المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثامن - الإصدار الخامس والثمانون
تاريخ النشر: 20 نوفمبر 2026 م

التحديات القانونية لتدفقات البيانات عبر الحدود في المملكة العربية السعودية (نحو إطار وطني متوافق مع المعايير الدولية)

Legal Challenges to Cross-Border Data Flows in the Kingdom of Saudi Arabia (Towards a National Framework Aligned with International Standards)

إعداد الدكتورة/ منيرة فهد الحمدان

أستاذ مساعد في القانون، كلية الحقوق والعلوم السياسية، جامعة الملك سعود، المملكة العربية السعودية

Email: monalhamdan@ksu.edu.sa

الملخص:

يتناول هذا البحث موضوع التحديات القانونية لتدفقات البيانات عبر الحدود في المملكة العربية السعودية في ضوء التحولات العالمية نحو الاقتصاد الرقمي ورؤية السعودية 2030. حيث يهدف البحث إلى تحليل الأسس الدستورية والتشريعية والتنظيمية التي تحكم حماية البيانات الشخصية ونقلها عبر الحدود، مع التركيز على نظام حماية البيانات الشخصية السعودي (PDPL 2021) وتعديلاته اللاحقة. واستعرض البحث الخلفية النظرية لتدفقات البيانات من حيث السيادة الرقمية، وحماية الخصوصية، وحرية التجارة الدولية، إضافة إلى أبعادها الاقتصادية والتكنولوجية. كما تناول التحديات العملية المتمثلة في غموض معايير النقل الدولي، التحديات التطبيقية المتعلقة بتحديد المسوغ النظامي الملائم لمعالجة البيانات الشخصية وإدارة الموافقة وفق الضوابط النظامية، التحديات التطبيقية للبنود التعاقدية القياسية، وضعف التكامل بين PDPL وتشريعات أخرى. اعتمد البحث على المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية الوطنية (PDPL) واللوائح التنفيذية، ودراسة التشريعات الدولية ذات الصلة، مع توظيف الدراسات الأكاديمية والتقارير المؤسسية، كما سيتم الاستعانة بالمنهج الوصفي لعرض التطور التاريخي والإطار التنظيمي، إضافة إلى المنهج النقدي لاستخلاص التوصيات.

أظهرت النتائج أن النظام السعودي اتخذ خطوة مهمة نحو مواءمة التشريعات الوطنية مع المعايير الدولية، غير أنه يواجه تحديات مرتبطة بتطوير الخبرة القضائية، وغياب الاستقلالية المؤسسية الكاملة، وصعوبة الامتثال بالنسبة للشركات الصغيرة والمتوسطة. كما تبرز أهمية وضوح إجراءات تطبيق القيود المرتبطة بالأمن الوطني. ويوصي البحث بضرورة تعزيز التكامل الإقليمي مع تشريعات مجلس التعاون، وتعزيز تبني آليات واضحة مثل العقود القياسية، وتطوير برامج تدريب وتوعية للشركات، إضافة إلى تحقيق توازن أفضل بين حماية الخصوصية وجذب الاستثمار الأجنبي.

الكلمات المفتاحية: التحديات القانونية، تدفق البيانات عبر الحدود، المملكة العربية السعودية، نظام حماية البيانات السعودي (PDPL)، المعايير الدولية.

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثامن - الإصدار الخامس والثمانون
تاريخ النشر: 20 نوفمبر 2026 م

Legal Challenges to Cross-Border Data Flows in the Kingdom of Saudi Arabia (Towards a National Framework Aligned with International Standards)

Dr. Monirah Fahad Alhamdan

Assistant Professor of Law, College of Law and Political Science, King Saud University, Saudi Arabia

Abstract:

This research examines the legal challenges surrounding cross-border data flows in the Kingdom of Saudi Arabia, in light of global shifts toward a digital economy and the Kingdom's Vision 2030. It aims to analyze the constitutional, legislative, and regulatory foundations governing the protection and cross-border transfer of personal data, with a specific focus on the Saudi Personal Data Protection Law (PDPL 2021) and its subsequent amendments. The research explores the theoretical underpinnings of data flows—encompassing digital sovereignty, privacy protection, and the freedom of international trade—alongside their economic and technological dimensions. Furthermore, it addresses practical challenges, such as the ambiguity of standards for international data transfers, the complexities of identifying appropriate legal bases for personal data processing and managing consent in compliance with regulatory requirements, the application of standard contractual clauses, and the limited integration between the PDPL and other relevant legislation. This research employs a comparative analytical approach, examining national legal texts—specifically the Personal Data Protection Law (PDPL) and its executive regulations—alongside relevant international legislation, academic studies, and institutional reports. A descriptive approach is also utilized to outline the historical development and regulatory framework, while a critical approach is applied to derive recommendations. The findings indicate that Saudi Arabia has taken a significant step toward aligning its national legislation with international standards. However, the country faces challenges related to the development of judicial expertise, the absence of full institutional independence, and difficulties for small and medium-sized enterprises (SMEs) in achieving compliance. Furthermore, there is a clear need for greater transparency regarding the procedures for implementing restrictions related to national security. The research recommends strengthening regional integration with the legislation of the Gulf Cooperation Council (GCC), promoting the adoption of clear mechanisms—such as standard contractual clauses—developing training and awareness programs for companies, and striking a better balance between protecting privacy and attracting foreign investment.

Keywords: Legal challenges; cross-border data flows; Saudi Arabia; Personal Data Protection Law (PDPL); international standards.

1. المقدمة:

شهد العالم خلال العقدين الأخيرين تحولا جذريا بفعل الثورة الرقمية والاعتماد المتزايد على البيانات كمورد إستراتيجي يفوق في أهميته الموارد التقليدية كالنفط والمعادن. وأصبحت البيانات اليوم العمود الفقري للاقتصاد الرقمي العالمي، حيث ترتبط بها التجارة الإلكترونية، والخدمات المالية، والرعاية الصحية الذكية، والتطبيقات الحكومية، وحتى الأمن القومي للدول (Bradford, 2020). غير أن هذا التطور السريع رافقه بروز إشكالية معقدة تتمثل في تدفقات البيانات عبر الحدود (Cross-border Data Flows)، أي انتقال البيانات الشخصية والتجارية بين أنظمة قانونية مختلفة. تطرح تدفقات البيانات عبر الحدود تحديات قانونية وسياسية واقتصادية متعددة، نتيجة تداخل اعتبارات السيادة الوطنية وحماية الخصوصية الفردية مع متطلبات التجارة الرقمية الدولية والانفتاح الاقتصادي. ففي الوقت الذي تسعى فيه الدول إلى تنظيم انتقال البيانات وحماية المصالح العامة المرتبطة بها، تتزايد الحاجة إلى أطر قانونية تتيح تدفق المعلومات عبر الحدود بصورة آمنة ومتوافقة مع الالتزامات الدولية. وقد أوضحت Burri (2021) أن تنظيم تدفقات البيانات أصبح من القضايا المحورية في قانون التجارة الدولية، نظرًا لتداخل المصالح التجارية مع الاعتبارات المتعلقة بالخصوصية والسيادة والتنظيم الوطني. ومن ثم، تبرز أهمية إيجاد توازن تشريعي بين حماية الحقوق والمصالح الوطنية وتيسير الأنشطة الاقتصادية الرقمية العابرة للحدود.(Burri, 2021) .

في هذا السياق، برزت التجربة الأوروبية مع اللائحة العامة لحماية البيانات (GDPR) كنموذج عالمي صارم يسعى لحماية الحقوق الأساسية للأفراد، ويمتد أثره خارج الاتحاد الأوروبي فيما يعرف بـ " تأثير بروكسل" (The Brussels Effect) الذي جعل تشريعات البيانات الأوروبية معيارا دوليا يفرض نفسه على مختلف الأنظمة القانونية (Bradford, 2020؛ European Parliament & Council of the European Union, 2016). في المقابل، تتبنى الولايات المتحدة نهجا قطاعيا أكثر مرونة، في المقابل، تتسم القواعد الأمريكية بطابع قطاعي، بينما طورت الصين إطارًا يجمع حماية المعلومات الشخصية ومتطلبات أمن البيانات من خلال قانونين صدرا عام 2021، وتناولتهما دراسة Creemers (2022).

أما على المستوى الإقليمي، فقد تبنت دول مجلس التعاون الخليجي تشريعات وطنية مختلفة لحماية البيانات الشخصية، من بينها القانون القطري لعام 2016 والقانون الإماراتي لعام 2021. وفي المملكة العربية السعودية صدر نظام حماية البيانات الشخصية عام 2021، ثم عُدّل عام 2023 ودخل حيز النفاذ في سبتمبر من العام نفسه. ورغم تقارب أهداف هذه التشريعات، تظل شروط المعالجة والنقل الدولي والامتثال مختلفة بين الدول، وهو ما يستدعي دراستها بصورة مقارنة دون افتراض وجود إطار خليجي موحد (المملكة العربية السعودية، 2021؛ Whelan, 2024).

ورغم هذه الخطوات، ما زال الإطار القانوني السعودي يواجه تحديات حقيقية في مجال تدفقات البيانات عبر الحدود، خصوصا في ظل انخراط المملكة في مشاريع التحول الرقمي ورؤية 2030، التي تستند بشكل أساسي إلى جذب الاستثمارات الأجنبية وتوطين التكنولوجيا. وتظهر التحديات بشكل خاص في ثلاثة محاور:

1. التوفيق بين حماية الخصوصية والسيادة الوطنية وبين الانفتاح على الاقتصاد الرقمي العالمي.
2. التوافق مع المعايير الدولية، وعلى رأسها GDPR، لضمان الاعتراف الدولي بالإطار السعودي.
3. التحديات التقنية والمؤسسية المتعلقة بالتنفيذ والرقابة وتوفير البنية التحتية الآمنة.

من هنا تأتي أهمية هذه الدراسة التي تسعى إلى تحليل التحديات القانونية لتدفقات البيانات عبر الحدود في المملكة، من خلال دراسة نقدية مقارنة بين النظام السعودي والمعايير الدولية، وبحث مدى قدرة المملكة على بناء إطار وطني متكامل ومتوافق مع تلك المعايير.

1.1. مشكلة البحث:

تتمثل المشكلة الرئيسة في وجود فجوة بين التشريعات الوطنية السعودية المتعلقة بحماية البيانات وتدفقات البيانات عبر الحدود، وبين المعايير الدولية التي أصبحت تشكل شرطا أساسيا للتكامل في الاقتصاد الرقمي العالمي.

2.1. أسئلة البحث:

1. ما هي التحديات القانونية الرئيسة التي تواجه المملكة في مجال تدفقات البيانات عبر الحدود؟
2. إلى أي مدى يتوافق نظام حماية البيانات السعودي (PDPL) مع المعايير الدولية مثل GDPR؟
3. ما هي الدروس المستفادة من التجارب الدولية التي يمكن تطبيقها في المملكة؟
4. كيف يمكن صياغة إطار وطني متكامل يحمي البيانات ويحافظ على السيادة الوطنية مع مراعاة الانفتاح الاقتصادي ؟

3.1. أهداف البحث:

- تحليل الوضع القانوني الراهن لتدفقات البيانات عبر الحدود في المملكة.
- تحديد أبرز التحديات القانونية والمؤسسية التي تواجه تطبيق النظام السعودي.
- إجراء مقارنة مع الأطر الدولية والإقليمية، وخاصة GDPR والتشريعات الآسيوية.
- تقديم مقترحات عملية لصياغة إطار وطني متكامل ومتوافق مع المعايير الدولية وذلك من خلال تطوير الإطار القائم.

4.1. منهجية البحث:

يعتمد البحث على المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية الوطنية لنظام (PDPL) واللوائح التنفيذية، ودراسة المعايير الدولية ذات الصلة، مع توظيف الدراسات الأكاديمية والتقارير المؤسسية، كما سيتم الاستعانة بالمنهج الوصفي لعرض التطور التاريخي والإطار التنظيمي، إضافة إلى المنهج النقدي لاستخلاص التوصيات.

2. الإطار النظري والمفاهيمي لتدفقات البيانات عبر الحدود:

1.2. مقدمة:

أصبحت البيانات في القرن الحادي والعشرين أحد أهم عناصر الاقتصاد الرقمي، حيث باتت تُوصف بـ " نفط العصر الرقمي" نظرا لقيمتها الاقتصادية الهائلة ودورها في تشكيل السياسات العامة، والأمن القومي، والتجارة العالمية (Bygrave, 2014). ومع توسع شبكات الاتصالات والتقنيات السحابية، تزايدت حركة انتقال البيانات بين الدول بشكل غير مسبوق، مما أثار إشكاليات قانونية وتنظيمية عابرة للحدود. ومن هنا، يكتسب الإطار النظري والمفاهيمي لتدفقات البيانات عبر الحدود أهمية بالغة لفهم التحديات التي تواجه المملكة في هذا المجال.

