جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة ميسان / كلية القانون
الدراسات العليا / قسم القانون الخاص

الحماية التأمينية للشركات التجارية من المخاطر السيبرانية

رسالة تقدمت بها الطالبة:

أماني تموز عبد الرحمن الخفاجي

إلى:
مجلس كلية القانون /جامعة ميسان
كجزء من متطلبات نيل شهادة الماجستير في القانون الخاص

بإشراف:

أ. د. جعفر كاظم جبر

١٤٤٦ هـ ٢٠٢٤ م

بسم الله الرحمن الرحيم

﴿وَأَنفِقُوا فِي سَبِيلِ اللَّهِ وَلَا تُلْقُوا بِأَيْدِيكُمْ إِلَى التَّهْلُكَةِ وَأَحْسِنُوا إِنَّ اللَّهَ يُحِبُّ الْمُحْسِنِينَ﴾

صدق الله العلي العظيم

[سورة البقرة/١٩٥]

الإهداء:

- إلى روح والدي رحمه الله..

- إلى والدتي أدامها الله لي التي كانت ولا تزال مصدر إلهامي وقوتي وقد منحتني الحافز في كل خطوة ..

- إلى أخي وأخواتي الذين لطالما قدموا لي كل الدعم المعنوي والروحي والعاطفي..

- إلى عائلتي الصغيرة التي وهبتني كل الحب (زوجي العزيز وابنتي الغالية)..

- إلى الأصدقاء الذين شاركوني نصائحهم وشجعوني لإنجاز هذا البحث..

أهديكم جميعاً هذا الجهد المتواضع..

شكروعرفان

في البدء أود أن أشكر الله عز وجل على نعمهِ الدائمة وتوجيهه وحمايته لي ومنحي التوفيق لكتابة وإكمال الرسالة..

وأود أن أعبر عن خالص شكري وإمتناني إلى مشرفي العزيز الأستاذ الدكتور **جعفر كاظم جبر** عميد كلية القانون /جامعة ميسان حيث منحني من وقته الثمين وأمدني بالدعم والإرشاد وساعدني لإكمال هذه الدراسة فكان متفهماً لظروفي وكريماً في منحي كل ما احتاجه من ثروته العلمية..

كما أتوجه بالشكر والعرفان إلى أساتذتي الأفاضل من الكادر التدريسي في كلية القانون /جامعة ميسان إبتداءً من مرحلة البكالوريوس وإنتهاءً بالمرحلة التحضيرية لدراسة الماجستير على أمانتهم العلمية و حرصهم على تقديم الدعم العلمي و المعنوي لجميع الطلبة ..

وأتقدم بجزيل الشكر والإمتنان إلى موظفي كلية القانون/جامعة ميسان، وبالأخص موظفي مكتبة الكلية الذين لم يبخلوا في تقديم المساعدة لي ولجميع طلاب العلم، فكانوا خير مثال للموظفين الكفوئين.

الباحثة

المستخلص:

يعد توفير الحماية التأمينية للشركات التجارية ضد المخاطر السيبرانية وسيلة حديثة و ناجعة لإستيعاب الخسائر المالية الناجمة عن إنتهاك أمن أنظمة التشغيل، ذلك أن سوق التأمين بصوره عامة يميل إلى خلق العديد من الحوافز لبناء أنظمة أكثر أماناً لتلك الشركات، إلا أنه في الوقت ذاته لا يزال التأمين من المخاطر السيبرانية يكتنفه نوع من الغموض، نظراً لإنعدام التشريعات المتخصصة بهذا النوع من التأمين وقلة عدد الشركات التي تتعامل مع هذا النوع من التغطيات التأمينية، الأمر الذي يؤدي إلى تردد وحذر الشركات التجارية بصورة عامة من التأمين ضد المخاطر السيبرانية، لا سيما وأن هذه المخاطر لا تزال غير مقيدة بمعيار محدد وواضح، مما يؤدي أحياناً 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 التقليدية بجملة من المتطلبات التي قد تسبق او تواكب مرحلة إنعقاد 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 السيبرانية، فضلاً عن وجود جملة من التحديات القانونية والفنية التي أفرزها التعامل بهذا النوع الجديد من المخاطر غير الملموسة مما برر الحاجة لدراسة الحماية التأمينية للشركات التجارية من المخاطر السيبرانية.

المحتويات

المقدمة

المقدمة

أولاً: التعريف بموضوع الدراسة

أصبحت الشركات التجارية في الوقت الحالي أمام تحدي كبير للحفاظ على سرية معلوماتها وحماية بياناتها الشخصية وبيانات العملاء و أسرارها التجارية أمام الكم الهائل من المخاطر السيبرانية التي تهدد سلامة البيئة التجارية. ومهما كانت الشركات التجارية ممتثلة لإجراءات الأمن والسلامة السيبرانية إلا أن ذلك لا يعني إمكانية تجنب هذه المخاطر السيبرانية بصورة كلية، إذ لا تزال العديد من هذه المخاطر غير قابلة للسيطرة عليها كونها تمتاز بالتطور المستمر فمن غير الممكن تجنب وقوعها، إلا انه لا يزال بالإمكان التخفيف من الآثار المتخلفة عنها، ومن أجل السعي للتخفيف من حدة الآثار الناجمة عن المخاطر السيبرانية. وإدراكاً 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 (المخاطر السيبرانية)، أضحى تجنب هذا النوع من المخاطر في حد ذاته هدفاً طموحاً إلى حد كبير، نظراً لإعتماد الشركات التجارية حديثاً على التكنولوجيا الرقمية وانتشارها في التعاملات التجارية، وعلى الرغم من انه قد يكون بالامكان تجنب انواع محددة من المخاطر السيبرانية والقضاء عليها، إلا أنه لا تزال الشركات التجارية تواجه تحديات في كيفية تجنبها تماماً. قد يكون الخيار الاول الذي يتبادر إلى الذهن لتجنب هذا النوع من المخاطر هو الإمتناع 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 الانظمة الالكترونية المتصلة بالانترنت، مع الأخذ بنظر الإعتبار 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 أجزاء من الثانية لتحقق هذه الخسائر.

ومن هذا المنطلق ادركت الشركات التجارية أنها لا يمكن أن تحمي نفسها من جميع المخاطر السيبرانية طوال الوقت، وأنها بحاجة إلى إدارة هذه المخاطر و تحديد أولويات جديدة للشركة من خلال حماية البيانات سواء كانت بيانات الشركة أو بيانات العميل بالإضافة لحماية انظمة التشغيل والشبكات

التي تمارس من خلالها انشطتها التجارية خصوصاً أن الإحصائيات قد أشارت الى تصاعد وتيرة المخاطر 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 الإختراق أو التأمين من توقف الخدمة أو من القرصنة الإلكترونية للعمليات المصرفية على سبيل المثال، وما يستتبع ذلك من تحديات فنية وقانونية في تقدير مدى إحتمالية 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 الألكترونية والعملاء وأصحاب المصالح بصورة عامة. مما يدلل على حجم الأضرار المراد تغطيتها وما يستتبع ذلك من صعوبة تقدير الأقساط التأمينية ذلك أن المخاطر السيبرانية تمتاز بالحداثة والغموض والتطور المستمر وصعوبة التحقق من أن الخطر لا أرادي اي لم تتسبب فيه الشركة المؤمن لها، مما يصعب المهمة على شركات التأمين ذاتها نظراً لقلة التجارب السابقة، كون العديد من الشركات التي تعرضت للمخاطر السيبرانية تحجم عن ذكر حجم الضرر الذي تسببت به المخاطر السيبرانية 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.

ثانياً: أهمية موضوع الدراسة وأسباب إختياره:

تتجسد أهمية موضوع هذه الدراسة كونه يعالج موضوعاً يتعلق بحماية الشركات التجارية من مخاطر أضحت في وقتنا الحاضر تشكل تحدياً واضحاً لنشاط هذه الشركات، وخير دليل على ذلك تزايد الإهتمام – لا على المستوى المحلي فحسب بل على المستوى الدولي – بالتأمين من المخاطر 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، لاسيما وأن المخاطر السيبرانية لا يزال يكتنفها الغموض

بسبب طبيعتها المعقدة وتداخلها مع العديد من التخصصات العلمية كالهندسة والاقتصاد وعلوم الإدارة والعلوم السياسية، والذي يعد سبباً واضحاً للبحث في هذا الموضوع لا سيما مع انعدام التشريعات المنظمة للتأمين من المخاطر السيبرانية بشكل عام والخطر السيبراني بشكل خاص، بالتزامن مع توجه العديد من الدول ومنها العراق إلى طرح استراتيجيات وطنية تتعلق بالأمن السيبراني تشدد فيها على أهمية زيادة الوعي بهذه المخاطر.

ثالثاً: مشكلة الدراسة:

تكمن مشكلة موضوع الدراسة في غياب التنظيم التشريعي الخاص به 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 بالمخاطر السيبرانية؟ وما هي طبيعتها؟
- هل يخضع الخطر 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؟
- ما هو نطاق تعويض الأضرار الناجمة عن تحقق الخطر السيبراني سواء للشركة المؤمن لها أو الغير؟
- ما هي التحديات التي تواجه نمو سوق التأمين السيبراني؟
- ما مدى امكانية أن تشكل اللائحة الأوروبية لحماية البيانات النواة لتأطير التأمين من المخاطر السيبرانية بتشريعات خاصة؟

رابعاً: صعوبات الدراسة:

قلة وندرة الدراسات القانونية المتخصصة في هذا الموضوع على مستوى الفقه العراقي والفقه العربي. لذلك فقد تم الإعتماد بشكل كبير وأساسي على المصادر الأجنبية للفقه الفرنسي والإنكليزي

والأمريكي، وقد شكل هذا الأمر صعوبة بالغة بشأن الترجمة القانونية، فضلاً عن التكاليف المالية العالية لهذه الترجمة.

خامساً: منهجية الدراسة

في ظل غياب التنظيم القانوني للتأمين من المخاطر السيبرانية بشكل خاص فسوف نعتمد في دراستنا على كلا المنهجين: المنهج التأصيلي (الإستقرائي) والمنهج الإستنباطي. ومن خلالهما سيتم البحث في موضوع الدراسة وذلك عن طريق التعريف بالجزئيات وصولاً لتعريف الكليات ومن ثم العمل على تحليل النصوص القانونية ذات الصلة بما فيها من قواعد عامة للوصول إلى القواعد القانونية المنظمة لموضوع الدراسة فضلاً عن تحليل عدد من القرارات القضائية الحديثة ذات الصلة المباشرة بمحل البحث.

سادساً: هيكلية الدراسة

من خلال البحث في موضوع الحماية التأمينية للشركات التجارية من المخاطر السيبرانية ارتأينا تقسيمه الى فصلين، نتناول في الفصل الأول البحث في ماهية التأمين من المخاطر السيبرانية، حيث سنتناول في المبحث الأول منه مفهوم المخاطر السيبرانية، أما في المبحث الثاني فسنبحث في المفهوم القانوني لعقد التأمين من المخاطر السيبرانية. أما الفصل الثاني للدراسة فسيتم البحث في آثار عقد التأمين من المخاطر السيبرانية وتحدياته، وتم تقسيم الفصل الى مبحثين: نتناول في المبحث الأول منه آثارعقد التأمين من المخاطر السيبرانية، أما المبحث الثاني منه فسنتناول فيه تحديات التأمين من المخاطر السيبرانية ثم نختتم البحث بجملة من الإستنتاجات والمقترحات التي توصلنا إليها من خلال البحث في موضوع الدراسة.

الفصل الأول

ماهية التأمين من المخاطر السيبرانية

الفصل الأول

ماهية التأمين من المخاطر السيبرانية

تشكل الشركات التجارية بمختلف أنواعها ونشاطاتها هدفاً طبيعياً للمخاطر السيبرانية بسبب نشاطها الرقمي وإحتوائها على كم هائل من البيانات السرية والممتلكات غير المادية المخزنة في الفضاء السيبراني، في حين لا يزال مفهوم المخاطر السيبرانية يكتنفه بعض الغموض، على الرغم من وجود محاولات جدية لوضع تعريف دقيق له، وتحديد ماهيته لتجنب الخلط بينه وبين مصطلحات مشابهه له. ولا يمكننا انكار تأثر الشركات التجارية بالمخاطر السيبرانية على اختلاف أنواعها بسبب ممارسة النشاط التجاري في الفضاء السيبراني كونه وسط غير مادي يمتاز بقابليته للإختراق والتلاعب من قبل اي طرف ذي مصلحة، مما يلحق خسائر مادية ومعنوية جسيمة للشركات التجارية قد تكون في غنى عنها. ومن هنا شرعت بعض شركات التأمين بطرح نماذج عقود متخصصة بالتأمين من المخاطر السيبرانية، مع الأخذ بنظر الإعتبار أن تلك العقود لا تغطي جميع أنواع المخاطر السيبرانية، وانما تستثني شركات التأمين بعض المخاطر السيبرانية من شمولها بالتغطية. وبناء على ما تقدم سنبحث في ماهية التأمين من المخاطر السيبرانية من خلال تقسيم هذا الفصل إلى مبحثين: حيث نتناول في (المبحث الأول) **مفهوم المخاطر السيبرانية**، أما (المبحث الثاني) فسنتناول فيه **المفهوم القانوني لعقد التأمين من المخاطر السيبرانية**.

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 المخاطر السيبرانية، وبما أن الخطر يشكل جوهر التأمين فلا بدّ من بيان تعريف هذا النوع الحديث من المخاطر وتمييزه عما يشتبه به جهة، ومن ثم بيان أنواع المخاطر السيبرانية وأثرها على الشركات التجارية من جهة أخرى. عليه سوف نقسم هذا المبحث إلى مطلبين، حيث نخصص **(المطلب الأول)** للتعريف بالخطر السيبراني وتمييزه عما يشتبه به، أما في **(المطلب الثاني)** سنتناول أنواع الخطر السيبراني وأثره على الشركات التجارية.

المطلب الأول

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[١]. 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 الاوساط 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. عليه سوف نتناول **تعريف الخطر السيبراني** في (مطلبٍ أول)، ومن ثم **تمييز الخطر السيبراني عما يشتبه به** في (مطلبٍ ثانٍ).

(١) محمد شرعان، الخطر في عقد التأمين، منشأة المعارف، الاسكندرية، بدون سنة نشر، ص٨.

الفرع الأول

تعريف الخطر السيبراني

أولاً: الخطر السيبراني (لغةً)

الخَطَرُ في اللغة هو (اسم) يأتي بعدة معاني منها: الإشراف على الهلاك [١] [٢]، ويأتي بمعنى: الرِّهان، العِوَضُ والجمع: أَخطارٌ [٣].

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)[٤]. فيقال فضاء سيبراني أي: فضاء كمبيوتري[٥] كما يأتي بمعنى تخيلي أو شبكي أو ما يقع ضمن الفضاء الرقمي[٦]، 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[٧]. و يعد 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[٨].

---

(١) محمد بن ابي بكر الرازي، مختار الصحاح، دار الكتاب العربي بدون سنة نشر، بيروت، ص ٩٧.

(٢) أحمد مختار عمر، معجم اللغة العربية المعاصرة، المجلد الأول، ط١، عالم الكتب للنشر والتوزيع، القاهرة، ٢٠٠٨، ص٦٦١.

(٣) إبراهيم أنيس وآخرون، المعجم الوسيط، ط٤، الناشر: مجمع اللغة العربية – مكتبة الشروق الدولية، القاهرة، ٢٠٠٤، ص٢٤٣.

(٤) انظر: منير البعلبكي و رمزي منير، قاموس المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩، ص٣٠٧.

(٥) انظر: علي محمد الموسوي، المشاركة المباشرة في الهجمات السيبرانية، رسالة ماجستير مقدمة إلى مجلس كلية الحقوق – جامعة النهرين، ٢٠١٧، ص٨.

(٦) انظر: معجم المعاني الجامع (www. almaany.com)، تاريخ الزيارة ٢٠٢٢/٨/١٢ الساعة ٣:٠٠م.

(٧) معجم المصطلحات السيبرانية https://www.dictionary.com/browse/cyber تاريخ الزيارة ٢٠٢٢/٨/١٢ الساعة ٤:٠٠ م.

(8) Wiener, Norbert: Cybernetics or Control and Communication in The Animal and The Machine, M.I.T، Press, Second Edition, Cambridge, Massachusetts, 1948, p144.

إنّ انعدام وجود مصطلح مناظر في اللغة العربية شكل تحدياً للمختصين العرب لإختيار 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 كالقرار رقم (٥٧/٢٣٩) والذي يتمحور حول إنشاء ثقافة عالمية للأمن السيبراني[١].

ومن هنا تم اعتماد هذا المصطلح في الدول العربية ومنها العراق والسعودية والمغرب وقطر وتونس والبحرين، حيث تم إنشاء هيئات متخصصة مثل (الهيئة الوطنية للأمن السيبراني) في المملكة العربية السعودية [٢]، و (المركز الوطني للأمن السيبراني) في الأردن[٣]. وفي العراق صدر عن مستشارية الأمن الوطني / أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات (**إستراتيجية الأمن السيبراني العراقي لسنة ٢٠٢٢**)[٤] وهذا دلالة على اعتماد الترجمة الواردة في وثائق الأمم المتحدة لمصطلح (cyber) محل البحث. وبناء على ما تقدم نستنتج أن الخطر السيبراني لغةً يأتي بمعنى الخطر (الرقمي – الإلكتروني) أو (التخيلي) أو (الشبكي)، أي أنه يشير إلى كل خطر يقع في فضاء غير ملموس مادياً أي أنه يتم ضمن فضاء رقمي ذي تحكم آلي.

وقبل وجود مصطلح الأمن السيبراني، كان هناك علم التحكم الآلي .في أواخر الأربعينيات من القرن الماضي، الذي ظهر كدراسة لأنظمة التحكم والاتصالات بين الأشخاص والآلات. وتطورت بعد ذلك إلى نهج متعدد التخصصات، وعلم التحكم الآلي مشتق من الكلمة اليونانية

---

(١) زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير مقدمة إلى كلية القانون/ جامعة الكوفة، ٢٠١٦، ص٨.

(٢) الموقع الرسمي للهيئة الوطنية للأمن السيبراني السعودي: nca.gov.sa
تاريخ الزيارة ٢٠٢٢/١٢/٤ الساعة ٧:٣٠ م.

(٣) الموقع الرسمي للمركز الوطني للأمن السيبراني الأردني: ncsc.jo
تاريخ الزيارة ٢٠٢٢/١٢/٤ الساعة ٧:٣٠ م.

(٤) تتألف استراتيجية الامن السيبراني الوطنية من استراتيجيات قصيرة ومتوسطة وطويلة الامد تعنى بمعالجة التعرض الوطني للمخاطر السيبرانية التي تقع في الفضاء السيبراني والذي هو عبارة عن شبكة مترابطة من الهياكل الاساسية للمعلومات الحرجة وغير الحرجة ويشمل جميع اشكال التدخلات الرقمية وهو فضاء ذي قدرة هائلة على سد الفجوات في التنقل والتجارة والابتكارات والتعليم والحد من الفقر والتمكين الاقتصادي نظر استراتيجية الامن السيبراني العراقي انظر:
https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf
تاريخ الزيارة ٢٠٢٢/١٢/٤ الساعة ٧:٣٠

(**kubernētēs**)، والتي تشير إلى طيار أو قائد وهي ذات صلة بالكلمة اليونانية(**kubernēsis**) والتي تعني "هبة التحكم" وتنطبق على القيادة ؛ نظراً لأن دراسة علم التحكم الآلي تشمل مجالات علوم الكمبيوتر والهندسة والبيولوجيا وتطوراتها[١]. والسيبرانية بوصفها مصطلحاً جديداً، فقد اشتقت العديد من المصطلحات منه لوصف كل شيء، ابتداء من وظائف الإنترنت وانتهاءً بوصف أنواع الجرائم. التي أصبحت شائعة الاستخدام كمصطلحي ((الفضاء السيبراني)) و((الأمن السيبراني)). حيث ان مصطلح الفضاء السيبراني يشير 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 والبرامجيات و أجهزة الحاسب الآلي ومعطيات النقل والتحكم الرقمي وغيرها فهو بيئة تفاعلية حديثة تعد من المنظور العسكري بمثابة الذراع الرابعة للجيوش في وقتنا الحاضر[٢]. 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 الإهتمام 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 [٣].

ثانياً: الخطر السيبراني اصطلاحاً

تعد مهمة وضع تعريف منهجي و شامل ودقيق للخطر السيبراني بمثابة نقطة الانطلاق أو الأساس الذي سيبنى عليه البحث في تأمين الشركات التجارية من المخاطر السيبرانية، ولا يخلو هذا الأمر من صعوبة كون الخطر السيبراني هو مصطلح واسع الإستخدام وله تعريفات عديدة، وسبب ذلك هو تداخله في العديد من التخصصات العلمية والإنسانية، فمفهوم المخاطر السيبرانية يستخدم في علوم الكمبيوتر والهندسة وإدارة الأعمال والاقتصاد والعلوم الانسانية، فضلاً عن ذلك فإن تنوع هذه المخاطر وطبيعتها المتغيرة تجعل مهمة وضع تعريف موحد وشامل له لا يخلو من الصعوبة والتعقيد. حيث يتميز الخطر

(١) زهراء عماد محمد، مصدر سابق، ص٧.

(٢) هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية مجلة مصر المعاصرة المجلد (١١٤)، العدد، (٥٤٩)، ٢٠٢٣، ص٤٧٠.

(٣) هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي،مجلة كلية الاقتصاد والعلوم السياسية، المجلد (٢٤)، العدد (١)، الرقم المسلسل للعدد ٩٤، ٢٠٢٣، ص١٩٠.

السيبراني بكونه يجمع بين جانبين: الجانب الفني و الجانب الاقتصادي، فمن الناحية الفنية نجد أن المخاطر السيبرانية تتمتع بتقنية عالية و تصميم معقد يتعلق ببرمجة المكونات المتصلة بالشبكة، أما الجانب الاقتصادي فيتعلق بقوة تأثير الخطر السيبراني على الجوانب المالية للأشخاص الطبيعية والمعنوية على حد سواء[١].

وعلى الرغم من الإشارة إلى المخاطر السيبرانية في العديد من الدراسات القانونية والعلمية وكونها نقطة الإهتمام المركزية في الأوراق البحثية إلا أنه لم يتم تحديد ماهية هذه المخاطر بصورة دقيقة وكافية لتزيل الغموض الذي يكتنف هذا المصطلح.

عليه يجب إبتداءً أن نضع في نظر الإعتبار نقطة أساسية ألا وهي أن جميع التعاريف المقترحة للخطر السيبراني لا تكاد تخلو من أحد هذه الجوانب الثلاثة: (مصدر الخطر، موضوع الخطر، الأثر المترتب على وقوع الخطر). وعلى هذا الأساس انقسم الفقهاء والباحثون في هذا المجال عند تعريفهم للخطر السيبراني إلى ثلاثة اقسام:

القسم الأول: قد تناول تعريف الخطر السيبراني من منظور يمكن وصفه بأنه **أحادي الجانب**، أي من خلال الإشارة إلى جانب واحد فقط من الجوانب الثلاثة سالفة الذكر (المصدر، الموضوع، الأثر)[٢]. من ذلك المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة الامريكية (NIST)[٣] حيث عرف الخطر السيبراني على أنه: كل خطر يؤثر على العمليات

(1) Grzegorz Strupczewski, Defining cyber risk, Safety Science, Volume (135), 2021, 105143, ISSN 0925-7535, p1.

(2) Grzegorz Strupczewski, Ibid, p2.

(٣) تأسس المعهد الوطني للمعايير والتكنولوجيا (NIST) في عام ١٩٠١ وهو جزء من وزارة التجارة الأمريكية، وهو أحد أقدم مختبرات العلوم الفيزيائية في البلاد. أنشأه الكونجرس لإزالة التحدي الرئيسي الذي كان يواجه القدرة التنافسية الصناعية للولايات المتحدة في ذلك الوقت، وهو البنية التحتية للقياس من الدرجة الثانية التي تخلفت عن قدرات المملكة المتحدة وألمانيا وغيرهما من المنافسين الاقتصاديين، من شبكة الطاقة الكهربائية الذكية والسجلات الصحية الإلكترونية إلى الساعات الذرية والمواد النانوية المتقدمة ورقائق الكمبيوتر، تعتمد منتجات وخدمات لا حصر لها بطريقة ما على التكنولوجيا والقياس والمعايير التي يقدمها المعهد الوطني للمعايير والتكنولوجيا. تدعم قياسات NIST أصغر التقنيات إلى أكبر الابتكارات التي صنعها الإنسان وأكثرها تعقيدًا – بدءًا من الأجهزة النانوية الصغيرة جدًا بحيث يمكن وضع عشرات الآلاف منها في نهاية شعرة بشرية واحدة وحتى ناطحات السحاب المقاومة للزلازل وشبكات الاتصالات العالمية، وتعتبر شركة ذات مهمة حيث تسعى لتعزيز الابتكار والقدرة التنافسية الصناعية في الولايات المتحدة من=

التنظيمية كالنشاطات أو السمعة أو الأصول أو الأفراد، و الناتج عن تشغيل نظام المعلومات، وذلك وفقاً لأثر التهديد واحتماله[١]. وعلى الرغم من أن التعريف قد تناول الأثر المترتب على وقوع الخطر السيبراني إلا أنه يفتقر إلى الشمولية حيث لم يتطرق إلى ذكر مصدر الخطر أو موضوعه.

وهناك من عرفه على أنه: الخطر الناجم عن خطر إلكتروني يحدث في الفضاء الإلكتروني[٢]. ونلاحظ أن هذا الجانب من الفقه قد إستند في تعريفه للخطر السيبراني من خلال بيان مصدره لكن يؤاخذ عليه أنه تعريف مقتضب حيث إنه لم يوضح معنى الخطر السيبراني واكتفى بجعله مصطلحاً مرادفاً للخطر الالكتروني مما زاد التعريف غموضاً.

في حين عرفه البعض على أنه: الضرر المادي المحتمل (للأشخاص أو الممتلكات) وفقدان الأرباح بسبب خلل النظم الرقمية أو البيانات التالفة[٣]. وفي اعتقادنا أن هذا التعريف لا يخلو من النقد حيث إن فقدان الارباح يقع ضمن فئة الأضرار المادية فلا حاجة لذكرها منفردة، كما أن تعريف الخطر السيبراني من حيث الأثر المترتب على وقوعه من دون بيان مصدره أو المكونات التي يقع عليها أمر غير دقيق.

وقد تم تعريفه من قبل البعض على أنه خرق نزاهة وفشل أنظمة تكنولوجيا المعلومات والاتصالات[٤]. ويؤخذ على هذا التعريف المآخذ الواردة على سابقه.

=خلال تطوير علوم القياس والمعايير والتكنولوجيا بطرق تعزز الأمن الاقتصادي وتحسن نوعية الحياة. للمزيد أنظر: https://www.nist.gov/about-nist

تاريخ الزيارة ٢٠٢٤/٥/١٠ الساعة ٢:١٨ ص.

(1) NIST, Minimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2006, p8.

(2) Refsdal, A., Solhaug, B., Stolen, K. Cyber-risk Management. Springer briefs in computer scince, 2015, P33.

(3) Nieuwesteeg, B., Visscher, L., de Waard, B., 2015. The law & economics of cyber insurance contracts: a case study, European Review of Private Law, Volume (26), Issue (3), 2018, p3.

(4) Böhme, Rainer and Gaurav Kataria. "Models and Measures for Correlation in Cyber-Insurance." Workshop on the Economics of Information Security", University of Cambridge, UK, England, June 2006.

أما **القسم الثاني** من الفقهاء فقد عرّفوا الخطر السيبراني تعريفاً **ثنائي الجانب** أي أنهم قد أشاروا إلى جانبين فقط من الجوانب الثلاثة (المصدر، الموضوع، الأثر)، فقد عرف البعض المخاطر السيبرانية تعني بأنها أي خطر من الخسارة المالية أو الاضطراب 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: (١) الخرق المتعمد وغير المصرح به للوصول إلى نظم المعلومات لأغراض التجسس أو الابتزاز أو الإحراج (٢) الخرق غير المقصود أو العرضي للأمن، والذي قد لا يزال يشكل مع ذلك تهديداً يحتاج إلى معالجة (٣) الخرق التشغيلي [١]. إن ما يميز هذا التعريف هو أنه ينظر للخطر السيبراني من جهة مصدره والأثر المترتب على وقوعه، فضلاً عن أنه لم يقتصر على ذكر الاضرار المادية كأثر ناتج على تحقق الخطر مدار البحث بل اشار للأضرار المعنوية كالاضطرابات وتلك التي تلحق بالسمعة حتى وان ترتب عليها فيما بعد ضرر مادي. الا انه اختص المنظمات بالذكر دون الافراد مما أدى بالتعريف إلى افتقاره العمومية حسب اعتقادنا.

وقد عرّف آخرون المخاطر السيبرانية بأنها مخاطر تشغيلية لأصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية أو توافر أو سلامة المعلومات أو نظم المعلومات[٢]، ويتضح لنا أن هذا التعريف قد أشار إلى موضوع الخطر وتأثيره إلا أنه لم يتطرق بالذكر إلى مصدر هذا الخطر.

وعرّف 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[٣]. وهذا التعريف حسب اعتقادنا قد قصر نطاق وقوع الاخطار السيبرانية على العمل التجاري وهذا الأمر غير صائب كون المخاطر

(1) (IRM) organization, Cyber Risk. Resources for Practitioners The Institute of Risk Management 2014, p10.

(2) Cebula, J.J. and Young, L.RA, Taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN- 028, Software Engineering Institute, Carnegie Mellon University, (2010), p13.

(3) ISACA. The Risk IT framework, Information Systems Audit and Control Association, 2009, p7.

السيبرانية تطال الأعمال التجارية وغير التجارية على حد سواء، كما أنه خص الشركات بالذكر وعلى سبيل الحصر دون ذكر الأفراد الطبيعية والمعنوية الأخرى.

وعرّف البعض الآخر المخاطر السيبرانية على أنها المخاطر التي ينطوي عليها حدث إلكتروني ضار يتسبب في تعطيل الأعمال التجارية والخسارة النقدية[١].يتضح لنا أن هذا التعريف قد أشار إلى الحدث الإلكتروني كدلالة على مصدر الخطر وإلى تعطيل الاعمال التجارية والنقدية كدلالة على الأثر المترتب على وقوعه، لكنه لم يشير إلى المكونات التي يقع عليها الخطر، فضلاً عن أنه بين تأثير الخطر على الأعمال التجارية حصراً وما يلحقها من خسارة نقدية، بينما يؤثر الخطر السيبراني على الاعمال التجارية وغير التجارية مسبباً خسائر قد تكون مادية أو معنوية أو كلاهما.

وإزاء ما ذكره الاتجاهان السابقان حاول بعض الفقه وضع تعريف متكامل للخطر السيبراني من خلال ذكر مصدره وموضوعه والأثر المترتب على وقوعه لتلافي القصور الوارد في التعريفات الفقهية السابقة، حيث عرف الخطر السيبراني تعريفاً **شاملاً** عن طريق الإشارة إلى مصدره وموضوعة والأثر المترتب على وقوعه فتم تعريفه بأنه "أي خطر ناشئ عن استخدام تكنولوجيا المعلومات والاتصالات ويضر بسرية البيانات أو الخدمات أو توافرها أو سلامتها ويؤدي إلى ضعف التكنولوجيا التشغيلية وتعطيل الأعمال، وانهيار البنية التحتية، والأضرار المادية التي تلحق بالبشر والممتلكات. وينجم خطر الإنترنت إما عن الكوارث الطبيعية أو من صنع الإنسان كالفشل البشري أو الجريمة السيبرانية (مثل الابتزاز أو الاحتيال) أو الحرب الإلكترونية أو الإرهاب السيبراني، ويتميز بالأحداث المتطرفة المحتملة، وعدم اليقين الشديد فيما يتعلق بنهج البيانات والنمذجة، وخطر التغيير[٢].

ويتميز هذا التعريف بكونه أحاط بمفهوم الخطر السيبراني من جميع جوانبه، حيث ذكر كلاً من مصادر الخطر والمكونات التي يقع عليها والآثار المترتبة على وقوعه بصوره مفصلة ومتسلسلة ومع

(1) Mukhopadhyay, Arunabha, Chatterjee, Samir, Saha, Debashis, Mahanti, Ambuj, Sadhukhan, Samir K, Cyber-risk decision models: to insure IT or not?, Decision Support Systems 56(1), 2013, p11.

(2) Eling, M., Schnell, W, Ten key questions on cyber risk and cyber risk insurance, Technical Report, The Geneva Association organization, Zurich. (2016), p12.

ذلك نعتقد أن هذا التعريف كان مطولاً بسبب ذكر بعض الأمثلة والمميزات ضمن منطوق التعريف من جهة، فضلاً عن أنه قد أغفل ذكر الأضرار المعنوية واكتفى بذكر الأضرار المادية من جهة أخرى.

وهناك من عرّف المخاطر السيبرانية بأنها "مخاطر عدم الإمتثال للمتطلبات التنظيمية والقانونية نتيجةً لعدم الإمتثال للحماية الإلكترونية"[١]، حيث يشير مصطلح الخطر السيبراني إلى المخاطر المرتبطة بالتكنولوجيا أو معلومات الشبكة، ولا نعتقد بدقة هذا التعريف كون الخطر السيبراني قد يقع حتى في حالة الإمتثال للحماية الإلكترونية ؛لأنه لا يمكن توفير حصانة من التهديدات الإلكترونية بصورة مطلقة.

كما تم تعريف المخاطر السيبرانية وفقاً للمفهوم الشامل بأنها "مخاطر تشغيلية تتمثل بفقدان البيانات أو تعطل تكنولوجيا المعلومات والاتصالات الذي يؤثر على سرية أو توافر أمن و سلامة المعلومات"[٢]. والملاحظ على هذا التعريف أنه مقتضب، حيث لم يحدد ماهية الخطر السيبراني بصورة دقيقة بل اكتفى بذكر بعض صوره والآثار المترتبة عليها.

وعرفت المخاطر السيبرانية كذلك بأنها "أعمال عدائية يمكن أن تمارس ضد النظام فيتناول أمن الشبكات وأمن الانترنت من ناحيتين، الأولى هي البنى التحتية وما تحويه من نقاط دخول وخروج وتخزين واعتراض بيانات والناحية الأخرى تتناول عمليات التخريب والتعطيل والتدمير التي تطال الأموال والأشخاص من خلالها مما يؤدي إلى توقف النظام عن اداء الخدمات التي كان يقدمها أو تعرض أسرار المؤسسات أو الافراد للخطر أو يؤدي إلى تلف البيانات الحساسة و بث معلومات مغلوطة[٣] . وعلى الرغم من أن التعريف سالف الذكر قد أسهب في بيان صور الخطر السيبراني والنتائج المترتبة على وقوعه إلا انه لم يكن موفقاً في إيضاح ماهية الخطر السيبراني.

(1) Simon Holtz, Patrick Dummermuth, Simon Künzler, Melanie Koller, nadine janser, cyber risk and insurance updated 3rd edition, (2021), p9.

(٢) حنين جميل ابو حسين، الاطار القانوني لخدمات الامن السيبراني، رسالة ماجستير مقدمة إلى كلية الحقوق، جامعة الشرق الاوسط، ٢٠٢١، ص١٩.

(٣) هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الاحمر، مجلد (٩٤)، ٢٠١٢، ص٥١٨.

