مجلة العلوم الإسلامية الدولية

INTERNATIONAL ISLAMIC SCIENCES JOURNAL

eISSN: 2600-7096

AN ACADEMIC QUARTERLY PEER-REVIEWED JOURNAL

مجلة علمية محكمة ، ربع سنوية

Vol : 9 Issue : 2 Year : 2025

المجلد: 9 العدد: 2 السنة: 2025

في هذا العدد:

eISSN 2600-7096

9 772600 709003

جامعة المدينة العالمية
Al-Madinah International University

تصدرها
PUBLISHED BY
كلية العلوم الإسلامية، جامعة المدينة العالمية
FACULTY OF ISLAMIC SCIENCES
AL-MADINAH INTERNATIONAL UNIVERSITY

International Islamic Sciences Journal
Vol. 9, Issue. 2, June 2025
eISSN: 2600-7096
Al-Madinah International University

Manuscript Received Date: 14/05/24 | Manuscript Acceptance Date: 23/05/25 | Manuscript Published Date:27/06/25

DOI: https://doi.org/10.63226/iisj.v9i2.5508

تأثير الجرائم المعلوماتية على التجارة الإلكترونية في ظل التحول الرقمي في النظام السعودي

[The Impact of Cybercrime on E-Commerce Amid Digital Transformation in the Saudi Legal System]

Saad Al-Azzam[1] & Abdullah bin Abdulhadi Al-Azwary[2]

[1]Researcher in Department of Law, College of Sharia and Law, University of Jeddah. Kingdom of Saudi Arabia
[2]Professor in Department of Law, College of Sharia and Law, University of Jeddah Kingdom of Saudi Arabia.

* Corresponding Autor: Snazzam.199@gmail.com

الملخص

يسعى هذا البحث إلى دراسة منهجية للجرائم الإلكترونية وأبرز مظاهرها التي تؤثر على قطاع التجارة الإلكترونية، مع التأكيد على التشريعات والأطر التنظيمية السعودية ذات الصلة بالتخفيف من هذه الجرائم، فضلاً عن فعاليتها في حماية المعاملات الرقمية وتعزيز ثقة المستهلك والشركات. وعلاوة على ذلك، تطمح الدراسة إلى توضيح التحديات السائدة التي تعوق تنفيذ هذه التدابير التشريعية واقتراح حلول عملية تهدف إلى تعزيز البنية التحتية القانونية التي تحكم التجارة الإلكترونية. كانت منهجية البحث المستخدمة في الغالب وصفية وتحليلية، مما سهل مراقبة النصوص ذات الصلة والتدقيق فيها، إلى جانب مراجعة شاملة للأدبيات الموجودة والتحقيقات السابقة ذات الصلة. أشارت النتائج إلى أن التشريعات السعودية تمثل تقدمًا كبيرًا في مكافحة الجرائم الإلكترونية؛ ومع ذلك، هناك ضرورة ملحة لتحسين آليات الإنفاذ وتعزيز الوعي العام. بالإضافة إلى ذلك، تم اكتشاف أن المشاركة النشطة للأفراد والمؤسسات في الالتزام ببروتوكولات الأمان والإبلاغ عن التهديدات الرقمية هي حجر الزاوية الأساسي لإنشاء نظام بيئي رقمي آمن. وشدّدت الدراسة على انتشار الابتزاز الإلكتروني باعتباره أحد أكثر أشكال الجرائم المتصلة بالمعلومات انتشاراً، وشدّدت على ضرورة تعزيز الوعي بالاستراتيجيات الفعّالة لمعالجة هذه المسائل. ويدعو البحث إلى الارتقاء بمعايير الحماية التقنية، وتضخيم الجهود من قبل السلطات ذات الصلة لمواجهة هذه الأنشطة الإجرامية، فضلاً عن تسهيل قنوات الاتصال للإبلاغ عن الحوادث الإلكترونية.

الكلمات المفتاحية: الجرائم الإلكترونية، التجارة الإلكترونية ، الحماية القانونية، المستهلك.

ABSTRACT

This research aims to conduct a systematic study of cybercrimes and their most prominent manifestations that impact the e-commerce sector, with an emphasis on Saudi legal frameworks and regulations related to mitigating such crimes. It also examines the effectiveness of these frameworks in protecting digital transactions and enhancing consumer and business trust. Furthermore, the study aspires to clarify the prevailing challenges that hinder the implementation of these legislative measures and propose practical solutions to strengthen the legal infrastructure governing e-commerce.The research methodology was primarily descriptive and analytical, facilitating the observation and examination of relevant texts, along with a comprehensive review of existing literature and related prior investigations. The findings indicated that Saudi legislation represents a significant advancement in combating cybercrimes; however, there remains an urgent need to improve enforcement mechanisms and raise public awareness. Additionally, it was found that the active participation of individuals and institutions in adhering to security protocols and reporting digital threats is a cornerstone for establishing a secure digital ecosystem. This research aims to conduct a systematic study of cybercrimes and their most prominent manifestations that impact the e-commerce sector, with an emphasis on Saudi legal frameworks and regulations related to mitigating such crimes. It also examines the effectiveness of these frameworks in protecting digital transactions and enhancing consumer and business trust. Furthermore, the study aspires to clarify the prevailing challenges that hinder the implementation of these legislative measures and propose practical solutions to strengthen the legal infrastructure governing e-commerce. The research methodology was primarily descriptive and analytical, facilitating the observation and examination of relevant texts, along with a comprehensive review of existing literature and related prior investigations. The findings indicated that Saudi legislation represents a significant advancement in combating cybercrimes; however, there remains an urgent need to improve enforcement mechanisms and raise public awareness. Additionally, it was found that the active participation of individuals and institutions in adhering to security protocols and reporting digital threats is a cornerstone for establishing a secure digital ecosystem. The study emphasized the prevalence of cyber extortion as one of the most widespread forms of cybercrime and stressed the need to enhance awareness of effective strategies to address such issues. The research calls for the elevation of technical protection standards and greater efforts by relevant authorities to combat these criminal activities, as well as the facilitation of communication channels for reporting cyber incidents..

Keyword: *Cybercrime, E-commerce, Legal Protection, Consumer.*

مقدمة:

تُعدّ الجرائمُ الإلكترونية من أبرز التحديات التي تواجه البيئة الرقمية الحديثة، إذ تشمل أنشطةً غير مشروعة تعتمد على استخدام أجهزة الحاسوب أو الشبكات لتحقيق أهداف ضارّة، سواء كانت مادية أو معنوية. وعلى الرغم من أن الدافع الأساسي لغالبية مرتكبي هذه الجرائم هو تحقيق مكاسب مالية، فإن بعضهم يسعى إلى إلحاق الضرر بالأجهزة أو الشبكات بصورة مباشرة، أو إلى نشر محتويات ضارّة أو غير مشروعة. وتتعدد أساليب الهجوم الإلكتروني لتشمل زرع البرمجيات الخبيثة أو نشر الفيروسات التي تنتقل بين الأجهزة، وقد تمتد إلى شبكات كاملة، مما يزيد من حجم الأثر ودرجة الخطورة.

وتُعدّ الخسائرُ المالية من أبرز آثار هذه الجرائم، إذ تنطوي على مجموعة واسعة من الأفعال غير القانونية، مثل: الاحتيال الرقمي، وسرقة البيانات الشخصية أو البنكية، وانتحال الهوية، وهجمات برامج الفدية، إضافةً إلى محاولات اختراق الحسابات والأنظمة الرقمية الحساسة. وتكمن أهمية المواجهة في حماية البيانات، لا سيما النسخ الاحتياطية، من الوصول غير المشروع أو التسريب.

وفي سياق التجارة الإلكترونية في المملكة العربية السعودية، شهد هذا القطاع نموًا متسارعًا في ظل التحول الرقمي والتشريعات التنظيمية الحديثة. إلا أن هذا التطور صاحبه تصاعد في وتيرة الجرائم الإلكترونية التي استهدفت المعاملات والمستخدمين، مما يطرح تحديات قانونية وتقنية تتطلب حلولًا شاملة. ويسعى هذا البحث إلى دراسة طبيعة الجرائم الإلكترونية في هذا السياق، وتحليل الأنظمة السعودية ذات العلاقة، وتقييم أثرها على بناء الثقة في البيئة التجارية الرقمية.

مشكلة الدراسة:

تشهد المملكة العربية السعودية تحولًا رقميًا متسارعًا في مختلف القطاعات، وفي مقدمتها قطاع التجارة الإلكترونية، الذي يُعد من أبرز روافد الاقتصاد الرقمي الوطني. ورغم هذا التقدم، فإن الجرائم الإلكترونية تمثل تحديًا خطيرًا ومتناميًا يهدد استقرار هذا القطاع، من خلال استهداف المعاملات الرقمية وسرقة البيانات وانتحال الهوية والابتزاز الإلكتروني، وغيرها من الممارسات الإجرامية التي تؤثر سلبًا على ثقة المستهلكين وسلامة البنية التحتية التقنية.

ورغم الجهود التنظيمية والتشريعية التي تبنّتها المملكة، مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية، إلا أن مؤشرات الجرائم الإلكترونية تشير إلى استمرار التهديدات، ووجود قصور في تطبيق الأنظمة، وضعف التنسيق بين الجهات المختصة، فضلاً عن محدودية التوعية المجتمعية بالحقوق والآليات القانونية المتاحة.

ومن هنا، تنبع أهمية هذه الدراسة في تحليل مدى فعالية التشريعات السعودية في مواجهة الجرائم الإلكترونية المرتبطة بالتجارة الإلكترونية، وتقييم قدرتها على التصدي للمخاطر الناشئة في البيئة الرقمية. كما تسعى الدراسة إلى الكشف عن أبرز الثغرات القانونية والتطبيقية، والتحديات المؤسسية التي تعوق الإنفاذ الفعّال، وصولًا إلى اقتراح حلول عملية تدعم استدامة النمو الرقمي وتعزز ثقة المستخدمين في السوق الإلكترونية السعودية.

