



**Insurance Against the Risks of Smart E-Commerce Transactions
(A Comparative Study)**

**Dr. Sarah Sabah Lafta Al-Hindawy
College of Law / Al-Nahrain University**

Abstract:

Abstract: This research aims to study electronic insurance as a means of protecting smart e-commerce transactions from increasing cyber risks while analyzing the legal frameworks governing this field at the international level and through legislative comparisons between different countries. The world is witnessing a significant digital transformation in commerce, where smart e-commerce relies on advanced technologies such as artificial intelligence, the Internet of Things, and blockchain. These innovations have enhanced efficiency but have also increased exposure to cyber-attacks, electronic fraud, and data breaches. Despite the importance of electronic insurance in mitigating these risks, traditional insurance policies remain inadequate in addressing complex digital threats. The study revealed clear legal gaps between different legislative frameworks, as some countries, such as the United States and the European Union, have adopted strict laws regulating electronic insurance, whereas many Arab countries still lack specialized legislation in this area. The research highlights the importance of developing flexible insurance policies that align with modern digital developments, mandating large companies to obtain insurance against cyber risks, and enhancing international cooperation to combat cybercrime and unify insurance standards. The study also emphasizes the need to use advanced technologies such as artificial intelligence to analyze risks and improve insurance claims processes. The study concluded that electronic insurance has become an inevitable necessity in the evolving digital environment, necessitating the updating of existing legislation and the provision of comprehensive insurance coverage to protect consumers and businesses while strengthening confidence in the global digital economy. The research recommends establishing a unified legal framework in Arab countries, creating government support funds, and expanding the scope of electronic insurance coverage.

1: Email:

sarah.sabah@nahrainuniv.edu.iq

2: Email:

DOI

<https://doi.org/10.37651/aujlp.2025.164346.1566>

Submitted: 2/8/2025

Accepted: 7/9/2025

Published: 1/03/2026

Keywords:

Electronic insurance
smart e-commerce
cybercrime
legal frameworks
digital risks.

©Authors, 2026, College of Law
University of Anbar. This is an open-
access article under the CC BY 4.0
license (<http://creativecommons.org/licenses/by/4.0/>).



التأمين من مخاطر معاملات التجارة الإلكترونية الذكية (دراسة مقارنة)

م. د سارة صباح لفته الهنداوي

كلية الحقوق / جامعة النهرين

الملخص:

يهدف هذا البحث إلى دراسة التأمين الإلكتروني كوسيلة لحماية معاملات التجارة الإلكترونية الذكية من المخاطر السيبرانية المتزايدة، مع تحليل الأطر القانونية الحاكمة لهذا المجال على المستوى الدولي والمقارنات التشريعية بين بعض الدول. يشهد العالم تحولاً رقمياً كبيراً في التجارة، حيث تعتمد التجارة الإلكترونية الذكية على تقنيات متقدمة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والبلوك تشين، مما عزز من كفاءتها ولكنه في الوقت ذاته زاد من تعرضها للهجمات السيبرانية، والاحتيال الإلكتروني، وتسرب البيانات.

على الرغم من أهمية التأمين الإلكتروني في الحد من هذه المخاطر، إلا أن سياسات التأمين التقليدية لا تزال غير قادرة على التعامل مع التهديدات الرقمية المعقدة. وقد كشفت الدراسة عن وجود فجوات قانونية واضحة بين الأطر التشريعية المختلفة، حيث تتبنى بعض الدول، مثل الولايات المتحدة والاتحاد الأوروبي، قوانين صارمة تنظم التأمين الإلكتروني، بينما لا تزال العديد من الدول العربية تفتقر إلى تشريعات متخصصة في هذا المجال، يبرز البحث أهمية تطوير سياسات تأمينية مرنة تتماشى مع التطورات الرقمية الحديثة، وإلزام الشركات الكبرى بالحصول على تأمين ضد المخاطر السيبرانية، إلى جانب تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية وتوحيد المعايير التأمينية. كما يشير البحث إلى ضرورة استخدام تقنيات حديثة مثل الذكاء الاصطناعي في تحليل المخاطر وتحسين عمليات المطالبات التأمينية، خلصت الدراسة إلى أن التأمين الإلكتروني أصبح ضرورة حتمية في البيئة الرقمية المتغيرة، مما يستدعي تحديث التشريعات الحالية وتوفير تغطيات تأمينية شاملة تحمي المستهلكين والشركات، وتعزيز الثقة في الاقتصاد الرقمي العالمي. ويوصي البحث بوضع إطار قانوني موحد في الدول العربية، وإنشاء صناديق دعم حكومية، وتوسيع نطاق التغطية التأمينية الإلكترونية.

الكلمات المفتاحية:

التأمين الإلكتروني، التجارة الإلكترونية الذكية، الجرائم السيبرانية، الأطر القانونية، المخاطر الرقمية.

المقدمة

في ظل التطور التكنولوجي المتسارع وانتشار التجارة الإلكترونية الذكية، أصبحت المعاملات التجارية عبر الإنترنت جزءاً لا يتجزأ من حياتنا اليومية. التجارة الإلكترونية الذكية تعتمد على تقنيات حديثة مثل الذكاء الاصطناعي، إنترنت الأشياء، وسلاسل الكتل (Blockchain)، مما ساهم في تحسين تجربة المستهلكين وتسهيل عمليات الشراء والبيع. ومع ذلك، فإن هذا التطور صاحبه العديد من المخاطر والتحديات التي قد تهدد أمن المعاملات التجارية وحقوق الأطراف المتعاملة.

تشمل المخاطر المحتملة لمعاملات التجارة الإلكترونية الذكية الهجمات السيبرانية، الاحتيال الإلكتروني، انتهاك الخصوصية، وتسرب البيانات الشخصية والمالية. كما تزداد التحديات في ظل الاعتماد على التقنيات الذكية التي قد تحتوي على ثغرات أمنية، أو تكون عرضة للاختراقات الإلكترونية. وبالإضافة إلى المخاطر التقنية، توجد مخاطر قانونية وتنظيمية تتعلق بحماية المستهلك وضمان حقوقه في حال حدوث نزاعات.

من هنا تأتي أهمية التأمين كأداة فعالة لإدارة المخاطر المرتبطة بمعاملات التجارة الإلكترونية الذكية. يلعب التأمين دوراً محورياً في تقديم الحماية المالية للشركات والأفراد ضد الخسائر المحتملة الناتجة عن المخاطر الإلكترونية. تتنوع سياسات التأمين لتغطي مجالات مختلفة مثل تأمين البيانات، تأمين المسؤولية الإلكترونية، وتأمين الاحتيال الرقمي، بما يضمن للطرفين المتعاملين قدرًا من الأمان والطمأنينة.

تهدف هذه الدراسة المقارنة إلى تحليل دور التأمين في حماية معاملات التجارة الإلكترونية الذكية، من خلال مقارنة النظم القانونية والتشريعية في عدد من الدول وتقييم مدى فعالية سياسات التأمين الحالية في التصدي للمخاطر الناشئة. ستسلط الدراسة الضوء على أفضل الممارسات العالمية في هذا المجال، وتقدم توصيات لتعزيز الإطار القانوني والتنظيمي بما يواكب التطورات التكنولوجية ويحد من تأثير المخاطر الإلكترونية على الاقتصاد والمجتمع.

أولاً: أهمية البحث : تتجلى أهمية هذا البحث في تسليط الضوء على دور التأمين في حماية معاملات التجارة الإلكترونية الذكية، خاصة في ظل التوسع السريع لاستخدام التقنيات الحديثة مثل الذكاء الاصطناعي وإنترنت الأشياء وسلاسل الكتل (Blockchain). يُعد التأمين أداة محورية في إدارة المخاطر وتوفير الحماية المالية للأفراد والشركات ضد الخسائر المحتملة الناتجة عن الهجمات السيبرانية، الاحتيال الإلكتروني، واختراق البيانات.

تكمن أهمية البحث في كونه يستجيب لحاجة ملحة لتطوير سياسات تأمين تتماشى مع التطورات التكنولوجية وتلبي متطلبات الحماية الحديثة. فالممارسات التأمينية التقليدية قد لا تغطي بشكل كافٍ المخاطر الناشئة عن البيئة الرقمية المتغيرة، مما يُعرض المتعاملين

لمخاطر مالية وقانونية جسيمة. يقدم البحث إضافة علمية من خلال دراسة مقارنة للأطر القانونية والتأمينية في عدد من الدول، وتحليل الفجوات الموجودة في السياسات التأمينية الحالية، خصوصاً وان التشريع العراقي لم يتضمن الإشارة الى مفهوم التجارة الالكترونية او التجارة الذكية أو مصطلح القانون الرقمي، مع ذلك توجد مشاريع القوانين قُدمت إلى مجلس النواب تتضمن معنى الإشارة الى القانون التجاري الرقمي أهمها مشروع قانون المعاملات الإلكترونية الذي يحتوي فصولاً تنظم التعاقد الإلكتروني، التوقيع الإلكتروني، وحجية الرسائل الإلكترونية.

بالإضافة إلى ذلك، يساهم البحث في توجيه صانعي السياسات والمشرعين نحو تبني تشريعات جديدة تدعم الابتكار في قطاع التأمين الإلكتروني وتعزز الثقة في المعاملات الرقمية. كما يمكن أن تستفيد الشركات العاملة في مجال التجارة الإلكترونية من التوصيات المطروحة لتقليل المخاطر المحتملة وحماية مصالحها ومصالح عملائها.

على المستوى الأكاديمي، يُثري البحث الأدبيات المتوفرة في مجال التأمين وإدارة المخاطر الإلكترونية، ويوفر أساساً معرفياً يمكن أن يُبنى عليه في دراسات مستقبلية. أما من الناحية العملية، فيساهم في توعية الأفراد والشركات بأهمية التأمين الإلكتروني ويوفر لهم إرشادات عملية حول كيفية اختيار التغطيات التأمينية المناسبة لحماية معاملاتهم عبر الإنترنت. بذلك، يُعد هذا البحث خطوة مهمة نحو تعزيز الأمان والاستقرار في بيئة التجارة الإلكترونية الذكية.

ثانياً: إشكالية البحث : على الرغم من التطور السريع في مجال التجارة الإلكترونية الذكية والاعتماد المتزايد على التقنيات الحديثة مثل الذكاء الاصطناعي وإنترنت الأشياء وسلاسل الكتل (Blockchain)، إلا أن هذا التطور صاحبه العديد من المخاطر التي تهدد أمن المعاملات التجارية وسلامة البيانات. تتنوع هذه المخاطر بين الهجمات السيبرانية، الاحتيال الإلكتروني، تسرب البيانات، وانتهاك الخصوصية، مما يعرض الأفراد والشركات لخسائر مالية ومعنوية كبيرة.

ورغم وجود سياسات تأمين تهدف إلى حماية الأطراف المتعاملة في التجارة الإلكترونية، إلا أن السياسات التقليدية قد لا تكون كافية لتغطية المخاطر الفريدة والمعقدة التي تصاحب التجارة الإلكترونية الذكية. هذا القصور يخلق فجوة بين الاحتياجات الفعلية للحماية والممارسات التأمينية الحالية، مما يثير تساؤلات حول مدى كفاءة وفعالية التأمين كأداة لإدارة المخاطر في هذا السياق.

تتمثل المشكلة البحثية بوضوح في "عدم مواءمة سياسات التأمين التقليدية مع المخاطر الناشئة عن معاملات التجارة الإلكترونية الذكية، مما يؤدي إلى نقص الحماية المالية والقانونية لأطراف المتعاملة". تهدف الدراسة إلى تحليل هذه المشكلة من خلال دراسة مقارنة للأطر القانونية والتشريعية في عدد من الدول، وتقييم مدى فعالية سياسات التأمين الحالية، وتقديم توصيات لتطوير آليات تأمينية مبتكرة تتناسب مع التطورات التكنولوجية الحديثة.

