

الجرائم السيبرانية في نظام مكافحة الجرائم المعلوماتية السعودي

دراسة تأصيلية تحليلية مقارنة لأحكام نظام مكافحة الجرائم المعلوماتية
وتطبيقاته القضائية

إعداد الطالب:	المقداد بن صالح المقرن
المرحلة الأكاديمية:	الماجستير في القانون الرقمي
الكلية والتخصص:	كلية العلوم الإنسانية - قسم القانون
المشرف الأكاديمي:	قسم الدراسات القانونية العليا
العام الدراسي:	1447 هـ - 1448 هـ / 2025 م - 2026 م

خطة البحث والملخصات (Research Framework & Abstracts)

ملخص البحث

تناول هذا البحث موضوع "الجرائم السيبرانية في نظام مكافحة الجرائم المعلوماتية السعودي"، بهدف إبراز الأطر القانونية والنظامية التي اعتمدها المشرع السعودي لمواجهة التحديات الأمنية الناشئة عن طفرة التقنية المتسارعة وانتشار الفضاء السيبراني. اعتمدت الدراسة على المنهج التحليلي التأصيلي المقارن للنصوص النظامية الصادرة بالمرسوم الملكي رقم (م/17) وتاريخ 8/3/1428هـ، مع تفكيك الأركان القانونية للجرائم المعلوماتية وصور الاعتداء على الأنظمة والبيانات والأفراد، وبيان العقوبات التدرجية والتدابير الوقائية والمصادرة وإجراءات الإثبات الرقمي. وتتوصل الدراسة إلى أن النظام السعودي يقدم نمطاً تشريعياً متكاملاً يوازن بين حماية الحقوق والحريات الرقمية وصيانة الأمن القومي للبنية التحتية الحيوية، مع تقديم توصيات تفصيلية لتحديث النظام لمواكبة تقنيات الذكاء الاصطناعي والتزييف العميق والعملات الرقمية المشفرة.

Abstract

This study examines "Cybercrimes in the Saudi Anti-Cybercrime Law", aiming to highlight the legal and regulatory frameworks adopted by the Saudi legislator to address cybersecurity threats arising from rapid technological advancements. Utilizing an analytical and foundational comparative methodology, the paper evaluates Royal Decree No. (M/17) dated 8/3/1428H. It dissects the legal elements of cyber offenses, categories of attacks against system integrity and individual rights, digital evidence standards, and the scale of statutory penalties and preventative measures. The findings indicate that Saudi law provides a robust framework balancing digital rights protection with national security, while emphasizing the critical need for statutory updates addressing artificial intelligence, deepfakes, and digital currency offenses.

أهمية البحث (Research Importance)

تكمن أهمية البحث في المزاوجة بين الجانب التطبيقي العملي والتأصيل الفقهي النظامي، حيث يوفر للممارس القانوني، والقاضي، والباحث الأكاديمي فهماً عميقاً وشاملاً

لنصوص نظام مكافحة الجرائم المعلوماتية السعودي والأنظمة المكملة له. وتزداد هذه الأهمية تسارعاً مع التحول الرقمي الشامل الذي تشهده المملكة العربية السعودية وفق رؤية 2030، وما يرتبط به من ضرورة حماية البنية التحتية الحساسة، وضمان أمان المعاملات المالية والتجارية الإلكترونية، وصيانة حرمة الحياة الخاصة للأفراد والمجتمع ضد الاختراقات والجرائم العابرة للحدود.

مشكلة البحث (Research Problem)

تتلور مشكلة البحث في التساؤل المباشر والمركز عن مدى كفاية وقدرة النصوص النظامية الحالية في "نظام مكافحة الجرائم المعلوماتية السعودي" الصادر عام 1428هـ على استيعاب وتجريم الأشكال الحديثة والمستحدثة للجرائم السيبرانية ذات الخصائص الفنية المعقدة (مثل الجرائم العابرة للحدود، السرعة الفائقة في التنفيذ، التخفي البرمجي، استخدام تقنيات الذكاء الاصطناعي)، وما إذا كانت الأركان والعقوبات المقررة قادرة على تحقيق الردع بشقيه العام والخاص، ومدى الحاجة لسد الفجوات التشريعية الإجرائية والموضوعية.

تساؤلات البحث (Research Questions)

تسعى هذه الدراسة للإجابة عن التساؤلات الرئيسة والفرعية التالية:

- ما الماهية القانونية للجريمة السيبرانية في النظام السعودي، وما أبرز خصائصها الفنية والشرعية؟
- ما هي الصور والأشكال التشريعية للجرائم الواقعة على البيانات والأنظمة والمؤسسات وفق التبويب النظامي السعودي؟
- ما هي الصور الأشكال للجرائم الواقعة على الأفراد وحقوقهم وحرمة حياتهم الخاصة؟
- كيف تتحدد الأركان القانونية (النظامي، المادي، المعنوي) المؤسسة للمسؤولية الجزائية في الجريمة المعلوماتية؟

