



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

إعداد الطالب / Dhuha AIQAWSi
الرقم الجامعي / 242001584

إشراف / Dr. ASMAA ABUANZAH

العام الدراسي

2024

المحتويات

٣	المقدمة
٣	أهمية الدراسة
٤	مشكلة الدراسة
٥	أهداف البحث
٥	تساؤلات الدراسة
٦	الدراسات السابقة
٧	منهجية البحث وطرق البحث
٨	حدود الدراسة
١١	دراسة حالة
١٤	الجدول الزمني
١٤	الخاتمة
١٦	المراجع

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 ٢٠٣٠، 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

١. 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.

٢. 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.

٣. التأثير على الاقتصاد الوطني

تُعد حماية البيانات الشخصية جزءاً أساسياً من بناء بيئة رقمية آمنة ومستدامة. عندما تُظهر الحكومات والشركات التزاماً 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 فعالة لضمان خصوصية الأفراد وسلامة المعلومات. ومع ذلك، تواجه 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 قائماً حول مدى كفاية هذه الأدوات لتحقيق الامتثال الكامل، و بالإضافة 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 سلباً 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

١. 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.

٢. 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.

٣. 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؟

الدراسات السابقة

١. دراسة: "تطبيق قانون حماية البيانات الأوروبي (GDPR) في الشركات الصغيرة والمتوسطة"

الهدف: تحليل مدى قدرة الشركات الصغيرة على الامتثال لقانون GDPR وتكاليف الالتزام.

النتائج:

قدمت الدراسة دليلاً على أن الامتثال يتطلب استثمارات كبيرة في البنية التحتية التقنية.

أظهرت أيضاً أن الامتثال يحسن ولاء العملاء وثقتهم.

العلاقة بالدراسة الحالية: توفر فهماً معمقاً لتحديات الامتثال التي قد تواجهها الشركات السعودية عند تطبيق قانون PDPL.

٢. دراسة: "أثر قوانين حماية البيانات على الاقتصاد الرقمي في منطقة الخليج العربي"

الهدف: قياس تأثير قوانين حماية البيانات على استقطاب الاستثمارات في دول الخليج.

النتائج:

الدول ذات القوانين الصارمة لحماية البيانات جذبت استثمارات أكبر في مجالات التكنولوجيا.

حماية البيانات أسهمت في تعزيز الابتكار الرقمي.

العلاقة بالدراسة الحالية: تبرز أهمية قانون PDPL في دعم رؤية ٢٠٣٠ لتحقيق التحول الرقمي وجذب الاستثمارات.

٣. دراسة: "تحديات حماية البيانات الشخصية في المملكة العربية السعودية: دراسة استقصائية"

الهدف: استقصاء آراء الشركات والخبراء حول التحديات التي تواجه تطبيق قوانين حماية البيانات.

النتائج:

نقص الوعي وضعف التخصص التقني أبرز التحديات.

الحاجة إلى مبادرات حكومية لدعم الشركات الصغيرة والمتوسطة.

العلاقة بالدراسة الحالية: تدعم هذا البحث في تحليل التحديات والفرص التي يوفرها تطبيق PDPL.

منهجية البحث وطرق البحث

١. المنهج المستخدم

• المنهج الوصفي التحليلي:

يساعد في وصف واقع تطبيق قانون PDPL وتحليل البيانات المتاحة لفهم تأثيره على القطاعات الخاصة.

• المنهج المقارن:

يتم استخدامه لمقارنة قانون PDPL مع قوانين حماية البيانات الأخرى مثل GDPR.

٢. أدوات البحث

• الاستبيانات:

إعداد استبيان موجه للشركات الصغيرة والمتوسطة والشركات الكبرى لقياس وعيها ومتطلبات الامتثال.

محاور الاستبيان تشمل: الوعي، التكاليف، الإجراءات المتبعة، ومدى تأثير القانون.

- المقابلات:

مقابلات مع خبراء قانونيين ومسؤولين حكوميين لمعرفة رؤيتهم حول تطبيق PDPL.

مقابلات مع مديري تكنولوجيا المعلومات في القطاع الخاص.

٣. طرق جمع البيانات

- المصادر الأولية:

جمع البيانات من الاستبيانات والمقابلات.

- المصادر الثانوية:

تحليل النصوص القانونية والتقارير الصادرة عن الهيئات التنظيمية في السعودية.

مراجعة الدراسات السابقة ذات العلاقة.

٤. تحليل البيانات

- استخدام برنامج SPSS لتحليل الاستبيانات.
- استخراج العلاقات بين التحديات وفرص الامتثال.

