International Journal of Educational Sciences and Arts (IJESA)

المجلة الدولية للعلوم التربوية والآداب

IJESA

Vol. (5), No. (8) August 2026 الإصدار (5)، العدد (8)

قوانين حماية البيانات الشخصية في المملكة العربية السعودية وأثرها في تطوير تطبيقات الإعلام الرقمي

محمد عبد الرحمن الأحمري*، سالم غويزي الحربي

باحث دكتوراه، تخصص إعلام رقمي وتكنولوجيا الاتصال، كلية الآداب والعلوم، جامعة الأهلية، البحرين

*ahmari_ma@hotmail.com

كاظم مؤنس عزيز

أستاذ دكتور، كلية الآداب والعلوم، الجامعة الأهلية، البحرين

ملخص الدراسة

هدفت هذه الدراسة إلى تحليل الإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية، ممثَّلاً في نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) وتعديلاته ولوائحه التنفيذية، وبيان أثره في مسار تطوير تطبيقات الإعلام الرقمي، مع مقارنته باللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) لتحديد أوجه التوافق والاختلاف. واعتمدت الدراسة المنهج الوصفي التحليلي المقارن القائم على تحليل النصوص النظامية واللوائح والأدبيات العلمية والتقارير المتخصصة، واستندت في إطارها النظري إلى نظرية إدارة الخصوصية التواصلية (CPM) لتفسير العلاقة بين المستخدمين والتطبيقات في ضوء متغير الخصوصية. وخلصت الدراسة إلى أن النظام السعودي يمثّل نقلةً تشريعيةً تتوافق مع كثير من المعايير الدولية من حيث الاستناد إلى الموافقة، وكفالة حقوق صاحب البيانات، واشتراط تدابير الأمن والإبلاغ عن خرق البيانات، وتنظيم النقل عبر الحدود، تشرف عليه الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) بمنظومةٍ من اللوائح والأدلة الإرشادية والجزاءات. غير أن النظام يفرض على مطوري تطبيقات الإعلام الرقمي تحديات تتصل بالامتثال التقني والتنظيمي، وبالموازنة بين تقليل البيانات وتخصيص المحتوى، وبتكلفة الامتثال لدى المنشآت الناشئة، ونقل البيانات عبر الحدود والاعتماد على خدمات الطرف الثالث. وأوصت الدراسة بتعزيز الإطار التنظيمي وإصدار أدلة إرشادية تطبيقية، وتوفير الدعم التقني والقانوني للمطورين، وترسيخ مبدأ الخصوصية منذ التصميم، ورفع مستوى الوعي القانوني، بما يدعم بيئةً إعلاميةً رقميةً آمنة تتسق مع مستهدفات رؤية المملكة 2030.

الكلمات المفتاحية: حماية البيانات الشخصية؛ نظام حماية البيانات الشخصية؛ تطبيقات الإعلام الرقمي؛ الخصوصية الرقمية؛ المملكة العربية السعودية؛ اللائحة العامة لحماية البيانات (GDPR).

International Journal of Educational Sciences and Arts (IJESA)
المجلة الدولية للعلوم التربوية والآداب
Vol. (5), No. (8) August 2026 الإصدار (5)، العدد (8)

Personal Data Protection Laws in the Kingdom of Saudi Arabia and Their Impact on the Development of Digital Media Applications

Mohammed Abdulrahman Al-Ahmari*, Salem Ghwaizi Al-Harbi
PhD Researcher, Digital Media and Communication Technology, College of Arts and Sciences, Ahlia University, Bahrain
*ahmari_ma@hotmail.com

Kazem Mounis Aziz
Professor, College of Arts and Sciences, Ahlia University, Bahrain

Abstract

This study analyses the legal framework for personal data protection in the Kingdom of Saudi Arabia—represented by the Personal Data Protection Law (PDPL) issued by Royal Decree No. (M/19), its amendments and Implementing Regulations—and examines its impact on the development of digital media applications, comparing it with the European Union's General Data Protection Regulation (GDPR) to identify points of convergence and divergence. The study adopts a descriptive-analytical and comparative approach based on the analysis of legislative texts, regulations, scholarly literature and specialised reports, and draws on Communication Privacy Management (CPM) theory to interpret the relationship between users and applications in light of the privacy variable. The study concludes that the Saudi law represents a significant legislative milestone that aligns with many international standards—in its reliance on consent, the rights it affords data subjects, its security and breach-notification requirements, and its regulation of cross-border transfers—overseen by the Saudi Data and Artificial Intelligence Authority (SDAIA) through a body of regulations, guidelines and sanctions. Nevertheless, the law imposes on digital-media application developers challenges relating to technical and regulatory compliance, to balancing data minimisation with content personalisation, to the cost of compliance for start-ups, and to cross-border transfers and reliance on third-party services. The study recommends strengthening the regulatory framework and issuing practical guidelines, providing technical and legal support to developers, embedding privacy by design, and raising legal awareness, so as to support a secure digital media environment consistent with the objectives of Saudi Vision 2030.

Keywords: Personal Data Protection, PDPL, Digital Media Applications, Digital Privacy, Saudi Arabia, GDPR.

المقدمة

يشهد العالم في السنوات الأخيرة تطوراً متسارعاً في مجال التقنية، حتى غدت البيانات الرقمية من أهم الأصول التي يقوم عليها تطوير التطبيقات الذكية. ومع اتساع استخدام التطبيقات الرقمية، ولا سيما في مجال الإعلام الرقمي، تزايدت الحاجة إلى وضع أطر قانونية تنظّم جمع البيانات الشخصية واستخدامها وتخزينها وحمايتها، بما يحقق التوازن بين الابتكار التقني وحماية حقوق الأفراد، ويضمن استخداماً عادلاً ومسؤولاً للبيانات.

وفي المملكة العربية السعودية، صدر نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ الموافق 16 سبتمبر 2021م، ثم عُدِّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ الموافق 27 مارس

2023م، ودخل حيز التنفيذ في 14 سبتمبر 2023م، مع منح المنشآت مهلةً للامتثال انتهت في 14 سبتمبر 2024م. ويهدف هذا النظام إلى تعزيز خصوصية الأفراد، وضمان سرية بياناتهم، وتوفير إطار تنظيمي يُلزم الشركات والمؤسسات بالامتثال لمتطلبات حماية البيانات، وتتولى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) الإشراف على تطبيقه. ومع ذلك، فإن إنفاذ هذه الأحكام يمثل تحدياً لمطوري التطبيقات، خصوصاً في قطاع الإعلام الرقمي الذي يعتمد على جمع البيانات وتحليلها لتقديم محتوى مخصص للمستخدمين.

وتتناول هذه الدراسة أثر قوانين حماية البيانات في المملكة في تطوير تطبيقات الإعلام الرقمي، من خلال تحليل آليات امتثال الشركات لهذه القوانين، ودراسة التحديات التي تواجهها في تطوير تطبيقات متوافقة مع المتطلبات القانونية، مع تسليط الضوء على أثر ذلك في حرية تدفق المعلومات وتجربة المستخدم والابتكار في مجال الإعلام الرقمي.

