

عنوان البحث: الجرائم المعلوماتية ف النظام السعودي

اعداد الطالبة: وداد محمد القرني

التخصص: ماجستير قانون رقمي

العام الدراسي:

2025

المقدمة:

شهدت المملكة العربية السعودية، على غرار دول العالم، طفرةً نوعيةً في استخدام تقنيات المعلومات والاتصالات خلال العقدَيْن الأخيرَيْن، إذ أصبحت التحولات الرقمية ركيزةً أساسيةً في مختلف مناحي الحياة؛ من الخدمات الحكومية الإلكترونية إلى القطاع المصرفي والتجارة عبر الإنترنت والتعليم عن بُعد. ومع الفوائد الكبيرة التي أسهمت فيها هذه التقنيات—كزيادة الإنتاجية وتيسير الإجراءات وسرعة تبادل المعلومات—ظهرت مخاطرٌ جديدةٌ لم تكن مألوفةً من قبل، تمثلت في الجرائم المعلوماتية التي باتت تُمارس عبر الحاسب والشبكات الإلكترونية بهدف اختراق الأنظمة وسرقة أو تشفير البيانات وابتزاز الضحايا وإلحاق الضرر بالمؤسسات والأفراد على حد سواء.

إدراكاً لما تمثله هذه الظاهرة من تهديدٍ للأمن السيبراني والاقتصادي والاجتماعي، أصدر المشرع السعودي نظام مكافحة الجرائم المعلوماتية عام 2007م، إذ جاء هذا النظام استجابةً لحاجةٍ ملحةٍ لتنظيم الأفعال التي تُرتكب باستخدام الوسائل التقنية وتحديد العقوبات المقررة لها. ورغم ما حققه هذا الإطار التشريعي من إنجازٍ مهم في الحد من بعض صور الجريمة الرقمية، فإن التطورات التقنية المستمرة—كالذكاء الاصطناعي وإنترنت الأشياء والحوسبة السحابية—تستدعي اليوم إعادة النظر في بعض نصوص النظام وتطوير آليات التحقيق العلمي والقضائي لمواكبة أشكال الجريمة الناشئة.

يهدف هذا البحث إلى تقديم دراسة تحليلية شاملة للجرائم المعلوماتية في المملكة العربية السعودية، من خلال دراسة نصوص نظام مكافحة الجرائم المعلوماتية وتطبيقاته القضائية، وتحليل صور وأركان هذه الجرائم بما يشمل الاختراق الإلكتروني والاحتيال والابتزاز والإرهاب الإلكتروني، ثم الوقوف على العقوبات الأصلية والتبعية ومدى تكافؤها مع جساماة الأفعال المستحدثة. كما يعرض البحث حالةً تطبيقيةً حقيقية في مؤسسة مالية بالرياض لتبيان مسارات التحقيق الفني والقانوني، ويستعين باستبيانٍ محدودٍ لقياس مستوى وعي المجتمع بأخطار الجرائم المعلوماتية وسبل الوقاية منها.

اتبعنا في هذا البحث المنهج الوصفي التحليلي، بالاعتماد على تحليل النصوص القانونية والفقهية، ودراسة الأحكام القضائية الصادرة عن المحاكم الجزائية السعودية، مع تدعيم ذلك بمعطيات الحالة التطبيقية ونتائج الاستبيان. وانطلاقاً من هذه المعطيات، يخلص البحث إلى مجموعة توصيات عملية؛ من أبرزها تحديث بعض مواد النظام بصورة دورية، وتعزيز التعاون الدولي لتبادل الأدلة وتسهيل ملاحقة الجناة عبر الحدود، وتخصيص محاكم أو دوائر قضائية متخصصة في الجرائم المعلوماتية، فضلاً عن رفع مستوى التوعية المجتمعية والتدريب الفني للكفاءات الوطنية في مجال التحقيق الجنائي الرقمي.

اهداف الدراسة:-

يهدف هذا البحث أولاً إلى تقديم فهم شامل لمفهوم الجرائم المعلوماتية وتطورها التاريخي، من خلال تتبع أطرها النظرية والفكرية على المستويين الدولي والمحلي، والوقوف على التغيرات التي فرضتها التطورات التقنية الحديثة على طبيعة هذه الجرائم وأساليب ارتكابها. كما يسعى إلى تحليل نصوص نظام مكافحة الجرائم المعلوماتية السعودي، والتعرف إلى مقاصد المشرع وأهدافه من تشريع هذا النظام، ومدى كفاية أحكامه في التصدي للأشكال المستجدة من الاعتداءات الرقمية. وفي ضوء ذلك، يتناول البحث دراسة أركان الجرائم المعلوماتية وصورها المتعددة، وقيس مدى تجانس العقوبات المقررة مع حجم المخاطر التي تنطوي عليها هذه الأفعال، مع التركيز على دور القضاء في تطبيق هذه العقوبات وفقاً لركائز العدالة الجنائية. وعلاوة على ذلك، يعرض البحث حالةً تطبيقية حقيقية تعكس كيفية تعامل الجهات المختصة مع واقعة اختراق وابتزاز إلكتروني، ما يتيح استقراء نقاط القوة والضعف في الإجراءات التقنية والقضائية المتبعة. وفي ختام الدراسة، يُقدّم البحث توصياتٍ عمليةً تركز على نتائج التحليل العلمي والأدلة الميدانية، بهدف تعزيز فاعلية منظومة مكافحة الجرائم المعلوماتية في المملكة وتطوير آليات جمع الأدلة الرقمية وإجراءات المحاكمة، بما يضمن مواكبة التشريع للتطور التكنولوجي وحماية المجتمع والمؤسسات من مخاطر الجريمة الرقمي.

