

العنوان باللغة العربية
حماية الخصوصية في الوزارات الحكومية
وزارة البيئة والمياه والزراعة أنموذجاً

إعداد الطالب/
محمد سعيد علي الشريف

إشراف/
د. الفیصل عبد الحمید
د. فايز جراد

العام الدراسي:
2026

فهرس المحتويات:

المحتويات

1.....	فهرس المحتويات:
3.....	قائمة الجداول :
3.....	فهرس الأشكال:
4.....	المقدمة:
5.....	-مشكلة الدراسة.
6.....	-أهمية الدراسة.
7.....	-أهداف الدراسة.
8.....	-تساؤلات الدراسة.
9.....	- فروض الدراسة.
10.....	-النظرية العلمية المتبعة لإعداد البحث.
11.....	الفصل الثاني
11.....	الدراسات السابقة.
12.....	مقدمة.
13.....	-الدراسات السابقة.
16.....	-الإطار النظري.
24.....	الفصل الثالث
24.....	منهجية الدراسة.
25.....	-المنهجية وطرق البحث.
26.....	مجتمع البحث.
27.....	حدود البحث.
29.....	الفصل الرابع
29.....	النتائج والتوصيات.
29.....	مقدمة.
30.....	تحليل البيانات.
34.....	المراجع.
35.....	-المراجع العربية.
35.....	-المراجع الأجنبية.
36.....	الملاحق.

قائمة الجداول :

فهرس الأشكال:

المقدمة:

تشكل حماية الخصوصية والبيانات الشخصية في العصر الرقمي أحد أبرز التحديات التي تواجه الحكومات والمؤسسات على اختلاف طبيعتها، لا سيما مع التوسع المتسارع في استخدام التقنية لتقديم الخدمات العامة، وما رافق ذلك من تحول جوهري في طريقة جمع البيانات ومعالجتها وتخزينها وتبادلها بين الجهات المختلفة. وقد ازدادت أهمية هذا الموضوع مع تنامي الوعي المجتمعي بحقوق الأفراد في التحكم بمعلوماتهم الشخصية، ومع تصاعد المخاطر المرتبطة بإساءة استخدام البيانات أو تسريبها أو معالجتها دون سند نظامي.

وقد أدركت المملكة العربية السعودية أهمية هذا الملف في وقت مبكر ضمن مسيرة التحول الرقمي التي تركز عليها رؤية المملكة 2030 ، فأصدرت نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم م 19/ وتاريخ 9/2/1443 هـ، ثم أجرت عليه تعديلات جوهرية بموجب المرسوم الملكي رقم م 148/ وتاريخ 5/9/1444 هـ، ليصبح النظام نافذاً وواجب التطبيق اعتباراً من 14 سبتمبر 2024م، بعد فترة انتقالية أتيحت للجهات الحكومية والخاصة لمواءمة أوضاعها. ويؤسس هذا النظام لإطار تنظيمي شامل يحكم جمع البيانات الشخصية ومعالجتها، ويثبت مبادئ الشفافية والمشفرة ويمنح أصحاب البيانات حقوقاً واضحة، في مقابل التزامات محددة تقع على عاتق الجهات التي تعالج هذه البيانات.

وتُعد الوزارات الحكومية من أكثر الجهات تعاملًا مع البيانات الشخصية للمواطنين والمقيمين، نظرًا لطبيعة الخدمات التي تقدمها والتي تستلزم جمع معلومات دقيقة عن المستفيدين لأغراض إصدار التراخيص والتصاريح وتقديم الدعم واتخاذ القرارات التنظيمية. وتمثل وزارة البيئة والمياه والزراعة نموذجًا بارزًا في هذا السياق، إذ تتعامل يوميًا مع بيانات شخصية متنوعة تخص المزارعين وملاك الحيازات الزراعية وأصحاب تراخيص الآبار والمنشآت البيئية والمشاركين في خدمات المياه، عبر منصاتها الإلكترونية المتعددة التي تقدم من خلالها عشرات الخدمات الرقمية.

وانطلاقًا مما سبق، تسعى هذه الدراسة إلى تحليل واقع تطبيق متطلبات حماية الخصوصية في الوزارات الحكومية السعودية، من خلال دراسة حالة تطبيقية على وزارة البيئة والمياه والزراعة، بهدف الوقوف على مواطن القوة والقصور في الممارسة الفعلية، ومقارنتها بالمتطلبات النظامية، وتقديم توصيات عملية تسهم في تعزيز منظومة حماية البيانات في القطاع الحكومي بصفة عامة.

مشكلة الدراسة.

على الرغم من صدور نظام حماية البيانات الشخصية في المملكة العربية السعودية ودخوله حيز التنفيذ الفعلي، ومن الجهود الملموسة التي تبذلها الجهات الحكومية للامتثال لمتطلباته، إلا أن تطبيق هذا النظام على أرض الواقع لا يزال يواجه عددًا من التحديات المرتبطة بالبنية التنظيمية والتقنية والثقافة المؤسسية داخل الوزارات. وتتجلى مشكلة الدراسة في وجود فجوة محتملة بين ما تنص عليه التشريعات من مبادئ وضمانات لحماية البيانات الشخصية، وبين واقع التطبيق الفعلي داخل الجهات الحكومية، ومنها وزارة البيئة والمياه والزراعة التي تُعد من أكثر الوزارات تعاملًا مع البيانات الشخصية الحساسة للمزارعين وملاك الحيازات وأصحاب التراخيص.

ومن هنا تسعى هذه الدراسة إلى الإجابة عن التساؤل الرئيس التالي :ما واقع حماية الخصوصية والبيانات الشخصية في الوزارات الحكومية السعودية، مع التطبيق على وزارة البيئة والمياه والزراعة؟

-أهمية الدراسة-

تسليط الضوء على مشكلة فرضت نفسها مع الانفجار التقني والمعلوماتي فلكل تطور ايجابيات وسلبيات فلا بد من ايجاد حل للسلبيات للحصول على جل فائدة التطور المعلوماتي. ومن سلبيات التقنية الحديثة سهولة الوصول لمعلومات خاصة بطرق سهلة لم يكن المتلصصين او اصحاب النوايا السيئة يحلمون ان تكون بهذه السهولة. وتوجد المشكلة لعدة أسباب اما لنقص تجهيزات الجهة التي يتم التعامل معها تقنيا او لعدم تدريب الكادر البشري في الجهة التي تقدم الخدمة او لجهل المستفيد نفسه بالتقنية ومخاطرها.

ولان البيانات تنقسم لعدة اقسام اما ان تكون سرية او عادية او خاصة وفي اقل احوالها لا يجب ان يتم الاطلاع عليها الا بموافقة صاحب الشأن.

وعليه يجب على الجهات المقدمة للخدمات الاستعداد تقنيا مع تدريب الكوادر البشرية العاملة بها وتنقيف المستفيد عبر الاعلانات والدورات والرسائل العامة.

-أهداف الدراسة-

- التعرف على المفاهيم الأساسية المرتبطة بالخصوصية وحماية البيانات الشخصية وتطورها الفكري والتشريعي.
- تحليل الإطار التشريعي والمؤسسي لحماية البيانات الشخصية في المملكة العربية السعودية.
- دراسة واقع تطبيق وزارة البيئة والمياه والزراعة لمتطلبات حماية الخصوصية بوصفها أنموذجاً للوزارات الحكومية.
- تحديد أوجه التوافق والفجوات بين الممارسة الفعلية للوزارة والمتطلبات النظامية لحماية البيانات.
- الوقوف على أبرز التحديات المؤسسية والتقنية والبشرية التي تواجه تطبيق حماية الخصوصية حكومياً.
- تقديم توصيات عملية قابلة للتطبيق تسهم في تعزيز منظومة حماية البيانات الشخصية في الجهات الحكومية

تساؤلات الدراسة

1. ما المقصود بمفهوم الخصوصية والبيانات الشخصية، وما أهمية حمايتهما في القطاع الحكومي؟
2. ما الإطار التشريعي والمؤسسي الناظم لحماية البيانات الشخصية في المملكة العربية السعودية؟
3. ما آليات وزارة البيئة والمياه والزراعة المعلنة في حماية البيانات الشخصية لمستفيديها؟
4. ما مدى اتساق السياسات والإجراءات المطبقة في الوزارة مع متطلبات نظام حماية البيانات الشخصية؟
5. ما أبرز التحديات التي تواجه الوزارة في تطبيق متطلبات حماية الخصوصية؟
6. ما السبل والآليات المقترحة لتعزيز حماية الخصوصية في الوزارة وبقية الجهات الحكومية؟

- فروض الدراسة

- الفروض الصّفرية (Null Hypotheses)
النفي الفرض الأول: "لا يوجد أثر ذو دلالة إحصائية لتطبيق معايير الأمن السيبراني على مستوى حماية خصوصية بيانات المواطنين في الوزارات الحكومية".
الفرض الثاني: "لا توجد فروق ذات دلالة إحصائية في مستوى الوعي بحماية الخصوصية بين الموظفين تُعزى للمتغيرات الديموغرافية (العمر، سنوات الخبرة، المسمى الوظيفي)".
- الفروض البديلة الموجهة (Directed Hypotheses) تتوقع وجود أثر إيجابي أو سلبي بشكل مباشر: الفرض الأول: "يؤدي ارتفاع مستوى وعي موظفي الوزارات الحكومية بالتشريعات القانونية إلى زيادة كفاءة حماية خصوصية البيانات".
الفرض الثاني: "توجد علاقة طردية موجبة بين حجم الاستثمار في الأنظمة الرقمية الحديثة وانخفاض معدل اختراق خصوصية البيانات الحكومية"
- الفروض البديلة غير الموجهة (Undirected Hypotheses) تثبت وجود أثر أو اختلاف، دون تحديد اتجاهه: الفرض الأول: "يوجد أثر لتطبيق الحوكمة الرقمية على آليات حماية الخصوصية وسرية المعلومات في القطاع الحكومي".

الفرض الثاني: "يختلف مستوى حماية الخصوصية في الوزارات الحكومية باختلاف نوع الخدمات المقدمة (خدمات إلكترونية بالكامل مقابل خدمات هجينة)".

