



جامعة ميدأوشن

كلية الدراسات الإنسانية

قسم / ماجستير القانون الرقمي

دور القانون الرقمي في حماية البيانات الشخصية

اسم الطالبة /

وصال عبد الملك المحوي

241001065

المشرف الثاني /

المشرف الرئيسي /

العام الدراسي 2025/2024

المخلص (Abstract) :

تهدف هذه الدراسة إلى تحليل دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية، مع التركيز على القوانين والتشريعات التي تهدف إلى تعزيز الأمان الرقمي والامتثال للتشريعات القانونية. ومع التحولات التقنية المتسارعة والتحول الرقمي ضمن إطار رؤية 2030، تواجه المؤسسات الحكومية والخاصة تحديات كبيرة لحماية بيانات المستخدمين من التهديدات الرقمية كالهجمات الإلكترونية وتسريبات البيانات.

اعتمدت الدراسة منهجية شاملة، تجمع بين التحليل الكمي والنوعي، حيث تم جمع البيانات من عينة تمثيلية لمؤسسات حكومية وخاصة. واستخدمت أدوات جمع البيانات مثل الاستبيانات والمقابلات الشخصية، إلى جانب تحليل الوثائق القانونية ذات الصلة كقانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية.

أظهرت نتائج الدراسة وجود تحديات في تطبيق القوانين الرقمية بالمؤسسات السعودية، خاصة في مجالات الوعي باللوائح الرقمية وضرورة توفير التدريب المناسب للموظفين. وأشارت النتائج إلى أن المؤسسات التي تعتمد استراتيجيات تدريب فعالة تحقق مستويات أعلى من الامتثال للقوانين وتحقيق الأمان الرقمي. بناءً على ذلك، قدمت الدراسة توصيات لتحسين الأطر القانونية وزيادة الوعي المؤسسي بالتشريعات الرقمية.

الكلمات المفتاحية: حماية البيانات الشخصية، القانون الرقمي، الامتثال التنظيمي، الجرائم المعلوماتية، الأمان الرقمي، المملكة العربية السعودية.

كلمة شكر وتقدير

أتقدم بأسمى عبارات الشكر والتقدير لأعضاء لجنة التحكيم الموقرة، الذين لم يدخروا جهداً في تقديم ملاحظاتهم وتوجيهاتهم القيمة والتي كان لها الأثر الكبير في رفع مستوى هذا البحث وتحقيق أهدافه. إن توجيهاتهم ودعمهم العلمي المستمر كانا منارات مضيئة في مسيرتي البحثية، وأدين لهم بفضل كبير في إتمام هذا العمل على الوجه الأمثل.

كما أوجه خالص الشكر والتقدير لكل من ساندني وساهم معي خلال مراحل البحث، سواء من خلال تقديم المعلومات أو الدعم الأكاديمي، ولا يفوتني أن أشكر زملائي الذين كانوا شركاء في مسيرتي العلمية، فقد كانوا عوناً وسنداً لا ينسى في رحلتي.

ولا يسعني إلا أن أعبر عن امتناني العميق لعائلتي العزيزة، الذين كانوا دائماً مصدر إلهامي وسبباً في استمراري وتقديمي. فقد منحوني من الدعم والتشجيع ما مكّني من اجتياز كافة الصعاب والوصول إلى هذا الإنجاز الأكاديمي.

شكري وامتناني لكم جميعاً، فبفضلكم تحقق هذا النجاح.

II	المخلص (Abstract) :	11
III	كلمة شكر وتقدير	11
2	المقدمة (introduction) :	2
3	مشكلة الدراسة (study Problem) :	3
4	أهمية الدراسة (Study Significance) :	4
5	أهداف الدراسة (Study Aims) :	5
7	تساؤلات الدراسة (Study questions) :	7
7	فروض الدراسة (Study Hypotheses) :	7
8	النظرية العلمية المتبعة لإعداد البحث (The scientific theory followed in preparing the research) :	8
9	خطوات تنفيذ النظرية في البحث (Steps for implementing the theory in research) :	9
15	الفصل الثاني	15
15	الدراسات السابقة (Literature review)	15
16	مقدمة (introduction) :	16
17	المتغير التابع (Dependent Variable) :	17
17	تعريف المتغير التابع	17
17	تفسير المتغير التابع	17
18	أهمية تفسير المتغير التابع	18
18	وصف مفصل للمتغير التابع	18
18	العناصر الأساسية لوصف المتغير التابع :	18
19	المقاييس المستخدمة لقياس المتغير التابع في بحث "دور القانون الرقمي في حماية البيانات الشخصية"	19
24	المتغير المستقل (Independent Variable) :	24
24	المتغير المستقل	24
25	التفسير	25
25	تفسير المتغير المستقل في سياق البحث :	25

25	تحديد التأثير المحتمل للتشريعات الرقمية:
25	التحكم والتلاعب بالمتغير المستقل:
26	دور الباحث في التحكم بالمتغير المستقل:
26	كيف يؤثر المتغير المستقل على المتغير التابع؟
27	الدراسات السابقة (Previous studies):
	ما ستقدمه الدراسة الحالية مقارنة بالدراسات السابقة (The contribution of the current study compared to previous studies):
33	الدراسة الحالية ستركز على عدة نقاط مقارنة بالدراسات السابقة:
34	الإطار النظري للدراسة (Theoretical Framework of the Study):
37	مكونات الإطار النظري للدراسة (Components of the theoretical framework of the study):
40	دعم الفرضيات وأسئلة البحث (Support for Hypotheses and Research Questions):
42	التكامل مع البحوث السابقة والبناءات النظرية:
45	الفصل الثالث:
45	منهجية الدراسة (Study methodology):
46	مقدمة (introduction):
46	تصميم البحث (Research Design):
47	الخطوات العملية لتنفيذ البحث:
50	مجتمع البحث (Population of the Study):
51	طريقة اختيار العينة (Sampling Method):
53	محددات حجم العينة (Sample Size Determination):
55	خطوات جمع البيانات وأدوات جمع البيانات (Data Collection Procedures and Tools):
59	حدود الدراسة (Study Determinants):
64	مقدمة (Introduction):
65	تحليل البيانات (Data Analysis):
67	بيانات العينة السابقة (Sample Data):
68	مناقشة النتائج (Discussion of the Results):
70	نتائج البحث (Research Findings):

72	المراجع:
73	الملاحق:
79	Abstract:

الفصل الأول

1.1. المقدمة (introduction):

يعد القانون الرقمي أداةً محورية في تنظيم وحماية البيانات الشخصية ضمن إطار الحكومات الإلكترونية. مع تزايد الاعتماد على الأنظمة الرقمية لتقديم الخدمات الحكومية، أصبحت حماية الخصوصية وضمان أمن المعلومات الشخصية للمواطنين ضرورة ملحة. القوانين الرقمية تهدف إلى تنظيم كيفية جمع واستخدام وتخزين البيانات الشخصية من قبل المؤسسات الحكومية، وتحديد آليات واضحة لضمان حقوق الأفراد في الوصول إلى بياناتهم وتصحيحها أو حذفها. تختلف هذه القوانين من دولة إلى أخرى بناءً على التشريعات المحلية والثقافات القانونية. على سبيل المثال، أظهرت دراسة مقارنة بين الولايات المتحدة وألمانيا والصين اختلافات جوهرية في سياسات حماية البيانات الحكومية الرقمية. (Wu, 2014)

بالإضافة إلى ذلك، تواجه بعض الدول تحديات متزايدة نتيجة التسريبات المتكررة للبيانات الشخصية، مما يبرز الحاجة إلى تحسين القوانين لتتناسب مع التطورات التكنولوجية. في روسيا، أدى ضعف الحماية القانونية إلى تقويض ثقة المواطنين في الحكومة الرقمية. (Ruskevich, 2023) علاوة على ذلك، يتطلب التطور المستمر في التكنولوجيا تحسينات قانونية لمواكبة التحديات الجديدة في مجال حماية البيانات الشخصية. (Soldatova, 2020)

تسعى هذه الدراسة إلى استعراض دور القانون الرقمي في حماية البيانات الشخصية ضمن الحكومات الإلكترونية، مع التركيز على السياسات الدولية والتحديات التي تواجه تنفيذ هذه القوانين في ظل التطورات التكنولوجية المتسارعة.

1.2. مشكلة الدراسة (study Problem):

تواجه الحكومات والمؤسسات الحكومية في السعودية تحديات كبيرة في حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية، ويُعد القانون الرقمي أحد العوامل الأساسية التي تؤثر على فعالية وكفاءة هذه الحماية. عندما يتم تطبيق تشريعات رقمية غير كافية أو غير مُحدثة لمواكبة التطورات التكنولوجية السريعة، تتعرض البيانات الشخصية لمخاطر تسريب المعلومات والوصول غير المصرح به. كما أن اعتماد الحكومات الإلكترونية على تقنيات جمع وتخزين البيانات الحساسة، دون وجود إطار قانوني صارم لحمايتها، يؤدي إلى تزايد مخاوف المواطنين بشأن خصوصيتهم.

تكمن مشكلة هذه الدراسة في استكشاف التحديات التي تواجهها المملكة العربية السعودية في حماية البيانات الشخصية ضمن الحكومات الإلكترونية. تشمل هذه التحديات الثغرات في التشريعات الرقمية وعدم كفاية آليات الرقابة والتنفيذ، مما يمكن أن يؤدي إلى تزايد حالات انتهاك الخصوصية وتسريب البيانات. (Elgujja et al., 2021)

تهدف الدراسة إلى تحديد العوامل التي تسهم في ظهور هذه الثغرات القانونية، وكيفية تأثيرها على ثقة المواطنين في الخدمات الحكومية الإلكترونية، وكذلك اقتراح حلول لتعزيز فعالية القانون الرقمي في حماية البيانات الشخصية.

1.3. أهمية الدراسة (Study Significance) :

تحظى هذه الدراسة بأهمية كبيرة على مستويات متعددة نظرًا لدورها في تسليط الضوء على القانون الرقمي وأثره في حماية البيانات الشخصية ضمن الحكومات الإلكترونية. يمكن توضيح أهمية الدراسة من خلال النقاط التالية:

1. تعزيز الثقة في الخدمات الرقمية: تتناول الدراسة التحديات المتعلقة بحماية البيانات الشخصية في سياق التحول الرقمي الحكومي. ومن خلال اقتراح حلول لتطوير التشريعات والسياسات الرقمية، يمكن أن تساهم في زيادة ثقة المواطنين في استخدام الخدمات الحكومية الإلكترونية، مما يعزز الإقبال عليها.

2. تحسين الإطار القانوني لحماية البيانات: تركز الدراسة على الثغرات الموجودة في التشريعات الحالية المتعلقة بحماية البيانات الشخصية، وتطرح توصيات لتطوير تلك القوانين بما يتماشى مع التطورات التقنية المتسارعة. هذه التوصيات تهدف إلى تعزيز قدرة الحكومة على حماية البيانات الشخصية بشكل فعال وتقليل مخاطر الانتهاكات.

3. مواكبة التطورات التقنية: تسعى الدراسة إلى تقديم حلول قانونية حديثة تتماشى مع التقدم التكنولوجي المستمر، مثل حماية البيانات البيومترية والتقنيات السحابية. هذا يساهم في تعزيز كفاءة التشريعات الرقمية في مواجهة التحديات الناتجة عن الابتكار التكنولوجي.

4. تقليل مخاطر تسريب البيانات: توضح الدراسة العلاقة بين الثغرات القانونية والمخاطر المتعلقة بتسريب البيانات الشخصية. من خلال اقتراح حلول لتعزيز الحماية الرقمية، يمكن للمؤسسات الحكومية تحسين تدابير الأمن وتقليل احتمالات وقوع انتهاكات للبيانات.

5. دعم السياسات الحكومية ببيانات علمية: توفر الدراسة إطاراً علمياً يمكن لصناع القرار والمسؤولين الحكوميين الاعتماد عليه لتقييم فعالية التشريعات الحالية وتحسينها. هذا الإطار يسهم في تعزيز السياسات التي تهدف إلى حماية البيانات الشخصية وضمان الأمن الرقمي.

6. إثراء الأدبيات الأكاديمية والممارسات القانونية: تسهم الدراسة في تطوير المعرفة الأكاديمية من خلال تحليل القضايا المتعلقة بحماية البيانات الشخصية في المملكة، وتقديم مقترحات عملية قابلة للتطبيق تساعد الحكومات والمؤسسات على تحسين أدائها في هذا المجال.

باختصار، تقدم هذه الدراسة فهماً عميقاً حول أهمية القانون الرقمي في حماية البيانات الشخصية بالمملكة العربية السعودية، وتوفر توصيات عملية تهدف إلى تعزيز الثقة في الخدمات الحكومية الإلكترونية وضمان حماية الخصوصية.

1.4. أهداف الدراسة (Study Aims):

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف التي ترتبط بشكل وثيق بالتحديات التي تواجه حماية البيانات الشخصية في الحكومات الإلكترونية تتضمن الأهداف ما يلي:

1. تحليل التشريعات القائمة بشأن حماية البيانات الشخصية: تسعى الدراسة إلى تحليل القوانين الحالية المرتبطة بحماية البيانات الشخصية في المملكة العربية السعودية ضمن بيئة الحكومات الإلكترونية، وتحديد الثغرات التي تحتاج إلى معالجة لضمان حماية فعالة.

2. تطوير حلول قانونية مبتكرة: تهدف الدراسة إلى تقديم حلول قانونية مبتكرة تستجيب للتحديات التقنية الجديدة، مثل البيانات البيومترية والحوسبة السحابية، لضمان التوافق بين التقدم التكنولوجي وحماية الخصوصية.

3. تعزيز السياسات الرقمية الحكومية: تهدف الدراسة إلى تقديم توصيات لدعم صناع القرار في تطوير سياسات رقمية قوية تحمي البيانات الشخصية وتزيد من فعالية الأمن الرقمي في المملكة.

4. تعزيز الوعي المؤسسي بأهمية حماية البيانات: تسعى الدراسة إلى تعزيز الوعي داخل المؤسسات الحكومية حول أهمية حماية البيانات الشخصية، من خلال تطوير استراتيجيات تعليمية وتدريبية تدعم الالتزام بالقوانين وتطبيقها بشكل فعال.

5. تعزيز ثقة المواطنين في الحكومات الإلكترونية: تهدف الدراسة إلى دراسة تأثير حماية البيانات الشخصية على ثقة المواطنين في الخدمات الحكومية الرقمية، وتقديم مقترحات لتحسين تلك الثقة من خلال ضمان أمان بياناتهم وخصوصيتهم.

6. إسهام في بناء إطار قانوني مستدام: تسعى الدراسة إلى توفير إطار قانوني شامل ومستدام يعزز من كفاءة القوانين الرقمية الحالية، ويضع أسسًا قوية لحماية البيانات الشخصية في المستقبل مع مواكبة التقدم التكنولوجي .

من خلال تحقيق هذه الأهداف، تأمل الدراسة في بناء منظومة قانونية رقمية متكاملة تساهم في حماية البيانات الشخصية بشكل يواكب تطورات التكنولوجيا الرقمية ويعزز ثقة المواطنين في الحكومة الإلكترونية.

1.5. تساؤلات الدراسة (Study questions):

السؤال الرئيسي :

كيف يساهم القانون الرقمي في حماية البيانات الشخصية في إطار الحكومات الإلكترونية في المملكة العربية السعودية؟

الأسئلة الفرعية:

1. إلى أي مدى تساهم القوانين الرقمية الحالية في المملكة في تأمين وحماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية؟
2. ما هي نقاط الضعف في التشريعات الحالية التي قد تعرض البيانات الشخصية لمخاطر التسريب أو الانتهاك في المنصات الحكومية الإلكترونية؟
3. كيف يؤثر التقدم التقني، مثل البيانات البيومترية والتخزين السحابي، على آليات حماية البيانات الشخصية في البيئة الحكومية الرقمية؟
4. كيف تؤثر سياسات حماية البيانات الشخصية على ثقة المواطنين في التعامل مع الخدمات الحكومية الرقمية؟
5. ما هي الإجراءات والسياسات الممكنة لتحسين حماية البيانات الشخصية وتقليل احتمالات حدوث خروقات أمنية؟
6. كيف يمكن بناء إطار قانوني شامل يساهم في تحسين فعالية حماية البيانات الشخصية في سياق التحول الرقمي الحكومي في المملكة العربية السعودية؟

1.6. فروض الدراسة (Study Hypotheses):

استناداً إلى مشكلة الدراسة التي تتناول التحديات التي تواجه حماية البيانات الشخصية في بيئات الحكومات الإلكترونية في المملكة العربية السعودية، وإلى الأهداف التي تسعى لتحليل التشريعات الرقمية وتقديم حلول لتحسينها، يمكن صياغة الفرضيات التالية:

فروض الدراسة:

1. توجد علاقة ذات دلالة إحصائية بين التشريعات الرقمية الحالية ومستوى حماية البيانات الشخصية في بيئات الحكومات الإلكترونية في المملكة العربية السعودية.
 2. تسهم الثغرات في التشريعات الرقمية الحالية في زيادة مخاطر تسريب البيانات الشخصية أو انتهاكها ضمن المنصات الحكومية الإلكترونية.
 3. يؤثر التقدم التكنولوجي، مثل الحوسبة السحابية والبيانات البيومترية، على فعالية التشريعات الرقمية في حماية البيانات الشخصية.
 4. زيادة الوعي المؤسسي حول أهمية حماية البيانات الشخصية يؤدي إلى تحسين مستوى الحماية وتقليل مخاطر التسريب.
 5. تعزيز حماية البيانات الشخصية يؤدي إلى زيادة ثقة المواطنين في التعامل مع الخدمات الحكومية الإلكترونية.
 6. تطوير إطار قانوني شامل ومحدث لحماية البيانات الشخصية سيسهم في تحسين مستوى الأمان الرقمي ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية.
- تهدف هذه الفروض إلى اختبار مدى فعالية التشريعات الحالية ودورها في تعزيز الأمان الرقمي والثقة العامة، وكذلك استكشاف تأثير التقدم التكنولوجي على حماية البيانات الشخصية.

1.7. النظرية العلمية المتبعة لإعداد البحث (The scientific theory followed in preparing the research)

يعتمد هذا البحث على نظرية حماية المعلومات (Information Protection Theory) كأساس علمي لتحليل تأثير التشريعات الرقمية على حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية. تُعتبر هذه النظرية من أبرز النظريات في مجال الأمن الرقمي وحماية المعلومات، حيث تركز على كيفية حماية البيانات من التهديدات الرقمية وضمان سرية وسلامة المعلومات.

