

التنظيم القانوني للجرائم السيبرانية وأثره في تعزيز الأمن الرقمي: دراسة تطبيقية في ضوء نظام
مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية

إعداد الطالب/

عمار محمد الضحيان

الرقم الجامعي/

253000792

العام الدراسي

2026

قائمة المحتويات

3.....	المقدمة
4.....	مشكلة الدراسة
5.....	أهمية الدراسة
6.....	أهداف الدراسة
6.....	تساؤلات الدراسة
7.....	فرضيات الدراسة
8.....	الدراسات السابقة
12.....	المنطلقات النظرية للدراسة
15.....	المنهجية وطرق البحث
17.....	أدوات الدراسة
19.....	حدود الدراسة
21.....	المراجع

المقدمة

شهد العالم خلال العقدین الأخيرین ثورة غير مسبوقة في مجال التقنية الرقمية والاتصالات، مما أتاح فرصاً هائلة للتطوير الاقتصادي والاجتماعي والثقافي. ومع ذلك، صاحبت هذا التحول الرقمي تحديات جديدة تتعلق بالأمن الرقمي وحماية المعلومات، إذ أصبح الأفراد والمؤسسات والحكومات معرضين لمخاطر متعددة تشمل الاختراقات الإلكترونية، والاحتيال المالي الرقمي، والهجمات السيبرانية التي تستهدف البنية التحتية الحيوية. وقد أدى هذا الواقع إلى ظهور ما يعرف بـ الجرائم السيبرانية أو الجرائم المعلوماتية، والتي تتميز بكونها غير محدودة جغرافياً، وسريعة الانتشار، وصعبة التتبع، مما يفرض على الأنظمة القانونية ضرورة تطوير تشريعات فعالة للحد منها ومكافحتها (عطيه، 2024).

في المملكة العربية السعودية، ومع التوسع الكبير في الخدمات الرقمية الحكومية والخاصة واعتماد المملكة على التحول الرقمي ضمن رؤية استراتيجية طويلة الأمد، أصبح الأمن الرقمي أولوية وطنية. ويعد نظام مكافحة الجرائم المعلوماتية من الركائز الأساسية التي صممت لتنظيم التعامل مع الجرائم السيبرانية ومعاقبة مرتكبيها، وحماية الأفراد والمؤسسات من الأضرار الناتجة عن استخدام التكنولوجيا بطرق غير مشروعة. وتأتي أهمية هذا النظام في كونه يحدد إطاراً قانونياً واضحاً للتصرفات المسموح بها والممنوعة على الشبكة الرقمية، كما يساهم في رفع مستوى الوعي القانوني لدى مستخدمي التقنية، وتعزيز الثقة في البيئة الرقمية، ما يعزز من قدرة المملكة على مواجهة التحديات الإلكترونية وحماية المعلومات الحساسة (الرازق، 2023).

وتتمثل أهمية دراسة التنظيم القانوني للجرائم السيبرانية وأثره في تعزيز الأمن الرقمي في تقديم تحليل علمي وموضوعي لكيفية تنظيم الدولة للجرائم الإلكترونية، ومدى فاعلية هذا التنظيم في الحد من الانتهاكات الرقمية، وتأثيره على سلوك الأفراد والمؤسسات في استخدام التكنولوجيا الرقمية. كما تهدف الدراسة إلى توضيح دور القوانين في خلق بيئة آمنة للتفاعل الرقمي، وتشجيع الاستخدام المسؤول للتقنية، وتعزيز المبادئ الأخلاقية والمهنية المرتبطة بالتعامل مع البيانات والمعلومات (ساتي، 2023).

وتعكس هذه الدراسة اهتمام المملكة العربية السعودية بتحقيق التوازن بين التوسع الرقمي السريع ومتطلبات الأمن الرقمي، بما يضمن حماية المجتمع من الانتهاكات السيبرانية، ويعزز القدرة المؤسسية والقانونية على التعامل مع

التحديات الرقمية المستمرة. كما تقدم الدراسة قاعدة علمية تساعد الباحثين وصناع القرار على فهم نقاط القوة والقصور في الإطار القانوني الحالي، واستشراف الحلول المستقبلية لتطوير الأمن السيبراني وفق أفضل الممارسات الدولية، بما يخدم رؤية المملكة في التحول الرقمي وأفاق التنمية المستدامة.

مشكلة الدراسة

تتمثل مشكلة الدراسة الرئيسية في التنامي المتسارع للجرائم السيبرانية في ظل التطور الكبير في استخدام التقنيات الرقمية وشبكات المعلومات، وما يترتب على ذلك من تحديات قانونية وأمنية تتعلق بمدى كفاية وفعالية التنظيم القانوني القائم لمواجهة هذه الجرائم والحد من آثارها على الأفراد والمؤسسات والمجتمع. فقد أدى الانتشار الواسع للإنترنت والتطبيقات الرقمية إلى خلق بيئة إلكترونية متشابكة تتيح فرصاً متعددة للتواصل وتبادل المعلومات، لكنها في الوقت ذاته وفرت مجالاً خصباً لظهور أنماط جديدة من الجرائم التي تستهدف البيانات والمعلومات والأنظمة الإلكترونية. وفي هذا السياق، أصدرت نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية ليشكل الإطار القانوني المنظم لمكافحة هذه الجرائم والحد من آثارها، إلا أن التطور المستمر في أساليب الجريمة السيبرانية يثير تساؤلات حول مدى كفاية هذا التنظيم القانوني وقدرته على مواكبة المستجدات التقنية المتسارعة، ومدى إسهامه الفعلي في تعزيز الأمن الرقمي وحماية المجتمع من المخاطر الإلكترونية.

ويترتب على هذه المشكلة مجموعة من الإشكاليات المرتبطة بطبيعة الجرائم السيبرانية، من أبرزها صعوبة اكتشاف مرتكبي الجرائم الإلكترونية وتتبعهم نظراً لطبيعتها العابرة للحدود، وتعدد الأساليب التقنية المستخدمة في تنفيذها مثل الاختراقات الإلكترونية والاحتيال الرقمي وانتهاك الخصوصية وسرقة البيانات. كما تظهر إشكاليات تتعلق بمدى وعي الأفراد والمؤسسات بأحكام النظام القانوني الخاص بالجرائم المعلوماتية، إضافة إلى التحديات المرتبطة بآليات تطبيق القانون والإجراءات القضائية المتعلقة بإثبات الجرائم الرقمية. كذلك قد يؤدي القصور في الوعي القانوني أو في آليات الحماية الرقمية إلى زيادة فرص وقوع الأفراد والمؤسسات ضحية لهذه الجرائم، الأمر الذي ينعكس سلباً على مستوى الثقة في البيئة الرقمية ويؤثر في مسار التحول الرقمي الذي تسعى الدولة إلى تعزيزه في مختلف القطاعات (Sarkar، 2024). وبناءً على ما سبق، يمكن صياغة السؤال الرئيس للدراسة على النحو الآتي: ما مدى فاعلية التنظيم