حدود الدراسة

١. الحدود الزمانية

تمت الدراسة على مدى العامين الماضيين (٢٠٢٢-٢٠٢٤) بهدف فهم تطورات تطبيق قانون PDPL.

٢. الحدود المكانية

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

٣. الحدود المنهجية

استخدام الاستبيانات والمقابلات فقط قد يحد من شمولية النتائج.

عدم شمول جميع القطاعات الخاصة بسبب تنوعها الواسع.

الإطار النظري

١. تعريف البيانات الشخصية

البيانات الشخصية هي كل معلومة تتعلق بفرد يمكن من خلالها تحديد هويته بشكل مباشر أو غير مباشر. تشمل هذه البيانات معلومات مثل الاسم، الرقم الوطني، العنوان، البريد الإلكتروني، رقم الهاتف، المعلومات الصحية، وحتى البيانات الرقمية مثل عنوان IP وسجل التصفح. يُعتبر تعريف البيانات الشخصية حجر الزاوية في أي نظام لحماية البيانات، حيث يساعد في تحديد ما يجب حمايته وكيفية تنظيمه.

٢. أهمية حماية البيانات الشخصية

• ضمان خصوصية الأفراد

حماية البيانات الشخصية هي ضرورة لضمان خصوصية الأفراد في جميع تعاملاتهم الرقمية. يؤدي جمع البيانات دون حماية كافية إلى انتهاكات خطيرة، مثل التجسس أو سرقة الهوية، مما يهدد سلامة وخصوصية الأفراد.

• تقليل مخاطر الاختراقات الأمنية

عند حماية البيانات الشخصية بشكل صحيح، تقل مخاطر الاختراقات التي قد تؤدي إلى تسرب معلومات حساسة. يمكن أن تؤثر هذه التسريبات سلباً على الأفراد والشركات، سواء من خلال فقدان الثقة أو التعرض لمطالبات قانونية وتعويضات مالية كبيرة.

• تعزيز الثقة في النظام الرقمي

تعتبر حماية البيانات عاملاً أساسياً لتعزيز ثقة المستخدمين في البيئة الرقمية، سواء كانت مواقع إلكترونية، تطبيقات، أو خدمات حكومية. عندما يشعر الأفراد بأن بياناتهم محمية، فإنهم يكونون أكثر استعداداً للمشاركة والتفاعل مع هذه الأنظمة.

٣. مقارنة بين نظم حماية البيانات عالمياً

نظام حماية البيانات الأوروبي (GDPR)

يُعد النظام العام لحماية البيانات (GDPR) في الاتحاد الأوروبي أحد المعايير العالمية الرائدة في مجال حماية البيانات. يضع هذا النظام متطلبات صارمة على المؤسسات التي تجمع أو تعالج بيانات الأفراد، بما في ذلك:

- الحصول على موافقة واضحة من المستخدمين.
- ضمان الشفافية في كيفية استخدام البيانات.
- تمكين الأفراد من الوصول إلى بياناتهم وتصحيحها أو حذفها.
- فرض غرامات عالية على المؤسسات غير الملتزمة.

نظام حماية البيانات في السعودية (PDPL)

يشترك قانون حماية البيانات الشخصية السعودي (PDPL) مع GDPR في العديد من المبادئ، مثل أهمية الموافقة والشفافية وحقوق الوصول. ومع ذلك، يتميز PDPL بتركيزه على الخصوصية في السياق المحلي والتكيف مع رؤية ٢٠٣٠ للتحويل الرقمي. كما يأخذ القانون بعين الاعتبار التحديات الخاصة بالسعودية، مثل نقص الوعي التقني لدى بعض المؤسسات الصغيرة والمتوسطة.

مقارنة عامة

التشابهات: كلا النظامين يسعيان لحماية حقوق الأفراد وضمان الاستخدام المسؤول للبيانات.

الاختلافات: يشمل GDPR مجالاً جغرافياً أوسع، بينما يركز PDPL على تعزيز التحول الرقمي المحلي ودعم رؤية ٢٠٣٠.

يوضح الإطار النظري أهمية البيانات الشخصية كأصل رقمي يجب حمايته، كما يبرز أهمية تطوير أطر قانونية وتنظيمية تتماشى مع التطورات العالمية والمحلية. تُعد المقارنة بين PDPL وGDPR فرصة لفهم نقاط القوة والتحديات في تطبيق قوانين حماية البيانات، مما يمكن من تحسين التنفيذ على الصعيد المحلي.