-النظرية العلمية المتبعة لإعداد البحث-

1. النظريات السلوكية والبشرية (تدرس وعي الموظفين والمواطنين)نظرية الفعل المخطط (Theory of Planned Behavior - TPB):مفهومها: تفسر كيف تؤثر معتقدات الموظف وضغوط العمل على سلوكه تجاه حماية البيانات. استخدامها: قياس مدى التزام الموظفين بتطبيق سياسات الخصوصية داخل الوزارة.
2. نظرية التراجع عن الحماية (Protection Motivation Theory - PMT):مفهومها: تدرس كيف يتصرف الأفراد لحماية أنفسهم والمنظمة عند شعورهم بوجود تهديد سيبراني.استخدامها: قياس مدى استجابة الموظفين للتدريب على الأمن السيبراني لتجنب تسريب البيانات.
3. مفارقة الخصوصية (Privacy Paradox):مفهومها: الفجوة بين قول الأفراد إنهم يهتمون بالخصوصية، وسلوكهم الفعلي الذي يفرض فيها بسهولة. استخدامها: دراسة سلوك المواطنين عند استخدام منصات الوزارات الحكومية
4. النظريات التنظيمية والتقنية (تدرس الأنظمة والبيئة الحكومية)النظرية المؤسسية (Institutional Theory):مفهومها: تدرس كيف تتبنى المنظمات القوانين والأنظمة (مثل تشريعات الخصوصية) لكسب الشرعية وليس فقط للأمان التقني. استخدامها: تحليل دوافع الوزارات الحكومية لتبني سياسات الخصوصية (هل هو التزام قانوني أم ضغط مجتمعي؟).

5. نظرية قبول التكنولوجيا (Technology Acceptance Model - TAM): مفهومها:
تبحث في مدى سهولة وفائدة الأنظمة التقنية الجديدة بالنسبة للموظفين. استخدامها: دراسة
مدى تقبل موظفي الوزارات للأنظمة الأمنية الصارمة الجديدة لحماية الخصوصية.

الفصل الثاني

الدراسات السابقة

مقدمة

تعد حماية الخصوصية الرقمية ركيزة أساسية في العصر الحديث، لا سيما مع توسع نطاق المعاملات الإلكترونية التي تفرض تحديات متزايدة على أمن البيانات الشخصية وحمايتها من الانتهاكات المحتملة. وتكتسب هذه الحماية أهمية مضاعفة في ظل تزايد التهديدات السيبرانية العالمية، مما يستوجب تبني إطار عمل شاملة لتعزيز الوعي الرقمي وضمان سرية المعلومات الحساسة وعلى الصعيد الوطني، تكتسب حماية الخصوصية أهمية كبرى بوصفها حقاً أساسياً يرتبط بسلامة الأفراد، وهو ما يفرض على المؤسسات ضرورة تطبيق إجراءات تقنية وإدارية فعالة لحماية البيانات المخزنة رقمياً من أي مخاطر. وفي هذا السياق، يبرز دور المملكة العربية السعودية في تعزيز حماية البيانات الشخصية عبر تبني تدابير إدارية متقدمة تتماشى مع مستهدفات رؤية 2030، مع التركيز على الدور الإشرافي للهيئة السعودية للبيانات والذكاء الاصطناعي في تنظيم هذا المجال. علاوة على ذلك، يأتي نظام حماية البيانات الشخصية ليمثل إطاراً تشريعياً حيوياً يحدد بوضوح التزامات الجهات الحكومية وحقوق الأفراد، مما يساهم في تعزيز الثقة في التحول الرقمي الوطني. وتتمثل المشكلة الرئيسية لهذه الدراسة في تقييم مدى كفاءة وقدرة هذه التدابير القانونية والتقنية على مواجهة التهديدات السيبرانية المتصاعدة التي قد تشكل خطراً على سرية بيانات المستفيدين. ولتحقيق أهداف الدراسة، تتبنى هذه الورقة المنهج الوصفي التحليلي لتقييم السياسات الأمنية المطبقة وتحديد الفجوات في إجراءات حماية المعلومات، وذلك بالاستناد إلى الضوابط الأساسية للأمن السيبراني والمعايير الوطنية المعتمدة. كما تهدف هذه الدراسة إلى تقييم كفاءة التدابير التقنية والإدارية في معالجة نقاط الضعف التي قد يستغلها المخترقون للوصول إلى البيانات الحساسة في القطاع الحكومي. وتسعى الدراسة أيضاً إلى وضع نموذج عملي لزيادة قدرة الوزارة على التصدي للتهديدات الأمنية، عبر التركيز على تطبيق إجراءات تقنية وتنظيمية فاعلة تضمن حماية المعلومات وسلامتها وسريتها واستمرار توفرها. ولتحقيق أهداف هذا البحث، تم تصميم استبانة متخصصة لقياس محاور رئيسية تتضمن طرق إدارة الأمن السيبراني، وآليات التصدي للمخاطر والتهديدات الرقمية، إلى جانب تقييم مدى فاعلية الأدوات والحلول التقنية الأمنية المستخدمة داخل البيئة الإدارية للوزارة. واستُخدمت هذه الأداة لاستطلاع آراء عينة من الموظفين في الجوانب التقنية والإدارية المتعلقة بحماية المعلومات، مما يساعد في الوصول إلى نتائج واقعية وشاملة للدراسة. وتأتي هذه الجهود في إطار مواءمة الممارسات المتبعة مع متطلبات الأمن السيبراني الوطنية، مما يقلل من احتمالية التعرض للثغرات البرمجية التي قد يستغلها المتسللون للوصول إلى الأصول المعلوماتية الحساسة. وتعتمد الدراسة في هذا السياق على دمج الأطر التشريعية، مثل نظام حماية البيانات الشخصية والضوابط الأساسية للأمن السيبراني، لتعزيز صمود البنية التحتية المعلوماتية للوزارة في وجه التهديدات الرقمية المعاصرة. كما تعتمد المنهجية على تحليل الفجوات بين الإجراءات الحالية والمعايير الوطنية للأمن السيبراني، بما يضمن بناء درع رقمي متكامل يعزز من مرونة الوزارة ضد الهجمات السيبرانية المعقدة. وبالإضافة إلى ذلك، تهتم هذه الدراسة بفحص التحديات التقنية والعملية التي تواجه تأمين البيانات الحساسة، مع التشديد على أهمية

تنفيذ خطط وقائية مسبقة لرفع مستوى الثقة الرقمية لدى المستفيدين من الخدمات الإلكترونية للوزارة . وتستند المنهجية المتبعة في هذا البحث إلى دمج أطر إدارة المخاطر مع السياسات الوطنية المعتمدة، لضمان استمرارية الخدمات الرقمية وحماية الأصول المعلوماتية من الاختراقات المتطورة ويتحقق ذلك من خلال دمج تقنيات التحليل الكمي والنوعي التي تسهم في رصد الثغرات الأمنية المحتملة وتصنيف التهديدات السيبرانية بناءً على أثرها التشغيلي على أمن المعلومات بالوزارة .وتسعى الدراسة من خلال هذا المسار المنهجي المتكامل إلى تعزيز الموقف الأمني للمؤسسات في مواجهة التهديدات السيبرانية المتطورة، بما يسهم في حماية الأصول الرقمية وضمان سرية البيانات الحساسة .

-الدراسات السابقة-

تستعرض هذه المراجعة الأدبيات النظرية والتطبيقية التي تناولت أطر الخصوصية وأمن البيانات، مع التركيز على الاستراتيجيات المتبعة في المؤسسات الحكومية لتعزيز مرونة أنظمتها الرقمية .حيث تشير الدراسات إلى أن فعالية الحماية السيبرانية تزداد بشكل ملحوظ في المنظمات التي تعامل الأمن السيبراني كمخاطرة استراتيجية تتطلب تكاملاً بين التكنولوجيا والعنصر البشري والهيكل التنظيمي . وفي هذا السياق، تؤكد الأدبيات أن تبني أطر معيارية دولية، مثل إرشادات المنظمة الدولية للمعايير، يمنح المؤسسات العامة قدرة أعلى على مواجهة التهديدات السيبرانية المتزايدة وضمان استمرارية الخدمات الرقمية . كما يشدد المتخصصون على أن تحقيق هذا المستوى من الأمن لا يقتصر على الحلول التقنية وحدها، بل يتطلب تنفيذ استراتيجيات استباقية تشمل تدريب الموظفين ووضع سياسات صارمة لتنظيم الوصول إلى البيانات والموارد الرقمية .وفي هذا السياق، يعد التنسيق الفعال والمستمر بين القطاعات الحكومية والمؤسسات الخاصة عنصراً أساسياً في تبادل المعلومات الضرورية وصياغة تشريعات متطورة تواكب التحديات السيبرانية المستجدة . كما تؤكد الدراسات أن دمج تقنيات الذكاء الاصطناعي وتحليل السلوك الرقمي يلعب دوراً محورياً في تعزيز أنظمة الدفاع الاستباقية ضد التهديدات المستمرة والمتقدمة . كما تعزز النماذج الإحصائية المتطورة من فهم المشهد السيبراني، مما يتيح تحديد الثغرات الأمنية بدقة عبر تحليل سيناريوهات الهجوم المختلفة .بالإضافة إلى ذلك، تبرز الدراسات أن إدارة مخاطر الأطراف الثالثة وتكثيف برامج التوعية الأمنية للموظفين تعد من العوامل الحاسمة في الحد من الثغرات الناتجة عن الأخطاء البشرية التي قد تستغلها الهجمات السيبرانية المعقدة .وبالتوازي مع ذلك، يتجه التركيز التقني نحو تبني حلول متقدمة لتعزيز الخصوصية تتجاوز وسائل الحماية التقليدية، مما يُتيح للمؤسسات الحكومية معالجة وتحليل البيانات بفعالية عالية مع ضمان الالتزام التام بحماية خصوصية الأفراد والامتثال للأنظمة الوطنية، وهو ما يُسهم في تعظيم الاستفادة من البيانات الضخمة وسد الفجوة بين طموحات التحول الرقمي ومتطلبات حماية المعلومات الحساسة . وفي سياق تعزيز هذه المنظومة في المملكة العربية السعودية، اقترح الباحثون تطوير أطر عمل سيبرانية شمولية لمشاريع الحكومة الإلكترونية، والتي تدمج بين المبادئ العلمية والمعايير التقنية لضمان حماية المعلومات في بيئة رقمية متطورة وتشدد البحوث الحديثة على ضرورة تبني استراتيجية شاملة لإدارة الأمن السيبراني، تجمع بين الحلول التقنية المتقدمة لرصد الاختراقات وتدابير إدارية تنظيمية تعتمد على تدريب العاملين بصفة مستمرة ووضع خطط استباقية للاستجابة لأي خروقات أمنية محتملة. ويبرز كذلك الدور المحوري لتطبيق نموذج الثقة الصفرية، الذي يقوم على مبدأ التحقق المتواصل من المستخدمين وتحديد صلاحياتهم بالقدر الضروري فقط، سعياً للتقليل من فرص تعرض الأنظمة الرقمية المترابطة لأي مخاطر. كما تشدد الدراسات على أهمية الاستعانة بتقنيات الذكاء الاصطناعي لتطوير أنظمة رصد التهديدات والاستجابة لها بشكل تلقائي، مما يساعد في الحد من الحاجة إلى التدخل البشري المستمر عند التصدي للهجمات والاختراقات السيبرانية

