

جامعة ميدأوشن

كلية العلوم الانسانية

قسم / تخصص ماجستير القانون الرقمي



عنوان البحث

النظام القانوني لحماية البيانات الشخصية في المملكة العربية السعودية في ظل التحول الرقمي: دراسة تحليلية

The Legal Framework for Personal Data Protection in the Kingdom of Saudi Arabia in the Context of Digital Transformation: An Analytical Study

إعداد الطالب/

مريم مشرد المطيري

إشراف/

عام من الجامعة

العام الدراسي:

2025

الملخص

يطمح هذا البحث إلى تقديم تحليل نقدي للنظام السعودي لحماية البيانات الشخصية الصادر عام 2021 ولائحته التنفيذية المُحدّثة سنة 2025، من أجل استكشاف مدى اتساقه مع المعايير الدولية وخاصة اللائحة الأوروبية العامة لحماية البيانات (GDPR) ومدى قدرته على ترسيخ الثقة الرقمية وتعزيز الابتكار. يعتمد العمل منهجاً وصفيّاً-تحليليّاً ذا شقين: تحليل وثائقي يقارن بنود النظام السعودي بمبادئ الخصوصية العالمية، ودراسة ميدانية تستطلع وعي طلاب كليات القانون في الجامعات السعودية واتجاهاتهم نحو الامتثال عبر استبانة إلكتروني موزّع على نطاق جغرافي ومؤسسي متنوّع. تُعالج البيانات باستخدام اختبارات وصفية واستدلالية لفحص الفروق بحسب الجامعة والمستوى الدراسي، مع الربط بين المعرفة القانونية والقصد السلوكي لتطبيق أحكام النظام مستقبلاً. ومن المنتظر أن تُظهر النتائج مكانة القوة الحالية مثل وضوح حقوق أصحاب البيانات وصرامة التزامات المعالجة إلى جانب ثغرات تتعلق بالموافقة المستنيرة ونقل البيانات عبر الحدود واستيعاب تقنيات الذكاء الاصطناعي. وتخلص الدراسة إلى توصيات عملية وتشريعية تساعد صنّاع القرار والمؤسسات التعليمية على تحسين حوكمة البيانات وتحفيز ثقافة الامتثال، بما يدعم أهداف التحول الرقمي في رؤية 2030.

الكلمات المفتاحية: حماية البيانات الشخصية، التحول الرقمي، النظام القانوني السعودي، اللائحة الأوروبية العامة لحماية البيانات، حوكمة البيانات، الامتثال التشريعي، الخصوصية الرقمية

فهرس المحتويات

2.....	الملخص.....
4.....	1. مقدمة:.....
5.....	2. مشكلة الدراسة:.....
6.....	3. أهمية الدراسة:.....
6.....	3.1 الأهمية العلمية (الأكاديمية).....
7.....	3.2 الأهمية العملية (التطبيقية).....
7.....	4. أهداف الدراسة:.....
8.....	5. تساؤلات الدراسة.....
9.....	6. فروض الدراسة:.....
9.....	7. المصطلحات العلمية.....
11.....	8. الدراسات السابقة:.....
11.....	8.1 الدراسات العربية:.....
12.....	8.2 الدراسات الإنجليزية:.....
15.....	8.3 التعقيب على الدراسات السابقة:.....
16.....	9. المنطلقات النظرية للدراسة:.....
17.....	10. المنهجية وطرق البحث:.....
18.....	10.1 أدوات الدراسة:.....
18.....	11. حدود الدراسة:.....
19.....	12. الجانب الأخلاقي.....
21.....	المراجع:.....
21.....	المراجع العربية:.....
21.....	المراجع الأجنبية:.....

يشهدُ العالمُ منذ مطلعِ الألفية الثالثة تحوُّلاً بنيويًا عميقًا في بنية الاقتصاد والإدارة؛ ذلك بفعل الثورة الرقمية التي أعادت رسم طرائق تقديم الخدمات وتبادل البيانات. ويُعرَّف التحوُّل الرقمي بأنَّه الانتقال من الأساليب التقليدية إلى التوظيف الشامل لتقنيات المعلومات والاتصالات في العمليات المؤسسية بهدف رفع الكفاءة والجودة (الشمراي، 2024). وتُظهر دراسةً تحليليةً سابقة أنَّ هذا التحوُّل يُسهم مباشرةً في تحسين سرعة اتخاذ القرار وتقليل التكاليف التشغيلية (Aljahdaly, 2020).

في السياق السعودي، أولت «رؤية 2030» محور الاقتصاد الرقمي اهتمامًا خاصًا؛ إذ أطلقت الدولة «برنامج التحوُّل الوطني» ضمن حزمة مبادرات تُعزِّز الاعتماد على البيانات والذكاء الاصطناعي في إدارة شؤون القطاعين العام والخاص، الأمر الذي يدعم التنافسية والتنوع الاقتصادي. (Khalaf, 2025) وقد أشار تقريرٌ صادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي SDAIA إلى أنَّ الاستثمار في البنية التحتية الرقمية ارتفع بمعدل سنوي مركَّب يزيد على 12 % منذ عام 2018، ما يؤكِّد التزام المملكة بتحويل اقتصادها إلى اقتصاد معرفي متكامل (SDAIA, 2025).

مع التوسع الكبير في استخدام المنصَّات الإلكترونية والتطبيقات الذكية، برزت حاجةً ملحةً لإطارٍ قانونيٍّ يُنظِّم التعامل مع البيانات الشخصية ويحفظ خصوصية الأفراد. استجابةً لذلك، صدر نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم م/19 بتاريخ 9 سبتمبر 2021، ودخل حيِّز النفاذ في 14 سبتمبر 2023. ويُعدَّ هذا النظام أول تشريع وطني شامل لحماية البيانات؛ إذ وضع حقوقًا واضحةً لأصحاب البيانات مثل الحق في الوصول والتصحيح والمحو، وفرض التزامات صارمةً على الجهات المُعالِجة تتعلَّق بالحصول على الموافقة المسبقة، واعتماد ضوابط أمنية ملائمة (Alzahrani, 2024) ولاحقًا، أصدرت SDAIA اللائحة التنفيذية المُحدَّثة لعام 2025 لتفصيل آليات الامتثال والإشراف بما يتماشى مع المعايير الدولية (Alkhamsi & Alqahtani, 2024).

تُشكِّل حماية الخصوصية الرقمية ركيزةً أساسيةً لبناء الثقة الرقمية التي يعتمد عليها نموُّ التجارة الإلكترونية وجذب الاستثمارات الأجنبية المباشرة. فقد أظهرت دراسةً ميدانيةً أنَّ الأطر التنظيمية الصارمة تُعزِّز موثوقية بيئة الأعمال الإلكترونية وتُوسِّع قاعدة المستخدمين داخل المملكة. (Alhoussari, 2025) كذلك، كشفت تحليلاتٌ قانونية أنَّ

التطوير المستمر لتشريعات الذكاء الاصطناعي والبيانات في السعودية يُسهم في ترسيخ العدالة الرقمية وتحفيز الابتكار، بما ينسجم مع أفضل الممارسات العالمية (Alhejaili, 2024).

