



جامعة ميدأوشن

كلية الإدارة

قسم / تخصص إدارة أعمال

دور الحكومات في تعزيز حماية البيانات الشخصية في القطاعات الخاصة في المملكة العربية السعودية:

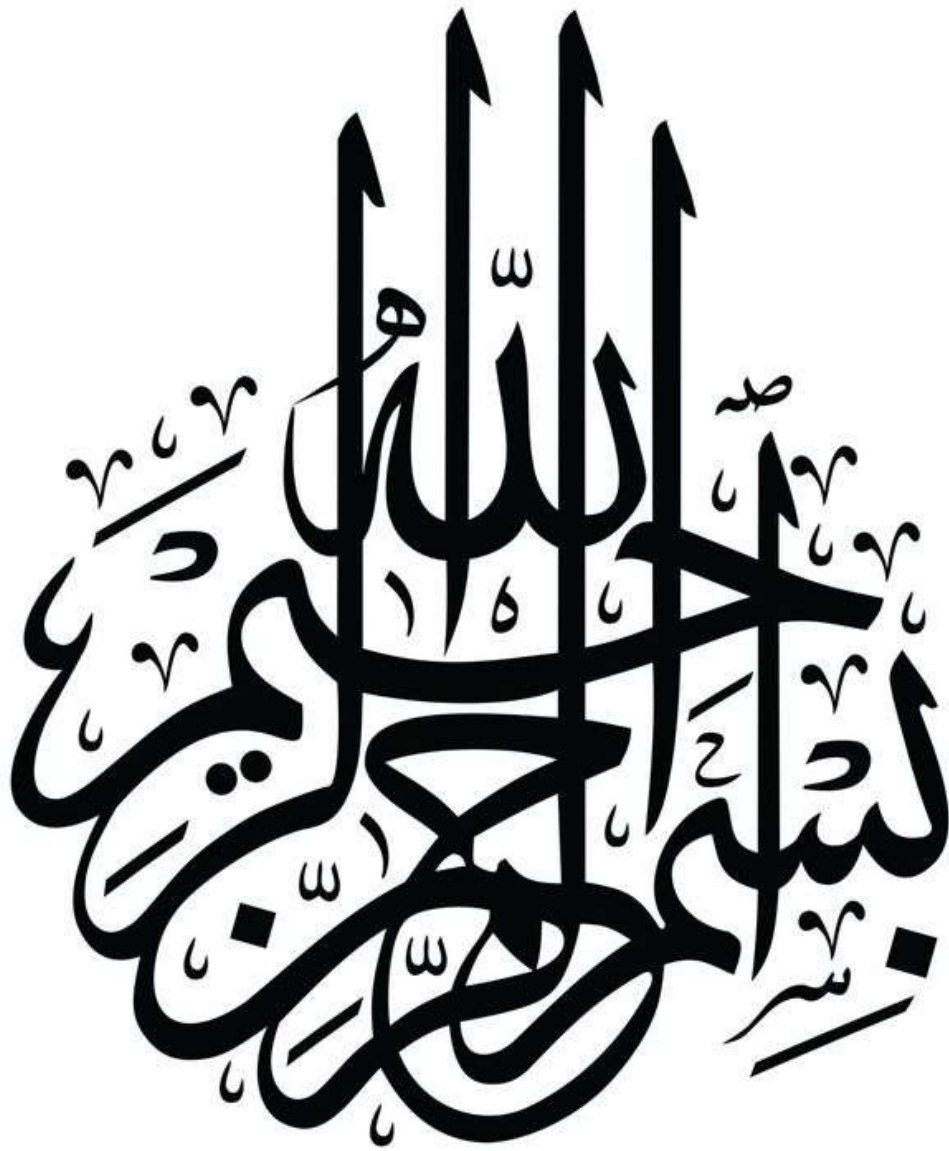
دراسة لقانون حماية البيانات الشخصية

اعداد الطالبة / ضحى خالد القوصي

الرقم الجامعي / 242001584

العام الدراسي

2025



إهداء

إلى كل من كان له الأثر في رحلتي العلمية والعملية، إلى من غرس في قلبي حب المعرفة والسعي الدائم
نحو التطوير...

إلى والديّ العزيزين، اللذين كانا دائماً سندي وملهمي، بفضل دعائكما وتشجيعكما المستمر استطعت المضي
قدماً بثقة وعزيمة.

إلى أساتذتي الأفاضل، الذين لم يبخلوا بعلمهم وتوجيهاتهم، فكان لهم الدور الأكبر في تنمية فكري وتوسيع
آفاقي العلمية.

إلى أصدقائي وزملائي، الذين شاركوني هذه المسيرة بكل ما فيها من تحديات وإنجازات، فكنتم خير رفاق
الطريق.

وأخيراً، إلى كل من يسعى لنشر العلم والمعرفة، إلى كل من يعمل بجد لإحداث فرق في هذا العالم... أهدي
هذا العمل بامتنان وتقدير.

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تتحقق الطموحات.

أتقدم بخالص الشكر والتقدير لكل من ساهم في إنجاز هذا البحث وساندي خلال رحلتي العلمية.

أولاً، إلى والديّ العزيزين، اللذين كانا مصدر دعمي وإلهامي، بفضل صبركما وتشجيعكما المستمر استطعت تجاوز التحديات والوصول إلى هذه المرحلة.

إلى أساتذتي الكرام، الذين لم يخلوا بعلمهم وتوجيهاتهم القيّمة، وكان لهم الدور الأكبر في تطوير فكري وصقل مهاراتي البحثية، جزاكم الله خير الجزاء.

إلى زملائي وأصدقائي، الذين كانوا عوناً وسنداً، وشاركوا معي هذه الرحلة بكل ما فيها من تحديات وتحفيز، لكم مني كل الامتنان والتقدير.

كما أتوجه بالشكر لكل من قدم لي المساعدة أو أتاح لي الفرصة لاكتساب المعرفة، سواء من خلال النقاشات المثمرة أو المصادر العلمية التي ساهمت في إثراء هذا البحث.

وأخيراً، إلى كل من يسعى لنشر العلم والمعرفة، وإلى كل من يؤمن بأن البحث العلمي هو مفتاح التقدم والتطور...

شكراً لكم جميعاً.

المخلص

يهدف هذا البحث إلى دراسة دور الحكومة في تعزيز حماية البيانات الشخصية داخل القطاعات الخاصة في المملكة العربية السعودية، من خلال تحليل مدى تأثير التشريعات والرقابة الحكومية والمبادرات الداعمة على مستوى امتثال المؤسسات الخاصة لقانون حماية البيانات الشخصية. تم استخدام المنهج الوصفي التحليلي لجمع البيانات وتحليلها، حيث شملت الدراسة مجموعة من المؤسسات الخاصة لتقييم مستوى التزامها باللوائح والقوانين ذات الصلة.

أظهرت النتائج أن هناك علاقة إيجابية قوية بين الجهود الحكومية ومستوى الامتثال، حيث ساهمت التشريعات الواضحة والرقابة الفعالة في تحسين التزام المؤسسات بالقانون. كما كشفت الدراسة عن وجود تحديات تواجه القطاعات الخاصة، مثل نقص الوعي لدى الموظفين، وضعف الدعم التقني، وقلة الموارد المالية، مما يؤثر على قدرتها على تحقيق الامتثال الكامل. بالإضافة إلى ذلك، تبين أن المبادرات الحكومية، مثل تقديم الإرشادات، والدورات التدريبية، والدعم المالي، لها دور إيجابي في تعزيز الامتثال وتحسين سياسات حماية البيانات داخل المؤسسات الخاصة.

بناءً على هذه النتائج، توصي الدراسة بضرورة تعزيز الوعي حول قانون حماية البيانات الشخصية من خلال حملات توعوية ودورات تدريبية، بالإضافة إلى توفير حوافز مالية وتقنية للمؤسسات الصغيرة والمتوسطة لدعم امتثالها للقانون.

الكلمات المفتاحية: حماية البيانات الشخصية، الامتثال، التشريعات، الرقابة الحكومية، القطاع الخاص، المملكة العربية السعودية.

Abstract

This study aims to examine the role of the government in enhancing personal data protection within the private sector in Saudi Arabia. It analyzes the impact of legislation, government oversight, and supportive initiatives on the level of compliance among private sector institutions with the Personal Data Protection Law. The study employs a descriptive-analytical approach to collect and analyze data, focusing on various private organizations to assess their adherence to relevant regulations and laws.

The findings indicate a strong positive relationship between government efforts and compliance levels. Clear legislation and effective oversight have significantly improved institutional adherence to the law. However, the study also highlights several challenges facing the private sector, including a lack of employee awareness, weak technical support, and limited financial resources, which hinder full compliance. Additionally, government initiatives such as providing guidelines, training programs, and financial support play a crucial role in promoting compliance and strengthening data protection policies within private institutions.

Based on these findings, the study recommends increasing awareness of personal data protection laws through awareness campaigns and training programs. Furthermore, it suggests providing financial and technical incentives to small and medium-sized enterprises (SMEs) to support their compliance efforts. Simplifying regulations and procedures to facilitate compliance and fostering public-private partnerships to develop more adaptable policies are also recommended.

Keywords: Personal data protection, compliance, legislation, government oversight, private sector, Saudi Arabia.

المحتويات

5.....	الملخص
6.....	Abstract
12.....	الفصل الأول : المقدمة
13.....	المقدمة
14.....	أهمية الدراسة
15.....	مشكلة الدراسة
16.....	أهداف البحث
17.....	تساؤلات الدراسة
17.....	حدود الدراسة
19.....	الفصل الثاني: الدراسات السابقة
20.....	الدراسات السابقة
26.....	الإطار النظري
26.....	مفهوم حماية البيانات الشخصية:
29.....	مبادئ حماية البيانات المتعارف عليها دوليًا.
32.....	أهمية حماية البيانات في تعزيز الثقة بين الأفراد والقطاعات الخاصة
34.....	الأطر النظرية لحماية البيانات الشخصية
36.....	العلاقة بين حماية البيانات وحقوق الإنسان
38.....	تأثير حماية البيانات على الابتكار والتطور التكنولوجي
40.....	وضع السياسات والتشريعات اللازمة لحماية البيانات

43.....	أهداف نظام حماية البيانات الشخصية
52.....	التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام
54.....	دور الحكومة في دعم القطاعات الخاصة للامتثال:
56.....	الفصل الثالث: المنهجية
57.....	المقدمة
57.....	تصميم البحث
57.....	مجتمع وعينة الدراسة
58.....	أداة جمع البيانات
58.....	إجراءات جمع البيانات
58.....	تحليل البيانات
59.....	أخلاقيات البحث
59.....	الخاتمة
60.....	الفصل الرابع: مناقشة النتائج
61.....	المتغيرات الديموغرافية لعينة الدراسة
66.....	الإحصاء الوصفي
72.....	اختبار الفرضيات
77.....	الفصل الخامس
77.....	النتائج والتوصيات
78.....	خاتمة
80.....	النتائج

82.....	التوصيات
85.....	البحوث المستقبلية
87.....	المراجع
91.....	الملاحق

قائمة الجداول

- جدول 1 توزيع عينة الدراسة وفقاً للجنس.....61
- جدول 2 توزيع عينة الدراسة وفقاً للعمر.....62
- جدول 3 توزيع عينة الدراسة وفقاً لسنوات الخبرة.....64
- جدول 4 المتوسطات الحسابية والانحرافات المعيارية لمحور مدى الامتثال لنظام حماية البيانات الشخصية.....66
- جدول 5 المتوسطات الحسابية والانحرافات المعيارية لمحور التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام.....68
- جدول 6 المتوسطات الحسابية والانحرافات المعيارية لمحور دور الحكومة في دعم الامتثال.....70

قائمة الأشكال

- رسم توضيحي 1 توزيع عينة الدراسة وفقاً للجنس 62
- رسم توضيحي 2 توزيع عينة الدراسة وفقاً للعمر 63
- رسم توضيحي 3 توزيع عينة الدراسة وفقاً لسنوات الخبرة 65

الفصل الأول: المقدمة

المقدمة

في العصر الرقمي الحديث، أصبحت البيانات الشخصية من أهم الأصول التي يتم جمعها واستخدامها من قبل الشركات والحكومات على حد سواء فهي تتنوع في استخدامها عبر مختلف المجالات، مثل التجارة الإلكترونية التي تعتمد بشكل أساسي على البيانات لتخصيص العروض وتحسين تجربة المستخدم، وكذلك في تقديم الخدمات الحكومية حيث يتم جمع بيانات المواطنين لتحسين الأداء الحكومي وتسهيل الوصول إلى الخدمات. بالإضافة إلى ذلك، تلعب البيانات الشخصية دورًا محوريًا في القطاع الصحي، حيث يتم استخدام سجلات المرضى وبياناتهم الطبية لتقديم رعاية صحية مخصصة وفعالة، ومع تزايد الاعتماد على التكنولوجيا في جميع جوانب الحياة، ازداد القلق بشأن كيفية جمع هذه البيانات ومعالجتها واستخدامها، خاصة مع تزايد حالات الاختراقات الأمنية وسوء استخدام البيانات من قبل جهات غير موثوقة أو حتى من قبل أطراف غير مختصة. هذا القلق يعكس الخوف من تهديدات خصوصية الأفراد، مما يجعل حماية البيانات الشخصية أمرًا بالغ الأهمية لضمان أمن الأفراد وحفظ خصوصياتهم في بيئة متصلة بشكل متزايد؛ لذلك، أصبحت حماية البيانات الشخصية تحديًا عالميًا يستدعي تدخلًا قانونيًا وتنظيميًا على مستوى الحكومات والهيئات التشريعية لضمان حماية حقوق الأفراد. في هذا السياق، تبنت العديد من الدول قوانين وتشريعات لحماية البيانات الشخصية، ومن أبرز هذه التشريعات قانون حماية البيانات الشخصية (PDPL) في المملكة العربية السعودية. في ظل التقدم السريع في التحول الرقمي الذي تشهده المملكة بموجب رؤية 2030، ظهرت الحاجة إلى وضع إطار قانوني قوي لتنظيم وحماية البيانات الشخصية. جاء قانون حماية البيانات الشخصية (PDPL) كأحد المبادرات الرائدة التي تهدف إلى تحقيق هذا الهدف، حيث يحدد معايير صارمة لجمع البيانات، ومعالجتها، وتخزينها، ويضمن حقوق الأفراد في الوصول إلى بياناتهم والتحكم فيها، وتعتبر هذه الدراسة بمثابة تسليط الضوء على دور الحكومات في تعزيز

حماية البيانات الشخصية، مع التركيز على التجربة السعودية في تطبيق هذا القانون في القطاعات الخاصة، وكيفية تأثير ذلك على الأفراد والمؤسسات. تهدف الدراسة أيضًا إلى تحليل التأثيرات المحتملة لهذا القانون على حماية خصوصية الأفراد في عصر التكنولوجيا الرقمية، مع تقديم توصيات لتعزيز الالتزام بالقوانين وزيادة الوعي بأهمية حماية البيانات في بيئة رقمية متسارعة التغير.

أهمية الدراسة

1. التأثير على الأفراد

في العصر الرقمي، تُعتبر البيانات الشخصية أحد الأصول الأساسية التي يجب حمايتها لضمان الخصوصية الفردية. يساهم تعزيز حماية البيانات الشخصية في بناء ثقة الأفراد في التعاملات الرقمية، سواء كانت تجارية، أو تعليمية، أو صحية. فعندما يشعر الأفراد بأن معلوماتهم محمية وآمنة، يزيد ذلك من مشاركتهم في الأنشطة الرقمية، مما يؤدي إلى نمو الاقتصاد الرقمي وتعزيز المجتمع الرقمي.

2. التأثير على الشركات

من منظور الشركات، يمثل الامتثال لقوانين حماية البيانات الشخصية فرصة لتحسين سمعتها وزيادة مصداقيتها أمام العملاء. الشركات التي تلتزم بالقوانين مثل قانون حماية البيانات الشخصية (PDPL) تقلل من المخاطر القانونية، مثل العقوبات والغرامات، وتزيد من قدرة العملاء على الوثوق بخدماتها ومنتجاتها. كما يساعد الالتزام بهذه القوانين على تحسين الكفاءة التشغيلية من خلال تبني ممارسات حديثة لإدارة البيانات وحمايتها.

3. التأثير على الاقتصاد الوطني

تُعد حماية البيانات الشخصية جزءًا أساسيًا من بناء بيئة رقمية آمنة ومستدامة. عندما تُظهر الحكومات والشركات التزامًا بحماية البيانات، تصبح الدولة أكثر جاذبية للمستثمرين الدوليين الذين يبحثون عن بيئات موثوقة ومستقرة. بالإضافة إلى ذلك، يساهم ذلك في تعزيز الابتكار الرقمي، حيث يشعر المطورون والمبدعون بأمان أكبر لتطوير حلول تكنولوجية جديدة تخدم المجتمع.