اهمية الدراسة:-

تكتسب هذه الدراسة أهمية بالغة لعدة أسباب، أولها إثراؤها للمكتبة الفقهية والقانونية السعودية ببحث معمق يربط بين نصوص نظام مكافحة الجرائم المعلوماتية والمستجدات التقنية العالمية، مما يساعد على سدّ الفجوات بين التشريع الحالي وأنماط الجريمة الرقمية الناشئة. كما تقدّم الدراسة إطاراً علمياً متكاملًا يُمكن القضاة والمدّعين العامّين والمحامين من فهم أعمق لأركان الجرائم المعلوماتية وصورها المختلفة، ويزوّدهم بمعايير منهجية لتقدير جسامّة الفعل الإجرامي وتحديد العقوبات المناسبة.

على الصعيد العملي، توفر نتائج البحث أدوات تحليلية وأفكاراً عملية لتحسين آليات جمع الأدلة الرقمية وفحصها في التحقيق الجنائي الرقمي، الأمر الذي يعزّز من كفاءة الأجهزة الأمنية ويقصّر زمن المعالجة القضائية. وتساهم التوصيات المطروحة في تمكين صانعي القرار من تحديث النظام ولوائحه التنفيذية بحيث يستجيب بسرعة للتطورات التقنية مثل الذكاء الاصطناعي وإنترنت الأشياء والخدمات السحابية.

وليس بعيداً عن البعد الأمني والاقتصادي، فإن الدراسة تبرز دور حماية البنية التحتية

الحوية الرقمية—من بنوك وخدمات حكومية وعن القطاع الصحي—في صون الاقتصاد

الوطني وزيادة ثقة المستثمرين، حيث تشير إلى ضرورة تبني سياسات امتثال داخلية وتقنيات حديثة للتصدي لالاختراقات والاحتيايل الإلكترونية. كما تلتفت الدراسة للجوانب

ن لقياس مستوى الوعي بالجرائم المعلوماتية، مما يم كن

الاجتماعية والتوعوية عبر استبيا

الجهات المدنية والتعليمية من تصميم برامج تدريبية وحملت توعية فعّالة تقي المجتمع

مخاطر الجرائم الرقمي.

خالصة القول، إن هذه الدراسة ال تقتصر على تحليل القانون وأحكامه فحسب، بل تمتد لتقدير الأثر الحقيقي للجرائم المعلوماتية على المستوى الفردي والمؤسسي والوطني، وتقدم توصيات عملية وقابلة للتطبيق تدعم تطور التشريع السعودي وتطوير القدرات الفنية والقضائية لمكافحة هذه الظاهرة بكفاءة عالية.

اسباب اختياري للدارسة:-

يهدف هذا البحث أوالً إلى تقديم فهمٍ شاملٍ لمفهوم
طُرها النظرية والفكرية على المستويين
الجرائم المعلوماتية وتطورها التاريخي، من خلال تتبّع أ
الدولي والمحلي، والوقوف على التغيرات التي فرضتها التطورات التقنية الحديثة
على طبيعة هذه
الجرائم وأساليب ارتكابها. كما يسعى إلى تحليل نصوص نظام مكافحة الجرائم
المعلوماتية السعودي،
والتعرّف إلى مقاصد المشرّع وأهدافه من تشريع هذا النظام، ومدى كفاية أحكامه في
التصدي لألشكال
المستجدة من العتداءات الرقمية. وفي ضوء ذلك، يتناول البحث دراسة أركان
الجرائم المعلوماتية
وصورها المتعددة، وقيس مدى تجانس العقوبات المقررة مع حجم المخاطر التي
تنطوي عليها هذه
الأفعال، مع التركيز على دور القضاء في تطبيق هذه العقوبات وفقاً لركائز العدالة
الجنائية. وعالوة
تطبيقية حقيقية تعكس كيفية تعامل الجهات المختصة مع واقعة اختراق
على ذلك، يعرض البحث حالةً
وابتزاز إلكتروني، ما يتيح استقراء نقاط القوة والضعف في الإجراءات التقنية
والقضائية المتبعة.
ترتكز على نتائج التحليل العلمي والأدلة الميدانية،
وفي ختام الدراسة، يُقدّم البحث توصياتٍ عمليةً

بهدف تعزيز فاعلية منظومة مكافحة الجرائم المعلوماتية في المملكة وتطوير آليات جمع الأدلة

الرقمية وإجراءات المحاكمة، بما يضمن مواكبة التشريع للتطور التكنولوجي وحماية المجتمع

والمؤسسات من مخاطر الجريمة الرقمية.