وتشكل السؤال الرئيسي : ما مدى تأثير الجرائم الالكترونية على التجارة الإلكترونية في النظام السعودي ؟

أسئلة الدراسة:

1. ما أبرز الجرائم الإلكترونية التي تؤثر على التجارة الإلكترونية في المملكة العربية السعودية؟
2. كيف يعالج النظام السعودي الجرائم الإلكترونية التي تؤثر على التجارة الإلكترونية؟
3. ما التحديات التي تعيق تنفيذ القوانين المعنية بمكافحة الجرائم الإلكترونية للحفاظ على التجارة الاكترونية؟
4. ما الحلول المقترحة لتعزيز الحماية القانونية للتجارة الإلكترونية في المملكة؟

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق الأهداف التالية:

1. تحليل أنواع الجرائم الإلكترونية التي تستهدف قطاع التجارة الإلكترونية في المملكة العربية السعودية، وبيان آثارها على الأفراد والمؤسسات وثقة المستخدمين.
2. دراسة فعالية النظام السعودي في معالجة الجرائم الإلكترونية ذات الصلة بالتجارة الإلكترونية، من خلال تحليل التشريعات والأنظمة المطبقة حاليًا.
3. تحديد التحديات التي تعيق تنفيذ التشريعات الخاصة بمكافحة الجرائم الإلكترونية، سواء على المستوى القانوني أو المؤسسي أو التقني، وتقييم آثارها.
4. اقتراح حلول عملية وتشريعية وتقنية تسهم في تعزيز الحماية القانونية للتجارة الإلكترونية، وتحقيق بيئة رقمية آمنة ومستقرة في المملكة.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في إسهامها في إثراء الأدبيات القانونية المتعلقة بالعلاقة بين التجارة الإلكترونية والجرائم الإلكترونية في المملكة العربية السعودية. كما تهدف إلى تعزيز الأمن القانوني في هذا القطاع الحيوي، بما يُوفّر قيمة مضافة للمشرّعين، وأصحاب الأعمال، والمستهلكين على حدّ سواء. ومن خلال هذه الدراسة، يمكن تعميق فهم الأبعاد القانونية للتجارة الإلكترونية، بما يسهم في بناء بيئة قانونية أكثر أمانًا وموثوقية.

منهجية الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، الذي يُعدّ من أبرز المناهج العلمية المستخدمة في البحوث القانونية والاجتماعية، حيث يجمع بين رصد الوقائع والنصوص التنظيمية، وتحليلها تحليلاً نقديًا منهجيًا. ويقوم هذا المنهج على دراسة الأنظمة والتشريعات السعودية ذات العلاقة بالجرائم الإلكترونية والتجارة الإلكترونية، من خلال تفكيك نصوصها النظامية، وتحليل مضامينها، واستخلاص أوجه القوة والقصور فيها، بما يتناسب مع أهداف البحث.

كما تعتمد الدراسة على البيانات الثانوية المستقاة من مصادر متنوعة، تشمل: الكتب المتخصصة، والمقالات العلمية المحكمة، والدوريات القانونية، والرسائل الجامعية، بالإضافة إلى الأنظمة الرسمية الصادرة عن الجهات السعودية المختصة، والمواقع الإلكترونية الموثوقة ذات الصلة. ويسهم هذا التعدد في المصادر في تقديم رؤية شاملة ومتوازنة، تُمكّن الباحث من الإحاطة بجوانب الموضوع المختلفة، وتحقيق نتائج علمية رصينة تستند إلى أسس منهجية دقيقة.

الدراسات السابقة:

عبد الرحيم، و.، بن سعيد، أ.، &عبد الرحيم، ن. (2019). الجرائم الإلكترونية من خلال مؤشرات عالمية وآثارها على المؤسسات .*دراسات المجلة الاقتصادية*، .(10) :

تهدف هذه الدراسة إلى تحديد أنواع الجرائم الإلكترونية وآثارها السلبية على الاقتصاد، وبصورة خاصة على الشركات، مع التركيز على المؤسسات المصرفية التي تُعد من أكثر الجهات عرضةً لهذا النوع من الجرائم. ويعود ذلك إلى أن الأموال تُشكّل العنصر الأساسي في تعاملات هذه المؤسسات، مما يجعلها هدفًا رئيسيًا للمهاجمين. وقد تسببت الجرائم الإلكترونية في خسائر مالية جسيمة سنويًا لهذه الشركات، فضلًا عن تراجع مستوى الثقة التي يضعها العملاء في هذه المؤسسات.

وبالتالي، أضحت الجرائم الإلكترونية عقبة رئيسة أمام نمو وازدهار الشركات، وسعيها إلى جذب أكبر عدد من العملاء وكسب ثقتهم. كما تفاقمت هذه الظاهرة بشكل متزايد، على الرغم من تبني العديد من الأساليب الأمنية المتطورة والتقنيات الحديثة. وتشير التقارير العالمية الصادرة عن الجهات المختصة إلى اتساع نطاق هذه المشكلة على مستوى العالم، حيث تُظهر البيانات أن الولايات المتحدة تُعد من أكثر الدول تضررًا من هذا النوع من الجرائم بشكل مستمر.

التعليق على الدراسة :

تشير هذه الدراسة إلى الأضرار الكبيرة التي تسببت فيها الجرائم الإلكترونية للمؤسسات المالية والمصرفية، مؤكدة على تأثيرها السلبي على ثقة الزبائن. ومع أن الدراسة تناولت تفصيلًا التأثيرات الاقتصادية، إلا أنها لم تتطرق بشكل محدد إلى الانظمة السعودية والإجراءات القانونية المتبعة لمكافحة الجرائم الإلكترونية. هذا يبرز الحاجة إلى فحص فعالية النظام السعودي في الحد من هذه الجرائم، وهي نقطة مهمة دراستنا الحالية.

عبد الله، م. (2021). جرائم التجارة الإلكترونية وظاهرة انتشارها وآلية مكافحتها من خلال التشريعات :

تُعدّ جرائم التجارة الإلكترونية ظاهرة عالمية تشكل تهديدًا خطيرًا على الأفراد بصورة شخصية، وعلى المؤسسات والدول على حدٍ سواء، إذ إن أمنها الإلكتروني بات مهددًا بشكل متزايد. ومن هذا المنطلق، تبرز الحاجة المُلِحّة إلى وجود تشريعات رادعة تحدّ من انتشار هذه الجرائم، إلى جانب توافر آليات فعّالة للكشف عنها ووسائل دقيقة لإثباتها، لا سيما أن هذه الجرائم تتسم بدرجة عالية من الخفاء والسرّية، مما يصعّب من عملية تعقب مرتكبيها.

وقد توصلت الدراسة إلى عدد من النتائج الهامة، من أبرزها أن الجرائم المرتبطة بالتجارة الإلكترونية تتخذ أشكالًا وصورًا متعددة، وتتميز التجارة الإلكترونية بخصائص تجعل من مكافحتها أكثر تعقيدًا، من أهمها كونها نشاطًا عابرًا للحدود، وصعوبة إثبات الجريمة نظرًا للطبيعة التقنية الخفية التي تُنفذ من خلالها. كما أن هذه الجرائم غالبًا ما تكون أقل عنفًا في التنفيذ مقارنة بالجرائم التقليدية، وتحتاج إلى قدر كبير من الخصوصية لدى الجاني.

التعليق على الدراسة :

تشير هذه الدراسة إلى الأضرار الجسيمة التي تسببت بها الجرائم الإلكترونية للمؤسسات المالية والمصرفية، مؤكدةً على أثرها السلبي المباشر في تقويض ثقة العملاء. وعلى الرغم من أن الدراسة تناولت بشكل مفصل التأثيرات الاقتصادية المترتبة على هذه الجرائم، إلا أنها لم تُعالج بوجه خاص التشريعات السعودية

والإجراءات القانونية المعتمدة لمكافحتها. وهذا ما يُبرز الحاجة إلى فحص فعالية النظام القانوني السعودي في الحد من الجرائم الإلكترونية، وهي النقطة الجوهرية التي تسعى دراستنا الحالية إلى معالجتها وتحليلها.

عزام، س. (2021). العقوبات المتعلقة بجرائم المعلوماتية في السعودية: دراسة في التأصيل الشرعي والقانوني وضوابط الاجتهاد القضائي:

هدفت الدراسة إلى تحليل العقوبات المتعلقة بجرائم المعلوماتية في المملكة العربية السعودية، من خلال طرح تساؤلات حول طبيعة العقوبات المقررة، والأساس الشرعي والقانوني الذي تستند إليه، بالإضافة إلى ضوابط اجتهاد القاضي في تحديد مقدار العقوبة. وقد اعتمد الباحث على المنهج الوصفي التأصيلي، حيث قام بوصف النصوص القانونية الواردة في نظام مكافحة الجرائم المعلوماتية، وتأصيلها شرعًا بالاستناد إلى المصادر الفقهية الإسلامية.

وتوصلت الدراسة إلى أن نظام مكافحة الجرائم المعلوماتية يتماشى مع المبادئ العقابية في الشريعة الإسلامية، إذ يحدد العقوبات من حيث النوع والمقدار، مع مراعاة التناسب بين الجريمة والعقوبة. كما نص النظام على عقوبات تكميلية، مثل المصادرة أو إغلاق الموقع المستخدم في الجريمة، وأكد على عدم استثناء أي جهة أو فرد من الخضوع لأحكامه.

التعليق على الدراسة :

تركز هذه الدراسة على العقوبات الخاصة بجرائم المعلوماتية في المملكة العربية السعودية، وتُبرز توافق نظام مكافحة الجرائم المعلوماتية مع القواعد العقابية المستمدة من الشريعة الإسلامية. وتسهم هذه الدراسة في إثراء الفهم المتعلق بكيفية تحديد العقوبات المقررة، إلا أنها لم تتناول التحديات العملية التي يواجهها القضاة عند تطبيق هذه العقوبات على أرض الواقع. ومن هذا المنطلق، تسعى دراستنا الحالية إلى تقديم تحليل أعمق لهذه التحديات، مع التركيز على جوانب تطبيق الأنظمة ورصد فعالية مراقبة الجرائم الإلكترونية في البيئة السعودية.

جدو، ع.، &درار، ع. (2022). الجريمة الإلكترونية: الأنواع، الخصائص، والتأثيرات الاقتصادية العالمية .*مجلة أبحاث اقتصادية معاصرة*، .(5) :

تهدف هذه الدراسة إلى استعراض الجريمة الإلكترونية، وأنواعها، وخصائصها، إلى جانب تحليل الأضرار الاقتصادية المترتبة عليها وتأثيراتها المتزايدة على الاقتصاد العالمي. وتشير التقارير الحديثة إلى تصاعد الخسائر المالية الناجمة عن اختراق المؤسسات المالية والمصرفية، حيث أظهرت الإحصائيات ارتفاعًا ملحوظًا في عدد الهجمات الإلكترونية، إذ تم تسجيل العديد من حالات اختراق البيانات خلال عام 2019، بالإضافة إلى

الزيادة الحادة في هجمات التصيّد الاحتيالي خلال عام 2020. كما شهدت فترة جائحة (COVID-19) تصاعدًا كبيرًا في هجمات برامج الفدية التي استهدفت مختلف القطاعات.

