Journal of Al-Farabi for Humanity Sciences Volume (6), Issue (2) December (2024)

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://www.iasj.net/iasj/journal/419/issues
مجلة الفارابي للعلوم الإنسانية تصدرها كلية الفارابي الجامعة

دور التأمين في حماية الشركات العراقية من التهديدات السيبرانية المتزايدة

بوران فاضل صالح

كلية النخبة الجامعة

The role of insurance in protecting Iraqi companies from increasing cyber threats

Researcher/ Boran Fadhel Saleh
E-mail:bwranfadeel@gmail.com

الملخص:

يشكل توفير الحماية التأمينية للشركات التجارية العراقية ضد المخاطر السيبرانية إحدى أهم الوسائل الحديثة والناجعة لاستيعاب وتدارك الخسائر المالية الناجمة عن انتهاك أمن أنظمة التشغيل، حيث أن سوق التأمين بصورة عامة يميل إلى إيجاد العديد من الحوافز لبناء أنظمة أكثر أماناً لتلك الشركات ، إلا أنه في الوقت نفسه لا يزال التأمين من المخاطر السيبرانية محاطاً بنوع من الغموض، نظراً لقلة التشريعات المتخصصة بهذا النوع من التأمين ونقص عدد الشركات التي تتعامل مع هذا النوع من التغطيات التأمينية، الأمر الذي يؤدي إلى تردد وقلق الشركات التجارية بصورة عامة من التأمين ضد المخاطر السيبرانية، لا سيما أن هذه المخاطر لا تزال غير محددة بمعيار واضح، مما يؤدي في بعض الأحيان بالعملاء من أصحاب الشركات التجارية إلى عدم فهم طبيعة المخاطر الواردة في بنود عقد التأمين من المخاطر السيبرانية .ويتميز التأمين من المخاطر السيبرانية عن عقود التأمين من المخاطر الشائعة بجملة من المتطلبات التي تواكب مرحلة توقيع عقد التأمين، بالإضافة إلى ارتفاع الأقساط مقارنة بأنواع عقود التأمين التقليدية بسبب ندرة البيانات التاريخية الخاصة بهذا النوع من المخاطر نظراً لحداثتها الأمر الذي يؤدي لصعوبة تقييم هذه المخاطر أو نمذجتها، مما يثير العديد من التساؤلات حول ماهية هذه المخاطر، والآثار القانونية المترتبة على تحققها والتساؤل عن مدى كفاية القواعد العامة للتأمين لتطبيقها على عقد التأمين من المخاطر والتهديدات السيبرانية.**الكلمات المفتاحية: التأمين، حماية، الشركات، الهجمات، السيبرانية.**

Abstract

Providing insurance protection for Iraqi commercial companies against cyber risks constitutes one of the most important modern and effective means of absorbing and reversing financial losses resulting from violating the security of operating systems, as the insurance market in general tends to create many incentives to build more secure systems for these companies, but at the same time Cyber insurance is still shrouded in ambiguity. Due to the lack of legislation specialized in this type of insurance and the lack of companies that deal with this type of insurance coverage, which leads to hesitation and concern of commercial companies in general about insuring against cyber risks, especially since these risks are still not defined by a clear standard, which leads to... Sometimes clients who own commercial companies do not understand the nature of the risks contained in the terms of the insurance contract from cyber risksInsurance against cyber risks is distinguished from insurance contracts against common risks by a set of requirements that accompany the stage of signing the insurance contract, in addition to higher premiums compared to types of traditional insurance contracts due to the scarcity of historical data on this type of risk due to its recentness, which leads to the difficulty of evaluating or modeling these risks. Which raises many questions about what these risks are, And the legal implications resulting from its verification and the question of the adequacy of the general insurance rules for their application to the insurance contract against cyber risks and threats. **Keywords: insurance, protection, companies, attacks, cyber.**

مقدمة:

أصبحت الشركات التجارية العراقية في الوقت الحالي أمام تحدي كبير للحفاظ على سرية وخصوصية معلوماتها وحماية بياناتها الشخصية وبيانات العملاء و أسرارها التجارية أمام الكم الهائل من المخاطر والتهديدات السيبرانية التي تهدد سلامة البيئة التجارية، ومهما كانت الشركات التجارية محصنة بإجراءات الأمن والسلامة من التهديدات السيبرانية إلا أن ذلك لا يعني إمكانية تجنب هذه التهديدات السيبرانية بصورة كلية، حيث لا تزال العديد من هذه التهديدات غير قابلة للسيطرة عليها كونها تمتاز بالتطور المستمر فمن غير الممكن تجنب حدوثها، إلا أنه لا يزال بالإمكان التخفيف من الآثار الناتجة عنها، ومن أجل السعي للتخفيف من حدة الآثار الناجمة عن التهديدات السيبرانية .و إدراكاً لهذه التحديات وما ينجم عنها من تأثيرات سلبية على مستقبل الشركات التجارية بصورة عامة، برزت عدد من شركات التأمين تقدم خدمات غير تقليدية متمثلة بالتأمين من المخاطر السيبرانية، وذلك بهدف الحد من هذه المخاطر أو التقليل من حدة آثارها على الشركة، وبعد انتشار (التهديدات السيبرانية)أضحى تجنب هذا النوع من التهديدات في حد ذاته هدفاً طموحاً إلى حد كبير ، نظراً لاعتماد الشركات التجارية حديثاً على التكنولوجيا الرقمية وانتشارها في التعاملات التجارية، قد يكون الخيار الاول الذي يتبادر إلى الذهن لتجنب هذا النوع من التهديدات هو الامتناع عن استخدام أنظمة الحوسبة بصورة كلية أو التقليل من استخدامها إلى حد كبير، إلا أن هذا القرار غير عملي ولا يتناسب مع بيئة العمل التجارية الحديثة والتي تكاد تعتمد بالكامل على الأنظمة الالكترونية المتصلة بالإنترنت، مع الأخذ بنظر الاعتبار فوائد عمل الشركات التجارية وفقاً لوسائل التكنولوجيا الحديثة والتي تؤدي إلى تقليل الوقت والجهد والنفقات إلى حد كبير مقارنة بالشركات التي لا تتعامل مع وسائل التواصل الشبكي، إلا أنه بالمقابل ستتعرض الشركات التي تزاول العمل التجاري في البيئة الرقمية إلى خسائر كبيرة ولا يتطلب الأمر سوى اجزاء من الثانية لتحقق هذه الخسائر .ومن هذا المنطلق أدركت الشركات التجارية أنها لا يمكن أن تحمي نفسها من جميع التهديدات السيبرانية طوال الوقت، و أنها بحاجة إلى إدارة هذه التهديدات و تحديد أولويات جديدة للشركة من خلال حماية البيانات سواء كانت بيانات الشركة أو بيانات العميل بالإضافة لحماية أنظمة التشغيل والشبكات التي تمارس من خلالها أنشطتها التجارية خصوصاً أن الإحصائيات قد أشارت الى تصاعد وتيرة التهديدات السيبرانية وضخامة الأضرار الناشئة عنها في السنوات القليلة الماضية، ومن هنا ظهرت في الآونة الأخيرة شركات تأمين تقدم نوع جديد من الخدمات التأمينية تختلف عن باقي التأمينات التقليدية، كون هذه الشركات أصبحت تؤمن الشركات التجارية أو الاشخاص الطبيعية والمعنوية ممن هم في حاجة للتأمين من مخاطر سيبرانية غير ملموسة مثل التأمين على أصول البيانات الخاصة بالشركة والعملاء من مخاطر الاختراق أو التأمين من توقف الخدمة أو من القرصنة الإلكترونية للعمليات المصرفية على سبيل المثال، وما يستتبع ذلك من تحديات فنية وقانونية في تقدير مدى احتمالية وقوع هذه المخاطر السيبرانية و حجم الأضرار الغير محددة النطاق كونها تقع في فضاء سيبراني تشترك فيه شركات التأمين مع الطرف المؤمن له وموظفي الخدمات الإلكترونية والعملاء وأصحاب المصالح بصورة عامة .مما يدلل على حجم الأضرار المراد تغطيتها وما يستتبع ذلك من صعوبة تقدير الأقساط التأمينية ذلك أن التهديدات السيبرانية تمتاز بالحداثة والغموض والتطور المستمر مما يصعب المهمة على شركات التأمين ذاتها نظراً لقلة التجارب السابقة ، كون العديد من الشركات التي تعرضت للتهديدات السيبرانية تحجم عن ذكر حجم الضرر الذي تسببت به المخاطر لتأثيره المباشر على سمعتها التجارية.وعلى الرغم من تزايد الطلب على التأمين من الأخطار السيبرانية، إلا أنه لا يزال يكتنفه الغموض وغير محدد المعالم نتيجة التطور السريع في تكنولوجيا المعلومات وانعدام وجود التشريعات المنظمة له على الصعيدين الوطني والدولي.

مشكلة الدراسة:

تكمن مشكلة الدراسة في غياب التنظيم التشريعي الخاص بالتأمين من التهديدات السيبرانية والذي من شأن هذا التنظيم أن يزيل منه الغموض ويبعده عما يشتبه به، لذلك فإن الحماية التأمينية للشركات التجارية من المخاطر السيبرانية تثير عدة تساؤلات والتي يحاول الباحث معالجتها والإجابة عنها في البحث، وأهمها ما المقصود بالتهديدات السيبرانية ؟ وما هي طبيعتها؟ –هل يخضع التهديد السيبراني القابل للتأمين منه للشروط ذاتها المطلوبة في الخطر التقليدي؟ –ما مدى ملائمة وكفاية القواعد العامة لعقد التأمين في تنظيم الخطر السيبراني؟ –هل أن جميع المخاطر السيبرانية قابلة للتأمين منها؟ وبعبارة أخرى هل هناك مخاطر سيبرانية لا يمكن التأمين منها؟ –هل أن انعدام وجود معيار عام للخطر السيبراني يعد سبباً لعدم وجود تنظيم قانوني خاص ينظم التأمين من هذه المخاطر؟

أهمية البحث:

تتجسد أهمية موضوع البحث كونه يعالج موضوعاً يتعلق بدور التأمين في حماية الشركات التجارية من تهديدات أضحت في وقتنا الحاضر تشكل تحدياً واضحاً لنشاط هذه الشركات ، وخير دليل على ذلك تزايد الاهتمام لا على المستوى المحلي فحسب بل على المستوى الدولي

بالتأمين من التهديدات السيبرانية في مقابل قلة الدراسات العراقية والعربية في هذا الموضوع بسبب حداثته، كما تكمن أهمية الدراسة في الدور الفعال الذي يلعبه تأمين الشركات التجارية من المخاطر السيبرانية، فبغض النظر عن كونه أداة لتقليل المخاطر والتخفيف من آثارها، تبرز أهمية دراسته باعتباره نوع جديد من التأمين غير مألوف سابقاً في سوق التأمين التقليدي.