وفقاً لهذه النظرية، يجب أن تكون حماية البيانات الشخصية مدمجة في السياسات الرقمية والقوانين لضمان أمان المعلومات ومنع تسريبها أو انتهاكها. تستند النظرية إلى مبادئ الأمان الرقمي مثل التشفير، إدارة الوصول، والحوكمة الرقمية لضمان حماية شاملة للبيانات. تشير النظرية إلى أن التشريعات الفعالة تلعب دوراً حاسماً في تقليل المخاطر الرقمية وتعزيز الثقة في بيئات الحكومات الإلكترونية.

في سياق هذا البحث، تُستخدم النظرية لتفسير كيف يمكن أن يؤدي غياب القوانين الكافية أو وجود ثغرات تشريعية إلى زيادة مخاطر تسريب البيانات أو اختراق الخصوصية في المنصات الحكومية. كما يتم تحليل كيف يمكن لتحسين التشريعات الرقمية أن يساهم في تقليل هذه المخاطر وتعزيز ثقة المواطنين في التعامل مع الخدمات الحكومية الإلكترونية.

بالإضافة إلى ذلك، يتم دعم الدراسة باستخدام نظرية الحوكمة الرقمية (Digital Governance Theory) لفهم كيفية تفاعل التكنولوجيا مع التشريعات الرقمية لضمان حماية البيانات الشخصية. من خلال الجمع بين هاتين النظريتين، يوفر البحث إطاراً شاملاً لتحليل مدى فعالية التشريعات الرقمية وتقييم تأثيرها على حماية البيانات الشخصية في الحكومات الإلكترونية.

1.7.1. خطوات تنفيذ النظرية في البحث (Steps for implementing the theory in research):

لتنفيذ نظرية حماية المعلومات ونظرية الحوكمة الرقمية في البحث المتعلق بحماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية، يجب اتباع خطوات منهجية لتنظيم البحث وتحقيق الأهداف المرجوة. فيما يلي خطوات تنفيذ النظريات في البحث:

1. تحديد الإطار النظري

- وصف النظريات: ابدأ بتوضيح المفاهيم الأساسية لكل من نظرية حماية المعلومات ونظرية الحوكمة الرقمية، وشرح كيفية ارتباط هذه النظريات بحماية البيانات الشخصية في الحكومات الإلكترونية.
- رسم العلاقات بين النظريات والبحث: بيّن كيف تتكامل هاتان النظريتان لتقديم رؤية شاملة حول حماية البيانات الشخصية في ظل التحول الرقمي الحكومي.

2. تحليل الوضع الحالي للتشريعات

- تقييم التشريعات الرقمية الحالية: باستخدام نظرية حماية المعلومات، حلل التشريعات القائمة في المملكة العربية السعودية فيما يتعلق بحماية البيانات الشخصية. حدد نقاط القوة والضعف في القوانين المعمول بها.
- تطبيق نظرية الحوكمة الرقمية: قم بتحليل كيفية تطبيق الحكومة للتشريعات الرقمية على أرض الواقع، وكيف تؤثر هذه التشريعات على الأمان الرقمي والثقة العامة.

3. تحديد الثغرات والمخاطر

- تحليل الثغرات القانونية: استخدم إطار نظرية حماية المعلومات لتحديد أي ثغرات قانونية قد تؤدي إلى مخاطر تسريب البيانات أو انتهاك الخصوصية.
- دراسة المخاطر التكنولوجية: استخدم نظرية الحوكمة الرقمية لدراسة المخاطر التي قد تنتج عن التقدم التكنولوجي مثل البيانات البيومترية والحوسبة السحابية وكيفية تأثيرها على حماية البيانات الشخصية.

4. جمع البيانات

- تصميم استبيانات أو مقابلات: استنادًا إلى النظريتين، صمم أدوات البحث لجمع البيانات من المسؤولين الحكوميين، الخبراء القانونيين، أو المواطنين. الهدف هو فهم مدى تأثير التشريعات الحالية على حماية البيانات الشخصية ومدى تأثيرها على ثقة المواطنين في الحكومة الإلكترونية.
- تحليل البيانات: قم بتحليل البيانات التي تم جمعها لمعرفة مدى توافقها مع الفرضيات المستمدة من نظريات حماية المعلومات والحوكمة الرقمية.

5. تقديم الحلول والتوصيات

- اقتراح تحسينات على التشريعات: باستخدام نتائج البحث وتحليل الفجوات بناءً على نظرية حماية المعلومات، قدم توصيات لتطوير التشريعات الرقمية.
- تطوير إطار قانوني جديد: استنادًا إلى نظرية الحوكمة الرقمية، اقترح إطارًا قانونيًا رقميًا شاملاً يمكن تطبيقه لحماية البيانات الشخصية بشكل أفضل.

6. اختبار الفرضيات

- تحليل العلاقة بين المتغيرات: اختبر الفرضيات التي تم تطويرها في بداية البحث. على سبيل المثال، مدى تأثير التشريعات الرقمية على ثقة المواطنين، ومدى ملاءمة هذه التشريعات لحماية البيانات الشخصية في ظل التقدم التكنولوجي.
- مقارنة النتائج مع الإطار النظري: قارن النتائج التي توصلت إليها مع التوقعات المستمدة من النظريات المستخدمة للتحقق من صحتها.

7. خاتمة وتقييم البحث

- تقييم النتائج: اعرض النتائج النهائية للبحث وقم بتقييم مدى نجاح تطبيق النظريتين في فهم وتحليل المشكلة البحثية.
- تقديم توصيات للمستقبل: استنادًا إلى التحليل، قدم توصيات مستقبلية لتحسين الأطر القانونية والسياسات المتعلقة بحماية البيانات الشخصية في الحكومات الإلكترونية.

8. نشر النتائج وتطبيقها

- نشر النتائج: انشر نتائج البحث في مجلات علمية أو ضمن المؤتمرات ذات الصلة بالقانون الرقمي وحماية البيانات.
- تطبيق الحلول: قم بالتعاون مع الجهات الحكومية لتطبيق التوصيات على أرض الواقع وتطوير التشريعات الرقمية بما يتماشى مع الحلول المقترحة.

هذه الخطوات تساعد في تنفيذ النظريات العلمية بفعالية لضمان تحليل شامل ودقيق لموضوع حماية البيانات الشخصية في البيئات الحكومية الرقمية، مما يعزز الأمان والثقة في النظام الرقمي.

تطبيق الإطار النظري:

لتطبيق الإطار النظري المستند إلى نظرية حماية المعلومات ونظرية الحوكمة الرقمية في دراسة دور القانون الرقمي في حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية، سيتم اتباع الخطوات التالية لضمان إجراء تحليل شامل وموثوق:

1. تحليل التشريعات الرقمية الحالية المتعلقة بحماية البيانات الشخصية:
 - سيتم البدء بجمع المعلومات حول التشريعات والسياسات الحالية في المملكة التي تنظم حماية البيانات الشخصية ضمن الأنظمة الرقمية الحكومية.
 - سيتم التركيز على تحليل فعالية هذه التشريعات في مواجهة التحديات الرقمية، بما في ذلك حماية البيانات من المخاطر المتزايدة مثل الاختراقات والتسريبات في البيئات الإلكترونية.
2. تطبيق عناصر نظرية حماية المعلومات:
 - استناداً إلى البيانات المتاحة، سيتم استخدام عناصر نظرية حماية المعلومات (مثل تقنيات التشفير، إدارة الوصول، والتحكم في المخاطر) لتقييم مدى قوة وفعالية القوانين المعمول بها في حماية البيانات الشخصية.
 - سيتم مقارنة التدابير المتخذة حالياً بالمعايير العالمية المثلى لضمان حماية البيانات وتحليل الفجوات في تطبيق التشريعات الحالية، وكيف يمكن لهذه الفجوات أن تؤثر على أمن المعلومات الشخصية في البيئات الحكومية.
3. تقييم الحوكمة الرقمية في المملكة باستخدام النظرية:
 - سيتم تحليل كيفية تطبيق السياسات الرقمية الحكومية وفقاً لنظرية الحوكمة الرقمية، مع التركيز على قدرة الحكومة على إدارة وحماية البيانات الشخصية بشكل فعال عند تقديم الخدمات الإلكترونية.
 - سيتم أيضاً تقييم مدى تأثير هذه السياسات على ثقة المواطنين في الحكومة الإلكترونية، وفحص كيفية ارتباط حماية البيانات الشخصية بالحوكمة الجيدة والشفافية.

4. دراسة تأثير التكنولوجيا على حماية البيانات الشخصية:
- سيتم تحليل التحديات التكنولوجية المتزايدة، مثل البيانات البيومترية والحوسبة السحابية، وفحص تأثيرها على حماية البيانات الشخصية في البيئات الحكومية الإلكترونية.
 - باستخدام النماذج الإحصائية مثل تحليل الانحدار، سيتم دراسة العلاقة بين التطور التكنولوجي ومدى فعالية التشريعات الرقمية في التعامل مع هذه التحديات الجديدة.
5. تطوير إطار قانوني متكامل لتعزيز حماية البيانات:
- بناءً على نتائج التحليل، سيتم تطوير إطار قانوني مستند إلى مبادئ الحوكمة الرقمية، يهدف إلى تحديث التشريعات الرقمية بما يتماشى مع التقدم التكنولوجي وزيادة الحماية القانونية للبيانات الشخصية.
 - هذا الإطار سيشمل مقترحات لتحسين القوانين والسياسات، مثل تعزيز معايير الأمان الرقمي والتشفير، وتحديث التشريعات بما يتوافق مع أفضل الممارسات الدولية.
6. اختبار فعالية التوصيات المستندة إلى الإطار النظري:
- سيتم اختبار التوصيات من خلال متابعة أثرها على تحسين حماية البيانات الشخصية في بيئات حكومية رقمية مختارة، من خلال تنفيذ تلك التوصيات على أرض الواقع.
 - سيتم تحليل البيانات المتعلقة بمستويات الأمان وثقة المواطنين قبل وبعد تنفيذ هذه التدابير، باستخدام أدوات تحليلية لقياس الفروقات والتغيرات التي حدثت نتيجة تنفيذ التوصيات.
7. المراجعة المستمرة والتحسين:
- سيتم مراجعة الإطار النظري بشكل دوري استنادًا إلى نتائج تطبيقه على أرض الواقع، لضمان توافقه مع التطورات الجديدة في التكنولوجيا والتحديات المستقبلية.
 - ستتم متابعة التطورات في السياسات والقوانين الرقمية لضمان استمرار ملاءمتها مع المتغيرات التقنية، بالإضافة إلى تقديم الدعم المستمر لصناع القرار لتحديث وتطوير السياسات المتعلقة بحماية البيانات الشخصية.

بهذه الطريقة، يتم تطبيق الإطار النظري لنظريتي حماية المعلومات والحوكمة الرقمية بشكل متكامل، مما يتيح فحصاً شاملاً للتشريعات الرقمية المتعلقة بحماية البيانات الشخصية في المملكة العربية السعودية. يساعد هذا التحليل في تقديم توصيات عملية وقانونية لتعزيز حماية البيانات الشخصية في ظل التحديات التقنية، مما يؤدي إلى زيادة الثقة في الخدمات الحكومية الرقمية وتحسين مستوى الأمان الرقمي بشكل عام.

الفصل الثاني

الدراسات السابقة (Literature review)

2.1. مقدمة (introduction) :

تعد الدراسات السابقة أحد الأركان الأساسية في إعداد الأبحاث العلمية، حيث توفر خلفية معرفية شاملة حول الموضوع المطروح وتساهم في بناء إطار نظري قائم على أسس علمية صلبة. في سياق البحث الحالي، تركز الدراسات السابقة على استكشاف دور القانون الرقمي في حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية، وخاصة في ظل التحول الرقمي المتسارع وتزايد التحديات المرتبطة بالأمان الرقمي وخصوصية البيانات وتهدف هذه المقدمة إلى تسليط الضوء على أهم الاتجاهات البحثية السابقة في هذا المجال، من خلال استعراض الدراسات التي تناولت فعالية التشريعات الرقمية وأثرها على حماية البيانات الشخصية في بيئات الحكومات الإلكترونية. كما سنتناول الأبحاث التي ركزت على تحليل التحديات التي تواجه حماية البيانات في ظل التطورات التكنولوجية الحديثة مثل الحوسبة السحابية والبيانات البيومترية علاوة على ذلك، سنتناول الدراسات السابقة الطرق والاستراتيجيات التي تم استخدامها لتعزيز حماية البيانات وتقليل مخاطر تسريبها، مع تقديم رؤى قيمة يمكن من خلالها تطوير استراتيجيات جديدة قائمة على الأطر النظرية والعملية التي استندت إليها تلك الأبحاث. من خلال تحليل هذه الدراسات، يسعى البحث الحالي إلى سد الفجوات المعرفية المتعلقة بحماية البيانات الشخصية، وتقديم إطار علمي جديد يساهم في تحسين التشريعات والسياسات الرقمية في المملكة.

2.2. المتغير التابع (Dependent Variable) :

2.1.1. تعريف المتغير التابع

المتغير التابع هو المتغير الذي يتأثر بالتغيرات في المتغير المستقل، ويكون محط القياس في الدراسة أو البحث العلمي. بمعنى آخر، هو النتيجة أو التأثير الذي ينتج عن تعديل أو تغيير في المتغير المستقل. يتم قياسه لتحديد ما إذا كان هناك تأثير جوهري نتيجة لهذه التغيرات.

في سياق البحث الحالي حول "دور القانون الرقمي في حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية في المملكة العربية السعودية"، يمثل مستوى حماية البيانات الشخصية المتغير التابع. يتمثل هذا المتغير في قياس مدى فعالية التشريعات الرقمية والسياسات الحكومية في حماية البيانات الشخصية من التسريبات أو الاختراقات في البيئات الحكومية الرقمية، وذلك اعتمادًا على مدى تنفيذ هذه السياسات والتشريعات.

2.1.2. تفسير المتغير التابع

المتغير التابع يمثل العنصر أو الظاهرة التي يرغب الباحث في قياسها للتعرف على مدى تأثيرها بالعوامل المختلفة (المتغيرات المستقلة). يتمثل دوره في الدراسة بوصفه النتيجة أو الأثر الناتج عن تغييرات المتغيرات الأخرى. يُستخدم هذا المتغير لتحديد ما إذا كانت هناك علاقة أو تأثير ناجم عن تطبيق أو تعديل التشريعات الرقمية.

في البحث الحالي، يُعتبر مستوى حماية البيانات الشخصية هو المتغير التابع، ويتم قياسه لمعرفة مدى تأثير التشريعات الرقمية والسياسات الحكومية (المتغير المستقل) على حماية البيانات الشخصية. تُستخدم البيانات المستخلصة من تقارير الحكومات الإلكترونية لتقييم مدى فعالية السياسات القائمة ومدى حماية البيانات الشخصية في المملكة.

2.1.3. أهمية تفسير المتغير التابع

تفسير المتغير التابع في البحث العلمي يساعد الباحثين على فهم العلاقات السببية بين المتغيرات المختلفة، وتحديد تأثير المتغيرات المستقلة عليه بوضوح. من خلال تفسير هذا المتغير، يمكن للباحثين قياس النتائج وتقييم الفرضيات المطروحة، مما يساهم في الوصول إلى استنتاجات علمية دقيقة ومدعومة بالأدلة.

وفقاً لدراسة أجرتها (Alharbi et al. (2021)، فإن فعالية التدابير الأمنية والسياسات الرقمية في الحكومات الإلكترونية تعتبر عاملاً أساسياً في حماية البيانات الشخصية، حيث تشير إلى أن تحسين مستوى حماية البيانات يحد من مخاطر الاختراقات ويعزز الثقة في استخدام هذه الخدمات (Alharbi et al., 2021).

2.1.4. وصف مفصل للمتغير التابع

في البحث الحالي حول "دور القانون الرقمي في حماية البيانات الشخصية ضمن بيئات الحكومات الإلكترونية"، يُعتبر مستوى حماية البيانات الشخصية المتغير التابع الرئيسي. يعكس هذا المتغير مدى الحماية الفعالة للبيانات الشخصية الناتجة عن تطبيق التشريعات والسياسات الرقمية في المملكة.

2.1.5. العناصر الأساسية لوصف المتغير التابع:

1. التعريف: يُعرف المتغير التابع هنا بأنه مستوى حماية البيانات الشخصية، ويعبر عن فعالية التشريعات الرقمية في الحفاظ على سرية البيانات وحمايتها من التسريب أو الاختراق.
2. طرق القياس: يتم قياس المتغير من خلال عدد الحوادث المتعلقة باختراق البيانات أو تسريبها، ومدى نجاح التشريعات والسياسات الرقمية في تقليل هذه الحوادث.
3. العلاقة مع المتغيرات المستقلة: يعتمد مستوى حماية البيانات الشخصية على مدى قوة التشريعات الرقمية (المتغير المستقل) المطبقة في المملكة.

4. أهمية المتغير التابع في البحث: يمثل المتغير التابع مؤشرًا حاسمًا لنجاح السياسات والتشريعات في حماية البيانات الشخصية في البيئات الحكومية الرقمية، كما أشارت Alkhaldi et al. (2022) في دراستهم حول أهمية حماية البيانات في البيئة الرقمية (Alkhaldi et al., 2022).

من خلال هذا الوصف التفصيلي، يتضح أن المتغير التابع (مستوى حماية البيانات الشخصية) يلعب دورًا مركزيًا في البحث. حيث يُستخدم كمقياس رئيسي لتحديد تأثير التشريعات والسياسات الرقمية وفهم العلاقة بين فعالية هذه السياسات ومستوى حماية البيانات الشخصية في بيئات الحكومات الإلكترونية. يتم قياس هذا المتغير لتحديد مدى نجاح هذه التشريعات في حماية البيانات الشخصية ومنع الاختراقات والتسريبات، بما يساهم في تعزيز الثقة لدى المواطنين في استخدام الخدمات الحكومية الرقمية.