وتُقدّر الخسائر السنوية الناجمة عن الجرائم الإلكترونية في الولايات المتحدة بما يتراوح بين 10 إلى 12 مليار دولار، في حين تُقدّر الخسائر على مستوى العالم بما يقارب 50 إلى 60 مليار دولار، مما يعكس خطورة هذه الظاهرة وأثرها الواسع على استقرار الأنظمة الاقتصادية حول العالم.

التعليق على الدراسة :

أظهرت هذه الدراسة زيادة ملحوظة في معدلات الجرائم الإلكترونية على مستوى العالم، مع تركيز خاص على الأضرار المالية التي لحقت بالمؤسسات المالية والمصرفية. إلا أن الدراسة لم تُعالج بشكل محدد التشريعات المعمول بها في المملكة العربية السعودية أو مدى تأثير تلك التشريعات على المؤسسات المحلية. وفي هذا السياق، تسعى دراستنا الحالية إلى تقديم تحليل معمق للأنظمة والتشريعات السعودية ذات الصلة، مع التركيز على مدى تأثيرها الفعلي على أداء الشركات في المملكة، خاصة في ظل التحديات الرقمية المتزايدة.

دهشان، ي. إ. (2024). الحماية الجنائية للمستهلك الإلكتروني *مجلة روح القوانين*، (36) :

أصبح توفير الحماية للمستهلك أمرًا ذا أهمية متزايدة في ظل الانتشار الواسع لاستخدام الإنترنت والأجهزة الذكية، حيث تحوّلت المعاملات التجارية من الواقع التقليدي إلى الفضاء الرقمي. وعلى الرغم من الفرص الجديدة التي أتاحها هذا التحول، فقد برزت في المقابل مخاطر متزايدة تهدد خصوصية وأمان المستهلكين على الإنترنت. وتكمن أهمية الحماية في تعزيز ثقة المستهلكين بالتعاملات الإلكترونية، ومكافحة الجرائم الإلكترونية من خلال تطوير تشريعات وأدوات تنظيمية خاصة لهذا الغرض، فضلًا عن تعزيز الابتكار والتنافسية بين الشركات.

وتسعى الحماية القانونية والتنظيمية إلى التصدي للجرائم الإلكترونية التي تمسّ حقوق الأفراد ومصالحهم في البيئة الرقمية. وتتمثل أبرز نتائج الدراسة في أن معضلة حماية المستهلك لا تكمُن فقط في قصور النصوص القانونية، بل أيضًا في ضعف أداء الأجهزة الرقابية المختصة، وتأخّر استجابة الجهات المعنية بالشكاوى. وقد أوصت الدراسة بضرورة تعزيز المنظومة التشريعية، وتحسين آليات الرصد والتتبع، إلى جانب رفع الوعي الرقمي، وتشجيع الإبلاغ عن الجرائم الإلكترونية، وتعزيز الأمان السيبراني للمنصات الإلكترونية المختلفة.

التعليق على الدراسة :

ناقشت الدراسة أهمية حماية المستهلكين وتعزيز الأمان السيبراني، مع الإشارة إلى ضعف الأجهزة الرقابية وتأخر استجابة الجهات المعنية في التصدي للجرائم الإلكترونية. ومع ذلك، لم تتناول الدراسة بشكل محدد كيفية تطبيق التشريعات الخاصة بحماية المستهلك من الجرائم الإلكترونية في المملكة العربية السعودية. ومن هذا المنطلق، تسعى دراستنا الحالية إلى سدّ هذه الفجوة من خلال تقديم حلول وتوصيات عملية لتعزيز الحماية القانونية والرقابية للتجارة الإلكترونية في المملكة، بما يواكب التطورات الرقمية ويسهم في بناء بيئة إلكترونية آمنة وموثوقة.

الفجوة البحثية :

تتركز الدراسة الحالية على تقديم تحليل شامل للتجارة الإلكترونية في المملكة العربية السعودية، مع التركيز على فعالية التشريعات المحلية في مكافحة الجرائم الإلكترونية. تهدف الدراسة إلى استكشاف التحديات التي تواجه المملكة في تطبيق هذه التشريعات على أرض الواقع، وكيف تؤثر الجرائم الإلكترونية على ثقة المستهلكين والشركات. ومن خلال هذه الدراسة، نسلط الضوء على الجوانب القانونية والتنظيمية والرقابية في السعودية، بما في ذلك دور الأجهزة الحكومية في تطبيق القوانين وضمان حماية حقوق الأفراد في الفضاء الرقمي.

ورغم أن الدراسات السابقة قد تناولت جوانب عدة للجرائم الإلكترونية وأثرها على التجارة الإلكترونية، بما في ذلك تأثيراتها الاقتصادية والعقوبات المتعلقة بها وأهمية التشريعات، إلا أنها لم تتعمق في تحليل فعالية التشريعات السعودية بشكل محدد. إذ لم تركز الدراسات السابقة على مدى نجاح هذه التشريعات في مواجهة الجرائم الإلكترونية في المملكة، ولا على تأثير هذه الجرائم في ثقة المستهلكين والشركات المحلية. علاوة على ذلك، تفتقر الأدبيات الحالية إلى دراسة شاملة تسلط الضوء على التحديات التي تواجه المملكة في مكافحة الجرائم الإلكترونية مقارنة بالتحديات العالمية، بما في ذلك التأصيل الشرعي والقانوني للعقوبات في المملكة وأثرها على حماية التجارة الإلكترونية.

تمهيد :

في ظل التطورات التقنية المتسارعة، أصبحت الجريمة الإلكترونية والتجارة الإلكترونية من أبرز القضايا القانونية التي تتطلب فهماً نظريًا عميقًا وتأصيلاً علميًا دقيقًا. فقد بات من الضروري على الباحثين في المجال القانوني الإحاطة الكاملة بالمفاهيم المرتبطة بهاتين الظاهرتين، خصوصًا في ظل التحديات التي تفرضها البيئة الرقمية على الأنظمة القضائية والتشريعية التقليدية.

ويأتي هذا الفصل ليؤسس للإطار النظري الذي يُشكّل القاعدة المعرفية لهذا البحث، حيث يتم من خلاله استعراض المفاهيم الأساسية للجريمة الإلكترونية والتجارة الإلكترونية، وتحليل تطورها، وبيان خصائصها وأشكالها، مع التركيز على البيئة السعودية. كما يهدف هذا الإطار إلى تحديد المصطلحات القانونية ذات العلاقة، واستعراض المواقف التشريعية السعودية المقارنة، بما يتيح فهماً دقيقاً للمنظومة النظامية التي تحكم هذه المعاملات.

ويُسهم هذا الفصل في توضيح السياق النظري للبحث، عبر تتبع جذور المصطلحات القانونية، وتحليل النصوص النظامية ذات الصلة، واستعراض أبرز ما ورد في الدراسات والكتابات الفقهية والأنظمة المقارنة. كما يُعزز الإطار النظري من إمكانية تقييم مدى كفاية التنظيم القانوني السعودي لمواجهة الجريمة الإلكترونية، ومدى قدرته على تنظيم وحماية التجارة الإلكترونية، وهو ما يشكل مدخلاً مهماً لفهم الإشكالية القانونية التي تتناولها هذه الدراسة.

المبحث الأول: الجريمة الإلكترونية في المملكة العربية السعودية :

المطلب الأول : مفهوم الجريمة الإلكترونية وتطورها في السعودية :

تُعرَّف الجريمة الإلكترونية بأنها استخدام أجهزة الحاسوب أو الشبكات في تنفيذ أعمال غير قانونية، مثل اختراق الحسابات البنكية أو سرقة بطاقات الائتمان (الدمياطي، 2019م). كما تشمل الجرائم التي تُرتكب عبر الإنترنت، مثل ابتزاز الأفراد أو سرقة الحسابات والمعلومات الشخصية (الصغير، 2022م). ويذهب بعض الباحثين إلى تعريف الجريمة الإلكترونية بأنها أي فعل غير مشروع يرتبط باستخدام أجهزة الحاسوب أو الشبكات (محمد، 2015م)، وتشمل كذلك الأنشطة غير القانونية التي تستهدف أنظمة الحواسيب من خلال البرمجيات الخبيثة والفيروسات (حجازي، 2019م).

وفي إطار نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية، تُعرَّف الجريمة الإلكترونية بأنها "أي فعل يُعدّ مخالفًا للأنظمة والتعليمات المتعلقة باستخدام أجهزة الحاسوب أو الشبكات المعلوماتية" (وزارة الداخلية السعودية، 2024م).

وعليه، يتضح أن الجريمة الإلكترونية في السياق السعودي تشمل الأفعال غير القانونية التي تُرتكب ضد الأفراد أو المؤسسات باستخدام الوسائل التقنية، ويعمل النظام السعودي على مواجهتها من خلال حزمة من التشريعات والإجراءات التنظيمية التي تهدف إلى الحد منها وتعزيز الأمن السيبراني الوطني.

المطلب الثاني :أبرز أنواع الجرائم الإلكترونية في البيئة السعودية :

تشمل أنواع الجرائم الإلكترونية العديد من الأنشطة غير القانونية، من أبرزها:

1. **الاحتيال عبر البريد الإلكتروني** :حيث يتم استخدام أساليب خادعة لإقناع الضحايا بالكشف عن معلوماتهم الشخصية.
2. **تزوير الهويات** :عبر سرقة واستخدام البيانات الشخصية للأفراد.
3. **سرقة بيانات الدفع الإلكتروني** :مثل سرقة معلومات بطاقات الائتمان والبيانات المالية.
4. **سرقة بيانات المؤسسات** :تشمل سرقة المعلومات الحساسة وبيعها.
5. **الابتزاز الإلكتروني** :حيث يُطلب المال مقابل منع هجوم مهدد.
6. **هجمات برامج الفدية** :نوع من الابتزاز الذي يطال البيانات أو الأنظمة.
7. **السرقة المشفرة** :تزوير العملات الرقمية أو سرقتها.
8. **التجسس الإلكتروني** :التسلل إلى البيانات الحكومية أو الخاصة بالشركات.
9. **الاختراق في الأنظمة الإلكترونية** :يتضمن التلاعب بالشبكات الإلكترونية لتهديد أمان المعلومات.
10. **انتهاك حقوق التأليف والنشر** :من خلال توزيع محتوى محمي بحقوق ملكية فكرية دون إذن.
11. **المقامرة غير القانونية** :تنظيم أو المشاركة في ألعاب قمار غير مشروعة عبر الإنترنت.
12. **بيع السلع غير المشروعة** :من خلال منصات التجارة الإلكترونية.
13. **استغلال الأطفال في المواد الإباحية** :بما في ذلك طلب أو توزيع صور أو أفلام مسيئة للأطفال.