المعقدة. وبالإضافة إلى ذلك، يرى المختصون أن غياب ثقافة الحوكمة السيبرانية داخل الهيئات يقلل من ثقة المستخدمين في الخدمات الرقمية، الأمر الذي يحتم تكثيف التعاون على المستويين المحلي والدولي لتبادل الخبرات وتطوير منظومات دفاعية مرنة قادرة على مواجهة التهديدات المتلاحقة. وبناءً على ذلك، يمثل توظيف أدوات التعلم الآلي والتقنيات المتقدمة لتحليل السلوك الرقمي ركيزة أساسية لتعزيز القدرة الاستباقية في رصد الثغرات والأنشطة غير الطبيعية، مما يضمن انسجام العمليات الإدارية مع التوجهات الوطنية المعتمدة لحماية البنية التحتية المعلوماتية. وتشير الأبحاث كذلك إلى ضرورة تكثيف الاستثمارات في مجالات البحث والتطوير لتوليد حلول تقنية مبتكرة قادرة على صد البرمجيات الضارة المتقدمة ومخاطر التجسس الرقمي، مع التركيز على تعزيز آليات التعاون الدولي لتوحيد المعايير الأمنية وتسهيل تبادل المعلومات حول التهديدات السيبرانية العالمية. وتأتي هذه التوجهات لتؤكد على أهمية المساءلة القانونية للجهات غير الممتثلة لمعايير الأمن، مما يضمن حماية البنية التحتية الحساسة من الاختراقات المتطورة. وفي الجانب التشريعي، تُعتبر اللائحة العامة لحماية البيانات في الاتحاد الأوروبي مرجعاً مهماً يبرز دور القوانين في إلزام المؤسسات بضوابط أمنية مشددة تضمن حماية خصوصية بيانات المستفيدين. وفي هذا الإطار، تساهم هذه الأطر التنظيمية الدولية في توجيه الحكومات نحو تبني معايير صارمة لإدارة المخاطر التقنية، مثل إطار عمل NIST، الذي يوفر إرشادات حيوية لتعزيز الوضع الأمني للبنية التحتية الحساسة كما تؤكد هذه الأطر على أن التوافق التنظيمي لا يقتصر على الامتثال للقوانين فحسب، بل يمتد ليشمل الاستثمار في القوى العاملة وتطوير مهاراتهم لمواجهة التهديدات السيبرانية المعتمدة على الذكاء الاصطناعي كما تبرز الشراكات الاستراتيجية بين القطاعين الحكومي والخاص كأداة أساسية لتبادل معطيات التهديدات وتطوير حلول سيبرانية متطورة تهدف إلى التصدي للمخاطر الناشئة بشكل استباقي. وعلاوة على ذلك، لا تقتصر هذه الشراكات على التنسيق التشغيلي فحسب، بل تمتد لتشمل التكامل التقني الاستراتيجي؛ إذ يساهم دمج الذكاء الاصطناعي في أطر إدارة المخاطر والامتثال في تحسين دقة الكشف عن التهديدات وتطوير أنظمة استجابة مؤتمتة، مما يساهم في تعزيز نزاهة وشفافية البيانات المتبادلة عبر المنصات الرقمية الحكومية، وتقليل الفجوة الزمنية بين رصد الاختراقات ومعالجتها، وهو ما يدعم التوجهات الوطنية نحو بناء بيئة رقمية آمنة ومرنة تتماشى مع رؤية المملكة في التحول الرقمي الموثوق. على ذلك، يساهم دمج الذكاء الاصطناعي في أطر إدارة المخاطر والامتثال في تحسين دقة الكشف عن التهديدات وتطوير أنظمة استجابة مؤتمتة، مما يساهم في تعزيز نزاهة وشفافية البيانات المتبادلة عبر المنصات الرقمية الحكومية، وتقليل الفجوة الزمنية بين رصد الاختراقات ومعالجتها، وهو ما يدعم التوجهات الوطنية نحو بناء بيئة رقمية آمنة ومرنة تتماشى مع رؤية المملكة في التحول الرقمي الموثوق. كما أن تبني هذه التقنيات يتيح للجهات الحكومية إجراء تقييمات دورية للأثر الأخلاقي لضمان توافق خوارزميات الذكاء الاصطناعي مع مبادئ الخصوصية والشفافية. وفي هذا السياق، تبرز تقنيات تعزيز الخصوصية -مثل التعلم الموحد والخصوصية التفاضلية- كحلول تقنية مبتكرة تتجاوز مجرد الامتثال الإجرائي؛ حيث تمكن هذه التقنيات الوزارات من استخراج الرؤى التحليلية القيمة من قواعد البيانات الضخمة دون الحاجة إلى الوصول المباشر أو الكشف عن المعلومات الشخصية، مما يؤسس عملياً لمبدأ "الخصوصية بالتصميم" كركيزة أساسية في بنية التحول الرقمي الحكومي، ويُسهم في بناء نموذج تقني يضمن حماية البيانات بشكل ذاتي ومستمر بعيداً عن التدخل البشري. وفي هذا السياق، أكدت دراسات سابقة على أهمية تبني أطر عمل سيبرانية شمولية تتجاوز الامتثال التقني، حيث اقترح الباحثون في سياق المملكة العربية السعودية تطوير منظومات دفاعية لمشاريع الحكومة الإلكترونية تدمج بين المبادئ العلمية والمعايير التقنية. كما أشارت أبحاث أخرى إلى أن حماية البيانات الحكومية الحساسة تستلزم مزيجاً استراتيجياً من الحلول التقنية المتقدمة وتدابير إدارية تنظيمية تعتمد على التقييم المستمر للمخاطر وتدريب الكوادر البشرية، وهو ما يتوافق

مع التوجهات الدولية التي تؤكد على الدور الجوهري للمعايير العالمية، مثل NIST وISO، في تعزيز الحوكمة السيبرانية وبناء ثقافة أمنية مرنة تضمن ثقة المستخدمين وتؤسس لضوابط أمنية فعالة للأنظمة الحكومية. إضافة إلى ذلك، توضح الأبحاث أن استخدام تقنيات مثل التشفير المتقدم والتعلم الموحد يُمكن المؤسسات من تحليل البيانات الضخمة مع الحفاظ على الخصوصية، مما يقلل من فرص الوصول غير المصرح به للمعلومات الحساسة. علاوة على ذلك، أثبتت الدراسات أن توظيف خوارزميات الذكاء الاصطناعي في إدارة الامتثال يمنح الهيئات الحكومية قدرة فائقة على الكشف الاستباقي عن الأنماط غير الطبيعية، مما يُعزز من دقة ونزاهة حماية البيانات في بيئة رقمية تتسم بالتعقيد المتزايد. ومع ذلك، تواجه هذه التقنيات تحديات جوهرية مثل انحياز الخوارزميات ونقص الكوادر المؤهلة في مجال الأمن السيبراني، مما يفرض ضرورة تبني برامج تدريبية متخصصة ومراجعة دورية للمعايير الأخلاقية لتعزيز فاعليتها. بالإضافة إلى ذلك، تشير النتائج الميدانية إلى وجود فجوة في مستوى النضج التقني لبعض المؤسسات، حيث يتطلب سدها تكثيف الجهود نحو مواءمة الحوكمة مع الاحتياجات الثقافية والمبادئ القيمية المحلية. كما تُعد مراجعة الخوارزميات بشكل مستقل خطوة أساسية لضمان عدالة القرارات الآلية عند توزيع الموارد المائية والبيئية، مما يدعم شفافية الوزارة ويحقق التوازن بين الأداء التقني والمبادئ الأخلاقية أثناء التحول الرقمي. وفي سياق الدراسات السابقة التي تناولت حماية البيانات في القطاعات الحكومية، أظهرت الأبحاث أن تبني استراتيجيات دفاعية استباقية لا يقتصر على الحلول التقنية فحسب، بل يتطلب تكاملاً وثيقاً بين التقييم المستمر للمخاطر وتطوير كفاءات الكوادر البشرية. كما أشار الباحثون إلى أن دمج مبادئ "الخصوصية بالتصميم" في مشاريع التحول الرقمي الحكومي يعزز من قدرة هذه المؤسسات على إدارة البيانات الحساسة بفعالية، وذلك من خلال تطبيق أطر عمل سيبرانية شمولية تراعي الخصوصيات الثقافية والتشريعية المحلية، كما هو الحال في تجربة المملكة العربية السعودية التي ربطت بين المعايير التقنية والقيم الثقافية لضمان ذكاء اصطناعي أخلاقي وتؤكد هذه الدراسات أن النجاح في حماية الخصوصية داخل الهيئات العامة يرتبط ارتباطاً وثيقاً بالالتزام بالمعايير التنظيمية الدولية، التي توفر إرشادات حيوية لتعزيز الوضع الأمني للبنى التحتية الحساسة وعليه، فإن غياب أطر الحوكمة السيبرانية الواضحة يضعف ثقة المستخدمين في الخدمات الرقمية، مما يتطلب الاستفادة من خبرات المؤسسات الرائدة في تطبيق معايير الأمن لضمان الموثوقية الرقمية، لا سيما في ظل التوسع في استخدام البيانات الضخمة التي تستوجب رقابة مشددة للوقاية من التهديدات والحد من الأخطاء البشرية.

-الإطار النظري-

يتناول هذا الفصل الأسس المفاهيمية التي تقوم عليها الدراسة، من خلال استعراض مفهوم الخصوصية وتطوره التاريخي والفكري، وتمييزه عن المفاهيم المتقاربة، ثم الانتقال إلى مفهوم البيانات الشخصية وتصنيفاتها، وصولاً إلى بيان أهمية حماية الخصوصية في القطاع الحكومي تحديداً، بوصفه القطاع الذي يجمع أكبر قدر من بيانات المواطنين والمقيمين.

مفهوم الخصوصية وتطوره:

لا يوجد تعريف جامع مانع متفق عليه للخصوصية، إذ تباينت التعريفات بحسب الزاوية القانونية أو الاجتماعية أو التقنية التي تناولها الباحثون. فمن الناحية القانونية التقليدية، عُرِّفت الخصوصية بأنها «الحق في أن يُترك الفرد وشأنه» دون تدخل من الآخرين في شؤونه الخاصة. أما في العصر الرقمي، فقد تطور هذا المفهوم ليشمل «حق الفرد في التحكم بمعلوماته الشخصية»، أي القدرة على تحديد من يحق له الوصول إلى بياناته، وفي أي سياق، ولأي غرض، ولأي مدة.