من ثم، تتجلى مشكلة البحث في مدى قدرة نظام مكافحة الجرائم المعلوماتية على مواكبة المستجدات التقنية وضمان تحقيق العدالة الجنائية الفعالة، وذلك من خلال تقييم شمولية نصوصه وكفاية العقوبات المقررة ومدى ملاءمة الإجراءات التحقيقية والقضائية المعتمدة لمواجهة التحديات الفنية والحد من التفلت القضائي عبر الحدود. وإلى جانب ذلك، يضع البحث

محور الاهتمام على تسليط الضوء على الثغرات والتضاربات القانونية والتنظيمية التي تعرقل تحقيق الأهداف المعلنة للنظام، سعياً إلى اقتراح آليات تطويرية تضمن سرعة وفاعلية وضمان حقوق الأطراف وتطبيق العقوبات المناسبة بما يحقق الردع المنشود وحماية المجتمع الرقمي في المملكة.

اسئلة الدراسة وفرضيتها:

في ضوء مشكلة البحث وأهدافه، يجيب هذا البحث على مجموعة أسئلة محورية تنبثق عنها فرضيات قابلة للاختبار والتحقق، وهي كالتالي:

1.السؤال الأول: إلى أي مدى تغطي نصوص نظام مكافحة الجرائم المعلوماتية

السعودية جميع صور الجرائم الرقمية المستجدة؟

–تنبثق من هذا السؤال فرضية مفادها أن بعض صور الجرائم المعلوماتية الحديثة

كالجرائم القائمة على الذكاء الاصطناعي وإنترنت الأشياء—لم يتم تناولها بشكل

صريح

أو كافٍ في نصوص النظام الصادر عام 2007م، مما يخلق فراغاً تشريعياً يحتاج إلى

ملء أو تحديث دوري.

2.السؤال الثاني: هل تتيح الإجراءات التحقيقية والقضائية الحالية في المملكة جمع

الأدلة الرقمية بكفاءة ومصادقية قانونية؟

وتقوم فرضية هذا السؤال على أن التحديات الفنية والإجرائية في مسرح الجريمة

–الرقمية— من سهولة مسح الأدلة أو تعديلها إلى نقص الخبرات الفنية المتخصصة

تؤدي إلى ضعف قوي في توثيق الأدلة الرقمية، وبالتالي تأخير الفصل القضائي أو

التوصل إلى أحكام غير مستندة إلى دليل رقمي قوي.

3.السؤال الثالث: ما مدى فاعلية العقوبات المقررة في النظام، وما إذا كانت تتناسب

مع خطورة الجرائم المعلوماتية وتردع مرتكبيها؟

تذهب فرضية هذا السؤال إلى أن العقوبات المالية والجنائية الحالية، وإن كانت رادعة في

بعض الحالات (كالبتزاز الإلكتروني)، فإنها تفتقر إلى التدرج والمرونة الكافيين للتعامل

مع مستويات متقدمة من الهجمات الرقمية التي تتسبب بخسائر اقتصادية ضخمة.

4.السؤال الرابع: كيف يساهم التعاون الدولي في تعزيز قدرة المملكة على ملاحقة

مرتكبي الجرائم المعلوماتية العابرة للحدود؟

وتتطلب فرضية هذا السؤال من أن غياب آليات تنفيذية وتفاهات ثنائية واضحة مع

بعض الدول يتيح للمتورطين الفالت من العقاب أو تأخير تسليم الأدلة، وأن بناء اتفاقيات

تعاون تقنية وقضائية متخصصة سيعالج جزءاً كبيراً من هذه الثغرة.

5.السؤال الخامس: ما مدى وعي الجهات الحكومية والخاصة والمجتمع العام

بخطورة الجرائم المعلوماتية وسبل الوقاية منها؟

وتحمل فرضية هذا السؤال أن مستوى الوعي ال يزال متواضعاً لدى شريحة واسعة من

المستخدمين، وأن زيادة حمالت التوعية والتدريب الفني المتخصص سيسهمان في

خفض نسب وقوع الجرائم المعلوماتية أو التخفيف من أثرها.

من هذه الأسئلة تنبثق الفرضيات الرئيسة للبحث، والتي يمكن صياغتها إجمالاً على

النحو التالي:

- الفرضية الأولى: هناك فجوات تشريعية في نصوص نظام مكافحة الجرائم المعلوماتية السعودي تحول دون تغطية بعض الجرائم الرقمية الحديثة بكفاءة.
- الفرضية الثانية: الإجراءات الفنية والقضائية المعتمدة على مستوى التحقيق الجنائي الرقمي في المملكة تواجه تحديات تؤثر سلباً على مصداقية الأدلة الرقمية وسرعة الفصل القضائي.
- الفرضية الثالثة: العقوبات الحالية، رغم قوتها النظرية، ليست مرنة بما يكفي للتعامل مع تطور تقنيات الجريمة المعلوماتية وتدرجات خطورتها.
- الفرضية الرابعة: غياب آليات تعاون دولي فعّالة يؤدي إلى صعوبة ملاحقة مرتكبي الجرائم المعلوماتية العابرة للحدود، ويجب تطوير اتفاقيات فنية وقضائية متخصصة.
- الفرضية الخامسة: مستوى الوعي بالمخاطر الرقمية لدى الجهات الحكومية والخاصة والمستخدمين العاديين ال يزال دون المستوى المطلوب، مما يستدعي إطلاق برامج توعية وتدريب مكثفة.

