كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

دار نشر جامعة قطر
Qatar University Press

OPEN ACCESS
Submitted: 16/3/2021
Accepted: 1/6/2021

التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن

محمد سعيد إسماعيل

أستاذ القانون التجاري المساعد، كلية أحمد بن محمد العسكرية، قطر

msesmaeel@abmmc.edu.qa

ملخص

تواجه الشركات التجارية اليوم تحديات كبيرة في الحفاظ على سياسة الخصوصية، وحماية البيانات، وأمن المعلومات. وإدراكًا لهذه التهديدات؛ تدخلت شركات التأمين، وقدمت منتجًا جديدًا نسبيًا، وهو التأمين السيبراني، أو ما يُطلق عليه بالتأمين الإلكتروني، ويمثل هذا التأمين استجابة لمطالب الشركات؛ بالدفاع عنها، والتخفيف من الأضرار الناتجة عن الهجمات الإلكترونية لإحداث خرق البيانات وانتهاك الخصوصية. يهدف هذا البحث إلى دراسة المشكلات القانونية للتأمين الإلكتروني ضد المخاطر السيبرانية، في الوقت الذي تزداد فيه الهجمات الإلكترونية، ويزيد بالمقابل الطلب على التأمين الإلكتروني في ظل الظروف الاستثنائية لجائحة (كوفيد-19). وتشير النتائج إلى ضرورة تنظيم الإطار القانوني لعقد التأمين الإلكتروني في التشريعات الوطنية.

الكلمات المفتاحية: التأمين الإلكتروني، المخاطر السيبرانية، الهجمات الإلكترونية، جائحة (كوفيد-19)، انتهاك الخصوصية، المسؤولية السيبرانية

للاقتباس: إسماعيل، محمد. «التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن»، **المجلة الدولية للقانون**، المجلد العاشر، العدد الثالث، 2021، عدد خاص بمؤتمر «القانون في مواجهة الأزمات العالمية – الوسائل والتحديات»، كلية القانون، جامعة قطر، 7-8 فبراير 2021

https://doi.org/10.29117/irl.2021.0195

دار نشر جامعة قطر
Qatar University Press

كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

OPEN ACCESS

Submitted: 16/3/2021
Accepted: 1/6/2021

Electronic insurance vs. Cyber Risks: Legal issues and suggested solutions - A study on Qatari and Comparative Law

Mohamad Saeed Ismaeel

Assistant Professor of Commercial Law, Ahmed Bin Mohammed Military College, Qatar

msesmaeel@abmmc.edu.qa

Abstract

Today, commercial companies face great challenges in maintaining privacy policy, data protection and information security. In recognition of these threats, insurance companies have intervened and introduced the cyber insurance called also electronic insurance. The cyber insurance is a response to the companies' needs (demands) to defend their interests and reduce data breach and privacy violation damages resulting from electronic attacks. This research aims to study the legal problems related to electronic insurance for cyber risks with an increased cyber-attacks and demands for electronic insurance under the exceptional circumstances of the (Covid-19) pandemic. The results indicate the need to regulate the legal framework for an electronic insurance contract in the national legislation.

Keywords: Electronic insurance; Cyber risks; Cyber-attacks; Pandemic (Covid-19); Privacy violation; Cyber responsibility

Cite this article as: Ismaeel M., "Electronic insurance vs. Cyber Risks: Legal issues and suggested solutions - A study on Qatari and Comparative Law", *International Review of Law*, Volume 10, Issue 3, 2021, Special Issue on the conference of "Law in the Face of Global Crises: Means and Challenges", Collage of Law, Qatar University, 7-8 February 2021

https://doi.org/10.29117/irl.2021.0195

المقدمة

أصبح الإنترنت اليوم عاملًا مهمًا في حياتنا اليومية، وإن كل ما نفعله باستخدام الأجهزة الذكية يمكن للأشخاص الآخرين الاطلاع عليه، سواء أكان ذلك بإرادتنا من خلال مشاركة هذه الأعمال على مواقع التواصل الاجتماعي، أم بدون الحصول على موافقتنا ومعرفتنا بذلك، وقد يبدو الأمر بسيطًا للوهلة الأولى إلا أنه في حقيقته يشكل تهديدًا خطيرًا بما يتضمنه من انتهاك للخصوصية وسرقة البيانات، ويتعاظم دور التهديدات عندما تؤثر هذه الانتهاكات فعليًا على الشركات التجارية والعملاء وجمهور المستهلكين، وقد تشمل هذه التهديدات دولة ما، أو عدة دول بل قد تلحق الضرر بالعالم كله وهذا ما شهدناه في ظل الظروف الاستثنائية لأزمة (COVID-19).

فرضت الظروف الاستثنائية لجائحة كورونا الحاجة إلى الإغلاق الكلي، أو الجزئي للشركات التجارية، واعتماد معظم الدول لبروتوكولات التباعد الاجتماعي والبقاء في المنزل لتقليل الآثار السلبية للجائحة، وتسبب العمل عن بُعد في زيادة المخاطر السيبرانية. تشير الدراسات والإحصائيات إلى زيادة كبيرة في الهجمات الإلكترونية سنة 2020 عن سنة 2019، وتتصدر المخاطر السيبرانية مقياس (Allianz) للمخاطر لأول مرة سنة 2020، وذلك بسبب ازدياد الهجمات الإلكترونية التي تواجه الشركات التجارية (مثل الجرائم الإلكترونية، وفشل/ انقطاع تكنولوجيا المعلومات، وانتهاكات البيانات، وحوادث برامج الفدية)؛ حيث تُستهدف هذه الشركات لأنها تجمع وتستخدم عدد كبير من البيانات الشخصية للعملاء أكثر من أي وقت مضى، وانتهاكات البيانات تصبح أكبر وأكثر تكلفة مع الظروف الاستثنائية التي فرضتها جائحة (COVID-19). ويتضمن مقياس مخاطر (Allianz)، تقرير المخاطر العالمية، سنة 2020 وسنة 2021 الكثير من الدراسات والإحصائيات التي تدل على الزيادة الكبيرة في الهجمات الإلكترونية، ومنها الإحصائيات التالية:

- صدر في الولايات المتحدة الأمريكية وخلال الموجة الأولى من عمليات الإغلاق في أبريل 2020؛ حيث أعلن مكتب التحقيقات الفيدرالي الأمريكي عن زيادة بنسبة 300٪ في الحوادث السيبرانية والهجمات الإلكترونية.
- أصدرت وكالة يوروبول هي وكالة تطبيق القانون الأوربية تقريرًا ذكرت فيه أن هجمات برامج الفدية وسرقة البيانات الشخصية بين يناير ويونيو سنة 2020 بلغت 100.001 من الجرائم الإلكترونية، وبذلك فقد زادت هذه الحوادث السيبرانية بأكثر من الثلث منذ بداية سنة 2020.
- صدرت في المملكة المتحدة تقارير تشير إلى زيادة بنسبة 400٪ في محاولات الهجمات الإلكترونية في قطاع الطاقة البحرية منذ بدء الجائحة وحتى مايو 2020.

تتنوع التهديدات والمخاطر السيبرانية المرتبطة بالبيانات وتكنولوجيا المعلومات في الأعمال التجارية، ومع زيادة اعتماد الأفراد على الاتصالات الإلكترونية والتسوق من الشركات الإلكترونية يتزايد الجمهور المعرض للانتهاكات في حالة اختراق البيانات والحصول على المعلومات الشخصية والمالية والتجارية واستخدامها في الابتزاز الإلكتروني للشركات والأفراد، والقرصنة لوسائل الدفع الإلكترونية مثل بطاقات الائتمانية، والبرامج

الضارة مثل الفيروسات، وبرامج التتبع، والتنصت على المكالمات الهاتفية وغيرها من المخاطر السيبرانية الأخرى.

وتواجه الشركات التجارية اليوم تحديات كبيرة في الحفاظ على سياسة الخصوصية وحماية البيانات وأمن المعلومات، وإدراكًا لهذه التهديدات تدخلت شركات التأمين وقدمت منتجًا جديدًا نسبيًا وهو التأمين السيبراني، أو ما يُطلق عليه بالتأمين الإلكتروني، ويمثل هذا الأخير استجابة لمطالب الشركات بالدفاع عنها والتخفيف من العواقب المحيطة بهجوم الإنترنت لإحداث خرق البيانات وانتهاكات الخصوصية من خلال الهجمات الإلكترونية. ويبدو أن الوعي المتزايد بالأمن السيبراني والحاجة إلى تحديد الأصول المعرضة للخطر يجعل من التأمين على المخاطر الإلكترونية ضرورة حتمية ولا يقدر بثمن، وبالمقابل فإن التأمين الإلكتروني يوفر إمكانات نمو كبيرة في سوق صناعة التأمين.

ومع تنامي السوق السيبراني وتحول الكثير من الشركات وقطاع الأعمال إلى تقديم الخدمات والبيع عن بُعد، قامت شركات التأمين بتنقيح سياسات التأمين ضد المخاطر السيبرانية والترويج لمنتجها الجديد وهو منتج مالي يمكّن الشركات من تغطية التكاليف التي ينطوي عليها التعافي من اختراق الأمن السيبراني، أو الأحداث المماثلة. ومع ذلك فإن المراقبين يرون بأن التأمين الإلكتروني مازال في المهد ويحتاج المزيد من الممارسة والوقت ليصل إلى مرحلة النضج، وتأتي هذه الدراسة لتقف على أهم التحديات القانونية التي تعترض تقدم وتطور التأمين الإلكتروني وتقديم التوصيات والحلول المناسبة التي من الممكن أن تساهم في تنظيم عقود التأمين الإلكتروني بشكل أكثر وضوحًا في المستقبل.

تستكشف هذه الدراسة إلى أي مدى يمكن أن يساعد التأمين الإلكتروني في حماية الأعمال التجارية والشركات واقتصاديات الدول من تغطية تكاليف الهجمات الإلكترونية، وكيف يكون للعوامل المؤسسية لشركات التأمين من جهة ولسياسات الأمن والخصوصية وحماية البيانات للشركات التجارية من جهة أخرى دورًا ايجابيًا، أو سلبيًا قد يعيق أوجه عدم اليقين القانونية في تطور هذا السوق.

ويهدف البحث إلى دراسة المشكلات القانونية للتأمين ضد المخاطر السيبرانية في الوقت الذي تزداد فيه الهجمات الإلكترونية ويزيد بالمقابل الطلب على التأمين الإلكتروني في ظل الظروف الاستثنائية لجائحة (كوفيد – 19) وحالة عدم اليقين القانوني حول إمكانية قيام شركات التأمين بتغطية مخاطر الإنترنت والمسؤولية الإلكترونية للتعويض عن الأضرار المحتملة للمخاطر السيبرانية.

وتثير إشكالية البحث العديد من التساؤلات التي سنحاول الإجابة عنها في هذه الدراسة، ومن أهمها :

- هل حقًا ستقدم شركات التأمين حلًا سحريًا للشركات والأفراد للوصول إلى تعويض عادل عن الأضرار للهجمات الإلكترونية؟
- هل فعلًا سيكون الأفراد والشركات التي لديها بوليصة التأمين الإلكتروني محمية بشكلٍ كافٍ؟
- هل يمكن أن يساهم سوق التأمين الإلكتروني القوي بشكل كبير في حماية اقتصاد الدولة وأمنها السيبراني؟

منهجية البحث:

يركز هذا البحث من منظور قانوني على التأمين الإلكتروني ضد المخاطر السيبرانية ونظرًا لخصوصية الموضوع وأهميته في الوقت الحاضر، فإنه سيعتمد على عدة مناهج علمية، وأهمها المنهج القانوني التحليلي، والمنهج التطبيقي والاستنباطي، والمنهج المقارن لدراسة عقد التأمين الإلكتروني في التشريع القطري والقانون المقارن.