- ما هي طبيعة حجية الدليل الرقمي وإجراءات ضبط المعايينات والتحقيق في الفضاء السيبراني؟
- ما مدى تناسب العقوبات الأصلية والتبعية والتدابير الوقائية والمصادرة المقررة في النظام مع جسامة الجرم المستحدث؟

أهداف البحث (Research Objectives)

- تأصيل المفاهيم القانونية والفنية المنظمة للفضاء السيبراني في التشريع والقضاء السعودي.
- تصنيف واستعراض صور الاعتداء الإلكتروني الموجه ضد الأنظمة الوطنية البنكية والخدمية والأشخاص.
- تفكيك الأركان الجنائية العامة والخاصة المؤسسة للمسؤولية الجزائية السيبرانية وبيان قصد الإضرار.
- تحليل آليات الإثبات الرقمي وقواعد التعامل مع الأدلة الإلكترونية والتفتيش الرقمي وفق الأنظمة السعودية.
- تقديم توصيات علمية وعملية للمشروع والأجهزة القضائية والأمنية لمواكبة التطورات التقنية الحديثة.

منهجية البحث (Methodology)

يعتمد الباحث على المنهج التحليلي التأصيلي المقارن، وذلك من خلال استقراء مواد نظام مكافحة الجرائم المعلوماتية السعودي، ونظام الإثبات، ونظام الإجراءات الجزائية، والأنظمة ذات الصلة، وتحليل الآراء الفقهية والأحكام والقرارات القضائية الصادرة عن المحاكم السعودية، للوصول إلى استنتاجات علمية دقيقة وتوصيات تشريعية عملية.

المبحث الأول: ماهية الجرائم السيبرانية وخصائصها الفنية والقانونية

المطلب الأول: التعريف المفهومي والتأصيلي للجريمة السيبرانية

تُعرّف الجريمة السيبرانية (Cybercrime) في أصلها المفهومي الأكاديمي والفقهي بأنها كل فعل إجرامي غير مشروع يتخذ من الحواسيب، أو الشبكات المعلوماتية، أو الوسائط الإلكترونية والبرمجية أداة للارتكاب، أو موضوعاً وهدفاً منصّباً عليه بالاعتداء والتعطيل.

وفي إطار التشريع السعودي، عرّف المشرع الجريمة المعلوماتية في المادة الأولى من نظام مكافحة الجرائم المعلوماتية (الصادر بالمرسوم الملكي رقم م/17 وتاريخ 8/3/1428هـ) بأنها:

"أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية معالجة أو نقل أو تخزين، بالمخالفة لأحكام هذا النظام".

ويلاحظ من الشرح القانوني والتحليلي لهذا التعريف أن المشرع السعودي اعتمد المفهوم المزدوج الموسع للجريمة المعلوماتية؛ بحيث يشمل الأفعال التي تكون التكنولوجيا فيها وسيلة للارتكاب (كالابتزاز، الاحتيال المالي، والتشهير عبر المنصات الرقمية والتطبيقات)، والأفعال التي تكون التكنولوجيا فيها هي المعصوم المستهدف بالاعتداء ذاته (كالاختراق، إتلاف البيانات، وتخريب الخوادم والأنظمة البنكية والسيادية).

وتتصف هذه الجريمة بالذكاء التقني العالي؛ إذ تتطلب من مرتكبها قدرات تقنية في التعامل مع البرمجيات والشبكات والتشفير، مما يستوجب مقابلة هذا الذكاء بآليات تحقيق وأدلة إثبات رقمية على قدر مماثل من التخصص والدقة الفنية من جانب السلطات القضائية وضباط الضبط الجنائي.

المطلب الثاني: الخصائص المميزة للجريمة السيبرانية عن الجرائم التقليدية

تتفرد الجريمة السيبرانية بجمعها بين خصائص فنية ونظامية فريدة تجعلها تشكل تحدياً أمنياً وقضائياً مستمرًا للسلطات القضائية عبر العالم، ويمكن إيجاز أهم هذه الخصائص التأصيلية في النقاط التالية:

1. **اللامكانية والعبور للحدود (الجريمة العابرة للقارات)** تعترف الجريمة السيبرانية بالحدود الجغرافية والسياسية بين الدول؛ إذ يمكن للجاني المتواجد في دولة ما أن يهاجم خوادم بنك أو مؤسسة حكومية في دولة أخرى تفصله عنها آلاف الكيلومترات، مما يثير إشكاليات تنازع الاختصاص القضائي والقانون الواجب التطبيق بين الدول وآليات تسليم المجرمين.

2. **السرعة الفائقة وسهولة محو الأثر** نفذ الأفعال الإجرامية في أجزاء من الثانية عبر أوامر برمجية سريعة، كما يستطيع الجاني طمس معالم جرمه ومحو الأدلة الرقمية المسجلة عبر خوادم السجلات (Log Files) أو استخدام برامج التشفير والشبكات الافتراضية الوهمية (VPN) والشبكة المظلمة (Dark Web) بضغط زر واحدة.