انطلاقاً من هذه المعطيات، يسعى البحث الحالي إلى تحليل الإطار القانوني السعودي لحماية البيانات الشخصية في ظل التحول الرقمي، وتقويم مدى اتساقه مع المعايير الدولية، إضافة إلى قياس كفايته في صون الحقوق الرقمية وتعزيز التنمية الاقتصادية.

2. مشكلة الدراسة:

شهدت المملكة العربية السعودية في السنوات الأخيرة طفرة رقمية مدفوعة بـ«رؤية 2030»، تمثلت في تبني سياسات وطنية تعزز التحول الرقمي وتوسع نطاق استخدام التقنيات الذكية في مختلف القطاعات. وقد أسهم هذا التحول في تحسين الكفاءة التشغيلية وتعزيز الابتكار في مجالات كالصحة، والتعليم، والمالية، إلا أن هذه الثورة الرقمية أدت في المقابل إلى تعاظم التحديات المرتبطة بحماية البيانات الشخصية وضمان الخصوصية الرقمية (Khalaf, 2025).

ففي ظل تزايد الاعتماد على المنصات الإلكترونية، ومع تنامي استخدام الذكاء الاصطناعي والتحليلات الضخمة، برزت الحاجة إلى إطار قانوني فعال يوازن بين الابتكار وحماية الحقوق الرقمية. وعلى الرغم من إصدار «نظام حماية البيانات الشخصية» عام 2021 ودخوله حيز التنفيذ في 2023، إلا أن الدراسات تشير إلى وجود ثغرات في التطبيق العملي، خاصة فيما يتعلق بتحديد المسؤوليات بين الجهات المعالجة للبيانات، وآليات الحصول على الموافقة، وتقييم المخاطر المرتبطة بنقل البيانات عبر الحدود (Alzahrani, 2024).

أظهرت دراسة حديثة أن التحديات التقنية مثل غموض المصطلحات القانونية، وصعوبة ترجمة التشريعات إلى ممارسات تقنية واضحة، تعرقل الامتثال الكامل للقانون، وهو ما قد يؤدي إلى ضعف ثقة الأفراد والمؤسسات في البيئة الرقمية (Alkhamsi & Alqahtani, 2024). ويدعم ذلك ما أشار إليه (Alhoussari, 2025) من أن نقص التكامل بين الأطر التقنية والتنظيمية يُعد من أبرز المعوقات التي تهدد أمن البيانات، خاصة في القطاعات الحيوية كالصحة والتعليم (Alhoussari, 2025).

كما بيّنت دراسة (Alhejaili, 2024) أن البيئة التشريعية في المملكة، رغم تطورها، لا تزال تفتقر إلى المرونة الكافية لمواكبة التطورات التكنولوجية المتسارعة، خصوصًا فيما يتعلق بالتجارة الإلكترونية وحوكمة البيانات (Alhejaili, 2024). وهذا ما يتقاطع مع ما ذكره Al-Ruithe و (2017) Benkhelifa حول أن حوكمة البيانات في السعودية لا تزال في مراحلها الأولية، مما يُضعف قدرة المؤسسات على الالتزام الفعلي بالتشريعات الجديدة (Al-Ruithe & Benkhelifa, 2017). بناءً عليه، تتمثل المشكلة البحثية في تحليل كفاءة وفعالية الإطار القانوني السعودي لحماية البيانات الشخصية في ظلّ التحوّل الرقمي، وتقصّي مدى قدرته على تحقيق توازنٍ عمليّ بين تشجيع الابتكار الرقمي من جهة، وصّون الحقوق الرقمية للأفراد والمؤسسات من جهة أخرى، مع مقارنته بأفضل الممارسات العالمية.

3. أهمية الدراسة:

3.1 الأهمية العلمية (الأكاديمية)

تكتسب الدراسة أهمية علمية إضافية في ضوء ما أشارت إليه أبحاث حديثة حول دور الأطر التنظيمية في تعزيز حوكمة البيانات والابتكار الرقمي في البيئات الخليجية. فقد أوضحت دراسة مقارنة أن مواءمة التشريعات الوطنية مع المبادئ الدولية للخصوصية مثل اللائحة الأوروبية العامة لحماية البيانات (GDPR) يعزز الامتثال القانوني ويحفّز بناء الثقة في التحوّل الرقمي. (Alharthi & Walters, 2021) كما أكدت أبحاث أخرى أن نقص الأدبيات المعيارية المقارنة في العالم العربي يمثل فجوة بحثية مهمة تستدعي تقديم دراسات نقدية تستند إلى أسس منهجية واضحة وتقارن بين نماذج الحوكمة المختلفة. (Walters & Alharthi, 2023) كذلك، أشارت مراجعة دولية حديثة إلى أن بناء إطار مفاهيمي لدراسة نضج حوكمة البيانات يساعد على تطوير سياسات أكثر كفاءة في إدارة البيانات وضمان حماية الحقوق الفردية في البيئات الرقمية الناشئة. (Ullah et al., 2022)

انطلاقًا من هذه الخلفية، تبرز أهمية الدراسة الحالية في كونها تتناول نظام حماية البيانات الشخصية السعودي في لحظة مفصلية من مسار التحوّل الرقمي الوطني، وتقدّم تحليلًا نقديًا معمقًا لبنود النظام ولائحته التنفيذية في ضوء المعايير العالمية. فهي لا تكتفي بمقارنة النصوص التشريعية، بل تسعى إلى بلورة إطار مفاهيمي يوضح كيفية مواءمة التشريعات الوطنية مع التزامات الخصوصية الدولية، ويقدم تصورًا علميًا يمكن توظيفه في بناء سياسات متوازنة

تحقق التقدم التقني دون الإخلال بحقوق الأفراد. ومن هنا، فإن نتائج الدراسة من شأنها أن تثري الأدبيات العربية وتسد الفجوة البحثية، وتوفّر أساساً علمياً للأبحاث المستقبلية حول العدالة الرقمية والامتثال التشريعي ونضج حوكمة البيانات في البيئات التقنية الناشئة.

3.2 الأهمية العملية (التطبيقية)

بيّنت دراسات متخصصة أن تبني ممارسات «الخصوصية بالتصميم» يساهم في رفع جاهزية المؤسسات للامتثال، ويزيد قدرتها على إدارة المخاطر المرتبطة بتدفقات البيانات العابرة للحدود (Wende, 2021) كما أوضحت أبحاث مقارنة في سياق دول الخليج أن وجود لوائح تنفيذية واضحة وإرشادات معيارية لصنّاع القرار يمثل ركيزة أساسية لضمان التطبيق الفعّال للتشريعات الجديدة وحماية الحقوق الرقمية للأفراد (Alharthi & Walters, 2021) وأظهرت دراسة أخرى أن الوعي المؤسسي بحقوق البيانات وتدريب مسؤولي حماية البيانات بشكل مستمر يعدان من العوامل الحاسمة لترسيخ بيئة رقمية آمنة ومحفزة على الابتكار (Walters & Alharthi, 2023).

