الحماية القانونية للمعلومات الشخصية
في ظل الفضاء الرقمي بالنظام القانوني السعودي

د. عُلا أحمد جابر عبد اللهّ
كليات الخليج – السعودية

ملخص البحث:
تتناول هذه الورقة الإطار القانوني والتشريعي لحماية المعلومات والبيانات الشخصية في المملكة العربية السعودية، لا سيما في ظل التحول الرقمي المتسارع. وقد اعتمدت الباحثة على المنهج الوصفي التحليلي من خلال استقراء النصوص النظامية في "نظام حماية البيانات الشخصية" وتحليل دور الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في حماية الخصوصية الرقمية. تهدف الدراسة إلى تسليط الضوء على أهمية المعلومات كأصل استراتيجي، مستعرضة آليات التصدي للاختراقات المعلوماتية وضوابط الوصول إلى المعلومة. خلصت الدراسة إلى أن النظام السعودي نجح في إيجاد توازن بين تعزيز الرقمنة وبين ضمان حقوق الأفراد، مع فرض عقوبات رادعة لضمان الامتثال، بما يتماشى مع أفضل الممارسات الدولية، وذلك في ظل التحول المستدام مما يفرض على المجتمعات أهمية مراعاة التوازن ما بين اتاحة الحرية الرقمية وما تسمح بها من اتاحة البيانات وبين فرض سياج حماية نظامية لحماية المعلومات الشخصية للأفراد من كافة صور التعدي المعتادة والمستحدثة وفق متغيرات العصر، ولقد القت الدراسة الضوء على أهم الملامح التطبيقية في ملف حماية البيانات والمعلومات في النظام السعودي عن طريق استقراء آليات الحماية التطبيقية من مؤسسات وهيئات نظامية بالمملكة ولوائح وانظمة من جانب أخر تضمن تفعيل التوازن بين الاتاحة والحماية للمعلومات سواء على المستوى الفردي او المجتمعي بالنظام السعودي مما يعكس رؤية ذلك النظام وخطواتها السباقة في مجال الرقمنة والحماية المعلوماتية.

الكلمات المفتاحية: حماية المعلومات – حق الوصول – امن المعلومات –الرقمنة – الفضاء الرقمي – المعلومات الشخصية

Legal Protection of Personal Data within the Digital Space under the Saudi Legal System

OLA AHMED GABER ABDALLAH

Abstract:

This study examines the legal and legislative framework for protecting information and personal data in the Kingdom of Saudi Arabia, particularly considering rapid digital transformation. The study employs a descriptive-analytical methodology by surveying the statutory provisions of the "Personal Data Protection Law" (PDPL) and analysing the role of the Saudi Data and AI Authority (SDAIA) in safeguarding digital privacy. The research aims to highlight the significance of information as a strategic asset, reviewing mechanisms to counter cyber-breaches and regulations governing the right of access to information. The study concludes that the Saudi legal system has successfully balanced the promotion of digitization with the protection of individual rights, imposing deterrent penalties to ensure compliance in alignment with international best practices.

This is within the context of the sustainable transformation, which imposes upon societies the importance of observing a balance between the provision of digital freedom and the data availability it allows, on the one hand, and the imposition of a systematic protective framework to safeguard individuals' personal information from all forms of customary and emergent infringements according to the variables of the era, on the other hand. The study shed light on the most significant practical features in the data and information protection file within the Saudi system by extrapolating the practical protection mechanisms from systemic institutions and bodies in the Kingdom, as well as regulations and bylaws, to ensure the activation of the balance between the accessibility and protection of information, whether at the individual or societal level within the Saudi system. This reflects the vision of that system and its proactive steps in the field of digitalization and informational protection.

Keywords: Information Protection, Right of Access, Information Security, Digitization, Cyberspace, Personal Data.

مشكلة البحث:

تتمثل مشكلة البحث في خطورة ما يترتب على انتهاك الخصوصية للمعلومات الشخصية من آثار وما ينعكس على ذلك من خطورة خاصة في ظل التحول الرقمي وسهولة الوصول للمعلومات في الفضاء الرقمي الذي يزيد من درجة التهديدات التي قد تمس أمن وسلامة الأفراد والدول، وضرورة وضع سياج حماية تنظيمية لحماية تلك المعلومات.

أهمية البحث:

تكمن أهمية البحث في الدخول الى عالم شائك يلتمسه العالم اجمع من حماية المعلومات الشخصية وضمان عدم التعدي عليها ولا استغلالها بشكل غير مشروع ، الامر الذي يظهر اكثر صعوبة في ظل التطور الرقمي الذي يشهده العالم اجمع والفضاء الرقمي الذي يتيح لأى فرد الاطلاع بسهولة على اسى معلومة بضغطة زر او لمسة شاشة ، فيقف البحث على ملف الحماية النظامية للمعلومات الشخصية بالنظام السعودي وما هي الاجراءات التي اتخذتها للسيطرة على حماية المعلومات في ذات التوقيت الذي تلتزم فيه الدولة بسهولة لوصول للمعلومات واتاحتها عبر الانترنت والفضاء الرقمي .

نطاق البحث:

يتناول البحث مشكلة حماية المعلومات الشخصية على نطاقين، الاول دولياً بالمعاهدات والاتفاقيات الدولية التي نظمت حماية المعلومات الشخصية، والاخر هو النظام القانون السعودي لحماية البيانات الشخصية.

الدراسات السابقة

تناولت عدة دراسات سابقة بعض التجارب العربية في مجال حماية المعلومات الشخصية منها:

1. نجود بنت علي بن محمد السعوي، 2024، الحماية النظامية للخصوصية المعلوماتية (دراسة تأصيلية تحليلية)، الجمعية العلمية القضائية السعودية، مجلة قضاء، العدد 34، فبراير 2024

والتي تناولت خطورة ما يترتب على انتهاك الخصوصية المعلوماتية من آثار، وما تنعكس عليه من ضرورة حمايتها خاصة في ظل التحول الرقمي

2. عبد الله المهيدب وأخرين، 2022، حماية البيانات وخصوصية إنترنت الأشياء للرعاية الصحية، مجلة العلوم التطبيقية المجلد 12، العدد الرابع

وناقشت هذه المقالة مختلف مكونات إنترنت الأشياء للرعاية الصحية، وتصنف أجهزة الرعاية الصحية المختلفة بناءً على وظائفها واستخدامها، كما تسلط الضوء على النقاط والأسباب المحتملة لتسرب البيانات، مثل تضارب القوانين.

3. فهد الشمري، 2023، الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية " دراسة تحليلية " / الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية، مجلة البحوث الفقهية والقانونية، مجلة كلية الشريعة والقانون فرع جامعة الازهر، دمنهور، المجلد 35، العدد 43

والتي تناولت تعريف المعلومات الشخصية وماهية حقوق الافراد تجاه معلوماتهم في النظام السعودي.

4. رسالة مقدمة لنيل درجة الماجيستير من إعداد الطالب/ منصور بن صالح السلمي، 2010، المسؤولية المدني لانتهاك الخصوصية في نظام مكافحة الجرائم المعلوماتية السعودي – من قسم العدالة الجنائية بجامعة نايف العربية للعلوم الامنية

والتي تناولت حق الخصوصية من خلال منظور نظام الجرائم المعلوماتية قبل صدور قانون حماية المعلومات الشخصية

المقدمة

خطة البحث

المبـــحث الأول: التطور التاريخي لحماية المعلومات الشخصية

المطلب الأول: الحماية القانونية للمعلومات الشخصية دولياً

المطلب الثاني: الاتفاقيات والهيئات الخاصة بحماية المعلومات الشخصية

المبـــحث الثاني: المملكة العربية السعودية ومجال حماية المعلومات الشخصية بالفضاء الرقمي

المطلب الأول: واقع حماية البيانات في المملكة العربية السعودية

المطلب الثاني: التشريعات والجهات السعودية التطبيقية لحماية المعلومات

المقدمـــــــة:

عرف الانترنت على أنه شبكة عامة يستخدم حول العالم، ويربط بين ملايين الحواسيب المكونة من شبكات متعددة المصادر والمهام، كالشبكات المنزلية التي تقتصر في استخدامها في استخدامها على مجموعة من الأفراد، والشبكات الأكاديمية، والتجارية، والحكومية الصغيرة، وقد بدأت شبكة الإنترنت على شكل شبكة وكالة مشاريع الأبحاث المتطورة في عام 1969م، وهي عبارة عن شبكة واسعة أُنشأت من قبل وكالة مشاريع البحوث المتقدمة التابعة لوزارة الدفاع الأمريكية، وكانت تعتبر كشبكة لاختبار التقنيات الشبكية الجديدة.