مشكلة الدراسة

مع التطور التكنولوجي السريع والتحول الرقمي الذي يشهده العالم، أصبحت البيانات الشخصية أحد أهم الأصول التي تتطلب حماية فعّالة لضمان خصوصية الأفراد وسلامة المعلومات. ومع ذلك، تُواجه القطاعات الخاصة في المملكة العربية السعودية تحديات كبيرة في تحقيق الامتثال الكامل لقانون حماية البيانات الشخصية (PDPL). تكمن المشكلة الرئيسية في ضعف الوعي بمقتضيات القانون وأهميته، مما يؤدي إلى قصور في الالتزام بالإجراءات المطلوبة، وظهور حالات متكررة من خروقات البيانات التي تُعرض الأفراد لمخاطر مثل الاحتيال وانتهاك الخصوصية، وعلى الرغم من جهود الحكومة السعودية لتوفير أدوات تنظيمية ودعم القطاعات الخاصة في هذا المجال، يبقى السؤال قائمًا حول مدى كفاية هذه الأدوات لتحقيق الامتثال الكامل، وبالإضافة إلى ذلك، تواجه الشركات الصغيرة والمتوسطة تحديات تقنية وتنظيمية، مثل التكاليف المرتبطة بتطبيق السياسات والإجراءات اللازمة لحماية البيانات. من جهة أخرى، يمكن أن يؤدي عدم الامتثال إلى تأثيرات سلبية على الاقتصاد الوطني، مثل فقدان الثقة بين العملاء والمستثمرين، مما قد يؤثر سلبًا على سمعة المملكة كمركز رقمي عالمي. تعكس هذه التحديات الحاجة إلى استراتيجيات مبتكرة لدعم القطاعات الخاصة وتعزيز الامتثال،

مع التركيز على تطوير برامج توعية وتوفير الحلول التقنية المناسبة لضمان حماية البيانات وتحقيق الأهداف الوطنية في التحول الرقمي.

أهداف البحث

1. تحليل الإطار القانوني لحماية البيانات الشخصية في السعودية

يهدف البحث إلى دراسة الجوانب المختلفة لقانون حماية البيانات الشخصية (PDPL) في المملكة، بما يشمل بنوده الأساسية، ومجالات تطبيقه، والهيئات المسؤولة عن تنفيذه.

2. تقييم مدى التزام القطاعات الخاصة بتطبيق قانون PDPL

سيتم التركيز على تحليل التزام الشركات والمؤسسات الخاصة بالقانون، وكيف يؤثر ذلك على العمليات اليومية والتفاعل مع العملاء.

3. اقتراح استراتيجيات لتعزيز الامتثال وحماية البيانات

بناءً على نتائج التحليل، سيتم تقديم توصيات محددة لتعزيز الامتثال للقانون، مثل تنظيم برامج توعية، وتقديم حوافز للشركات الملتزمة، وتطوير آليات رقابية فعالة.

تساؤلات الدراسة

تهدف الدراسة للإجابة على التساؤلات التالية بشكل مفصل:

- ما مدى وعي القطاعات الخاصة في المملكة العربية السعودية بمتطلبات قانون حماية البيانات الشخصية (PDPL) ؟
- هل تمتلك الشركات المعرفة الكافية حول المتطلبات التنظيمية؟
- ما مدى التزام الشركات بتوثيق السياسات والإجراءات المتعلقة بحماية البيانات؟
- كيف يؤثر تطبيق قانون PDPL على ثقة الأفراد والشركات في التعاملات الرقمية؟
- ما العلاقة بين الامتثال للقانون وزيادة ثقة العملاء؟
- كيف يؤثر الامتثال على تعزيز الشفافية داخل القطاع الخاص؟
- ما التحديات التي تواجه القطاعات الخاصة في المملكة عند تطبيق القانون؟ وكيف يمكن التغلب عليها؟

حدود الدراسة

1. الحدود الزمانية

تمت الدراسة على مدى العامين الماضيين (2022-2024) بهدف فهم تطورات تطبيق قانون PDPL.

2. الحدود المكانية

ركز البحث على المملكة العربية السعودية مع تحليل عينات من الشركات في الرياض، جدة، والدمام لتمثيل القطاعات الخاصة.

3. الحدود المنهجية

استخدام الاستبيانات والمقابلات فقط قد يحد من شمولية النتائج.

عدم شمول جميع القطاعات الخاصة بسبب تنوعها الواسع.

الفصل الثاني: الدراسات السابقة

الدراسات السابقة

1. نجم عبدالله الشمري (2023). "حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة".

- الهدف: تهدف هذه الدراسة إلى التعرف على سياسة حماية البيانات الشخصية في المملكة العربية السعودية وأهميتها، والجهات المسؤولة عنها. كما تسعى إلى مقارنة السياسة السعودية بنظيراتها في الاتحاد الأوروبي والمملكة المتحدة، بهدف تحديد الفجوات واقتراح سبل التطوير والتحديث في هذا المجال الحيوي.

- المنهجية: اعتمدت الدراسة على تحليل الوثائق الرسمية للجهات الحكومية المعنية بسياسة حماية البيانات الشخصية، بالإضافة إلى استعراض الأدبيات ذات الصلة. تم التركيز على مقارنة السياسات والإجراءات المتبعة في السعودية مع تلك المعمول بها في الاتحاد الأوروبي والمملكة المتحدة.

- النتائج: أظهرت النتائج أن السياسة السعودية لم تتطرق إلى مفهوم "الخصوصية في التصميم والإعدادات الافتراضية (Privacy by Design and Default)"، وهو عنصر أساسي في السياسات الأوروبية والبريطانية لضمان حماية البيانات منذ المراحل الأولى لتطوير الأنظمة والتطبيقات. بالإضافة إلى ذلك، وبسبب حداثة نظام حماية البيانات الشخصية في المملكة، تفنقر العديد من المنظمات إلى سياسات واضحة لحماية البيانات الشخصية، ولا يوجد لديها مختصون مسؤولون عن هذا الجانب.

- التوصيات: أوصت الدراسة بضرورة إدراج مفهوم "الخصوصية في التصميم والإعدادات الافتراضية" كجزء أساسي من السياسة السعودية لحماية البيانات الشخصية. كما حثت جميع المنظمات على تطوير سياسات خاصة بها لحماية البيانات الشخصية، وتوظيف مختصين مؤهلين لمتابعة تنفيذ هذه السياسات وضمان الامتثال للتشريعات ذات الصلة. بالإضافة إلى ذلك، اقترحت الدراسة استخدام أداة "تقييم الأثر على الخصوصية (Privacy Impact Assessment)" كوسيلة لتقييم المخاطر المحتملة وتعزيز الامتثال.

2. د. سلطان بن عبدالرحمن بن عبدالقادر العبيدان (2024). "التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي".

- الهدف: يسعى البحث إلى بيان أهمية حماية البيانات الشخصية، والكشف عن القواعد الفقهية التي يستند إليها نظام حماية البيانات الشخصية في المملكة العربية السعودية. كما يهدف إلى توضيح كيفية تصدي النظام للتعديات على البيانات الشخصية من خلال العقوبات المنصوص عليها، مع بيان التأصيل الشرعي لهذه العقوبات.
- المنهجية: استخدم الباحث المنهج الاستقرائي والمنهج الوصفي التحليلي، حيث تم وصف نظام حماية البيانات الشخصية السعودي وتحليله وتأصيله فقهيًا. تم التركيز على استنباط القواعد الفقهية والمقاصد الشرعية التي يستند إليها النظام، وتحليل العقوبات المنصوص عليها في ضوء الشريعة الإسلامية.

- النتائج: توصل البحث إلى أن أحكام نظام حماية البيانات الشخصية السعودي تستند إلى مجموعة من المقاصد الشرعية الكبرى والقواعد الفقهية، مثل قاعدة "تصرف الإمام على الرعية منوط بالمصلحة"، وقاعدة "دفع المفسدة مقدم على جلب المصلحة"، وقاعدة "المصلحة العامة مقدمة على المصلحة الخاصة"، وقاعدة "الاحتياط". بالإضافة إلى ذلك، فإن العقوبات المنصوص عليها في النظام، والتي تشمل السجن، والغرامة المالية، والمساءلة التأديبية، ومصادرة الأموال المخالفة، والتعويض عن الضرر، ومضاعفة العقوبة عند التكرار، كلها عقوبات تعزيرية لها أصول مشروعة في الشريعة الإسلامية.

- التوصيات: لم تذكر الدراسة توصيات محددة، لكنها أكدت على أهمية احترام الخصوصية الشخصية وتحريم التجسس، وضرورة تطبيق العقوبات التعزيرية المنصوص عليها في النظام لضمان حماية البيانات الشخصية والحد من التعديات عليها.

3. عبد العزيز بن أحمد المزيني (2023). "موافقة صاحب البيانات الشخصية لمعالجة بياناته في النظام السعودي (دراسة تحليلية مقارنة)".

- الهدف: تهدف الدراسة إلى تحليل مفهوم موافقة صاحب البيانات الشخصية على معالجة بياناته في النظام السعودي، ومقارنتها بالقانون العام لحماية البيانات في الاتحاد الأوروبي (GDPR). تسعى الدراسة إلى تحديد مدى توافق النظام السعودي مع المعايير الدولية في هذا المجال، واقتراح تحسينات لتعزيز حماية حقوق الأفراد.

- المنهجية :اتبعت الدراسة المنهج التحليلي المقارن، حيث تم تحليل نصوص نظام حماية البيانات الشخصية السعودي ولائحته التنفيذية، ومقارنتها بأحكام القانون العام لحماية البيانات الأوروبي. تم التركيز على شروط وضوابط الموافقة، وحقوق الأفراد المتعلقة ببياناتهم الشخصية، والتزامات الجهات المعالجة للبيانات.

- النتائج :أظهرت الدراسة أن البيانات الشخصية التي بحوزة الشركات ذات قيمة كبيرة، وتزداد فائدتها بعد معالجتها. ولهذا السبب، تسعى الشركات إلى معالجة تلك البيانات بطرق مختلفة، مما يستدعي وجود قوانين ولوائح تنظم عمليات المعالجة. كما تبين أن الموافقة التي يصدرها صاحب البيانات الشخصية لها ضوابط يجب توفرها لتكون سليمة ومقبولة.

- التوصيات :أوصت الدراسة بضرورة توعية الأفراد بالضوابط المتعلقة بالموافقة على معالجة بياناتهم الشخصية، لحمايتهم من استغلال شركات التقنية. كما أكدت على أهمية أن تكون الشركات على دراية تامة بهذه الضوابط لتجنب المساءلة القانونية وضمان الامتثال للتشريعات المعمول بها.

4. Michael L. Rustad & Thomas H. Koenig (2019). "Towards a Global Data Privacy Standard".

- الهدف: تسعى هذه الدراسة إلى تحدي الرأي السائد بأن تحديثات الاتحاد الأوروبي الأخيرة لقوانين حماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR)، ستؤدي إلى فجوة بين أنظمة الخصوصية في الاتحاد الأوروبي والولايات المتحدة. بدلاً من ذلك، يقترح الباحثان أن هناك تقاربًا متزايدًا بين النظامين القانونيين، مما يمهد الطريق نحو معيار عالمي لحماية البيانات.
- المنهجية: اعتمد الباحثان على تحليل نقدي للتشريعات والممارسات المتعلقة بحماية البيانات في كل من الاتحاد الأوروبي والولايات المتحدة. ركزا بشكل خاص على كيفية تأثير "تأثير بروكسل (Brussels Effect)" (D.C. Effect) في تشكيل معايير الخصوصية العالمية.
- النتائج: أشارت الدراسة إلى أن اللائحة العامة لحماية البيانات (GDPR) لا تفرض فقط معايير الاتحاد الأوروبي على الكيانات الأمريكية (تأثير بروكسل)، بل تستوعب أيضًا العديد من ابتكارات الخصوصية الأمريكية، مثل الغرامات الرادعة، والتعويضات الجماعية، والعقوبات المستندة إلى الثروة، وحقوق الأفراد في تنفيذ القانون العام (تأثير واشنطن العاصمة). هذا التبادل المتبادل أدى إلى تقارب عبر الأطلسي في قوانين الخصوصية، مما يشير إلى تطور نحو معيار عالمي لحماية البيانات.
- التوصيات: يوصي الباحثان بالاعتراف بهذا التقارب والعمل على تطوير معيار عالمي لحماية البيانات يستفيد من أفضل الممارسات من كلا النظامين القانونيين. هذا المعيار يمكن أن يقلل من التعقيدات للشركات متعددة الجنسيات ويعزز حقوق الخصوصية للأفراد على مستوى العالم.

2. Paul M. Schwartz (2019). "Global Data Privacy: The EU Way".

- **الهدف:** تهدف هذه الدراسة إلى تقديم فهم جديد لكيفية انتشار قانون حماية البيانات في الاتحاد الأوروبي عالميًا، من خلال دراسات حالة لليابان والولايات المتحدة.
- **المنهجية:** اعتمد الباحث على تحليل قانوني مقارنة لتطور قوانين حماية البيانات في اليابان والولايات المتحدة، مع التركيز على تأثير نهج الاتحاد الأوروبي في هذه الدول.
- **النتائج:** وجدت الدراسة أن الاتحاد الأوروبي أصبح يُعتبر "شرطي الخصوصية" في العالم، حيث يؤثر نهجه في حماية البيانات على التشريعات في دول أخرى، مما يؤدي إلى تقارب في معايير حماية البيانات عالميًا.
- **التوصيات:** أوصى الباحث بضرورة فهم أعمق للقوى التي تدفع نحو التقارب والتباعد في قوانين حماية البيانات، والعمل على تعزيز التعاون الدولي لضمان حماية فعّالة للبيانات الشخصية.

3. Eduardo Ustaran (2020). "Data Protection Around the World: Privacy Laws in Action".

- **الهدف:** يسعى الكتاب إلى استكشاف كيفية تطبيق قوانين الخصوصية وحماية البيانات في مختلف أنحاء العالم، مع التركيز على التحديات والفرص التي تواجهها الدول في هذا المجال.
- **المنهجية:** يعتمد المؤلف على تحليل مقارنة لقوانين حماية البيانات في دول مختلفة، مع استعراض دراسات حالة لتوضيح كيفية تطبيق هذه القوانين في الممارسة العملية.
- **النتائج:** يوضح الكتاب أن هناك تنوعًا كبيرًا في كيفية تطبيق قوانين حماية البيانات حول العالم، مما يعكس الاختلافات الثقافية والقانونية بين الدول.

- **التوصيات:** يوصي المؤلف بضرورة تعزيز التعاون الدولي وتبادل الخبرات بين الدول لضمان تطبيق فعال لقوانين حماية البيانات، مع مراعاة الخصوصيات الثقافية والقانونية لكل دولة.

الإطار النظري

مفهوم حماية البيانات الشخصية:

تُعتبر البيانات الشخصية من المفاهيم الأساسية في مجال حماية الخصوصية وأمن المعلومات، حيث تُشكّل محوراً رئيسياً في التشريعات والسياسات المتعلقة بحماية حقوق الأفراد في العصر الرقمي. يُشير مصطلح "البيانات الشخصية" إلى أي معلومات تتعلق بفرد محدد أو يمكن تحديده بشكل مباشر أو غير مباشر. هذا التعريف يشمل مجموعة واسعة من المعلومات التي يمكن استخدامها للتعرف على هوية الشخص، سواء كانت هذه المعلومات مباشرة أو غير مباشرة.

وفقاً لـ "نظام حماية البيانات الشخصية" في المملكة العربية السعودية، تُعرّف البيانات الشخصية بأنها: "كل بيان -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص، والسجلات، والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي".

هذا التعريف يُبرز أن البيانات الشخصية لا تقتصر فقط على المعلومات الأساسية مثل الاسم ورقم الهوية، بل تشمل أيضًا أي معلومات يمكن استخدامها للتعرف على الفرد، سواء كانت هذه المعلومات مباشرة أو غير مباشرة.

أمثلة على البيانات الشخصية:

تشمل البيانات الشخصية مجموعة واسعة من المعلومات، منها:

- المعلومات التعريفية الأساسية: مثل الاسم الكامل، تاريخ الميلاد، والجنسية.
- المعلومات المالية: مثل أرقام الحسابات البنكية، تفاصيل البطاقات الائتمانية، والسجلات المالية.
- المعلومات الصحية: مثل السجلات الطبية، التاريخ الصحي، والمعلومات المتعلقة بالحالة الصحية للفرد.
- المعلومات البيومترية: مثل بصمات الأصابع، بصمة العين، والصور الفوتوغرافية.
- المعلومات الإلكترونية: مثل عناوين البريد الإلكتروني، عناوين IP، وسجلات التصفح.