وتجدر الإشارة إلى أن البعض قد جعل المخاطر السيبرانية فئة فرعية من المخاطر الإلكترونية وعرّفها بأنها "المخاطر الناجمة عن استخدام الإنترنت والاجهزة المتصلة به"[١]، وعلى الرغم من بيان التعريف للوسيلة التي تؤدي لحدوث الخطر إلا أنه لم يحدد طبيعته وآثاره بدقة حيث جاء مقتضباً . وهناك من عرّفها بأنها "هجوم عبر الانترنت يقوم على التسلل إلى المواقع الإلكترونية غير المرخص بدخولها بهدف تعطيل أو إتلاف البيانات المتوفرة فيها او الإستحواذ عليها ، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد اخرى"[٢] . ومما يحسب لهذا التعريف حسب إعتقادنا أنه قد أوضح الوسط الذي يتم فيه حدوث الخطر السيبراني، إلا أنه غير دقيق كونه قد ضيق من نطاق الاخطار السيبرانية إلى الحد الذي جعلها تقتصر على الهجمات التي تتم من خلال التسلل إلى المواقع الإلكترونية على هيئة حروب الكترونية دولية بينما الخطر السيبراني يتضمن معنى اوسع من ذلك يكاد يشمل اي إعتداء غير ملموس مادياً يتم عبر الفضاء السيبراني.

وعلى الصعيد الدولي نجد ان مجلس الاستقرار المالي (Financial Stability Board)[٣] قد عرّف الخطر السيبراني بأنه "كل ما يهدد نظام المعلومات التي يعالجها النظام او ينقلها او يخزنها او ينتهك إجراءات الأمان أو سياسات الإستخدام المقبولة قانوناً سواء كان ناتجا عن نشاط ضار أم لا "، وبإعتقادنا أن التعريف آنف الذكر قد حدد طبيعة الخطر إلا أنه لم يحدد مصدره أو الوسط الذي ينحصر فيه و **استخدم مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا (UNODC)** مصطلح السيبرانية مرادفاً لمصطلح (الإلكترونية) و اعتبر الجرائم السيبرانية شكل متطور من أشكال الجريمة عبر الوطنية ونوع من أنواع الجريمة المنظمة ذات طابع معقد والتي تحدث في مجال الفضاء الإلكتروني الذي لا حدود له. ويمكن لمرتكبي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة، ويمكن أن تمتد آثار الجريمة عبر المجتمعات في جميع

(1) Pojištění kybernetických rizik. Autor diplomové práce: Bc. Jan Linert. Vedoucí diplomové práce: prof. Ing. Eva Ducháčková VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. Fakulta financí a účetnictví, CSc. Rok obhajoby: 2019, p3.

(٢) شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، مجلد (١٧)، العدد الاول، ٢٠٢٠، ص٧٤١.

(٣) وهي هيئة دولية تراقب وتقدم توصيات حول النظام المالي العالمي تم تأسيسها بعد قمة مجموعة العشرين في لندن في ابريل ٢٠٠٩ كخليفة لمنتدى الاستقرار المالي ومقره في بازل، سويسرا. انظر: www.fsb.org تاريخ الزيارة ٢٠٢٢/١٢/٤ الساعة ٨:٣٠م.

أنحاء العالم، مما يبرز الحاجة الي وضع استجابة عاجلة وديناميكية ودولية[١] ونلاحظ أن ال **(UNODC)** لم يعرّف الخطر السيبراني ولم يحدد ماهيته وانما قد أعطى مفهوماً للجريمة السيبرانية التي تندرج تحت مفهوم المخاطر السيبرانية.

في حين عرفت اللجنة الدولية للصليب الأحمر الخطر السيبراني بأنه "استخدام أنشطة متعمدة لإفساد أو خداع أو تغيير أو إضعاف أو تدمير أنظمة أو شبكة الحاسوب أو المعلومات أو البرامج المدرجة في هذه الأنظمة أو الشبكات والتي ترسل من خلالها وتؤثر هذه الانشطة في الكيانات المرتبطة بهذه الأنظمة أو الشبكات "[١]. ويؤخذ على هذا التعريف أنه حصر الخطر السيبراني بالسلوك المتعمد (الإرادي) في حين أن الخطر مدار البحث قد يكون غير متعمد وإنما ناجم عن خلل تقني أو إهمال على سبيل المثال فيؤدي بدوره إلى حدوث الخطر السيبراني. أما بالنسبة **للجمعية الدولية لمشرفي التأمين (IAIS)**[٢] فقد عرّفت الخطر السيبراني بأنه "اي خطر ناجم عن استخدام البيانات الإلكترونية ونقلها بما في ذلك أدوات التكنولوجيا مثل الإنترنت وشبكات الإتصال، كما يشمل الأضرار المادية التي تسببها حوادث الأمن السيبراني والإحتيال المرتكب عن طريق اساءة استخدام البيانات وأي مسؤولية تنشأ عن تخزين البيانات والمعلومات الالكترونية وسلامتها و سريتها سواء متعلقة بالأفراد أو الجماعات أو الحكومات"[٣]. وفي اعتقادنا أن ما يميز تعريف الجمعية الدولية سابق الذكر أنه قد

---

(١) (UNODC): مكتب الأمم المتحدة المعني بالمخدرات والجريمة، وهو تنظيم يهدف إلى جعل العالم آمن من المخدرات والجريمة المنظمة والفساد والإرهاب. ويلتزم بتحقيق الصحة والأمن والعدالة للجميع من خلال معالجة هذه التهديدات وتعزيز السلام والرفاهية المستدامة كرادع لها. ويقدم مساعدة عملية ويشجع مناهج العمل عبر الوطنية. انظر الموقع الرسمي للمكتب:

www.unodc.org/romena/en/cybercrime.html

تاريخ الزيارة ٢٠٢٢/٨/١٤ الساعة ٣:٣٠م.

(٢) هي هيئة عالمية مسؤولة عن التطوير والمساعدة في تنفيذ المبادئ والمعايير والإرشادات و المواد الداعمة للإشراف على قطاع التأمين. تأسست سنة ١٩٩٤ بالإضافة إلى ذلك، وتلعب دورًا اشرافيًا في معالجة المخاطر والتحديات الناشئة. عن الابتكار التكنولوجي (بما في ذلك الرقمي)، والمخاطر السيبرانية، ومخاطر المناخ، والسلوك والثقافة، والشمول المالي، والتنمية الاقتصادية المستدامة والتنوع، والمساواة للمزيد انظر: الموقع الرسمي للهيئة www.iaisweb.orgm تاريخ الزيارة ٢٠٢٢/١٢/٤ الساعة ٨:٤٠ م

(3) cyber risk for insurance،challenges and opportunities، Luxembourg: Publications Office of the European Union, 2019. p7.
https://register.eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf
date of visit 12/5/2024 6:30 pm

احاط بمفهوم الخطر السيبراني إلا أنه كان من الأفضل تحديد مفهوم الخطر بطريقة نبتعد فيها عن الإطالة في تعريفه. وعلى الرغم من إختلاف تعريف الخطر السيبراني في التعاريف السابقة إلا أنه لا يمكن إنكار بأن هذا الاختلاف ناجم عن اختلاف الزاوية التي تم النظر من خلالها للمصطلح وفقاً للتوجهات التي تتبناها الجهة التي صدر منها التعريف سواء كانت من المنظمات الدولية أو الفقهاء ، ويتفق الباحث مع تعريف **الجمعية الدولية لمشرفي التأمين (IAIS)** سالف الذكر كونه تعريفاً دقيقاً وشاملاً لأي خطر ناجم عن استخدام البيانات الالكترونية، كما يشمل الاضرار المادية التي تسببها حوادث الأمن السيبراني وأي مسؤولية تنشأ عنها سواء كانت متعلقة بالأفراد أو الجماعات أو الحكومات.

وبناء على ما سبق يمكن تعريف الخطر السيبراني بأنه: **كل خطر يقع في الفضاء السيبراني ينجم عن اعتداء غير ملموس مادياً على أنظمة المعلومات بغض النظر عن الأشخاص المستهدفة أو نوع الضرر أو الغاية من الإعتداء مخلفاً أضراراً مادية ومعنوية هائلة.**

الفرع الثاني

تمييز الخطر السيبراني عما يشتبه به

على الرغم من أن السيبرانية كمصطلح قائم بذاته لها مدلول واضح لدى الباحثين في هذا المجال، إلا أن الفقهاء كانوا قد اختلفوا في مدى إمكانية اعتبار المخاطر السيبرانية هي ذاتها الهجمات السيبرانية، أم أنها مجموعة جرائم سيبرانية، أم انها ذات مدلول عام قائم بذاته.

وتظهر الفائدة من التمييز بين هذه المصطلحات بإعتقادنا نظراً لحداثتها وإمكانية حدوث خلط فيما بينها من قبل بعض الباحثين أو حتى المنظمات والهيئات الدولية كونها للوهلة الأولى تبدو مترادفة. فعلى الرغم من أن كلاً من الخطر السيبراني والهجوم السيبراني والجريمة السيبرانية مشتركين في وسط واحد وهو الفضاء السيبراني، وينتج عنهم نوعين من الأضرار: المادية والمعنوية، كما أنهم يستهدفون بصور مباشرة أو غير مباشرة الاشخاص الطبيعية والمعنوية على حد سواء ومن خلال الأساليب الإحتيالية ذاتها، لكن الأمر يستدعي أولاً ضرورة بيان مفهوم كل من الهجمات السيبرانية والجرائم السيبرانية للوصول إلى التمييز بينها وبين المخاطر السيبرانية مدار البحث.

أولاً: مفهوم الهجمات السيبرانية:

نظراً لحداثة مصطلح الهجوم السيبراني، لذا فإن الفقهاء القانونيين حاولوا وضع تعريف يحدد ماهيته ويزيل عنه اللبس والغموض. ذلك أن بيان مفهوم الهجمات السيبرانية أمر ضروري للتحليل القانوني بل أنه من الواجب بيان هذا المفهوم كون الدراسات القانونية التي تعرضت لمفهوم الهجمات السيبرانية تستخدم غالبا مصطلح الهجوم السيبراني (cyber attack)، والجريمة السيبرانية (cyber crime) كمترادفين مع عدم التركيز على اختلاف كل مصطلح منهما عن المصطلح الآخر، وإن انعدام وجود تعريف محدد للهجوم السيبراني يجعل من الصعب وضع توصيات منسقة أو إتفاق دولي حول مبادئ موحدة للتعامل مع الآثار الناشئة عن هذه الكوارث[١] فضلاً عن أن التطور الهائل في البرامج وتقنيات الحاسوب وضعف التشريعات العقابية أو إنعدامها قد ينبئ بخطورة هذه الهجمات وضرورة الحد منها ولا يمكن ذلك من دون ايضاح مفهوم هذه الهجمات بصورة كافية[٢].

تجدر الإشارة ان معظم التعريفات التي وردت بشأن تحديد ماهية الهجمات السيبرانية تشترك في معنى متقارب وهو هجوم عبر الفضاء السيبراني بهدف السيطرة على مواقع إلكترونية معينة لتعطيلها وتدميرها أو الإضرار بها، وأن المختصين في مجال القانون الدولي العام يقرون بأن المصطلح قد يكتنفه نوع من الغموض والإلتباس بسبب عدم وضع تعريف موحد له[٣].

فقد عرّف البعض الهجوم السيبراني بأنه "مجموعة من الإجراءات الصادرة عن الدولة أو إحدى مؤسساتها بهدف إضعاف الوظيفة التي تقوم بها أجهزة الحاسوب المستهدفة للدولة المعادية"[٤].

وفي المعنى ذاته عرّفها البعض الآخر من الفقهاء بأنها هجوم عبر الانترنت من خلال التسلل إلى مواقع الكترونية غير مرخص الدخول إليها لغرض إتلاف أو تعطيل أو تغيير البيانات أو الإستحواذ عليها وتتم في مواجهة دولة ضد أخرى. وذهبت المستشارة القانونية في اللجنة الدولية

---

(١) زهراء عماد محمد، مصدر سابق، ص ٨ وما بعدها.

(٢) علي فاضل علي سليمان، حق الدفاع الشرعي عن الهجمات السيبرانية، مجلة جامعة تكريت للحقوق السنة (٤) المجلد (٤) العدد (٤) الجزء الأول، ٢٠٢٠، ص٢٤٩.

(٣) حيدرة محمد وآخرون، الهجمات السيبرانية ومواجهتها في القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد (٤)، ٢٠١٧، ص١٨٨.

(٤) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد (١٥)، العدد (٢)، ٢٠١٨، ص٣٤٦.

لصليب الأحمر (كورديلا دورغيه) لتعريف الهجمات السيبرانية بأنها هجمات لإستغلال الشبكات التي تنفذ لأغراض جمع المعلومات غير المشروعة وتحصل خارج نطاق النزاعات المسلحة غير أنه في حالة النزاعات المسلحة عندما تلجأ الأطراف إلى الحرب وتعتمد العمليات السيبرانية فيها فيكون القانون الدولي الإنساني هو الواجب التطبيق[١].

أما الخبراء القانونيين في القاعدة (٣٠) من دليل تالين (Tallinn de Manuel)[٢] فقد عرفوها بأنها عمليات سيبرانية قد تكون هجومية أو دفاعية تهدف إلى التسبب بوفاة الاشخاص أو اصابتهم أو الإضرار وتدمير الأهداف[٣].

وعرفه المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والإقتصادية [٤] بأنه استخدام متقن للطاقة موجهه لمهاجمة الأفراد والمؤسسات من أجل إضعاف قدرة المستهدَف. كما أن هذه الهجمات تؤدي إلى تدمير قطاعات مهمة في الدولة ولا يمكن أن تحدث بصورة عرضية لذلك سميت بالهجمات أي انها عملية إعتداء واضحة وليست حادث طارئ[٥].

---

(١) زهراء عماد محمد، مصدر سابق، ص١١.

(٢) صدرت النسخة الأولى منه في مارس،٢٠١٣ بطلب من حلف الناتو وقد تمثل هدفه الرئيسي في التحقيق في القضايا وتطبيق القانون الدولي في مجال الحرب السيبرانية. ويتكون الدليل من قسمين رئيسيين هما: قانون الأمن السيبراني الدولي، وقانون النزاعات السيبرانية المسلحة وذلك في سبعة فصول. ويتضمن (٩٥) قاعدة قانونية صاغتها لجنة الخبراء في القانون الدولي البارزين في تالين / باستونيا على نحو يحدد الخطوط الحمراء التي تستوجب التدخل العسكري، وطرق مشاركة مختلف الأطراف. وفى عام ٢٠١٦ تم إصدار النسخة المحدثة لدليل تالين القانون الدولي المطبق على عمليات الإنترنت، ويضم أربعة أجزاء رئيسية، وبلغت عدد القواعد التي يمكن تطبيقها على العمليات السيبرانية (١٥٤) قاعدة من قواعد القانون الدولي.
للمزيد انظر: ناجي محمد اسامة الشاذلي الجوانب القانونية للحرب السيبرانية: دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، المجلد (٣٥)، العدد (١٠٣)، (ج٢)، ٢٠٢٣، ص١٢٧١.

(٣) نور أمير موصلي، الهجمات السيبرانية في ضوء القانون الدوي الإنساني، رسالة ماجستير مقدمة إلى الجامعة الإفتراضية السورية،٢٠٢١، ص٩؛ درويش سعيد، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة في ضوء احكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد (٥٤)، العدد (٥)، ٢٠١٧، ص١٨١.

(٤) وهو مؤسسة مستقلة تعمل في إطار البحث العلمي الأكاديمي والتحليلات السياسية والقانونية و الإعلامية و الإقتصادية حول الشؤون الدولية والإقليمية ذات الصلة بالواقع العربي والدولي ،تأسس سنة ٢٠٠٧ في جمهورية مصر العربية . للمزيد أنظر الموقع الرسمي للمركز:

democraticac.de

(٥) علي فاضل علي سليمان، مصدر سابق، ص ٢٤٩.

و أورد معجم الإستخدامات العسكرية الخاص بهيئة الاركان المشتركة في الولايات المتحدة الأمريكية بأن الهجوم السيبراني هو نشاط عدائي يتم تنفيذه من خلال الحواسيب أو الشبكات أو الانظمة ذات الصلة بهدف تعطيل أنظمة الخصم أو ممتلكاته ووظائفه، أو تدميرها(١).

وعلى الرغم من تركيز التعريفات السابقة على موضوع الهجوم ونوعه لتعريف الهجمات السيبرانية إلا أنه لا يمكن إنكار الاتجاهات التي تنظر للهجوم السيبراني من منظور أوسع و بغض النظر عن الوسيلة المستخدمة في الهجوم السيبراني فيمكن أن تشمل هذه الهجمات أي إستخدام للتكنولوجيا السيبرانية لتقويض الإستقرار السياسي لدولة ما، وهذا ما تبنته منظمة شنغهاي للتعاون(sco)(٢).

ويتضح لنا من خلال ما ذكرناه سابقاً أن مفهوم الهجمات السيبرانية لا يزال غير واضح في الفقه القانوني ويتم الخلط بينه وبين مصطلحات أخرى مشابهة له كون هذه المواضيع من المواضيع المستجدة على الدراسات القانونية نوعاً ما ولم يحظ بما يكفي من الدراسات القانونية وبإهتمام الفقهاء القانونيين(٣).

وتجدر الإشارة إلى أن أغلب الدول تتعرض للهجمات السيبرانية وقد يكون ذلك بصورة منظمة ومستمرة حيث تمتاز هذه الهجمات بكونها واسعة النطاق وكل شيء مرتبط بالفضاء السيبراني هو

---

(1) DOD Dictionary of Military and Associated Terms, 2021, p55.
=https://irp.fas.org/doddir/dod/dictionary.pdf

تاريخ الزيارة ٢٠٢٣/٩/١ الساعة ٤:٠٠م

(٢) وهي منظمة دولية حكومية دائمة. تأسست في ١٥ يونيو ٢٠٠١ في شانغهاي، على يد قادة ستة دول آسيوية؛ هي الصين، وكازاخستان، وقيرغيزستان، وروسيا، وطاجيكستان، وأوزبكستان. وقع ميثاق منظمة شانغهاي للتعاون في يونيو ٢٠٠٢، ودخل حيز التنفيذ في ١٩ سبتمبر ٢٠٠٣. كانت هذه البلدان باستثناء أوزبكستان أعضاء في «مجموعة شانغهاي الخماسية» التي تأسست في ٢٦ أبريل ١٩٩٦ في شانغهاي. تتمحور أهداف المنظمة حول تعزيز سياسات الثقة المتبادلة وحسن الجوار بين دول الأعضاء، ومحاربة الإرهاب وتدعيم الأمن ومكافحة الجريمة وتجارة المخدرات ومواجهة حركات الانفصال والتطرف الديني أو العرقي. والتعاون في المجالات السياسية والتجارية والاقتصادية والعلمية والتقنية والثقافية وكذلك النقل والتعليم والطاقة والسياحة وحماية البيئة، وتوفير السلام والأمن والاستقرار في المنطقة). http://eng.sectsco.org/cooperation/20170110/192193.html تاريخ الزيارة ٢٠٢٣/٥/١٥ الساعة ٤:٠٠م.

(٣) أحمد عطا حسين، وسائل حماية التجارة الالكترونية من المخاطر الهجمات السيبرانية، مجلة جامعة واسط للعلوم الإنسانية، مجلد (١٨) العدد (٥٢) لسنة ٢٠٢٢، ص٦٦٩.

هدف لهذه الهجمات، كما تتميز بأنها تمثل تهديداً خطيراً للبنى التحتية للدولة مما يسبب تعطيل استخدام الدولة لأنظمتها الإلكترونية لتسيير شؤونها الداخلية أو تدمير تلك الأنظمة مما يهدد الأمن القومي للدولة. وللدولة المتعرضة للهجوم السيبراني الحق في استخدام القوة للدفاع عن نفسها وفقاً للمادة (٥١) من ميثاق الأمم المتحدة لذا فإن النقطة الجوهرية في عد الهجوم سيبرانياً هو من خلال النظر للجهة المستهدفة والنتائج التي يخلفها على تلك الجهة. لذا فإن الخلط بين الهجمات السيبرانية والجريمة السيبرانية قد يؤدي إلى خرق قواعد القانون الدولي فيما إذا مارست الدولة حق الدفاع الشرعي في غير حالة الهجوم السبراني[١].

أما بالنسبة للمشرع العراقي فإنه لم يبين موقفه من الهجمات السيبرانية وبالتالي لم يحدد معالمها وطبيعتها القانونية، مما يخلف فراغاً تشريعياً يجب تلافيه في المستقبل القريب.

وقد حاول البعض تأطير الهجمات السيبرانية بإطار المنافسة غير المشروعة من خلال الرجوع إلى قانون المنافسة ومنع الإحتكار رقم (١٤) لسنة ٢٠١٠ حيث وجدوا في المفهوم الواسع للإحتكار الواردة في مواد القانون السابق الذكر مكاناً لإدراج الهجمات السيبرانية ضمن أعمال المنافسة غير المشروعة الواردة في الفقرة الثانية من المادة الأولى من القانون، والتي عرفت الإحتكار بأنه كل اتفاق أو فعل أو تفاهم صدر من شخص أو أكثر سواء كان طبيعياً أو معنوياً للتحكم بالسعر أو نوعية السلع أو الخدمات مما يؤدي للإضرار بالمجتمع[٢].

وفي اعتقادنا أن هذا الرأي قد يجانب الصواب وفيه خلط بين الهجمات السيبرانية والجريمة السيبرانية فالمنافسة غير المشروعة تكاد تنحصر في إطار القانون الخاص في التعاملات التجارية لكن الهجمات السيبرانية يختلف هدفها تماماً عما سبق حيث إنها تتوجه لتستهدف دولة أو نظام سياسي أو أمن وطني لدولة ما، وكان الأفضل عدم الخلط بينها وبين الجرائم السيبرانية التي تستهدف الافراد والأشخاص المعنوية الخاصة بصورة عامة لتحقيق أغراض قد تكون ربحية أو تخريبية في الدرجة الأساس دون أن تستهدف دولة أو نظامها بحد ذاته، أي أن المنافسة غير المشروعة قد تكون إحدى صور الجريمة السيبرانية لا الهجمات السيرانية.

(١) علي فاضل علي سلمان، مصدر سابق، ص٢٤٨.

(٢) أحمد عطا حسين، مصدر سابق، ص ٦٧٢.

ثانياً: الجريمة السيبرانية:

يعدّ مصطلح الجريمة السيبرانية من المصطلحات الحديثة والتي يتم استخدامها للتعبير عن جرائم الانترنت نظراً لتطور ظاهرة الاجرام واتصالها بتقنية المعلومات، وهو في الأصل يعتبر من المصطلحات غير العربية لكن تم استخدامه لدى العديد من الجهات الوطنية والعالمية على الرغم من تباين التسميات التي أطلقت على الجريمة السيبرانية في مراحل تطورها على مر السنوات السابقة، ففي بادئ الأمر أطلق البعض على الجريمة السيبرانية مصطلح (إساءة استخدام الحاسوب) أو (إحتيال الحاسوب)، وأطلق البعض الآخر عليها الجريمة المعلوماتية أو جرائم الانترنت. وبسبب حداثة المصطلح فأن فقهاء القانون لم يستقروا على تعريف محدد له ؛ قد يكون ذلك خشية لأن يتم حصر المصطلح بنطاق ضيق ومحدد أو بسبب إختلاف الثقافات والقوانين بين الدول(١).

ولقد عرف البعض الجريمة السيبرانية بالنظر إلى وسيلة إرتكابها ومنهم الفقيهين (Tiedemann) و(Ball) حيث عرفاها بأنها ارتكاب كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي، كما عرفها (David Thompson) بالنظر لإرادة الفاعل بأنها سلوك غير مشروع معاقب عليه قانوناً ناشئ عن إرادة جرمية محلة أنظمة الحاسوب، ومنهم من عرفها من جانب موضوع الجريمة مثل الفقيه (Rosenblatt)، والذي عرفها بأنها نشاط غير مشروع موجه لإتلاف البيانات المخزونة في النظام أو الاعتراض غير القانوني لها عن طريق نقلها من جهاز حاسوب لآخر كأدخال بيانات خاطئة أو العبث بها و يتم إرتكابها ضد اشخاص أو جماعات بدافع إجرامي(٢).

ونلحظُ أن الجانب الآخر من الفقهاء قد جمع بين الاتجاهين من خلال تعريف الجريمة السيبرانية بأنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود(٣).

---

(١) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد (٢٤) الشهر (٥) لسنة ٢٠٢٠، ص ٨.

(٢) محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢، ص٢٦؛ علي فاضل علي سلمان، مصدر سابق، ص٢٥٠.

(٣) روان بنت عطية الله الصحفي، مصدر سابق، ص٨.

ومن الفقهاء من عرّف الجريمة السيبرانية على أساس توافر المعرفة التقنية ، حيث يستند هذا الإتجاه إلى معيار شخصي وهو إلمام مرتكب الجريمة السيبرانية بتقنية المعلومات حيث يستلزم توافر سمات شخصية لدى مرتكبها تتمحور حول الدراية والمعرفة التقنية، وقد عرفها الأستاذ (Thomos david) بأنها كل جريمة يكون متطلباً لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب، لكن يؤخذ على هذا الإتجاه أن معيار المعرفة التقنية ضيق وغير دقيق إذ لابدّ الأخذ بإعتبارات أخرى تتعلق بموضوع الجريمة أو وسيلتها ليتم تصنيف الفعل بأنه ضمن الجرائم السيبرانية(١).

أما على المستوى التشريعي فقد عرّف نظام مكافحة جرائم المعلوماتية السعودي المرقم (م/١٧) لسنة ٢٠٠٧ الجريمة السيبرانية في الفقرة الثامنة من المادة الأولى من النظام واطلق عليها مصطلح (الجريمة المعلوماتية) وهي أي فعل يرتكب متضمناً استخدام الحاسب الآلي او الشبكة المعلوماتية بصورة مخالفة لأحكام هذا النظام(٢).

أما المشرع الأردني فقد اكتفى بتعريف الحادث السيبراني في المادة الثانية من قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ بأنه الفعل أو الهجوم الذي يشكل خطراً على البيانات أو المعلومات أو نظم المعلومات أو البنى التحتية أو الشبكة المعلوماتية ويتطلب إستجابة لإيقافه أو للتخفيف من الآثار والعواقب المترتبة عليه. ويعتقد الباحث أن مصطلح الحادث السيبراني المشار إليه أعلاه هو مصطلح مرن وواسع غير محدد، لكن فحوى التعريف تدل دلالة قاطعة على شمول الجريمة السيبرانية كون المشرع لم يحصر هذه الافعال بالدولة أو بشخص محدد وإنما ركز المشرع على محل وقوع الفعل بغض النظر عن الشخص المستهدف. وكان من الأفضل أن يستبدل مصطلح الحادث السيبراني بالخطر السيبراني كون التعريف عام وشامل لكل ما يندرج تحت الخطر السيبراني من مفاهيم.

أما بالنسبة للمشرع العراقي فلا يوجد قانون خاص بالجرائم السيبرانية أو الأمن السيبراني، على الرغم من الإشارة للجريمة السيبرانية وتطبيقاتها في استراتيجية الأمن السيبراني العراقي الصادرة عن

---

(١) بن عميروش ريمة، عن خصوصية الجريمة المعلوماتية، مجلة الفقه القانوني و السياسي، المجلد (٢) العدد (٢) لسنة ٢٠٢١، ص٧٦.

(٢) وهو نظام صادر عن هيئة الإتصالات وتقنية المعلومات في المملكة العربية السعودية بالمرسوم الملكي رقم (م/١٧) في(٨) ربيع الأول ١٤٢٨هـ الموافق ٢٦ مارس ٢٠٠٧.للمزيد ينظر إلى الموقع الرسمي للهيئة:
https://www.cst.gov.sa/ar/mediacenter/awarenesscampaigns/Documents/AW_08_E_Crime.pdf
تاريخ الزيارة ٢٠٢٤/٤/٢٣ الساعة ١:٠٠ ص.

مستشارية الامن الوطني لأمن الاتصالات والمعلومات إلا أنه لم يضع لها تعريف محدد واكتفت بتعريف المخاطر السيرانية والتهديد السيبراني والفضاء السيبراني مع الابقاء على مصطلح الجريمة السيبرانية دون تعريف على الرغم من تكرار ذكره في الاستراتيجية ووضع مصطلح الجريمة الالكترونية كمرادف له في ذات الاستراتيجية.

وجاء في ارشادات الاسكوا للتشريعات السيبرانية (ESCWA)[١] أن جريمة الحاسوب أو جريمة الفضاء السيبراني حسب وصفهم تكون على نوعين، النوع الأول: حيث يكون الحاسب الآلي هو أداة تنفيذ الجريمة والوسيلة التي سمحت بإرتكابها،أما النوع الثاني فيكون الحاسب الآلي ونظم المعلومات والشبكات هو موضوع الجريمة مثل التعدي على إسم موقع على الإنترنت ، مما يشكل جرماً يطال حقاً من حقوق الملكية الفكرية. ومايميز هذه الارشادات أنها عرفت كل صورة من صور الجريمة السيبرانية على حدى، إلا أنها لم تعرف المفهوم العام للجريمة السيبرانية بصورة مباشرة[٢]، ومن خلال تعريفها لمكافحة الجرائم السيبرانية يمكن استنتاج تعريف الجريمة السيبرانية وفق وجهة نظر منظمة (الانسكوا) حيث عرفتها المنظمة بأنها مكافحة النشاطات الإجرامية التي تتم بواسطة الحواسيب والإنترنت ويتضمن ذلك أي موضوع من تحميل ملفات الموسيقى إلى سرقة ملايين من الدولارات من المصارف الإلكترونية. وبالتالي فإن الجريمة السيبرانية وفقا للمنظمة سالفة الذكر هي نشاطات إجرامية تمارس من خلال أجهزة الحاسب الآلي في الفضاء السيبراني وتشمل كل اعتداء يتم من خلال إستخدام هذه الواسطة مهما كان صغيراً [٣].

---

(١) وهي اللجنة الاقتصادية والاجتماعية لغربي آسيا و واحدة من خمس لجان إقليمية تخضع لولاية المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة. يتمثل دور اللجنة في تعزيز التنمية الاقتصادية والاجتماعية لغربي آسيا من خلال التعاون والتكامل على الصعيدين الإقليمي ودون الإقليمي، تأسست الإسكوا عام ١٩٧٣ لتحفيز النشاط الاقتصادي في الدول الأعضاء وتعزيز التعاون فيما بينها وتعزيز التنمية. وتضم٢٠ دولة عربية بينها العراق الذي انضم لها سنة ١٩٧٣. الموقع الرسمي للإنسكوا https://www.unescwa.org/ar/about تاريخ الزيارة ٢٠٢٢/٩/١٨ الساعة ٢:٤٩م.

(٢) ارشادات الإسكوا للتشريعات السيبرانية/ مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية الصادر في ٣/١ لسنة ٢٠١٢، ص١١٧، منشورة على الموقع:

https://digitallibrary.un.org/record/1292295?ln=ar&v=pdf

تاريخ الزيارة ٢٠٢٤/٤/٢٣ الساعة ١:٣٠ ص.

(٣) انظر الموقع الرسمي للإنسكوا:

https://www.unescwa.org/ar/about

تاريخ الزيارة ٢٠٢٢/٩/١٨ الساعة ٢:٤٩ م

ولا تزال العديد من الدول العربية خالية من تشريع يخص الجرائم السيبرانية على الرغم من أنها تمثل ناقوس خطر على جميع مفاصل العمل التجاري في الدولة بالدرجة الأساس ناهيك عن أنها تمثل تهديداً صريحاً للبيانات الشخصية للأفراد المتعاملين مع الفضاء السيبراني. ومن الدول التي شرعت قوانين خاصة بالجريمة السيبرانية هي السعودية (نظام مكافحة الجرائم المعلوماتية لسنة ٢٠٠٧) والاردن (قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ بالاضافة للقانون المؤقت لسنة ٢٠١٠ والخاص بجرائم انظمة المعلومات) والامارات العربية المتحدة (القانون الاتحادي بشأن مكافحة جرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦) والسودان (قانون مكافحة جرائم المعلوماتية رقم ١٤ لسنة ٢٠٠٧).

ومن خلال ايضاح مفهوم كل من الهجمات السيبرانية والجريمة السيبرانية نجد أن الهجوم السيبراني أضيق نطاقاً من الجريمة السيبرانية وإن كانتا تشتركان في البيئة ذاتها وهي الفضاء السيبراني. إلا أنها تختلف من حيث الأشخاص والأهداف، فالأولى عبارة عن ممارسات إلكترونية تتسبب في قتل أو تدمير أو إحداث أضرار مادية تقوم بها دولة أو مجموعة مسلحة ضد دولة اخرى بهدف سياسي وتخضع لقواعد القانون الدولي العام، بينما تشمل الجريمة السيبرانية مجالاً أوسع بكثير من ذلك أي تتضمن كل النشاطات الالكترونية غير القانونية بما في ذلك استخدام الوسائل المعتمدة على الكمبيوتر لإرتكاب أعمال غير قانونية في التشريعات الوطنية والهدف الأساسي لها هو إما أن يكون شخصاً طبيعياً و المتمثل بالأفراد، أو الأشخاص المعنوية كالشركات التجارية أو المؤسسات المالية التابعة للقطاع الخاص وتخضع لقواعد القانون العام. كما أن هدف الجريمة السيبرانية هو في الغالب تحقيق مكاسب مادية شخصية أو إثبات المهارة الفنية أو حتى بهدف التسلية كالممارسات الإحتيالية على الانترنت والقذف والسب عبر الوسائل الالكترونية وغيرها، على عكس الهجمات السيبرانية ذات الأهداف العسكرية أو السياسية أو الأمنية التي يكون الأمن القومي والسياسي والبنى التحتية للدولة وزعزعة النظام فيها هو هدفها المباشر[١].

وبإعتقادنا أن مفهوم المخاطر السيبرانية هو المصطلح الأكثر شمولية لكل فعل أو تهديد وقع أو سيقع ضمن نطاق الفضاء السيبراني، فهو يشمل كل من الهجمات السيبرانية والجرائم السيبرانية وما يندرج تحتها من مصطلحات على حد سواء حيث أن الهجمة أو الجريمة تصنف ضمن المخاطر بصورة عامة ومن ثم يتم تخصيص هذه المخاطر وفق تصنيفات محددة كما وجدناه فيما سبق ذكره من مفاهيم كالهجوم السيبراني أو الجريمة السيبرانية.

(١) رزق أحمد سمودي، مصدر سابق، ص ٣٦٤.

المطلب الثاني

أنواع الخطر السيبراني وأثره على الشركات التجارية

قد تتعرض الشركات التجارية في أثناء ممارسة نشاطها التجاري في الفضاء السيبراني إلى أنواع مختلفة من المخاطر السيبرانية، وبطريقة أو بأخرى يؤثركل نوع من هذه المخاطر على الشركة التجارية بطريقة مختلفة عن الأنواع الأخرى، لذا سنبحث في أنواع الخطر السيبراني في الفرع الأول من هذا المطلب، ثم سنبحث في تأثر الشركات التجارية بالخطر السيبراني في فرعٍ ثانٍ.

الفرع الأول

أنواع الخطر السيبراني

يتحدد مفهوم المخاطر 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 اشارت الدراسات إلى إن عدد الهجمات السيبرانية ارتفع بنسبة ٥١ بالمائة في فرنسا في عام ٢٠١٥ وبنسبة ٣٨ بالمائة في جميع انحاء العالم(١).

