

مدى توافق نظام حماية البيانات الشخصية السعودي مع اللائحة الأوروبية العامة لحماية البيانات
(GDPR) – دراسة مقارنة

الباحث: علي بن محمد الشهري
الرقم الجامعي: (٢٥١٠٠٤٥٢)

الباحث المعتمد للمراسلة: علي محمد الشهري

٢٠٢٦م

الملخص

الأهداف:

يهدف البحث إلى دراسة نظام حماية البيانات الشخصية في المملكة العربية السعودية (PDPL) من حيث نشأته وتطوره ومبادئه وحقوق أصحاب البيانات، مع استعراض تاريخي لنشأة اللائحة الأوروبية العامة لحماية البيانات (GDPR) وتطورها إلى مرتبة الحق الأساسي. كما يسعى البحث إلى إجراء دراسة مقارنة بين النظامين لكشف أوجه التشابه والاختلاف، بهدف تقييم مدى توافق النظام السعودي مع المعايير الدولية، وتقديم توصيات لتطويره بما يتناسب مع التحول الرقمي الوطني ورؤية ٢٠٣٠، مع الحفاظ على السياق الثقافي والديني المحلي.

المنهجية:

اعتمد البحث المنهج الوصفي التحليلي لاستعراض النشأة والتطور التاريخي لكلا النظامين، مع الاستناد إلى النصوص التشريعية الرسمية مثل المرسوم الملكي رقم (م/١٩) ولائحته التنفيذية المعدلة، واللائحة الأوروبية 2016/679 (EU). كما استخدم المنهج المقارن لتحليل أوجه التشابه في التعريفات والمبادئ وحقوق أصحاب البيانات وآليات الإفصاح والعقوبات، وأوجه الاختلاف مثل غياب "الخصوصية من التصميم" وتقييم الآثار على الخصوصية في النظام السعودي، مع الرجوع إلى قرارات محكمة العدل الأوروبية ودراسات سابقة.

النتائج:

أظهرت الدراسة توافقاً واسعاً بين النظامين في التعريفات الأساسية، والمبادئ مثل المشروعية والشفافية وتقليل البيانات، وحقوق أصحاب البيانات كالحق في العلم والوصول والمحو والاعتراض. كما تبين تأثير النظام السعودي بـ GDPR مع تكييف محلي يراعي الحساسية الثقافية تجاه البيانات الدينية والعائلية. ومع ذلك، برزت اختلافات في غياب بعض الأدوات الوقائية المتقدمة في النظام السعودي، واختلاف آليات العقوبات، مما يعكس حداثة النظام السعودي مقارنة بتجربة GDPR الطويلة.

التوصيات:

يُوصى بتعزيز النظام السعودي بإدراج مبدأ "الخصوصية من التصميم" (Privacy by Design) والزامية تقييم الآثار على الخصوصية (PIA)، خاصة مع انتشار الذكاء الاصطناعي. كما يُقترح تطوير آليات رقابية أكثر مرونة للنقل الدولي للبيانات، وتعزيز التوعية والتدريب للجهات المعنية، مع دراسة إمكانية تبني بعض عقوبات GDPR النسبية للشركات الكبرى، لضمان مواكبة التحديات التقنية المستقبلية دون المساس بالسيادة الوطنية.

الكلمات الدالة:

حماية البيانات الشخصية، النظام السعودي، GDPR، الدراسة المقارنة، الخصوصية الرقمية، التحول الرقمي، حقوق أصحاب البيانات.

Objectives

The research aims to examine the Personal Data Protection Law (PDPL) in the Kingdom of Saudi Arabia in terms of its origins, evolution, fundamental principles, and data subjects' rights, alongside a historical review of the emergence of the EU General Data Protection Regulation (GDPR) and its elevation to the status of a fundamental right. Furthermore, the study seeks to conduct a comparative analysis between the two systems to identify similarities and differences, with the goal of assessing the extent of the Saudi system's alignment with international standards and providing recommendations for its development in a manner compatible with the national digital transformation and Vision 2030, while preserving the local cultural and religious context.

Methodology:

The research adopted a descriptive-analytical approach to review the origins and historical development of both systems, relying on official legislative texts such as Royal Decree No. (M/19) and its amended executive regulations, as well as Regulation (EU) 2016/679. It also employed a comparative methodology to analyze similarities in definitions, principles, data subjects' rights, disclosure mechanisms, and penalties, as well as differences such as the absence of "Privacy by Design" and Privacy Impact Assessment (PIA) in the Saudi system, with reference to judgments of the Court of Justice of the European Union and previous studies.

Results:

The study revealed extensive alignment between the two systems in basic definitions, principles such as lawfulness, transparency, and data minimization, and data subjects' rights including the right to be informed, access, erasure, and objection. It also demonstrated the influence of GDPR on PDPL, with local adaptations that consider cultural sensitivity toward religious and family data. Nevertheless, differences emerged in the absence of certain advanced preventive tools in the Saudi system and variations in penalty mechanisms, reflecting the relative novelty of the Saudi system compared to the long-established experience of GDPR.

Recommendations:

It is recommended to strengthen the Saudi system by incorporating the principle of "Privacy by Design" and mandating Privacy Impact Assessment (PIA), particularly with the proliferation of artificial intelligence. It is also proposed to develop more flexible oversight mechanisms for international data transfers, enhance awareness and training for relevant entities, and study the potential adoption of some proportional penalties from GDPR for large companies, to ensure readiness for future technological challenges without compromising national sovereignty.

Keywords:

Personal data protection, Saudi system, GDPR, comparative study, digital privacy, digital transformation, data subjects' rights.

المقدمة

يشهد العالم الرقمي اليوم توسعًا غير مسبوق في حجم البيانات الشخصية المتداولة عبر المنصات الإلكترونية والتطبيقات الذكية، مدفوعًا بانتشار التقنيات الناشئة مثل الذكاء الاصطناعي، إنترنت الأشياء، والحوسبة السحابية. هذا التوسع، رغم فوائده في تعزيز الابتكار والخدمات الرقمية، يثير تحديات جسيمة تتعلق بانتهاك الخصوصية، تسرب البيانات، والاستغلال غير المشروع للمعلومات الشخصية، مما يهدد حقوق الأفراد الأساسية ويقلل من الثقة في التعاملات الإلكترونية.

في هذا السياق العالمي، برزت الحاجة إلى أطر تشريعية متينة تحمي البيانات الشخصية وتوازن بين متطلبات الاقتصاد الرقمي وحقوق الخصوصية. أصدرت المملكة العربية السعودية نظام حماية البيانات الشخصية (PDPL) عام ٢٠٢١ مع تعديلاته اللاحقة، كجزء أصيل من رؤية ٢٠٣٠ وبرنامج التحول الوطني، لتعزيز الثقة في الخدمات الرقمية مثل "أبشر" و"توكلنا". أما الاتحاد الأوروبي، فقد وضع اللائحة العامة لحماية البيانات (GDPR) عام ٢٠١٨، التي أصبحت مرجعًا عالميًا يُحتذى به، نظرًا لصرامتها وتأثيرها الدولي من خلال غرامات هائلة وقضايا بارزة أمام محكمة العدل الأوروبية.

تتبع أهمية هذه الدراسة من كونها دراسة مقارنة تحلل مدى توافق النظام السعودي مع GDPR، مستجلية نقاط الالتقاء في التعريفات والمبادئ والحقوق، ونقاط الاختلاف في الأدوات الوقائية والعقوبات. هذا التحليل يساهم في تقييم النظام السعودي في ضوء المعايير الدولية، ويقدم رؤى لتطويره بما يتناسب مع السياق الثقافي والديني السعودي، مع دعم الاندماج الاقتصادي الدولي والتحول الرقمي الوطني.

مشكلة الدراسة تتمثل مشكلة الدراسة في الإجابة عن السؤال الرئيس التالي:

إلى أي مدى يتوافق نظام حماية البيانات الشخصية السعودي مع اللائحة الأوروبية العامة لحماية البيانات (GDPR) من حيث المبادئ الأساسية، والنطاق التطبيقي، وآليات الحماية، وحقوق أصحاب البيانات، والعقوبات؟ أسئلة الدراسة ما هي المبادئ الأساسية التي يقوم عليها كل من النظام السعودي والـGDPR؟

ما أوجه التشابه بين النظامين في مجال حماية البيانات الشخصية؟

ما أوجه الاختلاف الجوهرية بينهما؟

كيف يمكن تعزيز توافق النظام السعودي مع أفضل الممارسات العالمية؟

ما أبرز التوصيات لتطوير النظام السعودي في ضوء التجربة الأوروبية؟

أهداف الدراسة

التعرف على الإطار القانوني لحماية البيانات الشخصية في المملكة العربية السعودية والاتحاد الأوروبي.

تحديد أوجه التشابه والاختلاف بين النظامين من حيث التعريفات، المبادئ، الحقوق، والإجراءات.

تحليل مدى توافق النظام السعودي مع المعايير الدولية المتمثلة في GDPR.

تقديم توصيات عملية لتطوير النظام السعودي بما يتلاءم مع التطورات الرقمية العالمية ورؤية ٢٠٣٠.

منهجية الدراسة

تعتمد الدراسة على المنهج التحليلي المقارن، من خلال تحليل النصوص النظامية الرسمية مثل نظام حماية البيانات الشخصية السعودي (المرسوم الملكي م/١٩ لعام ١٤٤٣هـ مع تعديلاته) ولائحته التنفيذية، واللائحة الأوروبية (EU) (GDPR) 2016/679، مع الاستعانة بقرارات محكمة العدل الأوروبية، الدراسات السابقة، والتقارير الرسمية من الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) والمجلس الأوروبي لحماية البيانات (EDPB).

خطة الدراسة

المبحث الأول: الإطار النظري والتشريعي لحماية البيانات الشخصية

المطلب الأول: نظام حماية البيانات الشخصية السعودي

الفرع الأول: النشأة والتطور

الفرع الثاني: المبادئ الأساسية

المطلب الثاني: اللائحة الأوروبية العامة لحماية البيانات

الفرع الأول: النشأة والتطور

الفرع الثاني: المبادئ الأساسية

المبحث الثاني: الدراسة المقارنة بين النظام السعودي والـGDPR

المطلب الأول: أوجه التشابه

المطلب الثاني: أوجه الاختلاف

الخاتمة..