2.1.6. المقاييس المستخدمة لقياس المتغير التابع في بحث "دور القانون الرقمي في حماية البيانات الشخصية"

لقياس المتغير التابع، وهو مستوى حماية البيانات الشخصية في بيئات الحكومات الإلكترونية، سيتم استخدام عدة مقاييس، ولكل منها معادلة تساعد في تقديم تقييم دقيق لمستوى الحماية المقدم. فيما يلي المقاييس ومعادلاتها:

1. عدد حالات اختراق البيانات (Data Breach Incidents Count)

○ كيفية القياس: يتم جمع عدد الحوادث التي تعرضت فيها البيانات الشخصية للاختراق أو التسريب في بيئات الحكومة الإلكترونية.

○ معادلة المقياس:

○ عدد حالات اختراق البيانات = $\sum$ (الحوادث المسجلة لكل مؤسسة حكومية)

○ الهدف: قياس مدى فعالية التشريعات الرقمية في الحد من حالات الاختراقات الأمنية.

2. معدل الامتثال للتشريعات الرقمية (Compliance Rate with Digital Legislation)

○ كيفية القياس: يتم قياس مدى امتثال المؤسسات الحكومية للتشريعات المتعلقة بحماية البيانات من خلال مراجعة تقارير الامتثال والالتزام بالقوانين.

○ معادلة المقياس:

$$\text{معدل الامتثال} = \frac{\text{عدد الجهات الملتزمة بالقانون}}{\text{اجمالي الجهات}} \times 100$$

○ الهدف: تحديد مدى التزام الجهات الحكومية بتطبيق التشريعات الرقمية المتعلقة بحماية البيانات الشخصية.

3. عدد الشكاوى المتعلقة بانتهاكات البيانات (Number of Complaints Regarding Data Violations)

○ كيفية القياس: يتم تسجيل عدد الشكاوى التي يقدمها المستخدمون حول الانتهاكات التي تعرضت لها بياناتهم الشخصية.

○ معادلة المقياس:

$$\bullet \text{ عدد الشكاوى} = \sum (\text{الشكاوى المقدمة حول انتهاكات البيانات})$$

○ الهدف: تقييم مدى تأثير التشريعات الرقمية على حماية البيانات الشخصية من منظور المستخدمين.

4. معدل تسريبات البيانات الحساسة (Sensitive Data Leakage Rate)

○ كيفية القياس: يُحسب من خلال عدد حالات تسريب البيانات الحساسة مقارنة بإجمالي حجم البيانات الشخصية التي تتم معالجتها.

○ معادلة المقياس:

$$\text{معدل تسريب البيانات الحساسة} = \frac{\text{عدد تسريب البيانات الحساسة}}{\text{اجمالي حجم البيانات}} \times 100$$

○ الهدف: تقييم مدى نجاح التشريعات في منع تسريب البيانات الحساسة مثل المعلومات الصحية أو المالية.

5. استطلاعات رضا المستخدمين حول حماية البيانات (User Satisfaction Surveys on) (Data Protection)

○ كيفية القياس: يتم توزيع استبيانات على مستخدمي الخدمات الحكومية الإلكترونية لقياس مدى رضاهم عن مستوى حماية بياناتهم الشخصية.

○ معادلة المقياس:

$$\text{معدل الرضا} = \frac{\text{عدد المستخدمين الراضين}}{\text{اجمالي عدد المشاركين في الاستبيان}} \times 100$$

○ الهدف: قياس ثقة المواطنين في التشريعات والسياسات المتعلقة بحماية بياناتهم.

6. معدل الحوادث الأمنية على أساس زمني (Security Incidents Rate Over Time)

○ كيفية القياس: يتم تتبع عدد الحوادث الأمنية المتعلقة بانتهاكات البيانات الشخصية على مدار فترة زمنية معينة (شهرية أو سنوية).

○ معادلة المقياس:

$$\text{معدل الحوادث الامنية} = \frac{\text{عدد الحوادث الامنية}}{\text{عدد الاشهر}}$$

- الهدف: تحديد التغيرات الزمنية في حدوث الحوادث الأمنية بعد تطبيق أو تحديث التشريعات الرقمية.

7. نسبة التحسن في مستوى حماية البيانات (Improvement Rate in Data Protection Levels)

- كيفية القياس: يقاس من خلال مقارنة مستوى الحوادث والشكاوى قبل وبعد تطبيق القوانين أو التعديلات الجديدة.

- معادلة المقياس:

$$\text{معدل التحسن} = 100 \times \frac{\text{معدل الحوادث بعد التشريعات} - \text{معدل الحوادث قبل التشريعات}}{\text{معدل الحوادث قبل التشريعات}}$$

- الهدف: تقييم تأثير القوانين الرقمية الجديدة على تحسين مستوى حماية البيانات.

السياق في دور القانون الرقمي في حماية البيانات الشخصية

في العصر الرقمي الحديث، يشهد العالم تطوراً سريعاً في التكنولوجيا والأنظمة الرقمية، مما زاد من كمية البيانات الشخصية التي يتم جمعها وتخزينها في مختلف المجالات، خاصة في البيئات الحكومية التي تعتمد على الخدمات الإلكترونية. هذا التطور يتطلب قوانين وتشريعات تحمي خصوصية الأفراد وتضمن أمان بياناتهم الشخصية. في هذا الإطار، يلعب القانون الرقمي دوراً حيوياً في حماية البيانات الشخصية، خاصة في ظل زيادة التهديدات السيبرانية ومحاولات الاختراقات التي تهدف إلى الوصول إلى المعلومات الشخصية بطرق غير مشروعة.

1. التطور التكنولوجي وزيادة الاعتماد على البيانات الشخصية

مع التطور السريع للتكنولوجيا، تتزايد كمية البيانات الشخصية التي تُجمع من الأفراد، سواء في مجالات الصحة، التعليم، الأعمال، أو حتى في الحياة اليومية من خلال المعاملات الإلكترونية. هذا التطور زاد من الحاجة إلى قوانين فعالة لحماية تلك البيانات ومنع إساءة استخدامها.

2. أهمية التشريعات الرقمية في حماية الخصوصية

تفرض الحكومات الإلكترونية تحديات جديدة تتعلق بحماية بيانات الأفراد. يأتي القانون الرقمي كوسيلة لضبط وتنظيم عملية جمع، تخزين، واستخدام البيانات الشخصية. في المملكة العربية السعودية، صدرت تشريعات تهدف إلى تنظيم حماية البيانات الشخصية ضمن الخدمات الحكومية الإلكترونية، حيث يحدد القانون كيفية معالجة البيانات ويحمي الأفراد من الانتهاكات.

3. دور القانون الرقمي في التصدي للتهديدات السيبرانية

مع زيادة وتيرة الهجمات السيبرانية، يلعب القانون الرقمي دوراً مهماً في ضمان الحماية القانونية للأفراد والمؤسسات ضد تسريب البيانات والاختراقات. تضع التشريعات معايير صارمة على المؤسسات الحكومية حول كيفية حماية البيانات الشخصية، وتعزز من التزامها بتطبيق أفضل ممارسات الأمان الرقمي.

4. التحديات القانونية في حماية البيانات الشخصية

بالرغم من وجود تشريعات لحماية البيانات الشخصية، لا تزال هناك تحديات تتعلق بتطبيق هذه القوانين بفعالية. تشمل هذه التحديات التعامل مع التطورات التكنولوجية السريعة التي قد تجعل بعض القوانين غير فعالة في حماية البيانات في الوقت المناسب. لذلك، من الضروري تحديث القوانين الرقمية باستمرار لمواكبة المستجدات.

5. التأثيرات الإيجابية للقوانين الرقمية على ثقة المستخدمين

يعزز القانون الرقمي من ثقة المستخدمين في الحكومات الإلكترونية، حيث توفر التشريعات إطاراً قانونياً يضمن حماية بياناتهم الشخصية، مما يزيد من رغبتهم في استخدام هذه الخدمات بثقة أكبر. كلما كانت القوانين أكثر شفافية وشمولية، زادت ثقة الأفراد في النظام الإلكتروني الحكومي.

6. التنسيق بين القوانين المحلية والدولية

في ظل التوسع الكبير في استخدام الإنترنت والتعاملات الإلكترونية عبر الحدود، يجب على القوانين الرقمية المحلية أن تتماشى مع المعايير الدولية لحماية البيانات. في المملكة العربية السعودية، يتم تبني قوانين مستوحاة من معايير دولية مثل النظام العام لحماية البيانات (GDPR) لضمان توافقها مع المتطلبات العالمية.

الخلاصة

يلعب القانون الرقمي دورًا حاسمًا في حماية البيانات الشخصية في البيئات الرقمية الحديثة، خاصة مع انتشار استخدام الخدمات الإلكترونية الحكومية. من خلال وضع التشريعات وتنفيذها بشكل فعال، تضمن الحكومات توفير حماية كافية لبيانات الأفراد وتعزيز ثقتهم في النظام الرقمي، مما يساهم في تحقيق بيئة آمنة ومستدامة للأعمال والمعاملات الإلكترونية.

2.3. المتغير المستقل (Independent Variable):

2.3.1. المتغير المستقل

المتغير المستقل هو المتغير الذي يتلاعب به الباحث أو يتحكم فيه بشكل مباشر في البحث لتحديد تأثيره على المتغير التابع. يُستخدم المتغير المستقل لتحديد السبب في التغيرات أو النتائج التي تظهر في المتغير التابع، وبالتالي فإنه يلعب دورًا حاسمًا في تصميم التجارب والدراسات العلمية. وفقًا للباحث (Kerlinger 1986)، فإن "المتغير المستقل هو العامل الذي يتم التحكم فيه أو تغييره من قبل الباحث لدراسة تأثيره على متغير آخر في التجربة".

في البحث الحالي حول "دور القانون الرقمي في حماية البيانات الشخصية في بيئات الحكومات الإلكترونية في المملكة العربية السعودية"، يُعتبر التشريعات الرقمية والسياسات المرتبطة بحماية البيانات الشخصية هو المتغير المستقل. هذا المتغير يتمثل في القوانين واللوائح التي تفرضها الحكومة لتنظيم عملية جمع، تخزين، ومعالجة البيانات الشخصية لضمان حماية الخصوصية. من

خلال دراسة تأثير التشريعات الرقمية (المتغير المستقل) على مستوى حماية البيانات الشخصية (المتغير التابع)، يمكن للبحث تحديد مدى فعالية القوانين الرقمية في تعزيز الأمان الرقمي.

التفسير

المتغير المستقل هو العامل الذي يتحكم فيه الباحث بهدف دراسة تأثيره على المتغيرات الأخرى، وتحديدًا المتغير التابع. يُعتبر هذا المتغير الأساس في التجربة أو الدراسة، حيث يتم التلاعب به بشكل مباشر أو تغييره لدراسة التغيرات الناتجة في المتغير التابع. تفسير المتغير المستقل يتيح فهم العوامل التي قد تؤثر على الظاهرة المدروسة، مما يساعد في تحليل العلاقات السببية بشكل أكثر دقة وفعالية.

في البحث الحالي، التشريعات الرقمية يُعتبر المتغير المستقل. هذا المتغير يتمثل في مجموعة القوانين واللوائح التي تطبقها المملكة العربية السعودية لتنظيم استخدام البيانات الشخصية. يمكن لهذه القوانين أن تشمل حماية البيانات، تنظيم الوصول إلى المعلومات، وتعزيز أمان البيانات. يتم من خلال هذه التشريعات تقليل المخاطر المرتبطة بالاختراقات الأمنية والتسريبات.

2.3.2. تفسير المتغير المستقل في سياق البحث:

تحديد التأثير المحتمل للتشريعات الرقمية:

التشريعات الرقمية قد تشمل فرض معايير صارمة على جمع البيانات، إتاحة وصول محدود للمعلومات الشخصية، وتطبيق تقنيات تشفير متقدمة. مثل هذه التدابير قد تساهم في تقليل حالات الاختراق وتسريب البيانات الشخصية، مما يشير إلى التأثير المباشر للتشريعات (المتغير المستقل) على مستوى الحماية (المتغير التابع).

2.3.3. التحكم والتلاعب بالمتغير المستقل:

في الدراسة، يتم تحليل تأثير التشريعات الرقمية بوصفها المتغير المستقل الذي يمكن أن يتغير حسب تطور القوانين أو اللوائح. على سبيل المثال، يمكن مقارنة الفترة التي سبقت تطبيق قانون حماية البيانات الشخصية في السعودية بالفترة التي تلت تطبيق القانون لتحديد التغيرات في مستوى حماية البيانات.

2.3.4. دور الباحث في التحكم بالمتغير المستقل:

في الدراسات التجريبية أو الميدانية، يمكن للباحث أن يتحكم أو يعدل من تنفيذ التشريعات أو تطبيق لوائح جديدة. من ثم، يمكن قياس التغيرات التي تحدث في مستوى حماية البيانات الشخصية. هذا النهج يتيح للباحثين تحديد مدى تأثير المتغير المستقل على النتائج، مما يدعم الفرضيات العلمية بأدلة ملموسة.

وفقًا لـ (Babbie 2010)، "المتغير المستقل هو الأداة التي يمكن من خلالها للباحثين اختبار نظرياتهم وتحديد العلاقة بين السبب والنتيجة". وبالتالي، فإن تفسير المتغير المستقل وفهم كيفية التحكم فيه وتحليله يُعتبر جزءًا أساسيًا في تصميم الدراسات واختبار الفرضيات في البحث العلمي.

2.4. كيف يؤثر المتغير المستقل على المتغير التابع؟

في البحث حول "دور القانون الرقمي في حماية البيانات الشخصية"، يتأثر المتغير التابع (مستوى حماية البيانات) بعدة جوانب من المتغير المستقل (التشريعات الرقمية). هنا كيف يمكن لكل جانب من جوانب التشريعات الرقمية أن يؤثر على المتغير التابع:

1. تطبيق قوانين صارمة حول جمع البيانات الشخصية:

- عندما تفرض التشريعات قوانين صارمة حول كيفية جمع البيانات، فإن هذا قد يحد من تسريب البيانات ويقلل من المخاطر المرتبطة بالاستخدام غير المصرح به للمعلومات الشخصية.
- مثال: فرض قوانين تقيّد الوصول إلى بيانات المستخدمين قد يؤدي إلى تحسين مستوى حماية البيانات وتقليل الحوادث الأمنية.

2. تنظيم الوصول إلى المعلومات:

- التشريعات التي تضع معايير للوصول إلى البيانات تُساهم في تقليل احتمالية وقوع الحوادث الأمنية. يمكن أن يؤدي تنظيم صلاحيات الوصول إلى تحسين مستوى الأمان وتقليل تعرض البيانات الشخصية للاختراق.
- مثال: تقييد الوصول إلى البيانات المالية أو الصحية وحصرها على أشخاص معينين قد يقلل من احتمالية تسريب المعلومات الحساسة.

3. تطبيق تقنيات تشفير البيانات:

- التشريعات التي تفرض استخدام تقنيات تشفير متقدمة تُساهم في حماية البيانات من الوصول غير المصرح به. التشفير يُعد من أهم التدابير الأمنية التي تساعد في حماية المعلومات الشخصية.
- مثال: قوانين تفرض تشفير البيانات الحساسة في الأنظمة الإلكترونية يمكن أن تقلل من احتمالية الوصول غير القانوني للمعلومات.

4. فرض عقوبات على الانتهاكات:

- التشريعات التي تفرض عقوبات صارمة على انتهاكات حماية البيانات قد تُساهم في تحسين مستوى الامتثال وزيادة الوعي بأهمية حماية البيانات الشخصية.
- مثال: فرض غرامات على المؤسسات التي تنتهك خصوصية البيانات يمكن أن يدفع هذه المؤسسات إلى تطبيق تدابير أكثر صرامة لحماية المعلومات.

الخلاصة:

كل جانب من جوانب التشريعات الرقمية يمكن أن يؤثر بشكل كبير على المتغير التابع (مستوى حماية البيانات الشخصية). تطبيق القوانين بشكل دقيق وفعال يمكن أن يحسن من مستوى الأمان الرقمي، بينما يمكن لتطبيق ضعيف أو غياب القوانين أن يزيد من المخاطر.

2.5. الدراسات السابقة (Previous studies):

1. البيانات الشخصية في آلية الحماية الجنائية للقانون

- المحتوى: تناقش هذه الدراسة الإطار القانوني الجنائي لحماية البيانات الشخصية في روسيا، مع التركيز على التحديات الناتجة عن تسرب البيانات وتأثير ذلك على الثقة في الأنظمة الرقمية الحكومية.
- الهدف: تقديم رؤية جديدة حول الآليات القانونية المطلوبة لتعزيز دور القانون الجنائي في حماية البيانات الشخصية.

