنة، وبناء تحالفات دولية لمواجهة التحديات العابرة للحدود، كما أن استدامة الأنظمة الذكية لن

تتحقق إلّا من خلال تكامل الجهود التقنية والقانونية والاجتماعية، وهو ما يُشكل جوهر الإطار النظري لهذه الدراسة.

10. العلاقة التكاملية بين الذكاء الاصطناعي المستدام والحوكمة الرقمية

تتضح العلاقة التكاملية بين الذكاء الاصطناعي المستدام والحوكمة الرقمية من خلال عدة أبعاد تشغيلية واستراتيجية، إذ تُعد الحوكمة الرقمية الإطار الذي يضمن تطبيق مبادئ الاستدامة في تصميم وتشغيل الأنظمة الذكية، من خلال وضع سياسات واضحة لكفاءة الطاقة، وإدارة المخاطر السيبرانية، وضمان الشفافية والمساءلة (Batool et al., 2025).

وتؤدي الحوكمة دوراً محورياً في ترجمة المبادئ الأخلاقية إلى متطلبات تنفيذية ملزمة، كالإزام المطورين بإجراء تقييمات الأثر الأخلاقي قبل النشر، وتوفير آليات للرقابة البشرية، واعتماد معايير التدقيق المستمر (Birkstedt et al., 2023). كما تُسهم الحوكمة في تحقيق التوازن بين الابتكار والامتثال من خلال إنشاء بيئات اختبار تنظيمية (Sandbox) تسمح بتجربة تقنيات جديدة تحت رقابة، وتوفير حوافز للالتزام بالاستدامة كالتخفيضات الضريبية أو الأولوية في العقود الحكومية (Zaidan & Ibrahim, 2024).

ويتجلى التكامل أيضاً في مجال حماية البيانات الشخصية، حيث تفرض الحوكمة ضوابط صارمة على جمع ومعالجة وتخزين البيانات المستخدمة في تدريب الأنظمة الذكية، مما يُقلل مخاطر انتهاك الخصوصية ويعزز ثقة الأفراد (هلال وآخرون، 2022). وتعمل الحوكمة الرقمية كجسر يربط بين الأهداف التقنية للذكاء الاصطناعي المستدام (كخفض البصمة الكربونية، وتحسين الكفاءة)، والأهداف المجتمعية (كحماية الحقوق وتعزيز العدالة)، وهو ما يحقق قيمة مضافة تتجاوز مجموع الأجزاء (OECD, 2024).

جدول (2.3): ملخص تحليلي لمتطلبات الحوكمة الرقمية للذكاء الاصطناعي المستدام

البُعد	المتطلبات الرئيسية	الآليات التنفيذية	المؤشرات المقترحة
الأخلاقي	العدالة، الشفافية، المساءلة، عدم الإضرار	تقييم الأثر الأخلاقي، الرقابة البشرية، مدونات السلوك	نسبة التحيز المكتشف، عدد التظلمات، درجة الشفافية
البيئي	خفض البصمة الكربونية، كفاءة الطاقة	تحسين الخوارزميات، استخدام طاقة متجددة، تبريد فعال	استهلاك الطاقة لكل تدريب، انبعاثات CO ₂ ، كفاءة التبريد
الأمني	حماية البيانات، مقاومة الهجمات، الاستجابة للحوادث	تشفير، مراقبة مستمرة، خطط استجابة	عدد الحوادث، زمن الاستجابة، مستوى الامتثال الأمني
القانوني	الامتثال للتشريعات، حماية الخصوصية	أدوات امتثال آلية، تدقيق دوري، توثيق	نسبة الامتثال، عدد الغرامات، جودة السجلات
الاقتصادي	الجدوى المالية، العائد على الاستثمار	تحليل التكلفة، حوافز الاستدامة	ROI، خفض التكاليف، نمو الحصة السوقية

(المصدر: إعداد الباحث بالاعتماد على: Batool et al., 2025; Birkstedt et al., 2023; Zaidan & Ibrahim, 2024).

يُظهر الجدول (2.3) تنوع أبعاد الحوكمة وترابطها، مما يؤكد أن تحقيق الاستدامة في الذكاء الاصطناعي ليس مجرد تحدٍ تقني، بل هو مسعى متعدد التخصصات يتطلب تنسيقاً بين السياسات الأخلاقية والبيئية والقانونية والاقتصادية، وهذا يفرض على المؤسسات تطوير كفاءات إدارية متكاملة.

وفي هذا السياق، يرى الباحث أن الذكاء الاصطناعي المستدام والحوكمة الرقمية ليسا مجالين منفصلين، بل وجهان لعملة واحدة، إذ لا يمكن تحقيق الاستدامة دون حوكمة رشيدة، ولا يمكن للحوكمة أن تكون فعالة دون الاستفادة من إمكانات الذكاء الاصطناعي في تحسين عمليات الرقابة والامتثال، وهذا الترابط يُشكل الأساس المنطقي للدراسة الحالية التي تسعى إلى تحليل آليات الامتثال في إطار حوكمة متكامل، وهو ما سيتم تناوله بالتفصيل في المحاور اللاحقة من الإطار النظري.

المحور الثاني: حماية البيانات الشخصية

يُعد هذا المحور الأساس القانوني والتقني لضمان خصوصية الأفراد في البيئة الرقمية، إذ يتناول الماهية المفاهيمية، والمبادئ الجوهرية للمعالجة، والحقوق الرقمية، وتقنيات الأمن السيبراني، ومنهجيات الخصوصية بالتصميم، وإدارة الحوادث، وحماية البيانات في الحوسبة السحابية، ونقاط البيانات الضخمة مع الخصوصية، والتوعية المؤسسية. وتُعد حماية البيانات الشخصية مطلباً أساسياً للحوكمة الرشيدة، إذ تشكل الأساس الذي يمكن الأفراد من ممارسة سيطرتهم على معلوماتهم، وتفرض على المؤسسات التزامات تنظيمية وتقنية لضمان المعالجة المسؤولة.

1. الماهية القانونية والتقنية للبيانات الشخصية

تُعرف البيانات الشخصية في الفضاء السيبراني المعاصر بأنها كل معلومة تتعلق بفرد محدد أو يمكن التعرف عليه مباشرة أو بطريقة غير مباشرة، وقد توسع هذا المفهوم ليشمل المعارف الرقمية كالبريد الإلكتروني وعناوين (IP) وبيانات الموقع والمعرفات الحيوية (الحسّات، 2025). وتصنف البيانات وفقاً لمستويات الحساسية إلى: بيانات عادية (كالاسم والعنوان)، وبيانات حساسة (كالمعتقدات الدينية والانتماءات السياسية والبيانات الصحية)، وبيانات حيوية (كبصمات الأصابع والجيّينات)، ولكل فئة متطلبات حماية تتناسب مع درجة المخاطر المرتبطة بها (أبو خمرة، 2021).

وتُعالج البيانات الحساسة والحيوية تقنياً بتشفير أقوى وضوابط وصول مشددة، وفقاً لمتطلبات تشريعية مثل المادة (9) من GDPR والمواد (5-6) من PDPL (الجيجلي، 2025). ويتمثل الفرق البرمجي الجوهرى بين البيانات المجهلة (Anonymous) التي لا يمكن نسبتها إلى فرد، والبيانات ذات الأسماء المستعارة (Pseudonymous) التي تحتاج إلى مفتاح لإعادة التعريف؛ في أن الأخيرة لا تزال تصنف بيانات شخصية وفقاً لمعظم التشريعات، إذ يُمكن إعادة ربطها بالهوية عبر المفتاح، مما يستوجب تطبيق ضوابط الحماية نفسها (الشمري، نجم، 2023).

وتؤدي البيانات دوراً محورياً في تشكيل الهوية الرقمية للأفراد والمؤسسات، إذ تسهم ملفات البيانات الرقمية في بناء صورة شاملة عن الشخص، مما يُعزز الحاجة إلى حماية دقيقة لمنع إساءة الاستخدام (رجب، 2024). وتتضمن دورة حياة البيانات مراحل متسلسلة؛ تبدأ بجمع البيانات، ثم تسجيلها وتخزينها، ثم معالجتها وتحليلها، ثم نقلها ومشاركتها، وأخيراً إتلافها بشكل آمن عند انتهاء الغرض، وتخضع كل مرحلة لمتطلبات قانونية وتقنية تهدف إلى ضمان الخصوصية والأمان طوال العمر الافتراضي للبيانات (العجمي، 2023).

ويُلخص الجدول الآتي تصنيف البيانات الشخصية وفقاً لمستويات الحساسية ومتطلبات الحماية الأساسية لكل مستوى والأساس التشريعي المقابل:

جدول (2.5): تصنيف البيانات الشخصية وفقاً لمستويات الحساسية ومتطلبات الحماية

مستوى الحساسية	أنواع البيانات	متطلبات الحماية الأساسية	الأساس التشريعي
بيانات عادية	الاسم، العنوان، البريد الإلكتروني، رقم الهاتف	تشفير أساسي، التحكم في الوصول، إشعار الشفافية	المادة (5) PDPL، المادة (6) GDPR
بيانات حساسة	المعتقدات الدينية، الانتماءات السياسية، البيانات الصحية، البيانات الجنائية	تشفير متقدم، موافقة صريحة، تقييم الأثر، تقييد النقل	المادة (9) GDPR، المادة (6) PDPL
بيانات حيوية	بصمات الأصابع، التعرف على الوجه، بيانات الحمض النووي، بيانات الشبكية	أعلى مستويات التشفير، موافقة خاصة، حظر المعالجة إلا لضرورة قصوى	المادة (9) GDPR، المادة (6) PDPL (فئة مستقلة)

(المصدر: إعداد الباحث بالاعتماد على: الحسنة، 2025؛ أبو خمرة، 2021؛ الجبجلي، 2025).
يُصنف الجدول (2.5) البيانات الشخصية وفقاً لثلاثة مستويات حساسية، مُبيناً متطلبات الحماية الأساسية لكل مستوى والأساس التشريعي المقابل، مما يُساعد المؤسسات على تحديد الإجراءات المناسبة لمعالجة كل فئة من البيانات وضمان الامتثال للمعايير القانونية.

2. المبادئ الجوهرية لمعالجة البيانات في البيئات الذكية

تستند معالجة البيانات الشخصية إلى مبادئ جوهرية نصت عليها كبرى التشريعات الدولية والوطنية، وتتمثل في المشروعية (أي وجود أساس قانوني للمعالجة)، والعدل (أي عدم التمييز أو التحيز في المعالجة)، والشفافية (أي إعلام أصحاب البيانات بكيفية معالجة بياناتهم وأغراضها

والجهات المشاركة) (سويلم، 2022). وتتمثل الآليات التقنية لتقييد الغرض (Purpose Limitation) في تصميم أنظمة تمنع استخدام البيانات لأغراض غير مصرح بها، عبر إرفاق سياسات الاستخدام (Usage Policies) بالبيانات نفسها وتطبيق ضوابط برمجية تمنع الوصول غير المصرح به (الوادي، 2025).

وتُعد خوارزميات تقليل البيانات (Data Minimization) من الممارسات التقنية الأساسية، إذ تُحصر جمع البيانات في الحد الأدنى الضروري لتحقيق الغرض المعلن، مما يقلل من مخاطر التسريب والاستخدام غير المشروع ويُخفض التكاليف التشغيلية (محمود، 2024). وتضمن دقة السجلات الرقمية من خلال آليات التحقق الآلي والمستمر، كاستخدام المصادقة متعددة العوامل، وتحديث البيانات بشكل دوري بناءً على إشعارات الأفراد، وتطبيق خوارزميات تنظيف البيانات التي تكتشف الأخطاء وتصحيحها تلقائياً (الشامسي، 2023).

وتُبرمج فترات التخزين والإتلاف التلقائي وفقاً لسياسات الاحتفاظ المحددة، حيث تُحذف البيانات تلقائياً بعد انقضاء الغرض أو بناءً على طلب الفرد، مع ضمان عدم إمكانية استعادتها عبر تقنيات المسح الآمن وإعادة الكتابة (الرحلي، 2026). وتُعد النزاهة والسرية مبدأين جوهريين لحماية الخصوصية، وتُطبقان عبر التشفير الشامل، والتحكم الدقيق في الوصول، وتسجيل جميع عمليات المعالجة والوصول في سجلات تدقيق غير قابلة للتلاعب (القطاطشة، 2022).

وبناءً على ما سبق، يرى الباحث أن المبادئ الجوهرية للمعالجة ليست مجرد التزامات قانونية شكلية، بل تمثل معايير تصميمية جوهرية تُشكل بنية الأنظمة التقنية، إذ ينبغي أن تُدمج في كل مرحلة من مراحل تطوير البرمجيات لضمان أن تكون المعالجة قانونية وعادلة وشفافة منذ البداية، وهذا التكامل يُقلل من احتمالات الانتهاك ويُعزز ثقة الأفراد في الأنظمة الرقمية.

3. الحقوق الرقمية لأصحاب البيانات الشخصية

يمنح قانونا حماية البيانات أصحاب البيانات مجموعة من الحقوق الرقمية التي تُعد تجسيدا لسيادتهم على معلوماتهم الشخصية، وأولها حق الوصول والاطلاع، الذي يُمكن الأفراد من طلب نسخة من بياناتهم التي تحتفظ بها المنشأة، وتُقدم هذه الخدمة عبر بوابات إلكترونية آمنة مزودة

بآليات مصادقة قوية لضمان هوية الطالب (العتيبي، 2025). ويسمح حق التصحيح والتعديل للفرد بطلب تعديل بياناته غير الدقيقة أو الناقصة، ويتطلب ذلك آليات تحقق لتوثيق الطلب وتنفيذه دون تأخير مفرط، وغالباً ما تُدمج هذه الآلية مع أنظمة إدارة الهوية الرقمية لتسهيل التحديث الفوري (الشمري، 2023).

ويُعد حق المسح أو النسيان الرقمي من الحقوق المحورية في البيئة الرقمية، إذ يسمح للفرد بطلب حذف بياناته من قواعد البيانات الموزعة، وهو تحدٍ تقني كبير يتطلب تنسيقاً بين الأنظمة المختلفة لضمان الحذف الشامل دون ترك أثر، وقد يتطلب ذلك تقنيات الحذف الآمن وإعادة الكتابة (الجندي، 2023). وتشمل المعايير التقنية لنقل البيانات (القابلية للنقل) توفير البيانات بتنسيقات مفتوحة قابلة للقراءة آلياً (مثل JSON، XML، CSV)، مما يُسهل نقلها بين مقدمي الخدمات المختلفين دون فقدان الجودة أو سلامة البيانات (المدبولي، 2022).

ويُمكن حق الاعتراض على المعالجة الآلية الفرد من تعديل تفضيلاته أو إلغاء موافقته، وهو ما يُترجم تقنياً عبر واجهات المستخدم المتقدمة وإدارة التفضيلات (Preferences Management) التي تتيح للمستخدم التحكم الدقيق في كيفية معالجة بياناته (البقلي، 2021). ويُعد الحق في عدم الخضوع لقرارات آلية بالكامل دون تدخل بشري ضماناً مهماً، خاصة في القرارات التي تمس حقوق الفرد بشكل كبير كالقرارات الائتمانية والتوظيفية، ويتطلب ذلك توفير آليات للاستئناف البشري للقرارات الآلية، مع إتاحة تفسيرات واضحة لكيفية وصول النظام إلى قراره (فلانة، 2025).

وفي ضوء ذلك، يرى الباحث أن الحقوق الرقمية ليست مجرد بنود قانونية نظرية، بل تمثل معايير تشغيلية يجب أن تُترجم إلى ميزات تقنية قابلة للتنفيذ في الأنظمة، كما أن فعالية هذه الحقوق تعتمد على سهولة ممارستها من قبل الأفراد، مما يستدعي تصميم واجهات مستخدم بديهية وإجراءات مبسطة، وهذا يُشكل تحدياً هندسياً يتطلب موازنة بين الأمان وسهولة الاستخدام.

4. الأمن السيبراني وتقنيات حماية الخصوصية المتقدمة

يُعد التشفير بجميع أشكاله المتمثل، مثل: (AES-256)، وغير المتمثل، مثل: (RSA-4096) الدعامة الجوهرية لحماية تدفق البيانات أثناء التخزين والنقل، وتُستخدم أيضاً تقنيات التشفير

المتجانسة (Homomorphic Encryption) التي تسمح بإجراء عمليات حسابية على بيانات مشفرة دون فك تشفيرها، مما يوفر حماية عالية أثناء المعالجة ويُمكن من تحليل البيانات دون كشف محتواها (El Mestari et al., 2024). وتشمل تقنيات إخفاء الهوية، وتعمية السجلات استبدال المعارف بقيم عشوائية أو إضافة تشويش مضبوط، مما يحول دون إعادة تحديد الهوية، وتُستخدم هذه التقنيات على نطاق واسع في بيئات الاختبار والتحليل الإحصائي (المحروقي، 2023).

وتُعد الخصوصية التفاضلية (Differential Privacy) منهجية رياضية حديثة تُضيف تشويشاً مضبوطاً إلى نتائج الاستعلامات لضمان عدم إمكانية استنتاج معلومات فردية من الإحصائيات المنشورة، وهي معيار معتمد لدى المؤسسات الكبرى وتُعد من أفضل الممارسات في النشر الآمن للإحصاءات (Oh et al., 2025). وتُستخدم جدران الحماية (Firewalls) المتطورة وأنظمة كشف التسلل الرقمي المعرفية (IDS/IPS) المدعومة بتقنيات تعلم الآلة لكشف الأنماط الشاذة والهجمات في الوقت الفعلي، مما يُتيح استجابة سريعة للتهديدات المحتملة (رِفَافِي، 2025).

وتُطبق خوارزميات التحكم في الوصول، مثل: (RBAC و ABAC)، وإدارة الهويات الرقمية الموحدة (IAM) لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى البيانات وفقاً لصلاحياتهم، وتُدمج هذه الخوارزميات مع أنظمة المصادقة متعددة العوامل (MFA) لتعزيز الأمان (السعودي، 2024). وتُدمج استراتيجيات الحماية في معمارية النظم السحابية من خلال عزل المستأجرين، وتشفير البيانات عند السكون وأثناء النقل باستخدام مفاتيح أمان مدارة مركزياً، وتطبيق سياسات النسخ الاحتياطي المتكرر واستعادة البيانات (Almaghrabi & Bugis, 2022).

وتتجلى أهمية هذه التقنيات في قدرتها على توفير حماية متعددة الطبقات تعمل بشكل تكاملي، إذ أن الاعتماد على طبقة واحدة فقط يُشكل نقطة فشل واحدة، بينما التكامل بين طبقات التشفير، والتحكم في الوصول، والمراقبة، والإخفاء يُوفر دفاعاً متيناً ضد التهديدات المتطورة.

5. منهجية الخصوصية بالتصميم وبالإعداد الافتراضي

تُعد منهجية الخصوصية بالتصميم (Privacy by Design) نهجاً استباقياً يدمج متطلبات الخصوصية في مراحل هندسة البرمجيات منذ البداية، وليس كإضافة لاحقة، وذلك وفق المبادئ

السبعة التي وضعتها الدكتورة آن كافوكيان Ann Cavoukian، والتي تشمل: الاستباقية وليس رد الفعل، والخصوصية كإعداد افتراضي، وتضمن الخصوصية في التصميم، والوظائف الكاملة، والأمن الشامل، والشفافية والانفتاح، واحترام خصوصية المستخدم (Chhetri et al., 2024). وتُبرمج الإعدادات الافتراضية لتكون صديقة للخصوصية، أي أن أعلى مستويات الحماية تكون مفعلة بشكل افتراضي، ويُترك للمستخدم خيار تخفيضها بوعي وقصد، مما يقلل من المخاطر الناتجة عن جهل المستخدمين أو إهمالهم في تكوين الإعدادات (Al-Khalifa et al., 2023).

ويُعد تحليل الأثر التقني والأمني (PIA و DPIA) إلزامياً قبل إطلاق الأنظمة الذكية الجديدة، ويتضمن تحديد المخاطر المحتملة على خصوصية الأفراد، وتقييمها من حيث الاحتمالية والشدة، واقتراح تدابير تخفيفية مناسبة، وهو متطلب صريح في كل من GDPR (المادة 35)، و PDPL (المادة 19) (الشمري، نجم، 2023). ويقع على عاتق المطورين والمهندسين دور محوري في تفعيل قيم الخصوصية برمجياً، وذلك من خلال استخدام أدوات تحليل ثابتة للكشف عن نقاط الضعف الأمنية، وتطبيق ممارسات الترميز الآمن، وتوثيق معالجة البيانات وكيفية تدفقها داخل النظام (فلانة، 2025).

وتُدمج أدوات الحماية الاستباقية في معمارية النظام كآليات الكشف عن التسرب ومنع فقدان البيانات (DLP)، وأنظمة إدارة السجلات والتدقيق الآلي التي تُسجل كل عملية وصول وتعديل وحذف، مما يوفر أثراً رقابياً شاملاً (الرحلي، 2026). ويُقيّم الأثر البيئي والتقني لانتهاكات الخصوصية المحتملة من خلال محاكاة سيناريوهات الاختراق وقياس تكاليف التعافي والخسائر السماعية، مما يُساعد في تحديد أولويات الاستثمار في الحماية (رجب، 2024).

6. الالتزامات التقنية لجهات التحكم ومعالجي البيانات

يُحدد التشريع مسؤوليات جهة التحكم (Controller) التي تُقرر أغراض المعالجة ووسائلها، ومعالج البيانات (Processor) الذي ينفذ المعالجة نيابة عنها، وتشمل الالتزامات الفنية الصارمة: تنفيذ تدابير أمنية مناسبة (كالتشفير، وإدارة الوصول، والتسجيل)، والاحتفاظ بسجلات أنشطة المعالجة، والتعاون مع السلطات الرقابية وتزويدها بالمعلومات المطلوبة (القطاطشة، 2022). وتُستخدم الأتمتة الشاملة لسجلات أنشطة المعالجة (مثل تسجيل كل عملية وصول، وتعديل،

وحذف، ونقل) لضمان التتبع والمراجعة، وهو مطلب صريح في المادة (30) من GDPR والمادة (17) من PDPL (المحروقي، 2023).

وتشترط الشروط الفنية والأمنية في اتفاقيات الإسناد التقني الخارجي (كالاتفاقيات مع مقدمي الخدمات السحابية ومعالجي البيانات الخارجيين) تحديد مستويات الخدمة الأمنية، وضمانات حماية البيانات، وإجراءات الإبلاغ عن الحوادث، وآليات التدقيق والرقابة (الشمري، 2023). وتُطبق معايير التفتيش والرقابة على مقدمي الخدمات التقنية من خلال عمليات تدقيق دورية واختبارات اختراق، مع إمكانية فرض عقوبات على المخالفين، وتتضمن هذه المعايير متطلبات محددة للاحتفاظ بالسجلات وإتاحتها للجهات الرقابية عند الطلب (Al-Khalifa et al., 2023).

وتُعد إدارة التوافق بين الأطراف المتعددة في معالجة البيانات (كالمعالجين المساعدين والمتعاقدين من الباطن) تحدياً معقداً، ويتطلب وضع بروتوكولات واضحة لتبادل البيانات وضمان الامتثال المشترك عبر سلسلة المعالجة، وذلك من خلال عقود ملزمة تحدد مسؤوليات كل طرف وتلتزم بأعلى معايير الحماية (المعداوي، 2018). ويوضح الشكل الآتي شبكة العلاقات التعاقدية بين جهة التحكم وعدة معالجين للبيانات، موضحاً ضرورة وجود اتفاقيات معالجة بيانات موحدة تُلزم جميع الأطراف بالالتزامات الأمنية نفسها:



شكل (2.3): العلاقة التعاقدية والرقابية بين جهة التحكم ومعالجي البيانات

يُبرز الشكل (2.3) تعدد الأطراف المشاركة في معالجة البيانات، مما يُشكل تحدياً كبيراً للامتثال، إذ أن ضعف أي طرف في السلسلة قد يُعرض البيانات للخطر، ولذا ينبغي على جهة

التحكم القيام بالعناية الواجبة في اختيار المعالجين، وتقييم أدائهم باستمرار، وضمان وجود آليات رقابية فعالة على جميع المستويات، وهذا يستدعي استثماراً في إدارة العقود والتدقيق المستمر.

7. إدارة حوادث تسرب البيانات والامتثال الرقابي

تُعد خطط الاستجابة التقنية لحوادث الاختراق السيبراني عنصراً حيوياً في منظومة حماية البيانات، وتشمل أربع مراحل رئيسية متسلسلة، هي:

- **مرحلة الاستعداد:** التي تتضمن إنشاء فريق استجابة متخصص، وتحديد الأدوات والتقنيات اللازمة، ووضع بروتوكولات الاتصال الداخلية والخارجية، وإجراء تدريبات دورية لاختبار الجاهزية (الشمري، 2023).
 - **مرحلة الكشف والتحليل:** التي تعتمد على استخدام أنظمة الإنذار المبكر، وأدوات كشف التسلسل، وتحليل السجلات لتحديد مصدر الاختراق ونطاقه والأطراف المتأثرة، ويتطلب ذلك قدرات تحليلية متقدمة للتمييز بين الحوادث الحقيقية والإنذارات الكاذبة (رفرافي، 2025).
 - **مرحلة الاحتواء والاستئصال:** التي تتضمن عزل الأنظمة المتأثرة لمنع انتشار الاختراق، وإزالة البرمجيات الخبيثة، وتصحيح الثغرات الأمنية، وتطبيق التصحيحات اللازمة، وقد يتطلب ذلك إيقافاً مؤقتاً للخدمات لمنع تفاقم الأضرار (العجمي، 2023).
 - **مرحلة التعافي والدروس المستفادة:** التي تشمل استعادة البيانات من النسخ الاحتياطي، وإعادة تشغيل الأنظمة بشكل آمن، وإجراء تحليل ما بعد الحادث لتحديد نقاط الضعف وتحسين الإجراءات المستقبلية (الرحلي، 2026).
- وتُستخدم أنظمة الإنذار المبكر والكشف الآلي عن تسرب السجلات أدوات تعلم الآلة لرصد الأنماط غير العادية في تدفق البيانات، مثل الزيادة المفاجئة في طلبات الوصول أو محاولات التصدير غير المصرح بها، مما يسمح بالتدخل الفوري لتقليل الأضرار ووقف نزيف البيانات (هيوب، 2023). وتتضمن البروتوكولات التقنية للإبلاغ الفوري عن الحوادث الأمنية إشعار السلطات الرقابية والأفراد المتضررين خلال مدة زمنية محددة (72 ساعة في GDPR، وخلال مدة معقولة في PDPL)، مع توفير تفاصيل الحادث ونوع البيانات المتأثرة والإجراءات المتخذة للحد من الأضرار، وتُعد هذه الإجراءات ضرورية لبناء الثقة والامتثال التنظيمي (أشقر، 2025).

وتُعد إجراءات التدقيق الدوري على نظم حماية البيانات الشخصية أداة رقابية أساسية، وتشمل مراجعة سياسات الأمن وتحديثها، واختبار فعالية الضوابط الأمنية، وتقييم امتثال المعالجين والأطراف الخارجية، وإصدار تقارير التدقيق للإدارة والجهات الرقابية (الوادي، 2025). وتُستخدم آليات العزل الرقمي (كعزل الشبكات وتقسيمها إلى مناطق أمنية) لاحتواء الأضرار ومنع انتشار الاختراق إلى الأنظمة السليمة، بالإضافة إلى أنظمة النسخ الاحتياطي المتكرر (Backup) التي تُجرى بشكل دوري وتُخزن في مواقع منفصلة لضمان التعافي من الكوارث الرقمية واستعادة البيانات المشفرة أو التالفة (النيداني، 2024).

وفي هذا السياق، يرى الباحث أن فعالية إدارة الحوادث لا تقاس فقط بسرعة الاستجابة، بل بالقدرة على التعلم من الحوادث وتحسين المنظومة الأمنية بشكل مستمر، كما أن الإبلاغ الشفاف عن الحوادث يُعد مؤشراً على نضج المؤسسة في إدارة المخاطر ويعزز ثقة الأفراد والجهات الرقابية، مما يجعل إدارة الحوادث جزءاً لا يتجزأ من استراتيجية الامتثال الشاملة.

8. حماية البيانات في بيئة الحوسبة السحابية

تُثير الحوسبة السحابية تحديات خاصة تتعلق بالسيادة الرقمية للبيانات، إذ قد تُخزن البيانات في مراكز بيانات في بلدان مختلفة، مما يتعارض مع متطلبات بعض التشريعات التي تقيد نقل البيانات خارج الحدود الوطنية أو تشترط موافقة صريحة على ذلك (المعداوي، 2018). وتُستخدم تقنيات العزل الافتراضي للبيانات في الاستضافة المشتركة، كالمحاكاة الافتراضية على مستوى نظام التشغيل والحاويات (Containers)، لفصل بيانات العملاء عن بعضها البعض وحماية كل مستأجر من الوصول غير المصرح به من قبل مستأجرين آخرين، مما يُشكل طبقة حماية إضافية في البيئات السحابية متعددة المستأجرين (Almaghrabi & Bugis, 2022).

وتستدعي متطلبات الامتثال الأمني عند تخزين البيانات خارج الحدود إما الحصول على موافقة صريحة من الأفراد، أو الاعتماد على آليات نقل قانونية كالقواعد المؤسسية الملزمة (BCR)، والبنود التعاقدية القياسية (SCCs) التي تضمن مستوى مناسباً من الحماية، وهو ما ورد في كل من GDPR (الفصل الخامس)، و PDPL (المادة 29) (الشامسي، 2023). وتقع على مقدمي خدمات السحاب مسؤولية تأمين البنية التحتية من خلال تشفير البيانات عند السكون وأثناء النقل،

وإدارة الوصول والهويات بشكل مركزي، ومراقبة الأنشطة وتسجيلها، وتوفير شهادات امتثال معترف بها دولياً كـ ISO 27001 و SOC 2 و FedRAMP، مما يُعزز ثقة العملاء في أمان خدماتهم (سويلم، 2022).

وتُحدد مقاييس الأداء الأمني في اتفاقيات مستوى الخدمة (SLA) مؤشرات قابلة للقياس كمتاح الخدمة (Uptime)، وزمن الاستجابة للحوادث، ومستوى التشفير المطبق، وتكرار التدقيق الأمني، ويُعد الالتزام بهذه المقاييس شرطاً أساسياً لاستمرارية العلاقة التعاقدية (فلاتة، 2025). ويُعد الامتثال لمعايير الحماية العالمية، مثل: (GDPR و PDPL) عند التخزين السحابي الخارجي شرطاً أساسياً للمؤسسات العاملة دولياً، مما يستدعي اختيار موفري خدمات سحابية يدعمون هذه المتطلبات ويقدمون ضمانات تعاقدية واضحة، كما يستلزم إجراء تقييمات دورية للمخاطر المرتبطة بالاستعانة بمقدمي خدمات من ولايات قضائية مختلفة (الجيجلي، 2025).