تحت عبارة مخاطر الانترنت أو المخاطر السيبرانية تنطوي جميع الاضرار المختلفة التي تصيب الممتلكات والتي تسببها أنظمة معالجة البيانات والمعلومات والتقنيات الاخرى المنبثقة منها، ووفقاً **لمقياس (FFA)** "**الاتحاد الفرنسي للتأمين**" **لعام ٢٠١٩** تعد المخاطر السيبرانية إحدى اهم المخاطر الرئيسية على المدى القصير، والأعلى على المدى المتوسط مما شكل تحدياً كبيراً لشركات التأمين نظراً للطبيعة المعقدة نوعاً ما لهذه المخاطر و تطورها المستمر(٢).

(1) Assurance des risques cyber. Guide Pratique، club de la securite de l`information Franceais,. Janvier 2018, p8.

(2) L'assurance du risque cyber Colloque de l'Université du Mans du 5 décembre sur les nouvelles technologies et les mutations des assurances Pierre-Grégoire Marly, Professeur agrégé de droit privé à l'Université du Mans, Directeur du Master de droit des assurances, Directeur adjoint de l'IAP Sorbonne Alexis Valençon, Avocat associé, Kennedys AARPI, 2019, p1.

وبصورة عامة فأنه لا يمكننا تصور وجود أي شخص طبيعي أو معنوي محصن من هذه المخاطر وكذلك الحال بالنسبة للشركات التجارية على اختلاف أنواعها ونشاطاتها، فهي تبقى معرضه لهذه المخاطر طالما تستخدم في نشاطها وسائل الاتصال الحديثة والتقنيات المعاصرة والتي تعمل في فضاء سيبراني غير محصن من الهجمات السيبرانية، ومن أبرز هذه المخاطر واكثرها شيوعاً:

١- **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 ازدحاماً على هذه المواقع فيصعب وصول المستخدمين اليها وتعرضت لهذا النوع من المخاطر العديد من المواقع المهمة والحساسة مثل: **Word press،Amazon** [١] ويتم تنفيذ الهجوم باستخدام اجهزة كمبيوتر آمنة جداً و متفرقة في عدد من دول العالم مما يجعل معرفة الفاعل أمراً صعباً جداً مقارنةً بالمخاطر التقليدية، وفي الوقت الذي تسبب فيه وباء **(COVID-19)** في تحول هائل في استخدام الإنترنت، انقض مجرمو الإنترنت بسرعة، وشنَو أكثر من ١٠ ملايين من هجمات الحرمان من الخدمة (DDoS) والتي تهدف إلى شل الخدمات الأساسية عبر شبكة الإنترنت التي تعتمد على العمل عن بعد عبر الفضاء السيبراني. وتعتبر من أكثر الأنشطة الحيوية التي اصبحت معرضة لهذا الهجوم بعد تفشي الوباء: التجارة الإلكترونية وخدمات البث والتعلم عبر الانترنت، والرعاية الصحية، وضربت الآلاف من الشركات في جميع أنحاء العالم. وكانت اكثر القطاعات تعرضاً للهجوم في العام ٢٠٢٠ هي: ناقلو الاتصالات اللاسلكية، معالجة البيانات ونظم الإتصالات الأخرى، الخطوط الجوية، الفنادق والموتيلات، الجهات المصدرة لبطاقات الائتمان، ناشرو البرمجيات[٢].

٢- **أعمال التجسس او اختراق الحاسب الالي:** يعرَف التجسس الإلكتروني بأنه استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير قانوني لأنظمة المعلومات التابعة للدول أو المنظمات أو المواطنين

---

(١) خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للابحاث ودراسة السياسات، سبتمبر ٢٠١٣، ص٩.

(٢) سلوى يوسف الأكيابي، مدى انطباق القانون الدولي الانساني على الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق، جامعة الزقازيق، العدد (١٠١)، المجلد (٢)، ٢٠٢٣، ص١٣٤٦، تقرير." NETSCOUT 2H 2020 Threat Intelligence " المملكة العربية السعودية لسنة٢٠٢٠. منشور على الموقع:

https://www.netscout.com/sites/default/files/2021-05/SECR_036_AR-2101%20TR2H2020_Country_Saudi_Arabia.pdf

تاريخ الزيارة: ٢٠٢٤/٤/٢٤ الساعة ٣:٠٠ م

أو الشركات بهدف التنصت عليها بقصد الحصول على معلومات مهمة تتعلق بالنواحي العسكرية أو السياسية أو الإقتصادية أو العلمية أو الإجتماعية. 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 الإختراق وهي في الغالب لا تسبب أي ضرر أو تعطيل في الأجهزة(١).

٣- **برامج الفدية:** وهي برامج إلكترونية ضارة تعد الأكثر شيوعاً بين جميع أنواع المخاطر السيبرانية الأخرى، تعمل على إختراق 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 الكومبيوترية بشكلٍ تام. ويعمد مرتكبو الاعتداء إلى طلب مبالغ مالية (سميت بالفدية) لفك تشفير الملفات وتسهيل استئناف الوصول إلى الأنظمة المعتدى عليها(٢)، ويعود هذا الخطر إلى الثمانينات، إلا أنه تحول إلى تهديدٍ بارز بعد عام ٢٠١٠ مع تصاعد نشاط العملات الرقمية، والتي تعد وسيلة الدفع المفضلة للمجرمين السيبرانيين. وقد ساهم بروز فيروسات الفدية كتهديد جدي برفع قيمة عروض التغطية التأمينية حتى أصبحت اعتداءات فيروسات الفدية اليوم تسيطر على ٧٥ في المائة من طلبات التأمين السيبراني(٣).

ووفقا لتصريح **وكالة الاتحاد الاوروبي للامن السيبراني** وجد هناك زيادة بنسبة ١٥٠ بالمائة في هجمات برامج الفدية بين عامي ٢٠٢٠ و ٢٠٢١(٤)، وقد لوحظت هذه الزيادة في وتيرة هذه الهجمات من قبل الشركات المتخصصة بالأمن السيبراني ويمكن تفسير تلك الزيادة من خلال المكاسب المتزايدة

---

(١) علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة، ط١، منشورات زين الحقوقية، بيروت،٢٠١٣، ص ٥٦٩.

(٢) أحمد الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، الجامعة المصرية –الروسية، المجلد (٢٤)، العدد (٤) ٢٠٢٣ ص١٥٦.

(3) https://aawsat.com/home/article/3714976

date of visit 13/8/2023 8:00pm

(٤) للمزيد انظر الموقع الرسمي لوكالة الاتحاد الاوروبي للامن السيبراني:

https://www.enisa.europa.eu /

تاريخ الزيارة ٢٠٢٢/٨/١٧ الساعة ٢:٣٠م

للمهاجمين كون الشركات التجارية غير محمية بشكل كاف مع قلة الخبرات التقنية في هذه الشركات وانخفاض احتمالية تحديد هوية المهاجمين(١).

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 (٢).

وتجدر الإشارة إلى أن الشركة التجارية عندما تواجه احتمالًا منخفضًا 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، فلن تتردد شركات التأمين السيبراني في تقديم التغطية، وبالتالي، يمكن للشركات التجارية الاستثمار في وثائق التأمين السيبراني لحماية نفسها من الخسائر المستقبلية الناجمة عن هجمات برامج الفدية، نظراً لأن موظفي أمن المعلومات في الشركة قد قاموا بنقل المخاطر إلى شركات التأمين السيبراني.وكذلك الحال إذا كانت الشركة التجارية تواجه احتمالية منخفضة وخطورة منخفضة لهجوم برامج الفدية، فإن موظفي أمن المعلومات يميلون إلى الاستثمار في التأمين السيبراني أكثر من استراتيجيات التخفيف من المخاطر.اما اذا كان احتمال وقوع الخطر السسيبراني مرتفعاً ولكن شدة الهجوم منخفضة، فيجب على مديري أمن المعلومات في هذه الشركات أن يلجأوا إلى إعطاء الأولوية للإستثمار في تكنولوجيا الأمان لمنع المخاطر السيبرانية (التأمين الذاتي) مثل وضع جدران الحماية النارية، ومكافحة الفيروسات، حيث ستساعد مثل هذه الإجراءات على تقليل احتمالية هجمات برامج الفدية(٣).

---

(1) Assurance des risques cyber. Guide Pratique، op.cit, p8.

(٢) عبد الحليم محمود شاهين، تقييم اقتصادي أولي لمخاطر البيت كوين، مجلة كلية الاقتصاد والعلوم السياسية، جامعة الاسكندرية، مجلد (٢٢)، العدد (٣)، ٢٠٢١، ص٥٠.

(3) Arunabha Mukhopadhyay, Swati Jain, A framework for cyber-risk insurance against ransomware: A mixed-method approach، International Journal of Information Management، Volume (74), February 2024, p13.

٤- **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 إنتقالها 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 إنتشاراَ وشيوعاَ منذ سنوات عديدة(١).

٥- **الهندسةالاجتماعية (SocialEngineering):** 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. وتشكل المدخل لحوالي (٧٠) بالمائة من عمليات الإختراق التي تحدث في العالم فهي لا تحتاج إلى معرفة تقنية عميقة وبالتالي يستطيع أي شخص تتوافر لديه الحنكة والدهاء بأن يقوم بهذا الهجوم، من خلال التلاعب بعقول الاشخاص بإستخدام أسلوب إنتحال الشخصية أو الحصول على ثقة الضحية بصورة تدريجية حتى يتم الإختراق من خلال التلاعب بالبشر وليس الاجهزة الرقمية للوصول إلى البيانات السرية والمعلومات الحساسة المطلوبة(٢).

٦- **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 متمثلةً بموظفيها وعملائها من الدخول إلى الموقع المعني(٣).

---

(١) وهذه الفيروسات تتميز بقدرتها على فقدان قدرة نظام التشغيل في الشركة التجارية على التعامل مع البيانات او الملفات الخاصة بالشركة وعملائها بالرغم من انها لا تزال موجودة على القرص الصلب ولم يتم حذفها. للمزيد أنظر: علي عبود جعفر، مصدر سابق، ص٥٥٢.

(٢) محمد الدمرداش ابو التوح، متطلبات تنمية المهارات الرقمية للمنظم الاجتماعي للحد من هجمات الهندسة الاجتماعية، مجلة الخدمة الاجتماعية، المجلد (٧٦)، العدد (٢)، ٢٠٢٣، ص٢٦؛ قيصر بهاء، أشهر الهجمات السيبرانية، تقرير الفريق الوطني للاستجابة للأحداث السيرانية، ص١٧.

(٣) خالد وليد محمود، مصدر سابق، ص٨.

٧- التصيد والخداع (phishing):

وهو محاولة الحصول على البيانات الشخصية من الشركة التجارية أو العملاء تتعلق بالإسم أو كلمة المرور أو البطاقات الإئتمانية أو المفتاح الخاص بالعملات الرقمية كالبيتكوين، حيث يتم ارسال هجمات التصيد والإحتيال عبر البريد الالكتروني ويتم طلب النقر على رابط معين وإدخال البيانات الشخصية للشركة الضحية، وتكمن فاعلية هذه الهجمات في صعوبة التمييز بين الموقع الحقيقي وبين الموقع المزيف(١).

٨- برامج القنابل المعلوماتية (الشفرة الموقوتة):

وهي نوع من أنواع البرامج الخبيثة يتم إدخالها بطرق غير قانونية لأنظمة الشركة التجارية وإخفائها في البرامج الأخرى، فهي شفرة توضع ضمن مجموعة من الملفات وليست ملف متكامل ويتم تقسيمها لأجزاء متفرقة هنا وهناك بحيث يصعب التعرف عليها وتتجمع تلقائياً على وفق الأمر المعطى لها في زمان ومكان معينين ولا يمكن اكتشافها لأشهر أو حتى لسنوات، والغرض منها تدمير معلومات وبيانات الشركة أو تغيير برامج ومعلومات النظام ومن الأمثلة على هجمات القنابل المعلوماتية الهجوم الإلكتروني الذي استهدف الهيئة العامة للطيران السعودي وعدد من المؤسسات الحكومية في العام ٢٠١٦ مما أدى إلى محو البيانات المخزنة في أجهزة الكمبيوتر و من ثم منع إعادة تشغيلها(٢).

٩- هجوم الوسيط (Man in middle):

هو هجوم يدخل فيه شخص خارجي أو طرف ثالث بين إثنين من المستخدمين عبر الإنترنت، كأن يدخل طرف ثالث في مراسلات الشركة التجارية مع أحد عملائها أو وكلائها، بحيث لا يدرك كل منهما ذلك، حيث يتم التلاعب بالمعلومات الحساسة الخاصة بهما. و يسمح هجوم الوسيط بشكل أساسي لمستخدم غير مصرح به داخل نظام التشغيل بالوصول إلى معلومات الشركة التجارية أو العملاء وتغييرها دون ترك أي أثر مادي(٣). وغالباً ما تكون الفئة المستهدفة هم عملاء التطبيقات

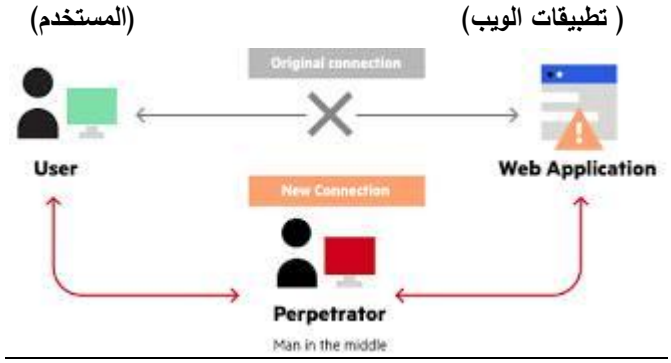
---

(١) عبد الحليم محمود شاهين، مصدر سابق، ص٤٥.

(٢) نور أمير الموصلي، مصدر سابق، ص١٧.

(3) Danish Javeed، Man in the Middle Attacks: Analysis، Motivation and Prevention International Journal of Computer Networks and Communications Security, vol.(8) issue.(7), 2020، p52.

المالية، والشركات التجارية التي تمارس نشاطها التجاري عبر الفضاء السيبراني، أو عملاء تلك الشركات الذين يتعاملون بالدفع عبر بطاقات الائتمان او النقود الرقمية[1]. كما في الشكل أدناه:



(مرتكب الإعتداء)

الفرع الثاني

تأثر الشركات التجارية بالخطر السيبراني

يأتي الخطر السيبراني في مقدمة المخاطر التي تهدد الشركات التجارية بمختلف أنواعها و أحجامها فتلحق أضراراً جسيمة بالعلامات التجارية والسمعة التجارية للشركات، مما ينتج عنها في الغالب أضراراً مالية جسيمة، فيؤثر الخطر السيبراني على صافي أرباح تلك الشركات الأمر الذي يؤدي إلى زيادة التكاليف و تخفيض الإيرادات، فضلاً عن تأثير الخطر السيبراني على قدرة الشركات التجارية على إكتساب العملاء والحفاظ عليهم، بالإضافة لتقليل الإبتكار[2].

(1) Mallik Avijit Ahsan Abid, Shahadat Mhia, Tsou, Jia-Chi. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, vol.(3), issue.(2), 2019، P78.

(٢) اشارت دراسة اجراها معهد المراجعين الداخليين في أمريكا الشمالية لسنة ٢٠٢٢ إلى ان مخاطر الأمن السيبراني تعتبر المتصدرة من بين ١٣ خطر أخر يؤثر على منظمات الأعمال، كما توصلت دراسة أجراها معهد المراجعين الداخليين في الإتحاد الأوروبي إلى ان مخاطر الأمن السيبراني تعد من بين أعلى خمسة مخاطر تهدد بيئة الأعمال. للمزيد انظر: رمضان عارف رمضان وأبو الحمد مصطفى صالح، استخدام المنهجية الرشيقة في تطوير اداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، مجلة البحوث المالية والتجارية، المجلد (٢٣)، العدد (٣)، ٢٠٢٢، ص٤٣٥.

إنّ المتتبع لتأثيرات المخاطر السيبرانية يجد أنها أقوى وقعاً على الشركات التجارية مقارنة بباقي الأشخاص الطبيعية أو المعنوية الأخرى، كون ما يخلفه الخطر السيبراني من ضرر يتزايد بصورة طردية بأزدياد حجم نشاطها التجاري. فالمخاطر السيبرانية بحد ذاتها لا يتصور أن تتغير، إلا أن خصائصها وآثارها هي التي تتغير بتغير الأدوات والوسائل المستخدمة في تحقيقها، فتدمر الشركات التجارية بطريقة غير مادية، لما لتلك المخاطر من خصائص غير ملموسة ذات أبعاد تقنية تميزها عن باقي المخاطر التي تتعرض لها الشركات التجارية وتؤمن منها، فالخطر السيبراني هو نتاج لتطور تقنيات المعلومات وهذا الذي أكسبها طابعاً خاصاً يميزها عن المخاطر التقليدية[١].

لذا يمكن القول أن الخطر السيبراني الذي يهدد هذه الشركات التجارية على اختلاف انواعها يؤثر عليها من نواحي مختلفة أبرزها ما يأتي:

١. **زيادة التكاليف:** حيث ترتفع التكاليف الملقاة على عاتق الشركات التجارية للدفاع عن أنظمتها ضد المخاطر السيبرانية المتوقعة وغير المتوقعة كتغطية النفقات القانونية المترتبة عن تحقق الخطر السيبراني أو التأكد من أن الشركة تلتزم بالمعايير القانونية الواجب إتباعها لتجنب فرض الغرامات عليها، وتكاليف ادارة الازمات من اتصالات ومحامين وتكاليف التحقيق من خبراء ومستشارين تقنيين وتكاليف الاصلاح واعادة الاعمار وتكاليف استعادة البيانات المفقودة ورسوم الاخطار. والغرامات التأخيرية الناتجة عن الاخلال في تنفيذ العقود مع العملاء والخسائر التشغيلية عقب وقوع الخطر السيبراني[٢].

٢- **فقدان الثقة و صعوبة جذب العملاء والشركاء التجاريين:** حيث إن اكتشاف العديد من الإنتهاكات الناجمة عن المخاطر السيبرانية التي تتعرض لها الشركات التجارية وصعوبة معرفة فاعلها في أغلب الحالات يخلّف في أغلب الحالات اضراراً مادية ومعنوية فادحة فيما يخص الثقة بين الشركاء التجاريين والعملاء وصعوبة جذبهم، لا سيما بعد اعتماد الشركات

(١) أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، مجلد(٣) العدد (٣٥)، ٢٠٢٠،ص٤٠٢.

(2) kala،op.cit, p56. sonakshi kathuriya, graphic era, impact of cybersecurity on business environment, de jure nexus law journal, volume (2), issue (4), 2022, p6.

التجارية على الوسط السيبراني لإيصال أغلب خدماتها وما يحمله ذلك من تهديدات كبيرة [١]، حيث يشعر العملاء، وحتى الموردين، بأمان أقل عندما يتركون معلوماتهم الحساسة في أيدي شركة تم كسر بنيتها التحتية لتكنولوجيا المعلومات مرة واحدة على الأقل من قبل[٢]. فعلى سبيل المثال، وعقب الخطر السيبراني الذي تعرضت له شركة (Equifax) تأثرت سلباً كل من وكالتي (Trans Unions) و (Experian) واللتان تعدان أكبر وكالتين للإئتمان في الولايات المتحدة حيث تخوف العملاء من حدوث اختراق مماثل لهذه الشركات مرة أخرى مما أدى إلى تجميد الإئتمان في تلك الشركات،كما فرضت الجهات الرقابية المختصة إجراءات أكثر صرامة لمنع حدوث إختراقات مماثلة في المستقبل [٣] ، فمثلاً أبلغت واحدة من أصل خمس شركات فرنسية عن صعوبة في جذب العملاء من جديد بعد وقوع حادث أو خرق سيبراني ونسبة (١٦) بالمائة من الشركات البلجيكية التي تعرضت للهجوم خسرت شركائها التجاريين وفقاً لتقرير شركة هيسوكس البريطانية للتأمين من مخاطر الانترنت للعام٢٠٢٠[٤].

٣- **التأثير على سمعة الشركة وعلامتها التجارية و انخفاض معدل نمو مبيعاتها:** إن تعرض شركة تجارية ما لخطر سيبراني أو إحتمال تعرضها لهذا الخطر يؤثر على سمعتها التجارية و سيؤدي بعملائها غالبا إلى تجنب الإستثمار فيها مما يؤدي بالتالي إلى انخفاض معدل نمو مبيعاتها، ومن الصعوبة بمكان التعرف على جميع الاثار المترتبة على المخاطر السيبرانية ؛ لأنه من الصعب الإحاطة بها وتحديدها، وبشكل عام فإن الشركات التي تتعرض لأحد هذه المخاطر ستقوم بزيادة الإستثمار في إدارة المخاطر السيبرانية للحد من آثارها، بسبب ان هذه المخاطر ذات تأثير قوي على مدى ثقة العملاء بالشركة و علامتها التجارية الأمر الذي يؤثر على سمعتها التجارية و بالتالي

---

(١) شذى عبد جمعة، التأمين على مخاطر انتهاك حقوق الملكية الفكرية الرقمية، دار الجامعة الجديدة، الاسكندرية، ٢٠١٩، ص ١١.

(2) Okereafor, Kenneth، Impacts Of Cyber Attacks On Corporate Business Continuity: Fostering Cyber Security Consciousness In The Citizenry, 1st National Cybersecurity and Cybercrime ConferenceAt: Abuja,. (2008), p18.

(٣) علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط، العدد (٦٣)، الكويت، ٢٠١٩، ص٢١.

(4) Gareth Wharton, Cyber CEO, Hiscox Cyber Readiness Report, 2020, p9.
https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF
date of visit 15/12/2023 8:30 pm

انخفاض مبيعاتها[١]، ومن وجهة نظر شركة (Hiscox)[٢] للتأمين كلما كانت الشركة تتمتع بقدرات جيدة لاكتشاف المخاطر السيبرانية مبكراً كلما كان التأثير أقل. الأمر الذي أدى إلى ارتفاع الإنفاق على الأمن السيبراني في الميزانيات المخصصة لتكنولوجيا المعلومات من قبل الشركات التجارية، وبالتالي كلما زاد الانفاق على الأمن السيبراني للشركات كلما زاد معدل نمو مبيعاتها، وتأتي ايرلندا في رأس قائمة البلدان التي لدى شركاتها تغطية سيبرانية متخصصة. يليها الولايات المتحدة الامريكية وبلجيكا بينما تقع المملكة المتحدة وفرنسا في المركز الثالث[٣].

٤- **انخفاض قيمة الأسهم:** إن تأثر الشركات التجارية بالمخاطر السيبرانية يختلف حسب طبيعة نشاط الشركة وحسب نوع الهجوم كما أن الافصاح عن وجود انتهاك سيبراني لشركة تجارية غالباً ما يكون ذي اثر اقتصادي كبير على قيمة اسهم تلك الشركة، وبسبب ذلك تعزف العديد من الشركات التجارية ممن وقعت ضحية هذه الهجمات عن الإبلاغ أو الإعلان عنها، حيث أن الإعلان عن وقوع مثل هذه الانتهاك خصوصاً تلك التي تنطوي على الكشف عن معلومات العملاء، إلى الاضرار بسمعة الشركة من جهة وقد يصل الأمر بها إلى دفع غرامات مالية للجهات الحكومية المختصة من جهة اخرى، كما ان هناك تأثير عكسي على أداء الشركات ، حيث أثبتت الدراسات انخفاض أداء الشركة بسبب انخفاض مبيعاتها عقب تعرضها للخطر السيبراني[٤].

---

(1) shinichi kamiya jun-koo kang jungmin kim andreas milidonis rené m. stulz, what is the impact of successful cyberattacks on target firms?, working paper no. 24409, national bureau of economic research 1050 massachusetts avenue cambridge, 2018, p12.

(٢) هيسكوكس المحدودة هي شركة تأمين أنجلو-برمودية، مدرجة في بورصة لندن. تتخصص الشركة، وهي شركة ضامنة في لويدز لندن، إلى حد كبير في مجالات متخصصة في السوق، حيث تقدم تأمينًا على الممتلكات والحوادث يستهدف الشركات والأفراد ذوي الثروات العالية، بالإضافة إلى التغطية ضد مخاطر مثل القرصنة والاختطاف وتلف الأقمار الصناعية مجموعة تأمين دولية متنوعة تتمتع بعلامة تجارية قوية وميزانية عمومية قوية ومساحة كبيرة للنمو .شركة مدرجة في بورصة لندن ومقرها الرئيسي في برمودا، ولديها حاليًا أكثر من ٣٠٠٠ موظف في ١٤ دولة و٣٤ مكتبًا. انظر الموقع الرسمي للشركة:

https://www.hiscoxgroup.com/about-hiscox

تاريخ الزيارة ٢٠٢٣/٨/١٤ الساعة ٩:٠٠ص.

(3) Gareth Wharton، op.cit, p10.

(4) Samuel Tweneboah-Koduah، Samuel Tweneboah-Koduah، William J Buchanan Impact of Cyberattacks on Stock Performance: A Comparative Study, Information and Computer Security journal, vol.(26), No.(3), 2018, p5.

٥- **قلة الايرادات وزيادة العبء المالي للشركة بسبب فرض الغرامات و إنفاق الوقت والجهد الإضافيين لتصحيح الأضرار الناشئة عن الخطر السيبراني:** ومثال على ذلك حادث إختراق شركة (Home Depot) والتي تعمل في مجال الأجهزة المنزلية في العام ٢٠١٤ حيث تم تسريب بيانات بطاقات الدفع الإلكتروني لعملائها والتي قدرت بحوالي ٥٦ مليون بطاقة عميل إضافة لذلك تم تسريب ٥٣ مليون بريد الكتروني للشركة وعملاءها ، وتم استخدام الهجوم الوسيط عن طريق طرف ثالث ادعى انه بائع وقام بإطلاق برمجيات ضارة بغرض الحصول على اجهزة نقاط البيع التي تمتلكها الشركة مما أدى إلى تكبد الشركة أعلاه لخسارة تقدر ب ٣٠٠ مليون دولار موزعة بين غرامات مستحقة الدفع بسبب الضرر نتيجة الخطر السيبراني الذي لحق بالشركة التجارية، بالاضافة لنفقات إعادة إصدار بطاقات الإئتمان الجديدة [١]. فالشركات عادةً ما تسعى لإيجاد الطريقة الأسرع للخروج من آثار الخطر السيبراني فهي غالباً ما ترضخ لدفع الفدية، حتى وإن كان العبء المالي كبيراً والنتيجة غير مضمونة، فقد وجدت دراسة حديثة شملت (٣٠) شركة أن (٦٤) بالمائة منها وقعت ضحية اعتداء بفيروس الفدية خلال العام الفائت، وأن (٨٣) بالمائة من هذه الشركات دفعت الفدية المطلوبة. وتبين أيضاً أن (٨) بالمائة من الشركات التي سددت الفدية تمكنت من استعادة كل بياناتها، مقابل (٦٣) بالمائة استعادت نصف بياناتها فقط. وقد تتلقى بعض الشركات طلباً لتسديد فدية ثانية أو ربما أكثر رغم تسديد الأولى في الوقت المحدد، والمشكلة تكون أكثر تعقيداً عندما تدفع الشركة التجارية الفدية ولا تتمكن من استعادة بياناتها، بالمقابل تتحمل الشركات التي تتخذ قراراً بعدم الدفع، التكلفة على مستوى توقف الأعمال وخسارة العائدات. أما الشركات التي تباغتها هذه الاعتداءات وهي غير مجهزة بنظام دعم متين أو بخطة استجابة، فتعاني أكثر من الجميع[٢].

٦- **إنتهاك حقوق الملكية الفكرية الرقمية:** هي مجموعة من الحقوق لحماية الإبداعات الفكرية للأشخاص حيث تمنح هذه الحقوق للمبدع حقاً حصرياً لاستعمال مصنفاته لفتره معينة من الزمن وتكون متاحة على الفضاء السيبراني[٣] وتمثل هذه الحقوق الأعمال الإبداعية أو المبتكرة والمتجسدة

---

(١)علم الدين بانقا، مصدر سابق، ص٢١.

(2) Gareth Wharton, op. cit, p10.

(٣) مكتب الامم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، ٢٠١٣ مسودة شباط و فبراير، ص ٥٢. منشورة على الموقع:

https://www.unodc.org/documents/organized crime/cybercrime/Cybercrime_Study_Arabic.pdf

تاريخ الزيارة ٢٠٢٣/٧/٢ الساعة ٠٠:٥م.

في بيئة تكنولوجيا المعلومات والتي بدأت بالظهور مع انشار الحاسب الآلي، وقد وسع التطور التكنولوجي من مفهوم حقوق الملكية الفكرية الرقمية من خلال استحداث انماط جديدة من المصنفات والتي اطلق عليها (المصنفات الرقمية) التي اصبحت تعد على وسائط الكترونية بشكل دعامات أو ملفات أو بيانات أو رسائل أو مستندات إلكترونية ويتم ترميزها لغرض تداولها الكترونياً، حيث تم إعداده أصلا في بيئة رقمية أو أن يكون بمثابة الشكل الرقمي ، فالبيانات أيا كان شكلها سواء كانت مكتوبة أو صوتية أو على شكل صور أو رموز أو موسيقى عندما يتم نقلها عبر وسائل الاتصال الحديثة تتحول إلى أرقام يتعامل معها الحاسوب ليتم بعد ذلك نقلها عبر قنوات الكترونية مرتبطة بالفضاء السيبراني. والمصنف الرقمي إما ان يكون كذلك منذ وجوده لمصنف تقليدي، وان مضمون حق المؤلف في البيئة الرقمية هو ذاته في مجال الملكية الفكرية التقليدية ولكن بسبب التقنيات الرقمية الحديثة اضحت المخاطر السيبرانية التي تطال حق المؤلف في الفضاء السيبراني من الصعب السيطرة عليها نظرا لقلة التشريعات التي تحميها،وتشمل هذه الحقوق حقوق المؤلف الرقمية والحقوق الرقمية المجاورة وحقوق الملكية الصناعية الرقمية كبراءات الإختراع والرسوم والنماذج الصناعية الرقمية وحقوق الملكية التجارية الرقمية كالعلامات التجارية الرقمية(١).

وقد اعتبرت مؤسسات القطاع الخاص أن الافعال التي ترتكب ضد النظم الحاسوبية تشكل تهديداً أكبر بكثير من الانواع الاخرى للمخاطر وهذا يعكس قلقاً اساسياً يساور كيانات القطاع الخاص والذي يتمثل بالوصول إلى نظمها الحاسوبية والاطلاع على بياناتها مما يؤدي لانتهاك سرية وخصوصية هذه البيانات. حيث ان الشركات التجارية كافة تكون عرضة للمخاطر السيبرانية مما يمكن أن يجعل التكاليف المتكبدة نتيجة هذه المخاطر عالية جداً، حيث أن ابرز المخاطر لدى الشركات التجارية تتمثل بالنفاذ غير المشروع للنظام وسرقة حقوق الملكية الفكرية واختراق المواقع الالكترونية الخاصة بالخدمات المصرفية وتسريب المعلومات من قبل الموظفين وهجمات حجب الخدمة(٢).

فعلى سبيل المثال قد يتم اللجوء إلى اتخاذ تدابير أو وسائل وقائية من قبل أصحاب مصنف ما وهو ما يعرف بأسلوب الحماية الخاصة كوسيلة لمنع استغلال المصنفات إلا بترخيص من صاحب الحق فيها ويتم ذلك باستخدام إمكانات تقنية معينة كالبرامج الالكترونية المتخصصة بحيث توفر هذه

(١) شذى عبد جمعة موسى، مصدر سابق ٢٠١٩، ص ٣٨ وما بعدها.

(٢) مكتب الامم المتحدة المعني بالمخدرات والجريمة، مصدر سابق، ص٣٩.

التقنيات الحماية لحقوق اصحاب الأعمال الفكرية المحمية وتم الاعتراف بهذا النوع من الحماية في العديد من القوانين حول العالم(١).

٧- **انقطاع الأعمال وتغيير سياسات العمل بسبب تعطل الخدمات:** يمكن للمخاطر السيبرانية أن تؤدي إلى تعطيل ممارسة الشركات لنشاطها التجاري أو ايقافه مؤقتاً، الأمر الذي يؤدي إلى انخفاض انتاجيتها والتأخر في تقديم خدماتها حيث يتعين على هذه الشركات إعادة التفكير في كيفية جمع المعلومات وتخزينها للتأكد من أن المعلومات الحساسة ليست معرضة للخطر، حيث تتوقف العديد من الشركات عن تخزين المعلومات المالية والشخصية للعملاء مثل أرقام بطاقات الائتمان وأرقام الضمان الاجتماعي وتواريخ الميلاد، أو اغلاق بعض متاجرها الإلكترونية خشية عدم قدرتها على توفير الحماية الكافية ضد المخاطر السيبرانية(٢). ففي العام ٢٠١٢ تعرضت عدد من المصارف في الولايات المتحدة الأمريكية إلى هجمات وقف الخدمة (DOSS) مما أدى إلى عدم تمكن العملاء من الوصول لحساباتهم أو دفع الفواتير عبر الانترنت على الرغم من انفاق هذه المصارف لملايين الدولارات سنوياً على الأمن السيبراني للحماية من المخاطر السيبرانية، وعلى الرغم من عدم وجود سرقة لبيانات البنوك وعملائهم إلا أن الهدف من هجوم رفض الخدمة هو تعطيل المواقع الالكترونية للمصارف بشكل مؤقت مما يؤدي إلى تعطيل الأعمال وتوقفها ومن ثم التسبب بإحباط العملاء وزعزعة ثقتهم(٣).

٨- **تخفيض اجور وحوافز موظفي الشركات التجارية:** يتأثر موظفي الشركة التجارية بصفة عامة بالمخاطر السيبرانية وما يستتبعها من زيادة الأعباء المالية للشركة و تكاليف التخلص من الضرر الناجم عنه على المدى الطويل و بمعدل ثلاث سنوات من وقوع الخطر السيبراني على الشركة مما يؤدي إلى تقاضي الموظفين مبالغ أقل بكثير من الأجور التي كانوا يتقاضونها قبل تحقق الخطر، إضافة إلى دفع مكافئات أقل بكثير مما هو عليه في السابق(٤).

---

(١) شذى عبد جمعة، مصدر سابق، ص ٩٣.

(2) Kala، op. cit, p59.

(3) Nida Tariq, IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce، vol.(23), issue (.2), 2018, p5.

(4) Shinichi Kamiya Jun-Koo Kang Jungmin Kim Andreas Milidonis René M. Stulz, WHAT IS THE IMPACT OF SUCCESSFUL CYBERATTACKS ON TARGET FIRMS?, Working Paper NO. 24409, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, 2018, p30.

وتعرضت الشركات التجارية على مر السنوات الماضية إلى العديد من الهجمات السيبرانية البارزة كان اشهرها بالنسبة الوطن العربي ما حدث في السعودية لأكبر شركات النفط في العالم **(ارامكو)** حيث شهدت اسوأ حادث خرق الكتروني خلال عطلة الموظفين في شهر رمضان من العام ٢٠١٢، فقد لوحظ اختفاء الملفات بشكل غريب من أجهزة الحاسوب وتوقف أجهزة أخرى عن العمل من دون تفسير إلى ما يصل نحو ٣٥ الف جهاز معطل مما دفع الشركة لإعادة العمل بالطرق التقليدية للطباعة وأجهزة الفاكس، وفي العام ٢٠٢١ تعرضت الشركة ذاتها لهجوم الكتروني اخر حيث تم تسريب البيانات الخاص بالشركة من موظفين وعملاء وكشوف المرتبات ومواقع مصافي النقل على يد احد المتعاقدين وتم طلب فدية ٥٠ مليون دولار من العملات المشفرة مقابل حذف البيانات المسربة مما دفع شركة ارامكو إلى توقيع اتفاقية لتعزيز الامن السيبراني مع شركة الإلكترونيات المتقدمة التابعة للشركة السعودية للصناعات العسكرية، لاستخدام تقنية **(صمام البيانات)** المصممة والمصنعة داخل المملكة لتفادي تأثيرات الهجمات السيبرانية المتكررة على سمعة الشركة وإستعادة ثقة العملاء والموردين والشركاء التجاريين[١].