تقسيم البحث:

تنقسم الدراسة إلى مبحثين؛ وفقًا لخطة البحث التالية:

المبحث الأول: التأمين على المسؤولية الإلكترونية ضد المخاطر السيبرانية

المطلب الأول: المخاطر السيبرانية والمسؤولية القانونية.

المطلب الثاني: تغطية التأمين للأضرار الناتجة عن الهجمات الإلكترونية.

المبحث الثاني: نحو عقد نموذجي للتأمين الإلكتروني

المطلب الأول: التحديات القانونية لسياسات التغطية السيبرانية.

المطلب الثاني: مستقبل التأمين الإلكتروني.

المبحث الأول: التأمين على المسؤولية الإلكترونية ضد المخاطر السيبرانية

تشكل المخاطر السيبرانية في بيئتنا الرقمية خطرًا كبيرًا، وتُصنف الحوادث السيبرانية على أنها الخطر الأكبر الذي يواجه الشركات التجارية على مستوى العالم في مقياس ألينز 2020 (Allianz) للمخاطر، ولقد نما الوعي بالتهديد السيبراني بسرعة في السنوات الأخيرة، مدفوعًا باعتماد الشركات المتزايد على بياناتها وأنظمة تكنولوجيا المعلومات وعدد من الحوادث البارزة.

تواجه الشركات عددًا متزايدًا من المخاطر الإلكترونية ذات الهجمات المتطورة التي تستهدف بشكل خاص الشركات الكبيرة والمتوسطة، وزيادة في حوادث برامج الفدية واختراق البريد الإلكتروني للأعمال التجارية ومطالب ابتزاز ضخمة، ويكون للاختلافات السياسية بين الدول دورًا هامًا في الفضاء الإلكتروني يزيد تعقيدًا إضافيًا للمخاطر، في حين أن الاندماج، أو الاستحواذ بين الشركات يمكن أن يؤدي أيضًا إلى مشاكل في التقنية وأنظمة المعلومات.

يُقصد بالتأمين الإلكتروني في هذه الدراسة التأمين ضد المخاطر السيبرانية ولا يشمل البحث التأمين بالوسائل الإلكترونية؛ حيث إن هذا الأخير يشمل كل أنواع التأمين التقليدي ويتميز فقط بأن إبرام العقد يتم عبر الوسائل الإلكترونية ويدخل ضمن دراسة العقود الإلكترونية. ويمكننا أن نعرف التأمين الإلكتروني ضد المخاطر السيبرانية بأنه منتج تأميني جديد مصمم لمساعدة الشركات على التخفيف من الأضرار والآثار المدمرة المحتملة للجرائم

الإلكترونية والمخاطر السيبرانية. ويختلف التأمين الإلكتروني بشكل كبير في النطاق بين مختلف شركات التأمين وأشكال السياسة التأمينية. وبشكل عام، يمكن تصنيف التأمين الإلكتروني على أنه تأمين يوفر تغطية الخسائر المتعلقة بالضرر، أو فقدان المعلومات من ضعف الخدمة المقدمة من قبل تكنولوجيا المعلومات الأنظمة والشبكات. وتقوم شركات التأمين بتغطية المسؤولية الإلكترونية لتأمين الحماية لحاملي وثائق التأمين بالتغطية من المخاطر الإلكترونية التالية:[1]

- مخاطر الطرف الأول والثالث.
- الإضرار بالسمعة التجارية.
- التعدي على حقوق الملكية الفكرية.
- الابتزاز الإلكتروني.
- سرقة، أو فقدان البيانات.
- انقطاع الأعمال.
- مسؤولية الأمن الخصوصية.
- انقطاع / تشغيل أنظمة تكنولوجيا المعلومات.
- تعطل الأعمال السيبرانية، إضافة إلى الغرامات والتكاليف التنظيمية لحماية البيانات.

وسنتناول موضوع التأمين على المسؤولية الإلكترونية في المطلبين التاليين:

المطلب الأول: المخاطر السيبرانية والمسؤولية القانونية

مؤخرًا ومع الزيادة المستمرة في جرائم الإنترنت أصبح التأمين الإلكتروني ضد المخاطر السيبرانية عنصرًا أساسيًا في استراتيجية إدارة المخاطر لدى الشركات التجارية. تشير الدراسات إلى أن الهجمات الإلكترونية تؤدي إلى تكاليف ضخمة على الشركات وتأثيرها يمتد إلى العلامة التجارية ويحدث تغيرات في سلوك المستهلك وهو أمر لا مفر منه، والسؤال الآن ليس «ما إذا كان» سيحدث انتهاكًا أم لا، ولكن «متى»[2].

الفرع الأول: المخاطر السيبرانية

لا يزال سوق التأمين الإلكتروني جديدًا نسبيًا ومتطورًا ولا يزال متأخرًا نسبيًا لمنتجات التأمين التجارية الأخرى في السوق، ويتطلب تطوير سوق التأمين الإلكتروني مزيدًا من التطور لتصميم منتج يمكنه التعامل مع الطبيعة الديناميكية للمخاطر الإلكترونية، وهذا المنتج الجديد مصمم لتوفير الحماية ضد الأضرار، أو الخسائر التي تسببها تهديدات تكنولوجيا المعلومات.

1 Steven Hadwin, Norton Rose Fulbright LLP and Jamie Monck-Mason, Willis Towers Watson, Cyber Insurance: An Overview, Practical Law, 2020, UK. Retrieved on 13/5/2021, from uk.practicallaw.com/w-026-4193.

2 See website, Cyber Insurance, Retrieved on 14/3/2021, from https://www2.deloitte.com/us/en/insights/focus/human-capital-trends.htm

تُسمى مخاطر الإنترنت بالمخاطر السيبرانية. ويبدو أن كلمة السيبرانية جاءت من كلمة (cyber) باللغة الإنجليزية، وهي مشتقة من كلمة (cybernetics) وتعني (علم التحكم الآلي)، الذي صاغه عالم الرياضيات الأمريكي نوربرت فينر سنة 1948، وأصل كلمة (cyber) من الفعل اليوناني القديم (kybereo) وتعني التوجيه، أو التحكم. وذهب بعض الفقه إلى أن هذه التسمية جاءت من كلمة لاتينية هي (Cyber) وتعني الفضاء المعلوماتي[3].

هناك تعريفات كثيرة ومتعددة للمخاطر السيبرانية، ويمكننا أن نستخلص منها تعريفًا جامعًا بأنها «أي خطر لوقوع حادث إلكتروني ناشئ عن استخدام تكنولوجيا المعلومات والاتصالات الذي يضر بسرية البيانات، أو الخدمات، أو توفرها، أو سلامتها، أو إمكانية تتبعها، ويؤدي إلى ضعف التكنولوجيا التشغيلية في النهاية، وإلى اضطراب الأعمال، وانهيار البنية التحتية، وإلحاق أضرار مادية بالبشر والممتلكات». ويتضح لنا بأن المخاطر الإلكترونية هي أي مخاطر تنشأ عن استخدام البيانات الإلكترونية ونقلها، بما في ذلك أدوات التكنولوجيا مثل الإنترنت وشبكات الاتصالات، كما يشمل الضرر المادي الذي يمكن أن ينجم عن حوادث الأمن السيبراني، والاحتيال المرتكب عن طريق إساءة استخدام البيانات، وأي مسؤولية تنشأ عن تخزين البيانات، وتوافر المعلومات الإلكترونية وسلامتها وسريتها – سواء كانت متعلقة بالأفراد، أو الجماعات، أو الحكومات.

والحادث الإلكتروني الذي قد يتسبب في حدوث أعطالًا للعمليات التشغيلية، سواء كانت عرضية، أو ناتجة عن عمد من قبل طرف ثالث غير مصرح له، لذلك فإنه لا يشمل الأخطاء التي تقع من الشركات، أو الأفراد. وبشكلٍ عام يمكن أن تؤدي انتهاكات الالتزامات والسرية المتعلقة بحماية البيانات وانقطاع الأعمال وسرقة البيانات إلى أضرار مالية وخسائر في السمعة التجارية، لذلك من الضروري للشركات التجارية أن تقدر نطاق وطبيعة سياسات المخاطر الإلكترونية المتاحة والعلاقة بين هذه السياسات والمنتجات الجديدة للتأمين الإلكتروني. ويتبيّن لنا بأن الحدث الإلكتروني عبارة عن حدث يمكن ملاحظته في نظام المعلومات، وتقدم الأحداث السيبرانية أحيانًا إشارة إلى وقوع حادث إلكتروني يؤدي إلى: (1) يهدد الأمن السيبراني لنظام المعلومات، أو المعلومات التي يعالجها النظام، أو يخزنها، أو ينقلها؛ أو (2) ينتهك سياسات الأمان، أو الإجراءات الأمنية، أو سياسات الاستخدام المقبولة، سواء كانت ناتجة عن نشاط ضار أم لا[4].

التحول إلى الاقتصاد الرقمي كان دافعًا ومحركًا للنمو الاقتصادي في الدول المتقدمة، لذلك فإن التهديدات السيبرانية تُعد من أكبر المخاطر الأمنية في القرن الحادي والعشرين، وإن الاستخدام المتزايد للتقنيات الجديدة ووسائل الاتصال الحديثة مثل الجيل الخامس (G5) واعتمادنا على الأجهزة الذكية كلها أجزاء من التحول الرقمي العالمي للشركات والمجتمع. ويبدو أن التقنيات الجديدة تجلب نقاط ضعف جديدة، والتكنولوجيات الحديثة تشبه الأضواء الساطعة التي تلقي بظلالها القاتمة فهي تنطوي على الفرص الواعدة الموجهة للمستقبل وتتضمن أيضًا

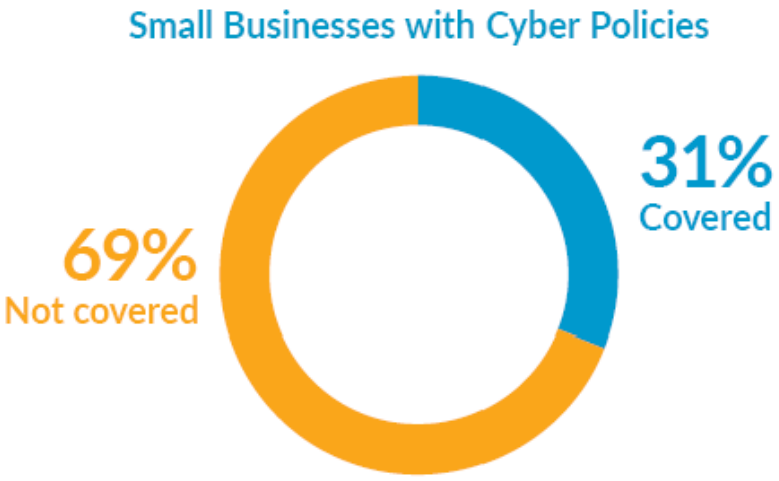
3 «هل أنت جاهز لمواجهة المخاطر السيبرانية؟»، مقالة على موقع شركة التعاونية للتأمين في 17/ 5/ 2017، على الرابط التالي:
https://www.tawuniya.com.sa/about-us/media/blog/blog-detail/tawuniya-blog/2018/05/17/are-you-ready-to-face-cyber-threats (accessed 12/3/2021); "What Does Cyber Mean?" Retrieved on 18/5/2021 from https://www.cyberdefinitions.com/definition_of_cyber.html

4 Cyber Risk for Insurers – Challenges and Opportunities, Luxembourg: Publications Office of the European Union, 2019. © EIOPA, 2019, Reproduction is authorised provided the source is acknowledged.

مخاطر إلكترونية مثل التجسس والتخريب وسرقة البيانات وانتهاك الخصوصية، وينتج عن الهجمات الإلكترونية خسائر مادية ومعنوية كبيرة[5].