وتعتمد الدراسة على مراجعة الأطر القانونية المحلية ومقارنتها بأنظمة حماية البيانات العالمية، وفي مقدمتها اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، لتحديد أوجه التشابه والاختلاف، وقياس مدى مواءمة الأنظمة السعودية للمعايير الدولية. كما تسعى إلى تقديم توصيات عملية للمطورين والجهات التنظيمية تحقق التوازن بين الامتثال القانوني وتشجيع الابتكار، بما يدعم تطوير قطاع الإعلام الرقمي وحماية البيانات في آنٍ واحد، اتساقاً مع مستهدفات رؤية المملكة 2030 في التحول الرقمي.

مشكلة الدراسة

يتزايد في المملكة العربية السعودية -كما في غيرها من المجتمعات في العصر الرقمي- الاعتمادُ على التطبيقات الرقمية بوصفها ركيزةً أساسيةً في صناعة الإعلام ونقل المحتوى، الأمر الذي جعل البيانات الشخصية محوراً جوهرياً تتقاطع عنده اعتباراتُ الابتكار التقني ومتطلباتُ حماية حقوق الأفراد. وفي هذا السياق تتبلور إشكالية الدراسة في جملةٍ من القضايا المتشابكة التي يطرحها نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) على مطوري تطبيقات الإعلام الرقمي؛ إذ تواجه هذه التطبيقات تحدياً في ضبط جمع البيانات الشخصية ومعالجتها على نحوٍ يمنع الاستخدام غير المشروع وغير المصرَّح به لها، ويثور في الوقت ذاته تساؤلٌ عن تحديد المسؤولية القانونية المترتبة على هذه التطبيقات حيال ما تجمعه من بيانات، وعن مدى كفاية الإطار القانوني القائم ووضوح لوائحه في الإحاطة بمستجدات البيئة الرقمية وتنظيم حماية البيانات تنظيماً فاعلاً. وتلتقي هذه القضايا جميعها عند إشكاليةٍ محوريةٍ مؤداها كيفية تحقيق التوازن بين صون خصوصية البيانات والامتثال لضوابطها من جهة، وضمان حرية الابتكار وتطوير تطبيقات الإعلام الرقمي من جهةٍ أخرى، فضلاً عن مدى مواءمة النظام السعودي للمعايير الدولية في هذا المجال. ومن هنا تأتي هذه الدراسة لتحليل الضوابط القانونية لحماية البيانات في المملكة وتقييمها، انطلاقاً من التساؤل الرئيسي الآتي:

كيف تؤثر قوانين حماية البيانات في المملكة العربية السعودية في تطوير تطبيقات الإعلام الرقمي؟

أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف الآتية:

1. التعرف على نظام حماية البيانات في المملكة العربية السعودية ومدى توافقه مع الأنظمة العالمية.
2. دراسة أثر هذه القوانين في تطوير تطبيقات الإعلام الرقمي.
3. استكشاف التحديات التي تواجه تطبيقات الإعلام الرقمي في الالتزام بالضوابط القانونية.
4. تقييم مستوى وعي منتجي تطبيقات الإعلام الرقمي بالضوابط القانونية المنظِّمة لعملهم.

تساؤلات الدراسة

1. ما أبرز القوانين واللوائح المتعلقة بحماية البيانات في المملكة العربية السعودية؟
2. كيف تؤثر هذه القوانين في تطوير تطبيقات الإعلام الرقمي؟
3. ما التحديات التي تواجه المطورين في الامتثال لهذه القوانين؟

4. ما مستوى وعي منتجي تطبيقات الإعلام الرقمي بالضوابط القانونية المنظِّمة لعملهم؟

منطلقات الدراسة

بوصف هذه الدراسة دراسةً تحليليةً مقارنة، فإنها تنطلق بدلاً من الفرضيات الإحصائية من جملةٍ من المنطلقات التحليلية التي يختبرها التحليل في ضوء النصوص النظامية والأدبيات، وهي:

1. أن وضوح الضوابط القانونية واكتمال لوائحها التنفيذية شرطٌ أساسٌ لتمكين مطوري التطبيقات من الامتثال الفعّال.
2. أن التزام تطبيقات الإعلام الرقمي بضوابط حماية البيانات ينعكس إيجاباً على مستوى حماية بيانات المستخدمين وثقتهم في هذه التطبيقات.
3. أن الإطار القانوني لحماية البيانات يؤثر تأثيراً مزدوجاً في تطوير تطبيقات الإعلام الرقمي؛ إذ يفرض قيوداً وتكاليف امتثال من جهة، ويتيح فرصاً لبناء الثقة والميزة التنافسية من جهةٍ أخرى.

أهمية الدراسة

تستمد هذه الدراسة أهميتها من تحليلها للإطار القانوني المنظِّم لحماية البيانات في المملكة العربية السعودية، في ظل تنامي أهمية المنصات الرقمية وتأثيرها في المجتمع السعودي ضمن سياق التحول الرقمي المتسارع. وتتجلى هذه الأهمية في الحاجة المتزايدة إلى فهم العلاقة بين الأطر التشريعية لحماية البيانات الشخصية وتطور تطبيقات الإعلام الرقمي؛ إذ غدا الالتزام بقوانين حماية البيانات عاملاً رئيساً في بناء الثقة بين المستخدمين والمطورين، بما يؤثر مباشرةً في نجاح هذه التطبيقات وانتشارها. كما تسهم الدراسة في بيان كيفية امتثال مطوري الإعلام الرقمي للوائح حماية البيانات، ودور ذلك في تشجيع الابتكار مع صون حقوق الأفراد وخصوصيتهم. وتقدّم الدراسة فضلاً عن ذلك إسهاماً علمياً يفيد الجهات التنظيمية والمطورين على حدٍّ سواء في تعزيز بيئة إعلامية رقمية آمنة ومستدامة تدعم مستهدفات رؤية المملكة 2030 في التحول الرقمي.

حدود الدراسة

الحدود الموضوعية: تقتصر الدراسة على تحليل الضوابط القانونية لحماية البيانات في المملكة العربية السعودية وأثرها في تطوير تطبيقات الإعلام الرقمي، مع التركيز على الامتثال القانوني وأثره في ابتكار التطبيقات الرقمية وتحسينها.

الحدود المكانية: المملكة العربية السعودية.

الحدود الزمانية: تُجرى الدراسة في المدة من ابريل إلى ديسمبر 2026م، مع متابعة ما يستجد بشأن نظام حماية البيانات الشخصية في المملكة.

الحدود البشرية: تشمل العاملين في التطبيقات الرقمية، ومطوري تطبيقات الإعلام الرقمي، والمختصين في القانون والتشريعات الرقمية.