وقد مرّ مفهوم الخصوصية بمراحل تطور متعددة، بدأت بالتركيز على الخصوصية المكانية والجسدية (حرمة المسكن والمراسلات)، ثم اتسعت لتشمل الخصوصية المعلوماتية مع ظهور الحوسبة وقواعد البيانات الإلكترونية في النصف الثاني من القرن العشرين، ثم تعمقت أكثر مع انتشار الإنترنت والهواتف الذكية والخدمات الحكومية الإلكترونية، لتصبح الخصوصية الرقمية أحد أكثر فروع الخصوصية أهمية وتعقيداً في الوقت الراهن.

خصائص الخصوصية في البيئة الرقمية:

- الطابع النسبي: تختلف حدود الخصوصية باختلاف الثقافات والمجتمعات والأنظمة القانونية، فما يُعد معلومة خاصة في مجتمع قد لا يكون كذلك في مجتمع آخر.
- الترابط مع الثقة المؤسسية: يرتبط استعداد الأفراد لمشاركة بياناتهم مع الجهات الحكومية بمدى ثقتهم في قدرة تلك الجهات على حماية هذه البيانات وعدم إساءة استخدامها.
- التزايد المستمر للمخاطر: مع تنامي حجم البيانات المتبادلة إلكترونياً، تتزايد المخاطر المرتبطة بالاختراقات والتسريبات وسوء الاستخدام.
- الحاجة إلى توازن: تتطلب حماية الخصوصية تحقيق توازن دقيق بين حق الفرد في الخصوصية وحاجة الجهات الحكومية إلى البيانات لتقديم خدماتها وتحقيق المصلحة العامة.

مفهوم البيانات الشخصية وتصنيفاتها

تُعرّف البيانات الشخصية بأنها كل معلومة تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه بصورة مباشرة أو غير مباشرة، سواء كانت هذه المعلومة اسمًا أو رقم هوية أو بيانات موقع جغرافي أو معرفًا إلكترونيًا أو أي عامل آخر خاص بهويته البدنية أو الفسيولوجية أو الاقتصادية أو الاجتماعية. وتتسع هذه البيانات في السياق الحكومي لتشمل بيانات الهوية الوطنية، وبيانات الاتصال، والبيانات المالية، وبيانات الملكية العقارية والزراعية، وبيانات التراخيص والتصاريح، وسجلات المعاملات الإلكترونية.

تصنيف البيانات الشخصية:

يمكن تصنيف البيانات الشخصية إلى فئتين رئيسيتين وفق نظام حماية البيانات الشخصية السعودي:

- البيانات الشخصية العادية: وتشمل المعلومات الأساسية للتعريف بالفرد كالاسم والعنوان ورقم الهاتف والبريد الإلكتروني وأرقام الحسابات والسجلات المدنية.

- البيانات الشخصية الحساسة: وتشمل البيانات التي تكشف عن الأصل العرقي أو القبلي، أو الرأي السياسي أو الديني أو الفكري، أو البيانات الأمنية الجنائية، أو البيانات البيومترية والوراثية، أو بيانات الحالة الصحية الجسدية أو النفسية، أو بيانات تدل على أن الفرد مجهول الأبوين أو أحدهما، أو أن أحد أبويه غير معروف، وتخضع هذه الفئة لضوابط أشد في المعالجة والحماية.

وفي سياق قطاع البيئة والمياه والزراعة، تتخذ البيانات الشخصية أشكالًا متخصصة، مثل بيانات ملكية الأراضي الزراعية وحيازتها، وبيانات تراخيص حفر الآبار واستخراج المياه الجوفية، وبيانات المخالفات البيئية المرتبطة بأشخاص بعينهم، وبيانات المستفيدين من الدعم الزراعي والحيواني، وهي بيانات تحمل طابعًا اقتصاديًا حساسًا لارتباطها المباشر بمصادر رزق المستفيدين ونشاطهم التجاري.

أهمية حماية الخصوصية في القطاع الحكومي:

تكتسب حماية الخصوصية في القطاع الحكومي أهمية خاصة تفوق نظيرتها في القطاع الخاص من عدة أوجه، يمكن إجمالها في النقاط التالية:

أولاً: اتساع نطاق البيانات المجمعة

تتعامل الجهات الحكومية مع بيانات شبة كامل السكان، من خلال الخدمات الإلزامية كالسجل المدني والتأمينات والخدمات الصحية والتعليمية والزراعية، مما يجعل حجم البيانات المعرضة للخطر في حال حدوث اختراق أو تسريب أكبر بكثير مما هو عليه الحال في أي مؤسسة خاصة منفردة.

ثانيًا: الطابع الإلزامي لتقديم البيانات

خلافاً للقطاع الخاص الذي يمكن للفرد فيه الامتناع عن التعامل مع جهة معينة إذا لم يثق في سياسات خصوصيتها، فإن التعامل مع الجهات الحكومية غالباً ما يكون إلزامياً لممارسة حقوق أو الحصول على خدمات أساسية، مما يفرض على هذه الجهات مسؤولية أخلاقية ونظامية مضاعفة في حماية ما تجمعه من بيانات.

ثالثاً: تعزيز الثقة الرقمية ودعم التحول الرقمي

يشكل ضمان حماية الخصوصية عاملاً محورياً في نجاح مبادرات التحول الرقمي الحكومي، إذ إن ثقة المستفيدين في أمان بياناتهم تنعكس مباشرة على إقبالهم على استخدام الخدمات الإلكترونية بدلاً من القنوات التقليدية، وهو ما يخدم أهداف رؤية المملكة 2030 في رفع كفاءة الخدمات الحكومية وتوسيع نطاق التحول الرقمي.

رابعاً: الالتزام بالمعايير الدولية وتعزيز التنافسية

يسهم الالتزام الحكومي بمعايير حماية البيانات في تعزيز مكانة المملكة ضمن المؤشرات الدولية المتعلقة بالحوكمة الرقمية وحماية البيانات، ويدعم جهود جذب الاستثمار الأجنبي في قطاع تقنية المعلومات، إذ باتت مصفوفات الامتثال لحماية البيانات معياراً أساسياً تنظر إليه الشركات العالمية عند تقييم بيئة الأعمال في أي دولة.

خامساً: الحد من المخاطر القانونية والمالية

يترتب على الإخلال بمتطلبات حماية البيانات الشخصية في القطاع الحكومي مخاطر نظامية وتأديبية على منسوبي الجهة المخالفة، فضلاً عن الأضرار المعنوية والمالية التي قد تلحق بأصحاب البيانات، وهو ما يجعل من الامتثال الاستباقي لمتطلبات الحماية أمراً ضرورياً لا يمكن تأجيله أو التهاون فيه.

وقد شهدت المملكة العربية السعودية خلال السنوات الأخيرة نقلة نوعية في بناء منظومة تشريعية ومؤسسية متكاملة لحماية البيانات الشخصية، تماشيًا مع أهداف رؤية المملكة 2030 في تعزيز التحول الرقمي وبناء اقتصاد رقمي تنافسي قائم على الثقة. ويستعرض هذا الفصل أبرز محطات هذا الإطار التشريعي والمؤسسي، بدءاً من نظام حماية البيانات الشخصية ولوائحه التنفيذية، مروراً بالجهات الإشرافية المعنية، وصولاً إلى أبرز مبادئ النظام وحقوق أصحاب البيانات والتزامات الجهات المعالجة والعقوبات المقررة.

نشأة نظام حماية البيانات الشخصية وتطوره

صدر نظام حماية البيانات الشخصية في المملكة العربية السعودية بموجب المرسوم الملكي رقم م (19) وتاريخ 9/2/1443 هـ الموافق 16 سبتمبر 2021 م، بوصفه أول تشريع وطني شامل ينظم جمع البيانات الشخصية ومعالجتها والإفصاح عنها ونقلها، سواء من قبل الجهات الحكومية أو الخاصة العاملة داخل المملكة. وقد جاء صدور هذا النظام تنويعاً لجهود الهيئة السعودية سدايا (في بناء منظومة وطنية لحوكمة البيانات، تتسجم مع أفضل الممارسات الدولية في هذا المجال).

وفي إطار السعي نحو معالجة الملاحظات العملية التي رافقت التطبيق الأولي للنظام، صدر المرسوم الملكي رقم م (148) وتاريخ 5/9/1444 هـ بالموافقة على عدد من التعديلات الجوهرية على النظام، تناولت بشكل خاص إعادة صياغة أحكام نقل البيانات الشخصية إلى خارج المملكة بما يوازن بين متطلبات الحماية ومتطلبات الانفتاح الاقتصادي والرقمي. وقد أصبح النظام بصورته المعدلة نافذاً وواجب الإنفاذ الكامل اعتباراً من 14 سبتمبر 2024 م، بعد انقضاء فترة انتقالية أُتيحت لجميع الجهات لمواءمة أنظمتها وسياساتها الداخلية مع متطلباته.

الجهات الإشرافية والمؤسسية

الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)

تُعد سدايا الجهة المختصة بالإشراف على تطبيق نظام حماية البيانات الشخصية ووضع لوائح التنفيذ والمعايير المكملة له، وذلك خلال المرحلة الأولى من التطبيق. وتتولى سدايا إصدار الأدلة الإرشادية للجهات الحكومية والخاصة، وتلقي الشكاوى المتعلقة بمخالفات النظام، وإصدار تراخيص أنشطة حماية البيانات الشخصية، إلى جانب دورها العام في وضع السياسات الوطنية للبيانات والذكاء الاصطناعي ضمن مكتب إدارة البيانات الوطنية (NDMO).

مكتب إدارة البيانات الوطنية (NDMO)

يضطلع مكتب إدارة البيانات الوطنية بوضع السياسات والمعايير الوطنية لإدارة البيانات وحوكمتها وتصنيفها، بما يشمل معايير تصنيف البيانات) عام، داخلي، سري، سري للغاية)، ومعايير جودة البيانات، وضوابط مشاركتها بين الجهات الحكومية، وهو ما يشكل الإطار المرجعي الذي تسترشد به الوزارات ومنها وزارة البيئة والمياه والزراعة في تصميم سياساتها الداخلية لحماية البيانات.

هيئة الحكومة الرقمية (DGA)

تتولى هيئة الحكومة الرقمية الإشراف على منصات الخدمات الحكومية الإلكترونية وتسجيلها واعتمادها، وتضع معايير تقنية وإجرائية للأمن السيبراني وجودة الخدمات الرقمية، وتشتترط على الجهات الحكومية تسجيل منصاتها الإلكترونية لديها والإفصاح عن سياسات الخصوصية المعتمدة، وهو ما يتضح جلياً في تسجيل المنصات الإلكترونية لوزارة البيئة والمياه والزراعة لدى الهيئة.