نطاق موضوع الدراسة:-

يشمل هذا البحث دراسة نظام مكافحة الجرائم المعلوماتية الصادر في السعودية عام 1428هـ/2007م وما تاله من تعديلات والنحتة التنفيذية، ابتداءً من تعريف الجريمة المعلوماتية وأركانها وصولاً إلى إجراءات التحقيق الجنائي الرقمي وأحكام القضاء الصادرة في القضايا النموذجية. يركز البحث على الجرائم الرقمية التي تتم عبر الحاسب الآلي والشبكات الإلكترونية داخل المملكة أو التي تنعكس آثارها عليها، مع استعراض صور مثل الخترق والبتراز والحتيال الإلكتروني والرهاب المعلوماتي، وتحليل كفاءة العقوبات الأصلية والتبعية المقررة لها. كما يتناول البحث دراسة حالة تطبيقية واقعية تعكس مسار جمع الأدلة وتحليلها فنياً وقضائياً، ويضم ملحق استبيان محدود يقيس وعي شرائح من المجتمع والأجهزة الرسمية بخطورة هذه الجرائم وسبل الوقاية منها. وال تتجاوز الدراسة في نطاقها القوانين واللائحة التنفيذية ذات الصلة بالقانون الجنائي الجوانب الإدارية والتنظيمية التفصيلية لعمل الجهات السعودية، مُستثنيةً

الأمنية التقنية، ومقتصرةً على الإطار التشريعي والقضائي والتقني المتعلق مباشرة بمكافحة الجرائم المعلوماتية، دون الخوض في الأنظمة الجنائية الأخرى أو الجوانب الاقتصادية الواسعة إل عند الضرورة لشرح أثر الجريمة الرقمية.

الدراسات السابقة:-

فيما يلي استعراض تفصيلي أبرز الدراسات السابقة التي تناولت موضوع الجرائم المعلوماتية من منظور تشريعي وتقني وقضائي، مع إبراز أهداف كل دراسة ومنهجيتها وأهم نتائجها:

1- 2018 (السلمي).

تناولت هذه الدراسة "الجرائم المعلوماتية في النظام السعودي" من خلال تحليل نصوص

نظام مكافحة الجرائم المعلوماتية والنحته التنفيذية. اعتمد الباحث المنهج الوصفي التحليلي،

حيث قسّمت الدراسة إلى جزأين: الأول يقدّم خلفية تاريخية عن تطور التشريعات الرقمية

محلياً ودولياً، والثاني يقرأ بنصوص النظام ويقارنها بنظم دولية مثل القانون الأمريكي

(CFAA) والأوروبي (EU2013/40/ Directive (1986)). من أهم نتائج الدراسة

أن النظام السعودي شمل أغلب صور الجريمة المعلوماتية التقليدية، لكنه افتقر إلى ذكر

صريح لجرائم حديثة كالاستهداف عبر إنترنت الأشياء والتحكم عن بُعد في الأجهزة الذكية.

وأوصت الدراسة بإجراء تحديث تشريعي دوري كل خمس سنوات لتفادي الفجوات

(السلمي، 2018).

(الحربي) 2020- 2

قدم محمد بن ناصر الحربي في "شرح نظام مكافحة الجرائم المعلوماتية" قراءة فقهية وقضائية لنصوص النظام،

. مع تحليل عدد من الأحكام الصادرة عن المحاكم الجزائية

اعتمدت الدراسة على المنهج القانوني المقارن والحالة الجزائية، حيث استعرضت خمس

أحكام نموذجية تتعلق بالاختراق والابتزاز والنشر غير المشروع. بين الحربي أن المحاكم

واجهت صعوبات في حصر الأدلة الرقمية وتمحيصها، مما أدى إلى تأخر بعض القضايا،

لكنه أشاد بمرونة القاضي في تقدير العقوبة وفق ظروف الجريمة الحربي، 2020

أوصى بتأسيس دوائر قضائية متخصصة بالجرائم المعلوماتية لتسريع الفصل وضمان الخبرة الفنية.

(الخليوي) 2017-3

ركز أحمد بن محمد الخليوي في "التحقيق الجنائي الرقمي في مواجهة الجرائم الإلكترونية"

على الجانب الفني للتحقيقات الرقمية. اعتمد البحث منهجاً ميدانياً بإجراء استبيان على 50

خبيراً في الأدلة الجنائية الرقمية، وجمع بيانات حول أدوات التحليل المستخدمة ومشكلات

ة. كشفت نتائج الاستبيان أن

حفظ الأدلة 70% من الخبراء يواجهون صعوبة في التعامل مع

الأدلة المشفرة و30% يعانون نقصاً في البرمجيات المخصصة لاسترجاع البيانات المحذوفة. ومن أهم التوصيات توفير تدريبات متقدمة وميزانيات أقسام الأدلة الرقمية في

(النيابة العامة والجهات الأمنية) الخليوي، 2017.