أهداف البحث:

يهدف البحث إلى التعرف على مفهوم التهديدات السيبرانية و دراسة المفهوم القانوني لعقد التأمين من المخاطر السيبرانية والبحث في آثار عقد التأمين من المخاطر السيبرانية وتحدياته.

المبحث الأول: مفهوم المخاطر السيبرانية.

تعد السيبرانية من المصطلحات الحديثة نسبياً والتي تم تداولها بين فقهاء القانون في الآونة الأخيرة، حيث برز هذا المصطلح في القانون التجاري مؤخراً نظراً لظهور نوع جديد من عقود التأمين والذي يعرف بالتأمين من التهديدات والمخاطر السيبرانية، وبما أن الخطر يشكل جوهر التأمين فلا بد من بيان تعريف هذا النوع الحديث من التهديد وتمييزه عما يشتبه به جهة، ومن ثم بيان أنواع التهديدات السيبرانية وأثرها على الشركات التجارية من جهة أخرى.

أولاً: التعريف بالخطر السيبراني وتمييزه عما يشتبه به:لقد شكل الخطر ولا يزال العنصر الجوهري في عقد التأمين، فضلاً عن كونه محلاً لعقد التأمين، الأمر الذي يستوجب تعيينه في العقد وبتخلفه لا نكون بصدد عقد تأمين بالمعنى القانوني الصحيح والدقيق، بل هو كذلك حادثة محتملة لا يتوقف تحققها على محض إرادة أحد طرفي العقد (شرعان، بدون سنة، ٨). ويعتبر الخطر السيبراني نوع جديد من المخاطر التي أصبح بالإمكان التأمين منها من قبل الشركات التجارية، فقد بدأ هذا النوع غير التقليدي من التأمين بالانتشار في الوقت الحاضر، نظراً لكثرة استخدام شبكات الأنترنت في معظم الأعمال التجارية. وعلى الرغم من كثرة تداول المصطلح في الأوساط القانونية إلا أنه لا يوجد تعريف موحد ومعتمد للخطر السيبراني ولعل السبب يكمن في اعتقادنا بتداخل المصطلح وشيوعه في أكثر من تخصص علمي أو بسبب طبيعته المتغيرة.بالنسبة للمصطلح cyber فهو مصطلح غير موجود في اللغة العربية؛ لأنه يوناني الأصل ولكن تم تعريب المصطلح إلى سيبراني بما معناه كومبيوتري أو عصري جداً، ويقصد به كل ما يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية Cybernetics (البعلبكي ومنير، ٢٠٠٩، ٣٠٧) فيقال فضاء سيبراني أي: فضاء كمبيوتري كما يأتي بمعنى تخيلي أو شبكي أو ما يقع ضمن الفضاء الرقمي كما تشير كلمة cyber لغة إلى وجود علاقة مع تكنولوجيا المعلومات أي أجهزة الحاسب الآلي بما تتضمنه من عمليات تخزين وحماية البيانات والوصول إليها ومعالجتها ونقلها. وغالباً ما تستخدم هذه الكلمة بصورة مركبة كأن نقول فضاء سيبراني أو خطر سيبراني أو تهديدات سيبرانية سواء بصورة مفصولة ام مدمجة ويعد العالم Norbert wiener أول من استخدم هذا المصطلح في أحد مؤلفاته الصادر في عام ١٩٤٨ بعنوان cybernetics وكان يعنى بعلم الدراسة والتحكم بالآليات في الأنظمة الحيوانية البشرية والحاسوبية (Wiener, 1948, 144).إن انعدام وجود مصطلح مناظر في اللغة العربية شكل تحدياً للمختصين العرب لاختيار مصطلح مقارب لمعنى cyber لذا تم استخدام مصطلح سيبرانية في العديد من المحافل والوثائق والهيئات الدولية أو الوطنية، فنجد مثلاً وثائق الأمم المتحدة الصادرة بهذا الخصوص استخدمت مصطلح السيبرانية بدلاً من الالكترونية كتعريب لمصطلح cyber في قراراتها (عمر، ٢٠٠٨، ٣٦٥)يشير مصطلح الفضاء السيبراني إلى مجال افتراضي من صنع الإنسان ويعتمد على شبكات الانترنت وأنظمة الحاسوب و كم هائل من المعلومات والبيانات والأجهزة، فهو مجال غير مادي ينتج عن عناصر متعددة وهي الشبكات والبرمجيات و أجهزة الحاسب الآلي ومعطيات النقل والتحكم الرقمي وغيرها فهو بيئة تفاعلية حديثة (الموسوي،٢٠١٨، ٣٥) ،أما مصطلح الأمن السيبراني فيعني أمن الحاسوب أو أمن المعلومات ويعد ضمن فروع تكنولوجيا المعلومات والذي يهتم بحماية الأنظمة والممتلكات والشبكات وما إلى ذلك من الهجمات الرقمية، وقد ظهر الاهتمام بالأمن السيبراني بعد تزايد المخاطر السيبرانية وانعكاس ذلك على الأمن والسلم الدوليين حيث من المتوقع ان تتسبب المخاطر السيبرانية بأضرار مادية و معنوية كارثية بحلول العام ٢٠٢٥ .لقد عرف البعض المخاطر السيبرانية بأنها أي خطر من الخسارة المالية أو الضرر الذي يلحق بسمعة المنظمة على أن تكون ناشئة عن نوع من فشل أنظمة تكنولوجيا المعلومات الخاصة بها، وهذا الخطر يمكن أن يتحقق بالطرق التالية :الخرق المتعمد وغير المصرح به للوصول إلى نظم المعلومات لأغراض التجسس أو الابتزاز ،الخرق غير المقصود أو العرضي للأمن، والذي قد لا يزال يشكل مع ذلك تهديداً يحتاج إلى معالجة، الخرق التشغيلي (IRM) organization, 2014, 10))، إن ما يميز هذا التعريف هو أنه ينظر للخطر

السيبراني من جهة مصدره والأثر المترتب على وقوعه، فضلاً عن أنه لم يقتصر على ذكر الأضرار المادية كأثر ناتج على تحقق الخطر مدار البحث بل أشار للأضرار المعنوية وتلك التي تلحق بالسمعة حتى وإن ترتب عليها فيما بعد ضرر مادي.