ولكن السؤال الذي تثيره هذه المخاطر ومن المنظور القانوني، إلى أي مدى تنتشر تلك المخاطر الإلكترونية، وما تأثيرها على الشركات التجارية؟

خلصت دراسة في الولايات المتحدة الأمريكية أجريت على الشركات الصغيرة والمتوسطة إلى النتائج التالية: 76٪ من الشركات الصغيرة والمتوسطة تعرضت لهجوم إلكتروني في عام 2019، ومع ذلك فإن 31٪ فقط من هذه الشركات حصلت على تأمين إلكتروني سنة 2020.



الشكل (1): السياسات السيبرانية للشركات الصغيرة[6].

لماذا لا تشتري المزيد من الشركات الأمريكية الصغيرة والمتوسطة بوليصة التأمين الإلكتروني؟

أوضحت الدراسة السابقة إلى أن انخفاض نسبة الشركات الصغيرة والمتوسطة في شراء بوليصة التأمين الإلكتروني، رغم أهميته، يرجع إلى سببين هما:

1. **نقص الوعي والمعرفة بالمخاطر السيبرانية**: يقع على عاتق شركات التأمين واجب المساعدة في سد الفجوة التعليمية بين التعرض للمخاطر السيبرانية والحماية منها، وتثقيف العملاء حول كيفية التعامل معها لزيادة الوعي بالمخاطر الإلكترونية.

5 طورت شركة التأمين وإعادة التأمين (Munich Re) نظامًا إلكترونيًا خاصًا بها، يضم شركات التكنولوجيا وموفري أمن تكنولوجيا المعلومات والشركات الناشئة لتطوير حلول للمخاطر السيبرانية؛ لأن متطلبات الحماية الشاملة معقدة، والحماية من الخسائر المالية ليست سوى عنصر واحد من مفهوم شامل. وفقًا لذلك، تقوم الشركة بتطوير خدمات وقائية مؤتمتة عالية الفعالية لعملائها، وهي مصممة لمراقبة البنية التحتية للعميل بشكل دائم، وتحديد المخاطر على الفور، ومنع الخسائر.
Munich Re worldwide, See website, Retrieved on 14/3/2021, from https://www.munichre.com/en.html

6 Molly Corbett, Ransomware, COVID-19 and Cyber Insurance - The Big Disconnect, December 09, 2020, Region: North America. Retrieved on 14/3/2021, from https://www.genre.com/knowledge/blog/ransomware-covid-19-and-cyber-insurance-the-big-disconnect-en.html

2. **التكلفــة المرتفعــة للتأمين الإلكتروني**: لذلك يجــب أن توفر شركات التأمين خيــارات أكثر، للتغطية من المخاطر السيبرانية، وبأسعار معقولة في السوق، وتحتاج شركات التأمين دعم الحكومات الوطنية لتشجيع الشركات التجارية للحصول على التأمين الإلكتروني.

الفرع الثاني: التنظيم القانوني

من الصعوبات التي تعترض تحديد المســؤولية الإلكترونية عن المخاطر الســيبرانية تتعلق بعدم وجود تعريف موحد لمصطلحي «الأمن السيبراني» و«الهجمات الإلكترونية» على المستوى العالمي، وقد تصدى بعض المتخصصين لضبط هذين المصطلحين، ويُعرف «الأمن الســيبراني» بأنه يشمل «مجموعة الأدوات والسياسات ومفاهيم الأمن، والضمانات الأمنية، والمبادئ التوجيهية، وأســاليب إدارة المخاطر، والإجراءات، والتدريب، وأفضل الممارسات، والضمانــات والتقنيات التي يمكن اســتخدامها لحماية البيئــة الإلكترونية وأصول المنظمة والمســتخدمين»، أما «الهجوم الإلكتروني» فإنه يشير إلى التعطيل المتعمد لـ سرية نظام المعلومات، أو سلامته، أو توفره. ويبدو أيضًا من الضروري تحديد المخاطر المتعلقة بالمســؤولية المدنية المرتبطة بمثل هذه الهجمات بموجب القانون الوطني، وضبط حدود المسؤولية التي يمكن أن تساعد على إيجاد حوافز معززة للأمن السيبراني دون التسبب في آثار جانبية تحد من الوصول إلى ابتكارات واختراعات جديدة[7].

فرضــت بعض الدول التزامات على الــشركات لحماية أمن المعلومات والبيانات الشــخصية، ومن أهمها دول الاتحاد الأوروبي وفقًا لتعليــمات اللائحة رقم 679/ 2016 للبرلمان الأوروبي والمجلس الأوروبي بتاريخ 27 أبريل 2016 بشأن حماية الأشــخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات[8]؛ حيث تضمن القسم الثاني التزامات أمن البيانات الشخصية، وألزم كل من المراقب[9] والمعالج[10] التقيد بما يلي:

1. ينبغي مراعاة أحدث التطورات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها وسياقها وأغراضها، فضلًا عن مخاطر تنوع الاحتمالات وشــدتها فيما يتعلق بحقوق وحريات الأشــخاص الطبيعيين والمراقب والمعالج،

7 REGULATING CYBERSECURITY What civil liability in case of cyber-attacks? Jacques de Werra, Evelyne Studer, Project: Internet & Information Technology Law, August 2017.

8 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

9 (EU) 2016/679, controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

– المراقب: يعني الشخص الطبيعي، أو الاعتباري، أو السلطة العامة، أو الوكالة، أو أي هيئة أخرى تحدد، بمفردها، أو بالاشتراك مع آخرين، أغراض ووسائل معالجة البيانات الشخصية؛ عندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب قانون الاتحاد، أو قانون الدول الأعضاء، يجوز توفير المراقب، أو المعايير المحددة لترشيحه بموجب قانون الاتحاد، أو قانون الدول الأعضاء.

10 (EU) 2016/679, processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

– المعالج: يعني شخصًا طبيعيًا، أو اعتباريًا، أو سلطة عامة، أو وكالة، أو هيئة أخرى تعالج البيانات الشخصية نيابة عن المراقب.

ويجب أن تنفذ وفقًا لما يلي[11]:

- الاسم المستعار[12]، وتشفير البيانات الشخصية.
- القدرة على ضمان السرية المستمرة والنزاهة، وتوافر المرونة في أنظمة وخدمات المعالجة.
- القدرة على اســتعادة توافر البيانات الشــخصية والوصول إليها في الوقت المناسب في حالة وقوع حادث مادي، أو تقني.
- عملية الاختبار والتقييم بانتظام لفعالية التدابير التقنية والتنظيمية لضمان أمن المعالجة.

2. عند تقييم المســتوى المناسب لحســاب الأمان، يجب أن تؤخذ على وجه الخصوص المخاطر التي تظهر من خلال المعالجة، ولا سيما من التدمير العرضي، أو غير القانوني، أو الفقد، أو التغيير، أو الكشف غير المصرح به، أو الوصول إلى البيانات الشخصية المنقولة، أو المخزنة، أو المعالجة، أو غير ذلك.
3. يمكن استخدام الالتزام بمدونة سلوك معتمدة على النحو المشار إليه في المادة 40، أو آلية اعتماد معتمدة كما هو مشــار إليه في المادة (42) كعنصر لإثبات الامتثــال للمتطلبات المنصوص عليها في الفقرة (1) من هذه المادة.
4. يجب على وحدة التحكم والمعالج اتخاذ خطوات لضمان عدم قيام أي شــخص طبيعي يتصرف تحت سلطة جهــاز التحكم، أو المعالج الذي لديه حق الوصول إلى البيانات الشــخصية لا يقوم بمعالجتها إلا بناءً على تعليــمات من وحدة التحكم، ما لم يكن مطلوبًا منهــا القيام بذلك لذلك بموجب قانون الاتحاد، أو الدول الأعضاء.

وألزم القانون القطري رقم (13) لسنة 2016 بشــأن حماية خصوصية البيانات الشخصية[13]، كلًا من المراقب[14] والمعالج[15] بما يلي:

- اتخاذ الاحتياطات اللازمة لحماية البيانات الشــخصية من الضياع، أو التلف، أو التعديل، أو الإفشــاء، أو الوصول إليها، أو استخدامها بشكل عارض، أو غير مشروع.

11 See, (EU) 2016/679, Article 32 Security of processing, General Data Protection Regulation (GDPR).

12 (EU) 2016/679, Pseudonymisation: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

– الاسم المستعار: يعني معالجة البيانات الشخصية بطريقة لا يمكن أن تُنسب البيانات الشخصية إلى بيانات شخص طبيعي معين دون استخدام معلومات إضافية، شريطة الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل وتخضع للتقنية والتدابير التنظيمية للتأكد من أن البيانات الشخصية لا تُنسب إلى شخص طبيعي محدد، أو يمكن التعرف عليه.

13 انظر، الفصل الثالث، القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، ويتضمن التزامات المراقب والمعالج، المواد (13،14،15).

14 انظر، القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، المراقب: الشخص الطبيعي، أو المعنوي الذي يقوم منفردًا، أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها.

15 انظر، قانون حماية خصوصية البيانات الشخصية القطري، المعالج: الشخص الطبيعي، أو المعنوي الذي يقوم بمعالجة البيانات الشخصية لصالح المراقب.

- يجب أن تتناسب تلك الاحتياطات مع طبيعة وأهمية البيانات الشخصية المراد حمايتها. وعلى المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشـار إليها، أو عند حدوث أي خطر يهدد البيانات الشـخصية للأفراد بأي وجه، فور علمه بذلك.
- يجـب على المراقب إعلام الفرد والإدارة المختصة، بحـدوث أي إخلال بالاحتياطات المنصوص عليها في المادة السابقة، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية، أو بخصوصية الفرد.
- يُحظر على المراقب اتخاذ أي قرار، أو إجراء من شـأنه الحد من تدفق البيانات الشخصية عبر الحدود، إلا إذا كانت معالجة تلك البيانات مخالفة لأحكام هذا القانون، أو كان من شـأنها إلحاق ضرر جسـيم بالبيانات الشخصية، أو بخصوصية الفرد.

الفرع الثالث: المسؤولية المدنية عن الهجمات الإلكترونية

عـلى الرغم من المخاطر المتزايدة التي تشـكلها الهجـمات الإلكترونية، فإن التداعيـات القانونية، وعلى وجه التحديد، المسـؤولية المدنية الناتجة عن مثل هذه الهجمات لا تزال غير واضحة وتثير قضايا قانونية معقدة بسـبب تنوع أنظمة المسؤولية القابلة للتطبيق (التي تشمل البيانات الشخصية ولوائح مسؤولية المنتج). وبالتالي، قد يكون إجراء تعديل تشريعي بشأن هذه المسألة مبررًا في مرحلة ما في المستقبل لتنظيم الأمن السيبراني، فما المسؤولية المدنية في حالة الهجمات الإلكترونية؟

تواجه الشركات حاليًا قدرًا كبيرًا من المسـؤولية القانونية عند تقييم المخاطر السـيبرانية التي قد تنشأ، أو تتبع وقوع هجوم إلكتروني. وتقع المسـؤولية المدنية بشـكل عام في إحدى فئتين؛ إما المسـؤولية العقدية، أو المسؤولية التقصيرية.