ويُلخص الجدول الآتي متطلبات الامتثال الأمني الأساسية في بيئة الحوسبة السحابية، مُبيناً الآليات التقنية لكل مطلب والمرجع التشريعي المقابل وجهة المسؤولية:

جدول (2.6): متطلبات الامتثال الأمني في بيئة الحوسبة السحابية

المتطلب الأمني	الآلية التقنية	المرجع التشريعي	جهة المسؤولية
تشفير البيانات	تشفير AES-256 للبيانات المخزنة، TLS 1.3 للبيانات المنقولة	المادة (32) GDPR، المادة (10) PDPL	مزود الخدمة وجهة التحكم
التحكم في الوصول	ABAC، RBAC، المصادقة متعددة العوامل	المادة (5) GDPR، المادة (7) PDPL	جهة التحكم
عزل المستأجرين	المحاكاة الافتراضية، الحاويات، الشبكات الافتراضية الخاصة	المادة (28) GDPR، المادة (15) PDPL	مزود الخدمة
تسجيل الأنشطة وتدقيقها	سجلات الوصول، أنظمة SIEM، الاحتفاظ بالسجلات لمدة محددة	المادة (30) GDPR، المادة (17) PDPL	جهة التحكم ومعالج البيانات
الإبلاغ عن الحوادث	بروتوكولات الإبلاغ خلال 72 ساعة (GDPR) أو مدة معقولة (PDPL)	المادة (33) GDPR، المادة (20) PDPL	جهة التحكم

(المصدر: إعداد الباحث بالاعتماد على الشامسي، 2023؛ فلاتة، 2025؛ الجيجلي، 2025).

يُلاحظ من الجدول (2.6) توزيع المسؤوليات الأمنية بين مزود الخدمة وجهة التحكم، مما يُشير إلى أن الامتثال في البيئة السحابية يتطلب تعاوناً وثيقاً بين الطرفين، وأن جهة التحكم

تتحمل المسؤولية النهائية عن حماية البيانات حتى في البيئات المستضافة خارجياً، مما يستدعي اختياراً دقيقاً للمزودين وعقوداً واضحة تحدد الالتزامات.

وبناءً على ما تقدم، يرى الباحث أن الحوسبة السحابية تقدم فرصاً هائلة للمؤسسات من حيث المرونة وتخفيض التكاليف، لكنها في الوقت نفسه تفرض تحديات امتثال كبيرة تتطلب فهماً عميقاً للتشريعات المختلفة وقدرة على إدارة المخاطر المرتبطة بنقل البيانات عبر الحدود، ولذا ينبغي على المؤسسات تطوير استراتيجية سحابية متكاملة تدمج الاعتبارات القانونية والتقنية والإدارية، مع إجراء مراجعات دورية لاتفاقيات الخدمة وضمانات الحماية.

9. تقاطع البيانات الضخمة مع خصوصية المستخدمين

تمثل البيانات الضخمة مورداً هائلاً للتحليل والاستفادة، لكنها تثير مخاطر خوارزمية خطيرة تتمثل في إعادة تحديد الهوية عبر دمج سجلات من مصادر متعددة، حتى لو كانت كل سجل مجهلاً على حدة، إذ يمكن لخوارزميات الربط المتقدمة استنتاج هويات الأفراد من خلال السمات الفريدة المتبقية في البيانات، مما يهدد خصوصية الأفراد ويُمكن من استنتاج معلومات حساسة عنهم دون علمهم أو موافقتهم (Ploug, 2023). وتُستخدم تقنيات تحليل البيانات الضخمة دون المساس بالخصوصية، كالتعلم الفيدرالي (Federated Learning) الذي يُدرّب النماذج محلياً على أجهزة المستخدمين أو في مواقع البيانات الموزعة دون نقل البيانات المركزية، مما يُحقق استفادة تحليلية مع حماية الخصوصية ويُقلل من مخاطر التسريب (Yang & Beil, 2024).

وتتضمن أساليب التتقيب الآمن في السجلات الرقمية المشفرة استخدام التشفير المتجانس (Homomorphic Encryption)، والحساب الآمن متعدد الأطراف (Secure Multi-Party Computation) لإجراء عمليات إحصائية وتحليلية على بيانات مشفرة من مصادر مختلفة دون كشف محتواها، وهو ما يُتيح استخلاص رؤى قيمة مع الحفاظ على السرية التامة للبيانات (El Mestari et al., 2024). ويُعد التوفيق التقني بين متطلبات الابتكار (كتطوير نماذج دقيقة وفعالة)، وحقوق الخصوصية (كضمان عدم كشف المعلومات الشخصية) تحدياً مركزياً في عصر البيانات الضخمة، ويتطلب تصميم خوارزميات تراعي الخصوصية تحقق أداءً مقبولاً مع حماية قوية، وهو مجال بحثي نشط يشهد تطورات مستمرة (Murdoch, 2021).

ويؤدي الذكاء الاصطناعي دوراً في مراقبة وتحليل البيانات بمسؤولية من خلال أدوات التحليل الأخلاقي التي تكتشف الانحيازات وتقيم المخاطر قبل اتخاذ القرارات، وتُساعد في تحديد ما إذا كانت المعالجة تتناسب مع الأغراض المعلنة وما إذا كانت تنتهك حقوق الأفراد (Taylor et al., 2025). ويُعد أثر الحوكمة على جودة وسلامة تدفق البيانات الكبرى مهماً، إذ تضمن الحوكمة وضع سياسات واضحة لجمع البيانات واستخدامها ومشاركتها، وفرض ضوابط على مدة الاحتفاظ، وتحديد آليات للرقابة والتدقيق، مما يقلل من مخاطر الاستخدام غير المشروع ويعزز ثقة الأفراد في النظام البيئي للبيانات (van der Schyff et al., 2024).

10. التوعية والثقافة الرقمية والوعي المؤسسي

تُعد التوعية الرقمية إحدى الدعائم الأساسية للامتثال الفعال لحماية البيانات، وتشمل تصميم برامج توعوية بمخاطر الهندسة الاجتماعية (كالتصيد والاحتيال والانتحال) تستهدف مختلف مستويات الموظفين والمستخدمين، وتستخدم محاكاة الهجمات (Simulated Attacks) لاختبار مدى استجابة الأفراد وتحسين وعيهم بالمخاطر وتعزيز سلوكياتهم الوقائية (العنبي، 2025). وتُعنى هندسة السلوك الرقمي للموظفين بتشكيل ممارساتهم في التعامل مع البيانات الحساسة، من خلال وضع سياسات استخدام واضحة للأنظمة والشبكات الداخلية، وتطبيق مبدأ الحد الأدنى من الامتيازات للوصول إلى البيانات، وتوفير أدوات سهلة الاستخدام للإبلاغ عن الحوادث أو الشكوك الأمنية (البقلي، 2021).

وتُعد برامج تدريب متخصصة لمسؤولي حماية البيانات (DPOs)، والموظفين المعنيين بمعالجة البيانات، لتزويدهم بالمعرفة القانونية والتقنية اللازمة لأداء مهامهم، وفقاً لمتطلبات المادة (37) من GDPR والمادة (20) من PDPL، وتشمل هذه البرامج موضوعات كتقييمات الأثر، وإدارة الموافقات، والإبلاغ عن الحوادث، والتدقيق الداخلي (الشمري، 2023). ويُعد أثر الثقافة التنظيمية على مستوى الامتثال الداخلي للسياسات كبيراً، إذ تتبنى المؤسسات الناجحة ثقافة الخصوصية كقيمة مؤسسية تُدمج في استراتيجياتها وسياساتها الداخلية، مما يُعزز التزام الموظفين بالسياسات ويقلل من الحوادث الناتجة عن الإهمال أو نقص الوعي (القطاطشة، 2022).

ويهدف بناء مجتمع رقمي واعٍ بمخاطر مشاركة البيانات الشخصية إلى تمكين الأفراد من اتخاذ قرارات مستنيرة بشأن بياناتهم، من خلال حملات توعوية مستمرة، ومناهج تعليمية تُدمج في المراحل الدراسية المختلفة، ومنصات تفاعلية تقدم محتوى مخصصاً لمختلف الفئات العمرية والثقافية (أشقر، 2025). وتُدمج آليات التوعية في تصميم التطبيقات والخدمات الرقمية (كإشعارات الخصوصية التفاعلية التي تشرح كيفية استخدام البيانات بلغة مبسطة، ودروس التوعية المدمجة التي تظهر عند أول استخدام للتطبيق، ونوافذ منبثقة تذكيرية عند محاولة مشاركة بيانات حساسة) لتعزيز السلوك المسؤول للمستخدمين في سياق استخدامهم الفعلي للخدمات (رجب، 2024).

ويرى الباحث أن التوعية والثقافة الرقمية ليست مجرد أنشطة إضافية أو تدريبية، بل هي استثمار استراتيجي طويل الأمد يُعزز نضج المؤسسة في حماية البيانات ويقلل من المخاطر البشرية التي تُشكل غالبية حوادث الاختراق، كما أن تمكين الأفراد من فهم حقوقهم وواجباتهم يُساهم في بناء نظام بيئي رقمي أكثر أماناً وثقة، مما يُعزز فعالية التشريعات والسياسات التقنية.

المحور الثالث: استراتيجيات الحوكمة الرقمية للذكاء الاصطناعي

يُشكل هذا المحور الدعامة التنظيمية والإشرافية التي تضمن تطوير واستخدام أنظمة الذكاء الاصطناعي بشكل مسؤول وأخلاقي وقانوني، إذ يتناول الأطر المفاهيمية للحوكمة الرقمية، والنماذج العالمية، وآليات الرقابة التقنية، والمساءلة، واستراتيجيات الامتثال، والمعايير الدولية، والحوكمة التشاركية، والتكامل بين التشريعات والكود البرمجي. وتُعد الحوكمة الرقمية الآلية التي تترجم المبادئ الأخلاقية والقانونية إلى ممارسات تنفيذية ملموسة، مما يُمكن المؤسسات من تحقيق التوازن بين الابتكار والالتزام التنظيمي.

1. الأطر المفاهيمية للحوكمة الرقمية في المؤسسات

تُعرف الحوكمة الرقمية بأنها الإطار المتكامل من السياسات والعمليات والهياكل التنظيمية التي تهدف إلى توجيه وإدارة ومراقبة استخدام التقنيات الرقمية والبيانات في المؤسسات، بما يحقق الأهداف الاستراتيجية مع الالتزام بالمتطلبات القانونية والأخلاقية (Batoool et al., 2025). وتتمثل الأهداف الاستراتيجية لحوكمة تقنيات المعلومات والاتصال في:

- ضمان توافق الاستثمارات التقنية مع أهداف العمل.
- تحسين جودة الخدمات الرقمية.
- إدارة المخاطر التقنية.
- ضمان الامتثال للتشريعات والمعايير.
- تعزيز الثقة بين أصحاب المصلحة (Birkstedt et al., 2023).

وتشمل المكونات الأساسية لبناء إطار حوكمة تقني متكامل: هيكل الحوكمة الذي يُحدد اللجان والأدوار والمسؤوليات، وسياسات وإجراءات تقنية مكتوبة وموثقة، ومقاييس الأداء الرئيسية (KPIs) لقياس الفعالية، وآليات الرقابة والتدقيق المستمرة، واستراتيجيات إدارة المخاطر التي تحدد وتصنف وتعالج المخاطر المحتملة (Papagiannidis et al., 2025). ويُعد دور الحوكمة الرقمية في نجاح مبادرات التحول المؤسسي محورياً، إذ تساعد في تجنب الفشل الناتج عن سوء إدارة المشاريع التقنية، وضمان تحقيق العائد المتوقع من الاستثمارات الرقمية، وتعزيز التنسيق بين الوحدات التنظيمية المختلفة (Sharma et al., 2020).

ويتلاقى وظيفياً بين **حوكمة البيانات** (Data Governance) التي تركز على جودة البيانات وأمانها وامثالها وسهولة الوصول إليها، و**حوكمة الذكاء الاصطناعي** (AI Governance) التي تُعنى بتطوير واستخدام الأنظمة الذكية بشكل مسؤول وأخلاقي، وتضمن الشفافية والمساءلة في قراراتها (Zaidan & Ibrahim, 2024). وتتنوع النماذج الدولية لحوكمة التقنيات الناشئة بين نموذج الاتحاد الأوروبي القائم على التشريع الشامل والمخاطر، والنموذج الأمريكي القائم على التوجيهات القطاعية غير الملزمة، والنموذج الصيني القائم على الرقابة المركزية والسيطرة الحكومية، مما يُشير إلى تعدد المقاربات حسب السياق الثقافي والسياسي (Roberts et al., 2024).

وبناءً على ما سبق، يرى الباحث أن نجاح الحوكمة الرقمية لا يعتمد على وجود سياسات مكتوبة فحسب، بل على قدرة المؤسسة على تنفيذها ومراقبتها وتحديثها باستمرار، وهذا يتطلب التزاماً من القيادة العليا واستثماراً في بناء القدرات الداخلية وتعزيز ثقافة الامتثال على جميع المستويات التنظيمية، مما يُشكل تحدياً استراتيجياً يتطلب موارد وجهوداً متواصلة.

2. نماذج وأطر حوكمة الذكاء الاصطناعي العالمية

صدرت العديد من المبادئ التوجيهية لحوكمة الذكاء الاصطناعي من منظمات دولية مرموقة، أبرزها: مبادئ منظمة التعاون الاقتصادي والتنمية (OECD) لعام 2019 التي تركز على الاستثمار في البحث والتطوير وبناء نظم ذكية تركز على الإنسان، وتوصيات اليونسكو لعام 2021 التي تُشدد على حماية حقوق الإنسان والكرامة والمساواة، ومبادئ مجموعة العشرين التي تؤكد على الشفافية والمساءلة، وإطار عمل المعهد الوطني للمعايير والتكنولوجيا (NIST) لإدارة مخاطر الذكاء الاصطناعي الذي يوفر منهجية شاملة لتقييم المخاطر وتخفيفها (Corrêa et al., 2023). وتتنوع المقاربات التنظيمية بين:

1. **المقاربة المبنية على المبادئ الأخلاقية:** كالتوجيهات الأوروبية للثقة في الذكاء الاصطناعي التي صدرت عام 2019.
2. **المقاربة القائمة على المخاطر:** كقانون الذكاء الاصطناعي الأوروبي الذي يصنف الأنظمة حسب مستوى المخاطر إلى غير مقبولة، وعالية، ومحدودة، وضئيلة.
3. **المقاربة القائمة على النتائج:** كسياسات حوكمة الذكاء الاصطناعي في الصين التي تركز على الأثر الاجتماعي والرقابة الحكومية (Stix, 2022).

وتُشكل لجان الرقابة التقنية والأخلاقية داخل المؤسسات هيئات متخصصة تضم خبراء تقنيين وقانونيين وأخلاقين، وتتولى مراجعة مشاريع الذكاء الاصطناعي، وتقييم المخاطر، وضمان الامتثال للمبادئ والسياسات، وإصدار التوصيات للإدارة العليا (Hulok, 2025). وتُستخدم أدوات قياس التوافق مع التوجهات العالمية للحوكمة، كإطار عمل تقييم الاستعداد للذكاء الاصطناعي الصادر عن البنك الدولي، ومؤشر النضج التنظيمي للذكاء الاصطناعي الذي طويرته جامعة ستانفورد، مما يُمكن الدول والمؤسسات من تحديد مواقعها النسبية ومجالات التحسين (Tjondronegoro, 2024).

ويُقيّم مستوى النضج في استخدام الذكاء الاصطناعي المسؤول عبر مصفوفات متعددة الأبعاد تقيس الأبعاد التقنية (كجودة البيانات وقابلية التفسير)، والأخلاقية (كالعدالة والشفافية)، والقانونية (كالامتثال للتشريعات)، والاجتماعية (كالقبول العام والأثر المجتمعي). وفي ضوء ذلك، يرى الباحث أن تعدد النماذج والأطر العالمية يُوفر ثراءً وخيارات متعددة للمؤسسات، لكنه في الوقت نفسه يُشكل تحدياً في اختيار النموذج الأنسب للسياق المحلي. ولذا ينبغي على المؤسسات تبني نهج هجين يجمع بين أفضل الممارسات العالمية ويراعي خصوصيتها التنظيمية والثقافية، مع إجراء مراجعات دورية لمواكبة التطورات في هذا المجال المتسارع.

جدول (2.7): المقاربات التنظيمية الرئيسية لحوكمة الذكاء الاصطناعي عالمياً

المقاربة	الخصائص الرئيسية	الأمثلة النموذجية	نقاط القوة	نقاط الضعف
المبنية على المبادئ	تركيز على القيم الأخلاقية، غير ملزمة قانونياً، طوعية	توجيهات الثقة في (EU AI, 2019)، مبادئ OECD	مرونة عالية، تشجع الابتكار، سهولة التبني	ضعف التنفيذ، غياب العقوبات، قابلية للتفسير المتباين
القائمة على المخاطر	تصنيف الأنظمة حسب مستوى المخاطر، متطلبات متفاوتة	قانون الذكاء الاصطناعي الأوروبي (EU AI Act)	توازن بين الابتكار والحماية، وضوح في المتطلبات	تعقيد التصنيف، صعوبة التطبيق على الأنظمة سريعة التطور
القائمة على النتائج	تركيز على الأثر الفعلي، رقابة حكومية مركزية	سياسات الصين، مبادئ مجموعة العشرين	فعالية في تحقيق الأهداف المجتمعية، رقابة صارمة	جمود محتمل، إعاقة للابتكار، تركيز على النتائج دون العمليات

(المصدر: إعداد الباحث بالاعتماد على (Corrêa et al., 2023; Stix, 2022; Hulok, 2025).

يُصنف الجدول (2.7) المقاربات التنظيمية الرئيسية لحوكمة الذكاء الاصطناعي عالمياً، مُبيناً الخصائص الرئيسية والأمثلة النموذجية ونقاط القوة والضعف لكل مقارنة، مما يُساعد المؤسسات وصناع السياسات على اختيار المقاربة الأنسب وفقاً لسياقها الوطني والتنظيمي وأهدافها الاستراتيجية.

3. آليات الرقابة التقنية والتدقيق الخوارزمي المستمر

تُعد أدوات المراقبة الآلية والمستمرة لأداء النماذج الذكية ضرورية لضمان بقائها ضمن معايير الجودة والأمان المحددة، وتشمل أنظمة مراقبة الانحراف (Drift Detection) التي تكشف التغيرات في توزيع البيانات المدخلة (Data Drift) أو العلاقات بين المتغيرات (Concept Drift) التي قد تؤدي إلى تدهور الأداء، مما يتطلب إعادة تدريب أو تحديث النماذج (Lazcoz & De Hert, 2023).

وتتبنى منهجيات التدقيق التقني (Algorithmic Auditing) اكتشاف وتصحيح التحيز، وتقييم قابلية التفسير، والتحقق من الامتثال للسياسات والمعايير، وتستخدم أدوات آلية مفتوحة المصدر، مثل: (What-If Tool; AI Fairness 360) التي طورتها شركات كبرى، بالإضافة إلى أدوات تجارية متخصصة للتدقيق المستمر (Kirat et al., 2023).

وتُجرى المراجعة البرمجية لضمان شفافية مسارات اتخاذ القرار من خلال تحليل الكود المصدري، وتوثيق معمارية النظام وخطوات المعالجة، وتوفير وثائق شرح للمطورين والجهات الرقابية، مما يُمكن من فهم كيفية وصول النظام إلى قراراته وتقييم مدى اتساقها مع المتطلبات (Cheong, 2024). وتؤدي تقنيات الفحص الآلي، مثل: (Static Vulnerability Scanning; Analysis) دوراً في تقييم جودة وسلامة المخرجات، واكتشاف الثغرات الأمنية والانحيازات الخفية في الكود والبيانات، وإصدار تنبيهات للمطورين لاتخاذ إجراءات تصحيحية (Camilleri, 2023).

وتُعد معايير المراجعة الخارجية والتدقيق المستقل من قبل جهات معتمدة (كشركات تدقيق تقني متخصصة أو هيئات تنظيمية) ممارسة متزايدة الأهمية، خاصة في القطاعات الحساسة كالمالية والصحية، حيث تُنتج تقارير شاملة عن أداء النظام وامتناله وترفع للجهات الرقابية وأصحاب المصلحة (Mökander et al., 2022). كما تؤدي الهيئات التنظيمية (كهيئة البيانات

والذكاء الاصطناعي السعودية، والمفوضية الأوروبية، وهيئات حماية البيانات الوطنية) دوراً رقابياً في مراقبة سوق التقنيات الناشئة من خلال وضع معايير وإصدار التراخيص وفرض العقوبات على المخالفين، مما يُشكل رادعاً للامتثال ويعزز الثقة في السوق (Ibrahim, 2024).

واتساقاً مع ما تقدم، يرى الباحث أن الرقابة التقنية والتدقيق الخوارزمي المستمر ليسا مجرد إجراءات إضافية، بل يشكلان جزءاً جوهرياً من دورة حياة الأنظمة الذكية، إذ أن المراقبة اللحظية والتدقيق المنتظم يُمكنان من اكتشاف المشكلات مبكراً وتصحيحها قبل أن تتحول إلى أزمات، مما يُعزز الموثوقية والثقة ويُقلل من مخاطر الامتثال والتكاليف القانونية، وهذا يتطلب استثماراً في أدوات التدقيق وكوادر متخصصة.

4. المساءلة وإدارة المخاطر في مشاريع الذكاء الاصطناعي

يتطلب تحديد المسؤوليات التقنية والتنفيذية في مشاريع الذكاء الاصطناعي تعريفاً دقيقاً لأدوار المطورين ومشغلي الأنظمة والمستخدمين، وتوثيق ذلك في عقود وسياسات داخلية، مع تحديد سلاسل المسؤولية في حالة حدوث أخطاء أو أضرار، بحيث يكون كل طرف مدركاً لالتزاماته وتبعات تقصيره (Novelli et al., 2024).

وتُصمم مصفوفة المخاطر التقنية لتصنيف المخاطر وفقاً لاحتمالية حدوثها وشدة تأثيرها، وتُشمل مخاطر تتعلق بكل من:

- جودة البيانات: كنقصها أو تحيزها.
- أداء النماذج: كانخفاض الدقة أو التجهيز المفرط.
- الأمن السيبراني: كالهجمات والتسريبات.
- الامتثال القانوني: كمخالفة التشريعات.
- الأخلاقيات: كالتحيز وعدم العدالة (Cech, 2021).

وتتضمن خطط التخفيف والاحتواء للتعامل مع فشل الخوارزميات إجراءات متسلسلة كإيقاف النظام مؤقتاً لمنع تفاقم الضرر، والتحول إلى المعالجة اليدوية أو الاحتياطية، وتصحيح النموذج وإعادة تدريبه على بيانات محدثة، وإخطار الأطراف المتأثرة والجهات الرقابية وفقاً للبروتوكولات المحددة (Poehhacker & Kacianka, 2021). وتُبنى أطر التعويض عن الأضرار الناجمة عن

القرارات الآلية الخاطئة على مبادئ القانون التقصيري، مع صعوبات في إثبات السببية بسبب تعقيد الأنظمة وتعدد العوامل المؤثرة في قراراتها، مما يستدعي تطوير آليات تأمين خاصة تغطي مخاطر الذكاء الاصطناعي (Hickman & Petrin, 2021).

ويُعد التأمين السيبراني أداة فعالة لنقل وإدارة المخاطر التقنية، حيث تُغطي عقود التأمين تكاليف التعافي من الاختراقات، والغرامات التنظيمية، وتعويضات الأطراف المتضررة، وتكاليف الدعاوى القضائية، مما يُشجع المؤسسات على تبني ممارسات أمنية أفضل لتقليل أخطار التأمين (Shmueli & Vardi, 2021). وتُكامل الحوكمة المؤسسية مع الحوكمة الرقمية من خلال دمج إدارة المخاطر التقنية في استراتيجية المؤسسة العامة، ورفع تقارير المخاطر إلى مجلس الإدارة بشكل دوري، وضمان وجود ثقافة تنظيمية تدعم الامتثال والشفافية (Cordeiro et al., 2025).

وفي هذا السياق، يرى الباحث أن المساءلة الفعالة وإدارة المخاطر لا تتحققان بوجود سياسات مكتوبة فحسب، بل تتطلبان آليات تنفيذية واضحة، وتدريباً مستمراً للكوادر، وثقافة تنظيمية تشجع على الإبلاغ عن الأخطاء والتعلم منها، كما أن التأمين السيبراني يُعد أداة تكميلية مهمة لكنها لا تغني عن التزام المؤسسة بأعلى معايير الأمان والجودة في تصميم وتشغيل أنظمتها.

5. استراتيجيات الامتثال التقني والرقابة الاستباقية

تُصمم أدوات امتثال آلية مدمجة في معمارية الأنظمة لتقليل الاعتماد على الإجراءات اليدوية المعرضة للخطأ البشري، ومن أبرز هذه الأدوات:

- أدوات التحقق من الموافقات (Consent Management): لتتبع موافقات المستخدمين وتحديثاتها.
- إدارة سياسات الخصوصية (Privacy Policy Management): لتطبيق القواعد تلقائياً.
- ضوابط الوصول والاستخدام (Access & Usage Controls): لتنظيم الصلاحيات بشكل آلي ودقيق (Lorè et al., 2023).

وتتبنى منهجيات الرقابة الاستباقية (Proactive Monitoring) التنبؤ بالمخالفات قبل وقوعها، عبر تحليل سلوك النظام واكتشاف الأنماط الشاذة التي قد تشير إلى انتهاكات محتملة، واتخاذ إجراءات تصحيحية تلقائية كتنقيح الوصول أو إيقاف المعالجة مؤقتاً (Holtz & Ledendal, 2026).

وتُستخدم أتمتة إصدار تقارير الشفافية والامتثال الرقمي الدورية لتوفير بيانات موثوقة للجهات الرقابية وأصحاب المصلحة، مما يُسهل عمليات المراجعة ويعزز الشفافية والثقة (Gonalves & Correia, 2026).

وتُعالج الآليات التقنية التعارض بين الابتكار والقيود التنظيمية من خلال تصميم أنظمة مرنة تسمح بالتجريب في بيئات محمية (Sandbox) خاضعة للرقابة، مع ضمان عدم تأثير ذلك على الإنتاج الفعلي أو سلامة البيانات، وهو نهج تتبناه هيئات تنظيمية كالسلطة التنظيمية في المملكة المتحدة وهيئة البيانات والذكاء الاصطناعي السعودية (Hulok, 2025).

ويُعد التحديث البرمجي المستمر استجابة لتغيرات متطلبات الحوكمة ممارسة أساسية، حيث تُصدر تحديثات دورية للأنظمة لتتوافق مع التشريعات الجديدة والمعايير المتطورة (Batool et al., 2025). ويؤدي الذكاء الاصطناعي نفسه دوراً في تعزيز كفاءة عمليات الحوكمة، كاستخدامه في تحليل النصوص القانونية لاستخراج المتطلبات الآلية، وأتمتة تقييمات الأثر، واكتشاف حالات عدم الامتثال في قواعد البيانات الضخمة (Papagiannidis et al., 2025).

ويدرك الباحث أن التحول من الرقابة التفاعلية إلى الاستباقية يُعد نقلة نوعية في إدارة الامتثال، إذ يُمكن المؤسسات من توقع المشكلات ومعالجتها قبل وقوعها، مما يُقلل التكاليف ويُعزز السمعة، لكنه يتطلب استثماراً في تحليلات متقدمة وكوادر ماهرة، ويستلزم تحديثاً مستمراً للأدوات والنماذج لمواكبة تطور التهديدات والمتطلبات التنظيمية.

6. المعايير القياسية والشهادات الدولية للحوكمة الرقمية

تُعد المواصفات العالمية الصادرة عن المنظمات الدولية كالمنظمة الدولية للتوحيد القياسي (ISO)، واللجنة الكهروتقنية الدولية (IEC) أدوات حاسمة لتوحيد ممارسات الحوكمة وضمان جودة الأنظمة، ومن أبرزها:

- ISO/IEC 38505: (حوكمة البيانات) التي تركز على مسؤوليات الإدارة في توجيه استخدام البيانات.

- **ISO/IEC 42001**: (نظام إدارة الذكاء الاصطناعي) التي توفر متطلبات إنشاء وتطبيق نظام إدارة للذكاء الاصطناعي المسؤول.
- **ISO/IEC 27001**: (أمن المعلومات) التي تُعد المعيار الأكثر انتشاراً لأنظمة إدارة أمن المعلومات (van der Schyff et al., 2024).

وتُعد شهادات الامتثال لأمن المعلومات والخصوصية، كشهادة ISO 27701 (خصوصية المعلومات) التي توسع نطاق ISO 27001 ليشمل الخصوصية، وشهادة معيار الأمن في صناعة بطاقات الدفع (PCI DSS) للمؤسسات المالية، مؤشرات على التزام المؤسسة بأعلى معايير الحماية، مما يُعزز ثقة العملاء والشركاء ويُقلل من مخاطر الاختراق (Pamuk et al., 2024). ويُعد الاعتماد التقني لمزودي حلول الذكاء الاصطناعي (كشهادة مطور AI موثوق من جهة معتمدة، أو شهادة الامتثال لقانون الذكاء الاصطناعي الأوروبي) عاملاً مهماً في السوق الرقمي، حيث يُفضّل العملاء والمؤسسات التعامل مع مزودين حاصلين على هذه الشهادات لتقليل مخاطر الامتثال وضمان الجودة (Albous et al., 2025).

ويؤثر الامتثال للمعايير الدولية على التنافسية في السوق الرقمي، إذ يُعد شرطاً للدخول إلى أسواق معينة (كالاتحاد الأوروبي الذي يشترط الامتثال لقانونه للذكاء الاصطناعي) أو للتعاقد مع جهات حكومية كبرى تطلب شهادات محددة، مما يُشكل حافزاً للمؤسسات للاستثمار في الحوكمة (Tjondronegoro, 2024). وتُطور المؤسسات مقاييس داخلية تتوافق مع أفضل الممارسات العالمية، وتُصمم لوحات معلومات رقمية (Dashboards) لقياس الأداء في مجالات الأمن والخصوصية والامتثال في الوقت الفعلي، مما يُسهل الإدارة واتخاذ القرار والتحسين المستمر (Corea et al., 2023).

وتُشكل التوجهات العالمية (كقانون الذكاء الاصطناعي الأوروبي وقانون الخوارزميات الأمريكية) ضغطاً على الدول لتطوير سيادتها الرقمية من خلال تشريعات وطنية تحمي مصالحها مع الانفتاح على التعاون الدولي، مما يُحفز الدول على بناء قدراتها التنظيمية والتقنية (Zaidan & Ibrahim, 2024). ويُلخص الجدول (2.8) المعايير الدولية الرئيسية المُطبقة في مجال جودة وأمن وخصوصية أنظمة الذكاء الاصطناعي، مُبيناً نطاق كل معيار ومجاله الرئيسي ومتطلباته.