وقد عرف آخرون المخاطر السيبرانية بأنها مخاطر تشغيلية لأصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية أو توافر أو سلامة المعلومات أو نظم المعلومات (Cebula, J.J. and Young, 2010, 13)، ويتضح لنا أن هذا التعريف قد أشار إلى موضوع الخطر وتأثيره إلا أنه لم يتطرق بالذكر إلى مصدر هذا الخطر.وعرف البعض هذه المخاطر على أنها مخاطر تكنولوجيا المعلومات وهي مخاطر الأعمال التجارية، وعلى وجه التحديد مخاطر الأعمال المرتبطة باستخدام تكنولوجيا المعلومات وملكيتها وتشغيلها ومشاركتها وتأثيرها واعتمادها داخل الشركة التجارية. ويتكون من الأحداث المتعلقة بتكنولوجيا المعلومات التي يمكن أن تؤثر على الأعمال التجارية (ISACA, 2009, 7).وعرف آخرون المخاطر السيبرانية على أنها المخاطر التي ينطوي عليها حدث إلكتروني ضار يتسبب في تعطيل الأعمال التجارية والخسارة النقدية (Eling, Schnell, 2016, 12).

ثانياً: أنواع الخطر السيبراني يتحدد مفهوم المخاطر والتهديدات السيبرانية بتحديد أنواعها أولاً ، وهذا الأمر ضروري لكي يتم معالجتها بصورة ملائمة من الناحية الفنية و القانونية فالخسائر الناجمة عن هذه المخاطر تمتاز بأنها ذات أصل غير مادي وتتصدر هذه المخاطر الساحة لسبب بسيط وهو ازديادها السريع، فقد أشارت الدراسات إلى إن عدد الهجمات السيبرانية ارتفع بنسبة 51 بالمائة في فرنسا في عام 2015 وبنسبة 38 بالمائة في جميع انحاء العالم (Assurance, 2018, 8)، تحت عبارة مخاطر الانترنت أو المخاطر السيبرانية تنطوي جميع الاضرار المختلفة التي تصيب الممتلكات والتي تسببها أنظمة معالجة البيانات والمعلومات والتقنيات الاخرى المنبثقة منها، ووفقا لمقياس "FFAالاتحاد الفرنسي للتأمين " لعام 2019 تعد المخاطر السيبرانية إحدى أهم المخاطر الرئيسية على المدى القصير، والأعلى على المدى المتوسط مما شكل تحديا كبيراً لشركات التأمين نظراً للطبيعة المعقدة نوعاً ما لهذه المخاطر و تطورها المستمر (الأكيابي، ٢٠٢٣، ٣٩)، ومن أبرز هذه المخاطر وأكثرها شيوعاً هجمات رفض الخدمة DDOS: وهو إغراق المواقع الخاصة بالشركة التجارية بكم هائل من البيانات غير الضرورية التي يتم إرسالها ببرامج متخصصة تعمل على التسبب ببطء الخدمات أو تسبب ازدحام على هذه المواقع فيصعب وصول المستخدمين اليها وتعرضت لهذا النوع من المخاطر العديد من المواقع المهمة والحساسة مثل Amazon (الباسوسي، ٢٠٢٣، ١٥٦)، ويتم تنفيذ الهجوم باستخدام أجهزة كمبيوتر آمنة جداً ومتفرقة في عدد من دول العالم مما يجعل معرفة الفاعل أمراً صعباً مقارنة بالمخاطر التقليدية.أعمال التجسس او اختراق الحاسب الالي :يعرف التجسس الإلكتروني بأنه استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير قانوني لأنظمة المعلومات التابعة للدول أو المنظمات أو المواطنين أو الشركات بهدف التنصت عليها بقصد الحصول على معلومات مهمة تتعلق بالنواحي العسكرية أو السياسية أو الاقتصادية أو العلمية أو الاجتماعية حيث يتم اختراق الحواسيب الآلية بصورة بطريقة تمكن المتجسس من التعرف على محتويات هذه الحواسيب من دون الحاق الضرر بمحتوياتها عن طريق نقل الفيروسات إلى تلك الاجهزة المستهدفة، ويختلف التجسس عن (عملية استغلال شبكات الحاسوب) والتي هي صورة من صور التجسس إلا أنه يتم من خلالها استخراج المعلومات التي تم التعرف عليها من خلال عملية الاختراق وهي في الغالب لا تسبب أي ضرر أو تعطيل في الأجهزة (جعفر، ٢٠١٣، ٥٦٩)برامج الفدية :وهي برامج إلكترونية ضارة تعد الأكثر شيوعاً بين جميع أنواع المخاطر السيبرانية الأخرى، تعمل على اختراق أمن الشبكات عبر ثغرات أمنية محددة عن طريق النقر على رابط أو تحميل ملف أو عند استخدام ناقل بيانات مصاب .وتستخدم التشفير لمنع الوصول إلى البيانات على الأنظمة التي تستهدفها ولشل الأنظمة الكمبيوترية بشكل تام، ويعمد مرتكبو الاعتداء إلى طلب مبالغ مالية (سميت بالفدية) لفك تشفير الملفات وتسهيل استئناف الوصول إلى الأنظمة المعتدى عليها (شاهين، ٢٠٢١، ٨٩).