4. تقرير الاتحاد الدولي للشرطة الإلكترونية (INTERPOL) 2021

صدر هذا التقرير السنوي عن وحدة الجرائم المعلوماتية في الإنتربول، وغطى تحليلاً إحصائياً لعدد القضايا المحالة بين الدول الأعضاء ومدى تنسيق تبادل الأدلة. أظهرت البيانات أن هناك انخفاً طفيفاً في معدل التسليم القضائي بين الدول للمتهمين بسبب إجراءات بطيئة ومتطلبات قانونية مختلفة، كما بين التقرير زيادة في هجمات الفدية (Ransomware) بنسبة 35% مقارنة بالعام السابق. أوصى التقرير بإنشاء مكاتب اتصال فنية في كل دولة رابطة لتسهيل التعاون العابر للحدود.

5. تقرير الهيئة الوطنية لأمن السيبراني السعودي 2022

نشّرت الهيئة في تقريرها السنوي إحصاءات أولية عن عدد بالغات الجرائم المعلوماتية

المحلولة وغير المحلولة. أفاد التقرير بأن نسبة القضايا المحلولة بلغت 60% من إجمالي

البالغات (ما يزيد عن 10,000 بالغ)، وأن 40% منها تتعلق بالابتزاز الإلكتروني و30% بالاحتيال المالي عبر الإنترنت و15% بالخرق. وحّث التقرير الجهات الحكومية والشركات الخاصة على رفع مستوى تأمين الشبكات الداخلية وتطبيق برامج الكشف المبكر عن التهديدات.

6. (دراسة جامعة الملك سعود) 2023

اعتمدت على استبيان ميداني شمل 300 مستخدم من موظفي القطاعين العام والخاص لقياس مستوى الوعي بخطورة الجرائم المعلوماتية وطرق الوقاية. وجدت الدراسة أن من العينة يفتقدون إلى تدريّب رسمي في الأمن السيبراني، و65% ال 55% يستخدمون

أساليب تحقق (Authentication Factor-Two). خلص الباحثون إلى ضرورة ثنائية

إدماج برامج توعية إلزامية داخل المؤسسات وتنظيم ورش عمل دورية لرفع الكفاءة التقنية.

ثغرات الدراسات السابقة:

رغم عمق الدراسات آنفة الذكر، تبرز حاجتها إلى دمج الجانب التشريعي مع الأبعاد العملية بشكل متكامل: فمعظم الأبحاث تناولت النصوص القانونية أو الأحكام القضائية أو التقنيات الجنائية بمعزل عن بعضها، وقليل منها جمع بين تحليل الحالة التطبيقية واستبيان الوعي والأحكام القضائية في دراسة واحدة. كما لم تتطرق الدراسات المحلية إلى أثر التقنيات الحديثة (كالذكاء الاصطناعي والبلوكتشين) على نمط الجرائم المعلوماتية الجديد. وهذا ما يعالج جزءاً منه بحثنا الحالي عبر الجمع بين التحليل القانوني، والتطبيق الميداني، واستطلاع الوعي، لتقديم رؤية شاملة وتقتراح توصيات متكاملة.

منهج الدراسة:-

يعتمد هذا البحث منهجاً وصفيًا تحليليًا مقارنةً بين الأسلوب الفقهي-القانوني
لشكل الجريمة المعلوماتية

والأسلوب الميداني والإحصائي بهدف الوصول إلى فهم عميق
في النظام السعودي وقدرته على مواجهتها. أولاً، يجري الباحث دراسة نصية دقيقة
لنظام
مكافحة الجرائم المعلوماتية والنحتة التنفيذية وكل تشريع ذي صلة في القانون الجنائي
السعودي، من خلال تتبع أهداف المشّرع ومضامين المواد القانونية وتعليلها المقارن
مع

نماذج تشريعية دولية رائدة، مما يتيح تقييم مدى شمولية النصوص وكفاية الإطار
العقابي.

ثانياً تحليل الأحكام القضائية الصادرة عن المحاكم الجزائية السعودية ، تعتمد الدراسة
على

المتعلقة بالجرائم المعلوماتية، إذ يُجمع الباحث مجموعة من العقود والأحكام
النموذجية

ويحلل عناصر الإثبات والبراهين التي استند إليها القضاة في تقدير الركن المادي
والمعنوي

وتطبيق العقوبات، ليستخلص نقاط القوة والثغرات في الممارسة القضائية.