دراسة حالة

تحليل تطبيق PDPL: دراسة حالة شركة تعمل في القطاع التقني

١. استراتيجيات الشركة للامتثال

أ. مراجعة سياسات جمع البيانات ومعالجتها

قامت الشركة بإجراء مراجعة شاملة لسياسات جمع البيانات الشخصية ومعالجتها لتتوافق مع متطلبات قانون حماية البيانات الشخصية (PDPL).

تضمنت المراجعة تحديد أنواع البيانات التي يتم جمعها، وضمان أن البيانات المطلوبة هي فقط الضرورية لتقديم الخدمات.

ب. إنشاء قسم مختص بحماية البيانات

أسست الشركة قسمًا متخصصًا بحماية البيانات بقيادة مسؤول حماية البيانات (Data Protection Officer).

كانت مهام القسم تشمل مراقبة الامتثال للقانون، إعداد تقارير دورية، وتطوير خطط إدارة البيانات.

ج. تطبيق تقنيات التشفير والحماية

استخدمت الشركة تقنيات تشفير متقدمة لحماية البيانات أثناء النقل والتخزين، مما يقلل من مخاطر الاختراقات الأمنية.

تضمنت هذه الإجراءات تحديث الأنظمة الأمنية بشكل دوري وإجراء اختبارات اختراق للتحقق من كفاءتها.

د. التدريب ورفع الوعي الداخلي

قدمت الشركة دورات تدريبية لجميع موظفيها لفهم متطلبات القانون وأفضل الممارسات في التعامل مع البيانات الشخصية.

ركزت الدورات على أهمية الخصوصية وكيفية التعامل مع بيانات العملاء بطرق شفافة وآمنة.

٢. التحديات التي واجهتها وكيفية التغلب عليها

أ. نقص الوعي الداخلي

التحدي: واجهت الشركة في البداية نقصاً في وعي الموظفين بأهمية حماية البيانات الشخصية ومتطلبات الامتثال.

الحل: نظمت حملات توعوية داخلية مكثفة ودورات تدريبية مخصصة لرفع الوعي.

ب. تكاليف التحديث التكنولوجي

التحدي: كانت تكلفة تطوير الأنظمة الأمنية والبنية التحتية التكنولوجية مرتفعة بالنسبة للشركة.

الحل: تعاونت الشركة مع مزودي خدمات تكنولوجيا المعلومات لتطوير حلول مخصصة تتوافق مع احتياجاتها وميزانياتها.

ج. التعامل مع البيانات القديمة

التحدي: كانت هناك بيانات قديمة تم جمعها قبل صدور قانون PDPL ولم يتم تنظيمها بشكل يتوافق مع المتطلبات الجديدة.

الحل: قامت الشركة بإطلاق مشروع لتنقية وتنظيم البيانات القديمة للتأكد من توافقها مع القانون.

د. التحديات القانونية والإدارية

التحدي: واجهت الشركة صعوبة في تفسير بعض بنود القانون وتطبيقها بشكل دقيق.

الحل: استعانت بمستشارين قانونيين مختصين للحصول على إرشادات واضحة حول كيفية الامتثال للقانون.

تأثير الممارسات على ثقة العملاء

١. زيادة ثقة العملاء بعد الالتزام بالقانون

أ. تعزيز الشفافية

قامت الشركة بإطلاق سياسة خصوصية شفافة وواضحة على موقعها الإلكتروني، مما عزز ثقة العملاء.

أصبح العملاء على دراية بكيفية استخدام بياناتهم والحقوق التي يتمتعون بها وفقًا للقانون.

ب. التواصل المفتوح مع العملاء

قدمت الشركة وسائل مخصصة للعملاء للتواصل معها بشأن أسئلتهم أو مخاوفهم حول البيانات، مثل مركز اتصال وخدمات دعم عبر الإنترنت.

ساهم هذا التواصل المفتوح في بناء علاقة قوية بين الشركة والعملاء.

٢. تحسين العلاقة بين الشركة والعملاء

أ. تقليل المخاوف من استخدام البيانات

بعد تطبيق الإجراءات الجديدة، شعر العملاء بالاطمئنان إلى أن بياناتهم في أيدي أمينة، مما زاد من إقبالهم على الخدمات التي تقدمها الشركة.

ب. زيادة الولاء والثقة

لاحظت الشركة زيادة في ولاء العملاء، حيث أبدوا استعدادًا أكبر للتعامل مع الشركة لفترات أطول بسبب شعورهم بالثقة.

أدى الالتزام بالقانون إلى تحسين سمعة الشركة في السوق، مما جذب عملاء جدد.

ج. إطلاق برامج جديدة استنادًا إلى رضا العملاء

استنادًا إلى ردود أفعال العملاء، تمكنت الشركة من تطوير خدمات وبرامج جديدة تتناسب مع احتياجاتهم، مما عزز نجاحها في السوق.

