International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
IJLRS
Vol. (5), No. (7)
July 2026
الإصدار (5)، العدد (7)

الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية وأثره على التزامات الجهات التقنية

محمد الحسين القرشي
كلية العلوم الإنسانية، جامعة ميدأوشن، الإمارات العربية المتحدة
qmr@outlook.it

المستخلص

هدفت هذه الدراسة إلى تحليل الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدَّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، مع الوقوف على أثره القانوني والتشغيلي على التزامات جهات التحكم والمعالجة (الجهات التقنية)، وذلك في ضوء دراسة مقارنة باللائحة الأوروبية العامة لحماية البيانات .(GDPR) واعتمدت الدراسة على المنهج التحليلي المقارن، عبر تحليل النصوص التشريعية للنظام ولائحته التنفيذية ولائحة نقل البيانات خارج المملكة، ومقارنتها بالنصوص المقابلة فيGDPR ، مع الاستئناس بالفقه القانوني والدراسات الميدانية الحديثة.

وتناولت الدراسة في مبحثَيْن رئيسَيْن: الأحكام العامة للنظام (الإطار المفاهيمي، والنطاق التطبيقي، والمبادئ الحاكمة، وحقوق أصحاب البيانات)، والتزامات الجهات التقنية (القانونية والتنظيمية، والتقنية والأمنية، وضوابط النقل خارج المملكة، ومنظومة المسؤولية والحماية الجزائية).

وخلصت الدراسة إلى جملة من النتائج، أبرزها: أن النظام السعودي يُمثّل نقلةً تشريعية نوعية تُواكب رؤية المملكة 2030، وأن المشرّع السعودي تبنّى مقاربةً موسّعة لمفهوم البيانات الحساسة بما يفوق نظيره الأوروبي في بعض الجوانب، وأن النظام يمتد أثره خارج الإقليم بما يُرسّخ مبدأ السيادة الرقمية، وأن منظومة الجزاءات السعودية تُغلّب الطابع الجزائي مع عقوبة السجن، خلافاً لنظيرتها الأوروبية التي تُغلّب الطابع الإداري بغرامات مالية ضخمة. كما رصدت الدراسة فجوةً قائمة بين النص النظامي والممارسة التطبيقية، لا سيما في التزام المواقع والتطبيقات الرقمية السعودية بمتطلبات الشفافية والخصوصية بالتصميم.

وأوصت الدراسة بإصدار أدلة إرشادية قطاعية متخصصة من قِبَل الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، وتفعيل الرقابة اللاحقة على الجهات التقنية، وإصدار قائمة بالدول ذات الحماية الكافية على غرار نموذج قرارات الكفاية الأوروبية، وتطوير القدرات القضائية والادعائية المتخصصة، وتعزيز ضمانات استقلال مسؤول حماية البيانات، وتطوير إطار تنظيمي متخصص لمعالجة البيانات في سياق تقنيات الذكاء الاصطناعي.

الكلمات المفتاحية: حماية البيانات الشخصية، النظام السعودي، اللائحة الأوروبية العامة (GDPR)، جهات التحكم، جهات المعالجة، السيادة الرقمية، سدايا، الخصوصية بالتصميم.

International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (7)
IJLRS
July 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (7)

The regulatory framework for protecting personal data in the Kingdom of Saudi Arabia and its impact on the obligations of technical authorities

Mohammed Al-Hussain Al-Qurashi
Faculty of Humanities, Med-Ocean University, United Arab Emirates
qmr@outlook.it

Abstract

This study aimed to analyze the legal framework for personal data protection in the Kingdom of Saudi Arabia, established by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, focusing on its legal and operational impact on the obligations of data controllers and processors (technical entities), through a comparative study with the European Union General Data Protection Regulation (GDPR). The study adopted the analytical-comparative methodology, examining the legislative texts of the Law, its Executive Regulations, and the Regulation on Personal Data Transfer Outside the Kingdom, comparing them with the corresponding provisions in the GDPR, drawing upon contemporary legal scholarship and empirical studies.

The research was organized into two main chapters: the general provisions of the Law (conceptual framework, scope of application, governing principles, and data subject rights), and the obligations of technical entities (legal and organizational, technical and security, cross-border transfer controls, and the liability and criminal protection regime).

The study concluded with several key findings, most notably: the Saudi Law represents a qualitative legislative leap aligned with Saudi Vision 2030; the Saudi legislator adopted an expanded conception of sensitive data that exceeds its European counterpart in certain aspects; the Law's extraterritorial application reinforces the principle of digital sovereignty; and the Saudi sanctions regime emphasizes criminal penalties including imprisonment, contrary to the GDPR which prioritizes administrative sanctions with substantial monetary fines. The study also identified a persistent gap between the legislative text and practical implementation, particularly regarding compliance of Saudi websites and digital applications with transparency and privacy-by-design requirements.

The study recommended the issuance of specialized sectoral guidelines by the Saudi Data and Artificial Intelligence Authority (SDAIA), activating ex-post supervision of technical entities, publishing a list of countries with adequate protection modeled on the European adequacy decisions, developing specialized judicial and prosecutorial capacities, strengthening safeguards for the independence of the Data Protection Officer (DPO), and establishing a specialized regulatory framework for data processing in the context of artificial intelligence technologies.

Keywords: Personal Data Protection, Saudi PDPL, GDPR, Data Controllers, Data Processors, Digital Sovereignty, SDAIA, Privacy by Design.

المقدمة

يشهد العالم تحولاً رقمياً متسارعاً أصبحت فيه البيانات الشخصية تمثّل ثروةً استراتيجيةً وركيزةً أساسيةً لاقتصاد المعرفة، إذ تعتمد عليها المؤسسات والشركات التقنية في تقديم خدماتها وتطوير منتجاتها واتخاذ قراراتها، وقد أدّى هذا الاعتماد المتزايد على البيانات إلى تصاعد المخاطر المرتبطة بانتهاك خصوصية الأفراد؛ من خلال الجمع غير المشروع للبيانات، أو معالجتها لأغراض تتجاوز الغرض الذي جُمعت من أجله، أو نقلها عبر الحدود دون ضمانات كافية.

وأولت المملكة العربية السعودية اهتماماً بالغاً بحماية البيانات الشخصية بوصفها ركيزةً من ركائز رؤية المملكة 2030 التي تسعى إلى بناء اقتصاد رقمي متقدّم وبيئة استثمارية موثوقة؛ فصدر نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، ثم عُدّل بالمرسوم الملكي رقم (م/148) بتاريخ 5/9/1444هـ، وصدرت لائحته التنفيذية بقرار مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) رقم (1445/3) بتاريخ 1445/2/7هـ، ودخل النظام حيّز النفاذ الكامل في 14 سبتمبر 2024م بعد انتهاء الفترة الانتقالية.

ويُعدّ هذا النظام أول تشريع شامل لحماية البيانات الشخصية في المملكة، وقد جاء متأثراً إلى حدٍّ كبير باللائحة الأوروبية العامة لحماية البيانات (GDPR) الصادرة عام 2016م، التي تُعدّ المعيار الدولي الأبرز في هذا المجال، ويفرض النظام السعودي التزامات محددة على جهات التحكّم وجهات المعالجة تشمل الحصول على الموافقة، والشفافية في الإفصاح عن أغراض المعالجة، واتخاذ التدابير التقنية والتنظيمية لحماية البيانات، وتقييم الأثر على الخصوصية، فضلاً عن تنظيم نقل البيانات خارج المملكة.

ومن هنا تأتي هذه الدراسة لتحليل هذا الإطار النظامي تحليلاً معمّقاً، مع مقارنته باللائحة الأوروبية العامة لحماية البيانات (GDPR)، وبيان أثره على التزامات الجهات التقنية العاملة في المملكة، بما يشمل شركات التقنية ومقدمي الخدمات السحابية ومنصات التجارة الإلكترونية وتطبيقات الذكاء الاصطناعي.