في ضوء هذه النتائج، تنبع الأهمية العملية للدراسة الحالية من قدرتها على تقديم خارطة طريق تنفيذية للجهات المعنية بحماية البيانات الشخصية في المملكة العربية السعودية. فهي تسلط الضوء على الثغرات والتحديات التي تواجه المؤسسات عند الامتثال للنظام الجديد، وتقترح آليات واقعية لتطوير إجراءات الموافقة وإدارة المخاطر ونقل البيانات عبر الحدود. كما توفّر الدراسة إطاراً إرشادياً يمكن للجهات الرقابية استخدامه لتصميم أدوات التقييم والإشراف، وتساعد الشركات على تبني ممارسات الخصوصية بالتصميم لتعزيز الثقة الرقمية وتحقيق ميزة تنافسية مستدامة. وعلى المستوى المجتمعي، ترفع الدراسة مستوى الوعي بحقوق الأفراد الرقمية وتدعم برامج التدريب والتوعية، بما يسهم في بناء بيئة رقمية آمنة ومحفزة للاستثمار والابتكار.

4. أهداف الدراسة:

- تحليل نصوص نظام حماية البيانات الشخصية السعودي ولوائحه التنفيذية لعام 2025 لتحديد نطاق الحماية الذي يوفره ومواضع التركيز فيه في سياق التحوّل الرقمي الوطني.

- مقارنة الأحكام الرئيسية للنظام بأهم المعايير والممارسات الدولية الرائدة في خصوصية البيانات، ولا سيما اللائحة العامة لحماية البيانات الأوروبية، للكشف عن نقاط الالتقاء والاختلاف.
- تقييم مستوى الامتثال الفعلي لأحكام النظام في القطاعات الرقمية الحيوية داخل المملكة مثل الصحة والتجارة الإلكترونية والخدمات المالية وبيان أثر ذلك على ثقة المستخدمين والفاعلية التنظيمية.
- تحديد الفجوات التشريعية أو الإجرائية التي قد تقلل من كفاءة النظام في مواجهة التحديات التقنية الحديثة، خصوصاً في المسائل المتعلقة بالموافقة المسبقة ونقل البيانات عبر الحدود والأمن السيبراني.
- وضع توصيات تشريعية وتنفيذية عملية تهدف إلى تعزيز توازن الإطار القانوني بين دعم الابتكار الرقمي وصون الحقوق الشخصية، مع اقتراح آليات متابعة لقياس مدى تحقق هذه التوصيات مستقبلاً.

5. تساؤلات الدراسة

1. إلى أي مدى يُؤقّر نظام حماية البيانات الشخصية السعودي، مع لائحته التنفيذية لعام 2025، حمايةً شاملةً وفعالةً للبيانات الشخصية في ظل التحوّل الرقمي المتسارع داخل المملكة؟
2. ما أوجه الاتفاق والاختلاف الجوهرية بين الأحكام الرئيسية للنظام السعودي واللائحة العامة لحماية البيانات الأوروبية (GDPR) فيما يتعلق بحقوق أصحاب البيانات، والتزامات جهات المعالجة، وآليات نقل البيانات عبر الحدود؟
3. ما مستوى امتثال القطاعات الرقمية الحيوية في المملكة ولا سيما الصحة، التجارة الإلكترونية، والخدمات المالية لمتطلبات النظام، وكيف ينعكس هذا الامتثال على ثقة المستخدمين وفاعلية الحوكمة الرقمية؟
4. ما أبرز الفجوات التشريعية أو الإجرائية التي تعوق التطبيق الكامل للنظام، خصوصاً فيما يخص الحصول على الموافقة المستنيرة، والأمن السيبراني، ونقل البيانات خارج الحدود الوطنية؟
5. ما التوصيات التشريعية والتنفيذية القابلة للتطبيق التي يمكن أن تعزّز قدرة النظام على تحقيق التوازن بين دعم الابتكار الرقمي وصون الحقوق الشخصية، وكيف يمكن قياس أثر تلك التوصيات مستقبلاً؟

6. فروض الدراسة:

1. وجود فجوات ملموسة في أحكام الموافقة المسبقة ونقل البيانات خارج الحدود يحدّ من قدرة نظام حماية البيانات الشخصية السعودي على تحقيق حماية شاملة للبيانات في بيئة التحوّل الرقمي.
2. تختلف درجة الامتثال لأحكام النظام بين القطاعات الرقمية الحيوية، بحيث يحقق قطاع الخدمات المالية أعلى مستوى امتثال مقارنة بقطاعي الصحة والتجارة الإلكترونية.
3. يرتبط ازدياد درجة الامتثال المؤسسي لأحكام النظام بارتفاع ثقة المستخدمين في التعاملات الرقمية.

7. المصطلحات العلمية

1. النظام القانوني لحماية البيانات الشخصية

يعرف النظام القانوني بأنه: "مجموعة متناسقة من القواعد التي تتأتى من مصادر مرتبطة على نحو تدريجي، وتستلهم نفس المجموعة من المبادئ، وذات الرؤية للحياة والعلاقات داخل الوحدة الاجتماعية التي يجب أن تحكمها" (سمير وعمار، 2010، ص 69).

التعريف الإجرائي:

النظام القانوني لحماية البيانات الشخصية يُقصد به في هذا البحث جميع الأحكام الملزمة الواردة في نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي م/19 (9 سبتمبر 2021) ولائحته التنفيذية المحدثة لعام 2025؛ ويُترجم هذا المفهوم إلى بيانات قابلة للتحليل عبر ترميز كل مادة من مواد النظام واللائحة على جدول يربطها بثمانية مبادئ خصوصية دولية (الإخطار، الموافقة، تحديد الغرض، تقليل البيانات، الدقة، الأمن، حدّ الاحتفاظ، المساءلة)، ثم تقدير مستوى تحقق كل مبدأ على مقياس ثلاثي (متوافر، متوافر جزئياً، غير متوافر) وحساب «مؤشر امتثال» كُلي يُعبّر عن نسبة المواد التي تطبّق المبدأ على نحو كامل، لتكون قيمة هذا المؤشر هي المتغيّر الكمي الذي يدخل نماذج التحليل.

2. التحوّل الرقمي

يعرف التحول الرقمي بأنه: "عملية إعادة تصميم الأنشطة والأعمال والإجراءات والعمليات والخدمات وتحويلها إلى عمليات رقمية إلكترونية باستخدام تكنولوجيا المعلومات لتحقيق الاستفادة من الواقع الرقمي في جميع جوانب الأعمال". (إبراهيم، 2023، ص 140)

التعريف الإجرائي:

التحول الرقمي يُعرّف إجرائياً على أنه درجة الاعتماد الفعلي على العمليات والخدمات الإلكترونية في القطاعات السعودية الحيوية المشمولة بالبحث (الصحة، التجارة الإلكترونية، الخدمات المالية) خلال الفترة 2023–2025؛ ويُقاس ذلك برصد ثلاثة مؤشرات لكل قطاع (نسبة المعاملات المؤتمتة، وجود منصة رقمية مرتبطة ببيانات المستخدمين، حجم الاستثمار المُعلن في البنية الرقمية)، وترمز كل مؤشر على مقياس رباعي من «منخفض» إلى «مرتفع جداً»، ثم حساب متوسط مركّب (Digital Transformation Score) يُمثّل مستوى التحول الرقمي لكل قطاع ويُستخدم في اختبار علاقته بمتغيرات الامتثال القانوني وثقة المستخدمين.