مصطلحات الدراسة

حماية البيانات:

هي مجموعة من المبادئ والممارسات والتدابير التي تهدف إلى حماية بيانات الأفراد وضمان الالتزام بالأنظمة واللوائح، إذ يُعدّ تخصيص برنامج للالتزام بأحكام النظام ولوائحه ضرورياً لتمكين الجهات من معالجة البيانات الشخصية مع احترام حقوق الأفراد المتعلقة ببياناتهم (الهيئة السعودية للبيانات والذكاء الاصطناعي، د.ت.).

تطوير التطبيقات:

هو عملية تخطيط التطبيق وتصميمه وإنشائه واختباره ونشره لأداء عمليات متنوعة، وقد تقوم به مؤسسات كبيرة ذات فرق عمل واسعة، أو مطوّر مستقل واحد (Zoho Corporation, n.d.).

التطبيقات الرقمية:

هي تطبيقات برمجية تُصمَّم خصيصاً للأجهزة الذكية، كالهواتف الذكية والأجهزة اللوحية، لتقديم مجموعة من الخدمات أو المحتوى التعريفي، ويمكن تحميلها من متاجر التطبيقات الرسمية (الهيئة الحكومية الرقمية، د.ت.).

الدراسات السابقة

تتناول الدراسات والمراجع العلمية والتقارير المتخصصة الآتية الإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية ومقارنته بالمعايير الدولية، وقد رُتِّبت وفق تسلسلها الزمني:

دراسة ريهام (Rahme, 2022) المنشورة عن مؤسسة SMEX بعنوان «حماية البيانات في المملكة العربية السعودية: تحليل مقارن»، أجرت تحليلاً مقارناً بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات (GDPR)، مركّزةً على حقوق أصحاب البيانات والتزامات الجهات المعالِجة. وانتهت إلى أن النظام يتوافق مع المعايير الدولية في جوانب عدة، غير أن بعض مواده وما تضمنته من استثناءات قد يثير إشكالاتٍ تتصل بالتطبيق والإنفاذ، وأوصت بإصدار إرشاداتٍ تفصيلية تعزز فعاليته العملية.

الدراسة المنشورة في مجلة Laws (2025) بعنوان «الموازنة بين الخصوصية والمخاطر: تحليل نقدي لاستخدام البيانات الشخصية في ضوء نظام التأمين السعودي»، اعتمدت المنهج الفقهي–المقارن (doctrinal–comparative) في تحليل نظام حماية البيانات السعودي وموازنته باللائحة الأوروبية في سياق بيانات قطاع التأمين. وخلصت إلى أن أحكام النظام تبدو سليمةً ومتوافقةً مع التوجهات الدولية، لكن قِصَر مدة تطبيقه -نحو ثلاث سنوات- لا يكفي للحكم النهائي على مدى تحقيقه التوازن المنشود بين حماية البيانات والاستخدام المشروع لها، مع إبراز أثر المرجعية الشرعية في تشكيل البيئة التنظيمية للبيانات.

الدراسة المنشورة في مجلة Access to Justice in Eastern Europe (2025) بعنوان «الحقوق الرقمية والذكاء الاصطناعي والقانون: رؤى دولية حول الإطار القانوني للمملكة العربية السعودية»، تناولت الإطار القانوني السعودي للحقوق الرقمية والذكاء الاصطناعي من منظورٍ دوليّ مقارن، معتمدةً منهجاً نوعياً تحليلياً لفحص النصوص والسياسات. وأبرزت الحاجة إلى مواكبة التشريعات للتطورات التقنية المتسارعة، وضمان حماية الحقوق الرقمية في ظل التوسع في استخدام الذكاء الاصطناعي ومعالجة البيانات.

دليل Chambers Global Practice Guides (2025) بعنوان «حماية البيانات والخصوصية 2025 – المملكة العربية السعودية»، قدّم عرضاً تحليلياً لمنظومة حماية البيانات والخصوصية في المملكة، مركّزاً على نظام حماية البيانات الشخصية ولوائحه التنفيذية وآليات إنفاذه، وموازنته بالمعايير الدولية. وأبرز اتساق النظام مع كثيرٍ من تلك المعايير، مع استمرار تطور إطاره التنظيمي عبر ما تصدره الجهة المختصة من لوائح وأدلة.

سلسلة تحليلات Clyde & Co (2024، 2025) حول التحديثات التشريعية في مجال التقنية والبيانات بالمملكة، رصدت التطورات المتلاحقة على النظام بعد دخوله حيز الإنفاذ، ومنها لائحة نقل البيانات خارج المملكة، والنماذج التعاقدية المعتمدة من الجهة المختصة (الشروط التعاقدية القياسية SCCs والقواعد المُلزِمة للشركات BCRs)، وأدلة سياسة الخصوصية وتقليل البيانات وسجل أنشطة المعالجة. وخلصت إلى أن الامتثال غدا ضرورةً استراتيجيةً للمنشآت العاملة في المملكة أو المتعاملة مع بيانات المقيمين فيها، نظراً لاتساع نطاق تطبيق النظام خارج الحدود.

دليل ICLG لحماية البيانات (2025) – فصل المملكة العربية السعودية، عرض في صيغةٍ مقارنةٍ الأحكام الرئيسة للنظام السعودي مقابل أنظمة دولية أخرى، متناولاً الأسس القانونية للمعالجة، وحقوق أصحاب البيانات، والتزامات جهات التحكم، وآليات الإنفاذ والجزاءات، مبرزاً مواضع التوافق والتمايز مع التوجهات العالمية.

تقرير مكتب الغزاوي وشركاه (AlGhazzawi & Partners, 2025) التعريفي بنظام حماية البيانات الشخصية، أوضح نطاق تطبيق النظام وتعريفه للبيانات الشخصية وأثره الممتد خارج الحدود، في ظل بيئةٍ رقميةٍ سعوديةٍ مرتفعة الكثافة تتجاوز فيها تغطية الإنترنت (73%) ونفاذ الهواتف الذكية (80%)، مبرزاً أهمية الامتثال لأحكام النظام لحماية خصوصية الأفراد وضمان المعالجة المسؤولة للبيانات.

التعليق على الدراسات السابقة وموقع الدراسة الحالية

يتبيّن من استقراء الدراسات والمراجع السابقة أنها تتوزع على مسارين رئيسين: مسارٌ أكاديميٌّ تحليليٌّ مقارن يوازن بين النظام السعودي واللائحة الأوروبية وأنظمةٍ أخرى، كما في دراسة ريهام (2022) والدراسة المنشورة في مجلة Laws (2025) والدراسة المنشورة في مجلة AJEE (2025)؛ ومسارٌ مهنيٌّ تطبيقيٌّ يرصد التطورات التنظيمية وآليات الامتثال، كما في أدلة Chambers (2025) وICLG (2025) وتحليلات Clyde & Co (2024، 2025) وتقرير الغزاوي وشركاه (2025).