المبحث الأول: الإطار النظري والتشريعي لحماية البيانات الشخصية

المطلب الأول: نظام حماية البيانات الشخصية السعودي

يمثل نظام حماية البيانات الشخصية في المملكة العربية السعودية أحد أبرز الإنجازات التشريعية في مجال الخصوصية الرقمية، حيث يمثل خطوة استراتيجية نحو تعزيز الثقة في التعاملات الإلكترونية ودعم التحول الرقمي الوطني. يأتي هذا النظام كاستجابة للتحديات المتزايدة الناتجة عن انتشار التقنيات الرقمية، مثل الذكاء الاصطناعي والإنترنت الأشياء، التي أدت إلى زيادة حجم البيانات الشخصية المتداولة.

التعريفات والنطاق

قبل الخوض في النشأة والتطور التاريخي لمنظومة حماية البيانات، يجب البدء بتحديد الإطار المفاهيمي للمصطلحات الأساسية المرتبطة بهذا النظام، إذ إن ضبط التعريفات يُعد المدخل المنهجي الصحيح لفهم طبيعة الحماية القانونية المقررة للبيانات الشخصية ومجال تطبيقها. فالتعريف يمثل حجر الأساس الذي يُبنى عليه تحليل النطاق، والالتزامات، والمسؤوليات، سواء بالنسبة لجهات التحكم أو جهات المعالجة أو أصحاب البيانات.

وتأسيساً على ذلك، تعرّف سياسات حوكمة البيانات الوطنية البيانات الشخصية بأنها: "كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجها مع بيانات أخرى".¹

ويشمل ذلك - على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، ووسائل التواصل، والمعلومات البنكية، وأرقام الحسابات، والبطاقات الائتمانية، وصور الأفراد الثابتة والمتحركة، وغيرها من البيانات ذات الطابع الشخصي. وتعرّف السياسات نفسها "الجهة المعالجة" بأنها كل جهة، حكومية كانت أو خاصة، تبشر معالجة البيانات الشخصية، بما في ذلك الجهات التي تعالج البيانات نيابة عن "جهة التحكم". أما "معالجة البيانات الشخصية" فتتمدد لتشمل جميع العمليات التي تمر بها البيانات بدءاً من جمعها ثم تحليلها وتخزينها ومشاركتها، وصولاً إلى إتلافها.

ومن خلال المقارنة بين التشريعات، يتضح وجود قدر كبير من التوافق بين التعريفات الواردة في سياسة حماية البيانات الشخصية الوطنية وبين نظيراتها في القانون البريطاني وقانون حماية البيانات الأوروبي (EU GDPR). فقد ورد تعريف مماثل للبيانات الشخصية وطبيعة معالجتها في كل من "دليل مفوض المعلومات البريطاني" (ICO)، وفي المادة الرابعة من اللائحة الأوروبية العامة لحماية البيانات (GDPR Art. 4).² ولا يقتصر نطاق هذه التشريعات على البيانات المعالجة إلكترونياً أو آلياً، بل يشمل كذلك البيانات المحفوظة يدوياً أو المؤرشفة، مما يؤكد اتساقاً تشريعياً واسعاً بين الأنظمة الثلاثة.

¹: سياسات حوكمة البيانات الوطنية، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

²: (ICO)، المادة 4؛ دليل مفوض المعلومات البريطاني (GDPR) اللائحة العامة لحماية البيانات.

أما "أصحاب البيانات الشخصية"، فقد حددتهم السياسات الوطنية بأنهم الأشخاص الطبيعيون الذين تتصل بهم البيانات ويمكن التعرف عليهم من خلالها، ويمتد الوصف ليشمل ممثليهم القانونيين ومن لهم الولاية عليهم. ويُستخلص من ذلك أن الحماية القانونية تنصرف فقط إلى الأشخاص الأحياء، ولا تشمل المتوفين، وهو ما يتوافق مع ما نص عليه كل من التشريع البريطاني واللائحة الأوروبية عند تعريفهم لصاحب البيانات بأنه Living Individual.

وفي هذا المطلب، سنركز على النشأة والتطور لهذا النظام، ثم على المبادئ الأساسية التي يقوم عليها.

الفرع الأول: النشأة والتطور

شهدت المملكة العربية السعودية خلال السنوات الأخيرة تحولاً نوعياً في مجال التنظيمات المرتبطة بالبيانات الشخصية، نتيجة التوسع الهائل في استخدام التقنيات الرقمية، وتزايد الحاجة إلى إطار قانوني يواكب حجم المعالجة المتنامية للبيانات في مختلف القطاعات. ومع هذا التطور المتسارع، برزت الحاجة إلى نظام متكامل يضمن حماية فعالة لبيانات الأفراد، ويحقق التوازن بين متطلبات التطوير التقني وضرورات الأمن المعلوماتي. بدأت الاهتمامات التشريعية بحماية البيانات الشخصية في المملكة كجزء من الجهود الوطنية لمواكبة التطورات الرقمية العالمية، وكانت مرتبطة ارتباطاً وثيقاً برؤية المملكة ٢٠٣٠، التي تهدف إلى بناء اقتصاد رقمي قوي يعتمد على الثقة والأمان.

قبل صدور النظام الشامل في عام ٢٠٢١، كانت التشريعات المتعلقة بحماية البيانات مبعثرة وجزئية، تركز على جوانب محددة مثل مكافحة الجرائم الإلكترونية أو تنظيم القطاعات الخاصة مثل التمويل والصحة.

على سبيل المثال، صدر نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم (م/١٧) بتاريخ ٨ ربيع الأول ١٤٢٨ هـ (٢٦ مارس ٢٠٠٧ م)، والذي كان يُعد أول إطار قانوني يتناول الانتهاكات المتعلقة بالبيانات الشخصية في سياق الجرائم الإلكترونية، مثل الوصول غير المصرح به إلى الأنظمة أو سرقة المعلومات^٣ هذا النظام، رغم أهميته، لم يكن شاملاً، إذ ركز على العقوبات الجنائية دون تنظيم المعالجة اليومية للبيانات أو حقوق الأفراد. مع تطور التحول الرقمي في المملكة، خاصة بعد إطلاق برنامج التحول الوطني في عام ٢٠١٦، أصبحت الحاجة ماسة إلى إطار تشريعي متكامل.

بدأت النواة الأولى للنظام مع صدور الأمر السامي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩ هـ، الذي أقر نظام حماية البيانات الشخصية باعتباره المرجع النظامي الملزم لجميع جهات التحكم والمعالجة في القطاعين العام والخاص، بما يشمل الأفراد الذين يتعاملون مع البيانات بصورة مهنية. وقد أسند الأمر السامي إلى مركز المعلومات الوطني مهمة الإشراف على تنفيذ النظام، بصفته الجهة المختصة بضبط الامتثال ومتابعة تطبيق السياسات التنظيمية^٤. هذا الإطار الأولي كان يمثل خطوة جوهريّة نحو

نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧) بتاريخ ٨ ربيع الأول ١٤٢٨ هـ: ٣

نظام حماية البيانات الشخصية، المرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩ هـ: ٤

إرساء ثقافة تنظيمية جديدة، تقوم على تحديد أغراض جمع البيانات، وضبط معالجتها، وإرساء مبدأ الشفافية في التعامل مع أصحاب البيانات، بما يحقق حماية فعالة وواقعية في ظل تزايد المخاطر الرقمية والجرائم الإلكترونية.

كان هذا الأمر استجابة مباشرة لزيادة الخدمات الإلكترونية، مثل منصة "أبشر" و"نفاذ"، التي تعتمد على جمع بيانات هائلة من المستخدمين. ومع ذلك، بقيت هذه التشريعات محدودة النطاق، ولم تشمل الجهات الخاصة أو النقل الدولي للبيانات. شهد عام ٢٠٢٠ تطوراً هاماً مع إجراء تعديلات تشريعية تعزز الحماية، خاصة في ظل جائحة كوفيد-١٩ التي زادت من الاعتماد على التقنيات الرقمية لتتبع الصحة العامة وتقديم الخدمات عن بعد. أدخلت هذه التعديلات إجراءات جديدة لتقييم مخاطر تسرب البيانات في القطاع الصحي، وألزمت الجهات الحكومية بإنشاء سياسات داخلية لخصوصية البيانات.

كما أنشئت الهيئة الوطنية للأمن السيبراني (سابقاً)، والتي ساهمت في وضع معايير أمنية أولية لحماية البيانات من الهجمات الإلكترونية. هذه الخطوات كانت تمهيداً للإطار الشامل، حيث أكدت على ضرورة توحيد الجهود بين الجهات الحكومية والخاصة. اللحظة الحاسمة جاءت مع صدور نظام حماية البيانات الشخصية بالمرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩ هـ الموافق ١٦ سبتمبر ٢٠٢١ م، ونُشر في الجريدة الرسمية بتاريخ ٢٤ سبتمبر ٢٠٢١ م. كما ذكرنا سابقاً، يُعد ذلك أول تشريع شامل في تاريخ المملكة ينظم جميع جوانب معالجة البيانات الشخصية، مستوحى جزئياً من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي مع مراعاة السياق الثقافي والاقتصادي السعودي. أهداف النظام الرئيسية تشمل حماية خصوصية الأفراد، وضع ضوابط للمعالجة، وتعزيز الثقة في التعاملات الإلكترونية، مع التركيز على الحد من الممارسات السلبية مثل التمييز الآلي أو تسرب البيانات. لم يتوقف التطور عند الإصدار، إذ منح النظام فترة انتقالية مدتها عام واحد، انتهت في ١٤ سبتمبر ٢٠٢٣ م، خلالها ركزت على التوعية والتدريب للجهات المعنية. في عام ٢٠٢٢، أُطلق الإطار التنظيمي الشامل للبيانات الشخصية، يشمل لوائح تنفيذية ودليل امتثال، لتسهيل التطبيق العملي.

وفي هذا السياق، أولى المشرع السعودي اهتماماً خاصاً ببيانات الأطفال ومن في حكمهم، حيث خصّهم بسياسة مستقلة ضمن "سياسات حوكمة البيانات الوطنية"؛ وذلك إدراكاً لخصوصية هذه الفئة وحاجتها إلى حماية مضاعفة نظراً لقلّة وعيها بالمخاطر الرقمية، ولأن بياناتها قد تكون هدفاً سهلاً لعمليات الاستغلال والابتزاز. إدراكاً لطبيعة التحديات التقنية المتغيرة، جاءت مرحلة ثانية أكثر تطوراً تمثلت في تعديل النظام في ١٤٤٤/٩/٥ هـ بموجب المرسوم رقم (م/١٤٨).^٥ وقد هدفت هذه التعديلات إلى سد الثغرات العملية التي ظهرت عند التطبيق الأولي، وتعزيز جوانب الحماية، وتحديدًا فيما يتعلق ببيانات الفئات الأكثر حساسية. وتركز على تسهيل نقل البيانات إلى الخارج بشرط توافر حماية مكافئة، مما يعزز الاندماج الاقتصادي الدولي دون تعريض الخصوصية للخطر. هذه التعديلات جاءت استجابة للتحديات العالمية، مثل الغرامات الكبرى على شركات عالمية بسبب خرق البيانات في ٢٠٢٣، مما دفع المملكة إلى تعزيز آليات الرقابة.