3. حوكمة البيانات

يمكن تعريف حوكمة البيانات بأنها: "النظام الذي يوفر العمليات، والضوابط التي تضمن صحة البيانات التي تجمعها الجهة، وتضمن دقتها، وتفردتها، وريادتها – باعتبار البيانات مدخلات لنظم عمل الجهة... –؛ وذلك كله لضمان صلاحية البيانات المقدمة للجهة، ومصداقيتها؛ لاتخاذ القرارات السليمة فيما يخص كل أنشطة الجهة" (اللبان، 2021، ص 242).

التعريف الإجرائي:

حوكمة البيانات تُعرّف في إطار الدراسة بأنها منظومة العمليات والضوابط التنظيمية التي تتبنّاها الجهات المعالجة للبيانات لضمان صحتها ودقتها وأمنها وشرعيتها وفقاً لمتطلبات نظام PDPL؛ وتُقاس عبر أداة مزدوجة تتألف من استبيان موجّه لمسؤولي حماية البيانات (DPOs) يتضمن عشرين بنداً تغطي سياسات الاحتفاظ بالبيانات وتحديثها، تقييم الأثر، تعيين DPO، وآليات التبليغ عن الاختراقات، بحيث يُقيّم كل بند بمقياس ليكرت خماسي، إضافة إلى مطابقة وثائقية لسياسات الخصوصية الداخلية للتحقق من وجود عناصر الحوكمة فعلياً. تُجمع درجات الاستبيان والمطابقة

في «مؤشر حوكمة بيانات» من مئة نقطة تُصنّف المنشآت بموجبه إلى «منطبقة»، «منطبقة جزئياً»، أو «غير منطبقة»، ومن ثم يُستخدم هذا المؤشر الرقمي في التحليلات الإحصائية والاختبارات الفرضية.

8. الدراسات السابقة:

8.1 الدراسات العربية:

الأطر القانونية لحماية المستهلك في عقود التجارة الإلكترونية في المملكة العربية السعودية: دراسة تحليلية مقارنة بالنظام الأمريكي.

نُشرت هذه الدراسة في مجلة قطاع الشريعة والقانون، وهدفت إلى تحليل الإطار القانوني المنظم لعقود التجارة الإلكترونية في السعودية، مع التركيز على حقوق المستهلك وحماية البيانات الشخصية. أبرزت الدراسة أوجه القصور التشريعي قبل صدور نظام حماية البيانات الشخصية، وأشارت إلى أن النظام السعودي لا يزال بحاجة إلى مزيد من التحديث ليتواءم مع تطور التجارة الرقمية. وأوصى الباحث بإدراج مبادئ أكثر دقة حول حماية البيانات في البيئة الإلكترونية، وزيادة التوعية القانونية للمستهلكين بحقوقهم الرقمية (الشمrani، 2024).

تأثير استخدام الذكاء الاصطناعي على القواعد الدستورية والإدارية في النظام السعودي.

تناولت هذه الدراسة العلاقة بين تطور أدوات الذكاء الاصطناعي وتنظيم الحقوق الرقمية في المملكة، خاصةً من زاوية حماية البيانات الشخصية. توصل الباحثان إلى أن استخدام الذكاء الاصطناعي يتطلب تطويراً جذرياً في القواعد الدستورية والإدارية، بحيث تُراعى حقوق الأفراد في بيئة رقمية متسارعة. وقد أشادا بإصدار نظام حماية البيانات الشخصية عام 2021، لكنه، بحسب الدراسة، ما يزال بحاجة إلى لوائح تنظيمية تتناسب مع استخدامات الذكاء الاصطناعي. من أبرز التوصيات: تعديل بعض مواد النظام الأساسي للحكم لتضمين حماية الخصوصية كحق دستوري، وتعزيز الإشراف الرقابي على الشركات التقنية (المحيا والسيد، 2025).

التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي بسبب انتهاك الخصوصية والهجمات السيبرانية في المملكة العربية السعودية

تناولت هذه الدراسة أثر الانتهاكات المتكررة للخصوصية والهجمات السيبرانية على ثقة الجمهور في الإعلام الرقمي بالمملكة. وقد خلصت إلى أن ضعف السياسات المنظمة لحماية البيانات الشخصية يُعد من أبرز أسباب تآكل الثقة الرقمية، خاصة في منصات التواصل والإعلام الرقمي. كما كشفت أن قلة وعي المستخدمين بحقوقهم الرقمية تُضاعف من حجم المخاطر. أوصى الباحث بضرورة تفعيل نصوص نظام حماية البيانات السعودي من خلال إجراءات تنفيذية أكثر صرامة، وتأسيس حملات وطنية لرفع الوعي بأهمية الخصوصية الرقمية (كلنتن، 2024).

فعالية الخدمات الاجتماعية الرقمية في أوقات الأزمات: منظور شامل بين التكنولوجيا والإكلينيك – دراسة حالة على المملكة العربية السعودية من 2019 حتى 2024

تتناول هذه الدراسة العلاقة بين التحوّل الرقمي للخدمات الاجتماعية ومستوى حماية البيانات الشخصية خلال الأزمات مثل جائحة كورونا. أظهرت النتائج أن تسريع التحول الرقمي لم يكن مصحوبًا ببنية تنظيمية قوية لحماية البيانات، مما أدى إلى تخوّف المستخدمين من الإفصاح عن معلوماتهم. ركّزت الدراسة على تطبيقات مثل «توكلنا» و«تباعد»، وأوصت بضرورة تضمين إجراءات حماية الخصوصية ضمن تصميم المنصات الرقمية الحكومية منذ البداية، وتدريب الكوادر العاملة على التعامل القانوني مع البيانات (الفحطاني، 2025).

8.2 الدراسات الإنجليزية:

في الدراسة الموسومة "Securing Health Data in the Digital Age: Challenges, Regulatory Frameworks, and Strategic Solutions in Saudi Arabia" (Alhoussari, 2025)، والمنشورة في Journal of Ecohumanism، يُقيّم الباحث التحديات السيبرانية والتشريعية في نظم إدارة البيانات الصحية بالسعودية، مقارنةً بين نظام حماية البيانات الشخصية (PDPL) والمعايير الدولية مثل GDPR و HIPAA. اعتمدت الدراسة منهجًا مقارنةً للقوانين بهدف وضع توصيات تنظيمية وتكنولوجية لتحسين الحوكمة والامتثال. تُفيد هذه النتائج البحث الحالي إذ تبرهن على مدى كفاية PDPL في القطاعات الحساسة خلال التحول الرقمي، مع إبراز النقاط التي تتطلب تعزيزًا تشريعيًا أو تقنيًا.