ومن الجدير بالملاحظة أنه لم تعد الإصابة ببرامج الفدية هي الهدف النهائي للهجوم السيبراني وانما قد تكون هذه الاصابة بهدف الحصول على الأموال من الشركة الضحية بصورة غير مشروعة ولذلك يطلق عليها "بعملية الابتزاز المزدوج" حيث يتم طلب الفدية بصورة عامة بعملة البيتكوين Bit–coin ويتم سرقة معلومات الشركة قبل تشفيرها من قبل منفذي الهجوم ليتم بعد ذلك ابتزاز الشركة من خلال التهديد بنشر المعلومات المسروقة أو بيعها في حال لم تدفع الفدية، لذا تعد برامج الفدية من أبرز المخاطر السيبرانية (Assurance des risques cyber,2018, p8).وتجدر الإشارة إلى أن الشركة التجارية عندما تواجه احتمالاً منخفضاً لوقوع هجوم برامج الفدية وبخطورة عالية، فعلى الموظف المسؤول عن أمن المعلومات في الشركة إعطاء الأولوية لمزيد من الاستثمار في تكنولوجيا الأمان واكتشاف المخاطر السيبرانية وتقييدها.الفيروسات: وهي عبارة عن برمجيات مشفرة صممت لغرض إلحاق أكبر ضرر ممكن بأنظمة التشغيل التابعة للدول أو الشركات

التجارية وتتميز بقدرتها على الانتشار من نظام إلى آخر مما يسهل من انتقالها عبر الحدود من دولة إلى أخرى حول العالم حيث يعمل المخترقون على زج ما يعرف بديدان الانترنت والفيروسات ونشرها في شبكة الانترنت بقصد إحداث خلل دائم أو مؤقت في الملفات ونظم التشغيل للشركات المستهدفة، وتعد الفيروسات من أكثر البرامج انتشاراً وشيوعاً منذ سنوات عديدة (ابو التوح، ٢٠٢٣، ٦٥).الهندسة الاجتماعية Social Engineering: هي أسلوب من أساليب الاختراق التي تعتمد بالدرجة الأساس على تدخل العنصر البشري وليس لها أي متطلبات تكنولوجية خاصة، حيث يتم استخدام مهارات المجرم السيبراني من خلال خداع الآخرين ليحصل على معلومات تقنية معينة تساعده على عملية الاختراق ويتم في الغالب عبر الهاتف الحمول، كأن يتم الادعاء من قبل شخص ما بأنه عميل للشركة التجارية مثلا ويوهمهم بذلك ومن ثم يوعز للموظفين بإجراء عملية تحويل مالي إلى حساب آخر (محمد، ٢٠٢٠، ٤٠٢)الحصار الافتراضي Virtual Sit-Ins and Blocked: ويعمل على احداث خلل في آليات سريان العمليات التقليدية في الأجهزة الرقمية الأمر الذي يؤدي إلى رفض عملية الدخول إلى الأنظمة والخدمات الرقمية الخاصة بالشركة التجارية بجميع اشكالها خلال مدة زمنية معينة مما يمنع الشركة متمثلة بموظفيها وعملائها من الدخول إلى الموقع المعني (محمد، ٢٠٢٠، ٤٠٢).التصيد والخداع (phishing): وهو محاولة الحصول على البيانات الشخصية من الشركة التجارية أو العملاء تتعلق بالاسم أو كلمة المرور أو البطاقات الائتمانية أو المفتاح الخاص بالعملات الرقمية كالبيتكوين، حيث يتم ارسال هجمات التصيد والإحتيال عبر البريد الالكتروني ويتم طلب النقر على رابط معين وادخال البيانات الشخصية للشركة الضحية، وتكمن فاعلية هذه الهجمات في صعوبة التمييز بين الموقع الحقيقي وبين الموقع المزيف (محمد، ٢٠٢٠، ٤٠٢)

المبحث الثاني: عقد التأمين من المخاطر السيبرانية:

تمتلك عقود التأمين من المخاطر السيبرانية خصوصية تميزها عما يقابلها من الأنواع التقليدية للتأمين وذلك من حيث الأهداف أو طبيعة المخاطر أو الأضرار التي تتم تغطيتها، كما يجب عدم الخلط بين عقد التأمين من المخاطر السيبرانية، وبين عقد التأمين الإلكتروني من جهة، وبين عقود الأمن السيبراني من جهة أخرى، لذا فمن الضروري في بادئ الأمر بيان ماهية عقد التأمين من المخاطر السيبرانية وايضاح خصوصيته مقارنة بباقي أنواع التأمين من حيث بيان أطرافه وشروطه والأهداف التي يرمي الى تحقيقها مقارنة بالأنواع التقليدية من التأمين، فضلاً عن توضيح الأضرار التي تشملها التغطية التأمينية وبيان الاستثناءات التي قد ترد على هذا العقد (إسماعيل ، ٢٠٢١، ١١٤).