وقد أضحت صيانة المعلومات الشخصية أحد المحاور الأساسية في النقاشات المتصلة بالتحول الرقمي والحوكمة الإلكترونية، ونظرًا لما تشهده المجتمعات الحديثة من توسع غير مسبوق في استعمال التقنيات الرقمية وتبادل المعطيات عبر الشبكات.وتحدد المعلومات الشخصية بأنها كل ما من شأنه أن يفضي إلى التعرّف على هوية الفرد، سواء بصورة مباشرة أو غير مباشرة، وتشمل على سبيل المثال لا الحصر: الأسماء، أرقام الهويات، العناوين، المعلومات المصرفية، والسجلات الصحية.ويعتبر تأمين هذه البيانات وحمايتها من الوصول غير المشروع والاستعمال غير المصرح به ضرورة ملحة لضمان حقوق الأفراد وتعزيز الثقة في البيئة الرقمية ، وتنبثق أهمية حماية المعلومات الشخصية من كونها ترتبط ارتباطًا وثيقًا

بحقوق الإنسان الأساسية لا سيما الحق في الخصوصية ،ويتطلب تحقيق هذا الهدف اعتماد مجموعة من المبادئ والمعايير التي تضمن الشفافية في جمع البيانات ، وتحدد الغرض من استخدامها، وتكفل لصاحب البيانات جملة من الحقوق، من بينها الحق في الاطلاع على بياناته، وتصحيحها أو حذفها، والاعتراض على معالجتها في بعض الحالات. كما يجب أن تلتزم الجهات المعنية بمعالجة البيانات باتخاذ تدابير فنية وتنظيمية فعّالة لضمان سلامة البيانات وسريتها، والحد من المخاطر المرتبطة بفقدانها أو إساءة استخدامها، وفي هذا السياق تواجه المؤسسات تحديات متعددة اثناء حماية المعلومات مثل الهجمات السيبرانية، وسوء إدارة البيانات، وضعف البنية التحتية الرقية، ونقص الوعي الأمني لدى بعض المستخدمين.

واخيراً تُعد الحماية القانونية للبيانات الشخصية عنصرًا أساسيًا في صون خصوصية الأفراد وتعزيز ثقتهم في البيئة الرقمية. فهي تُوفر إطارًا تنظيميًا يُلزم الجهات بجمع البيانات ومعالجتها وفق ضوابط محددة، ويمنح الأفراد حقوقًا قانونية في التحكم بمعلوماتهم. كما تسهم هذه الحماية في الحد من الانتهاكات والتجاوزات المحتملة، وتُشكل دعامة رئيسية للأمن السيبراني والاستقرار الاجتماعي في العصر الرقمي، وهو ما يمثل ضمان وجود سياج حماية مشروعة للأفراد من جهة والدول من جهة اخرى.

المبــحث الأول

التطور التاريخي لحماية المعلومات الشخصية

شهد مفهوم حماية المعلومات الشخصية تطورًا تدريجيًا على الصعيد العالمي، تأثر بالتحولات التقنية والاجتماعية والسياسية التي رافقت العصر الرقمي. تعود البدايات الأولى للاعتراف القانوني بالحق في الخصوصية إلى أواخر القرن التاسع عشر، عندما نُشرت مقالة "الحق في الخصوصية" عام 1890 في الولايات المتحدة على يد صامويل وارن ولويس براندیز، معتبرة الخصوصية حقًا مستقلًا يجب حمايته من التدخل غير المشروع. ومع تطور وسائل الإعلام والاتصال، ظهرت الحاجة إلى أطر قانونية تنظم جمع البيانات الشخصية واستخدامها،

خاصة مع دخول الحواسيب إلى المؤسسات الحكومية والخاصة منتصف القرن العشرين، مما أثار مخاوف بشأن الرقابة والمراقبة الإلكترونية.

في سبعينيات القرن الماضي، بدأت الدول بوضع تشريعات صريحة لحماية البيانات، وكان من أبرزها القانون السويدي الصادر عام 1973، الذي يُعد أول قانون وطني ينظم معالجة البيانات الشخصية آليًا. تبع ذلك إصدار اتفاقية مجلس أوروبا رقم 108 عام 1981، والتي شكلت مرجعًا دوليًا مهمًا لحماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي. ومع التوسع الهائل في تقنيات الإنترنت وتطبيقات الذكاء الاصطناعي، ازدادت التحديات المرتبطة بحماية الخصوصية، ما دفع الاتحاد الأوروبي إلى تبني اللائحة العامة لحماية البيانات (GDPR)في عام 2016، التي دخلت حيّز التنفيذ عام 2018، وأصبحت تمثل المعيار العالمي الأبرز في هذا المجال. وقد ألهمت هذه التطورات العديد من الدول حول العالم لوضع أنظمة وتشريعات مماثلة تعكس التوازن بين الابتكار التقني وحماية الحقوق الفردية.

أما في العالم العربي، فقد بدأت فكرة حماية المعلومات الشخصية تحظى باهتمام متزايد مع انتشار الخدمات الرقمية والتحول الإلكتروني في المؤسسات الحكومية والخاصة. إلا أن الاستجابة القانونية والتنظيمية تأخرت نسبيًا مقارنة بالدول الغربية، حيث اقتصر التعامل مع البيانات الشخصية في بداية الأمر على قواعد عامة ضمن قوانين العقوبات أو قوانين الاتصالات. ومع تزايد الارتباط بالبيئة الرقمية العالمية، واتساع نطاق المعاملات الإلكترونية، بدأت بعض الدول العربية بوضع تشريعات مستقلة لحماية البيانات، من بينها تونس التي أصدرت قانونًا خاصًا في هذا المجال عام 2004، ثم المغرب ومصر والإمارات في السنوات اللاحقة، مستندة غالبًا إلى نماذج أوروبية مثل اللائحة العامة لحماية البيانات (GDPR).

أما في المملكة العربية السعودية، فقد تطورت المنظومة التشريعية لحماية البيانات الشخصية تدريجيًا، تماشيًا مع رؤية المملكة 2030 التي أولت اهتمامًا بالغًا بالتحول الرقمي وحوكمة البيانات. وجاء التطور النوعي بإصدار "نظام حماية البيانات الشخصية "بموجب المرسوم الملكي رقم (م/ 19) وتاريخ 9/ 2/ 1443هـ (الموافق 16 سبتمبر 2021م)، والذي

أُنيطت مسؤولية تطبيقه بـ الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) .يهدف النظام إلى تنظيم عمليات جمع ومعالجة وتخزين ونقل البيانات الشخصية بما يضمن حماية الخصوصية الفردية، ويحافظ على حقوق أصحاب البيانات، مع فرض التزامات صارمة على الجهات التي تتعامل معها، سواء كانت عامة أو خاصة. وقد دخل النظام حيّز التنفيذ بعد فترة انتقالية، وتم تحديث بعض مواده لاحقًا لتواكب المستجدات التقنية، مما يعكس رغبة المملكة في تأسيس بنية قانونية حديثة ومتوافقة مع المعايير الدولية لضمان أمن البيانات وتعزيز الثقة في البيئة الرقمية.

ختامًا، يُظهر تطور حماية المعلومات الشخصية على الصعيدين الدولي والعربي تحولًا جوهريًا من المبادئ العامة إلى تشريعات متخصصة ومُلزمة، تعكس وعيًا متزايدًا بأهمية الخصوصية في العصر الرقمي، وقد استطاعت المملكة العربية السعودية من خلال نظام حماية البيانات الشخصية أن تضع إطارًا قانونيًا متقدمًا يواكب المعايير الدولية، ويعزز من ثقة الأفراد والمؤسسات في التعاملات الرقمية.

المطلب الأول: الحماية القانونية للمعلومات الشخصية دولياً

إن حماية المعلومات تشير إلى مجموعة من الإجراءات والتقنيات التي تهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها، وتشمل هذه الإجراءات تدابير متعددة مثل التشفير، وإدارة الوصول، والمراقبة الأمنية، وسياسات الخصوصية، وكلها تسعى إلى التصدي للتهديدات السيبرانية المتزايدة، مثل الاختراقات، وسرقة الهوية، والبرمجيات الخبيثة، والهجمات المنظمة على البنى التحتية الرقمية. في المقابل، فإن إتاحة المعلومات تُعدّ مبدأ أساسيًا في مجتمع المعرفة الحديث، حيث تُمكّن الأفراد والمؤسسات من اتخاذ قرارات مبنية على بيانات دقيقة، كما تسهم في تعزيز الشفافية، وتمكين التعليم، ودعم الابتكار، ومع تزايد الاعتماد على الإنترنت كوسيلة رئيسية لتبادل المعلومات، تبرز الحاجة الماسة إلى إيجاد أطر تنظيمية وأخلاقية واضحة تضمن تحقيق التوازن بين الحق في الوصول إلى المعلومات، والحق في حماية الخصوصية والأمن الرقمي ، وفي ظل العولمة الرقمية وتزايد التهديدات السيبرانية العابرة للحدود، أصبح من الضروري وجود إطار قانوني دولي ينظم حماية المعلومات وإتاحة

الوصول إليها عبر الإنترنت بشكل عادل وآمن، وقد سعت الدول والمنظمات الدولية إلى وضع قواعد ومعايير مشتركة لمواجهة التحديات المتعلقة بأمن المعلومات، والخصوصية، وحماية البيانات، من خلال عدد من الاتفاقيات والمعاهدات الدولية، هذه الجهود تهدف إلى تحقيق توازن دقيق بين ضرورة حماية الأنظمة والمستخدمين من الجرائم الإلكترونية، وبين احترام الحق في الوصول إلى المعلومات وضمان حرية التعبير في الفضاء الرقمي، وهو ما يُعد من المبادئ الأساسية لحقوق الإنسان في العصر الحديث.