أما دراسة (Al-Khalifa et al., 2023) "The Saudi Privacy Policy Dataset" المنشورة في ArXiv، فتقدّم مجموعة بيانات موسعة تتضمن 1000 سياسة خصوصية من مواقع إلكترونية سعودية مصنفة وفق عشرة مبادئ رئيسية

للخصوصية. تهدف هذه المجموعة إلى دعم تطوير نماذج الذكاء الاصطناعي لرصد الامتثال وتحليل ممارسات حماية البيانات، ما يسهل تقييم مستويات الشفافية والالتزام عبر مختلف القطاعات.

أما دراسة "Developing a Blockchain-Based Digitally Secured Model for the Educational Sector in Saudi Arabia toward Digital Transformation" (Alangari et al., 2022) المنشورة في PeerJ Computer Science، فتركز على تصميم نموذج رقمي مؤمن بتكنولوجيا البلوكشين لتوثيق والتحقق من الشهادات الأكاديمية. وقد بينت الدراسة أن النموذج المقترح يعزز الأمان ويقلل مخاطر التلاعب بالبيانات التعليمية، بما يدعم التحول الرقمي المستدام.

أما دراسة "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation" (Johri & Kumar, 2023) المنشورة في Human Behavior and Emerging Technologies، فتستعرض مستويات وعي عملاء البنوك في السعودية بمخاطر الأمن السيبراني ورضاهم عن تدابير الحماية. وأوضحت الدراسة أن تعزيز الوعي بالتصيد والهجمات الإلكترونية يزيد ثقة العملاء في الخدمات المصرفية الرقمية.

أما دراسة "COVID-19 and the Digital Transformation that Followed in the Kingdom of Saudi Arabia" (Alomar et al., 2023) المنشورة في Academic Journal of Research and Scientific Publishing، فتستعرض أثر جائحة كوفيد-19 في تسريع تبني الحلول الرقمية بالمملكة في مجالات مثل العمل والتعليم والصحة. وتوصي الدراسة باستمرار الاستثمار في البنية التحتية الرقمية وتعزيز الوعي الأمني لحماية البيانات الشخصية.

أما دراسة "Nudging Data Privacy of Mobile Health Applications in Saudi Arabia" (Sabur & Showail, 2024) المنشورة في International Journal of Information Security and Privacy، فتقوم بتقييم امتثال تطبيقات الصحة الإلكترونية في المملكة العربية السعودية لمتطلبات نظام حماية البيانات الشخصية (PDPL). كشفت الدراسة أن مستويات الامتثال متفاوتة بشكل ملحوظ بين التطبيقات، مما يبرز الحاجة لتطوير استراتيجيات حماية خصوصية المستخدمين وتعزيز التدابير التقنية والقانونية ذات الصلة.

أما دراسة "Compliance Framework for Personal Data Protection Law Standards" (Alkhamsi & Alqahtani, 2024) المنشورة في International Journal of Advanced Computer Science and Applications، فتطوّر نموذج امتثال قانوني-تقني يترجم متطلبات PDPL إلى ممارسات حوكمة بيانات قابلة للتنفيذ. واختبر الباحثان النموذج من خلال دراسة حالة استعملت نماذج ذكاء اصطناعي لرصد الثغرات التنظيمية في مواقع سعودية، فأظهر كفاءة عالية في اكتشاف عدم التوافق. تمكّن هذه النتائج من فهم التحديات التقنية للتنفيذ وتدعم الجهد التحليلي في البحث الحاضر حول قابلية PDPL للتطبيق العملي.

وفي ورقته "An Overview of AI Data Protection in the Context of Saudi Arabia" (Alzahrani, 2024)، المنشورة في International Journal for Scientific Research، يتناول الباحث التقاطع بين الذكاء الاصطناعي وحماية البيانات داخل المملكة، محللاً مدى اتساق PDPL مع الأطر الأوروبية ومناقشاً المخاطر الأخلاقية المرتبطة بالانحياز الخوارزمي وسوء استخدام البيانات. تُبرز هذه الدراسة أهمية التنبّه إلى جاهزية التشريع السعودي لمواجهة التطورات التقنية السريعة، وهو محور يعزّز أهداف البحث الراهن بشأن ملاءمة PDPL للمستقبل.

تقدّم دراسة "A Comparative Analysis: Health Data Protection Laws in Malaysia, Saudi Arabia and EU" (Sarabdeen & Ishak, 2024) الصادرة في International Journal of Law and Management، تحليلاً مقارناً باستخدام منهج المحتوى القانوني لقياس مدى توافق قوانين حماية البيانات الصحية في السعودية مع متطلبات GDPR، خصوصاً ما يتعلق بنقل البيانات وتقييم ملاءمة الحماية. توفّر هذه المقارنة بُعداً دولياً يدعم تقييم البحث الحالي للفجوات والقدرات داخل القطاع الصحي السعودي.

أما مقال "Restrictive Approach to Data Protection in the GCC: Is the EU GDPR a Potential Inspiration?" (Haidar, 2024)، المنشور في Global Journal of Comparative Law، فيحلّل تطوّر تشريعات حماية البيانات في دول مجلس التعاون، مبيناً أثر مبادئ GDPR في تشكيل أنظمتها الحديثة، ومن ضمنها PDPL. يقدم المقال إطاراً مقارناً إقليمياً يُعين على قياس مدى تماهي النظام السعودي مع المعايير الدولية ومع قوانين الجوار الخليجية.

أخيراً ترصد دراسة "Cross-Border Data Transfer Between the GCC Data Protection Laws and the GDPR" (Alhababi, 2024)، المنشورة في Global Journal of Comparative Law، آليات نقل البيانات الشخصية عبر الحدود

في تشريعات الخليج مقارنة بمتطلبات الملاءمة في GDPR ، كاشفة عن فجوات تنظيمية وتحديات في التنفيذ. تضيق هذه النتائج منظورًا حاسمًا للبحث الحالي فيما يخص قدرة PDPL على دعم التدفقات الآمنة للبيانات في النظام الرقمي العالمي.

8.3 التعقيب على الدراسات السابقة:

تبرز الأدبيات العربية والإنجليزية حول حماية البيانات في المملكة العربية السعودية صورةً ثرية في ظاهرها، لكنها تكشف عند القراءة المتقاطعة عن فجوات منهجية وتطبيقية ما تزال بحاجة إلى استكمال. فقد ركزت الدراسات العربية مثل الشمراني (2024) والمحيا والسيد (2025) على تحليل نصوص الأنظمة القائمة واستجلاء أوجه القصور فيها، إلا أن اعتمادها الرئيس على المنهج الوصفي-التحليلي حصر نتائجها في التوصيات النظرية دون اختبار ميداني لفاعلية أحكام نظام حماية البيانات الشخصية بعد صدور لوائحه التنفيذية. وفي السياق ذاته، ناقش كلنتن (2024) أثر انتهاكات الخصوصية والهجمات السيبرانية على ثقة الجمهور، غير أنه استند إلى استقراء حالات نشر إعلامي بدل قياسات كمية فعلية لمستوى الثقة، ما يترك فراغًا في الأدلة التجريبية.