مشكلة الدراسة

على الرغم من أنّ نظام حماية البيانات الشخصية السعودي قد أرسى إطاراً قانونياً شاملاً لحماية البيانات الشخصية وحدّد التزامات جهات التحكّم والمعالجة، إلا أنّ دخوله حيّز النفاذ الكامل في 14 سبتمبر 2024م قد أحدث أثراً قانونياً وتشغيلياً مباشراً على الجهات التقنية العاملة في المملكة، سواء من حيث إعادة هيكلة عملياتها الداخلية لمعالجة البيانات، أو من حيث فرض التزاماتٍ جديدةٍ تتعلق بالحوكمة والشفافية والمساءلة والتدابير التقنية والتنظيمية (المطيري، 2025). وقد أشارت دراسة القحطاني (2024) إلى أنّ هذا الأثر رتّب على شركات التقنية ومقدّمي الخدمات السحابية ومنصات التجارة الإلكترونية أعباءً امتثاليةً إضافيةً تتضمّن مراجعة سياسات الخصوصية، وتعيين مسؤولي حماية البيانات، وإجراء تقييمات الأثر، وتوثيق سجلات أنشطة المعالجة، وتنظيم آليات نقل البيانات عبر الحدود، فضلاً عن التعرّض لعقوباتٍ نظاميةٍ إداريةٍ وجزائيةٍ عند المخالفة (الجعيد، 2025؛ الرواحي، 2025؛ Alharbi, 2025)، وتتمحور مشكلة هذه الدراسة حول التساؤل الرئيس التالي: ما مدى كفاية الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية في تنظيم التزامات الجهات التقنية، وما أوجه التقارب والافتراق بينه وبين اللائحة الأوروبية العامة لحماية البيانات(GDPR)؟

أسئلة الدراسة

1. ما الأحكام العامة لنظام حماية البيانات الشخصية السعودي من حيث نطاق التطبيق والمبادئ الأساسية وحقوق أصحاب البيانات؟
2. ما الالتزامات النظامية المفروضة على الجهات التقنية بوصفها جهات تحكّم أو جهات معالجة بموجب النظام ولائحته التنفيذية؟
3. ما التدابير التقنية والتنظيمية التي يتطلبها النظام من الجهات التقنية لضمان حماية البيانات الشخصية ومنع تسريبها؟
4. ما أوجه التقارب والافتراق بين نظام حماية البيانات الشخصية السعودي واللائحة الأوروبية العامة لحماية البيانات (GDPR)فيما يخصّ التزامات الجهات التقنية؟
5. ما التوصيات المقترحة لتطوير الإطار النظامي السعودي بما يعزّز فعالية التزامات الجهات التقنية في حماية البيانات الشخصية؟

أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق الأهداف التالية:

1. بيان الأحكام العامة لنظام حماية البيانات الشخصية السعودي ولائحته التنفيذية من حيث نطاق التطبيق والمبادئ والحقوق.
2. تحديد الالتزامات النظامية المفروضة على الجهات التقنية بوصفها جهات تحكّم أو معالجة، وتحليل مضمونها ونطاقها.
3. تحليل التدابير التقنية والتنظيمية المطلوبة نظامياً من الجهات التقنية لحماية البيانات الشخصية.
4. إجراء مقارنة بين النظام السعودي واللائحة الأوروبية العامة لحماية البيانات (GDPR) فيما يتصل بالتزامات الجهات التقنية.
5. تقديم توصيات لتطوير المنظومة النظامية السعودية بما يواكب التطورات التقنية ويعزّز حماية البيانات الشخصية.

أهمية الدراسة

تنبع أهمية هذه الدراسة من كونها تعالج موضوعاً حيوياً يقع عند نقطة التقاطع بين القانون والتقنية في ظل التحوّل الرقمي الذي تشهده المملكة العربية السعودية ضمن رؤية 2030.

فمن الناحية العلمية: تُسهم الدراسة في إثراء المكتبة القانونية العربية بدراسة تحليلية مقارنة متخصصة في مجال لا يزال حديث العهد في الفقه القانوني السعودي، لا سيما فيما يتعلق بالتزامات الجهات التقنية تحديداً.

ومن الناحية العملية: تكتسب الدراسة أهميتها من حاجة الجهات التقنية العاملة في المملكة إلى فهم دقيق لالتزاماتها النظامية في ظل بدء مرحلة الإنفاذ الفعلي للنظام وصدور قرارات العقوبات من لجان النظر في مخالفات النظام، كما تفيد الدراسة المشرّع السعودي من خلال تقديم رؤية مقارنة مع التجربة الأوروبية قد تُسهم في تطوير الأدلة الإرشادية والتنظيمات التفصيلية المتعلقة بالقطاع التقني.

منهجية الدراسة

تعتمد هذه الدراسة على المنهج التحليلي المقارن؛ إذ يُستخدم المنهج التحليلي في دراسة نصوص نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم (م/19) لعام 1443هـ المعدّل، ولائحته التنفيذية، والأدلة الإرشادية الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)؛ وذلك لاستخلاص الأحكام والالتزامات المتعلقة بالجهات التقنية وتحليل مضامينها، كما يُستخدم المنهج المقارن في مقارنة هذه الأحكام بما يقابلها في اللائحة الأوروبية العامة لحماية البيانات (GDPR)الصادرة عام 2016م؛ بهدف الوقوف على أوجه التقارب والافتراق بين النظامين، واستخلاص ما يمكن الاستفادة منه في تطوير الإطار النظامي السعودي.

الخطة البحثية

المبحث الأول: الأحكام العامة لنظام حماية البيانات الشخصية السعودي:

- المطلب الأول: التعريف بالنظام ونطاق تطبيقه والتطور التشريعي له:
  - الفرع الأول: التعريف بنظام حماية البيانات الشخصية وسياقه التشريعي.
  - الفرع الثاني: نطاق تطبيق النظام من حيث الأشخاص والموضوع والمكان.
- المطلب الثاني: المبادئ الأساسية لحماية البيانات الشخصية وحقوق أصحابها:
  - الفرع الأول: المبادئ العامة التي يقوم عليها النظام.
  - الفرع الثاني: حقوق أصحاب البيانات الشخصية وضماناتها.

المبحث الثاني: التزامات الجهات التقنية في ضوء نظام حماية البيانات الشخصية السعودي واللائحة الأوروبية العامة لحماية البيانات - (GDPR) دراسة مقارنة:

- المطلب الأول: الالتزامات النظامية لجهات التحكّم والمعالجة التقنية في النظام السعودي:
  - الفرع الأول: التزامات جهة التحكم التقنية (الموافقة، الشفافية، تقييم الأثر، حفظ السجلات).

- الفرع الثاني: التزامات جهة المعالجة التقنية والتدابير التقنية والتنظيمية المطلوبة.
- المطلب الثاني: المقارنة مع اللائحة الأوروبية العامة لحماية البيانات(GDPR):
  - الفرع الأول: أوجه التقارب بين النظام السعودي واللائحة الأوروبية في تنظيم التزامات الجهات التقنية.
  - الفرع الثاني: أوجه الافتراق والفجوات التنظيمية وسُبل تطوير النظام السعودي.

الخاتمة:

وتشمل أبرز النتائج التي توصّلت إليها الدراسة، والتوصيات المقترحة لتطوير الإطار النظامي.

المبحث الأول الأحكام العامة لنظام حماية البيانات الشخصية السعودي

يُمثّل صدور نظام حماية البيانات الشخصية بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدَّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، نقلةً تشريعية نوعية في المنظومة القانونية السعودية، إذ انتقل المشرّع من الحماية المتناثرة للخصوصية عبر نصوص متفرقة في نظام مكافحة جرائم المعلوماتية ونظام التعاملات الإلكترونية وغيرهما، إلى تشريع موحّد ومتكامل يُنظّم دورة حياة البيانات الشخصية من الجمع حتى الإتلاف. وقد وصف الشهري (2023) هذا التحول بأنه "استجابة تشريعية ناضجة لمتطلبات الاقتصاد الرقمي ورؤية المملكة 2030"، مؤكداً أن النظام جاء ليسدّ فراغاً تشريعياً طالما شكّل عائقاً أمام تدفق الاستثمارات الرقمية وثقة المستهلك في البيئة الإلكترونية السعودية. ويرى عبد الرحمن (2024) أن النظام يُجسّد ما يُعرف بـ "السيادة الرقمية"، حيث فرض المشرّع رقابة إقليمية على البيانات الشخصية للمواطنين والمقيمين بوصفها ثروة وطنية تستوجب الحماية القانونية.