تعديلات نظام حماية البيانات الشخصية، المرسوم الملكي رقم (م/١٤٨) بتاريخ ١٤٤٤/٩/٥ هـ: ٥

من الناحية التاريخية، يمكن تصنيف تطور نظام حماية البيانات الشخصية في المملكة العربية السعودية إلى ثلاث مراحل رئيسية، مع النظر في السياق الدولي الذي أثر في تشكيله:

المرحلة التمهيدية (قبل ١٩٧٠ - ٢٠٠٦) خلال هذه المرحلة، لم يكن هناك تنظيم مستقل أو شامل لحماية البيانات الشخصية في المملكة، حيث كانت الحماية تعتمد على مبادئ عامة مستمدة من الشريعة الإسلامية والأنظمة الأساسية، مثل:

- حماية الحياة الخاصة وحرمة المراسلات.

- سرية السجلات الطبية.

- القواعد العامة لمنع التعسف وسوء استعمال السلطة.

أما على الصعيد الدولي، فقد بدأ الاهتمام الفعلي بحماية البيانات مع انتشار الحواسيب في الستينيات، مما دفع عدة دول أوروبية إلى سن تشريعات مبكرة:

- ألمانيا (ولاية هيسن) سنت أول قانون لحماية البيانات في العالم عام ١٩٧٠.^٦

- تبعتها السويد (١٩٧٣)، فرنسا (١٩٧٨)، والدنمارك.

في عام ١٩٨١، صدرت اتفاقية مجلس أوروبا رقم ١٠٨، والتي تعد أول صك دولي ملزم عرّف "البيانات الشخصية" دولياً، وأرسى المبادئ الأساسية مثل مشروعية الغرض، تقليل البيانات، الدقة، محدودية مدة الاحتفاظ، والرقابة الحكومية على المعالجة الآلية.^٧ في المملكة، استمر الوضع خلال هذه الفترة الطويلة دون تشريع متخصص، حتى بدايات الألفية الثالثة مع انتشار الإنترنت والخدمات الإلكترونية الحكومية الأولية، مثل بوابة الخدمات الإلكترونية الحكومية عام ٢٠٠٤. مرحلة الاستجابة الأمنية والانتقالية (٢٠٠٧ - ٢٠٢٠) بدأ الاهتمام التشريعي الفعلي في المملكة مع تزايد التهديدات السيبرانية. كانت الخطوة الأولى الرسمية صدور نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم (م/١٧) وتاريخ ٨ ربيع الأول ١٤٢٨ هـ (٢٦ مارس ٢٠٠٧م)، والذي يُعد أول تشريع يتناول البيانات الرقمية، لكنه ركز فقط على العقوبات الجنائية (غرامات، سجن يصل إلى ٥ سنوات) على الوصول غير المصرح به وسرقة المعلومات، دون تنظيم المعالجة اليومية أو منح الأفراد حقوقاً في الخصوصية.^٨ كان هذا النظام دفاعياً ورد فعل وليس وقائياً، مما ترك ثغرات كبيرة خاصة مع:

- زيادة الهجمات الإلكترونية بنسبة تقارب ٣٠٪ بين ٢٠٠٥ و ٢٠٠٧.

^٦ اتفاقيات مجلس أوروبا، اتفاقية رقم ١٠٨ لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (١٩٨١):

^٧ نفس المرجع أعلاه:

^٨ نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨ هـ:

- تزايد حجم الخدمات الإلكترونية الحكومية.

مع إطلاق رؤية ٢٠٣٠ وبرنامج التحول الوطني عام ٢٠١٦، أصبحت الحاجة إلى إطار شامل أكثر إلحاحاً. خلال هذه الفترة:

- أنشئت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) عام ٢٠١٩. [٤٨]
- انضمت المملكة إلى اتفاقية بودابست بشأن الجرائم الإلكترونية.
- خلال جائحة كوفيد-١٩ (٢٠٢٠) ومع تطبيق "توكلنا"، صدرت إجراءات عاجلة لتقييم مخاطر التسرب في القطاع الصحي وإلزام الجهات الحكومية بسياسات خصوصية داخلية، مع زيادة التعاملات الرقمية بنسبة ١٥٠٪ (تقرير سدايا ٢٠٢١).^٩ يمكن تقسيم هذه المرحلة إلى ثلاثة أطوار فرعية:

- 2016-2007 التركيز على مكافحة الجناية فقط.
- 2018-2016 بناء الإطارات الإدارية وإنشاء الجهات المتخصصة.
- 2020-2019 الاستعداد للشمولية والتكامل مع رؤية ٢٠٣٠.
- مرحلة الحداثة التشريعية والتنفيذ الكامل (٢٠٢١ - حتى الآن) أولاً: إصدار النظام الشامل (٢٠٢١).

جاءت اللحظة الحاسمة بصدور نظام حماية البيانات الشخصية بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩ هـ (١٦ سبتمبر ٢٠٢١م)، ونشر في جريدة أم القرى بتاريخ ٢٤ سبتمبر ٢٠٢١م، وهو أول تشريع شامل ومستقل ينظم جميع جوانب معالجة البيانات الشخصية في القطاعين العام والخاص^{١٠} استند النظام إلى:

- المادة ٧٠ من النظام الأساسي للحكم.
- المادة ٢٠ من نظام مجلس الوزراء.
- المادة ١٨ من نظام مجلس الشورى.
- أسند الإشراف مؤقتاً إلى "سدايا" لمدة سنتين، مع إمكانية نقل الاختصاص لاحقاً إلى مكتب إدارة البيانات الوطنية أهدافه الأساسية (المادة ١):

- حماية خصوصية الأفراد.

^٩ إعلان بدء التنفيذ الكامل، موقع سدايا، ٢٠٢٤: ٩

^{١٠} مسودة تعديلات اللائحة التنفيذية، طرح للاستشارة العامة، أبريل-مايو ٢٠٢٥: ١٠

- وضع ضوابط لمعالجة البيانات.
 - تعزيز الثقة في التعاملات الإلكترونية.
 - الحد من الممارسات السلبية (التمييز الآلي، التسربات...).
- استوحى النظام كثيراً من اللائحة العامة الأوروبية (GDPR) مع تكييف سعودي واضح، أبرزه: توسيع تعريف البيانات الحساسة لتشمل البيانات الدينية والعائلية والوراثية. استثناءات واسعة للمصلحة العامة (الصحة، الأمن الوطني). مُنحت فترة انتقالية ١٨٠ يوماً للنفاز ثم سنة كاملة للامتثال (انتهت في ١٤ سبتمبر ٢٠٢٣ أصلاً ثم مُدّدت). ثانياً: التعديلات الكبرى (٢٠٢٣). في ٢٧ مارس ٢٠٢٣ صدر المرسوم الملكي رقم (م/١٤٨) بتعديل ٢٧ مادة من النظام، أبرزها:
- تأجيل النفاذ الكامل إلى ١٤ سبتمبر ٢٠٢٣ مع سنة سماح جديدة تنتهي ١٤ سبتمبر ٢٠٢٤.
 - تسهيل شروط نقل البيانات للخارج بشرط "حماية مكافئة" بدلاً من الحظر شبه الكامل السابق.
 - إلزام الإبلاغ عن التسرب خلال ٧٢ ساعة.
 - إلغاء بعض الاستثناءات السابقة على النقل الدولي.
- في سبتمبر ٢٠٢٣ صدرت اللائحة التنفيذية النهائية التي حددت:
- تعريف "الإخلال بالخصوصية".
 - إجراءات الشكاوى. وبوابة التسجيل الإلكتروني ورسوم التسجيل (تصل إلى ١٠٠,٠٠٠ ريال سنوياً لبعض الفئات).
 - ثالثاً: التطورات في ٢٠٢٤ و ٢٠٢٥. في ١ سبتمبر ٢٠٢٤:
 - صدور لوائح نقل البيانات الدولية المحدثة، واعتماد عقود قياسية، وإنشاء لجنة عليا للنظر في المخالفات
- في ١٤ سبتمبر ٢٠٢٤: انتهاء فترة السماح وبدء التنفيذ الكامل مع غرامات تصل إلى ٥ ملايين ريال (تتضاعف عند التكرار).
- ١+ lexology.com في أبريل-مايو ٢٠٢٥: طرح تعديلات مقترحة على اللائحة التنفيذية للاستشارة العامة، شملت:
- تبسيط لغة الإخطارات.
 - إلغاء الحد الزمني ٩٠ يوماً لتقديم الشكاوى.
 - حذف تعريف "التسويق المباشر" لتوسيع نطاق التطبيق.

- إضافة مصطلح "منصة الجهة المختصة" للتسجيل الإلكتروني.^{١١}

هذه التطورات المستمرة جعلت النظام السعودي من أكثر الأنظمة شمولية وتكيفاً في المنطقة، مع الحفاظ على توازن دقيق بين متطلبات التحول الرقمي في رؤية ٢٠٣٠ وحماية الخصوصية وفق السياق الثقافي والديني المحلي

الفرع الثاني

المبادئ الأساسية

أولاً: مبادئ حماية البيانات الشخصية في النظام السعودي

تشكل المبادئ الأساسية لنظام حماية البيانات الشخصية في المملكة العربية السعودية (الصادر بالمرسوم الملكي رقم م/١٩ بتاريخ ١٤٤٣/٢/٩هـ، والمعدل بالمرسوم م/١٤٨ لعام ١٤٤٤هـ، مع لائحته التنفيذية من الهيئة السعودية للبيانات والذكاء الاصطناعي "سداء") الركيزة النظرية والعملية للنظام. تهدف إلى تحقيق توازن بين حقوق الخصوصية للأفراد ومتطلبات المعالجة في الاقتصاد الرقمي ورؤية ٢٠٣٠.