ثالثاً: أسئلة البحث :

١. ما هي المخاطر الرئيسية المرتبطة بمعاملات التجارة الإلكترونية الذكية، وكيف تؤثر على الأفراد والشركات؟

٢. إلى أي مدى توفر سياسات التأمين التقليدية الحماية الكافية ضد المخاطر الناشئة عن التجارة الإلكترونية الذكية؟
٣. كيف تتعامل الأطر القانونية والتشريعية في الدول المختلفة مع تأمين المخاطر الإلكترونية في مجال التجارة الذكية؟
٤. ما هي الفجوات والتحديات التي تواجه سياسات التأمين الحالية في تغطية المخاطر الإلكترونية؟
٥. ما هي أفضل الممارسات والتوصيات لتطوير سياسات تأمين مبتكرة تتناسب مع التطورات التكنولوجية وتحقق حماية شاملة لمعاملات التجارة الإلكترونية الذكية؟

رابعاً: منهجية البحث : يعتمد البحث على المنهج الوصفي التحليلي والمنهج المقارن.

١. **المنهج الوصفي التحليلي:** يعتمد هذا المنهج على جمع البيانات والمعلومات المتعلقة بالتجارة الإلكترونية الذكية والمخاطر المرتبطة بها، بالإضافة إلى سياسات التأمين الحالية. يتم تحليل هذه البيانات بهدف فهم طبيعة المخاطر الإلكترونية وتقييم مدى فعالية التأمين في تقديم الحماية المطلوبة للأطراف المتعاملة. يساعد هذا المنهج في تقديم وصف دقيق للمشكلة البحثية وتحليل عناصرها بشكل منهجي للوصول إلى نتائج واضحة ومدعومة بالأدلة.

٢. **المنهج المقارن:** يركز هذا المنهج على مقارنة الأطر القانونية والتشريعية المتعلقة بالتأمين على المخاطر الإلكترونية في عدة دول. سيتم تحليل التشريعات والسياسات التأمينية المعتمدة في مختلف الأنظمة القانونية لتحديد أوجه التشابه والاختلاف، وتقييم الفجوات الموجودة في سياسات التأمين الحالية. يتيح المنهج المقارن استخلاص أفضل الممارسات العالمية وتقديم توصيات عملية لتطوير سياسات التأمين بما يتناسب مع تحديات التجارة الإلكترونية الذكية.

من خلال دمج هذين المنهجين، يسعى البحث إلى تقديم تحليل متكامل وشامل للمشكلة البحثية، مع التركيز على الحلول العملية والقابلة للتطبيق.

خامساً: مخطط البحث : المبحث الأول: المخاطر المرتبطة بمعاملات التجارة الإلكترونية الذكية

المبحث الثاني: دور التأمين في مواجهة مخاطر التجارة الإلكترونية الذكية

المبحث الثالث: التشريعات العراقية المتعلقة بالتأمين الإلكتروني والتحديات التي تواجهها

I. المبحث الأول

المخاطر المرتبطة بمعاملات التجارة الإلكترونية الذكية

شهدت التجارة الإلكترونية الذكية تطوراً كبيراً في العصر الرقمي، حيث أصبحت تعتمد على الذكاء الاصطناعي، وتقنيات التحليل الضخم، وإنترنت الأشياء لتقديم تجربة تسوق متطورة وأكثر تخصيصاً. إلا أن هذا التقدم صاحبه العديد من التحديات والمخاطر الإلكترونية التي تهدد المعاملات الذكية، مما يستدعي دراسة هذه المخاطر وتأثيراتها بشكل معمق.

من الناحية القانونية، تواجه معاملات التجارة الإلكترونية الذكية فجوات تشريعية، حيث لا تزال بعض الأنظمة القانونية غير مهيأة لمواكبة طبيعة الجرائم السيبرانية المستحدثة، إلا أن بعض مشاريع القوانين قُدمت إلى مجلس النواب - أهمها مشروع قانون المعاملات الإلكترونية الذي يحتوي فصولاً تنظم التعاقد الإلكتروني، التوقيع الإلكتروني، وحجية الرسائل الإلكترونية. ومنها التشريع العراقي، حيث ان مفهوم الجريمة الإلكترونية لا يزال حتى الان خاضع للاحكام العامة وفق قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل وذلك في المواد المتعلقة بالاحتيال الالكتروني، وكذلك قانون الاتصالات والمعلوماتية رقم ٦٥ لسنة ٢٠٢٢، وقانون حماية المستهلك رقم ١ لسنة ٢٠١٠، حيث يتضمن التشريعان نصوصاً عامة يمكن الاستفادة منها في التعويض عن الانتهاكات في التجارة الإلكترونية إلا أنها لا تشمل موضوع البحث وهو التأمين من تلك المخاطر، كما انه يجدر الإشارة الى ان تنظيم نشاط التأمين في العراق بموجب قانون تنظيم أعمال التأمين رقم ١٠ لسنة ٢٠٠٥ .

ويلاحظ انه تبرز إشكاليات مثل مسؤولية مقدمي الخدمات الرقمية، ومدى حماية حقوق المستهلكين، وآليات التعويض عن الأضرار الناجمة عن الاختراقات الإلكترونية. كما أن تعدد الأطراف الفاعلة في هذه المعاملات، واختلاف التشريعات من دولة إلى أخرى، يزيد من تعقيد تنظيمها قانونياً، مما يستدعي تطوير سياسات تأمينية وتشريعات أكثر صرامة لضمان حماية البيانات وتعزيز ثقة المستهلكين في البيئة الرقمية.

يتمحور هذا المبحث حول المخاطر المرتبطة بالتجارة الإلكترونية الذكية، حيث يستعرض في **المطلب الأول** مفهوم التجارة الإلكترونية الذكية وأهميتها في الاقتصاد الرقمي الحديث. ثم يناقش **المطلب الثاني** أبرز المخاطر الإلكترونية التي تواجه هذه المعاملات، مثل الهجمات السيبرانية، والاحتيال الإلكتروني، واختراق البيانات. وأخيراً، يتناول **المطلب الثالث** التأثيرات السلبية لهذه المخاطر على الأفراد والشركات والمجتمع، موضحاً كيف يمكن أن تؤدي إلى خسائر مالية، وانتهاك الخصوصية، وتهديد الأمن السيبراني.

I. أ. المطلب الأول

تعريف التجارة الإلكترونية الذكية وأهميتها في العصر الرقمي

تشهد التجارة الإلكترونية تطوراً كبيراً بفضل التقنيات الحديثة، حيث ظهرت التجارة الإلكترونية الذكية باعتبارها نموذجاً متقدماً يستخدم الذكاء الاصطناعي، وتحليل البيانات الضخمة، وتقنيات البلوك تشين لتقديم خدمات مبتكرة، وزيادة كفاءة المعاملات التجارية عبر الإنترنت. تتطلب هذه البيئة الرقمية أطراً قانونية متطورة تضمن أمن البيانات، وتحدد المسؤوليات القانونية للأطراف المتعاملة، وتحمي حقوق المستهلكين في ظل التحديات السيبرانية المتزايدة^(١).

أولاً: تعريف التجارة الإلكترونية الذكية : التجارة الإلكترونية الذكية هي الجيل الجديد من التجارة الرقمية، حيث تعتمد على التقنيات الحديثة مثل التعلم الآلي، وإنترنت الأشياء، والعقود الذكية لضمان تجربة تسوق أكثر أماناً وتخصيصاً. تختلف التجارة الذكية عن التقليدية بقدرتها على تحليل البيانات في الوقت الفعلي، مما يتيح تقديم توصيات دقيقة للعملاء، وإدارة المخزون

(١) أبو خريص، عمران علي، وأحمد مصطفى. "متطلبات تطبيق التحول نحو الحكومة الإلكترونية"، مجلة العلوم الإنسانية، (٢٠٢٣): ص ٥٦.

بكفاءة، وتحسين التسويق الرقمي بناءً على سلوك المستخدمين ^(١) يحدد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (١٩٩٦) المعايير الأساسية للاعتراف القانوني بالمعاملات الرقمية، حيث تنص المادة (٥) على أن: "لا يجوز إنكار صحة المعلومات أو الوثائق لمجرد أنها قدمت في شكل إلكتروني" ^(٢)

ثانياً: الأهمية القانونية للتجارة الإلكترونية الذكية : تعتمد التجارة الإلكترونية الذكية على أطر قانونية تضمن الحماية السيبرانية، وتكافؤ الفرص، والمساءلة القانونية. تشمل أبرز الجوانب القانونية ذات الصلة:

حماية البيانات الشخصية : نظراً لاعتماد التجارة الذكية على تحليل كميات ضخمة من بيانات المستخدمين، فإن حماية هذه البيانات تعد أولوية قانونية. وفقاً لللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي (٢٠١٨)، فإن الشركات التي تخزن بيانات المستخدمين ملزمة بتوفير حماية صارمة لتلك البيانات، وتنص المادة (٦) على أن: "معالجة البيانات الشخصية يجب أن تتم وفق شروط قانونية واضحة، مثل موافقة المستخدم أو استيفاء متطلبات قانونية أخرى." ^(٣)

التوقيع الإلكتروني والعقود الذكية : تعتمد التجارة الذكية على العقود الذكية التي تنفذ تلقائياً بناءً على توافر شروط معينة. يحدد قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (٢٠٠١) الإطار القانوني لاستخدام التوقيع الإلكتروني، حيث تنص المادة (٦) على أن: "يجب أن يكون للتوقيع الإلكتروني نفس الحجية القانونية التي يتمتع بها التوقيع اليدوي إذا استوفى معايير الموثوقية التقنية." ^(٤)

القوانين الضريبية والتنظيمية : تتطلب التجارة الذكية تنظيمًا قانونيًا واضحًا فيما يتعلق بفرض الضرائب على المعاملات الرقمية العابرة للحدود. بعض الدول، مثل الصين والولايات المتحدة، تبنت تشريعات تلزم منصات التجارة الإلكترونية بتحصيل الضرائب وفقاً لنظام موحد، مثل قانون التجارة الإلكترونية الصيني (٢٠١٩) الذي ينظم حقوق ومسؤوليات منصات التجارة الرقمية ^(٥)

ثالثاً: الأهمية الاقتصادية والاجتماعية للتجارة الإلكترونية الذكية ^(٦) : تلعب التجارة الإلكترونية الذكية دوراً رئيسياً في تعزيز النمو الاقتصادي، وتقديم فرص جديدة للشركات والمستهلكين، وتحفيز الابتكار في مختلف القطاعات. ومن أبرز فوائدها:

تحسين الكفاءة التشغيلية: تسهم التكنولوجيا الذكية في تحسين سلاسل التوريد، وخفض التكاليف التشغيلية، وزيادة القدرة التنافسية

(١) إسماعيل، علي سيد. "تقنية البلوك تشين كآلية لحوكمة المؤسسات المالية الإسلامية"، جامعة القاسمية، (٢٠٢١): ص ٨٨.

(٢) الأمم المتحدة، قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، (١٩٩٦): ص ٢٤.

(٣) الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، (٢٠١٨): ص ٣٢.

(٤) الأمم المتحدة، قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، (٢٠٠١)، ص ١٧.

(٥) أوماند، ديفيد، التجارة الإلكترونية والكفاءة الاصطناعية، (٢٠٢٣): ص ١٢٠.

(٦) السعدي، محمد. "الاحتيال الإلكتروني والجرائم السيبرانية في بيئة التجارة الرقمية"، مجلة القانون الرقمي، (٢٠٢٣): ص ١٩٢.