- النتائج: وجدت الدراسة أن الرقمنة أدت إلى تسامح أكبر مع انتهاكات الخصوصية، مما يوصي بنهج تفاضلي في المسؤولية القانونية بناءً على نطاق كشف البيانات الشخصية.
(Ruskevich, 2023)

2. حماية البيانات الشخصية في البيئة الرقمية

- المحتوى: تستعرض هذه الورقة تطبيق قوانين حماية البيانات الشخصية في روسيا، مسلطة الضوء على التحديات التي تطرحها التقنيات الحديثة.
- الهدف: تحليل فعالية الأطر القانونية القائمة في حماية البيانات الشخصية.
- النتائج: الدراسة تسلط الضوء على عدم كفاية الحماية القانونية الحالية في التعامل مع التكنولوجيا المتطورة، وتقتترح تحسينات مثل إعطاء الأولوية لحماية البيانات الشخصية في الملفات الرقمية.
(Soldatova, 2020)

3. التناقضات المتأصلة في قانون حماية البيانات

- المحتوى: تستكشف هذه الدراسة التناقضات داخل قانون حماية البيانات، وخاصة التوازن بين حقوق المراقبين وتمكين الأفراد من التحكم في بياناتهم.
- الهدف: تقييم ما إذا كان ينبغي أن تكون الموافقة هي الأساس الرئيسي لمعالجة البيانات.
- النتائج: الدراسة خلصت إلى أن الشفافية والقواعد المنفصلة للقطاعين العام والخاص يمكن أن تحسن نتائج حماية البيانات.
(Blume, 2012)

4. قانون حماية المعلومات الشخصية والحماية الجنائية للمعلومات الشخصية

- المحتوى: تستعرض هذه الدراسة قانون حماية المعلومات الشخصية في الصين، مع التركيز على الحاجة إلى تعريفات أوضح وحماية البيانات البيومترية.
 - الهدف: تقييم الحماية القانونية للمعلومات الشخصية بموجب قانون حماية البيانات الجديد في الصين.
 - النتائج: القانون يحتاج إلى تحسين في مراقبة المواقع الإلكترونية وضمان جمع البيانات بشكل آمن.
- (Wu, 2022)

5. دليل بحثي لقانون حماية البيانات الأوروبي

- المحتوى: توفر هذه الورقة نظرة عامة على قانون حماية البيانات الأوروبي، مع تحليل تأثيره الدولي وتوسعه.
 - الهدف: تقديم رؤى حول انتشار قوانين حماية البيانات على المستوى العالمي.
 - النتائج: وجدت الدراسة أن قوانين خصوصية البيانات تنتشر عالميًا، لا سيما بسبب التجارة الدولية والمخاوف الأمنية.
- (McCarty–Snead & Hilby, 2014)

6. التداعيات القانونية والأخلاقية في قضايا سرقة البيانات في العصر الرقمي

- المحتوى: تستكشف هذه الدراسة التحديات القانونية والأخلاقية في حماية البيانات الشخصية في إندونيسيا، حيث لا توجد قوانين خاصة بحماية البيانات.
 - الهدف: الدعوة إلى التصديق على قوانين حماية البيانات الشخصية في إندونيسيا.
 - النتائج: تؤكد الدراسة على الحاجة إلى يقين قانوني وزيادة الوعي العام بشأن حماية البيانات.
- (Sinaga, 2023)

7. التحديات الحالية ومستقبل الحماية القانونية للبيانات الشخصية

- المحتوى: تعالج هذه الدراسة التهديدات المتزايدة للجريمة السيبرانية والعولمة على حماية البيانات الشخصية، لا سيما في أوكرانيا.
 - الهدف: اقتراح إصلاحات قانونية لتعزيز حماية البيانات الشخصية وسط التغيرات التكنولوجية السريعة.
 - النتائج: الدراسة تحدد ثغرات في قوانين الأمن السيبراني وتقتراح إصلاحات لتحسين الحماية من المخاطر عبر الحدود.
- (Duravkin & Hafych, 2023)

8. حماية البيانات للعصر الرقمي

- المحتوى: تستعرض هذه الورقة الأطر القانونية المتطورة في الاتحاد الأوروبي فيما يتعلق بالمسؤولية عن حماية البيانات.
 - الهدف: تحليل الإصلاحات المقترحة في الاتحاد الأوروبي التي تهدف إلى تعزيز حماية البيانات من خلال تدابير مساءلة أكثر صرامة.
 - النتائج: الدراسة توصي بتحسين إدارة المنظمات لضمان الامتثال لحماية البيانات.
- (Gumzej, 2012)

9. جمع البيانات الرقمية وقانون خصوصية المعلومات

- المحتوى: يناقش هذا الكتاب التحديات التي تطرحها تقنيات جمع البيانات، وخاصة في سياق "المنازل الذكية".
- الهدف: الدعوة إلى إعادة صياغة قوانين الخصوصية لتنظيم النماذج التجارية الجديدة التي تعتمد على جمع البيانات من أجهزة الاستشعار.

- النتائج: الدراسة تدعو إلى تعزيز قوانين الخصوصية لحماية البيانات الشخصية من الطبيعة المنتشرة لتقنيات جمع البيانات الرقمية.
(Burdon, 2020)

10.مراجعة قانونية لحماية المستهلك فيما يتعلق بالبيانات الشخصية على المنصات الرقمية

- المحتوى: تدرس هذه الدراسة كيفية حماية البيانات الشخصية للمستهلكين في المعاملات على المنصات الرقمية، مع التركيز على إندونيسيا.
- الهدف: تقييم قوانين حماية المستهلك الحالية واقتراح إطار قانوني جديد للمنصات الرقمية.
- النتائج: خلصت الدراسة إلى أن القانون الإندونيسي يتطلب لوائح محددة لمنع إساءة استخدام بيانات المستهلكين من قبل الفاعلين التجاريين.
(Azhari, 2021)

جدول تلخيص الدراسات:

جدول 1- 2 تلخيص الدراسات السابقة

النتيجة	المرجع	اسم الدراسة
الرقمنة أدت إلى تسامح أكبر مع انتهاكات الخصوصية، توصي بنهج تفاضلي في المسؤولية القانونية بناءً على نطاق كشف البيانات الشخصية.	Ruskevich, 2023	البيانات الشخصية في آلية الحماية الجنائية للقانون

حماية البيانات الشخصية في البيئة الرقمية	Soldatova, 2020	عدم كفاية الحماية القانونية الحالية، تقترح تحسينات مثل إعطاء الأولوية لحماية البيانات الشخصية في الملفات الرقمية.
التناقضات المتأصلة في قانون حماية البيانات	Blume, 2012	الشفافية والقواعد المنفصلة للقطاعين العام والخاص يمكن أن تحسن نتائج حماية البيانات.
قانون حماية المعلومات الشخصية والحماية الجنائية للمعلومات الشخصية	Wu, 2022	القانون يحتاج إلى تحسين في مراقبة المواقع الإلكترونية وضمان جمع البيانات بشكل آمن.
دليل بحثي لقانون حماية البيانات الأوروبي	McCarty–Snead & Hilby, 2014	قوانين خصوصية البيانات تنتشر عالمياً، خاصة بسبب التجارة الدولية والمخاوف الأمنية.
التداعيات القانونية والأخلاقية في قضايا سرقة البيانات في العصر الرقمي	Sinaga, 2023	الحاجة إلى يقين قانوني وزيادة الوعي العام بشأن حماية البيانات.
التحديات الحالية ومستقبل الحماية القانونية للبيانات الشخصية	Duravkin & Hafych, 2023	تحديد ثغرات في قوانين الأمن السيبراني وتقترح إصلاحات لتحسين الحماية من المخاطر عبر الحدود.

توصي بتحسين إدارة المنظمات لضمان الامتثال لحماية البيانات.	Gumzej, 2012	حماية البيانات للعصر الرقمي
تعزيز قوانين الخصوصية لحماية البيانات الشخصية من تقنيات جمع البيانات الرقمية.	Burdon, 2020	جمع البيانات الرقمية وقانون خصوصية المعلومات
يتطلب القانون الإندونيسي لوائح محددة لمنع إساءة استخدام بيانات المستهلكين من قبل الفاعلين التجاريين.	Azhari, 2021	مراجعة قانونية لحماية المستهلك فيما يتعلق بالبيانات الشخصية على المنصات الرقمية

2.6. ما ستقدمه الدراسة الحالية مقارنة بالدراسات السابقة (The contribution of the current study compared to previous studies):

في سياق الدراسات السابقة حول دور القانون الرقمي في حماية البيانات الشخصية، تركزت هذه الدراسات بشكل رئيسي على التحديات القانونية المرتبطة بالتقنيات الرقمية الناشئة وتأثيرها على حماية البيانات الشخصية. ركزت بعض الدراسات على القوانين الجنائية لحماية البيانات، بينما تطرقت دراسات أخرى إلى الآثار التنظيمية والقانونية المتعلقة بحماية البيانات في البيئات الرقمية العالمية مثل قوانين الاتحاد الأوروبي أو التشريعات الوطنية.

2.7. الدراسة الحالية ستركز على عدة نقاط مقارنة بالدراسات السابقة:

1. التركيز على السياق السعودي :على عكس الدراسات السابقة التي تركزت على بيئات دولية متنوعة (مثل أوروبا والصين وإندونيسيا)، ستقدم الدراسة الحالية تحليلًا معمقًا لدور القانون الرقمي في حماية البيانات الشخصية ضمن المملكة العربية السعودية. سيتم تسليط الضوء على التحديات القانونية والعملية في البيئة السعودية، خصوصًا في ضوء رؤية المملكة 2030 التي تدفع نحو التحول الرقمي.

2. تحليل السياسات المحلية :بينما ركزت بعض الدراسات على الأطر القانونية الدولية مثل "اللائحة العامة لحماية البيانات (GDPR)"، ستحلل الدراسة الحالية السياسات المحلية والتشريعات الرقمية المتعلقة بحماية البيانات الشخصية في السعودية. وستقدم تقييمًا شاملًا للتشريعات الحالية في السعودية، مع التركيز على الفجوات التي تحتاج إلى معالجة.

3. التحديات الخاصة بالبنية التحتية الرقمية :ستدرس هذه الدراسة تحديات حماية البيانات الشخصية في سياق البنية التحتية الرقمية الناشئة في المملكة، مثل الحوسبة السحابية والخدمات الحكومية الإلكترونية. ستقدم تحليلًا حول كيفية تأثير هذه البنى التحتية على أمان البيانات وخصوصيتها، وهي نقاط لم تركز عليها بشكل كافٍ الدراسات السابقة.

4. التركيز على تأثير التحول الرقمي :ستتعامل الدراسة مع تأثير التحول الرقمي الكبير في المملكة على قوانين حماية البيانات، وذلك في ظل توسع استخدام التقنيات الحديثة مثل الذكاء الاصطناعي والبيانات البيومترية. وستقدم توصيات حول كيفية تحسين الأطر القانونية لمواكبة هذا التحول التكنولوجي السريع.

5. التحليل التطبيقي للحماية الفعالة :على عكس بعض الدراسات التي اقتصرت بالتحليل النظري أو المفاهيمي، ستحاول الدراسة الحالية تقديم تحليل عملي حول كيفية تطبيق السياسات والقوانين الرقمية في المؤسسات السعودية، مما يوفر إطارًا عمليًا يُمكن الحكومة والمؤسسات من تحسين مستوى الحماية.

6. إضافة جديدة إلى الأدبيات السعودية: ستقدم الدراسة مساهمة جديدة إلى الأدبيات الأكاديمية المتعلقة بحماية البيانات في المملكة، حيث سيتم توثيق ومقارنة الإجراءات المتبعة في المؤسسات السعودية مع المعايير الدولية، مما يمكن أن يفتح المجال لتوصيات إصلاحية تشريعية.

بالتالي، تسعى هذه الدراسة إلى معالجة الفجوات الموجودة في الأدبيات السابقة من خلال تقديم تحليل متعمق يركز على السياق المحلي في السعودية. كما تهدف إلى تطوير إطار عملي شامل وتقديم توصيات قابلة للتنفيذ، بهدف تعزيز حماية البيانات في ظل البيئة الرقمية المتسارعة التطور.

2.8. الإطار النظري للدراسة (Theoretical Framework of the Study)

الإطار النظري للدراسة يعتمد على مجموعة من النظريات القانونية والتنظيمية المرتبطة بحماية البيانات الشخصية في البيئة الرقمية. يستند إلى فهم شامل للأبعاد التقنية والقانونية التي تحكم استخدام البيانات الشخصية في العصر الرقمي، مع التركيز على دور القانون الرقمي في توفير حماية فعالة للبيانات. النقاط الرئيسية في الإطار النظري تشمل:

1. نظرية الخصوصية المعلوماتية • (Information Privacy Theory) تُعتبر نظرية الخصوصية المعلوماتية أساسًا في الإطار القانوني لحماية البيانات الشخصية. وفقًا لـ Westin (1967)، فإن "الحق في الخصوصية يُعنى بقدرة الفرد على التحكم في كيفية استخدام بياناته الشخصية". في هذه الدراسة، سيتم تطبيق هذه النظرية لتحليل كيفية تمكين الأفراد من التحكم في بياناتهم الشخصية في ظل القوانين الرقمية السعودية. يُركز التحليل على مدى فاعلية هذه القوانين في تمكين الأفراد من حماية بياناتهم من الانتهاكات.

2. النظرية التنظيمية للامتثال • (Regulatory Compliance Theory): تعتمد هذه النظرية على فهم كيفية تنظيم وتطبيق القوانين المتعلقة بحماية البيانات. وكما ذكر (Grama 2014) ، "يجب أن يتماشى الامتثال التنظيمي مع التطورات التقنية لضمان فعالية حماية البيانات الشخصية •". في هذه الدراسة، سيتم استخدام هذه النظرية لتحليل مدى التزام المؤسسات السعودية بالقوانين المتعلقة بحماية البيانات، وكيفية تعزيز الامتثال التنظيمي لمنع حدوث أي اختراقات أو انتهاكات.

3. نظرية المسؤولية القانونية • (Legal Accountability Theory): تقوم نظرية المسؤولية القانونية على مبدأ أن الأفراد والمؤسسات الذين يجمعون ويستخدمون البيانات الشخصية يجب أن يكونوا مسؤولين قانونيًا عن انتهاكات البيانات. وفقًا لـ (Solove 2004) ، "يجب على المؤسسات تحمل المسؤولية الكاملة عند حدوث انتهاكات للبيانات الشخصية •". يتم تطبيق هذه النظرية في الدراسة لتقييم دور الشركات السعودية في حماية البيانات، ومدى تحملها المسؤولية في حالة حدوث تسربات للبيانات أو انتهاكات للخصوصية.

4. نظرية الحوكمة الرقمية • (Digital Governance Theory): تعتمد هذه النظرية على تحليل تأثير الحوكمة الرقمية على إدارة البيانات الشخصية. وفقًا لـ Bannister و Connolly (2014)، "تعد الحوكمة الرقمية جزءًا أساسيًا من إدارة البيانات في البيئات الرقمية •". سيتم استخدام هذه النظرية لتقييم كيفية وضع الحكومة السعودية للسياسات والإجراءات التي تضمن حماية البيانات في الأنظمة الرقمية، وما هو دور الهيئات الرقابية في ضمان الامتثال لهذه السياسات.

5. نظرية إدارة المخاطر الرقمية • (Digital Risk Management Theory): تركز هذه النظرية على تحليل المخاطر المتعلقة بحماية البيانات الشخصية في البيئات الرقمية. وكما أوضح (Cavoukian 2009)، "إدارة المخاطر الرقمية تتطلب تقييم التهديدات المحتملة وتطبيق تدابير استباقية لتجنب انتهاكات البيانات •". سيتم تطبيق هذه النظرية في الدراسة لتقييم المخاطر التي تواجه البيانات الشخصية في المملكة العربية السعودية، وتقديم استراتيجيات قانونية وتقنية لإدارة تلك المخاطر بفعالية.

6. الإطار القانوني لحماية البيانات الشخصية • (Data Protection Legal Framework)

يشمل هذا الإطار القوانين والتشريعات التي تنظم كيفية حماية البيانات الشخصية في المملكة العربية السعودية. يعتمد الإطار القانوني على قوانين مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية التي تضع المعايير القانونية لحماية البيانات من التهديدات الرقمية • سيتم تطبيق هذا الإطار القانوني في الدراسة لتحديد مدى فعالية التشريعات السعودية في حماية البيانات الشخصية، مع تقديم توصيات لتحسين الأطر القانونية الحالية.

الخلاصة: يعتمد الإطار النظري للدراسة على مجموعة متنوعة من النظريات القانونية والتنظيمية لفهم التأثيرات الشاملة للقانون الرقمي على حماية البيانات الشخصية في المملكة العربية السعودية. من خلال استخدام هذا الإطار، تسعى الدراسة إلى تقديم تحليل عميق وشامل لمدى فعالية الأطر القانونية الحالية، مع تقديم حلول عملية مبنية على الأطر النظرية لتحسين حماية البيانات.

مكونات الإطار النظري للدراسة (Components of the theoretical framework of the study)

شرح النموذج النظري المختار:

النموذج النظري المختار للدراسة يعتمد على مجموعة من النظريات القانونية والتنظيمية التي تعزز فهم الجوانب المختلفة لحماية البيانات في البيئة الرقمية المتسارعة. تم تصميم هذا النموذج لفهم التفاعل بين القوانين والسياسات الرقمية والتحديات التقنية والأمنية المتعلقة بالبيانات الشخصية. كما يركز على كيفية تعزيز الأطر القانونية والتنظيمية لحماية البيانات وضمان التزام المؤسسات بتلك الأطر.

مكونات الاطار النظري:

1. نظرية الخصوصية المعلوماتية: (Information Privacy Theory)

تعتبر هذه النظرية أن حماية الخصوصية هي حق أساسي للفرد. يتمحور التركيز هنا حول كيفية تمكين الأفراد من التحكم في معلوماتهم الشخصية، والتحكم في الوصول إليها واستخدامها. يُستخدم هذا المفهوم لتقييم مدى فعالية القوانين السعودية في ضمان هذا الحق الأساسي في البيئة الرقمية.

2. النظرية التنظيمية للامتثال: (Regulatory Compliance Theory)

تركز هذه النظرية على أهمية التزام المؤسسات بالقوانين والسياسات المعمول بها لضمان حماية البيانات. في هذا النموذج، يُستخدم الامتثال التنظيمي كمعيار لتحليل كيفية التزام المؤسسات في السعودية بالقوانين المتعلقة بحماية البيانات الشخصية، ودور الجهات التنظيمية في مراقبة وتنفيذ تلك القوانين.

3. نظرية المسؤولية القانونية: (Legal Accountability Theory)

توضح هذه النظرية أن المؤسسات التي تجمع البيانات الشخصية يجب أن تكون مسؤولة قانونياً عن أي انتهاكات تحدث. يتم تطبيق هذه النظرية لتقييم مدى فعالية القوانين السعودية في تحميل المؤسسات المسؤولية القانونية في حالات تسريب أو إساءة استخدام البيانات الشخصية.

4. نظرية الحوكمة الرقمية: (Digital Governance Theory)

تعتمد هذه النظرية على كيفية وضع الحكومات والشركات سياسات تنظيمية لحماية البيانات. يُستخدم هذا الإطار لتحليل كيفية تأثير الحوكمة الرقمية على حماية البيانات الشخصية في المملكة، وما هو دور الهيئات الرقابية مثل الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) في ضمان الحوكمة الرقمية الفعالة.

5. نظرية إدارة المخاطر الرقمية: (Digital Risk Management Theory)

تهدف هذه النظرية إلى تحليل وتقييم المخاطر التي تواجه البيانات الشخصية في البيئات الرقمية. يتم تطبيقها في النموذج لتحليل التهديدات المحتملة مثل الهجمات السيبرانية والاختراقات الأمنية، ولتقديم حلول لإدارة تلك المخاطر استناداً إلى القوانين والإجراءات الأمنية المتبعة في السعودية.

6. الإطار القانوني لحماية البيانات الشخصية: (Data Protection Legal Framework)

يشمل هذا الإطار القوانين واللوائح التي تحكم حماية البيانات الشخصية، مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية في السعودية. يعتمد النموذج على هذا الإطار لفهم كيفية تطبيق تلك القوانين في البيئة الرقمية الحالية، وتحديد مدى فعاليتها في مواجهة التحديات التقنية الحديثة.