القانوني للجرائم السيبرانية في تعزيز الأمن الرقمي في المملكة العربية السعودية في ضوء نظام مكافحة الجرائم المعلوماتية؟

أهمية الدراسة

- الأهمية العلمية

تنبع الأهمية العلمية لهذه الدراسة من كونها تتناول أحد الموضوعات الحديثة والمهمة في مجال الدراسات القانونية والتقنية، وهو موضوع الجرائم السيبرانية والتنظيم القانوني المرتبط بها في ظل التطور المتسارع في تقنيات المعلومات والاتصال. فقد أصبحت الجرائم الإلكترونية من أبرز التحديات التي تواجه الأنظمة القانونية المعاصرة، نظراً لطبيعتها المتطورة وأساليبها المتغيرة التي تعتمد على استغلال الفضاء الرقمي وشبكات الإنترنت. ومن هذا المنطلق، تسعى هذه الدراسة إلى تقديم إطار معرفي وتحليلي يوضح طبيعة التنظيم القانوني للجرائم السيبرانية، ويبين مدى كفاءته في تحقيق الردع القانوني وحماية المجتمع الرقمي، وذلك في ضوء تطبيقات نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية. كما تسهم الدراسة في إثراء الأدبيات العلمية في مجال القانون الرقمي والأمن السيبراني، من خلال تحليل العلاقة بين التشريعات القانونية والتحديات التقنية الحديثة، وتقديم رؤية علمية تساعد الباحثين والدارسين في فهم أبعاد الجرائم السيبرانية وآليات مواجهتها قانونياً. كذلك تمثل هذه الدراسة إضافة معرفية مهمة للدراسات القانونية المعاصرة، إذ تجمع بين الجانب النظري والتحليل التطبيقي، الأمر الذي يساهم في تطوير المعرفة القانونية المرتبطة بحماية الفضاء الرقمي وتعزيز الأمن المعلوماتي في المجتمعات الحديثة (Atrey, 2023).

- الأهمية العملية

تكتسب هذه الدراسة أهمية عملية كبيرة لكونها تسلط الضوء على الدور الذي يؤديه التنظيم القانوني في الحد من الجرائم السيبرانية وتعزيز مستوى الأمن الرقمي في المجتمع. فمع التوسع الكبير في استخدام الخدمات الرقمية في مختلف المجالات مثل المعاملات المالية الإلكترونية والخدمات الحكومية الرقمية والتجارة الإلكترونية، أصبحت الحاجة ملحة إلى وجود إطار قانوني فعال يضمن حماية المستخدمين والبيانات الرقمية من المخاطر والاعتداءات الإلكترونية. ومن هنا تأتي أهمية هذه الدراسة في تقييم فاعلية القوانين والتشريعات المعمول بها، وخاصة نظام مكافحة الجرائم المعلوماتية، في مواجهة الجرائم السيبرانية وتعزيز الثقة في البيئة الرقمية داخل المملكة العربية السعودية. كما يمكن أن تساهم نتائج هذه الدراسة في دعم صناع القرار والجهات التشريعية والقضائية من خلال تقديم مجموعة من

المؤشرات العلمية التي تساعد في تطوير السياسات القانونية والتشريعية المرتبطة بالأمن السيبراني. إضافة إلى ذلك، قد تساعد الدراسة المؤسسات الحكومية والخاصة في فهم المخاطر القانونية المرتبطة باستخدام التقنية الرقمية، وتعزيز الوعي القانوني لدى الأفراد والمؤسسات بشأن الجرائم الإلكترونية وطرق الوقاية منها، الأمر الذي يساهم في بناء بيئة رقمية أكثر أمناً واستقراراً، ويدعم توجهات التحول الرقمي والتنمية المستدامة في المجتمع (Suseno, 2025).

أهداف الدراسة

الهدف الرئيسي للدراسة

- يتمثل الهدف الرئيسي لهذه الدراسة في تحليل التنظيم القانوني للجرائم السيبرانية وبيان أثره في تعزيز الأمن الرقمي في المملكة العربية السعودية، وذلك من خلال دراسة تطبيقية لأحكام نظام مكافحة الجرائم المعلوماتية ومدى فاعليته في الحد من الجرائم الإلكترونية وحماية المجتمع الرقمي.

الأهداف الفرعية للدراسة

1. التعرف على مفهوم الجرائم السيبرانية وخصائصها وأهم صورها في البيئة الرقمية المعاصرة.
2. تحليل الإطار القانوني المنظم للجرائم المعلوماتية في المملكة العربية السعودية من خلال دراسة أحكام نظام مكافحة الجرائم المعلوماتية.
3. بيان دور التنظيم القانوني في الحد من الجرائم السيبرانية وتحقيق الردع القانوني.
4. تقييم مدى إسهام النظام القانوني في تعزيز الأمن الرقمي وحماية البيانات والمعلومات.
5. تقديم مجموعة من المقترحات والتوصيات التي تساهم في تطوير التنظيم القانوني لمكافحة الجرائم السيبرانية وتعزيز الأمن الرقمي.

تساؤلات الدراسة

التساؤل الرئيسي للدراسة

- ما مدى فاعلية التنظيم القانوني للجرائم السيبرانية في تعزيز الأمن الرقمي في المملكة العربية السعودية في ضوء تطبيق نظام مكافحة الجرائم المعلوماتية؟

الأسئلة الفرعية للدراسة

1. ما المقصود بالجرائم السيبرانية وما أبرز خصائصها وأنواعها في العصر الرقمي؟
2. ما الإطار القانوني الذي ينظم مكافحة الجرائم السيبرانية في المملكة العربية السعودية؟
3. ما الآليات القانونية التي يتضمنها نظام مكافحة الجرائم المعلوماتية لمواجهة الجرائم الإلكترونية؟
4. إلى أي مدى يسهم التنظيم القانوني الحالي في تعزيز الأمن الرقمي وحماية مستخدمي الإنترنت؟
5. ما أبرز التحديات التي تواجه تطبيق القوانين المتعلقة بالجرائم السيبرانية، وما السبل المقترحة لمعالجتها؟

فرضيات الدراسة

الفرضية الرئيسية للدراسة

- يسهم التنظيم القانوني للجرائم السيبرانية، المتمثل في نظام مكافحة الجرائم المعلوماتية، في تعزيز الأمن الرقمي والحد من الجرائم الإلكترونية في المملكة العربية السعودية.

الفرضيات الفرعية للدراسة

1. توجد علاقة إيجابية بين وضوح التشريعات القانونية الخاصة بالجرائم السيبرانية ومستوى الحد من الجرائم الإلكترونية.
2. يسهم تطبيق العقوبات الواردة في نظام مكافحة الجرائم المعلوماتية في تحقيق الردع القانوني لمستخدمي الفضاء الرقمي.
3. يؤدي تعزيز الوعي القانوني لدى الأفراد والمؤسسات إلى تقليل فرص الوقوع في الجرائم السيبرانية.
4. يسهم التنظيم القانوني الفعال في حماية البيانات والمعلومات الرقمية وتعزيز الثقة في البيئة الإلكترونية.
5. توجد علاقة بين تطور التشريعات المتعلقة بالجرائم المعلوماتية ومستوى تحقيق الأمن الرقمي في المجتمع.