وتلتقي هذه الأعمال على أن النظام السعودي يمثّل نقلةً تشريعيةً متوافقةً مع كثيرٍ من المعايير الدولية، مع تأكيدها أن جوهر التحدي يكمن في التطبيق والإنفاذ، وفي اكتمال اللوائح والأدلة الإرشادية. وقد أفادت الدراسة الحالية من هذا الإرث في تحديد مواطن القوة والقصور في النظام، وفي بناء المقارنة المنهجية مع اللائحة الأوروبية، وفي تأطير تحديات الامتثال التي تواجه الجهات المعالِجة.

ومع ثراء هذه الأعمال، يُلحَظ أن أغلبها يعالج النظام من زاويةٍ قانونيةٍ عامةٍ أو قطاعيةٍ (كالتأمين والصحة)، في حين تَقِلّ الدراسات التي تربط الإطار القانوني لحماية البيانات تحديداً بتطوير تطبيقات الإعلام الرقمي بوصفه قطاعاً يقوم جوهره على جمع بيانات المستخدمين وتحليلها لتخصيص المحتوى. ومن هنا تسعى الدراسة الحالية إلى سدّ هذه الفجوة، عبر تحليلٍ قانونيٍّ مقارنٍ يستهدف هذا القطاع نوعياً، ويستثمر نظرية إدارة الخصوصية التواصلية إطاراً تفسيرياً، ويخلص إلى مقترحاتٍ عمليةٍ تحقق الموازنة بين الامتثال والابتكار.

الإطار النظري للدراسة

أولاً: نظرية إدارة الخصوصية التواصلية (Communication Privacy Management – CPM):

ظهرت نظرية إدارة الخصوصية التواصلية على يد الباحثة ساندرا بيترونيو عام 2002م، وتقوم على افتراضٍ مفاده أن الأفراد يَعُدّون معلوماتهم الشخصية ملكيةً خاصةً بهم، ويتخذون قراراتٍ بشأن الكشف عنها أو إخفائها استناداً إلى قواعد لإدارة الخصوصية يضعونها بأنفسهم. وتتأثر هذه القواعد بالسياق القانوني والثقافي والتقني، وهو ما ينطبق على تطبيقات الإعلام الرقمي عند تعاملها مع بيانات المستخدمين.

وتوضح النظرية أن المستخدمين يسعون إلى التحكم في بياناتهم، ويقيّمون التطبيقات بناءً على مدى احترامها لخصوصيتهم، في حين يُطالَب المطورون بتصميم حلول تقنية وقانونية متوافقة مع توقعات المستخدمين ومع متطلبات نظام حماية البيانات. وبذلك يغدو القانون -ممثَّلاً في نظام حماية البيانات الشخصية- جزءاً من «قواعد الخصوصية» التي تنظّم التعامل مع البيانات.

ووفقاً للنظرية، يتعزز أثر قواعد إدارة الخصوصية كلما اتسمت السياسات بالوضوح واقترنت بموافقة صريحة من المستخدمين على مشاركة بياناتهم. وكلما التزمت التطبيقات بهذه القواعد ازدادت ثقة المستخدمين وتحسّنت تجربتهم، وهو ما يتحقق عبر تصميماتٍ توازن بين مراعاة الخصوصية والامتثال القانوني. وتوفّر هذه النظرية إطاراً تفسيرياً مناسباً للدراسة، إذ تكشف العلاقة بين المستخدمين والتطبيقات في ضوء متغير الخصوصية، وتبيّن أثر الضوابط القانونية في تصميم التطبيقات وآليات جمع البيانات، بما يسهم في تفسير نتائج الدراسة استناداً إلى مدى احترام التطبيقات للخصوصية التي يحددها المستخدم أو يفرضها القانون (Petronio, 2002).

ثانياً: المبحث الأول – ماهية حماية البيانات الشخصية في المملكة العربية السعودية:

تُعرَّف البيانات الشخصية في النظام السعودي بأنها كل بيانٍ -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصورة مباشرة أو غير مباشرة، ومن ذلك الاسم ورقم الهوية والعناوين وأرقام التواصل وأرقام السجلات والبيانات الصحية والمالية وغيرها. ويُفرد النظام عنايةً خاصةً بـ«البيانات الحساسة» التي يترتب على إفشائها أو إساءة استخدامها ضررٌ بالغٌ بصاحبها، كالبيانات الصحية والوراثية والبيومترية وبيانات المعتقد والانتماء.

ويقوم النظام على جملةٍ من المبادئ الحاكمة لمعالجة البيانات، أبرزها: مشروعية المعالجة واستنادها إلى أساسٍ نظامي كموافقة صاحب البيانات؛ وتحديد الغرض من الجمع وقصر المعالجة عليه؛ وتقليل البيانات بحيث لا تُجمع إلا بالقدر اللازم

لتحقيق الغرض؛ والدقة والتحديث؛ والشفافية والإفصاح؛ والحفظ الآمن للبيانات وحمايتها من الاختراق أو الفقد أو الاستخدام غير المصرَّح به.

ويكفل النظام لصاحب البيانات حزمةً من الحقوق، منها: حق العلم بالأساس النظامي والغرض من جمع بياناته؛ وحق الوصول إلى بياناته والحصول على نسخةٍ منها؛ وحق طلب تصحيحها أو تحديثها؛ وحق طلب إتلافها متى انتفت الحاجة إليها؛ وحق سحب الموافقة على المعالجة. وتمثل هذه الحقوق جوهر التوازن الذي يسعى النظام إلى تحقيقه بين تمكين الجهات من معالجة البيانات وصون خصوصية الأفراد.

ثالثاً: المبحث الثاني – قوانين حماية البيانات في المملكة العربية السعودية:

يمثّل نظام حماية البيانات الشخصية الإطار التشريعي الرئيس لحماية البيانات في المملكة، وقد صدر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ الموافق 16 سبتمبر 2021م، وعُدِّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ الموافق 27 مارس 2023م، ودخل حيز التنفيذ في 14 سبتمبر 2023م، مع منح المنشآت مهلةً للامتثال انتهت في 14 سبتمبر 2024م. ويُكمَّل النظام بلائحته التنفيذية ولائحة نقل البيانات الشخصية خارج المملكة، اللتين فصّلتا أحكامه وآليات تطبيقه.

وتتولى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) الإشراف على إنفاذ النظام، بوصفها الجهة المختصة بإصدار اللوائح والأدلة الإرشادية، ومسك السجل الوطني لجهات التحكم، وتلقّي البلاغات والشكاوى المتعلقة بمخالفة أحكامه، ومتابعة الامتثال عبر المنصة الوطنية لحوكمة البيانات.