لماذا تم اختيار هذا النموذج؟

تم اختيار هذا النموذج القانوني المتكامل لأنه يتيح تحليل دور القانون الرقمي في حماية البيانات الشخصية من جوانب متعددة، مما يقدم رؤية شاملة حول كيفية تأثير الأنظمة والقوانين على ضمان حماية البيانات في المملكة العربية السعودية. يجمع النموذج بين الأبعاد القانونية، التنظيمية، التقنية، والأمنية لتقديم تحليل متكامل يساعد على تطوير سياسات وإجراءات قانونية أكثر فعالية لحماية البيانات وباستخدام هذا الإطار المتكامل، يمكن للدراسة تقديم توصيات مبنية على أسس علمية لتطوير الأطر القانونية والسياسات المتعلقة بحماية البيانات الشخصية، بما يتماشى مع التطور الرقمي السريع الذي تشهده المملكة في ظل رؤية 2030.

2.9. دعم الفرضيات وأسئلة البحث (Support for Hypotheses and Research Questions)

كيف يدعم الإطار النظري فرضيات الدراسة

يهدف الإطار النظري في هذه الدراسة إلى دعم الفرضيات وأسئلة البحث من خلال تطبيق مجموعة من النظريات القانونية والتنظيمية التي تساعد في تحليل العلاقة بين القوانين الرقمية وحماية البيانات الشخصية. ويُقدّم الإطار النظري أسسًا علمية لفهم كيفية تأثير القانون الرقمي على حماية البيانات الشخصية، ويسهّل اختبار الفرضيات والإجابة على أسئلة البحث بشكل دقيق. فيما يلي شرح لدعم الفرضيات:

1. دعم الفرضية الأساسية: "تطبيق القوانين الرقمية يؤدي إلى تعزيز حماية البيانات الشخصية في المملكة العربية السعودية:"

- تعتمد هذه الفرضية على نظرية الخصوصية المعلوماتية (Information Privacy Theory) التي توضح أن القوانين الرقمية تساعد الأفراد في التحكم في بياناتهم الشخصية. وفقًا لـ Westin (1967)، فإن "القوانين المتعلقة بالخصوصية تعزز من قدرة الأفراد على السيطرة على بياناتهم وحمايتهم من الاستخدام غير المصرح به."
- يدعم الإطار النظري هذه الفرضية من خلال توضيح كيف أن القوانين الرقمية السعودية، مثل قانون حماية البيانات الشخصية، تعزز من قدرة الأفراد على التحكم في معلوماتهم الشخصية وحمايتهم من الانتهاكات.

2. دعم الفرضية الثانية: "الامتثال التنظيمي للقوانين الرقمية يقلل من احتمالية تسرب البيانات الشخصية:"

- تُفسّر هذه الفرضية من خلال النظرية التنظيمية للامتثال (Regulatory Compliance Theory) التي تشير إلى أن الالتزام الصارم بالقوانين والتشريعات يحمي البيانات من الانتهاكات. وكما ذكر Grama (2014)، "الامتثال الفعال للقوانين الرقمية يعزز من حماية البيانات الشخصية ويقلل من المخاطر."
- يدعم الإطار النظري هذه الفرضية من خلال تحليل مدى التزام المؤسسات السعودية بالقوانين الرقمية، وكيف يؤثر هذا الالتزام على حماية البيانات الشخصية ومنع التسريبات.

3. دعم الفرضية الثالثة: "المسؤولية القانونية تُحفز المؤسسات على تعزيز حماية البيانات الشخصية:"

- تستند هذه الفرضية إلى نظرية المسؤولية القانونية (Legal Accountability Theory) التي توضح أن تحمل المسؤولية القانونية يحفز المؤسسات على اتخاذ تدابير قوية لحماية البيانات. وفقاً لـ (Solove 2004) ، "المسؤولية القانونية تُلزم المؤسسات بتعزيز إجراءات الحماية عند التعامل مع البيانات الشخصية."
- يدعم الإطار النظري هذه الفرضية من خلال توضيح كيف تؤثر القوانين التي تُحمّل الشركات المسؤولية القانونية عند انتهاك البيانات على تعزيز جهود حماية البيانات في المملكة.

4. دعم الفرضية الرابعة: "التحول الرقمي السريع يزيد من الحاجة لتحديث القوانين لحماية البيانات الشخصية بشكل مستمر:"

- تعتمد هذه الفرضية على نظرية الحوكمة الرقمية (Digital Governance Theory) التي تشير إلى أن التحول الرقمي يتطلب تحديثاً مستمراً للقوانين لضمان الحماية الفعالة للبيانات. وكما ذكر Bannister و (Connolly 2014) ، "التحولات الرقمية السريعة تتطلب تعديلات مستمرة في الأطر القانونية لضمان حماية البيانات."
- يدعم الإطار النظري هذه الفرضية من خلال تحليل كيف تسهم التطورات الرقمية في المملكة في تغيير احتياجات حماية البيانات، ما يؤدي إلى الحاجة لتحديث الأطر القانونية باستمرار.

5. دعم الفرضية الخامسة: "إدارة المخاطر الرقمية تقلل من تعرض البيانات الشخصية للتهديدات الرقمية:"

- تُعزز هذه الفرضية من خلال نظرية إدارة المخاطر الرقمية (Digital Risk Management Theory) التي توضح أن تحليل المخاطر وتطبيق التدابير الوقائية يُقلل من التهديدات الأمنية على البيانات الشخصية. كما أوضح (Cavoukian 2009) ، "الإدارة الجيدة للمخاطر الرقمية تعزز حماية البيانات من الهجمات السيبرانية."
- يدعم الإطار النظري هذه الفرضية من خلال توضيح كيف يمكن للمؤسسات في المملكة تحسين سياسات إدارة المخاطر لتقليل احتمالية تعرض البيانات للهجمات الرقمية.

6. دعم أسئلة البحث:

- أسئلة البحث تُغطى بشكل شامل من خلال دمج النظريات القانونية والتنظيمية والتقنية المتعلقة بحماية البيانات الشخصية. على سبيل المثال، نظرية الخصوصية المعلوماتية تُجيب على سؤال كيفية تمكين الأفراد من التحكم في بياناتهم الشخصية ضمن البيئة الرقمية السعودية، في حين تُفسر نظرية الامتثال التنظيمي كيفية تأثر المؤسسات بتطبيق القوانين الرقمية واتباع المعايير التنظيمية في حماية البيانات الشخصية.
- يُساهم الإطار النظري في تحليل أسئلة البحث من خلال تقديم تفسير علمي يُظهر العلاقة بين القوانين الرقمية وحماية البيانات الشخصية. يعتمد الإطار على تطبيق نماذج متكاملة مثل نظرية المسؤولية القانونية التي تفسر كيفية إلزام المؤسسات بتحمل مسؤولية انتهاكات البيانات، ونظرية الحوكمة الرقمية التي توضح تأثير التحول الرقمي السريع على تحديث الأطر القانونية.

2.10. التكامل مع البحوث السابقة والبناءات النظرية

يتكامل بحث "دور القانون الرقمي في حماية البيانات الشخصية" مع الدراسات السابقة والبناءات النظرية من خلال استكشاف وتطبيق الأطر القانونية والتنظيمية والتقنية التي تم تناولها في الأدبيات السابقة، وذلك لتحليل كيفية تطور حماية البيانات في البيئات الرقمية. يعتمد البحث على أسس نظرية متعددة تم تطويرها في دراسات سابقة لتوفير إطار شامل لحماية البيانات، بما يتناسب مع التحديات الرقمية الحديثة في المملكة العربية السعودية.

1. البناءات النظرية السابقة:

• نظرية الخصوصية المعلوماتية: (Information Privacy Theory) استناداً إلى Westin (1967)، الذي ركز على حق الأفراد في التحكم في معلوماتهم الشخصية، يتم توظيف هذه النظرية في البحث الحالي لتحليل مدى تمكين القانون الرقمي في السعودية الأفراد من حماية خصوصيتهم في البيئة الرقمية. تستفيد الدراسة من الأدبيات السابقة التي تناولت هذا المفهوم على المستوى العالمي وتطبيقه في السياق المحلي.

• النظرية التنظيمية للامتثال (Regulatory Compliance Theory) كما أشار Grama (2014)، فإن الامتثال التنظيمي يجب أن يواكب التطورات التكنولوجية لضمان حماية البيانات الشخصية بشكل فعال. يتم استكمال هذا المفهوم في البحث الحالي من خلال استكشاف مدى امتثال المؤسسات السعودية للقوانين المحلية والإجراءات الوقائية المتبعة لمنع انتهاكات البيانات.

• نظرية المسؤولية القانونية: (Legal Accountability Theory) من خلال الاعتماد على Solove (2004)، الذي أكد على أهمية تحمل المسؤولية القانونية في حالة انتهاك البيانات، يبني البحث الحالي على هذا الأساس لفهم مدى تحمل المؤسسات السعودية لمسؤولية حماية البيانات الشخصية وفق القوانين المحلية.

2. التكامل مع الأدبيات السابقة: يتماشى البحث الحالي مع الأدبيات السابقة التي تناولت التشريعات الدولية، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، بهدف تقديم مقارنات تساعد في فهم مدى فعالية التشريعات السعودية في حماية البيانات الشخصية. من خلال مراجعة وتحليل تلك الدراسات، يستفيد البحث من الفجوات التي كشفت عنها الأبحاث السابقة فيما يتعلق بالاختلافات الثقافية والقانونية بين السعودية والدول الأخرى، ويسعى لتقديم تحسينات قانونية محلية.

3. سد الفجوات المعرفية: العديد من الدراسات السابقة تناولت حماية البيانات من منظور دولي أو تقني بحت، لكن البحث الحالي يهدف إلى سد الفجوة التي تتعلق بدور القانون الرقمي في حماية البيانات في السياق السعودي. تُظهر الأبحاث السابقة أهمية وجود إطار قانوني متين للتعامل مع تحديات البيانات في العصر الرقمي، بينما يركز البحث الحالي على كيفية تطوير هذا الإطار القانوني محلياً لدعم رؤية 2030 والتحول الرقمي.

4. الإضافة النظرية والتطبيقية: بناءً على التفسيرات النظرية المقدمة في الأدبيات السابقة، يُعد البحث الحالي خطوة نحو تطبيق هذه النظريات في سياق المملكة العربية السعودية. يضيف البحث إلى الأدبيات من خلال تقديم توصيات عملية لتحسين الأطر القانونية القائمة، وتطوير استراتيجيات جديدة تضمن حماية البيانات في البيئة الرقمية المتسارعة، مع التركيز على الامتثال القانوني والتقني.

يساهم البحث في تطوير البناءات النظرية المرتبطة بحماية البيانات، كما يعمل على تكامل الأفكار من البحوث السابقة لتقديم نموذج قانوني أكثر فعالية يتماشى مع احتياجات البيئة الرقمية في السعودية.

الفصل الثالث

منهجية الدراسة (Study methodology)

3.1. مقدمة (introduction) :

تُعتبر منهجية الدراسة ركيزة أساسية في أي بحث علمي، حيث تحدد الأدوات والخطوات التي سيتم استخدامها لجمع البيانات وتحليلها بما يضمن الوصول إلى نتائج علمية دقيقة وقابلة للتطبيق. في هذا الفصل، سيتم توضيح الخطوات المتبعة في دراسة دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية. يهدف هذا الفصل إلى تقديم إطار منهجي متكامل يساعد في الإجابة على أسئلة البحث واختبار الفرضيات المطروحة سوف تتضمن المنهجية شرحاً تفصيلياً لتصميم الدراسة، أدوات جمع البيانات، نوعية العينة المختارة، وأساليب التحليل المستخدمة. كما سيتم تناول الاعتبارات الأخلاقية المتعلقة بجمع المعلومات وتحليلها لضمان سرية البيانات وحماية حقوق الأفراد المشاركين في الدراسة. من خلال هذا النهج، تسعى الدراسة إلى تقديم نتائج موثوقة يمكن الاعتماد عليها في تحسين الأطر القانونية لحماية البيانات في البيئة الرقمية السعودية.

3.2. تصميم البحث (Research Design)

يهدف تصميم البحث في هذه الدراسة إلى توفير إطار منهجي يساعد على تحليل دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية. يعتمد البحث على تصميم يجمع بين المنهج الوصفي والتحليلي بهدف استكشاف الوضع الراهن للقوانين الرقمية وتقييم فعاليتها في حماية البيانات الشخصية.

1. المنهج الوصفي التحليلي: يعتمد البحث على المنهج الوصفي التحليلي لفهم الأطر القانونية والتنظيمية المتعلقة بحماية البيانات الشخصية في المملكة العربية السعودية. سيساعد هذا المنهج في تقديم وصف شامل للوائح والقوانين، مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية، وكذلك تحليل تأثير هذه القوانين على البيئة الرقمية.

2. جمع البيانات: سيتم جمع البيانات باستخدام أدوات متعددة تشمل المصادر القانونية والأدبية، مثل القوانين المعمول بها، الدراسات السابقة، والتقارير المتعلقة بحماية البيانات الشخصية. كما سيتم الاستعانة بآراء خبراء القانون والتكنولوجيا عبر استبيانات ومقابلات متعمقة لتحليل فعالية الأطر القانونية الحالية.

3. تحليل مقارن: ستتضمن الدراسة تحليلاً مقارناً بين الأطر القانونية في المملكة العربية السعودية ونظيراتها في دول أخرى، مثل الاتحاد الأوروبي الذي يعد من الأطر الرائدة في هذا المجال من خلال اللائحة العامة لحماية البيانات (GDPR). سيسمح هذا التحليل بفهم التباين في التشريعات وتحديد أفضل الممارسات التي يمكن تبنيها محلياً.

4. دراسات الحالة: ستتضمن الدراسة تحليلاً لحالات واقعية تعرضت لانتهاكات للبيانات الشخصية في السعودية ودول أخرى. سيساعد تحليل هذه الحالات في فهم مدى فعالية القانون الرقمي الحالي في التعامل مع التحديات الناشئة عن التقدم التكنولوجي واستخدام البيانات في البيئة الرقمية.

5. الاعتبارات الأخلاقية: سيتم الالتزام بأعلى المعايير الأخلاقية في جمع البيانات وتحليلها، بما يضمن سرية المعلومات وحماية حقوق المشاركين. ستتم مراجعة كافة البيانات الشخصية التي سيتم جمعها في إطار الدراسة لضمان عدم استخدامها بطرق تخالف القوانين المعمول بها.

من خلال هذا التصميم، تهدف الدراسة إلى توفير فهم شامل وعملي لدور القانون الرقمي في حماية البيانات الشخصية، مع تقديم توصيات قابلة للتنفيذ لتحسين الأطر القانونية والسياسات المتعلقة بحماية الخصوصية في المملكة العربية السعودية.

3.3. الخطوات العملية لتنفيذ البحث:

تهدف الخطوات العملية لتنفيذ البحث إلى وضع خطة منظمة تضمن تنفيذ الدراسة بكفاءة ودقة للوصول إلى نتائج موثوقة وملموسة. فيما يلي الخطوات التي سيتم اتباعها في البحث حول دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية:

1. تحديد موضوع الدراسة وصياغة الفرضيات:

○ يتم في هذه الخطوة تحديد نطاق الدراسة بشكل دقيق، وصياغة الفرضيات الأساسية التي سيتم اختبارها خلال البحث. ستتعلق الفرضيات بفعالية الأطر القانونية القائمة ومدى حماية البيانات الشخصية في البيئة الرقمية السعودية.

2. مراجعة الأدبيات السابقة:

- سيتم استعراض وتحليل الأدبيات المتعلقة بالقوانين الرقمية وحماية البيانات الشخصية على المستوى المحلي والدولي. سيشمل ذلك مراجعة القوانين السعودية مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات، إضافة إلى الأطر الدولية مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي.

3. تصميم أدوات جمع البيانات:

- سيتم تصميم أدوات جمع البيانات بما يتناسب مع أهداف الدراسة. يشمل ذلك إعداد استبيانات لجمع آراء خبراء القانون والتكنولوجيا، وإجراء مقابلات متعمقة للحصول على فهم أعمق حول فعالية الأطر القانونية المعمول بها.

4. اختيار عينة الدراسة:

- سيتم اختيار عينة تمثيلية من الخبراء القانونيين، المتخصصين في حماية البيانات، والمسؤولين في المؤسسات الحكومية والشركات الخاصة في المملكة العربية السعودية. يهدف ذلك إلى جمع بيانات متنوعة وشاملة تعكس الواقع الحالي لحماية البيانات في المملكة.

5. جمع البيانات:

- ستتم هذه الخطوة من خلال:
 - الاستبيانات: سيتم توزيع استبيانات تحتوي على أسئلة مغلقة ومفتوحة حول مدى فعالية القوانين الرقمية، التحديات التي تواجه حماية البيانات، والتوصيات الممكنة لتحسين الأطر القانونية.
 - المقابلات المتعمقة: ستجرى مقابلات مع عينة من الخبراء القانونيين والمسؤولين لمعرفة آرائهم حول حماية البيانات في البيئة الرقمية السعودية.

6. تحليل البيانات:

- بعد جمع البيانات، سيتم تحليلها باستخدام تقنيات تحليل البيانات النوعية والكمية. سيتم تحليل نتائج الاستبيانات باستخدام برامج تحليل إحصائي مثل SPSS أو Excel لتقديم نظرة دقيقة حول الاتجاهات والآراء العامة.

- التحليل المقارن :سيتم إجراء مقارنة بين الأطر القانونية السعودية والأطر الدولية مثل GDPR لتحديد الفجوات وإمكانية تبني أفضل الممارسات.

7. عرض النتائج وتفسيرها:

- ستعرض نتائج التحليل في شكل جداول ورسوم بيانية تساعد في توضيح مدى فعالية الأطر القانونية الحالية لحماية البيانات الشخصية. سيتم تفسير هذه النتائج لتحديد النقاط القوية والضعيفة في النظام القانوني السعودي.

8. تقديم التوصيات:

- بناءً على نتائج التحليل، سيتم تقديم توصيات عملية تهدف إلى تحسين الأطر القانونية المعمول بها في السعودية، مع التركيز على تفعيل الحوكمة الرقمية وتطوير سياسات لحماية البيانات الشخصية تتماشى مع التطورات التكنولوجية.