من أبرز الإجراءات الدولية التي تولت الاهتمام بحماية البيانات، تأتي اتفاقية بودابست (2001) ، والمعروفة باسم الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، والتي تُعد أول معاهدة دولية تهدف إلى مكافحة الجرائم التي تُرتكب عبر الإنترنت، مع وضع آليات للتعاون بين الدول في هذا المجال، كما تُعد اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) مثالاً صارخًا للتشريعات التي تسعى إلى حماية خصوصية الأفراد وتنظيم استخدام معلوماتهم الشخصية، وعلى مستوى الأمم المتحدة، تواصل لجنة الأمم المتحدة المعنية بالاستخدام السلمي للفضاء الإلكتروني (UNCCT) العمل على تطوير إطار قانوني للتعامل مع قضايا الأمن السيبراني وحرية المعلومات، إلى جانب ذلك هناك مبادرات دولية مثل "شراكة حرية الإنترنت(Freedom Online Coalition) "، والتي تضم عدة دول ملتزمة بتعزيز حرية التعبير والخصوصية والأمن عبر الإنترنت، كل هذه الاتفاقيات والمبادرات تُظهر مدى أهمية التعاون الدولي في تنظيم الفضاء الرقمي وضمان أمنه وعدالته وهو ما سوف نستعرضه بشيء من التفصيل في التالي :

1. اتفاقية بودابست2001 – (Budapest Convention)

هي أول معاهدة دولية تهدف إلى مكافحة الجرائم الإلكترونية، ووضعتها مجلس أوروبا بمشاركة دول غير أوروبية أيضًا. تضع الاتفاقية إطارًا قانونيًا موحدًا لتجريم أنشطة مثل اختراق الأنظمة، التلاعب بالبيانات، والاحتيال الإلكتروني. كما تنظم التعاون الدولي بين أجهزة إنفاذ القانون لتسهيل تبادل المعلومات والاستجابة السريعة للهجمات السيبرانية

العابرة للحدود. ورغم أنها أوروبية الأصل، فإن دولًا من خارج القارة مثل الولايات المتحدة وكندا واليابان انضمت إليها، بينما لا تزال غالبية الدول العربية خارجها.

2. **اللائحة العامة لحماية البيانات2018 – (GDPR)**

هي تشريع صادر عن الاتحاد الأوروبي يهدف إلى حماية البيانات الشخصية للمواطنين الأوروبيين، سواء تمت معالجتها داخل أو خارج الاتحاد. تلزم هذه اللائحة أي جهة (شركة، مؤسسة، موقع إلكتروني...) تحصل على بيانات المستخدمين، بالحصول على موافقة صريحة، وتوضيح كيفية استخدام البيانات، مع منح الأفراد حق الوصول إليها، وتصحيحها، أو طلب حذفها. وتُعد واحدة من أكثر القوانين صرامة في العالم في مجال الخصوصية الرقمية، وقد أثرت في سياسات شركات عالمية وحتى تشريعات بعض الدول خارج الاتحاد الأوروبي.

3. **مبادرة شراكة حرية الإنترنت(Freedom Online Coalition)**

هي تحالف دولي تأسس في عام 2011، يضم حاليًا أكثر من 30 دولة، ويهدف إلى تعزيز حرية التعبير والخصوصية والأمن على الإنترنت .تسعى المبادرة إلى دعم سياسات الإنترنت المفتوح، وضمان ألا تُستخدم أدوات الرقابة أو المراقبة لانتهاك حقوق الإنسان. تعمل من خلال التعاون مع الحكومات، ومنظمات المجتمع المدني، وشركات التكنولوجيا، وتصدر تقارير وتوصيات تساعد في تعزيز حقوق المستخدمين في الفضاء الرقمي.

4. **جهود الأمم المتحدة (UNCCT)– وفرق عمل الأمن السيبراني**

الأمم المتحدة، من خلال عدة وكالات ومبادرات، مثل مركز الأمم المتحدة لمكافحة الإرهاب (UNCCT) ومجموعة الخبراء الحكومية المعنية بتطورات الفضاء السيبراني (GGE)، تتابع عن كثب قضايا الأمن السيبراني. تعمل هذه الجهات على تطوير قواعد دولية لاستخدام الفضاء السيبراني في سياق الأمن الدولي، وتشجع الدول على تبادل الخبرات، وتطوير قدراتها التقنية والتشريعية، وتحقيق توازن بين مكافحة التهديدات الرقمية وضمان الحريات الأساسية.

المطلب الثاني: الاتفاقيات والهيئات الخاصة بحماية المعلومات الشخصية

أولًا: الاتفاقيات الدولية الخاصة بحماية البيانات الشخصية:

1. اتفاقية مجلس أوروبا رقم 108 لعام 1981

تعد تلك أول وثيقة دولية ملزمة قانونيًا تهدف إلى حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات ذات الطابع الشخصي، وقد أرست الاتفاقية مبادئ أساسية مثل مشروعية جمع البيانات، وتحديد أغراض استخدامها، وضمان حق الأفراد في الاطلاع على بياناتهم وتصحيحها، كما تُعد الاتفاقية مرجعًا أساسيًا للعديد من التشريعات الوطنية، وقد خضعت لتحديثات لاحقة، أبرزها "البروتوكول المعدل" الذي صدر عام 2018 (اتفاقية 108+)، لمواكبة تطورات العصر الرقمي.

2. اللائحة العامة لحماية البيانات الأوروبية(GDPR)

وتعد من أبرز الأطر التنظيمية أيضًا التي أقرها الاتحاد الأوروبي عام 2016 ودخلت حيز التنفيذ في مايو 2018، تُعتبر هذه اللائحة الأكثر شمولًا وتفصيلًا على المستوى العالمي، إذ تنظم كيفية جمع البيانات الشخصية ومعالجتها وتخزينها، وتمنح الأفراد حقوقًا واسعة كحق النسيان، والاعتراض، ونقل البيانات. وقد أثرت اللائحة بشكل مباشر في تشريعات العديد من الدول، بما في ذلك دول خارج الاتحاد الأوروبي، نظرًا لاتساع نطاق تطبيقها على أي جهة تتعامل مع بيانات لمقيمين في أوروبا.

3. المبادئ التوجيهية لحماية الخصوصية وتدفق البيانات عبر الحدود الدولية((OECD)

كذلك اعتمدت منظمة التعاون والتنمية الاقتصادية عام 1980 مجموعة من المبادئ والتي تُعد أول محاولة لوضع معايير غير ملزمة لحماية البيانات بين الدول الأعضاء، وعلى الرغم من أنها لم تُشكّل إطارًا قانونيًا ملزمًا، إلا أنها ساهمت في بناء التوافق الدولي حول مفاهيم مثل الشفافية، والمسؤولية، وتقييد الغرض من استخدام البيانات. وتم تحديث المبادئ عام 2013 لتشمل مفاهيم الأمن السيبراني والمسؤولية المؤسسية في حماية الخصوصية.

وبناء عليه فأن الاتفاقيات الدولية لحماية المعلومات الشخصية تشكل أداة أساسية لضمان توحيد المعايير القانونية والأخلاقية بين الدول في التعامل مع البيانات، خاصة في ظل الانفتاح الرقمي وتدفق المعلومات عبر الحدود بكل سهولة ، فغياب هذه الاتفاقيات وضعف نصوصها والالتزام بها قد يؤدي إلى تفاوت في مستويات الحماية، واستغلال بيانات الأفراد في دول لا توفر ضمانات كافية للخصوصية ومن خلال وضع مبادئ مشتركة، وتسهم هذه الاتفاقيات في تعزيز الشفافية وحماية الحقوق الأساسية، وتقوية الثقة في الاقتصاد الرقمي العالمي ، كما تساعد في تنظيم العلاقات بين الحكومات والشركات والمؤسسات، وتُوفّر إطارًا قانونيًا للتعاون في مواجهة الجرائم السيبرانية والانتهاكات العابرة للحدود وفي ظل الاعتماد المتزايد على الذكاء الاصطناعي وتحليل البيانات، تبرز أهمية هذه الاتفاقيات كضمانة لحماية كرامة الإنسان في البيئة الرقمية.