ونظّم النظام نقل البيانات الشخصية خارج المملكة وإفشاءها لجهات خارجية ضمن حالات وضوابط محددة تراعي المصلحة الوطنية وحماية خصوصية الأفراد. كما يتقاطع النظام مع أطر تنظيمية أخرى ذات صلة، كأنظمة الأمن السيبراني وضوابطه، والأنظمة القطاعية الخاصة ببعض القطاعات كالقطاع المالي والصحي.

ويُلزم النظام جهات التحكم باتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة للمحافظة على البيانات، بما في ذلك الإبلاغ عن حوادث التسريب، وتعيين مسؤول لحماية البيانات عند الاقتضاء، وإجراء تقييمات الأثر. وتترتب على مخالفة أحكام النظام جزاءاتٌ نظامية، بما يعزز جدية الالتزام (Chambers Global Practice Guides, 2025؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، د.ت.).

رابعاً: المبحث الثالث – التحديات والصعوبات التي تواجه الابتكار والتطوير في تطبيقات الإعلام الرقمي:

يطرح إنفاذ نظام حماية البيانات تحدياتٍ عمليةً أمام مطوري تطبيقات الإعلام الرقمي، تنبع من طبيعة هذه التطبيقات التي تقوم على جمع كمياتٍ كبيرة من بيانات المستخدمين وتحليلها لتخصيص المحتوى والإعلانات. ومن أبرز هذه التحديات تبنّي مبدأ «الخصوصية منذ التصميم وبالإعداد الافتراضي» (Privacy by Design and by Default)، بما يقتضي إعادة هندسة دورة حياة البيانات داخل التطبيق منذ مراحل التصميم الأولى.

كما تبرز صعوبة إدارة موافقة المستخدمين على نحوٍ صريحٍ ومفهوم، وتحقيق مبدأ تقليل البيانات دون الإخلال بجودة الخدمات القائمة على التخصيص؛ إذ يواجه المطورون معادلةً دقيقةً بين الحاجة إلى البيانات لتحسين التجربة، والالتزام بعدم جمع ما يزيد على الغرض المحدد.

وتتصل تحدياتٌ أخرى بالتكلفة والموارد، لا سيما لدى المنشآت الناشئة والصغيرة التي قد تفتقر إلى الكوادر والخبرات القانونية والتقنية اللازمة للامتثال، فضلاً عن تعقيدات نقل البيانات عبر الحدود والاعتماد على خدمات الطرف الثالث ومزوّدي الحوسبة السحابية، وما يستلزمه ذلك من ضماناتٍ تعاقديةٍ وتنظيمية.

ويُضاف إلى ما تقدّم تفاوت مستوى الوعي القانوني لدى المطورين بالضوابط المنظِّمة لعملهم. ومع ذلك، فإن الامتثال لا يُنظر إليه بوصفه عبئاً فحسب، بل يمثل فرصةً لبناء الثقة مع المستخدمين وتعزيز الميزة التنافسية للتطبيقات، بما ينعكس إيجاباً على انتشارها واستدامتها.

نوع الدراسة ومنهجها

تنتمي هذه الدراسة إلى نمط الدراسات الوصفية التحليلية المقارنة، وتعتمد المنهج الوصفي التحليلي مقترناً بالمنهج المقارن والمنهج الوثائقي (المكتبي). ويقوم المنهج الوصفي التحليلي على استقراء النصوص النظامية واللوائح والأدبيات وتحليل مضامينها لاستخلاص أحكام حماية البيانات وأثرها في تطوير تطبيقات الإعلام الرقمي، في حين يتيح المنهج المقارن الموازنة بين النظام السعودي واللائحة العامة الأوروبية لحماية البيانات (GDPR) لتحديد أوجه التوافق والتمايز، ويسهم المنهج الوثائقي في تتبّع تطور الإطار التنظيمي عبر المرسوم الملكي وتعديلاته ولوائحه التنفيذية والأدلة الإرشادية الصادرة عن الجهة المختصة.

مصادر البيانات:

اعتمدت الدراسة على مصادر أولية وثانوية؛ فالمصادر الأولية تشمل النصوص النظامية ذات الصلة، وفي مقدمتها نظام حماية البيانات الشخصية ولائحته التنفيذية ولائحة نقل البيانات الشخصية خارج المملكة والأدلة الإرشادية الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، فضلاً عن اللائحة العامة الأوروبية لحماية البيانات بوصفها مرجعاً للمقارنة. أما المصادر الثانوية فتشمل الدراسات العلمية المحكَّمة والتقارير القانونية المتخصصة والمراجع المشار إليها في الدراسة.

أداة التحليل ومعاييره:

استخدمت الدراسة أداة التحليل القانوني المقارن، القائم على تفكيك أحكام النظام ومقابلتها بأحكام اللائحة الأوروبية وفق معايير محددة، هي: النطاق الإقليمي للتطبيق، والأساس النظامي للمعالجة، وحقوق صاحب البيانات، والتزامات جهات التحكم، وآليات الإبلاغ عن خرق البيانات، وضوابط نقل البيانات عبر الحدود، والجزاءات، والجهة المشرفة. ثم جرى تحليل انعكاسات هذه الأحكام على عمليات تطوير تطبيقات الإعلام الرقمي وتحدياتها.

محددات الدراسة:

تتركّز الدراسة على البُعد القانوني التحليلي المقارن لأثر حماية البيانات في تطوير تطبيقات الإعلام الرقمي، ولا تتضمن في مرحلتها الحالية دراسةً ميدانيةً مسحية؛ إذ يُوصى بإجراء دراسةٍ ميدانيةٍ مكمّلةٍ تستطلع آراء المطورين والخبراء القانونيين بوصفها امتداداً مستقبلياً يتيح التحقق التجريبي من نتائج التحليل وقياس مستوى الوعي والامتثال بدقة.

نتائج التحليل ومناقشتها:

تُعرض في هذا الجزء نتائج تحليل الإطار القانوني ومناقشتها، منظَّمةً وفق محاور أسئلة الدراسة الأربعة، ثم تُختتم بنتيجة المقارنة بين النظام السعودي واللائحة الأوروبية.

المحور الأول: أبرز قوانين حماية البيانات ولوائحها في المملكة

يتصدّر منظومةَ حماية البيانات في المملكة نظامُ حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ الموافق 16 سبتمبر 2021م، والمعدَّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ الموافق 27 مارس 2023م. وقد استُكمل النظام بلائحته التنفيذية ولائحة نقل البيانات الشخصية خارج المملكة الصادرتين في سبتمبر 2023م، ودخل النظام ولوائحه حيز التنفيذ في 14 سبتمبر 2023م، مع مهلة امتثالٍ انتهت في 14 سبتمبر 2024م ليصبح النظام نافذاً نفاذاً كاملاً.