أولًا: المسؤولية العقدية:

تكون هذه المسـؤولية في حالة وجود علاقة تعاقدية بين الأطـراف، مثل العلاقة بين منصة الإنترنت والعملاء مسـتخدمي المنصة، لذلك فإن المسـتخدم الذي تعرض لضرر نتيجة هجوم إلكتروني على موقع المنصة يمكن أن يرفع دعـوى قضائية ضدها والمطالبة بالتعويـض عن الضرر، وذلك للإخلال بالالتـزام القانوني الواردة ضمن سياسة الخصوصية للمنصة. حدث هذا على سـبيل المثال في الولايات المتحدة؛ حيث تعرض موقع (LinkedIn) لدعوى قضائية من قبل العملاء لتضليلهم بشـأن سياسـات حماية البيانات الشخصية للعملاء، وكان الادعاء أنها قدمت معايير غير كافية في الأمن السـيبراني؛ حيـث تمّ رفع الدعوى بعد تعرض موقـع (LinkedIn) لاختراق بيانات المستخدمين أدى إلى نشر ملايين من رسـائل البريد الإلكتروني وكلمات المرور عبر شبكة الإنترنت؛ حيث قضت محكمة فيدرالية في نيويورك (في 18أغسـطس 2014) بفرض تسـوية بقيمـة 1.25 مليون دولار على موقع (LinkedIn) في قضية اختراق البيانات الشخصية للمستخدمين[16].

16 LinkedIn Strikes $1.25M Settlement In Data Breach Action, Retrieved on 14/3/2021, from https://www.law360.com/articles/568135/linkedin-strikes-1-25m-settlement-in-data-breach-actio

الشروط العامة للمسؤولية العقدية:

1. **الإخـــلال بالعقد، الخطأ العقدي**، (مثل الإخلال بواجب تقديم المســتوى الموعود به للأمن الســيبراني)، وتضمن المرســوم بقانون رقم (16) لســنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية القطري بأنه يجب على مقدم الخدمة الإفصاح للعملاء عن الأغراض التي من أجلها، يتم جمع المعلومات الشخصية عــن العميل، وذلك عنــد، أو قبل جمع هذه المعلومات، ولا يجوز له أن يجمع، أو يســتخدم، أو يحتفظ، أو يفصح عن المعلومات الشــخصية للعميل، لأغراض غير مصرح، أو مسموح بها، إلا إذا كان مطلوبًا منه، أو مصرحًا له بموجب القانون. ويتحمل مقدم الخدمة المسؤولية بالحفاظ على السرية وضمان عدم تعرض أي سجلات تحتوي على المعلومات الشخصية للعميل، أو أي سجلات للاتصالات الإلكترونية للعميل، تكون في عهدة مقدم الخدمة، أو تحت ســيطرته، أو مع وكلائه. ويجب عــلى مقدم الخدمة اتخاذ الخطوات المعقولة والضرورية، لضمان أن المعلومات الشخصية للعميل، والسجلات ذات الصلة، محمية بطريقة أمنية تناسب أهميتها ومنع تعرضها إلى أي اختراق[17].
2. **الضرر الفعلي**، والضرر يشــمل نوعي الضرر المادي والمعنوي وهذا مــا تضمنته المادة 264 (القانون المدني القطري رقم «22» لسنة 2004) بأن يشمل التعويض الضرر الأدبي إضافة إلى الضرر المادي، ومثاله الضرر الذي يصيب الســمعة التجارية للشركات التي تتعرض للهجــمات الإلكترونية، ويحق الجهات الحكومية المختصة في دولة قطر، وفقًا للإجراءات القانونية المقررة بالمرســوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية، في أن تفرض عــلى مقدم خدمة التجارة الإلكترونية، أو خدمات الاستضافة اتخاذ إجراءات معينة بإخطارها عن أي أنشطة، أو معلومات غير قانونية، مع إلزامه بتزويد تلك الجهات بأي معلومات لتحديد هوية المستخدم المتعامل في الأنشطة والمعلومات غير القانونية. ويكون ذلك في الحالتين التاليتين[18]:

أ. ارتكب خارج قطر فعلًا، يجعله فاعلًا، أو شريكًا، في جريمة وقعت كلها، أو بعضها داخل قطر.

ب. ارتكــب داخل قطر فعلًا، يجعله فاعلًا، أو شريكًا، في جريمة وقعت كلها، أو بعضها خارج قطر، متى كان معاقبًا عليها بمقتضى هذا القانون وقانون البلد الذي وقعت فيه الجريمة.

العلاقة الســببية بين الخطأ والضرر، لقيام المســؤولية الإلكترونية لا بد من إثبــات العلاقة بين الخطأ والضرر، وباعتبار أن المخاطر الســيبرانية هي حدث لاحق يسبب الخســارة ويترتب عليه نتائج ضارة فإن مجرد وقوع الخطر المؤمن عليه فإن الأضرار الناتجة عنه يتحقق فيها رابطة السببية ولا تحتاج إثبات من قبل المضرور.

حالــة الخطأ (المفترض). ومــن الأمثلة على الخطأ المفــترض في حالة التقصير من قبل الــشركات التجارية في عدم الامتثال مع المتطلبات التنظيمية والقانونية التي وعدت بها العملاء، أو المســتخدمين وفقًا لسياســات الحماية الإلكترونية التي تعتمدها هذه الشركات.

وتثير المســؤولية العقدية العديــد من القضايا المتعلقة بإثبــات الخطأ الذي عادة ما يرتبــط بعدم وفاء الشركة

17 انظر، المادة 59، المرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية القطري.

18 المادتان (50، 73)، قانون المعاملات والتجارة الإلكترونية القطري.

بالتزاماتها تجاه حماية بيانات العملاء، أو المستخدمين من توفير برامج الحماية التقنية؛ حيث أدى ذلك إلى عملية الاختراق للبيانات، وعلى الرغم من ذلك فقد يتم استبعاد المسؤولية عن الشركة في حالة تقديمها خدمة، أو بيعها منتجًا للعملاء فيما لو استطاعت الشركة أن تثبت عدم ارتكاب أي خطأ فيما يتعلق بالهجوم الإلكتروني، أو أنها قد تضمن العقد شروطًا لإخلاء المسؤولية كشروط لتقديم خدمتهم، أو بيع منتجاتهم مثل (البرمجيات)، وأيضًا يمكن استبعاد المسؤولية في حالة الخطأ الصادر من العميل، أو المستخدم، كما في حالة عدم المحافظة على اسم المستخدم وكلمة المرور، أو تعرضه لسرقة بياناته، وكذلك فيما يتعلق بصعوبة إثبات علاقة السببية بين الخطأ والضرر كما في حالة وجود السبب الأجنبي كالقوة القاهرة، أو الحادث المفاجئ، ومثاله الأضرار التي تنتج عن تعطل النظام لأسباب تتعلق بمزود خدمة الإنترنت، أو خطأ المضرور كما في حالة وجود فيروسات في جهاز المستخدم تسببت بالإضرار بالنظام، وأدت إلى توقفه عن العمل، أو بسبب فعل، أو خطأ الغير، ومثالها في قضايا طلب دفع الفدية (Pay Ransom)، والابتزاز الإلكتروني (Cyber Extortion)؛ حيث قام كثير من المجرمين الإلكترونيين؛ الهاكرز (Hackers)، باختراق أجهزة أشخاص ومنظمات وشركات وحصلوا من خلال تلك الأجهزة على معلومات مهمة، أو وثائق سرية، أو وسائط متعددة ثم قاموا بنسخ تلك البيانات واستخدموها في ابتزاز أصحابها بطلب مبالغ مادية كبيرة حتى يقوموا بإعادة تلك المعلومات لهم، أو حتى يقوموا بعدم نشرها على الإنترنت[19].

يعرف القانون المدني القطري التأمين بأنه عقد يلتزم المؤمن بمقتضاه أن يؤدي للمؤمن له، أو إلى المستفيد الذي اشترط التأمين لصالحه مبلغًا من المال، أو إيرادًا مرتبًا، أو أي عوض مالي آخر، في حالة وقوع الحادث، أو تحقق الخطر المبين بالعقد، وذلك في نظير قسط، أو أية دفعة مالية أخرى يؤديها المؤمن له للمؤمن.[20] ويجوز وفقًا لأحكام القانون المدني القطري الاتفاق بين المتعاقدين على إعفاء المدين من أية مسؤولية تترتب على عدم تنفيذ التزامه التعاقدي، أو على التأخير في تنفيذه، إلا ما ينشأ عن غشه، أو خطئه الجسيم. ويجوز أيضًا الاتفاق بين الطرفين على إعفاء المدين من المسؤولية عن الغش، أو الخطأ الجسيم الذي يقع من أشخاص يستخدمهم في تنفيذ التزامه. ويقع باطلًا كل اتفاق يبرم قبل قيام المسؤولية عن العمل غير المشروع، ويكون من شأنه أن يعفي منها كليًا، أو جزئيًا[21]. ونستنتج من ذلك أن المشرع القطري وضع قيدين؛ الأول يتعلق بحالة وجود الغش، أو الخطأ الجسيم؛ فإن شرط الإعفاء من المسؤولية، أو التخفيف منها يقع باطلًا. والقيد الثاني يتمثل في عدم جواز الاتفاق على الإعفاء من المسؤولية، أو التخفيف منها عندما يتعلق الأمر بأضرار تصيب الإنسان في كيانه المادي، أو الأدبي، وهذا القيد الأخير لم ينص عليه القانون القطري ولكنه محل إجماع في الفقه القانوني[22].

أما القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، فإنه يعطي الحق لكل فرد في حماية خصوصية بياناته الشخصية، ولا يجيز معالجة تلك البيانات إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، وفقًا لأحكام هذا القانون[23].

19 نشرة الاتحاد المصري للتأمين، عدد أسبوعي رقم 67، سنة 2019، على الرابط التالي:
https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324 (accessed 14/3/2021).

20 انظر، المادة 771، القانون المدني القطري رقم (22) لسنة 2004.

21 المادة 259، القانون المدني القطري.

22 جابر محجوب علي، **النظرية العامة للالتزام، مصادر الالتزام في القانون القطري**، ج 1، جامعة قطر، 2016، ص 399–401.

23 انظر، المادة 3، القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.

ثانيًا: المسؤولية التقصيرية:

نظم المشرع القطري أحكام المسؤولية التقصيرية في القانون المدني، وتقوم المسؤولية التقصيرية أما على أساس الخطأ واجب الإثبات بالنسبة إلى المسؤولية عن الأعمال الشخصية، أو على أساس الخطأ المفترض، أو فكرة الضمان بالنسبة إلى المسؤولية عن عمل الغير، ولا تترتب المسؤولية بمجرد توافر الخطأ ولكن يلزم أيضًا أن يؤدي هذا الخطأ إلى ترتب الضرر، ويجب لقيام المسؤولية التقصيرية أن يكون الخطأ هو السبب الذي أدى إلى حدوث الضرر، وبالتالي يلزم قيام علاقة السببية بين الخطأ والضرر.

وحسب (المادة 22) فإن قانون حماية خصوصية البيانات الشخصية القطري نظم عملية التواصل الإلكتروني بين الشركات التجارية وعملائها بحيث يُحظر إرسال أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة. ويجب أن يتضمن الاتصال الإلكتروني هوية مُنشئه، وما يفيد بأنه مرسل لأغراض التسويق المباشر، كما يجب أن يتضمن عنوانًا صحيحًا يسهل الوصول إليه، ويستطيع الفرد من خلاله أن يرسل طلبًا إلى المنشئ بإيقاف تلك الاتصالات، أو الرجوع في موافقته على إرسالها في أي وقت ويبلغ بذلك الشركة، أو من خلال حظر الإرسال للبريد الإلكتروني المرسل من هذه الشركة[24]. ويستنتج من ذلك تقوم المسؤولية التقصيرية على الشركات التجارية التي تقوم بالإعلان عن منتجاتها عبر الوسائل إلكترونية بدون رضاء، أو موافقة العملاء، أو في الحالات التي يعلن فيها العميل عدم رغبته في استلام تلك الإعلانات. ويترتب على مخالفة أحكام المادة 22 من القانون؛ حيث يعاقب المخالف بالغرامة التي لا تزيد على (1.000.000) مليون ريال، مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر[25]. أما وفقًا لأحكام المرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية فإنه يُعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (300.000 ريال) ثلاثمائة ألف ريال، أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر، كل شخص ارتكب عمدًا، الوصول غير المشروع إلى أي نظام معلومات، أو رسالة بيانات، أو خدمة تجارة إلكترونية، أو معاملة ذات صلة، بما في ذلك تجاوز الإجراءات التقنية الأمنية، وذلك بقصد الحصول على المعلومات، أو استخدام آخر غير مشروع لنظام المعلومات، أو رسالة البيانات، أو خدمة التجارة الإلكترونية، أو المعاملة ذات الصلة[26].