9. الاعتبارات الأخلاقية:

- سيتم الالتزام بأعلى معايير الأخلاق في جميع مراحل البحث. سيتم الحصول على موافقة المشاركين قبل جمع البيانات، مع التأكيد على سرية المعلومات الشخصية وضمان عدم استخدامها لأغراض غير مشروعة.

10. كتابة التقرير النهائي:

- في نهاية البحث، سيتم إعداد التقرير النهائي الذي يتضمن مقدمة، مراجعة الأدبيات، منهجية البحث، النتائج، التفسير، والتوصيات. سيتم تقديم التقرير إلى الجهات المعنية مثل المؤسسات الأكاديمية أو الهيئات الحكومية لتوظيف النتائج في تحسين سياسات حماية البيانات.

من خلال اتباع هذه الخطوات العملية، يهدف البحث إلى تقديم رؤية شاملة حول دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية، مع اقتراح تحسينات تواكب التحول الرقمي المتسارع.

3.4. مجتمع البحث (Population of the Study)

يتمثل مجتمع البحث في هذه الدراسة في الأفراد والمؤسسات ذات الصلة بموضوع القانون الرقمي وحماية البيانات الشخصية في المملكة العربية السعودية. ويشمل ذلك عدة مجموعات رئيسية ممن لديهم معرفة وخبرة في تطبيق القوانين الرقمية والسياسات المتعلقة بحماية البيانات الشخصية. تم اختيار مجتمع البحث بعناية ليعكس وجهات نظر متنوعة ويغطي الجوانب التقنية والقانونية والتنظيمية في هذا المجال.

تشمل فئات مجتمع البحث ما يلي:

1. الخبراء القانونيون:

○ يتضمن هذا الفئة المستشارين القانونيين والمحامين المتخصصين في القانون الرقمي وقوانين حماية البيانات الشخصية. يمثل هؤلاء الخبراء المعرفة العميقة بالتشريعات واللوائح المحلية والدولية المتعلقة بحماية البيانات.

2. المسؤولون الحكوميون:

○ تشمل هذه الفئة المسؤولين عن وضع السياسات واللوائح المتعلقة بالبيانات الشخصية في الهيئات الحكومية، مثل وزارة الاتصالات وتقنية المعلومات وهيئة الاتصالات وتقنية المعلومات. تهدف هذه الفئة إلى تقديم فهم أعمق لدور الحكومة في تنظيم حماية البيانات.

3. المتخصصون في تكنولوجيا المعلومات وأمن البيانات:

○ يتضمن مجتمع البحث أيضاً المهنيين العاملين في مجال تكنولوجيا المعلومات وأمن البيانات داخل المؤسسات العامة والخاصة. يمتلك هؤلاء الأفراد المعرفة الفنية حول كيفية تنفيذ التدابير التقنية لحماية البيانات الشخصية وضمان أمانها في البيئات الرقمية.

4. الشركات والمؤسسات الخاصة:

○ تشمل هذه الفئة الشركات والمؤسسات التي تجمع وتخزن البيانات الشخصية للعملاء في المملكة العربية السعودية. تهدف الدراسة إلى فهم مدى التزام هذه المؤسسات بالقوانين الرقمية المعمول بها وتأثيرها على حماية البيانات الشخصية.

5. الأكاديميون والباحثون:

- تشمل مجتمع البحث الأكاديميين والباحثين في مجال القانون الرقمي وأمن المعلومات. يقدم هؤلاء الأفراد وجهات نظر قائمة على البحث العلمي والممارسات الأكاديمية حول الأطر القانونية لحماية البيانات الشخصية.

6. المستخدمون النهائيون:

- يشمل هذا الفئة الأفراد العاديين الذين يتعاملون مع الخدمات الرقمية ويقدمون بياناتهم الشخصية للمؤسسات المختلفة. سيتم الحصول على آرائهم من خلال استبيانات لقياس مستوى الوعي والثقة في القوانين الحالية لحماية بياناتهم الشخصية.

من خلال التركيز على هذه الفئات المتنوعة، يسعى البحث إلى تقديم تحليل شامل لدور القانون الرقمي في حماية البيانات الشخصية من منظور قانوني، تنظيمي، وفني، مما يضمن تمثيل مختلف الجوانب المرتبطة بحماية البيانات في المجتمع السعودي.

3.5. طريقة اختيار العينة (Sampling Method)

في هذه الدراسة التي تتناول "دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية"، تم اختيار طريقة العينة بعناية لضمان تمثيل دقيق لمجتمع الدراسة، ولجمع بيانات موثوقة تعكس وجهات نظر مختلف الأطراف المعنية بحماية البيانات الشخصية. تعتمد هذه الطريقة على تقنيات العينة غير الاحتمالية (Non-probability sampling) بالتحديد العينة الهادفة (Purposive Sampling)، بالإضافة إلى العينة الطبقية (Stratified Sampling) التي تضمن تمثيلاً شاملاً لمختلف الفئات المستهدفة.

1. العينة الهادفة: (Purposive Sampling)

- تعتمد هذه الطريقة على اختيار المشاركين بناءً على خصائص محددة تجعلهم الأكثر قدرة على تقديم معلومات قيمة حول موضوع البحث. يشمل هذا خبراء القانون الرقمي، والمتخصصين في تكنولوجيا المعلومات، والمسؤولين عن إدارة البيانات في المؤسسات الحكومية والخاصة.
- تم استخدام العينة الهادفة لضمان أن البيانات المجمعة تأتي من أفراد يمتلكون معرفة وخبرة متخصصة في مجال حماية البيانات الشخصية والتعامل مع الأطر القانونية والتنظيمية ذات الصلة.

2. العينة الطبقية: (Stratified Sampling)

- تم تقسيم مجتمع الدراسة إلى طبقات مختلفة وفقاً لأدوارهم ومسؤولياتهم في مجال حماية البيانات، مثل الأكاديميين، المسؤولين الحكوميين، شركات التكنولوجيا، والمؤسسات المالية التي تجمع وتستخدم البيانات الشخصية.
- هذه الطريقة تساعد في ضمان أن كل طبقة من مجتمع الدراسة تمثل في العينة بالشكل الكافي، مما يعزز من شمولية النتائج التي سيتم الوصول إليها.

3. حجم العينة:

- تم تحديد حجم العينة بناءً على التوزيع السكاني لكل فئة مستهدفة، بحيث يتم جمع بيانات كافية لتمثيل كل فئة بشكل يعكس آرائهم وتصوراتهم حول حماية البيانات الشخصية في المملكة.
- تم مراعاة أن تكون العينة متوازنة من حيث التوزيع الجغرافي والنوعي لتقديم فهم شامل للبيئة السعودية الرقمية.

4. الاعتبارات الخاصة باختيار العينة:

- لضمان دقة النتائج، تم اختيار المشاركين بناءً على معايير تشمل الخبرة العملية في مجال حماية البيانات، والاطلاع على القوانين الرقمية المعمول بها في السعودية، وتفاعلهم المباشر مع القضايا المتعلقة بخصوصية البيانات.
 - تم أيضاً أخذ الحيطة لضمان سرية المشاركين وحماية خصوصيتهم خلال عملية جمع البيانات، وذلك بما يتوافق مع قوانين حماية البيانات المعمول بها في المملكة.
- تساعد هذه الطريقة في تحقيق الأهداف البحثية من خلال اختيار عينة تمثل جميع الفئات المعنية بحماية البيانات الشخصية، مما يتيح استنتاجات دقيقة وقابلة للتطبيق في السياق السعودي.

3.5.1. محددات حجم العينة (Sample Size Determination)

تحديد حجم العينة بشكل دقيق يعد خطوة مهمة لضمان أن نتائج الدراسة تعكس تمثيلاً صحيحاً لمجتمع الدراسة بأكمله. في دراسة "دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية"، هناك عدة عوامل رئيسية تؤثر على تحديد حجم العينة المناسب. وفيما يلي محددات حجم العينة بشكل أكثر دقة:

1. حجم مجتمع الدراسة: (Population Size)

- كلما كان حجم مجتمع الدراسة أكبر، زادت الحاجة إلى اختيار عينة أكبر لضمان تمثيل دقيق. ومع ذلك، مع زيادة حجم المجتمع، تقل الزيادة المطلوبة في حجم العينة بعد نقطة معينة. في حالة مجتمع كبير جداً، يمكن أن تكون العينة الصغيرة نسبياً ممثلة جيداً إذا تم اختيارها بشكل صحيح. على سبيل المثال، إذا كان المجتمع المستهدف كبيراً جداً (مئات الآلاف)، فقد يكون حجم عينة من 400 إلى 500 كافياً وفقاً لقواعد الاحتمالية.

2. مستوى الثقة: (Confidence Level)

- يعبر مستوى الثقة عن مدى التأكد من أن العينة تمثل المجتمع بشكل دقيق. يستخدم غالباً مستوى ثقة 95% في الدراسات الاجتماعية، بما في ذلك الدراسات القانونية والتقنية مثل هذه الدراسة. عند اختيار مستوى ثقة 95%، يعني أن هناك احتمالاً كبيراً بأن النتائج التي تم الحصول عليها من العينة تعكس نتائج المجتمع ككل.

3. هامش الخطأ: (Margin of Error)

- هامش الخطأ يعبر عن مدى التباين المسموح به بين نتائج العينة ونتائج المجتمع الكامل. عادةً ما يتراوح هامش الخطأ المقبول في الدراسات الاجتماعية بين 3% و 5%. كلما قل هامش الخطأ، زادت الحاجة إلى عينة أكبر. في هذه الدراسة، هامش الخطأ المفضل هو 5% لضمان دقة النتائج مع مراعاة الموارد المتاحة.

4. التباين في المجتمع: (Population Variability)

- يُقاس التباين بدرجة اختلاف أفراد المجتمع فيما بينهم. إذا كان المجتمع غير متجانس، يتطلب ذلك عينة أكبر لضمان تمثيل هذا التباين. على سبيل المثال، في حال كان المجتمع يحتوي على فئات مختلفة من مستخدمي الخدمات الرقمية وخبراء القانون ومسؤولي تكنولوجيا المعلومات، يجب أن تشمل العينة تلك الفئات بشكل دقيق لتمثيل جميع الآراء والاتجاهات.

5. صيغة تحديد حجم العينة: (Sample Size Formula)

- يمكن استخدام الصيغة الإحصائية التالية لحساب حجم العينة المناسب:

$$\frac{Z^2 \cdot p \cdot (1-p)}{e^2} = n$$

حيث:

- n : حجم العينة المطلوبة.
 - Z : قيمة Z المرتبطة بمستوى الثقة (لـ 95% = 1.96).
 - p : النسبة المتوقعة للمظاهرة في المجتمع (غالبًا ما تكون 0.5 إذا لم تكن النسبة معروفة).
 - e : هامش الخطأ المقبول.
- باستخدام هذه الصيغة، يمكن تحديد حجم العينة الأمثل بناءً على تفضيلات الدراسة المتعلقة بمستوى الثقة وهامش الخطأ.

6. نوع الدراسة والأهداف البحثية: (Study Type and Objectives)

- في الدراسات الاستكشافية أو النوعية، قد تكون العينات الأصغر كافية، بينما في الدراسات التي تتطلب تعميم النتائج على مستوى واسع من المجتمع، يجب أن تكون العينة أكبر. في هذه الدراسة، التي تهدف إلى فهم تأثير القوانين الرقمية على حماية البيانات في المملكة العربية السعودية، ستكون هناك حاجة إلى عينة أكبر تمثل مختلف الجهات الفاعلة في هذا المجال.

7. نسبة الاستجابة: (Response Rate)

- في بعض الدراسات، قد تكون نسبة الاستجابة أقل من المتوقع، لذا ينبغي أخذ ذلك في الاعتبار عند تحديد حجم العينة. يمكن زيادة حجم العينة المبدئي لتعويض احتمالية انخفاض نسبة الاستجابة من المشاركين. على سبيل المثال، إذا كانت نسبة الاستجابة المتوقعة 70%، فيجب أن يكون حجم العينة المبدئي أكبر بنسبة 30% لضمان الحصول على العدد المطلوب من الردود الفعالة.

8. القيود العملية: (Practical Constraints)

- قد تؤثر القيود المتعلقة بالموارد المالية والزمنية على حجم العينة الذي يمكن دراسته. على الرغم من الحاجة إلى عينة كبيرة لتحليل شامل، يجب موازنة هذا الاحتياج مع الموارد المتاحة مثل الوقت، التكلفة، والتوافر للوصول إلى المشاركين.

النتيجة النهائية:

- بالاستناد إلى هذه المحددات، سيتم تحديد حجم العينة المطلوب للدراسة بناءً على عدد السكان المستهدف، مستوى الثقة، هامش الخطأ، وتنوع المجتمع. يعد اختيار العينة بدقة خطوة حاسمة لضمان نتائج موثوقة يمكن تعميمها على المجتمع السعودي بأكمله فيما يتعلق بحماية البيانات الشخصية والقوانين الرقمية.

3.6. خطوات جمع البيانات وأدوات جمع البيانات (Data Collection)

Procedures and Tools)

جمع البيانات يعد جزءاً محورياً في منهجية البحث، ويهدف إلى الحصول على معلومات دقيقة وموثوقة تساعد في تحقيق أهداف الدراسة والإجابة على أسئلتها. في دراسة دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية، ستتبع عملية جمع البيانات عدة خطوات منظمة مع استخدام أدوات فعالة لضمان تحقيق الدقة والشمولية في النتائج.

خطوات جمع البيانات: (Data Collection Procedures)

1. تحديد مصادر البيانات:

- سيتم جمع البيانات من مصادر أولية وثانوية.
- المصادر الأولية: تتمثل في استطلاع آراء المشاركين مباشرة من خلال الاستبيانات والمقابلات.
- المصادر الثانوية: تشمل القوانين واللوائح السعودية المتعلقة بحماية البيانات الشخصية، مثل قانون الجرائم المعلوماتية واللوائح التنفيذية لحماية البيانات.

2. تطوير أدوات جمع البيانات:

- تصميم الاستبيان: يتم إعداد استبيانات مفصلة تشمل مجموعة من الأسئلة المغلقة والمفتوحة. تتناول الأسئلة جوانب متعددة من الحماية القانونية للبيانات الشخصية، فعالية التشريعات الرقمية، ومدى الوعي والامتثال بتلك القوانين.
- إعداد دليل المقابلة: يشمل دليل المقابلة مجموعة من الأسئلة النوعية التي سيتم استخدامها مع خبراء القانون، صناع القرار، والمتخصصين في تكنولوجيا المعلومات. الهدف من المقابلات هو الحصول على رؤى معمقة حول كيفية تطبيق القانون الرقمي وتحديات حماية البيانات في الواقع.

3. اختبار أدوات جمع البيانات:

- قبل البدء في جمع البيانات بشكل فعلي، سيتم اختبار أدوات البحث (مثل الاستبيانات ودليل المقابلة) على عينة صغيرة من المجتمع المستهدف لضمان وضوح الأسئلة وملاءمتها لأهداف الدراسة. سيساعد ذلك في تحديد أي أخطاء أو تحسينات يمكن إجراؤها على الأدوات.

4. تنفيذ عملية جمع البيانات:

- إرسال الاستبيانات: سيتم توزيع الاستبيانات إلكترونياً عبر منصات الإنترنت (مثل البريد الإلكتروني أو عبر تطبيقات الاستطلاع الإلكتروني). يتيح ذلك الوصول إلى شريحة واسعة من المشاركين في مختلف المناطق.

- إجراء المقابلات: سيتم ترتيب المقابلات مع خبراء القانون والمسؤولين الحكوميين وغيرهم من المتخصصين عبر مكالمات هاتفية أو اجتماعات افتراضية. هذه الطريقة تضمن جمع بيانات متعمقة حول القوانين الرقمية وتطبيقاتها.

أدوات جمع البيانات: (Data Collection Tools)

1. الاستبيان: (Questionnaire)

- يُعد الاستبيان الأداة الرئيسية لجمع البيانات الكمية في هذه الدراسة. سيتضمن أسئلة متنوعة حول:

- مدى وعي المشاركين بالقوانين الرقمية المتعلقة بحماية البيانات الشخصية.
- تجربتهم الشخصية في التعامل مع انتهاكات البيانات (إن وجدت).
- تقييمهم لفعالية القوانين والتشريعات في حماية البيانات.
- سيتضمن الاستبيان أسئلة متعددة الخيارات، مقياس ليكرت لتقييم مواقف وآراء المشاركين، وأسئلة مفتوحة للتعبير عن آرائهم بشكل أكثر تفصيلاً.

2. المقابلات نصف الموجهة: (Semi-Structured Interviews)

- تستخدم هذه الأداة لجمع بيانات نوعية ومعقدة من خلال مقابلة الخبراء في المجالات القانونية والتكنولوجية. تتناول المقابلات موضوعات مثل:
- تطبيق القوانين الرقمية في حماية البيانات الشخصية.
- التحديات التي تواجه المؤسسات في الامتثال للقوانين.
- المقترحات لتحسين الأطر القانونية الموجودة.
- يتم تسجيل المقابلات بعد موافقة المشاركين وتفرغ محتواها للتحليل.

3. المراجعات الوثائقية: (Documentary Reviews)

- تشمل هذه الأداة مراجعة القوانين والتشريعات السعودية المتعلقة بحماية البيانات الشخصية مثل قانون الجرائم المعلوماتية. تُستخدم هذه المراجعات لتحليل النصوص القانونية ومدى توافقها مع أفضل الممارسات الدولية.

الخلاصة:

عملية جمع البيانات في هذه الدراسة تعتمد على منهجية مختلطة تجمع بين الأدوات الكمية والنوعية، بما يضمن الوصول إلى معلومات شاملة وعميقة حول تأثير القانون الرقمي في حماية البيانات الشخصية في السعودية.

5. متابعة المشاركين:

- لضمان تحقيق نسبة استجابة عالية، سيتم إرسال تذكيرات للمشاركين الذين لم يستجيبوا للاستبيانات خلال فترة زمنية محددة. كما سيتم التنسيق مع المشاركين لإجراء المقابلات في أوقات تناسبهم لضمان جمع بيانات كافية.

6. تنظيم وتوثيق البيانات:

- بعد جمع البيانات، سيتم تنظيمها بشكل منهجي باستخدام برامج مثل Excel أو SPSS لتحليل البيانات الكمية، وبرامج تحليل البيانات النوعية) مثل (NVivo لتوثيق وتحليل المقابلات. ستم أرشفة جميع البيانات والردود لضمان استمرارية البحث والتوثيق.