يتضح مما سبق أن المخاطر السيبرانية تؤثر على التجارة الإلكترونية بصورة مباشرة كما تلحق أضراراً بليغة بالاقتصاد العالمي ناهيك عن زعزعة ثقة الأفراد بالأعمال التجارية الإلكترونية وتجنب التعامل بها، مما يتسبب بخسارة العديد من الشركات التي تعمل في الوسط السيبراني. وعلى الرغم من أن هذه المخاطر تستهدف النشاط الإلكتروني للشركات التجارية إلا أنه لا يمكن انكار تأثر دخل الموظفين من ناحية و انتهاك خصوصيته العملاء من الناحية الأخرى فالمتضرر الأخير هو الفرد الذي يمارس اعماله بالاستعانه بإحدى الشركات التجارية التي تعمل بوسائل التجارة الإلكترونية الحديثة[٢]، الأمر الذي دفع البعض إلى اطلاق تسمية (التعطيل الشامل) على المخاطر السيبرانية لتقابل مصطلح الدمار الشامل للأسلحة النووية والكيميائية والبيولوجية للدلالة على جسامة الآثار الناجمة عن هذه المخاطر من حيث الأضرار التي تخلفها ولا سيما تلك التي تمس شركات خطوط النقل الجوي أو شبكة الكهرباء أو خدمات الطوارئ وغيرها[٣].

---

(1) https://attaqa.net/2021/02/11

تاريخ الزيارة ٢٠٢٢/٨/١٨ الساعة ٤:٠٠م

(٢) أحمد عطا حسين، مصدرسابق، ص٦٧٠.

(٣) زهراء عماد محمد، مصدر سابق، ص٣٢.

نستنتج مما سبق أنه من الصعوبة بمكان في الوقت الحاضر وجود شركة تجارية تتعامل في الفضاء السيبراني أو تعتمد على النقود الرقمية أو تقوم بتخزين البيانات الشخصية والمالية إلكترونياً محصنة من المخاطر السيبرانية بصورة تامة بل على العكس، حيث تزداد قابلية تعرض الشركة وتأثرها بالمخاطر السيبرانية كلما اعتمد على تكنولوجيا المعلومات في ممارسة نشاطها التجاري.

و يمكن الحد من المخاطر السيبرانية و التقليل من آثارها قدر الإمكان من خلال مايلي:[1]

١- وضع عقد التأمين من المخاطر السيبرانية ووسائل الأمن السيبراني ضمن إطار تشريعي يوفر قواعد قانونية تهدف إلى حماية العملاء بالدرجة الأساس ومن ثم حماية الشركات التجارية ذاتها.

٢- توفير بيئة قانونية مرنة وفاعلة في الوقت ذاته تبسط الإجراءات اللازمة لحماية الأنشطة التجارية التي تتم ممارستها في الفضاء السيبراني.

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

(١) نضال إسماعيل إبراهيم، أحكام عقود التجارة الإلكترونية،ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥، ص١٩.

المبحث الثاني

المفهوم القانوني لعقد التأمين من المخاطر السيبرانية

تمتلك عقود التأمين من المخاطر السيبرانية خصوصية تميزها عما يقابلها من الأنواع التقليدية للتأمين وذلك من حيث الأهداف أوطبيعة 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 خصوصيتة 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 الإستثناءات التي قد ترد على هذا العقد لذلك سوف نقسم هذا المبحث إلى مطلبين، نخصص الأول للتعريف بعقد التأمين من المخاطر السيبرانية والاستثناءات الواردة فيه، ونتناول في المطلب الثاني تمييز عقد التأمين من المخاطر السيبرانية عما يشتبه به.

المطلب الأول

التعريف بعقد التأمين من المخاطر السيبرانية والاستثناءات الواردة فيه

لقد تزايدت في الآونة الأخيرة حاجة الشركات التجارية إلى شراء وثائق تأمين من المخاطر السيبرانية بسبب التهديدات المستمرة والمتزايدة لتلك المخاطر على إختلاف أشكالها كالقرصنة وبرامج الفدية والقنابل الفيروسية وغيرها، على أنظمة تشغيل التابعة لها والتي تحتوي على قاعدة البيانات الخاصة بكلاً من الشركة التجارية وعملائها، لذا فإنه من الضروري أن تحيط الشركات التجارية علماً بما يمكن لوثيقة التأمين من المخاطر السيبرانية تغطيتة، لكن في الوقت ذاته نجد أنه من الصعوبة بمكان تحديد الإستثناءات الشائعة الواردة في عقود التأمين من المخاطر السيبرانية نظراً لكونه حديث نسبياً، لذا سنتناول في هذا المطلب تعريف عقد التأمين من المخاطر السيبرانية في فرعٍ أول، ومن ثم بيان أبرز الإستثناءات التي قد يتضمنها هذا النوع من عقود التأمين في فرع ثانٍ.

الفرع الأول

التعريف بعقد التأمين من المخاطر السيبرانية

في ضوء ما تقدم ، باتت الشركات التجارية معرضة لخطر غير تقليدي وغير مادي يهدد سمعتها التجارية أو علامتها التجارية أو مكانتها في السوق، لذا 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[١] أو هو عملية تأمينية يقوم بها المؤمن لتعويض اضرار الكارثة السيبرانية[٢].

وتقوم شركات التأمين عند كتابة عقود التأمين من المخاطر التقليدية بتجميع العديد من الأخطار طبقاً لقوانين الإحصاء ومن ثم إجراء المقاصة بينها على أساس علمي لكي تتمكن من الوفاء بإلتزاماتها عند تحقق الخطر المؤمن منه، إلا أن الأمر مختلف في عقود التأمين من المخاطر السيبرانية حيث يصعب التأمين على هذا النوع من المخاطر بسبب غياب البيانات التاريخية حول هذا النوع الجديد من المخاطر كالحوادث الناشئة عن قرصنة أنظمة القيادة في السيارات ذاتية التحكم أو قرصنة الأجهزة الطبية وما يتبع ذلك من أضرار وخسائر كارثية للشركات المؤمن لها، وهذا بدوره يؤدي إلى صعوبة التأمين من هذه المخاطر، حيث يحتاج التأمين عامة الى توفير عدد كبير من البيانات والاحصاءات حول الخسائر والأضرار وكيفية تسعيرها[٣]؛ الأمر الذي حدا بالعديد من شركات التأمين إلى التغاضي عن طرح عقود تأمين ضد المخاطر السيبرانية في الوقت الذي طرحت فيه بعض شركات التأمين عقود تأمين تغطي

---

(١) محمد سعيد إسماعيل، التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن، المجلة الدولية للقانون، المجلد العاشر، العدد الثالث، عدد خاص بمؤتمر "القانون في مواجهة الازمات العالمية – الوسائل والتحديات"، كلية القانون، جامعة قطر، ٢٠٢١، ص٢٠٧.

(٢) بغداد شامبي، تأمين الخطر السيبراني، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد (٧) العدد (٢٥)، ٢٠٢٣، ص٢٦٩.

(٣) محمد سعد أحمد، دور التأمين في مواجهة المخاطر الناشئة عن الذكاء الاصطناعي وتكنولوجيا المعلومات، مجلة مصر المعاصرة، العدد (٥٤٣)، ٢٠٢١، ص٤٨٤.

الأضرار الناتجة عن فئات محددة من المخاطر السيبرانية [١]. ونتيجة لتطور التجارة الإلكترونية جراء التغييرات الجوهرية في أساليب العمل بسبب نمو وتطور تكنولوجيا المعلومات والإتصالات و إدراكاً لهذا الواقع الجديد أصبحت شركات التأمين تقدم خدماتها بما يتلائم مع هذا الواقع الجديد وما تمخض عنه من مخاطر جديدة كالمخاطر السيبرانية. وتعتبر عملية تقييم المخاطر في عقد التأمين من المخاطر السيبرانية هي الخطوة الأصعب مقارنة بالمخاطر الأخرى في عقود التأمين التقليدية حيث تتكون عملية ادارة المخاطر السيبرانية بشكل اساسي من ثلاث خطوات اساسية[٢]:

١- تقييم المخاطر وتحليلها.

٢- معالجة تلك المخاطر.

٣- الابلاغ والمراقبة والتحديث.

وبناءً على ذلك برز عقد التأمين من المخاطر السيبرانية كي يوفر تغطية من تلك المخاطر للأطراف ذات المصلحة سواء كانت الشركة التجارية المؤمن لها من الخطر السيبراني أو الغير أو حتى شركات تأمين أخرى، وعلى كل حال فإن تغطية المخاطر السيبرانية في عقود التأمين قد تكون إما على شكل وثائق منفردة (**stand- alone policies**) حيث يتم تغطية كل خطر بوثيقة خاصة به، أو قد لا تكون كذلك بالنسبة لبعض شركات التأمين من المخاطر السيبرانية

(١) حيث اعدت شركة (HSB) للتأمين من المخاطر السيبرانية، وهي إحدى أكبر شركات التأمين في المملكة المتحدة، عقد تأمين ضد القرصنة الإلكترونية والأخطار المرتبطة بها بما في ذلك التوقف عن العمل والأضرار التي تلحق بالسمعة للشركات التجارية التي لا يقل حجم اعمالها ١٥ مليون دولار ولا يزيد عن ٧٥ مليون دولار، ويغطي هذا العقد نفقات الصيانة حال تعرض الشركة التجارية للاحتيال الالكتروني او الاختراق، بالإضافة للمسؤولية الناجمة عن اختراق أنظمة تشغيل الشركة، وخسائر التوقف عن العمل جراء تعرض قاعدة البيانات للاختراق. انظر وثيقة التأمين من المخاطر السيبرانية للشركة والمنشورة على الموقع:
https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf
تاريخ الزيارة ٢٠٢٤/٥/٢ الساعة ٣:٣٠ م.

(٢) صدام فيصل كوكز، اتمتة التأمين والتأمين على مخاطر الفضاء الرقمي، دار الفكر الجامعي، الاسكندرية، ٢٠٢٣، ص١٩ وما بعدها.

الأخرى حيث أن لكل شركة تأمين نظام عمل خاصة بها تحدد من خلالها الشكل النهائي الذي ستكون عليه التغطية[١].

ويقوم عقد التأمين من المخاطر السيبرانية على مبدأ أساسي وهو نقل تبعة المخاطر الناشئة عن استخدام أنظمة تكنولوجيا المعلومات إلى طرف ثالث وهي شركات التأمين من المخاطر السيبرانية، وعلى الرغم من إمكانية الحد من المخاطر السيبرانية وآثارها الكارثية على الشركات التجارية عن طريق إدارة المخاطر السيبرانية بصورة تقليدية من خلال تجنبها أو اللجوء لتغطية تقليدية قد تؤدي بصورة ضمنية إلى إمكانية شمول بعض المخاطر السيبرانية بالتغطية إلا انه لا يمكن انكار أهمية التأمين من المخاطر السيبرانية كأداة لنقل تبعة المخاطر السيبرانية على اختلاف انواعها والتي قد يصعب على الشركات التجارية تجنبها حتى وإن امتثلت لإجراءات الأمن والسلامة السيبرانية المعتادة، و لاسيما أن صور التأمين التقليدية قد اتفقت على استبعاد بعض المخاطر السيبرانية كالهجمات السيبرانية من شمولها بالتغطية[٢] نظراً للطبيعة المتغيرة والديناميكية للمخاطر السيبرانية، نجد ان ما يميز عقود التأمين من المخاطر السيبرانية عن غيرها من العقود التقليدية هو صعوبة توحيد بنود وثائق التأمين من المخاطر السيبرانية والمصطلحات الواردة فيها. ونتيجة لذلك، فإنه غالبا ما يكون الاكتتاب في التأمين من المخاطر السيبرانية مخصصاً للغاية حيث يكون لكل عميل من الشركات التجارية تغطية خاصة به، وعلى عكس الأنواع التقليدية من التأمين،نجد التأمين من المخاطر السيبرانية يمكن أن يختلف بشكل كبير من حيث نطاقه بإختلاف شركة التأمين أو وثيقة التأمين، كما انه يمكن ان يتم بواسطة وثيقة تأمين قائمة بذاتها أو إمتداد لوثيقة تأمين سابقة، حيث توفر بعض وثائق التأمين غطاء لبعض المخاطر السيبرانية بشكل مباشر أو غير مباشر، إلا أنه قد يكون من الصعب تحديد نطاق المخاطر المغطاة بدقة من قبل شركة التأمين أو المؤمن لهم، مما جعل التأمين على هذه الاخطار

---

(١) نشرة الاتحاد المصري للتأمين، مخاطر الهجمات الالكترونية في المؤسسات المالية عدد (٢٤٥)، ٢٠٢٢ منشورة على الموقع:

https://www.ifegypt.org/News.aspx?Page_Id=1244

تاريخ الزيارة ٢٠٢٣/٧/٢٢ الساعة ١٢:٥٠ص

(2) Even Langfeldt Friberg, The Cyber-Insurance Market in Norway: An Empirical Study of the Supply-side and a Small Sample of the Maritime Demand-side, Master's thesis, TALLINN UNIVERSITY OF TECHNOLOGY School of Information Technologies 2018, p15.

بصورة مستقلة أو ما يعرف بالخطر المسمى هو الاكثر شيوعاً، لأن الطبيعة المتغيرة للمخاطر السيبرانية تجعل نطاق تغطية التأمين في حالة تغير مستمر[١].

وتسعى الشركات التجارية من إبرام عقد التأمين من المخاطر السيبرانية لتحقيق هدفين أساسيين[٢]:

١- 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 وعياً بهذا التعرض من خلال تلبيتها لمعايير أعلى فيما يتعلق بحماية البيانات والأمن السيبراني.

٢- سد النقص الحاصل في وثائق التأمين التقليدية: بإعتبار 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 بإرتفاع 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[٣].

---

(1) Yogesh Malhotra, PhD،Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics, MS Network and Computer Security Thesis On Model Risk Management of Statistical Probability Distributions in Cyber Insurance،Thesis Presented to the state university of NY, p.

(2) Steven Hadwin, Norton Rose Fulbright LLP and Jamie Monck-Mason، Willis Towers Watson, CYBER INSURANCE: AN OVERVIEW, UK, 2020, p5.

(٣) نشرة الاتحاد المصري للتأمين، الهجمات الالكترونية (السيبرانية) والتأمين، العدد (٦٧)، ٢٠١٩. منشورة على الموقع:

https://www.ifegypt.org/Default.aspx?Page_ID=2

تاريخ الزيارة ٢٠٢٣/٨/١٤ الساعة ٨:٠٠ م.

ولا تزال إشكالية تحديد طبيعة المخاطر السيبرانية التي من الممكن ان تكون مشمولة بالتغطية هي أبرز التحديات التي تواجه العديد شركات التأمين. 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(١).

وفي إعتقادنا أن هذه الشروط غير كافية لتمييز المخاطر السيبرانية القابلة للتأمين من مثيلاتها غير القابلة للتأمين كونها شروط نظرية بحته تمتاز بكونها شروط عامة تنطبق على جميع المخاطر السيبرانية، ولا يمكن من خلالها الجزم بالمخاطر الممكن شمولها بالتغطية من عدمها، وإن إمكانية تحديد المخاطر القابلة للتأمين لابدّ له من جانب عملي ؛ كون هذه المخاطر حديثة لا تتوفر بصددها نظريات كافية يمكن الاعتماد عليها، وإنما لا بدّ من تحديد المخاطر القابلة للتأمين من جانب عملي وفق معطيات سوق التأمين السيبراني.

أما القسم الآخر من شركات التأمين فقد إستخدمت منهجاً عملياً لتحديد المخاطر السيبرانية القابلة للتأمين من تلك غير القابلة للتأمين(٢)، وتطلبت توافر عدة شروط في الخطر السيبراني حتى يمكن التأمين منه: وهي ما اطلق عليه تسميه (منهج برلينر) والذي حدد تلك الشروط بناء على اسس اكتوارية وسوقية ومجتمعية، وتتمثل الشروط الاكتوارية بما يلي(٣):

١- عشوائية حدوث الخسارة، أي أن يكون هناك تنبئ لإحتمالية حدوث الخسارة.

(1) Biener, C., Eling, M., Wirfs, J. Insurability of Cyber Risk: An Empirical Analysis. Geneva Pap Risk Insur Issues Pract 40, (2015). p6.

(٢) حيث يرى جانب من الفقه ان الخطر السيبراني لا يمكن التأمين عليه في الاصل مقارنة بالأخطار الاخرى، فهو خطر لا يمكن التحكم فيه بصورة مطلقة بسبب خصائصه الفنية المعقدة حيث انه خطر ديناميكي للغاية وان عدم القدرة على التنبؤ بسلوك الانسان سواء الناتج عن جريمة او خطأ (عمدي وغير العمدي) يجعل الاخطار السيبرانية بطبيعتها اكثر تنوعاً وصعوبة بالتنبؤ والتحكم والنمذجة مقارنة بالأخطار التقليدية، انظر: بغدادي شامبي، مصدر سابق، ص٢٤٣.

(3) Biener, C., Eling, M., Wirfs, J., op. cit. p8.

٢- قابلية توقع أقصى خسارة ناتجة عن هذا الخطر للتثبت من مدى ملاءة شركة التأمين لتغطية المطالبات.

٣- أن يكون متوسط مبلغ الخسارة الناجمة عن الخطر معتدلة.

٤- أن يكون الضرر الناجم عن الخسارة ضررا غير تافه.

٥- عدم وجود تضارب في المعلومات التي تم تجميعها عن الخطر.

أما شروط سوق التأمين تتمثل ب:

١- معرفة مدى كفاية اقساط التأمين لتوفير عائد كاف لرأس مال شركة التأمين ومدى ملائمتها مع الامكانية المادية للشركات التجارية طالبة التأمين .

٢- ومقبولية العملاء المستقبليين لحدود التغطية.

وبالنسبة للشروط المجتمعية:

١- يجب أن تكون تغطية الخطر السيبراني متوافقة مع السياسة العامة للتأمين كإتفاق شركات التأمين على عدم التأمين ضد المخاطر السيبرانية التافهة أو التأمين ضد العقوبات الجزائية.

٢- أن تتقيد شركة التأمين بالأنشطة المسوح لها بممارستها قانوناً اي ان يتم التأمين ضد الاخطار المشروعة والمسموح بالتأمين ضدها قانوناً في الدولة التي يقع مقر شركة التأمين فيها حيث يعد الاستقرار القانوني امر مهم لمعرفة المخاطر السيبرانية القابلة للتأمين.

وفي اعتقادنا نجد أنه على الرغم من صرامة هذا المنهج لكنه عملي وشمولي ومبسط في الوقت ذاته، حيث يمكن شركات التأمين من وضع الخطوط العامة لسياساتها وبما يتوافق مع أسس علمية وعملية دقيقة بالإعتماد على الإحصاء وتجارب السوق وسلامة الموقف القانوني وهذا كفيل بفهم طبيعة الخطر السيبراني القابل للتأمين منه لدى شركات التأمين. فعدم إتفاق هذه الاخيرة على المخاطر السيبرانية المشمولة بالتغطية يعرقل نمو سوق التأمين من المخاطر السيبرانية ويؤدي إلى إرباك للعملاء بسبب وجود عدم يقين بكفاية التأمين من المخاطر السيبرانية كوسيلة للحماية، مما يساهم في إنخفاض الطلب على هذا المنتج التأميني وتدهوره.

وغالباً ما يشمل عقد التأمين من المخاطر السيبرانية تغطية الخسائر الآتية:

١- تكاليف إدارة الأزمات المتكبدة في التعامل مع المخاطر السيبرانية وخاصة إنتهاك البيانات الشخصية ويشمل ذلك نفقات الإخطار والطب الشرعي لتكنولوجيا المعلومات ونفقات الإستشارات القانونية وتكاليف العلاقات العامة ومراقبة الإئتمان ومراكز الاتصال وتكاليف إستعادة البيانات(١).

٢- إنقطاع الأعمال غير المادي الذي تتسبب به المخاطر السيبرانية للشركات التجارية، ويختلف عن إنقطاع الأعمال التقليدية كون الأخيرة ناشئة عن خطر مادي كالحريق مثلاً. أما إنقطاع 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 إنتظار تحسب بالساعات وبمجرد انتهائها يتم التعويض عن الخسائر بأثر رجعي على سبيل المثال بعد (١٢٠) يوماً من بدء الإنقطاع أو(٩٠) يوماً بعد انتهاء الانقطاع. بالإضافة الى الخسائر الناجمة عن الابتزاز الالكتروني والتي تعد من اكثر المطالبات شيوعاً وفق سياسات التأمين ضد المخاطر السيبرانية(٢).

٣- تكاليف المتخصصين في مجال الإبتزاز الإلكتروني وتكاليف الفديات الناجمة عن عملية الإبتزاز (٣).

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 إدعاء الغير بوجود خرق للبيانات السرية الخاصة به أو تعرضه لخسارة ناجمة عن افتقار

(1) The Hartford steam Boiler Inspection and Insurance Company و (HSB) cyber risk insurance Application،2019:
https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf

(2) Pavel V Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, Stefan Trück, The nature of losses from cyber-related events: risk categories and business sectors, *Journal of Cybersecurity*, Volume (9), Issue (1), 2023 و p10.

(3) Steven Hadwin, op.cit, p9.

الشركة التجارية وهي الطرف المؤمن له في العقد الى متطلبات الأمن السيبراني الأمر الذي يتسبب للغير بالضرر[١] مع الأخذ بنظر الاعتبار أنه من الممكن أن تفوق قيمة الأضرار التي تصيب الغير قيمة الضرر الحاصل للشركة[٢].

٥- تكاليف ما يعرف بالإستجابة الأولى (First Response): عندما تشتبه الشركة التجارية المؤمن لها في وجود إنتهاك للأمن السيبراني في أنظمة تشغيل الشركة، فإن معظم هذه الشركات لا تمتلك المعرفة الفنية لغرض تشخيص المشكلة ومن ثم حلها، لذا تلتزم شركات التأمين من المخاطر السيبرانية وفقاً للعقد المبرم بينها وبين الشركة التجارية بتغطية تكاليف الإستجابة الأولى للكشف عن وجود الخطر السيبراني، كما تفرض بنود العقد تغطية تكاليف المستشار قانوني أوالمتخصص في تكنولوجيا المعلومات من اللذين يمكنهم تقديم الدعم والتنسيق المطلوبين للتقليل من الضرر الناجم عن تحقق الخطر السيبراني[٣].

٦- الرسوم والتكاليف الضرورية لحماية البيانات وإسترداد التكاليف والنفقات التي تكبدتها الشركة صاحبة التغطية لإستعادة أو إعادة إنشاء أو استعادة الوصول إلى أي برامج أو بيانات إلكترونية من النسخ الاحتياطية أو من النسخ الأصلية. أو معاً تجميع وإعادة إنشاء مثل هذه البرمجيات أو البيانات الإلكترونية من مصادر أخرى إلى المستوى أو الحالة التي كانت موجودة عليها مباشرة قبل تغييرها، أو تدميرها، أو حذفها أو إلحاق أضراراً بها [٤].

٧- توفر غالبية عقود التأمين التغطية من خطر طريق الهندسة الاجتماعية[٥] من خلال البند التالي: "سيدفع المؤمن مقابل خسارة الأموال أو الأوراق المالية الناتجة مباشرة عن تحويل أو دفع أو تسليم

(1) Bc. Jan Linert Pojištění kybernetických rizik, VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE, Fakulta financí a účetnictví, 2019 p3.

(2) 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, p5.

(3) AXIS Cyber ransomeware Supplement Application, No. 1012729 10 20: https://www.euclidspecialty.com/wp-content/uploads/2021/05/AXIS_Ransomware_App-2021-1.pdf
date of visit 5/7/2023 6:00 pm.

(٤) نشرة الاتحاد المصري للتأمين، الهجمات الالكترونية (السيبرانية) والتأمين، العدد ٦٧، ٢٠١٩.

(٥) تشير الهندسة الاجتماعية وفقاً لتعريف وكالة الاتحاد الأوروبي للأمن السيبراني (ensia) إلى جميع التقنيات التي تهدف إلى إقناع الهدف بالكشف عن معلومات محددة أو القيام بإجراء محدد لأسباب غير مشروعة.=

الأموال أو الأوراق المالية من المبنى أو حساب التحويل إلى شخص أو مكان أو حساب خارج عن سيطرة الشركة التجارية المؤمن لها عن طريق موظف او(مؤسسة مالية) يتصرف بحسن نية بالاعتماد على تعليمات هاتفية أو مكتوبة أو إلكترونية ولكن في الواقع لم يتم إصدارها من قبل العميل أو الموظف أو البائع"[١].

٨- التعويض عن الأضرار التي تلحق بالأنظمة التشغيلية للشركة التجارية وما تحتوي عليه من مكونات مادية كالحواسيب مثلاً. بالإضافة للأضرار التي تلحق بالسمعة التجارية – للشركة المؤمن لها- على المدى الطويل والذي في الغالب يصعب على القاضي تقديره، إلا أنه بالإمكان الإعتماد على عدد من القرائن لتقديره عادة كفقدان العملاء أو خسارة الارباح نتيجة الآثار السلبية للخطرالسيبراني على الشركات التجارية[٢].

٩- المسؤولية القانونية الناجمة عن إنتهاك حقوق الملكية الفكرية والنشر حيث يتم النص صراحة في بعض عقود التأمين من المخاطر السيبرانية على شمول التغطية التأمينية لتكاليف الدفاع عن

=وعلى الرغم من أن هذا النوع من المخاطر السيبرانية كان موجودًا في القدم، إلا أنه تطور بشكل ملحوظ مع ظهور تقنيات تكنولوجيا المعلومات والاتصالات .في هذا السياق الجديد، ويمكن النظر إلى تقنيات الهندسة الاجتماعية في تكنولوجيا المعلومات من زاويتين مختلفتين:

- إما عن طريق استخدام التلاعب النفسي للحصول على مزيد من الوصول إلى نظام تكنولوجيا المعلومات حيث يوجد الهدف الفعلي للمحتال، على سبيل المثال انتحال شخصية عميل مهم عبر مكالمة هاتفية لجذب الهدف إلى تصفح موقع ويب ضار لإصابة محطة عمل الهدف؛
- أو استخدام تقنيات تكنولوجيا المعلومات كدعم لتقنيات التلاعب النفسي لتحقيق هدف خارج نطاق تكنولوجيا المعلومات، على سبيل المثال، الحصول على بيانات الاعتماد المصرفية عبر هجوم التصيد لسرقة أموال الهدف.

وبطبيعة الحال، أدى الاستخدام المتزايد لتكنولوجيا المعلومات إلى زيادة في استخدام مثل هذه التقنيات، فضلا عن الجمع بينها، إلى درجة أن معظم الهجمات السيبرانية في الوقت الحاضر تشمل شكلا من أشكال الهندسة الاجتماعية. مثال على بعض الأساليب الأكثر شيوعًا للهندسة الإجتماعية الذريعة، والإغراء، والمقايضة، والتتبع .بالإضافة لإعتماد هجمات التصيد الاحتيالي أيضًا على الهندسة الاجتماعية.

للمزيد انظر موقع الوكالة:

https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

تاريخ الزيارة ٢٠٢٤/١/١ الساعة ٦:٠٠ ص

(١) قرار محكمة الاستئناف بالولايات المتحدة / للدائرة الخامسة:

Miss. Silicon Holdings v. Axis Ins. Co.، No. 20-60215 (5th Cir. Feb. 4، 2021)

https://casetext.com/case/miss-silicon-holdings-llc-v-axis-ins-co-2

تاريخ الزيارة ٢٠٢٣/٣/١٣ الساعة ١٢:٠٠م

(2) Steven Hadwin, Norton Rose op. cit, p8.

المطالبات المتعلقة بإنتهاكات حقوق الملكية الفكرية للشركات التجارية، بشرط أن يكون الإنتهاك الواقع على هذه الحقوق من ضمن أضرار النشر المنصوص عليها في الوثيقة مع الأخذ بنظر الإعتبار أن الشركات التجارية في الغالب لا تعتبر كناشر لأعمالها إلا حين إمتلاكاها لموقع إلكتروني على شبكة الإنترنت حيث تتزايد إحتمالات تعرضها للإنتهاكات التي تطول ملكيتها الفكرية(١).

١٠- مسؤولية أمن الشبكة: حيث يوفر التأمين ضد المخاطر السيبرانية تغطية لتكاليف الدفاع والتسوية في حال قيام الغير برفع دعوى ضد الشركة التجارية بسبب خرق الخصوصية أو النشر غير المقصود للبرامج الضارة او التحريض على هجوم رفض الخدمة أو الوصول غير المصرح به للنظام أو الاستخدام غير المصرح به أو هجوم رفض الخدمة من قبل الغير أو نقل البرامج الضارة للشركة التجارية أو عملائه(٢). كما يمكن أن تغطي عقود التأمين الأضرار الناتجة عن الهجمات الفيروسية على الرغم من أن الخطر السيبراني غير إحتمالي وإنما عشوائي، ومعنى ذلك أن الخطر السيبراني لا يوجد له معيار محدد أو ظروف محدده لتكرار وقوعه مقارنة بباقي أنواع المخاطر التقليدية فهو بالنسبة للشركة التجارية الواحدة قد يكون نادر الوقوع أو كثير الوقوع ، وهذا ما يميز التأمين من المخاطر السيبرانية عن التأمين التقليدي الذي لا يغطي سوى الخطر المحتمل الوقوع؛ ويكمن سبب تغطية الأضرار الناتجة عن البرامج الفيروسية على الرغم من صعوبة حسابها وفق نظرية الاحتمالات هو أن شركات التأمين من المخاطر السيبرانية لا تعول على نسبة احتمالية تحقق الخطر وانما تعتمد على ما يتخذه المؤمن له من اجراءات تتعلق بالأمن السيبراني وبعد ذلك يمكن لشركة التأمين الى تقدير درجة احتمالية معينة لوقوع الخطر وفقاً لما تمتلكه الشركة التجارية الراغبة بشراء التغطية من إمكانيات خاصة بالأمن السيبراني(٣).

١١- قد تغطي بعض شركات التأمين من المخاطر السيبرانية الوفاة أو الاصابة الجسدية والعقوبات التنظيمية على الرغم من أن الوضع الغالب في عقود التأمين من المخاطر السيبرانية هو عدم إمكانية شمولها بالتغطية(٤).

---

(١) شذى عبد جمعة، مصدر سابق، ص١٤١.

(2) Pavel V Shevchenko، Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, Stefan Trück, op.cit, 2023, p3.

(٣) اسراء فهمي ناجي، التأمين ضد الأخطار الالكترونية مجلة رسالة الحقوق السنة الثالثة عشرة، العدد الأول جامعة كربلاء كلية القانون، ٢٠٢١، ص٢٠٥.

(٤) محمد سعيد اسماعيل، مصدر سابق، ص٢٠٩.

١٢- الأضرار الناجمة عن الإبتزاز الإلكتروني والإحتيال الإلكتروني أو الأضرار الناتجة عن البرامج الضارة التي تتسبب في إفساد أو تعديل أو اتلاف أو التلاعب في البيانات الالكترونية[١].

ويقوم عقد التأمين من المخاطر السيبرانية على مبدأ الأمن المتعدد الأطراف حيث لا يمكن ان نفترض بأن جميع الأطراف في العقد يثقون ببعضهم البعض، لذا تكمن خصوصية العقد في انه لا يتم تقييم الأمن من خلال مراقبة المخاطر السيبرانية الناجمة عن اطراف خارجية، بل يتطلب ايضا ادراج المهاجمين الداخليين المحتملين لأطراف العقد اي انه ينبغي حماية الجميع ضد اي شخص اخر[٢].

وتجدر الإشارة أن صياغة عقود التأمين من المخاطر السيبرانية غالباً ما تكون بصيغة عامة بحيث يتم التعامل مع جميع الأخطار التي تندرج تحتها على وفق تغطية واحدة ، والغرض من ذلك هو تقليل الالتزامات المطلوب من شركة التأمين في المستقبل تنفيذها إلى الحد الأدنى بحيث لا يتجاوز إجمالي ما تدفعه للشركات التجارية للحد المتفق عليه لكل التزام، وهذا ما يعرف بـ(لغة التجميع او بند التجميع) في عقد التأمين وهو بند مذكور بعقد التأمين من المخاطر السيبرانية يتصف بعموميته ويمكن ان يندرج تحته عدد غير محدد من المطالبات الأمر الذي اثار عدد من التساؤلات حول كيفية تفسيره، فعندما عندما يحصل نزاع قانوني حول استحقاق مبالغ التغطية التأمينية فقد يختلف تفسير النصوص العامة والغامضة في العقد وفقاً لقناعة المحكمة حول بند التجميع لكن ما استقر عليه قضاء المحكمة العليا في المملكة المتحدة في قضية (**AIG Euorpe limited**) ضد (**woodman**) مثلاً ان جميع الدعاوى الناشئة عن فعل أو إغفال والمرتبطة ببعضها إرتباط حقيقي وتتلائم مع بعضها البعض بطريقة ما من وجهة نظر المحكمة فإنه كفيل بعدّها دعوى واحدة[٣].

---

(1) chubb،Cyber Enterprise Risk, Terms and Conditions Management Insurance, 2016, p4.

(2) Torsten Grzebiela, Insurability of Electronic Commerce Risks, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002, p2.

(٣) كان لدى شركة AIG للتأمين، بوليصة تأمين بحد أقصى ٣ ملايين جنيه إسترليني لأي مطالبة واحدة كانت شروط السياسة ذات الصلة خاضعة لأحكام بند التجميع الموجودة في البند ٢,٥ من التغطية والذي حصل حوله النزاع وهو:

..." تغطي شركة التأمين ما يلي:

أ) جميع المطالبات ضد أي مؤمن له أو أكثر والتي تنشأ عن: فعل واحد أو إغفال؛ سلسلة واحدة من الأفعال أو الإغفالات ذات الصلة؛ نفس الفعل أو الإغفال في سلسلة من الأمور أو المعاملات ذات الصلة؛ أفعال أو إغفالات مماثلة في سلسلة من الأمور أو المعاملات ذات الصلة.

ب) سيتم اعتبار جميع المطالبات المرفوعة ضد مؤمن له أو أكثر والتي تنشأ عن أمر أو معاملة واحدة بمثابة مطالبة واحدة .==

واستناداً لما سبق ذكره يمكننا تعريف عقد التأمين من المخاطر السيبرانية بأنه: "عقد يغطي الأضرار الناجمة عن المخاطر المرتبطة بتكنولوجيا المعلومات بصورة مباشرة أو غير مباشرة والتي تستهدف كل شخص طبيعي أو معنوي يمارس نشاطه عبر الفضاء السيبراني".

الفرع الثاني

الإستثناءات الواردة في عقد التأمين من المخاطر السيبرانية

الإستثناءات هي الظروف أو الشروط التي بموجبها لا تغطي فيها شركة التأمين للمخاطر السيبرانية التي قد تصيب الشركة التجارية، فمن الأهمية بمكان أن يقوم المؤمن له بتدقيق وفهم الإستثناءات الواردة في وثيقة التأمين من المخاطر السيبرانية التي يوقع عليها، حيث أن شركات التأمين سوف ترفض تلقائياً التغطية عند وجود هذه الإستثناءات. وبما أنه لا توجد قاعدة عامة وثابتة تسري على جميع عقود التأمين من المخاطر السيبرانية فإن النتيجة التي تستتبع ذلك هو التضارب الحاصل بين عقود شركات التأمين من ناحية الإستثناءات الواردة في بنود عقودها بشأن المخاطر السيبرانية غير القابلة للتأمين منها. ومن خلال الإطلاع على عدد من العقود والدراسات المتعلقة بالتأمين من المخاطر السيبرانية نجد أن الإستثناءات الأكثر شيوعاً هي تلك التي لا تتعلق بصورة مباشرة بالخطر السيبراني بحد ذاته وإنما بالظروف المحيطة به.