أولا: الحماية المتقدمة من الجرائم الإلكترونية:

يقوم مرتكبو الجرائم الإلكترونية باستخدام البرمجيات الخبيثة بهدف إتلاف الأجهزة أو تعطيلها، وقد تشمل هذه الأفعال حذف البيانات أو سرقتها، بالإضافة إلى حرمان المستخدمين من الوصول إلى الإنترنت، أو منع الشركات من التواصل مع عملائها. ويُطلق على هذا النوع من الهجمات "هجوم الحرمان من الخدمة " .(Denial of Service)وفي كثير من الحالات، ينفّذ الجناة هاتين العمليتين معًا، حيث يبدأون باستهداف الأجهزة بالفيروسات، ثم يستخدمونها لاحقًا لنشر البرمجيات الخبيثة على أجهزة أخرى أو عبر الشبكة.

وتُصنّف بعض الدول نوعًا ثالثًا من الجرائم الإلكترونية، يتمثل في استخدام أجهزة الحاسوب كوسيلة لارتكاب الجريمة، كأن تُستخدم لتخزين بيانات مسروقة أو لإدارة نشاط غير قانوني (الصغير، 2022، ص 20).

ثانيا : تأثير الجرائم الإلكترونية:

تُعدّ سرقة الهوية ظاهرة متنامية تشهد ازديادًا مستمرًا، فوفقًا لتقرير *حالة مرونة الأمن السيبراني لعام 2021* الصادر عن شركةAccenture ، ارتفعت الهجمات الأمنية بنسبة 31٪ من عام 2020 إلى عام 2021، حيث زاد عدد الهجمات على كل شركة من 206 إلى 270 هجومًا سنويًا. وتؤثر هذه الهجمات على الشركات والأفراد على حد سواء، نظرًا لقيام العديد من الشركات بتخزين بيانات حساسة ومعلومات شخصية تتعلق بعملائها.

ويمكن لهجوم إلكتروني واحد—سواء أكان اختراقًا للبيانات أو نشرًا لبرمجيات خبيثة، أو برنامج طلب فدية، أو هجوم حرمان من الخدمة—(DoS) أن يُكلّف الشركات، بغضّ النظر عن حجمها، ما متوسطه 200 ألف دولار. وتشير الإحصاءات إلى أن عددًا كبيرًا من الشركات المتضررة تخرج من السوق خلال ستة أشهر فقط من وقوع الهجوم، وذلك بحسب بيانات شركة التأمين.Hiscox

كما أظهرت دراسة صادرة عن *Javelin Strategy & Research* حول احتيال الهوية في عام 2021 أن الخسائر الناتجة عن هذا النوع من الاحتيال بلغت نحو 56 مليار دولار في ذلك العام (إبراهيم، 2021، ص 93).

وبالنسبة للأفراد والشركات، فإن أثر الجريمة الإلكترونية قد يكون بالغًا، إذ يتسبب في خسائر مالية فادحة، بالإضافة إلى تآكل الثقة والإضرار بسمعة الكيانات المتأثرة. ومع تزايد وتيرة هذه الجرائم، تبرز الحاجة إلى تبنّي تدابير وقائية لحماية الأجهزة والبيانات الشخصية من الاختراقات والهجمات الإلكترونية المتنوعة.

1. استخدام برنامج حماية الفيروسات، لحماية أنظمة الحاسب من الهجمات.
2. استخدام كلمات مرور قوية: التأكد من استخدام كلمات مرور قوية بحيث لا يمكن للأشخاص معرفتها ولا عدم القيام بتسجيلها في أي مكان، ويمكن كذلك استخدم تطبيق مدير كلمات مرور حسن السمعة لإنشاء كلمات مرور قوية بشكل عشوائي لتسهيل الأمر.
3. عدم فتح أي رسائل فى البريد الإلكتروني والتي تكون عشوائية: فهي تعد طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الإلكترونية.
4. الاتصال بالشركات مباشرةً بشأن الطلبات المشبوهة: إذا اتصلت بالشخص شركة وطلبت منه معلومات شخصية أو بيانات، يجب إنهاء المكالمة بدون إعطائهم شيء، ثم أعادة الاتصال بهم مرة أخرى باستخدام الرقم الموجود على الموقع الإلكتروني الرسمي الخاص بهم للتأكد من التحدث إليهم وليس مع مجرمي الإنترنت.

5. التنبّه لعناوين مواقع URL التي يتم زيارتها: يجب مراقبة عناوين مواقع URL التي يتم فتحها، ومعرفة هل تبدو مشروعة؟ تجنب الضغط على الروابط التي تحتوي على عناوين URL غير مألوفة أو التي تبدو كرسالة غير مرغوب فيها.
6. مراقبة البيانات المصرفية: من الضروري اكتشاف تعرضك للجريمة الإلكترونية في أسرع وقت ممكن. يجب متابعة حساباتك المصرفية بشكل دوري والتحقق من أي معاملات غير معتادة. في حال وجود أي شكوك، يمكن للمصرف فحص تلك المعاملات للتحقق من مدى مشروعيتها.

ثالثا: آثار الجرائم الإلكترونية:

في غالب الأمر يكون هدف المجرم الإلكتروني تعريض أمن الأشخاص للخطر في محاولة لاستدراجهم وتوريطهم في أعمال خطرة قد تصل عقوبتها في كثير من الأحيان إلى مراحل لا يحمد عقباها أو لاستهدافهم للحصول على مبالغ مالية بدون وجه حق أو تحقيق مكاسب غير مشروعة، فغالبًا ما تكون هذه الجرائم بمثابة مصباح علاء الدين بالنسبة للمجرمين في نفس الوقت الذي قد ينجم عنها دخول الضحايا في حالة نفسية سيئة وتعريضهم لمواجهة أزمات مالية سيئة(قشقوش، 2019م، ص 78).

رابعا : التجارة الإلكترونية:

تشمل التجارة الإلكترونية عمليات بيع وشراء السلع والخدمات التي تتم عبر الإنترنت، سواء من قبل الشركات أو الأفراد، باستخدام أجهزة الحاسوب أو الأجهزة الذكية مثل الهواتف المحمولة والأجهزة اللوحية. وتتيح هذه العملية للمستهلكين تنفيذ عمليات الشراء عبر أجهزتهم الرقمية المتنوعة، بما في ذلك الأجهزة المدمجة مثل أجهزة Echo من(Amazon البياضي، 2020)

وتسعى معظم الشركات إلى تمكين العملاء من شراء ما يرغبون فيه في أي وقت ومن أي مكان، باستخدام أي جهاز رقمي. ويعتمد هذا النموذج من التجارة على التعامل مع كميات ضخمة ومعقدة من البيانات، التي تأتي من مصادر متعددة، مما يستدعي استخدام تقنيات متقدمة لمعالجة هذه البيانات بكفاءة، نظرًا لأن حجمها يتجاوز قدرات البرامج التقليدية على إدارتها وتحليلها (مطر، 2014).

- **آلية عمل التجارة الإلكترونية:**

تعمل التجارة الإلكترونية بشكل أساسي عبر الشبكات، حيث يمكن للمستهلك الراغب بالحصول على سلعة معينة تصفح المواقع الخاصة ببيع هذا النوع من السلع. ومن ثم ينبغي على العميل القيام ببعض الخطوات من أجل الحصول على السلعة (الشوا، 2021م، ص 30).

خامسا: أهمية التجارة الإلكترونية:

أهمية التجارة الإلكترونية يمكن تلخيصها في عدة نقاط رئيسية:

1. **سهولة الحصول على المنتجات والخدمات** :حيث أن سلع التجارة الإلكترونية متاحة على مدار الساعة وطوال أيام الأسبوع، مما يسهل على العملاء الوصول إليها في أي وقت.
2. **تنوع السلع والخدمات** :تتيح التجارة الإلكترونية الوصول إلى مجموعة واسعة من السلع والخدمات، مما يوفر خيارات متعددة للعملاء.
3. **زيادة عدد العملاء** :يمكن للشركات الوصول إلى عدد أكبر من العملاء في أي مكان وزمان، ما يعزز من انتشار التجارة الإلكترونية.
4. **تقليل التكلفة والوقت** :يساهم استخدام التجارة الإلكترونية في تقليل التكاليف والوقت، خاصة بالنسبة للشركات التي تعرض منتجاتها وخدماتها عبر الإنترنت (الشوا، 2021م، ص 32).

سادسا : عيوب التجارة الإلكترونية:

1. عدم وجود خدمات ما بعد البيع فى بعض الشركات التجارية.
2. عدم قدرة المشتري على معاينة المنتج أو السلعة قبل إتمام عملية الشراء.
3. قد تكون فترة الشحن خاصة طويلة.
4. يمكن أن تسرق بعض بيانات بطاقات الائتمان بالنسبة للعملاء عبر مواقع البيع(غنام، 2010م، ص 146).

- **القطاعات الرئيسية للتجارة الإلكترونية:**

تعمل التجارة الإلكترونية في أربعة قطاعات تجارية رئيسية على النحو التالي:

1. **البيع من شركة إلى شركة** :وهي العمليات التي يتم فيها البيع المباشر لمختلف السلع والخدمات بين الشركات نفسها.
2. **البيع من شركة إلى مستهلك** :تشمل هذه العمليات البيع المباشر للسلع والخدمات بين الشركات التجارية والعملاء المستهلكين (نصار، 2020م، ص 92).
3. **البيع من مستهلك إلى مستهلك آخر** :يتم فيها بيع السلع والخدمات بين الأفراد المستهلكين، حيث يكون هناك طرف ثالث غالبًا، مثل المواقع الإلكترونية التي تقدم هذه الخدمة، مثل موقع "إيباي."

4. **البيع من مستهلك إلى شركة** :هي العمليات التي تتم عندما يقوم الأفراد ببيع منتجاتهم أو خدماتهم إلى الشركات التجارية، كما في حالة قيام فنان ببيع لوحاته الفنية لشركة عبر الإنترنت (نصار، 2020م، ص 88).

سابعا: قيمة التجارة الإلكترونية للأعمال:

تشهد التجارة الإلكترونية نموًا متسارعًا على مستوى العالم، حيث من المتوقع أن ترتفع مبيعاتها بنسبة تصل إلى 97% بحلول عام 2027م. وقد بلغت قيمة مبيعات التجزئة عبر الإنترنت عالميًا نحو 4.3 تريليون دولار أمريكي، ومن المتوقع أن تصل الإيرادات إلى ما يقارب 4.88 تريليون دولار أمريكي بحلول عام 2026م. هذا التوسع السريع يعكس التحول الجذري في أنماط الاستهلاك والبيع، ويؤكد على أهمية التجارة الإلكترونية كأداة استراتيجية في تعزيز أداء الشركات.