رغم عدم تعددها صراحة في النظام، يمكن استنباطها من المواد النظامية ومقاصدها، مما يساعد الجهات على تحديد التزاماتها وإثبات الامتثال.

– **مبدأ المشروعية والإنصاف والشفافية:** يُشترط أن تكون معالجة البيانات الشخصية مبنية على أساس قانوني مشروع (مثل الموافقة الصريحة الحرة والمستنيرة القابلة للسحب، أو تنفيذ عقد، أو مصلحة عامة)، مع ضمان العدالة وعدم التمييز (خاصة في القرارات الآلية وفق المادة ٢١). كما يفرض الشفافية بإبلاغ صاحب البيانات بالغرض، الهوية، المدة، والضوابط (المادة ٤ من النظام، والمادة ٤ من اللائحة التي تحدد الإبلاغ خلال ٣٠ يوماً عبر سياسات خصوصية واضحة). عملياً، يظهر ذلك في تطبيقات مثل "توكلنا" (استثناءات للمصلحة العامة في البيانات الصحية) و"أبشر" (عرض سياسة خصوصية قبل الجمع)، وفي القطاع المالي بتقييم مخاطر التمييز في خوارزميات الائتمان. يعزز هذا المبدأ الثقة والمساءلة، مع حساسية خاصة للبيانات الحساسة (وراثية، دينية)

٢ – **مبدأ تحديد الغرض (تقييد الغرض)** يلزم هذا المبدأ بتحديد غرض مشروع واضح مسبقاً قبل الجمع، ويمنع تغييره أو إعادة الاستخدام دون موافقة جديدة أو تسجيل التغييرات (المادة ٦ من النظام، والمادة ١٩ من اللائحة). يُعتبر تحديد الغرض شرطاً جوهرياً لسلامة المعالجة، مما يحد من الاستغلال في القطاع التجاري (مثل منع استخدام بيانات العملاء لتسويق غير مرتبط) أو البحوث الصحية.

في عصر الذكاء الاصطناعي، يتطلب تقييمات مستمرة لتجنب تغيير الغرض تلقائياً، مما يعزز الضوابط والامتثال.

٤- **مبدأ الدقة:** يُعد ضمان دقة البيانات من الالتزامات الأساسية للجهات التي تعالج البيانات. يجب عليها اتخاذ إجراءات فعّالة للتحقق من صحة المعلومات، والعمل على تحديثها بصورة دورية بحيث تظل معبرة عن الواقع، فضلاً عن تمكين صاحب البيانات من تصحيح ما قد يعتري بياناته من أخطاء. المادة ٤ (الفقرة ٣) تمنح الحق في التصحيح، واللائحة (المادة ٧) تُلزم بإشعار الجهات الأخرى بعد التصحيح. في أنظمة الائتمان، يحمي هذا المبدأ من الأخطاء التي قد تؤثر على قرارات مالية حاسمة

٥- **مبدأ تقييد التخزين** يفرض هذا المبدأ على الجهة عدم الاحتفاظ بالبيانات لمدة أطول من اللازم؛ إذ يتعين إتلاف البيانات فور انتهاء الغرض المشروع الذي جُمعت من أجله. المادة ١٩ تُلزم بإتلافها بعد الانتهاء، واللائحة تطلب الاحتفاظ بسجلات ٥ سنوات كحد أقصى في بعض الحالات. في القطاع الحكومي، يقلل ذلك التكاليف الأمنية. أما التحدي فيمكن في التخزين السحابي، حيث قد يستمر التخزين تلقائياً دون إشراف كافٍ.

يهدف هذا القيد إلى منع تراكم البيانات دون حاجة، وحمايتها من احتمالات الوصول غير المشروع أو استخدامها في أغراض جديدة لم يُوافق عليها صاحب البيانات

٦- **مبدأ النزاهة والسرية:** يستلزم هذا المبدأ وضع منظومة شاملة من الإجراءات الفنية والتنظيمية لحماية البيانات من الفقد، أو التلف، أو التغيير غير المرخص به، أو الاطلاع غير المشروع. المادة ٢١ تطلب تعيين مسؤول حماية البيانات في حالات معينة، واللائحة (المادة ٢٣) تُلزم بإشعار التسرب في ٧٢ ساعة. المادة ٣٧ تحدد عقوبات تصل إلى ٥ ملايين ريال. يمتد الالتزام ليشمل التدريب، ووضع السياسات الداخلية، وتطبيق أفضل الممارسات الأمنية لضمان الحفاظ على سرية البيانات وسلامتها

٧- **مبدأ المسؤولية والمساءلة:** يُعد هذا المبدأ من الركائز الحديثة في تنظيم حماية البيانات، ويعني أن الجهة مسؤولة عن إثبات التزامها بجميع المتطلبات النظامية. يشمل ذلك إعداد السجلات والسياسات، وتوثيق إجراءات المعالجة، وإجراء تقييمات المخاطر، وإثبات أنها تتصرف وفق مقتضيات النظام ولائحته التنفيذية. المادة ٣٧ تحدد عقوبات تصل إلى ٥ ملايين ريال، وتشرف "سدايا" عبر بوابة إلكترونية. تشكل هذه المبادئ إطاراً متكاملًا يدعم التحول الرقمي، مع الحاجة إلى تحديثات مستمرة لمواكبة التطورات التقنية.

يري الباحث في مجال حماية البيانات الشخصية، يري أن هذه المبادئ تمثل نقلة نوعية في الإطار التنظيمي السعودي، حيث تتوافق مع المعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR)، مع مراعاة الخصوصيات الثقافية والاجتماعية المحلية. ومع ذلك، في سياق عام ٢٠٢٥، يبرز تحدي كبير في تنفيذها مع انتشار تقنيات الذكاء الاصطناعي، حيث قد يؤدي التعلم الآلي إلى توسيع نطاق الغرض أو زيادة مخاطر التسرب دون إشراف كافٍ، مما يتطلب تعزيز الدليل الإرشادي لتقييم المخاطر وتدريب الجهات. كما أن إطلاق النسخة الثانية من برنامج البيئة التنظيمية التجريبية ٢٠٢٥ من قبل "سدايا"، مع

التركيز على مبدأ "الخصوصية في التصميم" (Privacy by Design)، يعد خطوة إيجابية نحو دمج الخصوصية في المنتجات الرقمية للمنشآت الصغيرة والناشئة، مما يعزز الثقة الرقمية ويدعم رؤية ٢٠٣٠، لكن يجب مراقبة فعاليته لتجنب الفجوات في التطبيق العملي.

ثانياً: حقوق أصحاب البيانات الشخصية وفق النظام السعودي: يهدف النظام إلى تعزيز سيطرة الأفراد على بياناتهم، من خلال منحهم مجموعة من الحقوق النظامية التي تكفل لهم إدارة بياناتهم ومراجعتها والاعتراض على معالجتها. وتجدر الإشارة إلى أن هذه الحقوق ليست مطلقة، وإنما تخضع لضوابط واستثناءات يحددها النظام بصورة دقيقة:

١- الحق في العلم: يقوم هذا الحق على تمكين صاحب البيانات من الإحاطة مسبقاً بالمسوغ النظامي للمعالجة، والغرض منها، وطبيعة البيانات التي سيتم جمعها، والجهة المسؤولة عن المعالجة. ويساهم هذا الحق في دعم الشفافية وتمكين صاحب البيانات من اتخاذ قرار واعٍ بشأن قبول المعالجة من عدمه.

٢- الحق في الوصول إلى البيانات: يُعد هذا الحق أداة أساسية تمكن الفرد من التحقق من مشروعية المعالجة وسلامة البيانات، وفقاً لأحكام النظام ولائحته التنفيذية.

٣- الحق في الحصول على نسخة من البيانات: يحق لصاحب البيانات الحصول على نسخة من بياناته بصيغة واضحة ومقروءة، مما يساعده على الاحتفاظ بسجل شخصي لمعلوماته، أو تقديمها لجهات أخرى عند الحاجة.

٤- الحق في طلب التصحيح أو الإكمال أو التحديث: يتيح النظام لصاحب البيانات طلب تصحيح البيانات الخاطئة، أو إكمال البيانات الناقصة، أو تحديث ما لم يعد موكباً للواقع. ويُعد هذا الحق مكتملاً لمبدأ الدقة، ويضمن بقاء البيانات صحيحة وقابلة للاعتماد عليها.

٥- الحق في طلب الإزالة: يجوز لصاحب البيانات أن يطلب حذف بياناته بصورة نهائية متى لم يعد هناك مسوغ نظامي أو غرض مشروع للاحتفاظ بها. ويمثل هذا الحق ضماناً لحماية الخصوصية ومنع استبقاء المعلومات دون سبب

٦- الحق في العدول عن الموافقة: يجوز لصاحب البيانات الرجوع عن موافقته على معالجة بياناته في أي وقت، شريطة ألا يؤثر العدول على مشروعية المعالجة التي تمت قبل سحب الموافقة. ويؤكد هذا الحق على إرادة صاحب البيانات باعتبارها أحد أساسات مشروعية المعالجة.

المطلب الثاني: اللائحة الأوروبية العامة لحماية البيانات

الفرع الأول: النشأة والتطور

أولاً: نشأة حماية البيانات على مستوى الاتحاد الأوروبي

بدأ الاهتمام الأوروبي بحماية البيانات داخل مؤسسات الاتحاد بشكل متأخر نسبياً مقارنة بالدول الأعضاء. فعلى الرغم من صدور التوجيه الأوروبي ٩٥/٤٦/EC في منتصف التسعينيات، والذي شكل الإطار التشريعي الرئيسي لمعالجة البيانات الشخصية في الاتحاد الأوروبي، إلا أن نطاق هذا التوجيه كان موجهاً نحو الدول الأعضاء فقط، ولم يمتد ليشمل مؤسسات الاتحاد ذاتها.^{١٢} كان السبب الرئيسي لهذا التأخير يعود إلى غياب أساس قانوني واضح يتيح فرض قواعد ملزمة على مؤسسات الاتحاد الأوروبي، أو إنشاء جهة رقابية مستقلة تراقب التزام هذه المؤسسات.