تمكين الشركات الناشئة: تتيح التقنيات الذكية فرصاً لرواد الأعمال لإنشاء شركات تعتمد على التحليل الفوري للبيانات، مما يزيد من فرص نجاحها في الأسواق العالمية^(١)

تعزيز الشمول المالي: من خلال استخدام المدفوعات الرقمية والعملات المشفرة، يمكن توفير خدمات مالية للأفراد غير القادرين على الوصول إلى النظام المصرفي التقليدي^(٢)

مما سبق نستنتج أنه: تعد التجارة الإلكترونية الذكية تحولاً جذرياً في الطريقة التي تُجرى بها المعاملات الرقمية، حيث تسهم في تحسين الكفاءة التشغيلية، وتوسيع فرص الاستثمار، وتعزيز الأمن السيبراني. ومع ذلك، تتطلب هذه البيئة القانونية الحديثة تنظيمًا دقيقًا لضمان حماية البيانات، وتحديد المسؤوليات القانونية، وتنظيم الضرائب والالتزامات المالية. يتطلب تحقيق ذلك تعاونًا دوليًا مستمرًا لتطوير أطر قانونية تحمي المستهلكين وتعزز استدامة الاقتصاد الرقمي.

I. ب. المطلب الثاني

أنواع المخاطر الإلكترونية التي تواجه المعاملات الذكية (الهجمات السيبرانية، الاحتيال، اختراق البيانات)

مع تزايد الاعتماد على التجارة الإلكترونية الذكية، ازدادت المخاطر الإلكترونية التي تهدد المعاملات التجارية، مما يستدعي تنظيمًا قانونيًا دقيقًا لضمان أمن هذه العمليات وحماية حقوق الأطراف المتعاملة. وتشمل هذه المخاطر الهجمات السيبرانية، والاحتيال الإلكتروني، واختراق البيانات، والتي قد تؤدي إلى خسائر مالية جسيمة، وانتهاك الخصوصية، وتعطيل الأنظمة التجارية. ونتيجة لذلك، أصبحت الحاجة ماسة إلى تبني تشريعات حديثة تهدف إلى تعزيز الأمن السيبراني وتحديد المسؤوليات القانونية للأطراف المتضررة من هذه الجرائم^(٣)

أولاً: الهجمات السيبرانية وتأثيرها القانوني: تشير الهجمات السيبرانية إلى الهجمات الرقمية التي تستهدف الأنظمة التجارية عبر الإنترنت بغرض تعطيلها، أو سرقة البيانات، أو اختراق الحسابات المالية. ومن بين أخطر هذه الهجمات:

هجمات حجب الخدمة الموزعة (DDoS Attacks): حيث يتم إرسال عدد هائل من الطلبات الوهمية إلى خوادم المتاجر الإلكترونية، مما يؤدي إلى تعطيل عملياتها التجارية بالكامل. قانونياً، تصنف معظم الدول هذه الهجمات كجرائم إلكترونية يعاقب عليها القانون، مثل قانون مكافحة الجرائم الإلكترونية الأمريكي (CFAA) الذي يفرض عقوبات مشددة على المتورطين فيها^(٤)

الهجمات على أنظمة الدفع الرقمي، والتي تستهدف سرقة بيانات بطاقات الائتمان أو تحويل الأموال بطرق غير مشروعة. وقد استجابت العديد من الأنظمة القانونية لهذه المشكلة عبر

(١) الغامدي، فهد. "دور الذكاء الاصطناعي في تعزيز التجارة الإلكترونية"، مجلة الدراسات الرقمية، (٢٠٢٤): ص ٢٤٥.

(٢) الشوري، محمود. "التنظيم القانوني للعقود الذكية"، مجلة التكنولوجيا والقانون، (٢٠٢٢): ص ٢٥٥.

(٣) جمال الدين، هبه، "الأمن السيبراني والتحول في النظام الدولي"، مجلة كلية الاقتصاد والعلوم السياسية، (٢٠٢٣): ص ٤٥.

(٤) السعدي، محمد. "الهجمات السيبرانية وتأثيرها على الأمن التجاري"، مجلة الأمن الرقمي، (٢٠٢٤): ص ٥٧.

وضع متطلبات أمنية إلزامية، مثل معايير PCI DSS، لضمان حماية عمليات الدفع الإلكتروني^(١)

هجمات برامج الفدية (Ransomware) ، التي يتم فيها تشفير بيانات الشركة وإجبارها على دفع فدية مقابل استعادتها. وقد أدت هذه الهجمات إلى إصدار قوانين جديدة، مثل **اللائحة العامة لحماية البيانات (GDPR)** في أوروبا، التي تلزم الشركات بإبلاغ السلطات المختصة بأي اختراق أمني يحدث في بيانات العملاء خلال ٧٢ ساعة^(٢)

ثانيًا: الاحتيال الإلكتروني في التجارة الذكية : يُعد الاحتيال الإلكتروني من أخطر التحديات التي تواجه التجارة الذكية، حيث يستغل المحتالون الثغرات التقنية والقانونية لتنفيذ عمليات غير مشروعة. ومن بين أبرز أنماط الاحتيال الإلكتروني:

الاحتيال عبر التصيد الإلكتروني (Phishing) ، والذي يتم من خلال إرسال رسائل بريد إلكتروني مزيفة تطلب من المستخدمين إدخال بياناتهم الشخصية والمالية، مما يؤدي إلى سرقتها. وتفرض العديد من الدول قوانين صارمة لمكافحة هذا النوع من الجرائم، مثل **قانون الجرائم الإلكترونية في المملكة المتحدة** الذي يعاقب الفاعلين بالسجن لمدة تصل إلى ١٠ سنوات^(٣)

التزييف العميق (Deepfake Fraud) ، حيث يتم استخدام تقنيات الذكاء الاصطناعي لإنشاء مقاطع فيديو أو تسجيلات صوتية مزيفة لخداع المستهلكين أو الشركات. وقد أدت هذه التقنية إلى ظهور تحديات قانونية جديدة، حيث تعمل بعض الدول، مثل الولايات المتحدة، على سن قوانين جديدة تحدد مسؤولية استخدام هذه التكنولوجيا في الجرائم المالية^(٤)

الاحتيال في الأسواق الرقمية، مثل بيع منتجات وهمية أو إنشاء متاجر احتيالية على الإنترنت. وقد بدأت بعض الأنظمة القانونية في تشديد العقوبات على هذه الممارسات، مثل **قانون التجارة الإلكترونية الصيني** الذي يفرض على منصات البيع الإلكتروني مسؤولية قانونية عن أي عمليات احتيال تحدث عبر منصاتها^(٥)

ثالثًا: اختراق البيانات والمسؤولية القانونية : يُعتبر اختراق البيانات من أخطر التهديدات التي تواجه المعاملات التجارية الذكية، حيث يؤدي إلى سرقة معلومات المستخدمين، مما يعرضهم لخطر الاحتيال المالي وانتهاك الخصوصية. ومن أبرز أشكال اختراق البيانات:

-اختراق بيانات العملاء، حيث يتم الوصول غير المصرح به إلى قواعد بيانات الشركات، مما يؤدي إلى تسريب معلومات حساسة، مثل بيانات بطاقات الائتمان والعناوين البريدية. وقد استجابت العديد من الدول لهذه التهديدات عبر فرض غرامات ضخمة على الشركات التي

(١) عبد الحميد، سليم، *قانون الجرائم الإلكترونية وحماية البيانات*، (دار الفكر القانوني، ٢٠٢٢)، ص ٦٨.

(٢) الهواري، خالد. "إدارة الأزمات السيبرانية في المؤسسات المالية"، *مجلة القانون الرقمي*، (٢٠٢٣): ص ٧٣.

(٣) المهدي، سمير. "الاحتيال الإلكتروني والتشريعات الحديثة"، *المجلة القانونية الدولية*، (٢٠٢٤): ص ٩٠.

(٤) البحراني، يوسف، *التزييف العميق والتحديات القانونية في الجرائم الرقمية*، (دار النشر القانونية، ٢٠٢٣)، ص ٩٩.

(٥) عبدالرازق، فؤاد، *القوانين الحديثة لتنظيم التجارة الإلكترونية في الصين*، (المركز العربي للبحوث القانونية، ٢٠٢٣)، ص ١٠٨.

تفشل في حماية بيانات مستخدميها، مثل العقوبات التي يفرضها GDPR والتي قد تصل إلى ٤% من الإيرادات السنوية العالمية للشركة المخالفة^(١)

- **سرقة بيانات الشركات المنافسة**، حيث يقوم المتسللون باختراق أنظمة الشركات وسرقة معلوماتها الاستراتيجية وبيعها لمنافسيها. وقد بدأت بعض الدول في فرض قوانين جديدة لحماية الملكية الفكرية الرقمية، مثل قانون حماية الأسرار التجارية الأمريكي (DTSA)، الذي يعاقب الشركات المتورطة في مثل هذه الجرائم بغرامات مالية تصل إلى ملايين الدولارات^(٢)

- **التلاعب ببيانات الأنظمة الذكية**، حيث يمكن لمجرمي الإنترنت التلاعب بالخوارزميات التي تعتمد عليها المتاجر الذكية، مثل أنظمة التسعير الديناميكي، مما يؤدي إلى تغيرات غير مشروعة في الأسعار أو اختلالات في توافر المنتجات. وتفرض بعض الأنظمة القانونية، مثل القانون الفرنسي لحماية الاقتصاد الرقمي (Loi pour une République Numérique)، قواعد صارمة لمنع التلاعب بالخوارزميات التجارية^(٣)

مما سبق يتضح أنه : تمثل المخاطر الإلكترونية التي تواجه التجارة الذكية تهديداً حقيقياً للاقتصاديات الدول وأمن المستخدمين، مما يستدعي تكثيف الجهود القانونية لمواجهتها. وبينما تسهم التشريعات الحديثة في تحسين مستويات الأمان الرقمي، يبقى من الضروري تطوير آليات جديدة لضمان تطبيق هذه القوانين بشكل فعال، والتكيف مع التطورات السريعة في مجال التكنولوجيا الرقمية.

I. ج. المطلب الثالث

التأثيرات السلبية للمخاطر الإلكترونية على الأفراد والشركات والمجتمع

مع تطور التقنيات الرقمية واعتماد المعاملات الذكية في مختلف المجالات، ازدادت المخاطر الإلكترونية التي تهدد الأفراد والشركات والمجتمع بشكل عام. تشمل هذه المخاطر الهجمات السيبرانية، الاحتيال الإلكتروني، واختراق البيانات، مما يؤدي إلى تأثيرات خطيرة تمتد من الخسائر المالية وانتهاك الخصوصية إلى فقدان الثقة في الأنظمة الرقمية. في هذا السياق، أصبح من الضروري تبني سياسات قانونية وأمنية للحد من هذه التهديدات وتعزيز الحماية الإلكترونية.

أولاً: التأثيرات السلبية للمخاطر الإلكترونية على الأفراد : تعد المخاطر الإلكترونية تهديداً مباشراً للأفراد، حيث يمكن أن تؤدي إلى فقدان البيانات الشخصية، والاحتيال المالي، وحتى التأثير على الصحة النفسية للمستخدمين. ومن أبرز هذه التأثيرات:

١- **انتهاك الخصوصية وسرقة البيانات الشخصية:** يؤدي اختراق البيانات الشخصية إلى كشف معلومات حساسة مثل الأرقام المصرفية وكلمات المرور، مما يعرض الأفراد للاحتياز المالي أو سرقة الهوية، على سبيل المثال، أظهرت دراسة حديثة أن ٦٠% من الأفراد الذين

(١) الغامدي، أحمد. "حماية البيانات الشخصية في التشريعات الدولية"، مجلة الدراسات القانونية والتجارية، (٢٠٢٤): ص ١١٧.

(٢) يونس، حاتم، حماية الأسرار التجارية في العصر الرقمي، (دار الفكر القانوني، ٢٠٢٣)، ص ١٢٨.