ويتناول هذا المبحث الأحكام العامة للنظام في ثلاثة مطالب: يُخصَّص الأول للإطار المفاهيمي والنطاق التطبيقي، ويُعنى الثاني بالمبادئ الحاكمة لمعالجة البيانات، بينما يستعرض الثالث حقوق أصحاب البيانات وضماناتها القانونية.

المطلب الأول: الإطار المفاهيمي والنطاق التطبيقي للنظام:

الفرع الأول: التعريفات الجوهرية:

عرّفت المادة الأولى من النظام "البيانات الشخصية" 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 الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة والمتحركة، وغيرها من البيانات ذات الطابع الشخصي.

ويتّسم هذا التعريف بالسعة والمرونة، إذ يشمل البيانات المباشرة (كالاسم ورقم الهوية) والبيانات غير المباشرة التي يمكن ربطها بالفرد عبر التقاطع مع بيانات أخرى، وهو ما يتوافق مع المعيار الذي تبنّته المادة (1/4) من اللائحة الأوروبية العامة لحماية البيانات (GDPR) بشأن "المعلومات المتعلقة بشخص طبيعي محدد أو قابل للتحديد". وقد أشارت الشمري (2023) في دراستها المقارنة إلى أن المشرّع السعودي "استلهم من المعيار الأوروبي إطاره العام، لكنه صاغه بلغة أكثر تفصيلاً واستيعاباً للحالات التطبيقية"، وهو ما يُعزّز الوضوح التشريعي ويُقلّل من هامش التأويل الفقهي.

وفي السياق ذاته، عرّفت المادة الأولى "البيانات الشخصية الحساسة" بأنها": كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية، وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تدل على هويته، أو البيانات الوراثية، والبيانات الائتمانية، والبيانات الصحية، والموقع الجغرافي، والبيانات التي تدل على أن أحد والدَي الفرد أو كليهما مجهول."

ويلاحظ أن المشرّع السعودي وسّع مفهوم البيانات الحساسة ليشمل عناصر لم يتطرّق إليها نظيره الأوروبي صراحةً، كالبيانات الائتمانية والموقع الجغرافي وبيانات مجهولية الأبوين، وهو توسّع يعكس – كما يرى Alkhedhairy (2025) – "خصوصية السياق الاجتماعي والاقتصادي السعودي، لا سيما في القطاع المالي والتأميني، حيث تُشكّل البيانات الائتمانية أداةً حساسة قد يُساء استخدامها في تقييم المخاطر أو التسعير التمييزي". ويترتب على تصنيف البيانات بوصفها حساسة نظامٌ قانوني أشد صرامةً، يظهر في اشتراطات الموافقة الصريحة، والقيود على النقل خارج المملكة، والعقوبات المشدّدة في حال الإفشاء غير المشروع.

كما عرّفت المادة الأولى "المعالجة" بأنها": أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والتنظيم، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستخدام، والإفصاح، والنقل، والنشر، وتشارُك البيانات أو الربط البيني، والحجب، والمحو، والإتلاف ." ويتّضح من هذا التعريف الشمولي أن المشرّع تبنّى مقاربة "دورة حياة البيانات" الكاملة، بحيث لا تُفلت أي عملية تقنية من الخضوع لأحكام النظام.

وقد ميّز النظام بين طرفين محوريين في منظومة المعالجة :جهة التحكم التي عرّفتها المادة الأولى بأنها "أي شخص ذي صفة عامة أو خاصة يُحدّد – بمفرده أو بالاشتراك مع غيره – الغرض من معالجة البيانات الشخصية وطريقة معالجتها"، وجهة المعالجة التي هي "أي شخص ذي صفة عامة أو خاصة يُعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها ."ويُعدّ هذا التمييز جوهرياً لتحديد نطاق المسؤولية القانونية، وهو ما تناوله المطيري (2025) بالتحليل مبيّناً أن "جهة التحكم تتحمّل المسؤولية الأصيلة عن الامتثال، بينما تتحمّل جهة المعالجة مسؤولية تبعية مقيّدة بحدود التعليمات المكتوبة الصادرة إليها من جهة التحكم".

الفرع الثاني: النطاق التطبيقي للنظام:

حدّدت المادة الثانية من النظام نطاق تطبيقه، إذ نصّت على أن أحكامه تسري على "أي معالجة للبيانات الشخصية التي تتم داخل المملكة بأي وسيلة كانت، بما في ذلك معالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة بأي وسيلة كانت من قِبل أي جهة خارج المملكة ". ويتضح من ذلك أن النطاق التطبيقي يمتد على ثلاثة مستويات:

النطاق الشخصي :يشمل كل شخص طبيعي تُعالَج بياناته الشخصية، سواء أكان مواطناً أم مقيماً، ويستوي في ذلك أن يكون الشخص بالغاً أم قاصراً، مع اشتراطات خاصة بالقُصّر تتعلق بموافقة الولي الشرعي. وقد أشارت الغامدي (2024) إلى أن هذا النطاق الواسع "يُوفّر حماية شاملة تتجاوز فكرة المواطنة إلى معيار الإقامة، مما يُعزّز الثقة الرقمية في السوق السعودي".

النطاق الموضوعي :يشمل كل عمليات المعالجة بأي وسيلة، آلية كانت أم يدوية، ومن ذلك المعالجة عبر التطبيقات الإلكترونية والمنصات الرقمية التي أفرد لها فلاتة (2025) دراسة معمّقة، مبيّناً أن "المشرّع السعودي عالج تحديات المنصات الرقمية عبر توسيع مفهوم المعالجة ليشمل كل تفاعل تقني مع البيانات، بما في ذلك عمليات التحليل الآلي والتنميط والذكاء الاصطناعي".

النطاق المكاني (الأثر خارج الإقليمي) :وهو من أبرز ملامح النظام، إذ امتد ليطال الجهات الأجنبية التي تُعالج بيانات المقيمين في المملكة، وهو ما يتوافق مع مقاربة المادة (3) من GDPR بشأن الأثر خارج الإقليمي، ويرى AlSulaimi (2026) أن هذا التوسّع "يُرسّخ مبدأ السيادة الرقمية السعودية ويُلزم الشركات متعددة الجنسيات بالامتثال لأحكام النظام عند تقديم خدماتها لسوق المملكة، حتى لو كانت مقارّها خارجها"، كما وصف Suliman (2025) هذا الامتداد بأنه "خطوة استراتيجية تُموضِع المملكة ضمن منظومة الحوكمة الرقمية العالمية".

واستثنت المادة الثانية من التطبيق "المعالجة الشخصية أو العائلية للبيانات الشخصية "التي لا تتجاوز الاستخدام الخاص للفرد أو أسرته، بشرط ألا يتم نشر تلك البيانات أو الإفصاح عنها للغير، وهو استثناء يقابل ما يُعرف في GDPR بـ "الاستثناء المنزلي (Household Exemption) "الوارد في المادة (2/2/ج).

الفرع الثالث: التطور التشريعي وتاريخ النفاذ:

مرّ النظام بمراحل تطور تشريعي جدير بالإشارة؛ فبعد صدوره أولاً في عام 1443هـ، تدخّل المشرّع بتعديلات جوهرية عبر المرسوم الملكي رقم (م/148) في عام 1444هـ، شملت – وفق تحليل إمام والحربي (2024) – "تعديل أحكام الموافقة، وإعادة صياغة قواعد نقل البيانات خارج المملكة، وتخفيف بعض العقوبات مع تشديد أخرى، بما يعكس استجابة تشريعية مرنة للملاحظات التي أبدتها القطاعات الاقتصادية والتقنية خلال المهلة التصحيحية". وقد مُنحت الجهات المخاطبة بأحكام النظام مهلة تصحيحية امتدّت حتى 1445/9/14هـ لتوفيق أوضاعها، وهي مهلة اعتبرها Almebrad (2018) في دراسته الاستباقية عن كفاية حماية الخصوصية في المملكة "ضرورة عملية تُتيح للمنشآت بناء بنية امتثال متكاملة قبل بدء الإنفاذ الفعلي".