3. **انخفاض التكلفة وارتفاع حجم الأضرار** يحتاج المجرم السيبراني إلى جيوش أو أسلحة تقليدية مكلفة، بل يكفي حاسوب شخصي واتصال بالإنترنت ليحدث خسائر بمليارات الدولارات للمؤسسات والشركات والأفراد، مما يجعل النسبة بين جهد الجاني والنتيجة الإجرامية الخارقة غير متكافئة إطلاقاً.

4. **الطابع الخفي وغياب العنف المادي الظاهر**: الجريمة السيبرانية بالهدوء والتخفي، حيث لا تخلف وراءها دماءً أو كسر أبواب أو بصمات أصابع تقليدية، بل تخلف آثارات برمجية وأكواد مشفرة في عالم افتراضي لا يرى بالعين المجردة، مما يستوجب خبرة جنائية تقنية متخصصة للتعرف عليها واستخراجها.

5. **التطور المتسارع واستحداث صور إجرامية جديدة** تتطور أساليب الجريمة السيبرانية بشكل يومي بالتوازي مع التطور التكنولوجي، حيث ظهرت صور جديدة كالاختيال عبر الذكاء الاصطناعي والتزييف العميق (Deepfake) والتعدين غير المشروع

للعملات الرقمية، وهو ما يفرض تحدياً مستمراً لمبدأ الشرعية الجنائية "لا جريمة ولا عقوبة إلا بنص".

تحليل الباحث: دلالة التطور التقني على مبدأ الشرعية

يُفهم من معالجة العملات الرقمية في سياق الجرائم المعلوماتية أن المشرّع لا يستطيع أن يكتفي بتعداد صور الاعتداء التقليدية، بل يحتاج إلى صياغة قانونية تستوعب الوسيلة التقنية الجديدة دون أن تتحول المرونة إلى تجريم بغير نص. ومن ثم فإن الأساس التحليلي هو التوفيق بين مبدأ الشرعية الجنائية وبين التطور المستمر للوسائل الرقمية.

وتتأكد هذه النتيجة بالرجوع إلى نظام مكافحة الجرائم المعلوماتية السعودي، وإلى ما طرحته الأدبيات الحديثة حول تحديث الحماية الجزائية للأمن السيبراني؛ فالمعيار ليس اسم التقنية في ذاته، وإنما السلوك الضار الذي ينال من سلامة البيانات أو الأنظمة أو الحقوق الخاصة. ويؤدي هذا الفهم إلى حماية النص من التقادم السريع مع بقاء التجريم منضبطاً بحدوده القانونية.

وعليه، فإن الاتجاه الأنسب تشريعياً هو تحديث النصوص عند ظهور صور إجرامية جديدة، مع الاستفادة من الأطر التنظيمية للأمن السيبراني في الجانب الوقائي. وهذا الربط بين التجريم والوقاية ينسجم مع الغرض العام للنظام ومع التقارير التنظيمية للهيئة الوطنية للأمن السيبراني. المصادر: 2، 6، 9 في قائمة المراجع.

المبحث الثاني: صور وأشكال الجرائم المعلوماتية في النظام السعودي

المطلب الأول: الجرائم الواقعة على البيانات والأنظمة المعلوماتية والبنية التحتية

تستهدف هذه الفئة من الجرائم سلامة، وسرية، وتوافر البيانات والأنظمة والشبكات، وتعد من أشد الجرائم خطورة لكونها تمس البنية التحتية الرقمية للدولة، والمؤسسات المالية، والمرافق الحيوية، وتتحقق في الصور التشريعية التالية وفق نظام مكافحة الجرائم المعلوماتية:

أولاً: الدخول غير المشروع والاختراق (Unauthorized Access & Hacking)

جرم المشرع السعودي في المادة الثالثة والرابعة والخامسة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي أو حاسب آلي دون تسويق نظامي. ويشمل ذلك تجاوز إجراءات الحماية والتشفير للاطلاع على البيانات، أو الحصول على معلومات سريعة تخص الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني، أو المساس بالبيانات البنكية والتجارية.

ثانياً: إتلاف البيانات وتسريبها وتغيير مضمونها (Data Damage & Ransomware)

يتضمن ذلك القيام بمسح البيانات أو تعديلها أو إلغائها أو تسريبها دون إذن صاحب الحق. وتدخل في هذا الإطار هجمات "برمجيات الفدية" (Ransomware) الحديثة، حيث يقوم الجاني بتشفير بيانات المؤسسة أو الفرد قسراً ومطالبته بمبالغ مالية مقابل إعطاء مفتاح التفكيك، وهو ما يشكل جمعاً بين إتلاف البيانات والابتزاز المالي.

ثالثاً: تعطيل الأنظمة والشبكات وهجمات حجب الخدمة (DDoS Attacks)

يقصد بتعطيل الأنظمة القيام بأفعال تؤدي إلى إيقاف الحاسب الآلي أو الشبكة عن العمل أو إعاقتها أو إغراق الخوادم والمواقع الإلكترونية الحكومية والبنكية بسيل هائل من

الطلبات الوهمية، مما يؤدي إلى شل حركة الخدمات الإلكترونية وحرمان المستفيدين من الوصول إليها، ويعد ذلك من جرائم التخريب الرقمي الخطيرة.