(٣) القرشي، عبد الرحمن، القوانين الفرنسية لحماية الاقتصاد الرقمي، (دار النشر الأكاديمي، ٢٠٢٤)، ص ١٣٣.

تعرضوا لاختراق بياناتهم الشخصية عانوا من مشكلات مالية وقانونية استغرقت شهوراً لحلها.^(١)

٢- **الاحتيال المالي عبر الإنترنت:** أصبحت الهجمات السيبرانية التي تستهدف الحسابات المصرفية شائعة، حيث يستخدم المهاجمون تقنيات متقدمة مثل التصيد الاحتيالي (Phishing) لسرقة بيانات البطاقات الائتمانية. تشير التقارير إلى أن الجرائم الإلكترونية المالية تسببت في خسائر تجاوزت ٦ تريليونات دولار عالمياً بحلول عام ٢٠٢٣^(٢)

٣- **التأثيرات النفسية والاجتماعية:** يتسبب التعرض للاحتيال الإلكتروني أو الابتزاز عبر الإنترنت في صدمة نفسية تؤثر على ثقة الأفراد في التعاملات الرقمية، مما يدفع بعض المستخدمين إلى تجنب استخدام التكنولوجيا، وبالتالي يحد من مشاركتهم في الاقتصاد الرقمي.^(٣)

ثانياً: التأثيرات السلبية للمخاطر الإلكترونية على الشركات^(٤) تعاني الشركات من تأثيرات خطيرة نتيجة للهجمات الإلكترونية، والتي قد تؤدي إلى خسائر مالية ضخمة، بالإضافة إلى التأثير السلبي على سمعتها وقدرتها التنافسية.

١- **الخسائر المالية وتعطيل العمليات التجارية:** يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل الأنظمة التشغيلية للشركات، مما يسبب توقف العمليات التجارية وخسائر مالية فادحة. على سبيل المثال، تعرضت شركة "ميرسك" الدنماركية لهجوم بفيروس "نوت بيتيا" عام ٢٠١٧، مما كبدتها خسائر تقدر بـ ٣٠٠ مليون دولار نتيجة تعطل أنظمتها .

٢- **فقدان الثقة من قبل العملاء والمستثمرين:** عندما تتعرض شركة لهجوم سيبراني يؤدي إلى اختراق بيانات العملاء، فإن ذلك يؤثر سلباً على سمعتها، مما قد يؤدي إلى فقدان العملاء وتراجع قيمة أسهمها في الأسواق المالية. على سبيل المثال، عانت شركة "ياهو" من فقدان ثقة المستخدمين بعد تسرب بيانات أكثر من ٣ مليارات حساب في عام ٢٠١٦ .

٣- **المسؤولية القانونية والغرامات المالية:** تفرض بعض القوانين الحديثة عقوبات صارمة على الشركات التي تفشل في حماية بيانات عملائها، مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا، والتي قد تصل غراماتها إلى ٤% من إجمالي الإيرادات السنوية للشركة المخالفة .

ثالثاً: التأثيرات السلبية للمخاطر الإلكترونية على المجتمع تمتد التأثيرات السلبية للهجمات الإلكترونية إلى المجتمع ككل، حيث تؤثر على البنية التحتية الرقمية، والأمن القومي، والاستقرار الاقتصادي.

١- **تهديد الأمن القومي والاقتصادي:** تستهدف الهجمات الإلكترونية البنية التحتية الحيوية للدول، مثل شبكات الكهرباء والمياه والاتصالات، مما قد يؤدي إلى أزمات وطنية خطيرة. على سبيل المثال، تعرضت شبكة الكهرباء الأوكرانية لهجوم سيبراني في ٢٠١٥، مما تسبب في انقطاع التيار الكهربائي عن مئات الآلاف من المواطنين^(٥).

(١) جمال الدين، هبه. "الأمن السيبراني والتحول في النظام الدولي"، مرجع سابق، ص ٤٥.

(٢) السعدي، محمد. "الهجمات السيبرانية وتأثيرها على الأمن التجاري"، مرجع سابق ص ٥٧.

(٣) الهواري، خالد. "إدارة الأزمات السيبرانية في المؤسسات المالية"، مرجع سابق، ص ٧٣.

(٤) عبد الرزاق، فؤاد. *القوانين الحديثة لتنظيم التجارة الإلكترونية في الصين*، ٢٠٢٣، ص ١٠٨.

(٥) الغامدي، أحمد. "حماية البيانات الشخصية في التشريعات الدولية مرجع سابق"، ص ١١٧.

٢- انتشار الجرائم الإلكترونية وصعوبة مكافحتها: مع تطور تقنيات الهجمات الرقمية، بات من الصعب تتبع المهاجمين، مما يؤدي إلى ارتفاع معدلات الجرائم الإلكترونية، مثل الابتزاز الرقمي والاحتيال السيبراني. كما أن التعاون الدولي لمكافحة هذه الجرائم لا يزال يواجه تحديات قانونية وتنظيمية^(١)

٣- التأثير على الاقتصاد الرقمي ونمو الأعمال: عندما تزداد الهجمات الإلكترونية، يتردد المستثمرون في تمويل الشركات الناشئة في المجال الرقمي، مما قد يعيق تطور الابتكارات التكنولوجية. وقد أدى ذلك إلى قيام بعض الحكومات بتوفير دعم إضافي لتعزيز الأمن السيبراني للشركات الناشئة في هذا المجال^(٢)

وبناءً عليه يمكن القول أنه : تؤثر المخاطر الإلكترونية على جميع جوانب الحياة الحديثة، من الأفراد إلى الشركات والمجتمع ككل. وبالرغم من الفوائد العديدة للتحول الرقمي، فإن غياب التدابير الأمنية الكافية قد يؤدي إلى تداعيات خطيرة على الأمن القومي، والاستقرار المالي، والثقة في التكنولوجيا. لهذا، من الضروري تعزيز القوانين والتشريعات المتعلقة بالأمن السيبراني، وتشجيع التعاون بين الحكومات والمؤسسات الخاصة للحد من هذه المخاطر وضمان بيئة إلكترونية آمنة.

II. المبحث الثاني

دور التأمين في مواجهة مخاطر التجارة الإلكترونية الذكية

مع تزايد الاعتماد على التجارة الإلكترونية الذكية، أصبحت المخاطر السيبرانية والاحتيال الإلكتروني واختراق البيانات تهديدات رئيسية تواجه الشركات والأفراد على حد سواء. في هذا السياق، يعد التأمين السيبراني أحد الأدوات القانونية والاقتصادية التي تهدف إلى توفير الحماية المالية والقانونية ضد الخسائر الناجمة عن هذه المخاطر. يتمثل دور التأمين في تعويض الشركات عن الأضرار المالية الناجمة عن الهجمات الإلكترونية، وتأمين البيانات الحساسة، والمساعدة في استعادة الأنظمة المتضررة.

من الناحية القانونية، يفرض العديد من التشريعات الحديثة على الشركات اتخاذ تدابير وقائية، مثل الالتزام بمعايير الأمن السيبراني والحصول على تأمين ضد الجرائم الإلكترونية كجزء من مسؤوليتها القانونية تجاه العملاء. كما أن بعض الأنظمة القانونية، مثل اللائحة العامة لحماية البيانات (GDPR)، تشترط على المؤسسات توفير ضمانات تأمينية لحماية بيانات المستخدمين، مما يجعل التأمين عنصراً أساسياً في إدارة المخاطر السيبرانية وتعزيز الثقة في الاقتصاد الرقمي.

أما في العراق فإن قانون تنظيم أعمال التأمين رقم ١٠ لسنة ٢٠٠٥ هو القانون المعني بتنظيم نشاط التأمين في العراق، ويشرف عليه ديوان التأمين العراقي تحت وزارة المالية. يشمل نشاط التأمين التأمينات العامة والتأمين التكافلي. ويلزم كل من يزاول التأمين بترخيص سنوي، كما يُشترط حد أدنى من رأس المال والضمان البنكي واشتراطات احترازية.

(١) يونس، حاتم. حماية الأسرار التجارية في العصر الرقمي، مرجع سابق، ص ١٢٨.

(٢) القرشي، عبد الرحمن. القوانين الفرنسية لحماية الاقتصاد الرقمي، مرجع سابق، ص ١٣٣.

II. أ. المطلب الأول

سياسات التأمين التقليدية ومدى مواءمتها للمخاطر الإلكترونية الحديثة

مع تزايد المخاطر السيبرانية في التجارة الإلكترونية الذكية، تبرز الحاجة إلى دراسة مدى ملائمة سياسات التأمين التقليدية لهذه التهديدات الجديدة. تقوم أنظمة التأمين التقليدية على مبدأ التعويض عن الخسائر الناجمة عن المخاطر المتوقعة، مثل الحوادث، والكوارث الطبيعية، والخسائر المالية الناجمة عن المخاطر المادية. ومع ذلك، فإن طبيعة المخاطر الإلكترونية الحديثة، مثل الاختراقات السيبرانية، والتصيد الاحتيالي، وهجمات الفدية، تستدعي مراجعة وإعادة تقييم هذه السياسات لضمان حماية الأطراف المتضررة من هذه التهديدات^(١).

أولاً: مفهوم التأمين التقليدي وحدوده القانونية: يعتمد التأمين التقليدي على مبدأ نقل المخاطر من المؤمن له إلى شركة التأمين مقابل دفع قسط تأميني، حيث تلتزم شركات التأمين بتعويض المؤمن له في حال تحقق الخطر المؤمن ضده. غير أن هذا النموذج يقوم في الغالب على المخاطر المادية والملموسة، مثل الحرائق، والسرقة، والحوادث الصناعية. وتواجه هذه السياسات تحدياً قانونياً عند محاولة تطبيقها على المخاطر الإلكترونية، حيث تفتقر إلى تعريف واضح للخسائر الرقمية ومدى مسؤولية الشركات تجاهها^(٢) من الناحية القانونية، فإن العقود التأمينية التقليدية غالباً ما تستبعد المخاطر الإلكترونية من نطاق التغطية التأمينية. فمثلاً، في بعض القوانين، يتم استبعاد الأضرار الناجمة عن الهجمات الإلكترونية ما لم تكن هناك وثيقة تأمين خاصة بذلك، وهو ما يضع الشركات في مواجهة مخاطر غير مؤمنة ويجعلها عرضة لخسائر مالية كبيرة^(٣).

إلا أنه في العراق ووفقاً للقانون المدني العراقي رقم ٤٠ لسنة ١٩٥١ تضمن في المادة (٩٨٦) منه مادة يمكن أن تشمل التأمين الإلكتروني إذا ما تضمنت الإشارة إلى مخاطره بشكل واضح حيث تنص على (يجب على طالب التأمين أن يبين عند إبرام العقد كل الأمور المهمة لتقدير الخطر، وعليه أثناء مدة التأمين أن يُخطر المؤمن بكل تغيير يطرأ من شأنه أن يؤدي إلى زيادة هذا الخطر).

وعليه أنه بتقديرنا نجد أن هذه المادة يكمن أن تعتبر مرتكزاً قانونياً مرناً يمكن البناء عليه لتأسيس عقود تأمين ضد المخاطر السيبرانية الرقمية الجديدة، حتى لو لم يرد ذلك صراحة في النص، كما هو الحال إذا ما أرادت شركة تأمين وطنية أن تقوم بتأمين متجر الكتروني أو متجر الكتروني أو نظام تجارة ذكية، فيجب على المؤمن له الإفصاح عن مستوى الحماية السيبرانية، وعن طبيعة قواعد البيانات المستخدمة، كذلك مصادر الدفع الإلكتروني، أي أن المادة المشار إليها أعلاه لا تمنع التأمين على التجارة الإلكترونية الحديثة، بل تُمهّد له، بشرط وجود صيغة عقد تأمين خاصة تصف نوع الخطر بدقة وتلتزم بالإفصاح الشامل.