المطلب الثاني: المبادئ الحاكمة لمعالجة البيانات الشخصية:

استقرّت الأنظمة القانونية المعاصرة لحماية البيانات على مجموعة من المبادئ الجوهرية التي تُشكّل العمود الفقري لأي معالجة مشروعة، وقد تبنّى النظام السعودي هذه المبادئ صراحةً أو ضمناً في مواده، وسنستعرضها فيما يلي.

الفرع الأول: مبدأ المشروعية والشفافية:

يقتضي هذا المبدأ أن تكون معالجة البيانات مستندةً إلى أساس نظامي مشروع، وأن يكون صاحب البيانات على علم بها. وقد كرّسته المادة السادسة من النظام باشتراط الحصول على موافقة صاحب البيانات قبل جمعها أو معالجتها، مع استثناءات محدّدة وردت في المادة السادسة عشرة، منها: تحقيق مصلحة مشروعة لجهة التحكم دون الإخلال بحقوق صاحب البيانات، أو تنفيذ نظام أو تعاقد يكون صاحب البيانات طرفاً فيه.

ويرى Alhazmi & Daghistani (2025) في دراستهما الميدانية لممارسات الخصوصية في المواقع الإلكترونية السعودية الشهيرة أن "الشفافية تُمثّل التحدي التطبيقي الأبرز، إذ إن كثيراً من المواقع لا تُقدّم سياسات خصوصية واضحة ومتوافقة مع اشتراطات النظام، مما يستوجب تدخّلاً رقابياً أكثر فاعلية من سدايا"، ويتقاطع هذا مع ما لاحظته القحطاني (2024) من أن "الفجوة بين النص النظامي والممارسة التطبيقية لا تزال قائمة، لا سيما في القطاع الخاص، حيث يغيب الوعي المؤسسي بمتطلبات الإفصاح والشفافية".

الفرع الثاني: مبدأ تحديد الغرض وتقليل البيانات:

تنص المادة الحادية عشرة على أنه "لا يجوز لجهة التحكم أن تجمع من البيانات الشخصية إلا الحد الأدنى الذي يكفي لتحقيق غرض الجمع، وأن يكون الجمع بصورة مباشرة من صاحب البيانات الشخصية"، كما اشترطت المادة العاشرة أن يكون الغرض "مرتبطاً مباشرةً بأغراض جهة التحكم، وألا يتعارض مع الأنظمة".

ويُجسّد هذا المبدأ ما يُعرف بـ "تقليل البيانات (Data Minimization)" المنصوص عليه في المادة (5/1/ج) من GDPR. وقد أشارت الشمري (2023) إلى أن "المبدأ يُشكّل قيداً جوهرياً على النهم المؤسسي في جمع البيانات، ويُلزم الجهات التقنية بمراجعة سياساتها الداخلية لضمان التناسب بين البيانات المجموعة والغرض المُعلن". ويرى عبد الرحمن (2024) أن هذا المبدأ "يُعدّ الترجمة العملية لفكرة الخصوصية بالتصميم(Privacy by Design) ، إذ يُلزم المطوّرين ببناء الأنظمة على أساس الاقتصاد في البيانات منذ لحظة التصميم الأولى".

الفرع الثالث: مبدأ الدقة وتحديث البيانات:

اشترطت المادة الخامسة من اللائحة التنفيذية أن تكون البيانات المُعالَجة "دقيقة وصحيحة وكاملة ومحدّثة"، بما يتوافق مع الغرض من المعالجة. ويُلقي هذا المبدأ التزاماً إيجابياً على جهة التحكم بمراجعة البيانات دورياً وتصحيحها كلما لزم، بل ومحوها إذا انتفى الغرض من الاحتفاظ بها.

الفرع الرابع: مبدأ الأمن والسرية:

ألزمت المادة التاسعة عشرة جهةَ التحكم باتخاذ "التدابير التنظيمية والإدارية والفنية اللازمة لضمان الحفاظ على البيانات الشخصية، بما في ذلك عند نقلها"، ويُعدّ هذا المبدأ حجر الزاوية في التزامات الجهات التقنية، وسيُفصَّل تحليله في المبحث الثاني. وقد أوضحت حسن (2024) أن "الإخلال بمبدأ الأمن يُشكّل الأساس الأبرز للمسؤولية المدنية عن الاعتداء على البيانات الشخصية، إذ يُمثّل خرقاً لالتزام قانوني ببذل عناية مشدّدة".

الفرع الخامس: مبدأ المساءلة والحوكمة:

يُلزم هذا المبدأ جهة التحكم بأن تكون قادرةً على إثبات امتثالها لأحكام النظام، لا مجرد ادعاء ذلك. ويظهر تكريسه في اشتراطات تسجيل عمليات المعالجة، وإجراء تقييمات الأثر، وتعيين مسؤول حماية البيانات في الحالات التي تحددها اللائحة، ويرى Alharbi (2025) أن "مبدأ المساءلة يُحوّل عبء الإثبات في دعاوى خرق البيانات، إذ تُصبح جهة التحكم مطالَبة بإثبات بذلها للعناية الواجبة، لا صاحب البيانات مطالباً بإثبات التقصير".

المطلب الثالث: حقوق أصحاب البيانات وضماناتها:

منح النظام صاحب البيانات الشخصية جملةً من الحقوق التي تُشكّل الوجه المقابل لالتزامات جهات التحكم والمعالجة، وقد نصّت عليها المادة الرابعة من النظام بصورة إجمالية، وفصّلتها اللائحة التنفيذية.

الحق في العلم: وهو حق صاحب البيانات في معرفة الأساس النظامي والغرض من جمع بياناته، ومن سيطّلع عليها، وطبيعة البيانات المطلوبة. ويُمثّل هذا الحق التطبيق العملي لمبدأ الشفافية.

الحق في الوصول إلى البيانات: يخوّل صاحب البيانات الاطلاع على بياناته المُعالَجة والحصول على نسخة منها بصيغة واضحة ومقروءة، دون مقابل في الأصل، ما لم تتكرر الطلبات بصورة مبالغ فيها.

الحق في التصحيح: يُتيح لصاحب البيانات طلب تصحيح ما هو غير دقيق أو مكتمل أو محدّث من بياناته لدى جهة التحكم.

الحق في الإتلاف (المحو): يُمكّن صاحب البيانات من طلب إتلاف بياناته متى انتفى الغرض من الاحتفاظ بها، وهو ما يقابل "الحق في النسيان (Right to Be Forgotten)" في GDPR وفق المادة (17) منه. وقد أشارت الشمري (2023) إلى أن "المشرّع السعودي تبنّى الحق في الإتلاف بصيغة أكثر تحفّظاً من نظيره الأوروبي، إذ قيّده باستثناءات تتعلق بالمصلحة العامة والالتزامات النظامية".

الحق في نقل البيانات : يُتيح لصاحب البيانات الحصول على نسخة من بياناته بصيغة منظّمة تُمكّنه من نقلها إلى جهة تحكم أخرى، وهو حق مستحدث يعكس فلسفة تمكين الفرد من التحكم في بياناته الرقمية، ويرى AlSulaimi (2026) أن هذا الحق "يُعزّز المنافسة في الأسواق الرقمية ويُقلّل من ظاهرة الاحتجاز التقني للمستخدمين لدى مقدّمي الخدمة".

وتبقى فاعلية هذه الحقوق مرهونةً بوجود آليات تنفيذية واضحة، وهو ما لاحظته القحطاني (2024) بقولها إن "الفجوة بين تقرير الحق نظامياً وإعماله عملياً تستوجب تعزيز دور سدايا في إصدار الأدلة الإرشادية، وتفعيل قنوات الشكاوى، وتدريب الجهات المخاطبة على استيعاب هذه الحقوق ضمن سياساتها الداخلية".

المبحث الثاني التزامات الجهات التقنية (جهات التحكم والمعالجة) في ضوء النظام السعودي

تكتسب هذه الالتزامات أهميتها من كونها المحك الحقيقي لفاعلية النظام، إذ إن الحقوق المُقرّرة لصاحب البيانات تبقى نظريةً ما لم تُقابلها التزامات تفصيلية وقابلة للإنفاذ على الجهات المُعالِجة، وقد أشار المطيري (2025) إلى أن "منظومة الالتزامات في النظام السعودي تعكس تحوّلاً من نموذج الحماية السلبية إلى نموذج الحماية الإيجابية القائم على المسؤولية المؤسسية المُوثّقة".