أهمية تحديد مفهوم البيانات الشخصية:

تحديد مفهوم واضح وشامل للبيانات الشخصية يُعتبر أمرًا بالغ الأهمية لعدة أسباب:

1. حماية الخصوصية: يُساهم التعريف الدقيق للبيانات الشخصية في حماية خصوصية الأفراد ومنع إساءة استخدام معلوماتهم.

2. تطبيق التشريعات: يُسهّل التعريف الواضح للبيانات الشخصية عملية تطبيق القوانين واللوائح المتعلقة

بحماية البيانات.

3. تعزيز الثقة: يُعزّز التعريف الشامل للبيانات الشخصية ثقة الأفراد في المؤسسات التي تتعامل مع

معلوماتهم، مما يؤدي إلى تعزيز التعاون والشفافية.

مقارنة مع التعريفات الدولية:

على الصعيد الدولي، يتماشى تعريف البيانات الشخصية في المملكة العربية السعودية مع التعريفات المعتمدة في العديد من التشريعات الدولية. فعلى سبيل المثال، يُعرّف النظام الأوروبي العام لحماية البيانات (GDPR) البيانات الشخصية بأنها: "أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده ('صاحب البيانات')؛ الشخص الطبيعي الذي يمكن تحديده هو الشخص الذي يمكن التعرف عليه، بشكل مباشر أو غير مباشر، خاصةً بالرجوع إلى معرف مثل الاسم، رقم التعريف، بيانات الموقع، معرف عبر الإنترنت، أو إلى عامل أو أكثر خاص بالهوية البدنية، الفسيولوجية، الجينية، العقلية، الاقتصادية، الثقافية أو الاجتماعية لذلك الشخص الطبيعي".

هذا التعريف يُبيّن أن البيانات الشخصية تشمل مجموعة واسعة من المعلومات التي يمكن استخدامها لتحديد هوية الفرد، سواء بشكل مباشر أو غير مباشر.

مبادئ حماية البيانات المتعارف عليها دوليًا.

تُعتبر حماية البيانات الشخصية من القضايا الحيوية في العصر الرقمي، حيث تزايدت المخاوف بشأن كيفية جمع المعلومات الشخصية ومعالجتها وتخزينها ومشاركتها. استجابةً لهذه التحديات، تم تطوير مجموعة من المبادئ الدولية التي تهدف إلى ضمان حماية خصوصية الأفراد وبياناتهم الشخصية. تستند هذه المبادئ إلى معايير وقوانين دولية، مثل القانون العام لحماية البيانات (GDPR) في الاتحاد الأوروبي، ومبادئ الأمم المتحدة لحماية البيانات الشخصية والخصوصية.

1. مبدأ الشفافية والشفافية:

يُشير هذا المبدأ إلى ضرورة أن تكون عملية جمع ومعالجة البيانات الشخصية قانونية وشفافة. يجب على الجهات التي تجمع البيانات الحصول على موافقة صريحة من الأفراد المعنيين، مع توضيح الأغراض المحددة لاستخدام هذه البيانات. يُعزز هذا المبدأ ثقة الأفراد في كيفية تعامل المؤسسات مع معلوماتهم الشخصية. وفقًا لـ"القانون العام لحماية البيانات (GDPR)"، يجب أن تكون معالجة البيانات الشخصية قانونية وعادلة وشفافة فيما يتعلق بصاحب البيانات .

2. مبدأ تحديد الغرض:

يُركز هذا المبدأ على ضرورة جمع البيانات الشخصية لأغراض محددة ومشروعة وواضحة، وعدم استخدامها لاحقًا بطرق تتعارض مع هذه الأغراض. يهدف هذا إلى منع إساءة استخدام البيانات وضمان استخدامها فقط للأهداف التي تم جمعها من أجلها. على سبيل المثال، إذا تم جمع بيانات شخصية لغرض تقديم خدمة معينة، فلا يجوز استخدامها لأغراض تسويقية دون الحصول على موافقة إضافية من الفرد. يُشير "القانون العام لحماية

البيانات (GDPR) "إلى أنه يجب جمع البيانات لأغراض محددة وصريحة ومشروعة، وعدم معالجتها بطريقة تتعارض مع هذه الأغراض .

3. مبدأ تقليل البيانات:

يُعنى هذا المبدأ بجمع الحد الأدنى من البيانات الشخصية الضرورية لتحقيق الأغراض المحددة. يُساهم ذلك في تقليل المخاطر المرتبطة بتخزين ومعالجة كميات كبيرة من البيانات، ويُعزز من حماية خصوصية الأفراد. بموجب "القانون العام لحماية البيانات (GDPR)" ، يجب أن تكون البيانات الشخصية ملائمة وذات صلة ومقتصرة على ما هو ضروري بالنسبة للأغراض التي تُعالج من أجلها.

4. مبدأ الدقة:

يُشير هذا المبدأ إلى ضرورة الحفاظ على دقة البيانات الشخصية وتحديثها بانتظام. يجب اتخاذ جميع الخطوات المعقولة لضمان أن البيانات غير الدقيقة، فيما يتعلق بالأغراض التي تُعالج من أجلها، يتم محوها أو تصحيحها دون تأخير. تُعتبر البيانات الدقيقة والحديثة أساسية لتجنب القرارات الخاطئة التي قد تؤثر سلبًا على الأفراد. يؤكد "القانون العام لحماية البيانات (GDPR)" على ضرورة أن تكون البيانات الشخصية دقيقة وتُحدَّث عند الضرورة .

5. مبدأ الحد من التخزين:

يُركز هذا المبدأ على ضرورة عدم الاحتفاظ بالبيانات الشخصية لفترة أطول من اللازم لتحقيق الأغراض التي جُمعت من أجلها. بعد تحقيق هذه الأغراض، يجب حذف البيانات أو إخفاء هويتها لضمان عدم استخدامها بشكل غير مصرح به. يُشير "القانون العام لحماية البيانات (GDPR)" إلى أنه يجب الاحتفاظ بالبيانات الشخصية بشكل يسمح بتحديد هوية أصحابها لمدة لا تزيد عن اللازم للأغراض التي تُعالج من أجلها .

6. مبدأ النزاهة والسرية:

يُعنى هذا المبدأ بضمان حماية البيانات الشخصية من المخاطر المحتملة، مثل الوصول غير المصرح به، أو المعالجة غير القانونية، أو فقدان، أو التلف. يجب على المؤسسات اتخاذ التدابير التقنية والتنظيمية المناسبة لضمان أمن البيانات وحمايتها. يؤكد "القانون العام لحماية البيانات (GDPR)" على ضرورة معالجة البيانات الشخصية بطريقة تضمن أمنها المناسب، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية، ومن فقدان أو التلف أو التدمير العرضي .

7. مبدأ المساءلة:

يُشير هذا المبدأ إلى مسؤولية المؤسسات عن الامتثال لمبادئ حماية البيانات، وضرورة قدرتها على إثبات هذا الامتثال. يتطلب ذلك توثيق سياسات وإجراءات حماية البيانات، وتدريب الموظفين، وإجراء تقييمات دورية للتأكد من الامتثال. يُشير "القانون العام لحماية البيانات (GDPR)" إلى أن المُتحكم في البيانات يكون مسؤولاً عن الامتثال للمبادئ المذكورة أعلاه، ويجب أن يكون قادراً على إثبات هذا الامتثال .

، تُشكّل هذه المبادئ إطاراً أساسياً لحماية البيانات الشخصية على المستوى الدولي. يُساهم الالتزام بها في تعزيز ثقة الأفراد في كيفية تعامل المؤسسات مع معلوماتهم الشخصية، ويُعزز من حماية الخصوصية في العصر الرقمي. مع تطور التكنولوجيا وزيادة جمع ومعالجة البيانات، يصبح الالتزام بهذه المبادئ أكثر أهمية لضمان حماية حقوق الأفراد وخصوصيتهم.

أهمية حماية البيانات في تعزيز الثقة بين الأفراد والقطاعات الخاصة

في ظل التطور التكنولوجي المتسارع وزيادة الاعتماد على البيانات الشخصية في مختلف القطاعات الخاصة، أصبح من الضروري أن تلعب الحكومات دوراً رئيسياً في تعزيز حماية البيانات الشخصية. في المملكة العربية السعودية، أصدرت الحكومة نظام حماية البيانات الشخصية لضمان خصوصية الأفراد وتعزيز الثقة بين الأفراد والقطاعات الخاصة. ويُعد هذا النظام جزءاً من الجهود المبذولة لتحقيق رؤية المملكة 2030، التي تهدف إلى تعزيز التحول الرقمي وضمان استخدام البيانات بطريقة آمنة وعادلة.

تشكل حماية البيانات الشخصية عنصراً حيوياً في بناء الثقة بين الأفراد والقطاعات الخاصة، حيث إن الشعور بالأمان بشأن المعلومات الشخصية يعزز من التفاعل بين المستهلكين والمؤسسات الخاصة. وفقاً لدراسة الشمري (2023)، فإن الأنظمة الصارمة لحماية البيانات تساهم في زيادة ثقة الأفراد في المعاملات الإلكترونية، مما يؤدي إلى تحسين بيئة الأعمال وجذب الاستثمارات. كما أن وجود تشريعات واضحة يساهم في تقليل حالات إساءة استخدام البيانات ويضع أسساً قانونية لمعالجة أي انتهاكات.

تتبنى الحكومة السعودية نهجاً مستوحى من المعايير الدولية في حماية البيانات، حيث يتميز النظام السعودي بوجود متطلبات واضحة لموافقة الأفراد على معالجة بياناتهم الشخصية، بما يتماشى مع المبادئ الأوروبية

لحماية البيانات (العبيدان، 2024). فمثلاً، يشترط النظام السعودي أن تكون الموافقة صريحة وقابلة للإلغاء، مما يمنح الأفراد سيطرة أكبر على بياناتهم الشخصية. كما يشدد على ضرورة التزام الشركات الخاصة بحماية البيانات وضمان استخدامها فقط للأغراض التي تم جمعها من أجلها (المزيني، 2023).

من جهة أخرى، تلعب الحكومة دوراً تنظيمياً ورقابياً في ضمان الامتثال للقوانين من خلال إنشاء هيئات متخصصة لمراقبة تنفيذ سياسات حماية البيانات. على سبيل المثال، يشير الشمراني (2024) إلى أن فرض العقوبات على الجهات غير الملتزمة يعزز من امتثال الشركات للأنظمة ويشجعها على اتخاذ تدابير وقائية أكثر صرامة. إضافةً إلى ذلك، فإن الحكومة توفر الدعم التقني والتدريب للشركات لضمان تنفيذ أفضل الممارسات في حماية البيانات، مما يسهم في خلق بيئة آمنة للمعاملات الرقمية.

من منظور دولي، تُظهر التجربة الأوروبية في حماية البيانات أن التشريعات القوية تؤدي إلى تحسين الثقة الرقمية. وفقاً لـ (Voss 2016)، فإن النظام الأوروبي لحماية البيانات قد عزز من الثقة بين المستخدمين والشركات، مما أدى إلى زيادة الاعتماد على الخدمات الرقمية. وبالمثل، فإن المبادئ التي يقوم عليها النظام السعودي تسير في الاتجاه ذاته، حيث تتبنى المملكة سياسات شبيهة بتلك الموجودة في اللائحة العامة لحماية البيانات (GDPR)، بما في ذلك حقوق الأفراد في الوصول إلى بياناتهم وتصحيحها وحذفها (Schwartz, 2019).

علاوة على ذلك، فإن تعزيز حماية البيانات الشخصية لا يقتصر فقط على الجانب القانوني، بل يمتد ليشمل التوعية والتثقيف حول أهمية حماية الخصوصية. يُشير (Kiesow Cortez 2020) إلى أن السياسات الفعالة لحماية البيانات يجب أن تترافق مع جهود توعوية للمستخدمين حول حقوقهم وكيفية حماية بياناتهم. في هذا

السياق، تقوم الحكومة السعودية بإطلاق مبادرات تهدف إلى رفع الوعي حول أهمية الخصوصية الرقمية، مما يعزز من ثقافة الأمان الرقمي لدى الأفراد والمؤسسات.

تلعب الحكومات دورًا محوريًا في تعزيز حماية البيانات الشخصية، وذلك من خلال سن التشريعات الصارمة، وإنشاء هيئات رقابية، وتوفير التدريب والتوعية اللازمة. في المملكة العربية السعودية، يساهم نظام حماية البيانات الشخصية في تعزيز الثقة بين الأفراد والقطاعات الخاصة، مما ينعكس إيجابًا على الاقتصاد الرقمي ويعزز التحول الرقمي الآمن. ومع استمرار التطورات التقنية، سيكون من الضروري تحديث القوانين والأنظمة بشكل دوري لضمان مواكبة التحديات الجديدة وحماية خصوصية الأفراد بفعالية.

الأطر النظرية لحماية البيانات الشخصية

- استعراض النظريات والمفاهيم المتعلقة بحماية الخصوصية والبيانات.

ترتكز حماية البيانات الشخصية على مجموعة من النظريات والمفاهيم التي تحدد الأسس الفلسفية والقانونية لحماية الخصوصية والبيانات. إحدى هذه النظريات هي نظرية الحق في الخصوصية، والتي تعود جذورها إلى أعمال (Bygrave 1998)، حيث يتم التأكيد على أن الخصوصية تُعد حقًا أساسيًا يجب حمايته من التدخلات غير المشروعة. وتعتبر هذه النظرية أساسًا للعديد من التشريعات الحديثة، بما في ذلك النظام السعودي لحماية البيانات الشخصية.

من جهة أخرى، يشير (Tzanou 2013) إلى أن حماية البيانات الشخصية تطورت كحق مستقل بجانب الحق في الخصوصية، حيث تم التعامل معها بشكل أكثر تفصيلاً في القوانين الدولية. فبينما تركز الخصوصية على منع التدخل في الحياة الشخصية، فإن حماية البيانات تهتم بتنظيم كيفية جمع البيانات ومعالجتها واستخدامها بطريقة عادلة وشفافة. في هذا السياق، فإن اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي تُعد نموذجاً رئيسياً لتطبيق هذه المفاهيم.

إضافةً إلى ذلك، هناك نظرية الموافقة المستنيرة، والتي تؤكد على ضرورة أن يكون لصاحب البيانات الحق في الموافقة أو الرفض عند معالجة بياناته الشخصية. وفقاً لدراسة المزيني (2023)، فإن هذه النظرية تعزز من سيطرة الأفراد على بياناتهم وتقلل من إمكانية إساءة استخدامها من قبل الجهات المختلفة. وقد تم تبني هذا المبدأ في النظام السعودي، حيث يتطلب القانون أن تكون الموافقة واضحة وصريحة.

من جانب آخر، فإن النظرية الاقتصادية لحماية البيانات تُشير إلى أن المعلومات الشخصية تُعد مورداً ذا قيمة اقتصادية، مما يستدعي وضع آليات لحمايتها من الاستغلال غير المشروع. يشير Rustad & Koenig (2019) إلى أن البيانات الشخصية أصبحت جزءاً رئيسياً من الاقتصاد الرقمي، حيث يتم استخدامها في التسويق والإعلانات وتحليل السلوكيات الاستهلاكية. وبالتالي، فإن وجود تشريعات تحمي هذه البيانات يسهم في خلق توازن بين المصالح التجارية وحماية حقوق الأفراد.

فإن الأطر النظرية لحماية البيانات الشخصية تستند إلى مجموعة من المفاهيم القانونية، والحقوقية، والاقتصادية، التي تهدف إلى تحقيق التوازن بين حق الأفراد في الخصوصية واحتياجات المؤسسات في استخدام البيانات.

ومن خلال تطبيق هذه النظريات في التشريعات الوطنية مثل النظام السعودي لحماية البيانات الشخصية، يمكن تحقيق بيئة أكثر أمانًا وثقة في التعاملات الرقمية.

العلاقة بين حماية البيانات وحقوق الإنسان

تعد حماية البيانات الشخصية جزءًا أساسيًا من حقوق الإنسان في العصر الرقمي، حيث ترتبط ارتباطًا وثيقًا بالحق في الخصوصية وحرية التعبير والأمن الشخصي. ومع تزايد استخدام التكنولوجيا الرقمية، أصبح من الضروري وضع آليات قانونية وتنظيمية تحمي الأفراد من الانتهاكات المحتملة لبياناتهم الشخصية، سواء من قبل الحكومات أو الشركات الخاصة.