رابعاً: الاعتداء على المواقع الإلكترونية والوسوم المعتمدة

يشمل إعاقة الوصول إلى الموقع، أو تغيير تصميمه، أو إلغائه، أو تعديل محتواه، أو شغل عنوانه دون وجه حق، أو انتحال شخصية موقع حكومي أو رسمي لخداع المستخدمين وجمع بياناتهم الشخصية والائتمانية.

المطلب الثاني: الجرائم الواقعة على الأفراد والأموال وحقوقهم الشرعية والنظامية

حرص المشرع السعودي في نظام مكافحة الجرائم المعلوماتية على صيانة حرمة الحياة الخاصة للأفراد، وحماية أعراضهم وأموالهم المصونة شرعاً ونظاماً، وتنقسم الجرائم الموجهة ضد الأفراد إلى المحاور الأساسية التالية:

أولاً: الابتزاز الإلكتروني والتهديد (Cyber Extortion)

يتحقق الابتزاز باستغلال التقنية الحديثة والشبكات لتهديد الشخص أو مساومته بنشر صور فوتوغرافية، أو مقاطع فيديو، أو معلومات خاصة أو محادثات سرية تمس كرامته أو سمعة عائلته، وذلك لحثه على دفع مبالغ مالية أو القيام بأعمال غير مشروعة أو الامتثال لإملاءات تنافي إرادته وحرية. وقد أفرد المشرع عقوبات صارمة لهذه الجريمة للحفاظ على الاستقرار الاجتماعي.

ثانياً: التشهير والمساس بالحياة الخاصة (Defamation & Privacy Violation)

استخدام المنصات الرقمية ووسائل التواصل الاجتماعي (مثل منصة X، سناب شات، واتساب وغيرها) للإساءة إلى الآخرين، أو التشهير بهم، أو نشر أخبار ومعلومات كاذبة تهدف إلى حط قدرهم أو المساس بكرامتهم وشرفهم وشخصيتهم الاجتماعية أو المهنية. كما يشمل ذلك المساس بالحياة الخاصة عن طريق التجسس أو التقاط الصور ومقاطع الفيديو دون علم أصحابها ونشرها.

ثالثاً: الاحتيال المالي الإلكتروني والاستيلاء على الأموال (Cyber Fraud)

يتجسد الاستيلاء على أموال الآخرين أو الاستحواذ على سندات مالية باستخدام طرق احتيالية عبر الحاسب أو الشبكة، مثل إنشاء صفحات وبوابات دفع وهمية تشبه البنوك والمؤسسات الرسمية (Phishing)، أو استخدام أساليب الهندسة الاجتماعية (Social Engineering) لسحب (OTP) لاستدراج الضحايا والإفصاح عن الأرقام السرية ورموز التحقق (OTP) للمبالغ من حساباتهم.

رابعاً: انتحال الشخصية الرقمية واستخدام الهويات المسروبة

استخدام بيانات هوية شخص آخر أو حساباته الرقمية دون إذنه للقيام بمعاملات تجارية، أو نشر محتويات مسيئة، أو التواصل مع الآخرين باسمه، مما يلحق بالضحية أضراراً أدبية ومالية ونظامية بليغة.

المبحث الثالث: الأركان القانونية للجرائم السيبرانية والشروع فيها

المطلب الأول: الركن المفترض والركن المادي والجاسوسية الرقمية

تقوم المسؤولية الجزائية عن الجرائم السيبرانية على توافر الأركان العامة للجريمة، إضافة إلى الخصوصية الرقمية التي يتطلبها نظام مكافحة الجرائم المعلوماتية السعودي:

1. الركن المفترض (البيئة الرقمية):

يشترط لممارسة هذا النوع من الجرائم وجود بيئة تقنية معالجة أو ناقلة أو مخزنة للبيانات (حاسب آلي، شبكة معلوماتية، موقع إلكتروني، أو شريحة ذكية). فإذا وقع الفعل الوسيلة أو الموضوع بأساليب تقليدية دون تدخل التقنية، خرج الفعل عن نطاق تطبيق نظام مكافحة الجرائم المعلوماتية وخضع للقواعد الجزائية العامة.

2. الركن المادي (Actus Reus):

يتكون الركن المادي في الجريمة السيبرانية من عناصر ثلاثة رئيسية:

- **السلوك الإجرامي (الفعل الإيجابي أو الامتناع)** يتمثل في أفعال الاختراق، الدخول غير المشروع، نسخ البيانات، مسح الملفات، التهديد، أو النقر على أوامر تنفيذية ضارة.
- **النتيجة الإجرامية الضارة** الضرر المحقق الذي يلحق بالمجني عليه (سواء كان ضرراً مادياً كفقْدان الأموال وإتلاف الأنظمة، أو أدبياً كالمساس بالسمعة والحياة الخاصة).
- **رابطة السببية:** ثبوت أن النتيجة الضارة الحاصلة كانت سبباً مباشراً للسلوك الرقمي غير المشروع الذي اقترفه الفاعل عبر التقنية.