ويتناول هذا المبحث الالتزامات في أربعة مطالب: الأول للالتزامات القانونية والتنظيمية، والثاني للالتزامات التقنية والأمنية، والثالث لضوابط نقل البيانات خارج المملكة، والرابع لنظام المسؤولية والحماية الجزائية مقارنةً بـ.GDPR

المطلب الأول: الالتزامات القانونية والتنظيمية لجهات التحكم والمعالجة:

الفرع الأول: التزامات جهة التحكم:

تتحمّل جهة التحكم بوصفها المسؤول الأصيل عن معالجة البيانات جملةً من الالتزامات القانونية التي حدّدها النظام واللائحة التنفيذية، ويمكن تصنيفها على النحو الآتي:

أولاً: الالتزام بالتسجيل في السجل الوطني: اشترطت المادة الثالثة والثلاثون من اللائحة التنفيذية على جهات التحكم – في الحالات التي تحددها الهيئة – التسجيل في السجل الوطني لجهات التحكم في البيانات الشخصية، وتقديم بيانات تفصيلية عن طبيعة نشاطها وأنواع البيانات التي تُعالجها. ويُمثّل هذا الالتزام أداةً رقابية استباقية تُتيح للجهة التنظيمية (سدايا) الإحاطة بمشهد المعالجة على المستوى الوطني.

ثانياً: الالتزام بإعداد سياسة الخصوصية: ألزمت المادة الثانية عشرة جهة التحكم بأن تُتيح لصاحب البيانات، قبل جمع بياناته، الاطلاع على سياسة الخصوصية التي تُبيّن الغرض من الجمع، والبيانات المطلوبة، ووسائل الجمع، وكيفية معالجة البيانات وحفظها وإتلافها، وحقوق صاحب البيانات وسبل ممارستها. وقد كشفت الدراسة الميدانية التي أجراها Alhazmi &Daghistani (2025) أن "نسبةً معتبرة من المواقع السعودية الأكثر زيارةً لا تلتزم بالحد الأدنى من متطلبات سياسة

الخصوصية، إذ تفتقر إلى بيان واضح لأسس المعالجة أو مدد الاحتفاظ أو آليات ممارسة الحقوق"، وهو ما يستوجب – بحسب الباحثَيْن – تفعيل الرقابة اللاحقة وتوقيع جزاءات رادعة على المخالفين.

ثالثاً: الالتزام بالحصول على الموافقة: يُشكّل مبدأ الموافقة الحرّة والصريحة والمُستنيرة الأساسَ العام للمعالجة المشروعة، وفق ما نصّت عليه المادة السادسة من النظام. ويُقابل هذا الالتزام ما ورد في المادتين (6) و(7) من GDPR بشأن اشتراطات صحة الموافقة، إلا أن فلاتة (2025) لاحظت أن "المشرّع السعودي كان أكثر مرونةً في قبول الموافقة الضمنية في بعض حالات المعالجة ذات المصلحة المشروعة، بينما يميل المشرّع الأوروبي إلى التشدّد في اشتراط الموافقة الصريحة، مما يجعل النموذج السعودي أكثر ملاءمةً لبيئة الأعمال الرقمية دون التفريط في جوهر الحماية".

رابعاً: الالتزام بإجراء تقييم أثر معالجة البيانات: يستوجب النظام إجراء تقييم للأثر (Data Protection Impact Assessment) قبل الشروع في عمليات معالجة تنطوي على مخاطر مرتفعة على حقوق أصحاب البيانات، كعمليات التنميط الآلي، أو المعالجة واسعة النطاق للبيانات الحساسة. ويرى Alkhedhairy (2025) أن "تقييم الأثر يُمثّل أداةً استباقية لموازنة المصلحة المشروعة للجهة مع مخاطر المعالجة على الأفراد، لا سيما في القطاعات الحساسة كالتأمين والائتمان، حيث قد تُفضي المعالجة إلى تسعير تمييزي أو استبعاد غير مبرّر".

خامساً: الالتزام بتعيين مسؤول حماية البيانات (DPO): حدّدت اللائحة التنفيذية الحالات التي يجب فيها تعيين مسؤول لحماية البيانات، ومنها كون النشاط الرئيسي لجهة التحكم يقوم على معالجة واسعة النطاق للبيانات الحساسة، أو يستوجب مراقبةً منتظمة ومنهجية لأصحاب البيانات. ويتقاطع هذا مع المادة (37) من GDPR ، غير أن حسن (2024) لاحظت أن "الفارق يكمن في تفصيل اللائحة الأوروبية لضمانات استقلال المسؤول وحمايته من العزل التعسفي، وهو ما يستوجب من المشرّع السعودي مزيداً من التدقيق في الأدلة الإرشادية الصادرة عن سدايا".

الفرع الثاني: التزامات جهة المعالجة:

تتحمّل جهة المعالجة التزامات تبعية تنبع من علاقتها بجهة التحكم، أبرزها:

الالتزام بالتعليمات المكتوبة: لا يجوز لجهة المعالجة أن تُعالج البيانات إلا وفق التعليمات الصادرة إليها من جهة التحكم، وفي حدود العقد المبرم بينهما.

الالتزام بالسرية: يمتد التزام السرية إلى موظفي جهة المعالجة، ويستمر حتى بعد انتهاء العلاقة التعاقدية.

الالتزام بعدم الاستعانة بمعالج فرعي إلا بإذن: لا يجوز لجهة المعالجة إسناد كل أو بعض المعالجة إلى طرف ثالث إلا بموافقة كتابية مسبقة من جهة التحكم.

وقد أوضح المطيري (2025) أن "التمييز بين مسؤولية جهة التحكم ومسؤولية جهة المعالجة يُعدّ من أهم التطويرات التي جاء بها النظام، إذ يُتيح توزيعاً عادلاً للمسؤولية بين الأطراف بحسب دور كلٍّ منها الفعلي في المعالجة، مما يُقلّل من ظاهرة تحميل الطرف الأضعف تبعات لا يتحكم فيها".

المطلب الثاني: الالتزامات التقنية والأمنية:

يُعدّ البُعد التقني ركيزةً أساسية في منظومة حماية البيانات، إذ إن التشريع مهما بلغت دقّته يبقى قاصراً ما لم يُقابله التزام تقني فعّال. وقد أوجب النظام على الجهات التقنية اتخاذ تدابير تقنية وتنظيمية مناسبة تتناسب مع طبيعة البيانات ومستوى المخاطر.

الفرع الأول: تدابير الأمن السيبراني:

نصّت المادة التاسعة عشرة على وجوب اتخاذ "التدابير التنظيمية والإدارية والفنية اللازمة" لضمان أمن البيانات، وفصّلت اللائحة التنفيذية هذه التدابير لتشمل: التشفير أثناء التخزين والنقل، وضوابط التحكم في الوصول، وتسجيل عمليات المعالجة (Logging)، والاختبار الدوري لفاعلية التدابير، وإجراء تحديثات أمنية منتظمة.

ويرى Alharbi (2025) في تحليله الفقهي لخرق البيانات وفق النظام السعودي أن "معيار العناية الواجبة في التدابير التقنية يُقاس بمستوى المخاطر المرتبطة بطبيعة البيانات، لا بمعيار موحّد، مما يجعل الالتزام تناسبياً ومرناً"، مضيفاً أن "إثبات بذل جهة التحكم للعناية الواجبة يُشكّل الدفع الجوهري في دعاوى المسؤولية عن خرق البيانات".

الفرع الثاني: الخصوصية بالتصميم والافتراضية:

تبنّى النظام ولو ضمناً مفهومَي "الخصوصية بالتصميم (Privacy by Design)" و"الخصوصية بالإعداد الافتراضي(Privacy by Default)"، وهما مفهومان صريحان في المادة (25) من GDPR. ويقتضي المفهوم الأول أن تُدمج ضمانات الخصوصية في تصميم الأنظمة والتطبيقات منذ مراحلها الأولى، بينما يقتضي الثاني أن تكون الإعدادات الافتراضية للنظام هي الأكثر حمايةً للخصوصية.