يساهم هذا النمو في تمكين المؤسسات من تحقيق مزايا تنافسية متعددة، منها: توسيع قاعدة العملاء إقليميًا ودوليًا، وخفض التكاليف من خلال تقليل الاعتماد على المتاجر التقليدية، بالإضافة إلى توفير إمكانية الشراء للعملاء في أي وقت ومن أي مكان عبر أجهزتهم الرقمية. كما تتيح التجارة الإلكترونية إمكانية جمع وتحليل بيانات العملاء، واختبار المنتجات والخدمات والعلامات التجارية الجديدة بموارد محدودة. إلى جانب ذلك، تساعد في تقديم خيارات للخدمة الذاتية مما يعزز من كفاءة فرق المبيعات، ويوفر فرصة للتوسع السريع بتكاليف منخفضة.(Statista, 2024)

.(https://www.statista.com/statistics/379046)

التجارة الإلكترونية في المملكة العربية السعودية:

تُعدّ التجارة الإلكترونية من الأنشطة الاقتصادية الحيوية في المملكة العربية السعودية، حيث تمثل إحدى ركائز النمو في الاقتصاد الرقمي الوطني، وتُمارَس من خلال الوسائل الإلكترونية لعرض وبيع المنتجات أو تقديم الخدمات. وقد بدأت هذه المنظومة بالتشكل في المملكة منذ عام 1422هـ/2001م، وواصلت تطورها حتى بلغ حجم تعاملاتها حوالي 5.7 مليارات دولار في عام 1441هـ/2020م. وبفضل الخطط الوطنية المحفّزة، حققت السعودية معدلات نمو مرتفعة جعلتها ضمن أعلى عشر دول نموًا في مجال التجارة الإلكترونية عالميًا، بنسبة سنوية تفوق 32%، وذلك خلال الربع الأول من عام 2023م.

وفي سياق المساهمة الاقتصادية، سجلت التجارة الإلكترونية ما يقارب 10.48 مليارات دولار في الحسابات القومية لعام 1441هـ/2020م، وتصدّر قطاع الملابس والأحذية قائمة الإيرادات بقيمة 3.21 مليارات دولار، تلاه قطاع الإلكترونيات بنحو 3 مليارات دولار، ثم قطاع الأثاث والأجهزة المترلية بقيمة 1.48 مليار دولار، بينما كان قطاع الغذاء والدواء الأقل إيرادًا بـ776 مليون دولار.

وقد أظهرت الدراسات الحديثة أن نحو 84% من المنشآت الصغيرة والمتوسطة في المملكة، سواء التجارية أو الصناعية، تقع ضمن القطاعات المؤهلة للاستفادة من مزايا التجارة الإلكترونية، مما أسهم في توسيع السوق السعودية لتصبح من بين أكبر أسواق التجارة الإلكترونية في منطقة الشرق الأوسط وشمال أفريقيا. كما ارتفع ترتيب المملكة إلى المركز الـ26 عالميًا في مبيعات التجارة الإلكترونية، خاصة بعد التسارع الرقمي الذي فرضته جائحة فيروس كورونا.(SaudiPedia, 2024) (https://saudipedia.com).

المطلب الثالث :الإجراءات و التشريعية لمكافحة الجرائم الإلكترونية

التشريعات المتعلقة بالجريمة الإلكترونية في السعودية:

مع تنامي الاعتماد على التكنولوجيا والإنترنت في المملكة العربية السعودية في شتى المجالات، برزت الحاجة إلى مواجهة التهديدات الإلكترونية المتزايدة التي تستهدف الأفراد والمؤسسات. وفي إطار هذه التحديات، صدر نظام مكافحة الجرائم المعلوماتية عام 2007م، بموجب المرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ، ليؤسس إطارًا قانونيًا شاملاً للتصدي للجرائم الإلكترونية بأنواعها، ويُعد هذا النظام خطوة تنظيمية مهمة تعكس وعي المملكة بخطورة هذه الجرائم وتأثيرها على الأمن المجتمعي والاقتصادي يهدف النظام إلى حماية المجتمع من الآثار السلبية للجرائم المعلوماتية من خلال مجموعة من الأحكام التي تحدد أنواع الجرائم بدقة، مثل: الدخول غير المشروع إلى الأنظمة المعلوماتية، التعدي على الخصوصية، الاحتيال الإلكتروني، ونشر المحتوى الضار. كما يضع النظام عقوبات رادعة تتنوع بين الغرامات والسجن، إضافة إلى توفير آليات قانونية لملاحقة مرتكبي هذه الجرائم واتخاذ الإجراءات اللازمة بحقهم (المادة 8 نظام مكافحة الجرائم المعلوماتية، 2007) وقد تمت مراجعة النظام وتعديله في عام 2017م لمواكبة التغيرات المتسارعة في عالم التقنية، ولتعزيز فعالية التدابير القانونية في مواجهة المستجدات الرقمية، بما يتوافق مع رؤية المملكة 2030 وتوجهاتها نحو التحول الرقمي (الهيئة الوطنية للأمن السيبراني، 2022)

ويؤكد النظام على أهمية رفع الوعي المجتمعي بالأمن السيبراني، من خلال التوعية بطرق الوقاية وتعزيز ثقافة الاستخدام الآمن للتقنية. بالإضافة إلى الحماية القانونية، يسعى النظام لتحقيق أهداف استراتيجية تشمل : تعزيز الأمن المعلوماتي، حماية الحقوق الناتجة عن الاستخدام المشروع للتكنولوجيا، وصون المصلحة العامة، والقيم الأخلاقية، والاقتصاد الوطني، بما يُسهم في بناء بيئة رقمية آمنة ومتماسكة تحترم القوانين وتحافظ على الاستقرار الاجتماعي

يتألف نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية من ستة عشر مادة، تتناول تنظيم الجرائم الإلكترونية وبيان العقوبات المقررة بحق مرتكبيها. ويبيّن النظام العقوبات المقررة وفقًا لطبيعة الجريمة ودرجة خطورتها على النحو التالي:

1. **السجن لمدة لا تزيد عن سنة** و/أو **غرامة مالية تصل إلى 500 ألف ريال سعودي**، وذلك في الجرائم المتعلقة بـــ: التنصت غير المشروع، الدخول غير المشروع إلى المواقع الإلكترونية، التعدي على الخصوصية الشخصية، التشهير، أو الابتزاز الإلكتروني.

2. **السجن لمدة لا تتجاوز ثلاث سنوات** و/أو **غرامة مالية تصل إلى مليوني ريال سعودي**، في حالات الاحتيال المعلوماتي أو الوصول غير المشروع إلى بيانات بنكية أو ائتمانية.

3. **السجن لمدة لا تزيد على أربع سنوات** و/أو **غرامة لا تتجاوز ثلاثة ملايين ريال سعودي**، وذلك في الجرائم التي تشمل حذف أو تعديل بيانات إلكترونية، أو التسبب في إيقاف شبكة معلوماتية، أو إعاقة الوصول إلى الخدمة.

4. **السجن لمدة لا تتجاوز خمس سنوات** و/أو **غرامة مالية لا تتجاوز ثلاثة ملايين ريال سعودي**، في حال إنتاج أو نشر أو تداول محتوى إلكتروني يمس النظام العام، أو القيم الدينية، أو الآداب العامة، أو الخصوصية، أو المحتوى المتعلق بالاتجار بالبشر، أو المخدرات، أو المواد الإباحية.

5. **السجن لمدة تصل إلى عشر سنوات** و/أو **غرامة مالية تصل إلى خمسة ملايين ريال سعودي**، في حال إنشاء أو نشر مواقع إلكترونية تدعم الإرهاب أو تقوم بتسريب معلومات تمس الأمن الوطني أو الاقتصاد السعودي.

6. **تشدد العقوبات** المنصوص عليها في النظام إذا ارتكبت الجرائم ضمن تشكيل عصابي منظم، أو من قبل موظف عام مستغلًا سلطته الوظيفية، أو عند استغلال القُصّر في ارتكاب الجريمة، أو في حال سبق إدانة الجاني بجرائم مشابهة.

وقد وردت هذه الأحكام ضمن مواد النظام بهدف تحقيق الردع العام والخاص، وتعزيز الحماية القانونية للمجتمع الرقمي في المملكة (نظام مكافحة الجرائم المعلوماتية، 2007)

المبحث الثاني: التجارة الإلكترونية والتنظيم القانوني في المملكة :

المطلب الأول : :نظام التجارة الإلكترونية السعودي وأبرز مواده التنظيمية :

أولا : نظام التجارة الإلكترونية فى المملكة العربية السعودية:

صدر نظام التجارة الإلكترونية في المملكة العربية السعودية عام 1444هـ بموجب المرسوم الملكي رقم (م/126)، وذلك في إطار الالتزام بالمادة 70 من النظام الأساسي للحكم الذي صدر بالأمر الملكي في 1412/8/27هـ. كما استند النظام إلى المادة (العشرين) من نظام مجلس الوزراء، الذي صدر بالأمر الملكي في 1414/3/3هـ، وإلى المادة (الثامنة عشرة) من نظام مجلس الشورى، الصادر في 1412/8/27هـ. بعد الاطلاع على قراري مجلس الشورى الصادرين بتاريخ 1439/10/19هـ، تم اتخاذ القرارات التالية:

أولاً: تمت الموافقة على نظام التجارة الإلكترونية بالصيغة المرافقة، وتم إعداد مشروع مرسوم ملكي بذلك.

ثانيًا: تم تكليف مجلس التجارة الإلكترونية بمتابعة الأنشطة التجارية الإلكترونية في المملكة وتقييمها بعد نفاذ النظام، مع مراعاة الالتزامات الدولية للمملكة وأفضل الممارسات العالمية. كما يتعين على المجلس التأكد من توفير الحد الأدنى من الحماية للمستهلكين والمستثمرين المحليين ضد المنافسة غير المشروعة.

ثالثًا: تم تشكيل لجنة برئاسة معالي وزير المالية وعضوية كل من معالي وزير التجارة والاستثمار ومعالي وزير الاتصالات وتقنية المعلومات. وتتمثل مهمة اللجنة في وضع آلية تضمن استحصال الضرائب على المنتجات والخدمات المتعاقد عليها عبر الوسائل الإلكترونية، بما يضمن المساواة بين موفري الخدمة المحليين والدوليين. كما يجب أخذ التطبيقات العملية في المملكة بعين الاعتبار، مع مراعاة التجارب الدولية وتوجهات المنظمات العالمية ذات الصلة (نظام التجارة الإلكترونية السعودي، 1444هـ).