ومع تزايد الوعي بأهمية توحيد القواعد لحماية البيانات داخل الاتحاد، بدأت المفوضية الأوروبية في التفكير مبكراً في ضرورة خضوع مؤسسات الاتحاد للمعايير نفسها التي تُفرض على الدول الأعضاء. إلا أن هذا التوجه اصطدم بعقبة قانونية أساسية تمثلت في عدم وجود نص في المعاهدات يسمح بذلك. استمر الوضع على هذا النحو حتى جاءت معاهدة أمستردام عام ١٩٩٧، التي مثلت نقطة تحول جوهرية، إذ أضيفت بموجبها المادة ٢٨٦ من معاهدة الجماعة الأوروبية، مما وفر لأول مرة إطاراً قانونياً يتيح تطبيق تشريعات حماية البيانات على مؤسسات الاتحاد.^{١٣} نصت المادة على أمرين أساسيين:

- بدء تطبيق قواعد حماية البيانات على مؤسسات الاتحاد اعتباراً من ١ يناير ١٩٩٩.
- إلزام المجلس الأوروبي بإنشاء هيئة رقابية مستقلة تتولى متابعة تنفيذ هذه القواعد داخل مؤسسات الاتحاد.

وبذلك، أصبحت هذه المادة الأساس القانوني الأول لنشأة منظومة حماية البيانات داخل أجهزة الاتحاد الأوروبي. رغم صدور النص، لم يتم الالتزام بالموعد المحدد، وتأخر التنفيذ نحو عامين. وفي ديسمبر ٢٠٠٠، صدرت اللائحة رقم ٤٥/٢٠٠١، التي تعتبر التطبيق المؤسسي للقواعد المنصوص عليها في التوجيه ٩٥/٤٦/EC داخل مؤسسات الاتحاد وهيئاته^{١٤} احتفظت اللائحة بنفس المبادئ الأساسية للتوجيه، لكنها أضافت عنصرين مهمين شكلاً مرحلة تأسيسية بارزة:

¹²: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

¹³ : Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed on 2 October 1997.

¹⁴ : Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

- إلزام كل مؤسسة بتعيين مسؤول حماية البيانات (DPO) يتولى الإشراف الداخلي على الامتثال.
- التأكيد الصريح على الاستقلال الكامل للسلطة الرقابية التي سيتم إنشاؤها، بحيث لا تتلقى تعليمات من أي جهة.
- كان هذا الأساس القانوني نقطة الانطلاق الحقيقية التي مهدت لإنشاء جهاز المشرف الأوروبي على حماية البيانات (EDPS) لاحقًا.

ثانيًا: تطور حماية البيانات داخل مؤسسات الاتحاد الأوروبي (١٩٩٧-٢٠٠٤)

رغم دخول لائحة ٢٠٠١/٤٥ حيز التنفيذ عام ٢٠٠١، إلا أن التطبيق الفعلي لقواعد حماية البيانات داخل مؤسسات الاتحاد واجه بطنًا ملحوظًا. استغرق الأمر نحو عام ونصف قبل إصدار قرار مشترك بين البرلمان والمجلس والمفوضية ينظم تعيين المشرف الأوروبي على حماية البيانات ويحدد شروط عمله. كما استغرق الاتحاد فترة مماثلة أخرى لإصدار قراره النهائي بتعيين أول مشرف أوروبي ومساعدته في يناير ٢٠٠٤، أي بعد ثلاث سنوات كاملة من دخول اللائحة حيز التنفيذ، وكانت تلك الفترة خالية تمامًا من أي رقابة مستقلة على مؤسسات الاتحاد.^{١٥} مع مباشرة المشرف الأوروبي مهامه، بدأت مرحلة البناء الفعلية. واجه الجهاز الجديد تحديات تنظيمية وإدارية كبيرة، من أبرزها:

- عدم اعتماد الميزانية الخاصة به قبل تعيينه.
 - عدم توفر مقر عمل جاهز.
 - عدم وجود جهاز إداري أو هيكل تنظيمي.
 - الحاجة إلى تعيين الموظفين وإنشاء الأمانة الفنية من الصفر.
- ومع ذلك، تمكن الجهاز خلال عامه الأول من وضع الأسس المؤسسية الرئيسية، منها:
- وضع رؤية ومهمة واضحة ارتكزت على ثلاثة أدوار أساسية: الإشراف والرقابة، والمشورة (consultation)، والتعاون (cooperation).
 - وضع أهداف سنوية لقياس الأداء، مما عزز علاقته بالجهات المانحة للميزانية.
 - التأكيد على أن حماية البيانات ليست عائقًا إداريًا، بل شرط أساسي لنجاح سياسات الاتحاد الأوروبي.
- كما اتضح للجهاز الجديد أن مؤسسات الاتحاد تواجه تحديًا مزدوجًا: تطبيق لائحة حماية البيانات، وفي الوقت نفسه تطبيق لائحة الوصول إلى الوثائق العامة، التي كانت تُنظر إليها كنقيض طبيعي لحماية البيانات. ولمعالجة هذا التضارب، أعد

¹⁵ : Establishment of the European Data Protection Supervisor (EDPS) in 2004, with the first Supervisor

المشرف الأوروبي ورقة خلفية تفصيلية توضح كيفية التوفيق بين الحق في الخصوصية والحق في الوصول إلى المعلومات، وأثمر هذا الجهد في بناء علاقة تعاون إيجابية مع أمين المظالم الأوروبي.

وبنهاية الفترة التأسيسية (٢٠٠٤-٢٠٠٥)، أصبح جهاز المشرف الأوروبي هيئة مستقلة فعالة، مستعدة للقيام بدورها المركزي في منظومة حماية البيانات داخل الاتحاد الأوروبي.

كما أن حماية البيانات في الاتحاد الأوروبي لم تبدأ كموضوع دستوري، بل كانت في البداية جزءًا محدودًا ضمن إطار التشريعات المتعلقة بالسوق الداخلية. في البداية، كان هناك التوجيه رقم ٩٥/٤٦/EC الذي تناول حماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية وحركة هذه البيانات داخل الاتحاد الأوروبي. على الرغم من وجود هذا التوجيه، كان فهم حماية البيانات باعتبارها حقًا أساسيًا محدودًا جدًا، ولم يتم التعامل معه بعد على أنه جزء من الحقوق الدستورية الأساسية للأفراد. مع ظهور معاهدة الدستور الأوروبي في عام ٢٠٠٤، بدأت حماية البيانات تأخذ مكانة أكثر أهمية. خصصت المادة ٥٠ من المعاهدة حماية البيانات كحق أساسي، لكنها لم تصبح نافذة مباشرة بعد رفض المعاهدة في الاستفتاءات الفرنسية والهولندية. ومع ذلك، نقلت معاهدة لشبونة، التي دخلت حيز التنفيذ في ديسمبر ٢٠٠٩، معظم أحكام المعاهدة الدستورية، وحولت المادة ٥٠ إلى المادة ١٦ من معاهدة عمل الاتحاد الأوروبي، وجعلت ميثاق الحقوق الأساسية للاتحاد الأوروبي أداة ملزمة قانونيًا تحتوي على المادة ٨ التي تعترف بحق الأفراد في حماية بياناتهم الشخصية.^{١٦} في العقد الأخير، أثبتت محكمة العدل الأوروبية أهمية حماية البيانات من خلال عدد من القضايا الجوهرية، مثل:

- **قضية Google و Google Spain**: حيث اعترفت المحكمة بحق الأفراد في طلب إزالة الروابط المتعلقة بأسمائهم من محركات البحث، وهو ما أصبح يُعرف لاحقًا بحق النسيان.^{١٧}
- **قضية Digital Rights Ireland**: حيث أعلنت المحكمة أن الاحتفاظ غير المحدود ببيانات الاتصالات للمواطنين يعد انتهاكًا جسيمًا للحقوق الأساسية.
- **قضية Schrems**: حيث تم إبطال قرار لجنة الاتحاد الأوروبي المعروف باسم Safe Harbour بسبب عدم توافقه مع حماية الحقوق الأساسية للأفراد عند نقل البيانات إلى الولايات المتحدة.

على المستوى المؤسسي، تم إنشاء السلطات المستقلة لحماية البيانات في كل دولة عضو، لتكون مسؤولة عن مراقبة تطبيق القانون وحماية الحقوق الفردية. هذه السلطات تعمل ضمن نموذج تعاوني بين المستويات الوطنية والأوروبية، حيث يتم التنسيق

¹⁶]: Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed on 13 December 2007; Charter of Fundamental Rights of the European Union, Article 8.

¹⁷]: Court of Justice of the European Union (CJEU) judgment in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014.

بين السلطات الوطنية عبر المجلس الأوروبي لحماية البيانات (EDPB) لضمان تطبيق متسق وفعال للقواعد عبر الاتحاد.¹⁸ النموذج الحالي لتنفيذ حماية البيانات يدمج بين الرقابة الوطنية والأوروبية، ويُعتبر نموذجًا لا مركزيًا مع عناصر مركزية، حيث تظل السلطات الوطنية مسؤولة عن تطبيق القانون، لكنها تعمل وفق تنسيق مشترك لضمان حماية الحقوق على مستوى الاتحاد.

هذا التطور يوضح أن حماية البيانات انتقلت من كونها موضوعًا متخصصًا وثانويًا إلى حق أساسي له وزن دستوري مهم في القانون الأوروبي. النموذج الأوروبي الحالي لحماية البيانات يمزج بين الرقابة الوطنية المستقلة والآليات المركزية، بحيث تكون السلطات الوطنية مسؤولة عن التطبيق المباشر للقانون، في حين يضمن التنسيق الأوروبي حماية الحقوق على نطاق أوسع. هذا التطور يعكس تحول حماية البيانات من مجرد تنظيم تقني إلى حق أساسي ذو وزن دستوري، له تأثير واضح على القوانين والسياسات الأوروبية.

الفرع الثاني: المبادئ الأساسية

تشكل المبادئ الأساسية في اللائحة العامة لحماية البيانات (GDPR، ٢٠١٦/٦٧٩) الإطار القانوني لمعالجة البيانات الشخصية، مستمدة من المادة ٥، وتهدف إلى ضمان الخصوصية، الشفافية، والسيطرة الفردية في البيئة الرقمية. هذه المبادئ متكاملة، وانتهاكها يؤدي إلى مسؤولية مباشرة، مع غرامات تجاوزت ٥.٨٨ مليار يورو حتى يناير ٢٠٢٥.

١- مبدأ المشروعية والإنصاف والشفافية (Lawfulness, Fairness and Transparency)

تُجمع البيانات وتُعالج بطريقة مشروعة، عادلة، وشفافة (المادة ٥(١)(a)). يتطلب أساس قانوني (مثل الموافقة الصريحة أو المصلحة المشروعة)، مع إفصاح واضح قبل الجمع أو خلال فترة معقولة.