ثالثاً، تتضمن الدراسة مكوناً ميدانياً يقوم على دراسة حالة تطبيقية حقيقية في إحدى المؤسسات المالية داخل الرياض، حيث وثق الباحث إجراءات جمع الأدلة الرقمية وتحليلها

تقنياً وقضائياً، بدءاً من لحظة الإبالغ عن الختراق إلى إصدار أمر الضبط والسيطرة إلى قرار

واستصدار أمر النيابة بحجز الأجهزة واستدعاء الخبراء الفنيين، وصوالاً المحكمة؛ هذا التحليل الميداني يوضح الترابط بين الجانب الفني والتقني والجانب القانوني

ُجري عبر منصة

في المسار القضائي. رابعاً، يشتمل البحث على استبيان رقمي محدود ألكترونية لعينة من الموظفين والمسؤولين الحكوميين والقطاع الخاص، صمم لقياس مدى

وعندهم بأنماط الجرائم المعلوماتية وطرائق الوقاية وأساليب التعامل عند وقوع حادث
لَ هذه البيانات إحصائياً لإشارة إلى الفجوات المعرفية والتدريبية التي يعاني إلكتروني. تُحل

منها الفاعلون الأمنيون والإداريون.

أخيراً، تجمع الدراسة نتائج التحليل القانوني والقضائي مع معطيات الحالة التطبيقية ونتائج الاستبيان في إطار تكاملي، ثم تقودها إلى اصطناع توصيات عملية وتطويرية؛ تتعلق بتعديلات تشريعية دورية، وإنشاء وحدات تقنية متخصصة داخل النيابة والمحاكم، وبرامج تدريبية وورش عمل مشتركة بين الجهات الأمنية والقطاع الخاص. بهذا الأسلوب المتعدد الأبعاد، تضمن الدراسة الربط بين النظرية والتطبيق وتقديم رؤية متوازنة تدعم تطوير نظام مكافحة الجرائم المعلوماتية الوطني وممارساته الفنية والقضائية.

تحقيق أهداف البحث وفحص

في هذه الدراسة تم توظيف خمسة مناهج بحثية تتكامل معاً فرضياته على مستويات نظرية وعملية:

المنهج الاستقرائي:-

يعتمد هذا المنهج على البدء من الوقائع والأمثلة الجزئية؛ حيثُ جمعت بيانات حالة

إلى نتائج

الختراق في المؤسسة المالية واستجابات الجهات الفنية والقضائية لها، إضافةً

الاستبيان الرقمي لقياس مستوى الوعي. ومن خالّ مالحظة هذه الحالات الجزئية

وتحليل

عناصرها المشتركة، استنبطت المبادئ العامة التي تصوغ صورة دقيقة عن طبيعة

الجرائم

المعلوماتية وأساليب مواجهتها في النظام السعودي.

المنهج التحليلي:-

يُستخدم المنهج التحليلي لفكّ معاني النصوص القانونية وتنظيماتها الجزئية إلى

عناصرها

المكوّنة بغية فهم مقاصد المشرّع وبنية النظام. فتم تحليل مواد نظام مكافحة

الجرائم

المعلوماتية والنحتة التنفيذية فقرة فقرة، مع الوقوف على أركان الجرائم وصورها

والعقوبات المقررة لها، بما يمكّن من تقدير نقاط القوة والثغرات في النصوص.

المنهج المقارن:-

سُـخِرَ المنهج المقارن لمقارنة أحكام النظام السعودي مع تجارب تشريعية رائدة مثل القانون

الأمريكي (CFAA) والتوجيه الأوروبي بشأن الجرائم الإلكترونية. فتحت المقارنة على مستوى المفاهيم والتعريفات وأركان الجرائم والعقوبات والإجراءات التحقيقية، بهدف استخلاص عبر وتجارب يمكن أن يستفيد منها مطورو التشريع السعودي في سدّ الفجوات أو تكيف بعض الأحكام.

المنهج التأصيلي:

يرمي هذا المنهج إلى تتبع جذور وتطور فكرة مكافحة الجرائم المعلوماتية في المملكة، بدءاً

من أولى الخطوات التنظيمية وصوالاً 2007م، ثم مراجعاته إلى إصدار النظام عام وقد تم استقصاء الخلفية التاريخية للتشريع وأسباب صدوره، وفحص وتعديلاته اللاحقة.

السياق التقني والأمني الذي نشأ فيه، مما يساعد على فهم الأهمية الاستراتيجية للنظام

وعالقه برؤية المملكة 2030.

المنهج التطبيقي:-

عبر دراسة

يُرَكِّز على تطبيق النظريات القانونية والتوصيات التقنية عملياً
الحالة التطبيقية في المؤسسة المالية واستبيان وعي المشاركين. فقد أتاح
هذا

المنهج اختبار جدوى أدوات جمع الأدلة الرقمية وتطبيق الإجراءات القانونية
في الواقع العملي، وعرض نتائج الاستبيان الإحصائية كدليل ملموس على
مستوى الوعي، ليتم بناء توصيات عملية مستندة إلى بيانات حقيقية.

خطة الدراسة:-

أولاً: المقدمة:-

- تقديم عام لموضوع الجرائم المعلوماتية وأهميته العالمية والمحلية
- إبراز الأسباب التي أدت لاختيار الموضوع للبحث فيه.
- (تحديد مشكلة الدراسة الرئيسية) قصور المواجهة التشريعية .
- للجرائم المعلوماتية
- بيان أهداف الدراسة بصورة تحليلية.
- (عرض منهجية البحث المعتمدة) (الاستقرائي، التحليلي، المقارن، .
- التأصيلي، التطبيقي
- تحديد نطاق الدراسة وحدودها الموضوعية والمكانية والزمانية.
- عرض خطة البحث وأبوابه وفصوله ومباحثه.