رابعاً: يجب على وزارة التجارة والاستثمار، عند إعداد اللائحة التنفيذية للنظام، التنسيق مع الهيئة الوطنية للأمن السيبراني بشأن الأحكام المتعلقة بحماية بيانات المستهلك الشخصية. وقد تضمن النظام العديد من المواد التي يمكن تحديدها على النحو التالي:

المادة الأولى :لأغراض تطبيق أحكام هذا النظام، تُعرّف الكلمات والعبارات التالية، حيثما وردت في النظام، بالمعاني المبينة أمام كل منها، ما لم يقتضِ السياق غير ذلك:

- **النظام** :نظام التجارة الإلكترونية.
- **اللائحة** :اللائحة التنفيذية للنظام.
- **الوزارة** :وزارة التجارة والاستثمار.
- **الوزير** :وزير التجارة والاستثمار.

- **التجارة الإلكترونية** :نشاط اقتصادي يُنفذ من قبل موفر الخدمة والمستهلك، كليًا أو جزئيًا، باستخدام وسيلة إلكترونية بهدف بيع المنتجات أو تقديم الخدمات أو الإعلان عنها أو تبادل البيانات الخاصة بها.
- **البيانات** :كل بيان يُستخدم بشكل مباشر أو غير مباشر عند التعامل بالتجارة الإلكترونية.
- **الشخص** :الشخص ذو الصفة الطبيعية أو الاعتبارية.
- **التاجر** :الشخص المقيد في السجل التجاري الذي يمارس التجارة الإلكترونية.
- **الممارس** :الشخص غير المقيد في السجل التجاري الذي يمارس التجارة الإلكترونية.
- **موفر الخدمة** :التاجر أو الممارس.
- **المستهلك** :الزبون الذي يتعامل بالتجارة الإلكترونية بهدف الحصول على المنتجات أو الخدمات.
- **العقد** :الاتفاق الذي يُبرم إلكترونيًا بين الأطراف.
- **المحل الإلكتروني** :موقع إلكتروني يوفر الخدمة أو يعرض منتجًا أو يبيعه.
- **جهات توثيق المحلات الإلكترونية** :الجهات التي ترخص لها الوزارة بتولي عملية توثيق المحلات الإلكترونية.
- **الخطاب الإلكتروني** :بيان أو إعلان أو إشعار أو طلب أو عرض يوجهه أطراف العقد بوسيلة إلكترونية أثناء مرحلة التفاوض أو تنفيذ العقد.
- **الإعلان الإلكتروني** :كل دعاية إلكترونية تهدف إلى تشجيع بيع منتج أو تقديم خدمة بأسلوب مباشر أو غير مباشر.
- **وسيلة إلكترونية** :أي تقنية سواء كانت كهربائية، أو كهرومغناطيسية، أو بصرية، أو ضوئية، أو رقمية، أو أي شكل آخر من وسائل التقنية المشابهة.

المادة الثانية :تسري أحكام النظام على كل من:

- أ- موفر الخدمة داخل المملكة.
- ب- الممارس خارج المملكة الذي يقدم المنتجات أو الخدمات من داخل المملكة بعرضها بطريقة تمكّن المستهلك من الوصول إليها.
- ج- المستهلك.

المادة الثالثة :يقصد بمقر عمل موفر الخدمة لأغراض تطبيق أحكام النظام ما يأتي:

- أ- بالنسبة للتاجر، يكون مقر عمله هو العنوان المحدد في سجله التجاري.
- ب- بالنسبة للممارس، يكون مقر عمله هو المكان الذي يحدده في محله الإلكتروني، ما لم يثبت خلاف ذلك .إذا كان لموفر الخدمة أكثر من مقر عمل و لم يُحدد أحدها، يُعتَمد المقر الأوثق صلة بالعقد، مع مراعاة الظروف التي كان الأطراف على علم بها أو توقعوها قبل أو عند إبرام العقد .إذا لم يكن للممارس ذي الشخصية الطبيعية مقر عمل، يُعتَمد محل إقامته النظامي كمقر عمل. وتحدد اللائحة المعايير والشروط اللازمة لذلك .لا يُعد المكان مقر عمل لمجرد أنه يضم المعدات والتقنيات الداعمة لنظام المعلومات المستخدم من قبل موفر الخدمة في إبرام العقد، أو إذا كان يمكن للأطراف الأخرى الوصول إلى نظام المعلومات المعني .استخدام موفر الخدمة اسم نطاق أو عنوان بريد إلكتروني ذا صلة بدولة معينة (المادة الثانية من نظام التجارة الإلكترونية السعودي).

المادة الرابعة: إذا حدث خطأ من المستهلك في خطاب إلكتروني و لم تتح له تقنية الاتصال تداركه، فله أن يبلغ موفر الخدمة بموضع الخطأ فور علمه به خلال المهلة التي تحددها اللائحة، ويعد هذا الإبلاغ تداركاً للخطأ إن لم يكن قد استفاد من منتج موفر الخدمة أو خدمته أو حصل على منفعة من أي منهما.

المادة الخامسة :ما لم يتفق موفر الخدمة والعميل على مدة أخرى، ودون إخلال بما تقضي به الأنظمة الأخرى، لا يجوز لموفر الخدمة الاحتفاظ ببيانات المستهلك الشخصية أو اتصالاته الإلكترونية إلا للمدة التي تقتضيها طبيعة التعامل بالتجارة الإلكترونية. يجب اتخاذ كافة التدابير اللازمة لحماية هذه البيانات والحفاظ على خصوصيتها خلال فترة الاحتفاظ بها. ويكون موفر الخدمة مسؤولاً عن حماية البيانات الشخصية للمستهلك أو اتصالاته الإلكترونية التي تكون في عهدته أو تحت سيطرة الجهات المتعاملة معها أو مع وكلائها. كما تحدد اللائحة البيانات الشخصية التي يجب الحفاظ على خصوصيتها وفقًا لأهميتها. لا يجوز لموفر الخدمة استخدام بيانات المستهلك الشخصية أو اتصالاته الإلكترونية لأغراض غير مصرح بها أو الإفصاح عنها لجهة أخرى، سواء بمقابل أو بدونه، إلا بموافقة المستهلك المعني أو إذا اقتضت الأنظمة ذلك.

المادة السادسة :يجب على موفر الخدمة الإفصاح في محله الإلكتروني عن البيانات التالية:

- أ- اسمه أو أي بيان مميز له، وعنوانه، ما لم يكن مسجلاً لدى إحدى جهات توثيق المحلات الإلكترونية.
- ب- وسائل الاتصال به.
- ج- اسم السجل المقيد فيه ورقمه إذا كان مقيداً في سجل تجاري أو سجل آخر متاح للعموم.
- د- البيانات الأخرى التي تحددها اللائحة.

المادة السابعة :يلتزم موفر الخدمة بتقديم بيان للمستهلك يوضح فيه أحكام العقد المزمع إبرامه وشروطه، على أن يشتمل البيان على ما يلي:

- أ- الإجراءات الواجب اتخاذها لإبرام العقد.
- ب- البيانات المتعلقة بموفر الخدمة.
- ج- الخصائص الأساسية للمنتجات أو الخدمات محل العقد.
- د- إجمالي السعر شاملاً جميع الرسوم أو الضرائب أو المبالغ الإضافية المتعلقة بالتسليم إن وجدت.
- هـ- ترتيبات الدفع والتسليم والتنفيذ.
- و- بيانات الضمان إن وجدت.
- ز- البيانات الأخرى التي تحددها اللائحة.

وتحدد اللائحة الضوابط اللازمة للبيانات التي يلتزم موفر الخدمة بتقديمها وفقًا لطبيعة كل عملية.

المادة الثامنة :يجب على موفر الخدمة تقديم فاتورة للمستهلك بعد إبرام العقد، تتضمن تكاليف شراء كل منتج أو تقديم خدمة، وإجمالي السعر شاملاً الرسوم أو الضرائب أو المبالغ الإضافية المتعلقة بالتسليم إن وجدت، وتاريخ التسليم ومكانه، وذلك وفقاً لما تحدده اللائحة.

المادة التاسعة :يجب على موفر الخدمة الذي يمارس مهنة تخضع لتنظيم معين وتتطلب ترخيصًا أو تصريحًا بممارستها الإفصاح عن الآتي:

- أ- الجهة المسجل لديها، وبيانات الترخيص أو التصريح الصادر عنها.
- ب- اللقب المهني المعمول به، والدولة التي منحته.
- ج- البيانات الأخرى التي تحددها اللائحة.

المادة العاشرة :يجب أن يتضمن الإعلان الإلكتروني ما يلي:

- أ- اسم المنتج أو الخدمة المعلن عنها.
- ب- اسم موفر الخدمة، وأي بيان مميز له.
- ج- وسائل الاتصال بموفر الخدمة.
- د- البيانات الأخرى التي تحددها اللائحة.

المادة الحادية عشرة :يحظر تضمين الإعلان الإلكتروني ما يلي:

- أ- عرض بيانات كاذبة أو ادعاءً غير صحيح، أو أن تكون صياغته بعبارات من شأنها أن تؤدي بشكل مباشر أو غير مباشر إلى خداع المستهلك أو تضليله.
- ب- شعارًا أو علامة تجارية لا يملك موفر الخدمة حق استخدامها، أو علامة مقلدة.

المادة الثانية عشرة :مع عدم الإخلال بالعقوبات الواردة في المادة (الثامنة عشرة) من النظام، إذا ثبت أن موفر الخدمة خالف أيًا من أحكام الفقرة (2) من المادة (العاشرة) أو المادة (الحادية عشرة)، يحق للوزارة إلزامه بإزالة المخالفة أو سحب الإعلان خلال يوم واحد من تاريخ إبلاغه.

المادة الثالثة عشرة :مع عدم الإخلال بأحكام الضمان الاتفاقية والنظامية، للمستهلك الحق في فسخ العقد خلال الأيام السبعة التالية لتاريخ تسلمه المنتج أو التعاقد على تقديم الخدمة، بشرط ألا يكون قد استخدم المنتج أو استفاد من الخدمة. في هذه الحالة، يتحمل المستهلك التكاليف المترتبة على فسخ العقد، ما لم يتفق أطراف العقد على خلاف ذلك. ولا يحق للمستهلك فسخ العقد في الحالات التالية:

- أ- إذا كانت المنتجات مصنعة بناءً على طلب المستهلك أو وفق مواصفات حددها.
- ب- إذا كانت المنتجات عبارة عن أشرطة فيديو أو أسطوانات أو أقراص مدمجة أو برامج معلوماتية قد تم استخدامها.
- ج- إذا كان العقد يتناول شراء صحف أو مجلات أو منشورات أو كتب.
- د- إذا ظهر عيب في المنتج بسبب سوء استخدام المستهلك.
- هـ- إذا كان العقد يتعلق بتقديم خدمات إيواء أو نقل أو إطعام.
- و- إذا كان العقد يتعلق بشراء منتجات تحميل برامج عبر الإنترنت، باستثناء البرامج التي تحتوي على عيوب تحول دون إتمام التحميل أو غير المطابقة لما تم الاتفاق عليه.
- ز- الحالات الأخرى التي تحددها اللائحة.