الدراسات السابقة

شهد العصر الحديث زيادةً متسارعةً في استخدام الطلاب للإنترنت وتكنولوجيا المعلومات. ونتيجةً لذلك، واجه المعلمون في جميع أنحاء العالم مشكلةً كبيرةً بسبب هذا الاعتماد غير المسبوق، بل والاعتماد المفرط، على هذه التكنولوجيا. علاوةً على ذلك، وكما هو الحال مع أي ظاهرة اجتماعية ناشئة مماثلة، فقد أدى هذا الاعتماد على التكنولوجيا إلى ظهور أنماط جديدة من السلوك غير القانوني والمخالف للقانون. تقدم دراسة (Alhadidi, 2024) تحليلاً شاملاً لتأثير الوعي بالجرائم الإلكترونية والقانونية على سلوك الشباب في المجتمع، وذلك من خلال دمج منظورين نظري وتجريبي. ولمعالجة هذه المسألة، أُجريت دراسة كمية باستخدام استبيان وُزِعَ على عينة عشوائية من 2000 طالب مسجلين في الجامعة الأردنية، والتي كانت موضوع دراستنا. تُظهر نتائج دراستنا وجود ارتباط قوي لا جدال فيه بين مستوى الوعي القانوني بالجرائم الإلكترونية لدى الطلاب وانخراطهم في أعمال إلكترونية غير مشروعة. بالإضافة إلى ذلك، تشير النتائج إلى أن الجنس وعوامل أخرى تؤثر في ردع الطلاب عن الانخراط في مثل هذه السلوكيات الإجرامية. وبالتالي، يؤكد هذا على أهمية تطبيق استراتيجيات فعّالة لتعزيز الوعي القانوني لدى الطلاب فيما يتعلق بالجرائم الإلكترونية، للحد من تورطهم فيها.

مع تزايد شعبية تكنولوجيا المعلومات والاتصالات، ارتفعت جرائم الإنترنت بوتيرة متسارعة. وقد اتخذت دول العالم كافة التدابير اللازمة لضمان الأمن السيبراني. وتُعدّ المملكة العربية السعودية الأكثر تضرراً من جرائم الإنترنت في منطقة الخليج. تبحث دراسة (Alshammari, 2018) في مدى استعداد المملكة العربية السعودية للدفاع عن نفسها ضد هذه الجرائم. ففي سبيل مكافحة جرائم الإنترنت، سنّت المملكة قانون مكافحة جرائم الإنترنت عام 2007. وقد وضع مؤشر الأمن السيبراني العالمي لعام 2017 المملكة في مرحلة النضج، متأخرةً عن الدول الرائدة. يغطي قانون مكافحة جرائم الإنترنت جوانب أساسية لمكافحة هذه الجرائم، ويحدد عقوباتها. ومع ذلك، فقد وُجد أنه قاصر عن الحماية من سرقة الهوية، وانتهاك الخصوصية، والتنمر الإلكتروني، وغيرها. وتخلص هذه الدراسة إلى أن المملكة العربية السعودية شبه مستعدة للدفاع عن نفسها ضد جرائم الإنترنت. ولكي تتبوأ مكانة رائدة في مجال الأمن السيبراني، تحتاج المملكة إلى تعزيز قانون مكافحة جرائم الإنترنت، ولوائح الأمن السيبراني، وهيئة الأمن السيبراني

الوطنية. يجب عليها تطوير استراتيجية للأمن السيبراني، ومعايير، ومقاييس، وبرامج بحث وتطوير. كما ينبغي عليها تشجيع صناعة الأمن السيبراني المحلية، وتحفيز شركات الأمن السيبراني، وإبرام اتفاقيات متعددة الأطراف.

أحدث ظهور الثورة الصناعية الخامسة نقلة نوعية في مجال التكنولوجيا من خلال دمج الأنظمة المادية مع الشبكات الرقمية. وقد أدت هذه التطورات أيضًا إلى زيادة التهديدات السيبرانية، مما يشكل مخاطر جسيمة، لا سيما على الشركات الصغيرة والمتوسطة. يبحث دراسة (Rawindaran, 2023) في مقاومة الشركات الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة لإجراءات الأمن السيبراني في سياق الثورة الصناعية الخامسة، مع التركيز بشكل خاص على الحوكمة والسياسات. ويستكشف العوامل الثقافية والاقتصادية التي تسهم في هذه المقاومة، مثل محدودية الوعي بمخاطر الأمن السيبراني، والقيود المالية، وتضارب أولويات الأعمال. بالإضافة إلى ذلك، تتناول الدراسة دور السياسات واللوائح الحكومية في تعزيز ممارسات الأمن السيبراني بين الشركات الصغيرة والمتوسطة، وتقارن بين النهج المتبعة في المملكة العربية السعودية والمملكة المتحدة. وباستخدام منهجية تحليلية متعددة الأساليب، تشمل مقابلات مع أصحاب الشركات الصغيرة والمتوسطة وخبراء في هذا المجال، يسلط البحث الضوء على التحديات والفرص المتاحة لتحسين حوكمة وسياسات الأمن السيبراني في كلا البلدين. وتؤكد النتائج على ضرورة إيجاد حلول مصممة خصيصًا نظرًا لاختلاف السياقات الثقافية والاقتصادية بين المملكة العربية السعودية والمملكة المتحدة. تتناول هذه الدراسة بالتحديد مستوى الوعي بتطبيق تدابير الأمن السيبراني، مع التركيز على الشركات الصغيرة والمتوسطة في المملكة العربية السعودية ومدى التزامها بإرشادات ضوابط الأمن السيبراني الأساسية (ECC-1:2018). كما تبحث الدراسة في ممارسات الوعي والامتثال الحالية في مجال الأمن السيبراني في المملكة المتحدة، وتقارن في الوقت نفسه الوثائق الإرشادية الرسمية التي تهدف إلى دعم الشركات الصغيرة والمتوسطة في تبني ممارسات أفضل في هذا المجال. وبناءً على التحليل، توصي الدراسة بتعزيز التفاعل مع هذه الوثائق في كلا البلدين لرفع مستوى الوعي والثقة والامتثال لدى الشركات الصغيرة والمتوسطة، مما يُحسن في نهاية المطاف من وضعها في مجال الأمن السيبراني. تقدم هذه الورقة البحثية دراسة مقارنة حول الحوكمة والسياسات بين المملكة العربية السعودية والمملكة المتحدة، وتعرض مجموعة من التوصيات لتعزيز الوعي والتثقيف في مجال الأمن السيبراني، ودعم الأطر التنظيمية، وتشجيع الشراكات بين القطاعين العام والخاص لمكافحة تهديدات الأمن السيبراني في ظل الثورة الصناعية الخامسة.