ثانيًا: الجهات الدولية المعنية بحماية البيانات الشخصية:

تتعدد الجهات الدولية التي تضطلع بمهمة وضع السياسات والمعايير الخاصة بحماية البيانات الشخصية، ومن أبرزها:

1. **مجلس أوروبا** [1] (Le Conseil de l'Europe https: / /www.coe.int /web /portal /home)

والذي يُشرف على تنفيذ اتفاقية 108 [2] (https: / /www.coe.int /en /web /data-protection /convention108)، والتي تُعد أساسًا هامًا للتشريعات الوطنية في مجال حماية البيانات، كما أنها توفر إطارًا قانونيًا للتعاون الدولي في هذا المجال، وتنطبق الاتفاقية على معالجة البيانات الشخصية سواء كانت آلية أو غير آلية، وتلزم الأطراف باتخاذ التدابير اللازمة في قوانينها المحلية لضمان احترام حقوق الإنسان الأساسية للأفراد فيما يتعلق بمعالجة بياناتهم الشخصية، وفقًا لمجلس أوروبا.

ويعمل المجلس على تطويرها عبر التعاون مع الدول الأعضاء والشركاء، ويُعد المجلس رائدًا في دمج حقوق الإنسان في سياسات البيانات، ويُصدر تقارير وتوصيات دورية تتعلق بالممارسات الفضلى في هذا المجال، كما يسهم في دعم الدول غير الأوروبية في تطوير تشريعاتها الوطنية لحماية الخصوصية.

2. **منظمة التعاون والتنمية الاقتصادية ((OECD)**[3] (منظمة التعاون الاقتصادي والتنمية: https: / /www.dfat.gov.au/)

وهي منظمة دولية تأسست عام 1961، ومقرها باريس، وتضم 38 دولة عضوًا ملتزمة بالديمقراطية واقتصاد السوق .تهدف المنظمة إلى تعزيز السياسات التي من شأنها تحسين

الرفاه الاقتصادي والاجتماعي للشعوب حول العالم، وذلك من خلال دعم النمو الاقتصادي المستدام، وتعزيز فرص العمل، ورفع مستويات المعيشة، والمساهمة في نمو التجارة العالمي، ومن جهة أخرى تلعب تلك المنظمة دورًا مهمًا في وضع السياسات الدولية المتعلقة بحوكمة البيانات، وتوفر منصة للحوار بين الحكومات حول التوازن بين الابتكار الرقمي وحماية الخصوصية.

3. **الهيئات التنظيمية الوطنية**

مثل "مجموعة حماية البيانات في الاتحاد الأوروبي التي تحوّلت لاحقًا إلى "مجلس حماية البيانات الأوروبي (EDPB)والتي تساهم في تنسيق الجهود على المستوى القاري والدولي، وتشجع على تطبيق موحد للقواعد، بما يسهم في تقوية الإطار العالمي لحماية البيانات.، ويضمن المجلس تطبيق قوانين حماية البيانات بشكل موحد في جميع أنحاء الاتحاد الأوروبي.[1] (مجلس حماية البيانات الاوروبي: https://european-union.europa.eu/) وعلى الرغم من الجهود التي تبذلها تلك الهيئات، إلا أنها تواجه مجموعة من القضايا والتحديات المتصاعدة في ظل التطور التكنولوجي المتسارع. من أبرز هذه القضايا عدم التجانس في القوانين الوطنية، حيث تختلف مستويات الحماية بين الدول، مما يعقّد عملية تبادل البيانات ويثير مخاوف بشأن "مناطق الأمان المنخفض". كما تُطرح تساؤلات قانونية وأخلاقية حول استخدام الذكاء الاصطناعي والتحليل الضخم للبيانات، ومدى احترام هذه التقنيات لحقوق الخصوصية الفردية، خصوصًا في غياب الشفافية والخوارزميات التمييزية. كذلك تُعد الانتهاكات السيبرانية وتسريبات البيانات الكبرى من القضايا المتكررة التي تضع ضغطًا على المنظمات الدولية لتحديث سياساتها وتعزيز التعاون العابر للحدود. وتبرز أيضًا إشكالية نقل البيانات إلى الدول التي لا توفّر حماية كافية، وهو ما تطرقت إليه محاكم دولية مثل محكمة العدل الأوروبية في قضايا معروفة (مثل قضية Schrems II)[2] (لينك القضية:

https: / /www.cookiebot.com /en /schrems-ii-privacy-shiel)، والتي أبطلت بعض الاتفاقات الدولية السابقة، ما يدل على حساسية التوازن بين حماية البيانات وحرية التجارة الدولية، في هذا الإطار، تظل الحاجة قائمة لتعزيز التكامل بين الأنظمة القانونية، وتفعيل آليات رقابة فعّالة لضمان احترام مبادئ حماية المعلومات الشخصية عالميًا.

المبـــحث الثاني

المملكة العربية السعودية ومجال حماية المعلومات الشخصية في الفضاء الرقمي

قبل إصدار نظام حماية البيانات الشخصية في المملكة العربية السعودية، كان الإطار القانوني المتعلق بحماية البيانات محدودًا وغير موحد، ما أدى إلى وجود فجوة تنظيمية واضحة في هذا المجال. فلم يكن هناك قانون مستقل أو شامل يعالج موضوع حماية البيانات الشخصية بشكل مباشر، بل كانت الحماية تتوزع على عدد من الأنظمة واللوائح ذات الصلة، مثل نظام مكافحة الجرائم المعلوماتية لعام 2007، والذي ركز بشكل أساسي على المعالجة الجنائية للجرائم الإلكترونية، بما في ذلك الوصول غير المصرح به إلى البيانات أو تدميرها أو استخدامها بطريقة غير مشروعة.

وبسبب غياب تشريع متخصص، كانت الجهات الحكومية والخاصة تعتمد على اجتهاداتها في التعامل مع بيانات الأفراد، ما أدى إلى تفاوت كبير في آليات الحماية المطبقة، وانعدام الوضوح فيما يتعلق بحقوق الأفراد تجاه بياناتهم الشخصية. لم تكن هناك معايير إلزامية تحدد كيفية جمع البيانات أو استخدامها أو تخزينها، كما لم تكن هناك جهة رقابية مركزية تشرف على تطبيق ممارسات الخصوصية. هذا النقص في التنظيم ترك الأفراد دون ضمانات كافية، وجعل من الصعب مساءلة الجهات التي تقوم بإساءة استخدام البيانات أو تسريبها.

علاوة على ذلك، لم يكن هناك وعي واسع لدى الأفراد أو المؤسسات بأهمية حماية البيانات أو المخاطر المرتبطة بإساءة استخدامها، خاصة مع التوسع السريع في الخدمات الرقمية والمعاملات الإلكترونية. وقد أثار ذلك قلقًا متزايدًا على الصعيدين المحلي والدولي، وخصوصًا مع ازدياد متطلبات الامتثال العالمية، مثل اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، التي سلطت الضوء على أهمية وجود إطار قانوني صارم لحماية الخصوصية ، لذلك، فإن المرحلة السابقة لسنّ النظام الرسمي لحماية البيانات في المملكة تميزت بضعف التنظيم، وتفاوت الممارسات، وغياب جهة رقابية موحدة، وهو ما دفع الجهات التشريعية لاحقًا إلى إدراك أهمية معالجة هذا النقص من خلال وضع إطار قانوني واضح ومتسق يضمن حماية حقوق الأفراد، ويعزز الثقة في البيئة الرقمية الوطنية.

ولكن حالياً تولي المملكة العربية السعودية أهمية كبيرة لحماية المعلومات وأمنها في ظل التطور التقني والتحول الرقمي المتسارع الذي تشهده مختلف القطاعات. وقد أدركت الجهات المعنية في المملكة أن أمن المعلومات يشكل حجر الأساس في بناء بيئة رقمية آمنة ومستقرة، تحفظ خصوصية الأفراد، وتضمن سرية البيانات الحساسة، وتحمي البنى التحتية الحيوية من التهديدات السيبرانية ، ومن هذا المنطلق، وضعت المملكة إستراتيجيات وسياسات واضحة، أبرزها "الاستراتيجية الوطنية للأمن السيبراني، وأنشأت هيئات متخصصة مثل الهيئة الوطنية للأمن السيبراني، بهدف تعزيز منظومة الحماية وتطوير الكفاءات الوطنية القادرة على مواجهة التحديات الرقمية الحديثة ، وهو ما سوف نستعرضه في المطالب القادمة من واقع حماية المعلومات الشخصية بالمملكة والتنظيم التشريعي الحالي لذلك وحتى الجهات والهيئات التي تشرف على تطبيقه بشكل خاص .