وقد أشارت فلاتة (2025) إلى أن "التطبيقات الإلكترونية والمنصات الرقمية السعودية تواجه تحدياً حقيقياً في إعمال مبدأ الخصوصية بالتصميم، إذ إن كثيراً منها بُنيت قبل صدور النظام على معمارية تقنية لا تُراعي هذه المبادئ، مما يستوجب إعادة هندسة جوهرية لا مجرد تعديلات سطحية". وفي السياق ذاته، لاحظت الغامدي (2024) أن "تقنيات الذكاء الاصطناعي تُشكّل تحدياً استثنائياً لمبدأ الخصوصية بالتصميم، لأنها تعتمد على معالجة كميات هائلة من البيانات لأغراض تدريب النماذج، مما يستوجب تطوير أدوات تقنية جديدة كالتعلّم الاتحادي (Federated Learning) والخصوصية التفاضلية (Differential Privacy)".

الفرع الثالث: الإخطار بحوادث خرق البيانات:

ألزم النظام جهةَ التحكم بإخطار الهيئة (سدايا) فور علمها بأي حادثة خرق للبيانات أو تسرّب أو وصول غير مشروع، وذلك خلال المدة التي تحددها اللائحة، مع إخطار صاحب البيانات إذا كان من شأن الحادثة الإضرار به. ويُقابل هذا ما نصّت عليه المادتان (33) و(34) من GDPR بشأن الإخطار خلال 72 ساعة.

وقد أوضحت حسن (2024) أن "الالتزام بالإخطار يُعدّ من الالتزامات الجوهرية التي يترتب على الإخلال بها مسؤولية مدنية مستقلة عن مسؤولية الخرق ذاته، إذ يُشكّل الإخطار المتأخر إخلالاً بواجب الشفافية تجاه صاحب البيانات وتفويتاً لفرصته في اتخاذ التدابير الوقائية".

المطلب الثالث: ضوابط نقل البيانات الشخصية خارج المملكة:

أفرد المشرّع السعودي أحكاماً مفصّلة لنقل البيانات خارج المملكة، إدراكاً منه لخصوصية هذا الجانب وارتباطه بالسيادة الرقمية. فقد نصّت المادة التاسعة والعشرون من النظام – بعد تعديلها بالمرسوم م/148 – على اشتراطات نقل البيانات، وأصدرت سدايا لائحة تنفيذية مستقلة بعنوان "لائحة نقل البيانات الشخصية خارج المملكة" لتفصيل هذه الاشتراطات.

وتتلخّص ضوابط النقل في: (1) وجود ضرورة تستدعي النقل، (2) ألا يُخلّ النقل بالسيادة الوطنية أو الأمن الوطني، (3) توفير مستوى ملائم من الحماية في الدولة المُستقبِلة لا يقل عن المستوى المقرّر في النظام، (4) الحصول على موافقة الجهة المختصة عند الاقتضاء.

ويرى عبد الرحمن (2024) في دراسته عن السيادة الرقمية أن "أحكام نقل البيانات في النظام السعودي تعكس توازناً دقيقاً بين متطلبات الاقتصاد الرقمي المفتوح وضرورات السيادة الوطنية، وقد جاء التعديل بالمرسوم م/148 لتخفيف بعض القيود التي رأى المشرّع أنها مبالَغ فيها، دون التفريط في الجوهر الحمائي"، ويُقارن AlSulaimi (2026) هذه الأحكام بنظام قرارات الكفاية (Adequacy Decisions) الأوروبي، مبيّناً أن "المشرّع السعودي تبنّى مقاربة أكثر مرونة تعتمد على التقييم الفردي للحالات بدلاً من إصدار قرارات كفاية عامة، مما يمنح سدايا سلطة تقديرية واسعة قد تكون أداةً فاعلة أو مصدر عدم يقين للمنشآت العاملة عبر الحدود".

المطلب الرابع: نظام المسؤولية والحماية الجزائية:

يُشكّل نظام المسؤولية والجزاءات الضامنَ الأخير لفاعلية الالتزامات المتقدّمة، إذ لا قيمة للالتزام دون جزاء رادع على مخالفته. وقد تبنّى المشرّع السعودي منظومةً متعددة الأبعاد للمسؤولية، تشمل الجزائية والمدنية والإدارية.

الفرع الأول: الحماية الجزائية:

نصّت المواد الخامسة والثلاثون وما بعدها من النظام على العقوبات الجزائية للإخلال بأحكامه، وتتدرّج بحسب جسامة المخالفة. فقد قرّرت المادة الخامسة والثلاثون عقوبةَ السجن مدةً لا تزيد على سنتين، والغرامة التي لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، لكل من أفصح عن بيانات شخصية حساسة أو أتاحها بالمخالفة لأحكام النظام، بقصد الإضرار

بصاحبها أو تحقيق منفعة. كما قرّرت المادة السادسة والثلاثون عقوبةَ السجن مدةً لا تزيد على سنة، والغرامة التي لا تزيد على مليون ريال، أو بإحدى هاتين العقوبتين، لكل من نقل بيانات شخصية خارج المملكة بالمخالفة لأحكام النظام.

وقد أجرى الجعيد (2025) دراسةً معمّقة للحماية الجزائية في النظام السعودي، خلص فيها إلى أن "المشرّع السعودي انتهج سياسة جزائية متوازنة تجمع بين الردع العام عبر تشديد العقوبات على البيانات الحساسة، والردع الخاص عبر إتاحة الجزاءات البديلة والغرامات المالية على المخالفات الأقل جسامة". وأضاف أن "التعديل الوارد بالمرسوم م/148 خفّف العقوبة الأصلية التي كانت تصل إلى السجن خمس سنوات، وهو ما يعكس مراجعة تشريعية استجابت لملاحظات الفقه وممارسي القانون بشأن التناسب بين الجريمة والعقوبة".

وفي إطار المقارنة مع تشريعات إقليمية، أوضح العرمان (2022) في دراسته عن الحماية الجزائية للبيانات في التشريع الأردني أن "المشرّع الأردني اعتمد نهجاً أكثر تحفّظاً في تجريم الاعتداء على البيانات، إذ اكتفى بإحالات إلى قانون الجرائم الإلكترونية دون إفراد نصوص جزائية مستقلة، وهو ما يُفضّله البعض لتفادي التضخم التشريعي، لكنه يُنتقد لضعف الحماية المتخصصة". ويلتقي هذا مع تحليل عطية (2024) للسياسة الجنائية السعودية في مكافحة الجريمة المعلوماتية، الذي أكد فيه أن "الجمع بين نظام مكافحة جرائم المعلوماتية ونظام حماية البيانات الشخصية أنشأ منظومة جزائية متكاملة تُغطّي الفراغات التي كانت قائمة قبل صدور النظام".

ولاحظ عبد العزيز (2025) في دراسته عن الحماية الجزائية للخصوصية الرقمية في التشريع الفلسطيني والمعايير الدولية أن "التشريعات العربية تتفاوت تفاوتاً كبيراً في مستوى الحماية الجزائية للبيانات، ويُعدّ النظام السعودي من أكثرها تطوراً من حيث التفصيل والصياغة، وإن كان يحتاج إلى مزيد من الاجتهاد القضائي لبلورة مفاهيمه التطبيقية"، ويُضيف الرواحي (2025) أن "الحماية الجزائية للبيانات في الفضاء الرقمي تستوجب تطوير قدرات الضبط القضائي والادعاء العام، لأن جسامة النص التشريعي لا تُعوّض عن ضعف آليات الإنفاذ".

الفرع الثاني: المسؤولية المدنية:

بالإضافة إلى العقوبات الجزائية، تنعقد المسؤولية المدنية لجهة التحكم أو المعالجة عن الأضرار التي تُسبّبها للغير جراء الإخلال بأحكام النظام. وقد نصّت المادة الحادية والأربعون على حق كل من لحقه ضرر مادي أو معنوي جراء المخالفة في المطالبة بالتعويض أمام المحكمة المختصة.

وقد أفردت حسن (2024) دراسةً معمّقة للمسؤولية المدنية عن الاعتداء على البيانات الشخصية، بيّنت فيها أن "المسؤولية هنا تقوم على أساس الخطأ المفترض، إذ يكفي إثبات وقوع الخرق ونسبته إلى جهة التحكم، وتبقى الأخيرة مطالبةً بإثبات بذلها للعناية الواجبة لدفع المسؤولية"، ويلتقي هذا مع تحليل المطيري (2025) الذي أشار إلى أن "المسؤولية النظامية للشركات عن حماية البيانات لا تُقاس بمعيار الالتزام ببذل عناية عادية، بل بمعيار مشدّد يتناسب مع طبيعة النشاط ومستوى المخاطر".