2.2. تعريف تدفقات البيانات عبر الحدود:

يشير مفهوم تدفقات البيانات عبر الحدود (Cross-Border Data Flows) إلى انتقال البيانات الرقمية بين دول أو ولايات قضائية مختلفة، سواء تعلقت هذه البيانات بالأفراد أو بالأنشطة التجارية أو بالمؤسسات الحكومية. وقد تتم عمليات النقل من خلال شبكات الاتصالات الدولية أو خدمات الحوسبة السحابية أو المنصات الرقمية التي تتيح تخزين البيانات ومعالجتها وإتاحتها لأطراف موجودة في دول متعددة. وتثير هذه التدفقات إشكاليات قانونية تتعلق بالقانون الواجب التطبيق، والاختصاص القضائي، وحماية الخصوصية، ومدى خضوع عمليات نقل البيانات للقيود التنظيمية الوطنية والدولية (Kuner, 2011; Burri, 2021).

- البيانات الشخصية: تشمل معلومات الأفراد (الاسم، الهوية، السجلات الطبية).
- البيانات التجارية: تتعلق بالمعاملات، العقود، المعلومات المالية للشركات.
- البيانات الحكومية: تشمل سجلات المؤسسات الرسمية وبيانات الأمن القومي.

هذا الانتقال يتم غالبا بشكل لحظي وعبر بنية تحتية رقمية متعددة الجنسيات، مما يخلق صعوبة في تحديد القانون الواجب التطبيق، والجهة المسؤولة عن حماية الحقوق.

3.2. الأسس القانونية المرتبطة بتدفقات البيانات:

تشكل تدفقات البيانات عبر الحدود أحد أبرز القضايا القانونية المعاصرة في ظل الثورة الرقمية وتزايد الاعتماد على الخدمات السحابية والتجارة الإلكترونية. وقد انقسمت النقاشات القانونية حول هذه التدفقات إلى ثلاثة أسس رئيسة، هي: السيادة الوطنية، حماية الخصوصية والحقوق الفردية، وحرية التجارة الدولية. لكل أساس منها مبرراته القانونية والسياسية، كما أنها تتقاطع وتتعارض في كثير من الأحيان، مما يجعل صياغة أطر تنظيمية متوازنة تحديا معقدا أمام المشرعين، ونوضحها فيما يلي:-

1.3.2. السيادة الوطنية:

تعد السيادة الوطنية حجر الزاوية في أي نقاش حول تنظيم تدفقات البيانات، حيث تعتبر الدول أن البيانات شأن داخلي يقع ضمن نطاق سلطتها الإقليمية، شأنها شأن الموارد الطبيعية أو البنى التحتية الحيوية. وقد برز مفهوم "السيادة الرقمية" كامتداد للسيادة التقليدية ليشمل التحكم في البيانات التي تُنتَج داخل حدود الدولة أو تتعلق بمواطنيها. هذا التصور تعزز مع تزايد المخاوف من استغلال البيانات لأغراض تجارية أو أمنية من قبل أطراف أجنبية، وهو ما دفع العديد من الدول إلى تبني سياسات "توطين البيانات" أو "الاحتفاظ بالبيانات محليا".

فعلى سبيل المثال، أقرت الصين والهند وروسيا تشريعات تُلزم الشركات بالاحتفاظ بنسخ من بيانات المستخدمين على خوادم محلية، بحجة حماية الأمن القومي ودعم الاقتصاد الوطني. هذه الإجراءات تمثل ترجمة عملية لفكرة السيادة الرقمية، لكنها في الوقت ذاته تُثير جدلا واسعا حول مدى توافقها مع التزامات الدول في إطار منظمة التجارة العالمية. في السياق السعودي، لم يقتصر توجه المملكة نحو تعزيز السيادة الرقمية على إصدار نظام حماية البيانات الشخصية (PDPL)، وإنما اتخذت مجموعة من الإجراءات المؤسسية والتنظيمية التي تهدف إلى إحكام حوكمة البيانات الوطنية. فقد أُنشئت الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) بموجب أمر ملكي عام 2019 لتتولى رسم السياسات الوطنية للبيانات والإشراف على حوكمتها، كما أطلقت الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي (National Strategy for Data and AI – NSDAI) التي تستهدف بناء اقتصاد قائم على البيانات وتعزيز البنية التحتية الرقمية مع الحفاظ على أمن البيانات الوطنية (SDAIA, 2020).

وإلى جانب ذلك، ألزمت اللائحة التنفيذية لنظام حماية البيانات الشخصية الجهات المتحكمة في البيانات بعدم نقل البيانات الشخصية إلى خارج المملكة إلا وفق ضوابط محددة، من بينها التأكد من توفير مستوى مناسب من الحماية في الدولة المستقبلة، أو وجود ضمانات قانونية معتمدة تكفل حماية حقوق أصحاب البيانات، مع منح الجهة المختصة سلطة الإشراف على عمليات النقل الدولي (Saudi Data & Artificial Intelligence Authority [SDAIA], 2023).

كما شجعت المملكة على توطين مراكز البيانات والخدمات السحابية من خلال إطلاق الإطار التنظيمي للحوسبة السحابية، واستقطاب مزودي الخدمات العالميين لإنشاء مراكز بيانات داخل المملكة، بما يعزز الاحتفاظ بالبيانات الحساسة داخل الإقليم الوطني ويدعم مستهدفات الأمن السيبراني والسيادة الرقمية، مع المحافظة في الوقت ذاته على الانفتاح على الاقتصاد الرقمي العالمي.

وتوضح هذه الإجراءات أن التنظيم السعودي لا يقوم على حظر شامل لنقل البيانات الشخصية، بل يجيز النقل في الحالات المحددة نظامًا، مع اشتراط مستوى مناسب من الحماية أو ضمانات بديلة وفق اللوائح. ويرى الباحث أن هذا النهج يستهدف الموازنة بين حماية الحقوق والمصالح الوطنية ومتطلبات الخدمات الدولية (المملكة العربية السعودية، 2021؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024).

2.3.2. حماية الخصوصية والحقوق الفردية:

إلى جانب السيادة الوطنية، برزت حماية الخصوصية كأحد أهم الأسس القانونية في النقاشات الدولية حول تدفقات البيانات. يُنظر إلى الخصوصية باعتبارها حقا أساسيا من حقوق الإنسان، وهو ما أكدته العديد من المواثيق الدولية والإقليمية، مثل اللائحة الأوروبية العامة لحماية البيانات (GDPR). هذه اللائحة تُعد نموذجا عالميا، حيث تُقيّد نقل البيانات الشخصية إلى دول لا توفر مستوى حماية مكافئ، وذلك لضمان عدم انتهاك حقوق الأفراد عند انتقال بياناتهم عبر الحدود.

إن جوهر هذا التوجه يكمن في اعتبار حماية البيانات ليس مجرد التزام تعاقدي أو تنظيمي، بل حقا من حقوق الفرد في مواجهة الدولة والشركات الخاصة. وقد تبنت العديد من الدول خارج الاتحاد الأوروبي تشريعات مشابهة أو مستوحاة من الـGDPR، بما في ذلك بعض دول الخليج التي بدأت في إرساء قواعد صارمة لحماية البيانات الشخصية. في السعودية، نص نظام حماية البيانات الشخصية على مبادئ تتعلق بالشفافية، والموافقة المستنيرة، وحق الأفراد في الاطلاع والتصحيح والحذف، وهي مبادئ تتماشى مع المعايير الدولية.

غير أن هذا التوجه يخلق صعوبات عملية أمام الشركات متعددة الجنسيات التي تحتاج إلى نقل البيانات بشكل مستمر، مما يؤدي إلى تضارب بين مقتضيات حماية الخصوصية ومتطلبات التجارة الدولية. على سبيل المثال، القيود الأوروبية على نقل البيانات إلى الولايات المتحدة أثارت خلافات قانونية وسياسية طويلة، كما في قضية Schrems، التي أبطلت اتفاقية " درع الخصوصية " بين الطرفين (Schwartz & Peifer, 2017).

3.3.2. حرية التجارة الدولية:

الأساس الثالث يتمثل في مبدأ حرية التجارة الدولية، حيث تشجع المنظمات الدولية مثل منظمة التجارة العالمية (WTO) ومنظمة التعاون الاقتصادي والتنمية (OECD) على إزالة القيود المفروضة على تدفقات البيانات، باعتبارها شرطا أساسيا لازدهار التجارة الإلكترونية والخدمات الرقمية. وفقا لتقارير الـOECD، فإن التدفقات الحرة للبيانات تُعزز الابتكار وتخفض التكاليف وتدعم التكامل في الاقتصاد الرقمي العالمي (OECD, 2021).

غير أن التوجه نحو تحرير تدفقات البيانات عبر الحدود يواجه تحديات قانونية وسياسية تتعلق بالتوفيق بين المصالح الاقتصادية والمتطلبات الوطنية لحماية الخصوصية والأمن والسيادة الرقمية. فبينما تسعى الدول إلى تيسير انتقال البيانات باعتباره عاملًا مهمًا في دعم التجارة الرقمية والخدمات العابرة للحدود، تتبنى بعض الدول قيودًا تنظيمية تهدف إلى حماية البيانات الشخصية أو المصالح الأمنية والاستراتيجية.

وقد بيّنت Burri (2021) أن هذه التباينات أصبحت من المسائل الأساسية في تنظيم التجارة الرقمية، ولا سيما في ضوء اختلاف مواقف الدول بشأن التزامات حرية تدفق البيانات والاستثناءات المقررة لحماية المصالح العامة. وفي السياق السعودي، تبرز أهمية تحقيق توازن بين تيسير الأنشطة الاقتصادية الرقمية وجذب الاستثمار الأجنبي من جهة، وضمان حماية البيانات الشخصية والمصالح الوطنية وفق الضوابط النظامية من جهة أخرى.

4.2. الأبعاد الاقتصادية لتدفقات البيانات:

أصبحت تدفقات البيانات عبر الحدود أحد المحركات الرئيسة للاقتصاد العالمي في العصر الرقمي، إذ لم تعد التجارة الدولية تعتمد فقط على تبادل السلع المادية والخدمات التقليدية، بل أصبحت البيانات عنصرًا أساسيًا في دعم التجارة الإلكترونية والخدمات الرقمية وسلاسل القيمة العالمية. وتشير دراسة مشتركة صادرة عن منظمة التعاون الاقتصادي والتنمية ومنظمة التجارة العالمية إلى أن تبني أطر تنظيمية تسمح بتدفق البيانات عبر الحدود مع توفير ضمانات مناسبة لحمايتها قد يحقق مكاسب اقتصادية مهمة. فقد أظهرت نتائج النمذجة الاقتصادية في الدراسة أن اعتماد هذا النهج من جميع الاقتصادات يمكن أن يسهم في زيادة الناتج المحلي الإجمالي العالمي بنسبة تقديرية تبلغ 1.77%، وزيادة الصادرات العالمية بنسبة 3.6%، مقارنة بالسيناريو المرجعي المستخدم في الدراسة. وتؤكد هذه النتائج أهمية تحقيق التوازن بين الانفتاح على تدفقات البيانات وحماية الخصوصية وتعزيز الثقة في البيئة الرقمية، مع مراعاة أن هذه النسب تمثل تقديرات لسيناريوهات تنظيمية وليست قياسًا مباشرًا لمساهمة تدفقات البيانات في الناتج المحلي الإجمالي (OECD & WTO, 2025).

في السياق السعودي، يحظى تنظيم تدفقات البيانات عبر الحدود بأهمية اقتصادية في ضوء رؤية السعودية 2030، التي تضع تنويع الاقتصاد والتحول الرقمي وجذب الاستثمارات ضمن أولوياتها. ويبين التقرير السنوي للرؤية لعام 2024 توسع نشاط الاقتصاد الرقمي والاستثمارات المرتبطة بالتقنيات والذكاء الاصطناعي ومراكز البيانات، بما يعكس تنامي دور البنية التحتية الرقمية في التنمية (رؤية السعودية 2030، 2025). وفي هذا السياق، يرى الباحث أن وضوح قواعد نقل البيانات وتطبيق ضمانات الحماية بصورة متناسبة قد يساعد المؤسسات على الاستفادة من الخدمات السحابية والتجارة الإلكترونية، مع الحد من مخاطر الامتثال وتعزيز الثقة اللازمة لتطوير الخدمات المالية والتقنية العابرة للحدود.

في المقابل، قد تؤدي القيود الواسعة على انتقال البيانات عبر الحدود إلى ارتفاع تكاليف التشغيل والامتثال، ولا سيما لدى الشركات التي تعتمد على معالجة البيانات في مراكز أو أسواق متعددة. ويشير تقرير مشترك لمنظمة التعاون الاقتصادي والتنمية ومنظمة التجارة العالمية إلى أن التجزئة الشديدة لتدفقات البيانات ترتبط بتكاليف اقتصادية محتملة، بينما قد تحقق النظم التي تجمع الانفتاح مع ضمانات الحماية نتائج أفضل .(OECD & WTO, 2025) وفي الحالة السعودية، يرى الباحث أن تقييم أثر القيود على الاستثمار يتطلب النظر في نوع البيانات والضمانات المتاحة وتكاليف الامتثال، دون افتراض أن التنظيم القانوني يؤدي تلقائيًا إلى عزوف المستثمرين الأجانب.