المطلب الأول: واقع حماية البيانات في المملكة العربية السعودية

كما قدمنا انه قبل سنوات ليست بالكثير، لم يكن هناك إطار قانوني شامل ينظم حماية البيانات الشخصية في المملكة العربية السعودية. كانت السياسات المتعلقة بالخصوصية تُدار من قبل الجهات بشكل فردي دون وجود تشريعات موحدة أو معايير وطنية ملزمة نتيجة لذلك، كانت البيانات الشخصية عرضة لسوء الاستخدام أو المعالجة غير المنضبطة، خاصة مع

ازدياد الاعتماد على الخدمات الإلكترونية. كما لم يكن لدى الأفراد وعي كافٍ بحقوقهم المتعلقة بحماية بياناتهم، ما خلق فجوة في الثقة بين المستخدمين والجهات التي تتعامل مع معلوماتهم الشخصية.

ولكن شهدت المملكة خلال السنوات الأخيرة تطورًا كبيرًا في مجال حماية البيانات، في ظل التحول الرقمي المتسارع والاعتماد المتزايد على التكنولوجيا في مختلف القطاعات. وقد تم تعزيز هذا الجانب بإصدار نظام حماية البيانات الشخصية في عام 2021، والذي يمثل إطارًا قانونيًا شاملاً لحماية خصوصية الأفراد وتنظيم عمليات جمع ومعالجة البيانات. كما أسندت مسؤولية الرقابة على تطبيق النظام إلى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، التي تعمل على ضمان التزام الجهات بالمعايير الوطنية والدولية لحماية البيانات. هذا التطور يعكس التزام المملكة ببناء بيئة رقمية آمنة وموثوقة تعزز ثقة الأفراد والمستثمرين[1].(الموقع الرسمي للهيئة: https: / /sdaia.gov.sa/)

واعتمدت المملكة العربية السعودية إطارًا قانونيًا شاملًا لدعم التحوّل الرقمي في إنتاج وتقديم الخدمات الحكومية ، ويتوافق هذا الإطار القانوني تمامًا مع التوجّهات السائدة عالميًا، ويضمن توفّر عوامل التمكين الرئيسية للحكومة الإلكترونية ، ويتيح هذا الإطار إنشاء الهوية الرقمية والتوقيع الرقمي والبنية التحتية للمفاتيح العامة التي يُمكن الاستفادة منها في تقديم خدمات كلا القطاعين العام والخاص، ويدعم ذلك اعتماد نظام التعاملات الإلكترونية، ونظام الاتصالات، ونظام التجارة الإلكترونية ، وقد ساهم التحوّل الرقمي بالمملكة في زيادة مستوى الشفافية لدى الحكومة وفيما يتعلق بإنفاق الميزانية، وذلك من خلال المشتريات الإلكترونية والإعلان الإلزامي عن الميزانيات والإنفاق الحكومي سنويًا وذلك على خلفية انتهاج المملكة تعزيز مبدأ اتاحة المعلومات وسهولة الوصول اليها في اهم الجهات الرسمية وغيرها .

المطلب الثاني: التشريعات والجهات المعنية بحماية المعلومات بالمملكة العربية السعودية

قدّمت المملكة العربية السعودية نظامًا جديدًا لحماية البيانات يتماشى بشكل كبير مع المعايير الدولية مثل الـGDPR ، فقد أصدرت المملكة العربية السعودية نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم (م/ 19) في 17 سبتمبر 2021، ودخل حيز التنفيذ في مارس 2023 بعد تعديلات تنظيمية، وهو أول تشريع شامل يُنظّم جمع ومعالجة البيانات الشخصية في المملكة ، وعلى صعيد اخر ادركت المملكة العربية السعودية قيمة البيانات باعتبارها أحد الأصول الوطنية الاستراتيجية التي تسهم في عملية اتخاذ القرار والتحول الاقتصادي والشفافية وانطلاقًا من رؤية 2030، وضعت الحكومة مجموعة شاملة من السياسات واللوائح التي تضمن سهولة الوصل للبيانات المفتوحة لكل الافراد ، وتعتمد على سياسات حوكمة البيانات الوطنية ومعايير إدارة البيانات الوطنية وحماية البيانات الشخصية. وتوضح هذه اللائحة حقوق الأفراد في طلب الوصول إلى البيانات العامة غير المحمية، فضلاً عن مسؤوليات الجهات الحكومية في التعامل مع هذه الطلبات. بالإضافة إلى ذلك، تحدد اللائحة أدوار الهيئة السعودية للبيانات والذكاء الاصطناعي ومركز أدارة البيانات الوطني، والمركز الوطني للمعلومات في إدارة وحماية الوصول إلى المعلومات.

أولاً: نظام حماية البيانات الشخصية في السعودية الحالي2021

كما اوضحنا قد اصدرت المملكة العربية السعودية نظاماً شاملاً لحماية المعلومات الشخصية وتنظيم التعامل فيها ونقلها وحتى استخدامها والنظم أقر عدة مبادئ واهداف تعزز من الحماية التشريعية للمعلومات الشخصية وتتمثل الأهداف الرئيسية لنظام حماية البيانات الشخصية في حماية البيانات الشخصية للأفراد في المملكة العربية السعودية، وضمان احترام الحق في الخصوصية، وتنظيم معالجة البيانات الشخصية وتخزينها ونقلها، ويهدف النظام واللوائح المصاحبة له إلى تهيئة بيئة آمنة لإدارة البيانات من خلال وضع التزامات واضحة للشركات والجهات الأخرى التي تعالج البيانات الشخصية.

ويتمتّع نظام حماية البيانات الشخصية في المملكة (PDPL) بنطاق واسع ويؤثر على مجموعة كبيرة من الجهات والأفراد سواء داخل المملكة أو خارجها ، فينطبق النظام على الجهات المسؤولة عن معالجة البيانات في المملكة، وكذلك على الجهات خارج المملكة التي تعالج

البيانات الشخصية للأفراد فيها، ويعني هذا النطاق الواسع أن أي جهة تعالج البيانات الشخصية للأفراد في المملكة ملزمة بالامتثال للنظام واللوائح، بغض النظر عن مكان المعالجة ،وقد تم تصميم النظام لضمان إدارة البيانات الشخصية بشكل مسؤول وآمن، بما يتماشى مع المعايير العالمية، مع مراعاة الخصوصية والسياق المحلي للمملكة ، والذ بدوره خصص باب وموجب نظام حماية البيانات الشخصية في المملكة، يمكن أن تكون العقوبات المالية كبيرة في حال عدم الامتثال

ولقد اوضح النظام حقوق الافراد تجاه معلوماتهم الشخصية بشكل يشمل جميع التعاملات مع المعلومات الشخصية من العلم ولاطلاع والتعديل والنقل كالاتي:

*الحق في العلم: يشمل ذلك إحاطته علماً بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها، وهوية من يجمع البيانات الشخصية وعنوان مرجعه، والجهة أو الجهات التي سيُجرى إفصاح البيانات الشخصية لها وصفتها وما إذا كانت البيانات الشخصية ستنقل أو سيفصح عنها أو ستعالج خارج المملكة، والآثار والأخطار المحتملة التي تترتب على عدم إتمام إجراء الجمع، بالإضافة إلى حقوق صاحب البيانات الشخصية.

*الحق في الوصول إلى البيانات الشخصية: ويشمل ذلك طلب نسخة من بياناته الشخصية المتوفرة لدى جهة التحكم بصيغة مقروءة وواضحة.

*الحق في طلب تصحيح البيانات الشخصية: ويشمل ذلك طلب تصحيح البيانات الشخصية المتوفرة لدى جهة التحكم، أو إتمامها، أو تحديثها.

*الحق في طلب إتلاف البيانات الشخصية: يحق لصاحب البيانات الشخصية طلب إتلاف بياناته الشخصية المتوفرة لدى جهة التحكم مما انتهت الحاجة إليه منها.

*الحق في الرجوع عن الموافقة على معالجة البيانات الشخصية: يمكن لصاحب البيانات الشخصية الرجوع عن الموافقة على معالجة بياناته الشخصية في جميع الأحوال وفي أي وقت فيما عدا الأحوال المنصوص عليها في نظام حماية البيانات الشخصية ولائحته التنفيذية.

وبداية من المادة الثامنة للنظام تم تقنين عدة التزامات على عاتق الجهات الرسمية او الجهات التي قد تتحكم في بيانات الافراد الشخصية من الحفظ والمعالجة والنشر والقيود الواردة على كل منها فيما يلي

تعرض النظام للحالات التي لا تخضع فيها معالجة البيانات الشخصية للموافقة في نظام حماية البيانات الشخصية في المملكة ولخصها في الاتي:

-عندما تُحقق المعالجة مصلحة متحققة لصاحب البيانات وكان الاتصال به متعذراً أو كان من الصعب تحقيق ذلك.

-عندما تكون المعالجة بمقتضى نظام آخر أو تنفيذاً لاتفاق سابق يكون صاحب البيانات الشخصية طرفاً فيه.

-إذا كانت جهة التحكم جهة عامة، وكانت تلك المعالجة مطلوبة لأغراض أمنية أو لاستيفاء مُتطلبات قضائية.