جدول (2.8): المعايير الدولية الرئيسية لحوكمة الذكاء الاصطناعي والبيانات

المعيار	النطاق	المجال الرئيسي	المتطلبات الأساسية
ISO/IEC 38505	حوكمة البيانات	مسؤوليات الإدارة في توجيه استخدام البيانات	وضع سياسات حوكمة البيانات، تخصيص المسؤوليات، ضمان الامتثال
ISO/IEC 42001	الذكاء الاصطناعي	نظام إدارة الذكاء الاصطناعي	تطوير واستخدام مسؤول، إدارة المخاطر، الشفافية، التحسين المستمر
ISO/IEC 27001	أمن المعلومات	نظام إدارة أمن المعلومات	تطبيق ضوابط أمنية، إدارة المخاطر، المراقبة، التحسين المستمر
ISO 27701	خصوصية المعلومات	تمديد ISO 27001 ليشمل الخصوصية	إدارة معلومات التعريف الشخصية، الامتثال لقوانين الخصوصية
ISO 24029	قابلية تفسير النماذج	تقييم قابلية التفسير	تقييم مدى فهم قرارات النموذج وتوثيقها، توفير آليات للتحقق

(المصدر: إعداد الباحث بالاعتماد على: Pamuk et al., 2024; Albous et al., 2025).

يُلاحظ من الجدول (2.8) تعدد أطر الجودة والامتثال المعيارية وتداخلها الوظيفي، إذ تتقاطع معايير الأمن والخصوصية والحوكمة في نقاط عدة، مما يُشير إلى أن الامتثال الكامل يتطلب تنسيقاً استراتيجياً بين هذه المعايير، وهذا يُشكل تحدياً للمؤسسات، ولكنه في الوقت نفسه يُوفر مرونة في اختيار المسار المناسب لحوكمة أنظمتها وفق سياقها التشغيلي واحتياجاتها التنظيمية.

ومن ناحية أخرى، يُقدم الجدول (2.9) تحليلاً مقارناً معمقاً لمدى توافق هذه المعايير الدولية مع متطلبات كل من GDPR و PDPL، مُبيناً نقاط القوة والفجوات المحتملة في كل نظام.

جدول (2.9): التحليل المقارن لتوافق المعايير الدولية مع متطلبات GDPR و PDPL

المعيار الدولي	متطلبات GDPR ذات الصلة	متطلبات PDPL ذات الصلة	درجة التوافق مع PDPL	درجة التوافق مع GDPR	دلالات التحليل
ISO/IEC 38505 (حوكمة البيانات)	المادة 5 (مبادئ المعالجة)، المادة 24 (مسؤولية جهة التحكم)	المادة 2 (أهداف النظام)، المادة	متوسطة	عالية	يوفر المعيار إطاراً لحوكمة البيانات يتماشى مع مبدأ المساءلة في GDPR، لكنه قد

			12 (سياسات الخصوصية)	يحتاج إلى تكيف ليتوافق مع النهج المركزي لـ PDPL	
ISO/IEC 42001 (إدارة الذكاء الاصطناعي)	المادة 22 (القرارات الآلية)، اللائحة الأوروبية للذكاء الاصطناعي	المادة 6 (معالجة البيانات الحساسة)، اللوائح التنفيذية للذكاء الاصطناعي	عالية	منخفضة	يتوافق المعيار بشدة مع توجهات الاتحاد الأوروبي، لكن تطبيقه في السعودية لا يزال في مراحله الأولى، مما يُشير إلى فجوة تنظيمية مؤقتة
ISO/IEC 27001 (أمن المعلومات)	المادة 32 (أمن المعالجة)، المادة 33 (الإبلاغ عن الاختراق)	المادة 10 (التدابير الأمنية)، المادة 20 (الإبلاغ)	عالية جداً	عالية	يُعد هذا المعيار الأكثر توافقاً مع كلا النظامين، حيث تُشكل متطلباته الأمنية أساساً مشتركاً لحماية البيانات في كلا التشريعين
ISO 27701 (خصوصية المعلومات)	المادة 5-11 (حقوق الأفراد)، المادة 35 (تقييم الأثر)	المادة 8-9 (حقوق صاحب البيانات)، المادة 19 (تقييم الأثر)	عالية	متوسطة	يُلبّي المعيار متطلبات الخصوصية التفصيلية في GDPR، بينما قد يحتاج إلى توسيع ليشمل فئات البيانات الحيوية في PDPL
ISO 24029 (قابلية تفسير النماذج)	المادة 13-15 (الشفافية)، المادة 22 (التفسير)	المادة 9 (حق الاعتراض على القرار الآلي)	عالية	منخفضة	يُشير هذا التباين إلى أن PDPL لا يزال بحاجة إلى تطوير معايير واضحة لقابلية التفسير، خاصة في الأنظمة عالية المخاطر

(المصدر: إعداد الباحث بالاعتماد على: van der Schyff et al., 2024; Pamuk et al., 2024; Albous et al., 2025; طه، 2020; محمد، 2022).

يُظهر الجدول (2.9) تبايناً في درجات التوافق بين المعايير الدولية ومتطلبات النظامين، إذ يتفوق GDPR في الاستفادة من معظم المعايير، خاصة في مجالات حوكمة الذكاء الاصطناعي وقابلية التفسير، بينما يُظهر PDPL توافقاً عالياً مع معايير الأمن الأساسية (ISO 27001) لكنه

يحتاج إلى تطوير أطر تنظيمية لتواكب المعايير الأحدث، مثل: ISO 42001 و ISO 24029. ويُشير هذا التباين إلى أن المؤسسات العاملة في السعودية قد تحتاج إلى تبني معايير دولية طوعياً لتعزيز امتثالها، خاصة إذا كانت تخطط للتوسع في الأسواق الأوروبية.

وبناءً على ما تقدم، يرى الباحث أن المعايير والشهادات الدولية ليست مجرد أوراق اعتماد شكلية، بل تمثل التزاماً مؤسسياً باتباع أفضل الممارسات وتطبيق ضوابط رقابية فعالة، كما أن التنافسية في الاقتصاد الرقمي أصبحت مرتبطة ارتباطاً وثيقاً بالقدرة على إثبات الامتثال لهذه المعايير، مما يجعل الاستثمار في الحصول عليها استثماراً استراتيجياً يعزز الثقة ويفتح أسواقاً جديدة.

7. الحوكمة التشاركية والتعاون الدولي في المجال الرقمي

يُعد بناء التعاون بين القطاع العام والخاص في مجال الحوكمة الرقمية أمراً ضرورياً لتطوير سياسات فعالة ومستجيبة للتحديات، حيث يساهم القطاع الخاص بخبراته التقنية ورؤى السوق وقدراته الابتكارية، بينما يضمن القطاع العام حماية المصلحة العامة ووضع الأطر التنظيمية وضمان العدالة والشفافية (ECD, 2024). وتؤدي المؤسسات البحثية والجامعات دوراً محورياً في تطوير أطر الحوكمة من خلال البحوث العلمية الرصينة، وتقييم السياسات القائمة واقتراح تحسيناتها، وتدريب الكوادر وتأهيلها، وتقديم الاستشارات للحكومات والشركات، ونقل المعرفة بين الأطراف المختلفة (Corea et al., 2023).

ويتطلب التعاون الدولي لمواجهة مخاطر الذكاء الاصطناعي العابرة للحدود (كالهجمات السيبرانية، والتضليل المعلوماتي، والأتمتة الضارة، وانتهاكات الخصوصية عبر الحدود) تنسيقاً وثيقاً بين الدول عبر منظمات دولية كالأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية ومجموعة السبع ومجموعة العشرين، لوضع معايير مشتركة وآليات للاستجابة السريعة وتبادل المعلومات حول التهديدات (Roberts et al., 2024).

ويُعد تبادل الخبرات والممارسات الفضلى في التنظيم والرقابة الرقمية قناة مهمة للاستفادة من تجارب الدول الرائدة، كالاتحاد الأوروبي في GDPR وقانون الذكاء الاصطناعي، والولايات المتحدة

في قوانين الخصوصية القطاعية ومبادئ الخوارزميات، والصين في حوكمة البيانات المركزية، مما يُساعد الدول الناشئة على تجنب الأخطاء وتسريع تطوير أنظمتها (Zhong et al., 2025).

وتُصاغ السياسات التقنية الداخلية بما يحقق الامتثال التام للمتطلبات الدولية مع مراعاة السياق المحلي من حيث الثقافة والقيم والاحتياجات الوطنية، وهذا يتطلب فرقاً متعددة التخصصات تجمع بين القانونيين والتقنيين والإداريين لوضع سياسات متوازنة وفعالة (Timan et al., 2021). وتُبنى أطر حوكمة مرنة تستوعب التسارع التقني المستمر من خلال اعتماد مبادئ تصميمية كالطابع المعياري (Modularity) الذي يسمح بتحديث الأجزاء دون إعادة بناء الكل، والقابلية للتحديث (Updateability)، وإشراك أصحاب المصلحة في عمليات المراجعة الدورية، وإجراء تقييمات أثر مستقبلية لاستشراف المخاطر والفرص (Papagiannidis et al., 2025).

ويُخلص الجدول (2.10) أدوار ومشاركات الأطراف المختلفة في منظومة الحوكمة التشاركية، مُبيناً مساهمات كل طرف وآليات التفاعل فيما بينهم.

جدول (2.10): أدوار الأطراف الرئيسية في منظومة الحوكمة التشاركية الرقمية

الطرف	الدور الرئيسي	الآليات التنفيذية	أمثلة تطبيقية
القطاع العام (الحكومة)	وضع الأطر التنظيمية، ضمان المصلحة العامة، الرقابة والإنفاذ	إصدار التشريعات، إنشاء الهيئات الرقابية، فرض العقوبات	هيئة SDAIA في السعودية، المفوضية الأوروبية، هيئات حماية البيانات الوطنية
القطاع الخاص	تطوير الحلول التقنية، توفير الخبرات العملية، الابتكار	المشاركة في الاستشارات العامة، تطبيق معايير الامتثال، تمويل البحوث	شركات التقنية الكبرى (Microsoft، Google)، مزودي خدمات السحاب، الشركات الناشئة
المؤسسات الأكاديمية والبحثية	إنتاج المعرفة، تقييم السياسات، بناء القدرات	البحوث العلمية، ورش العمل، البرامج التدريبية، الدراسات الاستشارية	الجامعات، مراكز الأبحاث، المعاهد المتخصصة في القانون والتقنية
المجتمع المدني والمنظمات غير الحكومية	تمثيل مصالح الأفراد، تعزيز الشفافية، الرقابة المجتمعية	حملات التوعية، التقارير المستقلة، المشاركة في الحوارات العامة	منظمات حماية الخصوصية، جمعيات المستهلكين، النقابات المهنية

OECD، الأمم المتحدة، مجموعة العشرين، المنتدى الاقتصادي العالمي	إصدار المبادئ التوجيهية، تنظيم المؤتمرات، تسهيل الشراكات	تنسيق الجهود الدولية، وضع المعايير العالمية، تبادل المعلومات	المنظمات الدولية
--	--	---	------------------

(المصدر: إعداد الباحث بالاعتماد على: (ECD, 2024; Roberts et al., 2024; Zhong et al., 2025).

يُظهر الجدول (2.10) تنوع الأدوار وتكاملها في منظومة الحوكمة التشاركية، حيث لا يمكن لأي طرف بمفرده تحقيق حوكمة رقمية فعالة. ويُشير هذا التكامل إلى أن نجاح أنظمة مثل PDPL وGDPR يعتمد على قدرتها على استيعاب مساهمات جميع الأطراف، وتوفير آليات للحوار والتعاون المستمر، مما يُعزز شرعية القرارات التنظيمية ويُحسن فعالية تنفيذها.

وفي هذا السياق، يرى الباحث أن الحوكمة التشاركية والتعاون الدولي ليسا خياراً إضافياً، بل ضرورة حتمية في عالم مترابط رقمياً، إذ أن تحديات الذكاء الاصطناعي لا تعترف بالحدود الوطنية، كما أن تبادل الخبرات يُسرّع من نضج الأطر التنظيمية ويُقلل من تكاليف التجربة والخطأ، وهذا يتطلب من الدول استثماراً في الدبلوماسية الرقمية وبناء شراكات استراتيجية مع الدول والمنظمات الدولية.

8. التكامل بين التشريعات القانونية والكود البرمجي

تمثل الفجوة بين النص القانوني (الذي يغلب عليه الطابع اللغوي والوصفي والمرن)، والكود البرمجي (الذي يتطلب دقة منطقية وخوارزمية قابلة للتنفيذ) تحدياً هيكلياً في تنظيم الذكاء الاصطناعي، إذ يصعب ترجمة متطلبات قانونية عامة، مثل: (المعاملة العادلة، الشفافية المعقولة، الخصوصية بالتصميم) إلى قواعد برمجية محددة وقابلة للتحقق والاختبار (Lazcoz & De Hert, 2023). وتستلزم صياغة تشريعات مرنة تدعم الابتكار التقني استخدام لغة قانونية تعتمد على المبادئ والغايات (Principles-based) بدلاً من التفاصيل الفنية الجامدة، مع ترك مساحة للتفسير والتكيف مع التطورات المستقبلية، مع توفير أدلة إرشادية لتوضيح كيفية التطبيق (Hohmann & Kollár, 2025).

إن بناء لغة مشتركة بين المشرعين ومهندسي الأنظمة الذكية يُعد ضرورة ملحة، ويتحقق ذلك من خلال ورش عمل مشتركة، وأدلة تفسيرية (Interpretive Guidelines) تُترجم النصوص القانونية إلى متطلبات تقنية، ونماذج تطبيقية (Use Cases) تُوضح كيفية تحقيق الامتثال عملياً، وتطوير معاجم موحدة للمصطلحات (Kalodanis et al., 2025). ويُشكل التحديث القانوني المتسارع (كصدور قوانين جديدة للذكاء الاصطناعي بشكل متكرر) ضغطاً على استقرار الأنظمة التقنية، مما يستدعي تصميم أنظمة قابلة لإعادة التهيئة والتكوين بسرعة (Reconfigurable) عبر استخدام ملفات تكوين خارجية أو وحدات برمجية قابلة للتبديل، وتطوير أدوات ترجمة قانونية آلية تستخرج المتطلبات من النصوص وتحولها إلى قواعد (Lorè et al., 2023).

ويُمكن تحويل القواعد التنظيمية إلى محددات برمجية صلبة (كقيود في الكود تمنع استخدام البيانات لأغراض غير مصرح بها، أو تفرض حداً أقصى لفترة الاحتفاظ بالبيانات، أو تجبر على طلب موافقة قبل المشاركة)، مما يُعزز الامتثال التلقائي ويُقلل من الأخطاء البشرية والتجاوزات المتعمدة (Holtz & Ledendal, 2026). ويُعد التكامل بين الأطر القانونية والمعايير التقنية (كمعايير ISO الخاصة بالذكاء الاصطناعي) في الحوكمة نهجاً متكاملاً يضمن أن الأنظمة ليست قانونية فقط بل تتوافق أيضاً مع الممارسات الهندسية الفضلى، مما يُعزز فعالية الحوكمة واستدامتها ويُقلل من النزاعات القانونية (Zaidan & Ibrahim, 2024).

والشكل (2.4) يوضح عملية تحويل المتطلبات التشريعية إلى كود برمجي قابل للتنفيذ، والتي تمر بمراحل متسلسلة تبدأ بالنص التشريعي، ثم التحليل والتفسير القانوني، ثم استخراج المتطلبات الواضحة، ثم ترجمتها إلى مواصفات تقنية مفصلة، ثم تطوير الكود، ثم اختباره والتحقق من امتثاله، وأخيراً تحديثه دورياً مع التغيرات التشريعية.



شكل (2.4): عملية تحويل المتطلبات التشريعية إلى كود برمجي قابل للتنفيذ

يُبرز الشكل (2.4) الطبيعة الدورية والمستمرة لعملية تحويل التشريعات إلى كود برمجي، مما يُشير إلى أن الامتثال ليس حدثاً لمرة واحدة بل عملية متجددة تتطلب تنسيقاً مستمراً بين الفرق القانونية والتقنية. كما يُظهر الشكل أن نجاح هذه العملية يتوقف على جودة التفسير القانوني ودقة استخراج المتطلبات وكفاءة الترجمة إلى مواصفات تقنية، وهو ما يُشكل تحدياً معرفياً وتنظيماً يتطلب استثماراً في بناء القدرات المشتركة وتطوير أدوات متخصصة.

ويُقدم الجدول (2.11) تحليلاً مقارناً للتحديات والحلول المتعلقة بسد الفجوة بين النص القانوني والكود البرمجي، مع التركيز على دلالات ذلك على الامتثال في سياق GDPR و PDPL.

جدول (2.11): التحليل المقارن لتحديات وحلول التكامل بين التشريعات والكود البرمجي في سياق GDPR

PDPL و

التحدي الرئيسي	المظاهر في سياق GDPR	المظاهر في سياق PDPL	الحلول التقنية والتشريعية المقترحة	دلالات التحليل
غموض المصطلحات القانونية	مفاهيم مثل المعاملة العادلة والشفافية المعقولة	مفاهيم مثل الموافقة الصريحة والضرورة	تطوير أدلة تفسيرية مفصلة، إنشاء معاجم موحدة للمصطلحات القانونية والتقنية	يُواجه كلا النظامين تحديات في الترجمة الدقيقة، لكن GDPR يتمتع بخبرة أطول في إنتاج الأدلة التفسيرية
سرعة التطور التقني	مواكبة تشريعات 2018 لتقنيات 2025 (كالنماذج التوليدية)	مواكبة تشريعات 2024 لتقنيات متسارعة	اعتماد نهج تنظيمي مرن (Principles-based)، تحديث دوري للوائح التنفيذية	يُظهر GDPR مرونة أفضل في استيعاب التقنيات الجديدة، بينما قد يواجه PDPL تحديات أكبر بسبب توقيته وطبيعته تفصيلية
تعقيد الأنظمة الخوارزمية	صعوبة توفير تفسيرات للقرارات الآلية (المادة 22)	صعوبة تطبيق حق الاعتراض على القرارات الآلية (المادة 9)	تطوير أدوات XAI مدمجة، فرض متطلبات التوثيق والتدقيق الخوارزمي	يُشير التحدي إلى ضرورة الاستثمار في بحوث قابلية التفسير وتطوير معايير فنية واضحة في كلا النظامين
تعدد الولايات القضائية	تطبيق اللائحة على مؤسسات خارج الاتحاد	تطبيق النظام على المؤسسات الأجنبية التي تتعامل مع سوق السعودي	توحيد آليات النقل (SCCs، BCR)، الاعتراف المتبادل بالشهادات	يفرض التحدي حاجة ملحة للتعاون الدولي وبناء آليات امتثال عابرة للحدود

(المصدر: إعداد الباحث بالاعتماد على Hohmann & Kollár, 2025; Holtz & Ledendal, 2026;

Kalodanis et al., 2025).

يُظهر الجدول (2.11) أن التحديات المتعلقة بتكامل القانون والكود متشابهة في جوهرها بين GDPR و PDPL، لكنها تختلف في حدتها وتفاصيلها. فبينما يتمتع GDPR بخبرة أطول ومرونة أكبر، يواجه PDPL تحديات مرتبطة بحدائته وطبيعة تفاصيله التنفيذية. ويُشير هذا التباين إلى أن نجاح PDPL في تحقيق امتثال فعال سيعتمد على سرعة تطوير أدواته التفسيرية والرقابية، والاستفادة من الدروس المستفادة من تجربة GDPR في هذا المجال.

وبناءً على ما سبق، يرى الباحث أن تجاوز الفجوة بين القانون والكود يتطلب تعاوناً وثيقاً ومستمراً بين المشرعين والتقنيين، كما يستلزم تطوير أدوات وأطر جديدة تُمكن من ترجمة المتطلبات القانونية إلى قواعد برمجية قابلة للتنفيذ والاختبار، وهذا يُشكل مجاًلاً خصباً للابتكار في حوكمة الذكاء الاصطناعي، ويتطلب استثماراً في البحث والتطوير وبناء القدرات المشتركة بين التخصصات، مع إدراك أن هذه العملية ديناميكية وتتطلب مراجعة وتحديثاً مستمرين لمواكبة التغيرات التشريعية والتقنية.

المحور الرابع: التحليل المقارن لآليات الامتثال بين (GDPR)، و (PDPL)

يُخصص هذا المحور للجانب التطبيقي والمقارن لبيئة الدراسة في المملكة العربية السعودية والاتحاد الأوروبي، إذ يتناول الإطار التنظيمي لكلا النظامين، والتحليل المقارن للمفاهيم والحقوق، وآليات الامتثال ونقل البيانات، وسياسات العقوبات، وحوكمة الذكاء الاصطناعي في السياق السعودي، وتحليل الفجوات والدروس المستفادة من التجربة الأوروبية، والتوجهات المستقبلية للاندماج بين الابتكار والامتثال. ويُعد التحليل المقارن بين نظام حماية البيانات الشخصية السعودي (PDPL)، واللائحة العامة الأوروبية (GDPR) أداة منهجية لتحديد نقاط التقاطع والاختلاف، واستخلاص الدروس التي تُسهم في تطوير المنظومة الوطنية وتعزيز فعالية الامتثال في البيئة الرقمية.

وقد اعتمد الباحث في بناء هذا الإطار التحليلي المقارن على معايير حوكمة رشيدة مستمدة من الأدبيات الدولية، حيث تم اختيار أبعاد المقارنة بناءً على قدرتها الاختبارية في قياس كفاءة البيئة التنظيمية، وإعطاء الأولوية لآليات امتثال محددة نظراً لارتباطها المباشر بالبنية الهندسية للأنظمة الذكية.

1. الإطار التنظيمي لنظام حماية البيانات الشخصية السعودي (PDPL)

صدر نظام حماية البيانات الشخصية السعودي (PDPL) بموجب المرسوم الملكي رقم م/19 بتاريخ 1443/2/9هـ (الموافق 2021/9/16م)، ودخلت أحكامه التنفيذية حيز النفاذ في 2024/9/14م، وذلك ضمن جهود المملكة لمواكبة التطورات الرقمية وتحقيق مستهدفات رؤية 2030 المتعلقة ببناء مجتمع رقمي آمن وجاذب للاستثمار (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2025). ويتمثل الهدف الرئيس للنظام في حماية خصوصية الأفراد من خلال تنظيم جمع ومعالجة ونقل البيانات الشخصية، مع تحقيق التوازن بين حماية الحقوق وتعزيز الابتكار والنمو الاقتصادي (الشمري، نجم، 2023).

وتُسند الاختصاصات التنفيذية والإشرافية إلى الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) بوصفها الجهة المختصة بإصدار اللوائح والسياسات، ومنح التراخيص، وتلقي

وتُكْمَل النظامَ لاحتِته التنفيذية التي تحدد الإجراءات التفصيلية للموافقة، وتقييمات الأثر، ونقل البيانات، والإبلاغ عن الحوادث، بالإضافة إلى سياسات مكملّة كسياسة الخصوصية والنماذج المعيارية، مما يُوفّر إطاراً تشغيلياً متكاملًا للمؤسسات (العتيبي، أمانى، 2025). وتُطلق المملكة مبادرات وطنية لتعزيز الوعي والالتزام بخصوصية البيانات، كمنصة حوكمة البيانات الوطنية التي توفر أدلة وشروحات، وحملات توعوية تستهدف مختلف شرائح المجتمع والمنشآت، مما يُسهم في بناء ثقافة امتثال راسخة (الظفيري، 2025). ويُعد PDPL نقلة نوعية في التشريع السعودي، إذ يُحقّق توافقاً مع المعايير الدولية مع مراعاة الخصوصية الثقافية والدينية للمملكة، مما يعزز مكانتها كوجهة رقمية رائدة في المنطقة ويجذب الاستثمارات التقنية العالمية (Ibrahim, 2024).

يُبين الشكل (2.5) البنية التشريعية والتنفيذية لنظام PDPL، موضحاً العلاقة بين المرسوم الملكي، واللائحة التنفيذية، والهيئة الرقابية (SDAIA)، والسياسات المكملة، ونطاق التطبيق.

ويُبرز الشكل أن نجاح النظام يعتمد على تكامل هذه العناصر معاً، حيث تضع SDAIA المعايير وتُمارس الرقابة، بينما تُترجم اللائحة التنفيذية الأحكام العامة إلى إجراءات تفصيلية، وتُسهّم المنصة الوطنية في تعزيز الوعي والامتثال، مما يُشكل منظومة متجانسة لحماية البيانات.

2. البنية التشريعية لللائحة العامة لحماية البيانات الأوروبية (GDPR)

صدرت اللائحة العامة لحماية البيانات الأوروبية (GDPR) في 27 أبريل 2016، ودخلت حيز التطبيق في 25 مايو 2018، لتحل محل التوجيه EC46/95، وذلك بهدف تحديث وتوحيد قوانين حماية البيانات في جميع الدول الأعضاء بالاتحاد الأوروبي، وتوفير مستوى عالٍ من الحماية للأفراد في مواجهة التحديات الرقمية المعاصرة (Kuner et al., 2021). وتستند اللائحة إلى فلسفة تشريعية تقوم على مبادئ: حماية الحقوق الأساسية للأفراد، وضمان حرية تدفق البيانات داخل الاتحاد، وتعزيز الثقة في الاقتصاد الرقمي، وفرض عقوبات رادعة لضمان الامتثال (العيش، 2023).

ويُعد التطبيق الإقليمي لللائحة (المادة 3) من أبرز سماتها، إذ تنطبق ليس فقط على المنشآت المقيمة في الاتحاد الأوروبي، بل أيضاً على أي منشأة خارج الاتحاد تعالج بيانات أفراد موجودين في الاتحاد، مما يُعطيها أثراً عابراً للحدود يجعلها نموذجاً عالمياً يُحتذى به في تشريعات الخصوصية (طه، 2020). وتمنح اللائحة الأفراد في الاتحاد الأوروبي مجموعة شاملة ومفصلة من الحقوق (المواد 12-22)، تتضمن الحق في الوصول والتصحيح والمسح وتقييد المعالجة ونقل البيانات والاعتراض، وحق عدم الخضوع لقرار آلي، مما يُشكل حزمة حقوقية متكاملة تُعزز سيطرة الفرد على بياناته (الشامسي، 2023).

وتعمل آليات التعاون والرقابة من خلال هيئات حماية البيانات الوطنية في كل دولة عضو، التي تتنسق عبر المجلس الأوروبي لحماية البيانات (EDPB) لضمان تطبيق موحد لللائحة، مع صلاحيات للتحقيق وفرض العقوبات وإصدار التوجيهات (العيش، 2023). وتنص اللائحة على عقوبات مالية تصل إلى 20 مليون يورو أو 4% من الإيرادات العالمية السنوية للمنشأة (أيهما أكبر)، مما يُشكل رادعاً قوياً للامتثال، وقد تجاوز إجمالي الغرامات المفروضة منذ تطبيقها حتى عام 2025 مبلغ (4) مليارات يورو (Frey & Presidente, 2024). وقد أثرت اللائحة الأوروبية

بشكل جوهري في توجهات الشركات التقنية الكبرى، إذ أجبرتها على إعادة تصميم منتجاتها وخدماتها لتتوافق مع متطلبات الخصوصية، واعتماد ممارسات الشفافية والموافقة الصريحة، وإنشاء فرق متخصصة للامتثال، مما جعلها معياراً عالمياً لحماية البيانات (Kumar & Singh, 2024).

ويُلخص الجدول الآتي المقارنة العامة بين PDPL السعودي وGDPR الأوروبي في سبعة معايير رئيسية، مُبيناً أوجه التشابه والاختلاف في الإصدار والنطاق والجهة الرقابية والحقوق والغرامات وآليات نقل البيانات.

جدول (2.12): المقارنة العامة بين نظام PDPL السعودي ولائحة GDPR الأوروبية

معيار المقارنة	PDPL السعودي	GDPR الأوروبي
سنة الإصدار	2021 (نفذ 2024)	2016 (نفذ 2018)
النطاق الجغرافي	المملكة العربية السعودية، والأفراد المقيمين فيها	الاتحاد الأوروبي، وأي منشأة تعالج بيانات أفراد في الاتحاد
الجهة الرقابية	الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)	هيئات حماية البيانات الوطنية، والمجلس الأوروبي (EDPB)
الحقوق الرئيسية	الوصول، التصحيح، المسح، نقل البيانات، الاعتراض	الوصول، التصحيح، المسح، تقييد المعالجة، نقل البيانات، الاعتراض، عدم الخضوع لقرار آلي
الغرامات القصوى	5 ملايين ريال (10 ملايين في حال التكرار)	20 مليون يورو أو 4% من الإيرادات العالمية
نقل البيانات العابر للحدود	بقرار من الهيئة أو اتفاقية معتمدة	قرارات الملاءمة، القواعد المؤسسية الملزمة، البنود التعاقدية القياسية

(المصدر: إعداد الباحث بالاعتماد على: طه، 2020؛ العيش، 2023؛ Frey & Presidente, 2024).

يُلخص الجدول (2.12) المقارنة العامة بين PDPL وGDPR في سبعة معايير رئيسية، مُبيناً أوجه التشابه والاختلاف في الإصدار والنطاق والجهة الرقابية والحقوق والغرامات وآليات نقل البيانات، مما يُوفر رؤية شاملة للخصائص الأساسية لكل نظام ويسهل فهم موقعهما النسبي في المشهد التنظيمي العالمي.

وجدير بالذكر، أنه على الرغم من الريادة التشريعية للنموذج الأوروبي (GDPR)، إلا أنه واجه انتقادات واسعة تتعلق بالتجاوز التنظيمي (Regulatory Overreach) الذي قد يكبل تدفق الابتكار الرقمي، ويفرض قيوداً صارمة على خوارزميات التعلم العميق بسبب شرط التفسيرية الصارم، مما دفع المشرع السعودي في نظام (PDPL) إلى محاولة خلق توازن استراتيجي يضمن حماية الخصوصية دون التضحية بالمستهدفات الابتكارية لرؤية 2030.

3. التحليل المقارن للمفاهيم والتعريفات والحقوق الرقمية

يُظهر التحليل المقارن بين PDPL وGDPR تقاطعاً كبيراً في التعريفات الجوهرية مع بعض الاختلافات الدقيقة، فكلهما يُعرّف البيانات الشخصية بأنها كل ما يُمكن به التعرف على الفرد مباشرة أو غير مباشرة، لكن GDPR يوسع نطاق التعريف ليشمل المعرفات عبر الإنترنت كعنوان IP وملفات تعريف الارتباط (طه، 2020)، بينما يترك PDPL المجال لللائحة التنفيذية لتحديد ذلك بشكل أكثر تفصيلاً (الشمري، نجم، 2023). وتُصنف كلتا التشريعتين البيانات الحساسة (كالصحية والبيومترية) بدرجة حماية أعلى، مع إضافة PDPL فئة البيانات الحيوية التي تحظى بحماية مشددة، بينما يُدرجها GDPR ضمن البيانات الحساسة دون تمييز صريح (أبو خمرة، 2021).

وتتشابه الحقوق الممنوحة لأصحاب البيانات إلى حد كبير، مع تفوق GDPR في تفصيل بعض الحقوق كالحق في قابلية نقل البيانات (المادة 20) الذي يتطلب توفير البيانات بتنسيق منظم وشائع الاستخدام وقابل للقراءة آلياً، بينما يُقر PDPL الحق في النقل لكنه يترك التفاصيل لللائحة التنفيذية (إمام وآخرون، 2024). ويختلف النظامان في القواعد المتعلقة بمعالجة البيانات: إذ يُلزم GDPR بوجود أساس قانوني واضح للمعالجة من بين ستة أسس (كالموافقة، والعقد، والمصلحة المشروعة)، بينما يُركز PDPL على الموافقة كأساس رئيسي مع إضافة حالات خاصة للمعالجة دون موافقة (كالالتزام النظامي والمصلحة العامة) (محمد، 2022).