المبحث الثاني: تغطية التأمين للأضرار الناتجة عن الهجمات الإلكترونية

تاريخيًا فقد ورد في أدبيات سوق صناعة التأمين من خلال المراقبين للتأمين السيبراني أن ستيفن هاس هو أول من ساعد في كتابة أول بوليصة تأمين على الإنترنت في ربيع سنة 1997، وإن أول بوليصة تأمين إلكتروني كانت موجهة نحو تكنولوجيا المعلومات والشركات المسؤولة عن إدارة الشبكات والأنظمة المستخدمة من قبل الشركات الأخرى والمستهلكين. وفي منتصف العقد الأول من القرن الحادي والعشرين، بدأت شركات التأمين على الإنترنت في تقديم التغطية المكتوبة لنفقات الطرف الأول ومن ثم توسعت عروض التأمين لأي شركة تستخدم التكنولوجيا،

24 انظر، المادة 22، القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.

25 (المادة 23) من القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.

26 انظر، المادة (67)، المرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية القطري.

وتطور التأمين السـيبراني في تقديم النوع الثاني من التغطية المكتوبة للطرف الثالث، وتُعد مخاطر الإنترنت الصامتة [27] نوعًا ثالثًا من تغطية التأمين الإلكتروني وهي ليسـت بوليصة تأمين إلكتروني ولكن المصطلح يشـير إلى الخسائر الإلكترونية المحتملة الناجمة عن الممتلكات التقليدية غير المصممة خصيصًا لتغطية المخاطر الإلكترونية[28].

الفرع الأول: أهمية التأمين الإلكتروني

يؤدي التأمين السيبراني دورًا مهمًا في التخفيف من مخاطر الأعمال الناجمة عن هجوم إلكتروني، ويمكن لبوليصة التأمين الجديدة المصممة جيـدًا حماية حاملي الوثيقة من الشركات التجارية مـن عشرات الملايين من الدولارات نتيجة التعرض للمخاطر السـيبرانية الناتجة عن اختراق البيانات. لقد غيّر فيروس كورونا كل شيء حولنا بين ليلةٍ وضحاها؛ حيث أرسـلت الشركات القوى العاملة بأكملها إلى المنزل للعمل، وتحولت معظم الشركات من العمل المادي إلى الوجود الافتراضي والاتجاه نحو التجارة الإلكترونية.

القانون المدني القطري لم يورد تعريفًا خاصًا لعقد التأمين عن المسؤولية إلا أنه عرّف التأمين بصفة عامة في المادة 771 منه بأن: «التأمين عقد يلتزم المؤمن بمقتضاه أن يؤدي للمؤمن له، أو إلى المستفيد الذي اشترط التأمين لصالحه مبلغًا من المال، أو إيرادًا مرتبًا، أو أي عوض مالي آخر، في حالة وقوع الحادث، أو تحقق الخطر المبين بالعقد، وذلك في نظير قسط، أو أية دفعة مالية أخرى يؤديها المؤمن له للمؤمن».

وبشكلٍ عام، يجب أن تساعد منتجات التأمين الجديدة وسوق التأمين الإلكتروني الأكثر تطورًا في:

- رفع مستوى الوعي بالمخاطر والخسائر السيبرانية.
- مشـاركة أفضل ممارسات إدارة المخاطر الإلكترونية بين أصحاب المصلحة، بما في ذلك الصناعة وشركات التأمين والمنظمون.
- تشجيع استخدام المعلومات النوعية في حساب أقساط التأمين الفعال على أساس المخاطر.
- تسهيل الاستجابات والتعافي من الحوادث الإلكترونية من قبل حاملي وثائق التأمين.

إن العديد من السياسـات السيبرانية قد لا تغطي بشـكل كاف المخاطر الناشئة المحيطة ببيئات العمل البعيدة، وينبغـي النظر في التعديلات المحتملـة للحصول على حماية إضافية في عـصر (COVID-19). وعلى الرغم من أن سياسـات التأمين التقليدية قد توفر خيـارًا لتغطية بعض المجالات المحددة المتعلقة بالمخاطر السـيبرانية، إلا أنها ليسـت مصممة لتغطية جميع التكاليف والخسـائر المحتملة بالكامل. وتعتمد شركات التأمين مجموعة متنوعة من خيارات التغطية للأضرار الناتجة عن الهجمات الإلكترونية التي يجب مراعاتها عند شراء التأمين الإلكتروني:

- – تغطيـة الضرر للطـرف الأول: هو الضرر الذي يلحق بالمؤسسـة، أو المنظمـة، أو الشركة التي تمتلك نظـام تكنولوجيا المعلومات، وتتضمن التغطية الحماية من الخسـائر التي تتحملها الشركة مباشرة ردًا على

27 Baker, Tom, “Back to the Future of Cyber Insurance” (2019). Faculty Scholarship at Penn Law. 2184. Retrieved on 14/3/2021, from https://scholarship.law.upenn.edu/faculty_scholarship/2184

28 The Federal Reserve Bank of Chicago, Essays on Issues, 2019 Number 426. Retrieved on 14/3/2021, from https://doi.org/10.21033/cfl-2019-426

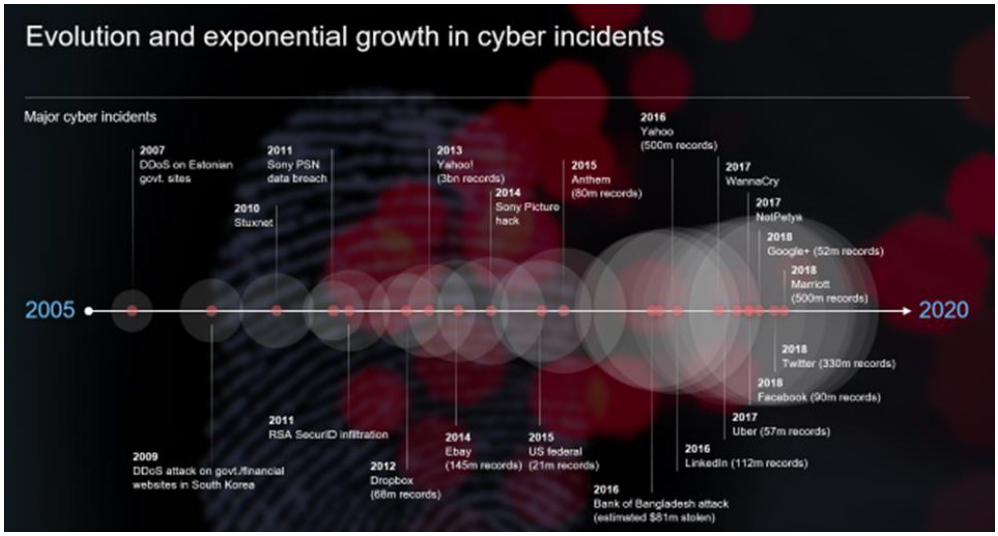
حادث إلكتروني، وعادة ما تشمل السرقة والاحتيال والتحقيق الجنائي، انقطاع الأعمال والابتزاز وفقدان واستعادة بيانات الكمبيوتر.

- تغطيــة الضرر للطــرف الثالث: وهو الضرر الــذي يلحق بالشركات الأخرى التــي يصيبها ضرر من المخاطــر والهجمات الإلكترونية، وتتضمن التغطية الحماية من الخســائر، أو الأضرار التي تقع على أطراف ثالثة في الاســتجابة لحادث إلكتروني، وعادة ما يتضمن التقــاضي، وتكاليف الإخطار، وإدارة الأزمات، ومراقبة الائتمان، والتأمين السيبراني مكتوب ومُسعّر ليكون مناسبًا للشركات والعملاء الأفراد. وفي حالة أنظمة المعلومات المترابطة لأطــراف ثالثة متعددة، من المحتمل أن تتجاوز قيمــة أصول الأطراف الثالثة قيمــة الطرف الأول، وبالتالي قد يفوق ضرر الطرف الثالث ضرر الطرف الأول، ومثال ذلك في الشركات الصغيرة والمتوسطة التي لديها أصول محدودة نسبيًا ولكنها قد تسبب ضرر كبير للطرف الثالث[29].

الفرع الثاني: التهديدات السيبرانية

تتعدد التهديدات الســيبرانية المحتملة في ثلاثــة أنواع هي: الجرائم الإلكترونية، والأخطاء البشرية، وفشــل النظــام. وبمجرد وقوع الحادث الإلكــتروني يكون هناك احتمالية وقوع خســائر، أو أضرار، ومع ذلك يمكن أن تقع الهجمات الإلكترونية ولا تحدث خســارة، أو ضرر كما في حالة الأنظمة المرنة التي تقوم بنسخ احتياطي تلقائي للملفات عند تعرضها للتهديدات السيبرانية، أو تأمين الحماية عن طريق الجدران النارية المناسبة على سبيل المثال في حالة التصدي لهجمات الفيروسات.

ويوضح الشــكل التالي الاتجاه التصاعدي وزيادة وتيرة الهجمات الإلكترونية التي تعرضت لها كبرى الشركات العالمية منذ سنة 2005 وحتى سنة 2020 تزامنًا مع التطورات التكنولوجية المتسارعة خلال تلك الفترة.



الشكل (2): التطور والنمو المتسارع للحوادث السيبرانية[30].

29 Bernold Nieuwesteeg, Louis Visscher & Bob de Waard, The Law & Economics of Cyber Insurance Contracts: A Case Study, ediss.sub.hamburg, 2018. Retrieved on 14/3/2021, from https://ediss.sub.uni-hamburg.de/handle/ediss/8189

30 The number of cyber attacks continues to rise - as do the resulting losses. In particular targeted cyber attacks of different =

الفرع الثالث: سياسات التأمين السيبرانية

تتضمن سياسات التأمين على الإنترنت بعض الاستثناءات، أو فرض حدود، أو إضافة بنود لحماية شركة التأمين من المخاطر العالية (على سبيل المثال، مزود الحوسبة، والأجهزة غير المشفرة التي تحتوي على البيانات الشخصية وغيرها، وأعطال برامج الكمبيوتر بسبب الأخطاء في البرمجة). يتضمن أيضًا تعويض الانقطاع عن العمل ويشمل خسارة الانقطاع التي يتحملها المؤمن له في فترة استرداد الأعمال وفترة الانتظار، وتعويض تهديد الإنترنت من تكاليف الاستجابة للابتزاز؛ حيث تقوم شركة التأمين بالسداد للمؤمن له، أو أي شركة تابعة له عن نفقات الابتزاز ومدفوعات الابتزاز التي تكبدها المؤمن له، أو أي شركة تابعة له مباشرة التي نتجت عن تهديد الابتزاز السيبراني، تكاليف الاستجابة للطوارئ والخبراء[31].

ففي سنة 2018 فقط، قُدِرَ الضرر الاقتصادي الناجم عن الهجمات الإلكترونية بنحو 600 مليار دولار أمريكي. أما في عام 2017، فقد تأثرت معظم الشركات في جميع أنحاء العالم نتيجة للهجمات الناتجة عن البرامج الضارة مثل (NotPetya WannaCry) في توقف الأعمال التجارية على نطاق واسع وتوقف الإنتاج في جميع أنحاء العالم، ووفقًا لتقديرات معهد أبحاث السوق (Cybersecurity Ventures)، تقع الشركات في جميع أنحاء العالم ضحية لمثل هذه الهجمات كل 14 ثانية في المتوسط في عام 2019.