الجدول الزمني

المرحلة	المدة الزمنية	التفاصيل
جمع المعلومات وتحليلها	٤ أسابيع	البحث عن المصادر وجمع البيانات.
الكتابة	٣ أسابيع	كتابة المسودة الأولى وتحريرها.
المراجعة	٢ أسبوع	تدقيق البحث وتحسينه.
التقديم	١ أسبوع	إعداد العرض النهائي.

الخاتمة

يبرز قانون حماية البيانات الشخصية (PDPL) كأداة قانونية أساسية تعزز من حماية البيانات الشخصية في المملكة. من خلال هذا القانون، يتم ضمان الخصوصية وحماية المعلومات الشخصية للأفراد، مما يساهم في بناء ثقة أكبر بين الأفراد والشركات. يتمكن الأفراد من الاطمئنان إلى أن بياناتهم

الشخصية محمية بشكل قانوني، في حين تتمكن الشركات من معالجة البيانات بما يتماشى مع المعايير القانونية، ومن خلال التزام الشركات التام بقانون PDPL، يمكن تحقيق فوائد هامة على المدى الطويل. الالتزام بالقانون لا يعزز فقط سمعة الشركات في السوق بل يساهم أيضاً في تجنب الغرامات والعقوبات التي قد تترتب على المخالفات. كما أن ذلك يفتح المجال للحصول على ثقة أكبر من العملاء، مما يعزز الاستدامة والنمو المستقبلي.

التوصيات:

١. تعزيز برامج التوعية على نطاق أوسع: يجب أن تسعى المؤسسات الحكومية والشركات إلى نشر الوعي حول أهمية حماية البيانات الشخصية وكيفية الامتثال للقوانين ذات الصلة. يمكن القيام بذلك من خلال تنظيم ورش عمل، ندوات، وحملات توعية للمواطنين والشركات على حد سواء. ويجب أن تكون هذه البرامج موجهة لجميع المستويات، بدءاً من الأفراد وصولاً إلى كبار المسؤولين في الشركات.

٢. تطوير أدوات تقنية لدعم الامتثال: في ظل التحول الرقمي المستمر، تصبح التكنولوجيا جزءاً لا يتجزأ من عملية الامتثال. من الضروري تطوير أدوات وبرمجيات تساعد الشركات على إدارة وحماية بيانات العملاء بفعالية أكبر، مع ضمان الامتثال لقانون PDPL. يمكن لهذه الأدوات أن تشمل أنظمة أمان متطورة، أدوات تشفير، وبرمجيات لمراقبة البيانات ومعالجتها ضمن الأطر القانونية.

٣. دعم الشركات الصغيرة من خلال استشارات ودعم تقني: من المهم تقديم الدعم اللازم للشركات الصغيرة والمتوسطة في مجال الامتثال لقانون حماية البيانات الشخصية. يمكن توفير استشارات قانونية وتقنية لتوجيه هذه الشركات في كيفية معالجة بيانات العملاء وفقاً للمتطلبات القانونية.

المراجع

١. الشمري، ن. ع. (٢٠٢٣). حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة. مجلة العلوم الإنسانية والاجتماعية، ١١(١)، ٨٢-٩٤.
٢. العبيدان، د. س. ب. ع. (٢٠٢٤). التأصيل الفقهي لنظام حماية البيانات الشخصية السعودي. مجلة أبحاث، ١١(٢)، ٤٦٠-٥٤١.
٣. المزيني، ع. ب. أ. (٢٠٢٣). موافقة صاحب البيانات الشخصية لمعالجة بياناته في النظام السعودي (دراسة تحليلية مقارنة). مجلة كلية الشريعة والقانون بتفهما الأشراف-دقهلية، ٢٧(٣)، ٣٥٦٠-٣٥١٩.
٤. الشمراني، أ. ع. ه. (٢٠٢٤). موافقة صاحب البيانات الشخصية لمعالجة بياناته في النظام السعودي. مجلة قطاع الشريعة والقانون، ١٦(١٦)، ١٣٤٠-١٣٠٣.
٥. 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.
٦. Bygrave, L. A. (1998). Right to privacy in human rights treaties. International Journal of Law and Information Technology, 6(3), 247-284.
٧. 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.
٨. Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. Florida Law Review, 71, 365.
٩. Schwartz, P. M. (2019). Global data privacy: The EU way. NYU Law Review, 94, 771.

Kiesow Cortez, E. (2020). Data protection around the world: Privacy .) .
.laws in action. Springer Nature