وتولّت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) إصدار حزمةٍ من الأدلة الإرشادية التطبيقية خلال عام 2024م، شملت دليل سياسة الخصوصية، ودليل الإفصاح عن البيانات، ودليل الإتلاف وإخفاء الهوية والترميز، ودليل سجل أنشطة المعالجة، ودليل تقليل البيانات. وتتولى سدايا الإشراف على الإنفاذ بوصفها الجهة المختصة، مع إمكانية انتقال الإشراف مستقبلاً إلى المكتب الوطني لإدارة البيانات ضمن منظومة الحوكمة الوطنية. ويتقاطع النظام مع أطرٍ تنظيميةٍ أخرى ذات صلة، كضوابط الأمن السيبراني والأنظمة القطاعية في المجالين المالي والصحي.

ويقرن النظام أحكامه بجزاءاتٍ رادعة، تشمل غراماتٍ مالية تصل إلى خمسة ملايين ريال، وعقوباتٍ جزائيةٍ لبعض المخالفات الجسيمة. وتؤكد ممارسات الإنفاذ جدية التطبيق؛ إذ أصدرت لجان النظر في المخالفات لدى سدايا عشرات القرارات بإثبات

مخالفاتٍ لأحكام النظام، شملت المعالجة دون أساسٍ نظامي، والإفصاح غير المصرَّح به، والإخفاق في تطبيق التدابير التقنية والتنظيمية، وإرسال الرسائل التسويقية دون موافقة.

المحور الثاني: أثر القوانين في تطوير تطبيقات الإعلام الرقمي

يفرض النظام على مطوري تطبيقات الإعلام الرقمي إعادة النظر في دورة حياة البيانات داخل التطبيق منذ مراحل التصميم الأولى، تطبيقاً لمبدأ «الخصوصية منذ التصميم وبالإعداد الافتراضي». ويترتب على ذلك التزاماتٌ عملية، أبرزها: تصميم آليات موافقةٍ صريحةٍ ومفهومة على جمع البيانات ومعالجتها؛ وإعمال مبدأ تقليل البيانات بقصر الجمع على القدر اللازم للغرض؛ وتعيين مسؤولٍ لحماية البيانات في الحالات التي يستوجبها النظام؛ وبناء آليات للإبلاغ عن خرق البيانات؛ ومراعاة ضوابط نقل البيانات عبر الحدود عند الاعتماد على خدمات الاستضافة والحوسبة السحابية.

ويكشف التحليل أن أثر النظام في تطوير التطبيقات أثرٌ مزدوج؛ فهو من جهةٍ يفرض قيوداً وتكاليف امتثالٍ قد تبطئ بعض دورات التطوير أو تقيّد نماذج الأعمال القائمة على التوسع في جمع البيانات وتخصيص المحتوى والإعلانات. وهو من جهةٍ أخرى يتيح فرصةً حقيقيةً لبناء الثقة مع المستخدمين وتعزيز الميزة التنافسية للتطبيقات الملتزمة، بما ينعكس إيجاباً على انتشارها واستدامتها وجاذبيتها للاستثمار، وهو ما يتسق مع ما تذهب إليه نظرية إدارة الخصوصية التواصلية من أن احترام قواعد الخصوصية يعزز ثقة المستخدمين وتجربتهم.

المحور الثالث: تحديات الامتثال أمام المطورين

يُظهر التحليل جملةً من التحديات التي تعترض امتثال مطوري تطبيقات الإعلام الرقمي، يمكن إجمالها في الآتي: التحدي التقني المتمثل في إعادة هندسة جمع البيانات ومعالجتها وتأمينها وفق متطلبات النظام؛ وتحدي التكلفة والموارد، ولا سيما لدى المنشآت الناشئة والصغيرة التي قد تفتقر إلى الكوادر القانونية والتقنية؛ وتحدي نقل البيانات عبر الحدود في ظل اشتراط النماذج التعاقدية المعتمدة (SCCs/BCRs) وعدم صدور قائمة الدول ذات الحماية الكافية حتى تاريخه؛ وتحدي الاعتماد على خدمات الطرف الثالث ومزوّدي الحوسبة السحابية وما يستلزمه من ضماناتٍ تعاقدية؛ وأخيراً تحدي تفاوت الوعي القانوني والكفاءات المتخصصة في حماية البيانات.

المحور الرابع: مستوى وعي المطورين بالضوابط القانونية

يتطلب القياس الدقيق لمستوى وعي مطوري تطبيقات الإعلام الرقمي بالضوابط القانونية أداةً ميدانيةً مباشرة، وهو ما يخرج عن نطاق المرحلة التحليلية الحالية. غير أن مؤشرات التحليل غير المباشرة -ومنها تعدد القرارات الصادرة بإثبات مخالفاتٍ لأحكام النظام، وما تشير إليه بعض الدراسات المقارنة من افتقار عددٍ من الجهات إلى سياساتٍ ملائمةٍ أو إلى مسؤولٍ مخصصٍ لحماية البيانات- تُرجّح وجود تفاوتٍ في مستوى النضج والوعي بالامتثال. ومن ثمّ توصي الدراسة بإجراء دراسةٍ ميدانيةٍ مكمّلةٍ لقياس هذا المستوى بدقةٍ وتحديد فجواته، تمهيداً لتصميم برامج توعيةٍ وتدريبٍ موجَّهة.

نتيجة المقارنة بين النظام السعودي واللائحة الأوروبية

تكشف الموازنة بين نظام حماية البيانات الشخصية السعودي واللائحة العامة الأوروبية لحماية البيانات (GDPR) عن توافقٍ جوهريٍ في المبادئ الكبرى، مع وجود فروقٍ في بعض الآليات ومستوى نضج الإنفاذ، ويوضح الجدول الآتي أبرز أوجه المقارنة:

جدول (1): مقارنة بين النظام السعودي (PDPL) واللائحة الأوروبية (GDPR)- المصدر: إعداد الباحث استناداً إلى نظام حماية البيانات الشخصية ولوائحه التنفيذية، واللائحة العامة الأوروبية لحماية البيانات، والمراجع المشار إليها.

وجه المقارنة	نظام حماية البيانات السعودي ((PDPL	اللائحة الأوروبية ((GDPR
النطاق الإقليمي	يسري على معالجة بيانات المقيمين في المملكة، بأثرٍ يمتد خارج حدودها	تسري على معالجة بيانات الأفراد في الاتحاد الأوروبي، بأثرٍ يمتد خارج حدوده
الأساس النظامي للمعالجة	الموافقة مع أسسٍ نظاميةٍ أخرى محددة في النظام ولائحته	ستة أسسٍ قانونية، من بينها المصلحة المشروعة
حقوق صاحب البيانات	العلم، والوصول، والتصحيح، والإتلاف، وسحب الموافقة	الوصول، والتصحيح، والمحو، وتقييد المعالجة، ونقل البيانات، والاعتراض