مع بداية أزمة جائحة (COVID-19) اضطرت الشركات التجارية إلى توسيع قدراتها في مجال تكنولوجيا المعلومات والاتصالات والسماح للموظفين بالعمل عن بُعد من المنزل. وأدت هذه الظروف الاستثنائية إلى زيادة كبيرة في الهجمات الإلكترونية في الأشهر القليلة الماضية، ومن المرجح أن يستمر هذا الاتجاه طوال مدة الوباء. ويلعب التأمين الإلكتروني دورًا مهمًا في التخفيف من مخاطر الأعمال الناجمة عن هجوم إلكتروني، ويمكن لسياسة التغطية السيبرانية المصممة جيدًا حماية حامل وثيقة التأمين الإلكتروني الناتج عن اختراق البيانات، بيد أن العديد من السياسات السيبرانية قد لا تغطي بشكل كافٍ المخاطر الناشئة الهجمات الإلكترونية.

معظم السياسات السيبرانية تحتوي على التغطيات الأساسية التالية:

- مصاريف اختراق البيانات، تغطي تكاليف الاستجابة القياسية للانتهاك للاستعانة بالمحامين وإخطار العملاء الذين تم اختراق معلوماتهم الشخصية.
- الخصوصية ومسؤولية أمان الشبكة، التي تغطي الدفاع وتسوية الدعاوى الجماعية ومطالبات الطرف الثالث.

= types will increase. While phishing and malware via email remain the most common types of attack, ransomware that targets user devices and the cloud can threaten infrastructure, resulting in significant insurance losses. According to estimates from market research institute Cybersecurity Ventures, companies around the world fall victim to such attacks every 14 seconds on average in 2019. See, Munich - Re worldwide, Retrieved on 14/3/2021, from https://www.munichre.com/en/risks/cyber-risks.html

31 Kjartan Palsson, Steinn Gudmundsson, Sachin Shetty, Analysis of the impact of cyber events for cyber insurance, Received: 16 September 2019 / Accepted: 5 May 2020 / Published online: 4 June 2020 © The Geneva Association 2020.

- المطالبات التنظيمية، التي تغطي الرسوم القانونية للرد على التحقيقات الحكومية، وكذلك الغرامات المدنية والعقوبات والتسويات.
- انقطاع الشبكة، وتغطية الأرباح المفقودة والنفقات الإضافية الناتجة عن إغلاق الشبكة.

تقــدم شركات التأمين عبر الإنترنت أيضًا مجموعة من التغطيات الاختيارية لمعالجة مخاطر محددة، مثل هجمات برامج الفدية واســتعادة البيانات ومســؤولية بطاقات الدفع، ويختلف نطاق التغطية اختلافًــا كبيرًا وفقًا للأنواع المختلفة من سياسات التغطية السيبرانية، وتحدد هذه السياسات الاختلاف في صياغة عقد التأمين الإلكتروني عند إبرام العقد، وتحدد العناصر التي تتضمنها وثيقة الخســائر التــي يقوم المؤمن له بتحويلها إلى شركة التأمين في حالة تحقق المخاطر السيبرانية[32].

المبحث الثاني: نحو عقد نموذجي للتأمين الإلكتروني

قد تظهر المخاطر الســيبرانية والتحديات مع اعتماد بروتوكولات التباعد الاجتماعــي والبقاء في المنزل لتقليل الآثار الســلبية لجائحة (COVID-19)، ومع مطالبة الموظفين والطــلاب والمرضى وغيرهم بالعمل عن بُعد في ظل الظروف الصعبة، وقد تمّ تطوير البنية التحتية للتعامل مع المزيد من الأنشــطة الإلكترونية، وكان من الواجب على المؤسسات التفكير في كيفية تأثر ملفات تعريف المخاطر الإلكترونية الخاصة بها.

التحــدي الأكبر هو الانتقال مــن الوجود المادي إلى الوجــود الافتراضي، بمجرد أن تدرك المؤسســات هذا التحدي، يجب عليها اتخاذ الإجراءات المناسبة للتخفيف من المخاطر المحتملة – على سبيل المثال، من خلال تعزيز وعي الموظفين والمستخدمين لديهم بالتهديدات السيبرانية، وتعزيز ودعم أنظمة التكنولوجيا، ومراجعة التغطيات التأمينية مع مراعاة الخسائر المحتملة في ظل الإنترنت، وسائل الاتصال، وسياسات الأخطاء التقنية. ويزيد العمل عن بُعد أيضًا من مخاطر سياســات وإجراءات الخصوصية لتســهيل العمل من المنزل، ويقوم الموظفين عادة بإزالة الملفات المطبوعة من مكان العمل، أو نقل معلومات التعريف الشــخصية إلى أجهزة تخزين، أو أجهزة شــخصية غير آمنة، أو غير مشــفرة مما قــد يؤدي إلى تعريض المعلومات للاختراق من قبل مســتخدمين غير مصرح لهم، أو الاستخدام غير الصحيح والتخلص منها.

تتضمن معظم سياســات التأمين الإلكتروني مجموعة واســعة من التغطيات التي تتعلق بالظروف الاستثنائية للجائحة، وتشمل هذه المسؤولية الأمنية للشبكة، ومسؤولية الخصوصية، والاستجابة الأمنية، واستعادة البيانات وتكاليف إلحاق الضرر بالسمعة، وانقطاع أعمال الشــبكة، وفشل النظام، وانقطاع الأعمال الطارئ وغيرها. ومع ذلك، ففي بعض الحالات، لا تشمل التغطية السيبرانية لسياسات التأمين الإلكتروني عادةً ما يلي[33]:

32 COVID-19 Crisis May Warrant Changes to Your Cyber Insurance Coverage, JULY 2020, article. Retrieved on 14/3/2021, from https://www.jonesday.com/en/insights/2020/07/covid19-crisis-may-warrant-changes-to-your-cyber-insurance-coverage

33 Justin Keevy, COVID-19: Implications for Cyber Coverage. Retrieved on 14/3/2021, from https://www.marsh.com/za/insights/research-briefings/covid-19-implications-cyber-media-tech-errors-omissions.html

- **اســتثناءات البنية التحتية**: عادةً ما تســتبعد السياسات تغطية فشــل الطاقة، أو المرافق، أو الميكانيكية، أو الاتصالات الســلكية واللاســلكية (بما في ذلك الإنترنت)، أو الخدمات التي لا تخضع للتحكم التشغيلي المباشر للمؤمن له.
- **قيــود تغطية الإغلاق الطوعي**: قد تنطبق التغطية فقط على عمليــات الإغلاق الطوعي المرتبطة بالظروف الاستثنائية لمنع انتشــار البرامج الضارة، أو الحد من الضرر، ولا تنطبق على عمليات الإغلاق التي تهدف إلى تحسين الوصول إلى الشبكة، أو وظائفها.
- **القيود في تعريفات نظام الكمبيوتر، أو الشبكة** يجب على حاملي الوثائق مراجعة التعريفات الرئيسية وما إذا كانت تؤثر على تغطية الأنظمة المملوكة، أو المشغلة، أو المؤجرة وتلك التي تديرها أطراف ثالثة.
- **القيود في تعريفات فشــل النظام**. قد تتطلب بعض السياســات وجود «خطأ» بشري، أو برمجي، أو إثبات الاختبار، أو التصحيحات للنظام، أو إثبات استخدام النظام قبل الفشل من أجل بدء التغطية.

مع نضوج ســوق الأمن الســيبراني، قامت شركات التأمين بتنقيح سياسات التأمين الإلكتروني والإعلان عن الأسعار المختلفة لأقســاط التأمين التي تتناسب مع التغطية للمخاطر الســيبرانية. بيد أنه، مازالت هناك جوانب أساســية للتأمين الإلكتروني تجعل من الصعب على شركات التأمين كتابة وتســعير السياسات التي تغطي مجموعة واسعة من المخاطر السيبرانية.

ســنتناول في هذا المبحث مــدى إمكانية الوصول إلى عقــد إلكتروني نموذجي موحد على المســتوى الوطني والدولي، ونناقش فيه أهم التحديات القانونية التي تواجه ســوق التأمين الإلكتروني ونســتشرق المستقبل للمنتج الجديد للتأمين في المطلبين التاليين:

المطلب الأول: التحديات القانونية لسياسات التغطية السيبرانية

يرتبط التأمين الإلكتروني بالأمن الســيبراني بعلاقة وثيقة، ونظرًا لطبيعتها العالمية، فإن كتابة سياسات التغطية الســيبرانية وتحديد الضوابط التي تحكمها تتطلب العمل على مستويات مختلفة (الدولية والوطنية والمحلية)، ويجب أن تتم بطريقة منســقة بين شركات التأمين والجهات الحكومية المختصة في الدولة ووضع الحلول المناســبة لوثيقة التأمين الإلكتروني ضد المخاطر الســيبرانية، تقوم شركات التأمين بالتعويض عــن الأضرار الناتجة عن الهجمات الإلكترونية، ويقاس الضرر على درجتين:

- **الضرر مــن الدرجة الأولى**: وهو التكاليف المباشرة التي تتكبدها الــشركات عند وقوع حادث إلكتروني، ومن الأمثلة: تُعد من هذه الأضرار عندما تفقد الشركات البيانات الشخصية للعملاء، أو البيانات المتعلقة بالشركة من خلال القرصنة، أو تعطل الأجهزة والبرامج، أو أخطاء الموظفين.
- **الضرر من الدرجة الثانية**: وهو التأثير الســلبي للحادث الإلكتروني ويتضح بمجرد أن يصبح عامًا، وعلى سبيل المثال الإضرار بالسمعة، الإخطار بالخروقات لسلطة العامة المختصة، والضرر الثاني هو أكثر صعوبة

في القياس من الضرر الأول وبالتالي قد يصعب نقله إلى طرف ثالث مثل شركة التأمين[34].

أهـــم التحديات القانونية التي تعترض شركات التأمين عند كتابة سياســـات التغطية الســـيبرانية لعقد التأمين الإلكتروني التالي[35]:

أولًا: تحديد أسعار واقساط التأمين الإلكتروني:

قد تتعرض شركات التأمين لخســـارة محدودة فقط عند تحديد أسعار التأمين الإلكتروني والأقساط المطلوبة من المؤمن له، وهذا يؤدي إلى مخاطر تتعلق بحدود خســـارة التغطية التأمينية، وعلى ســـبيل المثال عندما تضع شركات التأمين وثيقة التأمين على الســـيارات وتحدد فيها أقســـاط التأمين، يمكنهم الاعتماد على تاريخ طويل من الحوادث والأضرار لتصميـــم احتمالية تعرض ســـائق بمجموعة معينة من الخصائص لحادث ثم ضبطه في أقســـاط لتغطية هذه الخســـارة المتوقعة، أما في وثيقة التأمين الإلكتروني؛ حيث تعمل شركات التأمين على الإنترنت في سوق سريع التطور، ولا بد من الاعتماد على عدد من العوامل غير المباشرة لمحاولة تسعير السياسات بشكل مناسب، بما في ذلك تقديرات السوق من تكلفة الهجمات السيبرانية، واستقراء استبيانات يقوم بها مستشاري التأمين المختصين لتحديد مدى الأخطار المؤمن عليها، ولذلك تفتقر شركات التأمين للخبرة المطلوبة في تصميم المنتج الجديد.

وتقتصر الحماية من المسؤولية الإلكترونية الحالية في النماذج الثلاثة التالية:

- تغطية مكتوبة وموثقة من الطرف الأول،
- تغطية مكتوبة وموثقة من أطراف ثالثة،
- تغطية إلكترونية ضمنية صامتة.