شهد النظام القانوني لمكافحة الجرائم الإلكترونية في المملكة العربية السعودية تطوراً ملحوظاً منذ سنّ قانون مكافحة الجرائم الإلكترونية لعام 2007، والذي يشهد بدوره تحولاً رقمياً متسارعاً في إطار رؤية 2030. ستتناول دراسة (Moafa، 2026) تطور التشريعات الرئيسية والتعديلات والقواعد التكميلية، ودور الهيئة الوطنية للأمن السيبراني، وتأثير تزايد التهديدات على الأمن القومي، وسياسات الحوكمة الرقمية الأكثر شمولاً. وبالاستناد إلى مصادر متنوعة، كالمؤلفات الأكاديمية للدكتور فهد معاف، سيركز التحليل على تعزيز الرقابة على الجرائم الإلكترونية، كالاختراق والتشهير وبرامج الفدية، ومسألة إدارة التوازن بين الأمن والخصوصية والابتكار. وتقدم دراسة معاف حول التحرش الإلكتروني والتنمر والمطاردة في السعودية معلومات قيّمة يمكن الاستفادة منها في دراسة العوامل السلوكية والوقائية. ويُظهر مثال مقارنة مع التجربة الأسترالية تشابهاً بين النظام السعودي والنظام السعودي من حيث التطورات التي أعقبت عام 2020، إلا أن الاختلافات تكمن في نظام الحوكمة. لقد عززت أطر عمل NCA، بما في ذلك ضوابط الأمن السيبراني الأساسية، القدرة على الصمود، وأهداف رؤية 2030 لاقتصاد رقمي آمن من خلال التوصيات المتعلقة بالتحديثات المستمرة والتعاون الدولي والتوعية العامة للتصدي للتهديدات المتزايدة.

هدفت دراسة (Alahmari، 2025) إلى تحديد دور نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية، ومستوى تنظيم أخلاقيات الإعلام الرقمي، والكشف عن العلاقة بين دور نظام مكافحة الجرائم الإلكترونية وتنظيم أخلاقيات الإعلام الرقمي في المملكة. تكون مجتمع البحث من إعلاميين وناشطين يعملون على منصات الإعلام الرقمي في المملكة. بلغ حجم عينة البحث 94 مشاركاً. استخدم الباحث المنهج التحليلي كمنهج وأداة للدراسة. توصلت الدراسة إلى عدد من النتائج، أهمها: أظهر المحور الأول (نظام مكافحة الجرائم الإلكترونية) استجابة عالية، بينما أظهر المحور الثاني (تنظيم أخلاقيات الإعلام الرقمي) استجابة متوسطة. كما تبين وجود ارتباط إيجابي ذي دلالة إحصائية بين دور نظام مكافحة الجرائم الإلكترونية وتنظيم أخلاقيات الإعلام الرقمي في المملكة العربية السعودية. وقد أوصى البحث بالعديد من التوصيات، وكان أهمها: وضع تشريعات وقوانين صارمة لمكافحة الجرائم الإلكترونية، والإعلان بوضوح عن أخلاقيات الإعلام الرقمي.

التعليق على الدراسات السابقة:

- أوجه التشابه في الدراسات السابقة

تشابه الدراسات السابقة في اهتمامها المشترك بموضوع الجرائم السيبرانية والأمن الرقمي في ظل التوسع الكبير في استخدام التكنولوجيا الحديثة والإنترنت في مختلف مجالات الحياة. فقد ركزت معظم هذه الدراسات على تحليل طبيعة الجرائم الإلكترونية والتهديدات التي تفرضها على الأفراد والمؤسسات والمجتمعات، كما تناولت أهمية وجود تشريعات قانونية واضحة لمكافحة هذه الجرائم والحد من أثارها السلبية. كما أظهرت الدراسات اتفاقاً واضحاً حول الدور الحيوي الذي تؤديه القوانين والأنظمة القانونية في حماية الفضاء الرقمي وتعزيز مستوى الأمن السيبراني، خاصة في ظل تزايد الاعتماد على الخدمات الرقمية في الأنشطة الاقتصادية والاجتماعية.

اتفقت هذه الدراسات على أهمية رفع مستوى الوعي لدى الأفراد والمؤسسات حول مخاطر الجرائم السيبرانية وسبل الوقاية منها، حيث أشارت النتائج إلى أن ضعف الوعي القانوني أو التقني قد يؤدي إلى زيادة احتمالات الوقوع في الجرائم الإلكترونية أو الانخراط فيها. كما أكدت الدراسات على ضرورة تطوير الأطر التنظيمية والسياسات الحكومية التي تهدف إلى تعزيز الأمن الرقمي، مع الإشارة إلى أهمية التعاون بين الجهات الحكومية والقطاع الخاص في مواجهة التحديات المرتبطة بالجرائم السيبرانية. ويبرز في هذا السياق الدور التشريعي الذي يقوم به نظام مكافحة الجرائم المعلوماتية في تنظيم التعامل مع الجرائم الإلكترونية داخل المملكة العربية السعودية، باعتباره أحد أهم الأدوات القانونية التي تسعى إلى حماية المجتمع من مخاطر الفضاء الرقمي.

- أوجه الاختلاف في الدراسات السابقة

على الرغم من وجود العديد من نقاط التشابه بين الدراسات السابقة، إلا أنها اختلفت في طبيعة الأهداف والمنهجيات البحثية المستخدمة، وكذلك في نطاق التطبيق الجغرافي والموضوعي. فقد ركزت بعض الدراسات على تحليل مستوى الوعي القانوني لدى فئات محددة من المجتمع، مثل الطلاب أو مستخدمي الإنترنت، ودراسة تأثير هذا الوعي في الحد من الانخراط في الجرائم الإلكترونية. في المقابل، اهتمت دراسات أخرى بتحليل الإطار التشريعي والتنظيمي لمكافحة الجرائم السيبرانية، مع التركيز على السياسات الحكومية والاستراتيجيات الوطنية التي تهدف إلى تعزيز الأمن السيبراني.

كما ظهرت اختلافات واضحة في منهجيات البحث المستخدمة، حيث اعتمدت بعض الدراسات على المنهج الكمي باستخدام الاستبيانات لقياس اتجاهات الأفراد نحو الجرائم الإلكترونية، بينما استخدمت دراسات أخرى المناهج التحليلية أو المقارنة لدراسة الأطر القانونية والسياسات التنظيمية المرتبطة بالأمن السيبراني. كذلك تباينت الدراسات من حيث نطاقها الجغرافي، إذ تناولت بعض الدراسات موضوع الأمن السيبراني في سياقات دولية أو مقارنة بين عدة

دول، في حين ركزت دراسات أخرى على البيئة القانونية في دولة معينة مثل المملكة العربية السعودية، مع تحليل دور التشريعات الوطنية في مكافحة الجرائم الإلكترونية.

- الفجوات البحثية التي يميزها البحث الحالي

على الرغم من الجهود العلمية التي بذلتها الدراسات السابقة في تناول موضوع الجرائم السيبرانية والأمن الرقمي، إلا أن هناك عدداً من الجوانب التي لم تحظ بالاهتمام الكافي، وهو ما تسعى الدراسة الحالية إلى معالجته. فقد ركزت بعض الدراسات السابقة على جانب الوعي أو السلوك الرقمي للأفراد، في حين ركزت دراسات أخرى على الجوانب التشريعية بصورة نظرية أو تحليلية، دون الربط بشكل كافٍ بين التنظيم القانوني وتأثيره الفعلي في تعزيز الأمن الرقمي داخل المجتمع.