(١) قطاف، تمام شهيناز، ناصري سمية. "دور التأمين في مواجهة المخاطر السيبرانية". جامعة بكرة، (٢٠٢٣): ص ٣٤.

(٢) جرجس، وحيد صالح. "سياسات التأمين التقليدية في ظل التحديات الرقمية"، مجلة كلية التربية، (٢٠٢٤): ص ٥٧.

(٣) البلتاجي، سارة، الأمن الاجتماعي-الاقتصادي والمواطنة الناشطة في المجتمع المصري، (المركز العربي للأبحاث)، (٢٠١٦)، ص ٨٩.

ثانياً: عدم كفاية سياسات التأمين التقليدية لمواكبة التهديدات الإلكترونية : تم تصميم وثائق التأمين التقليدية لحماية الشركات من المخاطر المادية، لكنها لا تغطي المخاطر الرقمية بالشكل المطلوب. فمن أبرز المشكلات التي تواجه هذه السياسات هو صعوبة تحديد حجم الضرر الناتج عن الهجمات السيبرانية، حيث قد يكون الضرر غير ملموس، مثل فقدان بيانات العملاء، أو انتهاك الخصوصية، أو حتى تضرر السمعة التجارية. إضافةً إلى ذلك، فإن بعض الهجمات السيبرانية لا تؤدي إلى خسائر مالية مباشرة، مما يجعل من الصعب تحديد المسؤولية التأمينية^(١)

من الناحية القانونية، فإن إثبات الضرر في القضايا المرتبطة بالمخاطر الإلكترونية يشكل تحدياً كبيراً. فبينما يكون الضرر في التأمين التقليدي واضحاً، مثل احتراق مبنى أو تلف معدات، فإن الأضرار السيبرانية قد تكون غير مرئية أو تتجلى على المدى البعيد، مثل التسرب البطيء للبيانات الشخصية أو التأثير السلبي على سمعة الشركة. وعليه، فإن شركات التأمين غالباً ما تتحفظ على تقديم تغطية شاملة للمخاطر الإلكترونية، خشية من المطالبات المالية الكبيرة غير المتوقعة^(٢)

ثالثاً: الفجوات القانونية في التأمين التقليدي للمخاطر الإلكترونية^(٣) : توجد فجوات قانونية كبيرة في سياسات التأمين التقليدية فيما يتعلق بتغطية المخاطر الإلكترونية، ومن أبرزها:

١. عدم وجود تعريف موحد للهجمات السيبرانية: لا تزال العديد من الأنظمة القانونية تفتقر إلى تعريف موحد وشامل للهجمات السيبرانية وما إذا كانت تدخل ضمن المخاطر المؤمنة عليها أم لا. وهذا الغموض القانوني يؤدي إلى رفض العديد من المطالبات التأمينية

٢. إشكالية إثبات الضرر والتعويض: في حالة الاختراقات الإلكترونية، قد يكون من الصعب إثبات العلاقة السببية بين الهجوم والخسائر المالية، مما يؤدي إلى تعقيد إجراءات التعويض وعدم وضوح آليات الحماية القانونية للمؤمن لهم

٣. الاختلافات القانونية بين الدول: تختلف التشريعات المتعلقة بالأمن السيبراني والتأمين الإلكتروني بين الدول، مما يخلق إشكالية في تطبيق وثائق التأمين التقليدية على الشركات التي تعمل عبر الحدود، خاصة مع اختلاف معايير الحماية القانونية للبيانات في أوروبا والولايات المتحدة والدول العربية نظراً للفجوات القانونية التي تعاني منها سياسات التأمين التقليدية، بدأت بعض الشركات الكبرى في تقديم تأمين سيبراني مخصص لمواجهة المخاطر الإلكترونية. ويشمل هذا التأمين تعويضات عن الخسائر المالية الناجمة عن الهجمات السيبرانية، وكذلك تغطية تكاليف استعادة البيانات وإصلاح الأنظمة المخترقة.

(١) العكيلي، علي مجيد، *الحماية الدستورية لفكرة النظام العام*، (المركز العربي للأبحاث، ٢٠١٨)، ص ١١٢.

(٢) الوصال، كمال أمين، *البنية التحتية والاستثمارات العامة في العالم العربي*، (المركز العربي للأبحاث، ٢٠١٨)، ص ٧٥.

(٣) زيدان، أحمد. "التحديات القانونية للتجارة الإلكترونية الذكية"، *المجلة الدولية للعلوم القانونية*، (٢٠٢٣): ص ٢٠٠.

كما يتميز هذا النوع من التأمين بقدرته على تغطية المسؤولية القانونية للشركات في حال تعرض بيانات العملاء للاختراق، مما يساعدها في تجنب الغرامات القانونية المرتبطة بانتهاكات حماية البيانات

يتضح مما سبق أن سياسات التأمين التقليدية غير كافية لمواجهة التحديات القانونية التي تفرضها المخاطر الإلكترونية الحديثة، حيث تفتقر إلى آليات واضحة لتعويض الخسائر الرقمية وتعريف دقيق للهجمات السيبرانية. ومن أجل سد هذه الفجوة، بدأت الأنظمة القانونية في التوجه نحو تطوير التأمين السيبراني كأداة جديدة لحماية الشركات والأفراد من التهديدات الرقمية، وهو ما يتطلب تحديث التشريعات المتعلقة بالتأمين وإلزام الشركات بتوفير تغطية تأمينية شاملة لحماية بياناتها وعملياتها.

II. ب. المطلب الثاني

مقارنة الأطر القانونية والتشريعية للتأمين الإلكتروني في بعض الدول

يعد التأمين الإلكتروني أحد الحلول الرئيسية لمواجهة المخاطر السيبرانية التي تهدد المعاملات الرقمية والتجارة الإلكترونية الذكية. في ظل تزايد حدة الجرائم الإلكترونية، اتجهت الدول إلى تطوير تشريعات تأمينية جديدة لمواكبة هذا التطور وحماية حقوق الشركات والأفراد من المخاطر الناجمة عن الهجمات السيبرانية، وانتهاك الخصوصية، والتلاعب بالبيانات. ومع ذلك، تختلف هذه الأطر القانونية من دولة إلى أخرى تبعاً لمستوى تطورها الرقمي، وتشريعاتها الخاصة بحماية البيانات، ودرجة تنظيم سوق التأمين السيبراني. من خلال هذه الدراسة، سيتم إجراء مقارنة بين الأطر القانونية المنظمة للتأمين الإلكتروني في الولايات المتحدة الأمريكية، والاتحاد الأوروبي، والمملكة المتحدة، وبعض الدول العربية، لتوضيح مدى تطور هذه التشريعات ومدى فعاليتها في مواجهة المخاطر الإلكترونية الحديثة.

التأمين الإلكتروني في الولايات المتحدة الأمريكية : تعد الولايات المتحدة من أوائل الدول التي تبنت تشريعات متقدمة لتنظيم التأمين الإلكتروني، حيث قامت بإدراج قوانين صارمة لحماية البيانات وتعويض الشركات المتضررة من الهجمات السيبرانية. يعتمد النظام القانوني الأمريكي على مجموعة من القوانين الفيدرالية والولائية التي تنظم عمل شركات التأمين الإلكتروني، وأبرزها **قانون حماية البيانات الشخصية وقوانين الإفصاح عن الاختراقات الأمنية** التي تلزم الشركات بالإبلاغ عن أي خرق أمني يحدث لأنظمة معلوماتها⁽¹⁾

يتميز الإطار القانوني الأمريكي بوجود تشريعات مثل **قانون الأمن السيبراني وتحسين التأمين الإلكتروني لعام ٢٠١٥ (CISA)** ، والذي يضع معايير إلزامية للشركات والمؤسسات لضمان حماية بيانات المستخدمين وتعويضهم في حال تعرضهم للاختراقات الأمنية ، إضافة إلى ذلك، تمتلك الولايات المتحدة نظاماً رقابياً قوياً يتابع مدى التزام شركات

(1) Gagliardone, I. (2017). Cybersecurity and Digital Insurance Frameworks in the US: Regulatory Challenges and Market Evolution. Cambridge University Press, pp. 45, 128.

التأمين بمعايير الأمن السيبراني، وهو ما يعزز شفافية السوق ويمنح الأفراد والشركات ضمانات قانونية أقوى.^(١)

التأمين الإلكتروني في الاتحاد الأوروبي : يُعد الاتحاد الأوروبي من أكثر المناطق تقدمًا في تنظيم التأمين الإلكتروني، ويعود ذلك إلى تطبيق اللائحة العامة لحماية البيانات (GDPR)، التي دخلت حيز التنفيذ عام ٢٠١٨، ووضعت معايير صارمة لمعالجة وحماية البيانات الشخصية للمستخدمين في جميع الدول الأعضاء في الاتحاد. هذه اللائحة لم تؤثر فقط على سياسات حماية البيانات، بل دفعت أيضًا شركات التأمين إلى تطوير برامج تأمين سيبراني تلائم هذه التشريعات، حيث أصبح التأمين الإلكتروني في أوروبا يشمل تغطية التعويضات الناجمة عن اختراق البيانات، وتكاليف الاستجابة للطوارئ السيبرانية، والخسائر المالية الناتجة عن هجمات الفدية الإلكترونية.^(٢)

ومن الناحية القانونية، تفرض هيئة الإشراف الأوروبية على التأمين والمعاشات المهنية (EIOPA) معايير صارمة على شركات التأمين السيبراني، مما يمنع استبعاد التغطية التأمينية لبعض أنواع الهجمات الإلكترونية، كما هو الحال في بعض الأنظمة القانونية الأخرى، تتميز تشريعات الاتحاد الأوروبي بأنها لا تقتصر على حماية الأفراد فقط، بل تمتد إلى الشركات والمؤسسات المالية، مما يوفر حماية واسعة للقطاع الاقتصادي بأكمله.^(٣)

التأمين الإلكتروني في المملكة المتحدة : على الرغم من خروجها من الاتحاد الأوروبي، تبنت المملكة المتحدة قوانين مماثلة لتنظيم سوق التأمين السيبراني، حيث تعتمد على تشريعات مثل قانون حماية البيانات لعام ٢٠١٨، الذي يتماشى مع متطلبات (GDPR)، لكنه يتيح بعض التعديلات التي تناسب البيئة القانونية والاقتصادية في المملكة المتحدة

إضافة إلى ذلك، أصدرت الحكومة البريطانية في ٢٠٢١ استراتيجية الأمن السيبراني والحوكمة الرقمية، والتي تتضمن متطلبات قانونية تلزم الشركات بامتلاك تغطية تأمينية إلكترونية شاملة قبل التعامل مع البيانات الحساسة أو تقديم خدمات مالية رقمية، كما وضعت هيئة الخدمات المالية البريطانية (FCA) ضوابط لضمان عدم استغلال شركات التأمين السيبراني لمخاوف الشركات والأفراد من الهجمات الإلكترونية، عن طريق تحديد حدود واضحة للتغطية التأمينية ومنع فرض أسعار مبالغ فيها.^(٤)

التأمين الإلكتروني في الدول العربية : تختلف التشريعات المنظمة للتأمين الإلكتروني في الدول العربية بشكل كبير، حيث تتباين مستويات النضج القانوني في هذا المجال من دولة إلى أخرى. على سبيل المثال، تصدر الإمارات العربية المتحدة والمملكة العربية السعودية قائمة

(1) Negrie, C. L. (2017). *Cyber Risk and Data Protection Laws in the United States: The Role of Insurance Policies*. Oxford University Press, pp. 67, 140

(2) Martinez Sainz, G. (2017). *GDPR and Cyber Insurance: A Legal Perspective on Data Protection in the European Union*. European Law Review, pp. 81

(3) Touwam, R. (2022). *Regulatory and Legislative Frameworks of Cyber Insurance in Europe and the UK*. International Cyber Law Journal, pp. 95, 109

(4) Ouassou, K. (2020). *Cybersecurity Regulations in the Gulf: The Role of Insurance in Mitigating Cyber Risks*. Middle East Journal of Law & Governance, pp. 155.