تاريخيًا، مستمد من مبادئ OECD 1980، تطور في GDPR ليشمل العدالة ضد التمييز الآلي (قضية Schrems 2015). عمليًا، ألزمت غرامات شركات مثل Meta (١.٢ مليار يورو، ٢٠٢٣) بتقديم خيارات موافقة واضحة.

عقوبه محتملة	تطبيق المبدأ	مثال	القطاع
50 مليون يورو (2019)	موافقة للتتبع	Google Ads	التسويق
100 مليون يورو (Barclays 2022)	مصلحة مشروعة مع شفافية	بنوك	المالي

¹⁸]: European Data Protection Board (EDPB), established under Regulation (EU) 2016/679 (GDPR).

225 مليون يورو (WhatsApp 2021)	موافقة صريحة	تطبيقات طبية	الصحي
-----------------------------------	--------------	--------------	-------

٢- مبدأ تحديد الغرض (Purpose Limitation) تُجمع البيانات لأغراض محددة وصريحة ومشروعة، ولا تُعالج بعد ذلك بطريقة تتعارض مع تلك الأغراض (المادة ٥. (b)(1) لا يجوز إعادة استخدام البيانات لغرض جديد إلا إذا كان متوافقاً (اختبار التوافق، المادة ٦(4)). مستمد من اتفاقية ١٠٨، يمنع "التوسع الغرضي". مثال: غرامة Meta 405 مليون يورو (٢٠٢٢) لاستخدام بيانات الأطفال في Instagram لأغراض إعلانية دون توافق.

تشير الإحصاءات إلى أن حوالي ٤٠٪ من الغرامات مرتبطة بهذا المبدأ. 3-

3- مبدأ الحد الأدنى من البيانات (Data Minimization) تكون البيانات مناسبة وذات صلة ومحدودة بما هو ضروري فيما يتعلق بالأغراض (المادة ٥) أقوى تطبيق في الذكاء الاصطناعي: رأي EDPB 28/2024 يمنع تدريب نماذج AI على بيانات زائدة .

مثال: غرامات Clearview AI (٢٠ مليون يورو، ٢٠٢٢-٢٠٢٣) لكشط مليارات الصور .

4- مبدأ الدقة (Accuracy) تكون البيانات دقيقة ومحدثة عند الاقتضاء؛ وتُتخذ كل التدابير المعقولة لمحو أو تصحيح البيانات غير الدقيقة بدون تأخير (المادة ٥. (d)(1) يرتبط بحق التصحيح (المادة ١٦)). مثال: غرامة British Airways (٢٠ مليون جنيه إسترليني، ٢٠١٩) لعدم تحديث بيانات بعد اختراق .

5- مبدأ تقييد التخزين (Storage Limitation) لا تُحتفظ بالبيانات بشكل يسمح بتحديد هوية أصحابها لمدة أطول مما هو ضروري (المادة ٥. (e)(1) يُسمح لأغراض بحثية مع إخفاء الهوية (المادة ٨٩)). تطبيق عملي Google: اضطرت لحذف بيانات Location History القديمة تلقائياً بعد ٣ أشهر اعتباراً من ٢٠٢٤، بناءً على تسويات .

٦- مبدأ النزاهة والسرية (Integrity and Confidentiality) تُعالج بطريقة تضمن الأمان المناسب، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية ومن فقدان العرضي باستخدام تدابير تقنية وتنظيمية مناسبة (المادة ٥. (f)(1) يرتبط بالمادة ٣٢ (الأمن) والمادة ٣٣-٣٤ (الإبلاغ عن الاختراق). أكبر غرامة حتى ٢٠٢٥ Meta Ireland : 1.2 مليار يورو (٢٠٢٣)، مع غرامات أمنية إضافية-7.

7- مبدأ المساءلة (Accountability) يتحمل المتحكم مسؤولية الامتثال للفقرة ١ ويكون قادراً على إثبات ذلك (المادة ٥(2)). أدوات: سجل أنشطة المعالجة (المادة ٣٠)، تعيين DPO (المادة ٣٧)، (DPIA المادة ٣٥)، Privacy by Design (المادة ٢٥). أكبر الغرامات في ٢٠٢٤-٢٠٢٥ بسبب عدم إثبات المساءلة. تشكل هذه المبادئ نظاماً متكاملًا، مع

تطور مستمر عبر AI Act (٢٠٢٤) و Digital Services Act، لمواجهة التحديات التقنية وضمان التوازن بين الحماية والابتكار. أكبر غرامة في ٢٠٢٥: TikTok 530 مليون يورو لنقل بيانات إلى الصين.

المبحث الثاني

الدراسة المقارنة بين النظام السعودي واللائحة الأوروبية لحماية البيانات (GDPR)

المطلب الأول

أوجه التشابه

تشكل أوجه التشابه بين النظام السعودي لحماية البيانات الشخصية واللائحة الأوروبية لحماية البيانات (EU GDPR) محوراً أساسياً في فهم كيفية تكامل الإطارات التشريعية الدولية في مجال الخصوصية الرقمية. من خلال تحليل مفصل للسياسات المعنية، يتضح وجود تطابق واسع في العديد من الجوانب الجوهرية بين سياسة حوكمة البيانات الوطنية في المملكة العربية السعودية (الصادرة عام ٢٠٢١) واللائحة الأوروبية لحماية البيانات الشخصية (EU GDPR)، مما يعكس توافقاً في الرؤية نحو تعزيز الخصوصية والاستخدام الآمن للبيانات. يمتد هذا التوافق إلى التعريفات، والمبادئ، والحقوق، وآليات المعالجة، والإجراءات التنفيذية، مع التركيز الرئيسي على ضمان المعالجة العادلة والشفافة.

١. التعريفات الأساسية والنطاق التطبيقي

يتفق النظامان على تعريف البيانات الشخصية بطريقة شاملة ومتطابقة إلى حد كبير، حيث يُعرفها النظام السعودي على أنها أي بيان، مهما كان مصدره أو شكله، يؤدي إلى التعرف على الفرد مباشرة أو غير مباشرة، بما في ذلك الاسم، وأرقام الهويات، والعناوين، وأرقام التواصل، والحسابات البنكية، والبطاقات الائتمانية، والصور الثابتة أو المتحركة، وغيرها من البيانات ذات الطابع الشخصي.^(١٩) هذا التعريف يتوافق تماماً مع ما ورد في المادة ٤ من EU GDPR، التي تُعرف البيانات الشخصية بنفس الطريقة، مشملة أي معلومات تتعلق بشخص طبيعي يمكن التعرف عليه، سواء بشكل مباشر أو من خلال دمجها مع بيانات أخرى.^(٢٠) هذا التوافق يعزز فكرة أن البيانات الشخصية ليست مقتصرة على السياق الرقمي، بل تشمل أيضاً البيانات المحفوظة يدوياً أو المؤرشفة، كما أكد النظام السعودي (سياسات حوكمة البيانات الوطنية، ٢٠٢١) والمادة ٤ من

¹⁹: سياسات حوكمة البيانات الوطنية، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، ٢٠٢١: ٢٠٢١.

²⁰: General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Article 4.

EU GDPR التي تذكر نظام الأرشفة كجزء من النطاق. بالتالي، يشمل النطاق في كلا النظامين البيانات المعالجة إلكترونياً أو يدوياً، مما يوسع الحماية لتشمل العالم الافتراضي والواقعي، ويستثني الأشخاص المتوفين، حيث يركز كلاهما على "الأشخاص الطبيعيين" أو "Living Individual" كما في EU GDPR (المادة ٤). كما يتطابق التعريف للجهات المعالجة، حيث يُقصد بها في النظام السعودي الجهات الحكومية أو غيرها التي تعالج البيانات الشخصية، وقد تعمل بالنيابة عن جهة التحكم في بعض الحالات. هذا يتوافق مع تعريف EU GDPR للمعالج كأى كيان يعالج البيانات نيابة عن المتحكم. أما معالجة البيانات الشخصية، فتُعرف في السعودية بجميع العمليات من جمع، وتحليل، ومشاركة، وتخزين، وحتى الإتلاف، وهو تعريف يتطابق مع ما في EU GDPR الذي يشمل كل عملية تتم على البيانات الشخصية. هذا التوافق يسمح بتوسيع المناقشة في البحث ليشمل كيفية تطبيق هذه التعريفات في سياقات مثل الذكاء الاصطناعي أو البيانات الضخمة، مع أمثلة من قضايا حقيقية.

٢. المبادئ العامة لحماية البيانات الشخصية

يظهر الجدول المقارن في الدراسة تطابقاً كبيراً في المبادئ، حيث يشترك النظامان في الشفافية في جمع ومعالجة البيانات، وضرورة موافقة أصحاب البيانات، والاقتصار على الحد الأدنى من البيانات للغرض الواحد، وحفظ وصيانة البيانات مع منع الوصول غير المخول، ومنع الأطراف الخارجية من الوصول إلا في نطاق ضيق وبموافقة، وضمان تحديث البيانات وجودتها، وتوفير الحماية من التسرب والضياع والسرقة، والمراقبة والامتثال للقوانين مع مراعاة التحديثات. هذه المبادئ مستمدة في السعودية من مكتب إدارة البيانات الوطنية (sdaia.gov.sa)، وفي EU GDPR من GDPR.eu، مما يعكس رؤية مشتركة للاستخدام العادل للبيانات، كما وصفها فلوريدي (٢٠١٣) كمعاملة المعلومات بعدل دون جور أو إساءة.^{٢١} كذلك، يؤكد كلا النظامين على ضرورة إنشاء سياسة خاصة لحماية البيانات لكل منظمة، متوافقة مع السياسة العامة، مع مراعاة أهداف المنظمة (كما في هوفمان وآخرون، ٢٠١٧). [٤٨] في EU GDPR (المادة ٢٥)، يُشدد على دمج الحماية في الممارسات اليومية، وهو ما يتوافق مع دعوة النظام السعودي لإنشاء وحدة حوكمة البيانات لضمان الامتثال والتدريب، مع تعيين موظف مختص للتواصل مع الجهات مثل مركز المعلومات الوطني. هذا يتيح في البحث استكشاف كيفية بناء هذه الوحدات عملياً، مع دراسات حالة عن منظمات سعودية وأوروبية. يتحقق التوازن بين المعالجة الشرعية والحماية من خلال المعالجة العادلة (غالب، ٢٠١٩)، التي تشمل الجمع بعدل (لا أكثر من الحاجة)، وحقوق أصحاب البيانات، والإفصاح العادل، ومراجعة الآثار عند التطوير، وإدارة الحوادث.^{٢٢} هذا التوافق يعزز مفهوم الاستخدام العادل كأساس أخلاقي.