الفرع الثالث: المقارنة مع منظومة الجزاءات في GDPR:

تختلف منظومة الجزاءات في GDPR اختلافاً جوهرياً عن نظيرتها السعودية من ثلاث زوايا:

الطبيعة: تُغلّب GDPR الطابع الإداري للجزاءات (المادة 83)، بينما يُغلّب النظام السعودي الطابع الجزائي مع دمج بعض العقوبات الإدارية.

المقدار: يصل الحد الأقصى للغرامة في GDPR إلى 20 مليون يورو أو 4% من إجمالي الإيرادات السنوية العالمية للمنشأة، أيهما أعلى، وهو ما يفوق كثيراً الحد الأقصى في النظام السعودي (5 ملايين ريال مع مضاعفتها عند التكرار).

آلية الإنفاذ: تعتمد GDPR على السلطات الإشرافية المستقلة في كل دولة عضو، بينما تعتمد المنظومة السعودية على سدايا كجهة رقابية مركزية، مع إحالة الجانب الجزائي إلى النيابة العامة والمحاكم الجزائية.

وقد لخّصت الشمري (2023) هذه المقارنة بقولها إن "المنظومة الأوروبية أكثر ردعاً من الناحية المالية بحكم ضخامة الغرامات، بينما المنظومة السعودية أكثر ردعاً من الناحية الشخصية بحكم إدراج عقوبة السجن، والفاعلية الفعلية لكلا النموذجَيْن تعتمد على جدية الإنفاذ لا على النص وحده". ويؤيد Suliman (2025) هذا التقييم بقوله إن "فاعلية النظام

السعودي في الاقتصاد الرقمي العالمي ستُقاس خلال السنوات المقبلة بمدى صرامة سدايا في توقيع الجزاءات، ومدى استجابة المحاكم للمفاهيم التقنية الحديثة".

الخاتمة

في ختام هذه الدراسة التي تناولت الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية وأثره على التزامات الجهات التقنية، مع المقارنة التحليلية باللائحة الأوروبية العامة لحماية البيانات(GDPR) ، يمكن تلخيص أبرز ما توصّل إليه البحث من نتائج، وما يُوصي به من توصيات، على النحو الآتي:

أولاً: النتائج:

يُمثّل نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) والمعدَّل بالمرسوم الملكي رقم (م/148) نقلةً تشريعية نوعية، إذ انتقل المشرّع السعودي من مرحلة الحماية المتناثرة عبر نصوص متفرقة إلى تشريع موحّد ومتكامل يُنظّم دورة حياة البيانات كاملةً، وهو ما يُواكب متطلبات رؤية المملكة 2030 ويُعزّز الثقة الرقمية في السوق السعودي.

تبنّى المشرّع السعودي مقاربةً موسّعة لمفهوم البيانات الشخصية والبيانات الحساسة، حيث ضمّ إلى الأخيرة عناصر لم يتطرّق إليها نظيره الأوروبي صراحةً، كالبيانات الائتمانية والموقع الجغرافي، مما يعكس مراعاة الخصوصية الاجتماعية والاقتصادية السعودية، ويُوفّر حمايةً أوسع نطاقاً في بعض الجوانب مقارنةً بـ.GDPR

يمتد النطاق التطبيقي للنظام ليطال الجهات الأجنبية التي تُعالج بيانات المقيمين في المملكة، وهو ما يُرسّخ مبدأ السيادة الرقمية السعودية، ويتقاطع مع مقاربة الأثر خارج الإقليمي فيGDPR، ويُلزم الشركات متعددة الجنسيات بالامتثال لأحكام النظام عند تقديم خدماتها للسوق السعودي.

أرسى النظام منظومةً متكاملة من المبادئ الحاكمة للمعالجة، تشمل المشروعية والشفافية، وتحديد الغرض، وتقليل البيانات، والدقة، والأمن، والمساءلة. غير أن الفجوة بين النص النظامي والممارسة التطبيقية لا تزال قائمة، لا سيما في القطاع الخاص، حيث كشفت الدراسات الميدانية عن قصور واضح في التزام كثير من المواقع والتطبيقات السعودية بمتطلبات الشفافية وسياسات الخصوصية.

ميّز النظام تمييزاً جوهرياً بين جهة التحكم وجهة المعالجة، بما يُتيح توزيعاً عادلاً للمسؤولية بين الأطراف بحسب دور كلٍّ منها الفعلي، وهو تمييز يتقاطع مع مقاربة GDPR ويُقلّل من ظاهرة تحميل الطرف الأضعف تبعات لا يتحكم فيها.

أفرد المشرّع السعودي أحكاماً مفصّلة لنقل البيانات خارج المملكة عبر لائحة تنفيذية مستقلة، وقد جاء تعديل المرسوم م/148 لتخفيف بعض القيود دون التفريط في الجوهر الحمائي. غير أن اعتماد المشرّع السعودي على التقييم الفردي للحالات – خلافاً لنموذج قرارات الكفاية الأوروبي – يمنح سدايا سلطة تقديرية واسعة قد تُشكّل مصدر عدم يقين للمنشآت العاملة عبر الحدود.

تختلف منظومة الجزاءات السعودية عن نظيرتها الأوروبية اختلافاً جوهرياً؛ إذ يُغلّب النظام السعودي الطابع الجزائي مع إدراج عقوبة السجن، بينما تُغلّب GDPR الطابع الإداري مع غرامات مالية ضخمة قد تصل إلى 4% من الإيرادات العالمية للمنشأة. وتبقى فاعلية كلا النموذجَيْن مرهونةً بجدية الإنفاذ لا بالنص وحده.

يتبنّى النظام السعودي ولو ضمناً مفهومَي "الخصوصية بالتصميم" و"الخصوصية بالإعداد الافتراضي"، غير أن التطبيقات والمنصات الرقمية السعودية القائمة قبل صدور النظام تواجه تحدياً جوهرياً في إعادة الهندسة التقنية للامتثال لهذين المفهومَيْن، مما يستوجب دعماً فنياً وإرشادياً متخصصاً من الجهة التنظيمية.

تُشكّل تقنيات الذكاء الاصطناعي والمعالجة الآلية للبيانات تحدياً استثنائياً لمنظومة الحماية، إذ تعتمد هذه التقنيات على معالجة كميات هائلة من البيانات لأغراض التدريب، مما يستوجب تطوير أدوات تقنية جديدة كالتعلّم الاتحادي والخصوصية التفاضلية، وتطوير أدلة إرشادية تنظيمية متخصصة.

ثانياً: التوصيات:

- يُوصي الباحث الهيئةَ السعودية للبيانات والذكاء الاصطناعي (سدايا) بإصدار أدلة إرشادية قطاعية متخصصة تُفصّل تطبيق أحكام النظام على القطاعات الحساسة (المالي، والتأمين، والصحي، والتعليم)، بما يُقلّل من هامش عدم اليقين لدى

الجهات التقنية ويُوحّد الممارسات المهنية.