كما أن عدداً من الدراسات تناول موضوع الجرائم السيبرانية من منظور عام أو مقارنة دون التركيز بصورة تطبيقية على أثر القوانين الوطنية في تحقيق الأمن الرقمي. ومن هنا تأتي أهمية الدراسة الحالية التي تسعى إلى تحليل العلاقة بين التنظيم القانوني للجرائم السيبرانية وتعزيز الأمن الرقمي من خلال دراسة تطبيقية في ضوء نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية، وذلك بالاعتماد على منهجية كمية تساهم في قياس اتجاهات الأفراد وتحليل مدى إدراكهم لدور التشريعات القانونية في الحد من الجرائم الإلكترونية.

وبذلك تسعى الدراسة الحالية إلى سد فجوة بحثية تتمثل في الربط بين الإطار القانوني والتطبيق العملي للأمن الرقمي، مع تقديم تحليل علمي يساعد في تقييم فاعلية التنظيم القانوني القائم واقتراح سبل تطويره بما يتناسب مع التحديات المتزايدة التي تفرضها الجرائم السيبرانية في العصر الرقمي.

المنطلقات النظرية للدراسة

تستند الدراسات القانونية المعاصرة، وخاصة تلك المرتبطة بالجرائم السيبرانية، إلى مجموعة من المنطلقات النظرية التي تساعد على تفسير الظواهر القانونية والاجتماعية المرتبطة باستخدام التكنولوجيا الرقمية. ومع التطور المتسارع في تقنيات المعلومات والاتصال، ظهرت أنماط جديدة من الجرائم التي تستهدف الأنظمة المعلوماتية والبيانات الرقمية، الأمر الذي فرض على الأنظمة القانونية تطوير أطر نظرية وتشريعية قادرة على فهم هذه الجرائم وتحليلها ومواجهتها.

بفعالية. وتكمن أهمية المنطلقات النظرية في أنها تقدم أساساً علمياً يمكن من خلاله تفسير طبيعة الجرائم السيبرانية، وفهم العلاقة بين القواعد القانونية والأمن الرقمي، وكذلك تحليل مدى قدرة التشريعات القانونية على تحقيق الردع والحماية في البيئة الرقمية.

وفي هذا الإطار، تعتمد الدراسة الحالية على مجموعة من المفاهيم والنظريات المرتبطة بالقانون الرقمي والأمن السيبراني، والتي تسهم في تفسير دور التنظيم القانوني في الحد من الجرائم الإلكترونية وتعزيز حماية المجتمع الرقمي. كما ترتبط هذه المنطلقات النظرية بتحليل الإطار التشريعي المنظم للجرائم المعلوماتية في المملكة العربية السعودية، وخاصة ما ورد في نظام مكافحة الجرائم المعلوماتية، والذي يمثل الأساس القانوني لمكافحة الجرائم الإلكترونية وتنظيم التعامل مع الانتهاكات الرقمية (Achuthan, 2025).

- مفهوم الجرائم السيبرانية وطبيعتها القانونية

تشير الجرائم السيبرانية إلى الأفعال غير المشروعة التي يتم ارتكابها باستخدام الحاسب الآلي أو شبكات الإنترنت أو أي وسيلة تقنية رقمية بهدف الاعتداء على الأنظمة المعلوماتية أو البيانات أو الأفراد أو المؤسسات. وتتميز هذه الجرائم بخصائص تختلف عن الجرائم التقليدية، إذ تعتمد في تنفيذها على الوسائل التقنية الحديثة، كما أنها غالباً ما تتسم بالطابع العابر للحدود الجغرافية، مما يجعل ملاحقة مرتكبيها أكثر تعقيداً من الناحية القانونية.

ومن الناحية القانونية، تعد الجرائم السيبرانية من الجرائم المستحدثة التي ظهرت نتيجة التحول الرقمي المتسارع في المجتمعات المعاصرة. وقد دفعت هذه الجرائم المشرعين في مختلف دول العالم إلى سن تشريعات خاصة تنظم التعامل معها، وذلك بهدف حماية البيانات والمعلومات وضمان أمن الأنظمة الإلكترونية. وفي هذا السياق، يمثل نظام مكافحة الجرائم المعلوماتية الإطار القانوني الذي يحدد صور الجرائم الإلكترونية والعقوبات المقررة لها في المملكة العربية السعودية، بما يسهم في توفير حماية قانونية للفضاء الرقمي والحد من الانتهاكات المرتبطة باستخدام التكنولوجيا (Alawida, 2022).

- مفهوم التنظيم القانوني للجرائم السيبرانية

يقصد بالتنظيم القانوني للجرائم السيبرانية مجموعة القواعد والتشريعات التي تضعها الدولة بهدف تحديد الأفعال التي تشكل جرائم إلكترونية، وبيان العقوبات المقررة لها، وتنظيم الإجراءات القانونية المتعلقة بملاحقة مرتكبيها

ومحاكمتهم. ويعد هذا التنظيم أحد الأدوات الأساسية التي تعتمد عليها الدول لحماية الأمن الرقمي وضمان الاستخدام الآمن للتكنولوجيا الحديثة.

ويكتسب التنظيم القانوني للجرائم السيبرانية أهمية خاصة في ظل الطبيعة المعقدة لهذه الجرائم، إذ يتطلب الأمر وجود تشريعات واضحة ومتكاملة قادرة على مواكبة التطور التقني المستمر. كما يشمل هذا التنظيم تحديد المسؤوليات القانونية للأفراد والمؤسسات في استخدام الوسائل التقنية، إضافة إلى وضع آليات قانونية تتيح للجهات المختصة الكشف عن الجرائم الإلكترونية وجمع الأدلة الرقمية اللازمة لإثباتها أمام الجهات القضائية. ومن هذا المنطلق، يسهم التنظيم القانوني في تحقيق التوازن بين الاستفادة من مزايا التكنولوجيا الرقمية وبين حماية المجتمع من المخاطر المرتبطة بسوء استخدامها (Bacon، 2023).

- مفهوم الأمن الرقمي وأهميته في المجتمع المعاصر

يشير الأمن الرقمي إلى مجموعة الإجراءات والتدابير التقنية والقانونية والتنظيمية التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات الرقمية من التهديدات والهجمات الإلكترونية. ويعد الأمن الرقمي أحد الركائز الأساسية التي تقوم عليها المجتمعات الرقمية الحديثة، حيث يعتمد الأفراد والمؤسسات بشكل متزايد على التكنولوجيا في إدارة مختلف الأنشطة الاقتصادية والاجتماعية والإدارية.