لذا، لاتزال الشركات التجارية في وضع حرج أمام تزايد المخاطر السيبرانية والأضرار الخطيرة التي قد تنتج عنها، والسبب في ذلك أنها قد تتعرض للخسارة مرتين: **الأولى** عندما تقع ضحية الهجمات السيبرانية أما **الثانية** فتتحقق عندما تمتنع شركة التأمين عن تغطية الأضرار الناجمة عن البعض من تلك المخاطر بسبب إستثناءها من التغطية، والتي كان يتصور المؤمن له إمكانية تغطيتها عند التعاقد بسبب عمومية صياغة بنود عقد التأمين من المخاطر السيبرانية، والتي تفتقر للدقة والتحديد، أو قد يكون بسبب الحدود الضيقة للتغطية الراجعة لكثرة الإستثناءات الواردة في العقد بسبب السياسة المتبعة من قبل بعض شركات التأمين، فوثائق التأمين من المخاطر السيبرانية في الغالب لا تغطي بشكل كاف جميع المخاطر

== انظر القرار القضائي للمحكمة العليا في انجلترا في قضية:

AIG Europe Limited vs Woodman (and others)/ 22 march / [2017] UKSC 18:
https://www.insurancelaw.london/2017/03/aig-europe-limited-v-woodman-and-others-2017-uksc-18
date of visit 13/11/2023 7:30pm.

الناشئة عن العمل التجاري في الفضاء السيبراني، فهي ليست مصممة لتغطية جميع الخسائر والتكاليف المحتملة الناتجة عن الجرائم الإلكترونية والأخطاء البشرية وفشل النظام وغيرها من المخاطر السيبرانية(١). وبما إن وثائق التأمين التقليدية تغطي الأخطار ذات الطبيعة المادية أي تلك التي تخلف ضرراً مادياً، لذا فإنها تستبعد المخاطر السيبرانية كونها مخاطر غير ملموسة على الرغم من أنها قد تخلف اضراراً مادية او غير مادية، مما أدى الى حدوث نزاعات قضائية في هذا الشأن خلصت بأن الضرر الحاصل لأنظمة التشغيل التابعة للشركة او بياناتها ذات طبيعة مادية لأنها ذات قيمة مادية والضرر الذي يقع عليها هو ضرر مادي(٢) وكذلك الحال بالنسبة للعملات المشفرة حيث قضت المحكمة العليا في المملكة المتحدة بخصوص التأمين على الأصوال المشفرة بأنها ممتلكات قابلة للتعرض للمخاطر الإلكترونية وتسبب ضرراً مادياً (٣).

في حين أن بعض المحاكم قضت بأن مسؤولية شركة التأمين لا تشمل الأضرار الناجمة عن إستخدام الأرقام التسلسلية الإلكترونية أو أرقام تعريف الهاتف المحمول أو التصميم ؛ لأنها ممتلكات غير مادية ، وبما أن مبلغ التأمين يتحدد بمقدار الضرر لذا فإن التأمين من المخاطر السيبرانية يجب أن يتمحور حول الأخطار التي تسبب أضراراً مادية او أضراراً معنوية محددة تحديداً دقيقاً(٤). ومع ذلك فأن شركات التأمين التي تتعامل مع الخطر السيبراني غالباً ما تستثني تغطية المخاطر الآتية:

١. التأمين من الغرامات سواء كانت غرامات جزائية أو إدارية فمن غير الممكن عموماً التأمين منها حيث أن شركات التأمين من المخاطر السيبرانية في الغالب تمتنع عن تغطية مبلغ الغرامة التي يتم فرضها على الشركات التجارية بسبب خرق أحكام اللائحة الاوروبية العامة لحماية البيانات (GDPR)(٥). فالتأمين على الغرامة المفروضة على الشركة التجارية نتيجة خرق بيانات عملائها هو

(١) محمد سعيد اسماعيل، مصدر سابق، ص٣١٩.

(٢) اسراء فهمي ناجي، مصدر سابق، ص١٩٨.

(3) THE HIGH COURT OF JUSTICE، BUSINESS & PROPERTY COURTS OF ENGLAND AND WALES COMMERCIAL COURT (QBD) IN PRIVATE، CL-2019-000746, (reporting restrictions lifted and released for publication, 17 January 2020).
http://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html
date of visit 18/7/2023 7:30 pm

(٤) اسراء فهمي ناجي، مصدر سابق، ص١٩٨.

(5) Even Langfeldt Friberg op.cit, p48.

أمر غير وارد تغطيته عموماً من قبل شركات التأمين ويتم استثناءه غالباً في عقود التأمين من المخاطر السيبرانية.

٢. المخاطر الناشئة عن فشل في الصيانة أو عدم الحفاظ على الحد الأدنى من معايير الأمان وغالباً ما يرد هذا الإستثناء في العقد بصيغة معينة مثل "عدم التأكد من أن نظام الكمبيوتر محمي بشكل معقول من خلال ممارسات الأمان وإجراءات صيانة الأنظمة التي تعادل أو تزيد عن تلك التي تم الكشف عنها في العقد" أو "عدم التنفيذ المستمر للإجراءات وضوابط المخاطر المحددة لدى المؤمن له" ففي عام ٢٠١٤، رفع مساهمون دعوى جماعية ضد (**Cottage Health**) [١] وهي شركة تدير مجموعة من المستشفيات في جنوب ولاية كاليفورنيا في الولايات المتحدة، بإنتهاك أحكام قانون يتعلق بسرية المعلومات الطبية لولاية كاليفورنيا بعد أن نشرت الشركة عن غير قصد معلومات سرية للعميل عبر الإنترنت كانت موجودة على خوادمها حيث أن خطأ أحد الموظفين كان عاملاً مساهماً في وقوع الخطر السيبراني، وبناءً عليه قررت محكمة مقاطعة الولايات المتحدة/ الدائرة التاسعة في كاليفورنيا تغريم الشركة ؛ كونها تفتقر إلى الضوابط الأساسية مثل التشفير و إنتهاكها لقانون (HIPAA) [٢].

٣- على الرغم من أن عقود التأمين من المخاطر السيبرانية تغطي الضرر الناجم عن استخدام الهندسة الاجتماعية في الإحتيال الإلكتروني إلا أن العديد من نماذج التغطية تحتوي على بنود تسمح لشركة التأمين بالتنصل من تغطية هذه الأضرار في الحالات الآتية:

أولاً: عندما يكون الخطر السيبراني ناتجاً عن تجاوز ضوابط الأمان الخاصة بالشركة التجارية.

---

(1) COLUMBIA CASUALTY COMPANY Plaintiff v. COTTAGE HEALTH SYSTEM Defendant.
Court: United States District Court, Ninth Circuit, California, C.D. California Date published: May 7, 201:
https://casetext.com/case/columbia-casualty-co-v-cottage-health-system
date of visit 1/5/2023 6:00pm.

(٢) مصطلح HIPPA يعبّر عن قانون نقل التأمين الصحي والمسائلة (Health Insurance Portability and Accountability Act) والذي تم تشريعه عام ١٩٩٦ لغرض حماية الوثائق الطبية والمعلومات الطبية الخاصة الأخرى، بحيث يشمل هذا القانون حماية السجلات الطبية بشكلها الإلكتروني والورقي أيضًا للمزيد انظر:
https://www.cdc.gov/phlp/publications/topic/hipaa.html.
تاريخ الزيارة ٢٠٢٢/٩/١ الساعة ٨:٠٠م.

ثانياً: حالة تحقق الخطر السيبراني بفعل المؤمن له كأن يتم تحويل الأموال نتيجة حدوث الإحتيال الإلكتروني بصورة إرادية أو من قبل أشخاص طبيعيين مخولين لدخول نظام الكمبيوتر الخاص بالشركة.

ثالثاً: عند تنفيذ عملية الاحتيال عبر الهاتف بدلاً من استخدام الكمبيوتر مباشرةً.

رابعاً: عندما تكون الخسائر المتكبدة هي أضرار غير "مباشرة" للمؤمن له كأن تكون خسائر في أموال العملاء(١).

٤- توفر معظم عقود التأمين من المخاطر السيبرانية تغطية للتكاليف المتعلقة بإستعادة البيانات أو إستبدالها أو معالجتها. لكن نلاحظ بعض عقود التأمين تشترط أن تكون البيانات "تالفة" أو "مدمرة". فإذا ما قامت إحدى عصابات برامج الفدية بسرقة بيانات الشركة دون إتلافها ورفضت الإفراج عن الملفات، فيمكن القول أن البيانات قد سُرقت أي أنها لم تتضرر أو تتلف ؛ لذا سيتم استثناء شمولها بالتغطية التأمينية. الأمر الذي يستوجب على حاملي وثائق التأمين من المخاطر السيبرانية من الشركات التجارية التأكد من أن وثيقة التأمين تتضمن أيضًا بشكل صريح تغطية الضرر الناجم عن فقد أو سرقة البيانات(٢).

كما يشترط لتغطية الخسائر الناتجة عن سرقة البيانات أو إختراقها أن يكون هناك نشر للبيانات المتسمة بالخصوصية، وهذا ما أكدته محكمة الإستئناف في الولايات المتحدة / الدائرة الخامسة في قضية شركة (لاندريز للتأمين) في بنسلفانيا ضد سلسلة فنادق شهيرة تعرضت لإختراق أنظمة البيانات الموجودة في الكمبيوتر الخاص بها بسبب التقاط برامج ضارة قام المتسللون بتثبيتها على انظمة الكمبيوتر الخاصة بسلسلة الفنادق ونقل المعلومات السرية الواردة فيها(٣). وفي اعتقادنا أن القرار السابق محل نظر حيث أن اشتراط وجود تلازم بين النشر وبين الإستحقاق لمبلغ التأمين أمر غير

(1) Miss. Silicon Holdings v. Axis Ins. Co., No. 20-60215 (5th Cir. Feb. 4, 2021): https://casetext.com/case/miss-silicon-holdings-llc-v-axis-ins-co-2 date of visit 14/5/2023.

(2) Avoiding The Most Common Cyber Insurance Claim Denials report. https://www.gbainsurance.com/avoiding-cyber-claim-denials

تاريخ الزيارة ٢٠٢٣/٥/٢ الساعة ٦:٠٠م.

(3) Landry's Incorporated, as successor in interest to Landry's Management, United States Court of Appeals, Fifth Circuit, Date published: Jul 21، 2021. https://casetext.com/case/landrys-inc-v-the-insurance-company-of-the-state-of-pennsylvania date of visit 10/8/2023 9:00pm

دقيق ذلك أن الضرر الناجم عن انتهاك البيانات الخاصة قد يتحقق من دون حدوث نشر أو اعلان لتلك البيانات الخاصة بالعملاء ، فبمجرد تعرف المتسللين على هذه البيانات الخاصة يحقق ذات الضرر الذي يحققه نشر المعلومات حيث من الممكن أن يبتز المتسللون العملاء بناءً على المعلومات الخاصة التي تم الحصول عليها نتيجة اختراق نظام الكمبيوتر في الفندق وبالتالي يتم إلحاق الضرر بالعملاء في كلتا الحالتين، سواء تم النشر ام لم يتم.

٥- الالتزامات التعاقدية التي يتحملها المؤمن له خارج نطاق وثيقة التأمين من المخاطر السيبرانية: وتشمل أي إلتزام بموجب أي عقد أو إتفاقية أو أي ضمان يقبله المؤمن له (الشركة التجارية) حيث تستثني شركة التأمين من المخاطر السيبرانية المطالبات المتعلقة بالالتزامات التعاقدية الملقاة على عاتق الشركة التجارية تجاه الغير بعد تحقق الخطر السيبراني كالغرامات التنظيمية التي تفرضها بعض المنظمات غير الحكومية[١] مثل منظمة (PCI)[٢].

خلص قرار صدر مؤخرًا عن المحكمة الجزائية الأمريكية لمقاطعة أريزونا – شركة (PF Chang's China Bistro، Inc.) ضد شركة التأمين الفيدرالية – إلى أن ما يقرب من ٢ مليون دولار من الرسوم التي تكبدتها شركة (PF Chang's) بعد اختراق البيانات، لم يتم تغطيتها من خلال وثيقة التأمين السيبراني، تم فرض الرسوم والغرامات المعنية من قبل (Bank of America Merchant Services "BAMS")، وهي شركة تابعة لجهة خارجية تقدم خدمات تتعلق بمعالجة مدفوعات بطاقات الائتمان الخاصة بعملاء (PF Chang)، وافقت شركة (PF Chang)على تعويض (BAMS)عن أي رسوم أو غرامات أو عقوبات أو تقييمات مفروضة عليها من قبل جمعيات بطاقات الائتمان مثل MasterCard أو Visa. . وجدت المحكمة وثيقة شركة التأمين Chubb

(1) (QBE)Cyber Response Insurance Policy،Danmark:
https://qbe.dk/media/8241/qbe-cyber-response.pdf
date of visit 2/8/2023 3:00am.

(٢) وهي منظمة تهدف إلى تحسين أمان معاملات بطاقات الائتمان والخصم والبطاقات النقدية وحماية حاملي البطاقات من إساءة استخدام معلوماتهم الشخصية وتفرض غرامات على المخالفين وقد تم إنشاء (PCI DSS) بشكل مشترك في عام ٢٠٠٤ من قبل أربع شركات رئيسية لبطاقات الائتمان: Visa و MasterCard و Discover و American Express.

https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

تاريخ الزيارة ٢٠٢٢/٨/٢٣ الساعة ٤:٠٠م

– Policy لم توفر تغطية للرسوم المفروضة على شركة (PF Chang)لأن كل من رسوم إدارة القضية وتقييمات السداد التشغيلي والتعافي من الاحتيال تقع ضمن نطاق الاستثناء الذي يمنع تغطية الالتزامات التعاقدية التي يتحملها المؤمن له خارج نطاق عقد التأمين من المخاطر السيبرانية(١).

وبإعتقادنا أن قرار المحكمة كان صائباً ذلك أن بنود العقد صريحة في ذكر استثناء الإلتزامات التعاقدية من شمولها بالتغطية، و يمكننا أن نستنتج من ذلك وجوب تدقيق الشركات التجارية طالبة التأمين في شروط واستثناءات عقود التأمين من المخاطر السيبرانية لشركات التأمين، بهدف ضمان أن النموذج الذي تم التوقيع عليه لا يحتوي على أي بنود غامضة أو عامة أو صياغة تتطلب من المؤمن له الامتثال لدرجة عالية من ضوابط الأمن السيبراني فضلاً عن ذلك نعتقد أن على الشركات الراغبة في التأمين من المخاطر السيبرانية العمل بشكل وثيق مع المتخصصين أمن المعلومات وتقنية المعلومات من أجل تأكيد دقة جميع البيانات الواردة في العقد.

٦– إستثناءات الحرب والإرهاب: نظرًا لأن هجمات برامج الفدية غالبًا ما يتم نشرها من قبل جهات فاعلة أجنبية والنظر في احتمالية أن تكون الهجمات ترعاها دولة ما، يجب على حاملي وثائق التأمين مراجعة الاستثناءات التي تستبعد الحرب والارهاب لتجنب عدم تغطية الاضرار الناتجة عن برامج الفدية نتيجة الحروب الالكترونية فقد تستثني شركات التأمين تغطية الاضرار الناجمة عن برامج الفدية مثلاً اذا ماكان هناك شك أن المبتزين هم إرهابيون(٢).

٧– السلوك غير النزيه: وهو كل فعل أو إغفال متعمد أو إجرامي أو إحتيالي أو غير آمن، أو الانتهاك المتعمد لأي واجب أو التزام عقدي أو قانون أو لائحة، كأن تتسبب الشركة التجارية المؤمن لها في خسارة انقطاع الأعمال، فلا تنطبق سياسات التغطية على انقطاع الاعمال الذي يتم بصورة طوعية من قبل المؤمن له والتي تهدف إلى تحسين الوصول الى الشبكة أو وظائفها إلا انه يمكن ان تشمل التغطية عمليات الإغلاق الطوعية المرتبطة بالظروف الإستثنائية للحدّ من انتشار بعض المخاطر السيبرانية كالبرامج الضارة والفيروسات أو الحد من الضرر الناجم عن هذه المخاطر(٣).

---

(1) P.F. Chang's China Bistro، Inc.، Plaintiff, v. Federal Insurance Company, court: united states district court for the district of Arizona, no. cv-15-01322-phx-smm, date published: May 26, 2016.
https://casetext.com/case/pf-changs-china-bistro-inc-v-fed-ins-co
date of visit 11/9/2023 8:00 pm

(2) Steven Hadwin, Norton Rose op.cit, p13.

(٣) محمد سعيد اسماعيل، مصدر سابق، ص ٢.

٨- قد تتضمن عقود التأمين من المخاطر السبرانية أحياناً تاريخ نفاذ بأثر رجعي، بحيث يتم استثناء الخسائر الناتجة عن الحوادث التي حدثت قبل التاريخ بأثر رجعي من شمولها بالتغطية من المخاطر السيبرانية، حيث طبيعة الخطر السيبراني قد تحتم أن تمر شهور أو أحياناً سنوات قبل أن يتم تحديد خرق للأمن السيبراني. وعادة ما يكون التاريخ بأثر رجعي هو اليوم الذي تدخل فيه الوثيقة التأمين حيز التنفيذ.، حيث يمكن لطالب التأمين في كثير من الأحيان التفاوض على تاريخ بأثر رجعي يسبق تاريخ دخول العقد حيز التنفيذ(١).

٩- الاستثناءات المرتبطة بسرقة بيانات موظفي الشركة التجارية: حيث تستثني عقود التأمين من المخاطر السيبرانية المطالبات المتعلقة بسرقة بيانات موظفي الشركة التجارية، فمعظم هذه العقود تشتمل على تغطية بيانات العملاء دون غيرها(٢).

١٠- ويذهب البعض إلى أنه لا يمكن أن تشمل التغطية التأمينية انتهاكات السرية والخصوصية ؛ لأنه في الغالب يكون تقييم الأضرار التي لحقت بالمؤمن له أو عملائه يكاد يكون مستحيلاً وعلى وجه الخصوص عند عدم التعرف على الجاني والذي غالباً ما يكون من الصعب بمكان العثور على دليل لحدوث الاختراق لذا يفترضون ان المخاطر المؤدية لإنتهاك الخصوصية غير قابلة للتأمين بسبب صعوبة الإثبات(٣).

وبإعتقادنا أن مخاطر انتهاك السرية والخصوصية للشركات التجارية و عملائها تكاد تكون السبب الرئيس لظهور الحاجة للتأمين من المخاطر السيبرانية، حيث أن هدف هذه المخاطر بالدرجة الأساس هو خرق الخصوصية والسرية واستهداف البيانات لغرض إلحاق الخسائر الفادحة بالشركة التجارية وعملائها سواء أكانت خسائر مادية تلحق بأموال الشركة أم خسائر معنوية كتلك التي تلحق بسمعتها التجارية، فلا يمكن تصور تحقق خطر سيبراني لشركة تجارية ما دون انتهاك خصوصيتها، لذا فإن استثناء انتهاكات الخصوصية من التغطية سيؤدي إلى إنعدام الفائدة من التأمين على باقي

(1) chohen and co., 5 Cyber Liability Insurance Fundamentals for Your Business، July 09, 2021.
https://www.cohencpa.com/knowledge-center/insights/july-2021/5-cyber-liability-insurance-fundamentals-for-your-business date of visit 12/972022 6:00pm
(2) cyber insurance: a guide for smes, p8.
https://hamiltonleigh.com/cyber-insurance-a-guide-for-smes/
date of visit 28/5/2024.
(3) Torsten Grzebiela, op.cit, p7.

المخاطر السيبرانية كونها جميعاً تتحق من خلال حدوث إنتهاك الخصوصية أو سرقة البيانات، لكن هذا لا ينفي صواب الرأي السابق بشأن صعوبة تقدير التعويض الناتج عن انتهاك الخصوصية وسرقة البيانات كونها مسألة يختلف تقديرها بإختلاف طبيعة نشاط الشركة التجارية وحجمها وماهية عملائها.

١١- لا يمكن شمول الخطر السيبراني بالتغطية التأمينية إذا ما كان مصدر الخطر من داخل شركة المؤمن له كمشغلي الشبكة ومقدمي الخدمة أو عاملي الصيانة كون إمكانية تحقق الخطر تكون أكثر احتمالاً من المصادر الخارجية، فيفترض أن موظفي الشركة يمتلكون الخبرة التي تمكنهم من إختراق نظام الشركة التجارية بالإضافة إلى معرفتهم بأسرار الشركة التجارية بحكم عملهم داخلها مما يؤدي إلى صعوبة في تقييم الخطر بسبب تنوع مصادره. لذلك غالباً ما يتم استثناء المخاطر السيبرانية المتأتية من هذه المصادر من شمولها بالتغطية السيبرانية، و مع ذلك هناك من يرى أنه من الممكن أن تغطي بعض وثائق التأمين ذلك إذا ما نص العقد على شمولها صراحة و بصورة مستقلة ولا يشترط أن يحقق الخطر السيبراني الضرر مادياً بل يكفي في بعض الأحيان أن يرجع المتضرر على أساس الكسب الفائت نتيجة توقف الخدمة مثلاً[١].

١٢- كما تستبعد دائما شركة التأمين من المخاطر السيبرانية تلك الخسائر الناتجة عن تعطل المرافق العامة مثل الغاز والماء ومزودي خدمات الإنترنت والأقمار الصناعية. كما إن شركات التأمين محل البحث لا تهدف الى جعل المؤمن له في وضع افضل مما كان عليه قبل تحقق الخطر لذا فهي تستبعد تكلفة استعادة النظام الى مستوى وظيفي أعلى مما كانت عليه[٢]. وعلى الرغم من ان شركات التأمين في الغالب توفر غطاء لبعض الأضرار الصادرة نتيجة إهمال أو إغفال موظفي الشركة التجارية، إلا أن هذا الغطاء لا يمتد أثره إذا ما تسبب المؤمن له بصورة متعمدة بالخطر المؤمن منه، وهذا ما أكدته المحكمة العليا في المملكة المتحدة في احدى قرارتها الصادرة بهذا الشأن حيث قررت أن صاحب العمل أو الإدارة العليا غير مسؤولة عن تسبب بعض الموظفين سيئي النية بحدوث خرق في البيانات[٣].

(1) Philip Rawlings, Cyber Risk: Insuring the Digital Age, British Insurance Law Association Journal، volume (128), Paper No. 189/2015, Queen Mary School of Law Legal Studies Research, p5.

(2) Steven Hadwin, Norton Rose op.cit, p13.

(3) WM Morrisons Supermarkets plc (Appellant) v Various Claimants (Respondent), Judgment date, 01 Apr 2020, Neutral citation number, [2020] UKSC 12, Case ID UKSC 2018/0213:
https://www.supremecourt.uk/cases/uksc-2018-0213.html
date of visit 13/11/2022 8:00 pm.

وبإعتقادنا ان القرار محل نظر من ناحية عدم اقرار المحكمة لمسؤولية الشركة التجارية عن موظفيها عند حدوث خرق للبيانات الخاصة بالعملاء، حيث أن الشركة التجارية يجب أن تلتزم بتعويض الأضرار الصادرة عن موظفيها سيئي النية كون الموظف تابع لهذه الشركة، ولا يمنع ذلك رجوع الشركة بمبلغ التعويض على الموظف المسؤول عن الضرر فيما بعد، فالعميل يتعاقد مع الشركة التجارية ككل ويضع ثقته بموظفيها فمن غير المنصف أن تتنصل الشركة من دفع التعويض خصوصاً وأنها ملزمة بواجب الاشراف والرقابة على أفعال موظفيها سواء كان تحقق الخطر السيبراني ناتجاً عن عمد أم إهمال.

١٣- كما قد يم ردّ العديد من الدعاوى بسبب عدم إختصاص المحاكم المعروض أمامها النزاع حيث من الضروري أن تتحقق الشركة التجارية من المحكمة المختصة إذا ما ثار نزاع حول التغطية التأمينية مستقبلاً والذي يتم النص عليه غالباً في عقد التأمين من المخاطر السيبرانية، فلكل دولة او ولاية قوانينها التي تنطبق على منازعات عقد التأمين من المخاطر السيبرانية و التي تبين المحاكم المختصة بالنظر في منازعات تلك العقود فعلى سبيل المثال التغطية التي يتم شراؤها في المملكة المتحدة من الممكن أن تمتد لتشمل المخاطر السيبرانية الواقعة خارج حدود المملكة كدول الإتحاد الأوروبي وبعض الدول بينما قد يستثني عقد التأمين من المخاطر السيبرانية تلك المخاطر الواقعة في الولايات المتحدة أو كندا من اختصاص محكمة دولة العقد [١].

١٤- إن وثائق التأمين من المخاطر السيبرانية تستثني الأضرار التي تلحق بالممتلكات المادية أو الإصابات الجسدية الناتجة عن تحقق أحد المخاطر السيبرانية محل العقد من شمولها بالتغطية إلا أنه بالوقت ذاته يمكن لبعض عقود التأمين التقليدية أن تغطي بطريقة غير مباشرة الأضرار الحاصلة في الممتلكات المادية والاصابات الجسدية الناتجة عن أحد المخاطر السيبرانية في الشركة التجارية من خلال التأمين من المسؤولية العامة، وهذا ما يعرف ب (التغطية الصامتة للمخاطر السيبرانية) والتي تعرض شركات التأمين التقليدية لإلتزامات تثقل من كاهلها عند التعويض عن الاضرار الناتجة عن المخاطر السيبرانية دون ان تكون تلك المخاطر هي المشمولة بالتغطية[٢].

(1) Philip Rawlings 0p. cit, p13.

(2) kenneth s. Abraham, Daniel schwarcz, Courting disaster: the underappreciated risk of A Cyber insurance Catastrophe, Connecticut insurance law jornal vol (27), issue (2), 2021, p4.

تعد قضية (Miss. Silicon Holdings v. Axis Ins)[١] والمتعلقة بالنزاع حول بعض بنود عقد التأمين من المخاطر السيبرانية، من أبرز وأحدث القرارات القضائية لمحكمة الإستئناف الأمريكية/ الدائرة الخامسة في مجال التأمين من المخاطر السيبرانية. حيث ثار النزاع بين المدعي (شركة ميسيسيبي سيليكون القابضة/ شركة ذات مسؤولية محدودة) وبين المدعى عليه (شركة اكسيس للتأمين) حول تفسير بنود العقد المبرم بينهما والإدعاء على شركة اكسيس للتأمين بخرق بنود عقد التأمين من المخاطر السيبرانية المبرم بينهما بالإضافة لمطالبة شركة ميسيسيبي بأحقيتها بمبلغ التغطية المنصوص عليه في العقد بالرغم من ادعاء شركة التأمين بأن الضرر الناتج عن الاحتيال الالكتروني والهندسة الاجتماعية وتحويل الاموال لم يتسبب به الطرف المهاجم مباشرةً وانما تسبب في إحداثه موظف تابع للمؤمن له وتحت سيطرته الفعلية. حيث اقدم مصرف (Trustmark) على تحويل الأموال إلى حساب بنك الائتمان البلغاري الأمريكي المزيف وفقًا للتعليمات المحددة والتفويض المقدم من موظفي (MSH) (الطرف المؤمن له) نتيجة ورود بريد إلكتروني إحتيالي اليه صادر من البنك سابق الذكر، إلا ان ما يعيق المؤمن له في الحصول على مبلغ التغطية هو أن تعليمات التحويل التي اعتمد عليها (Trustmark Bank) لإكمال التحويل لم تكن صادرة من دون علمه أو موافقته حيث أن جميع الموظفين الثلاثة التابعين للمؤمن له، الذين يتصرفون بشكل مستقل عن بعضهم البعض، قد سمحوا لبنك (Trustmark) بإكمال التحويلات وكان النزاع حول ثلاثة بنود وهي:

١. (سيدفع المؤمن مبلغ التغطية عند خسارة الأموال أو الأوراق المالية الناتجة مباشرة عن تحويل أو دفع أو تسليم الأموال أو الأوراق المالية من المبنى أو حساب التحويل إلى شخص أو مكان أو حساب خارج عن سيطرة الكيان المؤمن له عن طريق موظف أو مؤسسة مالية يتصرف بحسن نية بالاعتماد على تعليمات هاتفية أو مكتوبة أو إلكترونية ولكن في الواقع لم يتم إصدارها من قبل العميل أو الموظف أو البائع).

(١) انظر قرار محكمة الاستئناف بالولايات المتحدة للدائرة الخامسة في قضية:
Miss. Silicon Holdings v. Axis Ins. Co.، No. 20-60215 (5th Cir. Feb. 4، 2021)
https://casetext.com/case/miss-silicon-holdings-llc-v-axis-ins-co-2
تاريخ الزيارة ٢٠٢٣/٣/١٣ الساعة ١٢:٠٠م

٢. (سيدفع المؤمن مقابل الخسارة أو الخسارة الناتجة عن الضرر الذي يلحق بالممتلكات المغطاة و الناتج مباشرةً عن الاحتيال في نقل الكمبيوتر الذي يتسبب في نقل أو دفع أو تسليم الممتلكات المغطاة من المبنى أو حساب النقل إلى شخص أو مكان أو حساب خارج نطاق الكيان المؤمن عليه ، دون علم أو موافقة الكيان المؤمن عليه).

٣. (وقوع خسارة ناتجة بصورة مباشرة من تحويل الأموال إلى شخص أو مكان أو حساب خارج عن سيطرة الكيان المؤمن له من قبل مؤسسة مالية تعتمد على تعليمات مكتوبة أو إلكترونية أو برقية أو عن بُعد يُزعم أنها تعليمات تحويل تم إصدارها بالفعل دون علم أو موافقة الكيان المؤمن له).

وقررت المحكمة بإن الحصول على مبلغ التغطية غير ممكن لأنه "لم يتم إدخال شيء "أو" لم يتم تغيير شيء "داخل نظام الكمبيوتر وإنما قام المؤمن له بفعل إيجابي وهذا يعني أن "الإحتيال الإلكتروني" وتحويل الأموال لم يحدث بشكل مباشر نتيجة الخطر السيبراني وإنما نتيجة تدخل المؤمن له والموظفين التابعين له. لذا يمكن للمؤمن له ان يحصل على مبلغ التغطية بناء على بند خطر الهندسة الاجتماعية دون الخطرين السيبرانيين الآخرين المؤمن عليهما.

وفي إعتقادنا ان قرار المحكمة كان صائباً حيث إن بنود العقد واضحة وصريحة بشأن الشروط الواجب توافرها بالخطر السيبراني لتم شموله بالتغطية الواردة في عقد التأمين من المخاطر السيبرانية حيث استبعد صراحة الخطر الذي يتسبب به المؤمن له من التغطية كما هو الحال في عقود التأمين التقليدية الأخرى، ومن خلال إستخدام مفهوم المخالفة فإننا نصل إلى استنتاج مهم مفاده أن المخاطر السيبرانية الواردة في القرار أعلاه سيتم استثنائها من التغطية التأمينية إذا ما تم فقد أحد الشروط الواردة في عقد التأمين من المخاطر السيبرانية، كعدم حدوث خسارة للمؤمن له أو أن الخسارة قد وقعت بصورة غير مباشرة نتيجة تدخل فعل مادي خارج عن الاجهزة الالكترونية كأن يكون الخطر قد وقع بسبب طرف تابع للشركة المؤمن لها أو أن الفعل الذي نتج عنه الخطر السيبراني قد تم بموافقة المؤمن له.

وفي قرار آخر نجد أن محكمة الاستئناف/ الدائرة التاسعة في الولايات قد أصدرت حكم مخالف للحكم أعلاه ففي العام (٢٠٢٢) قضت المحكمة بأن الخسارة الناتجة عن الأمر الصادر من موظف بتحويل مبلغ مالي إلى حساب مؤسسة بعد تلقيه رسائل بريد إلكتروني إحتيالية من قبل شخص يدعي أنه طرف مختص بإصدار تلك الأوامر تأمره بتحويل الأموال إلى تلك المؤسسة، من الممكن شمولها

بالتغطية الواردة في عقد التأمين من المخاطر السيبرانية كونها تندرج ضمن بند الاحتيال الإلكتروني وتحويل الأموال حتى وإن صدر من الموظف فعل إيجابي ساهم من خلاله بإحداث الخطر السيبراني والأضرار الناشئة عنه، حيث سببت المحكمة قرارها بأن رسائل البريد الإلكتروني الإحتيالية هي السبب المباشر للأضرار، ورفضت إتجاه بعض المحاكم التي اعتبرت فعل الموظف وهو إرسال البرقية هو السبب المباشر للضرر، وليس الطرف المحتال المرسل للبريد الإلكتروني الاحتيالي، والذي وجه الموظفة لبدء عملية التحويل. و رفضت المحكمة حجة شركة التأمين بأن عقد التأمين من المخاطر السيبرانية المبرم يغطي فقط العمليات الإحتيالية الإلكترونية المرسلة مباشرة من قبل طرف ثالث غير مصرح له ولا تغطي تلك التي يتسبب بوقعها موظفًا مخولًا، لذا قررت المحكمة بأن شركة التأمين ملزمة قانوناً بتغطية الخسائر الناتجة عن الخطر السيبراني في جميع ألاحوال[1].

وبإعتقادنا أن القرار الأخير قد قرر مبدأ مهم هو عدم العمل بحرفية بنود عقود التأمين من المخاطر السيبرانية وإنما الأخذ بروح النص كونه يتفق مع مبادئ العدالة وحسن النية.

المطلب الثاني

تمييز عقد التأمين من المخاطر السيبرانية عما يشتبه به من عقود

نظراً لحداثة موضوع التأمين من المخاطر السيبرانية، نجد أنه من الضروري التمييز بين عقد التأمين من المخاطر السيبرانية وبين العقود التي قد تثير نوعاً من اللبس والغموض للمتلقي للوهلة الأولى نظراً لوجود شيء من التقارب والتداخل فيما بينها.

ففي الوقت الذي لايزال فيه عقد التأمين الالكتروني محط إهتمام العديد من الفقهاء نظراً لقلة القواعد القانونية المتخصصة بتنظيم هذا النوع من العقود وإفساح المجال للقواعد العامة المتعلقة بالعقد الإلكتروني والتجارة الإلكترونية لتنظيم هذا العقد، كذلك الحال بالنسبة للأمن السيبراني الذي لا يزال تنظيمه التشريعي في بداياته، فالمشرع العراقي مثلاً لم يشرع الى هذه اللحظة قانون متخصص بالأمن السيبراني على الرغم من الحاجة إلى تشريعه سواءً للدولة أو لباقي الأشخاص الطبيعية والمعنوية فيها،

(1) Ernst & Haas Mgt. Co. v. Hiscox Inc.، 23 F.4th 1195 (9th Cir. 2022).
https://www.jdsupra.com/legalnews/commercial-crime-policy-covers-loss-4840071/
تاريخ الزيارة ٢٠٢٢/٧/١٢ الساعة ٢:٠٠ م.

حيث تم الإكتفاء بوضع استراتيجية للأمن السيبراني العراقي، في حين أن بعض التشريعات العربية المقارنة قد سبق وأن شرعت بعض قوانين الأمن السيبراني كقانون الأمن السيبراني الاردني رقم (١٦) لسنة ٢٠١٩ و قانون الامن السيبراني في المغرب رقم (٠٥,٢٠) لسنة ٢٠٢٠، و قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي رقم (٣٤) لسنة ٢٠٢١ و الضوابط الاساسية للامن السيبراني السعودي لسنة ٢٠١٨.