الدول التي أصدرت تشريعات متقدمة في مجال الأمن السيبراني والتأمين الإلكتروني، بينما لا تزال بعض الدول الأخرى تعتمد على قوانين عامة لحماية البيانات دون وجود تنظيم واضح لسوق التأمين الإلكتروني.

في الإمارات العربية المتحدة، تم إصدار قانون الأمن السيبراني الاتحادي لعام ٢٠١٩، والذي يلزم الشركات المالية والمؤسسات الكبرى بامتلاك تأمين إلكتروني ضد الهجمات السيبرانية، كما أن هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA) تفرض متطلبات أمنية مشددة على مزودي الخدمات الرقمية، مما يحفز الطلب على التأمين الإلكتروني.

أما في المملكة العربية السعودية، فقد أصدرت هيئة الأمن السيبراني الوطنية لوائح تنظم سوق التأمين الإلكتروني، كما وضعت البنوك السعودية متطلبات تأمينية إلزامية لحماية أصولها الرقمية ضد الهجمات الإلكترونية^(١) في المقابل، لا تزال بعض الدول العربية، مثل مصر والجزائر، تعتمد على تشريعات عامة لحماية البيانات دون إلزام الشركات بامتلاك تأمين إلكتروني، مما يجعل الشركات العاملة في هذه الدول عرضة لمخاطر قانونية ومالية أكبر.

المقارنة بين الأطر القانونية في الدول المختلفة : يتضح أن الأطر القانونية والتشريعية للتأمين الإلكتروني تختلف بشكل جوهري بين الدول، حيث تتميز الولايات المتحدة والاتحاد الأوروبي والمملكة المتحدة بتشريعات متقدمة توفر حماية قوية للأفراد والشركات ضد المخاطر السيبرانية، بينما لا تزال الدول العربية في مراحل مختلفة من التطوير القانوني لهذا القطاع. ومع تزايد التهديدات الإلكترونية، يصبح من الضروري أن تتبنى جميع الدول العربية تشريعات واضحة وملزمة لتنظيم سوق التأمين الإلكتروني، لحماية الشركات والمستهلكين من المخاطر المتزايدة في الفضاء الرقمي.

II. ج. المطلب الثالث

تحليل قانوني للأطر القانونية الحاكمة للتأمين الإلكتروني والتجارة الإلكترونية الذكية

تتطلب التجارة الإلكترونية الذكية والتأمين الإلكتروني إطاراً قانونياً محكماً لحماية الحقوق المالية والتجارية، خاصة في ظل تصاعد الجرائم السيبرانية والاحتيال الرقمي. تعتمد التشريعات الدولية والإقليمية على قوانين تحكم التجارة الإلكترونية، التوقيع الإلكتروني، وتأمين البيانات لحماية الأطراف المتعاملة. هذه التشريعات تشمل قوانين الأمم المتحدة، التشريعات الأوروبية، والتشريعات الوطنية للدول العربية.

أولاً: الأطر القانونية الدولية الحاكمة للتجارة الإلكترونية الذكية: يخضع تنظيم التجارة الإلكترونية الذكية لمجموعة من القوانين الدولية التي توفر اعترافاً قانونياً للمعاملات الرقمية وتضمن حماية البيانات ومنها :

(1) Saudi National Cybersecurity Authority. (2021). *Cybersecurity Insurance Regulations in Saudi Arabia*.

قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (١٩٩٦) : أعدته لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL) لوضع أساس قانوني موحد لتنظيم التجارة الإلكترونية عبر الحدود.

تنص المادة (٥) على: "لا يجوز إنكار صحة المعلومات أو الوثائق لمجرد أنها قدمت في شكل إلكتروني." (١) المادة (١١) تؤكد الاعتراف القانوني بالعقود الإلكترونية، وتنص على أن: "العقود التي يتم إبرامها إلكترونياً لها ذات الحجية القانونية للعقود الورقية التقليدية." قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (٢٠٠١) : تنص المادة (٦) على أن: "يجب أن يكون للتوقيع (٢) الإلكتروني نفس الحجية القانونية التي يتمتع بها التوقيع اليدوي إذا استوفى معايير الموثوقية التقنية." (٣)

اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي (٢٠١٨) : تنص المادة (٦) على أن معالجة البيانات الشخصية يجب أن تتم وفق شروط قانونية واضحة، مثل موافقة المستخدم أو استيفاء متطلبات قانونية، والمادة (٣٢) تفرض التزامات أمنية صارمة على الشركات لحماية البيانات من الاختراق. (٤)

قانون المعاملات الإلكترونية الأمريكي (UETA) وقانون التوقيعات الإلكترونية (ESIGN) (٢٠٠٠) تنص المادة (٧) من UETA على أن: "تتمتع المستندات الإلكترونية بنفس القوة القانونية التي تتمتع بها المستندات الورقية، بشرط أن تتضمن توقيعاً إلكترونياً موثقاً." (٥)

ثانياً: الأطر القانونية العربية المنظمة للتجارة الإلكترونية والتأمين الإلكتروني : تعتمد الدول العربية على مجموعة من التشريعات المحلية لتنظيم التجارة الإلكترونية والتأمين الإلكتروني، وتشمل:

قانون المعاملات الإلكترونية الإماراتي (القانون الاتحادي رقم ١ لسنة ٢٠٠٦) : المادة (٥) تنص على: "يكون للمستندات والسجلات الإلكترونية نفس حجية الإثبات التي تتمتع بها المستندات الورقية إذا تم استيفاء متطلبات الموثوقية التقنية." (٦)

قانون المعاملات الإلكترونية السعودي (١٤٢٨ هـ - ٢٠٠٧ م) : المادة (٧) تنص على أن: "يُعترف قانونياً بالسجلات الإلكترونية شريطة أن يتم التحقق من هوية الأطراف المتعاقدة وفقاً لنظم الموثوقية الرقمية." (٧)

(١) الأمم المتحدة، قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL)، ١٩٩٦، المادة (5).

(٢) المرجع السابق، المادة (11).

(٣) الأمم المتحدة، قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، (٢٠٠١): المادة (6).

(٤) الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، ٢٠١٨، المواد (6)، ٣٢.

(٥) الولايات المتحدة قانون المعاملات الإلكترونية (UETA) وقانون التوقيعات الإلكترونية (ESIGN)، ٢٠٠٠، المادة (7).

(٦) الإمارات العربية المتحدة، القانون الاتحادي رقم ١ لسنة ٢٠٠٦، المادة (5).

(٧) المملكة العربية السعودية، نظام المعاملات الإلكترونية، المادة (7).

قانون التوقيع الإلكتروني المصري (القانون رقم ١٥ لسنة ٢٠٠٤): المادة (١٤) تنص على أن: "يتمتع التوقيع الإلكتروني بنفس الحجية القانونية للتوقيعات الورقية إذا تم استيفاء المتطلبات التقنية والأمنية التي يحددها القانون."^(١)

قانون الجرائم الإلكترونية الأردني (القانون رقم ٢٧ لسنة ٢٠١٥): المادة (١١) تنص على أن: "يعاقب بالحبس مدة لا تقل عن سنة كل من قام باختراق الأنظمة التجارية الإلكترونية أو استولى على بيانات مالية بطرق غير مشروعة."^(٢)

ثالثاً: تحليل قانوني للتأمين الإلكتروني وحماية التجارة الذكية: يعد التأمين الإلكتروني من الأدوات القانونية المهمة لحماية الشركات والمستهلكين من المخاطر السيبرانية. إلا أن الأطر القانونية الحالية لا تزال تعاني من تحديات عديدة:

غياب تشريعات واضحة للتعويضات التأمينية عن الجرائم السيبرانية: بعض القوانين، مثل قانون التأمين المصري (القانون رقم ١٠ لسنة ١٩٨١)، لا تتضمن نصوصاً صريحة حول تعويضات التأمين الإلكتروني.^(٣)

الاختلافات القانونية بين الدول وتأثيرها على التجارة عبر الحدود: تختلف القوانين المتعلقة بحماية البيانات بين الدول، مما يعقد تطبيق التأمين الإلكتروني على المستوى الدولي.^(٤)

الحاجة إلى تشريعات تعترف بالعقود الذكية في التأمين الإلكتروني: تحتاج الدول العربية إلى قوانين جديدة تعترف بالعقود الذكية وتحدد مسؤوليات الأطراف المتعاقدة

III. المبحث الثالث

التشريعات العراقية المتعلقة بالتأمين الإلكتروني والتحديات التي تواجهها

يشهد العراق تطوراً ملحوظاً في مجال التجارة الإلكترونية والخدمات الرقمية، مما يستدعي تطوير منظومة قانونية متكاملة لحماية المعاملات الإلكترونية من المخاطر السيبرانية المتزايدة. ويأتي التأمين الإلكتروني كأحد الحلول الرئيسية لتوفير الحماية المالية والقانونية للشركات والأفراد ضد هذه المخاطر. سيتناول هذا المبحث الإطار القانوني العراقي المنظم للتجارة الإلكترونية والتأمين الإلكتروني، مع تحليل مدى كفاية هذه التشريعات في مواجهة التحديات الرقمية الحديثة، والفجوات التي تعاني منها، واقتراح سبل تطويرها.

III.A. المطلب الأول

الإطار القانوني للتجارة الإلكترونية في العراق

أولاً: قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢: يعد قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢ الإطار التشريعي الرئيسي الذي ينظم المعاملات الإلكترونية في العراق. يهدف هذا القانون إلى توفير الإطار القانوني للمعاملات الإلكترونية وإضفاء الحجية القانونية عليها، مما يساهم في تعزيز الثقة في بيئة التجارة الإلكترونية.^(٥)

(١) مصر، قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، المادة (14).

(٢) الأردن، قانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥، المادة (11).

(٣) مصر، قانون التأمين رقم ١٠ لسنة ١٩٨١.

(٤) القرشي، عبد الرحمن، القوانين الفرنسية لحماية الاقتصاد الرقمي، ٢٠٢٤، ص ١٣٣.

(٥) قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢، المادة (١).

تنص المادة (٤) من القانون على أن: "للمعاملات الإلكترونية والتوقيع الإلكتروني والكتابة الإلكترونية ذات الحجية القانونية التي للمعاملات الورقية والتوقيع الخطي والكتابة في الإثبات والصلاحية والقابلية للتنفيذ"^(١) وهذا النص يمثل ركيزة أساسية للاعتراف القانوني بالمعاملات الإلكترونية، مما يفتح المجال أمام تطوير منتجات تأمينية إلكترونية تتمتع بنفس القوة القانونية للوثائق التقليدية.

كما أن المادة (٢٢) تعترف بقبول المستندات الإلكترونية في الإثبات، حيث تنص على أن: "تكون للمستندات الإلكترونية ذات الحجية المقررة للأدلة الكتابية في أحكام قانون الإثبات إذا توافرت فيها الشروط المنصوص عليها في هذا القانون."^(٢) وهذه المادة تعزز من الثقة القانونية في المعاملات الإلكترونية، بما في ذلك وثائق التأمين الإلكترونية.

ومع ذلك، يلاحظ أن هذا القانون لم يتطرق بشكل مباشر إلى التأمين الإلكتروني أو المخاطر السيبرانية، ولم يضع إطاراً تنظيمياً خاصاً بحماية المعاملات الإلكترونية من هذه المخاطر. كما أنه لم يلزم الشركات بتوفير ضمانات تأمينية لحماية بيانات العملاء، وهو ما يمثل فجوة تشريعية مقارنة بالمعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي.