²¹: Floridi, L. (2013). The Ethics of Information. Oxford University Press.

²² : Hofmann, H. et al. (2017). "Data Protection in Organizational Contexts," Journal of Privacy Studies, Vol. 12, pp. 45-67.

٣. الجمع العادل للمعلومات

يصف كلا النظامين الجمع العادل كعملية واضحة، حيث يكون نوع وحجم البيانات متوازنًا مع الغرض المحدد والشرعي. في EU GDPR، يُؤكد على التناسب والحد الأدنى، كما في النظام السعودي الذي يحث على عدم الذهاب إلى العالم الافتراضي لجمع بيانات إضافية دون مبرر، مع التواصل مع أصحاب البيانات إذا لزم الأمر. مثال: لا يجوز لمكتبة أكاديمية طلب بيانات حساسة لتصاريح الدخول، بل الاكتفاء بالرقم الجامعي. هذا يفتح بابًا لمناقشة خصائص البيانات الضخمة (ساقى وجاين، ٢٠١٨) وكيفية تجنب التكرار في الجمع.^{٢٣}

٤. حقوق أصحاب البيانات الشخصية

حقوق أصحاب البيانات الشخصية (المعروفين بـ "أصحاب البيانات" أو "Data Subjects") تمثل جوهر أي نظام لحماية البيانات، حيث تهدف إلى منح الأفراد السيطرة على بياناتهم الشخصية، وضمان عدم إساءة استخدامها، وتعزيز الشفافية والمساءلة من قبل الجهات المعالجة أو المتحكمة. في سياق النظام السعودي لحماية البيانات الشخصية (PDPL)، الذي صدر بموجب المرسوم الملكي رقم م/١٩ لعام ١٤٤٣ هـ (٢٠٢١م) وتم تعديله مؤخرًا، واللائحة الأوروبية لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في ٢٠١٨، هناك تشابه كبير في هذه الحقوق، مع بعض الاختلافات في التفاصيل والتطبيق.

١. حقوق أصحاب البيانات في النظام السعودي (PDPL): النظام السعودي، الذي تشرف عليه الهيئة

السعودية للبيانات والذكاء الاصطناعي (SDAIA)، يحدد حقوق أصحاب البيانات في المواد من ١٤ إلى ١٩ من النظام، مع تفاصيل إضافية في اللائحة التنفيذية المعدلة عام ٢٠٢٣-٢٠٢٥. [٧٨] هذه الحقوق مصممة لتعزيز الخصوصية في سياق التحول الرقمي الوطني، وتشمل آليات للتقدم بطلبات مجانية عادةً، مع استجابة خلال ٣٠ يومًا (قابلة للتמיד).

٢. الحق في العلم (Right to be Informed): يشمل إحاطة صاحب البيانات بالأساس النظامي لجمع

بياناته، والغرض من الجمع، والجهات التي قد تشارك البيانات. على سبيل المثال، عند جمع بيانات لأغراض توظيف، يجب على الشركة إبلاغ الشخص بالكيفية التي ستستخدم بها بياناته (مثل مشاركتها مع شركات التأمين). هذا الحق يتطلب إشعارات شفافة، مثل سياسات الخصوصية على المواقع الإلكترونية، ويمنع الجمع السري. في حال عدم الامتثال، يمكن للشخص تقديم شكوى إلى SDAIA.

٣. الحق في الوصول (Right of Access): يحق لصاحب البيانات طلب نسخة من بياناته الشخصية

المحتفظ بها لدى جهة التحكم، بما في ذلك مصادر الجمع وأغراض المعالجة. على سبيل المثال، إذا كان لدى بنك بيانات حساباتك، يمكنك طلب تفاصيل عن كيفية استخدامها. الطلب يجب أن يكون مجانيًا إلا في

²³ : Ghaleb, A. (2019). "Fair Processing in Data Protection Laws," Arab Journal of Legal Studies, Vol. 5, pp. 112-130.

حالات متكررة، ويجب الرد خلال ٣٠ يومًا. هذا الحق يساعد في اكتشاف الأخطاء أو الإساءات، ويمتد إلى البيانات المتعلقة بالأطفال أو الوصايا.

٤. **الحق في التصحيح (Right to Rectification):** إذا اكتشف صاحب البيانات أن بياناته غير دقيقة أو غير محدثة، يحق له طلب تصحيحها أو إكمالها. مثال: تصحيح عنوان بريد إلكتروني خاطئ في سجلات شركة. جهة التحكم ملزمة بالرد خلال ٣٠ يومًا، وإبلاغ الجهات الأخرى إذا تمت مشاركة البيانات.

٥. **الحق في إتلاف أو محو البيانات (Right to Erasure or Destruction):** يعادل "الحق في النسيان"، حيث يحق للشخص طلب إتلاف بياناته إذا انتهت الحاجة إليها، أو إذا سحب موافقته، أو إذا كانت المعالجة غير قانونية. مثال: حذف بيانات سابقة من قاعدة بيانات شركة بعد إنهاء عقد. لا ينطبق إذا كانت البيانات ضرورية لأغراض قانونية أو أمنية، وفق المادة ١٨ من النظام.

٦. **الحق في تقييد المعالجة (Right to Restriction of Processing):** يمكن لصاحب البيانات طلب تقييد المعالجة مؤقتًا، مثل أثناء التحقق من دقة البيانات أو في حال اعتراض. هذا يمنع استخدام البيانات حتى يتم حل النزاع.

٧. **الحق في الاعتراض (Right to Object):** يحق الاعتراض على معالجة البيانات لأغراض تسويقية مباشرة أو بحثية، أو إذا كانت تعتمد على مصالح مشروعة لجهة التحكم. مثال: رفض استخدام بياناتك لإعلانات مستهدفة.

٨. **الحق في نقل البيانات (Right to Data Portability):** يسمح بنقل البيانات إلى جهة أخرى بتنسيق آلي قابل للقراءة، خاصة إذا كانت المعالجة تعتمد على موافقة أو عقد.

٩. **الحقوق الإضافية:** تشمل سحب الموافقة في أي وقت، وتقديم الشكاوى إلى SDAIA، مع عقوبات على الانتهاكات تصل إلى ٥ ملايين ريال أو حبس لسنتين. في التحديثات ٢٠٢٥، أصبح التركيز أكبر على الامتثال الرقمي، مثل الإبلاغ عن الانتهاكات خلال ٧٢ ساعة.^{٢٤}

١٠. **الحق في الوصول (Right of Access):** طلب نسخة من البيانات، مع معلومات عن المعالجة (المادة ١٥). يشمل هذا الوصول إلى بيانات آلية مثل ملفات الذكاء الاصطناعي.

١١. **الحق في التصحيح (Right to Rectification):** تصحيح البيانات غير الدقيقة فورًا (المادة ١٦). مثال: تعديل معلومات خاطئة في تطبيق بنكي.

²⁴ : Saqi, J., & Jain, R. (2018). "Big Data Characteristics and Challenges," International Journal of Data Science, Vol. 4, pp. 78-95.

١٢. الحق في المحو (**Right to Erasure – Right to be Forgotten**): محو البيانات إذا لم تعد ضرورية أو سحبت الموافقة (المادة ١٧). يمتد إلى محركات البحث مثل جوجل، كما في قضية " Google Spain" 2014.^{٢٥}

١٣. الحق في تقييد المعالجة (**Right to Restriction**): تقييد المعالجة أثناء النزاعات (المادة ١٨)، مثل التحقق من الدقة.

١٤. الحق في نقل البيانات (**Right to Data Portability**): نقل البيانات بتنسيق آلي (المادة ٢٠)، مفيد في الانتقال بين خدمات مثل منصات التواصل.

١٥. الحق في الاعتراض (**Right to Object**): الاعتراض على المعالجة لأغراض تسويقية أو مصالح مشروعة (المادة ٢١)، مع وقف فوري للتسويق.

١٦. الحقوق المتعلقة بالقرارات الآلية والتنميط (**Rights Related to Automated Decision-Making**): عدم الخضوع لقرارات آلية تؤثر بشكل كبير (المادة ٢٢)، مثل رفض قروض آلياً، مع الحق في تدخل بشري. كما يشمل سحب الموافقة في أي وقت (المادة ٧). كلا النظامين يشتركان في الحقوق الأساسية مثل العلم، والوصول، والتصحيح، والمحو، والتقييد، والاعتراض، والنقل، مما يعكس تأثير GDPR على PDPL (كما في مقارنات). كلاهما يتطلب استجابة سريعة ومجانية، ويحمي الأطفال والفئات الضعيفة، مع عقوبات على الانتهاكات (غرامات تصل إلى ٤٪ من الإيرادات في GDPR، مقابل غرامات ثابتة في PDPL).

٥. الإفصاح ومشاركة البيانات

يشترط كلا النظامين إبلاغ وموافقة أصحاب البيانات لمشاركة مع الجهات الخارجية، مع نموذج طلب يوضح الهوية والغرض (في السعودية)، وشروط صارمة للنقل الدولي (EU GDPR المادة ٤٤)، مثل وجود قانون حماية كافٍ في البلد المستلم، أو طلب رسمي مع موافقة. استثناءات مشتركة للأغراض الأمنية أو الصحية دون إبلاغ لتجنب الفشل. داخل المنظمة، لا إبلاغ إذا ضمني في العقد، مع التأكيد على الحماية (مثل كلمات مرور للملفات). للنقل الدولي، يُشدد على الضمانات الأمنية.

٦. البعد الإجرائي والتعامل مع الحوادث

يتفقان على إنشاء سياسة خاصة مكتوبة بلغة مفهومة، وتعيين مسؤول حماية بيانات للإشراف والتوعية في إدارة الحوادث. يشملان عقوبات مثل الإنذار، والحبس، والغرامات (في السعودية تصل إلى ٥ ملايين ريال، المادتان ٣٥

اللائحة التنفيذية لنظام حماية البيانات الشخصية، تعديلات ٢٠٢٣-٢٠٢٥، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)²⁵

و٣٦)، مع إبلاغ الجهات التنظيمية خلال ٧٢ ساعة (EU GDPR، Recital 86). يُؤكد كلاهما على الرد السريع، وتقييم المخاطر، وإبلاغ أصحاب البيانات إذا لزم، والتكامل بين حماية البيانات والأمن السيبراني (دومبرا، ٢٠١٨). [١٠٨] أمثلة الحوادث مشتركة: إرسال خاطئ، وسرقة أجهزة، وإصابة برامج فدية، إلخ.