من جهة أخرى، فإن الانفتاح غير المنضبط على تدفقات البيانات ينطوي على مخاطر اقتصادية وأمنية. فالسماح بتدفق البيانات بحرية تامة، دون ضوابط لحماية الأمن السيبراني أو ضمان خصوصية الأفراد، قد يعرض الدولة لخسائر اقتصادية جسيمة نتيجة الهجمات الإلكترونية أو تسرب البيانات الحساسة. وتقدّر بعض التقارير أن الهجمات السيبرانية تكلف الاقتصاد العالمي سنويا مئات المليارات من الدولارات، وهو ما يجعل مسألة الموازنة بين الانفتاح والحماية ضرورة استراتيجية. في هذا السياق، يمثل نظام حماية البيانات الشخصية السعودي (PDPL) خطوة متقدمة لتقنين التدفقات مع الحفاظ على حماية البيانات الوطنية، وهو توجه يعكس محاولة المملكة إيجاد صيغة وسط بين الانفتاح الاقتصادي والحماية القانونية.

إن البعد الاقتصادي لتدفقات البيانات يتجاوز مجرد تعزيز الناتج المحلي الإجمالي، ليشمل بناء الثقة في الاقتصاد الرقمي الوطني، وتوفير بيئة استثمارية جاذبة، وتطوير قدرات القوى العاملة الوطنية في مجالات تحليل البيانات والذكاء الاصطناعي. فكلما اتسمت البيئة التشريعية بالوضوح والتوازن، كلما زاد استعداد المستثمرين والشركات العالمية للعمل في السوق السعودي، بما يحقق أهداف رؤية 2030 ويعزز مكانة المملكة كلاعب محوري في الاقتصاد الرقمي العالمي (OECD, 2021).

5.2. الأبعاد التكنولوجية لتدفقات البيانات:

تُعد التكنولوجيا العنصر الأكثر تأثيرا في طبيعة تدفقات البيانات عبر الحدود، إذ تحدد الأدوات والمنصات الرقمية كيفية تخزين البيانات ومعالجتها وتأمينها. وتكشف التطورات التقنية الحديثة أن التحديات القانونية لا يمكن فصلها عن السياقات التكنولوجية التي تفرض أنماطا جديدة لتدفق المعلومات. ومن أبرز هذه الأبعاد التكنولوجية: الحوسبة السحابية، والذكاء الاصطناعي وتحليل البيانات الضخمة، والتشفير وأمن البيانات.

1. الحوسبة السحابية (Cloud Computing)

أصبحت الحوسبة السحابية إحدى الركائز الأساسية للبنية التحتية الرقمية الحديثة، حيث تعتمد معظم الشركات والمؤسسات الحكومية على خدمات يقدمها مزودون عالميون مثل Amazon Web Services (AWS) وMicrosoft Azure و Google Cloud. تتيح هذه الخدمات إمكانات هائلة لتخزين البيانات ومعالجتها دون الحاجة إلى استثمارات محلية ضخمة في البنية التحتية. غير أن هذه المزايا تصاحبها تحديات قانونية مهمة، أبرزها مسألة الاختصاص القضائي. فبما أن البيانات غالبا ما تُخزَّن وتُوزَّع عبر مراكز بيانات موجودة في دول مختلفة، فإن تحديد القوانين الوطنية التي تسري على تلك البيانات يصبح معقدا للغاية (Svantesson, 2017).

على سبيل المثال، إذا استخدمت شركة سعودية خدمات سحابية تعتمد على مراكز معالجة في أوروبا والولايات المتحدة، فقد تخضع بعض عملياتها لأكثر من نظام قانوني، بحسب مكان نشاط الجهة، وصفة أصحاب البيانات، ونطاق تطبيق التشريعات المعنية. ولا يكفي وجود الخادم في دولة أجنبية وحده للجزم بانطباق قانونها على جميع البيانات. ويمتد نطاق النظام السعودي إلى معالجة بيانات المقيمين في المملكة من جهات خارجها وفق المادة الثانية، بينما تحدد القواعد الأوروبية شروط انطباق GDPR خارج الاتحاد. ويرى الباحث أن تعدد روابط الاختصاص يستلزم تحليلًا تعاقديًا وتنظيميًا مسبقًا لتوزيع المسؤوليات وتقييم مشروعية النقل (المملكة العربية السعودية، 2021؛ European Parliament & Council of the European Union, 2016).

2. الذكاء الاصطناعي (AI) وتحليل البيانات الضخمة (Big Data Analytics):

يشكل الذكاء الاصطناعي وتحليل البيانات الضخمة بُعدا تكنولوجيا آخر بالغ الأهمية، إذ تعتمد تطبيقاتهما على تجميع ومعالجة كميات هائلة من البيانات، غالبا ما تتجاوز الحدود الوطنية. في مجالات مثل التعرف على الصور، ومعالجة اللغة الطبيعية، وتطوير الأنظمة التنبؤية، تحتاج الخوارزميات إلى بيانات متنوعة من مصادر متعددة، وهو ما يستلزم تدفقات مستمرة عبر الحدود.

إلا أن هذا الاعتماد على البيانات العابرة للحدود يثير عدة إشكاليات قانونية. فمن ناحية، يتعلق الأمر بالتحكم في البيانات: من يمتلك الحق القانوني في استخدامها ومعالجتها؟ هل هي الشركات التي تجمع البيانات، أم الأفراد الذين تُستمد بياناتهم، أم الدول التي تُنتَج فيها؟ ومن ناحية أخرى، تظهر قضية حماية الملكية الفكرية، خاصة عندما تُستخدم البيانات في تدريب نماذج الذكاء الاصطناعي التي قد تنتج عنها ابتكارات أو خوارزميات جديدة. فإذا كانت البيانات قد جُمعت من عدة دول، فإلى أي نظام قانوني تُنسب الحقوق الناتجة؟. هذه الأسئلة تجعل من الضروري تطوير أطر قانونية جديدة تنظم استخدام البيانات الضخمة في تطبيقات الذكاء الاصطناعي بما يحمي حقوق الأفراد ويشجع الابتكار في الوقت ذاته.

3. التشفير وأمن البيانات:

يُعتبر التشفير إحدى الوسائل التقنية الأكثر فاعلية لحماية البيانات أثناء انتقالها عبر الحدود. إذ يضمن التشفير أن تبقى البيانات غير قابلة للقراءة بالنسبة للأطراف غير المخوّلة، مما يساهم في تعزيز الثقة في البيئة الرقمية الدولية. غير أن التشفير نفسه أصبح

موضوعا للجدل القانوني والسياسي. ففي الوقت الذي ترى فيه الشركات والأفراد أن التشفير القوي هو الضمان الأساسي لحماية الخصوصية والأمن، تصر بعض الحكومات على فرض "أبواب خلفية" تسمح لها بالوصول إلى البيانات المشفرة عند الضرورة، سواء لأسباب تتعلق بالأمن القومي أو مكافحة الجرائم الإلكترونية. هذا التوجه يخلق توترا واضحا بين مقتضيات الأمن القومي من جهة، وضمان حقوق الأفراد في الخصوصية من جهة أخرى. فبينما ترى الحكومات أن غياب القدرة على الوصول إلى البيانات المشفرة قد يعيق جهودها في مكافحة الإرهاب والجريمة المنظمة، يرى خبراء الأمن والحقوق الرقمية أن أي باب خلفي يمكن أن يُستغل من قبل جهات خبيثة ويضعف من الحماية الأمنية للجميع. في السياق السعودي، يعكس نظام مكافحة جرائم المعلوماتية والاستراتيجية الوطنية للأمن السيبراني هذا التوازن الحساس، حيث يتم التأكيد على أهمية التشفير كوسيلة للحماية، مع منح السلطات صلاحيات للتدخل عند الضرورة.

6.2. المعايير الدولية الحاكمة لتدفقات البيانات:

أ) اللائحة العامة لحماية البيانات (GDPR)

- اعتمدها الاتحاد الأوروبي عام 2018 كأكثر الأنظمة صرامة في حماية الخصوصية.
- تنظم نقل البيانات للدول الثالثة بقرارات الملاءمة أو ضمانات كالبنود التعاقدية القياسية وقواعد الشركات الملزمة، أو باستثناءات قانونية (European Parliament & Council of the European Union, 2016).

ب) مبادئ منظمة التعاون الاقتصادي والتنمية (OECD Guidelines 2021)

- تركز على تحقيق توازن بين حرية تدفق البيانات وحماية الخصوصية.
- تعترف بحق الدول في تقييد نقل البيانات إذا كان ذلك لحماية الأمن القومي أو النظام العام (OECD, 2021).

ج) إطار APEC للخصوصية (APEC Privacy Framework)

- يهدف إلى وضع آليات لتسهيل التدفقات داخل منطقة آسيا-الباسيفيك مع احترام الخصوصية.

يركز على تنسيق مبادئ الخصوصية والتعاون الطوعي، مع استمرار سريان القوانين الوطنية (APEC, 2017).

د) اتفاقيات التجارة الدولية

- مثل اتفاقية التجارة الحرة بين الاتحاد الأوروبي واليابان، التي تتضمن فصولا خاصة بتدفقات البيانات.
- الاتجاه الحديث يشير إلى إدراج قواعد حماية البيانات ضمن الاتفاقيات التجارية كشرط أساسي (Irion, 2012).

7.2. التحديات النظرية:

يشكل النقاش حول تدفقات البيانات عبر الحدود تحديا نظريا متعدد الأبعاد، حيث يتقاطع مع قضايا السيادة، والعولمة، وتطورات القانون الدولي. فرغم إدراك المجتمع الدولي لأهمية هذه التدفقات في الاقتصاد الرقمي، لا تزال الإشكاليات النظرية الأساسية تحول دون بناء إطار قانوني عالمي متماسك. ويمكن إبراز هذه التحديات في ثلاثة محاور: التعارض بين السيادة الوطنية والعولمة الرقمية، عدم التجانس بين الأنظمة القانونية، وضعف آليات الإنفاذ الدولية.

- **التعارض بين السيادة الوطنية والعولمة الرقمية**

يتمثل التحدي الأول في الصراع بين منطق السيادة الوطنية ومتطلبات العولمة الرقمية. فبينما تتجه العولمة إلى إزالة الحواجز أمام حركة البيانات لتسهيل التجارة والاستثمار، تصر العديد من الدول على فرض قيود صارمة لحماية سيادتها الرقمية. ويُترجم هذا في

سياسات "توطين البيانات " (Data Localization)، التي تُلزم الشركات بتخزين البيانات داخل حدود الدولة وعدم نقلها للخارج إلا بشروط معينة. هذه السياسة تبنتها دول مثل روسيا والصين والهند بدرجات متفاوتة، بدافع حماية الأمن القومي ودعم الاقتصاد المحلي. غير أن سياسات توطين البيانات تثير تساؤلات بشأن مدى توافقها مع الالتزامات التجارية الدولية. ولا تتضمن قواعد منظمة التجارة العالمية التزامًا عامًا ومباشرًا بحرية جميع تدفقات البيانات عبر الحدود، وإن كانت بعض تدابير التقييد قد تؤثر في التجارة بالخدمات الرقمية. وقد تعالج اتفاقيات تجارية إقليمية هذه المسائل على نحو أكثر تحديدًا (Burri, 2021). كما أن المبالغة في اشتراط التخزين المحلي قد تزيد تكاليف الامتثال وتسهم في تجزئة الفضاء الرقمي. ومن ثم تظل الموازنة بين السيادة الرقمية والانفتاح الاقتصادي ضرورة تنظيمية.

- عدم التجانس بين الأنظمة القانونية

التحدي الثاني يتمثل في التباين بين النظم القانونية، إذ تختلف مقاربات حماية البيانات بين الأنظمة الأوروبية والأمريكية والآسيوية. ففي الاتحاد الأوروبي، يمثل النموذج الحقوقي حجر الأساس، حيث تُعتبر حماية البيانات حقا أساسيا من حقوق الإنسان بموجب اللائحة العامة لحماية البيانات (GDPR) بالمقابل، يستند التنظيم الأمريكي إلى تشريعات قطاعية تشمل الصحة والمال والأطفال، وتكملها قوانين خصوصية ببعض الولايات. ومن ثم، فإن وصف النظام الأمريكي بأنه يعتمد أساسًا على التنظيم الذاتي للشركات يتجاهل التزامات قانونية ملزمة، والتفاوت بين القواعد الاتحادية وقوانين الولايات (Linebaugh, 2025). أما في آسيا، تختلف تشريعات حماية البيانات بين الصين واليابان وسنغافورة. وتجمع الصين بين متطلبات الأمن وحقوق الأفراد وتنظيم النقل الدولي، لذا يلزم اعتماد معايير محددة قبل ترتيب النماذج بحسب المرونة (Creemers, 2022). هذا التباين يعقد عمل الشركات العالمية التي تضطر إلى الامتثال لمجموعة متنوعة من التشريعات الوطنية المتناقضة أحيانا. على سبيل المثال، قد يُطلب من الشركة ذاتها أن تحتفظ بالبيانات داخل حدود دولة معينة (بموجب قوانين التوطين)، بينما تُلزم في دولة أخرى بنقلها لأغراض الامتثال أو التعاون القضائي. ومن هنا، يشكل عدم التجانس بين الأنظمة القانونية عقبة جوهرية أمام بناء نظام دولي متكامل لتدفقات البيانات.