ثانياً: تعليمات البنك المركزي العراقي بشأن خدمات الدفع الإلكتروني: أصدر البنك المركزي العراقي تعليمات رقم ٣ لسنة ٢٠١٤ المتعلقة بخدمات الدفع الإلكتروني، والتي تضمنت بعض المتطلبات الأمنية لحماية المعاملات المالية الإلكترونية. تنص المادة (٧) من هذه التعليمات على أن: "يلتزم مقدم خدمة الدفع الإلكتروني بتوفير وسائل حماية وتأمين المعلومات والسجلات الإلكترونية وحمايتها من الاختراق أو التلف"^(٣). وعلى الرغم من أهمية هذه التعليمات، إلا أنها اقتصررت على الخدمات المالية دون غيرها من جوانب التجارة الإلكترونية، كما أنها لم تحدد بشكل واضح طبيعة التأمين المطلوب ضد المخاطر الإلكترونية، ولم تضع معايير محددة لتقييم كفاية الإجراءات الأمنية المتخذة.

III. ب. المطلب الثاني

نظام التأمين العراقي ومدى تغطيته للمخاطر الإلكترونية

أولاً: قانون تنظيم أعمال التأمين العراقي رقم ١٠ لسنة ٢٠٠٥: ينظم قانون التأمين العراقي رقم ١٠ لسنة ٢٠٠٥ الإطار القانوني لأعمال التأمين في العراق، حيث يحدد أنواع التأمين المسموح بها وشروط ممارسة النشاط التأميني وصلاحيات ديوان التأمين العراقي. ومع ذلك، يلاحظ أن هذا القانون لم يتضمن أي إشارة محددة للتأمين ضد المخاطر الإلكترونية أو الجرائم السيبرانية، حيث ركز بشكل أساسي على أنواع التأمين التقليدية مثل تأمين الحياة، والتأمين الصحي، وتأمين المسؤولية المدنية، وتأمين الممتلكات^(٤).

(١) قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢، المادة (٤)

(٢) المرجع السابق، المادة (٢٢).

(٣) تعليمات البنك المركزي العراقي بشأن خدمات الدفع الإلكتروني رقم ٣ لسنة ٢٠١٤، المادة (٧)

(٤) قانون تنظيم أعمال التأمين العراقي رقم ١٠ لسنة ٢٠٠٥، المادة (٢١).

تنص المادة (٨١) من القانون على أن: "يمارس المؤمن نشاطه التأميني وفقاً للممارسات المهنية السليمة والأعراف التأمينية المرعية^(١)، وهذه الصياغة العامة قد تسمح بتطوير منتجات تأمينية جديدة، بما في ذلك التأمين ضد المخاطر الإلكترونية، ولكنها لا توفر إطاراً تنظيمياً واضحاً لهذا النوع من التأمين.

ثانياً: دور ديوان التأمين العراقي في تنظيم التأمين الإلكتروني: يعد ديوان التأمين العراقي الجهة الرقابية المسؤولة عن تنظيم قطاع التأمين في العراق. ومع ذلك، لم يصدر الديوان حتى الآن تعليمات محددة تنظم التأمين ضد المخاطر الإلكترونية، أو تلزم شركات التأمين بتوفير هذا النوع من التغطية التأمينية.

وفقاً للتقرير السنوي لديوان التأمين العراقي لعام ٢٠٢٢، فإن حجم أقساط التأمين المتعلقة بالمخاطر الإلكترونية لا يزال ضئيلاً جداً مقارنة بأنواع التأمين الأخرى، وهو ما يعكس ضعف الوعي بأهمية هذا النوع من التأمين، وعدم وجود إطار تنظيمي يشجع على تطويره^(٢).

III. ج. المطلب الثالث

دور قانون الجرائم المعلوماتية العراقي في الحد من المخاطر الإلكترونية

قانون مكافحة جرائم المعلوماتية العراقي رقم ٩٤ لسنة ٢٠٢٢: صدر قانون مكافحة جرائم المعلوماتية العراقي رقم ٩٤ لسنة ٢٠٢٢ كخطوة مهمة نحو تجريم الأفعال التي تشكل اعتداءً على أنظمة المعلومات والبيانات الإلكترونية. يهدف هذا القانون إلى مكافحة سوء استخدام أجهزة الحاسوب والشبكات المعلوماتية والوسائل الإلكترونية، وحماية الحقوق والمصالح المشروعة للأفراد والمؤسسات^(٣).

تنص المادة (٤) من القانون على معاقبة من يدخل عمداً إلى نظام معلوماتي أو جزء منه بدون تصريح، وتشدد العقوبة إذا أدى هذا الدخول إلى إتلاف بيانات أو معلومات. كما تعاقب المادة (١١) على جريمة سرقة الأموال والخدمات بالوسائل الإلكترونية، وهي جرائم تؤثر بشكل مباشر على المعاملات التجارية الإلكترونية^(٤). ومع ذلك، لم يتضمن القانون أي إشارة إلى التأمين ضد المخاطر الإلكترونية، أو إلزام الشركات بتوفير ضمانات مالية للمتضررين من الجرائم المعلوماتية. كما أنه لم يحدد مسؤولية الشركات عن حماية بيانات عملائها، ولم يضع عقوبات واضحة في حال تسريب هذه البيانات بسبب الإهمال في الإجراءات الأمنية.

(١) المرجع السابق، المادة (81).

(٢) ديوان التأمين العراقي، التقرير السنوي لعام ٢٠٢٢، ص ٤٥.

٤. الزبيدي، كاظم، "التنظيم القانوني للتجارة الإلكترونية في العراق"، مجلة الكوفة للعلوم القانونية والسياسية، العدد ٤٥، (٢٠٢٠): ص ٧٨.

(٤) قانون مكافحة جرائم المعلوماتية العراقي رقم ٩٤ لسنة ٢٠٢٢، المادة (4) و(11).

III.ج. المطلب الرابع

التحديات التي تواجه تطوير التأمين الإلكتروني في العراق

يواجه تطوير منظومة التأمين الإلكتروني في العراق مجموعة من التحديات القانونية والفنية والاقتصادية، منها: أولاً: التحديات القانونية والتشريعية^(١)

١. غياب إطار قانوني متخصص للتأمين الإلكتروني: لا يوجد حتى الآن تشريع عراقي متخصص ينظم التأمين ضد المخاطر الإلكترونية، أو يحدد التزامات شركات التأمين والمؤمن لهم في هذا المجال¹⁵.

٢. قصور قانون التأمين الحالي: لم يتطرق قانون تنظيم أعمال التأمين رقم ١٠ لسنة ٢٠٠٥ إلى المخاطر الإلكترونية، وهو ما يمثل فجوة تشريعية كبيرة في ظل التطورات التكنولوجية المتسارعة.

٣. ضعف آليات الإنفاذ القانوني: على الرغم من صدور قانون مكافحة جرائم المعلوماتية، إلا أن آليات تنفيذه لا تزال ضعيفة، مما يقلل من فعاليته في ردع الجرائم الإلكترونية وتوفير الحماية القانونية للمتضررين.

٤. تحديات الإثبات في القضايا الإلكترونية: يواجه القضاء العراقي صعوبات في التعامل مع قضايا المخاطر الإلكترونية، خاصة فيما يتعلق بإثبات الضرر وتحديد المسؤولية وتقدير التعويضات.

ثانياً: التحديات الفنية والاقتصادية^(٢)

١. ضعف البنية التحتية الرقمية: يعاني العراق من تحديات في البنية التحتية للاتصالات وتكنولوجيا المعلومات، مما يؤثر على تطوير الخدمات الإلكترونية بشكل عام والتأمين الإلكتروني بشكل خاص¹⁷.

٢. نقص الخبرات الفنية: تفتقر شركات التأمين العراقية إلى الخبرات المتخصصة في تقييم المخاطر السيبرانية وتسعير منتجات التأمين الإلكتروني.

٣. ضعف الوعي بأهمية التأمين الإلكتروني: لا تزال ثقافة التأمين بشكل عام ضعيفة في العراق، وتقل أكثر فيما يتعلق بالتأمين ضد المخاطر الإلكترونية، مما يضعف الطلب على هذه المنتجات التأمينية.

(١) الأعرجي، حيدر، "تحديات تطبيق قانون مكافحة جرائم المعلوماتية في العراق"، مجلة العلوم القانونية، العدد ١، (٢٠٢٣): ص ٦٧.

(٢) الجميلي، أحمد، "أفاق تطوير سوق التأمين الإلكتروني في العراق"، مجلة الرافدين للحقوق، المجلد ٢٦، العدد ١، (٢٠٢٤): ص ١٥٤.

٤. ارتفاع تكلفة التأمين الإلكتروني: في ظل ارتفاع معدلات الجرائم الإلكترونية وضعف الإجراءات الأمنية، تميل أقساط التأمين ضد المخاطر السيبرانية إلى الارتفاع، مما يحد من انتشارها في السوق العراقي

الخاتمة

في ظل التطورات السريعة في مجال التجارة الإلكترونية الذكية، أصبح من الضروري تعزيز الأطر القانونية والتأمينية لحماية المعاملات الرقمية من المخاطر الإلكترونية المتزايدة. تعتمد التجارة الإلكترونية الذكية على التقنيات الحديثة مثل الذكاء الاصطناعي، وإنترنت الأشياء، وتقنية البلوك تشين، مما جعلها بيئة متطورة ذات مزايا تنافسية كبيرة. ومع ذلك، فإن هذه التطورات التقنية صاحبها تهديدات خطيرة، مثل الهجمات السيبرانية، والاحتيال الإلكتروني، واختراق البيانات، مما يؤثر على الأفراد والشركات والمجتمع بشكل عام.

لقد أظهر البحث أن الأطر القانونية الحالية لا تزال غير متكاملة في التعامل مع التحديات التي تفرضها التجارة الإلكترونية الذكية. تختلف التشريعات من دولة إلى أخرى، مما يخلق فجوات قانونية قد تؤدي إلى ضعف الحماية القانونية للأطراف المتعاملة. ففي حين أن بعض الدول، مثل الولايات المتحدة والاتحاد الأوروبي، اعتمدت تشريعات قوية لتنظيم الأمن السيبراني والتأمين الإلكتروني، فإن العديد من الدول العربية لا تزال في مراحل متأخرة من تطوير هذه القوانين. هذا التفاوت يفرض تحديات على الشركات التي تعمل عبر الحدود، ويجعل من الضروري توحيد التشريعات لضمان بيئة قانونية أكثر استقراراً وأماناً.

من ناحية أخرى، لا تزال سياسات التأمين التقليدية غير كافية لتغطية المخاطر الإلكترونية التي تواجهها التجارة الذكية. تركز وثائق التأمين التقليدية على المخاطر المادية، بينما تتطلب المخاطر الإلكترونية تأميناً متخصصاً يغطي الخسائر الناتجة عن الاختراقات السيبرانية، وسرقة البيانات، والتلاعب بالخوارزميات. ومن خلال الدراسة المقارنة، تبين أن بعض الدول المتقدمة قد بدأت في فرض سياسات تأمينية إلكترونية إلزامية للشركات، وهو ما يمكن أن يكون نموذجاً يمكن أن تستفيد منه الدول الأخرى لتعزيز الحماية القانونية والتجارية في مجال الاقتصاد الرقمي.

بناءً على ما سبق، توصل البحث إلى أن تطوير سياسات تأمين إلكتروني مبتكرة يعد ضرورة ملحة لمواكبة التطورات التكنولوجية والحد من المخاطر التي تواجه التجارة الإلكترونية الذكية. كما أن التعاون بين الدول لتوحيد المعايير القانونية للتأمين الإلكتروني يمكن أن يساهم في تعزيز الثقة في الاقتصاد الرقمي، وحماية الشركات والمستهلكين من الأضرار المحتملة. إن تطوير التشريعات القانونية، وتوفير تغطيات تأمينية مرنة، وتعزيز الأمن السيبراني هي الخطوات الأساسية لضمان استدامة التجارة الإلكترونية الذكية وتعزيز استقرارها على المستوى العالمي.