وتتباين اشتراطات الحصول على الموافقة الصريحة، فGDPR يشترط أن تكون الموافقة فعلية إيجابية (ليست افتراضية)، وقابلة للسحب بسهولة، بينما PDPL ينص على أن تكون الموافقة صريحة ومكتوبة أو عبر وسيلة تقنية موثوقة، مع اشتراطات إضافية للبيانات الحساسة والحوية (فلاتة، 2025). وتُحدد مدة الاحتفاظ بالبيانات في كلا النظامين بموجب الغرض من المعالجة، مع إلزامية الإتلاف الآمن بعد انتهاء الغرض، لكن PDPL يمنح الجهة التنظيمية صلاحية تحديد مدد قصوى للاحتفاظ ببعض فئات البيانات (الجيجكلي، 2025).

ويُعد تقييم مرونة النصوص النظامية تجاه استيعاب التقنيات المستقلة مجالاً للتباين، إذ تُعد لائحة GDPR أكثر مرونة وتعميماً مما يسمح بتفسير واسع يشمل التقنيات الناشئة، بينما يتجه

PDPL نحو تفصيل أحكامه في اللوائح التنفيذية مما قد يُبطئ التكيف مع المستجدات التقنية (الغافري، 2026). ويُخلص الجدول الآتي التحليل المقارن المعمق للمفاهيم والتعريفات والحقوق الرقمية بين PDPL وGDPR، مُبيناً أوجه التشابه والاختلاف في سبعة أبعاد رئيسية.

جدول (2.13): التحليل المقارن المعمق للمفاهيم والتعريفات والحقوق الرقمية بين PDPL وGDPR

البُعد المقارن	PDPL السعودي	GDPR الأوروبي	دلالات الاختلاف
تعريف البيانات الشخصية	كل ما يُمكن به التعرف على الفرد مباشرة أو غير مباشرة، مع ترك تفاصيل المعلومات الرقمية للائحة التنفيذية	كل ما يُمكن به التعرف على الفرد مباشرة أو غير مباشرة، ويشمل صراحةً عناوين IP وملفات تعريف الارتباط	يمنح GDPR وضوحاً فورياً، بينما يوفر PDPL مرونة في التحديد لاحقاً
البيانات الحساسة والحيوية	يميز بين الحساسة (الصحية والدينية)، والحيوية (البصمات والحيوانات) مع حماية مشددة للثانية	يُصنف الحيوية ضمن الحساسة دون تمييز صريح، مع متطلبات حماية موحدة	يوفر PDPL طبقة حماية إضافية للبيانات الحيوية، مما يعكس أولوية وطنية
أسس المعالجة القانونية	يركز على الموافقة كأساس رئيسي، مع حالات استثنائية محدودة (النظام والمصلحة العامة)	يحدد ستة أسس واضحة (الموافقة، العقد، المصلحة المشروعة، الالتزام القانوني، حماية المصالح الحيوية، المهمة العامة)	يوفر GDPR تنوعاً في الأسس، بينما PDPL أكثر تقييداً مما قد يحد من بعض المعالجات المشروعة
شروط الموافقة الصريحة	موافقة صريحة مكتوبة أو عبر وسيلة تقنية موثوقة، مع اشتراطات إضافية للحساسة	موافقة فعلية إيجابية، قابلة للسحب بسهولة، وغير مفترضة	اشتراطات GDPR أكثر صرامة في سهولة السحب، بينما PDPL يُشدد على الشكل الكتابي
حق نقل البيانات (قابلية النقل)	مُقر لكن تفاصيله (التنسيق، الآلية) تترك للائحة التنفيذية	مفصل في المادة 20، ويتطلب تنسيقاً منظماً وشائع الاستخدام وقابلاً للقراءة آلياً	تفوق GDPR في التفصيل يُسهل التطبيق العملي ويُعزز المنافسة بين الخدمات
مدة الاحتفاظ بالبيانات	تُحدد بموجب الغرض، مع صلاحية للجهة التنظيمية لتحديد مدد قصوى	تُحدد بموجب الغرض، دون تدخل تشريعي مباشر في تحديد مدد قصوى عامة	يمنح PDPL للهيئة صلاحية رقابية أوسع في تحديد الفترات الزمنية
المرونة تجاه التقنيات المستقلة	يتجه نحو التفصيل في اللوائح التنفيذية، مما قد يُبطئ التكيف	يعتمد لغة مبدئية عامة، مما يسمح بتفسير واسع ومرن يشمل التقنيات الجديدة	GDPR أكثر استعداداً لاستيعاب الابتكارات المستقبلية، بينما PDPL أكثر حذراً

(المصدر: إعداد الباحث بالاعتماد على: محمد، 2022؛ فلاتة، 2025؛ الجيجلي، 2025).

يُظهر الجدول (2.13) أن PDPL وGDPR يتقاطعان في المبادئ العامة لحماية البيانات، لكنهما يختلفان في درجة التفصيل والمرونة والأسس القانونية. ويُشير هذا التباين إلى أن PDPL، رغم استفادته من الخبرة الأوروبية، يُفضل نهجاً أكثر تحفظاً وتفصيلاً عبر اللوائح التنفيذية، بينما يعتمد GDPR على لغة مبدئية تسمح بتفسير ديناميكي يتواءم مع الابتكار التقني.

وفي ضوء ذلك، يرى الباحث أن هذا الاختلاف يعكس أولويات كل نظام؛ فGDPR يُعطي الأولوية للتوحيد والمرونة في سوق موحدة، بينما يُركز PDPL على الحماية التدريجية والرقابة المكثفة في سياق وطني ناشئ، مما يستدعي من المؤسسات العاملة في البيئتين فهماً عميقاً لهذه الفروق لتجنب مخاطر عدم الامتثال.

4. آليات الامتثال ونقل البيانات العابرة للحدود

تُشترط كل من PDPL وGDPR توافر ضمانات كافية لنقل البيانات الشخصية خارج النطاق الجغرافي، لكنهما يختلفان في الآليات المحددة: يُقرر GDPR أن النقل إلى دولة أو منظمة دولية جائز إذا قررت المفوضية الأوروبية أن الدولة توفر مستوى كافٍ من الحماية (قرارات الملاءمة)، أو في غياب ذلك، عبر الضمانات المناسبة كالقواعد المؤسسية الملزمة (BCR)، والبنود التعاقدية القياسية (SCCs)، والسلوك المهني المعتمد (المادة 45-46) (العيش، 2023).

بينما ينص PDPL (المادة 29) على أنه لا يُنقل البيانات الشخصية إلى خارج المملكة إلاّ بناءً على قرار من الهيئة المختصة يُحدد قائمة الدول أو المنظمات التي توفر مستوى مناسباً من الحماية، أو بموجب اتفاقية تعاقدية معتمدة من الهيئة، أو في حالات محددة كالضرورة لإنقاذ حياة الفرد أو تنفيذ التزام تعاقدية (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2025).

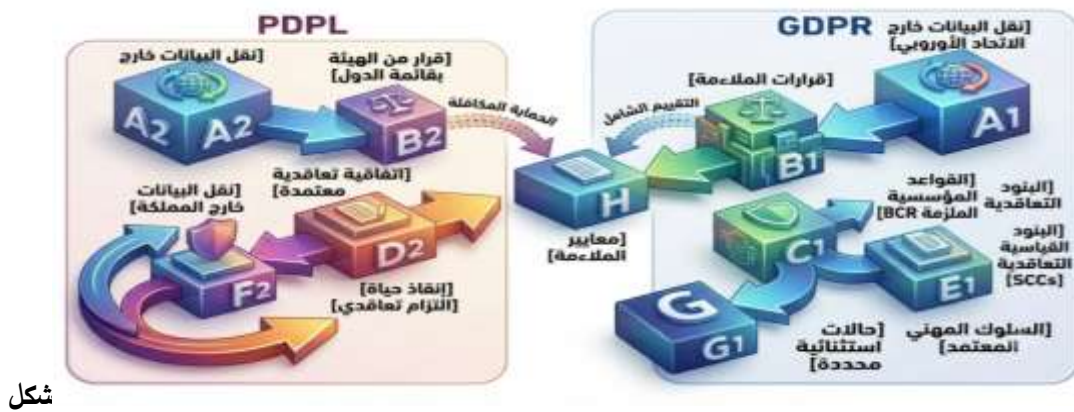
وتُقارن معايير الملاءمة بين النظامين: يركز GDPR على تقييم شامل لنظام الدولة من حيث حقوق الإنسان وسيادة القانون والرقابة الفعالة، بينما يُركز PDPL على توفر حماية مكافئة في الدولة المتلقية مع مراعاة العلاقات الدولية والسياسات الوطنية (الشمري، نجم، 2023). وتتشابه القواعد المؤسسية الملزمة والبنود التعاقدية القياسية في كلا النظامين من حيث الهدف، لكن

إجراءات الاعتماد في PDPL لا تزال قيد التطوير، بينما تمتلك GDPR خبرة متراكمة في هذا المجال (محمد، 2022).

ويُعد دور مسؤول حماية البيانات (DPO) محورياً في كلا النظامين، حيث يُلزم PDPL الجهات التي تعالج كميات كبيرة من البيانات الحساسة أو تراقب الأفراد على نطاق واسع بتعيين مسؤول (المادة 20)، ويُشابه ذلك متطلبات GDPR (المادة 37-39)، مع اختلافات في المؤهلات والاستقلالية ومهام التبليغ (الجربوع، 2024).

وتُحدد الإجراءات والمدد الزمنية للتبليغ عن حوادث الاختراق في كلا النظامين: تُلزم GDPR بتبليغ السلطة المختصة خلال (72 ساعة) من علم المنشأة بالحدث (المادة 33)، بينما يُلزم PDPL بالتبليغ فوراً دون تحديد مدة محددة في النص الرئيسي (المادة 20)، تاركاً التفاصيل لللائحة التنفيذية (عفيفي، 2025). وتشمل متطلبات التدقيق للمؤسسات العاملة في البيئتين إجراء تقييمات أثر دورية، وتوثيق أنشطة المعالجة، وتطبيق مبادئ الخصوصية بالتصميم، مما يُشكل عبئاً تشغيلياً لكنه يُعزز نضجها في حماية البيانات (الترك، 2025).

والشكل الآتي يوضح آليات نقل البيانات العابرة للحدود في كلا النظامين، مُبيناً أوجه التشابه والاختلاف في الأدوات والضمانات المطلوبة.



(2.6): آليات نقل البيانات العابرة للحدود - مقارنة بين GDPR و PDPL

يُبين الشكل (2.6) آليات نقل البيانات في كلا النظامين، حيث يعتمد GDPR على مسارين رئيسيين (قرارات الملاءمة والضمانات المناسبة) مع تنوع في الأدوات (BCR، SCCs)، بينما يعتمد PDPL على آليات أكثر مركزية (قرار الهيئة أو اتفاقية معتمدة). ويُبرز الشكل أن كلا

النظامين يشترطان وجود ضمانات كافية، لكن GDPR يوفر مرونة أكبر من خلال تعدد الأدوات، بينما يُركز PDPL على الرقابة المباشرة من الهيئة.

وبناءً على ما تقدم، يرى الباحث أن تعقيد آليات نقل البيانات العابرة للحدود يُشكل أحد أكبر التحديات أمام المؤسسات العاملة دولياً، خاصة في ظل تباين متطلبات PDPL وGDPR، مما يستدعي تطوير استراتيجيات امتثال مرنة وقابلة للتكيف، والاستثمار في أدوات إدارة الموافقات والنقل الآلي، وبناء شراكات مع مستشارين قانونيين وتقنيين متخصصين في كلا النظامين.

5. مقارنة سياسات العقوبات وآليات التنفيذ الرقابي

يُظهر تحليل هيكل الغرامات المالية تفوقاً واضحاً لللائحة العامة الأوروبية لحماية البيانات (GDPR) من حيث الحجم والتصنيف، إذ تُصنف الغرامات إلى مستويين؛ يصل الأول إلى (10) ملايين يورو أو (2%) من الإيرادات العالمية السنوية للانتهاكات الإدارية (كعدم التعاون مع الهيئة)، ويصل الثاني إلى (20) مليون يورو أو (4%) من الإيرادات العالمية السنوية للانتهاكات الجوهرية (كانتهاك مبادئ المعالجة وحقوق الأفراد) (المادة 83) (العيش، 2023).

وفي المقابل، ينص نظام حماية البيانات الشخصية السعودي (PDPL) على غرامات تصل إلى (5) ملايين ريال سعودي (نحو 1.33 مليون يورو) للمخالفات الواردة في النظام، و(10) ملايين ريال في حال تكرار المخالفة (المادة 37) (الشمري، نجم، 2023)، مما يُشكل فارقاً كبيراً في حجم الردع المالي قد يُؤثر في فعالية النظام في مرحلته الأولى، خاصة في ظل غياب التصنيف الهرمي للغرامات الذي يُتيح للسلطات الرقابية درجة من المرونة في تقدير العقوبات تتناسب مع جسامة المخالفة.

وتشمل الإجراءات التصحيحية والتدابير الإدارية التي تفرضها السلطات في كلا النظامين: الإنذارات، وأوامر وقف المعالجة، وتقييد المعالجة، وسحب التراخيص، والغرامات، مع تنوع في صلاحيات الهيئات ونطاق التدخل (الجربوع، 2024). ويختلف دور الجهات القضائية في الفصل في منازعات حماية البيانات؛ ففي الاتحاد الأوروبي، يملك الأفراد حق التقاضي المباشر أمام المحاكم الوطنية استناداً إلى اللائحة، بالإضافة إلى حق التظلم لدى هيئات حماية البيانات (المادة

(82)، بينما في السعودية يُحال النزاع إلى اللجنة القضائية المختصة وفق نظام المرافعات، مع دور للهيئة في التوفيق والوساطة (إمام وآخرون، 2024).

وتُوفر آليات التظلم والطعن على القرارات الرقابية في كلا النظامين ضمانات للمنشآت والأفراد، لكن GDPR يتميز بتنظيم تفصيلي للحق في الاستئناف القضائي ضد قرارات الهيئات (المادة 78) (طه، 2020). وتُظهر الأدلة أن عقوبات GDPR كانت فعالة في ردع الانتهاكات وتحسين ممارسات الخصوصية عالمياً، إذ سجلت الهيئات الأوروبية الآلاف من الغرامات التي تجاوزت قيمتها الإجمالية (4 مليارات يورو بحلول عام 2025) (Frey & Presidente, 2024)، بينما لا يزال نظام PDPL في مراحله الأولى، مما يصعب تقييم فعالية عقوباته بعدُ (الشمري، فهد، 2023).

ويُعد تأثير العقوبات في السمعة المؤسسية والقيمة السوقية للمنشآت عاملاً مهماً؛ إذ تؤدي الغرامات الكبيرة والإفصاح عنها إلى خسائر سماعية تؤثر في ثقة العملاء والمستثمرين، مما يُعزز دوافع الامتثال بما يتجاوز الجانب المالي (Kumar & Singh, 2024). ويلاحظ أن النظام السعودي، رغم حداثة، قد استفاد من التجربة الأوروبية في تصميم إطار عام للعقوبات، لكنه لا يزال بحاجة إلى تطوير آليات تنفيذية أكثر تفصيلاً لضمان فعالية الردع، خاصة فيما يتعلق بتحديد معايير تقدير الغرامات و ضمانات التقاضي العادل.

ويُلخص الجدول الآتي المقارنة التفصيلية بين سياسات العقوبات في النظامين، مُبيناً أوجه التشابه والاختلاف في هيكل الغرامات، والإجراءات التصحيحية، وآليات التقاضي، وفعالية الردع.

جدول (2.14): التحليل المقارن لسياسات العقوبات وآليات التنفيذ الرقابي بين PDPL وGDPR

معيار المقارنة	PDPL السعودي	GDPR الأوروبي	دلالات التحليل
هيكل الغرامات	مستوى واحد: 5 ملايين ريال (10 ملايين عند التكرار)	مستويان: 10 مليون يورو (2% من الإيرادات) للانتهاكات الإدارية، و20 مليون يورو (4% من الإيرادات) للانتهاكات الجوهرية	يُشير الفارق الكبير إلى أن GDPR يُوفر ردعاً مالياً أقوى، بينما قد يكون PDPL في مرحلته الأولى أقل تأثيراً
الإجراءات التصحيحية	إنذارات، وقف المعالجة، تقييد المعالجة، سحب التراخيص، غرامات	إنذارات، وقف المعالجة، تقييد المعالجة، سحب التراخيص، غرامات	تتشابه الإجراءات التصحيحية في كلا النظامين، لكن صلاحيات الهيئات ونطاق التدخل تختلف
آليات التقاضي	إحالة النزاع إلى اللجنة القضائية المختصة، مع دور للهيئة في التوفيق والوساطة	حق التقاضي المباشر أمام المحاكم الوطنية، وحق التظلم لدى هيئات حماية البيانات (المادة 82)	يُوفر GDPR حماية قضائية أوسع للأفراد من خلال التقاضي المباشر، بينما يعتمد PDPL على نظام قضائي أكثر مركزية
حق الاستئناف القضائي	غير مفصل بشكل صريح في النص الرئيسي	منظم تفصيلياً في المادة 78	يتميز GDPR بتفصيل دقيق لحق الاستئناف، مما يُعزز الشفافية والمساءلة
فعالية الردع	لا تزال في مراحلها الأولى، يصعب تقييمها بعدُ	فعالة في ردع الانتهاكات، تجاوزت الغرامات 4 مليارات يورو بحلول 2025	تُظهر التجربة الأوروبية فعالية الردع المالي، بينما يحتاج PDPL إلى وقت لتقييم تأثيره الفعلي
الأثر السماعي	لم تتضح معالمه بعدُ	الغرامات الكبيرة تؤدي إلى خسائر سماعية تؤثر في ثقة العملاء والمستثمرين	يُعزز الإفصاح عن العقوبات دوافع الامتثال بما يتجاوز الجانب المالي

(المصدر: إعداد الباحث بالاعتماد على: الجربوع، 2024؛ إمام وآخرون، 2024؛ Frey & Presidente, 2024؛ Kumar & Singh, 2024).

يُلاحظ من الجدول (2.14) أن GDPR يتفوق في حجم الغرامات وتنوع مستوياتها، وفي تفصيل آليات التقاضي والاستئناف، بينما يتميز PDPL ببساطة هيكله في مرحلته الأولى، مما قد يُشكل ميزة في التطبيق المبكر، لكنه قد يُحد من فعالية الردع في المدى البعيد. ويُشير هذا

التباين إلى أن نظام PDPL بحاجة إلى تطوير تدريجي في هيكل الغرامات وآليات التقاضي لتعزيز فعالية الردع، مع الاستفادة من الدروس المستفادة من التجربة الأوروبية في تطبيق العقوبات وإدارة الحوادث.

في ضوء ما تقدم، يرى الباحث أن فعالية العقوبات لا تُقاس بحجمها المادي فحسب، بل بمدى سرعة تطبيقها وعدالتها وقدرتها على تحقيق الردع العام، كما أن نظام PDPL قد يستفيد من تجربة GDPR في تحسين آليات التنفيذ وتدريب الكوادر القضائية والرقابية، مع مراعاة خصوصية النظام القانوني السعودي. ويُشير التحليل إلى أن تبني نظام تصنيف هرمي للغرامات في المستقبل، إلى جانب تعزيز آليات التقاضي والاستئناف، قد يُعزز فعالية الردع ويُحقق توازناً بين حماية الحقوق وتحفيز الامتثال.

6. حوكمة الذكاء الاصطناعي في ظل التحول الرقمي السعودي

أطلقت المملكة العربية السعودية العديد من المبادرات الوطنية والسياسات الموجهة لتنظيم الذكاء الاصطناعي، أبرزها: الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي (التي أطلقتها الهيئة السعودية للبيانات والذكاء الاصطناعي - SDAIA - في عام 2020)، ودليل تنظيم الذكاء الاصطناعي المسؤول، وميثاق أخلاقيات الذكاء الاصطناعي، مما يُشكل منظومة متكاملة تهدف إلى جعل المملكة رائدة في مجال الذكاء الاصطناعي على المستوى الإقليمي والدولي (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2025).

ويتمثل التوفيق الاستراتيجي بين نظام PDPL واستراتيجيات التقنية في ضمان أن تكون حماية البيانات الشخصية الأساس الذي تقوم عليه تطبيقات الذكاء الاصطناعي المستدامة، مع تشجيع الابتكار من خلال بيئات اختبار تنظيمية (Sandbox) تسمح بتجربة تقنيات جديدة في ظل رقابة وإشراف (Albous et al., 2025). ويُعد هذا التوجه متسقاً مع أفضل الممارسات العالمية التي تدمج بين المرونة التنظيمية وحماية الحقوق الأساسية، مما يُعزز قدرة المملكة على جذب الاستثمارات التقنية مع الحفاظ على معايير الخصوصية والأمان.

وتؤدي الهيئة السعودية للبيانات والذكاء الاصطناعي دوراً محورياً في حوكمة الذكاء الاصطناعي من خلال وضع السياسات والمعايير، وإصدار التراخيص، وبناء القدرات الوطنية، وتعزيز التعاون الدولي، ومتابعة تنفيذ التشريعات، كما تتسق مع الجهات الحكومية والخاصة لضمان توافق الممارسات مع المتطلبات الوطنية والدولية (Ibrahim, 2024).

وتواجه المملكة تحديات في الامتثال في القطاعين الحكومي والخاص، منها نقص الكوادر المتخصصة في حماية البيانات والذكاء الاصطناعي، وصعوبة ترجمة المتطلبات التشريعية إلى ممارسات تقنية، وتعدد الجهات الرقابية أحياناً، وتباين مستويات النضج بين المؤسسات، مما يستدعي برامج تدريب مكثفة وتوعوية (الظفيري، 2025). كما أن التحول الرقمي السريع في المملكة يفرض ضغوطاً إضافية على المؤسسات لمواكبة التحديثات التشريعية المتلاحقة، مما يستلزم تطوير آليات مرنة للامتثال تتناسب مع سرعة التطور التقني.

ويسهم وجود تشريعات واضحة ك PDPL في جذب الاستثمارات التقنية العالمية إلى المملكة؛ إذ تُشير الدراسات إلى أن المستثمرين يفضلون البيئات ذات الإطار القانوني الواضح لحماية البيانات، مما يُعزز مكانة المملكة كوجهة رقمية رائدة في المنطقة ويُحفز الشركات العالمية على إنشاء مراكز بيانات وخدمات في المملكة (الغافري، 2026).

وتتمثل الرؤية المستقبلية في تطوير بيئة تشريعية محفزة للابتكار المستدام، من خلال مراجعة دورية للتشريعات لتواكب المستجدات التقنية، وتعزيز المرونة التنظيمية، وبناء شراكات دولية لنقل المعرفة والممارسات الفضلى، مع الاستفادة من التجارب العالمية ك GDPR في تطوير الأدوات والمنهجيات (العبيدان، 2024). ويُعد هذا التوجه ضرورياً لضمان استدامة التنافسية الرقمية للمملكة في ظل التسارع التقني العالمي، مع الحفاظ على القيم الوطنية والخصوصية الثقافية.

ويُلخص الجدول الآتي المبادرات الوطنية السعودية في حوكمة الذكاء الاصطناعي، مُبيناً أهداف كل مبادرة وأدواتها التنفيذية ومدى ارتباطها بنظام PDPL.

جدول (2.15): المبادرات الوطنية السعودية في حوكمة الذكاء الاصطناعي وارتباطها ب PDPL

المبادرة	الجهة المسؤولة	الأهداف الرئيسية	الأدوات التنفيذية	مدى الارتباط ب PDPL
الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي	SDAIA	جعل المملكة رائدة في الذكاء الاصطناعي، تعزيز الابتكار، بناء اقتصاد رقمي	وضع سياسات وطنية، إطلاق مبادرات تقنية، بناء القدرات	عالٍ: تُشكل حماية البيانات ركيزة أساسية للاستراتيجية
دليل تنظيم الذكاء الاصطناعي المسؤول	SDAIA	توفير إرشادات لتطوير واستخدام أنظمة الذكاء الاصطناعي بشكل مسؤول وأخلاقي	إصدار أدلة إرشادية، تدريب الكوادر، تعزيز الوعي	مرتفع: يُعزز الالتزام بمبادئ الخصوصية والشفافية المنصوص عليها في PDPL
ميثاق أخلاقيات الذكاء الاصطناعي	SDAIA	ترسيخ المبادئ الأخلاقية في تطبيقات الذكاء الاصطناعي، حماية حقوق الأفراد	اعتماد مبادئ أخلاقية، مراجعة المشاريع التقنية	مرتفع: يُحقق التوافق بين الأخلاقيات الرقمية ومتطلبات PDPL
بيئات الاختبار التنظيمية (Sandbox)	SDAIA	تشجيع الابتكار في الذكاء الاصطناعي مع ضمان الامتثال التنظيمي	توفير بيئات محمية للتجريب، رقابة مستمرة	متوسط: تسمح بتجربة تقنيات جديدة في ظل ضوابط حماية البيانات
منصة حوكمة البيانات الوطنية	SDAIA	تسهيل التزام المنشآت بمتطلبات PDPL واللوائح المرتبطة	توفير أدلة وشروحات، حملات توعوية، أدوات امتثال	عالٍ جداً: أداة تنفيذية مباشرة لدعم الامتثال لـ PDPL

(المصدر: إعداد الباحث بالاعتماد على الهيئة السعودية للبيانات والذكاء الاصطناعي، 2025؛ Albous et al., 2025؛ Ibrahim, 2024؛ الظفيري، 2025).

يُظهر الجدول (2.15) تنوع المبادرات الوطنية السعودية في حوكمة الذكاء الاصطناعي وارتباطها الوثيق بنظام PDPL، حيث تُشكل حماية البيانات الشخصية محوراً مشتركاً في معظم هذه المبادرات. ويُلاحظ أن المملكة تبنت نهجاً تدريجياً في بناء منظومتها التشريعية والتنظيمية، بدءاً من الاستراتيجيات الوطنية وصولاً إلى الأدوات التنفيذية الملموسة كمنصة حوكمة البيانات الوطنية، مما يُعزز جاهزية السوق السعودي للتفاعل مع الأسواق العالمية، مع الحفاظ على

الخصوصية الثقافية والدينية للمملكة. ويُشير هذا النهج إلى إدراك المملكة لأهمية التكامل بين السياسات والأدوات لضمان فعالية الحوكمة، وهو ما يُعد نموذجاً يُحتذى به في المنطقة.

يتضح مما سبق، أن المملكة تسير بخطى متسارعة نحو بناء منظومة حوكمة رقمية متكاملة، لكن نجاح هذه المنظومة يتوقف على قدرتها على مواكبة التطورات التقنية المتسارعة، وتطوير الكوادر البشرية، وتعزيز التعاون بين القطاعين العام والخاص، وبناء ثقافة امتثال راسخة على جميع المستويات، مع الاستفادة من الدروس المستفادة من التجارب الدولية الرائدة، خاصة في مجال تطبيق العقوبات وإدارة الحوادث. ويُشير التحليل إلى أن الاستثمار في بناء القدرات الوطنية وتطوير الأدوات التقنية الداعمة للامتثال يُعد عاملاً حاسماً في تحقيق التوازن بين الابتكار وحماية الحقوق، مما يُعزز مكانة المملكة كمركز إقليمي للتقنيات الناشئة.

7. تحليل الفجوات والدروس المستفادة من التجربة الأوروبية

أسهمت لائحة GDPR في تطور تقنيات الخصوصية (Privacy-Enhancing Technologies) عالمياً، إذ حفزت الشركات على ابتكار حلول كالتشفير المتجانس (Homomorphic Encryption) الذي يسمح بإجراء عمليات حسابية على بيانات مشفرة دون فك تشفيرها، والخصوصية التفاضلية (Differential Privacy) التي تُضيف تشويشاً مضبوطاً إلى نتائج الاستعلامات لضمان عدم إمكانية استنتاج معلومات فردية، والتعلم الفيدرالي (Federated Learning) الذي يُدرب النماذج محلياً على أجهزة المستخدمين دون نقل البيانات المركزية، مما جعل أوروبا رائدة في مجال حماية البيانات وأحدث نقلة نوعية في الوعي المجتمعي بحقوق الخصوصية (Oh et al., 2025).

وتُعد الدروس المستفادة في تطبيق مبادئ الخصوصية بالتصميم (Privacy by Design) من أبرز إسهامات التجربة الأوروبية، حيث أثبتت أن دمج الخصوصية في دورة حياة تطوير البرمجيات منذ البداية أكثر فعالية من إضافتها بعد النشر، مما يُقلل التكاليف ويُعزز الامتثال، كما يُسهم في بناء ثقة المستخدمين في الأنظمة الرقمية (Chhetri et al., 2024). وقد تجلت هذه الفعالية في تقليل عدد الحوادث الأمنية المرتبطة بالخصوصية في المؤسسات التي طبقت المبادئ منذ مراحل التصميم الأولى، مقارنة بتلك التي أضافت الحماية كطبقة لاحقة.

وجدير بالذكر، أن الشركات واجهت تحديات عملية في الامتثال المزدوج (أي الامتثال لـ GDPR وقوانين دول أخرى ك PDPL)، وتضمنت هذه التحديات:

- تكاليف الامتثال المرتفعة (خاصة للمؤسسات الصغيرة والمتوسطة التي قد تفتقر إلى الموارد القانونية والتقنية اللازمة).
- تعقيد إدارة الموافقات عبر ولايات قضائية مختلفة ذات متطلبات متباينة (حيث تختلف شروط الموافقة الصريحة وآليات سحبها بين GDPR و PDPL).
- صعوبة تطبيق قواعد نقل البيانات العابرة للحدود بشكل عملي بسبب تعارض بعض التشريعات الوطنية مع متطلبات النقل.

وبهذا الشأن، أشارت دراسة (Ahmad, 2025) إلى أن اللائحة العامة لحماية البيانات (GDPR) أعادت تشكيل مشهد حماية البيانات للشركات متعددة الجنسيات، وأن القيود الصارمة على نقل البيانات خارج المنطقة الاقتصادية الأوروبية تُشكل تحديات عملية كبيرة لهذه الشركات، خاصة في ضوء تداعيات حكم Schrems II الذي أوجب على الشركات تقييم مستوى الحماية في الدولة المتفنية على أساس كل حالة على حدة، واتخاذ تدابير إضافية لضمان الامتثال. كما أشارت دراسة (Kumar & Singh, 2024) إلى أن تعارض القوانين الوطنية مع الالتزامات الدولية المتعلقة بحماية البيانات يُعقد عمليات النقل العابر للحدود، ويُصعب تحديد القانون الواجب التطبيق في حال وقوع انتهاكات سيبرانية عابرة للحدود.