- ضعف آليات الإنفاذ الدولية

التحدي الثالث يكمن في ضعف آليات الإنفاذ الدولية. فرغم وجود بعض الأطر الإقليمية مثل الاتحاد الأوروبي (GDPR)، أو اتفاقية APEC بشأن الخصوصية عبر الحدود، إلا أنه لا توجد حتى الآن معاهدة دولية شاملة تنظم تدفقات البيانات. وبدون إطار عالمي، تبقى المعايير الدولية مجزأة، وتُترك الشركات والأفراد للتنقل بين أنظمة متضاربة (OECD, 2021).

الجدير بالذكر أن محاولات إدراج قواعد ملزمة حول تدفقات البيانات في مفاوضات منظمة التجارة العالمية لا تزال تواجه خلافات حادة بين الدول، حيث تخشى بعض الدول النامية من فقدان سيطرتها على بياناتها إذا التزمت بانفتاح غير مشروط. في المقابل، ترى الدول المتقدمة أن غياب معايير ملزمة يعرقل الابتكار ويضر بالاقتصاد الرقمي العالمي. هذه الفجوة تعكس إشكالية نظرية كبرى: هل يجب التعامل مع البيانات كمورد سيادي يخضع للقانون الوطني، أم كمورد عالمي يحتاج إلى قواعد دولية موحدة؟

3. النظام القانوني السعودي لحماية البيانات:

1.3. مقدمة:

أدركت المملكة العربية السعودية أهمية البيانات بوصفها ركيزة للتحول الرقمي ورؤية 2030، فطورت أطرًا تشريعية ومؤسسية لتنظيم معالجتها وحمايتها. وصدر نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم م/19 عام 2021، ثم أُقرت تعديلاته بموجب المرسوم الملكي رقم م/148 عام 2023. ودخل النظام حيز النفاذ في 14 سبتمبر 2023، مع مهلة لتوفيق الأوضاع حتى سبتمبر 2024. ويوفر النظام إطارًا لحماية بيانات الأفراد وتنظيم نقلها عبر الحدود (المملكة العربية السعودية، 2021).

2.3. نظام حماية البيانات الشخصية السعودي (PDPL 2021)

1.2.3. الإطار العام للنظام

يُعَد نظام حماية البيانات الشخصية السعودي (PDPL 2021) نقطة تحول محورية في مسيرة التشريعات الرقمية بالمملكة، حيث يهدف بالأساس إلى حماية البيانات الشخصية من المعالجة غير المشروعة وضمان أن تُستخدم هذه البيانات بما يتوافق مع مبادئ الخصوصية وحماية الأفراد. ويأتي النظام في سياق التطورات العالمية المتسارعة في مجال حماية البيانات، وهو ما يعكس إدراك المملكة لأهمية توفير بيئة قانونية تعزز الثقة في الاقتصاد الرقمي وتدعم استراتيجيات التحول الرقمي التي تُعد إحدى ركائز رؤية السعودية 2030.

ويؤكد النظام السعودي مبادئ مشروعية المعالجة والشفافية وتحديد الغرض وحماية حقوق أصحاب البيانات. وتُعد الموافقة أحد المسوغات النظامية لمعالجة البيانات الشخصية، غير أن المادة السادسة تجيز المعالجة دون موافقة في حالات محددة، منها تنفيذ اتفاق سابق أو التزام نظامي وتحقيق مصلحة مشروعة وفق ضوابطها، دون أن يشمل ذلك معالجة البيانات الحساسة على أساس المصلحة المشروعة. كما يمتد نطاق تطبيق النظام إلى معالجة البيانات الشخصية المتعلقة بالمقيمين في المملكة بواسطة جهات تقع خارجها، وفق المادة الثانية، بما يعكس البعد العابر للحدود للحماية النظامية. وتتشابه هذه السمة من حيث المبدأ مع الامتداد الإقليمي لبعض أحكام اللائحة الأوروبية، مع اختلاف شروط التطبيق (المملكة العربية السعودية، 2021).

هذا التوجه يعكس رغبة المملكة في مواءمة سياساتها مع المعايير الدولية، بحيث لا تقتصر الحماية على المستوى المحلي فحسب، بل تمتد لتشمل أي جهة أجنبية تتعامل مع بيانات المواطنين والمقيمين السعوديين. ويمثل ذلك استجابة للتحديات التي تفرضها تدفقات البيانات عبر الحدود، وضمانا لعدم إساءة استخدام البيانات من قبل جهات أجنبية قد تكون خارج نطاق الرقابة المباشرة للسلطات السعودية. وبهذا، يمكن القول إن الإطار العام للنظام السعودي يجمع بين حماية الحقوق الفردية وتعزيز الثقة المؤسسية من جهة، وبين جذب الاستثمارات الأجنبية من جهة أخرى عبر توفير بيئة قانونية واضحة ومتناغمة مع الأطر الدولية.

2.2.3. المبادئ الأساسية:

- **الموافقة والمسوغات النظامية للمعالجة (Consent and Lawful Bases):** تعد الموافقة أحد المسوغات النظامية لمعالجة البيانات الشخصية، مع جواز المعالجة دون موافقة في الحالات التي يحددها النظام. ويجب أن تستوفي الموافقة الشروط المقررة في اللائحة التنفيذية، وأن تكون صريحة في الحالات التي تستلزم ذلك، مع ضمان حق صاحب البيانات في العدول عنها وفق الضوابط النظامية.
- **الحد من الغرض (Purpose Limitation):** استخدام البيانات فقط للغرض المحدد عند جمعها.
- **الشفافية (Transparency):** إلزام الجهات المتحكمة بالبيانات بتوضيح سياسات جمع ومعالجة البيانات.
- **المساءلة (Accountability):** تحميل الجهة المعالجة المسؤولية القانونية عن أي انتهاك.
- حقوق أصحاب البيانات: مثل الحق في الوصول، التصحيح، المحو، والاعتراض على المعالجة.

3.2.3. نطاق التطبيق والجزاءات

يُحدّد نظام حماية البيانات الشخصية نطاق تطبيقه بشكل شامل ليشمل جميع الكيانات، سواء كانت شركات خاصة أو جهات حكومية أو منظمات غير ربحية، شريطة أن تقوم بمعالجة البيانات الشخصية لأفراد داخل المملكة أو تتعلق بمقيمين سعوديين حتى

وإن تمت المعالجة خارجها. هذا الاتساع في النطاق يجعل النظام أداة فعّالة في ضبط التدفقات الرقمية ويضمن أن تكون جميع الجهات، المحلية والأجنبية، خاضعة لالتزامات قانونية واضحة في تعاملها مع البيانات الشخصية.

ومن أبرز الالتزامات التي يفرضها النظام على المؤسسات إلزامها بتعيين مسؤول لحماية البيانات (Data Protection Officer)، وهو منصب يتولى مهمة ضمان امتثال المؤسسة لأحكام النظام ومراقبة ممارساتها المتعلقة بجمع البيانات ومعالجتها. كما يتعين على المؤسسات تبني سياسات واضحة لإدارة البيانات، وتطبيق تدابير تقنية وتنظيمية لحماية البيانات من الاختراق أو التسريب. هذه المتطلبات تشبه إلى حد كبير ما هو معمول به في الأنظمة المقارنة، خصوصا النظام الأوروبي، الأمر الذي يسهم في تعزيز قدرة الشركات السعودية على التعامل مع الشركاء الدوليين دون مخاطر قانونية كبيرة.

أما الجزاءات، فقد ميز النظام السعودي بين العقوبات الجنائية المقررة للإفصاح عن البيانات الحساسة أو نشرها بالمخالفة لأحكامه بقصد الإضرار بصاحبها أو تحقيق منفعة شخصية، وبين الجزاءات المقررة للمخالفات الأخرى. وتجيز المادة الخامسة والثلاثون السجن لمدة لا تتجاوز سنتين أو الغرامة التي لا تتجاوز ثلاثة ملايين ريال أو كليهما في الحالة المحددة فيها، بينما تنظم المادة السادسة والثلاثون الإنذار أو الغرامة التي لا تتجاوز خمسة ملايين ريال للمخالفات الأخرى، مع أحكام لتكرار المخالفة. ويجيز النظام لصاحب البيانات تقديم شكوى إلى الجهة المختصة، والمطالبة بالتعويض عند تحقق الضرر وفق أحكامه (المملكة العربية السعودية، 2021، المواد 34–36 و40).

وعليه، فإن نطاق التطبيق والجزاءات في النظام السعودي يعكسان توجها جادا نحو إرساء ثقافة امتثال قانوني صارمة، توازن بين تمكين الاقتصاد الرقمي وتشجيع الابتكار من جهة، وحماية الحقوق الفردية وصون السيادة الوطنية من جهة أخرى.

3.3. التطور التشريعي والتنظيمي لنظام حماية البيانات الشخصية (2021–2024)

1.3.3. التعديلات التشريعية

- في عام 2022، أُدخلت تعديلات لتخفيف بعض القيود التي كانت تُعتبر صارمة بالنسبة للشركات الأجنبية، مثل متطلبات توطين البيانات.
- في 2023، صدرت اللوائح التنفيذية لتوضيح إجراءات الامتثال، وإدخال مفهوم "النقل الدولي للبيانات" مع اشتراط ضمانات تعاقدية مماثلة لـ Standard Contractual Clauses في الاتحاد الأوروبي (SDAIA, 2023).

2.3.3. أثر التعديلات على تدفقات البيانات عبر الحدود

أحدثت التعديلات التشريعية التي أُقرت عام 2023، وما تبعها من إصدار اللوائح التنفيذية والتنظيمية، تطورًا مهمًا في الإطار القانوني السعودي لحماية البيانات الشخصية، ولا سيما فيما يتعلق بتنظيم عمليات نقل البيانات إلى خارج المملكة. فقد أعادت التعديلات تنظيم الأحكام المتعلقة بالنقل الدولي بموجب المادة التاسعة والعشرين من النظام، وأتاحت نقل البيانات الشخصية أو الإفصاح عنها إلى جهات خارج المملكة لتحقيق الأغراض المحددة نظامًا، مع مراعاة الضوابط المتعلقة بحماية الأمن الوطني والمصالح الحيوية للمملكة، وتوفير مستوى مناسب من الحماية، والاقتصار على الحد الأدنى اللازم من البيانات، وفق الشروط والاستثناءات المقررة. كما جاءت لائحة نقل البيانات الشخصية إلى خارج المملكة لتفصيل الأحكام التنظيمية وآليات تقييم مستوى الحماية والضمانات المرتبطة بعمليات النقل. ويعكس هذا التطور توجه المنظم السعودي نحو إتاحة قدر أكبر من المرونة القانونية في نقل البيانات عبر الحدود، مع المحافظة على الضمانات الأساسية لحماية الخصوصية والسيادة الوطنية (المملكة العربية السعودية، 2021، المادة التاسعة والعشرون؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، 2023).

وتتعدد آليات تنظيم نقل البيانات الشخصية إلى خارج المملكة؛ إذ تتيح اللائحة النقل إلى الدول أو الجهات التي يتوافر لديها مستوى مناسب من الحماية، وفق التقييمات المعتمدة لدى الجهة المختصة. وعند توافر الشروط النظامية، يمكن الاستناد إلى ضمانات أخرى، مثل البنود التعاقدية القياسية والقواعد المشتركة الملزمة وشهادات الاعتماد، بدلًا من اقتصار التنظيم على اتفاقيات ثنائية بين الدول. ويقترب هذا النهج من التمييز الأوروبي بين النقل القائم على قرار الملاءمة والنقل المستند إلى ضمانات مناسبة، مع اختلاف الشروط والإجراءات (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024ب؛ European Parliament & Council of the European Union, 2016).

تختلف آليات نقل البيانات الشخصية في النظام السعودي عن النظام الأوروبي من حيث الإجراءات والجهات المختصة، مع وجود تشابه في الاعتماد على تقييم مستوى الحماية والضمانات المناسبة. فقد حددت اللائحة السعودية معايير لتقويم مستوى حماية البيانات في الجهات المستقبلة، وأجازت في الحالات المقررة الاستناد إلى ضمانات مثل البنود التعاقدية القياسية والقواعد المشتركة الملزمة. لذلك لا يصح وصف القواعد بأنها غير محددة مطلقًا، لكن تطبيقها قد يستلزم من الشركات مراجعة وضع الدولة المستقبلة والضمانات المطلوبة لكل عملية نقل، ولا سيما عند استخدام الخدمات السحابية الدولية. ويرى الباحث أن وضوح الإرشادات التطبيقية يسهم في تقليل عدم اليقين التنظيمي (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024).