وفقًا لـ (Bygrave 1998)، فإن الحق في الخصوصية قد تم تأكيده في العديد من المعاهدات والاتفاقيات الدولية، مثل الإعلان العالمي لحقوق الإنسان (المادة 12) والعهد الدولي للحقوق المدنية والسياسية (المادة 17)، حيث تنص هذه المواثيق على ضرورة حماية الأفراد من التدخل غير المشروع في حياتهم الشخصية. ومع ذلك، ومع ظهور الثورة الرقمية، أصبح هذا الحق أكثر تعقيدًا بسبب تطور تقنيات جمع البيانات وتحليلها.

يشير (Tzanou 2013) إلى أن حماية البيانات ليست مجرد امتداد للحق في الخصوصية، بل أصبحت حقًا مستقلًا بذاته، نظرًا لأهميتها في حماية الأفراد من إساءة استخدام معلوماتهم الشخصية. فعلى سبيل المثال، يمكن أن تؤدي عمليات جمع البيانات غير المنظمة إلى انتهاك خصوصية الأفراد، كما هو الحال في تقنيات المراقبة الرقمية والإعلانات المستهدفة. لذلك، فإن وجود قوانين صارمة مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي يهدف إلى ضمان حقوق الأفراد في السيطرة على بياناتهم.

على المستوى السعودي، يعكس نظام حماية البيانات الشخصية التزام المملكة بحماية حقوق الأفراد الرقمية، حيث يتطلب القانون الحصول على موافقة صريحة من صاحب البيانات قبل معالجتها، كما يمنحه الحق في الوصول إلى بياناته وتصحيحها أو حذفها (المزيني، 2023). وهذا يتماشى مع التوجهات العالمية في تعزيز حقوق الإنسان الرقمية وضمان عدم استغلال البيانات الشخصية بطرق تنتهك حريات الأفراد.

إضافة إلى ذلك، يشير (Voss 2016) إلى أن حماية البيانات ترتبط مباشرة بحرية التعبير، حيث قد تؤدي الرقابة الجماعية وجمع البيانات غير القانوني إلى تقييد حرية الأفراد في التعبير عن آرائهم. كما أن استخدام البيانات الشخصية دون ضوابط قد يؤدي إلى التمييز، كما هو الحال في تقنيات الذكاء الاصطناعي التي قد تعزز التحيزات ضد مجموعات معينة من الأفراد. لذا، فإن التوازن بين حماية البيانات وضمان حرية التعبير يعد أمرًا بالغ الأهمية في السياسات الرقمية الحديثة.

فإن العلاقة بين حماية البيانات وحقوق الإنسان علاقة تكاملية، حيث تساهم حماية البيانات الشخصية في ضمان الخصوصية، وتعزيز حرية التعبير، وحماية الأفراد من الانتهاكات الرقمية. ومن خلال التشريعات الفعالة مثل نظام حماية البيانات الشخصية في المملكة العربية السعودية، يمكن تحقيق بيئة رقمية أكثر أمانًا تحترم حقوق الإنسان وتعزز الثقة في التعاملات الرقمية.

تأثير حماية البيانات على الابتكار والتطور التكنولوجي

تلعب حماية البيانات الشخصية دورًا حيويًا في دعم الابتكار والتطور التكنولوجي، حيث توفر بيئة آمنة لاستخدام البيانات في تطوير التقنيات الحديثة مثل الذكاء الاصطناعي، وإنترنت الأشياء، وتحليلات البيانات الضخمة. ومع ذلك، فإن التشريعات الصارمة لحماية البيانات قد تشكل في بعض الأحيان تحديًا أمام الشركات والمؤسسات التي تعتمد على البيانات لتطوير خدماتها. لذا، فإن تحقيق توازن بين حماية البيانات وتعزيز الابتكار يعد أمرًا ضروريًا للنمو الاقتصادي والتكنولوجي.

وفقًا لـ (Voss 2016)، فإن التشريعات الأوروبية لحماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR)، قد أثرت على الابتكار من خلال فرض معايير صارمة على جمع البيانات ومعالجتها. فبينما توفر هذه القوانين حماية قوية لحقوق الأفراد، إلا أنها قد تزيد من التكاليف التشغيلية للشركات الناشئة التي تعتمد على البيانات في تطوير نماذج أعمالها. ومع ذلك، فإن الامتثال لهذه القوانين يعزز ثقة المستخدمين، مما يؤدي إلى زيادة الإقبال على الخدمات الرقمية المبتكرة.

في السياق السعودي، يساهم نظام حماية البيانات الشخصية في دعم الابتكار من خلال توفير إطار قانوني واضح يسمح باستخدام البيانات ضمن ضوابط محددة. يشير الشمراني (2024) إلى أن هذا النظام يعزز من قدرة الشركات على تطوير تقنيات جديدة مثل التعلم الآلي والذكاء الاصطناعي، مع ضمان عدم انتهاك خصوصية الأفراد. فمثلاً، يمكن للقطاع الصحي الاستفادة من البيانات الضخمة في تطوير حلول تشخيصية متقدمة، مع ضمان حماية معلومات المرضى وفقًا للقوانين المعمول بها.

من ناحية أخرى، يشير (Kiesow Cortez 2020) إلى أن وجود سياسات صارمة لحماية البيانات قد يدفع الشركات إلى تبني تقنيات أكثر أمانًا، مثل التشفير وتقنيات إخفاء الهوية، مما يعزز من جودة المنتجات التكنولوجية. كما أن تعزيز ثقافة الامتثال للمعايير القانونية يشجع على الابتكار المسؤول، حيث يتم تصميم المنتجات والخدمات الرقمية مع مراعاة مبادئ الأمان والخصوصية منذ المراحل الأولى للتطوير، وهو ما يُعرف بمفهوم "الخصوصية حسب التصميم".

على الرغم من الفوائد الكبيرة لحماية البيانات، فإن بعض الباحثين يشيرون إلى أنها قد تشكل عقبة أمام تبادل البيانات والتعاون البحثي. وفقًا لـ (Rustad & Koenig 2019)، فإن القيود المشددة على مشاركة البيانات قد تؤدي إلى إبطاء الأبحاث في مجالات مثل الطب والتكنولوجيا المالية، حيث تعتمد هذه المجالات بشكل كبير على تحليل البيانات الضخمة. لذا، فإن تبني سياسات مرنة تتيح مشاركة البيانات بشكل آمن يمكن أن يعزز من الابتكار دون المساس بالخصوصية.

فإن حماية البيانات تلعب دورًا مزدوجًا في مجال الابتكار والتطور التكنولوجي، حيث توفر بيئة آمنة تعزز من ثقة المستخدمين، لكنها قد تشكل في بعض الأحيان تحديات أمام الشركات التي تعتمد على البيانات. ومن خلال سياسات متوازنة مثل تلك التي يتبناها النظام السعودي، يمكن تحقيق التوافق بين حماية الخصوصية وتشجيع الابتكار، مما يساهم في تعزيز التحول الرقمي المستدام.

دور الحكومات في حماية البيانات الشخصية

تضطلع الحكومات بدور محوري في حماية البيانات الشخصية من خلال وضع السياسات والتشريعات المناسبة، وإنشاء هيئات رقابية للإشراف على الامتثال لهذه القوانين، وتعزيز الوعي العام حول أهمية حماية البيانات. في ظل التطورات الرقمية المتسارعة، أصبح من الضروري أن تواكب الدول هذه التغيرات لضمان أمن البيانات وحقوق الأفراد.

وضع السياسات والتشريعات اللازمة لحماية البيانات

يُعد سن القوانين والتشريعات من أولى الخطوات التي تتخذها الحكومات لضمان حماية البيانات الشخصية. وتشير دراسة الشمري (2023) إلى أن وجود إطار قانوني واضح يساعد في الحد من الانتهاكات الرقمية ويضمن استخدام البيانات وفقًا لمبادئ الشفافية والأمان. وتعتبر اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي نموذجًا بارزًا في هذا المجال، حيث تفرض معايير صارمة على كيفية جمع البيانات ومعالجتها.

على الصعيد المحلي، قامت المملكة العربية السعودية بإصدار نظام حماية البيانات الشخصية الذي يهدف إلى تنظيم عمليات معالجة البيانات وحماية حقوق الأفراد في الخصوصية وفقًا للبيديان (2024)، فإن هذا النظام يفرض قيودًا صارمة على جمع البيانات، ويتطلب الحصول على موافقة واضحة من الأفراد قبل استخدامها،

كما يمنحهم الحق في تصحيح أو حذف بياناتهم. كما أن العقوبات المفروضة على الجهات المخالفة تضمن التزام الشركات والمؤسسات بهذه الضوابط، مما يعزز الثقة الرقمية.

إنشاء هيئات رقابية لضمان الامتثال للتشريعات

إلى جانب إصدار القوانين، تعمل الحكومات على إنشاء مؤسسات رقابية متخصصة للإشراف على تنفيذ سياسات حماية البيانات وضمان امتثال الجهات المختلفة لها. فمثلاً، أنشأت المملكة العربية السعودية الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، التي تشرف على تطبيق نظام حماية البيانات الشخصية وتضع المعايير التنظيمية لضمان الامتثال. يشير الشمراني (2024) إلى أن وجود مثل هذه الهيئات يساهم في تعزيز الثقة بين الأفراد والقطاعين العام والخاص، كما يوفر آليات فعالة لمراقبة ومعاينة المخالفين.

في هذا السياق، يوضح (Voss 2016) أن وجود سلطات تنظيمية مستقلة يساعد في ضمان العدالة والشفافية، حيث تعمل هذه الهيئات على معالجة الشكاوى المتعلقة بانتهاكات البيانات، وتوفير الإرشادات للمؤسسات حول كيفية الامتثال للقوانين. كما أن التعاون بين الجهات التنظيمية على المستوى الدولي يعزز من الحماية الشاملة للبيانات في عصر العولمة الرقمية.

تعزيز الوعي العام والتثقيف حول أهمية حماية البيانات

لا تقتصر حماية البيانات الشخصية على إصدار القوانين فقط، بل تتطلب أيضاً توعية الأفراد والمؤسسات بأهمية حماية خصوصيتهم الرقمية. وفقاً لدراسة (Kiesow Cortez 2020)، فإن تثقيف الجمهور حول

مخاطر انتهاك البيانات وكيفية التعامل الآمن مع المعلومات الشخصية يعد عنصرًا أساسيًا في نجاح سياسات حماية البيانات.

في المملكة العربية السعودية، أطلقت الجهات المختصة حملات توعوية لرفع مستوى الوعي حول حماية البيانات، مثل مبادرات التثقيف الرقمي التي تستهدف المستخدمين والشركات على حد سواء. كما يتم تضمين مفاهيم الخصوصية وأمن المعلومات في المناهج التعليمية، مما يساهم في بناء ثقافة رقمية واعية لدى الأجيال القادمة.

يشير (Rustad & Koenig 2019) إلى أن تعزيز الوعي يساعد الأفراد على اتخاذ قرارات مستنيرة بشأن بياناتهم، مثل التحكم في إعدادات الخصوصية على المنصات الرقمية وتجنب مشاركة المعلومات الحساسة مع جهات غير موثوقة. كما أن تدريب العاملين في القطاعات المختلفة على كيفية التعامل مع البيانات الشخصية يقلل من مخاطر التسريبات والانتهاكات الأمنية.

تؤدي الحكومات دورًا رئيسيًا في حماية البيانات الشخصية من خلال سن التشريعات، وإنشاء الهيئات الرقابية، وتعزيز الوعي العام. ومن خلال التوازن بين توفير بيئة آمنة لحماية البيانات وتشجيع الابتكار الرقمي، يمكن تحقيق تحول رقمي مستدام يعزز الثقة بين الأفراد والمؤسسات. وتُعد المملكة العربية السعودية مثالاً على الدول التي تبنت نهجًا متكاملًا لحماية البيانات، مما يساهم في تعزيز الأمن الرقمي ودعم الاقتصاد المبني على البيانات.

نظام حماية البيانات الشخصية

يعد نظام حماية البيانات الشخصية السعودي أحد أبرز التشريعات التي تهدف إلى تعزيز أمن المعلومات وضمان خصوصية الأفراد في التعاملات الرقمية. صدر هذا النظام في إطار رؤية المملكة 2030 لتعزيز التحول الرقمي، حيث يضع الأسس القانونية لتنظيم جمع البيانات الشخصية ومعالجتها وحفظها، بما يتماشى مع المعايير الدولية في هذا المجال (الشمري، 2023).

نظرة عامة على النظام

تمت الموافقة على نظام حماية البيانات الشخصية في عام 2021، وتم تعديله لاحقًا لتعزيز التوازن بين حماية حقوق الأفراد ودعم الابتكار في الاقتصاد الرقمي. يشمل النظام جميع الجهات التي تقوم بجمع ومعالجة البيانات الشخصية، سواء كانت في القطاعين العام أو الخاص، ويضع قيودًا صارمة على كيفية استخدام هذه البيانات، بما يضمن عدم إساءة استغلالها (المزيني، 2023).

وفقًا للشراني (2024)، يحدد النظام مفهوم البيانات الشخصية ليشمل أي معلومات تتعلق بشخص معين أو يمكن التعرف عليه من خلالها، مثل الاسم، رقم الهوية، العنوان، أو أي بيانات حساسة مثل السجلات الصحية والمالية. كما ينص النظام على وجوب الحصول على موافقة صريحة من صاحب البيانات قبل معالجتها، مع منح الأفراد الحق في الوصول إلى بياناتهم وتصحيحها أو حذفها عند الضرورة.

أهداف نظام حماية البيانات الشخصية

يهدف النظام السعودي لحماية البيانات الشخصية إلى تحقيق عدة أهداف رئيسية، أبرزها:

1. حماية خصوصية الأفراد

يسعى النظام إلى ضمان سرية المعلومات الشخصية ومنع أي استخدام غير مصرح به لها. وقد أكدت دراسة العبيدان (2024) أن هذا النظام يعزز من حقوق الأفراد الرقمية، حيث يفرض التزامات قانونية على المؤسسات لحماية بيانات المستخدمين، مما يقلل من مخاطر تسريب البيانات أو إساءة استخدامها.

2. تعزيز الثقة في الاقتصاد الرقمي

يعد بناء بيئة رقمية آمنة أحد العوامل الأساسية لجذب الاستثمارات وتعزيز التجارة الإلكترونية. وفقًا لـ (Kiesow Cortez 2020)، فإن وجود إطار قانوني قوي لحماية البيانات يعزز من ثقة الأفراد والشركات في الخدمات الرقمية، مما يؤدي إلى نمو الاقتصاد الرقمي وخلق فرص جديدة في مجال التكنولوجيا المالية والصحة الرقمية.

3. تنظيم عمليات جمع البيانات ومعالجتها

يضع النظام معايير واضحة لكيفية جمع البيانات الشخصية ومعالجتها وتخزينها، بحيث يتم استخدامها فقط للأغراض المحددة التي تم جمعها من أجلها. كما يفرض على الشركات استخدام تقنيات التشفير والتخزين الآمن لحماية البيانات من الاختراقات والتهديدات السيبرانية (Rustad & Koenig, 2019).

4. توفير آليات لمساءلة المخالفين

لضمان الامتثال، يفرض النظام عقوبات صارمة على الجهات التي تنتهك أحكامه، سواء من خلال

تسريب البيانات أو استخدامها دون إذن. وقد أشار (Voss 2016) إلى أن فرض عقوبات قانونية

قوية يسهم في ردع المخالفين ويجبر المؤسسات على تبني سياسات صارمة لحماية البيانات.

5. مواءمة التشريعات المحلية مع المعايير الدولية

يهدف النظام إلى تحقيق التوافق مع القوانين والتشريعات العالمية، مثل اللائحة العامة لحماية

البيانات (GDPR) في الاتحاد الأوروبي، مما يسهل التعاون التجاري والرقمي بين المملكة والدول

الأخرى. (Schwartz, 2019)

دور الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في تطبيق نظام حماية البيانات الشخصية

تلعب الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) دورًا حيويًا في تنفيذ نظام حماية البيانات

الشخصية في المملكة العربية السعودية، حيث تتولى مسؤولية الإشراف على الامتثال لهذا النظام، ووضع

اللوائح التنظيمية، وتطبيق الإجراءات التي تضمن حماية خصوصية الأفراد وتعزيز الأمن السيبراني. يأتي

ذلك في إطار الجهود الوطنية لدعم التحول الرقمي وتحقيق أهداف رؤية المملكة 2030 (الشمري، 2023).