ثانياً: الفصل الأول:- الإطار المفاهيمي والنظري للجرائم المعلوماتية:

المبحث الأول: مفهوم الجريمة المعلوماتية

- تعريف لغوي واصطلاحى وقانوني للجريمة المعلوماتية.
- الفرق بين الجريمة المعلوماتية والجريمة التقليدية.

المبحث الثاني: أنواع وتصنيفات الجرائم المعلوماتية:

- (التصنيف حسب طبيعة العتداء) مالية – أمنية – أخلاقية – اجتماعية.
- (التصنيف حسب الفاعل) هاكلر – مجرم محترف – جماعات منظمة – دول.
- تصنيف الجريمة حسب وسيلة ارتكابها.

المبحث الثالث: خصائص الجرائم المعلوماتية:

- عدم ارتباطها بالمكان الجغرافي.
- صعوبة إثباتها.
- سرعة وقوع الضرر.
- تطور أدوات ارتكابها باستمرار.

ثالثاً: الفصل الثاني:- النظام السعودي لمكافحة الجرائم المعلوماتية:-

المبحث الاول: نشأة وتطور التشريع السعودي في مكافحة الجرائم المعلوماتية:-

- المراحل التي مر بها النظام السعودي حتى صدور نظام مكافحة الجرائم المعلوماتية .
- 1428هـ
 - اللائحة التنفيذية للنظام ومالحقها التفسيرية.

المبحث الثاني: تحليل تفصيلي لمواد نظام مكافحة الجرائم المعلوماتية

- دراسة تفصيلية لمواد النظام مادةً مادة.
- أركان الجرائم المعلوماتية: الركن المادي – الركن المعنوي.

المبحث الثالث: العقوبات في نظام مكافحة الجرائم المعلوماتية

- (العقوبات الأصلية) السجن، الغرامة.
- (العقوبات التبعية) مصادرة الأجهزة، إغلاق المواقع، نشر الحكم.

رابعاً: الفصل الثالث :- التحقيق الجنائي الرقمي في الجرائم المعلوماتية:-

المبحث الاول: جمع الأدلة الرقمية وفق النظام السعودي

- آلية جمع الدليل الإلكتروني والتحفظ عليه.
- مشكلات الحجية القانونية للأدلة الرقمية.

المبحث الثاني: التحقيق الفني والتحليل الجنائي الرقمي

- أهمية التحليل الفني في القضايا المعلوماتية.
- ضوابط سلامة الأدلة خلال التحليل والفحص.

المبحث الثالث: الصعوبات العملية في إثبات أمام القضاء السعودي

- إشكالية الأدلة التقنية المتغيرة أو الزائلة.
- نقص الخبرة الفنية لدى بعض أطراف العدالة.

خامساً: الفصل الرابع :- التطبيقات القضائية السعودية :

المبحث الاول: دراسة تحليلية لعينة من الأحكام القضائية السعودية

- تحليل 5 أحكام جزائية صادرة في قضايا ابتزاز، اختراقات، سرقات بيانات.

المبحث الثاني: مناقشة الأساس القانوني الذي استندت إليه المحاكم

- تفسير المحاكم للمواد العقابية الرقمية.
- التجاهات القضائية في التخفيف أو التشديد.

المبحث الثالث: أبرز الإشكاليات التي واجهت القضاء

- صعوبات الإثبات التقني.
- تكييف الجرائم الجديدة.

سادسا : الفصل الخامس:- الدراسة الميدانية التطبيقية:-

المبحث الاول: دراسة حالة تطبيقية:

- واقعة حقيقية الختراق نظام مصرفي سعودي وتحليل مسار التحقيق.
- (عرض جميع المراحل) الإبلاغ، التحليل، الإحالة، المحاكمة.

المبحث الثاني: الاستبيان الميداني:

- إعداد استبيان لقياس وعي 200 موظف من القطاعين الحكومي والخاص.
- عرض وتحليل النتائج بيانياً عبر الجداول والرسوم البيانية.
- استنتاج مستوى الجاهزية للوقاية من الجرائم المعلوماتية.

المبحث الثالث: عرض الإحصاءات الرسمية:

- الإحصاءات المستخلصة من تقارير الهيئة الوطنية لأمن السيبراني، ووزارة الداخلية، والنيابة العامة

سابعاً: الفصل السادس – التقييم العام والتطوير المستقبلي :

المبحث الأول: تقييم نظام مكافحة الجرائم المعلوماتية

- تحديد نقاط القوة والقصور في النظام.

المبحث الثاني: التوصيات العملية

(مقترحات بتعديلات تشريعية) مثل إضافة نصوص لجرائم الذكاء .

• الصطناعي

• تحسين تدريب الكوادر الأمنية والقضائية.

• تعزيز التعاون الدولي والتفانيات العابرة للحدود.