ومن الناحية العملية، يُتوقع أن تُسهم هذه التعديلات في تحفيز الاستثمارات الأجنبية المباشرة، إذ تمنح الشركات متعددة الجنسيات إطارا قانونيا أوضح للتعامل مع بيانات عملائها وموظفيها في المملكة. فالشركات العالمية في قطاعات مثل الخدمات المالية، والرعاية الصحية، والتكنولوجيا تحتاج إلى تدفقات بيانات سلسة لدعم عملياتها التشغيلية والإقليمية، وأي قيود صارمة قد تدفعها إلى إعادة النظر في استثماراتها. كما أن هذه المرونة تتماشى مع رؤية السعودية 2030 التي تضع التحول الرقمي وجذب الشركات العالمية في مقدمة أولوياتها. إلى جانب ذلك، يُلاحظ أن التعديلات السعودية جاءت في وقت يشهد فيه العالم تحولات جذرية في قواعد نقل البيانات، خصوصا بعد إبطال اتفاقية Privacy Shield بين الاتحاد الأوروبي والولايات المتحدة عام 2020 بقرار من محكمة العدل الأوروبية، الأمر الذي فتح نقاشا عالميا واسعا حول كيفية تحقيق التوازن بين متطلبات الخصوصية وحرية التجارة الرقمية. في هذا السياق، تعكس التعديلات السعودية استجابة واعية لهذا الجدل، إذ تحاول أن تستفيد من الخبرات الدولية مع تجنب التبعية المطلقة لأي نموذج خارجي. فهي لا تكتفي باستنساخ "قرارات الملاءمة" الأوروبية، بل تضيف إليها خيار الاتفاقيات الثنائية بما يتناسب مع خصوصية موقع المملكة الجيوسياسي والاقتصادي.

ومع أن هذه التعديلات تمثل خطوة مهمة نحو بناء إطار قانوني أكثر مرونة وتوافقا مع المعايير الدولية، إلا أنها لا تخلو من تحديات. أبرز هذه التحديات هو كيفية ضمان آليات إنفاذ قوية في حال نقل البيانات إلى دول ذات مستويات حماية أدنى، أو عندما تثار نزاعات قضائية حول خرق الالتزامات التعاقدية. كما أن نجاح هذه التعديلات يعتمد إلى حد كبير على فعالية الهيئة الوطنية لحماية البيانات في السعودية في متابعة الامتثال ومراقبة تنفيذ الاتفاقيات.

4.3. دور الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)

- أُسست SDAIA عام 2019 لتكون الجهة المركزية المسؤولة عن البيانات والذكاء الاصطناعي.
- تتولى الإشراف على تنفيذ PDPL، إصدار التراخيص، ومراقبة الامتثال.
- تعمل أيضا على تطوير الاستراتيجية الوطنية للبيانات، التي تهدف إلى جعل المملكة مركزا عالميا للبيانات الضخمة بحلول 2030.

5.3. العلاقة مع الأطر القانونية الخليجية والإقليمية:

تمثل العلاقة بين النظام السعودي لحماية البيانات الشخصية (PDPL) والأطر القانونية الخليجية والإقليمية جانبا مهما لفهم موقع المملكة في سياق الحوكمة الإقليمية للبيانات. فقد شهدت دول مجلس التعاون في السنوات الأخيرة توجها متزايدا نحو إقرار تشريعات لحماية البيانات، مثل القانون الاتحادي لحماية البيانات في دولة الإمارات (2021)، الذي يتقاطع في العديد من جوانبه مع النظام السعودي من حيث فرض التزامات على المؤسسات وتأكيد حقوق الأفراد في الخصوصية. هذا التشابه يعكس وجود تقارب تشريعي نابع من إدراك مشترك لأهمية حماية البيانات في دعم الاقتصاد الرقمي وجذب الاستثمارات الأجنبية. ومع ذلك، فإن هذا التقارب لا يرقى بعد إلى مستوى التوحيد الإقليمي المشابه لما هو قائم في الاتحاد الأوروبي عبر اللائحة العامة لحماية البيانات (GDPR)، التي أوجدت سوقا رقمية موحدة يسهل فيها انتقال البيانات دون قيود بين دول الاتحاد. في المقابل، تظل بيئة البيانات في دول الخليج مجزأة، حيث تضع كل دولة إطارا قانونيا خاصا بها، مما يخلق تحديات أمام الشركات متعددة الجنسيات التي تعمل عبر الحدود الخليجية. إذ قد تضطر هذه الشركات إلى الامتثال لمجموعة من القوانين الوطنية المختلفة، حتى وإن كانت متشابهة في الأهداف، إلا أنها تختلف في التفاصيل التنفيذية والجزاءات. هذا الوضع قد يحد من الكفاءة الاقتصادية، ويعيق تحقيق سوق رقمية خليجية موحدة. لذلك، فإن تعزيز التنسيق بين المملكة وبقية دول مجلس التعاون في مجال حماية البيانات يمكن أن يسهم في تقليل ازدواجية الامتثال وتسهيل حركة البيانات، وهو ما يتماشى مع الأهداف الاقتصادية المشتركة ورؤية التكامل الخليجي.

6.3. مقارنة أولية مع المعايير الدولية:

1- مع اللائحة الأوروبية (GDPR)

- أوجه التشابه: مبدأ الموافقة، حقوق الأفراد، الامتداد خارج الحدود.
- أوجه الاختلاف:

- في GDPR هناك هيئات مستقلة مستقرة (DPAs)، بينما في السعودية تتركز السلطة بيد SDAIA كجهة حكومية.
- يعترف كل من النظام السعودي واللائحة الأوروبية العامة لحماية البيانات (GDPR) بتعدد المسوغات القانونية لمعالجة البيانات الشخصية، بما فيها الموافقة، وتنفيذ الالتزامات القانونية أو التعاقدية، والمصلحة المشروعة وفق الضوابط المقررة في كل نظام. غير أن الاختلاف بين النظامين يظهر في نطاق تطبيق هذه المسوغات وشروط استخدامها والاستثناءات المرتبطة بها، مما يستدعي إجراء مقارنة تفصيلية بين المادة السادسة من النظام السعودي والمادة السادسة من اللائحة الأوروبية، بدلًا من افتراض اقتصار النظام السعودي على الموافقة.

2- مع الولايات المتحدة

- النموذج الأمريكي قطاعي وغير موحد، بينما يتبنى PDPL إطارا موحدا أقرب لـ GDPR.

الولايات المتحدة تتبع تنظيمًا اتحاديًا قطاعيًا تكمله قوانين للولايات، بينما يخضع نقل البيانات السعودي لضوابط وطنية محددة (Linebaugh, 2025؛ المملكة العربية السعودية، 2021).

3- مع الصين

- الصين تربط حماية البيانات بالأمن الوطني وتنظم نقلها وفق شروط محددة (Creemers, 2022).
- المملكة تبنّت نهجا أكثر توازنا، حيث خففت قيود التوطين لكنها أبقت على أدوات رقابية قوية عبر SDAIA.

7.3. التحديات المرتبطة بالنظام السعودي:

1. التوازن بين حماية الخصوصية وجذب الاستثمار: يتمثل التحدي في تحقيق حماية فعالة للبيانات الشخصية دون فرض متطلبات امتثال غير متناسبة مع طبيعة أنشطة الشركات العابرة للحدود. ويرى الباحث أن وضوح شروط النقل وتحديد الضمانات المناسبة قد يساعد على خفض مخاطر الامتثال، بينما قد يضعف التطبيق غير الفعال ثقة أصحاب البيانات. ولا يثبت هذا التحليل وحده تراجع الاستثمارات.
2. ضبابية بعض المفاهيم الأساسية: التي تبناها النظام، مثل تحديد معايير "الدولة ذات الحماية المكافئة"، وهو شرط رئيسي لنقل البيانات عبر الحدود لكنه لم يُحدد بشكل قاطع حتى الآن، مما يخلق حالة من الغموض القانوني للشركات التي تسعى للامتثال.
3. ضعف الخبرة المؤسسية: حيث إن نظام PDPL لا يزال حديث التطبيق، الأمر الذي يتطلب بناء قدرات مؤسسية وقضائية قادرة على الإشراف والرقابة والتفسير القانوني للنصوص في ضوء الممارسات العملية، خاصة وأن تجارب مشابهة في الاتحاد الأوروبي أظهرت أن التطبيق الفعّال يتطلب سنوات من الممارسة والتدريب.
4. التكامل الإقليمي والدولي: يعد تحديا مهما إذ تحتاج المملكة إلى تطوير آليات للاعتراف المتبادل مع شركائها التجاريين الرئيسيين مثل الاتحاد الأوروبي والولايات المتحدة ودول آسيا، بما يضمن استمرار انسياب البيانات عبر الحدود دون عوائق قانونية، وهو أمر ضروري لتعزيز تنافسية الاقتصاد السعودي ضمن النظام الرقمي العالمي.

4. التحديات القانونية لتدفقات البيانات عبر الحدود في المملكة العربية السعودية:

1.4. مقدمة:

أضحت البيانات في البيئة الرقمية المعاصرة أحد أهم عناصر الاقتصاد والأمن والسيادة الوطنية. وبالنسبة للمملكة العربية السعودية، فإن تدفقات البيانات عبر الحدود تشكل إشكالية قانونية وتنظيمية معقدة، نظرًا لتقاطعها مع عدة أهداف استراتيجية، تشمل حماية الخصوصية الفردية، وتعزيز الأمن الوطني، وتحقيق التحول الرقمي وفق رؤية المملكة 2030، وجذب الاستثمارات الأجنبية. وعلى الرغم من إصدار نظام حماية البيانات الشخصية عام 2021، وإقرار تعديلاته التشريعية عام 2023، ودخوله حيز النفاذ في 14 سبتمبر من العام نفسه، ثم استكمال فترة توفيق الأوضاع العامة خلال عام 2024، فإن التطبيق العملي لقواعد نقل البيانات الشخصية عبر الحدود يظل مجالًا مهمًا للتحليل القانوني، خاصة فيما يتعلق بمدى وضوح الإجراءات التنظيمية وفعالية الضمانات وآليات الامتثال. ومن ثم، تبرز أهمية دراسة قدرة الإطار القانوني السعودي على تحقيق التوازن بين حماية الحقوق الفردية والسيادة الوطنية ومتطلبات الاستثمار والتجارة الرقمية الدولية (المملكة العربية السعودية، 2021؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، 2023).

2.4. الإطار العام للتحديات:

يمكن تقسيم التحديات القانونية التي تواجه المملكة في مجال تدفقات البيانات عبر الحدود إلى خمسة مستويات رئيسية:

1. التحديات الدستورية والسيادية: تتعلق بحق الدولة في حماية بيانات مواطنيها واعتبارها موردا استراتيجيا.
2. التحديات التشريعية والتنظيمية: تنشأ من ثغرات أو غموض في صياغة PDPL ولوائحه التنفيذية.
3. التحديات القضائية والمؤسسية: تتعلق بضعف الخبرة، والاستقلالية، وآليات الإنفاذ.
4. التحديات الاقتصادية والتجارية: ترتبط بقدرة النظام القانوني على جذب الاستثمارات دون المساس بالسيادة.
5. التحديات الدولية والإقليمية: تتعلق بالاعتراف المتبادل والتوافق مع الأنظمة القانونية العالمية والإقليمية.

3.4. التحديات الدستورية والسيادية:

1.3.4. السيادة الرقمية والبيانات كأصل وطني

تُعد البيانات موردًا استراتيجيًا يرتبط تنظيمه بمفهوم السيادة الرقمية، دون أن يعني ذلك ملكية الدولة لجميع بيانات الأفراد والمؤسسات .(Creemers, 2022) وفي المملكة العربية السعودية، ينظم نظام حماية البيانات الشخصية نقل البيانات إلى الخارج بشروط وضمانات محددة، ولا يفرض حظرًا شاملًا على جميع عمليات النقل (المملكة العربية السعودية، 2021).

الإشكالية: السياسات المقيدة مثل " توطين البيانات" (Data Localization) قد تعزز من سيطرة الدولة، لكنها في المقابل تثير اعتراضات من الشركاء التجاريين والشركات متعددة الجنسيات.

مثال مقارن: ينظم قانون أمن البيانات الصيني لعام 2021 البيانات المهمة ونقلها دون توطين شامل، بينما ينظم النظام السعودي النقل بشروط مختلفة بعد تعديلاته عام 2023 (National People's Congress, 2021؛ المملكة العربية السعودية، 2021).

2.3.4. الأمن الوطني وحماية البيانات الحساسة

يُعد الأمن الوطني اعتبارًا أساسيًا عند نقل البيانات الشخصية خارج المملكة. فالمادة التاسعة والعشرون تشترط ألا يمس النقل الأمن الوطني أو مصالح المملكة الحيوية، إلى جانب توافر مستوى مناسب من الحماية والاقتصار على البيانات اللازمة وفق الأحوال النظامية. وتوجب لائحة النقل تقويم المخاطر في حالات محددة، منها نقل البيانات الحساسة بصورة مستمرة أو واسعة النطاق. ويرى الباحث أن تطبيق هذه الضوابط يستلزم فحص طبيعة البيانات ومخاطر الجهة المستقبلة، دون افتراض حظر عام لعمليات النقل (المملكة العربية السعودية، 2021؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024ب).

تثير القيود المرتبطة بالأمن الوطني إشكالات تتعلق بوضوح معايير تطبيقها على نقل البيانات خارج المملكة. فالمادة التاسعة والعشرون تشترط ألا يمس النقل الأمن الوطني أو المصالح الحيوية للمملكة. وفي الإطار الأوروبي، ينبغي التمييز بين أنشطة الأمن القومي الخارجة عن نطاق اللائحة العامة لحماية البيانات وبين القيود التي تجيزها المادة الثالثة والعشرون على بعض الحقوق والالتزامات وفق شروط الضرورة والتناسب. ومن ثم، يتمثل التحدي في وضع معايير وإجراءات واضحة لتطبيق القيود الأمنية بما يحمي المصالح الوطنية دون تجاوز ما تقتضيه الضرورة (المملكة العربية السعودية، 2021؛ European Parliament & Council of the European Union, 2016).