وبشكل عام، أسفرت هذه التحديات عن ظهور مفهوم "الامتثال المتقطع" الذي يُشير إلى صعوبة تحقيق امتثال كامل في جميع السياقات، حيث قد تلتزم المؤسسة بمتطلبات ولاية قضائية معينة بينما تعجز عن تلبية متطلبات أخرى (Kumar & Singh, 2024). وبهذا الصدد، أشارت دراسة (Ahmad, 2025) إلى أن المؤسسات العاملة في أكثر من ولاية قضائية تواجه صعوبات مضاعفة في تنسيق سياسات الخصوصية وتحديثها باستمرار، نتيجة غياب إطار حوكمة عالمي موحد للبيانات، مما يؤدي إلى مشهد تنظيمي مجزأ (fragmented regulatory landscape) يزيد من المخاطر القانونية والتشغيلية، ويستدعي حلولاً تقنية متقدمة لإدارة هذا التعقيد. وقد أشارت

دراسة (Freshfields, 2026) إلى أن غياب التوافق العالمي يُشكل "رقعة من الالتزامات" (patchwork of obligations) تزيد من المخاطر القانونية وتُعقد استخدام البيانات عبر الحدود.

ومن ناحية أخرى، تُتيح النماذج الأوروبية فرصاً للاستفادة منها في تطوير اللوائح السعودية، خاصة في مجالات: توحيد إجراءات تقييم الأثر (DPIA) لتكون أكثر كفاءة وقابلية للتطبيق، وتطوير أدوات التدقيق التقني المستمر، وبناء قدرات الهيئات الرقابية من خلال برامج تدريبية متخصصة، وتطوير آليات التظلم الفعالة التي تضمن حقوق الأفراد في الطعن على القرارات الرقابية، والاستفادة من الخبرة الأوروبية في تطبيق الغرامات وتحديد معايير تقديرها (محمد، 2022).

ويُعد التنبؤ بالاحتياجات التنظيمية المستقبلية بناءً على الممارسات الفضلى أمراً بالغ الأهمية، ومن المتوقع أن تركز التشريعات القادمة على: حوكمة الذكاء الاصطناعي التوليدي (Generative AI) لما يفرضه من تحديات جديدة في مجال الملكية الفكرية والتحيز الخوارزمي، والشفافية الخوارزمية (Algorithmic Transparency) لضمان فهم القرارات الآلية، وحماية البيانات في الحوسبة الكمية (Quantum Computing) التي قد تُحدث ثورة في التشفير وتعرض تحديات أمنية جديدة، والرقابة على الأنظمة المستقلة (Autonomous Systems) التي تتخذ قرارات دون تدخل بشري، مما يستدعي استعداداً استباقياً من المشرعين والجهات التنظيمية (Hohmann & Kollár, 2025).

وجدير بالذكر، أن المملكة تعمل على تطوير أدوات امتثال وطنية تتوافق مع المعايير الدولية، كمنصة الامتثال الرقمية التي تقدمها الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) لتسهيل التزام المنشآت بمتطلبات PDPL واللوائح المرتبطة، مما يُعزز جاهزية السوق السعودي للتفاعل مع الأسواق العالمية ويُقلل من تكاليف الامتثال (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2025). وتُعد هذه المنصة خطوة مهمة نحو تحقيق التكامل بين الأطر التنظيمية والأدوات التقنية، مما يُساهم في رفع مستوى الوعي والالتزام بحماية البيانات في المملكة.

ويُلخص الجدول الآتي الفجوات التنظيمية والتقنية التي كشفت عنها التجربة الأوروبية، والدروس المستفادة التي يمكن تطبيقها في تطوير نظام PDPL.

جدول (2.16): تحليل الفجوات والدروس المستفادة من التجربة الأوروبية وتطبيقاتها على PDPL

الفجوة/التحدي في التجربة الأوروبية	الدروس المستفادة	التطبيق المقترح على PDPL
تكاليف الامتثال المرتفعة، خاصة للمؤسسات الصغيرة والمتوسطة	ضرورة توفير أدوات امتثال مبسطة ومنخفضة التكلفة	تطوير أدوات امتثال وطنية ميسرة، وتقديم إرشادات مبسطة للمؤسسات الصغيرة والمتوسطة، وإنشاء برامج دعم فني
تعقيد إدارة الموافقات عبر ولايات قضائية مختلفة	أهمية توحيد آليات الموافقة وجعلها قابلة للتشغيل البيني (Interoperability)	اعتماد معايير موحدة للموافقات في PDPL، مع مرونة للتكيف مع المتطلبات الدولية، وتطوير واجهات برمجية موحدة
صعوبة تطبيق قواعد نقل البيانات العابرة للحدود	الحاجة إلى آليات نقل مرنة وواضحة، مع الاعتراف المتبادل بالضمانات	تطوير آليات نقل بيانات واضحة في PDPL، مع الاعتراف المتبادل بالشهادات والضمانات، وتبني آليات النقل القياسية كـ SCCs و BCR
غياب الوضوح في متطلبات الشفافية الخوارزمية	ضرورة وضع معايير واضحة لقابلية التفسير (Explainability)، والشفافية	تضمين متطلبات الشفافية الخوارزمية في اللوائح التنفيذية لـ PDPL، مع اعتماد معايير مثل ISO 24029 كمرجع
ضعف آليات التظلم والظعن في بعض الدول الأعضاء	أهمية توفير آليات تظلم فعالة وسريعة، مع ضمان الاستقلالية	تعزيز آليات التظلم والظعن في PDPL، مع ضمان استقلالية الهيئة الرقابية، وتوفير قنوات اتصال مباشرة للمتضررين
التحديث القانوني البطيء لمواكبة التقنيات الناشئة	ضرورة اعتماد نهج تنظيمي مرن وقائم على المبادئ (Principles-based)	اعتماد لغة مبدئية في PDPL تسمح بتفسير ديناميكي، مع تحديث دوري للوائح التنفيذية، وإنشاء آليات للتشاور المستمر مع الخبراء التقنيين

(المصدر: إعداد الباحث بالاعتماد على: Chhetri et al., 2024; Hohmann & Kollár, 2025; محمد، 2022).

يُظهر الجدول (2.16) أن التجربة الأوروبية كشفت عن فجوات تنظيمية وتقنية متعددة، وقدمت دروساً مستفادة يمكن تطبيقها في تطوير نظام PDPL. ويلاحظ أن معظم هذه الفجوات تتعلق بتكاليف الامتثال، وتعقيد إدارة الموافقات، وصعوبة نقل البيانات، وضعف الشفافية

الخوارزمية، وآليات التظلم، وبطء التحديث القانوني. وتُشير هذه الدروس إلى أن نظام PDPL بحاجة إلى تبني نهج تنظيمي مرّن وقائم على المبادئ، مع تطوير أدوات امتثال ميسرة، وتعزيز آليات التظلم والطعن، وضمان مرونة كافية لاستيعاب التقنيات الناشئة، مع الاستفادة من الخبرات الدولية في تصميم وتنفيذ هذه الآليات.

وفي هذا السياق، يرى الباحث أن التجربة الأوروبية تُقدم نموذجاً غنياً بالدروس للمملكة، خاصة في مجالات التطبيق العملي، وإدارة الحوادث، وتطبيق العقوبات، لكن ينبغي على المملكة ألاّ تتبنى النموذج الأوروبي بحذافيره، بل تطويره بما يتناسب مع سياقها الثقافي والديني والاقتصادي، مع الاستفادة من المرونة التي يتيحها كون نظامها في مرحلة التطوير الأولى لتجنب بعض الأخطاء التي وقعت فيها التجربة الأوروبية، كالجُمود التنظيمي الناتج عن التفسيرات المتضاربة لبعض المواد، وصعوبة التكيف مع التقنيات الناشئة بسبب بطء إجراءات التعديل التشريعي. ويُشير التحليل إلى أن الاستفادة المثلى من التجربة الأوروبية تتطلب تبني نهج انتقائي يدمج بين الممارسات الفضلى الأوروبية والخصوصيات الوطنية، مع الاستثمار في بناء القدرات المحلية وتطوير أدوات امتثال مرنة تتناسب مع حجم السوق السعودي واحتياجاته.

8. التوجهات المستقبلية والاندماج بين الابتكار والامتثال

تُشير التوجهات المستقبلية إلى ضرورة هندسة خوارزميات مرنة قادرة على الامتثال المزدوج لكل من PDPL وGDPR، وذلك عبر تصميم أنظمة تتعرف على الإطار التشريعي المُطبق استناداً إلى موقع المستخدم أو سياق المعالجة، وتُطبق الضوابط المناسبة تلقائياً، مما يُقلل من الأخطاء البشرية ويُعزز كفاءة الامتثال (Holtz & Ledendal, 2026).

ويُمكن توظيف الذكاء الاصطناعي نفسه في أتمتة ومراقبة عمليات الامتثال، من خلال أدوات تحليل النصوص التشريعية لاستخراج المتطلبات الآلية، وأنظمة الكشف الآلي عن المخالفات التي تراقب سلوك الأنظمة في الوقت الفعلي، ومنصات إدارة الموافقات الذكية التي تتبع موافقات المستخدمين وتحديثاتها، مما يُقلل العبء البشري ويُعزز الدقة والكفاءة، كما يُتيح للمؤسسات الاستجابة السريعة للتغيرات التنظيمية (Lorè et al., 2023).

وبهذا الشأن، أثبتت الدراسات الحديثة، مثل: دراسة (McKinsey & Company, 2024) التي وثقت تجربة Blackstone في تحويل عملياتها القانونية والامتثالية باستخدام الذكاء الاصطناعي، حيث أسهمت الأتمتة المدعومة بالذكاء الاصطناعي في تحقيق زيادة في إنتاجية المراجعين بنسبة تجاوزت (30%)، مع توقعات بتحقيق وفورات تشغيلية سنوية تقدر بـ (5) ملايين دولار أمريكي بحلول عام 2027.

كما حلت دراسة (Compliance.ai, 2020) أثر استخدام حلول RegTech في (11) مؤسسة مالية، وأثبتت أن تبني أدوات الامتثال الآلية أسهم في خفض التكاليف التشغيلية للامتثال بنسبة تجاوزت (30%)، من خلال أتمتة عمليات رصد التغيرات التنظيمية وتحليلها؛ ودراسة (Deloitte, 2026) التي أشارت إلى أن المؤسسات الرائدة في توظيف الذكاء الاصطناعي التوليدي والوكيل في عمليات الامتثال أبلغت عن تحسن في زمن الدورات بنسبة (30-60%)، وانخفاض في الجهد المطلوب للامتثال بنسبة (20-40%)، مما يُشكل حافزاً قوياً للمؤسسات للاستثمار في هذه الحلول.

وتتمثل إحدى الفرص الرئيسية في تحويل المتطلبات التشريعية المتباينة إلى ضوابط برمجية موحدة قابلة للتخصيص (Configurable)، مما يسمح للمؤسسات العاملة دولياً بتطبيق سياسات خصوصية مرنة تتكيف مع كل ولاية قضائية من خلال ملفات تكوين مختلفة، دون الحاجة إلى إعادة هندسة الأنظمة بالكامل، وهذا يُقلل التكاليف ويسرع التكيف مع المتغيرات التنظيمية (Zhong et al., 2025).

ويُتيح التكامل الاستراتيجي لبناء أنظمة موحدة لإدارة الخصوصية (Unified Privacy Management Platforms) إمكانية توحيد إدارة الموافقات، وسجلات المعالجة، وتقييمات الأثر، وطلبات الأفراد، مما يُحسن الكفاءة ويُقلل التكاليف التشغيلية ويعزز الشفافية، كما يُسهم في بناء ثقة المستخدمين من خلال توفير رؤية شاملة لكيفية معالجة بياناتهم (Cheong, 2024). وتُعد هذه المنصات خطوة نحو تحقيق الامتثال الشامل الذي يغطي جميع جوانب حماية البيانات في المؤسسة، مما يُقلل من مخاطر الفجوات الأمنية والقانونية.

ويتطلب استشراف مستقبل التشريعات الرقمية ضمان استدامة الابتكار من خلال تصميم قوانين مرنة وقائمة على المبادئ، مع ترك مساحة للتجريب في بيئات محمية (Regulatory Sandboxes) تسمح باختبار تقنيات جديدة في ظل رقابة، وإشراك القطاع الخاص والأكاديميا في عمليات التطوير التشريعي لضمان أن تكون القوانين عملية وقابلة للتطبيق وتعكس الاحتياجات الفعلية للسوق (Taeihagh, 2025).

ويُعد بناء مجتمع رقمي يحقق التوازن بين حماية البيانات والتقدم التقني مسؤولية مشتركة بين الحكومات والقطاع الخاص والأفراد، وتقوم على تعزيز الوعي بحقوق الخصوصية، وتطوير المهارات الرقمية، وبناء الثقة في الأنظمة الرقمية من خلال الشفافية والمساءلة، مما يُشكل أساساً للاقتصاد الرقمي المستدام والمزدهر (Taylor et al., 2025). وقد أظهرت التجارب الدولية أن المجتمعات التي تستثمر في التوعية الرقمية وبناء المهارات تكون أكثر قدرة على التكيف مع المتغيرات التقنية وتحقيق التوازن بين الابتكار وحماية الحقوق؛ إذ تؤكد الدراسات الحديثة أن التثقيف في مجال المواطنة الرقمية يُعزز بشكل كبير الوعي بالخصوصية الرقمية والمشاركة الفاعلة في الفضاء الرقمي (Iskandar et al., 2025).

ويُلخص الجدول الآتي التوجهات المستقبلية للاندماج بين الابتكار والامتثال في سياق PDPL وGDPR، مُبيناً الأدوات التقنية والمتطلبات التنظيمية والتحديات المتوقعة.

جدول (2.17): التوجهات المستقبلية للاندماج بين الابتكار والامتثال في سياق PDPL وGDPR

التوجه المستقبلي	الأدوات التقنية المطلوبة	المتطلبات التنظيمية	التحديات المتوقعة
هندسة خوارزميات للامتثال المزدوج	أنظمة تعرف على الإطار التشريعي، ضوابط آلية قابلة للتخصيص، خوارزميات تحليل السياق	تشريعات مرنة تسمح بتطبيق ضوابط مختلفة حسب الولاية القضائية، مع الاعتراف بالحلول التقنية كوسائل امتثال معتمدة	تعقيد التصميم، صعوبة التحديث المستمر مع تغير التشريعات، الحاجة إلى توحيد المعايير التقنية بين الولايات القضائية
أتمتة الامتثال باستخدام الذكاء الاصطناعي	أدوات تحليل النصوص التشريعية (NLP)، أنظمة كشف المخالفات (Anomaly)	الاعتراف بالأدوات الآلية كوسيلة معتمدة للامتثال، وضع معايير دقة للأدوات الآلية	مخاطر الاعتماد المفرط على الأتمتة، الحاجة إلى رقابة بشرية، تحديات تفسير

القرارات الآلية في السياقات القانونية		(Detection)، منصات إدارة الموافقات الذكية	
صعوبة الترجمة الدقيقة للنصوص القانونية إلى قواعد برمجية، خطر التبسيط المفرط للمتطلبات القانونية المعقدة	توحيد المعايير التقنية، الاعتراف المتبادل بالشهادات والضمانات، وضع معايير للتحقق من صحة الترجمة	ملفات تكوين مرنة (Configuration Files)، وحدات برمجية قابلة للتبديل (Plugins)، أدوات ترجمة قانونية آلية	تحويل المتطلبات التشريعية إلى ضوابط برمجية موحدة
تكاليف التطوير المرتفعة، تحديات التكامل مع الأنظمة الحالية، الحاجة إلى تدريب الكوادر على استخدام المنصات	متطلبات تشغيل البيئي (Interoperability)، ضمان أمن البيانات، اعتماد معايير تبادل البيانات الموحدة	منصات متكاملة لإدارة الموافقات، السجلات، تقييمات الأثر، طلبات الأفراد، لوحات معلومات تحليلية	بناء أنظمة موحدة لإدارة الخصوصية
خطر الجمود التنظيمي (Regulatory Lag)، صعوبة الموازنة بين المرونة والحماية، تحديات التنسيق بين الجهات التشريعية المختلفة	إشراك القطاع الخاص والأكاديميا في التطوير التشريعي، اعتماد مبادئ تنظيمية مرنة	آليات للتقييم الدوري (Periodic Review)، بيانات اختبار تنظيمية (Regulatory Sandboxes)، منصات للتشاور مع الخبراء	تصميم تشريعات مرنة وقائمة على المبادئ

(المصدر: إعداد الباحث بالاعتماد على: (Holtz & Ledendal, 2026; Cheong, 2024; Taeihagh, 2025).

يُلاحظ من الجدول (2.17) أن التوجهات المستقبلية للاندماج بين الابتكار والامتثال تتطلب تكاملاً وثيقاً بين الأدوات التقنية والمتطلبات التنظيمية، مع توقعات بتحديات متعددة في التصميم والتحديث والتكامل والترجمة. ويُشير هذا التكامل إلى أن نجاح الامتثال المستقبلي يعتمد على قدرة المشرعين والتقنيين على العمل معاً لتطوير حلول مبتكرة تضمن حماية البيانات دون إعاقة الابتكار، مما يُحقق التوازن المنشود بين الأهداف التقنية والقانونية والاجتماعية. وتُعد الشراكات بين القطاعين العام والخاص، والاستثمار في البحث والتطوير، وبناء القدرات الوطنية، عوامل حاسمة في تحقيق هذا التوازن وضمان استدامة الامتثال في ظل التسارع التقني المتواصل.

وبصفة عامة، يرى الباحث أن مستقبل الامتثال يتجه نحو الأتمتة والذكاء، حيث ستلعب التقنيات الذكية دوراً محورياً في تسهيل الامتثال وتقليل التكاليف، لكن هذا التحول يتطلب استثماراً في البنى التحتية الرقمية والكوادر الماهرة، كما يستلزم تعاوناً وثيقاً بين المشرعين والتقنيين لضمان

أن تكون التشريعات قابلة للتنفيذ برمجياً، وأن تكون الأدوات التقنية متوافقة مع المتطلبات القانونية، مما يُحقق التكامل المنشود بين الابتكار والامتثال. ويُشير التحليل إلى أن بناء منصات امتثال ذكية وتعزيز التعاون بين القطاعين العام والخاص يُعدان ركيزتين أساسيتين لتحقيق هذا التكامل، مع ضرورة مواكبة التطورات التقنية المتسارعة من خلال آليات تنظيمية مرنة وتحديثات دورية للتشريعات.

9. نموذج مقترح للمؤسسات السعودية في إطار نظرية (STS)، ومنهجية (DSR).

اتساقاً مع منهجية "بحث علم التصميم" (DSR)، تعتمد الدراسة الحالية "إطاراً مزدوجاً" (Dual Framework)؛ **الأول** "تصوري" يفسر العلاقات (التشخيص)، **والثاني** "تطويري" يوجه بناء الحل (العلاج). وبناءً على التحليل المقارن المتقدم، يطرح الباحث إطاراً تطبيقياً مقترحاً للمؤسسات السعودية يتكون من ثلاثة مسارات رئيسية، هي:

- (1) مسار المواءمة الهندسية: الخصوصية بالتصميم والابتكار الأخضر.
- (2) مسار الحوكمة الإجرائية: إدارة الموافقات وسجلات المعالجة.
- (3) مسار التدقيق الخوارزمي: المستمر لمواجهة الانحراف الرقمي.

9.1 النموذج التصوري

يمثل هذا النموذج إسقاطاً لنظرية (STS)، حيث يوضح كيف يؤثر النظام الاجتماعي (الحوكمة) في النظام التقني (الذكاء الاصطناعي) لتحقيق المخرج النهائي (الامتثال).

جدول (2.18): متغيرات وأبعاد النموذج التصوري

تصنيف المتغير	المفهوم (Construct)	الأبعاد المقاسة (Dimensions)
المتغير المستقل (Independent)	إستراتيجيات الحوكمة الرقمية (النظام الاجتماعي/الإداري)	1. القيادة المؤسسية (Institutional Leadership). 2. الشفافية والمساءلة (Transparency & Accountability). 3. إدارة المخاطر (Risk Management).
المتغير الوسيط (Mediator)	الذكاء الاصطناعي المستدام (النظام التقني)	1. النزاهة والعدالة (Integrity & Fairness). 2. كفاءة البيانات (Data Efficiency - PETs). 3. التحقق التقني (Technical Validation).
المتغير التابع (Dependent)	الامتثال لحماية البيانات (المخرج/الهدف)	1. الامتثال لـ (GDPR Compliance). 2. الامتثال لـ (PDPL Compliance).

ديناميكية العلاقات في النموذج:

- المسار المباشر (H2): يفترض أن وجود حوكمة قوية يؤدي مباشرة لرفع مستوى الامتثال.
- المسار غير المباشر (- H1 الوسطة): يفترض أن الحوكمة وحدها لا تكفي، بل يجب أن "تتجسد" تقنياً في أنظمة ذكاء اصطناعي مستدامة (نزيفة وفعالة) لضمان الامتثال الفعلي وتقليل المخاطر.

9.2 النموذج التطويري والمنتج العلمي (Developmental Model & Artifact)

يصف هذا النموذج "دورة التصميم" (Design Cycle) الخاصة بمنهجية (DSR)، موضحاً كيف سيتم تحويل المدخلات النظرية إلى منتج عملي قابل للتطبيق.

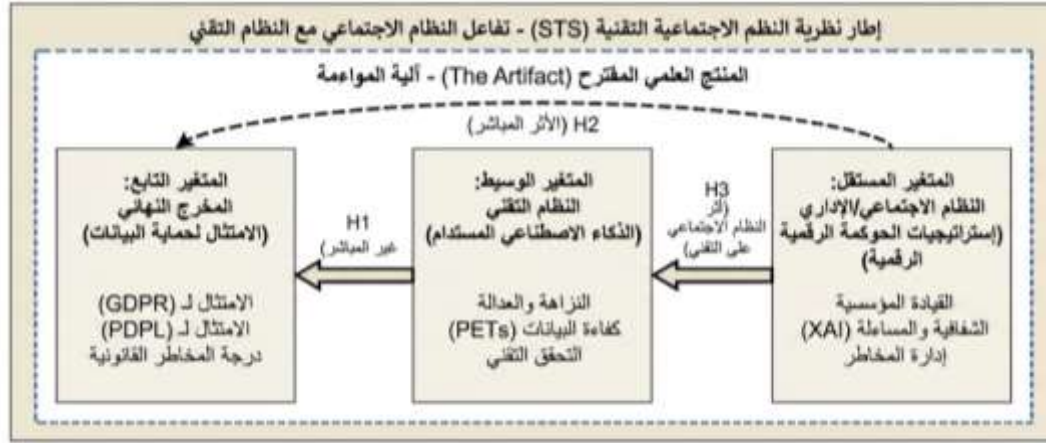
مصفوفة البناء التطويري:

المنتج العلمي (The Artifact)	العملية المنهجية (Process)	المرحلة (المدخلات)
الإطار الإستراتيجي المقترح للحوكمة الرقمية:	التحليل المقارن والهندسة العكسية:	المدخلات:
نموذج عملي (Framework) يهدف إلى سد الفجوة بين القانون والتطبيق، ويتضمن: 1. سياسات إدارية.	- تحليل نصوص (GDPR) و (PDPL) لاستخلاص الفجوات.	- نظرية النظم الاجتماعية التقنية (STS).
2. ضوابط تقنية.	- تحديد الضوابط التقنية (مثل XAI) التي تحقق الامتثال المزدوج.	- متغيرات الدراسة (الحوكمة + الذكاء المستدام).
3. قوائم تحقق للامتثال (Checklists).	(Hartman & Anders, 2025)	- التحديات الواقعية (فجوة التوتر).

آلية عمل النموذج التطويري:

1. مرحلة الفهم (Relevance): تبدأ بتحليل الفجوة بين المتطلبات القانونية والواقع التقني.
2. مرحلة البناء (Design): يتم فيها دمج "الضوابط التقنية" (مثل تقنيات تقليل البيانات) مع "الضوابط الإدارية" (مثل سياسات الخصوصية) في إطار موحد.
3. مرحلة التقييم (Evaluate): يتم اختبار هذا الإطار إحصائياً (عبر النموذج التصوري) للتأكد من قدرته على تحسين الامتثال في البيئة السعودية.

والشكل (2.7) الآتي يوضح تدفق العمليات من المدخلات إلى المخرجات، وتفاعل المتغيرات مع بعضها البعض. حيث يبرز العلاقة بين إستراتيجيات الحوكمة والذكاء الاصطناعي المستدام وتأثيرهما على الامتثال في ضوء نظرية النظم الاجتماعية التقنية (STS)، ومنهجية (DSR).



شكل (2.7): نموذج الدراسة المقترح (الإطار المزدوج: التصوري والتطويري).

يُبين الشكل (2.7) نموذج الدراسة المقترح في إطاره المزدوج (التصوري والتطويري)، حيث يوضح تفاعل النظام الاجتماعي (إستراتيجيات الحوكمة الرقمية) مع النظام التقني (الذكاء الاصطناعي المستدام) لتحقيق المخرج النهائي المتمثل في الامتثال لحماية البيانات الشخصية.

خاتمة الإطار النظري للدراسة

يُشكل الإطار النظري المتكامل للمحاور الأربعة البنية المعرفية التي تقوم عليها الدراسة، حيث انطلق من استعراض الأسس التقنية والفلسفية للذكاء الاصطناعي المستدام، متناولاً أبعاده الأخلاقية والاقتصادية وهندسته المعمارية، وصولاً إلى مفهوم الذكاء الاصطناعي الموثوق والقابل للتفسير. ثم انتقل إلى تحليل منظومة حماية البيانات الشخصية بأبعادها القانونية والتقنية والأمنية، مستعرضاً المبادئ الجوهرية للمعالجة، والحقوق الرقمية، ومنهجيات الخصوصية بالتصميم، وإدارة المخاطر والحوادث، قبل أن يربط ذلك بأطر الحوكمة الرقمية التي تضمن ترجمة المبادئ الأخلاقية والقانونية إلى ممارسات تنفيذية من خلال الامتثال التقني والرقابة الاستباقية والتكامل بين التشريعات والكود البرمجي.

واختتم بالتحليل المقارن بين نظامي PDPL وGDPR، الذي كشف نقاط التقاطع والاختلاف في المفاهيم والحقوق وآليات الامتثال وسياسات العقوبات، مع تقديم أطر تحليلية معمقة لتوافق المعايير الدولية وتحديات التكامل التشريعي التقني. وقد أظهر هذا الإطار أن فعالية الامتثال تتوقف على تكامل الأبعاد التقنية والقانونية والتنظيمية، وأن استدامة الأنظمة الذكية مرتبطة بقدرتها على تحقيق التوازن بين الابتكار وحماية الحقوق، مما يضع الأساس المنهجي للتحليل المقارن الذي تتبناه الدراسة للإجابة عن أسئلتها البحثية.

ثانياً: الدراسات السابقة

تمهيد

يُعرض في هذا القسم مراجعة منهجية للدراسات السابقة التي تناولت متغيرات الدراسة عبر أربعة محاور، وفقاً لتسلسلها في عنوان الدراسة، مرتبة من الأحدث إلى الأقدم ضمن كل محور. ويهدف هذا العرض إلى تحليل الأدبيات وتقييمها، لتحديد أوجه التشابه والاختلاف، والوصول إلى الفجوات البحثية التي تُشكل مبرراً للدراسة الحالية.

المحور الأول: الدراسات المرتبطة بالمتغير المستقل (الذكاء الاصطناعي المستدام)

1. دراسة (Taeihagh, 2025)، بعنوان: "Governance of Generative AI" (حوكمة الذكاء الاصطناعي التوليدي)، هدفت إلى وضع الأساس لفهم الذكاء الاصطناعي التوليدي وتسليط الضوء على مخاطره الرئيسية، كما هدفت إلى استكشاف التحديات التنظيمية والقانونية والاجتماعية لحوكمة الذكاء الاصطناعي التوليدي واقتراح إطار حوكمة شامل قائم على مناهج تكيفية وتشاركية واستباقية. واعتمدت الدراسة على منهجية تحليل السياسات المقارن والمراجعة المتعمقة للأدبيات، وشملت تحليل التحديات التي تفرضها هذه النماذج في سياقات متعددة تشمل حوكمة البيانات والملكية الفكرية وتحيز الخوارزميات وانتهاكات الخصوصية والمعلومات المضللة والاحتيال والآثار المجتمعية والاختلالات في توازن القوى. وتوصلت النتائج إلى أن النماذج التوليديّة تُحدث فجوات تنظيمية في مجالات تسرب المعلومات الحساسة والغموض (opacity)، وتحديات التحكم ومخاطر التصميم والتنفيذ، وأكدت الحاجة الملحة لتطوير مناهج مبتكرة وشاملة لضمان توافق تطوير الذكاء الاصطناعي التوليدي مع القيم المجتمعية، ودعت إلى تكييف قوانين حوكمة البيانات والملكية الفكرية واقتُرحت أطر تنظيمية جديدة تستفيد من أبحاث سلامة الذكاء الاصطناعي.

2. دراسة (فلاتة، 2025)، بعنوان: "حماية البيانات الشخصية في التطبيقات الإلكترونية والمنصات الرقمية في ضوء أحكام النظام السعودي والتشريعات المقارنة: نحو إطار قانوني أمثل لحماية بيانات المستهلك الإلكتروني"، هدفت إلى تقييم مدى فعالية الإطار التشريعي السعودي الجديد في تنظيم الممارسات الفعلية لجمع ومعالجة البيانات من قبل التطبيقات الإلكترونية والمنصات الرقمية، وتحديدًا فيما يتعلق بآليات الحصول على الموافقة واستخدام بيانات الموقع الجغرافي وتحديد المسؤوليات القانونية للمنصة، كما هدفت إلى تقديم إطار قانوني مقترح لتعزيز حماية بيانات المستهلك الإلكتروني بالاستفادة من التجربة الأوروبية. واعتمدت الدراسة على المنهج التحليلي المقارن، حيث خللت نصوص نظام حماية البيانات الشخصية السعودي ولائحته التنفيذية وقارنتها بالمبادئ الواردة في اللائحة الأوروبية، واتخذت من منصات "أمازون" و"مرسول" و"تويو" نماذج تطبيقية للدراسة. وأظهرت النتائج أن نظام حماية البيانات الشخصية السعودي يضع إطاراً عاماً متيناً، لكن هناك فجوة في القواعد التنظيمية التفصيلية التي تعالج خصوصية نماذج عمل المنصات الرقمية، خاصة فيما يتعلق بوضوح آليات الموافقة وحدود استخدام البيانات الشخصية، وقدمت الدراسة توصيات لتطوير المنظومة التشريعية شملت إصدار قواعد إرشادية لقطاعي التجارة الإلكترونية وخدمات التوصيل، وتبني معايير واضحة للموافقة الصريحة والواعية، وفرض التزامات تتعلق بالشفافية والخصوصية حسب التصميم.