ثانيًـــا: تقييم خطر الاختراق: تتطور الهجمات الإلكترونية باســـتمرار؛ حيث يطور المتســـللون الخاصون طرق التسلل إلى الشبكات، ومع التطور السريع لقدرات واستراتيجيات القرصنة السيبرانية يصعب على شركات التأمين، التي تعتمد على العملاء الذين لديهم ملفات مخاطر منخفضة نســـبيًا، التقييم الحقيقي لخطر اختراق محتمل لعملاء محددين. ومثال ذلك في الولايات المتحدة الأمريكية، أدى التطور المتزايد للقراصنة إلى ازدياد الهجمات الإلكترونية وتكاليفها في السنوات الأخيرة: ذكرت التقارير إلى ارتفاع تكلفة متوسط الهجوم الإلكتروني 29٪ من 21.2 مليون دولار في 2017 إلى 27.4 مليون دولار في 2018، ومع ذلك ظل سوق التأمين الإلكتروني مربحًا لشركات التأمين.

ثالثًا: قابلية الهجـــمات الإلكترونية للتطوير: وذلك بدرجة كبيرة؛ حيـــث يمكن أن تضرب آلاف الشركات في وقت واحد وينتج عنها أضرار كبيرة لحاملي وثيقة التأمين الإلكتروني، وتتســـبب في خسائر كبيرة مترابطة لشركات التأمين، ويتعين على شركة التأمين بعد ذلك دفع المطالبات لجميع حاملي وثائقها دفعة واحدة.

رابعًا: احتمالية الفشل المتتالي الذي يسببه هجوم الإنترنت، أحد الأمثلة الشائعة على الفشل المتتالي هو الهجوم على شبكة مزودي الخدمات؛ حيث يؤدي إلى تدمير جزء من البنية التحتية الحيوية وحدوث أعطال في باقي أجزاء الشبكة،

34 Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, The Law and Economics of Cyber Insurance Contracts: A Case Study, European Review of Private Law, Volume 26, Issue 3 (2018), pp (371 - 420).

35 Shauhin A. Talesh, SYMPOSIUM: INSURANCE COMPANIES AS CORPORATE REGULATORS: THE GOOD, THE BAD, AND THE UGLY, 66 DePaul L. Rev. 463, Winter, 2017.

ومن ذلك أيضًا تنتشر الهجمات السيبرانية التي تستخدم برامج ضارة ذاتية التكاثر عبر شبكة من أجهزة الكمبيوتر.

خامسًا: حالة عدم اليقين القانوني لعقود التأمين الإلكتروني؛ حيث تتفاعل شركات التأمين مع حالة عدم اليقين هذه عن طريق زيادة أقساطها لتعكس بذلك «غموض شركة التأمين»، ينتج الغموض على الأرجح بسبب افتقار المؤمن للبيانات والمعلومات المحدثة باستمرار من أجل تقديم وثائق تأمين ميسورة التكلفة، لكن هذه البيانات لن تكون متاحة طالما لا تستطيع شركات التأمين تقديم بواليص تأمين منخفضة التكلفة، وتكون المنافسة غير كافية بسبب أن عدد قليل فقط من شركات التأمين تقدم التأمين الإلكتروني.

سادسًا: الخطر المعنوي: يُسمى أيضًا بالمخاطر الأخلاقية وتبدو هذه المخاطر بعد إبرام عقد التأمين الإلكتروني ضد المخاطر السيبرانية؛ حيث يبدأ المؤمن له بعد العقد ببذل عناية أقل لحماية أمن المعلومات والبيانات لأنه لن يتحمل خسائر الضرر عند التعرض للهجمات الإلكترونية، ومن المتوقع أيضًا أن يقوم المؤمن له بزيادة الخسائر من أجل تأمين تعويضات أكبر بموجب عقد التأمين الإلكتروني، وهذا السلوك يُعد في الأساس احتيالًا.

ويتعذر على شركة التأمين ومن المكلف للغاية أن تقوم بمراقبة سلوك المؤمن له تمامًا، وهذا يؤثر على الخسائر المتوقعة لشركات التأمين، لذلك تقوم برفع قسط التأمين الإلكتروني. ويمكن لشركات التأمين التقليل من آثار الخطر المعنوي لعقد التأمين الإلكتروني عن طريق تزويد المؤمن له بالمعلومات الكافية حول الأمن السيبراني، وقد يُطلب من المؤمن له اتخاذ تدابير وإجراءات حماية محددة، وإذا لم يلتزم بها سيتم خفض التعويض، أو رفضه بسبب عدم تنفيذ متطلبات الحماية، أو عدم اتخاذها بشكل كافٍ[36].

المطلب الثاني: مستقبل التأمين الإلكتروني

كل حادث إلكتروني تمَّ الإبلاغ عنه لاختراق البيانات، أو فشل النظام سيؤدي حتمًا إلى خسارة مالية، أو الإضرار بالسمعة التجارية للشركات، وباعتبار أن عقود التأمين التقليدية لا تتضمن تغطية المخاطر السيبرانية في الوقت الحالي، فإن الحاجة تبدو ملحة للتحول نحو عقد التأمين الإلكتروني، وقد تشكل حداثة وتعقيد وديناميكية المخاطر الإلكترونية تهديدًا قانونيًا لوسطاء التأمين؛ حيث سيعرف وكيل التأمين، أو السمسار ذو الخبرة أن التنبؤ الدقيق لتغطية عقد التأمين ضد المخاطر السيبرانية غير ممكن، ومن شأن ذلك التأثير على الرغبة لدى الوكيل، أو السمسار في تقديم هذه المنتجات الجديدة، والنتيجة هي أن عددًا قليلًا فقط من المتخصصين سيكونون مستعدين وقادرين على بيع منتجات التأمين الإلكتروني، وأن هذا النقص في خبرة الاكتتاب ليس قيدًا قانونيًا مباشرًا، ولكنه يشكل لدى العملاء عدم اليقين القانوني بشأن ما يمكن اعتباره خطرًا إلكترونيًا قابلًا للتأمين وما لا يُعد كذلك، ويكون له تأثير سلبي على تطور السوق[37].

في الوقت الحالي يغطي سوق التأمين الإلكتروني نسبة صغيرة فقط من إجمالي الخسائر الناتجة عن طريق الهجمات

36 Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, The Law and Economics of Cyber Insurance Contracts.

37 Christian Biener, Martin Eling and Jan Hendrik Wirfs, Insurability of Cyber Risk: An Empirical Analysis, Article in Geneva Papers on Risk and Insurance - Issues and Practice · June 2014 DOI: 10.1057/gpp.2014.19. Retrieved on 14/3/2021, from https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis

الإلكترونية، ومن الصعوبة قياس التأثير الكامل للهجمات الإلكترونية على اقتصاديات الدول[38]. ولتفادي الأضرار الناشـئة عن المخاطر السيبرانية ناقش جانب من الفقه القانوني والمختصين في الأمن السيبراني والتأمين الإلكتروني إمكانية فـرض تأمين إلكتروني إلزامي على الشركات باعتباره من الالتزامـات المفروضة عليها لحماية الخصوصية وحفظ البيانات والمعلومات للعملاء والمسـتخدمين، وذهب اتجاه آخر إلى أنـه لا يمكن إلزام الشركات الصغيرة والمتوسـطة بالتأمين الإلكتروني الإجباري باعتباره ليس مناسـبًا جدًا لهذه الشركات، ويُضاف إلى ذلك أن التأمين الإلكتروني يغطي بشـكل عام كلًا مـن الأضرار التي تلحق بالطرف الأول المؤمن له وأطـراف ثالثة، لذلك فإن التأمين على الإنترنت ليس تأمينًا ضد المسـؤولية المدنية فقط، ولا يمكن تبرير فرض التأمين الإلكتروني الإجباري بـأي حال من الأحوال. لذلك ذهب معظم الخبراء وبالتوافق مع فقهاء القانون إلى إنشـاء تأمين إلكتروني إلزامي لدى بعض الشركات والصناعات المعرضة لخطر الهجمات الإلكترونية ومنها شركات التأمين والمحاماة والبنوك.

يمكن أن يستند التأمين الإلكتروني الإجباري إلى نوعين من المسؤولية الإلكترونية:

أولًا: نظام المسؤولية عن الخطأ؛ بحيث يدفع المؤمن التعويض مقابل الضرر الذي لحق بالمؤمن له حسب درجة خطأه، سـواء في الخطأ العقدي (المسـؤولية العقدية)، أو في المسـؤولية التقصيرية التي تقوم إما على أساس الخطأ واجب الإثبات بالنسـبة إلى المسؤولية عن الأعمال الشـخصية، أو الخطأ المفترض بالنسبة إلى المسؤولية عن عمل الغير. ووفقًا لبعض الخبراء، سيسـمح التأمين الإجباري بسبب الخطأ إلى تعويض المضرور في معظم الحالات، إلا في حالة حدوث خطأ من جانب الشركة المؤمن له.

ثانيًا: نظام مسـؤولية صارم خالٍ من الخطأ، أو ما يُسمى بالمسـؤولية بدون خطأ (بحيث يقوم المؤمن بتعويض المؤمن له، غالبًا إلى مبلغ معين؛ بغض النظر عما إذا كان الأخير قد ارتكب خطأ أم لا. ويذهب الخبراء إلى أن التأمين بدون خطأ سـيدفع الشركات إلى التراخي، وعدم الاهتمام بتطوير الأمن السيبراني، وقد ينعكس سلبًا على الحد من مخاطر الهجمات الإلكترونية[39].

الخاتمة

قبل سرد أهم النتائج والتوصيات التي توصلت بها الدراسة، ننوه إلى أنه يجب أن تعمل صناعة التأمين، جنبًا إلى جنب مع أصحاب المصلحة الآخرين، لزيـادة الوعي بالمخاطر الإلكترونية، وتثقيف العملاء حول كيفية التعامل

38 في الولايات المتحدة الأمريكية طور مجلس البيت الأبيض للمستشارين الاقتصاديين نموذجًا يستخدم لقياس ردود فعل سوق الأوراق المالية للشركات التي شهدت "نشاطًا إلكترونيًا ضارًا" لتقدير تكلفة الهجمات الإلكترونية. باستخدام هذا النموذج، وجدوا أن الهجمات الإلكترونية تكلف الاقتصاد الأمريكي ما بين 57 مليار دولار و109 مليارات دولار في عام 2016، أي ما يعادل 0.3% إلى 0.6% من الناتج المحلي الإجمالي. خلال نفس الفترة، تكبدت شركات التأمين الأمريكية 356 مليون دولار من المطالبات من حاملي وثائق التأمين؛ أي ما يعادل أقل من 1% من الخسائر المقدرة. تمت مقارنة ذلك بالكوارث الطبيعية؛ حيث دفعت شركات التأمين 50% من الخسائر بين عامي 2015 و2018. يوضح هذا الاختلاف في الخسائر المؤمن عليها مجال النمو في سوق التأمين الإلكتروني.

The Council of Economic Advisers February 2018. Retrieved on 14/3/2021from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

39 Jacques de Werra & Yaniv Benhamou, Cyberassurance : instrument utile pour la cybersécurité des entreprises ?, in : Jusletter 24 août 2020 ISSN 1424-7410, jusletter. Analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (PME), Catégories d'articles : Articles scientifiques Domaines juridiques : Informatique et droit; Droit des assurances privées.

معها. يمكن أن تحدد سياسات إدارة المخاطر التي يحتاج العملاء إلى الامتثال لها من أجل شراء التأمين الإلكتروني. يمكن لهذه الصناعة أن تزود العملاء بأدوات تساعدهم على الحماية من المخاطر الإلكترونية؛ كما تم القيام به في مجالات الأعمال الأخرى. إضافة ذلك، من المهم أيضًا أن تبني شركات التأمين المعرفة المطلوبة بأمن تكنولوجيا المعلومات، والاستفادة من كفاءة الشركات المتخصصة، كما تحتاج إدارة المبيعات والمخاطر إلى اكتساب معرفة تقنية محددة لتكنولوجيا المعلومات من أجل فهم المخاطر الإلكترونية بشكل كافٍ.