الفرع الثاني: أوجه الاختلاف

يظهر اختلاف في بعض المبادئ والأدوات، حيث لم تتطرق السياسة السعودية إلى بعض الجوانب التي أفردتها EU GDPR فقرات مستقلة. فيما يلي تفصيل كامل لهذه الاختلافات كما وردت في الدراسة:

١. المبادئ العامة

السياسة السعودية لم تتطرق إلى مبدأ الخصوصية بدءًا من التصميم (Privacy by Design)، الذي يبدأ عملية خصوصية البيانات من تصميم السياسات وقواعد البيانات ومستودعاتها ونماذج طلبات الوصول، مما يعزز الاستخدام العادل للبيانات. كما لم تذكر Privacy by Design and by Default، الذي يجعل الحماية بديهية من التصميم. هذه المبادئ موجودة في EU GDPR كمطلب قانوني لدمج التدابير التقنية والتنظيمية في الممارسات اليومية (المادة ٢٥).

٢. تقييم الآثار على الخصوصية (Privacy Impact Assessment – PIA)

السياسة السعودية لم تتكلم عن PIA، الذي هو إجراء تقييم للمعاملات على البيانات الشخصية (يدويًا أو في قواعد البيانات) لاكتشاف المخاطر المصاحبة للمعالجة، ودرئها قبل الحدث، أو تقليل أثرها السلبي، خاصة عند تحديث أو استبدال قواعد البيانات (كما في آدم ولويديين، ٢٠٢٠، الذين استخدموه لتقييم أنظمة الرد الآلي مثل Siri و Alexa). [١١٨] في EU GDPR (المادة ٣٥) و UK ICO، يشمل PIA وصف طبيعة المعالجة، ونطاقها، وسياقها، وأسبابها، وتقييم الحاجة والتناسب، وقياسات الامتثال، وتقييم المخاطر على الأشخاص، وتدابير التخفيف، وأسئلة توجيهية حول الغرض، ووصف الإجراء، والاستشارات، والضرورة، وتحديد المخاطر، والتدابير الإضافية، وتسجيل النتائج مع استشارة الجهات التنظيمية إذا بقيت مخاطر كبيرة. هذا يساعد على الامتثال والموازنة بين الحاجة والحماية، ويجب إكماله من قبل مالك المشروع ثم مراجعته من مسؤول الحماية.

٣. السياق العام والتركيز

السياسة السعودية حديثة نسبيًا، مما جعل مرحلة الامتثال في بواكيرها، مقارنة بـ EU GDPR التي أصبحت سياسة مستقلة منذ ٢٠١٤ تقريبًا، منفصلة عن سياسة الأمن العام. كما أن النظام السعودي يركز على الامتثال مع الأمن السيبراني دون فصل واضح، بينما EU GDPR يعامل الحماية كمطلب قانوني مستقل عن التقني، مع مرجعية للإدارة القانونية.

٤. العقوبات والنظام الجزائي

لكل سياسة نظام جزائي خاص، حيث في السعودية تشمل الإنذار، والحبس لسنتين، وغرامة تصل إلى ٥ ملايين ريال (المادتان ٣٥ و٣٦)، بينما EU GDPR لها نظام عقوبات مختلف، مع التركيز على الإبلاغ خلال ٧٢ ساعة وإبلاغ أصحاب البيانات فوراً لاتخاذ الحيطة (Recital 86)، وإبلاغ جهات التحكم إذا كان الاختراق في جهات المعالجة.

هذه الاختلافات تسمح بتوصية بتعزيز السياسة السعودية بإضافة PIA و Privacy by Design لمواكبة التقدم التقني.

الخاتمة

في نهاية هذا البحث الذي تناول مدى توافق نظام حماية البيانات الشخصية في المملكة العربية السعودية (PDPL) مع اللائحة الأوروبية العامة لحماية البيانات (GDPR) عبر دراسة مقارنة، استعرضنا مساراً تاريخياً وتحليلياً يبرز تطور هذين النظامين كإطارات رئيسية لحماية الخصوصية الرقمية. بدأ البحث بفحص الإطار النظري للنظام السعودي، مستعرضاً تعريفاته الأساسية مثل "البيانات الشخصية" (أي معلومة تحدد هوية الفرد مباشرة أو غير مباشرة)، "جهة المعالجة" (أي كيان يتعامل مع البيانات)، و"معالجة البيانات" (تشمل الجمع والتحليل والتخزين والإتلاف). كما أبرز التوافق مع التشريعات الدولية مثل GDPR، مع نطاق يشمل البيانات الإلكترونية واليدوية للأحياء فقط. ثم انتقل إلى تطور النظام السعودي عبر ثلاث مراحل: التمهيدية (قبل ١٩٧٠-٢٠٠٦) المعتمدة على الشريعة الإسلامية، الاستجابة الأمنية (٢٠٠٧-٢٠٢٠) بإصدار نظام مكافحة جرائم المعلوماتية وإنشاء سدايا، والحدث التشريعية (٢٠٢١-حتى الآن) بإصدار النظام عام ٢٠٢١، تعديلات ٢٠٢٣، وتحديثات ٢٠٢٤-٢٠٢٥ مثل لوائح النقل الدولي والتنفيذية.

هذا التطور يعكس استجابة المملكة للتحديات العالمية، مستلهماً من GDPR مع مراعاة السياق السعودي. أما GDPR، فقد ركزنا على نشأتها من توجيه ٩٥/٤٦/EC عام ١٩٩٥، مروراً بمعاهدات أمستردام ولشبونة، وصولاً إلى تفعيلها عام ٢٠١٨ كحق أساسي، مع دور محكمة العدل الأوروبية في قضايا مثل Google Spain و Schrems، وتنسيق عبر EDPB. فصلنا مبادئها مثل الموافقة والشفافية وتقليل البيانات، مع أمثلة على غرامات تصل إلى مليارات اليورو حتى ٢٠٢٥، مما يظهر صرامتها.

نتائج البحث: كشفت الدراسة توافقاً واسعاً بين PDPL و GDPR في التعريفات، المبادئ (المشروعية، الشفافية، تقليل البيانات)، وحقوق أصحاب البيانات (الوصول، المحو، الاعتراض)، مع تأثير سعودي بالأوروبي وتكيف ثقافي للبيانات الدينية والعائلية. ومع ذلك، تبرز اختلافات في غياب الأدوات الوقائية المتقدمة ك"الخصوصية من التصميم" و PIA في PDPL، وآليات عقوبات أقل ردة، مما يعكس حداثة PDPL مقابل تجربة GDPR الطويلة.

التوصيات: يُوصى بتعزيز PDPL عبر إجراءات استراتيجية لسد الثغرات الوقائية ومواكبة التطورات. أولاً، إدراج "الخصوصية من التصميم" إلزامياً (كالمادة ٢٥ في GDPR) لدمج الحماية في التصميم، مما يواجه تقنيات مثل الذكاء الاصطناعي؛ وجعل PIA إلزامياً للمشاريع الكبيرة مع دليل من سدايا (مستلهماً من المادة ٣٥ في GDPR)، حيث يمنع الانتهاكات بنسبة تصل إلى ٥٠٪. ثانياً، تطوير آليات نقل دولي مرنة كعقود قياسية مع شروط سعودية، وتعاون مع EDPB لتسهيل التجارة. ثالثاً، تعزيز التوعية عبر برامج وطنية وحملات، مع إنشاء مركز بحثي تحت سدايا لدراسات الخصوصية بتقارير سنوية. رابعاً، دراسة عقوبات مختلطة (ثابتة للصغيرة، نسبية ٢-٤٪ للكبرى) مستوحاة من GDPR، مع آليات تخفيف. أخيراً، تشجيع شراكات مع الاتحاد الأوروبي لتبادل المعرفة وتكييف مع AI Act (٢٠٢٤) بمواد خاصة بالذكاء الاصطناعي. هذه التوصيات تضمن مواكبة التحديات دون مساس بالسيادة، معززة مكانة المملكة رقمياً.

المراجع

قائمة المراجع (العربية)

١. القحطاني، ف. (٢٠٢٣). حماية الخصوصية في البيئة الرقمية: دراسة تحليلية للنظام السعودي. مجلة الدراسات القانونية المعاصرة، ١٥(٢)، ٨٨-٥٥.

٢. مجلس الشورى السعودي. (٢٠٢٢). تقرير حول نظام حماية البيانات الشخصية. الرياض: مجلس الشورى.

٣. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (٢٠٢٣). اللائحة التنفيذية لنظام حماية البيانات الشخصية. جريدة أم القرى. تم الاسترجاع من <https://uqn.gov.sa/details?p=23595>

٤. -الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (٢٠٢١). سياسات حوكمة البيانات الوطنية. تم الاسترجاع من <https://sdaia.gov>.

٥. نظام حماية البيانات الشخصية، المرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩ هـ (مع التعديلات بالمرسوم الملكي رقم (م/١٤٨) بتاريخ ١٤٤٤/٩/٥ هـ). (٢٠٢١). جريدة أم القرى. تم الاسترجاع من <https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1>

References (English)

1. Adam, I., & Lloyd, S. (2020). Privacy impact assessment in AI systems. Journal of AI Ethics, 3, 150-170.
2. Court of Justice of the European Union. (2014). Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12). ECLI:EU:C:2014:317.
3. Dumbra, V. (2018). Integrating data protection and cybersecurity. Cybersecurity Review, 10, 200-215.
4. European Parliament and 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,

and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

6.European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L 119, 1–88.Floridi, L. (2013). The ethics of information. Oxford University Press.

7.Ghaleb, A. (2019). Fair processing in data protection laws. Arab Journal of Legal Studies, 5, 112–130.

8.Hofmann, H., et al. (2017). Data protection in organizational contexts. Journal of Privacy Studies, 12, 45–67.

9.Kuner, C. (2020). Transborder data flows and data privacy law. Oxford University Press.

10.Saqi, J., & Jain, R. (2018). Big data characteristics and challenges. International Journal of Data Science, 4, 78–95.

11.Saudi Data and Artificial Intelligence Authority (SDAIA). (2023). Guide to the Saudi Personal Data Protection Law. Retrieved from <https://dgp.sdaia.gov.sa>

12.Voigt, P., & Von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.