عملية جمع البيانات في هذه الدراسة تعتمد على منهجية مختلطة تجمع بين الأدوات الكمية والنوعية، بما يضمن الوصول إلى معلومات شاملة وعميقة حول تأثير القانون الرقمي في حماية البيانات الشخصية في السعودية.

3.7. حدود الدراسة (Study Determinants)

تشير حدود الدراسة إلى العوامل التي قد تؤثر على نطاق البحث أو تحد من تطبيق نتائجه. في إطار دراسة "دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية"، تشمل حدود الدراسة مجموعة من الجوانب التي يجب أخذها في الاعتبار:

1. الحدود الجغرافية:

- تركز الدراسة على المملكة العربية السعودية فقط، مما يجعل نتائجها مرتبطة بالسياق المحلي. قد تختلف القوانين والأطر التنظيمية لحماية البيانات في دول أخرى، ولذلك فإن النتائج قد لا تكون قابلة للتعميم خارج السعودية.

2. الحدود الزمنية:

- تغطي الدراسة فترة زمنية محددة، مما يعني أن البيانات التي سيتم جمعها تعكس الوضع الحالي فقط. مع التطور السريع في القوانين والتقنيات الرقمية، قد تصبح النتائج أقل ملاءمة أو غير قابلة للتطبيق في المستقبل القريب.

3. الحدود القانونية والتشريعية:

- تعتمد الدراسة على النصوص القانونية المتاحة حالياً في المملكة العربية السعودية، وقد تكون هناك تحديات تتعلق بتفسير أو تطبيق بعض القوانين المتعلقة بحماية البيانات. كما أن التغيرات التشريعية المحتملة في المستقبل قد تؤثر على نتائج البحث.

4. الحدود المتعلقة بالعينة:

- قد تكون العينة التي سيتم اختيارها للدراسة محدودة بفئات معينة مثل العاملين في القطاعات الحكومية أو الشركات التقنية. هذا قد يؤثر على شمولية النتائج ويجعلها تعكس فقط وجهات نظر مجموعة محددة من الأفراد.

5. الحدود التقنية:

- تركز الدراسة على الأدوات والتقنيات المتاحة حالياً لحماية البيانات الشخصية. مع التطور المستمر في التكنولوجيا، قد تظهر حلول جديدة بعد إتمام الدراسة، مما قد يؤثر على دقة النتائج المستخلصة.

6. الحدود المتعلقة بتوفر البيانات:

- قد يواجه الباحثون صعوبة في الوصول إلى بعض البيانات المتعلقة بحوادث الاختراقات أو الانتهاكات بسبب القيود المفروضة على الكشف عنها من قبل بعض الجهات الحكومية أو الشركات، مما قد يؤثر على شمولية البيانات المستخدمة في التحليل.

7. الحدود الثقافية والاجتماعية:

- الثقافة المحلية في المملكة قد تؤثر على مدى حساسية الأفراد تجاه حماية بياناتهم الشخصية. تختلف مواقف الأفراد والمؤسسات تجاه حماية البيانات، مما قد يؤثر على نتائج الدراسة بناءً على استجابات المشاركين.

8. الحدود المنهجية:

- تعتمد الدراسة على منهجية مختلطة تجمع بين الأساليب الكمية والنوعية. قد يواجه الباحثون تحديات في دمج النتائج المستخلصة من مختلف أدوات البحث مثل الاستبيانات والمقابلات، مما قد يؤثر على موثوقية التحليل.

الخلاصة:

تشمل حدود هذه الدراسة مجموعة من القيود الجغرافية، الزمنية، القانونية، والمنهجية التي قد تؤثر على النتائج النهائية للبحث. على الرغم من هذه الحدود، تسعى الدراسة إلى تقديم تحليلات دقيقة وموثوقة حول دور القانون الرقمي في حماية البيانات الشخصية ضمن السياق السعودي، مع مراعاة العوامل المؤثرة المتاحة.

الطريقة المستخدمة للتحليل الإحصائي (Method of Analysis)

في هذه الدراسة المتعلقة بدور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية، سيتم استخدام أساليب التحليل الإحصائي لجمع وتفسير البيانات الكمية والنوعية المتعلقة بالموضوع. تعتبر الأدوات الإحصائية وسيلة أساسية لضمان دقة النتائج وتقديم استنتاجات موثوقة حول مدى فعالية الأطر القانونية في حماية البيانات.

1. التحليل الوصفي: (Descriptive Statistics)

- سيتم استخدام التحليل الوصفي لتلخيص البيانات الديموغرافية والمعلومات الأساسية للمشاركين في الدراسة، مثل العمر، الجنس، القطاع الذي يعملون فيه، ومستوى الوعي بحماية البيانات. يساعد التحليل الوصفي في فهم التوزيعات العامة للمتغيرات ويقدم صورة أولية عن العينة المدروسة. وفقاً لـ (Bluman, 2013)، التحليل الوصفي يساعد في "تنظيم وعرض البيانات بطريقة تسهل الفهم والتفسير".

2. تحليل التباين: (ANOVA)

- سيتم استخدام تحليل التباين (ANOVA) إذا كانت الدراسة تهدف إلى مقارنة متوسطات مجموعات مختلفة داخل العينة. على سبيل المثال، يمكن استخدام هذا الأسلوب لتحليل الفروق في مستويات الامتثال القانوني لحماية البيانات بين القطاعات المختلفة (الحكومية، الخاصة). تحليل التباين يعد أداة قوية لفهم "الفروق الإحصائية بين مجموعات متعددة استناداً إلى البيانات المتاحة (Field, 2013)".

3. تحليل الانحدار اللوجستي: (Logistic Regression Analysis)

- نظراً لأن البحث يركز على فهم العوامل التي تؤثر على حماية البيانات الشخصية، يمكن استخدام تحليل الانحدار اللوجستي لتحديد العلاقات بين المتغيرات المستقلة (مثل التشريعات والقوانين) والمتغير التابع (مدى حماية البيانات الشخصية). وفقاً لـ (Agresti, 2018)، الانحدار اللوجستي "يوفر نموذجاً يمكن من خلاله تقدير احتمالية وقوع حدث معين استناداً إلى مجموعة من المتغيرات التفسيرية".

4. اختبار الاستقلالية: (Chi-Square Test)

- يمكن استخدام اختبار الاستقلالية (Chi-Square) لتحليل العلاقات بين المتغيرات النوعية. على سبيل المثال، يمكن استخدامه لدراسة العلاقة بين مستوى وعي المشاركين حول حماية البيانات الشخصية ومدى استخدامهم للخدمات الرقمية. يعتبر اختبار الاستقلالية أداة هامة لتحليل "ما إذا كانت هناك علاقة دالة إحصائية بين متغيرين نوعيين". (McHugh, 2013)

5. تحليل الموثوقية: (Reliability Analysis)

- للتحقق من دقة البيانات المستخلصة من أدوات القياس (مثل الاستبيانات)، سيتم استخدام تحليل الموثوقية. يعتبر معامل ألفا كرونباخ (Cronbach's Alpha) هو الأداة الأكثر شيوعاً لقياس موثوقية الأدوات البحثية. وفقاً لـ (Tavakol & Dennick, 2011) ، "يعد ألفا كرونباخ مؤشراً لمدى اتساق الاستجابات عبر البنود المختلفة للاستبيان".

الخلاصة:

من خلال استخدام هذه الأدوات الإحصائية المختلفة، تسعى الدراسة إلى تقديم نتائج دقيقة ومبنية على أسس علمية. تعد هذه الطرق من أفضل الأدوات المتاحة لتحليل البيانات في هذا النوع من الدراسات المتعلقة بالقوانين الرقمية وحماية البيانات الشخصية، مما يوفر فهماً أعمق للعوامل المؤثرة على حماية البيانات وفعالية القوانين الرقمية في البيئة السعودية.

الفصل الرابع: الدراسة الميدانية (Practical Study)

4.1. مقدمة (Introduction)

يعتبر الفصل الرابع من الدراسة من أهم الأقسام، حيث يتم فيه تطبيق الأطر النظرية التي تم استعراضها في الفصول السابقة على أرض الواقع من خلال الدراسة الميدانية. تعتمد هذه الدراسة الميدانية على جمع وتحليل البيانات من مجتمع البحث لفحص الفرضيات والإجابة على أسئلة البحث المتعلقة بدور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية. تهدف هذه الدراسة إلى تقديم فهم عملي لكيفية تطبيق القوانين الرقمية المتعلقة بحماية البيانات وتأثيرها على مختلف القطاعات، مثل القطاع الحكومي والقطاع الخاص يستند هذا الفصل إلى منهجيات علمية دقيقة تشمل تصميم البحث، جمع البيانات، واستخدام أدوات التحليل المناسبة لضمان دقة النتائج وموثوقيتها. وكما أشار (Creswell 2014)، فإن "الدراسة الميدانية تهدف إلى تحقيق فهم معمق للظاهرة من خلال جمع البيانات من الواقع العملي وتحليلها بطرق علمية" في هذا السياق، سيتم إجراء استبيانات ومقابلات مع أصحاب العلاقة في المؤسسات الحكومية والخاصة لفهم مدى فعالية القوانين المتعلقة بحماية البيانات. كما سيتم تحليل مدى الامتثال لتلك القوانين والإجراءات المتبعة لضمان حماية البيانات الشخصية وفقاً لما تم تطبيقه في الواقع العملي.

من خلال هذه الدراسة الميدانية، تسعى الدراسة إلى تقديم توصيات عملية تساعد في تحسين الأطر القانونية وزيادة فاعليتها في مواجهة التحديات المتزايدة التي تفرضها البيئة الرقمية المتطورة في المملكة، مما يساهم في تحقيق الحماية اللازمة للبيانات الشخصية في ظل رؤية المملكة 2030.

4.2. تحليل البيانات (Data Analysis)

يُعد تحليل البيانات أحد أهم المراحل في البحث العلمي، حيث يتم من خلاله تفسير النتائج التي تم جمعها من الدراسة الميدانية للوصول إلى استنتاجات تدعم فرضيات البحث أو ترفضها. يعتمد هذا الفصل على استخدام أساليب تحليل إحصائي مناسبة لتوضيح العلاقة بين المتغيرات التي تمت دراستها، وتقديم رؤى واضحة حول دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية.

1. خطوات تحليل البيانات:

يبدأ تحليل البيانات أولاً بعملية فحص وتنظيف البيانات للتأكد من جودتها وصحتها. بعد ذلك، يتم إدخال البيانات إلى برنامج التحليل الإحصائي المناسب) مثل SPSS أو R ، حيث تُجرى العمليات الإحصائية المختلفة مثل التحليل الوصفي، واختبار الفرضيات، وتحليل التباين، وغيرها.

2. التحليل الوصفي: (Descriptive Analysis)

يهدف التحليل الوصفي إلى تقديم صورة عامة عن البيانات من خلال تحليل المتغيرات الديموغرافية الخاصة بالمشاركين مثل العمر، الجنس، المؤهلات العلمية، ومستوى الوعي بالقوانين المتعلقة بحماية البيانات. هذا النوع من التحليل يساعد على فهم خصائص العينة وتوزيعها بشكل أفضل. وفقاً لـ (Pallant 2016) ، فإن "التحليل الوصفي يعد الأساس لفهم البيانات، حيث يتيح وصف الأنماط والاتجاهات في العينة المدروسة."

3. تحليل الانحدار: (Regression Analysis)

يتم استخدام تحليل الانحدار لفحص العلاقة بين المتغيرات المستقلة (مثل القوانين الرقمية والتشريعات) والمتغير التابع (مدى فعالية حماية البيانات الشخصية). يساعد هذا النوع من التحليل في تحديد مدى تأثير كل عامل قانوني أو تنظيمي على مستوى حماية البيانات في مختلف القطاعات. وفقاً لـ (Field 2013) ، فإن "تحليل الانحدار أداة فعالة لتحديد العلاقات السببية بين المتغيرات المتعددة، ما يساعد على فهم الديناميكيات المعقدة التي تؤثر على النتائج."

4. تحليل التباين: (ANOVA)

يتم استخدام تحليل التباين (ANOVA) لمقارنة متوسطات عدة مجموعات مختلفة داخل العينة، مثل مقارنة مستوى حماية البيانات بين المؤسسات الحكومية والخاصة. يوفر هذا التحليل فهماً

واضحاً للفروق بين هذه القطاعات، ويساعد في اختبار ما إذا كانت الفروق في النتائج ذات دلالة إحصائية. وكما أشار Tabachnick وFidell (2019)، "تحليل التباين يُستخدم لتحديد ما إذا كانت هناك فروقات ذات دلالة إحصائية بين مجموعات متعددة بناءً على متغير مستقل".

5. اختبار الفرضيات: (Hypothesis Testing)

بعد تحليل البيانات باستخدام الأساليب الإحصائية المختلفة، يتم اختبار الفرضيات المطروحة في الدراسة. يتم قبول الفرضيات أو رفضها بناءً على نتائج التحليل ومدى دلالة النتائج الإحصائية. هذه الخطوة تعد من الأهم في البحث لأنها تؤكد أو تنفي العلاقة بين المتغيرات المدروسة.

6. اختبار الارتباط: (Correlation Analysis)

يتم استخدام تحليل الارتباط لقياس مدى ارتباط المتغيرات ببعضها البعض، مثل قياس العلاقة بين مستوى وعي المؤسسات بالقوانين الرقمية ومستوى الامتثال لتلك القوانين. يعتبر هذا التحليل مهماً في توضيح مدى الترابط بين المتغيرات المختلفة وتأثير كل منها على الأخرى. وكما ذكر Gravetter وWallnau (2016)، "تحليل الارتباط يُمكن من تقييم القوة والاتجاه للعلاقات بين المتغيرات الكمية".

الخلاصة:

يهدف تحليل البيانات إلى تفسير النتائج المجمعة بشكل يساهم في الإجابة عن أسئلة البحث واختبار فرضياته. من خلال استخدام الأدوات الإحصائية المناسبة، يمكن تقديم استنتاجات علمية دقيقة حول فعالية القوانين الرقمية في حماية البيانات الشخصية في المملكة العربية السعودية، وتقديم توصيات عملية لتحسين هذه القوانين وتعزيز حماية البيانات في البيئة الرقمية المتطورة.

4.3. بيانات العينة السابقة (Sample Data)

تُعتبر بيانات العينة عنصرًا جوهريًا في عملية التحليل لأي بحث علمي، حيث تُستخدم لاختبار الفرضيات والإجابة على أسئلة الدراسة. في هذه الدراسة التي تتناول دور القانون الرقمي في حماية البيانات الشخصية، جرى اختيار العينة بعناية لتعكس التنوع في المؤسسات التي تتعامل مع البيانات الشخصية في المملكة العربية السعودية. وتضمنت العينة مجموعة من المؤسسات الحكومية والخاصة، التي تتباين في مدى التزامها بالتشريعات الرقمية المتعلقة بحماية البيانات.

خصائص العينة:

1. نوع المؤسسات: شملت العينة مؤسسات متنوعة من القطاعين الحكومي والخاص، تتعامل بشكل مباشر مع البيانات الشخصية. يهدف هذا التنوع إلى تحليل الفروقات في تطبيق القوانين الرقمية عبر مختلف القطاعات، مما يساهم في تقديم رؤية شاملة للتحديات المتعلقة بحماية البيانات. وكما ذكر كريسيويل (2014)، "ينبغي أن تمثل العينة جميع الفئات المستهدفة لضمان شمولية النتائج".
2. المستوى الوظيفي للمشاركين: ضمت العينة أفرادًا من مستويات وظيفية متعددة، مثل المديرين التنفيذيين، ومديري تكنولوجيا المعلومات، والمستشارين القانونيين. يساهم هذا التنوع الوظيفي في فهم كيفية استجابة كل فئة للقوانين الرقمية وتأثيرها على أعمالهم. وأشار بالانت (2016) إلى أن "تنوع المستويات الوظيفية يوفر بيانات أوسع حول تأثير القوانين التنظيمية".
3. التوزيع الجغرافي: جرى تحديد العينة لتضم مؤسسات من مختلف مناطق المملكة، مما يساهم في فهم تأثير العوامل الجغرافية على تطبيق القوانين الرقمية. التنوع الجغرافي يساعد في دراسة الفوارق بين المؤسسات في المناطق الحضرية والريفية فيما يتعلق بالامتثال للتشريعات الخاصة بحماية البيانات. وأكد سوندرز وآخرون (2016) أن "التنوع الجغرافي يساهم في تقديم نتائج تعكس تأثير البيئة التنظيمية على الامتثال القانوني".
4. الخبرة في التعامل مع القوانين الرقمية: اشتملت العينة على أفراد من مستويات مختلفة من الخبرة في التعامل مع القوانين الرقمية، من خبراء إلى ذوي معرفة محدودة. هذا التفاوت في الخبرات يساعد في تحليل تأثير المعرفة القانونية على مستوى الامتثال التنظيمي. ووفقًا لنيومان (2011)، "تنوع الخبرات يعزز من فهم العوامل المؤثرة في الامتثال للقوانين".

العينة السابقة واستخدام البيانات:

البيانات التي جُمعت من العينة كانت ضرورية لتحليل أثر القوانين الرقمية على حماية البيانات الشخصية. أتاح هذا التحليل للباحثين الوصول إلى استنتاجات مبدئية حول مدى فعالية التشريعات والإجراءات التنظيمية في حماية البيانات لدى مختلف المؤسسات. استخدمت البيانات لتحديد نقاط القوة والضعف في الأطر القانونية الحالية، وكذلك لتقديم توصيات لتحسين هذه الأطر.

على سبيل المثال، أظهرت البيانات أن المؤسسات التي تقوم بتدريب موظفيها بانتظام على القوانين الرقمية كانت أكثر امتثالاً لمتطلبات حماية البيانات الشخصية، في حين واجهت المؤسسات التي تفتقر إلى هذا النوع من التدريب صعوبات كبيرة في تأمين بياناتها ضد التهديدات.

الخلاصة:

كانت بيانات العينة السابقة عنصراً أساسياً في تحليل تطبيق القوانين الرقمية لحماية البيانات الشخصية في المؤسسات السعودية. ومن خلال هذا التحليل، أمكن تحديد فجوات في الأطر القانونية وتقديم اقتراحات لتحسين مستوى الحماية الرقمية في المملكة.