الهيئة الوطنية للأمن السيبراني (NCA)

تختص الهيئة الوطنية للأمن السيبراني بوضع الضوابط والأطر التنظيمية اللازمة لحماية الفضاء السيبراني الوطني، وتشمل هذه الضوابط الأساسية للأمن السيبراني ومتطلبات حماية البيانات من الاختراق والتسريب، وتُعد هذه الضوابط مكملة لنظام حماية البيانات الشخصية من الناحية التقنية والوقائية، إذ إن حماية الخصوصية لا تتحقق دون بنية تحتية للبيانات والذكاء الاصطناعي (سيبرانية آمنة).

أبرز مبادئ نظام حماية البيانات الشخصية

أرسى نظام حماية البيانات الشخصية مجموعة من المبادئ الجوهرية التي يجب أن تلتزم بها جميع الجهات الخاضعة لأحكامه، ومن أبرزها:

- مبدأ المشروعية والشفافية: يجب أن تتم معالجة البيانات الشخصية وفق سند نظامي واضح، مع إشعار صاحب البيانات بغرض جمعها والجهة المسؤولة عن معالجتها.
- مبدأ الحد من الغرض: لا يجوز جمع البيانات الشخصية إلا للغرض المباشر الذي جمعت من أجله، ولا يجوز معالجتها بما يتعارض مع ذلك الغرض.
- مبدأ الحد الأدنى من البيانات: يقتصر جمع البيانات على القدر الذي يحقق الغرض المعلن، دون توسع غير مبرر في نطاق البيانات المجمعة.

- مبدأ الدقة: يجب أن تكون البيانات الشخصية دقيقة ومحدثة، وأن تُتخذ الإجراءات اللازمة لتصحيح أي بيانات غير دقيقة أو غير مكتملة.
- مبدأ الحفظ الآمن والتحديد الزمني: يجب إتلاف البيانات الشخصية أو إخفاء هويتها متى انتهت الحاجة إليها أو انتهى الغرض من جمعها، ما لم يوجد مسوغ نظامي للاحتفاظ بها لمدة محددة.
- مبدأ المساءلة: تتحمل الجهة المعالجة للبيانات المسؤولية الكاملة عن ضمان الامتثال لأحكام النظام، وعن أي إخلال يقع من جانبها أو من جانب من تتعاقد معه لمعالجة البيانات نيابة عنها.

حقوق صاحب البيانات الشخصية:

منح النظام صاحب البيانات الشخصية حزمة من الحقوق الجوهرية التي تمكنه من التحكم بمعلوماته، وتشمل أبرزها:

- الحق في العلم: معرفة السند النظامي والغرض من جمع بياناته الشخصية.
- الحق في الوصول: الاطلاع على بياناته الشخصية لدى الجهة المعالجة بالصيغة المتاحة وبدون مقابل، وفق ما تحدده اللوائح.
- الحق في طلب تصحيح البيانات: تصحيح أو استكمال أو تحديث بياناته الشخصية لدى الجهة المعالجة.
- الحق في طلب إتلاف البيانات: طلب إتلاف بياناته الشخصية متى لم تعد هناك حاجة إليها، مع مراعاة الاستثناءات النظامية.
- الحق في التقدم بالشكوى: تقديم شكوى إلى الجهة المختصة (سدايا) (في حال مخالفة أحكام النظام).

التزامات الجهة المتحكمة في البيانات

- يقابل هذه الحقوق مجموعة من الالتزامات المفروضة على الجهة المتحكمة بالبيانات (control-ler)، والتي تشمل الجهات الحكومية بما فيها الوزارات، وأبرزها:
- وضع سياسة خصوصية واضحة ومعلنة للمستفيدين، توضح أنواع البيانات المجمعة وأغراض معالجتها والجهات التي قد يتم مشاركة البيانات معها.
 - اتخاذ الإجراءات التنظيمية والتقنية والإدارية اللازمة لحماية البيانات الشخصية من فقدان أو التلف أو التسريب أو الوصول غير المصرح به.
 - عدم نقل البيانات الشخصية خارج المملكة إلا وفق الضوابط المحددة في النظام ولوائحه، وبما يضمن مستوى حماية مماثلًا لما هو مطبق داخل المملكة.
 - إجراء تقييم الأثر المتعلق بحماية البيانات الشخصية في حال كانت المعالجة تتضمن استخدام تقنيات حديثة قد تشكل خطرًا عاليًا على خصوصية أصحاب البيانات.

• الإبلاغ الفوري عن أي تسريب أو تلف أو وصول غير مصرح به للبيانات الشخصية للجهة المختصة، ولصاحب البيانات في حال ترتب على ذلك ضرر بحقوقه أو مصالحه.

• تعيين مسؤول لحماية البيانات الشخصية داخل الجهة عند استيفاء الشروط التي تحددها اللوائح، لمتابعة الامتثال والتنسيق مع الجهات الإشرافية.

آليات الرقابة والعقوبات

نص النظام على آليات رقابية وعقابية تهدف إلى ضمان الجدية في التطبيق وردع المخالفات. فقد أجاز النظام لصاحب البيانات الشخصية التقدم بشكوى إلى الجهة المختصة بشأن أي مخالفة ناشئة من تطبيق أحكامه. كما قرر النظام عقوبات جزائية على بعض المخالفات الجسيمة، منها الإفصاح عن البيانات الحساسة أو نشرها بقصد الإضرار بصاحبها أو تحقيق منفعة شخصية، إذ تصل عقوبة ذلك إلى السجن مدة لا تزيد على سنتين وغرامة لا تزيد على ثلاثة ملايين ريال، أو إحدى هاتين العقوبتين، مع جواز مضاعفة الغرامة في حال تكرار المخالفة.

وفيما يخص الجهات العامة تحديداً، أوجب النظام على الجهة العامة مساءلة أي من منسوبيها تأديبياً في حال مخالفته لأحكام النظام ولوائح، وفق أحكام وإجراءات المساءلة والتأديب المقررة نظاماً، بما يعني أن مسؤولية الامتثال داخل الوزارات لا تقع على عاتق الجهة فحسب، بل تمتد لتشمل المساءلة الفردية للموظفين المخالفين، وهو ما يعزز أهمية بناء ثقافة مؤسسية واعية بمتطلبات حماية البيانات لدى جميع منسوبي الجهات الحكومية.

بعد استعراض الإطار المفاهيمي والتشريعي في الفصلين السابقين، يخصص هذا الفصل لدراسة الحالة التطبيقية على وزارة البيئة والمياه والزراعة، بوصفها نموذجاً للوزارات الحكومية السعودية التي تتعامل مع كميات كبيرة ومتنوعة من البيانات الشخصية. ويتناول الفصل التعريف بالوزارة واختصاصاتها ومنصاتها الرقمية، ثم تحليل سياستها المعلنة لحماية البيانات الشخصية، ثم تحليل الآليات التطبيقية من الناحيتين التقنية والإدارية، وصولاً إلى تقييم مدى اتساق هذه الممارسات مع متطلبات نظام حماية البيانات الشخصية.

التعريف بوزارة البيئة والمياه والزراعة واختصاصاتها

تُعد وزارة البيئة والمياه والزراعة إحدى الوزارات الحكومية الرئيسية في المملكة العربية السعودية، وتتولى الإشراف على القطاعات البيئية والمائية والزراعية على المستوى الوطني، من خلال عدد من الوكالات المتخصصة، أبرزها وكالة البيئة، ووكالة المياه، ووكالة الزراعة، ووكالة الثروة السمكية. وتقدم الوزارة عشرات الخدمات الإلكترونية للمستخدمين عبر بواباتها الرقمية، تشمل إصدار تراخيص حفر الآبار وحصر المياه الجوفية، وتسجيل الحيازات الزراعية، وإصدار تراخيص المشاتل والمبيدات والأسمدة، ومتابعة برامج الدعم الزراعي والحيواني، ورصد المخالفات البيئية والتعامل مع بلاغات المواطنين.

ونظراً لطبيعة اختصاصات الوزارة، فإنها تعالج يومياً بيانات شخصية متنوعة تشمل بيانات الهوية الوطنية لمقدمي الطلبات، وبيانات الملكية والحيازة الزراعية، وبيانات الحسابات البنكية المرتبطة بصرف الدعم، وبيانات الموقع الجغرافي للمزارع والآبار والمنشآت، وبيانات المخالفات المرتبطة بأشخاص بعينهم، وهو ما يجعلها من الجهات الحكومية التي تحمل مسؤولية عالية في مجال حماية البيانات الشخصية.

تحليل سياسة حماية البيانات الشخصية المعلنة للوزارة

أصدرت وزارة البيئة والمياه والزراعة سياسة معلنة لحماية البيانات الشخصية، منشورة على موقعها الإلكتروني الرسمي ضمن قسم «سياسات الوزارة»، وذلك تنفيذًا لمتطلبات نظام حماية البيانات الشخصية ومتطلبات هيئة الحكومة الرقمية المتعلقة بتسجيل المنصات الإلكترونية الحكومية. ومن أبرز ما تضمنته هذه السياسة، وفق ما هو منشور رسميًا على موقع الوزارة، ما يلي:

- تحديد المعايير التي يجب استيفاؤها قبل جمع البيانات الشخصية من المستخدمين عبر منصة الوزارة الإلكترونية.

- النص صراحة على عدم جواز الكشف عن البيانات الشخصية للمستخدمين في حالات محددة، منها ما ينطوي على انتهاك لخصوصية طرف آخر غير مالك البيانات، أو ما يتعارض مع مصلحة عامة، أو ما ينتهك التزامات مهنية راسخة، أو ما يخل بحكم قضائي، أو ما يكشف عن مصدر سري للمعلومات.

- الالتزام بإتلاف البيانات الشخصية للمستخدمين فور انتهاء الغرض من جمعها، مع إجازة الاحتفاظ بها في حالات استثنائية محددة، كوجود مبرر نظامي يستوجب الاحتفاظ بها لمدة معينة، على أن يتم إتلافها بعد انتهاء تلك المدة أو انتهاء الغرض من جمعها أيهما أطول.

- الإحالة الصريحة إلى نظام حماية البيانات الشخصية السعودي بوصفه المرجع التشريعي الأساسي الذي تستند إليه سياسة الوزارة، مع إتاحة رابط مباشر للاطلاع على نص النظام.

- تسجيل منصة الوزارة الإلكترونية لدى هيئة الحكومة الرقمية برقم ترخيص معتمد، وهو ما يعكس التزامًا رسميًا موثقًا بمعايير الحوكمة الرقمية للخدمات الإلكترونية الحكومية.