مع مراعاة ضرورة موافقة صاحب البيانات قبل أي استخدام لها فوفقًا للنظام، لا يجوز معالجة البيانات الشخصية أو تعديل الغرض من معالجتها إلا بعد الحصول على موافقة صاحب البيانات، باستثناء الحالات المنصوص عليها في النظام وتُحدد اللوائح شروط الموافقة، والأحوال التي يجب أن تكون فيها الموافقة كتابية، بالإضافة إلى الشروط والأحكام المتعلقة بالحصول على الموافقة من الولي الشرعي إذا كان صاحب البيانات ناقصًا أو عديم الأهلية. كما يُسمح لصاحب البيانات في جميع الحالات بسحب الموافقة في أي وقت، وتحدد اللوائح الضوابط اللازمة لهذه العملية.

أيضاً تناول النظام شروط تقييد الوصول للمعلومات الشخصية في مادته التاسعة حيث نص على انه " يجوز لجهة التحكم تقييد حق الوصول إلى البيانات الشخصية في احوال محددة مسبقاً منها إذا كان التقييد لأسباب أمنية او لاستيفاء متطلبات قضائية.[1]

كما حدد مدد لممارسة حق الوصول فأجاز لجهة التحكم بالمعلومات تحديد مدد لممارسة حق الوصول إلى البيانات الشخصية، وتتولى الجهة المختصة تحديد المدة المناسبة لذلك. كما يجب على جهة التحكم أن تمتنع عن تمكين صاحب البيانات الشخصية من الوصول إليها إذا تحقق أي من الأحوال المنصوص عليها في الفقرات (1) إلى (6) من المادة[1].

ووضع حدود للجهات في جمع البيانات الشخصية من غير صاحب البيانات مباشرة وحظر على أي جهة جمع البيانات الا في الاحوال التالية:

- إذا وافق صاحب البيانات الشخصية على ذلك.
- إذا كانت البيانات الشخصية متاحة للعموم أو تم جمعها من مصدر متاح للجميع.
- إذا كانت جهة التحكم جهة عامة وكان جمع البيانات مطلوبًا لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء متطلبات قضائية وفقًا للأحكام المنصوص عليها في اللوائح.
- إذا كان التقيد بهذا الحظر قد يُلحق ضررًا بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية.
- إذا كان جمع البيانات الشخصية أو معالجتها ضروريًّا لحماية الصحة أو السلامة العامة أو حماية حياة أفراد معينين.
- إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تسمح بتحديد هوية صاحب البيانات بشكل مباشر أو غير مباشر.

وأوجب أن يكون الغرض من جمع البيانات الشخصية ذا علاقة مباشرة بأغراض جهة التحكم وألا يتعارض مع أي حكم مقرر نظامًا. كما يجب أن تتماشى طرق جمع البيانات ووسائلها مع القوانين، وأن تكون ملائمة لظروف صاحب البيانات ومباشرة وواضحة وآمنة، وخالية من أساليب الخداع أو الابتزاز .أيضًا، يجب أن يكون محتوى البيانات مقتصرًا على الحد الأدنى اللازم لتحقيق الغرض، مع عدم تضمين ما يؤدي إلى معرفة صاحبها بشكل

محدد. وإذا أصبحت البيانات التي تم جمعها غير ضرورية لتحقيق الغرض منه، فعلى جهة التحكم التوقف عن جمعها وإتلاف ما سبق جمعه فورًا[1].

ايضاً المتطلبات التي يجب على جهة التحكم اتباعها عند جمع البيانات الشخصية من صاحبها مباشرة وضع لها حدود متعددة ومنها الاتي:

- المسوغ النظامي أو العملي لجمع بياناته الشخصية.
- الغرض من جمع بياناته الشخصية، وما إذا كان جمعها إلزاميًا أم اختياريًا، وإبلاغه بأن بياناته لن تعالج لاحقًا بصورة تتنافى مع الغرض من جمعها أو في غير الأحوال المنصوص عليها في المادة (العاشرة) من النظام.
- هوية من يجمع البيانات الشخصية وعنوان مرجعه عند الاقتضاء، ما لم يكن جمعها لأغراض أمنية.
- الجهة أو الجهات التي سيفصح لها عن البيانات الشخصية، وصفتها، وما إذا كانت البيانات ستنقل أو تُعالج خارج المملكة.
- الآثار والأخطار المحتملة التي تترتب على عدم إتمام جمع البيانات الشخصية.
- حقوقه المنصوص عليها في المادة (الرابعة) من النظام.
- العناصر الأخرى التي تحددها اللوائح بحسب طبيعة النشاط الذي تمارسه جهة التحكم.

وحدود الافصاح عن البيانات الشخصية والتي حددها النظام في حالة موافقة صاحب البيانات الشخصية على الإفصاح، وإذا كانت البيانات الشخصية قد جرى جمعها من مصدر متاح للعموم، وإذا كانت الجهة التي تطلب الإفصاح جهة عامة، وذلك لأغراض أمنية، وإذا كان الإفصاح ضروريًّا لحماية الصحة، أو السلامة العامة، أو حماية حياة فرد، أو أفراد معينين، أو حماية صحتهم.2

اما عن حدود السماح بالاحتفاظ بالبيانات او اتلافها من قبل جهة التحكم والجمع فقد سمح النظام الاحتفاظ بالبيانات الشخصية في حالتين:

- إذا توافر مسوغ نظامي يوجب الاحتفاظ بها لمدة محددة، وفي هذه الحالة يجب إتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول.
- إذا كانت البيانات الشخصية مرتبطة بقضية منظورة أمام جهة قضائية وكان الاحتفاظ بها مطلوبًا لهذا الغرض، فيجب إتلافها بعد استكمال الإجراءات القضائية الخاصة بالقضية.[1]

والتي نظمتها اللائحة في مادتها **المادة الثامنة: الحق في طلب إتلاف البيانات الشخصية بالنص على** ان لجهة التحكم إتلاف البيانات الشخصية في أي من الأحوال الآتية:

أ-تنفيذاً لطلب صاحب البيانات الشخصية.

ب-إذا لم تعد البيانات الشخصية ضرورية لتحقيق الغرض الذي جمعت من أجله.

ج-إذا عدل صاحب البيانات الشخصية عن موافقته على جمع بياناته الشخصية، وكانت الموافقة هي المسوغ النظامي الوحيد للمعالجة.

د-إذا علمت أن البيانات الشخصية تجرى معالجتها بطريقة مخالفة للنظام.

1. على جهة التحكم عند إتلافها للبيانات الشخصية القيام بالآتي:

أ-اتخاذ الإجراءات الملائمة لإشعار الجهات الأخرى التي أفصحت لها جهة التحكم عن البيانات الشخصية ذوات الصلة، وطلب إتلافها.

ب-اتخاذ الإجراءات الملائمة لإشعار الأشخاص الذين تم الإفصاح لهم عن البيانات الشخصية بأي وسيلة كانت، وطلب إتلافها.

ج-إتلاف كافة النسخ المتعلقة بالبيانات الشخصية المخزنة في أنظمة جهة التحكم، بما في ذلك النسخ الاحتياطية، على أن تراعى المتطلبات النظامية ذوات العلاقة بهذا الشأن.

2. لا يخل ما ورد في هذه المادة ما نصت عليه المادة (الثامنة عشرة) من النظام والمتطلبات النظامية التي تقرها الجهات المختصة ذوات العلاقة.

وقصرت اللائحة التنفيذية للنظام الضوابط والإجراءات المحددة في اللوائح بشأن معالجة البيانات الصحية لحماية خصوصية أصحابها بما في ذلك الملفات الطبية، على أقل عدد ممكن من الموظفين أو العاملين وبالقدر اللازم فقط لتقديم الخدمات الصحية الضرورية، وتقييد إجراءات وعمليات معالجة البيانات الصحية إلى أقل عدد ممكن من الموظفين والعاملين اللازمين لتقديم الخدمات الصحية أو توفير برامج التأمين الصحي[1].

اما عن حماية البيانات خارج إقليم المملكة من نقل ومعالجة فقد تناولها النظام في مادته التاسعة والعشرون بالحماية وعدم اجازة نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارج المملكة، إلا في حالات الضرورة القصوى لحماية حياة صاحب البيانات أو مصالحه الحيوية، أو للوقاية من عدوى مرضية. يسمح بالنقل أو الإفصاح في الحالات التالية[2]:

- إذا كان ذلك تنفيذاً لالتزام بموجب اتفاقية تكون المملكة طرفاً فيها.
- إذا كان لخدمة مصالح المملكة.
- إذا كان لأغراض أخرى وفقاً لما تحدده اللوائح، بعد التحقق من عدة شروط.