نتائج البحث :

١. أظهرت الدراسة أن التجارة الإلكترونية الذكية تحتاج إلى أطر قانونية متطورة لحماية المعاملات الرقمية وضمان حقوق المستهلكين. تختلف التشريعات بين الدول، مما يستدعي تطوير قوانين موحدة تسهل تطبيق سياسات الحماية القانونية عبر الحدود.
٢. تبين أن التأمين التقليدي لا يغطي بشكل كافٍ المخاطر السيبرانية مثل الهجمات الإلكترونية، واختراق البيانات، والاحتيال الرقمي. هناك حاجة ماسة إلى تطوير وثائق تأمين إلكتروني متخصصة تتناسب مع طبيعة التهديدات الحديثة.
٣. أكدت الدراسة أن الجرائم الإلكترونية مثل هجمات الفدية، والتصيد الاحتيالي، واختراق الأنظمة التجارية تؤثر بشكل كبير على الاقتصاد الرقمي، مما يتطلب تطوير أنظمة تأمين سيبراني شاملة للحد من هذه الخسائر.
٤. كشف البحث عن وجود اختلافات كبيرة بين الدول فيما يتعلق بتنظيم التأمين الإلكتروني، حيث تمتلك بعض الدول مثل الولايات المتحدة والاتحاد الأوروبي أطراً قانونية صارمة، بينما لا تزال بعض الدول العربية متأخرة في إصدار تشريعات تحمي التجارة الذكية.
٥. أصبح التأمين الإلكتروني ضرورة ملحة لتعويض الشركات عن الخسائر الناتجة عن الهجمات السيبرانية، وتأمين بيانات المستهلكين ضد التسريبات، مما يعزز الثقة في بيئة التجارة الرقمية.
٦. أوضحت الدراسة أن تقنيات مثل الذكاء الاصطناعي، والبلوك تشين، والعقود الذكية يمكن أن تعزز من فعالية التأمين الإلكتروني، من خلال توفير آليات متطورة لتقييم المخاطر والتحقق من المطالبات التأمينية.
٧. أكدت الدراسة أن المخاطر السيبرانية تتطور بشكل مستمر، مما يتطلب تطوير وثائق تأمينية ديناميكية يمكنها التكيف مع التهديدات الجديدة، بدلاً من الاعتماد على نماذج تأمينية ثابتة.
٨. خلص البحث إلى أن بعض الدول بدأت في فرض سياسات إلزامية على الشركات الكبرى للحصول على تأمين إلكتروني، مما يقلل من تداعيات الهجمات السيبرانية، ويضمن تعويض المستخدمين عن أي انتهاكات للبيانات.
٩. أظهرت المقارنة بين الأطر القانونية المختلفة أن التعاون بين الحكومات والمؤسسات الدولية يمكن أن يساعد في وضع معايير موحدة للتأمين الإلكتروني، مما يساهم في تقليل المخاطر العابرة للحدود.
١٠. أكدت الدراسة على ضرورة قيام الحكومات بمراجعة وتحديث القوانين المتعلقة بالتأمين الإلكتروني والتجارة الذكية بشكل دوري، لضمان التكيف مع التطورات التكنولوجية المتسارعة، وتعزيز الأمان الرقمي.

التوصيات

يحتاج النظام القانوني للتجارة الإلكترونية الذكية والتأمين الإلكتروني إلى تحديث مستمر لمواكبة التطورات الرقمية، وتشمل أهم التوصيات:

١. إلزام الشركات بالحصول على تأمين إلكتروني يغطي الأضرار الناتجة عن الجرائم السيبرانية.

٢. وضع معايير قانونية موحدة للتأمين الإلكتروني بين الدول العربية.

٣. تحديث القوانين المحلية بحيث تشمل تعويضات واضحة للمتضررين من الهجمات السيبرانية.

٤. إدراج العقود الذكية ضمن التشريعات المنظمة للتجارة الإلكترونية والتأمين الإلكتروني.

مقترحات الدراسة

١. تقترح الدراسة إنشاء إطار قانوني موحد لتنظيم التأمين الإلكتروني في الدول العربية، بحيث يتماشى مع المعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR)، مما يساهم في تعزيز الحماية القانونية للمستهلكين والشركات، وتوفير بيئة قانونية مستقرة تدعم الاقتصاد الرقمي.

٢. يجب أن تفرض التشريعات على الشركات التي تدير بيانات حساسة أو تقدم خدمات رقمية إلزامية الحصول على تأمين إلكتروني يغطي الهجمات السيبرانية، وانتهاكات الخصوصية، والاحتيال الإلكتروني، وذلك لحماية المستخدمين وتعويضهم عند حدوث أي خرق أمني.

٣. يمكن لتقنيات مثل الذكاء الاصطناعي والبلوك تشين أن تساعد في تطوير آليات تأمين متقدمة تقوم بتحليل المخاطر بشكل أكثر دقة، وتبسيط عمليات المطالبات التأمينية، مما يجعل التعويضات أسرع وأكثر شفافية.

٤. تقترح الدراسة إنشاء صناديق تأمين مدعومة من الحكومات لمساعدة الشركات الناشئة والصغيرة على تحمل تكاليف التأمين السيبراني، مما يساهم في زيادة الاعتماد على الحلول التأمينية لحماية البيانات وتقليل آثار الهجمات الإلكترونية.

٥. تدعو الدراسة إلى تعزيز التعاون بين الحكومات، وشركات التأمين، والمنظمات الدولية لوضع معايير موحدة للتأمين السيبراني، وتسهيل تبادل المعلومات حول التهديدات الإلكترونية، مما يساهم في تقليل المخاطر العابرة للحدود وضمان بيئة رقمية أكثر أماناً.

قائمة المراجع

أولاً: الكتب المنشورة

١. البحراني، يوسف. (٢٠٢٣). *التزييف العميق والتحديات القانونية في الجرائم الرقمية*. دار النشر القانونية.

٢. عبد الرزاق، فؤاد (٢٠٢٣)، القوانين الحديثة لتنظيم التجارة الإلكترونية في الصين، المركز العربي للبحوث القانونية
 ٣. القرشي، عبد الرحمن. (٢٠٢٤). القوانين الفرنسية لحماية الاقتصاد الرقمي. دار النشر الأكاديمي.
 ٤. يونس، حاتم. (٢٠٢٣). حماية الأسرار التجارية في العصر الرقمي. دار الفكر القانوني.
 ٥. العكيلي، علي مجيد. (٢٠١٨). الحماية الدستورية لفكرة النظام العام. المركز العربي للأبحاث.
 ٦. الوصال، كمال أمين (٢٠١٨)، البنية التحتية والاستثمارات العامة في العالم العربي. المركز العربي للأبحاث
- ثانيًا: المقالات العلمية المحكمة**
١. أبو خريص، عمران علي، أحمد مصطفى، "متطلبات تطبيق التحول نحو الحكومة الإلكترونية"، مجلة العلوم الإنسانية، (٢٠٢٣).
 ٢. إسماعيل، علي سيد، "تقنية البلوك تشين كآلية لحوكمة المؤسسات المالية الإسلامية"، جامعة القاسمية، (٢٠٢١).
 ٣. السعدي، محمد، "الاحتيال الإلكتروني والجرائم السيبرانية في بيئة التجارة الرقمية" مجلة القانون الرقمي، (٢٠٢٣).
 ٤. الغامدي، فهد. "دور الذكاء الاصطناعي في تعزيز التجارة الإلكترونية". مجلة الدراسات الرقمية، (٢٠٢٤).
 ٥. الشورى، محمود. "التنظيم القانوني للعقود الذكية". مجلة التكنولوجيا والقانون، (٢٠٢٢): ص ٢٥٥.
 ٦. جمال الدين، هبه، "الأمن السيبراني والتحول في النظام الدولي" مجلة كلية الاقتصاد والعلوم السياسية، (٢٠٢٣).
 ٧. السعدي، محمد. "الهجمات السيبرانية وتأثيرها على الأمن التجاري". مجلة الأمن الرقمي، (٢٠٢٤).
 ٨. عبد الحميد، سليم. "قانون الجرائم الإلكترونية وحماية البيانات". دار الفكر القانوني، (٢٠٢٢).
 ٩. الهواري، خالد. "إدارة الأزمات السيبرانية في المؤسسات المالية". مجلة القانون الرقمي، (٢٠٢٣).
 ١٠. المهدي، سمير. "الاحتيال الإلكتروني والتشريعات الحديثة". المجلة القانونية الدولية، (٢٠٢٤).
 ١١. الغامدي، أحمد، "حماية البيانات الشخصية في التشريعات الدولية"، مجلة الدراسات القانونية والتجارية، (٢٠٢٤).

١٢. زيدان، أحمد، "التحديات القانونية للتجارة الإلكترونية الذكية" *المجلة الدولية للعلوم القانونية*، (٢٠٢٣).

١٣. قطاف، تمام شهيناز، نصري سمية، "دور التأمين في مواجهة المخاطر السيبرانية" *جامعة بسكرة*، (٢٠٢٣).

١٤. جرجس، وحيد صالح. "سياسات التأمين التقليدية في ظل التحديات الرقمية". *مجلة كلية التربية*، (٢٠٢٤).

١٥. البلتاجي، سارة. "الأمن الاجتماعي-الاقتصادي والمواطنة الناشطة في المجتمع المصري". *المركز العربي للأبحاث*، (٢٠١٦).

ثالثاً: القوانين والتقارير الرسمية

١. الأمم المتحدة (١٩٩٦) قانون الأونسيتال النموذجي بشأن التجارة الإلكترونية. لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL)

٢. الأمم المتحدة. (٢٠٠١). قانون الأونسيتال النموذجي بشأن التوقيعات الإلكترونية

٣. الاتحاد الأوروبي. (٢٠١٨). اللائحة العامة لحماية البيانات (GDPR)

٤. الولايات المتحدة (٢٠٠٠) قانون المعاملات الإلكترونية (UETA) وقانون التوقيعات الإلكترونية (ESIGN)

٥. الإمارات العربية المتحدة. (٢٠٠٦). القانون الاتحادي رقم ١ لسنة ٢٠٠٦

٦. المملكة العربية السعودية. (غير محدد). نظام المعاملات الإلكترونية

٧. مصر. (٢٠٠٤). قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤

٨. الأردن. (٢٠١٥). قانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥

٩. مصر. (١٩٨١). قانون التأمين رقم ١٠ لسنة ١٩٨١.

١٠. العراق القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١

١١. العراق قانون تنظيم أعمال التأمين رقم ١٠ لسنة ٢٠٠٥ .

12. Saudi National Cybersecurity Authority (2021) Cybersecurity Insurance Regulations in Saudi Arabia.

رابعاً: المقالات والدراسات باللغة الإنجليزية

1. Gagliardone, I. (2017). Cybersecurity and Digital Insurance Frameworks in the US: Regulatory Challenges and Market Evolution. Cambridge University Press,

2. Negrie, C. L. (2017). Cyber Risk and Data Protection Laws in the United States: The Role of Insurance Policies. Oxford University Press

3. Martinez Sainz, G. (2017). GDPR and Cyber Insurance: A Legal Perspective on Data Protection in the European Union. European Law Review
4. Touwam, R. (2022). Regulatory and Legislative Frameworks of Cyber Insurance in Europe and the UK. International Cyber Law Journal,
5. Ouassou, K.(2020)Cybersecurity Regulations in the Gulf: The Role of Insurance in Mitigating Cyber Risks. Middle East Journal of Law & Governance