ويلاحظ من تحليل هذه السياسة أنها تعكس وعيًا مؤسسيًا واضحًا بمتطلبات نظام حماية البيانات الشخصية من حيث المبدأ، وتتضمن إشارات محددة إلى مبادئ الحد من الغرض والحفظ الآمن والتحديد الزمني للبيانات. إلا أن السياسة المعلنة، بصيغتها المتاحة للعموم، تركز بشكل أكبر على الجوانب العامة للخصوصية، بينما تبقى التفاصيل الإجرائية الدقيقة المتعلقة بآلية تفعيل حقوق أصحاب البيانات (كطلب الوصول إلى البيانات أو تصحيحها أو إتلافها (أقل وضوحًا وتفصيلًا مقارنة بما هو متعارف عليه في السياسات المتقدمة عالميًا، والتي عادة ما تتضمن نموذجًا إلكترونيًا مباشرًا أو قناة تواصل مخصصة لتلقي طلبات أصحاب البيانات).

الآليات التقنية لحماية البيانات في منصات الوزارة

تعتمد وزارة البيئة والمياه والزراعة في تقديم خدماتها الإلكترونية على عدد من المنصات الرقمية المسجلة رسميًا لدى هيئة الحكومة الرقمية، وتتضمن هذه المنصات عددًا من الإجراءات التقنية التي تندرج ضمن متطلبات حماية البيانات، ومنها:

- استخدام بروتوكول النقل الآمن (HTTPS) لتشفير الاتصال بين متصفح المستخدم وخوادم الوزارة، بما يحد من إمكانية اعتراض البيانات أثناء نقلها.

- ربط المنصات الإلكترونية للوزارة بمنصة النفاذ الوطني الموحد (Absher/Nafath) للتحقق من هوية المستخدم قبل تمكينه من الوصول إلى بياناته أو تقديم طلباته، وهو إجراء يعزز من مبدأ التحكم في الوصول (Access Control).

- تسجيل منصات الوزارة لدى هيئة الحكومة الرقمية والحصول على تراخيص تشغيل معتمدة، وهو ما يفرض على الوزارة الالتزام بمعايير تقنية دنيا في تصميم وتشغيل هذه المنصات.
- اعتماد سياسات معلنة تنص على الالتزام بالمعايير الوطنية لإدارة البيانات الصادرة عن مكتب إدارة البيانات الوطنية، بما في ذلك متطلبات تصنيف البيانات وضوابط تداولها.

ومع ذلك، فإن المعلومات المتاحة للعموم حول التفاصيل التقنية الدقيقة) كآليات التشفير المستخدمة في قواعد البيانات الداخلية، أو إجراءات إدارة الحوادث السيبرانية، أو آليات النسخ الاحتياطي وضوابط الوصول الداخلي للموظفين (تبقى محدودة، وهو أمر متوقع ومبرر جزئياً من الناحية الأمنية، إذ إن الإفصاح التفصيلي عن الضوابط التقنية الداخلية قد يشكل بحد ذاته مخاطرة أمنية. إلا أن هذا الغموض يجعل من الصعب على الباحث أو المستفيد الخارجي تقييم درجة النضج التقني الفعلي لمنظومة حماية البيانات داخل الوزارة، ويستدعي الاعتماد على تقارير التدقيق الداخلية أو مؤشرات الامتثال الصادرة عن الجهات الرقابية كسدايا وهيئة الحكومة الرقمية للوقوف على واقع أدق.

الفصل الثالث

منهجية الدراسة

مقدمة.

للحصول على نتائج دقيقة واقرب للواقع لحل أي مشكلة لابد من استخدام منهجية علمية واضحة تناسب المجتمع الذي نرغب في تسليط الضوء على مشكلة يعاني منها. بالنسبة لمشكلة الدراسة الحالية فهي تختص بوزارة تخدم مستفيدين اغلبهم يجهل الامور التقنية وكادر مؤسساتي غير مدرب وتنقصه الخبرة. لذا يجب استخدام المنهج الوصفي التحليلي ويشمل الاستبيانات والمقابلات والملاحظة لتسجيل البيانات ومن ثم استخراج البيانات وفرزها للوصول للمعلومات بشكل دقيق.

-المنهجية وطرق البحث

تعتمد هذه الدراسة المنهج الوصفي التحليلي لتفكيك أبعاد حماية الخصوصية الرقمية بوزارة البيئة والمياه والزراعة، حيث يتم توظيف نهج "الخصوصية بالتصميم" لتقييم مدى مواءمة البنية التقنية للمعايير الوطنية والدولية ويتمثل هذا النهج في تحليل الفجوات بين الإجراءات المطبقة حالياً والمتطلبات التنظيمية الصارمة، مع التركيز على دور الحوكمة في إدارة البيانات الحساسة. كما يشمل هذا الإطار المنهجي إجراء مسح ميداني لاستكشاف وجهات النظر الإدارية والتقنية حول فاعلية البروتوكولات الأمنية المستخدمة في مواجهة التهديدات السيبرانية المتطورة. ويتضمن التصميم البحثي أسلوباً متكاملًا يجمع بين استطلاع آراء الموظفين لتقييم مدى وعيهم بسياسات أمن البيانات، وإجراء مقابلات مع المتخصصين والخبراء للوقوف على التحديات العملية التي تواجه تطبيق نظام حماية البيانات الشخصية. بالإضافة إلى ذلك، تُستخدم استبيانات متخصصة لتقييم مستويات النضج الرقمي لدى العاملين، مع ربط نتائجها بمتطلبات التحول الرقمي للوزارة وتحديات الامتثال التنظيمي التي تواجهها. ولتعزيز دقة النتائج، تم اختيار عينة عشوائية متنوعة من الكوادر الفنية والإدارية في الوزارة، بما يضمن تمثيل مختلف التوجهات الاستراتيجية والتطبيقات العملية داخل بيئة العمل. كما تستند الدراسة إلى مراجعة الوثائق التنظيمية والسياسات الداخلية لوزارة البيئة والمياه والزراعة، لضمان تقاطع الممارسات الميدانية مع النصوص القانونية الوطنية المنظمة لحماية البيانات الشخصية. وتستهدف هذه الدراسة الكوادر العاملة في الإدارات الفنية والتقنية بالوزارة، حيث اعتمدت عينة ممثلة تضم موظفين ومختصين في أمن المعلومات لضمان شمولية النتائج في تحديد العقبات التي تواجه التطبيق الأمثل لسياسات الخصوصية. ويرتكز هذا المنهج على المزاوجة بين الأدوات الكمية والنوعية لضمان إحاطة شاملة بالموضوع، إذ توفر الاستبيانات قياسات دقيقة لوعي الموظفين، في حين تتيح المقابلات رصد التحديات التقنية والإدارية التي تواجه عمليات حماية البيانات. وتكتمل هذه الجهود، تعتمد الدراسة على خطة عمل منظمة تتكون من ثلاث مراحل رئيسية؛ تبدأ بمراجعة دقيقة ما كتبه الباحثون سابقاً لتحديد جوانب حماية المعلومات والمخاطر الإلكترونية، تليها مرحلة المقابلات المعمقة لفهم أسباب هذه المخاطر، وتنتهي ببناء نموذج تحليلي شامل لاختبار فاعلية إجراءات الحماية المعمول بها. ولتحقيق ذلك، تتبع هذه الدراسة نهجاً منظماً يغطي كافة مراحل البحث، بدءاً من الأسس النظرية وصولاً إلى أدوات جمع المعلومات، لضمان فهم دقيق لطريقة تطبيق إجراءات حماية البيانات فعلياً في الوزارة. ولتحقيق ذلك، تم تصميم استبيانات موجهة لتقييم مدى وعي الموظفين بالامتثال التنظيمي، وتحديد التحديات التقنية الفعلية التي يواجهها مختصو أمن المعلومات بالوزارة. ولتدعيم الرصانة المنهجية، اعتمدت الدراسة على مراجعة دقيقة للسياسات الداخلية وتحليل معمق لنتائج الاستبيانات، مما وفر تقييماً دقيقاً لفاعلية إجراءات الأمن ومستوى الالتزام باللوائح. كما شمل الإطار المنهجي استبيانات تقنية موجهة لمديري وحدات معالجة البيانات، لاستجلاء التحديات التشغيلية التي تواجه الامتثال لمعايير الخصوصية الوطنية.

مجتمع البحث

-عينة من موظفين البيئة المياه والزراعة.

-عينة من مراجعين وزارة البيئة والمياه والزراعة.

حدود البحث

- الحدود الموضوعية :تقتصر الدراسة على تناول موضوع حماية الخصوصية والبيانات الشخصية في الوزارات الحكومية من الناحيتين التشريعية والتطبيقية، دون التطرق إلى الجوانب التقنية العميقة المتعلقة بالأمن السيبراني بتفاصيلها الهندسية.

- الحدود المكانية :اقتصرت الدراسة التطبيقية على وزارة البيئة والمياه والزراعة في المملكة العربية السعودية بوصفها أنموذجًا للوزارات الحكومية.
- الحدود الزمانية :اعتمدت الدراسة على الوثائق والسياسات والتشريعات النافذة حتى تاريخ إعداد هذا البحث، وما صدر من تعديلات على نظام حماية البيانات الشخصية ولوائحه التنفيذية.
- الحدود البشرية :اعتمدت الدراسة على تحليل الوثائق والسياسات الرسمية المعلنة، دون إجراء مسح ميداني شامل لموظفي الوزارة أو المستفيدين من خدماتها، وهو ما يفتح المجال أمام دراسات ميدانية مستقبلية.

الفصل الرابع

النتائج والتوصيات

مقدمة

تناولت هذه الدراسة موضوع حماية الخصوصية في الوزارات الحكومية السعودية، من خلال دراسة تطبيقية على وزارة البيئة والمياه والزراعة بوصفها أنموذجاً، وذلك عبر استعراض الإطار المفاهيمي للخصوصية والبيانات الشخصية، وتحليل الإطار التشريعي والمؤسسي المتمثل في نظام حماية البيانات الشخصية وجهاته الإشرافية، ثم تحليل الواقع التطبيقي للوزارة محل الدراسة من خلال سياستها المعلنة وآلياتها التقنية والإدارية، وصولاً إلى رصد أبرز التحديات وصياغة توصيات عملية.

وقد خلصت الدراسة إلى أن المملكة العربية السعودية قطعت شوطاً تشريعياً ومؤسسياً متقدماً في بناء منظومة وطنية لحماية البيانات الشخصية، تمثلت في نظام حماية البيانات الشخصية وتعديلاته، وفي الأدوار المتكاملة لكل من سدايا ومكتب إدارة البيانات الوطنية وهيئة الحكومة الرقمية والهيئة الوطنية للأمن السيبراني. كما خلصت إلى أن وزارة البيئة والمياه والزراعة أظهرت التزاماً معلناً وموثقاً بمتطلبات هذا النظام، من خلال سياستها الرسمية المعلنة وتسجيل منصات الإللكترونية، إلا أن هناك مجالات واضحة للتحسين، خصوصاً في الجوانب الإجرائية التفصيلية المرتبطة بتنفيذ حقوق أصحاب البيانات، والشفافية في التعامل مع الحوادث الأمنية، وبناء الوعي المؤسسي الشامل لدى جميع منسوبي الوزارة.