3. دراسة (منور وبلعيد، 2025)، بعنوان: "التحديات القانونية لحماية البيانات الشخصية في سياق الذكاء الاصطناعي"، هدفت إلى استعراض التحديات القانونية التي يفرضها الذكاء الاصطناعي على حماية البيانات الشخصية وتحليل مدى قدرة الأنظمة القانونية الوطنية على مواكبة هذه التحديات، كما هدفت إلى تقديم توصيات لتطوير الأطر التشريعية لضمان حماية فعالة في بيئات الذكاء الاصطناعي. واعتمدت الدراسة على المنهج التحليلي المقارن، وشملت عينتها تشريعات حماية البيانات في كل من الجزائر والمغرب والاتحاد الأوروبي. وأظهرت النتائج وجود فجوة واضحة بين التشريعات الوطنية العربية والتشريعات الأوروبية من حيث التفصيل والمرونة، وأكدت أن عدم مواءمة التشريعات مع تطورات الذكاء الاصطناعي يُعرض حقوق الأفراد للخطر، وأن جهود المشتغلين على الجوانب الأخلاقية والقانونية لتقنيات الذكاء الاصطناعي اقتصرت على وضع جوانب أخلاقية ومبادئ قانونية عامة.

4. دراسة (فلاق، 2025)، بعنوان: "الخوارزميات، سوق البيانات الشخصية وانتهاك الخصوصية: الإشكالات الرقمية الجديدة في ظل نظم الذكاء الاصطناعي"، هدفت إلى تحليل العلاقة بين الخوارزميات وسوق البيانات الشخصية ورصد الإشكالات الرقمية الجديدة التي تُثيرها نظم الذكاء الاصطناعي فيما يتعلق بانتهاك الخصوصية، كما هدفت إلى تقديم تصور للحد من هذه الانتهاكات في ظل غياب تشريعات كافية. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها مجموعة من التطبيقات الخوارزمية التي تعتمد على البيانات الشخصية كمنصات التواصل الاجتماعي والتسويق الرقمي. وأكدت النتائج أن الخوارزميات تعمل كمحرك رئيسي لسوق البيانات الشخصية، وأن انعدام الشفافية في آلية عملها يُعزز مخاطر انتهاك الخصوصية، كما أوضحت أن المستخدمين غالباً ما يفتقرون إلى الوعي الكافي بكيفية معالجة بياناتهم.

5. دراسة (عبد، 2025)، بعنوان: "الضوابط القانونية للقرار الإداري الصادر عن الذكاء الاصطناعي: دراسة تحليلية في ضوء التشريع العراقي"، هدفت إلى تحديد الضوابط القانونية الواجب توافرها في القرارات الإدارية الصادرة عن أنظمة الذكاء الاصطناعي ودراسة مدى كفاية التشريع العراقي في تنظيم هذه القرارات، كما هدفت إلى المقارنة بين المواقف القانونية المختلفة تجاه مسؤولية القرارات الآلية. واعتمدت الدراسة على المنهج التحليلي للنصوص القانونية العراقية ذات الصلة والمنهج المقارن للاستفادة من التجارب الدولية الرائدة كتجربة الاتحاد الأوروبي في لائحة الذكاء الاصطناعي واللائحة العامة لحماية البيانات (GDPR). وأظهرت النتائج أن المنظومة التشريعية العراقية غير مهيأة للتعامل مع الطبيعة الخاصة للقرار الخوارزمي، مما يخلق حالة من عدم اليقين القانوني ويهدد مبادئ الشفافية والمساءلة والرقابة القضائية.

6. دراسة (طاهر، 2024)، بعنوان: "الحوكمة القانونية للذكاء الاصطناعي في مصر: التحديات والفرص"، هدفت إلى تحليل الإطار القانوني الحاكم للذكاء الاصطناعي في مصر ورصد التحديات التي تواجه تطبيقه في القطاعات المختلفة، كما هدفت إلى استشراف الفرص المتاحة لتطوير تشريعات وطنية متكاملة لحوكمة الذكاء الاصطناعي. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها مجموعة من القوانين واللوائح المصرية ذات الصلة بالإضافة إلى استعراض تجارب دولية رائدة. وأوضحت النتائج أن التشريعات المصرية لا تزال

في مراحلها الأولى فيما يتعلق بتنظيم الذكاء الاصطناعي، مما يُشكل فجوة تنظيمية في ظل الانتشار المتسارع لهذه التقنيات.

7. دراسة (السعيد، رنا، 2023)، بعنوان: "الذكاء الاصطناعي وتطبيقاته في مجال القضاء (دراسة مقارنة)"، هدفت إلى استعراض تطبيقات الذكاء الاصطناعي في الأنظمة القضائية وتحليل أثر هذه التقنيات في تحسين كفاءة الإجراءات القضائية وسرعة الفصل في المنازعات، كما هدفت إلى المقارنة بين تجارب الدول المتقدمة في توظيف الذكاء الاصطناعي في القضاء وإمكانية الاستفادة منها في السياق العربي مع التركيز على تجربة دولة الإمارات العربية كنموذج ناجح. واعتمدت الدراسة على المنهج الوصفي التحليلي والمقارن، وشملت عينتها مجموعة من التشريعات والتطبيقات العملية في دول كالإمارات والمملكة المتحدة والصين والعراق. وأكدت النتائج أن تطبيقات الذكاء الاصطناعي في القضاء تُسهم في تحسين كفاءة الأنظمة القضائية وزيادة الشفافية وتقليل التكاليف، لكنها أوضحت وجود تحديات تتعلق بالشفافية الخوارزمية وحقوق المتقاضين في الحصول على تفسيرات واضحة للقرارات الآلية، مما يستدعي تنظيمًا قانونيًا دقيقاً لضمان التغلب على هذه التحديات وحماية الخصوصية وتحقيق العدالة.

8. دراسة (Sætra, 2023)، بعنوان: "The AI ESG protocol: Evaluating and disclosing the environment, social, and governance implications of artificial intelligence capabilities, assets, and activities" (بروتوكول الذكاء الاصطناعي للبيئة والمجتمع والحوكمة: تقييم والإفصاح عن الآثار البيئية والاجتماعية والحوكومية لقدرات وأصول وأنشطة الذكاء الاصطناعي)، هدفت إلى تطوير بروتوكول لتقييم والإفصاح عن الآثار البيئية والاجتماعية والحوكومية للذكاء الاصطناعي وتقديم إطار منهجي لقياس هذه الآثار، كما هدفت إلى اختبار البروتوكول المقترح على مجموعة من تطبيقات الذكاء الاصطناعي في قطاعات متنوعة. واعتمدت الدراسة على المنهج التطويري مع تطبيق البروتوكول على عينة من أنظمة الذكاء الاصطناعي في قطاعات الطاقة والنقل والخدمات المالية. وأظهرت النتائج أن البروتوكول يُمكن المؤسسات من تحديد المخاطر البيئية والاجتماعية المرتبطة بالذكاء الاصطناعي، كما أوضحت أن الإفصاح الشفاف عن هذه الآثار يُعزز ثقة المستثمرين ويُسهم في تحقيق أهداف التنمية المستدامة.

9. دراسة (Arrieta et al., 2020)، بعنوان: "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI" (الذكاء الاصطناعي القابل للتفسير: المفاهيم والتصنيفات والفرص والتحديات نحو ذكاء اصطناعي مسؤول)، هدفت إلى تقديم تصنيف شامل لمفاهيم الذكاء الاصطناعي القابل للتفسير (XAI)، ومراجعة المنهجيات والأدوات المستخدمة في تحقيق التفسيرية في النماذج المعقدة، كما هدفت إلى تحليل الفرص والتحديات التي تواجه تطبيق XAI في سياقات مختلفة. واعتمدت الدراسة على مراجعة منهجية للأدبيات العلمية من عام 2015 إلى 2020 وشملت عينتها أكثر من 200 بحث ومقال علمي في مجال التفسيرية. وأكدت النتائج على وجود عدة تصنيفات للتفسيرية (محلية مقابل عالمية، ومحددة بالنموذج مقابل مستقلة عنه)، وأشارت إلى أن التحديات الرئيسية تتمثل في التوازن بين الأداء وقابلية التفسير وعدم وجود معايير موحدة لتقييم جودة التفسيرات وضعف فهم المطورين لاحتياجات المستخدمين من التفسيرات.

10. دراسة (Sharma et al., 2020)، بعنوان: "Artificial intelligence and effective governance: A review, critique and research agenda" (الذكاء الاصطناعي والحوكمة الفعالة: مراجعة ونقد وأجندة بحثية)، هدفت إلى مراجعة الأدبيات المتعلقة بالذكاء الاصطناعي والحوكمة الفعالة ونقد الاتجاهات السائدة في هذا المجال، كما هدفت إلى اقتراح أجندة بحثية مستقبلية تركز على العلاقة بين الذكاء الاصطناعي وجودة الحوكمة. واعتمدت الدراسة على مراجعة منهجية للأدبيات شملت 74 دراسة منشورة في قاعدتي Web of Science و Scopus. وأكدت النتائج أن الذكاء الاصطناعي يُحدث تحولاً في ممارسات الحوكمة عبر تحسين كفاءة اتخاذ القرار وتقليل التحيز البشري، لكنها أشارت إلى وجود تحديات تتعلق بالمساءلة والشفافية وعدم المساواة في الوصول إلى التقنيات.

المحور الثاني: الدراسات المرتبطة بالمتغير التابع (حماية البيانات الشخصية)

1. دراسة (Oh et al., 2025)، بعنوان: "PETLP: A Privacy-by-Design Pipeline for Social Media Data in AI Research"، خط أنابيب للخصوصية بالتصميم لبيانات وسائل التواصل الاجتماعي في أبحاث الذكاء الاصطناعي)، هدفت إلى تقديم إطار امتثال يدمج الضمانات القانونية مباشرة في خطوط أنابيب معالجة البيانات، ومعالجة التداخلات التنظيمية بين اللائحة العامة لحماية البيانات وقانون حقوق النشر، كما هدفت إلى توفير دليل عملي للباحثين للوصول إلى بيانات وسائل التواصل الاجتماعي ومعالجتها وعرضها بشكل مسؤول مع الوفاء بالالتزامات القانونية طوال مسار البيانات. واعتمدت الدراسة على منهج تصميم إطار امتثال يدمج الضمانات القانونية مباشرة في خطوط أنابيب ETL الموسعة، مع معاملة تقييمات أثر حماية البيانات كوثائق حية تتطور من مرحلة ما قبل التسجيل حتى النشر. وأظهرت النتائج أن إطار PETLP يُعالج السؤال الأساسي حول كيفية وصول الباحثين إلى بيانات وسائل التواصل الاجتماعي والنماذج المشتقة منها بشكل مسؤول مع الوفاء بالالتزامات القانونية طوال مسار البيانات، كما أوضحت النتائج أن دمج الضمانات القانونية في خطوط أنابيب معالجة البيانات يُعزز الامتثال ويُقلل من المخاطر القانونية للباحثين.

2. دراسة (الجربوع، 2024)، بعنوان: "المسؤولية الجزائية لانتهاك حقوق البيانات الشخصية الرقمية في النظام السعودي: دراسة تحليلية مقارنة"، هدفت إلى تحديد الأفعال التي تُشكل انتهاكات للبيانات الشخصية الرقمية في النظام السعودي وتحليل المسؤولية الجزائية المترتبة عليها، كما هدفت إلى المقارنة بين النظام السعودي وبعض الأنظمة المقارنة في مجال المسؤولية الجزائية. واعتمدت الدراسة على المنهج التحليلي المقارن، وشملت عينتها نصوص النظام السعودي واللائحة العامة الأوروبية لحماية البيانات وبعض التشريعات العربية. وأكدت النتائج أن النظام السعودي يقر المسؤولية الجزائية عن انتهاكات البيانات الشخصية، بما في ذلك الغرامات المالية والعقوبات السالبة للحرية، لكنها أوضحت أن النصوص العقابية تحتاج إلى مزيد من التفصيل لتحديد نطاق الأفعال المجرمة بدقة، كما دعت الدراسة إلى توضيح الأحكام الجزائية في اللوائح التنفيذية وتدريب القضاة والمحققين على قضايا البيانات الشخصية.

3. دراسة (رجب، 2024)، بعنوان: "الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية"، هدفت إلى تحليل الإطار القانوني لحماية البيانات الشخصية في ضوء التطورات التكنولوجية الرقمية واستعراض التحديات التي تفرضها هذه التطورات على فعالية الحماية، كما هدفت إلى صياغة توصيات لتطوير التشريعات الوطنية لتواكب التحديات الرقمية. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها مجموعة من القوانين العربية والأجنبية لحماية البيانات، بالإضافة إلى الأدبيات القانونية ذات الصلة. وأكدت النتائج أن التكنولوجيا الرقمية تفرض تحديات متزايدة على حماية البيانات الشخصية، خاصة مع ظهور تقنيات كالذكاء الاصطناعي والبيانات الضخمة، كما أشارت النتائج إلى أن التشريعات الوطنية لا تزال في مراحلها الأولى مقارنة بالتشريعات الأوروبية، ودعت إلى تحديث التشريعات الوطنية بشكل دوري لمواكبة التطورات التقنية وتعزيز التعاون الدولي في مجال حماية البيانات.

4. دراسة (السعودي، 2024)، بعنوان: "الحماية النظامية للخصوصية المعلوماتية: دراسة تأصيلية تحليلية"، هدفت إلى تأصيل مفهوم الخصوصية المعلوماتية في النظام السعودي وتحليل آليات الحماية النظامية المقررة لهذا الحق، كما هدفت إلى رصد الثغرات الإجرائية التي قد تُعيق فعالية هذه الحماية. واعتمدت الدراسة على المنهج التأصيلي التحليلي، مع مراجعة النصوص النظامية والفتاوى القضائية ذات الصلة، وشملت العينة مجموعة من الأنظمة واللوائح السعودية المتعلقة بالخصوصية المعلوماتية. وأظهرت النتائج أن الحماية النظامية للخصوصية المعلوماتية في السعودية تشهد تطوراً ملحوظاً خاصة بعد صدور نظام حماية البيانات الشخصية، لكنها أشارت إلى وجود حاجة إلى مزيد من التفصيل في اللوائح التنفيذية وإلى تحسين آليات التظلم والرقابة، وأوصت الدراسة بإصدار أدلة إرشادية لتوضيح كيفية تطبيق النظام وتعزيز استقلالية الهيئات الرقابية.

5. دراسة (Chhetri et al., 2024)، بعنوان: "GDPR consent management and automated compliance verification tool" (أداة إدارة الموافقات والتحقق الآلي من الامتثال لللائحة العامة لحماية البيانات)، هدفت إلى تطوير أداة قابلة للتطوير والتشغيل البيني لإدارة الموافقات والتحقق الآلي من الامتثال لمتطلبات اللائحة العامة لحماية البيانات، وتقييم فعالية الأداة في تسهيل عمليات الامتثال للمؤسسات، كما هدفت إلى تقديم حل تقني يُقلل من الأخطاء

البشرية في إدارة الموافقات. واعتمدت الدراسة على المنهج التطويري، مع اختبار الأداة في بيئة تشغيلية حقيقية على عينة من المؤسسات الأوروبية في سياقات المدن الذكية والتأمين. وأكدت النتائج أن الأداة تمكن المؤسسات من تتبع موافقات المستخدمين وإدارتها بكفاءة، كما أظهرت النتائج أن التحقق الآلي يُقلل من وقت وجهد الامتثال ويُحسن دقة السجلات، وأوصت الدراسة بتعميم استخدام الأدوات الآلية في إدارة الامتثال ودمجها في معمارية الأنظمة الحالية.

6. دراسة (الجندي، 2023)، بعنوان: "البيانات الشخصية بين التهديد والحماية: دراسة في ضوء أحكام القانون المصري رقم 151 لسنة 2020"، هدفت إلى استعراض التهديدات التي تواجه البيانات الشخصية في البيئة الرقمية وتحليل أحكام القانون المصري رقم 151 لسنة 2020 في مواجهة هذه التهديدات، كما هدفت إلى تقييم مدى كفاية القانون في تحقيق الحماية المأمولة. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها نصوص القانون المصري، بالإضافة إلى استعراض حالات عملية من الواقع المصري. وأظهرت النتائج أن القانون المصري يُعد نقلة نوعية في مجال حماية البيانات، إذ يتضمن مجموعة من الحقوق للأفراد والتزامات على المؤسسات، لكنها أوضحت أن التطبيق العملي يواجه تحديات تتعلق بضعف الوعي وقلة الكوادر المتخصصة وغياب آليات رقابية فعالة، وأوصت الدراسة بضرورة وضع لائحة تنفيذية للقانون وتدريب الكوادر القانونية والقضائية وتوعية الجمهور بحقوقهم في حماية بياناتهم.

7. دراسة (العجمي، 2023)، بعنوان: "الحق في خصوصية البيانات الشخصية وضمانات حمايتها في عصر التحول الرقمي: دراسة تحليلية في النظام السعودي"، هدفت إلى تحليل مضمون الحق في خصوصية البيانات الشخصية في النظام السعودي ورصد الضمانات القانونية المتاحة لحماية هذا الحق في ظل التحول الرقمي، كما هدفت إلى تقييم مدى كفاية هذه الضمانات في مواجهة التحديات الرقمية المعاصرة. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها نصوص النظام السعودي واللوائح التنفيذية ذات الصلة، بالإضافة إلى استعراض بعض التجارب المقارنة. وأكدت النتائج أن النظام السعودي يُقر الحق في خصوصية البيانات الشخصية صراحة ويوفر مجموعة من الضمانات القانونية، لكنها أشارت إلى أن التطبيق العملي لا يزال يواجه تحديات تتعلق بضعف الوعي المجتمعي وغياب آليات رقابية فعالة ونقص الكوادر

المتخصصة، وأوصت الدراسة بتعزيز آليات التوعية بحقوق الخصوصية وتدريب الكوادر القانونية والتقنية وتطوير إجراءات الرقابة والتدقيق.

8. دراسة (الجعافرة، 2022)، بعنوان: "قانون حماية البيانات الشخصية في الأردن"، هدفت إلى تحليل قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2021 واستعراض أبرز أحكامه ومبادئه، كما هدفت إلى تقييم مدى توافق هذا القانون مع المعايير الدولية لحماية البيانات. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها نصوص القانون الأردني والمواد المقابلة في اللائحة العامة الأوروبية لحماية البيانات. وأكدت النتائج أن القانون الأردني يُحقق تقدماً ملحوظاً في مجال حماية البيانات الشخصية، إذ يتضمن مبادئ أساسية كالمشروعية والشفافية وتقييد الغرض، لكنها أشارت إلى وجود ثغرات تتعلق بآليات الرقابة وتحديد مسؤوليات المعالجين وإجراءات نقل البيانات العابر للحدود، وأوصت الدراسة بإصدار اللوائح التنفيذية للقانون الأردني بشكل عاجل وتعزيز دور الهيئة الرقابية وتوعية المؤسسات والأفراد بأحكام القانون.

9. دراسة (Georgiadis & Poels, 2022)، بعنوان: "Towards a privacy impact assessment methodology to support the requirements of the General Data Protection Regulation in a big data analytics context: A systematic literature review" (نحو منهجية لتقييم أثر الخصوصية لدعم متطلبات اللائحة العامة لحماية البيانات في سياق تحليلات البيانات الضخمة: مراجعة منهجية للأدبيات)، هدفت إلى تطوير منهجية لتقييم أثر الخصوصية تدعم متطلبات اللائحة العامة لحماية البيانات في سياق تحليلات البيانات الضخمة وتقديم إطار عملي لتنفيذ هذه المنهجية، كما هدفت إلى اختبار المنهجية في سياق تحليلي حقيقي. واعتمدت الدراسة على المراجعة المنهجية للأدبيات مع التطوير العملي للمنهجية وتطبيقها في مشروع تحليلات بيانات ضخمة. وأظهرت النتائج أن منهجية تقييم أثر الخصوصية المقترحة تُمكن المؤسسات من تحديد وتقييم مخاطر الخصوصية في مشاريع البيانات الضخمة بشكل منهجي، كما أوضحت النتائج أن تطبيق المنهجية يُعزز الامتثال لللائحة العامة لحماية البيانات ويُقلل من مخاطر الغرامات، وأوصت الدراسة بتبني المنهجية كأداة قياسية في مشاريع البيانات الضخمة وتدريب الكوادر على استخدامها.

10. دراسة (Murdoch, 2021)، بعنوان: "Privacy and artificial intelligence:

Challenges for protecting health information in a new era" (الخصوصية والذكاء الاصطناعي: تحديات حماية المعلومات الصحية في عصر جديد)، هدفت إلى استعراض التحديات التي يفرضها الذكاء الاصطناعي على حماية المعلومات الصحية وتحليل المخاطر المرتبطة باستخدام تقنيات التعلم الآلي في معالجة البيانات الطبية، كما هدفت إلى تقديم إطار لحماية الخصوصية في نظم الرعاية الصحية المعتمدة على الذكاء الاصطناعي. واعتمدت الدراسة على مراجعة منهجية للأدبيات الطبية والقانونية، مع تحليل دراسات حالة من قطاع الرعاية الصحية. وأكدت النتائج أن الذكاء الاصطناعي يُوفر فرصاً هائلة لتحسين الرعاية الصحية، لكنه يُثير مخاطر خصوصية جديدة تتعلق بإعادة تحديد الهوية والتحيز الخوارزمي والوصول غير المصرح به إلى البيانات الحساسة، كما أشارت النتائج إلى أن الأطر القانونية الحالية قد لا تكون كافية لمواجهة هذه التحديات، وأوصت الدراسة بتطوير تشريعات خاصة بالبيانات الصحية في عصر الذكاء الاصطناعي واعتماد مبادئ الخصوصية بالتصميم في النظم الصحية وتعزيز الشفافية في استخدام الخوارزميات الطبية.

11. دراسة (أبو خمرة، 2021)، بعنوان: "حماية بيانات الأفراد الشخصية عبر شبكة الإنترنت:

دراسة مقارنة"، هدفت إلى تحليل آليات حماية البيانات الشخصية في البيئة الرقمية من منظور قانوني مقارنة بين الأردن ومصر والاتحاد الأوروبي، كما هدفت إلى تحديد نقاط القوة والضعف في التشريعات الوطنية مقارنة بالمعايير الدولية. واعتمدت الدراسة على المنهج الوصفي التحليلي والمقارن، مع الاستعانة بتحليل المحتوى للقوانين واللوائح الصادرة في الدول محل المقارنة حتى عام 2021، وشملت العينة نصوص القوانين واللوائح التنفيذية بالإضافة إلى آراء الفقهاء والمحاكم. وأظهرت النتائج أن التشريعات الوطنية العربية تعاني من نقص في التفصيل مقارنة باللائحة العامة الأوروبية، خاصة في مجالات تعريف البيانات الحساسة وحق نقل البيانات وقواعد الموافقة الصريحة وآليات الرقابة والعقوبات، كما كشفت النتائج عن وجود فجوات في التطبيق العملي وضعف في آليات التظلم وقلة الوعي المجتمعي بحقوق الخصوصية، وأوصت الدراسة بسن تشريعات شاملة ومحدثة وإنشاء هيئات رقابية مستقلة ذات صلاحيات فعالة وتعزيز التعاون الدولي وتنظيم حملات توعوية مكثفة.

المحور الثالث: الدراسات التي جمعت بين المتغيرين (الذكاء الاصطناعي المستدام وحماية البيانات الشخصية)

1. دراسة (الغافري، 2026)، بعنوان: "حماية البيانات الشخصية في ظل تطبيق الذكاء الاصطناعي في الأنظمة القضائية: مقارنة بين سلطنة عُمان والتشريعات الدولية"، هدفت إلى تحليل مدى كفاية الحماية القانونية للبيانات الشخصية في تطبيقات الذكاء الاصطناعي القضائية، وإجراء مقارنة بين سلطنة عُمان وبعض التشريعات الدولية في هذا الشأن، كما هدفت إلى تقديم تصور لتطوير الحماية في السياق العماني. واعتمدت الدراسة على المنهج المقارن، وشملت عينتها نصوص التشريعات العمانية، واللائحة العامة الأوروبية لحماية البيانات (GDPR)، وبعض التشريعات العربية والأجنبية، بالإضافة إلى تطبيقات عملية للذكاء الاصطناعي في القضاء. وأكدت النتائج أن تطبيقات الذكاء الاصطناعي في الأنظمة القضائية تثير تحديات خصوصية متعددة، وأن التشريعات الوطنية لا تزال بحاجة إلى تطوير لمواكبة هذه التحديات، كما أشارت النتائج إلى أن الشفافية الخوارزمية وحقوق المتقاضين في الاعتراض على القرارات الآلية تحتاج إلى تعزيز، وأوصت الدراسة بوضع ضوابط قانونية واضحة لاستخدام الذكاء الاصطناعي في القضاء وتعزيز آليات الرقابة على الخوارزميات القضائية وتدريب القضاة على التعامل مع مخرجات الذكاء الاصطناعي.

2. دراسة (Hohmann & Kollár, 2025)، بعنوان: "Reflections on the data protection compliance of AI systems under the EU AI Act" (تأملات حول الامتثال لحماية البيانات في أنظمة الذكاء الاصطناعي بموجب قانون الذكاء الاصطناعي الأوروبي)، هدفت إلى تحليل متطلبات الامتثال لحماية البيانات في أنظمة الذكاء الاصطناعي في ضوء قانون الذكاء الاصطناعي الأوروبي، وتقييم مدى توافق هذا القانون مع متطلبات اللائحة العامة لحماية البيانات، كما هدفت إلى تحديد التحديات العملية التي تواجه المؤسسات في تحقيق الامتثال المزدوج لكلا الإطارين. واعتمدت الدراسة على المنهج التحليلي المقارن، مع مراجعة نصوص القانونين والوثائق التفسيرية الصادرة عن الهيئات الأوروبية. وأكدت النتائج وجود تداخل كبير بين متطلبات قانون الذكاء الاصطناعي واللائحة العامة لحماية البيانات، خاصة فيما يتعلق بالشفافية والمساءلة وتقييم

المخاطر، لكنها أشارت إلى وجود اختلافات قد تُشكل تحديات تطبيقية للمؤسسات، كما أظهرت النتائج أن المؤسسات تحتاج إلى استراتيجيات امتثال متكاملة لتلبية متطلبات كلا الإطارين، وأوصت الدراسة بتطوير أدوات امتثال موحدة تغطي كلا القانونين وتعزيز التعاون بين الهيئات الرقابية وتوفير إرشادات واضحة للمؤسسات حول كيفية تحقيق الامتثال المزدوج.

3. دراسة (السعيد، وفاء، 2024)، بعنوان: "تقنية الذكاء الاصطناعي وحماية البيانات الشخصية: دراسة مقارنة"، هدفت إلى تحليل العلاقة بين تقنية الذكاء الاصطناعي وحماية البيانات الشخصية من منظور قانوني مقارن، وتقييم مدى توافق التشريعات العربية مع متطلبات حماية البيانات في عصر الذكاء الاصطناعي، كما هدفت إلى تقديم توصيات لتطوير الأطر التشريعية. واعتمدت الدراسة على المنهج المقارن، وشملت عينتها تشريعات كل من مصر والسعودية والإمارات والاتحاد الأوروبي. وأظهرت النتائج وجود تباين في درجة مواءمة التشريعات العربية لمتطلبات الذكاء الاصطناعي، حيث تفوق التشريعات السعودية والإماراتية في بعض الجوانب، بينما لا تزال التشريعات المصرية في مراحلها الأولى، كما أكدت النتائج أن الذكاء الاصطناعي يمكن أن يُستخدم كأداة لتعزيز حماية البيانات من خلال التشغيل الآلي لعمليات الامتثال، وأوصت الدراسة بتحديث التشريعات العربية بشكل دوري والاستفادة من التجربة الأوروبية في مواءمة قوانين حماية البيانات مع تقنيات الذكاء الاصطناعي.

4. دراسة (علي، أمل، 2024)، بعنوان: "توظيف تطبيقات الذكاء الاصطناعي لحماية خصوصية البيانات: دراسة حالة جمعية المكتبات الأمريكية"، هدفت إلى استعراض كيفية توظيف تطبيقات الذكاء الاصطناعي في حماية خصوصية البيانات، وتحليل حالة جمعية المكتبات الأمريكية كنموذج تطبيقي، كما هدفت إلى استخلاص الدروس المستفادة من هذه التجربة وتطبيقها في السياق العربي. واعتمدت الدراسة على منهج دراسة الحالة، مع تحليل وثائق وتقارير الجمعية والمقابلات مع المعنيين. وأكدت النتائج أن الذكاء الاصطناعي يُمكن أن يكون أداة فعالة لحماية الخصوصية عند تصميمه وتطبيقه بشكل صحيح، كما أظهرت النتائج أن دمج مبادئ الخصوصية بالتصميم في تطبيقات الذكاء الاصطناعي يُعزز ثقة المستخدمين ويُقلل من مخاطر الاختراق، وأوصت الدراسة بالاستفادة من تجربة جمعية المكتبات الأمريكية في تصميم تطبيقات ذكاء اصطناعي تراعي الخصوصية وبناء قدرات المؤسسات العربية في هذا المجال.

5. دراسة (Zaidan & Ibrahim, 2024)، بعنوان: "AI governance in a complex and rapidly changing regulatory landscape: A global perspective" (حوكمة الذكاء الاصطناعي في مشهد تنظيمي معقد وسريع التغير: منظور عالمي)، هدفت إلى تقديم تحليل مقارن لأطر حوكمة الذكاء الاصطناعي في ست دول/مناطق رئيسية (الاتحاد الأوروبي، الولايات المتحدة، الصين، المملكة المتحدة، كندا، سنغافورة)، كما هدفت إلى تحديد التحديات المشتركة والفرص للتعاون الدولي في هذا المجال. واعتمدت الدراسة على تحليل السياسات والنصوص التشريعية والتقارير الرسمية الصادرة عن الحكومات والمنظمات الدولية بين عامي 2019 و2024، بالإضافة إلى مقابلات مع 25 خبيراً في السياسات التقنية. وتوصلت النتائج إلى تباين كبير في المقاربات التنظيمية، حيث يتبنى الاتحاد الأوروبي نهجاً تشريعياً شاملاً قائماً على المخاطر، بينما تفضل الولايات المتحدة نهجاً قطاعياً غير ملزم، وتتبنى الصين نهجاً مركزياً صارماً، ورصدت الدراسة تحديات مشتركة كسرعة التطور التقني وعدم وضوح حدود المسؤولية وصعوبة تطبيق القوانين على الأنظمة العابرة للحدود وندرة الكوادر المتخصصة، وأوصت الدراسة بتعزيز التنسيق الدولي عبر المنظمات متعددة الأطراف وتبادل الممارسات الفضلى وتطوير معايير تقنية دولية وإنشاء آليات للاعتراف المتبادل بالشهادات والتراخيص.