المطلب الثاني: الركن المعنوي والشرع والمشاركة الإجرامية

1. الركن المعنوي (القصد الجنائي - Mens Rea):

تعد الجرائم السيبرانية في أغلب صورها من الجرائم العمدية التي تتطلب توافر القصد الجنائي بعنصره:

- **العلم** الفاعل خطورة سلوكه وتوجهه نحو خرق حماية نظام إلكتروني أو الدخول بدون وجه حق، وعلمه بأن الفعل مجرم نظاماً ويحدث ضرراً للغير.
- **الإرادة** إرادة الفاعل بحرية واختيار كاملين نحو القيام بالسلوك الإجرامي وتحقيق النتيجة الضارة، مع انتفاء حالة الخطأ غير العمدية أو حسن النية (مثل الدخول العرضي نتيجة خلل في العنوان أو الشبكة دون قصد الاختراق).

2. الشرع والمشاركة الإجرامية (Attempt & Complicity):

أكد المشرع السعودي في المادة التاسعة من نظام مكافحة الجرائم المعلوماتية على تجريم الشرع والتحريض والمساعدة والاتفاق؛ حيث ينص النظام على عقاب كل من حرّض غيره، أو اتفق معه، أو ساعده على ارتكاب أي من الجرائم المنصوص عليها في النظام بعقوبة لا تتجاوز الحد الأعلى للعقوبة المقررة للجريمة نفسها إذا وقعت الجريمة، وبما لا يتجاوز نصف الحد الأعلى إذا لم تقع الجريمة الشرع.

المبحث الرابع: الإثبات الرقمي وإجراءات التفتيش والضبط السيبراني

المطلب الأول: حجية الدليل الرقمي في النظام القضائي السعودي

يحتل الدليل الرقمي (Digital Evidence) مكان الصدارة في الإثبات الجنائي الجرائم السيبرانية. والدليل الرقمي هو كل معلومات أو بيانات مترجمة أو مخزنة إلكترونياً تتمتع بالحجية القانونية أمام القضاء لإثبات وقوع الجريمة ونسبتها إلى فاعلها.

وقد نظم المشرع السعودي حجية المحررات والأدلة الرقمية في "نظام الإثبات" الصادر بالمرسوم الملكي رقم (م/43) وتاريخ 26/5/1443هـ، حيث نصت المواد على أن الدليل الرقمي يتمتع بالحجية الكاملة في الإثبات متى ما سلم من التعديل والعبث وتوافرت فيه الشروط الفنية والموثوقية. وتشمل الأدلة الرقمية المقبولة قضائياً:

- السجلات البرمجية المعتمدة (Log Files) الصادرة من خوادم الاتصالات والشركات المزودة.
- العناوين البروتوكولية للشبكة (IP Address) والمعرفات الفريدة للأجهزة (MAC Address).
- الرسائل الإلكترونية، والمحادثات الموثقة عبر منصات التواصل (WhatsApp, X, Email).
- الصور المأخوذة من التحليل الجنائي للذاكرة العشوائية والقرص الصلب (Forensic Imaging).
- التوقيع الرقمي والشهادات الإلكترونية الصادرة عن جهات توثيق معتمدة.

المطلب الثاني: ضوابط التفتيش والتحري والمعاينة الفنية للأجهزة

نظراً لطبيعة الأدلة الرقمية الدقيقة وسهولة تلفها أو تغييرها، وضع التشريع السعودي ضوابط صارمة لإجراءات الضبط والتفتيش الرقمي صيانة لحريات الأفراد وضماناً لسلامة الأدلة أمام المحكمة:

1. الإذن القضائي بالتعقب والتفتيش:

يشترط لوصول جهات ضبط الجرائم والمختصين إلى المحتويات الرقمية والتفتيش الأجهزة الشخصية الحصول على إذن كتابي من النيابة العامة وفقاً لأحكام نظام الإجراءات الجزائية، إلا في حالات التلبس الشديد المحددة نظاماً.

2. إجراء المعاينة الفنية والتحليل الجنائي الرقمي:

تتولى الفرق الميدانية المتخصصة التابعة للهيئة الوطنية للأمن السيبراني أو النيابة العامة والأجهزة الأمنية التحفظ على الأجهزة الإلكترونية المشتبه بها، واستخراج نسخة طبق الأصل (Bit-stream Image) دون إجراء أي تعديل على وحدة التخزين الأصلية لضمان سلامة الهاش الفني (Hash Value) واستمرار سلسلة الحيازة (Chain of Custody).

3. حماية السرية وعدم انتهاك الخصوصية:

يلتزم ضباط الضبط والخبراء الفنيون باقتصار التفتيش والمعاينة على البيانات المتعلقة بموضوع الجريمة محل التحقيق، وعدم الاطلاع أو الكشف عن خصوصيات الضحايا أو أطراف القضية التي لا صلة لها بالدعوى الجنائية.