أولًا: النتائج

- يحتل التأمين الإلكتروني والأمن السيبراني مرتبة متقدمة في اهتمامات القطاع المالي والشركات التجارية والحكومات.
- أثرت جائحة (كوفيد -19) على مدى السنة الماضية في أداء الاقتصاد العالمي، وأدت إلى زيادة الهجمات الإلكترونية على الشركات التجارية، وترافق ذلك مع نمو الطلب على التأمين الإلكتروني ضد المخاطر السيبرانية.
- تلعب شركات التأمين دورًا رئيسًا في إيجاد حلول تأمينية جديرة بالثقة للتعامل بشكل مناسب مع استدعاءات المخاطر السيبرانية.
- سوق التأمين الإلكتروني لا يزال غير ناضج، وتتوفر مجموعة واسعة من التغطية السيبرانية، والسياسات تختلف اختلافا كبيرًا باختلاف شركات التأمين.
- تُشكل الهجمات الإلكترونية تهديدًا كبيرًا للدول والأفراد والشركات التجارية، وإن نمو أنظمة الأمن السيبراني وحماية البيانات والخصوصية يجعل من عقد التأمين الإلكتروني مطلبًا وليس خيارًا.
- تُعد المخاطر السيبرانية أكبر تحدٍ لشركات صناعة التأمين في الوقت الحاضر، خاصة فيما يتعلق بالمخاطر التراكمية؛ حيث يمكن لحدث إلكتروني واحد أن يؤثر على العديد من الشركات المختلفة في نفس الوقت، فضلًا عن أن يؤدي إلى توقف الأعمال في المزيد من الشركات. وهناك عدد من المخاطر الشديدة التي لا تستطيع صناعة التأمين تحملها، أو تحمل التكاليف والخسائر التي تنتج عنها بمفردها، ، لذلك يجب أن تتحملها الحكومات والشركات بشكل مشترك[40].
- تستغرق الشركات 20 عامًا لبناء السمعة التجارية والاسم التجاري، ودقائق قليلة من الهجمات السيبرانية تكفي لتدميرها[41].
- يجب على شركات التأمين إعادة تقييم المخاطر الإلكترونية، ويُعد ذلك أمرًا ضروريًا؛ للأسباب التالية:

1. تفتقر صناعة التأمين إلى القدرة على تغطية حادث إلكتروني يشمل عددًا كبيرًا من العملاء.
2. لا تمنح التغطية الإلكترونية الحالية سوى جزءٍ صغيرٍ من الخسائر (ومن أهمها ما يرتبط بانتهاكات البيانات

40 Cyber Insurance: Risks and Trends, Categories, Cybercrime, Publications April, 2020. Retrieved on 14/3/2021, from https://bsabh.com/category/publications-2

41 Ajay Chawla, Stephane Nappo, Cybersecurity Insurance Coverage: Coronavirus Age, 2018.

والمعلومات وتعطيل الشبكة)، ويبقى جزءٌ كبيرٌ من المخاطر السيبرانية غير مؤمن عليه.

3. حكومات الدول ليســت قادرة، حتى الآن، على دعم الالتزامات غير المحــدودة المحتملة في حالة وقوع هجمات إلكترونية كبيرة يمكن أن تهدد اقتصاديات دول بأكملها. ومن ثَمَّ، فإننا نقترح شراكة بين القطاعين العام والخاص لمواجهة التحديات المحتملة.[42]

ثانيًا: التوصيات

- تنظيم الإطار القانوني لعقد التأمين الإلكتروني في التشريعات الوطنية.
- تأمين الحماية القانونية للشركات والعملاء والمســتخدمين في مجال قطاعــات العمل التجاري الإلكتروني بالوسائل القانونية والتقنية والتكنولوجية. وتعميق الروابط بين القانونيين والمختصين في مجال الاتصالات تكنولوجيا المعلومات للوصول إلى الهدف المنشود.
- التعاون الدولي، وبدء الحوارات والاتفاقيات العالمية التي تهدف إلى تقييد الهجمات السيبرانية، وتعزيز نظام تكنولوجيا المعلومات، ودعم تطوير قواعد البيانات الإلكترونية، واعتماد المعايير للحد من المخاطر.
- مساهمة الحكومات في إيجاد ســوق التأمين السيبراني المتطور الذي من شأنه أن يلعب دورًا رئيسًا في عملية التحول إلى الاقتصاد الرقمي من خلال زيادة الوعي بالمخاطر الســيبرانية، وتبادل المعرفة على الممارســات الجيدة لإدارة المخاطر السيبرانية.
- دعم شركات التأمين الوطنية، وتشــجيعها على إصدار عقد التأمين الإلكتروني ضد المخاطر الســيبرانية، وذلك من خــلال الشراكة بين القطاعين العام والخــاص، وتحفيز تطوير قواعد البيانات وتقاســمها مع المؤسسات والمنظمات الإقليمية والدولية؛ وتسهيل تطوير آليات نقل المخاطر التقليدية والبديلة.
- نظرًا لأن المخاطر السيبرانية ذات طبيعة عالمية، فيجب على شركات التأمين في مختلف الدول إبرام اتفاقيات التعاون وتبادل الخبرات فيما بينها.
- بذل المزيد من الجهود في تنظيم وثيقة التأمين الإلكتروني ضد المخاطر السيبرانية النموذجية من قبل الخبراء والمختصين في مجال التأمين.
- يجب أن يكون المجتمع الأكاديمي أيضًا جزءًا من الحوار العالمي حول كيفية منع المخاطر السيبرانية، وكيفية تعزيز التأمين الإلكتروني؛ من أجل تقديم وجهة نظرهم في مواجهات التحديات السيبرانية.

42 Martin Eling, Werner Schnell, edited by Fabian Sommerrock, Ten Key Questions on Cyber Risk and Cyber Risk Insurance, The Geneva Association, November 2016, pp (32-37). Published by The Geneva Association – 'International Association for the Study of Insurance Economics', Zurich.

المراجع

أولًا: العربية

علي، جابر محجوب. **النظرية العامة للالتزام، الجزء الأول مصادر الالتزام في القانون القطري**، جامعة قطر، 2016.

نشرة الاتحاد المصري للتأمين، ع 67، 2019.

«هل أنت جاهز لمواجهة المخاطر السيبرانية؟»، 2018، على الرابط التالي:

https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324 (accessed 14/3/2021).

ثانيًا: الأجنبية

Allianz Risk Barometer: Identifying the Major Business Risks for 2020. Retrieved on 14/3/2021, from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf.

Biener, Christian, Martin Eling & Jan Hendrik Wirfs. Insurability of Cyber Risk: An Empirical Analysis, Article in Geneva Papers on Risk and Insurance - Issues and Practice · June 2014 DOI: 10.1057/gpp.2014.19. Retrieved on 14/3/2021, from https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis.

Corbett, Molly. Ransomware, COVID-19 and Cyber Insurance - The Big Disconnect, December 09, 2020, Region: North America. Retrieved on 14/3/2021, from https://www.genre.com/knowledge/blog/ransomware-covid-19-and-cyber-insurance-the-big-disconnect-en.html

Chawla, Ajay & Nappo, Stephane. Cybersecurity Insurance Coverage: Coronavirus Age, 2018.

COVID-19 Crisis May Warrant Changes to Your Cyber Insurance Coverage, July 2020, article. Retrieved on 14/3/2021 from: https://www.jonesday.com/en/insights/2020/07/covid19-crisis-may-warrant-changes-to-your-cyber-insurance-coverage.

Cyber Insurance: Risks and Trends, Categories, Cybercrime, Publications April 2020. Retrieved on 14/3/2021, from: https://bsabh.com/category/publications-2.

Cyber Insurance, Retrieved on 14/3/2021, from https://www2.deloitte.com/us/en/insights/focus/human-capital-trends.htm.

Cyber Risk for Insurers – Challenges and Opportunities, Luxembourg: Publications Office of the European Union, 2019. © EIOPA, 2019 Reproduction is authorised provided the source is acknowledged.

Eling, Martin. Werner Schnell, edited by Fabian Sommerrock, *Ten Key Questions on Cyber Risk and Cyber Risk Insurance,* The Geneva Association, November 2016, pp (32-37). Published by The Geneva Association — 'International Association for the Study of Insurance Economics', Zurich.

Hadwin, Steven. Norton Rose Fulbright LLP and Jamie Monck-Mason, Willis Towers Watson, Cyber Insurance: An Overview, Practical Law, 2020, Uk.

Jacques de Werra / Yaniv Benhamou, Cyberassurance: instrument utile pour la cybersécurité des entreprises ?, in : Jusletter 24 août 2020 ISSN 1424-7410, jusletter. Analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (PME), Catégories d'articles : Articles scientifiques Domaines juridiques : Informatique et droit; Droit des assurances privies.

Keevy, Justin. "COVID-19: Implications for Cyber Coverage," Retrieved on 14/3/2021, from https://www.marsh.com/za/insights/research-briefings/covid-19-implications-cyber-media-tech-errors-omissions.html.

LinkedIn Strikes $1.25M Settlement in Data Breach Action, Retrieved on 14/3/2021, from https://www.law360.com/articles/568135/linkedin-strikes-1-25m-settlement-in-data-breach-actio,

Munich Re worldwide, Retrieved on 14/3/2021, from https://www.munichre.com/en.html.

Nieuwesteeg, Bernold, Louis Visscher & Bob de Waard. The Law & Economics Of Cyber Insurance Contracts: A Case Study, *ediss.sub.hamburg*, 2018. Retrieved on 14/3/2021, from https://ediss.sub.uni-hamburg.de/handle/ediss/8189.

Nieuwesteeg, Bernold, Louis Visscher & Bob de Waard. The Law and Economics of Cyber Insurance Contracts: A Case Study, *European Review of Private Law*, Volume 26, Issue 3 (2018).

Palsson, Kjartan, Steinn Gudmundsson & Sachin Shetty, "Analysis of the impact of cyber events for cyber insurance," Published online: 4/6/2020 © The Geneva Association 2020.

Regulation (Eu) 2016/679 of The European Parliament And Of The Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/Ec.

Studer, Evelyne & Jacques De Werra, "Regulating Cybersecurity What Civil Liability In Case Of Cyber-Attacks?" 19/8/2017.

Talesh, Shauhin A. Symposium: Insurance Companies As Corporate Regulators: The Good, The Bad, And the Ugly, 66 Depaul L. Rev. 463, winter, 2017.

The Council of Economic Advisers February 2018, Retrieved on 14/3/2021, from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

The Federal Reserve Bank Of Chicago, Essays On Issues, 2019 Number 426. Retrieved on 14/3/2021, from https://doi.org/10.21033/cfl-2019-426

Tom, Baker. "Back to the Future of Cyber Insurance" (2019). Faculty Scholarship at Penn Law. 2184. Retrieved on 14/3/2021, from https://scholarship.law.upenn.edu/faculty_scholarship/2184.

What Does Cyber Mean? Retrieved on 18/5/2021, from https://www.cyberdefinitions.com/definition_of_cyber.html.

References

ʿaly, jābr mḥjwb. *Alnẓryah alʿiāmah lililtzām, aljzā alawl mṣādr aliltzām fi alqānwn alqaṭary* (in Arabic), jāmʿiat qaṭar, sanat 2006.

"Hāl anta jāhz lmwājhat a1mkhātr a1sybrānīyah?" (in Arabic), 2018. Retrieved on 14/3/2021, from https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324.

Nashrat aliṭḥ ādal-miṣrī lilt'amyn (in Arabic), ʿadad usbwʿiy rqm 67, snat 2019.