وتتزايد أهمية الأمن الرقمي في ظل الانتشار الواسع للخدمات الإلكترونية مثل التجارة الإلكترونية والخدمات الحكومية الرقمية والتعاملات المصرفية عبر الإنترنت. إذ إن أي اختراق أو اعتداء على الأنظمة المعلوماتية قد يؤدي إلى خسائر مالية كبيرة أو تسريب معلومات حساسة أو تعطيل الخدمات الحيوية. ولذلك تسعى الدول إلى تعزيز الأمن الرقمي من خلال تطوير البنية التحتية التقنية، ورفع مستوى الوعي الرقمي لدى المستخدمين، إضافة إلى سن التشريعات القانونية التي تجرم الأفعال التي تهدد سلامة الأنظمة المعلوماتية. ويعد التنظيم القانوني للجرائم السيبرانية أحد أهم الوسائل التي تسهم في تحقيق الأمن الرقمي من خلال وضع إطار قانوني واضح يحدد السلوكيات المجرمة ويضمن معاقبة مرتكبيها (Nobanee، 2023).

العلاقة بين التنظيم القانوني وتعزيز الأمن الرقمي

ترتبط فعالية الأمن الرقمي ارتباطاً وثيقاً بمدى قوة ووضوح التنظيم القانوني الذي يحكم التعامل مع الجرائم السيبرانية. فوجود تشريعات قانونية واضحة يساهم في ردع الأفراد عن ارتكاب الجرائم الإلكترونية، كما يوفر إطاراً قانونياً يمكن الجهات المختصة من ملاحقة الجناة ومعاقبتهم وفقاً للإجراءات القانونية المعتمدة.

كما يساهم التنظيم القانوني في تعزيز الثقة في البيئة الرقمية، إذ يشعر المستخدمون بالأمان عند استخدام الخدمات الإلكترونية عندما يدركون أن هناك قوانين تحميهم من الانتهاكات الرقمية وتعاقب من يسيء استخدام التكنولوجيا. وفي هذا السياق، يمثل نظام مكافحة الجرائم المعلوماتية أحد الأدوات التشريعية المهمة التي تهدف إلى تعزيز الأمن الرقمي في المملكة العربية السعودية، حيث يحدد الأفعال المجرّمة في الفضاء الإلكتروني ويضع عقوبات رادعة لمرتكبيها، الأمر الذي يساهم في الحد من الجرائم الإلكترونية وحماية المجتمع من مخاطرها المتزايدة. وبذلك يتضح أن التنظيم القانوني يشكل أحد الركائز الأساسية في بناء منظومة متكاملة للأمن الرقمي، حيث يعمل جنباً إلى جنب مع الإجراءات التقنية والتوعوية لتحقيق بيئة رقمية آمنة ومستقرة قادرة على دعم التحول الرقمي والتنمية المستدامة في المجتمعات الحديثة (Althibyani، 2023).

المنهجية وطرق البحث

تشكل المنهجية العلمية من الركائز الأساسية التي يعتمد عليها الباحث في تنظيم دراسته وتحقيق أهدافها بصورة منهجية ومنظمة، إذ تساهم في تحديد الأساليب والإجراءات التي يتم من خلالها جمع البيانات وتحليلها والوصول إلى النتائج العلمية الدقيقة. وفي ظل طبيعة الدراسة الحالية التي تتناول موضوع التنظيم القانوني للجرائم السيبرانية وأثره في تعزيز الأمن الرقمي، فإن اختيار المنهجية المناسبة يعد أمراً ضرورياً لفهم العلاقة بين الإطار القانوني ومستوى تحقيق الأمن الرقمي في المجتمع. ومن هذا المنطلق، تعتمد هذه الدراسة على المنهجية الكمية التي تقوم على جمع البيانات وتحليلها باستخدام الأساليب الإحصائية، بهدف الوصول إلى نتائج موضوعية يمكن تعميمها على مجتمع الدراسة. وتكمن أهمية المنهجية الكمية في قدرتها على قياس الاتجاهات والآراء وتحليل العلاقات بين المتغيرات المختلفة المرتبطة بموضوع الدراسة، خاصة فيما يتعلق بمدى فاعلية التنظيم القانوني للجرائم السيبرانية في تعزيز الأمن الرقمي في المملكة العربية السعودية في ضوء أحكام نظام مكافحة الجرائم المعلوماتية.

- المنهج الكمي في الدراسة

يعتمد البحث في هذه الدراسة على المنهج الكمي باعتباره أحد المناهج العلمية التي تركز على تحليل الظواهر الاجتماعية والقانونية من خلال البيانات الرقمية القابلة للقياس والتحليل الإحصائي. ويهدف هذا المنهج إلى دراسة العلاقة بين المتغيرات المختلفة المرتبطة بموضوع البحث، مثل مستوى الوعي بالقوانين المتعلقة بالجرائم السيبرانية ومدى تأثيرها في تعزيز الأمن الرقمي لدى الأفراد والمؤسسات. ويتيح استخدام المنهج الكمي إمكانية قياس اتجاهات مجتمع الدراسة نحو فاعلية التنظيم القانوني في الحد من الجرائم الإلكترونية، إضافة إلى تحليل مدى إدراك الأفراد لأهمية القوانين التي تنظم استخدام الفضاء الرقمي.

كما يتميز المنهج الكمي بقدرته على توفير نتائج علمية دقيقة قائمة على البيانات والأرقام، الأمر الذي يعزز من موضوعية الدراسة ويقلل من احتمالات التحيز في تفسير النتائج. ومن خلال تطبيق هذا المنهج، يسعى الباحث إلى جمع البيانات المتعلقة بموضوع الدراسة من عينة محددة من مجتمع البحث، ثم تحليلها باستخدام الأساليب الإحصائية المناسبة بهدف اختبار الفرضيات المطروحة والتأكد من صحة العلاقات المفترضة بين المتغيرات. ويساعد هذا الأسلوب في تقديم نتائج قابلة للتعميم تسهم في تقييم مدى فاعلية التنظيم القانوني للجرائم السيبرانية في تحقيق الأمن الرقمي.

- مجتمع الدراسة والعينة

يشير مجتمع الدراسة إلى جميع الأفراد أو الفئات التي تتعلق بموضوع البحث والتي يسعى الباحث إلى دراسة خصائصها وتحليل آرائها واتجاهاتها. وفي إطار هذه الدراسة، يتمثل مجتمع الدراسة في الأفراد الذين يتعاملون مع البيئة الرقمية ويستخدمون التقنيات الحديثة في حياتهم اليومية، بالإضافة إلى المختصين في المجالات القانونية والتقنية المرتبطة بالجرائم السيبرانية في المملكة العربية السعودية. ويُعد اختيار هذا المجتمع مناسباً لطبيعة الدراسة، نظراً لارتباطه المباشر بموضوع الأمن الرقمي والتشريعات المتعلقة بالجرائم المعلوماتية.

أما عينة الدراسة فهي جزء من مجتمع الدراسة يتم اختيارها بطريقة علمية بحيث تمثل خصائص المجتمع الأصلي تمثيلاً دقيقاً. ويعتمد الباحث في هذه الدراسة على اختيار عينة مناسبة من مجتمع البحث باستخدام أساليب المعاينة الإحصائية، بهدف الحصول على بيانات كمية يمكن تحليلها واستخلاص النتائج منها. وتتيح العينة المختارة للباحث دراسة اتجاهات وآراء المشاركين بشأن فاعلية التنظيم القانوني في مكافحة الجرائم السيبرانية، ومدى إسهامه في تعزيز الأمن الرقمي في المجتمع.