الأثر المباشر لهذا الغموض يتمثل في تأثيره على ثقة المستثمرين الأجانب. فالشركات العالمية التي تفكر في الاستثمار داخل المملكة تبحث عادة عن بيئة قانونية واضحة ومستقرة، تضمن التنبؤ بالقرارات والسياسات المتعلقة بنقل البيانات. وإذا رأت هذه الشركات أن الاستثناءات الأمنية قد تُستخدم بشكل غير متوقع أو موسع، فقد يؤدي ذلك إلى ترددها في استضافة مراكز بيانات أو إدارة عمليات رقمية تعتمد على تدفقات سلسة للمعلومات عبر الحدود. ومن ثم، فإن تحقيق التوازن بين حماية الأمن الوطني من جهة والحفاظ على جاذبية المملكة كبيئة استثمارية من جهة أخرى يظل تحديا محوريا يتطلب عناية خاصة في تطوير اللوائح التنفيذية والتفسيرات القضائية المستقبلية للنظام.

4.4. التحديات التشريعية والتنظيمية:

1. غموض معايير النقل الدولي للبيانات

تُعد قواعد نقل البيانات الشخصية إلى خارج المملكة مجالًا مهمًا لتحليل مدى وضوح المتطلبات التنظيمية. فقد حددت المادة التاسعة والعشرون من نظام حماية البيانات الشخصية شروط النقل، ونظمت لائحة النقل إجراءات ومعايير تقييم مستوى الحماية في

الدولة أو المنظمة المستقبلة، بما يشمل التشريعات الرقابية وحقوق أصحاب البيانات وآليات الإنفاذ. كما أتاحت اللائحة ضمانات مناسبة في حالات محددة. ومن ثم، لا يصح وصف معايير الحماية المكافئة بأنها غائبة تمامًا، غير أن تطبيقها على عمليات النقل المختلفة قد يثير تساؤلات عملية بشأن الأدلة المطلوبة وتقييم مخاطر الدولة المستقبلة. ويرى الباحث أن نشر إرشادات تطبيقية واضحة يعزز اتساق الامتثال (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024).

وبناء على ما سبق يتضح للباحثة التداعيات العملية لهذا الغموض في تعقيد المعاملات التجارية الدولية. إذ أن غياب معايير واضحة لتحديد ما إذا كانت دولة معينة تتمتع بحماية مكافئة قد يعرقل نقل البيانات اللازمة للأنشطة التجارية والخدمات العابرة للحدود، مثل التجارة الإلكترونية والخدمات المالية السحابية. كما قد يؤدي ذلك إلى تضارب في التفسيرات بين الجهات التنظيمية المختلفة، بل وإلى تباطؤ في حركة الاستثمارات التي تعتمد بشكل أساسي على بيئة قانونية واضحة ومستقرة. وبالتالي، فإن وضع معايير دقيقة وشفافة لنقل البيانات إلى الخارج يمثل شرطا أساسيا لضمان الثقة القانونية والاقتصادية في النظام السعودي الجديد.

2. المسوغ النظامي لمعالجة البيانات الشخصية وإدارة الموافقة

يُعد تحديد المسوغ النظامي لمعالجة البيانات الشخصية من المسائل الأساسية التي يقوم عليها الامتثال لنظام حماية البيانات الشخصية السعودي (PDPL)، إذ يتطلب تحقيق التوازن بين حماية خصوصية الأفراد وتمكين المؤسسات من معالجة البيانات للأغراض المشروعة. وعلى الرغم من أن المادة الخامسة من النظام تقرر قاعدة الحصول على موافقة صاحب البيانات الشخصية على المعالجة، فإن المشرع السعودي لم يجعل الموافقة الأساس النظامي الوحيد؛ فقد أجازت المادة السادسة إجراء المعالجة دون موافقة في حالات محددة، من بينها تنفيذ التزامات مقررة بموجب نظام آخر أو اتفاق سابق يكون صاحب البيانات طرفًا فيه، وتحقيق مصلحة متحققة لصاحب البيانات عند تعذر التواصل معه أو صعوبته، وبعض حالات المعالجة لدى الجهات العامة للأغراض الأمنية أو القضائية، فضلًا عن المعالجة اللازمة لتحقيق مصالح مشروعة لجهة التحكم، بشرط عدم الإخلال بحقوق صاحب البيانات أو التعارض مع مصالحه، وألا تتعلق المعالجة ببيانات حساسة. كما حددت اللائحة التنفيذية ضوابط تطبيق هذه المسوغات، ولا سيما الشروط المتعلقة بالموافقة والمعالجة لتحقيق المصلحة المشروعة (المملكة العربية السعودية، 2021، المادتان الخامسة والسادسة؛ الهيئة السعودية للبيانات والذكاء الاصطناعي، 2023، المادتان الحادية عشرة والسادسة عشرة).

ومع ذلك، فإن تعدد المسوغات النظامية للمعالجة لا يلغي التحديات التطبيقية المرتبطة باختيار المسوغ الملائم لكل نشاط، خاصة في ظل تنوع عمليات المعالجة وتداخل أغراضها داخل المؤسسات. فقد يؤدي الاعتماد غير المبرر على الموافقة، في الحالات التي يتوافر فيها مسوغ نظامي آخر مستوفٍ لشروطه، إلى زيادة الأعباء الإجرائية المرتبطة بطلب الموافقات وتوثيقها وإدارتها. كما قد يؤدي عدم التمييز بين الحالات التي تستلزم الموافقة الصريحة والحالات التي تكفي فيها الموافقة المستوفية لشروطها العامة إلى ممارسات امتثال غير متسقة.

وتبرز أهمية هذه المسألة في المؤسسات التي تعتمد على المعالجة المستمرة للبيانات أو تتعامل مع أطراف متعددة داخل المملكة وخارجها. ويرى الباحث أن التحدي الرئيس لا يتمثل في قصور النظام عن إقرار مسوغات متعددة للمعالجة، وإنما في ضمان حسن تفسير هذه المسوغات وتطبيقها، وتطوير القدرات المؤسسية اللازمة لتحديد الأساس النظامي الملائم لكل عملية معالجة، وتوثيق مبررات الاعتماد عليه، وإجراء تقويم المصالح المشروعة عند الاقتضاء. ومن ثم، فإن تعزيز الإرشاد التنظيمي والتدريب المتخصص وتطوير إجراءات الامتثال الداخلية يمثل متطلبًا مهمًا لتحقيق التوازن بين حماية حقوق أصحاب البيانات ومرونة الأنشطة الاقتصادية الرقمية.

3. تحديات تطبيقية للبنود التعاقدية القياسية لنقل البيانات الشخصية خارج المملكة

شهد الإطار التنظيمي السعودي لنقل البيانات الشخصية عبر الحدود تطورًا مهمًا بإقرار البنود التعاقدية القياسية (Standard Contractual Clauses – SCCs) بوصفها إحدى الضمانات القانونية المناسبة لنقل البيانات الشخصية إلى خارج المملكة في الحالات التي تجيزها الأنظمة واللوائح ذات الصلة.

فقد نظمت لائحة نقل البيانات الشخصية إلى خارج المملكة استخدام هذه البنود، إلى جانب القواعد المشتركة الملزمة وشهادات الاعتماد، كما أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في سبتمبر 2024 نماذج رسمية للبنود التعاقدية القياسية، بهدف تحديد الالتزامات القانونية لأطراف عملية النقل وضمان مستوى من الحماية لا يقل عن المستوى المقرر في النظام السعودي ولوائحه التنفيذية. ويمثل هذا التطور خطوة مهمة نحو تعزيز الوضوح القانوني وتوفير آلية تعاقدية معتمدة لنقل البيانات الشخصية إلى الجهات الواقعة خارج المملكة، بما يسهم في مواءمة الإطار التنظيمي السعودي مع الممارسات الدولية في مجال حماية البيانات (الهيئة السعودية للبيانات والذكاء الاصطناعي، 2024أ، 2024ب).

ومع ذلك، فإن وجود البنود التعاقدية القياسية لا ينهي جميع التحديات القانونية والعملية المرتبطة بنقل البيانات عبر الحدود؛ إذ تبرز صعوبات تتعلق بالتحقق من قدرة الجهات المستوردة للبيانات على الالتزام بالضمانات التعاقدية، ولا سيما عندما تتعارض القوانين المطبقة في الدولة المستقبلة مع بعض الالتزامات المنصوص عليها في تلك البنود.

كما تفرض طبيعة العلاقات التعاقدية العابرة للحدود ضرورة تحديد مسؤوليات الأطراف المختلفة، وضمان الامتثال المستمر لمتطلبات حماية البيانات، والتحقق من سلامة عمليات النقل اللاحق والإجراءات المتخذة عند الإخلال بالالتزامات التعاقدية. ويرى الباحث أن التحدي الرئيس في هذا المجال لم يعد يتمثل في غياب الأداة القانونية، بل في مدى فاعلية تطبيقها وقدرة المؤسسات على توظيفها بصورة تحقق الحماية الفعلية للبيانات، دون فرض أعباء امتثال غير متناسبة مع طبيعة أنشطتها.

ومن ثم، فإن تعزيز الإرشاد التنظيمي، وتطوير القدرات المؤسسية، ورفع مستوى الوعي بالالتزامات التعاقدية، تمثل متطلبات مهمة لتحقيق التوازن بين حماية الخصوصية وتيسير تدفقات البيانات الدولية في إطار نظام حماية البيانات الشخصية السعودي.

4. ضعف التكامل بين PDPL وتشريعات أخرى

يُظهر تحليل النظام السعودي وجود ثغرة تتعلق بضعف التكامل بين PDPL وغيره من التشريعات ذات الصلة، مثل قوانين الأمن السيبراني، أو قوانين التجارة الإلكترونية، أو الأنظمة المتعلقة بالجرائم المعلوماتية. فبدلا من وجود إطار قانوني موحد يضمن الانسجام بين هذه التشريعات، نجد أن هناك بعض التداخلات وأحيانا التناقضات التي قد تؤدي إلى ارتباك في الامتثال. على سبيل المثال، قد تتطلب بعض اللوائح الأمنية الاحتفاظ بالبيانات لفترات طويلة، بينما يفرض PDPL مبادئ تقليل البيانات وعدم الاحتفاظ بها إلا للضرورة، وهو ما يخلق ازدواجية قد تربك المؤسسات والشركات، هذا الافتقار للمواءمة يعكس تحديا تشريعيا وتنظيميا مهما، لأنه يضعف الكفاءة التنفيذية ويؤدي إلى إرباك الجهات المعنية بتطبيق القوانين، سواء كانت جهات تنظيمية أو مؤسسات خاصة.

كما أن الشركات العاملة في المملكة قد تجد نفسها أمام التزامات متعارضة، ما يزيد من تكاليف الامتثال ويضعف قدرتها على التنبؤ بالمخاطر القانونية. وعليه، فإن تحقيق التكامل بين PDPL وبقية التشريعات الوطنية ذات الصلة يعد ضرورة ملحة لضمان فعالية النظام، ولتعزيز ثقة الفاعلين الاقتصاديين في البيئة الرقمية السعودية، بما يسهم في دفع عجلة التحول الرقمي وفق رؤية المملكة 2030.

5.4. التحديات القضائية والمؤسسية:

1. محدودية الخبرة القضائية

يثير التطبيق القضائي لنظام حماية البيانات الشخصية السعودي أسئلة تتعلق بتطور تفسير أحكامه، خاصة في المنازعات الناشئة عن المعالجة غير المشروعة أو نقل البيانات خارج المملكة. غير أن الجزم بغياب السوابق القضائية أو ضعف خبرة القضاء يستلزم مسحًا موثقًا للأحكام والقرارات القضائية، وهو ما لا يتوافر في المراجع المستخدمة هنا. ويقرر النظام وسائل للشكاوى والجزاءات والتعويض، بما يتيح أساسًا نظاميًا لمعالجة المنازعات. ومن منظور الباحث، قد يكون من المفيد تعزيز نشر القرارات ذات الصلة وتطوير التدريب التخصصي لمساندة الاتساق التفسيري، دون استنتاج أن المؤسسات القضائية تفتقر فعليًا إلى الكفاءة أو أن المستثمرين فقدوا الثقة فيها، أو نسبة نتائج محددة إلى القضاء الوطني دون مسح منهجي للأحكام المنشورة (المملكة العربية السعودية، 2021، المواد 34–36 و40).

2. استقلالية الجهة التنظيمية

يتولى الإشراف على تطبيق نظام حماية البيانات الشخصية السعودي الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، وهي جهة حكومية تتبع مباشرة للسلطة التنفيذية. ورغم أن هذا النموذج قد يوفر مرونة وسرعة في اتخاذ القرارات، إلا أنه يثير تساؤلات حول مدى استقلالية الجهة التنظيمية. ففي المقارنة مع أوروبا، تتمتع هيئات حماية البيانات بدرجة عالية من الاستقلال المؤسسي، وهو ما يعزز ثقة الأفراد والشركات في حياد قراراتها. أما في الحالة السعودية، فقد يُنظر إلى الارتباط المباشر بين SDAIA والسلطة التنفيذية باعتباره افتقارا إلى الحياد المؤسسي المطلوب، مما قد يحد من فعالية النظام في نظر بعض الأطراف الدولية (Greenleaf, 2021). هذا التحدي يرتبط أيضا برغبة المملكة في تعزيز ثقة المستثمرين والشركاء التجاريين، إذ أن الشفافية والاستقلالية تعدان من المعايير الجوهرية في البيئة الرقمية العالمية.