الإشراف على تنفيذ النظام والتأكد من الامتثال

تتولى سدايا مسؤولية مراقبة تطبيق نظام حماية البيانات الشخصية في مختلف القطاعات، حيث تضع

القواعد والتوجيهات اللازمة لضمان امتثال الشركات والمؤسسات لهذا النظام. وفقًا للعبيدان (2024)، تعمل

الهيئة على إصدار التراخيص والتصاريح المتعلقة بجمع ومعالجة البيانات الشخصية، بالإضافة إلى مراقبة

الامتثال عبر عمليات التدقيق والتفتيش الدوري. كما أنها تفرض عقوبات على الجهات المخالفة، مما يعزز

الالتزام بالمعايير القانونية.

وضع السياسات واللوائح التنظيمية

تعمل سدايا على تطوير السياسات والإجراءات التي تنظم آلية جمع البيانات الشخصية ومعالجتها وتخزينها، بهدف تحقيق التوازن بين حماية خصوصية الأفراد وتعزيز استخدام البيانات في الابتكار والتطوير التكنولوجي (المزيني، 2023). كما تسهم الهيئة في تحسين اللوائح التنظيمية بما يواكب التطورات التقنية والتغيرات في البيئة الرقمية، مما يساعد في تعزيز الأمن المعلوماتي والحد من الانتهاكات المحتملة للبيانات.

تعزيز الأمن السيبراني وحماية البيانات

بالتعاون مع الجهات المختصة، تلعب سدايا دورًا مهمًا في تعزيز الأمن السيبراني من خلال وضع معايير صارمة لتخزين البيانات ونقلها، وضمان استخدام تقنيات متقدمة مثل التشفير وإخفاء الهوية لحماية البيانات من الاختراقات والتسريبات. (Rustad & Koenig, 2019) كما تقوم الهيئة بتوجيه المؤسسات حول أفضل الممارسات في حماية المعلومات، مما يساهم في تقليل المخاطر الأمنية وتحسين بيئة العمل الرقمي.

التوعية والتثقيف حول حماية البيانات

إلى جانب دورها التنظيمي، تعمل سدايا على نشر الوعي والتثقيف حول حماية البيانات من خلال مبادرات تعليمية وحملات توعوية تستهدف الأفراد والشركات. يشير Kiesow Cortez (2020) إلى أن التوعية بالحقوق الرقمية وآليات حماية الخصوصية يعد عاملاً أساسياً في إنجاح سياسات حماية البيانات، حيث تساعد هذه الجهود الأفراد على اتخاذ قرارات أكثر أماناً عند مشاركة معلوماتهم الشخصية.

تطوير البنية التحتية للبيانات وتعزيز الابتكار

تسهم سدايا في تطوير بنية تحتية رقمية متقدمة تدعم الاستخدام الآمن للبيانات، مثل إنشاء مراكز بيانات محلية توفر حلول تخزين آمنة. كما تعمل الهيئة على تحفيز الابتكار في مجال الذكاء الاصطناعي وتحليل البيانات، مع ضمان الامتثال لمعايير الخصوصية وحماية البيانات (الشمراي، 2024). هذه الجهود تساعد في تعزيز ثقة المستثمرين والمستخدمين في البيئة الرقمية بالمملكة.

تمثل الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) الركيزة الأساسية في تنفيذ نظام حماية البيانات الشخصية في المملكة، حيث تقوم بالإشراف على الامتثال، ووضع السياسات، وتعزيز الأمن السيبراني، والتوعية المجتمعية، ودعم الابتكار. ومن خلال هذه الأدوار، تسهم الهيئة في بناء بيئة رقمية آمنة ومستدامة تدعم التحول الرقمي وتحمي خصوصية الأفراد.

أهمية نظام حماية البيانات الشخصية في تعزيز الثقة في البيئة الرقمية وتحقيق أهداف رؤية 2030

يُعد نظام حماية البيانات الشخصية في المملكة العربية السعودية أحد الركائز الأساسية لتعزيز الثقة في البيئة الرقمية، حيث يضمن حماية خصوصية الأفراد، ويضع معايير واضحة لتنظيم استخدام البيانات، مما يساهم في خلق بيئة رقمية آمنة ومتطورة. كما يتماشى هذا النظام مع أهداف رؤية المملكة 2030 التي تسعى إلى تحقيق تحول رقمي شامل يدعم الاقتصاد المعرفي والابتكار التكنولوجي (الشمري، 2023).

تعزيز الثقة في البيئة الرقمية

تعد الثقة الرقمية عنصراً أساسياً في نجاح التحول الرقمي، حيث يؤثر مستوى الأمان والشفافية في البيانات على مدى تقبل الأفراد والمؤسسات لاستخدام الخدمات الرقمية. وفقاً للمزيني (2023)، فإن نظام حماية البيانات الشخصية يعزز هذه الثقة من خلال:

- ضمان أمن البيانات ومنع إساءة استخدامها، مما يجعل المستخدمين أكثر راحة في مشاركة معلوماتهم الشخصية.
 - فرض معايير قانونية صارمة على الشركات والمؤسسات، مما يلزمها بتطبيق أفضل الممارسات في حماية المعلومات.
 - تمكين الأفراد من التحكم في بياناتهم، حيث يمنحهم النظام حقوقاً واضحة مثل الوصول إلى بياناتهم، وتصحيحها، وحذفها عند الضرورة.
- يشير Kiesow Cortez (2020) إلى أن وجود قوانين لحماية البيانات يزيد من ثقة المستثمرين والشركات في البيئة الرقمية، حيث يضمن إطاراً قانونياً واضحاً يحمي حقوق جميع الأطراف، مما يعزز النمو الاقتصادي القائم على التكنولوجيا.

تحقيق أهداف رؤية المملكة 2030

تمثل رؤية 2030 خارطة طريق طموحة تسعى إلى تحويل المملكة إلى مركز عالمي في مجال الاقتصاد الرقمي والابتكار التكنولوجي. ويسهم نظام حماية البيانات الشخصية في تحقيق هذه الرؤية من خلال:

1. تعزيز الاقتصاد الرقمي وجذب الاستثمارات

يعتمد الاقتصاد الرقمي على الثقة والأمان في البيانات، مما يجعل حماية البيانات عاملاً أساسياً لجذب الشركات العالمية والاستثمارات في قطاع التكنولوجيا. وفقاً لـ (Voss, 2016)، فإن وجود تشريعات واضحة لحماية البيانات يساهم في تحسين تصنيف الدولة في المؤشرات الدولية للأمن السيبراني والخصوصية، مما يشجع الشركات على الاستثمار في المملكة.

2. تحفيز الابتكار في الذكاء الاصطناعي والتقنيات الناشئة

تدعم الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) تطوير تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة، مع الالتزام بمعايير الخصوصية وأمن المعلومات (الشمrani, 2024). هذا يتيح استخدام البيانات بطريقة مسؤولة لتطوير حلول مبتكرة في مجالات مثل الرعاية الصحية، والخدمات الحكومية، والتجارة الإلكترونية.

3. تطوير بنية تحتية رقمية متقدمة

تعمل المملكة على بناء بنية تحتية رقمية قوية تدعم التحول الرقمي، حيث يساعد نظام حماية البيانات الشخصية في وضع أسس قانونية لهذه المنظومة، مما يضمن أن تكون البيانات المخزنة داخل المملكة آمنة ومتوافقة مع المعايير العالمية. (Rustad & Koenig, 2019)

4. تعزيز الشفافية والحوكمة الرقمية

تعكس القوانين الصارمة لحماية البيانات التزام المملكة بالشفافية والمساءلة في البيئة الرقمية. وفقاً للعبيدان (2024)، فإن وجود نظام قوي لحماية البيانات يساهم في تعزيز الحوكمة الرقمية، حيث تصبح الجهات الحكومية والخاصة أكثر التزاماً بمعايير الأمن والخصوصية.

يسهم نظام حماية البيانات الشخصية بشكل مباشر في تحقيق أهداف رؤية 2030 من خلال تعزيز الثقة في البيئة الرقمية، ودعم الابتكار، وتحفيز الاستثمارات، وتطوير بنية تحتية رقمية قوية. ومن خلال التوازن بين حماية خصوصية الأفراد وتمكين الاستخدام الآمن للبيانات، يُعد هذا النظام حجر الأساس لاقتصاد رقمي مستدام يحقق النمو والازدهار في المملكة.

التزامات القطاعات الخاصة بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية

يُلزم نظام حماية البيانات الشخصية السعودي القطاعات الخاصة بمجموعة من الضوابط والتدابير التي تهدف إلى ضمان الاستخدام المسؤول للبيانات الشخصية وحماية خصوصية الأفراد. وتُعد هذه الالتزامات ضرورية لتعزيز الثقة في البيئة الرقمية وضمان الامتثال للمعايير القانونية والأخلاقية في التعامل مع المعلومات الشخصية (الشمرى، 2023).

يُعد الحصول على موافقة الأفراد قبل جمع أو معالجة بياناتهم أحد المبادئ الأساسية التي يركز عليها النظام، حيث يُشترط أن تكون الموافقة صريحة وواضحة قبل القيام بأي عمليات تتعلق بالبيانات الشخصية. وفقاً للمزيني (2023)، يهدف هذا المبدأ إلى تعزيز سيطرة الأفراد على بياناتهم وتمكينهم من اتخاذ قرارات مستنيرة بشأن كيفية استخدامها. ومن أجل تحقيق ذلك، يجب على المؤسسات الخاصة تقديم إشعارات واضحة للمستخدمين توضح الأغراض التي سيتم استخدام بياناتهم من أجلها، إضافةً إلى منحهم الحق في رفض أو سحب موافقتهم في أي وقت. وتُعتبر هذه الممارسات جزءاً من التوجهات العالمية لحماية البيانات، حيث يشير (Tzanou 2013) إلى أن الموافقة المستنيرة تُعد حجر الأساس في القوانين الدولية لحماية البيانات، مما يمنح الأفراد مزيداً من التحكم في معلوماتهم الشخصية.

لا يقتصر التزام المؤسسات الخاصة على الحصول على الموافقة، بل يمتد أيضًا إلى تطبيق معايير الأمان اللازمة لحماية البيانات من التسرب أو الاختراق. يُلزم النظام الشركات والمؤسسات باتخاذ تدابير وقائية فعالة، تشمل استخدام تقنيات التشفير أثناء تخزين ونقل البيانات، بالإضافة إلى اعتماد جدران حماية وأنظمة كشف التسلل لمنع أي وصول غير مصرح به (العبيدان، 2024). وتُعد هذه الإجراءات ضرورية في ظل تزايد التهديدات السيبرانية، حيث أكد (Rustad & Koenig (2019 أن تطبيق معايير أمنية صارمة يساهم في تقليل المخاطر المرتبطة بسرقة البيانات أو استخدامها بطرق غير قانونية. وبذلك، تلتزم المؤسسات بمتابعة أحدث التقنيات في مجال الأمن السيبراني وتحديث أنظمتها بشكل دوري للحفاظ على حماية البيانات من الهجمات الإلكترونية المحتملة.

إلى جانب تطبيق تدابير الأمان، يفرض النظام على المؤسسات تعيين مسؤول لحماية البيانات داخل كل منشأة لضمان الامتثال للقوانين واللوائح التنظيمية. يلعب مسؤول حماية البيانات دورًا أساسيًا في الإشراف على سياسات الخصوصية داخل المؤسسة، إضافةً إلى ضمان الالتزام بالمعايير القانونية ومراقبة طرق جمع ومعالجة البيانات الشخصية. كما يكون مسؤولاً عن التعامل مع شكاوى الأفراد المتعلقة بحقوقهم في الوصول إلى بياناتهم أو طلب تصحيحها أو حذفها (الشمراي، 2024). ويؤكد (Voss (2016 أن تعيين مسؤول لحماية البيانات أصبح ممارسة ضرورية في العديد من الدول التي تعتمد قوانين صارمة لحماية البيانات، حيث يساعد ذلك في تعزيز الامتثال وتقليل المخالفات القانونية.

يُشكل التزام القطاعات الخاصة بهذه المتطلبات ركيزة أساسية لبناء بيئة رقمية آمنة تدعم الابتكار والتطور التكنولوجي في المملكة. ومن خلال الالتزام بالموافقة الصريحة، وتعزيز معايير الأمان، وتعيين مسؤول لحماية البيانات، تساهم المؤسسات في تحقيق توازن بين حماية خصوصية الأفراد ودعم الاستخدام الفعال

للبيانات، مما يعزز الثقة في الاقتصاد الرقمي ويحقق أهداف رؤية المملكة 2030 في بناء مجتمع رقمي آمن ومتقدم.

التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام

يمثل نظام حماية البيانات الشخصية السعودي خطوة مهمة نحو تعزيز الخصوصية في البيئة الرقمية، إلا أن القطاعات الخاصة تواجه تحديات عديدة في الامتثال لهذه اللوائح، مما يتطلب جهودًا مستمرة لضمان الامتثال الكامل. وتتنوع هذه التحديات بين التقنية والتكنولوجية، والتنظيمية والإدارية، وتلك المتعلقة بالوعي والتدريب، مما يؤثر على قدرة المؤسسات على تنفيذ النظام بفعالية (الشمري، 2023).

تُعد التحديات التقنية والتكنولوجية من أبرز العوائق التي تواجه المؤسسات الخاصة، حيث يتطلب الامتثال للنظام تبني أدوات وتقنيات حديثة لضمان حماية البيانات من التسريب أو الاختراق. وفقًا للعبيدان (2024)، تواجه العديد من الشركات صعوبات في تحديث أنظمة الحماية، خاصة المؤسسات الصغيرة والمتوسطة التي قد لا تمتلك الموارد المالية والتقنية الكافية لتطوير بنية تحتية متقدمة للأمن السيبراني. كما أن تطور الهجمات الإلكترونية وأساليب الاختراق يجعل من الصعب على الشركات مواكبة أحدث التهديدات، مما يعرض بيانات الأفراد لخطر الاستغلال. ويؤكد (Rustad & Koenig (2019 أن الحاجة إلى تقنيات حديثة في تشفير البيانات وإدارة الوصول تُعد تحديًا رئيسيًا يتطلب استثمارات ضخمة لضمان الامتثال الفعال للقوانين.

إلى جانب التحديات التقنية، تواجه المؤسسات تحديات تنظيمية وإدارية تتعلق بتكييف سياساتها الداخلية مع المتطلبات القانونية الجديدة. يُلزم النظام الشركات بوضع سياسات واضحة لحماية البيانات، وهو أمر قد

يكون معقدًا خاصةً في المؤسسات الكبيرة التي تتعامل مع كميات هائلة من البيانات. كما أن تعيين مسؤول لحماية البيانات داخل كل منشأة يمثل تحديًا إداريًا إضافيًا، حيث يتطلب وجود كوادر متخصصة في إدارة الامتثال وحماية المعلومات (الشمراي، 2024). وتشير دراسة (Voss 2016) إلى أن الشركات غالبًا ما تواجه صعوبات في تنسيق الامتثال بين الإدارات المختلفة، مما قد يؤدي إلى تأخير أو تعقيد تنفيذ سياسات الخصوصية.

أما على صعيد التحديات المتعلقة بالوعي والتدريب، فإن قلة المعرفة لدى الموظفين بأهمية حماية البيانات وكيفية الامتثال للقوانين يشكل عقبة كبيرة أمام تنفيذ النظام بفعالية. وفقًا للمزيني (2023)، تعاني العديد من المؤسسات من نقص في التدريب والتوعية، حيث لا يدرك الموظفون في بعض الأحيان كيفية التعامل مع البيانات الشخصية وفقًا للقوانين الجديدة. كما أن الثقافة التنظيمية داخل بعض الشركات قد لا تعطي الأولوية لحماية البيانات، مما يزيد من احتمالية حدوث انتهاكات غير مقصودة. وأكد (Kiesow Cortez 2020) أن الاستثمار في برامج التدريب المستمر للعاملين يُعد من أهم الحلول لضمان الامتثال، حيث يعزز من قدرة المؤسسات على التعامل مع البيانات بطريقة مسؤولة وآمنة.

تمثل هذه التحديات مجتمعة عقبة أمام الامتثال السلس لنظام حماية البيانات الشخصية، مما يتطلب جهودًا متكاملة من قبل القطاعات الخاصة والحكومة لتوفير الدعم التقني، وتسهيل الإجراءات التنظيمية، وتعزيز برامج التوعية والتدريب. ومن خلال التغلب على هذه العقبات، يمكن للقطاعات الخاصة تحسين قدرتها على حماية البيانات الشخصية، مما يساهم في تحقيق بيئة رقمية آمنة ومتوافقة مع أهداف رؤية المملكة 2030.

دور الحكومة في دعم القطاعات الخاصة للامتثال:

تمثل حماية البيانات الشخصية ركيزة أساسية في تعزيز البيئة الرقمية الآمنة، ولذلك تلعب الحكومة السعودية دوراً مهماً في دعم القطاعات الخاصة للامتثال لنظام حماية البيانات الشخصية. ويتجلى هذا الدعم من خلال وضع السياسات والتشريعات، وتوفير الأدوات والموارد التقنية، وتعزيز التوعية والتدريب، مما يساهم في تسهيل الامتثال وتقليل التحديات التي تواجه المؤسسات (الشمري، 2023).