المادة الرابعة عشرة :ما لم يتفق موفر الخدمة والمستهلك على مدة أخرى لتسليم محل العقد أو تنفيذه، يحق للمستهلك فسخ العقد إذا تأخر موفر الخدمة عن التسليم أو التنفيذ لمدة تزيد على خمسة عشر يومًا من تاريخ إبرام العقد أو الموعد المتفق عليه. في هذه الحالة، له الحق في استرداد ما دفعه بموجب العقد مقابل المنتج أو الخدمة أو أي تكاليف أخرى ترتبت على التأخير، ما لم يكن التأخير بسبب قوة قاهرة. يلتزم موفر الخدمة أيضًا بإبلاغ المستهلك بأي تأخير متوقع أو صعوبات تؤثر بشكل جوهري في تسليم محل العقد أو تنفيذه.

المادة الخامسة عشرة :يجب على التاجر تسجيل محله الإلكتروني في السجل التجاري وفقًا لنظام السجل التجاري، وتحدد اللائحة الضوابط اللازمة لذلك.

المادة السادسة عشرة :تشرف الوزارة على قطاع التجارة الإلكترونية، وتصدر القواعد اللازمة لتنظيمه بما يعزز دور التجارة الإلكترونية ويحمي سلامة التعاملات فيها، ويشمل ذلك تنظيم الآتي:

- أ- جهات توثيق المحلات الإلكترونية.
- ب- المنصات الإلكترونية التي تؤدي دور الوساطة بين موفر الخدمة والمستهلك.

المادة الثامنة عشرة :مع عدم الإخلال بأي عقوبة أشد ينص عليها نظام آخر، يعاقب كل من يخالف أيًا من أحكام النظام أو اللائحة بإحدى أو أكثر من العقوبات التالية:

- أ- الإنذار.
- ب- غرامة لا تزيد على مليون ريال.
- ج- إيقاف مزاولة التجارة الإلكترونية مؤقتًا أو دائمًا.
- د- حجب المحل الإلكتروني جزئيًا أو كليًا، مؤقتًا أو دائمًا، بالتنسيق مع الجهة المختصة.

المادة التاسعة عشرة :تكوّن بقرار من الوزير لجنة أو أكثر للنظر في مخالفات أحكام النظام أو اللائحة وتوقيع العقوبات المنصوص عليها في المادة (الثامنة عشرة)، على ألا يقل عدد أعضائها عن ثلاثة، ويكون من بينهم مستشار نظامي على الأقل، وتصدر قرارات اللجنة بالأغلبية.

المادة العشرون :يجوز لمن صدر ضده أي قرار بناءً على النظام الاعتراض عليه أمام المحكمة الإدارية وفقًا لأحكام نظام المرافعات أمام ديوان المظالم.

المادة الحادية والعشرون :يجوز تضمين القرار الصادر بتحديد العقوبة النص على نشر منطوقه على نفقة المخالف في صحيفة أو أكثر من الصحف المحلية التي تصدر في محل إقامته، أو في أي وسيلة أخرى مناسبة، بحسب نوع المخالفة المرتكبة وجسامتها وتأثيرها، على أن يكون النشر بعد تحصن القرار بمضي المدة المحددة نظامًا أو إذا كان الحكم الصادر في شأنه مكتسبًا للصفة القطعية.

المادة الثانية والعشرون :تتولى المحكمة المختصة الفصل في المنازعات، بما في ذلك دعاوى المطالبة بالتعويض الناشئة عن تطبيق أحكام النظام.

المادة الثالثة والعشرون :يتولى موظفون يصدر بتعيينهم قرار من الوزير أعمال الرقابة والتفتيش على تعاملات التجارة الإلكترونية وضبط مخالفات أحكام النظام واللائحة.

المادة الرابعة والعشرون :فيما لم يرد في شأنه نص خاص في النظام، تسري على التجارة الإلكترونية أحكام نظام التعاملات الإلكترونية والأنظمة الأخرى ذات الصلة.

المادة الخامسة والعشرون :يصدر الوزير اللائحة خلال تسعين يومًا من تاريخ نشر النظام في الجريدة الرسمية، ويعمل بها من تاريخ العمل بالنظام.

المادة السادسة والعشرون :يعمل بالنظام بعد مضي تسعين يومًا من تاريخ نشره في الجريدة الرسمية.

المطلب الثاني :التحديات القانونية المرتبطة بجرائم التجارة الإلكترونية

- **واقع الجرائم الإلكترونية في السعودية:**

شهدت المملكة العربية السعودية في السنوات الأخيرة تزايدًا ملحوظًا في الجرائم الإلكترونية نتيجة الانتشار الواسع للتكنولوجيا والإنترنت في كافة المجالات الحياتية. وتنوعت هذه الجرائم لتشمل العديد من الأشكال، مثل الاحتيال الإلكتروني، والاختراق وسرقة البيانات، والابتزاز الإلكتروني، وسرقة الهوية، وكلها تهدد الأفراد والشركات على حد سواء. إن التحديات التي تطرحها هذه الجرائم تتطلب استجابة فعالة من خلال تشريعات صارمة، هيئات مختصة، وكذلك توعية مستمرة من أجل حماية الحقوق والمصالح.

من أبرز الجرائم الإلكترونية التي تمس الأفراد والمؤسسات في المملكة:

1. **سرقة أو اختراق الحسابات البنكية والائتمانية** :يتم خلالها استغلال الحسابات المالية لأغراض شخصية، مثل تحويل الأموال أو استخدامها بطرق غير مشروعة.
2. **اختراق المواقع الإلكترونية التجارية** :حيث يتم اختراق المواقع الإلكترونية التجارية بهدف سرقة البيانات أو التلاعب بها من أجل الإضرار بالتجار أو العملاء.

المنظم السعودي قد وضع قوانين صارمة لهذه الجرائم في نظام مكافحة الجرائم المعلوماتية، حيث نصت المادة الرابعة على عقوبات مشددة ضد من يسرق الأموال أو البيانات البنكية، مثل السجن لمدة تصل إلى ثلاث سنوات وغرامات مالية تصل إلى مليوني ريال. كما أن المادة الثالثة من النظام نصت على عقوبات ضد من يخترق المواقع الإلكترونية التجارية أو يساء استخدام الأدوات التكنولوجية في تهديد أو ابتزاز الآخرين.

من خلال هذه التشريعات، تسعى المملكة لحماية مواطنيها ومؤسساتها من مخاطر الجرائم الإلكترونية التي تتزايد باستمرار في ظل التوجه العالمي نحو التعامل الإلكتروني في شتى المجالات. وإن هذه القوانين، بالتوازي مع التوعية المستمرة، تشكل خط الدفاع الأول ضد الجرائم التي قد تهدد أمن الأفراد والمجتمع.

- **التشريعات والإجراءات القانونية فى المملكة العربية السعودية:**

شهدت المملكة العربية السعودية في السنوات الأخيرة زيادة ملحوظة في الجرائم الإلكترونية. يعود ذلك إلى انتشار التكنولوجيا واستخدام الإنترنت بشكل واسع في جميع جوانب الحياة اليومية، سواء في الأعمال التجارية أو الحكومية أو الشخصية. تشمل الجرائم الإلكترونية الشائعة في المملكة ما يلي • :الاحتيال الإلكتروني: يتضمن هذا النوع من الجرائم استخدام الأساليب الاحتيالية للحصول على معلومات شخصية أو مالية من الأفراد أو الشركات. غالبًا ما يتم ذلك عبر البريد الإلكتروني المزيف أو المواقع الإلكترونية الوهمية • . الاختراق وسرقة البيانات: يشمل هذا النوع من الجرائم اختراق أنظمة الكمبيوتر أو الشبكات للحصول على بيانات حساسة، مثل المعلومات المالية أو الشخصية • .الابتزاز الإلكتروني: يتمثل في تهديد الأفراد أو الشركات بنشر معلومات حساسة أو القيام بأعمال ضارة ما لم يتم دفع مبلغ معين من المال • .سرقة الهوية: تشمل استخدام معلومات شخصية مسروقة للقيام بعمليات غير قانونية، مثل فتح حسابات مصرفية أو الحصول على قروض (البشري، 2007م، ص 136).

وقد تنوعت جرائم التجارة الإلكترونية في المملكة العربية السعودية، منها ما يمس الأفراد ومنها ما يمس المؤسسات والشخصيات الاعتبارية، واتفقت على الاعتداء على الحقوق والمصالح بغير وجه حق، على سبيل المثال:

1. **سرقة أو اختراق الحسابات البنكية والائتمانية** :وهذا بهدف استعمال هذه الحسابات لصالح المجرم سواء كان بتحويل الأموال أو استخدامها في غير ذلك. وقد حرص المنظم السعودي على إيقاع أشد العقوبات على المخالفين، وهذا ما تم النص عليه في المادة الرابعة من نظام مكافحة الجرائم المعلوماتية. "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :أ. الاستيلاء على مال منقول أو على سند لنفسه أو لغيره، أو التوقيع على هذا السند، بقصد الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .ب. الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات" (الفهد، 1440هـ، ص 105).
2. **اختراق المواقع الإلكترونية التجارية** :هذا بهدف معرفة بيانات أو سرقة ما يحتويه الموقع من بيانات أو التلاعب فيها بهدف الإضرار بالتاجر أو الزبون. كذلك حرص المنظم السعودي على إيقاع أشد العقوبات لهذه الجرائم، وذلك بالنص على ذلك في نظام مكافحة الجرائم المعلوماتية في المادة الثالثة. "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين

العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية والتي هي التنصت والدخول غير المشروع لتهديد شخص أو ابتزازه، والدخول إلى موقع إلكتروني بطريقة غير مشروعة، وإساءة استخدام الهواتف النقالة أو الكاميرا والتشهير بالآخرين بهدف إلحاق الضرر بهم" (الفهد، 1440هـ، ص 105).

أن الجرائم الإلكترونية تعد من أكبر التحديات التي تواجه المملكة العربية السعودية في العصر الحديث، من خلال التشريعات الصارمة، والهيئات المختصة، والتوعية المستمرة، وتسعى المملكة إلى حماية مواطنيها ومؤسساتها من مخاطر هذه الجرائم، كما أنه يجب تبيان أن التوجه العالمي بلا شك متجه إلى التعامل الإلكتروني سواء كان ذلك بغرض التجارة أو غيره، وهذا يحتاج إلى أنظمة وقوانين رادعة وتواكب هذا الاتجاه، وكذلك فقهاء وقانونيين متخصصين في هذا المجال (المنشاوي، 2012م، ص 349).