3. ضعف البنية المؤسسية للامتثال

يمثل الامتثال لمتطلبات PDPL تحديا كبيرا بالنسبة للعديد من الشركات السعودية، خصوصا تلك الصغيرة والمتوسطة التي لا تمتلك الموارد البشرية أو التقنية اللازمة لبناء هياكل متكاملة لحماية البيانات. ففي حين تتطلب النصوص القانونية تعيين مسؤول حماية بيانات (Data Protection Officer) وتطوير سياسات وإجراءات صارمة لإدارة البيانات، تواجه هذه المؤسسات صعوبة في التكيف مع المتطلبات، ما يخلق فجوة واضحة بين القانون النظري والواقع العملي. هذا الوضع لا يعكس فقط محدودية الموارد المؤسسية، بل يشير أيضا إلى الحاجة لتطوير برامج تدريب وتوعية واسعة النطاق، إضافة إلى توفير أدوات امتثال معيارية تساعد الشركات على الوفاء بمتطلبات القانون دون أعباء مفرطة. وفي غياب هذا الدعم، قد يبقى التطبيق الفعلي للنظام بعيدا عن تحقيق أهدافه في حماية البيانات وتعزيز الثقة بالبيئة الرقمية.

6.4. التحديات الاقتصادية والتجارية:

1. جذب الاستثمارات الأجنبية المباشرة، حيث تشير دراسات OECD (2021) إلى أن القيود الصارمة على تدفقات البيانات قد تؤثر سلبا على بيئة الاستثمار. والمملكة باعتبارها تسعى أن تصبح مركزا إقليميا للبيانات الضخمة والحوسبة السحابية، تحتاج إلى إيجاد توازن دقيق.

2. أثر اللوائح على الاقتصاد الرقمي المحلي، فالشركات الناشئة في مجالات مثل التجارة الإلكترونية والذكاء الاصطناعي تحتاج إلى تدفقات بيانات مفتوحة، فالقيود القانونية قد تعيق قدرتها على التوسع والابتكار، مقارنة بدول خليجية مثل الإمارات التي تقدم بيئة أكثر انفتاحا.

7.4. التحديات الدولية والإقليمية:

1. غياب الاعتراف المتبادل مع الاتحاد الأوروبي، حيث لا تتمتع السعودية حاليًا بقرار ملاءمة أوروبي؛ لذا يخضع نقل البيانات إليها لضمانات أو استثناءات تجيزها GDPR (European Commission, n.d.)، وهذا يعيق التبادل التجاري الرقمي بين السعودية والاتحاد الأوروبي، أحد أهم الشركاء التجاريين.

2. التباين مع النموذج الأمريكي، فبينما يركز النظام السعودي على حماية الخصوصية وفق نهج قريب من GDPR، فإن النظام الأمريكي قطاعي ومرن أكثر. هذا التباين قد يفرض اختلاف الالتزامات الأمريكية والسعودية أعباء امتثال إضافية على الشركات العابرة للحدود، بحسب نشاطها والبيانات المعالجة (Linebaugh, 2025).

3. غياب إطار خليجي موحد، فعلى رغم وجود تقارب بين قوانين السعودية والإمارات وقطر، لا يزال غياب إطار خليجي شامل لحماية البيانات عائقا أمام إنشاء سوق بيانات خليجية موحدة.

8.4. أمثلة تطبيقية على التحديات:

1. قطاع الخدمات السحابية، فشركات مثل AWS وMicrosoft Azure تواجه عراقيل قانونية في نقل البيانات بين مراكزها العالمية والمملكة. وهذه القيود قد تقلل من استعداد هذه الشركات للاستثمار في مراكز بيانات سعودية جديدة.

2. قطاع التجارة الإلكترونية، فشركات مثل Noon وAmazon تحتاج لمشاركة بيانات العملاء عبر الحدود من أجل تحسين سلسلة التوريد. فهذه التحديات القانونية تجعل هذه العمليات أكثر تعقيدا وتكلفة.

3. القطاع الصحي، مثل مشاركة بيانات المرضى للبحوث تخضع لضوابط البيانات الصحية والنقل خارج المملكة، دون حظر شامل (المملكة العربية السعودية، 2021).

9.4. استراتيجيات مقترحة لمعالجة التحديات:

1. تعزيز الشفافية القانونية عبر تحديد معايير واضحة لـ " النقل الدولي الآمن".
2. تعزيز وضوح تطبيق المسوغات النظامية المختلفة لمعالجة البيانات الشخصية.
3. إنشاء هيئة رقابية مستقلة لتعزيز الثقة الدولية.
4. تعزيز الاستخدام الفعّال للبنود التعاقدية القياسية السعودية.
5. السعي لاعتراف متبادل مع الاتحاد الأوروبي والولايات المتحدة.
6. التنسيق الخليجي نحو إطار موحد لحماية البيانات.

5. نحو إطار وطني متوافق مع المعايير الدولية:

1.5. مقدمة:

تزايدت أهمية تطوير الإطار الوطني لحماية البيانات الشخصية في المملكة العربية السعودية بالتوازي مع التحول الرقمي والتطورات التنظيمية الدولية، ومنها اللائحة الأوروبية العامة لحماية البيانات (GDPR) ومبادئ منظمة التعاون الاقتصادي والتنمية (OECD). وفي ضوء مستهدفات رؤية السعودية 2030، يكتسب وضوح القواعد المنظمة لتدفقات البيانات عبر الحدود أهمية خاصة لتيسير الأنشطة الرقمية وجذب الاستثمار. ويرى الباحث أن الاستفادة من المعايير الدولية، مع مراعاة خصوصية النظام السعودي والتزاماته القانونية، قد تسهم في تعزيز الثقة واليقين التنظيمي.

2.5. المعايير الدولية المرجعية:

1- اللائحة العامة لحماية البيانات (GDPR): توفر إطارًا شاملًا لمبادئ المشروعية والشفافية وتقليل البيانات، وحقوق أصحاب البيانات، وتقويم أثر المعالجة في الحالات المقررة، وضمانات النقل الدولي، ومنها البنود التعاقدية القياسية (SCCs). وتتمثل الدروس المستفادة للمملكة في تعزيز التطبيق الفعال للمسوغات النظامية المتعددة الواردة في النظام السعودي، وتطوير الإرشادات المتعلقة بالموافقة والمصلحة المشروعة، وتوضيح متطلبات التناسب وحماية حقوق الأفراد، مع مراعاة الاختلافات بين التنظيمين (European Parliament & Council of the European Union, 2016).

2- مبادئ OECD (2023) والتي تركز على التوازن بين التدفق الحر للبيانات وحماية الخصوصية، وتؤكد على ضرورة وجود قيود متناسبة (proportionality) بدلا من الحظر المطلق.

3- نظام قواعد الخصوصية العابرة للحدود (APEC CBPR): يوفر نموذجًا للتعاون والاعتماد المؤسسي لحماية البيانات، ويمكن الاستفادة من خبرته عند تطوير التنسيق الخليجي في إطار مشترك، مع مراعاة انطلاق نظام Global CBPR عام 2025.

4- اتفاقيات التجارة الدولية (WTO & CPTPP)، فمنظمة التجارة العالمية تشدد على أن القيود المفرطة على تدفقات البيانات قد تشكل حواجز تجارية غير مبررة (Aaronson, 2018)، وفي إطار المملكة يجب أن يراعي التزاماتها الدولية في هذا الصدد.

3.5. المبادئ الموجهة للإطار الوطني السعودي:

استنادا إلى الممارسات العالمية، يمكن صياغة المبادئ التالية:

1. الشفافية القانونية، من خلال توضيح تطبيق المعايير القائمة للنقل الدولي ونشر الإرشادات المرتبطة بها.
2. التناسب والضرورة، أي قيد يجب أن يكون متناسبا مع الغرض.
3. التوافق التشريعي، من خلال المواءمة بين PDPL وبقية الأنظمة مثل الأمن السيبراني والتجارة الإلكترونية.
4. الاعتراف المتبادل، بالسعي لقرارات "Adequacy" مع المفوضية الأوروبية ودول أخرى.
5. الاستقلالية المؤسسية، من خلال تعزيز الاستقلال الوظيفي والشفافية والمساءلة لدى الجهة المختصة القائمة.

4.5. التوصيات التشريعية والتنظيمية:

1- تعزيز وضوح تطبيق المسوغات النظامية لمعالجة البيانات الشخصية، من خلال تطوير الإرشادات التنظيمية المتعلقة بتطبيق المسوغات النظامية للمعالجة المنصوص عليها في نظام حماية البيانات الشخصية، ولا سيما المصلحة المشروعة، وتوضيح حالات الاعتماد على الموافقة والالتزامات القانونية أو التعاقدية، بما يساعد المؤسسات على اختيار المسوغ الملائم لكل عملية معالجة ويحد من التباين في تفسير الالتزامات النظامية.

2- تعزيز فاعلية تطبيق البنود التعاقدية القياسية، من خلال تطوير الأدلة الإرشادية لتطبيق النماذج السعودية المعتمدة، والسماح بالشهادات الدولية مثل Binding Corporate Rules (BCRs).

3- عزيز تطبيق تقويم أثر المعالجة (DPIA) في الحالات المنصوص عليها في اللائحة التنفيذية، وتقويم مخاطر النقل الدولي عند تحقق الحالات المحددة في لائحة النقل.

4- تعزيز فاعلية الشكاوى ووسائل الانتصاف، بتيسير الإجراءات وتوضيح حق المطالبة بالتعويض أمام المحكمة المختصة وفق الأحكام النظامية.

5.5. التوصيات المؤسسية والقضائية:

1- إنشاء هيئة مستقلة لحماية البيانات، على غرار European Data Protection Board. والاستقلالية تعزز ثقة الشركاء الدوليين (Greenleaf, 2021).

2- تطوير القدرات القضائية والقانونية المتخصصة، عبر برامج تدريب في منازعات حماية البيانات، ودراسة الحاجة إلى مسارات تخصصية عند الاقتضاء.

3- دعم الشركات الصغيرة والمتوسطة، بتوفير أدلة إرشادية ونماذج عقود جاهزة، ودعم مالي وتقني لضمان الامتثال.

6.5. التوصيات الاقتصادية والتجارية:

1- تعزيز البيئة الاستثمارية عبر وضوح قواعد نقل البيانات، وتقويم الآثار الاقتصادية المحتملة للقيود التنظيمية، مع الموازنة بين الانفتاح والثقة وحماية الخصوصية (OECD & WTO, 2025).

2- دعم الاقتصاد الرقمي المحلي، بمنح الشركات الناشئة استثناءات مرحلية لتخفيف أعباء الامتثال، وتشجيع حلول "الامتثال كخدمة" (Compliance-as-a-Service).

7.5. التنسيق الإقليمي والدولي:

1- تعزيز التنسيق الخليجي، من خلال تطوير مبادئ وإرشادات مشتركة لحماية البيانات ودراسة آليات التعاون والاعتراف التنظيمي بين الدول، مع مراعاة اختلاف تشريعاتها الوطنية، مما يسهم في بناء سوق رقمية موحدة على غرار الاتحاد الأوروبي.

2- عقد اتفاقيات اعتراف متبادل والسعي لاتفاقيات ثنائية مع الاتحاد الأوروبي، الولايات المتحدة، ودول آسيوية كاليابان وكوريا الجنوبية.

3- دور المملكة في صياغة قواعد دولية، باستثمار عضوية المملكة في مجموعة العشرين للمساهمة في صياغة قواعد عالمية حول البيانات.

6. الخاتمة العامة والتوصيات النهائية:

يتضح من مجمل الدراسة أن موضوع تدفقات البيانات عبر الحدود في المملكة العربية السعودية يمثل أحد أكثر القضايا القانونية المعاصرة حساسية وتعقيدا. فقد أظهرت الفصول السابقة أن حماية البيانات لم تعد مسألة تقنية فحسب، بل تحولت إلى قضية استراتيجية تمس الأمن الوطني، السيادة الرقمية، الاقتصاد الرقمي، والتزامات المملكة الدولية. وبالنظر إلى تسارع التحولات العالمية في مجال حماية البيانات، أصبح لزاما على المملكة صياغة إطار وطني متكامل بتطوير الإطار القائم يوازن بين الخصوصية الفردية، الأمن الوطني، والمصالح الاقتصادية الدولية.

1.6. أهم نتائج البحث:

1.1.6. الإطار القانوني القائم في المملكة العربية السعودية

- يمثل إصدار نظام حماية البيانات الشخصية (PDPL) نقطة تحول رئيسة في بناء الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية، إذ أرسى لأول مرة منظومة متكاملة لتنظيم جمع البيانات ومعالجتها والإفصاح عنها ونقلها عبر الحدود، بما يعزز حماية الخصوصية ويواكب مستهدفات التحول الرقمي ورؤية المملكة 2030. كما أسهمت التعديلات

التشريعية الصادرة خلال عامي 2022 و2023 في معالجة عدد من الملاحظات التي أثيرت بشأن النسخة الأولى من النظام، ولا سيما فيما يتعلق بتنظيم نقل البيانات الشخصية إلى خارج المملكة، وتوسيع الأسس القانونية لمعالجة البيانات، ومنح قدر أكبر من المرونة للأنشطة الاقتصادية مع المحافظة على الضمانات الأساسية لحماية الخصوصية.