اما عن متطلبات السجلات التي يجب على جهة التحكم الاحتفاظ فقد تناولتها المادة الحادية والثلاثون من نظام حماية البيانات الشخصية على ان تحتفظ جهة التحكم بسجلات لمدة تحددها اللوائح لأنشطة معالجة البيانات الشخصية بحسب طبيعة النشاط الذي تمارسه جهة التحكم؛ لتكون متاحة عندما تطلبها الجهة المختصة، والتي حددتها اللائحة التنفيذية بأنها أثناء فترة استمرار عمليات معالجة البيانات الشخصية، إضافة إلى خمس سنوات تبدأ من تاريخ انتهاء نشاط معالجة البيانات الشخصية..[3]

ونص النظام على المخالفات وعقوباتها لكافة الالتزامات الواردة بالنظام وحددها في الاتي:

- ان كل من أفصح عن بيانات حساسة أو نشرها مخالفًا أحكام النظام: يعاقب بالسجن مدة لا تزيد على (سنتين) وبغرامة لا تزيد على (ثلاثة ملايين) ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية.
- وكل من خالف أحكام المادة (التاسعة والعشرين) من النظام: يعاقب بالسجن مدة لا تزيد على (سنة) وبغرامة لا تزيد على (مليون) ريال، أو بإحدى هاتين العقوبتين.

وتختص النيابة العامة بمهمة التحقيق، والادعاء أمام المحكمة المختصة عن المخالفات المنصوص عليها في هذه المادة وتولى المحكمة المختصة النظر في الدعاوى الناشئة من تطبيق هذه المادة وإيقاع العقوبات المقررة،[1] ويجوز للمحكمة المختصة مضاعفة عقوبة الغرامة في حالة العود، حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد2، ورفع حد الغرامة غرامات مالية تصل إلى 5 ملايين ريال سعودي[3]، وأحيانًا عقوبات جزائية في حال انتهاك البيانات عمدًا أو إساءة استخدامها.

لائحة نظام حماية البيانات الشخصية السعودية

تُعد اللائحة التنفيذية لنظام حماية البيانات الشخصية الصادرة عام 2023م تفصيلًا مهمًا لأحكام النظام، وتشمل عدداً من المبادئ والإجراءات:

-الحقوق الأساسية لصاحب البيانات من الحق في العلم: يجب إبلاغ الفرد عند جمع بياناته عن هوية الجهة المتحكمة، وأغراض الجمع، ومدة الاحتفاظ، وحقوقه القانونية [1]، الى الحق في الوصول والتصحيح [2]، الى الحق في الإتلاف. [3]

-ضوابط الموافقة من أن تكون الموافقة صريحة، حرة، موثقة، ولا يجوز الحصول عليها بوسائل خادعة (المادة 11)، الى حق صاحب البيانات العدول عن الموافقة في أي وقت (المادة 12).

-وتسرب البيانات والإشعارات وإلزام الجهة إشعار الهيئة المختصة خلال 72 ساعة من علمها بأي تسرب بيانات، وإخطار الأفراد المتضررين بذلك. (المادة 24)

عقوبات ارتكاب مخالفات قانون حماية البيانات الشخصية

بالاعتماد على نظام حماية البيانات الشخصية واللائحة التنفيذية، فقد وردت مخالفات قانون حماية البيانات الشخصية والعقوبات المقررة لها فحدد تشكيل بقرار من رئيس الجهة المختصة، لجنة (أو أكثر) لا يقل عدد أعضائها عن (ثلاثة)، ويسمى أحدهم رئيساً، ويكون من بينهم مستشار شرعي أو نظامي؛ تتولى النظر في المخالفات وإيقاع عقوبة الإنذار أو الغرامة المنصوص عليها بالنظام، وذلك بحسب نوع المخالفة المرتكبة وجسامتها ومدى تأثيرها، على أن يعتمد قرار اللجنة رئيس الجهة المختصة أو من يفوضه بذلك. ويصدر رئيس الجهة المختصة -بقرار منه- قواعد عمل اللجنة، وتحدد فيها مكافآت أعضائها.

1. يحق لمن صدر ضده قرار من اللجنة المنصوص عليها في الفقرة (2) من هذه المادة التظلم منه أمام المحكمة المختصة.

-السجن لمدة لا تزيد على سنتين لمن نشر أو أفشى بيانات شخصية حساسة أو انتهك خصوصية الأفراد بقصد الإضرار أو تحقيق مكاسب شخصية حس نص المادة 35 من النظام.

-غرامة مالية لا تتجاوز 3٬000٬000 ريال سعودي، وتُضاعف في حال تكرار المخالفة دون أن تتجاوز الضعف نص المادة 35 من النظام.

-فرض غرامة إدارية تصل إلى 5٬000٬000 ريال سعودي على أي مخالفة لم يُحدد لها عقوبة جنائية، ويجوز مضاعفتها عند العود حسب المادة 36 من النظام.

-الإنذار الإداري من قبل لجنة مختصة تصدر بقرار من رئيس الهيئة نص المادة 36 من النظام.

-مساءلة تأديبية لموظفي الجهات العامة المخالفين، وفقًا لأنظمة الخدمة المدنية أو التأديب حسب المادة 39 من النظام.

-حظر تصوير أو نسخ الوثائق الرسمية التي تُحدد هوية الفرد، ما لم يكن ذلك بطلب من جهة حكومية أو تنفيذًا لنظام حسب المادة 31 من اللائحة.

-إلزام جهة التحكم بإشعار الهيئة المختصة خلال 72 ساعة من علمها بتسرب البيانات، وإشعار الأفراد المتضررين؛ ويُعد عدم الإشعار مخالفة تعرضها للمساءلة نص المادة 24 من اللائحة.

-جواز نشر العقوبة على نفقة المخالف في وسيلة إعلامية مناسبة إذا رأت الجهة المختصة أن للنشر أثرًا رادعًا المادة 38 من النظام.

-أحقية المتضرر في رفع دعوى تعويض أمام المحكمة المختصة والمطالبة بجبر الضرر المادي أو المعنوي حسب المادة 44 من النظام.

الجهات والهيئات:

الهيئة السعودية للبيانات والذكاء الاصطناعي:

الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) هي الجهة المختصة في المملكة بالبيانات والذكاء الاصطناعي وتشمل: البيانات الضخمة، وهي المرجع الوطني في كل ما

يتعلق بهما من تنظيم وتطوير وتعامل، وهي صاحبة الاختصاص الأصيل في كل ما يتعلق بالتشغيل والأبحاث والابتكار في قطاع البيانات والذكاء الاصطناعي[1].

وانطلقت سدايا لتكون حجر الأساس في تمكين الطاقات الوطنية الشابة عبر ابتكار حلول رقمية تساهم في مواجهة جميع التحديات وبناء مستقبل قائم على البيانات والذكاء الاصطناعي، وتحقيق أهداف رؤية السعودية 2030.والتى وضعت لها اهداف استراتيجية معلنة رسمياً ومنها:

-مواصلة تحديث برنامج البيانات الوطنية والذكاء الاصطناعي بما يتوافق مع المبادئ الرئيسية.

-تنفيذ برنامج البيانات والذكاء الاصطناعي على الصعيد الوطني.

-توجيه الجهات التابعة للهيئة بشأن تنفيذ أجندة البيانات والذكاء الاصطناعي.

-زيادة الوعي العام بشأن إنجازات المملكة العربية السعودية في مجال البيانات والذكاء الاصطناعي.

-زيادة مساهمة البيانات والذكاء الاصطناعي في تحقيق أهداف رؤية 2030.

-زيادة استفادة الجهات الحكومية كافة من أجندة البيانات والذكاء الاصطناعي.

-دعم تحقيق الأهداف الاستراتيجية في الجهات التابعة للهيئة فيما يتعلق بالتشريعات والتشغيل والابتكار.

-تعزيز صورة المملكة العربية السعودية باعتبارها دولة رائدة عالمياً في مجال البيانات والذكاء الاصطناعي.

سياسة الخصوصية بالمنصة الوطنية:

والتي تنص على انها "نلتزم بحماية خصوصية وسرية البيانات الشخصية وعدم الاطلاع عليها دون موافقة شخصية، إلا في الحالات القانونية التي يتطلبها النظام للإفصاح عنها.

[1] أنشئت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) بموجب الأمر الملكي رقم (أ/ 471) وتاريخ 1440/12/29هـ، وترتبط مباشرة برئيس مجلس الوزراء، ويرتبط بها تنظيمياً: مكتب إدارة البيانات الوطنية، والمركز الوطني للذكاء الاصطناعي، ومركز المعلومات الوطني، وتتمتع الهيئة بالشخصية الاعتبارية وبالاستقلال الإداري والمالي، ومقرها الرئيس في مدينة الرياض.

https://sdaia.gov.sa/

 ISBN: 978-9922-8178-3-5

نقوم بتأمين المعلومات التي تقدمها عن طريق تخزينها على خوادم الحاسب في بيئة آمنة خاضعة للرقابة ومحمية من الوصول أو الاستخدام أو الكشف غير المصرح به، كما نبقي على ضمانات إدارية وتقنية ومادية كافية للحماية من الوصول، أو الاستخدام، أو التعديل أو الكشف غير المصرح به للبيانات الشخصية الخاضعة لسيطرتنا.