تُعد وضع السياسات والتشريعات الواضحة من أهم أدوار الحكومة في دعم الامتثال، حيث تضمن القوانين التي تصدرها الجهات التنظيمية وضوح المتطلبات والإجراءات اللازمة لحماية البيانات. وقد عملت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) على تطوير إطار تنظيمي متكامل، يحدد مسؤوليات المؤسسات الخاصة في التعامل مع البيانات الشخصية، كما يضع معايير واضحة لمعالجة البيانات وتخزينها ونقلها بشكل آمن (العبيدان، 2024). وتشير دراسة (Schwartz 2019) إلى أن وجود إطار قانوني قوي يساعد المؤسسات على الامتثال بشكل أفضل، حيث يقلل من الغموض القانوني ويمنح الشركات خارطة طريق واضحة لتطبيق سياسات الخصوصية.

إلى جانب السياسات، توفر الحكومة الدعم التقني والتكنولوجي لمساعدة القطاعات الخاصة على تنفيذ تدابير الحماية اللازمة. وتتمثل هذه الجهود في تقديم الأدوات والاستشارات التقنية التي تساعد الشركات، وخاصة المؤسسات الصغيرة والمتوسطة، على تعزيز أمن البيانات. كما تعمل الجهات المختصة، مثل سدايا وهيئة الاتصالات والفضاء والتقنية، على توفير حلول مبتكرة لحماية البيانات، مثل أنظمة التشفير المتقدمة ومنصات تحليل المخاطر السيبرانية، مما يساعد الشركات على الامتثال للمعايير الأمنية بسهولة أكبر (المزيني، 2023).

وقد أكد Voss (2016) أن تقديم الدعم التقني من قبل الحكومات يعد عاملاً حاسماً في تعزيز قدرة المؤسسات على حماية بيانات الأفراد، خاصة في ظل التطورات السريعة في مجال الأمن السيبراني.

تعزز الحكومة أيضاً التوعية والتدريب كوسيلة رئيسية لرفع مستوى الامتثال في القطاعات الخاصة. ويشمل ذلك إطلاق حملات توعوية وبرامج تدريبية تستهدف الموظفين والمسؤولين داخل الشركات، لزيادة وعيهم بأهمية حماية البيانات ومتطلبات الامتثال. وفقاً للشمراي (2024)، تعمل الحكومة على تنظيم ورش عمل ودورات تدريبية لمساعدة المؤسسات في فهم الأنظمة واللوائح وتطبيقها بشكل صحيح. كما أن توفير إرشادات عملية وأدلة تنظيمية يساهم في تسهيل عملية الامتثال وتقليل الأخطاء المحتملة. ووفقاً لـ (Kiesow Cortez 2020)، فإن تعزيز ثقافة الامتثال داخل المؤسسات من خلال التعليم والتدريب المستمر يعد عنصراً أساسياً في نجاح قوانين حماية البيانات.

علاوة على ذلك، تفرض الحكومة آليات رقابية متوازنة لضمان الالتزام بالنظام، حيث يتم إجراء عمليات تفتيش دورية، وتقديم استشارات تنظيمية تساعد الشركات على تصحيح الأخطاء قبل فرض العقوبات. كما تعمل الجهات الرقابية على تطوير أدوات تقييم الامتثال الذاتي، والتي تمكن الشركات من قياس مدى التزامها بالقوانين واتخاذ التدابير التصحيحية عند الحاجة. ويؤكد (Rustad & Koenig 2019) أن وجود رقابة مرنة وإرشادية يعزز الامتثال الطوعي ويشجع المؤسسات على الالتزام دون الشعور بالضغط التنظيمي المفرط.

من خلال هذه الجهود، تساهم الحكومة في تسهيل عملية الامتثال لنظام حماية البيانات الشخصية، مما يعزز الثقة بين الأفراد والمؤسسات، ويدعم التحول الرقمي في المملكة. كما أن توفير بيئة قانونية وتقنية داعمة يعزز من قدرة القطاعات الخاصة على تحقيق الامتثال بفعالية، مما يساهم في تحقيق أهداف رؤية 2030 في بناء اقتصاد رقمي متطور وآمن.

الفصل الثالث: المنهجية

المقدمة

يهدف هذا الفصل إلى توضيح المنهجية العلمية التي تم اتباعها في الدراسة، والتي تهدف إلى تحليل دور الحكومة في دعم امتثال القطاعات الخاصة لنظام حماية البيانات الشخصية في المملكة العربية السعودية، إضافةً إلى استكشاف التحديات التي تواجه هذه القطاعات. ولتحقيق ذلك، تم تحديد تصميم البحث، واختيار عينة الدراسة وفق أسس علمية، بالإضافة إلى تحديد أداة جمع البيانات وإجراءات تحليلها.

تصميم البحث

تم اعتماد المنهج الوصفي التحليلي باعتباره المنهج الأنسب لدراسة الظواهر الاجتماعية والقانونية المرتبطة بحماية البيانات الشخصية. يساعد هذا المنهج في تقديم وصف دقيق للإطار القانوني والتنظيمي للنظام السعودي، وتحليل تأثير السياسات الحكومية على امتثال المؤسسات الخاصة. كما يُمكن المنهج التحليلي من تفسير البيانات المستخلصة من الاستبيانات لفهم أبرز التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام.

مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من جميع الشركات والمؤسسات الخاصة العاملة في المملكة العربية السعودية، والتي تخضع لأحكام نظام حماية البيانات الشخصية. وبما أن دراسة جميع أفراد المجتمع غير ممكنة، فقد تم اللجوء إلى تحديد حجم العينة بناءً على جدول مورغان، والذي يُستخدم لتحديد العينة التمثيلية للمجتمع.

بافتراض أن مجتمع الدراسة يشمل ما يقارب 5000 مؤسسة خاصة، فإن جدول مورغان يحدد العينة المطلوبة بحوالي 357 مؤسسة لضمان تمثيل دقيق للمجتمع. وقد تم اختيار العينة بالطريقة العشوائية الطبقية لضمان تنوع المؤسسات المشاركة، بحيث تشمل قطاعات مختلفة مثل المالية، والتكنولوجيا، والتجارة، والصحة، مما يوفر نظرة متكاملة عن مستوى الامتثال للنظام.

أداة جمع البيانات

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات الأولية من المشاركين، حيث تم تصميمه ليشمل عدة محاور تغطي مختلف جوانب الامتثال لنظام حماية البيانات الشخصية، والتحديات التي تواجه المؤسسات في تطبيقه، ومدى تأثير الدعم الحكومي في تسهيل الامتثال.

إجراءات جمع البيانات

تم تنفيذ الاستبيان إلكترونياً عبر منصات مخصصة لجمع البيانات لضمان سهولة الوصول إلى المشاركين وزيادة معدل الاستجابة كما تم إرسال الاستبيان إلى العينة المستهدفة عبر البريد الإلكتروني ووسائل التواصل المؤسسية، مع تقديم شرح واضح لأهداف الدراسة وأهمية المشاركة فيها.

تحليل البيانات

بعد جمع البيانات، تم تحليلها باستخدام برنامج SPSS، حيث تم إجراء:

- تحليل إحصائي وصفي لتحديد النسب والتكرارات المتعلقة بمستوى الامتثال والتحديات الرئيسية.
- تحليل ارتباطي لفحص العلاقة بين الدعم الحكومي ومستوى الامتثال لدى المؤسسات الخاصة.

- تحليل المقاييس التفسيرية لاستخلاص استنتاجات حول الفروقات بين القطاعات المختلفة فيما يتعلق بالامتثال للنظام.

أخلاقيات البحث

تم الالتزام بأخلاقيات البحث العلمي من خلال:

- الحفاظ على سرية معلومات المشاركين، وعدم استخدام البيانات إلا لأغراض البحث.
- الحصول على موافقة المشاركين قبل تعبئة الاستبيان، مع ضمان إمكانية الانسحاب في أي وقت.
- ضمان الموضوعية في التحليل والاعتماد على مصادر موثوقة لدعم النتائج والتوصيات.

الخاتمة

يوضح هذا الفصل المنهجية المتبعة في الدراسة، حيث تم اختيار المنهج الوصفي التحليلي لتقديم رؤية متكاملة حول دور الحكومة في دعم امتثال القطاعات الخاصة لنظام حماية البيانات الشخصية كما تم تحديد مجتمع وعينة الدراسة وفق جدول مورغان، واستخدام الاستبيان كأداة رئيسية لجمع البيانات، مع توضيح آليات تحليلها لضمان استخلاص نتائج دقيقة وموضوعية تدعم أهداف البحث.

الفصل الرابع: مناقشة النتائج

المتغيرات الديموغرافية لعينة الدراسة

أولاً: البيانات الأولية

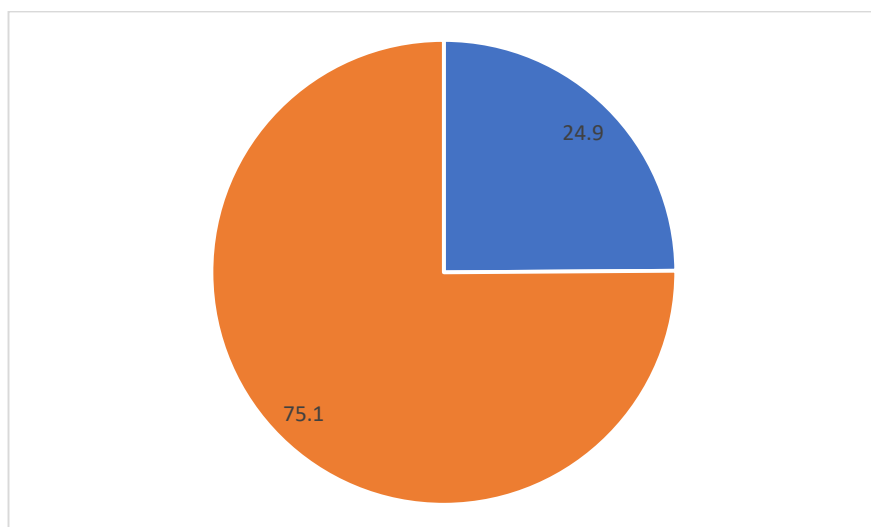
- الجنس

جدول 1 توزيع عينة الدراسة وفقاً للجنس

النسبة	التكرار	
24.9	89	ذكر
75.1	268	أنثى
100.0	357	المجموع

الجدول السابق يوضح توزيع عينة الدراسة وفقاً لمتغير الجنس، فبلغت نسبة الذكور 24.9%، بينما بلغت نسبة الإناث 75.1%.

رسم توضيحي 1 توزيع عينة الدراسة وفقاً للجنس

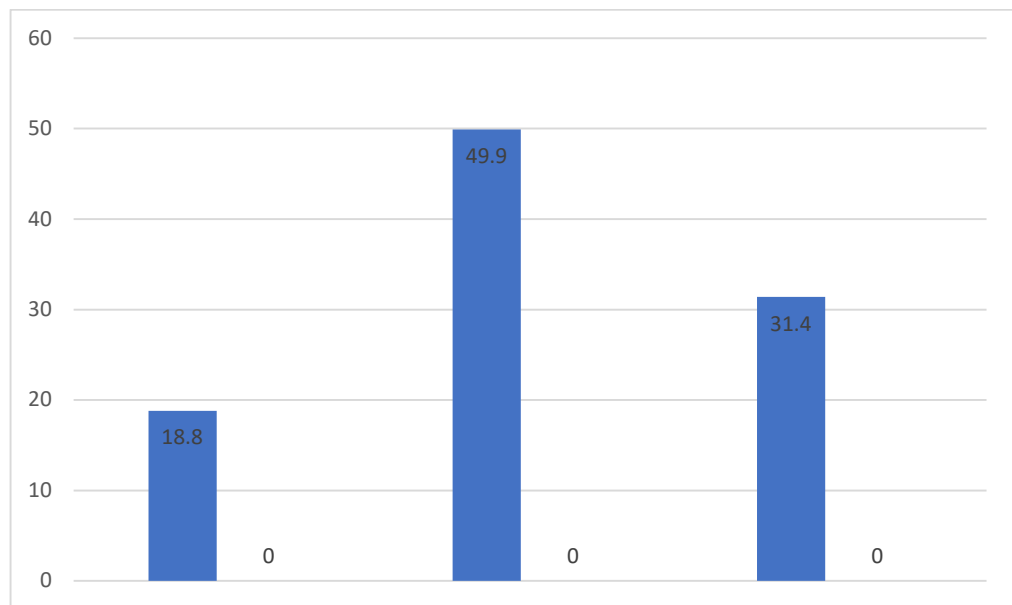


• العمر

جدول 2 توزيع عينة الدراسة وفقاً للعمر

النسبة	التكرار	
18.8	67	أقل من 25 سنة
49.9	178	من 25-34 سنة
31.4	112	45 فأكثر
100.0	357	المجموع

الجدول السابق يوضح توزيع عينة الدراسة وفقاً لمتغير العمر. حيث بلغت نسبة من هم أقل من 25 سنة 18.8% من إجمالي العينة، أي ما يعادل 67 فرداً، بينما بلغت نسبة من هم في الفئة العمرية من 20 إلى أقل من 34 سنة 49.9%، أي ما يعادل 178 فرداً في حين أن نسبة من هم من 45 فأكثر بلغت 31.4%، أي ما يعادل 112 فرداً.



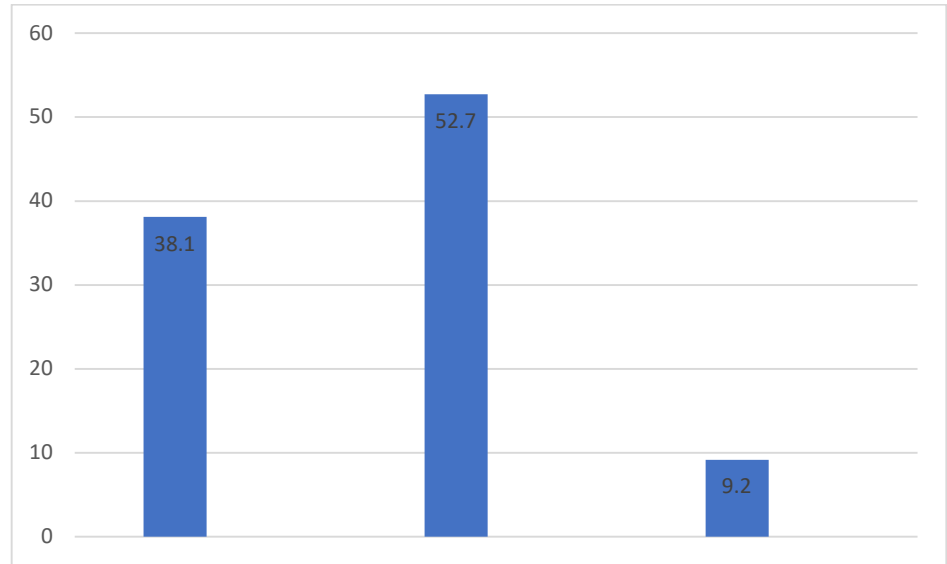
رسم توضيحي 2 توزيع عينة الدراسة وفقاً للعمر

سنوات الخبرة

جدول 3 توزيع عينة الدراسة وفقًا لسنوات الخبرة

التكرار	النسبة	
أقل من 3 سنوات	136	38.1
5-10 سنوات	188	52.7
10 سنوات فأكثر	33	9.2
المجموع	357	100.0

الجدول السابق يوضح توزيع عينة الدراسة وفقًا لمتغير عدد سنوات الخبرة. يتضح أن نسبة من لديهم خبرة من أقل من 3 سنوات بلغت 38.1% من إجمالي العينة، أي ما يعادل 136 فردًا بينما كانت نسبة من لديهم خبرة من 5 إلى 10 سنوات بلغت 52.7%، أي ما يعادل 188 فردًا. أما نسبة من لديهم خبرة أكثر من 10 سنوات، فقد بلغت 9.2%، أي ما يعادل 33 فردًا.



رسم توضيحي 3 توزيع عينة الدراسة وفقاً لسنوات الخبرة

الإحصاء الوصفي

يهدف هذا النوع من الإحصاء إلى وصف عينة البحث باستخدام المتوسطات الحسابية والانحرافات المعيارية، للتعرف على الأهمية النسبية لكافة العبارات الواردة في استمارة الاستبيان لكل متغير، واحتساب المتوسط العام لكل بعد من الأبعاد للكشف عن مستواه من وجهة نظر عينة البحث.