- يُوصي الباحث بتفعيل دور الرقابة اللاحقة على المواقع الإلكترونية والتطبيقات الرقمية للتحقق من التزامها بمتطلبات سياسات الخصوصية، مع توقيع جزاءات تدريجية على المخالفين، بدءاً بالتنبيه ثم الإنذار ثم الغرامة، بما يُحقّق الردع دون الإخلال بمبدأ التناسب.
- يُوصي الباحث المشرّع بمراجعة السلطة التقديرية الممنوحة لسدايا في تقييم كفاية حماية البيانات في الدول المُستقبِلة، وذلك بإصدار قائمة بالدول ذات الحماية الكافية على غرار نموذج قرارات الكفاية الأوروبية، مما يُوفّر يقيناً قانونياً أعلى للمنشآت العاملة عبر الحدود.
- يُوصي الباحث بتطوير القدرات القضائية والادعائية المتخصصة في قضايا حماية البيانات، عبر إنشاء دوائر متخصصة في المحاكم الجزائية، وتأهيل أعضاء النيابة العامة في المفاهيم التقنية المستجدّة، لأن جسامة النص التشريعي لا تُعوّض عن ضعف آليات الإنفاذ.
- يُوصي الباحث بتعزيز ضمانات استقلال مسؤول حماية البيانات (DPO) داخل المنشآت، عبر النص الصريح في اللائحة التنفيذية على حمايته من العزل التعسفي، وضمان تبعيته المباشرة للإدارة العليا، على غرار ما نصّت عليه المادة (38) من GDPR.
- يُوصي الباحث بإطلاق برامج توعوية موسّعة موجّهة للأفراد بشأن حقوقهم في نظام حماية البيانات، وسبل ممارستها، وقنوات الشكوى المتاحة، لأن فاعلية النظام تعتمد إلى حدٍّ بعيد على وعي أصحاب البيانات بحقوقهم وقدرتهم على المطالبة بها.
- يُوصي الباحث بتطوير إطار تنظيمي متخصص لمعالجة البيانات في سياق تقنيات الذكاء الاصطناعي، يُوازن بين متطلبات تطوير هذه التقنيات وضرورات حماية الخصوصية، عبر تبنّي مبادئ الخصوصية التفاضلية، والتعلّم الاتحادي، وأخلاقيات الذكاء الاصطناعي، بما يتوافق مع توجّهات المملكة الاستراتيجية في هذا المجال.
- يُوصي الباحث بتشجيع البحث العلمي القانوني والتقني المشترك في مجال حماية البيانات، عبر دعم الدراسات التطبيقية والميدانية التي ترصد الفجوات بين النص والتطبيق، وتُقدّم حلولاً عملية قابلة للتبنّي التشريعي والتنظيمي.
- يُوصي الباحث بإنشاء منصة وطنية موحّدة تُتيح لأصحاب البيانات ممارسة حقوقهم (الوصول، التصحيح، الإتلاف، النقل) عبر واجهة إلكترونية موحّدة مع كافة جهات التحكم المسجّلة، بما يُخفّف العبء على الأفراد ويُعزّز فاعلية الحقوق المُقرّرة.

قائمة المراجع

أولاً: التشريعات والأنظمة:

- نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدَّل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية. https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1 .
- اللائحة التنفيذية لنظام حماية البيانات الشخصية (1443هـ). الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). https://sdaia.gov.sa/ar/SDAIA/about/Files/PersonalDataEnglish.pdf .
- لائحة نقل البيانات الشخصية خارج المملكة (1443هـ). الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). https://sdaia.gov.sa/ar/SDAIA/about/Files/RegulationsDataTransferPersonalOutside.pdf .
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

ثانياً: المراجع العربية:

- إمام، م.، والحربي، م. (2024). الحماية القانونية للبيانات الشخصية في النظامين السعودي والعُماني: دراسة مقارنة .مجلة جهينة للدراسات القانونية والشرعية، 3(2)، 1-26828 https://jjls.hji.edu.om/index.php/jjls/article/view .
- الجعيد، ص. (2025). الحماية الجزائية لمعالجة البيانات الشخصية في النظام السعودي: دراسة مقارنة .مجلة جامعة الأندلس للعلوم الاجتماعية والتطبيقية، (114)، 1-32

https://aust.uni.ye/magazine/sh/2025/12/114/e6b6053d4d63e5bfd483d7e2d25fc346.pdf.
- حسن، ه. (2024). المسؤولية المدنية عن الاعتداء على البيانات الشخصية .مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، 40(6)، 200-250 https://kias.journals.ekb.eg/article_501228.html .
- الرواحي، خ. (2025). الحماية الجزائية للبيانات الشخصية في الفضاء الرقمي .مجلة الدراسات القانونية، جامعة الشرق العربي، (12)، 1-60

https://www.asu.edu.om/img/Dissertations/Dissertations_2025_m1d19_121329.pdf.
- الشمري، ن. (2023). حماية البيانات الشخصية في المملكة العربية السعودية والاتحاد الأوروبي: دراسة مقارنة .مجلة العلوم الإنسانية والاجتماعية، 7(45)، 1-25

https://journals.ajsrp.com/index.php/jhss/article/view/7120.
- الشهري، ع. (2023). الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية .مجلة البحوث القانونية والاقتصادية، (82)، 1-40 https://jlr.journals.ekb.eg/article_323132.html .
- عبد الرحمن، م. (2024). السيادة الرقمية في ضوء نظام حماية البيانات الشخصية السعودي: دراسة مقارنة .مجلة البحوث القانونية، (23)، 100-140 https://journals.ekb.eg/article_482375.html .
- عبد العزيز، ع. (2025). الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني ومن منظور المعايير الدولية: دراسة مقارنة (رسالة ماجستير غير منشورة). الجامعة العربية الأمريكية، فلسطين

https://repository.aaup.edu/handle/123456789/3502.
- العرمان، ع. (2022). الحماية الجزائية للبيانات الشخصية في التشريع الأردني: دراسة مقارنة (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمّان، الأردن https://www.meu.edu.jo/libraryTheses/24part2/.الحماية الجزائية للبيانات الشخصية في التشريع الأردنيpdf.
- عطية، ع. (2024). السياسة الجنائية لمكافحة الجريمة المعلوماتية في المملكة العربية السعودية .مجلة البحوث القانونية والاقتصادية، (85)، 1-45 https://jlr.journals.ekb.eg/article_377753.html .
- الغامدي، ن. (2024). الحق في الخصوصية في عصر الذكاء الاصطناعي: دراسة تحليلية .المجلة الدولية للبحوث القانونية والدراسات الشرعية، 2(3)، 45-80 https://vsrp.co.uk/index.php/ijlrs/article/view .
- فلاتة، ح. (2025). حماية البيانات الشخصية في التطبيقات الإلكترونية والمنصات الرقمية في ضوء أحكام النظام السعودي والتشريعات المقارنة .مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع، (108)، 1-30

https://www.jalhss.com/index.php/jalhss/article/view/1576.
- القحطاني، س. (2024). حماية البيانات الشخصية للشركات والمؤسسات والأفراد وفقاً للمعايير القانونية والتنظيمية .المجلة الدولية للأبحاث العلمية، 3(4)، 150-180

https://vsrp.co.uk/index.php/ijsr/article/view/1230 .

- المطيري، ف. (2025). المسؤولية النظامية للشركات عن حماية البيانات الشخصية في النظام السعودي .مجلة البحوث القانونية، (25)، 55-95. https://journals.ekb.eg/article_509048.html .

ثالثاً: المراجع الأجنبية:

- Alharbi, T. (2025). Negligence and data breaches under Saudi Arabian Personal Data Protection Law (PDPL): A doctrinal analysis approach. Journal of Advanced Development in Humanities and Universal Research, 4(2), 30-55

  https://www.jadhur.com/index.php/journal/article/view/321.

- Alhazmi, A., & Daghistani, F. (2025). Privacy practices of popular websites in Saudi Arabia. Journal of Umm Al-Qura University for Engineering and Architecture, 16(1), 1-20

  https://link.springer.com/article/10.1007/s43995-024-00085-x.

- Alkhedhairy, M. (2025). Balancing privacy and risk: A critical analysis of personal data use as governed by Saudi insurance law. Laws, 14(4), 47. https://www.mdpi.com/2075-471X/14/4/47

- Almebrad, A. (2018). The sufficiency of information privacy protection in Saudi Arabia [Doctoral dissertation, Indiana University Maurer School of Law]. IU Maurer School of Law Repository. https://www.repository.law.indiana.edu/etd/56/

- AlSulaimi, A. (2026). Navigating the data protection landscape in Saudi Arabia. Frontiers in Computer Science, 8, 1-15. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2026.1815716/full

- Suliman, H. (2025). Evaluating the effectiveness of Saudi Arabia's PDPL in the global digital economy. Journal of Data Protection & Privacy, 8(1), 97-111

  https://www.ingentaconnect.com/contentone/hsp/jdpp/2025/00000008/00000001/art00008.

رابعاً: المصادر المؤسسية الرسمية:

- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) .مركز المعرفة – البوابة الوطنية لحماية البيانات الشخصيةhttps://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter .
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) .الموقع الرسميhttps://sdaia.gov.sa .
- European Data Protection Board (EDPB). Official website. https://edpb.europa.eu