وجه المقارنة	نظام حماية البيانات السعودي ((PDPL	اللائحة الأوروبية ((GDPR
مسؤول حماية البيانات	إلزامي لفئاتٍ محددة (المعالجة الواسعة أو الحساسة أو المراقبة المنتظمة)	إلزامي في حالاتٍ محددةٍ مماثلة
الإبلاغ عن خرق البيانات	إلزامي بإبلاغ «سدايا» وأصحاب البيانات وفق الضوابط	إلزامي بإبلاغ السلطة المختصة خلال 72 ساعة
نقل البيانات عبر الحدود	نماذج تعاقدية معتمدة من سدايا (SCCs/BCRs)، دون قائمة دولٍ كافيةٍ حتى تاريخه	آليات قرار الكفاية والضمانات المناسبة SCCs/BCRs))
الجزاءات	غراماتٌ تصل إلى 5 ملايين ريال، وعقوباتٌ جزائيةٌ لبعض المخالفات الجسيمة	غراماتٌ تصل إلى 20 مليون يورو أو 4% من الإيراد العالمي السنوي
الجهة المشرفة	الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)	سلطات حماية البيانات الوطنية في الدول الأعضاء

ويتبيّن من الجدول أن النظام السعودي يتقاطع مع اللائحة الأوروبية في الاستناد إلى الموافقة، وكفالة حقوق صاحب البيانات، واشتراط تدابير الأمن والإبلاغ عن الخرق، وتنظيم النقل عبر الحدود، وإفراد البيانات الحساسة بحمايةٍ مشددة. ويبرز التمايز في اتساع الأسس القانونية للمعالجة في اللائحة الأوروبية، وفي تحديدها مهلةً صريحةً للإبلاغ عن الخرق، وفي مستوى نضج آليات الكفاية لنقل البيانات، وفي مقدار الغرامات. ويعكس هذا التوافق سعي المملكة إلى مواءمة نظامها مع المعايير الدولية بما يسهّل التعاملات عبر الحدود ويعزز الثقة في بيئتها الرقمية، اتساقاً مع مستهدفات رؤية 2030.

الخاتمة والتوصيات

خلصت الدراسة من تحليلها للإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية، ومقارنته بالمعايير الدولية، إلى جملةٍ من النتائج، أبرزها أن نظام حماية البيانات الشخصية يمثّل نقلةً تشريعيةً مهمة، ويتوافق مع كثيرٍ من المبادئ التي تقوم عليها الأنظمة الدولية الرائدة كاللائحة العامة لحماية البيانات (GDPR)، من حيث الاستناد إلى موافقة صاحب البيانات، وكفالة حقوقه، واشتراط تدابير الأمن والإبلاغ عن حوادث التسريب، وتنظيم نقل البيانات عبر الحدود. ومع ذلك، يفرض النظام على مطوري تطبيقات الإعلام الرقمي تحدياتٍ تتصل بالامتثال التقني والتنظيمي، وبالموازنة بين حماية البيانات وحرية الابتكار وتخصيص المحتوى.

وبناءً على ما تقدّم، توصي الدراسة بما يأتي:

1. تعزيز الإطار التنظيمي وإصدار أدلةٍ إرشاديةٍ تفصيلية تيسّر على المطورين فهم متطلبات الامتثال وتطبيقها.
2. توفير الدعم التقني والقانوني للمطورين، ولا سيما المنشآت الناشئة والصغيرة، عبر أدواتٍ ونماذج تساعد على الامتثال بكفاءةٍ وتكلفةٍ معقولة.
3. ترسيخ مبدأ «الخصوصية منذ التصميم وبالإعداد الافتراضي» في دورة تطوير التطبيقات.
4. رفع مستوى الوعي القانوني لدى المطورين من خلال برامج تدريبية متخصصة.
5. مواصلة مواءمة الأنظمة الوطنية مع المعايير الدولية مع مراعاة الخصوصية المحلية، ومراجعتها دورياً لمواكبة التطورات التقنية المتسارعة.
6. إجراء دراسةٍ ميدانيةٍ مكمّلةٍ تستطلع آراء المطورين والخبراء القانونيين، بما يتيح التحقق التجريبي من نتائج التحليل، وقياس مستوى الوعي والامتثال بدقة.

وبهذا تسهم الدراسة في دعم بيئةٍ إعلاميةٍ رقميةٍ آمنةٍ ومستدامةٍ توازن بين حماية البيانات وتشجيع الابتكار، بما يتسق مع مستهدفات رؤية المملكة العربية السعودية 2030 في التحول الرقمي.

المراجع

أولاً: المراجع العربية والمصادر النظامية:

- نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدَّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ. (2021). المملكة العربية السعودية.
- اللائحة التنفيذية لنظام حماية البيانات الشخصية. (2023). الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). المملكة العربية السعودية.
- لائحة نقل البيانات الشخصية خارج المملكة. (2023). الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). المملكة العربية السعودية.
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (د.ت.). الأنظمة واللوائح. استُرجع في 23 يونيو 2026م، من https://sdaia.gov.sa/
- ريهام، م. (2022). حماية البيانات في المملكة العربية السعودية: تحليل مقارن. مؤسسة SMEX. https://smex.org/data-protection-in-saudi-arabia-comparative-analysis/

ثانياً: المراجع الأجنبية:

- AlGhazzawi & Partners. (2025). Personal data protection law. https://www.ghazzawilawfirm.com/insights/personal-data-protection-law/
- Alkhedhairy, M. A. (2025). Balancing privacy and risk: A critical analysis of personal data use as governed by Saudi insurance law. Laws, 14(4), 47. https://doi.org/10.3390/laws14040047
- Chambers and Partners. (2025). Data protection & privacy 2025 – Saudi Arabia. Chambers Global Practice Guides. https://www.chambers.com/global-practice-guides/data-protection-privacy-2025-saudi-arabia
- Clyde & Co. (2024). Saudi Arabia's Personal Data Protection Law becomes enforceable: Essential insights for businesses. https://www.clydeco.com/en/insights/2024/09/saudi-arabia-s-personal-data-protection-law-become
- Clyde & Co. (2025). Legal updates in Saudi Arabia's technology and data laws. https://www.clydeco.com/en/insights/2025/02/10-legal-updates-ksa-tech-and-data-laws
- Digital rights, AI, and the law: International perspectives on Saudi Arabia's legal framework and international experience. (2025). Access to Justice in Eastern Europe. https://ajee-journal.com/
- DLA Piper. (n.d.). Data protection laws of the world: Saudi Arabia. Retrieved June 23, 2026, from https://www.dlapiperdataprotection.com/?c=SA
- International Comparative Legal Guides. (2025). Data protection laws and regulations: Saudi Arabia 2025–2026. ICLG. https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia
- Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. SUNY Press.

- PECB. (2025). Saudi Arabia's data privacy law in practice: What you need to know about the PDPL. https://pecb.com/en/article/saudi-arabias-data-privacy-law-in-practice-what-you-need-to-know-about-the-pdpl

الملاحق

ملحق (1): أداة الدراسة (الاستبانة):

تمثّل الاستبانة الآتية الأداة المقترحة لاستكمال الجانب الميداني الموصى به في منهجية الدراسة، وهي موجَّهة إلى فئتي مطوري تطبيقات الإعلام الرقمي والخبراء القانونيين، وتُقاس عباراتها وفق مقياس ليكرت الخماسي.