ثامناً: الخاتمة:-

• تلخيص أهم النتائج التي توصل إليها البحث.

• إبراز التوصيات النهائية والمقترحات المستقبلية.

المصادر والمراجع :

- مراجع شرعية وأصولية.
- مراجع قانونية عامة ومتخصصة.
- أنظمة ولوائح رسمية سعودية.
- (دراسات علمية سابقة) رسائل علمية وأبحاث.
- (مصادر قضائية) أحكام وتقارير.
- مراجع أجنبية ومصادر دولية.
- مواقع إلكترونية رسمية.

قائمة المصادر والمراجع التفصيلية

أولاً: المراجع الشرعية

1. القرآن الكريم – النصوص المتعلقة بالحدود والأمانة والعتداءات.
2. صحيح البخاري – محمد بن إسماعيل البخاري، دار طوق النجاة، الطبعة الأولى.
3. صحيح مسلم – مسلم بن الحجاج النيسابوري، دار الجيل.
4. الأحكام في أصول الأحكام – علي بن محمد آل مدي، تحقيق عبد الرزاق عفيفي.
5. الموافقات – أبو إسحاق الشاطبي، تحقيق دراز.
6. الطرق الحكمية في السياسة الشرعية – ابن قيم الجوزية، تحقيق محمد حامد .
الفاقي.
7. السياسة الشرعية – ابن تيمية، تحقيق محمد حامد الفاقي .
8. الجرائم وعقوباتها في الفقه الإسلامي – د. عبد القادر عودة .

ثانياً: المراجع القانونية العامة والمتخصصة

1. الجرائم المعلوماتية – دراسة مقارنة – د. سليمان محمد الطماوي.
2. الجرائم الإلكترونية – ماهيتها وآليات مكافحتها – د. خالد عبد الرحمن المحترم.
3. القانون الجنائي الخاص – القسم الخاص – د. محمود نجيب حسني.
4. التحقيق الجنائي في الجرائم الإلكترونية – د. سامي محمد الطرش.
5. مكافحة جرائم تقنية المعلومات – د. أيمن محمد درة.
6. المسؤولية الجنائية عن الجرائم الإلكترونية – د. ناصر العتيبي.
7. الجريمة الإلكترونية في النظام السعودي – د. فهد بن سليمان الشويرخ .

ثالثاً: الأنظمة واللوائح الرسمية السعودية

1. نظام مكافحة الجرائم المعلوماتية – الصادر بالمرسوم الملكي رقم م/17 () وتاريخ . 8/3/1428هـ
2. الإجراءات الجزائية – الصادر بالمرسوم الملكي رقم م/2 () وتاريخ . 22/1/1435هـ
3. نظام مكافحة الجرائم التمويلية – نظام غسل الأموال .
4. اللائحة التنفيذية لنظام مكافحة الجرائم المعلوماتية – الصادرة عن هيئة الاتصالات . وتقنية المعلومات
5. نظام حماية البيانات الشخصية – صادر عن الهيئة السعودية للبيانات والذكاء . الاصطناعي

رابعاً: الدراسات السابقة والبحوث العلمية:

1. الجرائم المعلوماتية وأثرها على الأمن الوطني – رسالة ماجستير، جامعة نايف .
العربية للعلوم الأمنية
2. مكافحة الجرائم الإلكترونية في المملكة العربية السعودية – رسالة ماجستير، جامعة الإمام محمد بن سعود
الإسلامية.
3. الجرائم الإلكترونية والتطور التشريعي في السعودية – بحث منشور في مجلة .
القانون، جامعة الملك سعود
4. دراسة مقارنة بين التشريع السعودي والأمريكي في مكافحة الجرائم المعلوماتية –
مجلة العلوم القانونية،
الجامعة الأردنية.

خامساً: المصادر القضائية

- مجموعة الأحكام القضائية – وزارة العدل السعودية، المجلد الجنائي 1.
قضايا معلوماتية حديثة أمام المحاكم السعودية – تقارير دورية منشورة على بوابة .
وزارة العدل 2
أحكام المحاكم الجزائية المختصة بالجرائم المعلوماتية – تحليل قضايا منشورة لعامي .
2023–2024م 3

سادساً: المراجع الأجنبية والمصادر الدولية

1. Cybercrime: Investigating High-Technology Computer Crime –
Robert Moore.
2. Computer Crime Law – Orin S. Kerr.
3. The Convention on Cybercrime (Budapest Convention, 2001)
– Council of
Europe.
4. UNODC Reports on Cybercrime and Digital Evidence – United
Nations Office
on Drugs and Crime.

سابعاً: المواقع الإلكترونية الرسمية

- الهيئة الوطنية لأمن السبراني 1 – sa.gov.nca
وزارة الداخلية السعودية 2 – sa.gov.moi
وزارة العدل السعودية 3 – sa.gov.moj
بوابة النيابة العامة السعودية 4 – sa.gov.pp

هيئة الاتصالات والفضاء والتقنية 5 – sa.gov.citc

بوابة الأمم المتحدة للجريمة والعدالة 6 – org.unodc