وتؤكد الدراسة أن تحقيق حماية فعّالة وشاملة للخصوصية في القطاع الحكومي لا يتحقق بمجرد الامتثال الشكلي للنصوص التشريعية، بل يستلزم ترسيخ ثقافة مؤسسية راسخة، ودعمًا قياديًا مستمرًا، واستثمارًا متوازنًا في الجوانب التقنية والبشرية والمالية. وتأمل الدراسة أن تشكل نتائجها وتوصياتها إضافة نوعية تسهم في دعم مسيرة التحول الرقمي الحكومي في المملكة العربية السعودية، بما يحقق التوازن المنشود بين تقديم خدمات حكومية رقمية متطورة وكفاءة، وبين صون خصوصية المواطنين والمقيمين وحماية بياناتهم الشخصية.

تحليل البيانات

النتائج

إن ترسيخ مبادئ الأمن السيبراني ضمن الممارسات اليومية للموظفين يعزز جاهزيتهم في التعامل مع المخاطر المتغيرة ويجعل بيئة العمل أكثر مرونة وقدرة على الاستجابة للمتطلبات الأمنية المتجددة. وفي هذا الإطار، يصبح من الضروري تعزيز الانضباط التنظيمي عبر تطبيق نماذج حوكمة تربط بين مسؤوليات الأفراد والحلول التقنية المتطورة، بهدف خفض المخاطر السيبرانية وضمان الاستمرار في تطبيق المعايير الأمنية. كما تشير الأدلة الميدانية إلى أن دمج ثقافة الأمن السيبراني ضمن الروتين اليومي للموظفين يسهم بشكل مباشر في تحسين مستويات التكيف التنظيمي، مما يقلل بدوره من احتمالات السلوك غير المتوافق مع السياسات المعتمدة. علاوة على ذلك، أظهرت النتائج أن ضعف الوصول إلى سياسات أمن المعلومات المحدثة يؤدي إلى تزايد السلوكيات غير الامتثالية، حيث أعربت نسبة كبيرة من المشاركين عن صعوبة في تحديد آليات الاطلاع على التعديلات التنظيمية. ويستلزم هذا القصور في قنوات التواصل التنظيمي من الوزارة ضرورة تفعيل منصات رقمية تفاعلية تتيح وصولاً مباشراً للمستجدات السياسية، بما يضمن تزويد الموظفين بالمعارف والمهارات اللازمة للتعامل الأمن مع البيانات الحساسة، وهو ما من شأنه تقليل المخاطر التشغيلية التي قد تنشأ نتيجة تضارب الممارسات الفردية مع المعايير الأمنية المعتمدة. علاوة على ذلك، يقتضي رفع مستوى الوعي الرقمي تجاوز الاكتفاء بالالتزام الظاهري بالقواعد، والعمل على ترسيخ حس المسؤولية الشخصية لدى الموظفين تجاه حماية الأصول المعلوماتية، مما يحد بشكل فعال من احتمالية تحول الفرد إلى نقطة ضعف في المنظومة الأمنية. وضمن هذا التوجه، يسهم اعتماد آليات للإبلاغ السري عن الثغرات أو الحوادث الأمنية في خلق بيئة عمل قائمة على الشفافية، مما يكسر حاجز الخوف لدى الموظفين ويؤدي إلى سرعة التعامل مع التهديدات السيبرانية بفاعلية أكبر. وتؤكد الدراسات أن الانتقال من مجرد التقيد الحرفي بالتعليمات إلى تعزيز حس المسؤولية الفردية يسهم في

تحويل الموظفين إلى حائط صد أول، يحرص على حماية بيانات الوزارة كجزء أصيل من مهامهم اليومية.

التوصيات

بناءً على ما تم استعراضه من إطار مفاهيمي وتشريعي، وتحليل واقع تطبيقي على وزارة البيئة والمياه والزراعة، ورصد لأبرز التحديات القائمة، يقدم هذا الفصل مجموعة من التوصيات العملية الموجهة إلى وزارة البيئة والمياه والزراعة تحديداً، وأخرى موجهة إلى الوزارات والجهات الحكومية بصفة عامة.

أولاً: توصيات موجهة إلى وزارة البيئة والمياه والزراعة

- تطوير قناة إلكترونية مخصصة وواضحة ضمن منصات الوزارة لتمكين المستفيدين من تقديم طلبات الوصول إلى بياناتهم أو تصحيحها أو طلب إتلافها، بما يعزز الشفافية العملية لا النظرية فقط.
- الإفصاح عن جهة اتصال محددة كمسؤول حماية البيانات أو إدارة مختصة يمكن للمستفيدين التواصل معها بشأن استفساراتهم أو شكاواهم المتعلقة بخصوصية بياناتهم، تعزيزاً لمبدأ المساءلة والشفافية.
- إصدار دليل إجرائي داخلي تفصيلي يوضح لكل وكالة من وكالات الوزارة البيئة، والمياه، والزراعة، والثروة السمكية كيفية تطبيق مبادئ حماية البيانات على طبيعة البيانات الخاصة بها، مع تخصيص إرشادات لبيانات الحيازات الزراعية وتراخيص الآبار.
- تصميم برنامج تدريبي إلزامي دوري لجميع منسوبي الوزارة، بما يشمل الموظفين الميدانيين في الفروع والمكاتب الزراعية، لرفع الوعي بأحكام نظام حماية البيانات الشخصية وتبعاتها التأديبية.
- إجراء مراجعة دورية تدقيق داخلي لمدى امتثال الأنظمة والمنصات الإلكترونية للوزارة لمتطلبات نظام حماية البيانات الشخصية والمعايير الوطنية لإدارة البيانات، مع توثيق نتائج هذه المراجعات ومتابعة معالجة الفجوات.

- اعتماد آلية معلنه للإبلاغ عن حوادث تسريب أو اختراق البيانات، تتضمن جدولاً زمنياً واضحاً للإبلاغ عن الحادثة لكل من الجهة المختصة وأصحاب البيانات المتضررين، تماشياً مع مبدأ الشفافية والاستجابة السريعة.
- تعزيز التكامل بين إدارات تقنية المعلومات والإدارات القانونية والتنظيمية داخل الوزارة، بحيث تصبح حماية الخصوصية جزءاً أصيلاً من دورة تصميم أي خدمة إلكترونية جديدة منذ مراحلها الأولى) نهج الخصوصية منذ التصميم.
- ثانياً: توصيات موجهة إلى الوزارات والجهات الحكومية بصفة عامة
- توحيد الحد الأدنى من متطلبات الإفصاح في سياسات الخصوصية المعلنه عبر جميع الجهات الحكومية، بحيث تتضمن جميعها عناصر موحدة كآلية تفعيل الحقوق وجهة الاتصال وآلية الإبلاغ عن الحوادث.
- إنشاء منصة وطنية موحدة أو دليل إرشادي قطاعي متخصص يوضح كيفية تطبيق نظام حماية البيانات الشخصية على أنماط البيانات الخاصة بكل قطاع حكومي بالتنسيق مع سدايا.
- تفعيل برامج قياس دوري لمستوى نضج حماية البيانات في الجهات الحكومية، ونشر مؤشرات أداء عامة (دون الإفصاح عن تفاصيل تقنية حساسة) تحفز الجهات على التحسين المستمر والمنافسة الإيجابية في هذا المجال.
- دعم برامج بناء القدرات الوطنية المتخصصة في حوكمة البيانات وحماية الخصوصية، من خلال برامج تدريب وشهادات مهنية معتمدة، وتحفيز الجامعات على استحداث برامج أكاديمية متخصصة في هذا المجال.

المراجع

-المراجع العربية-

- الهيئة السعودية للبيانات والذكاء الاصطناعي سدايا sdaia.gov.sa
- هيئة الحكومة الرقمية dga.gov.sa -
- الهيئة الوطنية للأمن السيبراني nca.gov.sa -
- وزارة البيئة والمياه والزراعة mewa.gov.sa -
- هيئة الخبراء بمجلس الوزراء منصة الأنظمة السعودية laws.boe.gov.sa
- الرحاحله، أ.م.أ.، (2025). دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني. *Humanitarian and Natural Sciences Journal*, 6(10), pp. 1325–1344. doi:10.53796/hnsj610/23.
- القاضي، أ.ب.أ. and قرادة، ن.ع.ع.، (2026). فاعلية الأمن السيبراني في حماية الأنظمة المالية بالمؤسسات العامة. *Comprehensive Journal of Science*, 10(39), pp. 1325–1344. doi:10.65405/hw9y9084.
- محروق، ش.أ.، et al. (2025). الاعتبارات الأخلاقية في دمج الذكاء الاصطناعي في رؤية المملكة العربية السعودية 2030 للتعليم "مجلة ابن خلدون للدراسات والأبحاث". 5(3). doi:10.56989/benkj.v5i3.1402.

-المراجع الأجنبية-

- Khawaji, A. and Martin, R.J. (2026) "ML-Based Threat Severity Detection in Cyber-Physical Systems for Smart Environments Using Behavioral Analysis," *Human-Centric Intelligent Systems* [Preprint]. doi:10.1007/s44230-026-00134-9.
- Markiewicz, I. (2026) "Cybersecurity management in organizations as a component of modern management systems: Integrating governance, risk, and continuous improvement," *Nowoczesne Systemy Zarządzania*, 21(1), pp. 41–52. doi:10.37055/nsz/218590.
- Uchendu, B. et al. (2021) "Developing a cyber security culture: Current practices and future needs," *arXiv (Cornell University)*, 109, pp. 102387–102387. doi:10.1016/j.cose.2021.102387.

الملاحق

-الاستبانة

مرفق في ملف ورد منفصل

Abstract الملخص

هدفت هذه الدراسة إلى تسليط الضوء على واقع حماية الخصوصية والبيانات الشخصية في الوزارات الحكومية بالمملكة العربية السعودية، من خلال اتخاذ وزارة البيئة والمياه والزراعة أنموذج تطبيقياً، وذلك في ظل التوسع الكبير الذي تشهده الجهات الحكومية في تقديم خدماتها إلكترونياً، وما يصاحب ذلك من جمع ومعالجة كميات ضخمة من البيانات الشخصية للمستفيدين من المزارعين وملاك الآبار والمنشآت البيئية والمشاركين في خدمات المياه.