لذا سنخصص هذا المطلب للتمييز بين عقد التأمين من المخاطر السيبرانية وعقد التأمين الإلكتروني في فرعٍ اول، ثم التمييز بين عقد التأمين من المخاطر السيبرانية وعقود الامن السيبراني في الفرع الثاني.

الفرع الأول

تمييز عقد التأمين من المخاطر السيبرانية عن التأمين الالكتروني

إن الشكل التقليدي لعقد التأمين هو الشكل الورقي، فهذا ما إعتادته شركات التأمين عند التعاقد مع عملائها، إلا أنه مع غزو الوسائل الإلكترونية الحديثة لجميع قطاعات الحياة ولا سيما الأعمال التجارية، كانت لتلك الوسائل الاثر الكبير في تبسيط إجراءات التأمين من حيث الوقت والجهد، مما أدى الى إمكانية إفراغ العقد بصورة إلكترونية عن طريق إستخدام شبكات الانترنت وتقنيات المعلومات ذات الصلة لإنتاج وتوزيع الخدمات والمنتجات التأمينية.

وبما أن التأمين الالكتروني مصطلح حديث نسبياً من الناحية القانونية حيث يتم عرض خدمات التأمين وإجراء المفاوضات وتقديم الطلبات وإبرام العقد بصورة إلكترونية مرنة بعيدة عن التعقيدات الإدارية، لذا فأن عقد التأمين الالكتروني ما هو إلا عقد يلتزم به المؤمن بتقديم خدماته التأمينية وما يتعلق بها من عروض أو مفاوضات أو تعاقد أو دفع أقساط من خلال وسائل الكترونية[١].

وحيث أن عقود التجارة الإلكترونية بصورة عامة تمتاز بصعوبة تركيز العقد مكانياً بسبب إنعدام مجلس العقد بمفهومه المادي في هذا النوع من العقود (على الرغم من وجود مجلس عقد إلكتروني)، لذا لا يمكن تطبيق ذات القواعد التقليدية لتسوية التنازع في هكذا عقود، حيث يجب الأخذ بنظر

(١) حبيب عبيد مرزة العمارة و ماهر محسن عبود الخيكاني، التنظيم القانوني للتأمين الالكتروني، مجلة جامعة بابل للعلوم الانسانية، مجلد (٢٦)، عدد (٨)، ٢٠١٨، ص١٣٩.

الإعتبار خصوصية عقد التأمين الإلكتروني وما يستلزمه من عرض وقبول وتنفيذ في فضاء سيبراني غير مادي مما يصعب من أمر تركيز العقد مادياً في مكان محدد إضافة لصعوبة تحديد هوية الأطراف المتعاقدة وأهليتهم على عكس العقود التقليدية الأخرى(١).

ويثور التساؤل حول ما إذا كان عقد التأمين يحتاج إلى وسيلة إلكترونية بذاتها حتى يمكن أن نطلق عليه عقد تجاري إلكتروني بالمعنى القانوني الدقيق أو أنه لا يشترط وجود وسيلة إلكترونية بحد ذاتها لنكون أمام عقد تأمين الكتروني؟

انقسمت الآراء إلى اتجاهين، الأتجاه الأول وهو الإتجاه الموسع: حيث يستند هذا الإتجاه إلى تحديد المقصود بالتجارة الإلكترونية كون التأمين بإعتباره من المشاريع التجارية يعد عمل تجاري، وبما أن التجارة الالكترونية هي كل نشاط تجاري يتم بأستخدام وسيلة إلكترونية في كل مراحلها أو بعضها، لذا يعتبر التأمين عقد الكتروني بأستخدام أي وسيلة الكترونية من دون تحديد مرحلة معينة لأستخدامها(٢)، أما الإتجاه الثاني وهو الإتجاه الضيق: فيستند على أن ذاتية التجارة الالكترونية تكمن في تبادل البيانات بين طرفي العملية التجارية فلا نكون أمام عقد تأمين إلكتروني من دون إستخدام وسيلة تتيح تبادل البيانات(٣)، فقد نص قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة ١٩٩٦ في الفقرة (ب) من المادة الثانية منه والتي عرفت تبادل البيانات بأنه نقل المعلومات الكترونياً من حاسوب إلى آخر بإستخدام معيار تفق عليه لتكوين المعلومات(٤)، وكذلك المادة (٢) من التوجيه الأوروبي رقم (٩٧/٧) الصادر عن البرلمان والمجلس الأوروبي عندما عرفت العقد عن بعد بأنه كل عقد يتعلق

(١) محمد محمد حسن، حماية المستهلك الالكتروني في القانون الدولي الخاص، دار النهضة العربية، القاهرة، ٢٠١٣، ص٣؛ سلطان عبد الله محمود، عقود التجارة الإلكترونية والقانون الواجب التطبيق، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠، ص١٥٣.

(٢) نضال إسماعيل إبراهيم، أحكام عقود التجارة الإلكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥، ص١٧؛ سلطان عبد الله محمود، مصدر سابق، ص٢٥؛ ماجد محمد سليمان، العقد الإلكتروني، ط١، مكتبة الرشد، الرياض، ٢٠٠٩، ص٢٠.

(٣) حنان مليكه، عقد التأمين الالكتروني، مجلة جامعة دمشق للعلوم القانونية، العدد الاول المجلد (٢)، ٢٠٢٢، ص١٧٥ وما بعدها.

(٤) قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة ١٩٩٦، منشور على الموقع الرسمي للأمم المتحدة / لجنة الأمم المتحدة للقانون التجاري الدولي:

https://uncitral.un.org/ar/texts/ecommerce/modellaw/electronic_commerce

تاريخ الزيارة ٢٠٢٣/٥/٣ الساعة ٤:٠٠م.

بالبضائع أو الخدمات أبرم بين مورد ومستهلك في نطاق نظام لبيع أو تقديم خدمات عن بعد نظمه المورد الذي يستخدم لهذا العقد فقط تقنية أو أكثر للإتصال عن بعد لإبرام العقد وتنفيذه' قد ضيقت من نطاق العقود الإلكترونية إلى الحد الذي يتم استخدام وسائل التعاقد الإلكترونية في جميع مراحل العقد من حين إبرامه إلى حد تنفيذه(١).

ونتفق مع الإتجاه الموسع، فبالرجوع الى قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ يقصد بالعقد الإلكتروني بصورة عامة وفقاً للفقرة (١١) من المادة الأولى منه: "إرتباط الإيجاب الصادر من أحد المتعاقدين بقبول الآخر على وجه يثبت أثره في المعقود عليه والذي يتم بوسيلة الكترونية"، فالنص قد جاء عاماً مطلقاً لم يتم تقييد العقد بوسيلة معينة في مرحلة معينة من العقد لكي يتم اعتباره عقداً إلكترونياً بالمعنى الدقيق.

وقد منح القانون أعلاه للعقود الإلكترونية ذات الحجية القانونية الممنوحة للعقود الورقية وفق المادة (١٣/ أولاً) من القانون ذاته شريطة أن تكون المعلومات الواردة في العقد قابلة للتخزين والحفظ ويمكن استعادتها في أي وقت، مع إمكانية الإحتفاظ بها بشكل يسهل به إثبات مدى دقة المعلومات الواردة فيه عند إنشاء العقد الإلكتروني أو إرساله أو تسلمه دون قابليته للتعديل وأن تكون تلك المعلومات الواردة في العقد تدل على من أنشئ العقد أو تسلمه مع تاريخ ووقت الارسال والتسليم. ويجوز اثبات العقد الالكتروني بجميع طرق الاثبات المقررة قانوناً. وبالرغم من انه لم يتم تشريع قانون خاص بالتأمين الالكتروني في القانون العراقي إلا أنه من الممكن الرجوع إلى النصوص الواردة في قانون التوقيع الإلكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ للتوصل الى القواعد الرئيسية التي من خلالها يمكن ابرام عقد التأمين الالكتروني. ويمكننا تعريف عقد التأمين الإلكتروني بأنه "عقد تأمين يتم ابرامه أو تنفيذه من خلال أية وسيلة إلكترونية".

---

(١) التوجيه الأوروبي رقم (٩٧/٧) هو توجيه صادر عن البرلمان والمجلس الأوروبي في ٢٠ مايو ١٩٩٧ وهو يختص بحماية المستهلك في التعاقد عن بعد او عقود المسافة حسب تعبيرهم، كما يهدف الى تقريب القوانين واللوائح والأحكام الإدارية للدول الأعضاء فيما يتعلق بالتعاقد عن بعد بين المستهلكين والموردين. منشور على الموقع الرسمي للإتحاد الأوروبي:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31997L0007

تاريخ الزيارة ٢٠٢٣/٩/٢٧ الساعة ٥:٠٠م

ويشترك عقد التأمين الإلكتروني مع عقد التأمين من المخاطر السيبرانية بأن كلا العقدين يعتبران من عقود الاذعان فالمؤمن له يوافق على شروط محددة على وفق نماذج معدة مسبقاً ولا يملك الحق في مناقشة هذه الشروط فهو لا يملك إلا التوقيع أو عدمه[١]، كما أنهما عقود غير مسماة حيث يحكمهما القواعد العامة الواردة بالقوانين المنظمة للعقود والمعاملات والتجارة الالكترونية واللوائح ذات الصلة ولا توجد قواعد قانونية متخصصة بالتأمين الالكتروني أو التأمين من المخاطر السيبرانية لذا لا يمكن اعتبارهما ضمن العقود المسماة[٢]، بالإضافة إلى أن عقد التأمين من المخاطر السيبرانية يشترك مع عقد التأمين الإلكتروني بكونهما عقوداً عابره للحدود فوسائل التعاقد الإلكترونية تمكنت من تجاوز الحدود السياسية للدول فسهلت من عملية التعاقد خصوصاً تلك التي يكون أطرافها تابعين لأكثر من دولة واحدة، وكذلك الأمر بالنسبة لعقد التأمين من المخاطر السيبرانية حيث يمكن ان يغطي عقد التأمين الشركات التجارية مع فروعها المنتشرة في أكثر من دولة حول العالم[٣].

كما إنهما يعتبران من عقود حسن النية التي تقوم على الثقة المتبادلة بين الطرفين من خلالها ، حيث يلتزم أطراف عقد التأمين بالإفصاح عن جميع المعلومات والبيانات اللازمة للعملية التأمينية خلال مرحلة المفاوضات أو إبرام العقد. ويساهم التأمين الالكتروني في توسيع نطاق التجارة الالكترونية بإعتبارها وسيلة للمبادلات الالكترونية مما يشجع العقود الدولية وخاصة عقود الاستثمار من خلال التأمين على الإستثمارات من المخاطر وغير التجارية من خلال الدخول على مواقع شركات التأمين وإجراء العقد الكترونياً، مما يؤدي الى اختصار عمليات التأمين التقليدية والمطولة بأقل خطوات ممكنة كما يساهم في تقليل الوقت والكلفة على العملاء وتوفير الية سريعة لأداء الاقساط من خلال ميزة الدفع الالكتروني[٤].

ومن الجدير بالذكر ان الإشكالية الجوهرية في عقود التأمين الالكتروني هي أن شركة التأمين عندما تبرم أحد عقود التأمين مع المؤمن لهم في صورته الإلكترونية، فإنها لن تتمكن من الحصول على معلومات موثوقة من الطرف الآخر للعقد بسبب أن عملية التعاقد برمتها تتم بصورة إلكترونية

(١) حزام فتيحة، الاحكام المتعلقة بخدمات التأمين الالكترونية، مجلة جامعة محمد بوقرة بومرداس، مجلد (١٤) العدد (١)، ٢٠٢١، ص١٣ وما بعدها.

(٢) حنان مليكة، مصدر سابق، ص١٧٥.

(٣) لما عبد الله صادق، مجلس العقد الإلكتروني، رسالة ماجستير مقدمة إلى كلية الدراسات العليا / جامعة النجاح الوطنية، ٢٠٠٨، ص٢٧.

(٤) ماجد محمد سليمان، مصدر سابق، ص٢٤.

فمن الصعوبة بمكان إثبات صحة المعلومات الواردة في عقد التأمين الإلكتروني لسهولة إدعاء العكس[١].

وبالرغم من صدور قانون التوقيع الإلكتروني والمعاملات الإلكترونية في العراق نجد أن التأمين لا يزال يمارس وفق الصورة التقليدية وفقاً لممارسات شركة التأمين الوطنية.

وعلى الرغم من بساطة مفهوم عقد التأمين الالكتروني إلا اننا نجد البعض قد وقعوا في لبس من خلال إطلاق مصطلح (التأمين الالكتروني) على عقد التأمين من المخاطر السيبرانية وجعلهما مترادفين[٢]، ولعل ذلك يرجع الى حداثة المصطلحات في الفقه القانوني أو ربما جراء الترجمة غير الدقيقة للتأمين من المخاطر السيبرانية من اللغات الاجنبية الى اللغة العربية حيث نجد أن التأمين من المخاطر السيبرانية يتم ترجمته كمرادف لمصطلح التأمين الالكتروني على الرغم من وجود اختلاف كبير بين التأمين الالكتروني الذي ما هو إلا عقد تأمين إعتيادي ينشأ بوسيلة الكترونية ما بين المؤمن والمؤمن له وتتم فيه مراحل التعاقد من مفاوضات وإبرام العقد والتوقيع عليه والدفع بوسائل الدفع الالكتروني دون حاجة لأي مستند ورقي وفي الوقت نفسه يمتلك العقد الالكتروني ذات حجية العقد الورقي، أما عقد التأمين من المخاطر السيبرانية فهو عقد تأمين يتم من خلاله تغطية نوع جديد من

(1) Shergunova E.A، The Electronic Insurance in the Context of Innovative Development of Digital Law in Russia, volume (138), 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth” (MTDE 2020), P1.

(٢) فعلى سبيل المثال نجد ان الاتحاد المصري للتأمين قد وقع في هذا الخلط فمن خلال التدقيق بالمفردات القانونية لنشرة الاتحاد المعنونة "الهجمات الالكترونية (السيبرانية) والتأمين في العدد(٦٧) لسنة ٢٠١٩ نجد ان العناوين الواردة ضمن محتويات النشرة غير دقيقة ومنها:

- سوق التأمين الإلكتروني Cyber Insurance العرض والطلب
- التوقعات العالمية بأرتفاع حجم سوق التأمين السيبراني / الالكتروني.
- الهجمات الالكترونية (السيبرانية) خطر يهدد كبري الكيانات الاقتصادية.
- مخاطر التأمين الإلكتروني "المخاطر السيبرانية" وكيفية مواجهتها.

وبإعتقادنا ان الاجدر بالإتحاد اعتماد مطلح التأمين من المخاطر الالكترونية او التأمين من المخاطر السيبرانية بدلاً من ذلك كونه أدق من الناحية القانونية، وكذلك الحال بالنسبة لبعض المؤلفين كالدكتور محمد سعيد اسماعيل في بحثه الموسوم (التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة) وهو احد مصادرنا السابقة، وحيدر شكري فيصل، في رسالته الموسومه: التأمين على اعمال الارهاب الالكتروني عابر الحدود، رسالة ماجستير مقدمة الى معهد العلمين للدراسات العليا، ٢٠٢٣. حيث تم استخدام مصطلح التأمين الالكتروني للتعبير عن التأمين ضد المخاطر السيبرانية.

المخاطر غير الملموسة في الغالب والتي تقع في فضاء سيبراني وتسمى بالمخاطر السبرانية والتي تتمثل ببرامج الفدية وهجمات الحرمان من الخدمة وأعمال التصيد والاحتيال والهندسة الاجتماعية وهجوم الوسيط والقنابل المعلوماتية والهجمات الفيروسية وغيرها من المخاطر التي سبق بحثها وتشمل التغطية التأمينية نوع جديد من الأضرار غير المغطاة سابقا بالتغطيات التأمينية التقليدية مثل تغطية المسؤولية القانونية الناجمة عن إنتهاك حقوق الملكية الفكرية والتشهير و الأضرار المادية التي لحقت بالممتلكات و التعويض عن الاضرار بالسمعة و الرسوم والتكاليف الضرورية لحماية البيانات و إسترداد التكاليف والنفقات التي تكبدتها الشركة صاحبة التغطية المسؤولية القانونية الناجمة عن خرق الخصوصية والسرية وأمن تكنولوجيا المعلومات ، والخسائر الناجمة عن الإبتزاز الإلكتروني وغيرها من الاضرار التي قد تختلف بإختلاف الوثيقة المعنية بتأمين هذا النوع من المخاطر السيبرانية. ولا يوجد مانع قانوني من انعقاد عقد التأمين من المخاطر السيبرانية بصورة إلكترونية فيتم العقد بصورته الإلكترونية ليغطي مخاطر إلكترونية، لذا يمكننا أن نستنتج أن عقد التأمين الالكتروني هو عقد تأمين اعتيادي يتميز بطريقة إبرامه الإلكترونية بغض النظر عن طبيعة المخاطر التي يغطيها، بينما عقد التأمين من المخاطر السيبرانية هو عقد تأمين يغطي مخاطر غير تقليدية وقد يتم بصورة ورقية أو إلكترونية.

الفرع الثاني

تمييز عقد التأمين من المخاطر السيبرانية عن عقد الأمن السيبراني

لغرض فهم مدى ضرورة التأمين من المخاطر السيبرانية للشركات التجارية بشكل متكامل لا بدّ لنا أن نبين ماهية الأمن السيبراني في بادئ الأمر لنتمكن من تمييزه عن عقد التأمين من المخاطر السيبرانية.

إن مصطلح الأمن السيبراني أو ما يطلق عليه أمن المعلومات والحاسب الآلي من المصطلحات المشتقة من السيبرانية وهو أحد فروع التكنولوجيا التي تعنى بحماية أنظمة التشغيل والممتلكات الرقمية والشبكات والبرمجيات من المخاطر السيبرانية التي قد تؤدي في الغالب إلى إتلاف البيانات أو ابتزاز العملاء او السيطرة على العمليات التجارية للشركات ، فهو مجموعة من الأدوات والسياسات ومفاهيم الأمن الالكتروني والمبادئ التوجيهية وأساليب إدارة المخاطر لتقديم أفضل الممارسات والضمانات

لحماية البيئة الرقمية وأصول المستخدم وله تعريفات متعددة، حيث يستخدم المصطلح من منظور قانوني للإشارة إلى مجمل القوانين والنصوص الخاصة بالأمن وطرق تسيير الأخطار والممارسات التكنولوجية وكل ما يتعلق بأمن تكنولوجيا المعلومات والاتصالات سواء المستخدمة لحماية الدول أو المنظمات أو الاشخاص(١).

بينما يعطي البعض مفهوماً أوسع للأمن السيبراني فهو يتعلق بجميع الإجراءات التي تتم على الفضاء السيبراني سواء بعلم المالك أو بدون علمه بالإضافة إلى جميع التقنيات و المنتجات والجهود المبذولة للدفاع ضد المخاطر السيبرانية، كما عرف بأنه حالة تمنح القدرة بالتصدي لكل ما يعترض سلامة البيانات المخزنة أو المعالجة أو المنقولة للتجسس أو التغيير أو التلف ويتوسع الأمن السيبراني ليدخل ضمن مجالات متعددة كقضايا الأمن السيبراني التجاري وعقود التأمين من المخاطر السيبرانية، والعملات الرقمية، وقضايا الملكية الفكرية الرقمية، والقوانين السيبرانية، وقوانين حماية الخصوصية، والجرائم السيبرانية، بالإضافة لتداخله مع الإختصاصات الدولية كمسائلة الحكومات عن الهجمات السيبرانية الصادرة منها وغيرها من المجالات(٢).

وعرفت وزارة الدفاع الأمريكية الأمن السيبراني بأنه "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها الالكترونية والمادية من مختلف الجرائم والهجمات والتخريب والتجسس و الحوادث (٣). ويجد الباحث أن التعريف سالف الذكر اعطى مفهوم واسع للأمن السيبراني عندما شمل حماية المعلومات بشكليها الالكتروني والمادي في حين أن الأمن السيبراني ينشط في الفضاء السيبراني الذي يتميز بكونه وسط غير مادي، لذا كان من الافضل قصر الحماية على المعلومات الالكترونية دون المادية للسبب أعلاه.

---

(١) اسلام مصطفى جمعة، جريمة اختراق الامن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية، مجلد (١٢)، العدد (٣)، لسنة ٢٠٢٢ ص٧٢٣ وما بعدها.

(2) Yaniv HarelI, rad Ben Gal, and Yuval Elovici. Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. ACM Trans. Intell. Syst. Technol. vol.(8), issue(4), Article 49 (July 2017), p3.

(٣) صلاح مهدي هادي و زيد محمد علي اسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، كلية العلوم السياسية جامعة النهرين، مجلة قضايا سياسية العدد (٦٢)، السنة (١٢)، ٢٠٢٠، ص ٢٧٦ وما بعدها.

كما عرفه **المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC)** بأنه "الطريقة التي يقلل بها الأفراد والمؤسسات من مخاطر الهجمات السيبرانية"[١]، ويؤخذ على هذا التعريف أنه جاء مقتضباً ولم ينجح في تحديد مفهوم الأمن السيبراني بصورة دقيقة حيث أن الأمن السيبراني إجراء أو تدبير وقائي ضد المخاطر السيبرانية بصورة عامة ولا يقتصر فقط على الهجمات السيبرانية كونها تعني الهجمات التي تستهدف الدولة وانما الجرائم السيبرانية والاخطاء الالكترونية الصادرة من العميل ذاته.

وعُرّف من قبل **نشرة الاتحاد المصري للتأمين** بأنه مصطلح جامع لمجال واسع من القضايا بدءاً من أمن تكنولوجيا المعلومات وصولاً إلى التدابير الأمنية الرامية إلى مكافحة إساءة إستخدام الإنترنت والجرائم السيبرانية[٢] ، وبإعتقادنا أن هذا التعريف فيه نوع من التكرار كون أمن تكنولوجيا المعلومات يشمل مكافحة إساءة إستخدام الانترنت وما يتخلف عنه من جرائم سيبرانية كما أنه لم يحدد مفهوم الأمن السبراني وإنما حدد مجاله.

ونجد تقارب في تعريف الأمن السيبراني في قانون الأمن السيبراني الأردني وتعريف الهيئة الوطنية للأمن السيبراني السعودي حيث **عرفته المادة الثانية من قانون الامن السيبراني الاردني لسنة ٢٠١٩ بأنه** "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على إستعادة عملها وإستمراريتها سواء أكان الوصول إليها من دون تصريح أم سوء إستخدام أم نتيجة الإخفاق في إتباع الإجراءات الأمنية أم التعرض للخداع الذي يؤدي لذلك. "بينما **عرفته الهيئة الوطنية للأمن السيبراني السعودية بأنه**" حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات من أي إختراق أو تعطيل أو تعديل أو دخول أو استخدام أو إستغلال غير مشروع[٣].

---

(١) وفقاً للموقع الرسمي للمركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC):
https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
تاريخ الزيارة ٢٠٢٢/٩/١٠ الساعة ٢:٠٠ م.

(٢) نشرة الاتحاد المصري للتأمين، العدد (٦٧)، لسنة ٢٠١٩، مصدر سابق.

(٣) الضوابط الاساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني السعودية لسنة ٢٠١٨، ص٣٢.
منشورة على الموقع:
https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf
تاريخ الزيارة ٢٠٢٣/٩/١٦ الساعة ٧:٠٠م.

وتجدر الإشارة إلى أن الأمن السيبراني يهدف إلى المحافظة على سرية المعلومة وسلامتها وتوافرها كما يهدف إلى توفير المتطلبات الاساسية المتمثلة بالحفاظ على سرية المعلومات من التهديدات الخارجية والداخلية لتقليل المخاطر السيبرانية على الاصول المعلوماتية والتقنية لكافة الجهات وتتحقق الأهداف التي يرمي اليها الامن السيبراني في حال توفر ثلاثة محاور أساسية للحفاظ على امن المعلومات [١]:

المحور الأول (التقنية): وتتمثل بأدوات الأمان اللازمة لحماية النظام الخاص بالشركة من الهجمات الإلكترونية.

المحور الثاني: ويتمثل بالأشخاص والمنظمات من مستخدمي المعلومات والأنظمة.

المحور الثالث: (الأنشطة والعمليات): وهي الاجراءات التي يتم من خلالها توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة التي من شأنها التصدي للهجمات الالكترونية.

ومما تجدر الاشارة إليه أن الحفاظ على مستوى جيد من الامن السيبراني قد يتطلب بالضرورة التعاقد مع شركات متخصصة في مجال الأمن السيبراني أو توظيف مختصين في مجال تكنولوجيا المعلومات في الشركات التجارية لغرض حماية أنظمة التشغيل والبرامج من التعرض للمخاطر السيبرانية، وهذا بدورة يشكل عائقاً أمام العديد من تلك الشركات خصوصاً الصغيرة أو المتوسطة بسبب إرتفاع تكلفة عقود الأمن السيبراني، حيث أن إعتماد الشركات الصغيرة والمتناهية في الصغر على التكنولوجيا الرقمية في مقابل الخبرات المحدودة في مجال الأمن السيبراني وإرتفاع تكاليف الشركات الأمنية، قد أدى إلى طرح فكرة تمويل شركات الامن السيبراني من قبل الدولة ودعم المشاريع الصغيرة أمنياً لتوفير بيئة عمل تجارية رقمية آمنة بعيداً عن التكاليف الباهظة التي تؤدي بالشركات الى العزوف عن الاستعانة بخبراء الامن السيبراني وتزيد من احتمالية تعرضها للمخاطر السيبرانية[٢].

---

(١) امنة محمد منصور، تأثير الامن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية، مجلة الادارة والاقتصاد الجامعة المستنصرية، العدد(١٢٧)، ٢٠٢١، ص٢٢٦.

(2) Anna Cartwright،، Edward Cartwright ،EstherSolomon Edun، Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies، Computers & Security jornal، vol.(131) issue (3)، 2023، p11.

والأمن السيبراني يعد من أهم فروع الأمن الوطني العراقي والذي يتطلب بناء منظومة إستراتيجية أمنية سيبرانية متكاملة بسبب مايعانيه العراق حاله حال دول الشرق الاوسط من انكشاف استراتيجي سيبراني(١).

نستنتج مما سبق أن الامن السيبراني يتمثل في الدفاع عن الحواسيب والخوادم والاجهزة المحمولة والانظمة الالكترونية والشبكات والبيانات، من الهجمات السيبرانية بشكل مباشر أو غير مباشر وبغض النظر عما اذا كانت ناشئة من داخل المؤسسة أو خارجها، ويطلق عليه أمن المعلومات الالكترونية او أمان تقنية المعلومات وتقدم الشركات المختصة بالامن السيبراني العديد من خدمات الأمن السيبراني مثل **حوكمة الامن السيبراني** والذي يتكون من مرحلتين، الأولى هي إدارة الأمن والثانية هي الحوكمة الأمنية. حيث تضمن إدارة الأمن التقليل من مخاطر الأمن السيبراني بشكل كافٍ من خلال نشر الضوابط الأمنية، في حين أن الحوكمة الأمنية تربط بسهولة بين استراتيجيات الأمن العامة مع أهداف العمل الرئيسية واللوائح الأساسية.

إن لدى شركة الامن السيبراني المُتقدّمة إطار عمل مُستقل من أجل صياغة سياسات وإجراءات حوكمة الأمن السيبراني، وإدارة المخاطر حيث يتم فيها تحديد الأصول المعلوماتية مثل الأجهزة وبيانات العملاء والملكية الفكرية التي يمكن اختراقها نتيجة الهجمات السيبرانية. ومن ثَمّ، يتم تقييم المخاطر المحتملة التي يمكن أن تؤثر على هذه الأصول لتطبيق عناصر التحكم الأمني المناسبة وفحص جاهزية تنفيذ البرامج(٢)، وتتمثل التحديات القانونية بشكل أساسي في غياب الإطار التشريعي والتنظيمي المناسب سواء للتصرفات القانونية أو الأعمال غير القانونية التي تتم ضمن الفضاء السيبراني حيث يتطلب النشاط التجاري والإقتصادي على وجه الخصوص تحديد واضح للواجبات والحقوق لمستخدمي هذه التقنيات حيث انهم بحاجة إلى إطار يؤمن حماية استخدامهم وفي حال غياب التشريعات مع تواجد المخاطر السيبرانية سيؤدي إلى أضرار خطيرة، لذا فأن ضمان إدارة مخاطر الأمن السيبراني على نحو منظم وممنهج يهدف إلى حماية الأصول التقنية والمعلوماتية وفق السياسات والاجراءات التنظيمية والمتطلبات التشريعية(٣).

---

(١) حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، المجلة الجزائرية للعلوم القانونية والسياسية، مجلد (٥٧)، العدد (٥)،٢٠٢٠، ص٥٦١.

(2) Anna Cartwright, op.cit, p9.

(٣) اسلام فوزي، الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، مجلد (٥٦)، العدد (٢)، ٢٠١٩، ص١١٣.

وعلى الرغم من عدم وجود إطار تشريعي منظم لعقود الأمن السيبراني في العراق بصورة خاصة وإجراءات الأمن السيبراني عموماً، إلا أننا نجد بوادر للإهتمام بتعزيز ثقافة الامن السيبراني من خلال عمل استراتيجية الأمن السيبراني العراقي والتي تعنى بالإستعداد لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات وبناء ورعاية مجتمع انترنت موثوق به[1].

ونستخلص مما سبق أن عقد الأمن السيبراني يتشابه مع عقد التأمين من المخاطر السيبرانية في النواحي التالية:

١- يعتبر عقد الأمن السيبراني وعقد التأمين من المخاطر السيبرانية أداة تتخذها الشركات التجارية على إختلاف أنواعها للحد أو القضاء على المخاطر السيبرانية والأضرار الناجمة عنها.
٢- إن محل العقد في كليهما هو (الخطر السيبراني).
٣- نحتاج في كلا العقدين لخبرات هندسية في مجال الفضاء السيبراني والمخاطر السيبرانية.
٤- لا يوجد تنظيم قانوني لكلا العقدين لحد الآن في التشريع العراقي والتشريعات المقارنة.

كما نرى أن مفهوم الأمن السيبراني اوسع من مفهوم التأمين من المخاطر السيبرانية حيث أن الأمن السيبراني هو عبارة عن مجموعة من الإجراءات الوقائية أو الدفاعية التي قد تمارس من قبل الدولة أو الأشخاص الطبيعية أو المعنوية الخاصة للحفاظ على أمن وسلامة البيانات والمعلومات التي يتم التعامل فيها ضمن الفضاء السيبراني ، أما بالنسبة للتأمين من المخاطر السيبرانية فهو عبارة عن وسيلة علاجية غير وقائية عقد هدفة نقل تبعة المخاطر السيبرانية لشركة التأمين حيث يتم من خلاله تغطية الخسائر الناجمة عن فشل أو ضعف اجراءات الأمن السيبراني للمؤمن لهم سواء كان متعمد أم غير متعمد، بحيث يعرّض أنظمة معلومات وبيانات الشركات المؤمن لها وبنيتها التحتية الحيوية للضرر؛ لذا فأن هدف التغطية هو إصلاح الضرر الناجم عن حدوث خلل في الأمن السيبراني للشركات التي تعمل ضمن الفضاء السيبراني.

كما نجد أن الأمن السيبراني هو أحد متطلبات إبرام عقد التأمين من المخاطر السيبرانية بالنسبة للشركات التجارية المؤمن لها والعكس ليس صحيح، حيث لا يحتاج إبرام عقد الأمن السيبراني إلى ضرورة وجود تغطية تأمينية ضد المخاطر السيبرانية التي قد تصيب الشركة.

---

(١) استراتيجية الامن السيبراني العراقية مستشارية الامن الوطني امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات لسنة ٢٠٢٢، مصدر سابق، ص٢.

الفصل الثاني

آثار عقد التأمين من المخاطر السيبرانية وتحدياته

الفصل الثاني

آثار عقد التأمين من المخاطر السيبرانية وتحدياته

يقوم التأمين على فكرة مؤداها توزيع النتائج الضارة لخطر معين على مجموعة من الأفراد بدلاً من تحمل فرد واحد لتلك النتائج، ويقوم على علاقتين، الأولى: علاقة قانونية تتمثل بعقد التأمين حيث يقوم فيها الطرف الأول (المؤمن) بتغطية خطر معين يتعرض له الطرف الثاني للعقد (المؤمن له) بمقتضى شروط محدده نظير دفعة مالية يدفعها للطرف الثاني. أما الثانية: فهي علاقة فنية تتمثل بالأسس الفنية التي يستند عليها المؤمن والمتمثل بشركة التأمين لتقييم المخاطر وحجم أضرارها[١] فضلاً عن عنصر المصلحة التأمينية والتي تعتبر من العناصر الجوهرية للعقد التي يستوجب توافرها طيلة مدة التعاقد وحتى عند استحقاق التعويض وتتمثل في النفع الذي يعود على المؤمن له من عدم وقوع الخطر المؤمن عليه[٢]، و التأمين وفقاً للمادة (١/٩٨٣) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١ ما هو إلا عقد يلتزم به المؤمن بأن يؤدي للمؤمن له أو المستفيد مبلغاً من المال أو ايراد مرتب أو أي عوض مالي آخر في حالة حدوث الخطر المؤمن منه مقابل اقسط أو اي دفعة مالية أخرى يؤديها المؤمن له للمؤمن، أما المادة(١/٩٨٤) فقد حددت محله حيث يمكن ان يكون محلاً للتأمين كل شيء مشروع يعود على الشخص بنفع من عدم وقوع خطر معين[٣]. ويرتب عقد التأمين من المخاطر السيبرانية كغيره من العقود آثاراً متعددة البعض منها يشابه الآثار التقليدية لعقود التأمين من المخاطر المتعارف عليها، إلا أنه في الوقت ذاته تتمحور خصوصية العقد مدار البحث بكونه ينتج عدداً من الآثار المتميزه عن سائر عقود التأمين التقليدية، كما تجدر الإشارة إلى أن عقد التأمين من المخاطر السيبرانية لا يزال يواجه العديد من التحديات والمعوقات القانونية والفنية الناتجة عن خصوصية الآثار الناجمة عنه، الأمر الذي يستدعي ضرورة البحث في تلك التحديات بعد ان نستكمل البحث في تلك الآثار . عليه سنقسم الفصل إلى مبحثين: نتناول في المبحث الأول منه آثار عقد التأمين من المخاطر السيبرانية، أما في المبحث الثاني سنتناول تحديات التأمين من المخاطر السيبرانية.

---

(١) محمد عبد الظاهر حسين، عقد التأمين، دار النهضة العربية، القاهرة، ٢٠٠٣، ص١١.

(٢) شذى عبد جمعة موسى، مصدر سابق، ص١٢٠.

(3) Ganbayar Uuganbayar, Relation between cyber insurance and securety investments/ controls،universita Degli studi Di Trento, PhD.Thesis, 2021, p2.