على الجانب الآخر، قدمت بعض الدراسات الإنجليزية حلولًا تطبيقية جزئية؛ إذ طوّر Alkhamisi و Alqahtani (2024) نموذج امتثال يترجم متطلبات النظام إلى آليات تقنية وقانونية ثم اختبراه على عينة محدودة من المواقع السعودية، بينما قارن Alhoussari (2025) و Ishak & Sarabdeen (2024) الإطار السعودي بنظم دولية كـ GDPR و HIPAA مع تركيز واضح على القطاع الصحي. ومع أن هذه الجهود تسد ثغرة في الاختبارات الميدانية، فإن انحصارها في قطاع الرعاية الصحية أو الخدمات الحكومية يترك تساؤلات جوهرية حول جاهزية النظام لحماية البيانات في قطاعات تجارية ناشئة مثل التجارة الاجتماعية أو سلاسل التوريد القائمة على إنترنت الأشياء، وهي قطاعات لم تنل حظًا وافرًا من البحث.

يتفق معظم الباحثين على أن فجوة الوعي الرقمي تمثل عقبة أساسية أمام فاعلية النظام، فتتكرر الدعوات إلى حملات تثقيفية وتشديد الرقابة، لكن التحليل المقارن الذي قدّمه Haidar (2024) يوضح أن محاكاة نموذج GDPR دون مواءمة ثقافية قد تحدّ من فاعلية تلك الحملات. أما فيما يتعلق بالذكاء الاصطناعي، فيتباين الباحثون بين من يرى أن نظام حماية البيانات الحالي كافٍ نظريًا ويحتاج لوائح تفصيلية، ومن يرى أنه قاصر بنيويًا عن استيعاب مخاطر

الخوارزميات؛ ما يعكس افتقار الساحة البحثية إلى مؤشرات قياس واضحة لتأثير تطبيقات الذكاء الاصطناعي في بيئات سعودية حقيقية.

أخيراً، ورغم دعوة بعض الأدبيات إلى ترسيخ الحق في الخصوصية داخل النظام الأساسي للحكم وتطوير مسارات دستورية واضحة، فإنها لا تعرض خطوات إصلاحية تفصيلية، وتظل آليات الإنفاذ وجسور التقاضي المتخصصة غائبة عن النقاش. من ثم، يمكن القول إن الدراسات السابقة توفر أساساً نظرياً غنياً لكنها موزعة قطاعياً ومحدودة زمنياً وتجريبياً، الأمر الذي يبرر تبني البحث الراهن إطاراً تكاملياً يجمع بين التحليل المقارن، والقياس الميداني للامتثال، واستشراف الأبعاد الثقافية والدستورية، بما يسد هذه الفجوات ويقدم خارطة طريق عملية لحوكمة بيانات تتسق مع أهداف رؤية 2030 ومعايير الخصوصية العالمية.

9. المنطلقات النظرية للدراسة:

ترتكز هذه الدراسة على مجموعة من المنطلقات النظرية التي تُشكل الإطار المعرفي لفهم الإشكالات القانونية والتنظيمية المرتبطة بحماية البيانات الشخصية في سياق التحول الرقمي بالمملكة العربية السعودية ودول الخليج. وتبدأ هذه المنطلقات من مفهوم الحوكمة الرقمية، الذي يُعنى بكيفية تنظيم العلاقة بين الدولة والمواطن في البيئة الرقمية، من خلال أدوات الشفافية والمساءلة والامتثال التشريعي. وتفترض الأدبيات أن وجود إطار قانوني قوي لحوكمة البيانات يعزز من ثقة الأفراد ويُسهّم في تحقيق الاستقرار القانوني في بيئة رقمية متغيرة (Alhejaili, 2024).

كما تنطلق الدراسة من فكرة الخصوصية كحق أساسي، وهو مبدأ جوهري في التشريعات الدولية مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR)، وقد بدأت دول الخليج، لا سيما المملكة العربية السعودية، في تضمينه ضمن تشريعاتها مثل نظام حماية البيانات الشخصية. تشير الدراسات إلى أن الاعتراف القانوني بالخصوصية الرقمية يُمثل نقطة تحول في علاقة الدولة بالمجتمع الرقمي، ويعزز من قدرة الأفراد على التحكم في بياناتهم (Sarabdeen & Ishak, 2024).

في هذا السياق، تستند الدراسة إلى نظرية الامتثال التنظيمي، التي ترى أن فعالية أي نظام قانوني تعتمد على قابليته للتطبيق من قبل المؤسسات العامة والخاصة، ومدى وضوحه وقابليته للتحول إلى آليات تقنية. وتؤكد الأدبيات أن

المؤسسات في السعودية تواجه تحديات في تطبيق PDPL ، تتعلق بعدم وضوح المفاهيم القانونية وصعوبة الترجمة التقنية للالتزامات القانونية، وهو ما يؤثر على كفاءة الامتثال (Alkhamsi & Alqahtani, 2024).

وتُبنى الدراسة أيضًا على المنهج المقارن في التشريع، الذي يُتيح تقييم الفعالية القانونية لنظام حماية البيانات السعودي من خلال مقارنته باللائحة الأوروبية (GDPR) والتشريعات الخليجية الأخرى، بما يكشف عن نقاط القوة والقصور. وقد بينت دراسات حديثة أن الإطار القانوني في السعودية يستلهم العديد من مبادئ GDPR ، إلا أنه يواجه تحديات تتعلق بالتنفيذ العملي، خاصة فيما يخص نقل البيانات عبر الحدود وحقوق النسيان والموافقة الصريحة (Alhababi, 2024).

وفي ضوء الاقتصاد الرقمي المتسارع، تستند الدراسة إلى نظرية الاقتصاد الرقمي المبني على الثقة، التي ترى أن حماية البيانات ليست مجرد مطلب قانوني، بل شرط أساسي لازدهار التجارة الإلكترونية وجذب الاستثمارات وتعزيز الابتكار. وقد أكدت دراسات ميدانية أن التزام المؤسسات بحماية الخصوصية الرقمية يعزز من ثقة المستخدمين ويُعد عاملاً محوريًا في نجاح البيئة الرقمية (Alhoussari, 2025).

وتُختتم المنطلقات النظرية بالاعتماد على نظرية التقاطع بين الأمن السيبراني والتشريع، التي ترى أن الفصل بين التشريعات الأمنية وأنظمة حماية البيانات يضعف من فاعلية كلا الجانبين. فالتشريعات يجب أن تُصمم بحيث تكون متوافقة تقنيًا مع نظم الحماية، وأن تدعم حلولاً تكنولوجية تعزز من تطبيق القانون بشكل فعلي، خاصة في بيئات عالية الحساسية كالقطاع الصحي والمالي (Alzahrani, 2024).

10. المنهجية وطرق البحث:

اعتمدت هذه الدراسة على المنهج الوصفي-التحليلي، لأنه الأنسب لاستقصاء مستوى الوعي القانوني والاتجاهات السلوكية لدى طلاب كليات القانون في الجامعات السعودية تجاه نظام حماية البيانات الشخصية الصادر عام 2021 ولائحته التنفيذية المُحدّثة سنة 2025. ويُعدّ هؤلاء الطلاب مجتمع البحث المقصود، إذ يُمثّلون الجيل المهني المقبل المعني بتطبيق التشريع وتأويله داخل الجهات الحكومية والخاصة (Issan et al., 2014).