- أساليب تحليل البيانات

بعد جمع البيانات من أفراد عينة الدراسة، يتم تحليلها باستخدام مجموعة من الأساليب الإحصائية التي تساعد في تفسير النتائج واختبار الفرضيات المطروحة في الدراسة. وتشمل هذه الأساليب استخدام الإحصاءات الوصفية التي تهدف إلى وصف خصائص البيانات مثل المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية، والتي تساعد في تقديم صورة عامة عن اتجاهات أفراد العينة نحو موضوع الدراسة.

كما يتم استخدام بعض الأساليب الإحصائية الاستنتاجية التي تساعد في اختبار الفرضيات وتحليل العلاقة بين المتغيرات المختلفة، مثل العلاقة بين التنظيم القانوني للجرائم السيبرانية ومستوى الأمن الرقمي. ويسهم هذا النوع من التحليل في تقديم نتائج علمية دقيقة تساعد في تفسير مدى فاعلية التشريعات القانونية، وخاصة ما ورد في نظام مكافحة الجرائم المعلوماتية، في الحد من الجرائم الإلكترونية وتعزيز الثقة في البيئة الرقمية في المملكة العربية السعودية.

وبذلك تتيح المنهجية الكمية المعتمدة في هذه الدراسة إطاراً علمياً دقيقاً يمكن من خلاله تحليل البيانات واستخلاص النتائج التي تسهم في فهم طبيعة العلاقة بين التنظيم القانوني للجرائم السيبرانية ومستوى الأمن الرقمي، وتقديم توصيات علمية يمكن الاستفادة منها في تطوير السياسات القانونية والتشريعية المرتبطة بالأمن السيبراني.

أدوات الدراسة

تعتمد الدراسات العلمية التي تتبع المنهجية الكمية على مجموعة من الأدوات البحثية التي تساعد الباحث في جمع البيانات بصورة منظمة ودقيقة، بما يتيح تحليلها إحصائياً للوصول إلى نتائج علمية موضوعية. وتكمن أهمية أدوات الدراسة في كونها الوسيلة التي يتم من خلالها الحصول على المعلومات المتعلقة بمتغيرات البحث، وقياس اتجاهات وآراء أفراد مجتمع الدراسة نحو الظاهرة محل البحث. وفي إطار الدراسة الحالية التي تتناول التنظيم القانوني للجرائم السيبرانية وأثره في تعزيز الأمن الرقمي، فقد تم الاعتماد على أدوات كمية تساعد في قياس مستوى الوعي القانوني ومدى إدراك الأفراد لأهمية التشريعات المتعلقة بمكافحة الجرائم المعلوماتية في المملكة العربية السعودية، وخاصة تلك الواردة في نظام مكافحة الجرائم المعلوماتية.

- الاستبانة كأداة رئيسية لجمع البيانات

تُعد الاستبانة الأداة الرئيسية المستخدمة في هذه الدراسة، نظراً لملاءمتها لطبيعة المنهج الكمي وقدرتها على جمع البيانات من عدد كبير من أفراد مجتمع الدراسة في فترة زمنية قصيرة نسبياً. وتقوم الاستبانة على مجموعة من الأسئلة المصممة بعناية والتي تهدف إلى قياس آراء واتجاهات المشاركين نحو موضوع البحث، وذلك من خلال أسئلة مغلقة تعتمد على مقاييس كمية يمكن تحليلها باستخدام الأساليب الإحصائية. وقد تم تصميم الاستبانة بما يتناسب مع أهداف الدراسة وتساؤلاتها، حيث تضمنت مجموعة من المحاور التي تتناول فهم المشاركين لمفهوم الجرائم السيبرانية، ومستوى معرفتهم بالتنظيم القانوني المرتبط بها، ومدى إدراكهم لدور التشريعات القانونية في تعزيز الأمن الرقمي.

كما تم إعداد أسئلة الاستبانة بطريقة منهجية تضمن وضوحها وسهولة فهمها من قبل أفراد العينة، مع مراعاة التنوع في الأسئلة بما يسمح بقياس مختلف جوانب موضوع الدراسة. وقد اشتملت الاستبانة على عدد من العبارات التي تقيس اتجاهات المشاركين باستخدام مقياس تدريجي، الأمر الذي يساعد في تحويل الآراء إلى بيانات رقمية يمكن تحليلها إحصائياً. ويسهم استخدام هذه الأداة في توفير معلومات دقيقة حول مدى إدراك أفراد المجتمع لدور التشريعات القانونية، مثل نظام مكافحة الجرائم المعلوماتية، في الحد من الجرائم السيبرانية وتعزيز الأمن الرقمي في البيئة الإلكترونية.

- اختبار الصدق والثبات للأداة

من أجل ضمان جودة البيانات التي يتم جمعها من خلال الاستبانة، يحرص الباحث على التحقق من مدى صدق وثبات أداة الدراسة قبل تطبيقها على العينة المستهدفة. ويقصد بصدق الأداة مدى قدرتها على قياس ما وضعت لقياسه بالفعل، أي مدى ارتباط أسئلة الاستبانة بموضوع الدراسة وأهدافها. ويتم تحقيق ذلك من خلال عرض الاستبانة على مجموعة من المختصين والخبراء في مجالات القانون والأمن السيبراني والبحث العلمي، وذلك بهدف مراجعة العبارات والتأكد من ملاءمتها لموضوع الدراسة ودقتها العلمية.

أما الثبات فيشير إلى مدى استقرار نتائج الأداة عند تطبيقها في ظروف متشابهة، أي أن تعطي النتائج نفسها تقريباً إذا تم استخدامها أكثر من مرة في قياس الظاهرة نفسها. ويتم اختبار الثبات باستخدام بعض الأساليب الإحصائية المعروفة في الدراسات الكمية، والتي تساعد في التأكد من اتساق الإجابات بين فقرات الاستبانة المختلفة. ويعد التحقق من الصدق والثبات خطوة أساسية في الدراسات الكمية، لأنه يساهم في تعزيز موثوقية النتائج التي يتم التوصل إليها،

ويضمن أن البيانات التي يتم تحليلها تعكس الواقع الفعلي للظاهرة المدروسة، والمتمثلة في تأثير التنظيم القانوني للجرائم السيبرانية في تعزيز الأمن الرقمي في المملكة العربية السعودية.

ومن خلال استخدام الاستبانة كأداة رئيسية لجمع البيانات، وبالاعتماد على إجراءات علمية دقيقة للتحقق من صدقها وثباتها، تسعى الدراسة إلى توفير بيانات كمية موثوقة يمكن تحليلها إحصائياً بهدف اختبار فرضيات البحث والوصول إلى نتائج علمية تسهم في فهم دور التنظيم القانوني في مكافحة الجرائم السيبرانية وتعزيز الأمن الرقمي في المجتمع.