المبحث الأول

آثارعقد التأمين من المخاطر السيبرانية

كما هو الحال في عقود التأمين التقليدية، يترتب على إنعقاد عقد التأمين من المخاطر السيبرانية عدد من الآثار القانونية والتي تتمثل بنشوء الإلتزامات والحقوق في ذمة طرفي العقد، وهما: شركة التأمين من المخاطر السيبرانية (المؤمن)، والشركة التجارية طالبة التأمين (المؤمن له). وكما هو الحال في عقود التأمين التقليدية نجد أن عقد التأمين من المخاطر السيبرانية يشترك مع العقود التقليدية في الإلتزامات الرئيسية المترتبة على طرفي العقد وحقوق كل منهما تجاه الآخر، لكن في المقابل نجد أن عقد التأمين من المخاطر السيبرانية ينفرد بترتيبه عدداً من الإلتزامات المتميزة عن سائر عقود التأمين، فبالإضافة لإختلاف طبيعة الحقوق الممنوحة لكلا الطرفين والتي تختلف في طبيعتها عن الحقوق الممنوحة لطرفي عقد التأمين التقليدي. نجد أن كلا الطرفين يلتزم تجاه الآخر بإلتزامات محددة قد تشترك مع عقود التأمين التقليدية في جانب منها، وتختلف عنها في جوانب أخرى، ويمكننا تصنيف هذه الإلتزامات إلى نوعين: الإلتزامات الناشئة قبل تحقق الخطر السيبراني المؤمن منه، وتلك التي تنشئ بعد تحقق الخطر السيبراني ، عليه سنقسم هذا المبحث إلى مطلبين، نتناول في المطلب الأول إلتزامات أطراف العقد قبل تحقق الخطرالسيبراني، أما في المطلب الثاني سنتناول إلتزامات أطراف العقد بعد تحقق الخطرالسيبراني.

المطلب الأول

إلتزامات أطراف العقد قبل تحقق الخطرالسيبراني

على الرغم من أن عقد التأمين من المخاطر السيبرانية قد يتشابه مع عقود التأمين التقليدية في بعض الإلتزامات المترتبة على أطرافه. إلا أن خصوصيته تكمن في طبيعة الإلتزامات المترتبة على أطرفه؛ نظراً لخصوصية الخطر المؤمن منه وخصوصية الوسط الذي يقع فيه هذا النوع من المخاطر وهو (الفضاء السيبراني)، كونه وسط غير مادي ينتج عنه اخطار غير مادية ذات أضرار هائلة قد يصعب حصرها لتعدد الأطراف المتضررة من وقوعه نظراً لسرعة انتشاره، مما أدى إلى أن تكون إلتزامات كلاً من المؤمن له (الشركة التجارية)، والمؤمن (شركة التأمين من المخاطر السيبرانية) متميزة عن تلك الواردة في عقود التأمين التقليدية. عليه سنبحث تلك الإلتزامات في

فرعين، نتناول في الفرع الأول إلتزامات المؤمن له (الشركة التجارية) من المخاطر السيبرانية، أما في الفرع الثاني سنبحث في إلتزامات المؤمن (شركة التأمين) من المخاطر السيبرانية.

الفرع الأول

إلتزامات المؤمن له (الشركة التجارية) من المخاطر السيبرانية

وفقاً للقواعد العامة في القانون المدني فإنه يقصد بالمؤمن له الشخص الذي يؤدي الإلتزامات المقابلة لإلتزامات المؤمن، وإذا كان المؤمن له هو صاحب الحق في قيمة التأمين كان هو المستفيد، حيث يقصد بالمستفيد الشخص الذي يؤدي إليه المؤمن قيمة التأمين[١]. فالمؤمن له هو الطرف المهدد بتحقق الخطر المؤمن منه وهو يختلف بدوره عن طالب التأمين والذي يقوم بتوقيع العقد و دفع القسط، أما المستفيد فهو من يحصل على التعويض وقد تتفرق هذه الصفات على أشخاص مختلفين أو قد تتجمع في شخص واحد[٢].

وإن القواعد القانونية التي تحدد إلتزامات المؤمن له في عقد التأمين التقليدي تنطبق على إلتزامات الشركة التجارية في عقد التأمين من المخاطر السيبرانية كون هذه القواعد هي قواعد عامة تشترك فيها جميع عقود التأمين دون إستثناء، مع الأخذ بنظر الإعتبار خصوصية العقد الأخير وتفرّده بإلتزامات معينة تختلف عن مثيلاتها من عقود التأمين التقليدية، ووفقاً لما تقرره القواعد العامة. ووفقاً لما سبق يمكن إجمال التزامات الشركة التجارية بموجب عقد التأمين من المخاطر السيبرانية بما يأتي:

١. **الإلتزام بالإفصاح أو الإدلاء بالبيانات:** يلتزم المؤمن له (الشركة التجارية) بالإفصاح للمؤمن (شركة التأمين من المخاطر السيبرانية) وقت إبرام العقد بكل ما يعتبر من الضروري إبلاغ شركة التأمين به، سواء تلك البيانات التي تتعلق بالخطر السيبراني أم بشركة التأمين ذاتها من حيث طبيعة نشاطها و عدد موظفيها ووسائل الأمن السيبراني المتخذة من قبلها، أم التي تتعلق بالعملاء، لتتمكن من تقدير المخاطر المؤمن منها في العقد، ويعتبر مهماً في هذا الشأن الوقائع التي جعلها المؤمن

(١) ننسي أحمد فاروق، التزام المؤمن عليه بالإدلاء بالبيانات المتعلقة بالخطر وجزاء الإخلال به، مجلة البحوث القانونية والاقتصادية، المجلد (٥٤)،العدد (١)،٢٠٢١، ص٣٤٣؛ والفقرة الثانية من المادة (٩٨٣) من القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

(٢) باسم محمد صالح، القانون التجاري، القسم الأول، المكتبة القانونية، بغداد، بدون سنة نشر، ص٢٥٥ وما بعدها.

محل أسئلة مكتوبة[١]، فعلى الشركة التجارية طالبة التأمين الإدلاء بالبيانات المتعلقة بالخطر السيبراني المؤمن منه عند إبرام العقد[٢]، ويتم ذلك من خلال الافصاح عن كل ما يتصل بالخطر السيبراني الذي تعرضت له الشركة التجارية سابقاً أو الذي من المحتمل أن تتعرض له مستقبلاً و إعلام المؤمن عما يحيط به من ظروف، بالإضافة إلى إلتزام الشركة المؤمنة من المخاطر السيبرانية بالإفصاح عن البيانات الشخصية الخاصة بها من حيث حالتها المادية و مقدار العناية المبذولة في شؤونها وسلوك الشركة التجارية أو المركز المالي الخاص بها وهل سبق أن تعرضت لخطر سيبراني في السابق أم لا وهل تمتلك نظام أمن سيبراني لحماية أنظمتها أم لا. كما تلتزم الشركة التجارية طالبة التأمين بالإدلاء بمجموعة من البيانات أثناء سريان عقد التأمين من المخاطر السيبرانية والتي تتمثل بكل ما يطرأ من مستجدات تؤدي إلى زيادة فرص وقوع الخطر السيبراني المؤمن منه. والهدف من هذه البيانات الاخيرة هو تأثيرها البالغ على عملية تقييم المخاطر، حيث أن إزدياد نسبة وقوع الخطر السيبراني سيؤدي بدوره إلى إرتفاع قسط التأمين بصورة طردية مع الخطر[٣]. كما يجب على الشركة التجارية إخطار المؤمن بما يطرأ اثناء العقد من احوال من شأنها أن تؤدي إلى زيادة هذه المخاطر[٤].

وبصورة عامة يمكن القول أن البيانات الشخصية التي يلتزم المؤمن له بإفصاحها لشركة التأمين من المخاطر السيبرانية بها هي البيانات التي من شأنها أن تطمئن المؤمن على الشخص الذي تعاقد معه لبيان مدى جديته في تنفيذ التزاماته التعاقدية، ولهذه البيانات أهميتها وتأثيرها على موقف المؤمن من عملية التأمين ليتمكن من تقدير المخاطر السيبرانية محل التأمين وبالتالي تقدير

---

(١) المادة (٩٨٦) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

(٢) هناك من يفرق بين مصطلحي البيانات والمعلومات فالبيانات تعرف بأنها مجموعة من الحروف أو الرموز أو الأرقام أو الكلمات أو الصور والتي تتعلق بموضوع ما، أما المعلومات فهي البيانات التي تم تحليلها ومعالجتها بشكل يجعل منها تحمل معنى وقيمة ويمكن الإفادة منها في اتخاذ القرارات. للمزيد انظر: فاطمة سرير، رباحي احمد، فعالية تنميط البيانات الشخصية في تخصيص التجارة الالكترونية على ضوء اللائحة العامة رقم ٦٧٩لسنة ٢٠١٦ المتعلقة بحماية البيانات، مجلة الدراسات القانونية المقارنة، المجلد (٨)، العدد (٢)، ٢٠٢٢، ص٦٥؛ اما المشرع العراقي فقد جعل البيانات جزء من المعلومات، حيث عرف المعلومات بأنها البيانات والنصوص والصور والاشكال والرموز وما شابه ذلك التي تنشأ أو تدمج أو تخزن أو تعالج أو ترسل أو تستلم بوسائل الكتروني. انظر المادة (١/ف٣) من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢.

(٣) سنا مازن فالح، مصدر سابق، ص٦٦.

(٤) انظر المادة (٩٨٦) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

قسط التأمين الواجب دفعه، اذاً فالبيانات المؤثرة في عقد التأمين هي الظروف والملابسات والوقائع التي تمكن المؤمن من اتخاذ قراره بشأن قبول أو رفض أو بشأن تحديد قيمة قسط[١] التأمين من المخاطر السيبرانية ، فمنها ما يتعلق بالخطر السيبراني ذاته ومنها ما يتعلق بالشركة طالبة التأمين، وهناك معيارين لتحديد البيانات المؤثرة بالخطر: الأول يتعلق بمدى إتصال البيانات بصفة جوهرية ويتلخص ذلك بأن إلتزام المؤمن له بالإفصاح عن البيانات المؤثرة بالخطر هو وسيلة من وسائل الوقاية وحماية الإرادة من العيوب، أما المعيار الثاني فهو معيار مدى ملائمة العلم بالبيان محل الإفضاء، حيث يشمل ضرورة الإفصاح عن كل بيان لو علم بوجوده المؤمن وقت التعاقد لكان قد إلتزم نحو المؤمن له بشكل مختلف عما هو عليه في العقد[٢].

وقد عرفت المادة (٤) من اللائحة الأوروبية العامة لحماية البيانات (GDPR)[٣] والصادرة عن الاتحاد الأوروبي في ٢٧ ابريل ٢٠١٦ البيانات الشخصية بأنها أي معلومات تتعلق بشخص طبيعي معين أو قابل للتعيين بشكل مباشر أو غير مباشر مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الانترنت أو واحدة أو اكثر من العوامل المحددة الفيزيائية أو الفسيولوجية أو الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي. كما عرفت المادة ذاتها خرق البيانات الشخصية بأنه خرق الأمن الذي يؤدي إلى التدمير العرضي أو غير

---

(١) أحمد شرف الدين، مصدر سابق، ص٢٠٣.

(٢) سيف هادي. أمل فاضل عنوز، الإلتزام بالإدلاء ببيانات المتعلقة بالخطر، مجلة المنهل الاقتصادي المجلد (٤) ، العدد (٢)، ٢٠٢١، ص ٢٩٧.

(٣) اللائحة الأوروبية العامة لحماية البيانات (GDPR) هي اختصار ل General Data Protection Regulation، وهي بمثابة قانون لحماية خصوصية البيانات الخاص بالاتحاد الأوروبي تم اصدار اللائحة في العام ٢٠١٦، لكنها دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨ وهي من اكثر قوانين الخصوصية والأمن تشدداً في العالم. الهدف من تشريعها هو تعريف الافراد بالآلية القانونية التي يجب ان يتم بها جمع بياناتهم الشخصية وكيفية حمايتها إذا ما تم استخدامها عبر الفضاء السيبراني. وعلى الرغم من أنه قد تمت صياغته وتمريره من قبل الاتحاد الأوروبي (EU)، فإنه يفرض التزامات على المنظمات في كل مكان حتى خارج نطاق الاتحاد الأوروبي، طالما أنها تستهدف أو تجمع البيانات المتعلقة بالأشخاص في الاتحاد الأوروبي. كما تتميز اللائحة العامة لحماية البيانات بفرضها غرامات قاسية على كل من ينتهك معايير الخصوصية والأمان، مع عقوبات تصل إلى عشرات الملايين من اليورو. للمزيد انظر: https://gdpr.eu
تاريخ الزيارة ٢٠٢٣/٢/١٣ الساعة ٦:٠٠ م.

القانوني أو الخسارة أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية المنقولة أو المخزنة أو التي تتم معالجتها بطريقة أخرى.

وفي إعتقادنا أنه على الرغم من أن اللائحة قد أوضحت ماهية البيانات الشخصية إلا أن التعريف كان مطولاً حيث أسهبت في سرد العديد من الأمثلة عن ما يمكن أن يعدّ من البيانات الشخصية، وكان الأحرى أن تضع تعريفاً موجزاً من خلال النص على قاعدة عامة تحدد فيها متى يعتبر البيان شخصي من عدمه لتجنب الاجتهادات الفقيه والقضائية حول هذه البيانات.

وجاءت الفقرة الرابعة من المادة الأولى لنظام حماية البيانات الشخصية السعودي المرقم (م/١٩) والصادر في ٢٠٢١/٩/١٦ بتعريف مشابه للتعريف الوارد في اللائحة العامة لحماية البيانات وهي "كل بيان – مهما كان مصدره أو شكله– من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي". إلا أن النظام قد فرق بين البيانات الشخصية والبيانات الحساسة؛ حيث عرفتها الفقرة (١١) من المادة السابقة الذكر من النظام بأنها "كل بيان شخصي يتضمن الاشارة إلى أصل الفرد العرقي أو أصله القبلي أو معتقده الديني أو الفكري أو السياسي أو يدل على عضويته في جمعيات أو مؤسسة اهلية والبيانات الجنائية والأمنية وبيانات السمات الحيوية التي تحدد الهوية أو البيانات الوراثية أو الائتمانية أو الصحية وبيانات تحديد الموقع والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما".

وبإعتقادنا أنه كان من الافضل الإكتفاء بتعريف البيانات الشخصية وعدم التطرق لوضع تعريف للبيانات الحساسة بصورة مستقلة، كونها تشكل جزءاً من تعريف البيانات الشخصية الوارد في النظام، حيث ذيل التعريف بعبارة ".. وغير ذلك من البيانات ذات الطابع الشخصي"، وهذا نص عام يشمل البيانات الحساسة وفق تعريف النظام فكل بيان حساس هو بيان ذي طابع شخصي في واقع الأمر[١].

(١) تجدر الإشارة إلى القانون رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية في دولة قطر حيث عرفت المادة الأولى من الفصل الأول من القانون البيانات الشخصية بأنها " بيانات عن الفرد الذي تكون هويته محدده أو يمكن تحديدها بصورة معقولة سواء من خلال هذه البيانات أو عن طريق الجمع بينهما وبين اية بيانات اخرى".

أما بالنسبة للمشرع العراقي فلم يشرع لحد الآن قانوناً خاصاً بحماية البيانات الشخصية أسوة بباقي الدول، ولم يتطرق لتعريف البيانات الشخصية بالقوانين ذات الصلة وإنما إكتفى بتعريف المعلومات في قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (٧٨) لسنة ٢٠١٢. ولم يعرف البيانات الشخصية على الرغم من أهميتها في القانون سالف الذكر وإكتفى بجعل البيانات جزءاً من المعلومات، حيث عرف المعلومات بأنها البيانات والنصوص والصور والأشكال و الرموز وما شابه ذلك التي تنشأ أو تدمج أو تخزن أو تعالج أو ترسل أو تستلم بوسائل الكتروني(١).

وتلتزم الشركة التجارية بأن تدلي لشركة التأمين من المخاطر السيبرانية بعدد من البيانات التفصيلية والدقيقة الخاصة بها وبفروعها، المتعلقة بأنظمة التشغيل وشبكات الكمبيوتر والاتصالات الخاصة بها، كما تفصح الشركة المؤمن لها عن جميع البيانات الخاصة ببياناتها المالية كإجمال الأصول والإيرادات، وطبيعة معاملاتها التجارية والعدد الكلي للموظفين و بياناتهم وهل يتم تدريبهم على مواجهة المخاطر السيبرانية أم لا، وأسماء العملاء، وهوية المسؤول عن أمن المعلومات في الشركة مع بيان هوية الطرف الذي يقدم له مسؤول امن المعلومات تقاريره، ومدى امتلاك الشركة خطة الإستجابة للمخاطر السيبرانية، ومدى قيام الشركة التجارية بعمل نسخ إحتياطي للبيانات الحساسة من عدمه، بالإضافة لإلتزام الشركة التجارية بالإفصاح عن الإجراءات المتعلقة بكلمات المرور ووقت تحديثها، كما تلتزم بالإفصاح عن جميع المعلومات التي تتعلق بالخسائر الناجمة عن تعرضها للمخاطر السيبرانية لثلاث سنوات ماضية. ويتم ذكر بيانات الشركة التجارية المفصح عنها في وثيقة التأمين والتي تكون متاحة لعدد من موظفين شركة التأمين من المخاطر السيبرانية أو وكلاءها، و تكمن أهمية هذا الالتزام بالسماح لشركة التأمين بالإحاطة بجميع البيانات أو السماح بالوصول اليها بالكيفية التي تمكنها من العمل على تأمين الشركات التجارية من المخاطر السيرانية المتوقعة في إطار البيانات المفصح عنها من قبل الشركة التجارية طالبة التأمين(٢).

---

(١) المادة (١/ف٣) من قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢.

(٢) وفقاً لوثيقة التأمين من المخاطر السيبرانية لشركة (TRAVELERS) الأمريكية لسنة ٢٠١٦ وهي شركة تأمين من الحوادث للمسافرين طرحت تغطية متخصصة بالمخاطر السيبرانية، والملاحظ عليها انها اتسمت بالتفصيل وبالدقة الشديدة بالنسبة للبيانات الشخصية المطلوبة من الشركات التجارية. خصوصا ما يتعلق بالمخاطر السيبرانية التي سبق وان تعرضت لها الشركة التجارية بالإضافة لإلزام الشركة التجارية بالافصاح عن المخاطر السيبرانية التي سبق وان تعرضت لها لفترة السنوات الثلاثة السابقة من تاريخ التغطية، نجد ان شركة التأمين من المخاطر السيبرانية أعلاه قد=

وفي إعتقادنا تظهر إشكالية قانونية تتعلق بإلتزام الشركة التجارية بالإفصاح عن البيانات الشخصية الخاصة بالعملاء في عقد التأمين من المخاطر السيبرانية، حيث يثور التساؤل عن مدى قانونية الافصاح عن هكذا بيانات خصوصاً ان معظم الاتفاقيات والقوانين واللوائح قد شددت على أهمية الحفاظ على سرية المعلومات أو البيانات الشخصية والامتناع عن الافصاح عنها وإلا عد ذلك انتهاكاً للسرية والخصوصية وبالتالي تتعرض الشركة التي افصحت عن هذه البيانات إلى المسائلة القانونية. فعلى سبيل المثال نجد أن المشرع العراقي في قانون المصارف رقم (٩٤) لسنة ٢٠٠٤ قد ألزم المصارف بالحفاظ على سرية البيانات الخاصة بالعملاء من حسابات وودائع وأمانات ومن جهة أخرى قد منع المشرع المصارف من الإدلاء بأي بيان يتعلق بهم سواء بطريقة مباشرة أو غير مباشرة حتى بعد إنتهاء العلاقة العقدية بين المصرف والعميل، بإستثناء حصول المصرف على موافقة خطية من عملائه بالكشف عن بياناتهم الشخصية أو الحصول على قرار قضائي بذلك أو وفقاً لما نص عليه القانون(١).

كما يكون محظوراً على أي مسؤول أو إداري أو موظف أو وكيل حالي أو سابق للمصرف أن يزوّد أي معلومات أو بيانات عن العملاء أو ودائعهم أو حساباتهم أو الأمانات أو الخزائن الخاصة بهم أو أي من معاملاتهم أو تمكين طرف ثالث من الإطلاع على هذه المعلومات في غير الحالات المسموح بها بمقتضى أحكام القانون، كما ينطبق الحظر على أي شخص بما في ذلك مسؤولو البنك

=ألزمت الشركة التجارية من خلال وثيقة التأمين بإرفاق تفاصيل كل دعوى أو شكوى أو إدعاء أو حادث بما في ذلك جميع التكاليف أو الخسائر أو الأضرار المتكبدة نتيجة لتحقق الخطر السيبرانية، بالإضافة لبيان قيمة التعويضات الممنوحة للمتضررين بموجب وثائق التأمين السابقة. للمزيد أنظر وثيقة التأمين المنشورة على الموقع:
https://www.profunderwriters.com/wp-content/uploads/2018/04/TRAVELERS_CyberRisk-app-1100-ind-0116.pdf
تاريخ الزيارة ٢٠٢٤/٥/٣ الساعة ٣:٣٠ م

(١) نص المادة (٤٩) من قانون المصارف العراقي رقم (٩٤) لسنة ٢٠٠٤:".. ويحافظ المصرف على السرية فيما يتعلق بجميع حسابات العمال وودائعهم واماناتهم وخزائنهم لديه. ويكون محظورا اعطاء اي بيانات عنها بطريق مباشر أو غير مباشر إلا بموافقة خطية من العميل المعني. أو في حالة وفاة العميل إلا بموافقة ممثله القانوني أو احد ورثة العميل أو احد الموصى لهم أو إلا بقرار جهة قضائية مختصة أو من المدعي العام في خصومة قضائية قائمة أو بسبب احدى الحالات المسموح بها بمقتضى احكام هذا القانون. ويظل هذا الخطر قائما حتى لو انتهت العلاقة بين العميل والمصرف لأي سبب من الأسباب".

المركزي العراقي و موظفو ومراجعو الحسابات فيه الذين يطلعون على هذه البيانات والمعلومات بطريقة مباشرة أو غير مباشرة بحكم عملهم[١].

ووفقاً للمادة التاسعة من اللائحة الأوروبية العامة لحماية البيانات (GDPR) فإنه يجب على شركة التأمين أن تلتزم بالسرية المهنية تجاه عملائها من خلال اتباع القواعد القانونية الملزمة في قانون الإتحاد الأوروبي أو الدول الاعضاء أو القاعدة التي تضعها الهيئات الوطنية المتخصصة كالهيئة الوطنية للأمن السيبراني مثلاً. وللوهلة الأولى نجد أن هذا الالتزام يتعارض مع إلتزام الشركة التجارية المؤمن لها بالإفصاح عن البيانات الضرورية للتعاقد ومن ضمنها البيانات الشخصية للعملاء، لكن من جانب آخر نعتقد أنه بالرغم من حدوث تعارض بين إلتزام الشركة التجارية طالبة التأمين بحماية البيانات الشخصية الخاصة بالعملاء والمحافظة على سريتها، وإلتزام الشركة ذاتها من جانب آخر بالافصاح عن كل ما تحتاج إليه شركة التأمين من بيانات للإحاطة بالخطر السيبراني وتقديره بصوره صحيحة والتي قد تتعلق العملاء أو الوكلاء المتعاونين مع الشركة التجارية حسب الضرورة الي يتطلبها عقد التأمين من المخاطر السيبرانية. إلا أن ذلك لا يمثل إنتهاك لإلتزام الشركة التجارية طالبة التأمين بالحفاظ على الخصوصية والسرية التي تتطلبها الإتفاقيات أو القوانين أو اللوائح والأنظمة. كون شركة التأمين مقيدة بجميع القوانين واللوائح والأنظمة والتي تتعلق بالبيانات الشخصية حيث تلتزم شركة التأمين السيبراني بالمقابل بحماية هذه المعلومات وعدم الكشف عنها أو إستخدامها بصورة غير مصرح بها دون موافقة الشركة التجارية طالبة التأمين أو عملائها. لا سيما وأن شركة التأمين من المخاطر السيبرانية تقوم بتشفير جميع البيانات الخاصة بعملائها وتلزم بالامتناع عن نقل هذه البيانات لطرف آخر دون موافقة كتابية مسبقة من الشركة التجارية طالبة التأمين[٢]، وهذا ما أكد عليه المشرع العراقي في المادة (٥١) من قانون المصارف حيث استثنى من أحكام المواد(٤٩) و(٥٠) بعض الحالات التي سمح فيها للمصارف بإفشاء المعلومات الخاصة بعمل المصرف أو عملائه ومن ضمنها الفقرة (ج) من المادة (٥١) والتي إستثنت الإجراءات المتخذة بحسن نية في سياق أداء الواجبات أو المسؤوليات التي يفرضها قانون المصارف حيث نرى أن الفقرة

(١) نص المادة (٥٠) من قانون المصارف العراقي رقم (٩٤) لسنة ٢٠٠٤.

(٢) كما ورد في وثيقة التأمين من المخاطر السيبرانية لشركة (MSIG Insurance) الفيتنامية، للمزيد انظر:
MSIG Insurance (Vietnam) Company Limited، cyber insurance policy
https://www.msig.com.vn/sites/default/files/downloads/CYBER_INSURANCE_0.pdf
تاريخ الزيارة ٢٠٢٤/٥/٣ الساعة ١١:٠٠ م.

سالفة الذكر قد جاءت بنص عام يمثل أساساً قانونيا لإفصاح المصرف عن البيانات الشخصية التي يحتاجها المؤمن في عقد التأمين من المخاطر السيبرانية، شريطة أن يتم ذلك بحسن نية حيث يلتزم المصرف بأن يدلي بهذه البيانات كجزء من واجبه الرئيسي والمتمثل بالمحافظة على هذه البيانات من التلاعب والاختراق.

كما قد شدد المشرع العراقي في قانون التوقيع الإلكتروني والمعاملات رقم (٧٨) لسنة ٢٠١٢ على سرية البيانات الالكترونية التي يتم الحصول عليها أو الاطلاع عليها بحكم العمل و عدم جواز افشائها أو استخدامها في غير الغرض الذي اعدت من اجله[١].

عليه يمكننا القول بوجود أساس قانوني لإمكانية قيام الشركات التجارية الراغبة في التأمين من المخاطر السيبرانية بالإفصاح عن بعض البيانات الخاصة بعملائها وفقاً لمبدأ حسن النية وبالقدر الذي يتطلبه المؤمن لغرض إمكانية الإحاطة بالخطر المؤمن منه وبالضرر المتوقع بصورة كافية، وبالمقابل قد منع القانون لأي جهة كانت من إستخدام هذه البيانات لأغراض أخرى غير التي أعدت من أجلها.

أما على الصعيد الدولي ، فإنه وفقاً للائحة الأوروبية العامة لحماية البيانات (GDPR) فإن الإفصاح عن البيانات الشخصية الخاصة بالشركة التجارية أو العملاء لا يتم بصورة قانونية إلا إذا كان صاحب البيانات قد وافق على معالجة بياناته الشخصية لأغراض محددة، لكن في الوقت ذاته أقرت اللائحة بأن معالجة البيانات تكون واجبة عند إبرام أي عقد يكون فيه صاحب البيانات طرفاً فيه أو بناء على طلبه أو اذا كانت معرفة هذه البيانات ضرورية للإمتثال لإلتزام قانوني ما، أو لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي اخر أو لأغراض المصلحة العامة أو أي مصلحة مشروعة مع ضرورة وجود ضمانات مناسبة تكفل حماية هذه البيانات من قبل طرفي عقد التأمين من المخاطر السيبرانية كالتشفير أو الاسم المستعار[٢].

نستنتج مما سبق أنه إذا ما رغبت أي شركة بالتأمين ضد المخاطر السيبرانية لدى شركة تأمين متخصصة بهذا النوع من التأمين فعلى الشركة الإلتزام بتقديم جميع البيانات المطلوبة من قبل

(١) نص المادة (١٢) من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢.
(٢) المادة (٦) من اللائحة الأوروبية العامة لحماية البيانات (GDPR) لسنة ٢٠١٦.

شركة التأمين والتي قد تتضمن بدورها بيانات شخصية خاصة بالعملاء لغرض تقييم المخاطر التي من الممكن أن يتعرض لها المؤمن له والأضرار التي قد تلحق به بعد تحقق الخطر السيبراني.

وتجدر الإشارة إلى أن الجزاء المترتب على إخلال الشركة التجارية بإلتزامها بإلادلاء بالبيانات التي يتطلبها عقد التأمين من المخاطر السيبرانية والتي يهم المؤمن معرفتها وقت ابرام العقد أو أثناء سريانه، هو جواز طلب شركة التأمين فسخ العقد في حال تعمد الشركة التجارية طالبة التأمين كتمان هذه البيانات أو تغييرها مما يقلل من أهمية الخطر في نظر شركة التأمين من المخاطر السيبرانية، وتصبح الأقساط المدفوعة حق خالص لشركة التأمين أما التي حلت ولم تدفع فيحق له المطالبة بها. أما اذا كانت الشركة المؤمن لها حسنة النية فيؤدي الفسخ إلى استرداد شركة التأمين للأقساط المدفوعة أو أن يرد منها الخطر القدر الذي لم يتحمل في مقابلة الخطر[١].

وتظهر أهمية هذا الإلتزام من ناحية تقييم المخاطر السيبرانية وتقدير سعر التأمين ؛ حيث أن شركة التأمين ستقرر في ضوء هذه البيانات مدى إمكانية قبول التأمين من تلك المخاطر أو رفضه، أو اذا ما كانت ستقبل التأمين بالسعر العادي أو بسعر أضافي نتيجة للطبيعة المتغيرة والمتطورة للمخاطر السيبرانية[٢].

٢. **الإلتزام بدفع قسط التأمين:** يلتزم المؤمن له بأن يدفع للمؤمن الاقساط أو الدفعات المالية الأخرى في الأجل المتفق عليه[٣] ويعتمد حساب قسط التأمين على أسس إحصائية وفنية محددة ، ففي ضوء بيانات الخسارة السابقة يتم تقدير التعرض المستقبلي للمخاطر مما يمكن شركة التأمين من تحديد الأقساط الواجب دفعها من قبل الشركات التجارية طالبة التأمين[٤] . ويمتاز عقد التأمين من المخاطر السيبرانية بدفع المؤمن له للقسط بصورة سنوية والذي يكون مرتفعاً للغاية الأمر الذي يؤدي

---

(١) المادة (٩٨٧) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

(٢) محمد غازي صابر، تأمين الحوادث، مركز التعليم المفتوح بجامعة القاهرة، القاهرة، ١٩٩٣، ص٢٨.

(٣) ان شركة التأمين في الواقع ما هي إلا مجرد وسيط يجمع الأقساط من الشركات التجارية المؤمن لها ليتم تجميعها ودفعها فيما بعد لتعويض الأضرار التي تحيق بهم، فالمؤمن لهم هم من يتحملون أثر المخاطر السيبرانية مثلاً، اما شركة التأمين فهي تمتلك ما يفيض من هذه الاقساط بعد دفع التعويضات وبذلك تحقق الربح. للمزيد انظر: مصطفى كمال طه، التأمين البحري، الدار الجامعية للنشر والتوزيع، القاهرة، ١٩٩٢، ص٢٣.

(4) Gaspard Ferey, Nicolas Grorod, Simon Leguil. L’assurance des risques cyber, Mémoire de fin de formation، Sciences de l’Homme et Société, 2017, P11.

بعديد من الشركات التجارية إلى فسخ العقد مبكراً مع شركات التأمين من المخاطر السيبرانية والإكتفاء بإتخاذ إجراءات الأمن السيبراني بجهود ذاتية أو إبرام عقود الأمن السيبراني إن لزم الأمر، وأدى ذلك إلى فرض شركات التأمين لشروط جزائية بمبالغ كبيرة لمنع الشركات التجارية من فسخ العقد، إلا أن الشركات التجارية في الغالب تقرر أن تلتزم بدفع الأقساط السنوية إلى شركات التأمين وعدم الفسخ، بسبب وجود يقين بعدم إمكانية تجنب المخاطر السيبرانية ومنع وقوعها والحد من آثارها الوخيمة، بالإضافة إلى اعتبار التأمين من المخاطر السيبرانية ميزة تنافسية بين الشركات التجارية، تؤدي إلى زيادة ثقة العملاء بها وإزدياد الإقبال عليها(١).

وقد تتعرض شركات التأمين من المخاطر السيبرانية لنوع من الخسارة عند تحديدها للأقساط المطلوبة من المؤمن له ؛ بسبب حداثة هذا النوع من التأمين وعدم وجود تاريخ طويل من الحوادث السيبرانية يمكن لشركة التأمين من خلالها معرفة نسبة احتمالية وقوع الخطر المؤمن منه وحجم الأضرار الناجمة عنه وفق أسسها الفنية والإحصائية مقارنة بمخاطر التأمين التقليدية: كالتأمين من الحريق أو حوادث السيارات أو التأمين على الحياة، حيث يمكن لشركة التأمين الاعتماد على العديد من الإحصائيات لغرض تحديد قسط التأمين الواجب دفعة لتغطية الخسارة المتوقعة، أما بالنسبة التأمين من المخاطر السيبرانية فإن الشركات التجارية تعمل بصورة سريعة التطور، ومن ثم لا بدّ من الإعتماد على عدد من العوامل غير المباشرة لغرض تسعير وثائق التأمين بشكل يتلائم وتقديرات السوق من تكلفة المخاطر السيبرانية وإستقراء الاستبيانات التي يقوم بها إستشاريو التأمين المختصين لغرض تحديد تكلفة المخاطر القابلة للتأمين ومن ثم تحديد قسط التأمين(٢).

وإستناداً للمادة (٩٨٧) من القانون المدني العراقي تصبح الأقساط التي تم دفعها حقاً خالصاً للمؤمن في حالة طلب المؤمن فسخ العقد إذا ما تعمد المؤمن له عدم الإفصاح عن أمر أو قدم عن عمد بياناً كاذباً، وكان من شأن ذلك ان يغير موضوع الخطر أو يقلل من أهميته في نظر المؤمن، أما الاقساط التي حلت ولم تدفع فيكون له حق المطالبة بها. ويطبق الحكم ذاته على كل الحالات التي يخل فيها المؤمن له بتعهداته عن غش وسوء نية، أما إذا كان المؤمن له حسن النية، فإنه يترتب على الفسخ أن يرد المؤمن الاقساط المدفوعة.

(1) Peters Gareth, Shevchenko Pavel, Cohen Ruben, Maurice Diane, Understanding Cyber Risk and Cyber InsuranceSSRN Electronic Journal. 10.2139, (2017), p14.

(٢) محمد سعيد اسماعيل، مصدر سابق، ص٢٢٣.

٣. **الإلتزام بالاعلام عن أي تغيير أو تحديث في أنظمة تشغيل الشركة التجارية المؤمن لها والذي من شأنه زيادة جسامة الخطر السيبراني:** حيث يلتزم المؤمن له بإعلام شركة التأمين عن كل ما يستجد من ظروف يكون من شأنها زيادة إحتمالية وقوع على نحو يؤثر في قرار شركة التأمين من المخاطر السيبرانية بالتعاقد معه أو بتحديد القسط المناسب وسواء كان ذلك التغيير بفعل المؤمن له أو بفعل الغير(١)، كأن تقوم الشركة بنشاط تجاري جديد غير منصوص عليه في عقد التأمين، لذا سيكون من الواجب على الشركة التجارية أن تلتزم بإعلام شركة التأمين بذلك من أجل التعرف على مدى تأثير تلك التغييرات على قيمة التأمين بسبب طبيعة وحجم البيانات الجديدة التي ستتم معالجتها، كأن تقوم الشركة التجارية (المؤمن له) بالاستعانة بمصادر خارجية لتطوير و إدارة أو تشغيل نظام المعلومات الخاص بها، أو أن تنشئ الشركة المؤمن لها خدمات رقمية جديدة غير مذكورة في عقد التأمين من المخاطر السيبرانية لغرض تنويع وتسريع نشاطها مما يغير بشكل كبير من مستوى المخاطر السيبرانية المعروفة للمؤمن(٢).