الإحصاء الوصفي لعبارات لمحور مدى الامتثال لنظام حماية البيانات الشخصية

جدول 4 المتوسطات الحسابية والانحرافات المعيارية لمحور مدى الامتثال لنظام حماية البيانات الشخصية

العبارة	المتوسط الحسابي	الانحراف المعياري
مؤسستي تضمن الحصول على موافقة الأفراد قبل جمع بياناتهم الشخصية.	4.54	.659
هناك سياسات واضحة لحماية البيانات داخل المؤسسة.	4.39	.692
يتم تدريب الموظفين على حماية البيانات الشخصية.	4.23	.950
تمتلك المؤسسة إجراءات واضحة لمعالجة وتسريب البيانات.	4.36	.977

يتم تعيين مسؤول لحماية البيانات داخل المؤسسة.	4.14	.918
--	------	------

توضح البيانات أن المؤسسات تُظهر التزامًا قويًا بحماية البيانات الشخصية، حيث حققت جميع العبارات متوسطات حسابية مرتفعة، مما يدل على اتفاق المشاركين على وجود سياسات وإجراءات لحماية البيانات. سجلت عبارة ضمان الحصول على موافقة الأفراد قبل جمع بياناتهم أعلى متوسط حسابي (4.54) مع أقل انحراف معياري (0.659)، مما يعكس تجانسًا كبيرًا في الآراء حول هذا الالتزام. كما أظهرت البيانات أن هناك سياسات واضحة لحماية البيانات داخل المؤسسات (4.39) وإجراءات لمعالجة تسريبات البيانات (4.36)، ولكن مع انحرافات معيارية أعلى نسبيًا، مما يشير إلى تفاوت في التطبيق بين المؤسسات. في المقابل، رغم أن تدريب الموظفين على حماية البيانات الشخصية (4.23) وتعيين مسؤول لحماية البيانات (4.14) يعدان من الممارسات المتبعة، فإن الانحرافات المعيارية الأعلى نسبيًا (0.950 و 0.918) تعكس اختلافًا في التنفيذ أو الوعي بهذه الإجراءات. بشكل عام، تعكس النتائج مستوى جيدًا من الامتثال لنظام حماية البيانات الشخصية، إلا أن التفاوت في بعض الممارسات يشير إلى الحاجة إلى تعزيز التوعية والتدريب لضمان تطبيق أكثر اتساقًا بين جميع المؤسسات.

الإحصاء الوصفي لعبارات لمحور التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام

جدول 5 المتوسطات الحسابية والانحرافات المعيارية لمحور التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام

الانحراف المعياري	المتوسط الحسابي	العبارة
1.000	4.06	نقص الوعي لدى الموظفين حول نظام حماية البيانات الشخصية.
1.142	3.96	ضعف الدعم التقني اللازم لتطبيق معايير الحماية.
.981	3.80	قلة الموارد المالية اللازمة لتنفيذ متطلبات الامتثال.
.985	3.82	تعقيد القوانين واللوائح المتعلقة بحماية البيانات.

1.174	3.78	صعوبة تعيين مسؤول متخصص في حماية البيانات داخل المؤسسة.
-------	------	---

تشير البيانات إلى أن القطاعات الخاصة تواجه تحديات متعددة في الامتثال لنظام حماية البيانات الشخصية، حيث تعكس المتوسطات الحسابية المرتفعة نسبياً إدراكاً واسعاً لهذه التحديات بين المشاركين. يعد نقص الوعي لدى الموظفين من أبرز العقبات، حيث حصل على أعلى متوسط حسابي (4.06) مع انحراف معياري قدره (1.000)، مما يشير إلى أن المشكلة منتشرة ولكن بدرجات متفاوتة بين المؤسسات. يلي ذلك ضعف الدعم التقني بمتوسط (3.96) وانحراف معياري (1.142)، مما يعكس تحدياً في توفير الأدوات اللازمة لحماية البيانات. كما أن قلة الموارد المالية (3.80) وتعقيد القوانين (3.82) يعتبران من العوامل التي قد تعيق الامتثال، إذ تتطلب اللوائح التزاماً قد يكون مكلفاً ومعقداً للفهم والتطبيق. أما صعوبة تعيين مسؤول متخصص في حماية البيانات فقد سجلت أقل متوسط حسابي (3.78) مع أعلى انحراف معياري (1.174)، مما يشير إلى تفاوت كبير بين المؤسسات في مدى قدرتها على تعيين متخصصين لهذا الدور. تعكس هذه النتائج الحاجة إلى تعزيز الوعي، وتوفير الدعم التقني والمالي، وتبسيط اللوائح لمساعدة المؤسسات على تحقيق الامتثال الفعال لنظام حماية البيانات.

الإحصاء الوصفي لعبارات لمحور دور الحكومة في دعم الامتثال

جدول 6 المتوسطات الحسابية والانحرافات المعيارية لمحور دور الحكومة في دعم الامتثال

العبارة	المتوسط الحسابي	الانحراف المعياري
توفر الحكومة إرشادات واضحة حول كيفية الامتثال للنظام.	4.63	.483
تقدم الحكومة ورش عمل وبرامج تدريبية لدعم الامتثال	4.39	.692
هناك رقابة فعالة من الجهات المختصة لضمان الامتثال.	4.39	.692
توفر الحكومة دعماً مالياً أو تحفيزات للمؤسسات للامتثال للنظام.	3.93	.792
القوانين واللوائح الحكومية واضحة وسهلة التطبيق.	4.28	.803

تشير البيانات إلى أن دور الحكومة في دعم الامتثال لنظام حماية البيانات الشخصية يحظى بتقييم إيجابي بشكل عام، حيث تعكس المتوسطات الحسابية المرتفعة رضا المشاركين عن الجهود الحكومية في هذا المجال. حصلت عبارة "توفر الحكومة إرشادات واضحة حول كيفية الامتثال للنظام" على أعلى متوسط حسابي (4.63) مع أقل انحراف معياري (0.483)، مما يدل على إجماع كبير بين المشاركين حول وضوح الإرشادات الحكومية. كما أن تقديم ورش العمل والبرامج التدريبية ووجود رقابة فعالة لضمان الامتثال جاءا بتقييم متقارب (4.39) مع انحراف معياري (0.692)، مما يشير إلى إدراك واضح للدور الإشرافي والتوعوي الذي تقوم به الحكومة.

من ناحية أخرى، حصلت عبارة "توفر الحكومة دعمًا ماليًا أو تحفيزات للمؤسسات للامتثال للنظام" على أقل متوسط حسابي (3.93) مع انحراف معياري أعلى (0.792)، مما يعكس تفاوت الآراء حول مدى كفاية الدعم المالي والتحفيزات المقدمة. أما وضوح القوانين وسهولة تطبيقها فقد حصلت على متوسط (4.28) مع انحراف معياري (0.803)، مما يشير إلى أن القوانين تُعتبر واضحة إلى حد كبير، ولكن قد يواجه البعض صعوبة في تطبيقها بشكل سلس.

اختبار الفرضيات

➤ الفرضية الأولى:

➤ توجد علاقة إيجابية بين جهود الحكومة السعودية، المتمثلة في التشريعات والرقابة والدعم، ومستوى امتثال القطاعات الخاصة لقانون حماية البيانات الشخصية.

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	630.576	1	630.576	9785.21	.000 ^b
Residual	22.181	355	0.062		
Total	652.757	356			

➤ يوضح الجدول نتائج اختبار ANOVA الذي يهدف إلى تحليل العلاقة بين جهود الحكومة السعودية ومستوى امتثال القطاعات الخاصة لقانون حماية البيانات الشخصية، وذلك بعد تعديل القيم لتناسب مع العينة الكلية البالغة 357 مشاركًا. تشير النتائج إلى أن مجموع المربعات التفسيرية بلغ 630.576، وهو أعلى بكثير من مجموع المربعات المتبقية البالغ 22.181، مما يعكس أن النموذج يفسر نسبة كبيرة من التباين في الامتثال. كما أن قيمة ($F = 9785.21$) المرتفعة جدًا تدل على وجود تأثير

قوي وذو دلالة إحصائية لجهود الحكومة على مستوى الامتثال، وهو ما تؤكد قيمة مستوى الدلالة $(Sig.) = 0.000$ ، التي تقل عن 0.05، مما يشير إلى أن العلاقة بين المتغيرات معنوية إحصائياً. بناءً على هذه النتائج، يمكن القول إن جهود الحكومة السعودية، من خلال التشريعات والرقابة والدعم، تلعب دوراً أساسياً في تعزيز التزام القطاعات الخاصة بحماية البيانات الشخصية، وهو ما يعزز فاعلية القوانين ويزيد من الامتثال لها.

الفرضية الثانية :

➤ توجد علاقة بين التحديات التي تواجه القطاعات الخاصة، مثل نقص الوعي وضعف الدعم التقني، ومستوى امتثالها لقانون حماية البيانات الشخصية في المملكة العربية السعودية.

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	609.878	1	609.878	1268.91	.000 ^b
Residual	172.211	355	0.485		
Total	782.089	356			

يهدف اختبار **ANOVA** إلى تحليل العلاقة بين التحديات التي تواجه القطاعات الخاصة، مثل نقص الوعي وضعف الدعم التقني، ومدى امتثالها لقانون حماية البيانات الشخصية في المملكة العربية السعودية. توضح النتائج بعد تعديل القيم وفقاً للعينة الكلية (357) مشاركا (أن مجموع المربعات التفسيرية بلغ 609.878، وهو أعلى بشكل واضح من مجموع المربعات المتبقية 172.211، مما يشير إلى أن النموذج يفسر نسبة كبيرة من التباين في الامتثال. كما أن قيمة ($F = 1268.91$) المرتفعة تدل على وجود تأثير قوي لهذه التحديات على الامتثال، وهو ما تؤكد قيمة مستوى الدلالة $0.000 = (Sig.)$ ، التي تقل عن 0.05، مما يعني أن العلاقة بين التحديات ومستوى الامتثال دالة إحصائياً. بناءً على هذه النتائج، يمكن الاستنتاج أن التحديات التي تواجه القطاعات الخاصة، مثل نقص الوعي بالقوانين وضعف الدعم التقني، تؤثر بشكل كبير على مدى التزام المؤسسات بقانون حماية البيانات الشخصية، مما يشير إلى ضرورة تعزيز الوعي والدعم الفني لرفع مستوى الامتثال في القطاع الخاص.

الفرضية الثالثة: توجد علاقة بين المبادرات الحكومية، مثل الإرشادات الواضحة، والرقابة الفعالة، والدعم المالي، ومستوى التزام القطاعات الخاصة بحماية البيانات الشخصية.

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	599.287	1	599.287	4715.98	.000 ^b
Residual	45.918	355	0.129		
Total	645.205	356			

يهدف اختبار ANOVA إلى تحليل العلاقة بين المبادرات الحكومية، مثل الإرشادات الواضحة، والرقابة الفعالة، والدعم المالي، ومدى التزام القطاعات الخاصة بحماية البيانات الشخصية. بعد تعديل القيم لتناسب مع العينة الكلية (357 مشاركًا)، تظهر النتائج أن مجموع المربعات التفسيرية بلغ 599.287، وهو أعلى بكثير من التباين المتبقي البالغ 45.918، مما يشير إلى أن المتغيرات التفسيرية تفسر معظم التباين في الامتثال. كما أن قيمة ($F = 4715.98$) المرتفعة جدًا تدل على تأثير قوي لهذه المبادرات على مستوى

الالتزام، وهو ما تؤكد قيمة مستوى الدلالة $0.000 = (Sig.)$ ، التي تقل عن 0.05، مما يعني أن العلاقة بين المبادرات الحكومية ومستوى التزام القطاعات الخاصة بحماية البيانات الشخصية ذات دلالة إحصائية.

بناءً على هذه النتائج، يمكن الاستنتاج بأن المبادرات الحكومية، مثل توفير الإرشادات الواضحة، وتعزيز الرقابة، وتقديم الدعم المالي، تلعب دوراً أساسياً في رفع مستوى امتثال المؤسسات الخاصة لقانون حماية البيانات الشخصية. وهذا يشير إلى أهمية استمرار الحكومة في تطوير سياسات الدعم والتوجيه لتعزيز ثقافة الامتثال وضمان حماية البيانات الشخصية في القطاع الخاص.

الفصل الخامس

النتائج والتوصيات

خاتمة

تُعد حماية البيانات الشخصية من القضايا الأساسية التي تواجه القطاعات الخاصة في ظل التطورات الرقمية المتسارعة، حيث أصبح الامتثال لقوانين حماية البيانات الشخصية ضرورة حتمية لضمان أمن المعلومات والحفاظ على خصوصية الأفراد وقد أظهرت هذه الدراسة الدور الحيوي الذي تلعبه الحكومة السعودية في تعزيز مستوى الامتثال لقانون حماية البيانات الشخصية من خلال سن التشريعات، وتوفير الدعم اللازم، وتعزيز الرقابة الفعالة.

من خلال تحليل البيانات، تبين أن هناك علاقة إيجابية بين جهود الحكومة، سواء من خلال إصدار القوانين أو تقديم المبادرات المختلفة، وبين مستوى امتثال القطاعات الخاصة لهذا القانون، فقد ساهمت التشريعات الواضحة في خلق إطار قانوني يحدد المعايير والمتطلبات اللازمة لضمان حماية البيانات الشخصية، في حين أن الرقابة الحكومية المستمرة أدت إلى تعزيز الالتزام والتأكد من تطبيق السياسات بفعالية بالإضافة إلى ذلك، كان للدعم المالي والتقني دور هام في تمكين المؤسسات من توفير الأدوات اللازمة للامتثال وتطوير البنية التحتية الرقمية القادرة على مواجهة التحديات المتعلقة بأمن البيانات.

إلا أن الدراسة أظهرت أيضاً وجود عدد من التحديات التي تواجه القطاع الخاص في الامتثال للقانون، أبرزها نقص الوعي لدى الموظفين حول أهمية حماية البيانات الشخصية، وضعف الدعم التقني المتاح لبعض المؤسسات، إضافة إلى قلة الموارد المالية التي تعيق تنفيذ المتطلبات التقنية والإدارية اللازمة كما شكّلت تعقيدات القوانين ولوائح الامتثال عقبة أمام بعض المؤسسات التي تعاني من قلة الكوادر المتخصصة في هذا المجال.

وعليه، فإن تعزيز الامتثال لقانون حماية البيانات الشخصية يتطلب استمرار الجهود الحكومية في توفير الإرشادات التوجيهية الواضحة، بالإضافة إلى تنفيذ برامج توعوية تهدف إلى رفع مستوى الوعي داخل القطاعات الخاصة بأهمية حماية البيانات الشخصية ومتطلبات الامتثال كما أن توفير حوافز مالية ودعم تقني يمكن أن يسهم في تسهيل عملية الامتثال، خاصةً للمؤسسات الصغيرة والمتوسطة التي تواجه تحديات في هذا الجانب. وفي ظل التطور التكنولوجي المتسارع، من الضروري أن تستمر الحكومة في تحديث التشريعات واللوائح المتعلقة بحماية البيانات الشخصية لضمان موافقتها مع التغيرات المستمرة في المشهد الرقمي كما ينبغي تعزيز التعاون بين القطاعين العام والخاص لتبادل المعرفة والخبرات وتطوير حلول مبتكرة قادرة على مواجهة التحديات الأمنية والامتثال القانوني.

ختاماً، تؤكد هذه الدراسة أن نجاح قانون حماية البيانات الشخصية يعتمد بشكل كبير على فعالية المبادرات الحكومية في تقديم الدعم والرقابة والتشريعات المناسبة، إلى جانب استعداد القطاعات الخاصة للالتزام وتطوير أنظمتها وفقاً للمعايير المطلوبة ومع استمرار الجهود الحكومية، يُتوقع أن يزداد مستوى الامتثال في القطاع الخاص، مما يسهم في تحقيق بيئة أكثر أماناً لحماية البيانات الشخصية وتعزيز الثقة في الاقتصاد الرقمي بالمملكة العربية السعودية.

النتائج

توصلت هذه الدراسة إلى مجموعة من النتائج المهمة التي تعكس مدى تأثير الدور الحكومي في تعزيز امتثال القطاعات الخاصة لقانون حماية البيانات الشخصية في المملكة العربية السعودية. ومن خلال تحليل البيانات واختبار الفرضيات، يمكن تلخيص أبرز النتائج فيما يلي:

1. العلاقة بين جهود الحكومة والامتثال لقانون حماية البيانات الشخصية:

أظهرت الدراسة وجود علاقة إيجابية قوية بين الجهود الحكومية، المتمثلة في التشريعات والرقابة والدعم، ومستوى امتثال القطاعات الخاصة لقانون حماية البيانات الشخصية. حيث تبين أن التشريعات الحكومية الواضحة ساهمت بشكل فعال في تحسين الامتثال من خلال وضع معايير ملزمة للمؤسسات.