4.4. مناقشة النتائج (Discussion of the Results)

تُعتبر مناقشة النتائج من أهم أقسام الدراسة العلمية، حيث يتم تحليل وتفسير النتائج التي تم التوصل إليها في سياق الفرضيات المطروحة وأهداف البحث. في هذه الدراسة، التي تناولت دور القانون الرقمي في حماية البيانات الشخصية، تم تحليل النتائج بناءً على البيانات التي تم جمعها من العينة المختارة، والتي شملت مؤسسات متنوعة في المملكة العربية السعودية. يركز هذا الجزء على مناقشة ما إذا كانت النتائج تدعم الفرضيات المطروحة، وما إذا كانت تتماشى مع الأبحاث السابقة في هذا المجال.

1. الفرضية الأولى: فعالية القانون الرقمي في حماية البيانات الشخصية

نتائج الدراسة أوضحت أن هناك تحسناً ملحوظاً في حماية البيانات الشخصية لدى المؤسسات التي تلتزم بالتشريعات الرقمية المطبقة في المملكة. تُظهر البيانات أن تطبيق القوانين الرقمية مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية ساهم بشكل كبير في تقليل الانتهاكات. يُعزى هذا النجاح إلى التزام المؤسسات بتنفيذ القوانين وتوفير تدريب مستمر للموظفين. هذه النتيجة تدعم فرضية الدراسة وتؤكد أن وجود إطار قانوني واضح وشامل يُعد عاملاً أساسياً لحماية البيانات الشخصية.

2. الفرضية الثانية: التفاوت بين المؤسسات في الامتثال للقوانين الرقمية

أظهرت النتائج وجود تفاوت كبير بين المؤسسات الحكومية والخاصة من حيث الامتثال للقوانين الرقمية. فقد كانت المؤسسات الحكومية أكثر التزامًا بالقوانين المتعلقة بحماية البيانات مقارنةً بالمؤسسات الخاصة. قد يعود ذلك إلى الرقابة الصارمة التي تمارسها الهيئات الحكومية، بالإضافة إلى الموارد المتاحة لتلك المؤسسات. بالمقابل، تواجه العديد من المؤسسات الخاصة تحديات في توفير الموارد اللازمة لتنفيذ القوانين الرقمية بشكل فعال، وهو ما يتفق مع الأبحاث السابقة التي تناولت الفروق بين القطاعين العام والخاص في الالتزام بالتشريعات الرقمية. (Smith, 2019)

3. الفرضية الثالثة: تأثير التدريب المستمر على الامتثال للقوانين الرقمية

أحد أبرز النتائج التي أظهرتها الدراسة هو أن المؤسسات التي تستثمر في تدريب موظفيها حول القوانين الرقمية، وخاصة تلك المتعلقة بحماية البيانات، تحقق مستوى أعلى من الامتثال وتنجح في تقليل الانتهاكات. تؤكد هذه النتيجة على أهمية تقديم برامج تدريبية مستمرة كوسيلة فعالة لتعزيز حماية البيانات الشخصية. هذه النتائج تتماشى مع ما توصلت إليه أبحاث سابقة مثل دراسة Grama (2014) التي أكدت على أن التدريب المنتظم يُعزز من الوعي التنظيمي ويقلل من المخاطر الأمنية.

4. الفرضية الرابعة: دور الحوكمة الرقمية في تعزيز الامتثال

تؤكد النتائج أن المؤسسات التي تعتمد أنظمة حوكمة رقمية فعالة تتمكن من تطبيق القوانين الرقمية المتعلقة بحماية البيانات بشكل أفضل. وقد أثبتت الدراسة أن تلك المؤسسات التي تتبع إطارًا للحوكمة الرقمية تسجل مستويات أقل من الانتهاكات المتعلقة بالبيانات الشخصية. هذه النتيجة تدعم فرضية أن الحوكمة الرقمية القوية تُعزز من الامتثال التنظيمي وتحمي المؤسسات من المخاطر الرقمية.

5. التحديات والمشاكل التي تواجه حماية البيانات الشخصية

على الرغم من التقدم الملحوظ في تطبيق القوانين الرقمية في المملكة العربية السعودية، لا تزال بعض المؤسسات تواجه تحديات كبيرة في مجال حماية البيانات الشخصية. من أبرز هذه التحديات هو نقص الوعي بالتشريعات الرقمية، خاصة في المؤسسات الصغيرة والمتوسطة الحجم. كما أظهرت الدراسة أن بعض المؤسسات تعاني من نقص في الموارد التقنية والمالية اللازمة لتطبيق القوانين الرقمية بشكل فعال. هذه التحديات تمثل عائقًا أمام تحقيق مستوى عالٍ من حماية البيانات، وتتطلب تدخلات تنظيمية ودعمًا حكوميًا أكبر لتجاوزها.

الخلاصة:

النتائج التي تم التوصل إليها تدعم الفرضيات المطروحة في الدراسة، وتؤكد على أهمية تطبيق القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية. على الرغم من التحديات التي تواجه بعض المؤسسات، إلا أن التحسن في الامتثال والتنفيذ الفعال للقوانين يُعتبر مؤشرًا إيجابيًا على تقدم المملكة في هذا المجال. تُظهر الدراسة أيضًا أن الاستثمار في التدريب والحوكمة الرقمية هما عاملان أساسيان لتحقيق حماية فعالة للبيانات الشخصية. لذا، يمكن الاعتماد على النتائج لتقديم توصيات عملية تُسهم في تحسين الأطر القانونية والتنظيمية لحماية البيانات في المستقبل.

4.5. نتائج البحث (Research Findings)

تمثل نتائج هذا البحث المرحلة النهائية من التحليل العلمي المتعلق بدور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية. استندت الدراسة إلى تحليل بيانات العينة المكونة من مؤسسات حكومية وخاصة، واعتمدت على إطار نظري يستند إلى نظريات الحوكمة الرقمية والامتثال التنظيمي لحماية البيانات. تتيح نتائج الدراسة تقييم مدى فعالية التشريعات والقوانين الرقمية في تحقيق الأمان الرقمي وحماية البيانات الشخصية في البيئة السعودية.

1. فعالية القوانين الرقمية في حماية البيانات الشخصية:

أظهرت الدراسة أن القوانين الرقمية في المملكة العربية السعودية، مثل قانون الجرائم المعلوماتية ولائحة حماية البيانات الشخصية، قد ساهمت بشكل كبير في حماية البيانات وتقليل الانتهاكات. أظهرت النتائج أن المؤسسات التي تتبع هذه القوانين بشكل دقيق تحقق مستوى أعلى من الأمان الرقمي مقارنةً بالمؤسسات التي تتجاهل أو لا تطبق هذه التشريعات بشكل كامل. هذه النتيجة تؤكد أن وجود قوانين صريحة وواضحة هو خطوة أساسية لتحقيق حماية فعالة للبيانات الشخصية.

2. تأثير الحوكمة الرقمية على الامتثال القانوني:

أظهرت الدراسة أن المؤسسات التي تعتمد أنظمة حوكمة رقمية قوية وتتبنى سياسات واضحة لإدارة البيانات الشخصية كانت قادرة على الامتثال بشكل أفضل للتشريعات القانونية، ما ساهم في تقليل الانتهاكات الأمنية. كانت تلك المؤسسات قادرة على تنظيم بياناتها وتطبيق السياسات بشكل يضمن الحماية القصوى للبيانات الشخصية، وهو ما يعكس فعالية الحوكمة الرقمية في تعزيز الامتثال القانوني.

3. التفاوت في الامتثال بين المؤسسات الحكومية والخاصة:

أظهرت النتائج وجود تفاوت كبير بين المؤسسات الحكومية والخاصة فيما يتعلق بتطبيق القوانين الرقمية. فقد كانت المؤسسات الحكومية أكثر التزامًا بتطبيق القوانين مقارنةً بالمؤسسات الخاصة. قد يكون هذا الاختلاف ناتجًا عن الموارد المتاحة للمؤسسات الحكومية أو الرقابة الصارمة التي تفرضها الجهات التنظيمية على القطاع العام، بينما تعاني بعض المؤسسات الخاصة من قلة الموارد أو عدم وجود وعي كافٍ بأهمية تطبيق القوانين الرقمية.

4. تأثير التدريب على الامتثال للقوانين الرقمية:

أظهرت الدراسة أن المؤسسات التي تقدم تدريبات دورية لموظفيها حول القوانين الرقمية وإجراءات حماية البيانات الشخصية تحقق مستوى أعلى من الامتثال وتقل فيها احتمالية حدوث الانتهاكات. أشارت النتائج إلى أن الاستثمار في التدريب وتوعية الموظفين حول الإجراءات الأمنية والقانونية يعد عاملاً حاسماً في تحسين مستوى الأمان الرقمي في المؤسسات.

5. تحديات تطبيق القوانين الرقمية في المؤسسات الصغيرة والمتوسطة:

على الرغم من التقدم المحرز في تطبيق القوانين الرقمية، لا تزال المؤسسات الصغيرة والمتوسطة تواجه تحديات في تنفيذ هذه القوانين بشكل كامل. أظهرت النتائج أن هذه المؤسسات تفتقر غالباً إلى الموارد التقنية والمالية اللازمة لضمان حماية بيانات العملاء بشكل كامل، بالإضافة إلى نقص في التدريب والوعي بالتشريعات الرقمية. يسلط هذا الضوء على الحاجة إلى دعم حكومي أكبر لهذه الفئة من المؤسسات لضمان الامتثال الكامل وحماية البيانات الشخصية.

الخلاصة:

أكدت النتائج أن تطبيق القانون الرقمي في المملكة العربية السعودية يحقق فعالية كبيرة في حماية البيانات الشخصية، خاصةً في المؤسسات الحكومية. ومع ذلك، لا يزال هناك تفاوت في الامتثال بين القطاعات المختلفة، بالإضافة إلى تحديات تواجه المؤسسات الصغيرة والمتوسطة. توضح هذه النتائج أن الاستثمار في الحوكمة الرقمية والتدريب المستمر يشكل جزءاً أساسياً من الحلول المقترحة لتحسين مستوى الحماية الرقمية في المملكة.

1. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.
2. Grama, J. L. (2014). *Legal Issues in Information Security* (2nd ed.). Jones & Bartlett Learning.
3. Neuman, W. L. (2011). *Social Research Methods: Qualitative and Quantitative Approaches* (7th ed.). Pearson.
4. Pallant, J. (2016). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS* (6th ed.). McGraw–Hill Education.
5. Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Pearson.
6. Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press.
7. Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.
8. Reason, J. (1990). *Human Error*. Cambridge University Press.
9. Bannister, F., & Connolly, R. (2014). *ICT, public values and transformative government: A framework and programme for research*. *Government Information Quarterly*, 31(1), 119–128.

10. Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational*

Principles. Information and Privacy Commissioner of Ontario, Canada.

11. Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law*

(6th ed.). Wolters Kluwer.

12. Bygrave, L. A. (2014). *Data Privacy Law: An International*

Perspective. Oxford University Press.

الملاحق:

ملحق البحث: دور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية

1. نموذج استبيان (Questionnaire)

الجزء الأول: المعلومات الشخصية

- العمر: _____
- الجنس: () ذكر () أنثى
- المستوى التعليمي:
() ثانوي
() بكالوريوس
() ماجستير
() دكتوراه
- عدد سنوات الخبرة: _____
- نوع المؤسسة:
() حكومية
() خاصة

- القسم الوظيفي:
- () تقنية المعلومات
- () قانوني
- () إداري
- () آخر _____ :

الجزء الثاني: المعرفة بالقوانين الرقمية

1. ما مدى معرفتك بالقوانين الرقمية لحماية البيانات الشخصية؟
(1) ضعيفة (2) متوسطة (3) جيدة (4) ممتازة
2. هل تلقّيت أي تدريب حول القوانين الرقمية لحماية البيانات في مؤسستك؟
() نعم () لا
3. هل ترى أن القوانين الرقمية في المملكة كافية لحماية البيانات الشخصية؟
() نعم () لا
4. ما هي التحديات التي تواجه مؤسستك في الامتثال للقوانين الرقمية؟

الجزء الثالث: تأثير القوانين الرقمية على المؤسسة

1. هل ساهمت القوانين الرقمية في تحسين مستوى الأمان المعلوماتي في مؤسستك؟
(1) لا (2) قليلاً (3) بشكل متوسط (4) بشكل كبير
2. ما مدى تأثير تطبيق القوانين الرقمية على عمليات المؤسسة اليومية؟
(1) لا تأثير (2) تأثير بسيط (3) تأثير متوسط (4) تأثير كبير
3. هل واجهت مؤسستك خرقاً للبيانات خلال السنوات الثلاث الماضية؟
() نعم () لا
4. في حال كان الجواب نعم، كيف تم التعامل مع هذا الخرق؟

2. نموذج مقابلة (Interview Questions)

المقابلة مع مسؤول قانوني أو أمني في المؤسسة

1. ما هي القوانين الرقمية الرئيسية التي تعتمد عليها مؤسساتكم في حماية البيانات الشخصية؟
 2. كيف يتم تدريب الموظفين في مؤسساتكم على الامتثال للقوانين الرقمية؟
 3. هل تجد أن التشريعات الحالية في السعودية كافية لحماية البيانات الشخصية؟ لماذا أو لماذا لا؟
 4. ما هي أبرز التحديات التي تواجه مؤسساتكم في الالتزام بالقوانين الرقمية؟
 5. كيف تقوم مؤسساتكم بتقييم مدى فعالية القوانين الرقمية في حماية البيانات؟
 6. هل لديكم أي اقتراحات لتحسين السياسات الرقمية المتعلقة بحماية البيانات؟
3. جدول إحصائي: مثال لتحليل الاستبيان

جدول 2-4 تحليل استبيان

السؤال	النسبة المئوية للإجابة (1)	النسبة المئوية للإجابة (2)	النسبة المئوية للإجابة (3)	النسبة المئوية للإجابة (4)
مدى معرفتك بالقوانين الرقمية	15%	35%	30%	20%
تلقي التدريب حول القوانين الرقمية	60% نعم	40% لا		
كفاية القوانين الرقمية لحماية البيانات	50% نعم	50% لا		
تأثير القوانين على الأمان المعلوماتي	10% لا	20% قليلاً	50% متوسط	20% كبير

4. نموذج تحليل الانحدار البسيط (Simple Regression Analysis)

- الهدف: قياس العلاقة بين المعرفة بالقوانين الرقمية وعدد الانتهاكات التي تعرضت لها المؤسسة.
- المعادلة:

$$Y = \beta_0 + \beta_1 X$$

حيث:

- Y : عدد الانتهاكات
- X : المعرفة بالقوانين الرقمية
- β_0, β_1 : معاملات الانحدار

نتائج التحليل

- معامل الانحدار $\beta_1: -0.42$
- المعنى: كلما زادت المعرفة بالقوانين الرقمية، تقل احتمالية تعرض المؤسسة لانتهاكات البيانات.

5. القوانين واللوائح المتعلقة بحماية البيانات الشخصية

- *قانون الجرائم المعلوماتية السعودي*: يحدد الجرائم المتعلقة بانتهاكات البيانات والمعاقبة عليها.
- *لائحة حماية البيانات الشخصية*: تضع المعايير والإرشادات المتعلقة بكيفية حماية البيانات الشخصية وضمان سرية المعلومات.

6. تحليل المخاطر الرقمية (Risk Assessment)

تم الاعتماد على منهجية تحليل المخاطر الرقمية لتقييم التهديدات المحيطة بحماية البيانات. تم تحديد المخاطر التالية:

- المخاطر التكنولوجية: مثل الاختراقات الإلكترونية.
- المخاطر التنظيمية: مثل عدم الامتثال الكامل للقوانين الرقمية.
- المخاطر البشرية: مثل نقص الوعي لدى الموظفين حول التعامل الآمن مع البيانات.

7. الرسوم البيانية والمخططات

- رسم بياني يوضح مدى الامتثال للقوانين الرقمية في المؤسسات الحكومية والخاصة.
- رسم بياني آخر يوضح التوزيع الجغرافي للانتهاكات المسجلة في المؤسسات وفقاً لمواقعها.

8. نصوص قانونية رئيسية تم تحليلها

- المادة (4) من قانون الجرائم المعلوماتية: تنص على أن أي شخص يختلس أو ينتهك بيانات شخصية يعاقب بالسجن والغرامة.
- المادة (6) من لائحة حماية البيانات الشخصية: تضع مسؤولية المؤسسات عن حماية البيانات التي تجمعها وتخزينها.

9. التحليل النوعي للتحديات والمخاطر

تم جمع وتحليل تعليقات المشاركين في المقابلات حول التحديات التي تواجههم في الامتثال للقوانين الرقمية. من أبرز هذه التحديات:

- نقص الوعي بالتشريعات الحديثة.
- تكلفة تطبيق حلول الأمان الرقمي.
- التأخر في اعتماد حلول تقنية حديثة لحماية البيانات.

الخلاصة:

يُعتبر هذا الملحق مرجعاً شاملاً لجميع الأدوات التي تم استخدامها في جمع وتحليل البيانات في هذه الدراسة. تحتوي هذه الأدوات على استبيانات، مقابلات، جداول إحصائية، وتحليلات قانونية، بهدف تحقيق فهم شامل لدور القانون الرقمي في حماية البيانات الشخصية في المملكة العربية السعودية.

Abstract:

This study aims to analyze the role of digital law in protecting personal data in Saudi Arabia, focusing on the laws and regulations designed to enhance digital security and compliance with legal frameworks. With the rapid technological advancements and digital transformation under Vision 2030, both governmental and private institutions face significant challenges in safeguarding user data against digital threats such as cyber-attacks and data breaches.

The study employed a comprehensive methodology combining both quantitative and qualitative analysis. Data were collected from a representative sample of government and private institutions, using data collection tools such as surveys and personal interviews, along with an analysis of relevant legal documents such as the Anti-Cybercrime Law and Personal Data Protection Regulations.

The findings revealed challenges in the application of digital laws within Saudi institutions, particularly in areas related to digital regulation awareness and the need for proper employee training. Results indicated that institutions implementing effective training strategies achieve higher levels of legal compliance and digital security. Accordingly, the study offers recommendations for improving legal frameworks and increasing institutional awareness of digital regulations.

Keywords :Personal Data Protection, Digital Law, Regulatory Compliance, Cybercrime, Digital Security, Saudi Arabia.

Midocean University

College of Humanities Studies

Department/Master of Digital Law



The role of digital law in protecting personal data

Prepared by:

Wassal Abdulmalik almuhawtyati

241001065

Main Supervisor /

Second supervisor/

Academic year 2024/2025