أولاً: حاجة الشركات لعقود التأمين لقد تزايدت في الآونة الأخيرة حاجة الشركات التجارية إلى شراء وثائق تأمين من المخاطر السيبرانية بسبب التهديدات المستمرة والمتزايدة لتلك المخاطر على اختلاف أشكالها كالقرصنة وبرامج الفدية والقنابل الفيروسية وغيرها، على أنظمة تشغيل التابعة لها والتي تحتوي على قاعدة البيانات الخاصة بكلا من الشركة التجارية وعملائها، لذا فإنه من الضروري أن تحيط الشركات التجارية علماً بما يمكن لوثيقة التأمين من المخاطر السيبرانية تغطيته، لكن في الوقت ذاته نجد أنه من الصعوبة بمكان تحديد الإستثناءات الشائعة الواردة في عقود التأمين من المخاطر السيبرانية نظراً لكونه حديث نسبياً ، لقد طرحت شركات التأمين عقود تأمين متخصصة ومصممة للتخفيف من شدة أثر الخطر السيبراني المدمر الذي قد يصيب الشركات التجارية في أي وقت، فهو نوع من عقود التأمين يوفر تغطية الخسائر المتعلقة بالضرر، أو فقدان المعلومات من ضعف الخدمة المقدمة من قبل تكنولوجيا المعلومات والأنظمة والشبكات (شامبي، تأمين الخطر ٢٠٢٣، ٦٦) أو هو عملية تأمينية يقوم بها المؤمن لتعويض أضرار الكارثة السيبرانية (أحمد، ٢٠٢١، ٣٤) ، وتسعى الشركات التجارية من إبرام عقد التأمين من المخاطر السيبرانية لتحقيق هدفين أساسيين (Biener, Eling, Wirfs, 2015, 6)تخفيف المخاطر عنها حيث إن عقد التأمين يضمن لها تعويض عن الخسائر المالية وتوقف أعمالها بسبب المخاطر السيبرانية التي يغطيها هذا العقد، كما يهدف العقد الى تعويض الشركة المؤمن له عن التعرض القانوني الذي يطالها ويجعلها أكثر وعيا بهذا التعرض من خلال تلبيته المعايير أعلى فيما يتعلق بحماية البيانات والأمن السيبراني. سد النقص الحاصل في وثائق التأمين التقليدية: باعتبار أن المخاطر السيبرانية واسعة ومتعددة وفي تطور مستمر وغير مغطاة في وثائق التأمين التقليدية، حيث يتم استثناء الخسائر الإلكترونية، لذا يمكن القول إن عقد التأمين من المخاطر السيبرانية جاء ليكمل النقص ويسد الثغرات الموجودة في سياسيات التأمين التقليدية لتصبح هذه المخاطر قابلة للتغطية بصورة قانونية. وعلى الرغم من أن عقد التأمين من المخاطر السيبرانية يتميز بارتفاع أسعاره مقارنة بأنواع التأمين الأخرى بسبب قلة شركات التأمين التي تقدم التغطية لهكذا مخاطر وصعوبة البت في تقدير حجم الخسائر المتوقعة من قبل أطراف العقد نظراً لطبيعة الخسائر المتغيرة والمترابطة، إلا أنه مع ذلك فإن غطاء التأمين من هذه المخاطر يكون واسع النطاق (نشرة الاتحاد المصري للتأمين،٢٠٢٢، ٢٤٥).وقد انقسمت شركات التأمين بالنسبة لتحديد طبيعة المخاطر التي من الممكن التأمين منها الى قسمين: الأول قد صنفت الخطر على أنه سيبراني وبالتالي امكانية شموله بالتغطية التأمينية

إذا توفرت فيه ثلاثة شروط: الأول هو أن يؤثر الخطر على أحد الاصول الهامة في الشركة التجارية كالخادم أو قاعدة البيانات، أما الشرط الثاني هو أن يتسبب بالخطر جهة فاعلة كالمتسللين والموظفين ونظام التشغيل ذاته، أما الشرط الثالث هو أن يكون الضرر الناشئ نتيجة تحقق الخطر كفقدان الوصول لنظام التشغيل في الشركة التجارية أو إساءة إستخدامه (أحمد، ٢٠٢١، ٤٩).

ثانياً: الخسائر التي يغطيها عقد التأمين:

١-تكاليف إدارة الأزمات المتكبدة في التعامل مع المخاطر السيبرانية وخاصة انتهاك البيانات الشخصية ويشمل ذلك نفقات الإخطار والطب الشرعي لتكنولوجيا المعلومات ونفقات الاستشارات القانونية وتكاليف العلاقات العامة ومراقبة الائتمان ومراكز الاتصال وتكاليف استعادة البيانات (منصور، ٢٠٢١، ١٠٠).

٢-انقطاع الأعمال غير المادي الذي تتسبب به المخاطر السيبرانية للشركات التجارية، ويختلف عن انقطاع الأعمال التقليدية كون الأخيرة ناشئة عن خطر مادي كالحريق مثلاً. أما انقطاع الأعمال غير المادي فإنه ناجم عن إنقطاع تكنولوجيا المعلومات غير المادي كفشل النظام مثلاً. وما يميز هذه التغطية عن باقي التغطيات في مجال التأمين السيبراني أنه يطبق فيها فترة انتظار تحسب بالساعات وبمجرد انتهائها يتم التعويض عن الخسائر بأثر رجعي على سبيل المثال بعد ١٢٠ يوما من بدء الانقطاع أو ٩٠ يوما بعد انتهاء الانقطاع. بالإضافة الى الخسائر الناجمة عن الابتزاز الالكتروني والتي تعد من اكثر المطالبات شيوعاً وفق سياسات التأمين ضد المخاطر السيبرانية (Gareth, Pavel, Ruben, Diane, 2022, 9)