مقدمة الاستبانة: تهدف هذه الاستبانة إلى دراسة أثر قوانين حماية البيانات الشخصية في المملكة العربية السعودية في تطوير تطبيقات الإعلام الرقمي. وتُستخدم الإجابات لأغراض البحث العلمي فقط، وتُعامل بسريةٍ تامة، ولا تُنسب إلى أشخاص المشاركين. والمشاركة طوعية، وللمشارك الانسحاب في أي وقت.

☐**أوافق على المشاركة في هذه الدراسة وفق ما ورد أعلاه.**

القسم الأول: البيانات الأولية:

1) فئة المشارك: ☐مطوّر/مختص تقني في التطبيقات الرقمية ☐ خبير/مختص قانوني في حماية البيانات

2) سنوات الخبرة: ☐أقل من 3 – 3 ☐ أقل من 7 – 7 ☐ أقل من 12 – 7 ☐ 12 فأكثر

3) المؤهل العلمي: ☐دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه

4) نوع المنصة/جهة العمل: ☐تواصل اجتماعي ☐ منصة إعلامية/إخبارية ☐ تجارة إلكترونية ☐ تعليمية ☐ ترفيه رقمي ☐ أخرى

5) حجم المنشأة: ☐ناشئة/متناهية الصغر ☐ صغيرة ☐ متوسطة ☐ كبيرة

6) هل سبق لك التعامل المباشر مع متطلبات نظام حماية البيانات الشخصية؟ ☐نعم ☐ لا

القسم الثاني: محاور الدراسة:

تعليمات: أمام كل عبارة، اختر درجة موافقتك وفق المقياس الخماسي: (5) موافق بشدة، (4) موافق، (3) محايد، (2) غير موافق، (1) غير موافق بشدة.

المحور الأول: مستوى المعرفة والوعي بنظام حماية البيانات الشخصية:

م	العبارة	5	4	3	2	1
1	لديّ معرفةٌ كافيةٌ بأحكام نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19).					
2	ألمّ باللوائح التنفيذية وأدلة «سدايا» الإرشادية ذات الصلة بعملي.					
3	أعرف حقوق صاحب البيانات التي كفلها النظام (العلم، الوصول، التصحيح، الإتلاف، سحب الموافقة).					
4	أدرك الجزاءات المترتبة على مخالفة أحكام النظام.					
5	أتابع التحديثات التي تطرأ على النظام ولوائحه أولاً بأول.					
6	تلقّيتُ تدريباً أو توعيةً كافيةً بشأن متطلبات حماية البيانات.					

المحور الثاني: وضوح الضوابط القانونية واكتمال لوائحها:

م	العبارة	5	4	3	2	1
1	تتسم أحكام نظام حماية البيانات بالوضوح وسهولة الفهم.					
2	توفّر اللوائح التنفيذية والأدلة الإرشادية تفصيلاً كافياً للتطبيق العملي.					

3	تُعدّ متطلبات الامتثال محددةً وقابلةً للقياس.					
4	تساعد الجهة المختصة («سدايا») في توضيح الالتزامات عبر قنواتها وأدلتها.					
5	وضوح الضوابط القانونية ييسّر على المطورين تحقيق الامتثال الفعّال.					

المحور الثالث: أثر القوانين في تطوير تطبيقات الإعلام الرقمي:

م	العبارة	5	4	3	2	1
1	تدفع القوانين إلى تبنّي مبدأ «الخصوصية منذ التصميم» في تطوير التطبيق.					
2	تؤثر متطلبات الموافقة وتقليل البيانات في طريقة تصميم التطبيق ووظائفه.					
3	ترفع القوانين مستوى أمان التطبيق وحماية بيانات المستخدمين.					
4	تؤثر متطلبات الامتثال في تجربة المستخدم داخل التطبيق.					
5	تفرض القوانين قيوداً على نماذج التخصيص والإعلان القائمة على البيانات.					
6	يدفع الامتثال نحو مزيدٍ من الابتكار في حلول حماية الخصوصية.					
7	يطيل الامتثال زمن تطوير التطبيق وإطلاقه.					

المحور الرابع: تحديات الامتثال:

م	العبارة	5	4	3	2	1
1	يمثّل الجانب التقني (إعادة هندسة جمع البيانات ومعالجتها) تحدياً رئيساً.					
2	تشكّل تكلفة الامتثال عبئاً على المنشأة، لا سيما الناشئة والصغيرة.					
3	يصعب الامتثال لضوابط نقل البيانات خارج المملكة (SCCs/BCRs).					
4	يزيد الاعتماد على خدمات الطرف الثالث والحوسبة السحابية من تعقيد الامتثال.					
5	يُعيق نقصُ الكوادر القانونية والتقنية المتخصصة تحقيقَ الامتثال.					
6	تشكّل الموازنة بين تقليل البيانات وجودة الخدمة تحدياً عملياً.					

المحور الخامس: حماية البيانات وثقة المستخدمين:

م	العبارة	5	4	3	2	1
1	يعزّز التزام التطبيق بحماية البيانات ثقة المستخدمين فيه.					
2	يفضّل المستخدمون التطبيقات التي تحترم خصوصيتهم وتمنحهم التحكم في بياناتهم.					
3	ينعكس مستوى حماية البيانات إيجاباً على انتشار التطبيق واستمراريته.					
4	وضوح سياسة الخصوصية يرفع رضا المستخدمين عن التطبيق.					
5	يقلّل الالتزام بالنظام من مخاطر تسريب البيانات والمساءلة القانونية.					

المحور السادس: الموازنة بين الامتثال والابتكار:

م	العبارة	5	4	3	2	1
1	يمكن تحقيق التوازن بين الامتثال القانوني وحرية الابتكار.					
2	يمثّل الامتثال فرصةً لبناء ميزةٍ تنافسيةٍ أكثر من كونه عبئاً.					

3	يشجّع الإطار القانوني الحالي الاستثمار في قطاع الإعلام الرقمي.					
4	تقدّم الجهات التنظيمية للمطورين دعماً كافياً لتحقيق هذا التوازن.					
5	يسهم النظام في بناء بيئةٍ إعلاميةٍ رقميةٍ آمنةٍ تتسق مع رؤية المملكة 2030.					

القسم الثالث: أسئلة مفتوحة:

1. ما أبرز التحديات التي واجهتك (أو تتوقعها) في الامتثال لنظام حماية البيانات عند تطوير التطبيقات؟
2. ما المقترحات التي تراها لتحقيق التوازن بين حماية البيانات وتشجيع الابتكار؟
3. ملاحظات إضافية (اختياري).

نشكر لكم وقتكم ومشاركتكم القيّمة.