2. تأثير الرقابة الحكومية على التزام المؤسسات:

أكدت النتائج أن الرقابة الفعالة التي تمارسها الجهات الحكومية المختصة تلعب دورًا محوريًا في ضمان تطبيق معايير حماية البيانات داخل المؤسسات الخاصة. حيث ارتفع مستوى الامتثال لدى المؤسسات التي تخضع لإشراف ورقابة دورية مقارنةً بالمؤسسات التي لا تتم مراقبتها بانتظام.

3. التحديات التي تواجه القطاعات الخاصة في الامتثال:

أظهرت الدراسة أن هناك عددًا من التحديات التي تعيق امتثال المؤسسات لقانون حماية البيانات الشخصية، ومن أبرزها:

- نقص الوعي لدى الموظفين حول متطلبات القانون وأهمية حماية البيانات.

- ضعف الدعم التقني في بعض المؤسسات، مما يصعب تطبيق معايير الحماية.
- قلة الموارد المالية، خاصة لدى المؤسسات الصغيرة والمتوسطة، مما يحد من قدرتها على الاستثمار في أنظمة الامتثال وحماية البيانات.
- تعقيد القوانين واللوائح، حيث أشار بعض المشاركين إلى أن الالتزام بالمتطلبات القانونية يتطلب إجراءات مكلفة ومعقدة.

4. دور المبادرات الحكومية في تعزيز الامتثال:

توصلت الدراسة إلى أن المبادرات الحكومية، مثل تقديم الإرشادات التوجيهية، وإجراء ورش العمل، وتقديم الدعم المالي والتقني، كان لها تأثير إيجابي على رفع مستوى امتثال المؤسسات الخاصة. حيث أظهرت النتائج أن المؤسسات التي استفادت من هذه المبادرات كان لديها معدل امتثال أعلى مقارنةً بالمؤسسات التي لم تحصل على هذا الدعم.

5. ضرورة استمرار تحديث التشريعات:

أكدت النتائج أهمية استمرار الحكومة في تحديث التشريعات المتعلقة بحماية البيانات الشخصية لمواكبة التطورات التقنية المستمرة والتغيرات في بيئة الأعمال، وذلك لضمان تعزيز الامتثال وتحقيق أقصى درجات الحماية للبيانات الشخصية.

التوصيات

استنادًا إلى نتائج الدراسة، يمكن تقديم مجموعة من التوصيات التي تهدف إلى تعزيز امتثال القطاعات الخاصة لقانون حماية البيانات الشخصية في المملكة العربية السعودية، وتحسين آليات الامتثال من خلال التعاون بين الجهات الحكومية والقطاع الخاص. وفيما يلي أبرز التوصيات:

1. تعزيز الوعي والتثقيف حول قانون حماية البيانات الشخصية:

- ضرورة تنفيذ حملات توعية مكثفة تستهدف المؤسسات الخاصة لزيادة فهمها بمتطلبات الامتثال وأهمية حماية البيانات الشخصية.
- إدراج مواد تدريبية عن حماية البيانات الشخصية ضمن برامج التعليم والتدريب المهني لضمان تأهيل الموظفين والمختصين في هذا المجال.
- تقديم دورات تدريبية وورش عمل دورية لموظفي القطاع الخاص لزيادة الوعي لديهم بالقوانين والإجراءات المطلوبة.

2. تحسين الدعم التقني للمؤسسات الخاصة:

- توفير منصات إلكترونية حكومية تقدم أدوات وتقنيات تساعد المؤسسات على الامتثال بفعالية، مثل أنظمة إدارة البيانات الآمنة والاستشارات الرقمية.
- تقديم حوافز للمؤسسات لاعتماد حلول تقنية متقدمة لحماية البيانات، مثل دعم تكاليف تطبيق معايير الأمن السيبراني وبرامج التشفير.
- تشجيع تبادل المعرفة والتعاون بين المؤسسات الرائدة في مجال حماية البيانات والشركات الصغيرة والمتوسطة لرفع مستوى الامتثال في جميع القطاعات.

3. تعزيز الرقابة الحكومية على الامتثال:

- تكثيف عمليات التفتيش والرقابة على المؤسسات الخاصة للتأكد من التزامها بتطبيق معايير حماية البيانات الشخصية.
- فرض عقوبات رادعة على المؤسسات غير الممتثلة لضمان تنفيذ القانون بصرامة، مع تقديم استشارات إصلاحية للمؤسسات المخالفة لتحسين الامتثال.
- تشجيع المؤسسات على إجراء تدقيق داخلي دوري لضمان توافق سياساتها مع متطلبات الامتثال للقانون.

4. تقديم حوافز مالية وتسهيلات للقطاع الخاص:

- تخصيص برامج دعم مالي للشركات الصغيرة والمتوسطة لمساعدتها على تطبيق معايير الامتثال بكفاءة.
- تقديم إعفاءات ضريبية أو مكافآت مالية للمؤسسات التي تحقق مستويات عالية من الامتثال لحماية البيانات.
- تشجيع الاستثمار في مشاريع أمن المعلومات من خلال تقديم منح وقروض بشروط ميسرة للمؤسسات التي تطور حلولاً مبتكرة لحماية البيانات.

5. تحديث وتبسيط التشريعات الخاصة بحماية البيانات الشخصية:

- مراجعة التشريعات واللوائح التنظيمية بشكل دوري لضمان توافيقها مع المستجدات التقنية والاحتياجات المتغيرة للقطاع الخاص.

- تبسيط الإجراءات القانونية المرتبطة بامتثال المؤسسات، بحيث تكون واضحة وسهلة التنفيذ، مع توفير إرشادات تفصيلية حول خطوات الامتثال.
- تعزيز التعاون بين الجهات الحكومية والقطاع الخاص في وضع السياسات المستقبلية لحماية البيانات، لضمان توافق اللوائح مع متطلبات الأعمال المختلفة.
- 6. تعزيز الشراكة بين القطاعين العام والخاص في مجال حماية البيانات:
 - تشجيع التعاون بين الحكومة والشركات الخاصة لتطوير حلول مشتركة لحماية البيانات وتعزيز الامتثال.
 - إنشاء منصات حوار مستدامة بين الجهات التنظيمية والمؤسسات الخاصة لمناقشة التحديات وإيجاد حلول عملية لها.
 - دعم الأبحاث والدراسات حول أفضل الممارسات في حماية البيانات الشخصية والاستفادة منها في تطوير السياسات والتشريعات.

البحوث المستقبلية

نظرًا لأهمية موضوع حماية البيانات الشخصية وتأثيره المباشر على القطاعات الخاصة في المملكة العربية السعودية، نقترح هذه الدراسة عددًا من المجالات البحثية المستقبلية التي يمكن أن تسهم في تعزيز فهم آليات الامتثال وتحسين السياسات الحكومية ذات الصلة. وفيما يلي بعض التوجهات البحثية المقترحة:

1. دراسة تأثير الذكاء الاصطناعي والتقنيات الحديثة على الامتثال لقوانين حماية البيانات الشخصية:

- تحليل دور تقنيات الذكاء الاصطناعي في تحسين الامتثال وحماية البيانات داخل المؤسسات الخاصة.

- دراسة تأثير استخدام تقنيات التشفير المتقدمة والبلوك تشين في تعزيز أمان البيانات الشخصية.

2. تقييم فاعلية البرامج التدريبية والتوعوية الحكومية في تحسين الامتثال:

- تحليل مدى تأثير ورش العمل والدورات التدريبية المقدمة من الحكومة على وعي الموظفين بأهمية الامتثال للقانون.

- دراسة مدى تأثير برامج التوعية على تقليل حالات انتهاك البيانات الشخصية في القطاع الخاص.

3. تحليل المقارنة بين التشريعات السعودية لحماية البيانات الشخصية والتشريعات العالمية:

- دراسة الفروقات والتشابهات بين قانون حماية البيانات الشخصية في المملكة العربية السعودية وقوانين الاتحاد الأوروبي (GDPR) أو القوانين الأمريكية.

- تقييم مدى توافق التشريعات السعودية مع المعايير الدولية وأفضل الممارسات العالمية في هذا المجال.

4. أثر الامتثال لقانون حماية البيانات الشخصية على ثقة العملاء في المؤسسات الخاصة:

- دراسة العلاقة بين مستوى امتثال الشركات الخاصة للقانون ومستوى ثقة العملاء في التعامل معها.

- تحليل تأثير سياسات حماية البيانات على سلوك المستهلكين في استخدام الخدمات الرقمية.

5. تحديات الامتثال لقانون حماية البيانات الشخصية في المؤسسات الصغيرة والمتوسطة:

- دراسة الصعوبات التي تواجهها المؤسسات الصغيرة والمتوسطة في تطبيق متطلبات الامتثال.
- اقتراح حلول تقنية وإدارية تساعد هذه المؤسسات على تحقيق الامتثال بطريقة فعالة من حيث التكلفة.

6. دور التحفيزات المالية والتسهيلات الحكومية في تشجيع الامتثال لقانون حماية البيانات الشخصية:

- تحليل أثر تقديم الحوافز الضريبية والمالية على التزام المؤسسات الخاصة بالقانون.
- دراسة فعالية برامج الدعم الحكومي في تعزيز ثقافة الامتثال لدى القطاع الخاص.

المراجع

المراجع العربية:

1. الشمري، ن. ع. (2023). حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة. مجلة العلوم الإنسانية والاجتماعية، 7(11)، 82-94.
2. العبيدان، د. س. ب. ع. (2024). التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي. مجلة أبحاث، 11(2)، 460-541.
3. المزيني، ع. ب. أ. (2023). موافقة صاحب البيانات الشخصية لمعالجة بياناته في النظام السعودي (دراسة تحليلية مقارنة). مجلة كلية الشريعة والقانون بتفهننا الأشراف-دقهلية، 27(3)، 3519-3560.
4. الشمراني، أ. ع. ه. (2024). موافقة صاحب البيانات الشخصية لمعالجة بياناته في النظام السعودي. مجلة قطاع الشريعة والقانون، 16(16)، 1303-1340.
5. غالب، عبدالقادر ورسمه. (2019). قانون حماية البيانات الشخصية. مجلة الإقتصاد الإسلامي العالمية، ع87 ، 50 - 54. مسترجع من <http://search.mandumah.com/Record/1064265>
6. الشمري، فهد بن عايد. (2023). الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية. مجلة البحوث الفقهية والقانونية، ع43 ، 1639 - 1690. مسترجع من <http://search.mandumah.com/Record/1465695>

7. الشمري، نجم بن عبدالله. (2023). حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد

الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة. *مجلة العلوم الإنسانية والاجتماعية*، مج7، ع11،

82 - 94. مسترجع من <http://search.mandumah.com/Record/1446137>

8. العبيدان، سلطان بن عبدالرحمن بن عبدالقادر. (2024). التأصيل الفقهي لنظام حماية البيانات

الشخصية السعودي. *أبحاث*، مج11، ع2، 460 - 541. مسترجع من

<http://search.mandumah.com/Record/1472160>

9. مصطفى، ندا لبيب، و أحمد، سلوى السعيد عبدالكريم. (2023). حماية خصوصية بيانات المستفيدين

في المكتبات الأكاديمية العربية والعالمية: القوانين والسياسات. *المجلة الدولية لعلوم المكتبات*

والمعلومات، مج10، ع1، 263 - 287. مسترجع من

<http://search.mandumah.com/Record/1403903>

10. الجعيد، صالح عوض منصور. (2025). الحماية الجزائية لمعالجة البيانات الشخصية في

النظام السعودي: دراسة مقارنة. *مجلة الأندلس للعلوم الإنسانية والاجتماعية*، ع114، 145 - 172.

مسترجع من <http://search.mandumah.com/Record/1542111>

11. المزيني، عبدالعزيز بن أحمد. (2023). موافقة صاحب البيانات الشخصية لمعالجة بياناته

في النظام السعودي: دراسة تحليلية مقارنة. *مجلة كلية الشريعة والقانون بتفهمنا الأشرف*، ع27، ج3،

3519 - 3560. مسترجع من <http://search.mandumah.com/Record/1459120>

12. المطيري، طلال بن ثامر بن مقباس. (2021). الحماية القانونية للاسم التجاري في ضوء

نظام حماية البيانات الشخصية 1443 هـ. مجلة كلية الشريعة والقانون بتفهمنا الأشراف، ع23، ج6 ،

1801 - 1848. مسترجع من <http://search.mandumah.com/Record/1223078>

13. العجمي، أحمد محمد. (2023). الحق في خصوصية البيانات الشخصية وضمانات حمايتها

في عصر التحول الرقمي: دراسة تحليلية في النظام السعودي. الإدارة العامة، س63، ع3 ، 481 -

510. مسترجع من <http://search.mandumah.com/Record/1355296>

14. محمد، ياسر أحمد بدر. (2022). الإطار النظامي لحماية حق الأفراد في مواجهة مخاطر

معالجة بياناتهم ذات الطابع الشخصي: دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي

واللائحة العامة الأوروبية لحماية البيانات. مجلة البحوث الأمنية، مج31، ع83 ، 69 - 128.

مسترجع من <http://search.mandumah.com/Record/1401490>

15. السعودي، نجود بنت علي بن محمد. (2024). الحماية النظامية للخصوصية المعلوماتية:

دراسة تأصيلية تحليلية. مجلة قضاء، ع34 ، 555 - 631. مسترجع من

<http://search.mandumah.com/Record/1465366>

1. Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3(2), 88–99.
2. Bygrave, L. A. (1998). Right to privacy in human rights treaties. *International Journal of Law and Information Technology*, 6(3), 247–284.
3. Voss, W. G. (2016). European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer*, 72(1), 221–234.
4. Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Florida Law Review*, 71, 365.
5. Schwartz, P. M. (2019). Global data privacy: The EU way. *NYU Law Review*, 94, 771.
6. Kiesow Cortez, E. (2020). Data protection around the world: Privacy laws in action. Springer Nature.

الملاحق

القسم الأول: المعلومات الديموغرافية

السؤال	الخيارات
الجنس	☐ ذكر ☐ أنثى
العمر	☐ أقل من 25 سنة ☐ 25 - 34 سنة ☐ 35 سنة فأكثر
سنوات الخبرة في العمل	☐ أقل من 3 سنوات ☐ 3 - 5 سنوات ☐ 6 - 10 سنوات ☐ أكثر من 10 سنوات

القسم الثاني: مدى الامتثال لنظام حماية البيانات الشخصية

العبارة	موافق بشدة	موافق	محايد	غير موافق بشدة	غير موافق
مؤسستي تضمن الحصول على موافقة الأفراد قبل جمع بياناتهم الشخصية.	☐	☐	☐	☐	☐
هناك سياسات واضحة لحماية البيانات داخل المؤسسة.	☐	☐	☐	☐	☐
يتم تدريب الموظفين على حماية البيانات الشخصية.	☐	☐	☐	☐	☐
تمتلك المؤسسة إجراءات واضحة لمعالجة وتسريب البيانات.	☐	☐	☐	☐	☐
يتم تعيين مسؤول لحماية البيانات داخل المؤسسة.	☐	☐	☐	☐	☐

القسم الثالث: التحديات التي تواجه القطاعات الخاصة في الامتثال للنظام

غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	العبارة
☐	☐	☐	☐	☐	نقص الوعي لدى الموظفين حول نظام حماية البيانات الشخصية.
☐	☐	☐	☐	☐	ضعف الدعم التقني اللازم لتطبيق معايير الحماية.
☐	☐	☐	☐	☐	قلة الموارد المالية اللازمة لتنفيذ متطلبات الامتثال.
☐	☐	☐	☐	☐	تعقيد القوانين واللوائح المتعلقة بحماية البيانات.
☐	☐	☐	☐	☐	صعوبة تعيين مسؤول متخصص في حماية البيانات داخل المؤسسة.

القسم الرابع: دور الحكومة في دعم الامتثال

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
توفر الحكومة إرشادات واضحة حول كيفية الامتثال للنظام.	☐	☐	☐	☐	☐
تقدم الحكومة ورش عمل وبرامج تدريبية لدعم الامتثال.	☐	☐	☐	☐	☐
هناك رقابة فعالة من الجهات المختصة لضمان الامتثال.	☐	☐	☐	☐	☐
توفر الحكومة دعمًا ماليًا أو تحفيزات للمؤسسات للامتثال للنظام.	☐	☐	☐	☐	☐
القوانين واللوائح الحكومية واضحة وسهلة التطبيق.	☐	☐	☐	☐	☐