بعد جمع الاستجابات، تُعالج البيانات باستخدام برنامج إحصائي مناسب لاستخراج المتوسطات والانحرافات المعيارية واختبارات الفروق (مثل t-test أو ANOVA) بحسب متغيرات الجنس والمستوى الدراسي ونوع الجامعة، مع فحص علاقات الارتباط بين المعرفة والاتجاهات والقصد السلوكي (Bin Shihah et al., 2022). وتُفسَّر النتائج في ضوء الإطار التشريعي السعودي والمراجعات المقارنة الواردة في القسم النظري، بما يتيح تقديم توصيات تستند إلى أدلة ميدانية خالصة من واقع طلاب القانون السعوديين دون افتراضات رقمية غير واردة في المعطيات (Huang et al., 2023).

10.1 أدوات الدراسة:

سوف تُجمَع البيانات بواسطة استبيان إلكتروني يُوزَع عبر المنصّات الجامعية الرسمية بعد الحصول على الموافقات اللازمة من الكليات المعنية ولجان أخلاقيات البحث. يتكوّن الاستبيان من أربعة محاور متتالية على مقياس ليكرت خماسي:

1. بيانات تعريفية مختصرة تسمح بوصف العينة دون المساس بهويّة المشاركين،
2. معرفة الطالب بالمفاهيم الجوهرية للنظام وأبرز التزامات الجهات الخاضعة له،
3. الاتجاهات نحو مدى كفاية الحماية التي يوفّرها التشريع في سياق التحول الرقمي،
4. القصد السلوكي المستقبلي للمشاركة في ترسيخ ثقافة الخصوصية والامثال.

سيُنْتَقَى المشاركون بطريقة ملائمة للظروف الميدانية: تُوجّه الدعوات إلى جميع طلبة برامج القانون في الجامعات الحكومية والأهلية، ويُسمَح بالاشتراك الطوعي عبر رابط واحد موحّد. يتيح هذا الإجراء الوصول إلى تمثيل جغرافي ومؤسسي متنوّع مع تركّ تحديد الحجم النهائي للعينة لما يُستجاب فعليّاً؛ ويُقيّم لاحقاً مدى كفاية ذلك الحجم وفق معايير الإحصاء الاستدلالي

11. حدود الدراسة:

تنحصر هذه الدراسة زمنياً في الفترة من عام 2025 إلى نهاية 2026؛ إذ تستند إلى النص النهائي لللائحة التنفيذية الصادرة في 2025 وتتابع آثار تطبيقها خلال عام لاحق لرصد أية تعديلات أو استدراقات تنظيمية قد تظهر أثناء التنفيذ الفعلي.

أما على المستوى المكاني، فتقتصر التحليلات على المملكة العربية السعودية، مع التركيز على القطاعات الرقمية الحيوية داخل نطاقها القانوني؛ ولا تمتد نتائج البحث إلى دول مجلس التعاون أو أي منظومات تشريعية أخرى إلا في سياق المقارنة المعيارية فحسب.

موضوعياً، تنحصر الدراسة في الإطار النظامي لحماية البيانات الشخصية وما يرتبط به من حقوق أصحاب البيانات، والتزامات جهات المعالجة، وآليات نقل البيانات عبر الحدود. لا تشمل الدراسة قوانين الأمن السيبراني أو البيانات الحكومية المفتوحة، كما تستبعد الجوانب التقنية البحتة التي لا تمسّ النص التشريعي مباشرة.

12. الجانب الأخلاقي

تؤكد الأدبيات الحديثة المتعلقة بحماية البيانات الشخصية على أن احترام خصوصية الأفراد يمثل حجر الزاوية في أي نشاط بحثي، إذ يُعد هذا الحق من الحقوق الأساسية التي يجب صونها وفقاً للتشريعات الدولية والوطنية. فقد نصت اللائحة العامة لحماية البيانات الأوروبية (GDPR) على التزامات واضحة تجاه ضمان سرية المعلومات وحمايتها من أي استخدام غير مشروع، وهو ما أشار إليه (Ishak & Sarabdeen (2024)، موضحين أن التشريعات السعودية تتلاقى مع هذه المبادئ في عدد من الجوانب الجوهرية. كما شدد (Alkhamsi & Alqahtani (2024) على أهمية الشفافية والوضوح في إبلاغ المشاركين بطبيعة البيانات المطلوبة والغرض من جمعها، بما يعزز ثقة الأفراد في العملية البحثية. من جهة أخرى، أوضحت الدراسات المقارنة التي أجراها (Haidar (2024) أن الحصول على الموافقة المستنيرة يُعد من الركائز الأخلاقية الأساسية، بحيث يُمنح المشاركون الحق الكامل في اتخاذ قراراتهم بحرية وإطلاع. وفي سياق التحول الرقمي المتسارع، بيّن (Alhoussari (2025) ضرورة اعتماد إجراءات حماية تقنية وتنظيمية صارمة لضمان أمن البيانات ومنع الوصول غير المصرح به. وبالإضافة إلى ما سبق، حذر (Alzahrani (2024) من مخاطر التمييز والتحيز عند تحليل البيانات، خصوصاً عند استخدام تطبيقات الذكاء الاصطناعي التي قد تؤثر على نزاهة النتائج ومصداقيتها.

أما فيما يخص هذا البحث تحديداً، فيلتزم الباحث بتطبيق أعلى المعايير الأخلاقية في كافة مراحل العمل البحثي، بدءاً من تصميم أدوات جمع البيانات وحتى تحليل النتائج وإعداد التقارير النهائية. سيتم ضمان سرية المعلومات المستخلصة من أي مصادر رسمية أو غير رسمية، ولن تُستخدم إلا للأغراض العلمية ذات الصلة بموضوع الدراسة. كما سيحرص الباحث على توثيق جميع الخطوات المتعلقة بالحصول على البيانات وفقاً للضوابط القانونية المنصوص عليها في نظام

حماية البيانات الشخصية المعمول به في المملكة العربية السعودية. وسيُطلع جميع الأطراف المعنية على أهداف البحث ومحتواه وطرق توظيف البيانات، مع الحصول على موافقتهم الصريحة قبل الشروع في أي إجراء ميداني. إضافة إلى ذلك، سيتخذ الباحث التدابير الأمنية اللازمة لحماية المعلومات من أي اختراق أو إساءة استعمال محتملة، مع الالتزام التام بالحياد والموضوعية وتجنب أي ممارسات قد تؤدي إلى انحياز النتائج أو الإضرار بحقوق المشاركين والمؤسسات المشمولة بالدراسة.