الخاتمة:

تسلط هذه الدراسة الضوء على ضرورة تحديث التشريعات في المملكة العربية السعودية بما يتناسب مع التطورات التقنية المتسارعة، كما تدعو إلى تعزيز التعاون بين الجهات الحكومية والشركات الرقمية لمكافحة الجرائم الإلكترونية وحماية بيئة التجارة الإلكترونية في المملكة.

النتائج :

1. يُعد نظام مكافحة الجرائم المعلوماتية السعودي من أبرز النماذج التشريعية في العالم العربي، إلا أن فعاليته لا تزال تعتمد على جودة التنفيذ والتنسيق المؤسسي.
2. تشير البيانات الميدانية إلى أن الجرائم الإلكترونية مستمرة في التزايد، وهو ما يفرض ضغطًا متزايدًا على المنظومة القانونية والتقنية.
3. لا يزال هناك قصور في الوصول السريع إلى الضحايا وتقديم الحماية القانونية لهم، خاصة في قضايا الابتزاز الإلكتروني.
4. غياب التوعية القانونية لدى فئات المجتمع المختلفة يؤدي إلى ضعف في الإبلاغ عن الجرائم وبالتالي إضعاف فاعلية الردع.
5. تُظهر المقارنة بين السعودية وبعض الدول المتقدمة أن المملكة أحرزت تقدمًا في المجال التشريعي، لكنها بحاجة لتقنيات كشف وتتبع أكثر تطورًا.

التوصيات:

1. تطوير منصة وطنية موحدة للإبلاغ عن الجرائم الإلكترونية، مرتبطة بجميع الجهات ذات العلاقة، لتسهيل سرعة الاستجابة.
2. تعزيز القدرات الفنية للقضاة وأعضاء النيابة من خلال برامج تخصصية في التحقيقات الرقمية.
3. مراجعة نظام مكافحة الجرائم المعلوماتية بشكل دوري، لضمان مواكبته للتطورات التقنية والجرائم المستحدثة.
4. إطلاق حملات توعوية على مستوى المدارس والجامعات لتعزيز ثقافة الأمن الرقمي لدى الشباب.
5. التوسع في الشراكات الدولية التقنية والأمنية لتبادل الخبرات وتوحيد الجهود في مواجهة الجريمة الإلكترونية العابرة للحدود.

REFERENCES (المصادر والمراجع)

[1] Ibrāhīm, Khalīl Muḥammad. *Fann al-taḥqīq al-jinā᾽ī fī al-jarā᾽im al-iliktrūniyya*. al-Iskandarīyah: Dār al-Fikr al-Jāmi᾽ī, Ṭ. 1, 2018.

[2] ᾽ al-Bishrī, Muḥammad Aḥmad. *al-Taḥqīq fī Jarā᾽im al-Ḥāsib al-Ālī wa-al-Internet*. al-Riyāḍ: al-Majallah al-᾽Arabiyyah lil-Dirāsāt al-Amniyyah wa-al-Tadrīb – Ākādīmiyyat Nāyif lil-᾽Ulūm al-Amniyyah, Ṭ. 1, 2007.

[3] ᾽ al-Minshāwī, Muḥammad Aḥmad. *Sulaṭat al-Qāḍī al-Jinā᾽ī fī Taqdīr al-Dalīl al-Iliktrūnī*. al-Kuwayt: Majma᾽ al-Nashr al-᾽Ilmī – Jāmi᾽at al-Kuwayt, Ṭ. 1, 2012.

[4] ᾽ al-Bayāḍī, Ḥasan Nūrī Dāwūd. *al-Jarā᾽im al-Iliktrūniyya: al-Taḥaddiyāt wa-al-Tashrī᾽āt*. ᾽ Ammān: Munsha᾽at al-Ma᾽ārif lil-Nashr, Ṭ. 1, 2020.

[5] ᾽ al-Dimyāṭī, Tāmir Muḥammad Sa᾽īd. *Ithbāt al-Ta᾽āqud al-Iliktrūnī ᾽abr al-Internet*. al-Iskandarīyah: Munsha᾽at al-Ma᾽ārif lil-Nashr, Ṭ. 1, 2019.

[6] ᾽ al-Shawwā, Aḥmad Sa᾽īd. *Thawrat al-Ma᾽lūmāt wa-al-Tijārah al-Iliktrūniyya wa-In᾽ikāsātuhā ᾽alá Qānūn al-᾽Uqūbāt*. al-Qāhirah: Dār al-Nahḍah al-᾽Arabiyyah, Ṭ. 1, 2021.

[7] □ al-Ṣaghīr, Jamāl ٠ Abd Allāh ibn Barīk. *al-Jawānib al-Ijrā٠iyyah lil-Jarā٠im al-Muta٠alliqa bi-al-Internet*. al-Qāhirah: Dār al-Nahḍah al-٠ Arabiyyah, Ṭ. 1, 2022.

[8] ٠ al-Fahd, Aḥmad ibn Rāshid. *al-Ḥimāyah al-Jinā٠iyyah lil-Tijārah al-Iliktrūniyya ٠abr al-Internet*. al-Riyāḍ: Dār al-Marīkh lil-Nashr, Ṭ. 1, 1440 H.

[9] ٠ Ibn Jaddū, ٠ Abd Allāh & Dirār, ٠ Abd al-Ra٠ ūf. *al-Āthār al-Iqtiṣādiyyah lil-Jarīmah al-Iliktrūniyya*. al-Jazā٠ ir: Majallat Abḥāth Iqtiṣādiyyah Mu٠ āṣirah, Ṭ. 1, 2022.

[10] ٠ Dahshān, Yāsir Ibrāhīm. *al-Ḥimāyah al-Jinā٠iyyah lil-Mustahlik al-Iliktrūnī*. al-Qāhirah: Majallat Rūḥ al-Qawānīn, Ṭ. 1, 2024.

[11] ٠ Ḥijāzī, ٠ Abd al-Fattāḥ Basiyūnī. *al-Jawānib al-Ijrā٠iyyah li-A٠māl al-Taḥqīq al-Ibtidā٠ī fī al-Jarā٠im al-Ma٠lūmātiyya*. al-Iskandarīyah: Munsha٠at al-Ma٠ārif lil-Nashr, Ṭ. 1, 2019.

[12] ٠ Muḥammad, Sharīf ٠ Abd al-Ghanī. *al-Ḥimāyah al-Jinā٠iyyah lil-Ta٠āmalāt al-Iliktrūniyya*. Baralīn: D. M. lil-Ṭibā٠ ah, Ṭ. 1, 2015.

[13] ٠ Maṭar, ٠ Abd al-٠ Azīz Fahd. *al-Tijārah al-Iliktrūniyya fī al-Tashrī٠āt al-٠Arabiyyah wa-al-Ajnabiyyah*. al-Iskandarīyah: Dār al-Jāmi٠ ah al-Jadīdah, Ṭ. 1, 2014.

[14] ٠ Naṣṣār, Nādirah Muḥammad. *al-Jawānib al-Ijrā٠iyyah li-Jarā٠im al-Internet fī Marḥalat Jam٠ al-Istidlālāt*. al-Iskandarīyah: Dār al-Fikr al-Jāmi٠ ī, Ṭ. 1, 2020.

[15] ٠ Nu٠ mān, Ḍiyā٠ ٠ Abd Allāh Aḥmad. *al-Ghishsh al-Ma٠lūmātī: al-Ẓāhirah wa-al-Taṭbīqāt*. Marrākish: al-Maṭba٠ ah wa-al-Warāqah al-Waṭaniyyah, Ṭ. 1, 2016.

[16] ٠ ٠ Abd al-Raḥīm, Walīd & Ibn Sa٠ īd, Aḥmad & ٠ Abd al-Raḥīm, Nādirah. *al-Jarā٠im al-Iliktrūniyya min Khilāl Mushirrāt ٠Ālamiyyah wa-Āthāruhā ٠alá al-Mu٠assasāt*. al-Jazā٠ ir: Dirāsāt: al-Majallah al-Iqtiṣādiyyah, Ṭ. 1, 2019.

[17] ٠ Wizārat al-Tijārah, al-Su٠ ūdiyyah. *Niẓām al-Tijārah al-Iliktrūniyya al-Su٠ ūdī*. al-Riyāḍ: Wizārat al-Tijārah, Ṭ. 1, 1444 H..

TRANSLITERATION

a. Consonant

Arabic	Latin	Example	
		Arabic	Latin
ء	ʾ	فَأْرٌ	faʾrun
أ	(a,i,u)	أَحكَام	a□kām
ب	b	بَابٌ	bābun
ت	t	تَمْرٌ	tamr
ث	th	ثَلاَثَ	thalātha
ج	j	جَبَلٌ	Jabal
ح	□	حَدِيث	□adīth
خ	kh	خَالِـــدْ	khālid
د	d	دِين	dīn
ذ	dh	مَذهَب	madhhab
ر	r	رَاهِبٌ	rāhib
ز	z	زَكِي	zakī
س	s	سَلاَم	salām
ش	sh	شَرَبَ	sharaba
ص	□	صَدْرٌ	□odrun
ض	□	ضَار	□ār
ط	□	طَهُرَ	□ahura
ظ	□	ظَهْرٌ	z□hohr
ع	ᶜ	عَبْدٌ	ᶜabdun
غ	gh	غَيـــبٌ	ghayb
ف	f	فَاتِحَةٌ	Fātihah
ق	q	قَبَسٌ	qabas
ك	k	كِتَابٌ	kitāb

ل	l	لَيلٌ	layl
م	m	مُنِير	munīr
ن	n	نِقَابٌ	niqāb
و	w	وَعَدَ	waᶜada
ه	h	هَدَفٌ	hadaf
ي	y	يُوسُف	Yūsuf

b. Short Wovel

Arabic	Latin	Example	
		Arabic	Latin
ـَـ	a	كَتَبَ	kataba
ـِـ	i	عَلِمَ	ᶜalima
ـُـ	u	غُلِبَ	ghuliba

c. Long Wovel

Arabic	Latin	Example	
		Arabic	Latin
ا ، ى	ā	عَالَم ، فَتَى	ᶜālam , fatā
ي	ī	عَلِيم ، دَاعِي	ᶜalīm , dāᶜī
و	ū	عُلُوم ، اُدعُو	ᶜulūm , ʼudᶜū

d. Diphthong

Arabic	Latin	Example	
		Arabic	Latin
أَو	aw	أَولَاد	aulād
أَيّ	ay	أَيَّام	ayyam
إِيّ	iy	إِيَّاكَ	iyyāka