المبحث الخامس: عقوبات الجرائم السيبرانية والتدابير الوقائية والمصادرة

المطلب الأول: العقوبات الأصلية والمشددة وفق نظام مكافحة الجرائم المعلوماتية

اعتمد المشرع السعودي سياسة عقابية تدرجية تتناسب مع جسامة الفعل الإجرامي ومدى الخطر الناتج عنه على الأفراد أو البنية التحتية للدولة. ويمكن تصنيف العقوبات الأصلية إلى درجات تتراوح بين السجن والغرامة المالية أو بهما معاً.

مادة النظام	نوع الجريمة والموضوع	عقوبة السجن (الحد الأعلى)	الغرامة المالية (الحد الأعلى)
المادة الثالثة	التنصت، الدخول غير المشروع دون إلحاق ضرر، الابتزاز، اختراق المواقع، التشهير والاعتداء على الحياة الخاصة.	سنة واحدة	500,000 ريال سعودي
المادة الرابعة	الاستيلاء على الأموال عن طريق الاحتيال المالي، أو الوصول غير المشروع لإلغاء وتعديل البيانات البنكية.	3 سنوات	2,000,000 ريال سعودي
المادة الخامسة	إتلاف البيانات، إلغاؤها، تسريبها، تعطيل الشبكات والخوادم، وإعاقة الخدمات الحكومية.	4 سنوات	3,000,000 ريال سعودي
المادة السادسة	إنتاج أو إعداد أو إرسال ما يمس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة.	5 سنوات	3,000,000 ريال سعودي
المادة السابعة	الدخول غير المشروع لمواقع منظمة، اختراق البيانات السيادية، أو خوادم الأمن الوطني والاقتصاد القومي.	10 سنوات	5,000,000 ريال سعودي

ظروف التشديد العقابي (Aggravating Circumstances):

نصت المادة الثامنة من النظام على ظروف تشديدية ترفع العقوبة إلى حدها الأعلى أو تزيد عليها، ومن أهمها:

- ارتكاب الجريمة من خلال عصابة منظمة إجرامية.
- استغلال الفاعل لسلطته الوظيفية أو نفوذه أو صلاحيات عمله (كالمهندس أو المسؤول عن الأنظمة).
- اقتران الجريمة بالتغريب بالقاصرين أو استغلال الفئات الضعيفة.
- وقوع الجريمة على المنشآت الحساسة كالمستشفيات، القواعد العسكرية، أو الخوادم السيادية للدولة.

المطلب الثاني: العقوبات التبعية والتدابير الوقائية وإغلاق المواقع والمصادرة

لم يكتف المشرع بالعقوبات الأصلية، بل أقر تدابير عقابية وإحرازية لضمان عدم عودة الجاني لارتكاب الجريمة وحماية المجتمع:

1. المصادرة (Confiscation):

توجب المادة الثالثة عشرة من النظام مصادرة الأجهزة، والبرامج، والوسائط، والأدوات المستخدمة في ارتكاب الجريمة، أو الأموال والمتحصلات الناشئة عنها لصالح الخزينة العامة للدولة، دون إخلال بحقوق الغير حسني النية.

2. إغلاق المواقع والحسابات وحظر الاستخدام:

تتضمن الأحكام القضائية إغلاق المحل أو الموقع الإلكتروني أو الحساب المستغل في ارتكاب الجريمة إغلاقاً نهائياً أو مؤقتاً، وحرمان الجاني من استخدام الوسائل التقنية لفترات محددة لمنع تكرار النشاط الإجرامي.

3. نشر ملخص الحكم (التشهير المحكوم به قضائياً):

يجوز للمحكمة المختصة النص في حكمها الجزائي على نشر ملخص الحكم على نفقة المحكوم عليه في إحدى الصحف المحلية أو الوسائط الرقمية المعتمدة بعد اكتساب الحكم الصفة النهائية، وذلك ليكون زاجراً للجاني ورادعاً لغيره.

تحليل الباحث: نشر ملخص الحكم كأداة ردع وحدودها

يظهر من النص أن نشر ملخص الحكم ليس مجرد إجراء إعلامي، بل هو جزء تكميلي يهدف إلى إظهار النتيجة القضائية وتعزيز الردع العام في الجرائم التي ترتكب عبر الوسائط الرقمية. غير أن فعالية النشر لا تُقاس باتساعه فقط، وإنما بمدى تناسبه مع جسامة الفعل وطبيعته والآثار التي يمكن أن تترتب على إعلان البيانات المرتبطة بالمحكوم عليه.

ومن زاوية الحقوق، ينبغي أن يظل النشر محكوماً بفكرة التناسب؛ فحماية الخصوصية لا تتعارض مع الردع، وإنما تحدد طريقة ممارسته. ولذلك فإن نشر ملخص الحكم، لا الحكم بكامل تفاصيله، يمثل في الأصل وسيلة لتحقيق التوازن بين المصلحة العامة في معرفة الجزاء وبين تقليل المساس بالحياة الخاصة.