المراجع:

المراجع العربية:

1. إبراهيم، إسلام جمال صابر. (2023). التحول الرقمي بجمهورية مصر العربية: دراسة تحليلية لمنصة مصر الرقمية. المجلة العلمية للمكتبات والوثائق والمعلومات، 5(13.2)، 135-171.
<https://doi.org/10.21608/jslmf.2022.153070.1129>
2. الشمراني، أحمد علي هزاع. (2024). الأطر القانونية لحماية المستهلك في عقود التجارة الإلكترونية في المملكة العربية السعودية: دراسة تحليلية مقارنة مع النظام الأمريكي. مجلة قطاع الشريعة والقانون، 16(16)، 1917-1953.
<https://doi.org/10.21608/jssl.2024.320354.1094>
3. اللبان، نرمن إبراهيم علي إبراهيم. (2022). حوكمة البيانات والوثائق في إدارة جامعة الإسكندرية العامة. المجلة العلمية للمكتبات والوثائق والمعلومات، 4(10)، 237-278.
4. المحيا، ناصر عبد المحسن & السيد، هدى محمد عبد الرحمن. (2025). تأثير استخدام الذكاء الاصطناعي على القواعد الدستورية والإدارية في النظام السعودي "دراسة مقارنة". المجلة القانونية: Doi: 3239-3336، 23(5)، 10.21608/jlaw.2025.360959.1182
5. الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (2025). اللائحة التنفيذية لنظام حماية البيانات الشخصية. الرياض: SDAIA.
6. خليف، سمير. (2010). حلّ النزاعات في عقود التجارة الإلكترونية [رسالة ماجستير، جامعة مولود معمري تيزي وزو، كلية الحقوق، مدرسة الدكتوراه في القانون والعلوم السياسية].
7. رؤية المملكة العربية السعودية 2030. (2020). الوثيقة الرسمية لرؤية المملكة 2030. الرياض: مجلس الشؤون الاقتصادية والتنمية.
8. كلنتن، فريد صالح. (2024). التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي بسبب انتهاك الخصوصية والهجمات السيبرانية في المملكة العربية السعودية. مجلة البحوث والدراسات الإعلامية، 29(29) - العدد التسلسلي (1)، 585-650.
<https://doi.org/10.21608/mjssm.2024.285381.1089>
9. مشيب القحطاني، منال. (2025). فعالية الخدمات الاجتماعية الرقمية في أوقات الأزمات منظور شامل بين التكنولوجيا والكلينيكية دراسة حالة على المملكة العربية السعودية خلال الفترة من عام 2019م إلى عام 2024م. مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية: Doi: 15-45، 39(1)، 10.21608/jfss.2025.424080

المراجع الأجنبية:

10. Alangari, S., Alshahrani, S., Khan, N., Alghamdi, A., Almalki, J., & Shehri, W. (2022). Developing a blockchain-based digitally secured model for the educational sector in

- Saudi Arabia toward digital transformation. *PeerJ Computer Science*, 8.
<https://doi.org/10.7717/peerj-cs.1120>.
11. Alhababi, H. (2024). Cross-Border Data Transfer between the gcc Data Protection Laws and the gdpr. *Global Journal of Comparative Law*. <https://doi.org/10.1163/2211906x-13020003>.
 12. Alhejaili, M. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. *Journal of Governance and Regulation*.
<https://doi.org/10.22495/jgrv13i2siart4>.
 13. Alhoussari, H. (2025). Securing Health Data in the Digital Age: Challenges, Regulatory Frameworks, and Strategic Solutions in Saudi Arabia. *Journal of Ecohumanism*.
<https://doi.org/10.62754/joe.v4i1.6052>.
 14. Aljahdaly, A. (2020). Business Digital Transformation: A Study to Evaluate the Current Digital Operating Model in Saudi Airlines Company to Realize the Impact of Digital Transformation. *International Journal of Advanced Engineering Research and Applications*. <https://doi.org/10.46593/ijaera.2020.v06i01.001>.
 15. Al-Khalifa, H., Mashaabi, M., Al-Yahya, G., & Alnashwan, R. (2023). The Saudi Privacy Policy Dataset. *ArXiv*, abs/2304.02757.
<https://doi.org/10.48550/arXiv.2304.02757>.
 16. Alkhamisi, N., & Alqahtani, S. (2024). Compliance Framework for Personal Data Protection Law Standards. *International Journal of Advanced Computer Science and Applications*. <https://doi.org/10.14569/ijacsa.2024.0150751>.
 17. Alomar, A., Alzahrani, A., Alzahim, A., & Alajaji, M. (2023). COVID-19 and the Digital Transformation that Followed in the Kingdom of Saudi Arabia. *Academic Journal of Research and Scientific Publishing*.
<https://doi.org/10.52132/ajrsp.e.2023.53.1>.
 18. Al-Ruithe, M., & Benkhelifa, E. (2017). Cloud Data Governance In-Light of the Saudi Vision 2030 for Digital Transformation. *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 1436-1442.
<https://doi.org/10.1109/AICCSA.2017.217>.
 19. Alzahrani, R. (2024). An Overview of AI Data Protection in the Context of Saudi Arabia. *International Journal for Scientific Research*.
<https://doi.org/10.59992/ijsr.2024.v3n3p8>.
 20. Haidar, S. (2024). Restrictive Approach to Data Protection in the gcc: Is the EU gdpr a Potential Inspiration? *Global Journal of Comparative Law*.
<https://doi.org/10.1163/2211906x-13020005>.
 21. Huang, X., Xie, Q., Jiang, X., Zhou, Z., Zhang, X., Cheng, Y., Wang, Y., & Chu, C. (2023). Research on Residents' Willingness to Protect Privacy in the Context of the Personal Information Protection Law: A Survey Based on Foshan Residents' Data. *Journal of Sustainable Business and Economics*.
<https://doi.org/10.30564/jsbe.v6i3.5840>.
 22. Issan, S., Kazem, A., & AlMundhiriyah, M. (2014). Legal Awareness and Attitude Towards Law among Teachers in The Sultanate of Oman. *The international journal of learning*, 2, 185-222. <https://doi.org/10.12785/IJLMS/020206>.
 23. Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital

Transformation. *Human Behavior and Emerging Technologies*.

<https://doi.org/10.1155/2023/2103442>.

24. Khalaf, N. (2025). The Impact of AI and Digital Transformation in Shaping the Saudi Legal System. *International Journal of Law Research and Studies*.
<https://doi.org/10.59992/ijlrs.2025.v4n3p2>.
25. Sabur, A., & Showail, A. (2024). Nudging Data Privacy of Mobile Health Applications in Saudi Arabia. *Int. J. Inf. Secur. Priv.*, 18, 1-19. <https://doi.org/10.4018/ijisp.345647>.
26. Sarabdeen, J., & Ishak, M. (2024). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). *International Journal of Law and Management*. <https://doi.org/10.1108/ijlma-01-2024-0025>.
27. Shihah, A., Alrashed, A., Al-Abduljabbar, K., Alamri, H., Shafiq, M., Ahmed, M., & Alkhenizan, A. (2022). Awareness of medical law among health care practitioners in Saudi Arabia. *Saudi Medical Journal*, 43, 954 - 958.
<https://doi.org/10.15537/smj.2022.43.8.20210920>.