حدود الدراسة

- الحدود البشرية

تشير الحدود البشرية للدراسة إلى الفئة أو الفئات التي يركز عليها البحث في جمع البيانات وتحليلها، والتي تمثل مجتمع الدراسة المستهدف. وفي إطار هذه الدراسة، تتمثل الحدود البشرية في مجموعة من الأفراد الذين يتعاملون مع البيئة الرقمية ويستخدمون وسائل التقنية الحديثة، إضافة إلى بعض المختصين في المجالات القانونية والتقنية المرتبطة بالأمن السيبراني. ويشمل ذلك مستخدمي الإنترنت من الأفراد الذين لديهم معرفة أساسية بالتعامل مع الخدمات الرقمية، فضلاً عن بعض العاملين في المجالات القانونية أو التقنية التي تتعلق بموضوع الجرائم السيبرانية. ويأتي اختيار هذه الفئة نظراً لارتباطها المباشر بموضوع الدراسة، حيث إن هذه الفئات تعد الأكثر تعرضاً للتعامل مع الأنظمة المعلوماتية والخدمات الرقمية، وبالتالي فهي الأكثر قدرة على تقييم مدى فاعلية التنظيم القانوني للجرائم السيبرانية ودوره في تعزيز الأمن الرقمي، خاصة في ظل تطبيق التشريعات المنظمة لهذا المجال مثل نظام مكافحة الجرائم المعلوماتية.

- الحدود الزمانية

تشير الحدود الزمانية إلى الفترة الزمنية التي يتم خلالها إجراء الدراسة وجمع البيانات وتحليلها. وفي هذه الدراسة تقتصر الحدود الزمنية على الفترة التي يتم خلالها تنفيذ البحث الميداني وجمع البيانات من أفراد عينة الدراسة، وهي الفترة المعاصرة التي تشهد توسعاً كبيراً في استخدام التكنولوجيا الرقمية والخدمات الإلكترونية في مختلف مجالات الحياة. وتكتسب هذه الفترة أهمية خاصة نظراً للتطور السريع في التقنيات الرقمية وتزايد الاعتماد على الإنترنت في

المعاملات اليومية، الأمر الذي أدى إلى ظهور أنماط متجددة من الجرائم السيبرانية. كما تتزامن هذه المرحلة مع الجهود التي تبذلها المملكة العربية السعودية لتعزيز التحول الرقمي وتطوير منظومة الأمن السيبراني، وهو ما يجعل دراسة أثر التنظيم القانوني للجرائم السيبرانية في هذه الفترة ذات أهمية علمية وعملية كبيرة لفهم مدى فاعلية التشريعات القانونية في مواجهة التحديات الرقمية الحديثة.

- الحدود المكانية

تتمثل الحدود المكانية للدراسة في النطاق الجغرافي الذي تُجرى فيه الدراسة ويتم من خلاله جمع البيانات المتعلقة بموضوع البحث. وفي هذا الإطار، تقتصر الدراسة على المملكة العربية السعودية، باعتبارها المجال التطبيقي الذي يتم فيه تحليل التنظيم القانوني للجرائم السيبرانية في ضوء التشريعات المعمول بها. ويأتي اختيار هذا النطاق الجغرافي نظراً لوجود إطار قانوني واضح ينظم التعامل مع الجرائم المعلوماتية، والمتمثل في نظام مكافحة الجرائم المعلوماتية، الذي يمثل الأساس التشريعي لمكافحة الجرائم السيبرانية وحماية الأنظمة المعلوماتية والبيانات الرقمية داخل الدولة. كما أن دراسة هذا الموضوع في السياق السعودي تكتسب أهمية خاصة في ظل التوسع الكبير في الخدمات الرقمية الحكومية والتجارية، وما يتطلبه ذلك من تطوير مستمر للتشريعات القانونية والإجراءات التنظيمية التي تهدف إلى تعزيز الأمن الرقمي وحماية المجتمع من المخاطر المرتبطة باستخدام التكنولوجيا الحديثة.

المراجع

- المراجع العربية:

- الرازق, ر. م. (2023). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية". Retrieved from https://journals.ekb.eg/article_286546.html
- ساتي, أ. م. (2023). الجريمة المعلوماتية في النظام السعودي . Retrieved from <https://aust.uni.ye/article/698/721>
- عطيه, ث. ع. (2024). السياسة الجنائية لمكافحة الجريمة المعلوماتية في المملكة العربية السعودية (دراسة مقارنة) . Retrieved from https://journals.ekb.eg/article_377753_0.html

- المراجع الأجنبية:

- Achuthan, K. (2025). Cybercrime through the public lens: a longitudinal analysis. Retrieved from <https://www.nature.com/articles/s41599-025-04459-x>
- Alahmari, M. (2025). The role of the anti-cybercrime system in the Kingdom of Saudi Arabia in regulating digital media ethics. Retrieved from https://www.researchgate.net/publication/388767343_The_role_of_the_anti-cybercrime_system_in_the_Kingdom_of_Saudi_Arabia_in_regulating_digital_media_ethics
- Alawida, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Retrieved from <https://pmc.ncbi.nlm.nih.gov/articles/PMC9367180/>
- Alhadidi, I. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2405844024084020>
- Alshammari, T. S. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Retrieved from https://www.researchgate.net/publication/329921787_Preparedness_of_Saudi_Arabia_to_Defend_Against_Cyber_Crimes_An_Assessment_with_Reference_to_Anti-Cyber_Crime_Law_and_GCI_Index
- Althibyani, H. A. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. Retrieved from <https://www.mdpi.com/2071-1050/15/15/11512>

- Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. Retrieved from https://www.researchgate.net/publication/382113366_Cybercrime_and_its_Legal_Implications_Analysing_the_challenges_and_Legal_frameworks_surrounding_Cybercrime_including_issues_related_to_Jurisdiction_Privacy_and_Digital_Evidence
- Bacon, L. H. (2023). Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines. Retrieved from <https://www.intechopen.com/chapters/1173031>
- Moafa, F. A. (2026). The Saudi Legal Approach To Cybercrime: A Comparative Analysis Of Cyber Law Evolution, National Security Implications, And Digital Governance In Saudi Arabia And Australia. Retrieved from <https://xlescience.org/index.php/IJASIS/article/view/571>
- Nobanee, H. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. Retrieved from <https://www.emerald.com/jfc/article/30/6/1736/222400/Bibliometric-analysis-of-cybercrime-and>
- Rawindaran, N. (2023). Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. Retrieved from <https://www.mdpi.com/2673-6470/3/3/14>
- Sarkar, G. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2949791423000349>
- Sarkar, G. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context☆. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2949791424000150>
- Suseno, S. (2025). Cybercrime in the new criminal code in Indonesia. Retrieved from <https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2439543>



Midocean Universi
College of Management
Master of Digital Law Specialization

**The Legal Regulation of Cybercrimes and its Impact on Enhancing Digital Security: An Applied
Study in Light of the Anti-Cybercrime Law in the Kingdom of Saudi Arabia**

Prepared by the student/

Amaar Mohamed Aldohian

University ID/

253000792

Year

2026