6. دراسة (Novelli et al., 2024)، بعنوان: "Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity" (الذكاء الاصطناعي التوليدي في القانون الأوروبي: المسؤولية والخصوصية والملكية الفكرية والأمن السيبراني)، هدفت إلى تحليل الآثار القانونية للذكاء الاصطناعي التوليدي في القانون الأوروبي، مع التركيز على المسؤولية والخصوصية والملكية الفكرية والأمن السيبراني، كما هدفت إلى تحديد الفجوات التنظيمية في التعامل مع هذه النماذج واقتراح سبل معالجتها. واعتمدت الدراسة على المنهج التحليلي للنصوص القانونية، مع مراجعة الأدبيات والتقارير الصادرة عن المفوضية الأوروبية والبرلمان الأوروبي. وأظهرت النتائج أن النماذج التوليدية تُثير تحديات قانونية غير مسبقة في مجالات الخصوصية، خاصة فيما يتعلق بجمع البيانات الضخمة غير المرخصة وإعادة استخدامها، كما أشارت النتائج إلى أن قوانين الخصوصية الحالية قد لا تكون كافية للتعامل مع هذه النماذج، مما يستدعي تطوير

تشريعات خاصة، وأوصت الدراسة بتعديل تشريعات الخصوصية لتشمل النماذج التوليدية صراحة وفرض متطلبات شفافية محددة وتطوير آليات للرقابة والتدقيق المستمر على هذه النماذج.

7. دراسة (المحروقي، 2023)، بعنوان: "الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً: دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي (GDPR)، هدفت إلى تحليل الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء التشريعات الجنائية المقارنة واللائحة العامة الأوروبية، وتقييم مدى كفاية هذه الحماية في مواجهة تحديات الذكاء الاصطناعي، كما هدفت إلى تقديم توصيات لتطوير التشريعات الجنائية العربية. واعتمدت الدراسة على المنهج التحليلي المقارن، وشملت عينتها نصوص القوانين الجنائية في مصر والسعودية والإمارات، بالإضافة إلى أحكام اللائحة العامة الأوروبية. وأظهرت النتائج أن التشريعات الجنائية العربية تتفاوت في درجة حماية البيانات الشخصية المعالجة إلكترونياً، مع وجود نقص في التجريم الخاص بانتهاكات البيانات المرتبطة بالذكاء الاصطناعي، كما أشارت النتائج إلى ضرورة توسيع نطاق المسؤولية الجنائية لتشمل معالجي البيانات والمطورين، وأوصت الدراسة بتحديث التشريعات الجنائية لتشمل جرائم البيانات الرقمية بوضوح وتدريب الجهات القضائية على هذه الجرائم وتعزيز التعاون الدولي في مكافحة جرائم البيانات.

8. دراسة (الشمري، فهد، 2023)، بعنوان: "الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية"، هدفت إلى تحليل الإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية، ورصد مدى توافقه مع متطلبات استراتيجية الذكاء الاصطناعي الوطنية، كما هدفت إلى تقديم توصيات لتطوير هذا الإطار بما يدعم الابتكار ويضمن حماية الحقوق. واعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينتها نصوص نظام حماية البيانات الشخصية، والاستراتيجية الوطنية للبيانات والذكاء الاصطناعي، واللوائح ذات الصلة. وأظهرت النتائج أن الإطار القانوني السعودي يُوفر حماية متقدمة للبيانات الشخصية، لكنه يحتاج إلى مزيد من التكامل مع استراتيجيات الذكاء الاصطناعي لضمان الامتثال الفعال، كما أشارت النتائج إلى أهمية تطوير أدوات تنفيذية لسد الفجوة بين النصوص القانونية وممارسات التقنية، وأوصت الدراسة بتعزيز التنسيق بين الجهات التنظيمية والتقنية وتطوير معايير فنية لدعم الامتثال وبناء قدرات الكوادر البشرية في مجال حماية البيانات والذكاء الاصطناعي.

9. دراسة (Meszaros et al., 2022)، بعنوان: "The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union" (التنظيم المستقبلي لأنظمة الذكاء الاصطناعي في خدمات الرعاية الصحية والبحث الطبي في الاتحاد الأوروبي)، هدفت إلى استكشاف التنظيم المستقبلي لأنظمة الذكاء الاصطناعي في قطاع الرعاية الصحية والبحث الطبي في الاتحاد الأوروبي، وتحليل كيفية تفاعل متطلبات اللائحة العامة لحماية البيانات مع التشريعات الصحية الجديدة، كما هدفت إلى تحديد التحديات التي تواجه تطبيق الذكاء الاصطناعي في هذا القطاع الحساس. واعتمدت الدراسة على تحليل الأطر التنظيمية القائمة والمرتبقة في الاتحاد الأوروبي، بما في ذلك اللائحة العامة لحماية البيانات وقانون الذكاء الاصطناعي المقترح، مع التركيز على تطبيقات الرعاية الصحية. وأكدت النتائج أن قطاع الرعاية الصحية يشكل بيئة عالية المخاطر لتطبيقات الذكاء الاصطناعي، مما يستدعي تدابير حماية مشددة للبيانات الصحية الحساسة، كما أشارت النتائج إلى ضرورة تحقيق التوازن بين الابتكار في المجال الطبي وحماية خصوصية المرضى، وأوصت الدراسة بتطوير تشريعات صحية خاصة بالذكاء الاصطناعي تتوافق مع متطلبات الخصوصية، واعتماد مبادئ الشفافية والمساءلة في النظم الطبية الذكية، وتعزيز التعاون بين المطورين والأطباء والجهات التنظيمية.

10. دراسة (Kuner et al., 2021)، بعنوان: "The GDPR and data protection in the age of AI: Challenges and opportunities" (اللائحة العامة لحماية البيانات وحماية البيانات في عصر الذكاء الاصطناعي: التحديات والفرص)، هدفت إلى استعراض التحديات والفرص التي يُتيحها الذكاء الاصطناعي في مجال حماية البيانات في ضوء اللائحة العامة لحماية البيانات، وتحليل كيفية تأثير اللائحة على تطوير ونشر أنظمة الذكاء الاصطناعي، كما هدفت إلى تقديم توصيات للمؤسسات لتحقيق الامتثال المزدوج. واعتمدت الدراسة على المنهج التحليلي، مع مراجعة الأدبيات والتقارير الصادرة عن الهيئات الأوروبية والمؤسسات الدولية. وأكدت النتائج أن اللائحة العامة لحماية البيانات تُشكل تحدياً للمؤسسات العاملة في مجال الذكاء الاصطناعي، لكنها أيضاً تُتيح فرصة لبناء ثقة المستخدمين وتعزيز جودة الأنظمة، كما أظهرت النتائج أن مبادئ الخصوصية بالتصميم وتقييم الأثر هي أدوات فعالة لتحقيق التوازن بين الابتكار وحماية الحقوق، وأوصت الدراسة باعتماد نهج استباقي في الامتثال والاستثمار في أدوات تقنية لدعم الخصوصية وتعزيز التعاون بين الفرق القانونية والتقنية في المؤسسات.

المحور الرابع: الدراسات المرتبطة بالمقارنة بين (GDPR)، و(PDPL)

1. دراسة (الشمري، نجم، 2023)، بعنوان: "حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة"، هدفت إلى إجراء مقارنة تحليلية بين أنظمة حماية البيانات في السعودية (PDPL)، والاتحاد الأوروبي (GDPR)، والمملكة المتحدة (UK GDPR)، كما هدفت إلى استخلاص الدروس المستفادة من التجريبتين الأوروبية والبريطانية لتطوير النظام السعودي. واعتمدت الدراسة على منهج التحليل المقارن للنصوص القانونية، مع مراجعة الأدبيات والتقارير الصادرة عن الهيئات الرقابية في الدول الثلاث حتى عام 2023، وشملت العينة النصوص التشريعية الأساسية واللوائح التنفيذية والسياسات المكملية. وأكدت النتائج على وجود تقارب كبير بين الأنظمة الثلاثة في المبادئ العامة والحقوق الأساسية، لكنها رصدت اختلافات في شروط الموافقة، وقواعد نقل البيانات، وهيكل الغرامات، وآليات الرقابة، وأشارت الدراسة إلى أن النظام السعودي يستفيد من خبرة النظامين الأوروبي والبريطاني، لكنه لا يزال في مرحلة التطوير، خاصة فيما يتعلق باللوائح التنفيذية وآليات التنفيذ الفعالة، وأوصت الدراسة بتعزيز استقلالية الهيئة الرقابية السعودية وتطوير إجراءات تقييم الأثر وبناء قدرات الكوادر البشرية والاستفادة من الممارسات الفضلى في تدقيق الامتثال.

2. دراسة (محمد، ياسر، 2022)، بعنوان: "الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر معالجة بياناتهم ذات الطابع الشخصي: دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات"، هدفت إلى تحليل الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر معالجة بياناتهم ذات الطابع الشخصي في كل من نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية، وإجراء دراسة مقارنة منهجية بينهما لتحديد أوجه التشابه والاختلاف، كما هدفت إلى تقديم توصيات لتطوير النظام السعودي بالاستفادة من التجربة الأوروبية. واعتمدت الدراسة على المنهج الوصفي التحليلي المقارن، من خلال استقراء النصوص النظامية في النظامين وتحليلها ومقارنتها، مع الرجوع إلى آراء الفقهاء والقرارات الصادرة عن هيئات حماية البيانات. وأظهرت النتائج وجود تقارب كبير بين النظامين في المبادئ العامة للحماية والحقوق المقررة لأصحاب البيانات، لكنها رصدت فروقاً جوهرية في شروط الموافقة على

المعالجة، وقواعد نقل البيانات إلى الخارج، وهيكل الغرامات والعقوبات، وآليات الرقابة والتنفيذ، كما أشارت النتائج إلى أن النظام السعودي يستفيد من خبرة اللائحة الأوروبية مع مراعاة خصوصية البيئة السعودية، وأوصت الدراسة بضرورة إصدار اللوائح التنفيذية للنظام السعودي بشكل عاجل، وتدريب الكوادر الوطنية، وتعزيز دور الهيئة الرقابية، وبناء آليات فعالة للتعاون الدولي في مجال حماية البيانات.

3. دراسة (علي، محمد، 2021)، بعنوان: "النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة"، هدفت إلى تحليل النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة، وإجراء دراسة مقارنة بين اللائحة الأوروبية والقانون الفرنسي والقانون المصري وقانون مركز دبي المالي العالمي، كما هدفت إلى تحديد أوجه القصور في التشريعات الوطنية واقتراح سبل تطويرها. واعتمدت الدراسة على المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية في التشريعات محل المقارنة، مع الرجوع إلى اجتهادات الفقه والمحاكم ذات الصلة. وأظهرت النتائج أن اللائحة الأوروبية تمثل النموذج الأكثر تقدماً في مجال حماية البيانات الشخصية، حيث تتميز بشمولية الأحكام وتفصيل الحقوق وصرامة الضوابط، بينما تعاني التشريعات الوطنية من نقص في التفصيل وغياب آليات رقابية فعالة، كما أشارت النتائج إلى أن قانون مركز دبي المالي العالمي يُعد الأقرب إلى اللائحة الأوروبية بين التشريعات التي شملتها المقارنة، وأوصت الدراسة بضرورة تطوير التشريعات الوطنية في ضوء المعايير الدولية، مع مراعاة الخصوصية الثقافية والقانونية لكل دولة، وإنشاء هيئات رقابية مستقلة ذات صلاحيات فعالة.

4. دراسة (Kaminski & Malgieri, 2021)، بعنوان: "Algorithmic impact assessments under the GDPR: Producing multi-layered explanations" (تقييمات الأثر الخوارزمي بموجب اللائحة العامة لحماية البيانات: إنتاج تفسيرات متعددة المستويات)، هدفت إلى تحليل متطلبات تقييم الأثر الخوارزمي بموجب اللائحة العامة لحماية البيانات، وكيفية إنتاج تفسيرات متعددة المستويات للقرارات الآلية، كما هدفت إلى تقديم إطار نظري وعملي لتصميم تقييمات أثر تراعي الخصوصية منذ البداية. واعتمدت الدراسة على المنهج التحليلي للنصوص القانونية، مع

مراجعة الأدبيات الأكاديمية والتقارير الصادرة عن هيئات حماية البيانات. وأكدت النتائج أن تقييمات الأثر الخوارزمي تُعد أداة أساسية لتحقيق الشفافية والمساءلة في أنظمة اتخاذ القرار الآلية، وأشارت النتائج إلى أن التفسيرات المتعددة المستويات (الموجهة للمطورين، والمدققين، والمستخدمين النهائيين) تُعزز الفهم العام للقرارات الآلية وتُمكن من اكتشاف التحيزات الخوارزمية، كما أوصت الدراسة بتبني نهج تشاركي في تصميم تقييمات الأثر، وإشراك أصحاب المصلحة في هذه العملية، وتطوير أدوات تقنية لدعم إنتاج التفسيرات متعددة المستويات.

تعقيب تحليلي عام على الدراسات السابقة

استناداً إلى المراجعة المنهجية للدراسات السابقة في محاورها الأربعة، يتبين أن الأدبيات البحثية قد أسهمت بشكل ملموس في بناء معرفة رصينة حول موضوعات الذكاء الاصطناعي المستدام، وحماية البيانات الشخصية، والحوكمة الرقمية، والمقارنة بين الأنظمة التنظيمية. غير أن التحليل النقدي لهذه الدراسات يكشف عن مجموعة من الجوانب التي تُحدد موقع الدراسة الحالية من هذه الأدبيات، وتُبرز مساهمتها العلمية، وفيما يأتي تفاصيل هذا التحليل:

أولاً: اتساق الدراسة الحالية مع الدراسات السابقة

تندرج الدراسة الحالية في سياق الجهود البحثية التي تسعى إلى فهم التداخلات المعقدة بين التقنيات الناشئة والأطر التنظيمية، وهو اتجاه تعكس معظم الدراسات السابقة، خاصة تلك التي جمعت بين المتغيرين كدراسات (الغافري، 2026)، و (Hohmann & Kollár, 2025)، و (Zaidan & Ibrahim, 2024) التي تناولت التحديات المزدوجة بين متطلبات حماية البيانات وتطبيقات الذكاء الاصطناعي. كما تتفق الدراسة الحالية مع الدراسات المحلية (كدراسة الشمري، فهد، 2023؛ والعجمي، 2023) في التركيز على البيئة السعودية بوصفها سياقاً بحثياً ناشئاً يستدعي فهماً متعمقاً لتحديات الامتثال في ظل التحول الرقمي المتسارع. ويتسق المنحى المقارن للدراسة مع الدراسات العربية التي اعتمدت المقارنة مع النماذج الدولية، كدراسة (الشمري، نجم، 2023)،

ودراسة (محمد، ياسر، 2022)، ودراسة (طه، 2020)، مما يؤكد أن المقارنة مع التجربة الأوروبية تُعد مدخلاً منهجياً راسخاً لتقييم الأنظمة الوطنية وتطويرها.

ثانياً: جوانب اتفاق الدراسة الحالية مع الدراسات السابقة

تتفق الدراسة الحالية مع الدراسات السابقة في عدة مبادئ جوهرية، أبرزها:

1. التأكيد على أن حماية البيانات الشخصية تمثل ركيزة أساسية للحوكمة الرشيدة في العصر الرقمي، وهو ما أظهرته دراسات المحور الثاني كدراسة (رجب، 2024)، ودراسة (السعودي، 2024).

2. تتفق مع الدراسات التي شددت على أهمية الشفافية الخوارزمية وقابلية التفسير كشرط للثقة في أنظمة الذكاء الاصطناعي، مثل دراسة (Arrieta et al., 2020)، ودراسة (Kaminski & Malgieri, 2021).

3. تتوافق الدراسة الحالية مع الدراسات التي أكدت على الطابع الديناميكي لمخاطر البيانات الشخصية في بيئات الذكاء الاصطناعي، وهو ما أبرزته دراسات (Murdoch, 2021)، و (Oh et al., 2025).

4. تتفق مع الدراسات التي شددت على أهمية التكامل بين الأطر القانونية والمعايير التقنية لتحقيق امتثال فعال، وهو ما تناولته دراسات (Chhetri et al., 2024)، و (Georgiadis & Poels, 2022).

ثالثاً: جوانب اختلاف الدراسة الحالية عن الدراسات السابقة

تختلف الدراسة الحالية عن معظم الدراسات السابقة في ثلاثة جوانب رئيسية، هي:

1. في التكامل الموضوعي؛ إذ ركزت الدراسات السابقة على كل متغير بمعزل عن الآخر، بينما تجمع الدراسة الحالية بين المتغيرات الثلاثة (الذكاء الاصطناعي المستدام، وحماية البيانات الشخصية، والحوكمة الرقمية) في نموذج تحليلي واحد.

2. في العمق المقارن؛ إذ اكتفت معظم الدراسات المقارنة (كدراسة الشمري، نجم، 2023؛ ودراسة محمد، ياسر، 2022) بالمقارنة العامة للنصوص التشريعية، بينما تتعمق الدراسة الحالية في تحليل الآثار العملية للاختلافات بين PDPL وGDPR على المؤسسات.

3. في الجانب التطبيقي؛ إذ اعتمدت معظم الدراسات السابقة على المنهج الوصفي التحليلي، بينما تسعى الدراسة الحالية إلى تقديم إطار عملي للامتثال المزدوج، وهو ما يميزها عن الدراسات السابقة التي اقتصرت على التحليل النظري.

رابعاً: الفجوة البحثية

تُحدد الفجوات البحثية التي تسعى الدراسة الحالية إلى سدها في الآتي:

1. **الفجوة الموضوعية (التكاملية):** ركزت معظم الدراسات السابقة على تناول كل متغير بمعزل عن الآخر؛ فدراسات الذكاء الاصطناعي اهتمت بالجوانب التقنية والأخلاقية (Arrieta et al., 2020; Sætra, 2023; Taeihagh, 2025)، ودراسات حماية البيانات ركزت على الجوانب القانونية والتشريعية (أبو خمرة، 2021؛ الجندي، 2023؛ رجب، 2024)، بينما تناولت دراسات الحوكمة الأطر المؤسسية والسياسية (طاهر، 2024؛ Birkstedt et al., 2025؛ Batoool et al., 2023). كما أن الدراسات التي جمعت بين المتغيرين (الغافري، 2026؛ Hohmann & Kollár, 2025؛ Zaidan & Ibrahim, 2024) أشارت إلى تحديات مزدوجة لكنها لم تقدم تحليلاً متكاملاً يربط بين استراتيجيات الحوكمة الرقمية وآليات الامتثال في نموذج واحد. وتُسهم هذه الدراسة في سد هذه الفجوة ببناء إطار نظري متكامل يدمج المتغيرات الثلاثة ويحلل تكاملها في آليات الامتثال، مع تقديم تحليل مقارنة معمق بين PDPL وGDPR.

2. **الفجوة المكانية (السياقية):** ركزت الدراسات العربية التي تناولت PDPL (الشمري، فهد، 2023؛ الجربوع، 2024؛ العجمي، 2023) على تحليل النص القانوني أو مقارنته سطحياً مع GDPR، دون التعمق في الجوانب التقنية للحوكمة الرقمية أو دراسة تحديات الامتثال في البيئة السعودية من منظور متكامل. وتتميز هذه الدراسة بتطبيقها في السياق السعودي كبيئة ناشئة، مع مقارنة متعمقة مع السياق الأوروبي، مما يُتيح استخلاص دروس عملية لتطوير المنظومة الوطنية.

3. **الفجوة الزمانية (الحدثة):** صدرت معظم الدراسات التحليلية للقوانين الوطنية العربية قبل دخول PDPL حيز النفاذ الفعلي (سبتمبر 2024)، مما يعني أنها لم تتناول اللوائح التنفيذية والتحديات العملية للامتثال. وتستند هذه الدراسة إلى مراجع حديثة (2020-2026) وتتناول

النظام في مرحلة تطبيقه الفعلية، مع التركيز على تحليل اللوائح التنفيذية الصادرة حديثاً والممارسات العملية للمؤسسات السعودية.

4. الفجوة المنهجية: اعتمدت معظم الدراسات السابقة على المنهج الوصفي التحليلي أو المقارن للنصوص، مع ندرة في الدراسات التطبيقية التي تقيس أثر آليات الامتثال أو تُقيّم فعالية الأدوات التقنية في تحقيق الامتثال المزدوج. وتسعى هذه الدراسة إلى تقديم منهجية تحليلية مقارنة متعمقة تجمع بين تحليل النصوص التشريعية ومراجعة الأدبيات التقنية واستخلاص مؤشرات الامتثال، مما يُعزز الجانب التطبيقي للبحث.

5. فجوة الربط بين الأطر القانونية والممارسات التقنية: أشارت دراسات عدة (فلاق، 2025؛ منور وبلعدي، 2025؛ Georgiadis & Poels, 2022؛ Chhetri et al., 2024) إلى وجود فجوة بين النصوص القانونية وقدرة المؤسسات على ترجمتها إلى ممارسات تقنية فعالة، لكنها لم تقدم نماذج تطبيقية شاملة لهندسة الامتثال في أنظمة الذكاء الاصطناعي. وتُعالج هذه الدراسة هذه الفجوة من خلال تحليل آليات التحويل من النص القانوني إلى الكود البرمجي، وتقديم تصور لأنظمة ذكاء اصطناعي قادرة على الامتثال المزدوج لمتطلبات PDPL وGDPR.

6. فجوة الدراسات المقارنة المعمقة: اقتصر معظم الدراسات المقارنة (الشمري، نجم، 2023؛ السعيد، وفاء، 2024؛ De Hert & Papakonstantinou, 2017) على المقارنة العامة بين النصوص التشريعية، دون التعمق في تحليل الفروقات الدقيقة أو دراسة دلالاتها على الممارسة العملية. وتتميز هذه الدراسة بتقديم تحليل مقارنة معمق يتجاوز النصوص إلى تحليل الآثار العملية للاختلافات بين النظامين، مع التركيز على مجالات نقل البيانات، والعقوبات، وآليات الرقابة، وحوكمة الذكاء الاصطناعي.

7. فجوة الدراسة التجريبية: يلاحظ الباحث من خلال رصده للدراسات السابقة وجود فجوة موضوعية تتمثل في طغيان التحليل الوثائقي والقانوني النظري، مع ندرة واضحة في الدراسات التجريبية التي تقيس تحديات الامتثال الفعلية من وجهة نظر الممارسين ومسؤولي حماية البيانات

في المؤسسات السعودية؛ وهو ما تسعى هذه الدراسة لسده من خلال تطبيق بُعد تطبيقي وميداني في فصولها القادمة لتجسير الفجوة بين النص التشريعي والواقع العملي.

وبناءً على هذه الفجوات، تُحدد الفجوة البحثية الرئيسية للدراسة في: ندرة الدراسات التي تُحلل بشكل متكامل العلاقة بين استراتيجيات الحوكمة الرقمية للذكاء الاصطناعي المستدام وآليات الامتثال لحماية البيانات الشخصية، مع مقارنة تطبيقية معمقة بين نظام PDPL السعودي وGDPR الأوروبي، في سياق تقني وإداري متطور، مع تقديم إطار عملي للمؤسسات لتحقيق الامتثال المزدوج. وتسعى الدراسة من خلال تحليلها المقارن إلى تقديم إسهام معرفي يسد هذه الفجوات ويفتح آفاقاً بحثية جديدة، كما تُقدم توصيات عملية للمؤسسات العاملة في البيئة السعودية لتطوير استراتيجيات امتثال فعالة تتوافق مع المعايير الدولية مع مراعاة الخصوصية الوطنية.

خامساً: جوانب استفادة الدراسة الحالية من الدراسات السابقة

تستفيد الدراسة الحالية من الدراسات السابقة في عدة جوانب:

1. في البناء النظري، حيث توفر الدراسات السابقة (كدراسة Arrieta et al., 2020؛ ودراسة Sætra, 2023) إطاراً مفاهيمياً لفهم الذكاء الاصطناعي المستدام وأبعاده.
2. في الجانب المنهجي، حيث تُعد الدراسات المقارنة (كدراسة الشمري، نجم، 2023؛ ودراسة محمد، ياسر، 2022) نماذج منهجية يمكن الاستفادة منها في تصميم التحليل المقارن.
3. في تحديد التحديات، حيث كشفت الدراسات السابقة (كدراسة منور وبلعدي، 2025؛ ودراسة فلاق، 2025) عن تحديات قانونية وتقنية تواجه المؤسسات في مجال حماية البيانات والذكاء الاصطناعي، مما يُساعد الدراسة الحالية في تحديد أولويات التحليل.
4. في الجانب التطبيقي، حيث تُعد دراسة (Chhetri et al., 2024)، ودراسة (Oh et al., 2025) نماذج لتوظيف الحلول التقنية في دعم الامتثال، مما يُثري التوصيات العملية للدراسة الحالية.

سادساً: الجوانب المميزة للدراسة الحالية عن الدراسات السابقة

تتميز الدراسة الحالية بعدة جوانب، هي:

1. التكامل المعرفي، إذ تجمع بين ثلاثة متغيرات رئيسية (الذكاء الاصطناعي المستدام، والحوكمة الرقمية، وحماية البيانات الشخصية) في إطار تحليلي واحد، وهو ما لم تتناوله الدراسات السابقة بشكل متكامل.
2. التحليل المقارن المعمق، حيث تتجاوز الدراسة المقارنة العامة للنصوص إلى تحليل الآثار العملية للاختلافات بين PDPL وGDPR، مع التركيز على مجالات نقل البيانات، والعقوبات، وآليات الرقابة، وحوكمة الذكاء الاصطناعي.
3. الحداثة الزمانية، إذ تتناول الدراسة النظام السعودي في مرحلة تطبيقه الفعلية بعد صدور اللوائح التنفيذية، مما يُعطيها قيمة معرفية معاصرة.
4. الجانب التطبيقي، حيث تقدم الدراسة إطاراً عملياً للمؤسسات لتحقيق الامتثال المزدوج لمتطلبات PDPL وGDPR، وهو ما يفتقر إليه الأدبيات السابقة.
5. التركيز على السياق السعودي كبيئة ناشئة في مجال حوكمة الذكاء الاصطناعي وحماية البيانات، مما يُتيح استخلاص دروس عملية لتطوير المنظومة الوطنية.

قائمة المراجع الشاملة

أولاً: المراجع العربية

1. أبو خمرة، ضرغام عبدالله فاضل. (2021). حماية بيانات الأفراد الشخصية عبر شبكة الإنترنت: دراسة مقارنة. (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان، الأردن. أسترجم من: <https://search.mandumah.com/Record/1209224>
2. أبو عزاق، هيثم. (2025). أثر التحول الرقمي في الإدارة العامة على حقوق المواطنين: دراسة تحليلية. مجلة البحوث الفقهية والقانونية، 50(50)، 4977-5071. https://journals.ekb.eg/article_453654.html
3. أشقر، أحمد حسني علي. (2025). الخصوصية الرقمية في عصر الذكاء الاصطناعي: قراءة في التشريعين الأردني والفلسطيني. مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية، 7(66)، 1-28. <https://doi.org/10.33977/0507-000-066-003>
4. إمام، ماهر إبراهيم عبيد، والحربي، مشاري محمد عمر، والغافري، حسين بن سعيد. (2024). الحماية القانونية للبيانات الشخصية في النظامين السعودي والعُماني: دراسة مقارنة. مجلة الدراسات الفقهية والقانونية (ملحق)، 19(1)، 8-51. <https://doi.org/10.70299/hji.i19.S1>
5. البقلي، أيمن مصطفى أحمد. (2021). حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة متطلبات التجارة الإلكترونية. المجلة القانونية، 9(4)، 1001-1144. <https://doi.org/10.21608/jlaw.2021.190687>
6. تخرج للمحاماة والاستشارات القانونية. (2026). أثر التكنولوجيا الحديثة على حماية البيانات الشخصية: دراسة مقارنة بين الأنظمة الخليجية والدولية. تم الاسترجاع من <https://takharuj.com/أثر-التكنولوجيا-الحديثة-على-حماية-البيانات-الشخصية> (takharuj.com)
7. الترك، وفاء كمال عبدالرحمن. (2025). مخاطر تعهيد معالجة البيانات الشخصية للطرف الثالث. جرش للبحوث والدراسات، 25(2)، 281-302. <https://doi.org/10.36091/0550-025-002-013>
8. الجربوع، عبدالله بن محمد. (2024). المسؤولية الجزائية لانتهاك حقوق البيانات الشخصية الرقمية في النظام السعودي: دراسة تحليلية مقارنة. مجلة جامعة تبوك للعلوم الإنسانية

- والاجتماعية، 4(4)، 384-357. استرجع من
<https://search.mandumah.com/Record/1539052>
9. الجعافرة، رويدا حسن. (2022). قانون حماية البيانات الشخصية في الأردن. المجلة العربية للنشر العلمي، 50(5)، 1100-1081. مسترجع من:
<https://search.mandumah.com/Record/1437425>
10. الجندي، يارا حافظ. (2023). البيانات الشخصية بين التهديد والحماية: دراسة في ضوء أحكام القانون المصري رقم 151 لسنة 2020. مجلة الدراسات القانونية والاقتصادية، 9(4)، 2866-2758.
<https://search.mandumah.com/Record/1514054>
11. الجيجكلي، تمام عبداللطيف. (2025). حماية البيانات الشخصية للشركات والمؤسسات والأفراد وفقاً للمعايير الدولية وأحكام القانون الدولي الخاص. المجلة الدولية للبحوث العلمية، 4(10)، 95-72.
<https://doi.org/10.59992/IJSR.2025.v4n10p3>
12. الحسنات، حنان خضر حسن. (2025). مفهوم البيانات الشخصية وحدودها. مجلة جرش للبحوث والدراسات، 25(2)، 994-978.
<https://doi.org/10.36091/0550-025-002-042>
13. رجب، هبة رمضان. (2024). الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية. مجلة العلوم القانونية والاقتصادية، 66، 449-417. استرجع من
<https://search.mandumah.com/Record/1554883>
14. الرحلي، رباب عبد الله. (2026). حماية البيانات الشخصية في البيئة الرقمية: دراسة مقارنة بين التشريعات العربية والدولية. مجلة الاتحاد العربي للنشر العلمي، 7(1).
<file:///C:/Users/PC/Downloads/5.pdf>
15. رفرافي، عبد الرحمن. (2025). حماية البيانات الشخصية والأمن السيبراني: تحليل من منظور القانون الدولي. مجلة المفكر، 20(1)، 389-367.
<https://doi.org/10.37136/0516-020-001-017>
16. السعودي، نجود بنت علي بن محمد. (2024). الحماية النظامية للخصوصية المعلوماتية: دراسة تأصيلية تحليلية. مجلة قضاء، 34(34)، 631-555.
<https://search.mandumah.com/Record/1465366>
17. السعيد، رنا علي. (2023). الذكاء الاصطناعي وتطبيقاته في مجال القضاء (دراسة مقارنة). مجلة جامعة الشارقة للدراسات القانونية والسياسية، 6(2)، 72-45.
<https://doi.org/10.33977/0207-000-015-003>