- ولم يقتصر التطور على التعديلات التشريعية، بل استمر خلال 2024–2025 من خلال إصدار الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) مجموعة من الأدلة والإرشادات التنظيمية والوثائق التفسيرية التي تهدف إلى دعم الامتثال، وتوضيح الالتزامات الواقعة على المتحكمين والمعالجين، وتعزيز التطبيق العملي للنظام داخل القطاعين العام والخاص. ويعكس ذلك انتقال الإطار النظامي السعودي من مرحلة بناء التشريع إلى مرحلة ترسيخ التطبيق والحوكمة المؤسسية، بما يسهم في تعزيز الثقة بالاقتصاد الرقمي السعودي، رغم استمرار الحاجة إلى مزيد من التطوير في بعض الجوانب التنظيمية، خاصة ما يتعلق بآليات نقل البيانات عبر الحدود والاعتراف الدولي بمستوى الحماية الذي يوفره النظام السعودي.

2.1.6. التحديات الرئيسية:

- التحديات السيادية والدستورية، والمتمثلة بالحاجة لتوضيح العلاقة بين الأمن الوطني وحماية البيانات.
- التحديات التشريعية، كالحاجة إلى مزيد من الوضوح في تطبيق معايير نقل البيانات الشخصية إلى خارج المملكة، والتحديات المرتبطة بتحديد المسوغ النظامي الملائم للمعالجة وإدارة الموافقة، والصعوبات العملية المحتملة في تطبيق البنود التعاقدية القياسية المعتمدة لنقل البيانات الشخصية عبر الحدود.
- التحديات القضائية والمؤسسية، المتعلقة بتطوير الخبرات التخصصية وتعزيز وضوح إجراءات الإنفاذ والشكاوى والتنسيق بين الجهات المختصة.
- التحديات الاقتصادية، كتأثير القيود القانونية على جذب الاستثمارات الأجنبية والشركات التقنية الكبرى.
- التحديات الدولية، كغياب قرارات الاعتراف المتبادل (Adequacy) مع الاتحاد الأوروبي وعدم وجود إطار خليجي موحد.

3.1.6. المقارنات الدولية

- GDPR في الاتحاد الأوروبي وفر نموذجا شاملا يعتمد على مبادئ أساسية مثل الشفافية والتناسب.
- النظام الأمريكي أظهر مرونة من خلال النهج القطاعي، لكنه يفتقر إلى قانون اتحادي شامل.
- التجربة الصينية أبرزت البعد الأمني والسيادي بشكل صارم.
- هذه النماذج قدمت دروسا يمكن للمملكة الاستفادة منها عند صياغة إطارها الوطني.

2.6. التوصيات النهائية:

1- على المستوى التشريعي

- تعزيز التطبيق الفعّال للمسوغات النظامية المتعددة لمعالجة البيانات الشخصية، وتطوير الأدلة الإرشادية وآليات الامتثال التي توضح شروط استخدام الموافقة والمصلحة المشروعة وغيرها من المسوغات المنصوص عليها في النظام، بما ينسجم مع GDPR.
- تعزيز تطبيق النماذج المعتمدة وتوفير الإرشادات والتدريب اللازم للامتثال (Saudi Standard Contractual Clauses) وتطوير النماذج التعاقدية الرسمية من قبل SDAIA لتنظيم نقل البيانات عبر الحدود، بما يحقق مزيدًا من الوضوح القانوني وييسر امتثال المؤسسات، على غرار العقود القياسية المعتمدة في الاتحاد الأوروبي.

- تطوير إرشادات أكثر تفصيلًا لتطبيق شرط عدم المساس بالأمن الوطني فيما يتعلق بنقل البيانات بحيث لا يكون غطاء لتقييد غير مبرر لتدفق البيانات.
- تطوير أدلة إرشادية تطبيقية أكثر تفصيلًا بشأن استخدام المصلحة المشروعة (Legitimate Interests) بوصفها مسوغًا نظاميًا لمعالجة البيانات الشخصية، مع توضيح إجراءات تقويم المصالح المشروعة والموازنة بين مصالح جهة التحكم وحقوق أصحاب البيانات وفق المادة السادسة عشرة من اللائحة التنفيذية لنظام حماية البيانات الشخصية. كما يوصي الباحث بتعزيز التزام المؤسسات بإجراء تقويم الأثر على معالجة البيانات الشخصية (Data Protection Impact Assessment – DPIA) في الحالات التي تستلزم ذلك وفق المادة الخامسة والعشرين من اللائحة التنفيذية، مع ضرورة التمييز بين تقويم المعالجة للمصلحة المشروعة وتقويم الأثر على معالجة البيانات الشخصية، باعتبارهما إجراءين تنظيميين مختلفين من حيث الغرض والنطاق والمتطلبات القانونية.

2- على المستوى المؤسسي والقضائي

- تعزيز الاستقلال الوظيفي والتنظيمي للجهة المختصة بالإشراف على حماية البيانات، مع دعم صلاحياتها الرقابية وآليات المساءلة والشفافية، بما يعزز الثقة المحلية والدولية في منظومة حماية البيانات الشخصية، وبما يقترب من أفضل الممارسات المقارنة دون المساس بالبنية المؤسسية القائمة.
- بناء قدرات قضائية متخصصة من خلال تدريب قضاة وخبراء قانونيين في مجال البيانات.
- تعزيز فعالية وسائل الانتصاف المنصوص عليها في نظام حماية البيانات الشخصية، من خلال تطوير إرشادات تقديم الشكاوى ومتابعتها، وتحسين وضوح الإجراءات والمدد النظامية، وتعزيز إتاحة المعلومات المتعلقة بقرارات الإنفاذ، بما يدعم اتساق التطبيق وثقة أصحاب البيانات، مع المحافظة على حق المطالبة بالتعويض أمام المحكمة المختصة.

3- على المستوى الاقتصادي

- إجراء تقييم دوري للأثر الاقتصادي للقيود المفروضة على تدفقات البيانات.
- تقديم دعم للشركات الصغيرة والمتوسطة لمساعدتها على الامتثال، عبر إرشادات وأدوات جاهزة.
- تحفيز الاستثمار في مراكز البيانات المحلية لتقليل الاعتماد على النقل الدولي مع الحفاظ على تنافسية السوق.

4- على المستوى الدولي والإقليمي

- السعي للحصول على اعتراف Adequacy من الاتحاد الأوروبي لتعزيز الثقة والتعاون التجاري.
- تعزيز التعاون والاتفاقيات الثنائية ومتعددة الأطراف مع الشركاء التجاريين، بما يتوافق مع الأحكام المنظمة لنقل البيانات الشخصية.
- العمل نحو إطار خليجي موحد لحماية البيانات يسهم في إنشاء سوق رقمية إقليمية.
- تعزيز المشاركة في مناقشات حوكمة البيانات والتجارة الرقمية ضمن مجموعة العشرين ومنظمة التجارة العالمية والمحافل الدولية ذات الصلة.

3.6. خاتمة عامة:

يمثل تنظيم تدفقات البيانات عبر الحدود أحد أبرز التحديات في الحقبة الرقمية. بالنسبة للمملكة، فإن هذا التحدي يرتبط بشكل مباشر بتحقيق أهداف رؤية 2030، وتعزيز دورها كمركز إقليمي للبيانات والتقنية. إن تطوير إطار وطني متوازن يضمن حماية

الخصوصية، احترام السيادة، دعم الاقتصاد الرقمي، والالتزام بالمعايير الدولية هو السبيل الأمثل لتحقيق هذا الهدف. وبذلك فإن المملكة تقف اليوم أمام فرصة استراتيجية أن تتحول من مستهلك للتشريعات العالمية إلى مساهم فاعل في صياغتها، بما يتناسب مع مصالحها الوطنية ودورها الإقليمي والدولي.

7. المراجع:

1.7. المراجع العربية:

الهيئة السعودية للبيانات والذكاء الاصطناعي. (د.ت.). الدليل الاسترشادي لإتلاف البيانات الشخصية وإخفاء الهوية والترميز. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PersonalDataDestruction

الهيئة السعودية للبيانات والذكاء الاصطناعي. (2023). اللائحة التنفيذية لنظام حماية البيانات الشخصية (بصيغتها المعدلة). https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2

الهيئة السعودية للبيانات والذكاء الاصطناعي. (2024أ). البنود التعاقدية القياسية لنقل البيانات الشخصية. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/StandardContractualClauses

الهيئة السعودية للبيانات والذكاء الاصطناعي. (2024ب). لائحة نقل البيانات الشخصية إلى خارج المملكة (الصيغة المعدلة لعام 2024). https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/RegulationonPersonalDataTransferOutsidetheKingdom

الهيئة الوطنية للأمن السيبراني. (2024). الضوابط الأساسية للأمن السيبراني (ECC-2:2024). https://nca.gov.sa/ar/regulatory-documents/controls-list/ecc/

المملكة العربية السعودية. (2021). نظام حماية البيانات الشخصية (المرسوم الملكي رقم م/19 بتاريخ 1443/2/9هـ، المعدل بالمرسوم الملكي رقم م/148 بتاريخ 1444/9/5هـ). هيئة الخبراء بمجلس الوزراء. https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1

رؤية السعودية 2030. (2025). التقرير السنوي لرؤية السعودية 2030 لعام 2024. https://www.vision2030.gov.sa/media/iv3f11uf/annual-report-2024.pdf

2.7. المراجع الأجنبية

Aaronson, S. A. (2018). Data is different: Why the world needs a new approach to governing cross-border data flows (CIGI Paper No. 197). Centre for International Governance Innovation. https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows /

Asia-Pacific Economic Cooperation. (2017). APEC privacy framework (2015). https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-%282015%29

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Burri, M. (2021). Data flows and global trade law. In M. Burri (Ed.), Big data and global trade law (pp. 11–41). Cambridge University Press. https://doi.org/10.1017/9781108919234.003

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Court of Justice of the European Union. (2020, July 16). Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18, ECLI:EU:C:2020:559). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011. https://doi.org/10.1093/cybsec/tyac011

Cyberspace Administration of China. (2024, March 22). 促进和规范数据跨境流动规定 [Provisions on promoting and regulating cross-border data flows]. https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

European Commission. (2023). Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–US Data Privacy Framework. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng

European Commission. (n.d.). Adequacy decisions. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Parliament & Council of the European Union. (2016). 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, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Global CBPR Forum. (2025). The Global CBPR and Global PRP systems are now live. https://www.globalcbpr.org/the-global-cbpr-and-global-prp-system-are-now-live/

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, 169, 3–5. https://doi.org/10.2139/ssrn.3836348

Irion, K. (2012). Government cloud computing and national data sovereignty. Policy & Internet, 4(3–4), 40–71. https://doi.org/10.1002/poi3.10

Kuner, C. (2011). Regulation of transborder data flows under data protection and privacy law: Past, present and future (OECD Digital Economy Papers No. 187). OECD Publishing. https://doi.org/10.1787/5kg0s2fk315f-en

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.001.0001

Linebaugh, C. D. (2025). Preemption and privacy law (CRS Report No. R48667). Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R48667/R48667.1.pdf

López González, J. (2021). Trade and cross-border data flows (OECD Going Digital Toolkit Notes No. 11). OECD Publishing. https://doi.org/10.1787/7bc12916-en

National Academies of Sciences, Engineering, and Medicine. (2018). Decrypting the encryption debate: A framework for decision makers. The National Academies Press. https://doi.org/10.17226/25010

National People's Congress. (2021). Data Security Law of the People's Republic of China. https://en.spp.gov.cn/2021-06/10/c_948426.htm

OECD. (2013). The OECD privacy framework. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD. (2025). Intellectual property issues in artificial intelligence trained on scraped data (OECD Artificial Intelligence Papers No. 33). OECD Publishing. https://doi.org/10.1787/d5241a23-en

OECD & World Trade Organization. (2025). Economic implications of data regulation: Balancing openness and trust. OECD Publishing. https://doi.org/10.1787/aa285504-en

Saudi Data & Artificial Intelligence Authority. (2020). National strategy for data and AI (NSDAI). https://wp.oecd.ai/app/uploads/2021/12/Saudi_Arabia_National_Strategy_for_Data_and_AI_2020.pdf

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. Georgetown Law Journal, 106(1), 115–180. https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law /

Svantesson, D. J. B. (2017). Solving the internet jurisdiction puzzle. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

Whelan, J. (2024, October 28). Personal data protection legislation in the GCC jurisdiction. HFW. https://www.hfw.com/insights/personal-data-protection-legislation-in-the-gcc-jurisdiction /

© Copyright 2026 (الدكتورة/ منيرة فهد الحمدان). تُنشر هذه الدراسة بموجب ترخيص المشاع الإبداعي Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

This article is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Doi: https://doi.org/10.52133/ijrsp.v8.85.8