واعتمدت الدراسة المنهج الوصفي التحليلي القائم على تحليل الوثائق الرسمية، ويشمل ذلك نظام حماية البيانات الشخصية ولوائحه التنفيذية، والسياسات المعلنة للوزارة محل الدراسة، إضافة إلى الأدبيات العلمية والتقارير الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي وهيئة الحكومة الرقمية.

وتناولت الدراسة في إطارها النظري مفهوم الخصوصية وتطوره، ومفهوم البيانات الشخصية وأنواعها، وأهمية حمايتها في القطاع الحكومي، ثم استعرضت الإطار التشريعي والمؤسسي لحماية البيانات في المملكة، متمثلاً في نظام حماية البيانات الشخصية وأدواره التنظيمية. كما خصصت فصلاً مستقلاً لتحليل واقع تطبيق وزارة البيئة والمياه والزراعة لمتطلبات حماية الخصوصية، من خلال دراسة سياساتها المعلنة وآلياتها التقنية والإدارية، وتحديد أبرز التحديات التي تواجهها.

وقد توصلت الدراسة إلى مجموعة من النتائج، أبرزها أن الوزارة اتخذت خطوات معلنة ومسجلة رسمياً نحو الامتثال لنظام حماية البيانات الشخصية، إلا أن هناك حاجة إلى مزيد من الوضوح في آليات تفعيل حقوق أصحاب البيانات، وتعزيز الوعي المؤسسي، وبناء قدرات بشرية متخصصة في حوكمة البيانات. وخلصت الدراسة إلى عدد من التوصيات الموجهة للوزارة ولبقية الجهات الحكومية، إلى جانب مقترحات لبحوث مستقبلية في هذا المجال الحيوي والمتجدد.

Midocean University

College of Management

Department of master of risk management



Title in English

**Privacy Protection in Government Ministries: The Ministry of Environment,
Water and Agriculture as a Model**

Prepared by:

Mohammed saed ali alsharif

Supervised by:

D.ALfaisal abduhamed

D.Faiz grrad

Year 2026

بحث علمي – أداة الدراسة

استبانة حول واقع حماية الخصوصية في الوزارات الحكومية

دراسة حالة: وزارة البيئة والمياه والزراعة – المملكة العربية السعودية

أخي المشارك / أختي المشاركة الكريمة،

تهدف هذه الاستبانة إلى جمع البيانات اللازمة لبحث علمي يتناول واقع حماية الخصوصية في الوزارات الحكومية بالمملكة العربية السعودية، من خلال دراسة حالة وزارة البيئة والمياه والزراعة. وتتكون الأداة من ثلاث استبانات متكاملة: استبانة مُقيّدة (مغلقة) بعبارات تُقاس واستبانة حرة (مفتوحة) بأسئلة تتيح لك التعبير عن رأيك بحرية، واستبانة مختلطة تجمع بين النوعين معاً.

يُرجى التكرم بقراءة كل عبارة أو سؤال بعناية والإجابة عنه بكل موضوعية ، علماً بأن جميع البيانات ستُستخدم لأغراض البحث العلمي فقط، وستُعامل بسرية تامة، ولن تُنسب أي إجابة إلى صاحبها بأي شكل من الأشكال.

شاكرين لكم حسن تعاونكم، وما ستقدمونه من وقت وجهد يُسهمان في إثراء هذا البحث والخروج بنتائج وتوصيات ذات فائدة عملية.

القسم الأول: الاستبيان المُقيّد (المغلق)

يتكوّن هذا القسم من مجموعة عبارات مغلقة موزعة على خمسة محاور رئيسة، يُطلب منك تحديد درجة موافقتك على كل عبارة من خلال وضع علامة (X) أمام الخيار المناسب وفق مقياس ليكرت الخماسي (أوافق بشدة، أوافق، محايد، لا أوافق، لا أوافق بشدة).

أولاً: البيانات الأولية

الجنس: ☐ ذكر ☐ أنثى

العمر: ☐ أقل من 30 سنة ☐ من 30 إلى أقل من 40 ☐ من 40 إلى أقل من 50 ☐ 50 سنة فأكثر

المؤهل العلمي: ☐ ثانوي فأقل ☐ بكالوريوس ☐ دراسات عليا (ماجستير / دكتوراه)

الإدارة / القطاع الذي تعمل به:

سنوات الخبرة: ☐ أقل من 5 سنوات ☐ من 5 إلى أقل من 10 ☐ من 10 إلى أقل من 15 ☐ 15 سنة فأكثر

هل سبق لك التعامل مع بيانات شخصية للمستفيدين أو الموظفين أثناء أداء مهام عملك؟ ☐ نعم ☐ لا

ثانياً: محاور الاستبانة (عبارات مغلقة)

المحور الأول: الإطار التنظيمي والسياسات المتعلقة بحماية الخصوصية

البيان	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
توجد لدى الوزارة سياسة واضحة ومكتوبة لحماية خصوصية البيانات الشخصية.	☐	☐	☐	☐	☐
تلتزم الوزارة بأحكام نظام حماية البيانات الشخصية الصادر في المملكة العربية السعودية.	☐	☐	☐	☐	☐
يتم تحديث السياسات والإجراءات المتعلقة بالخصوصية بشكل دوري لمواكبة المستجدات.	☐	☐	☐	☐	☐
تتوفر لدى الموظفين معرفة كافية بالسياسات والإجراءات المتعلقة بحماية الخصوصية.	☐	☐	☐	☐	☐
يوجد جهة أو إدارة مختصة داخل الوزارة مسؤولة عن متابعة الالتزام بحماية الخصوصية.	☐	☐	☐	☐	☐

المحور الثاني: الإجراءات التقنية والأمنية لحماية البيانات

البيان	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
تستخدم الوزارة أنظمة تقنية حديثة لحماية البيانات الشخصية من الاختراق أو التسريب.	☐	☐	☐	☐	☐
يتم تشفير البيانات الشخصية الحساسة المخزنة في أنظمة الوزارة.	☐	☐	☐	☐	☐
تُطبق الوزارة آلية للتحكم في صلاحيات الوصول إلى البيانات الشخصية حسب طبيعة العمل.	☐	☐	☐	☐	☐
تُجرى اختبارات واختراقات دورية لتقييم مدى أمان الأنظمة التقنية الخاصة بالبيانات.	☐	☐	☐	☐	☐
توجد آلية واضحة للتعامل مع الحوادث الأمنية المتعلقة باختراق أو تسريب البيانات.	☐	☐	☐	☐	☐

المحور الثالث: وعي وتدريب الموظفين حول حماية الخصوصية

البيان	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
تحرص الوزارة على تدريب موظفيها بشكل دوري على أسس حماية الخصوصية وأمن المعلومات.	☐	☐	☐	☐	☐
يدرك الموظفون أهمية حماية خصوصية بيانات المستفيدين والمتعاملين مع الوزارة.	☐	☐	☐	☐	☐
تتوفر لدى الموظفين إرشادات واضحة حول كيفية التعامل مع البيانات الشخصية.	☐	☐	☐	☐	☐
يشارك الموظفون في برامج توعية حول المخاطر المرتبطة بانتهاك الخصوصية.	☐	☐	☐	☐	☐
يتحمل الموظفون مسؤولية واضحة عند التعامل غير السليم مع البيانات الشخصية.	☐	☐	☐	☐	☐

المحور الرابع: آليات الرقابة والمساءلة

البيان	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
توجد آليات رقابية فعالة لضمان الالتزام بمعايير حماية الخصوصية داخل الوزارة.	☐	☐	☐	☐	☐
يتم محاسبة الموظفين الذين يخالفون سياسات حماية الخصوصية بشكل واضح وعادل.	☐	☐	☐	☐	☐
تتوفر قنوات واضحة للإبلاغ عن أي انتهاك محتمل لخصوصية البيانات.	☐	☐	☐	☐	☐
تخضع الوزارة لتدقيق دوري (داخلي أو خارجي) للتحقق من التزامها بحماية الخصوصية.	☐	☐	☐	☐	☐
يتم إشراك المستفيدين في معرفة حقوقهم المتعلقة بخصوصية بياناتهم لدى الوزارة.	☐	☐	☐	☐	☐

المحور الخامس: التحديات والمعوقات

البيان	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
تواجه الوزارة تحديات تقنية تحد من قدرتها على تطبيق معايير حماية الخصوصية بشكل كامل.	☐	☐	☐	☐	☐
يشكل نقص الكوادر المتخصصة في أمن المعلومات وحماية البيانات تحديًا أمام الوزارة.	☐	☐	☐	☐	☐
تُعد محدودية الموارد المالية عائقًا أمام تطوير أنظمة حماية الخصوصية.	☐	☐	☐	☐	☐
يمثل التوسع في استخدام التقنيات الحديثة (الذكاء الاصطناعي، الحوسبة السحابية) تحديًا إضافيًا لحماية الخصوصية.	☐	☐	☐	☐	☐
يؤدي ضعف الوعي المجتمعي بأهمية الخصوصية إلى تحديات في تطبيق السياسات المتعلقة بها.	☐	☐	☐	☐	☐

القسم الثاني: الاستبيان الحر (المفتوح)

يتضمن هذا القسم أسئلة مفتوحة تتيح لك التعبير عن رأيك ووجهة نظرك بحرية تامة وبأسلوبك الخاص، دون التقيّد بخيارات محددة مسبقًا. يُرجى الإجابة عن الأسئلة التالية في المساحة المخصصة لكل سؤال.

1. من وجهة نظرك، ما مفهوم "حماية الخصوصية" في سياق عمل الوزارات الحكومية؟

2. صف بإيجاز الإجراءات التي تتبعها وزارة البيئة والمياه والزراعة حاليًا لحماية البيانات الشخصية للموظفين والمستفيدين.

3. ما أبرز التحديات التي تواجه الوزارة في تطبيق معايير حماية الخصوصية من وجهة نظرك؟

4. هل مررت بموقف أو سمعت عن حالة تتعلق بانتهاك خصوصية بيانات داخل الوزارة؟ إن وُجدت، صف الموقف وكيف تم التعامل معه.

5. ما مدى كفاية التشريعات الحالية (مثل نظام حماية البيانات الشخصية) في تنظيم عمل الوزارة فيما يتعلق بالخصوصية؟ وضح إجابتك.

6. برأيك، ما الدور الذي تلعبه التقنيات الحديثة (الذكاء الاصطناعي، الحوسبة السحابية، إنترنت الأشياء) في التأثير على خصوصية البيانات داخل الوزارة؟

7. ما مقترحاتك وتوصياتك لتعزيز مستوى حماية الخصوصية في وزارة البيئة والمياه والزراعة؟