18. السعيد، وفاء حلمي. (2024). تقنية الذكاء الاصطناعي وحماية البيانات الشخصية: دراسة مقارنة. *مجلة الشريعة والقانون بالقاهرة*، 43(43)، 1389-1442.
<https://doi.org/10.21608/mawq.2024.295577.1059>
19. سويلم، خالد سويلم محمد. (2022). الحماية القانونية للبيانات الشخصية الإلكترونية: دراسة مقارنة. *المجلة القانونية*، 14(6)، 1885-1912.
<https://doi.org/10.21608/JLAW.2022.269929>
20. الشامسي، حبيبة سيف سالم راشد. (2023). حماية البيانات الشخصية في ضوء القانون الاتحادي رقم "45" لسنة 2021: دراسة مقارنة. *مجلة الأمن والقانون*، 31(1)، 9-54.
<https://doi.org/10.54000/0576-031-001-001>
21. الشمري، فهد بن عايد. (2023). الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية. *مجلة البحوث الفقهية والقانونية*، 43(43)، 1639-1690.
<https://search.mandumah.com/Record/1465695>
22. الشمري، نجم بن عبدالله. (2023). حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة. *مجلة العلوم الإنسانية والاجتماعية*، 7(11)، 82-94.
<https://doi.org/10.26389/AJSRP.M090723>
23. صالح، ثناء محمد. (2025). السوسيولوجيا وتحديات الذكاء الاصطناعي. *مجلة تسنيم الدولية للعلوم الإنسانية والاجتماعية والقانونية*، 4(2)، 510-534.
<https://doi.org/10.56924/tasnim.13.2025/26>
24. صميده، صلاح الدين رجب فتح الباب. (2025). آليات بناء القواعد القانونية لحماية البيانات الشخصية في البيئة الرقمية: دراسة تحليلية في ضوء تطور تقنيات الذكاء الاصطناعي. *جروش للبحوث والدراسات*، 25(2)، 213-238.
<https://doi.org/10.36091/0550-025-002-010>
25. طاهر، هالة محمد. (2024). الحوكمة القانونية للذكاء الاصطناعي في مصر "التحديات والفرص". *مجلة البحوث القانونية والاقتصادية*، 36(2)، 611-639.
<https://doi.org/10.21608/lsej.2024.283724.1070>
26. طه، علاء عيد. (2020). الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها: دراسة في ضوء اللائحة التنظيمية رقم 679/2016 الصادرة

- عن البرلمان الأوروبي. مجلة جامعة الملك سعود - الحقوق والعلوم السياسية، 32(1)، 1-60. <https://doi.org/10.33948/1203-032-001-001>
27. الظفيري، أنور فهد عوض. (2025). التحول الرقمي في الإدارة العامة وأثره على ضمانات الموظف العام في النظام السعودي: دراسة تحليلية مقارنة. مجلة أبحاث، 12(3)، 828-868. <https://doi.org/10.63679/ja.v12i3.869>
28. عبد، رؤى رزاق. (2025). الضوابط القانونية للقرار الإداري الصادر عن الذكاء الاصطناعي: دراسة تحليلية في ضوء التشريع العراقي. مجلة اشور للعلوم القانونية والسياسية، 2(3)، 436-469. <https://doi.org/10.64184/ajlps.V2.I3.Y2025.P436-469.137>
29. العبيدان، سلطان عبدالرحمن. (2024). التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي. مجلة أبحاث، 11(2)، 460-541. <https://doi.org/10.52840/1965-011-002-012>
30. العتيبي، أماني محمد سيف. (2025). الوظيفة الرقابية لحماية البيانات الشخصية: دراسة مقارنة. مجلة جرش للبحوث والدراسات، 25(2)، 383-413. <https://doi.org/10.36091/0550-025-002-017>
31. العتيبي، محمد عبد الله، والشمري، نادر سليمان. (2025). الامتثال للوائح حماية البيانات العامة (GDPR): التعريفات والمتطلبات وقائمة التحقق للامتثال. موقع Compliance. تم الاطلاع عليه بتاريخ: 2025/11/3 من <https://www.exabeam.com/ar/explainers/gdpr-compliance/gdpr-compliance-a-practical-guide>
32. العجمي، أحمد محمد. (2023). الحق في خصوصية البيانات الشخصية وضمانات حمايتها في عصر التحول الرقمي: دراسة تحليلية في النظام السعودي. مجلة الإدارة العامة، 63(3)، 481-510. <https://doi.org/10.36715/0328-063-003-001>
33. عفيفي، أيمن فتحي محمد. (2025). الإطار القانوني للقرارات المعالجة إلكترونياً: دراسة مقارنة بين القانون الأوروبي والقانون الفرنسي. مجلة جامعة الملك سعود - الحقوق والعلوم السياسية، 37(1)، 129-163. <https://search.mandumah.com/Record/1593045>

34. علي، أمل حسين عبدالقادر. (2024). توظيف تطبيقات الذكاء الاصطناعي لحماية خصوصية البيانات: دراسة حالة جمعية المكتبات الأمريكية. *المجلة المصرية لعلوم المعلومات*، 11(1)، 245-310. مسترجع من: <https://search.mandumah.com/Record/1478940>
35. علي، محمد حسن عبد الله. (2021). النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة. *مجلة العلوم القانونية*، 7(14)، 73-118. استرجع من <https://search.mandumah.com/Record/1197076>
36. العيش، الصالحين محمد. (2023). حماية البيانات الشخصية في القانون الأوروبي. *مجلة كلية القانون الكويتية العالمية*، 11(43)، 289-322. <https://doi.org/10.54032/2203-011-043-009>
37. الغافري، حسين بن سعيد. (2026). حماية البيانات الشخصية في ظل تطبيق الذكاء الاصطناعي في الأنظمة القضائية: مقارنة بين سلطنة عُمان والتشريعات الدولية. *المجلة الحديثة للدراسات القانونية*، 4(1)، 136-167. <https://doi.org/10.70411/MJLS.4.1.2026255>
38. الفارسية، العنود بنت إبراهيم بن عبيد. (2023). حقوق صاحب البيانات الشخصية ووسائل حمايتها وفقاً لقانون حماية البيانات الشخصية العماني: دراسة مقارنة. (رسالة ماجستير غير منشورة). كلية الحقوق، جامعة السلطان قابوس، عُمان. استرجع من <https://search.mandumah.com/Record/1468737>
39. فلاتة، حسام إبراهيم. (2025). حماية البيانات الشخصية في التطبيقات الإلكترونية والمنصات الرقمية في ضوء أحكام النظام السعودي والتشريعات المقارنة: نحو إطار قانوني أمثل لحماية بيانات المستهلك الإلكتروني. *مجلة الآداب والعلوم الإنسانية والاجتماعية*، 126(1)، 455-463. <https://doi.org/10.33193/JALHSS.126.2025.7516>
40. فلاق، فريدة. (2025). *الخوارزميات، سوق البيانات الشخصية وانتهاك الخصوصية: الإشكالات الرقمية الجديدة في ظل نظم الذكاء الاصطناعي*. في أعمال الملتقى الدولي المدمج: الوصول إلى المعلومات وحماية البيانات الخاصة (10 أكتوبر 2024). المركز الجامعي بربكة. https://www.researchgate.net/publication/392172145_alkhwarzmyat_swq_alby

41. القطاطشة، باسل فايز حمد. (2022). *الحماية الجنائية لخصوصية البيانات الشخصية الرقمية: دراسة مقارنة* (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان، الأردن. مسترجع من <https://search.mandumah.com/Record/1263702>
42. المحروقي، ميادة مصطفى محمد. (2023). *الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً: دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي (GDPR)*. *المجلة القانونية*، 16(7)، 1477-1608. <https://doi.org/10.21608/jlaw.2023.298064>
43. محمد، ياسر أحمد بدر. (2022). *الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر معالجة بياناتهم ذات الطابع الشخصي: دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات*. *مجلة البحوث الأمنية*، 31(83)، 69-128. استرجع من <https://search.mandumah.com/Record/1401490>
44. محمود، سيد أحمد. (2024). *حماية البيانات الشخصية الرقمية وفقاً لأحكام القانون المصري رقم 151 لسنة 2020 (حماية البيانات الشخصية المعالجة إلكترونياً) بين الواقع والمأمول*. *مجلة العلوم القانونية والاقتصادية*، 66(1)، 1439-1482. <https://doi.org/10.21608/jelc.2024.341026>
45. المدبولي، باسم محمد فاضل. (2022). *المسؤولية التقصيرية عن معالجة البيانات الشخصية في البيئة الرقمية: دراسة مقارنة*. *مجلة الدراسات الفقهية والقانونية*، 10(10)، 100-173. <https://doi.org/10.70299/hji.i10.3>
46. مسارات قانونية. (2026). *الحلقة المفقودة في الامتثال لنظام حماية البيانات الشخصية والأمن السيرياني والنكاء الاصطناعي: لماذا تُعد المراقبة المستمرة أمراً جوهرياً؟* تم الاسترجاع من (<http://legaltracks.sa>) *مسارات قانونية*
47. المعداوي، عبد ربة محمد احمد. (2018). *حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة*. *مجلة كلية الشريعة والقانون بطنطا*، (33، 4)، 1926-2057. <https://doi.org/10.21608/MKSQ.2018.30623>

48. منور، موسى، وبلعدي، فريد. (2025). التحديات القانونية لحماية البيانات الشخصية في سياق الذكاء الاصطناعي. *مجلة القانون العام الجزائري والمقارن*، 11(9)، 293-313.
<https://asjp.cerist.dz/en/downArticle/547/11/2/275641>
49. الموح، دينا فهد. (2024). تأثير التربية الإعلامية الرقمية على سلوكيات المستخدمين في حماية بياناتهم الشخصية: دراسة ميدانية. *مجلة العلوم التربوية والإنسانية*، (39)، 78-132.
<https://doi.org/10.33193/JEAHS.39.2024.545132>
50. النيداني، ياسر محمد علي. (2024). حماية البيانات الشخصية عبر تقنية البلوك تشين. *مجلة روح القوانين*، 36(107)، 1011-1178.
<https://doi.org/10.21608/las.2024.284186.1214>
51. هلال، غفران، وشعبان، يسرى، ونجاشي، أمل. (2022). حوكمة الذكاء الاصطناعي ضمن أحكام القانون الدولي لحقوق الإنسان. *مجلة دراسات العلوم الشرعية والقانونية*، 49(4)، 126-138.
<https://doi.org/10.35516/law.v49i4.1173>
52. هبوب، محمد إبراهيم. (2023). التنظيم الدستوري لحماية البيانات الشخصية عبر الوسائل الإلكترونية. *مجلة الدراسات القانونية*، 59(3)، 1040-1083.
<https://doi.org/10.21608/maal.2023.186971.1133>
53. الهيئة السعودية للبيانات والذكاء الاصطناعي. (2025). دليل نظام حماية البيانات الشخصية. منصة حوكمة البيانات الوطنية. تم الاسترجاع من <https://dgp.sdaia.gov.sa>
54. الوادي، آيات محمود حسين. (2025). حماية البيانات الشخصية الرقمية في التشريع الأردني. (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان، الأردن. استرجع من <https://search.mandumah.com/Record/1578856>

ثانياً: المراجع الأجنبية

1. Albous, M. R., Alhammadi, M., & Alhangash, H. (2025). AI governance in the GCC states: A comparative analysis of national AI strategies. *Journal of Artificial Intelligence Research*, (82), 2389–2422.
<https://doi.org/10.1613/jair.1.17619>
2. Alhazmi, A., & Daghistani, A. (2025). Privacy practices of popular websites in Saudi Arabia. *Journal of Umm Al-Qura University for Engineering and Architecture*, 16, 19-29.
<https://doi.org/10.1007/s43995-024-00085-x>
3. Al-Khalifa, H., Mashaabi, M., Al-Yahya, G., & Alnashwan, R. (2023). The Saudi Privacy Policy Dataset. *arXiv preprint*, arXiv:2304.02757. <https://doi.org/10.48550/arXiv.2304.02757>

4. Almaghrabi, N. S., & Bugis, B. A. (2022). Patient confidentiality of electronic health records: A recent review of the Saudi literature. *Dr. Sulaiman Al Habib Medical Journal*, 4, 126–135. <https://doi.org/10.1007/s44229-022-00016-9>
5. Altamimi, S., Storer, T., & Alzahrani, A. (2018). The role of neutralisation techniques in violating hospitals' privacy policies in Saudi Arabia. In *Proceedings of the 2018 4th International Conference on Information Management (ICIM)* (pp. 133–140). IEEE. <https://doi.org/10.1109/INFOMAN.2018.8392823>
6. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>
7. Balboni, P., & Francis, K. E. (2024). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. *Journal of Responsible Technology*, 22, Article 100099. <https://doi.org/10.1016/j.jrt.2024.100099>
8. Barthwal, A., Campbell, M., & Shrestha, A. K. (2025). Privacy ethics alignment in AI: A stakeholder-centric framework for ethical AI. *Systems*, 13(6), 455–472. <https://doi.org/10.3390/systems13060455>
9. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics*, 5, 3265–3279. <https://doi.org/10.1007/s43681-024-00653-w>
10. Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: Themes, knowledge gaps and future agendas. *Internet Research*, 33(7), 133–167. <https://doi.org/10.1108/INTR-01-2022-0042>
11. Boudierhem, R. (2024). Shaping the future of AI in healthcare through ethics and governance. *Humanities and Social Sciences Communications*, 11(1), Article 45. <https://doi.org/10.1057/s41599-024-02894-w>
12. Brière, É., & Uyar, A. (2024). Toward trustworthy AI: Ethical frameworks and governance approaches. *Expert Systems*, 41(8), 182–199. <https://doi.org/10.1111/exsy.13478>
13. Burnaev, E., Mironov, E., Shpilman, A., Mironenko, M., & Katalevsky, D. (2023). Practical AI Cases for Solving ESG Challenges. *Sustainability*, 15(17), Article 12731. <https://doi.org/10.3390/su151712731>
14. Camilleri, M. A. (2023). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems*, 41(7), 133–148. <https://doi.org/10.1111/exsy.13406>
15. Cech, F. (2021). The agency of the forum: Mechanisms for algorithmic accountability through the lens of agency. *Journal of Responsible Technology*, 7–8, Article 100015. <https://doi.org/10.1016/j.jrt.2021.100015>
16. Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making.

- Frontiers in Human Dynamics*, 6, Article 1421273. <https://doi.org/10.3389/fhumd.2024.1421273>
17. Chhetri, T. R., Fensel, A., & DeLong, R. J. (2024). GDPR consent management and automated compliance verification tool. *SoftwareX*, 27, Article 101821. <https://doi.org/10.1016/j.softx.2024.101821>
 18. Compliance.ai. (2020). *Compliance.ai Usage Case Study: Analysis of 11 financial services companies transforming their regulatory change management processes to lower their compliance operational costs by over 30 percent*. <https://www.compliance.ai/wp-content/uploads/2020/11/ComplianceAI-Case-Study-Financial-Services.pdf>
 19. Cordeiro, C. M., Adomaitis, L., & Huang, L. (2025). The AI-policy-governance nexus: How regulation and AI shift corporate governance toward stakeholders. *Technology in Society*, 84, Article 103117. <https://doi.org/10.1016/j.techsoc.2025.103117>
 20. Corea, F., Fossa, F., Loreggia, A., & Quintarelli, S. (2023). A principle-based approach to AI: The case for European Union and Italy. *AI & Society*, 38(2), 521–535. <https://doi.org/10.1007/s00146-022-01453-8>
 21. Corrêa, N. K., Galvão, C., Santos, J. W., Galvão, L., Terem, E., & de Oliveira, N. (2023). Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, 4(10), Article 100857. <https://doi.org/10.1016/j.patter.2023.100857>
 22. De Hert, P., & Papakonstantinou, V. (2017). *Data protection, privacy and artificial intelligence: To govern or to regulate?* *International Data Privacy Law*, 7(3), 166–177. <https://doi.org/10.1093/idpl/ix015>
 23. Dirutigliano, J. (2023). *The Right to Explanation* [Doctoral dissertation, University of Bologna]. ORBilu. <https://orbilu.uni.lu/handle/10993/57336>
 24. ECD. (2024). *AI, data governance and privacy: Synergies and areas of international co-operation* (OECD Artificial Intelligence Papers, No. 22). OECD Publishing. <https://doi.org/10.1787/2476b1a4-en>
 25. El Mestari, S. Z., Lenzi, G., & Demirci, H. (2024). *Preserving data privacy in machine learning systems*. *Computers & Security*, 137, Article 103605. <https://doi.org/10.1016/j.cose.2023.103605>
 26. European Data Protection Board. (2025). *AI Privacy Risks & Mitigations – Large Language Models (LLMs)*. <https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf>
 27. European Parliament Research Service. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (PE 641.530). [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
 28. Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards Transparency by Design for Artificial Intelligence. *Science and Engineering Ethics*, 26(6), 3333–3361. <https://doi.org/10.1007/s11948-020-00276-4>
 29. Francu, C. C., & Sava, Ș. (2025). Global perspectives on digital and AI legislation: A comparative study of data protection, AI governance, and healthcare innovations with a focus on Romania. *Proceedings of the*

- International Conference on Business Excellence*, 19(1), 2469–2481. <https://doi.org/10.2478/picbe-2025-0191>
30. Frey, C. B., & Presidente, G. (2024). Privacy regulation and firm performance: Estimating the GDPR effect globally. *Economic Inquiry*, 62(3), 1074–1089. <https://doi.org/10.1111/ecin.13213>
 31. Georgiadis, G., & Poels, G. (2022). *Towards a privacy impact assessment methodology to support the requirements of the General Data Protection Regulation in a big data analytics context: A systematic literature review*. *Computer Law & Security Review*, 44, Article 105640. <https://doi.org/10.1016/j.clsr.2021.105640>
 32. Gkiotsalitis, K., & Cats, O. (2022). *Artificial intelligence-based demand management: Towards sustainable public transport operations*. *Transportation Research Part C: Emerging Technologies*, 139, Article 103608. <https://doi.org/10.1016/j.trc.2022.103608>
 33. Gonçalves, A., & Correia, A. (2026). XAI-compliance-by-design: A modular framework for GDPR- and AI Act-aligned decision transparency in high-risk AI systems. *Journal of Cybersecurity and Privacy*, 6(2), 43. <https://doi.org/10.3390/jcp6020043>
 34. González-Zapata, D. I., & Celaya, R. (2020). *A formal framework for consent management*. *PLoS ONE*, 15(7), Article e0235930. <https://doi.org/10.1371/journal.pone.0235930>
 35. Habibulloh, M. (2025). Digital governance and the right to privacy: A comparative analysis of AI regulation in Southeast Asia and the European Union. *Journal of Law, Policy and Global Development*, 1(1), 1–15. <https://doi.org/10.71305/jlpgd.v1i1.333>
 36. Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V., & Ogiela, L. (2021). *Chatbots: Security, privacy, data protection, and social aspects*. *Concurrency and Computation: Practice and Experience*, 33(23), e6426. <https://doi.org/10.1002/cpe.6426>
 37. Hickman, E., & Petrin, M. (2021). Trustworthy AI and Corporate Governance: The EU's Ethics Guidelines for Trustworthy Artificial Intelligence from a Company Law Perspective. *European Business Organization Law Review*, 22(4), 643–670. <https://doi.org/10.1007/s40804-021-00224-0>
 38. Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act. *Cogent Social Sciences*, 11(1), Article 2560654. <https://doi.org/10.1080/23311886.2025.2560654>
 39. Holtz, H. M., & Ledendal, J. (2026). AI data governance – overlaps between the AI Act and the GDPR. *Law, Innovation and Technology*, 18(1), 1–28. <https://doi.org/10.1080/17579961.2026.2633677>
 40. Hulok, M. (2025). The EU model of AI governance: Regulating artificial intelligence through law and policy. *ERA Forum*, 26(1), 527–547. <https://doi.org/10.1007/s12027-025-00869-1>
 41. Ibrahim, N. M. H. (2024). Artificial intelligence (AI) and Saudi Arabia's governance: Insights and challenges. *Journal of Developing Societies*, 47(15), 1209–1222. <https://doi.org/10.1177/0169796X241288590>
 42. Iskandar, R., Maksum, A., & Marini, A. (2025). Digital citizenship literacy in Indonesia: The role of privacy awareness and social

- campaigns. *Social Sciences & Humanities Open*, 12, Article 101697. <https://doi.org/10.1016/j.ssaho.2025.101697>
43. Kalodanis, K., Feretzakis, G., Rizomiliotis, P., Verykios, V. S., Papapavlou, C., Koutsikos, I., & Anagnostopoulos, D. (2025). *Data governance in healthcare AI: Navigating the EU AI Act's requirements*. *Studies in Health Technology and Informatics*, 323, 66–70. <https://doi.org/10.3233/SHTI250050>
 44. Kaminski, M. E., & Malgieri, G. (2021). Algorithmic impact assessments under the GDPR: Producing multi-layered explanations. *International Data Privacy Law*, 11(2), 125–144. <https://doi.org/10.1093/idpl/ipaa020>
 45. Kamyshanskaya, S. (2021). *AI and data privacy: Managing risk in the boardroom*. *Board Leadership*, (174), 6–7. <https://doi.org/10.1002/bl.30185>
 46. Kazim, E., Denny, D. M. T., & Koshiyama, A. (2021). *AI auditing and impact assessment: According to the UK Information Commissioner's Office*. *AI & Ethics*, 1(4), 301–310. <https://doi.org/10.1007/s43681-021-00039-2>
 47. Kirat, T., Tambou, O., Do, V., & Tsoukiàs, A. (2023). Fairness and explainability in automatic decision-making systems: A challenge for computer science and law. *EURO Journal on Decision Processes*, 11, Article 100036. <https://doi.org/10.1016/j.ejdp.2023.100036>
 48. Kumar, A., & Singh, R. (2024). Mapping the empirical evidence of the GDPR (In-)Effectiveness: A systematic review. *arXiv*. <https://arxiv.org/pdf/2310.16735.pdf>
 49. Kumkar, L. K., & Roth-Isigkeit, D. (2021). A criterion-based approach to GDPR's explanation requirements for automated individual decision-making. *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 12(4). <https://www.jipitec.eu/jipitec/article/view/326>
 50. Kuner, C., Marelli, M., & Docksey, C. (2021). The GDPR and data protection in the age of AI: Challenges and opportunities. *Computer Law & Security Review*, 41, 105567. <https://doi.org/10.1016/j.clsr.2021.105567>
 51. Larsson, S. (2021). AI in the EU: Ethical guidelines as a governance tool. In A. Bakardjieva Engelbrekt, K. Leijon, A. Michalski, & L. Oxelheim (Eds.), *The European Union and the Technology Shift* (pp. 85–110). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-63672-2_4
 52. Lazcoz, G., & De Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems: Essential prerequisites against abdicating responsibilities. *Computer Law & Security Review*, 50, Article 105833, 1–20. <https://doi.org/10.1016/j.clsr.2023.105833>
 53. Lorè, F., Basile, P., Appice, A., de Gemmis, M., Malerba, D., & Semeraro, G. (2023). An AI framework to support decisions on GDPR compliance. *Journal of Intelligent Information Systems*, 61(2), 541–568. <https://doi.org/10.1007/s10844-023-00782-4>
 54. Lukács, A., & Váradi, S. (2023). *GDPR-compliant AI-based automated decision-making in the world of work*. *Computer Law &*

55. Majeed, A., & Hwang, S. O. (2024). Towards Unlocking the Hidden Potentials of the Data-Centric AI Paradigm in the Modern Era. *Applied System Innovation*, 7(4), 54. <https://doi.org/10.3390/asi7040054>
56. Malgieri, G. (2019). *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*. *Computer Law & Security Review*, 35(5), 105327. <https://doi.org/10.1016/j.clsr.2019.05.002>
57. Meszaros, J., & Ho, C.-H. (2021). *AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?* *Computer Law & Security Review*, 41, Article 105532. <https://doi.org/10.1016/j.clsr.2021.105532>
58. Meszaros, J., Minari, J., & Huys, I. (2022). *The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union*. *Frontiers in Genetics*, 13, Article 927721. <https://doi.org/10.3389/fgene.2022.927721>
59. Mishah, N., Bukhari, A., AlMutairi, B., & Mohreq, M. (2019). Status of e-security and privacy protection in Saudi hospitals. *Computer Methods and Programs in Biomedicine*, 171, Article 105–106. <https://doi.org/10.1016/j.cmpb.2018.12.012>
60. Mittal, S., & Sharda, R. (2023). Ethical AI for sustainable development: A framework for integrating XAI and GDPR principles. *Journal of Business Ethics*, 187(3), 455–472. <https://doi.org/10.1007/s10551-022-05183-z>
61. Mittelstadt, B. D. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501–507. <https://doi.org/10.1038/s42256-019-0114-4>
62. Mökander, J., Juneja, P., Watson, D. S., & Floridi, L. (2022). The US Algorithmic Accountability Act of 2022 vs. the EU Artificial Intelligence Act: What can they learn from each other? *Minds and Machines*, 32(4), 751–758. <https://doi.org/10.1007/s11023-022-09612-y>
63. Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics*, 22, Article 122. <https://doi.org/10.1186/s12910-021-00687-3>
64. Noë, A., Bouhouita-Guermech, S., & Zawati, M. H. (2025). The Right to Explanation in AI: In a Lonely Place. *Journal of Medical Internet Research*, 27, e64482. <https://doi.org/10.2196/64482>
65. Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, 55, 1–16. <https://doi.org/10.1016/j.clsr.2024.106066>
66. Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *AI & Society*, 39(4), 1871–1882. <https://doi.org/10.1007/s00146-023-01635-y>
67. OECD. (2024). *AI, data governance and privacy: Synergies and areas of international co-operation* (OECD Artificial Intelligence Papers, No. 22). OECD Publishing. <https://doi.org/10.1787/2476b1a4-en>

68. Oh, N., Vrakas, G. D., Brooke, S. J. M., Morinière, S., & Duke, T. (2025). PETLP: A Privacy-by-Design Pipeline for Social Media Data in AI Research. (No journal specified in source materials), arXiv preprint arXiv:2508.09232. <http://arxiv.org/abs/2508.09232v1>
69. Pamuk, M., Schumann, M., & Nickerson, R. C. (2024). What Do the Regulators Mean? A Taxonomy of Regulatory Principles for the Use of AI in Financial Services. *Machine Learning and Knowledge Extraction*, 6(1), 8. <https://doi.org/10.3390/make6010008>
70. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, 34(2), Article 101885. <https://doi.org/10.1016/j.jsis.2024.101885>
71. Patel, V., & Kumar, L. (2025). Integrating digitalization and AI in urban transport: Regulatory challenges and smart city initiatives. *IEEE Transactions on Intelligent Transportation Systems*, 26(6), 4605–4613. <https://doi.org/10.1109/TITS.2025.2958473>
72. Ploug, T. (2023). The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data-Privacy and the Exceptionalism of AI Profiling. *Philosophy & Technology*, 36, 14. <https://link.springer.com/article/10.1007/s13347-023-00616-9>
73. Poechhacker, N., & Kacianka, S. (2021). *Algorithmic accountability in context: Socio-technical perspectives on structural causal models*. *Frontiers in Big Data*, 3, Article 519957. <https://doi.org/10.3389/fdata.2020.519957>
74. Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in Digital Health*, 7, Article 1431246. <https://doi.org/10.3389/fdgth.2025.1431246>
75. Roberts, H., Leung, J., & Cows, J. (2024). Global AI governance: Barriers and pathways forward. *International Affairs*, 100(3), 1275–1292. <https://doi.org/10.1093/ia/kuad012>
76. Sætra, H. S. (2023). The AI ESG protocol: Evaluating and disclosing the environment, social, and governance implications of artificial intelligence capabilities, assets, and activities. *Sustainable Development*, 31(2), 1027–1037. <https://doi.org/10.1002/sd.2438>
77. Sharma, G. D., Yadav, A., & Chopra, R. (2020). Artificial intelligence and effective governance: A review, critique and research agenda. *Sustainable Futures*, 2, Article 100004. <https://doi.org/10.1016/j.sftr.2019.100004>
78. Shmueli, O., & Vardi, M. Y. (2021). The right to explanation: GDPR, AI accountability, and sustainable data governance. *AI Magazine*, 42(3), 115–126. <https://doi.org/10.1609/aimag.v42i3.18129>
79. Stahl, B. C., Andreou, A., Brey, P., Hatzakis, T., Kirichenko, A., Macnish, K., Laulhé Shaelou, S., Patel, A., Ryan, M., & Wright, D. (2021). *Artificial intelligence for human flourishing – Beyond principles for machine learning*. *Journal of Business Research*, 124, 374–388. <https://doi.org/10.1016/j.jbusres.2020.11.030>
80. Stix, C. (2022). *Foundations for the future: Institution building for the purpose of artificial intelligence governance*. *AI & Ethics*, 2(3), 463–476. <https://doi.org/10.1007/s43681-021-00093-w>

81. Taeihagh, A. (2025). Governance of generative AI. *Policy and Society*, 44(1), 1–19. <https://doi.org/10.1080/25741292.2022.2162241>
82. Taylor, L., de Souza, S. P., Martin, A., & López Solano, J. (2025). Governing artificial intelligence means governing data: (Re)setting the agenda for data justice. *Dialogues on Digital Society*. <https://doi.org/10.1177/29768640241306800>
83. Timan, T., van Oirsouw, C., & Hoekstra, M. (2021). *The role of data regulation in shaping AI: An overview of challenges and recommendations for SMEs*. In E. Curry, A. Metzger, S. Zillner, J. C. Pazzaglia, & A. García Robles (Eds.), *The elements of big data value* (pp. 355–376). Springer, Cham. https://doi.org/10.1007/978-3-030-68176-0_15
84. Tjondronegoro, D. W. (2024). *Strategic AI governance: Insights from leading nations* (arXiv:2410.01819). arXiv. <https://doi.org/10.48550/arXiv.2410.01819>
85. Truby, J. (2020). Governing Artificial Intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development*, 28(4), 946–959. <https://doi.org/10.1002/sd.2048>
86. Tzimas, T. (2023). Algorithmic transparency and explainability under EU law. *European Public Law*, 29(4), 385–411. <https://doi.org/10.54648/euro2023021>
87. van Binsbergen, L. T., Steketee, M. C., Kebede, M. G., Janssen, H. L., & van Engers, T. M. (2025). *Lawful and accountable personal data processing with GDPR-based access and usage control in distributed systems*. arXiv. <https://doi.org/10.48550/arXiv.2503.07172>
88. van der Schyff, K., Prior, S., & Renaud, K. (2024). Privacy policy analysis: A scoping review and research agenda. *Computers & Security*, 146, Article 104065. <https://doi.org/10.1016/j.cose.2024.104065>
89. van Kolschooten, H. B. (2024). A health-conformant reading of the GDPR's right not to be subject to automated decision-making. *Medical Law Review*, 32(3), 373–391. <https://doi.org/10.1093/medlaw/fwae029>
90. Yang, E., & Beil, C. (2024). Ensuring data privacy in AI/ML implementation. *New Directions for Higher Education*, (207), 63–78. <https://doi.org/10.1002/he.20509>
91. Ye, X., & Zhang, Y. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Technological Forecasting and Social Change*. <https://doi.org/10.1016/j.techfore.2024.121234>
92. Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, 11, Article 1121. <https://doi.org/10.1057/s41599-024-03560-x>
93. Zhong, H., Do, T., Jie, Y., Neuwirth, R. J., & Shen, H. (2025). *Global AI governance: Where the challenge is the solution - An interdisciplinary, multilateral, and vertically coordinated approach*. arXiv. <https://doi.org/10.48550/arXiv.2503.04766>