٣-تكاليف المتخصصين في مجال الابتزاز الإلكتروني وتكاليف الفديات الناجمة عن عملية الابتزاز (صادق، ٢٠١٣، ٣٦)

٤-المسؤولية القانونية الناجمة عن خرق الخصوصية والسرية وأمن تكنولوجيا المعلومات: حيث غالباً ما تتمثل هذه المسؤولية بضرر يحدث خارج نطاق أطراف عقد التأمين من المخاطر السيبرانية وهو الغير أو ما تطلق عليه شركات التأمين من المخاطر السيبرانية تسمية – الطرف الثالث وهو غالباً ما يكون أحد عملاء الشركة التجارية المؤمن لها، والتي تنهض عن طريق ادعاء الغير بوجود خرق للبيانات السرية الخاصة به أو تعرضه لخسارة ناجمة عن افتقار الشركة التجارية وهي الطرف المؤمن له في العقد الى متطلبات الأمن السيبراني الأمر الذي يتسبب للغير بالضرروتترتب على التأمين من المخاطر السيبرانية بصورة عامة جملة من الالتزامات الناجمة عن انعقاد عقد التأمين بغض النظر عن نوع الخطر المؤمن منه وطبيعته ويمكن إجمالها بما يأتي:الالتزام بالحفاظ على سرية بيانات المؤمن له الشركة التجارية والالتزام بأحكام اللائحة العامة لحماية البيانات عند معالجة بيانات المؤمن له والالتزام بالمتابعة التفتيش والتدقيق وتحري الدقة في تحديد قيمة قسط التأمين.

خاتمة:

وعلى ما سبق نلخص أن التأمين من المخاطر السيبرانية يحمي الشركات التجارية من مخاطر الفشل المتتالي ولابد للمختصين أن يأخذوا بنظر الاعتبار احتمالية قيام مسؤوليتهم المهنية في حالة عدم إبداء المشورة بضرورة شراء الشركة التجارية لتغطية الخاصة بالتأمين من المخاطر السيبرانية، كما حدث في الولايات المتحدة الامريكية عندما ضرب الإعصار ساندي إقليمها قامت الشركات التجارية برفع دعوى قضائية على وكلائها القانونيين لعدم التوصية بضرورة شراء التأمين من الفيضانات أو إنقطاع الأعمال بصفة منفصلة عن التأمين الذي قد تم شراؤه و الذي لا يغطي هكذا حوادث. وعلى مدار السنوات الماضية حاولت شركات التأمين توضيح نطاق تغطيتها القياسية وهل تتضمن التأمين ضد المخاطر السيبرانية كنوع من التغطية الصامتة (دراعو عز الدين، ٢٠٢٢، ١١٩) أم لا، حيث تكون عقود التأمين من المسؤولية بمثابة المصيدة التي تقع فيها الشركات التجارية ضحية لشركات التأمين وهنا يأتي دور مدير المخاطر في الشركة ليتفق مع شركة التأمين على نطاق التغطية بلغة وحدود واضحة ليتم تأكيد شمول المخاطر السيبرانية ضمن حدود تغطية عقد التأمين من المسؤولية من عدمه كون أحد مظاهر التميز فيما يتعلق بالمخاطر السيبرانية هو أن هذه المخاطر غالباً ما تكون فريدة من نوعها بالنسبة لصناعة التأمين وبالنسبة للشركة نفسها مما يتطلب قدراً كبيراً من العناية من قبل شركات التأمين في أثناء كتابة عقودها، حيث يجب أن تأخذ بنظر الاعتبار حجم الشركة التجارية طالبة التأمين وحجم العملاء ومقدار التواجد على شبكة الإنترنت ونوع البيانات التي يتم خزنها وجمعها حتى تستطيع في نهاية المطاف بأن تحدد الخطوط العامة للتأمين من المخاطر السيبرانية من ناحية شروط وأسعار وثيقة التأمين.

التوصيات والمقترحات:

-يوصى المشرع العراقي بضرورة تفعيل الاستراتيجية الوطنية للأمن السيبراني والتي سبق وأن حددت اتجاهات و رؤية الأمن السيبراني في العراق ، والمتمثلة بمجتمع آمن ومضمون ومرن وموثوقية يحمي الأصول والمصالح الوطنية ويعزز التفاعلات والمشاركة الاستباقية في

الفضاء السيبراني بهدف تحقيق الرخاء الوطني بما يوفره من فرص ممتازة لتأمين وتنمية اقتصاد الدولة العراقية والعمل على تعزيز القدرات الوطنية في مجال الأمن السيبراني في العراق بصورة متناسقة ومستدامة من أجل التصدي أو التخفيف من المخاطر السيبرانية وتقليل حدتها كونها ذات تأثير بارز على الأمن القومي في العراق والعالم، بإعتبار أن الفضاء السيبراني أصبح هو المجال الرابع بعد الارض والبحر و الجو وفقا للاستراتيجية الوطنية.

-نوصي المشرع العراقي بضرورة تشريع قانون للأمن السيبراني يحدد ماهية الخطر السيبراني وأنواعه وشروطه، مع الأخذ بنظر الاعتبار ضرورة التعريف بالإجراءات الواجبة الإتباع لتحقيق الأمن السيبراني و أن يكون ذلك بلغة قانونية سلسة وواضحة خالية من الابهام والغموض، كون الأمن السيبراني من أبرز متطلبات عقد التأمين من المخاطر السيبرانية والذي يميزه عن سائر عقود التأمين من المخاطر التقليدية.