ويؤيد هذا التحليل الربط بين أحكام نظام مكافحة الجرائم المعلوماتية وبين الدراسات المتعلقة بالحماية الجنائية للحياة الخاصة؛ كما أن قيمة النشر الردعية تزداد عندما يقتدرن بحكم نهائي وبصياغة مختصرة لا تتجاوز الغرض الذي أُجيز من أجله. المصادر: 2 و5 في قائمة المراجع.

المبحث السادس: التطبيقات القضائية والتحليل المقارن في الأحكام السعودية

المطلب الأول: قضايا الابتزاز والتسريب والتشهير الإلكتروني في القضاء الجزائي

تزر المحاكم الجزائية السعودية بالعديد من التطبيقات القضائية الفريدة التي تعكس التطبيق الدقيق لنظام مكافحة الجرائم المعلوماتية. ومن خلال استقراء نماذج من المبادئ القضائية المعتمدة:

التطبيق الأول: قضية ابتزاز وتديد عبر وسائل التواصل:

تتلخص وقائع إحدى القضايا في إقدام مدعى عليه على تهديد مجني عليها بنشر صورها ومحادثاتها الخاصة على منصة (سناب شات) ما لم تقم بدفع مبالغ مالية متكررة. وبإحالة القضية للمحكمة الجزائية وتطبيق المادة الثالثة (الفقرة 2)، أصدرت المحكمة حكماً بسجن المتهم لمدة تسعة أشهر وتغريمه بمبلغ 50,000 ريال، مع مصادرة هاتف المحمول المستخدم في الجريمة وإلغاء حسابه، مؤكدة المحكمة في حثياتها على ردع سلوكيات التهديد والمساس بالحرمان الخاصة.

التطبيق الثاني: قضية إعادة نشر مقاطع تشهير واسعة:

في قضية أخرى، قام شخص بتصوير أحد العاملين في منشأة تجارية دون إذنه ونشر المقطع مصحوباً بعبارات قذف وتشهير وتزييف للحقائق على منصة (X). وقضت المحكمة بسجنه لمدة 6 أشهر وتغريمه 30,000 ريال بناءً على المادة الثالثة (الفقرة 5)، مع نص الحكم على نشر ملخص الإدانة بعد اكتساب الحكم الصفة النهائية.

المطلب الثاني: قضايا الاختراق والاحتيال المالي وغسل الأموال عبر التشفير

التطبيق الأول: قضية إنشاء روابط بنكية وهمية (Phishing):

أدانت المحكمة الجزائية تشكيلاً عصابياً قام بإنشاء صفحات وبوابات إلكترونية وهمية تحاكي بوابات سداد حكومية وبنكية، وتمكنوا من الحصول على بيانات بطاقات الائتمان لعدد من الضحايا وتحويل مبالغ مالية لحسابات خارجية. وقضت المحكمة بسجن أدعياء التشكيل لمدد تتراوح بين 4 إلى 7 سنوات وغرامات مالية بلغت 2,000,000 ريال وفق المادة الرابعة والخامسة، مع إلزامهم برد الأموال المستولى عليها لأصحابها.

التطبيق الثاني: اختراق خوادم مؤسسة تجارية وتشفير بياناتها:

تم النظر في قضية إقدام مهندس تقني سابق على اختراق الخادم الرئيس لشركة المباشرة السابقة وإتلاف قواعد البيانات وسجلات العملاء انتقاماً لإنهاء خدماته. وعاقبته المحكمة بالسجن لمدة 3 سنوات وغرامة 200,000 ريال بناءً على المادة الخامسة، مبيّنة المحكمة أن استخدام الخبرة التقنية للإضرار بالأنظمة يعتبر ظرفاً مشدداً.

المبحث السابع: التحديات التشريعية المستحدثة والرؤية المستقبلية للتطوير

المطلب الأول: جرائم الذكاء الاصطناعي والتزييف العميق (AI & Deepfake)

تشكل النماذج الذكية والذكاء الاصطناعي التوليدي خطراً مستحدثاً لم يكن سائداً وقت إقرار النظام عام 1428هـ. فقد أصبحت تقنيات التزييف العميق (Deepfake) قادرة على توليد صور ومقاطع فيديو وأصوات مطابقة تماماً للشخصيات الحقيقية، واستخدامها في التضليل، والابتزاز، والاحتيال المالي، وزعزعة الثقة في الوسائط الرقمية.

ويرى الباحث ضرورة إفراد نص صريح يجرم تطوير أو استخدام أو تداول برمجيات التزييف العميق القائمة على الذكاء الاصطناعي بقصد الإضرار أو التزييف، وتحديد المسؤولية الجزائية لمطوري ومستخدمي هذه الخوارزميات.