الخـاتـمة

لقد شهدت حماية المعلومات الشخصية تطورًا كبيرًا على المستوى العالمي، مدفوعًا بتزايد الاعتماد على التكنولوجيا الرقمية وانتشار المعاملات الإلكترونية، مما استدعى سن تشريعات تنظم جمع البيانات واستخدامها، وقد كانت اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) من أبرز النماذج التنظيمية، حيث أرست مبادئ شاملة لحماية الخصوصية وأصبحت مرجعًا عالميًا. كما تبنّت العديد من الدول الأخرى أطرًا قانونية مشابهة، مدعومة بتوصيات من منظمات دولية مثل الأمم المتحدة ومنظمة التعاون والتنمية الاقتصادية(OECD) ، ومجلس اوروبا، ما يعكس إدراكًا متزايدًا بأهمية حماية البيانات كحق أساسي من حقوق الإنسان.

وعلى الجانب العربي، جاءت جهود المملكة العربية السعودية لتواكب هذا التوجه العالمي، حيث طورت منظومتها القانونية بما يتماشى مع التحول الرقمي السريع ورؤية السعودية 2030، ويعد نظام حماية البيانات الشخصية، خطوة محورية نحو تعزيز خصوصية الأفراد وتنظيم معالجة البيانات. كما يعكس هذا النظام التزام المملكة بتوفير بيئة رقمية آمنة ومتوازنة تحمي الحقوق وتدعم الابتكار، وانشاء جهات خاصة لتولي تنفيذ النظام مثل الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) يشهد على حرص المملكة الشديد على ضمان حيادية ملف حماية المعلومات الشخصية، ومن المتوقع أن تسهم التطورات المستمرة في الأنظمة الرقابية وآليات الإنفاذ في ترسيخ الثقة الرقمية، ودعم التحول الرقمي المستدام القائم على الشفافية والمساءلة وحماية المعلومات.

النتائـــج

ولقد خرجنا من الدراسة بعدة نتائج واقعية كتالي:

1- ترسّخ المملكة العربية السعودية إطارًا قانونيًا متينًا لحماية البيانات الشخصية، يعزز الثقة الرقمية، ويدعم تحولها نحو اقتصاد رقمي مبتكر ومتوافق مع المعايير العالمية.

2- يضمن النظام حقوق أصحاب البيانات بشكل واضح للأفراد كالاطلاع، والتعديل، والحذف، وسحب الموافقة، مع إلزام المؤسسة بالتبليغ عن خروقات البيانات حتى للمتوفين إذا كان ذلك ممكنًا تحديدهم

3- وجود هيئة مستقلة متخصصة تُشرف على تنفيذ القانون، وتتمتع بصلاحيات قوية تشمل التحقيق، التفتيش، إصدار التحذيرات، وفرض الغرامات وهي هيئة البيانات والذكاء الاصطناعي (SDAIA)

4- إقرار الغرامات والعقوبات الصارمة كنشر بيانات حساسة يعرض المتورطين للسجن حتى سنتين أو غرامة تصل إلى 3 مليون ريال، وتتضاعف في العود ومخالفات عامة يُفرض بشأنها تحذير أو غرامة تصل إلى 5 مليون ريال، وتتضاعف كذلك في حالات العود.

5- تعزيز الشفافية والمساءلة الحكومية حيث أتاحت الجهات الحكومية، بما فيها الوزارات والهيئات، آلاف مجموعات البيانات عبر منصة البيانات المفتوحة الوطنية، مما عزز الشفافية وساعد المواطنين والمهتمين ذوات العلاقة.

التوصيـات

1- تعزيز التوعية المجتمعية عن طريق زيادة الحملات التوعوية للأفراد والمؤسسات حول حقوقهم وواجباتهم في حماية البيانات الشخصية، وآليات التبليغ حال حدوث أي تعدى على البيانات الشخصية

2- تطوير القدرات البشرية والتقنية عن طريق تدريب موظفي الجهات الحكومية والقطاع الخاص المعنى بحماية البيانات

3- تعزيز التعاون بين الجهات الرقابية وتشجيع التنسيق بين هيئة البيانات والذكاء الاصطناعي (SDAIA)، والهيئة الوطنية للأمن السيبراني، وغيرها من الجهات ذات العلاقة لضمان تكامل الجهود الرقابية والوقائية.

المصادر والمراجـــع

الكتب العلمية:

1. مروة زين العابدين صالح، 2016، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، دار المنهل للنشر
2. خالد ممدوح إبراهيم، 2025، التحول الرقمي وحماية البيانات والمعلومات، دار الفكر الجامعي، الإسكندرية، مصر
3. منال البلقاسي ،2025، قوانين أمن البيانات، دار مصر للنشر والتوزيع
4. خالد حسن احمد، 2020، الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية، دار الكتب والدراسات العربية.

المجلات العلمية:

1. رؤى سعد القرني (2021) الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، المجلد 6، العدد 1
2. العنزي، سعد (2021) التنظيم القانوني لحق الاطلاع على المعلومات والوثائق الإدارية. مجلة كلية القانون الكويتية العالمية، 3 (35)
3. صالح عوض منصور الجعيد، 2025، الحماية الجزائية لمعالجة البيانات الشخصية في النظام السعودي ، مجلة الاندلس للعلوم الانسانية والاجتماعية العدد –114 المجلد 12 –فبراير 2025م
4. الرشيدي، خالد وكلايف، ووكر .(2024) قانون حرية المعلومات الكويتي: بناء الحكم الدستوري (The Kuwaiti Freedom of Information Act: the Construction of Constitutional Governance). المجلة العالمية للقانون المقارن، 1(13) https://www.researchgate.net/publication/380664205_The_Kuwaiti_Freedom_of_Information_Act_the_Construction_of_Constitutional_Governance
5. منصور، ماجدة عبد الشافي محمد الهادي خالد. (2023). الرقمنة كآلية لإعادة هندسة المرافق العامة للحد من الفساد الإداري .مجلة الدراسات القانونية والاقتصادية، مج9أع 1 http://search.mandumah.com/Record/1453171
6. محمد محمد القطب مسعد، 2018، الحماية المدنية للشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال، مجلة الجديدة والأصلية الإقتصادية (المنصورة) المجلد 8، العدد 67، ديسمبر 2018، https://journals.ekb.eg/article_156167.html
7. محمد احمد المعداوي،2018، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مجلة الشريعة والقانون، جامعة طنطا، العدد 33 الجزء الرابع

مقالات وأخبار رسمية:

1. مبادئ الأمم المتحدة العالمية بشأن سلامة المعلومات: مبادئ الأمم المتحدة العالمية بشأن سلامة المعلومات | الأمم المتحدة
2. زعنون، عبد الرفيع .(2024) فعلية الحق في الحصول على المعلومات بالمنطقة العربية: المكاسب والإخفاقات، رواق عربي : https://cihrs-rowaq.org/the-right-to-information-access
3. مقال بعنوان (تطبيق قانون الحصول على المعلومات يواجه تحديات بالجملة في المغرب)، 2025، الجريدة الإخبارية "هيس برس"، لينك المقال: https://www.hespress.com/%D8%AA%D8%B7%D8%A8%D9%8A
4. زغلول، جغدود .(2021) الحق في الحصول على المعلومة ودورها في مكافحة الفساد .مجلة الباحث للدراسات الأكاديمية، 8 (2):https://doi.org/10.59791/efas.v8i2.854
5. عبد الله المهيدب وأخرين، 2022، حماية البيانات وخصوصية إنترنت الأشياء للرعاية الصحية، مجلة العلوم التطبيقية المجلد 12، العدد الرابع https://www.mdpi.com/2076-3417/12/4/1927

المواقع الرسمية:

1. مشروع نزاهة بالأردن: About Nazaha – nazaha-jo
2. الموقع الرسمي لشبكة الكويت للمعلومات، https://cait.gov.kw/ar/projects/kuwait-information-network/
3. وزارة التعليم السعودية، الموقع الرسمي: https://moe.gov.sa/ar/knowledgecente
4. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا): https://sdaia.gov.sa
5. هيئة الخبراء بمجلس الوزراء: https://laws.boe.gov.sa/boelaws
6. منظمة التعاون الاقتصادي والتنمية: https://www.dfat.gov.au/
7. مجلس اوروبا :https://www.coe.int
8. مجلس حماية البيانات الاوروبي : https://european-union.europa.eu/
9. المنصة الوطنية السعودية: https://my.gov.sa/

القوانين والأنظمة:

1. اللائحة التنفيذية لنظام حماية المعلومات الشخصية: https://dgp.sdaia.gov.sa/
2. نظام حماية البيانات الشخصية 1443 هـ، بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ https://laws.boe.gov.sa/boelaws/laws/lawdetails
3. سياسة مشاركة بيانات الجهات الحكومية: سياسة مشاركة البينات بين الجهات الحكومية فقطpdf.
4. سياسات حوكمة البيانات الوطنية: PoliciesAr.pdf