-نوصي المشرع العراقي بتشريع نصوص قانونية تلزم الشركات التجارية بالعمل وفقاً لإجراءات الأمن السيبراني والتي من المفترض النص عليها في القانون والعمل على وضع أساليب التشجيع و الردع اللازمة لحث الشركات التجارية على التعامل في بيئة تجارية آمنة.

-نوصي المشرع العراقي بعدم الاكتفاء بالقواعد العامة للتأمين الواردة في قواعد القانون المدني العراقي وتشريع قانون خاص بعقد التأمين من المخاطر السيبرانية لما له من خصوصية مقارنة بعقود التأمين التقليدية تجعل من الصعب الاكتفاء بالقواعد العامة.

-توفير بيئة قانونية مرنة وفاعلة في الوقت ذاته تبسط الإجراءات اللازمة لحماية الأنشطة التجارية التي تتم ممارستها في الفضاء السيبراني تهدف إلى حماية العملاء بالدرجة الأساس ومن ثم حماية الشركات التجارية ذاتها.

-أن تكون البنى التحتية للدول مناسبة للعمل في الفضاء السيبراني كتوفير الأجهزة المتطورة وخدمات الانترنت الفائقة السرعة، وتطوير أنظمة التشغيل للشركات التجارية بصورة تتلاءم والطبيعة المتطورة للمخاطر السيبرانية.

-نوصي بضرورة الأخذ بعين الاعتبار التنسيق بين التشريعات الوطنية المقترحة مع التشريعات الدولية ذات الصلة والعمل على توحيد المصطلحات القانونية الواردة فيها قدر الإمكان خصوصاً المصطلحات الحديثة منها لتجنب الوقوع في إشكالية الغموض التشريعي.

- -نوصي بضرورة عمل ندوات علمية لطلبة الكليات وموظفي دوائر الدولة عن المخاطر السيبرانية وأضرارها وطرق التقليل منها والتثقيف عن أهمية التأمين من المخاطر السيبرانية على اختلاف أنواعها.

-نوصي بضرورة إنشاء شركات متخصصة بالتأمين من المخاطر السيبرانية .

-العمل على ترسيخ ثقافة الأمن السيبراني والتأمين من المخاطر السيبرانية في الشركات التجارية.

المراجع:

١. أبي الفضل هاني بن فتحي، التأمين: أنواعه المعاصرة، ط ١ ، دار العصماء، دمشق، ٢٠٠٩ .

٢ – أحمد شرف الدين، أحكام التأمين، ط ٣ ، القاهرة، ١٩٩١ .

٣ – أشرف وفا محمد، الوسيط في القانون الدولي الخاص، ط ١ ، دار النهضة العربية، القاهرة،٢٠٠٩ .

٤ – باسم محمد صالح، القانون التجاري، القسم الأول، المكتبة القانونية، بغداد، بدون سنة نشر.

٥ – ثروت عبد الحميد، العقود المدنية المسماة، الكتاب الثالث، الاحكام العامة في عقد التأمين، بدون سنة نشر.

٦ – سالم رشدي سيد، التأمين: المبادئ والأسس والنظريات، ط ١ ، دار ال ا رية للنشر والتوزيع، عمان، ٢٠١٥ .

٧ – سلطان عبد الله محمود، عقود التجارة الإلكترونية والقانون الواجب التطبيق، ط ١ ، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠ .

٨ – شذى عبد جمعة موسى، التأمين على مخاطر انتهاك حقوق الملكية الفكرية الرقمية، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩ .

٩ – صدام فيصل كوكز، أتمتة التأمين والتأمين على مخاطر الفضاء الرقمي، دار الفكر الجامعي، الاسكندرية، ٢٠٢٣ .

١٠ – طارق عفيفي صادق، الخطر محل التأمين من المسؤولية في مجال المعلوماتية، ط ١ ، دار الحكمة للطباعة والنشر والتوزيع، القاهرة،

١١ – عباس العبودي، تنازع القوانين والاختصاص القضائي الدولي وتنفيذ الاحكام الاجنبية، دار السنهوري، بيروت، ٢٠١٥ .

١٢ – عبد الرزاق السنهوري، الوسيط في شرح القانون المدني الجديد، الجزء السابع، دار احياء التراث العربي، بيروت، بدون سنة نشر.

١٣ – علاء النجار حسانين، نطاق الالتزام بالسرية في التحكيم التجاري الدولي، دار التعليم الجامعي للنشر والتوزيع، الإسكندرية، ٢٠١٩ .

١٤ – علي أحمد شاكر وآخرون، تأمين المسؤولية المدنية، مركز جامعة القاهرة للتعليم المفتوح، القاهرة، ١٩٩٤ .

١٥ – علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة، ط ١ ، منشورات زين الحقوقية، بيروت، ٢٠١٣ .

١٦ – ماجد محمد سليمان، العقد الإلكتروني، ط ١ ، مكتبة الرشد، الرياض، ٢٠٠٩ .

١٧ – محمد حسين منصور، مبادئ قانون التأمين، دار الجامعة الجديدة للنشر، بدون سنة نشر.

١٨ – محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢ .

١٩ – محمد شرعان، الخطرفي عقد التأمين، منشأة المعارف، الاسكندرية، بدون سنة نشر.

٢٠– محمد عبد الظاهر حسين، عقد التأمين، دار النهضة العربية، القاهرة، ٢٠٠٣ .

٢١ – محمد غازي صابر، تأمين الحوادث، مركز جامعة القاهرة للتعليم المفتوح، القاهرة، ١٩٩٣ .

٢٢ – محمد محمد حسن، حماية المستهلك الالكتروني في القانون الدولي الخاص، دار النهضة العربية، القاهرة، ٢٠١٣ .