المطلب الثاني: العملات المشفرة والشبكة المظلمة وتحديث النظام

أدى ظهور العملات الرقمية المشفرة (Bitcoin, Crypto) والشبكة المظلمة (Dark Web) إلى صعوبة تتبع المسارات المالية الناتجة عن الابتزاز وفدية الاختراقات. ويتطلب ذلك تطوير التشريعات الوطنية بالتعاون مع البنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني لتغليظ العقوبات على غسل الأموال الرقمية وتوسيع سلطات التحقيق في تعقب الحافظات الإلكترونية المشفرة.

الخاتمة والتوصيات وقائمة المراجع الموسعة

أولاً: النتائج (Conclusion & Findings)

1. كشف البحث عن امتلاك المملكة العربية السعودية لبنية نظامية وتشريعية متكاملة ومحكمة لمواجهة الجرائم السيبرانية عبر نظام مكافحة الجرائم المعلوماتية الصادر عام 1428هـ والأنظمة الإجرائية والإثباتية المكملة له.
2. أظهرت الدراسة أن النظام يوازن بدقة بين حماية الأمن القومي والبنية التحتية الحيوية للدولة من جهة، وبين حماية خصوصية وحقوق وأموال وأعراض الأفراد من جهة أخرى.
3. أثبتت الدراسة أن الدليل الرقمي أصل قائم بذاته في نظام الإثبات السعودي متى ما سلم من العبث واستوفى الضوابط الفنية المعتمدة.
4. تبين أن التطوير التكنولوجي المتسارع يفرض تحديات جديدة تتمثل في جرائم الذكاء الاصطناعي والتزييف العميق والعملات المشفرة، مما يستدعي تحديثاً مستمراً للنصوص النظامية.

ثانياً: التوصيات (Recommendations)

1. **التحديث التشريعي المستمر** الإسراع في مراجعة نصوص نظام مكافحة الجرائم المعلوماتية وإضافة مواد جديدة تتناول صراحة المسؤولية الجزائية عن تطبيقات الذكاء الاصطناعي (AI)، والتزييف العميق، والعملات المشفرة.
2. **تطوير التعاون الدولي**: تفعيل مذكرات التفاهم والاتفاقيات الدولية والإقليمية لتسليم المجرمين الإلكترونيين وتبادل البيانات الجنائية لمواجهة الجرائم العابرة للحدود والشبكة المظلمة.
3. **توسيع التوعية والتعليم الرقمي** إدراج مادة "التوعية بالأنظمة السيبرانية والجرائم الرقمية" ضمن المناهج الدراسية والجامعية لرفع الوعي الوقائي بالحقوق والالتزامات النظامية.

4. **دعم وحماية الضحايا** لتوسع في إنشاء المراكز المتخصصة لتقديم الدعم النفسي والقانوني السري لضحايا الابتزاز والاحتيال الرقمي تشجيعاً لهم على الإبلاغ وملاحقة الجناة.
5. **النشر الأكاديمي المعتمد:** العمل على نشر هذا البحث المستوفى للتعديلات في المجلات العلمية المحكمة المعتمدة لدى جامعة ميدأوشن والمجلات المتبوعة لمراكز علمية متقدمة.

ثالثاً: قائمة المصادر والمراجع المحكمة

1. القرآن الكريم.
2. نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) وتاريخ 8/3/1428هـ.
3. نظام الإثبات السعودي، الصادر بالمرسوم الملكي رقم (م/43) وتاريخ 26/5/1443هـ.
4. نظام الإجراءات الجزائية السعودي، الصادر بالمرسوم الملكي رقم (م/2) وتاريخ 22/1/1435هـ.
5. آل جار الله، عبد العزيز (2017م). جرائم الإنترنت وعقوباتها وفق النظام السعودي، الرياض: دار الكتاب الجامعي.
6. الشمري، نواف (2025م). "النظام الجزائي لجرائم المعلوماتية وحماية الأمن السيبراني"، مجلة روح القوانين، العدد 88، ص ص 215-240.
7. الجربوع، عبد الله (2023م). "الاعتداء على نظم المعلومات في التشريع السعودي"، مجلة البحوث الفقهية والقانونية، العدد 40، ص ص 120-155.
8. ساتي، أميرة (2023م). "دراسات تحليلية في الجريمة المعلوماتية" مجلة الآداب والعلوم الإنسانية، المجلد 12، ص ص 85-110.
9. الهيئة الوطنية للأمن السيبراني (NCA) (2024م). أطر تنظيمية لحماية البيئة الرقمية والبنية التحتية في المملكة العربية السعودية.
10. مجلة جامعة ميدأوشن (Midocean Journal) (2025م). الأبحاث المنشورة في العلوم القانونية والإنسانية ذات الصلة بالجرائم المستحدثة والفضاء السيبراني.

11. المالكي، خالد بن عبد العزيز (2022م). الحماية الجنائية للحياة الخاصة في التشريع السعودي: دراسة مقارنة، الرياض: مكتبة القانون والاقتصاد.
12. العتيبي، فهد بن سعد (2021م). الأدلة الرقمية وحجيتها في الإثبات الجنائي: دراسة تطبيقية في القضاء السعودي، جدة: دار الحكمة.