٤. **الإلتزام بتوفير متطلبات الأمن السيبراني:** ان عقد التأمين من المخاطر السيبرانية بمجرد إنعقاده فإنه يلزم الشركة التجارية بالتعهد بمراعاة الحد الأدنى من مستوى أمن الكمبيوتر من خلال تحديث الانظمة والبرامج الخاصة بمكافحة الفيروسات والامتثال لمعايير سلامة سيبرانية معينة مثل وجود معيار أمان بيانات صناعة بطاقات الدفع (PCI_DSS) والذي هو معيار لأمن معلومات المؤسسة التي تتعامل مع البطاقات الائتمانية أو الخصم المباشر أو الدفع المسبق، أو توفير نسخ احتياطية للبيانات الخاصة بها وبعملائها(٣)، عليه تلتزم الشركة التجارية في عقد التأمين من المخاطر السيبرانية بإتخاذ جميع الاجراءات اللازمة للحيلولة دون تحقق الخطر من خلال اتخاذ التدابير الأمنية المناسبة كالتعاقد مع شركات أمن سيبراني لتأمين حماية أنظمة التشغيل في الشركة بشكل يتناسب وطبيعة الاعتداءات التي تواجهها في الفضاء السيبراني، مع ضرورة مواكبة التغييرات الفنية والقانونية فيما يخص الأمن السيبراني؛ نظراً لأن شركات التأمين المتخصصة بالتأمين من المخاطر السيبرانية لا توفر تغطية تأمينية للشركة التجارية طالبة التأمين إلا بعد حصولها على شهادة من احدى شركات الامن السيبراني المختصة بالتكنولوجيا الأمنية، مع الزام المؤمن له بأن يوضح

---

(١) محمد حسين منصور، مبادئ قانون التأمين، دار الجامعة الجديدة للنشر، بدون سنة نشر، ص١٠٠.

(2) Assurance des risques cyber – Guide Pratique, club de la sécurité de l'information français (CLUSIF), 2018, p37.

(3) Even Langfeldt Friberg، op.cit, p15.

الاجراءات المتخذه ضد المخاطر السيبرانية المؤمن منها[1]، فإذا قررت شركة التأمين من المخاطر السيبرانية إصدار وثيقة التأمين فإنها ستدرج قيها العديد من البنود التي تمنع الشركة التجارية طالبة التأمين من استخدام عقد التأمين من المخاطر السيبرانية كوسيلة للتربح. لذا تضع العديد من شركات التأمين من المخاطر السيبرانية بنوداً تعاقب فيها الشركات التجارية (المؤمن لها) المهملة أو سيئة النية أو قد تكافئها على اتخاذها لإجراءات السلامة السيبرانية وتجنب الأخطار. كما يندرج ضمن هذا الإلتزام شرط الخضوع لمعايير الجودة العالمية حيث يلتزم المؤمن له بجلب تأكيد رسمي من قبل الأجهزة الرسمية الوطنية أو الدولية المتخصصة في الأمن السيبراني للتعرف على مدى صلاحية أنظمة التشغيل في الشركة للإستخدام في النشاط التجاري وبالأخص برامج التشغيل، وبناءً على ذلك تخلي الشركة التجارية طالبة التأمين مسؤوليتها عن تحقق المخاطر السيبرانية تجاه شركة التأمين، بسبب عيوب أنظمة التشغيل وبالتالي يحق لكلا طرفي عقد التأمين من المخاطر السيبرانية الرجوع على هذه الجهات الرسمية بالتعويض بسبب عدم تحريها الدقة في اصدار شهادة الجودة التي تثبت مطابقة الأنظمة والبرمجيات للمواصفات المطلوبة[2].

٥. **إلتزام المؤمن له بإعتماد مبدأ الامن متعدد الأطراف:** ترفض شركات التأمين من المخاطر السيبرانية عادةً تغطية المخاطر التي من الصعب تجنبها من الناحية الفنية، إذ لا يمكن أن نفترض الثقة بجميع الأطراف العاملة في الفضاء السيبراني من مقدمي خدمات الانترنت ومشغلي شبكات ومبرمجي النظام وعمال خدمات الصيانة، فالخطر السيبراني قد لا يتحقق بسبب المهاجمين الخارجيين حصراً، بل يمكن ان نعتبر جميع الاطراف المعنية في عقد التأمين من المخاطر السيبرانية بمثابة مصدر محتمل للخطر، فتساهم في وقوع الخطر السيبراني، ويمكن أن يتحقق الخطر السيبراني من داخل الشركة التجارية المؤمن لها – كقيام أحد الموظفين بإيقاف عمل أحد البرامج الرئيسية للشركة مما يتسبب بإنقطاع أعمالها وحجب الخدمة – لذا تلتزم الشركة التجارية بمراعاة قواعد الأمن السيبراني المتعدد الأطراف وأتخاذ جميع الإحتياطات الأمنية تجاه الجميع، **فمبدأ الأمن المتعدد الأطراف يعني اتخاذ الشركة التجارية لجميع وسائل الحماية من المخاطر السيبرانية تجاه كل طرف يحتمل مساهمته في تحقق الخطر السيبراني،**

(1) Peters Gareth, Shevchenko Pavel, Cohen Ruben, Maurice Diane, op.cit, p9.

(٢) طارق عفيفي صادق، الخطر محل التأمين من المسؤولية في مجال المعلوماتية، ط١، دار الحكمة للطباعة والنشر والتوزيع، القاهرة، ٢٠١٣، ص٤٤.

كموظفيها أو شركات الأمن السيبراني و مزودي الخدمة، أو حتى شركات التأمين من المخاطر السيبرانية ذاتها[١].

٦. **إلتزام الشركة التجارية ببذل عناية الرجل الحريص عند التعامل في الفضاء السيبراني:** يتم تنفيذ هذا الإلتزام من خلال تجنب إستخدام برامج حماية أو مواقع الكترونية مشبوهة أو فتح روابط من جهات مجهولة قد تتسبب في حدوث خرق امني للشركة[٢]. حيث يلتزم المؤمن له في عقد التأمين من المخاطر السيبرانية بالمحافظة على الشيء المؤمن عليه من الخطر السيبراني المحدد في وثيقة التأمين ويبذل في ذلك عناية الرجل الحريص ، فإذا ما وقع الخطر السيبراني المؤمن منه فيلتزم المؤمن له بإتخاذ كافة الوسائل والإجراءات اللازمة للتخفيف من آثار الخطر السيبراني ومنع تفاقمه[٣]، لكن ما الحكم فيما لو بذلت الشركة التجارية عناية الرجل الحريص في تعاملاتها التجارية السيبرانية بموجب عقد التأمين من المخاطر السيبرانية، لكن الخطر السيبراني تحقق عن طريق أحد موظفي الشركة بقصد الأضرار بها وبسمعتها التجارية وحرمانها من الحصول على مبلغ التأمين من شركة التأمين كون الخطر صدر عمدياً من أحد موظفي الشركة التجارية المطالبة بمبلغ التأمين فهل نطبق القواعد العامة بإعتبار أن الخطأ العمدي غير مشمول بالتغطية، أم أن شركات التأمين من المخاطر السيبرانية مُلزمة بدفع مبلغ التأمين للشركة التجارية بغض النظر عن أخطاء موظفيها؟

للإجابة عن هذا التساؤل نتتبع أحد أهم القرارات القضائية الخاصة بإلتزام المؤمن له بإجراءات الأمن السيبراني في المملكة المتحدة وهو قرار المحكمة العليا في قضية(موريسونز) والذي نقض قرار محكمة الاستئناف بشأن نشر أحد موظفي الشركة لبيانات شخصية لحوالي مئة ألف موظف تتعلق بالراتب ومعلومات الحساب المصرفي، وعندما طالبت الشركة التجارية بمبلغ التأمين من شركة التأمين من المخاطر السيبرانية، رفضت الأخيرة تنفيذ إلتزامها بدفع مبلغ التأمين للمؤمن له، فقرروا رفع الدعوى أمام القضاء، وبناء على معطيات القضية قررت المحكمة العليا بأن صاحب العمل غير مسؤول بشكل مباشر أو غير مباشر عن حالة خرق البيانات التي تسبب بها موظف لديه؛ كون

(1) MSIG Insurance (Vietnam) Company Limited, CYBER INSURANCE POLICY, op. cit, p12.

(٢) احمد عطا حسين، مصدر سابق، ص٦٧٩.

(٣) عمار ياسر رشيد، التأمين ضد مخاطر الالكترونية في التشريع الأردني، اطروحة دكتوراه مقدمة إلى جامعة العلوم الاسلامية /كلية الدراسات العليا /قسم القانون المقارن، ٢٠٢١، ص ٧٤ وص١٠٣.

الموظف قد تصرف بصورة مستقلة عن صاحب العمل وليس هناك إرتباط وثيق بين فعله وبين توجيهات صاحب العمل بسبب أن شركة (موريسونز) إلتزمت بمستوى كاف من الأمان وبذلت عناية الرجل الحريص في الحفاظ على إجراءات الأمن السيبراني لمنع وقوع المخاطر السيبرانية على أنظمة التشغيل فيها، كما لم تجد المحكمة أي خطأ في الإجراءات الأمنية المتخذة من قبلها لحماية البيانات، وقررت أن تصرف الموظف كان فردياً وبدوافع شخصية بقصد الإضرار بصاحب الشركة، ولو لم تكن الشركة قد إتخذت كافة الإحتياطات الفنية والأمنية اللازمة لحماية البيانات من الاختراق لكان القرار مختلفاً[1].

وفي إعتقادنا أن طريقة إثبات شركة التأمين صدور الخطأ العمدي من قبل أحد موظفي الشركة المؤمن لها بصورة شخصية، أمر في غاية الصعوبة، لا سيما عند إنعدام وجود معيار قانوني يحدد الإرتباط الوثيق بين خطأ الموظف وتوجيهات صاحب العمل، لذا نجد أن إستقرار المعاملات والحفاظ على الثقة فيها يحتم سقوط حق المؤمن له بالرجوع على شركة التأمين من المخاطر السيبرانية، كون الخطأ صادر بصورة عمدية من أحد تابعي الشركة، وبالتالي يقع على الشركة التجارية المؤمن لها دفع التعويض المحدد بمقدار الضرر الذي تسببت فيه للغير المتضرر من أعمال تابعيها على أساس مسؤولية المتبوع عن اعمال تابعه، ومن ثم الرجوع على التابع بقيمة التعويض المدفوع.

٧. **الإلتزام بعدم تغيير الشركة التجارية (المؤمن لها) لسلوكها الأمني بعد إبرام عقد التأمين من المخاطر السيبرانية:** وتجدر الإشارة إلى أن خصوصية التأمين من المخاطر السيبرانية تفرض على المؤمن له إضافةً لما تقدم من إلتزامات، إلتزاماً وهو الإلتزام بعدم التغير المحتمل في سلوك الشركة التجارية المؤمن لها تجاه المخاطر السيبرانية بعد إبرام عقد التأمين، كأن تتراجع في الإمتثال لمعايير الأمن والسلامة السيبرانية كونه سلوك غير قانوني و يجب أن يتم منعه من خلال فرضه كإلتزام إضافي في العقد، بسبب أن ذلك التغيير في السلوك المتبع من قبل الشركة التجارية المؤمن لها يعرقل عمل شركة التأمين من المخاطر السيبرانية في حساب إحتمالية حصول الأضرار، و لما كانت

(1) WM Morrisons Supermarkets plc (Appellant) v Various Claimants (Respondent), Judgment date, 01 Apr 2020, Neutral citation number, [2020] UKSC 12, Case ID: UKSC 2018/*0213*.
https://www.mcgradyinsurance.com/news/supreme-court-employer-liability
Date of visit: 5/6/2023 4:00pm.

الأضرار الواقعة في الفضاء السيبراني تحدث نتيجة جرائم أطرافاً ثالثة أو بسبب عيوب تقنية فإن إحداث المؤمن له للضرر من قبله عن تطريق تقليل اجراءات الأمان المتبعة لغرض الحصول على مبلغ التأمين هو فرض وارد ، حيث قد تتسبب الشركة التجارية المؤمن لها بإحداث الضرر أو إهمال الاجراءات الأمنية المفروضة عليها[١]. ووفقاً للقواعد العامة لا تستحق الشركة التجارية (المؤمن لها) مبلغ التأمين إذا تسببت عمداً بوقوع الخطر السيبراني المؤمن منه، وينتفي العقد ولا يكون المؤمن مسؤولاً عن التعويض عن هذا الخطر، فشركة التأمين من المخاطر السيبرانية لا تكون ملزمة قانوناً بتعويض الخسائر والأضرار التي تسببت بها الشركة التجارية المؤمن لها عن عمد أو غش حيث تنتفي صفة الإحتمالية من الخطر وبالتالي يبطل العقد[٢].

الفرع الثاني

إلتزامات المؤمن (شركة التأمين) من المخاطر السيبرانية

المؤمن هو الطرف المقابل للمؤمن له في عقد التأمين، وهو الطرف الأول في العقد والشخص الذي يتحمل عبء الخطر ويتعهد بسداد مبلغ التأمين أو التعويض عن الأضرار التي تلحق بالمؤمن من دعاوى الغير عليه وقد يباشر بإبرام العقد بنفسه أو قد يتم التعاقد من خلال وسيط أو وكيل يكون بمنزلة المؤمن وبمقابل عمولة محددة [٣]. وقد اكتفى المشرع العراقي في القانون المدني رقم (٤٠) لسنة ١٩٥١ بتعريف المؤمن له في المادة (٩٨٣ / ف٢) ولم يذكر تعريفاً للمؤمن، وبالرجوع لتعريف المشرع العراقي لعقد التأمين في الفقرة الأولى من المادة (٩٨٣) يمكن تعريف المؤمن بأنه "الطرف الذي يؤدي للمؤمن له أو المستفيد مبلغاً من المال أو ايراد مرتب أو أي عوض مالي آخر عند تحقق الحادث المؤمن منه مقابل قسط أو دفعة مالية يؤديه الطرف المؤمن له"، وقد عرفت المادة الثانية من قانون تنظيم أعمال التأمين العراقي رقم (١٠) لسنة ٢٠٠٥ المؤمن بأنه ((القائم بالتأمين أو إعادة التأمين الذي تسري عليه احكام هذا القانون وهو قد يكون شركة تأمين عراقية أو فرع شركة تأمين اجنبية أو اي كيان أو جهة مخولة لممارسة أعمال التأمين في العراق)).

(١) صدام فيصل كوكز، مصدر سابق، ص ١٣٦.

(٢) محمد حسين منصور، مصدر سابق، ص ٥١.

(٣)علي أحمد شاكر وآخرون، تأمين المسؤولية المدنية، مركز جامعة القاهرة للتعليم المفتوح، القاهرة، ١٩٩٤، ص٢٣.

وتترتب على شركة التأمين من المخاطر السيبرانية بصورة عامة جملة من الإلتزامات الناجمة عن إنعقاد عقد التأمين بغض النظر عن نوع الخطر المؤمن منه وطبيعته ويمكن إجمالها بما يأتي:

١. **الإلتزام بالحفاظ على سرية بيانات المؤمن له (الشركة التجارية):** وهو التزام يقع على عاتق شركة التأمين من المخاطر السيبرانية مضمونه الامتناع عن إفشاء الوقائع والمعلومات والأسرار التجارية التي تصل لعلمها بطريقة مباشرة من الشركة التجارية المؤمن لها، أو بطريقة غير مباشرة بمناسبة ممارستها لمهامها، ويعدّ الإلتزام بالسرية أحد أهم الإلتزامات شركات التأمين في عقد التأمين من المخاطر السيبرانية، فعلى المؤمن أن يحرص على سرية البيانات التي تم جمعها من المؤمن لهم أثناء الإدلاء بالمعلومات الواجب ذكرها لإتمام التعاقد ومنحهم وثيقة التأمين، فالشركات التجارية غالباً ما تفضل التعرض لخسارة مالية على أن تتعرض لخسارة في السمعة التجارية نتيجة إفشاء أسرارها التجارية[١]، وبدأت بعض الدول بالتوجه إلى تأطير الإلتزام سالف الذكر بإطار قانوني ؛ حيث تم تشريع عدد من القوانين المختصة بحماية البيانات ، فعلى سبيل المثال نص القانون القطري رقم (١٣) لسنة ٢٠١٦ والمتعلق بحماية خصوصية البيانات الشخصية في الفصل الثالث منه بالمواد (١٣-١٥) على الإلتزام بإتخاذ الاحتياطات لغرض حماية البيانات الشخصية من التلف أو الضياع أو التعديل أو الافشاء أو استخدامها بشكل عارض أو غير مشروع وبما يتناسب مع طبيعة وأهمية تلك البيانات وإعلام الجهات المختصة عند حدوث أي اخلال بتلك الاحتياطات الواجب اتخاذها. وقد شرعت العديد من الدول الأخرى في هذا السياق قوانين خاصة بحماية البيانات الشخصية كالمشرع التونسي والذي شرع قانون حماية المعطيات الشخصية رقم (٦٣) لسنة ٢٠٠٤، والمشرع المغربي الذي شرع قانون حماية المعطيات ذات الطابع الشخصي رقم (٠٩/٠٨) لسنة ٢٠٠٩، والامارات العربية المتحدة والتي اصدرت قانون حماية البيانات الشخصية الفيدرالي رقم (٤٥) لسنة ٢٠٢١. بالإضافة إلى قانون المعاملات الالكترونية العماني رقم (٦٩) لسنة ٢٠٠٧ حيث لم ينظم حماية البيانات الشخصية بشكل مستقل كالقوانين السابقة[٢] ، أما المشرع العراقي فقد إنتهج نهج المشرع

---

(١) علاء النجار حسانين، نطاق الإلتزام بالسرية في التحكيم التجاري الدولي، دار التعليم الجامعي للنشر والتوزيع، الإسكندرية، ٢٠١٩، ص٧.

(٢) دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي قراءة في قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، المجلد (٨) .العدد (٠) عدد خاص، ٢٠٢٢، ص١٠.

العماني ولم يشرع قانون خاص بحماية البيانات الشخصية حيث أدرج بعض نصوص حماية البيانات الشخصية ضمن قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢.

ونستنتج من خلال إطلاعنا على عدد من وثائق التأمين من المخاطر السيبرانية خصوصية هذا العقد والتي تكمن في البيانات المؤمن عليها، ومما لاشك فيه أن غالبية شركات التأمين المتخصصة في هذا النوع من التأمين تطلب إبتداءً من الشركة التجارية المؤمن لها عدداً من المعلومات التي تساعد المؤمن في تحليل المخاطر والوقوف على حجم الاخطار المحتملة لتحديد قيمة التأمين، فليس بالأمر الغريب أن تشدد جميع القوانين واللوائح والأنظمة سالفة الذكر على أهمية الإلتزام بالمعايير المهنية لدى جميع الشركات بصورة عامة، والشيء ذاته ينطبق على شركات التأمين من المخاطر السيبرانية(١).

ويرى البعض أن إخلال المؤمن له بإلتزامه بالحفاظ على البيانات داخل الوسط السيبراني، بعد أن تم الإدلاء بها من قبل الشركة التجارية بموجب أحكام عقد التأمين من المخاطر السيبرانية يخضع لأحكام قوانين حماية حقوق المؤلف نظراً لما تتمتع به من حقوق التأليف من حماية قانونية خاصة بإعتبار أن معلومات الشركة التجارية تعتبر من قبيل المصنفات الأصلية في الآداب أو الفنون أو العلوم التكنولوجية وغيرها، واستبعدوا المسؤولية العقدية أو التقصيرية كأساس لهذا الإلتزام(٢). وبإعتقادنا أن الأساس القانوني لإلتزام شركة التأمين بالسرية هو عقد التأمين من المخاطر السيبرانية، فتكون مسؤوليته عقدية تجاه المؤمن له وفقاً لذلك، أما مسؤولية شركة التأمين تجاه الغير، فتكون مسؤولية تقصيرية لعدم وجود التزام عقدي تم الاخلال به، وانما اساس الالتزام هو نص القانون الذي يحظر إفشاء الأسرار التجارية.

٢. **الإلتزام بأحكام اللائحة العامة لحماية البيانات عند معالجة بيانات المؤمن له:** يجب على شركة التأمين من المخاطر السيبرانية أن تلتزم بتنفيذ جميع التدابير الفنية والتنظيمية المناسبة بصورة تضمن أن المعالجة تتم وفق للائحة العامة للبيانات مع الأخذ بنظر الإعتبار مراجعة هذه التدابير وتحديثها

---

(١) وهذا نلاحظه في جميع وثائق التأمين من المخاطر السيبرانية مثل:
(MSIG) CYBER INSURANCE POLICY،(TRAVELERS (cyber policy)2016)
(QBE)Cyber Response Insurance Policy،Danmark(AXIS) Cyber ansomeware Supplement Application،No. 1012729 10 20

(٢) اسماعيل عبد النبي شاهين، مصدر سابق، ص٢١.

عند الضرورة[١]، وأن تتسم بالمهنية عند جمع بيانات الشركات التجارية المؤمن لها تكون بيانات التوقيع الالكتروني والوسائل الالكترونية والمعلومات سرية ولا يجوز لمن قدمت اليه أو اطلع عليها بحكم عمله افشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله [٢]. ويتفرع عن هذا الإلتزام إحاطة الشركات التجارية طالبة التأمين بالمسوغ القانوني أو العملي لجمع بياناتهم الشخصية وتحديد الغرض منها، والإمتناع عن معالجة البيانات المتوافرة لديها بصورة تتنافى مع الغرض من جمعها أو في غير الاحوال المنصوص عليها قانوناً، كما تلتزم بالسماح لصاحب البيانات الشخصية بتصحيح بياناته الشخصية المتوافرة لديه (الحق في التصحيح) أو تحديثها أو إتلافها إذا انتهت الحاجة إليها (الحق في النسيان)[٣]. ولا يجوز للمؤمن جمع البيانات الشخصية إلا من صاحبها مباشرةً وللغرض الذي أعدت من اجله بأستثناء بعض الحالات كالحصول على موافقة صاحب البيانات أو أن تكون تلك البيانات متاحة للعموم أو أن تكون عملية جمع البيانات تمت من قبل جهة عامة وكانت عملية الجمع مطلوبة لأغراض أمنية أو ضرورياً الحماية الفرد أو لتنفيذ القانون أو لغرض استيفاء متطلبات قضائية أو اذا كانت تلك البيانات التي تم جمعها من قبل شركة التأمين لن تسجل أو تحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها بصورة مباشرة أو غير مباشرة وفق القانون[٤]. وعلى شركة التأمين ان تحيط الشركات التجارية طالبة التأمين بهوية من يجمع البيانات وعنوان مرجعه وابلاغه بالجهة التي سيتم الإفصاح بالبيانات إليها ان وجدت وتحديد ما إذا كان سيتم نقل البيانات لجهة أخرى ام لا[٥]. كما تلتزم شركة التأمين بالإكتفاء بالحد الأدنى من

---

(١) المادة (٢٤) من اللائحة العامة لحماية البيانات (GDPR) لسنة ٢٠١٦.

(٢) المادة (١٢/ ثانياً) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم (٧٨) لسنة ٢٠١٢.

(٣) أكدت على ذلك بنصوص واضحة كل من: المواد (١٦ و ١٧) من اللائحة العامة لحماية البيانات (GDPR)، والمادة (٤) من نظام حماية البيانات الشخصية السعودي (م/١٩) لسنة ٢٠٢١ حيث تم النص في كل منهما حق النسيان وحق التصحيح بنصوص صريحة، قانون حماية المعطيات الشخصية التونسي رقم (٦٣) لسنة ٢٠٠٤ القسم الثاني / الفصول ٩/١٠/١١.

(٤) انظر: المادة (١٠) من نظام حماية البيانات الشخصية السعودي لسنة ٢٠٢١، قانون حماية المعطيات الشخصية التونسي رقم (٦٣) لسنة ٢٠٠٤ القسم الثاني / الفصل ١٢، المادة (٢/ف٢) و المادة (٤) من قانون حماية البيانات الشخصية الفيدرالي الإماراتي رقم (٤٥) لسنة ٢٠٢١.

(٥) انظر: المادة (١١) من نظام حماية البيانات الشخصية السعودي لسنة ٢٠٢١، قانون حماية المعطيات الشخصية التونسي رقم (٦٣) لسنة ٢٠٠٤ القسم الأول/ الفصل ٨/٧، المادة (٥) من قانون حماية البيانات الشخصية الفيدرالي الإماراتي رقم (٤٥) لسنة ٢٠٢١.

البيانات اللازمة لتحقيق الغرض من عملية التأمين مع تجنب طلب بيانات تؤدي إلى معرفة صاحبها بصورة محددة متى ما تحقق الغرض من جمعها. وإذا اتضح لشركة التأمين أن البيانات التي تم جمعها من قبل الشركات التجارية طالبة التأمين لم تعد ضرورية لتحقيق الغرض من جمعها فعليها التوقف عن جمعها واتلاف ما سبق وأن تم جمعه من بيانات فوراً[١].

أما إذا كانت عملية جمع البيانات قد تمت لأغراض احصائية ولم تتضمن ما يدل على هوية صاحبها بالتحديد أو أنه سيتم إتلافها قبل الافصاح عنها لجهة أخرى ولم تكن تلك البيانات بيانات حساسة فإنه يجوز جمعها أو معالجتها دون موافقة صاحبها[٢]. وفي السياق ذاته ميزت بعض قوانين حماية البيانات الشخصية بين البيانات الشخصية بصفة عامة والبيانات الحساسة و تم استثناء بعض البيانات من الحماية التشريعية الواردة في القانون وهي البيانات التي تستخدم في اطار شخصي أو تلك المستخدمة لأغراض الاحصائيات الرسمية أو لغرض تطبيق القانون أو الاعلام ونشر المعرفة أو الامن القومي والعمل القضائي أو المعاملات المالية الخاضعة لإشراف البنك المركزي من ناحية، ومن جهة أخرى فرض حماية مشددة على بعض البيانات أطلق عليها تسمية (البيانات الحساسة) وحظر التعامل بها بكل شكل من الأشكال إلا بعد الحصول على ترخيص من مركز حماية البيانات الشخصية وموافقة الشخص المعني موافقة كتابية وصريحة[٣]، والعلة من وراء فرض هذه الحماية المشددة هي إرتباط تلك البيانات بالحرية الشخصية والكشف عنها أو اساءة استخدامها يعد انتهاك لتلك الحرية وتهديد لأمن وسلامة الأفراد[٤].

٣. **الإلتزام بالمتابعة (التفتيش والتدقيق):** تلتزم شركة التأمين من المخاطر السيبرانية أو أي ممثل تقوم بتعيينه، بفحص أنظمة تشغيل الشركة التجارية و التحقق من مدى أمان الوسط التي تتم فيه العمليات الإلكترونية والإطلاع على تقارير موظفي إدارة الأمن السيبراني في الشركة، بالإضافة لمتابعة وتدقيق

(١) انظر: المادة (١٣) من اللائحة العامة لحماية البيانات (GDPR) والمادة (١٣) من نظام حماية البيانات الشخصية السعودي لسنة ٢٠٢١. قانون حماية المعطيات الشخصية التونسي رقم ٦٣ لسنة ٢٠٠٤ القسم الثاني / الفصل ١١.

(٢) انظر: المادة (٢٧) من نظام حماية البيانات الشخصية السعودي لسنة ٢٠٢١، قانون حماية المعطيات الشخصية التونسي رقم (٦٣) لسنة ٢٠٠٤ القسم الثاني / الفصل ١٢.

(٣) المادة الأولى من الفصل الأول من قانون حماية البيانات الشخصية المصري رقم (١٥١) لسنة ٢٠٢٠، المادة الأولى من قانون حماية البيانات الشخصية الفيدرالي الإماراتي رقم (٤٥) لسنة ٢٠٢١.

(٤) دعاء حامد محمد عبد الرحمن، مصدر سابق، ص٩.

أنواع البيانات قيد المعالجة، وتدقيق أي اتفاقية معالجة مع مصادر خارجية، وعمل تقرير بالنتائج، علماً أن التزام شركة التأمين من المخاطر السيبرانية بالتدقيق لا يعطي لها الحق بممارسة واجبها في أي وقت، بل انها ملزمة بتقديم اشعار للشركة التجارية المؤمن لها قبل بدء عملية التفتيش، ولا يمكن الاعتداد بهذا التقرير إلا بين أطراف عقد التأمين، فعادة ما تصرح شركات التأمين في عقود التأمين من المخاطر السيبرانية بعدم إمكانية الإعتداد بنتائج التقرير من قبل أي جهة أخرى، فهو يعتبر بمثابة إقرارمن شركة التأمين بضمان وجود مستوى معين للأمان في العمليات التجارية السيبرانية للشركة التجارية [١] وفي إعتقادنا أن متابعة وتدقيق شركة التأمين لأنظمة التشغيل أو تقارير الأمن السيبراني أقرب إلى أن يكون حق أكثر مما هو إلتزام، فمن حق شركة التأمين أن تحيط علماً بجميع البيانات والتقارير التي تساعدها في تحديد مركز الشركة التجارية من حيث الأمن السيبراني والذي يترتب عليه تحديد القسط التأمين، قبل أن تبادر بقبول التغطية.

٤. **تحري الدقة في تحديد قيمة قسط التأمين:** قد يكون هذا شاملاً لجميع أنواع التأمين وليس خاصاً بشركات التأمين من المخاطر السيبرانية إلا أن خصوصيته وأهمية التأكيد عليه ناتج عن أن المسؤولية في مجال تقنية المعلومات والتكنولوجيا تكون متميزة عن غيرها بضخامة الأضرار الناشئة عنها وصعوبة التعرف على محدث الضرر بالإضافة إلى صعوبة اثبات الخطأ، الأمر الذي يحتم على شركة التأمين من المخاطر السيبرانية ان تلتزم الدقة عند تحديد قسط عقد التأمين بشكل دقيق قدر الإمكان مع من خلال إحصاء المخاطر السيبرانية التي تعرضت لها لشركات التجارية المؤمنه أو قابليتها للتعرض لها بعد إبرام عقد التأمين، و إمكانية تقييم الخسائر بعد وقوع الخطر السيبراني المؤمن منه وهذا الأمر غاية في الصعوبة مقارنة بعقود التأمين من المخاطر التقليدية الأخرى، الأمر الذي يجعل الإلتزام في هذا العقد صعباً ومعقداً ومكلفاً[٢].

(1) Diamantopoulou V, Gritzalis S, Lambrinoudakis C. Cyber insurance: state of the art, trends and future directions، International Journal of Information Security،vol. (22), 2023, p742.

(٢) شذى عبد جمعة موسى، مصدر سابق، ص ٢٣٥.

المطلب الثاني

التزامات أطراف العقد بعد تحقق الخطر السيبراني

بعد أن تعرفنا على إلتزامات كل من طرفي عقد التأمين من المخاطر السيبرانية بقي لنا ان نبين ماهية الأثار المترتبة نتيجة وقوع الخطر السيبراني المؤمن منه والوارد ذكره في وثيقة التأمين. وبما أن الخطر السيبراني نادراً ما يكون أثره محصوراً بأطراف العقد بسبب طبيعة هذا الخطر التي تتعدى إلى الغير كعملاء الشركة التجارية والموردين والمستهلكين وغيرهم. لذا سنقسم المطلب إلى فرعين، حيث نبحث في الفرع الأول الإلتزامات المترتبة بين طرفي العقد بعد تحقق الخطر السيبراني، أما في الفرع الثاني سنبحث في إلتزامات أطراف العقد تجاه الغير بعد تحقق الخطر السيبراني.

الفرع الأول

الإلتزامات المترتبة بين طرفي العقد بعد تحقق الخطر السيبراني

يؤدي وقوع الخطر السيبراني إلى أضرار تختلف بحسب طبيعة الشركة التجارية وتتراوح من تدهور سمعتها مع عملائها سواء كانوا شركات أو أفراد أو موردين ؛ إلى فقدان ميزة تنافسية في الحالة التي يؤدي فيها تحقق الخطر السيبراني إلى انتهاك ملكيتها الفكرية فالأثر المترتب على تحقق خطر سيبراني معين لشركة تجارية ما، يختلف عن الأثر المتحقق لشركة أخرى نتيجة وقوع الخطر ذاته، فمثلاً سيكون الأثر المترتب على إنقطاع الأعمال بسبب إختراق نظام شركة مبيعات عبر الإنترنت أكثر ضرراً من الشركة التي لها مركز عمل مادي وتستخدم الحواسيب في أعمالها التجارية بصفه ثانوية كما أن حجم الشركة و منافسيها ومدى أهمية بياناتها وحتى مركزها داخل الدولة يجب أخذه بنظر الإعتبار عند وقوع الخطر السيبراني[1].

ويرتب عقد التأمين من المخاطر السيبرانية إلتزامات متبادلة تقع على عاتق الطرفين عند تحقق الخطر المؤمن منه، والتي يمكن إجمالها بالآتي:

(1) Gaspard Ferey, Nicolas Grorod, Simon Leguil, op. cit, p37.

أولاً: التزامات المؤمن له (الشركة التجارية) بعد تحقق الخطر السيبراني

١. **إخطار شركة التأمين بتحقق الخطر السيبراني المؤمن منه:** إن أهمية هذا الإلتزام تكمن في النتائج المترتبة على وقوع الخطر، حيث تلتزم شركة التأمين من المخاطر السيبرانية بدفع مبلغ التأمين بعد إخطارها بوقوع الخطر، ومن مصلحة المؤمن معرفة تحقق الخطر على وجه السرعة الممكنة ليتبين مداه ونتائجه ليتم دفع التعويض الملتزم به في العقد، فضلاً عن أهمية هذا الإخطار لإتخاذ المؤمن الإجراءات اللازمة للحد من آثار الخطر والتخفيف منها وتحديد المسؤول عن تحققه، ليتمكن من الرجوع عليه فيما بعد. ويتمثل مضمون هذا الإلتزام من خلال قيام المؤمن له (الشركة التجارية) بتقديم الوثائق والمستندات كافةً لشركة التأمين والتي تتعلق بتوقيت وقوع الخطر ومكانه وأسباب وقوعه والظروف التي أحاطت به، وما ترتب على وقوعه من أضرار، وغيرها..[١] وبمقتضى وثائق التأمين المعمول بها فإن على المؤمن له كذلك إشعار المؤمن بوقوع الخطر المؤمن منه خلال فتره زمنية محددة[٢]. ولكي تستطيع الشركة التجارية الوفاء بإلتزامها المتعلق بالإعلان عن الخطر السيبراني المؤمن منه وتطبيقاً لمبدأ حسن النية فعليها أن تقوم من تلقاء نفسها بالإدلاء ببعض البيانات الشخصية كالبيانات المتعلقة بالخطر السيبراني المؤمن منه وبالظروف المحيطة به كون المؤمن له هو الطرف الأكثر دراية بالظروف المحيطة بالخطر السيبراني محل التأمين ، ويتم ذلك من خلال الإجابة على مجموعة من الأسئلة المعدّة مسبقاً من قبل شركة التأمين وتتعلق بالخطر والظروف المحيطة به لتتمكن من تقدير الخطر من جانب ولإثبات إخلال المؤمن له بإلتزامه بالإعلان عن الخطر السيبراني من جانب آخر ، فإذا ما تعمدت الشركة التجارية إخفاء بعض هذه البيانات كونها تسيء إلى مركزها مثلاً أو كانت تعتقد بعدم أهميتها ولو بحسن نية فإنها تتعرض للمسؤولية نتيجة إخلالها بهذا الالتزام[٣].

٢. **إخطار الجهات المختصة قانوناً بتحقق الخطر السيبراني والتعاون معها:** تلتزم الشركة التجارية بإخطار الجهات المختصة قانوناً بتحقق الخطر السيبراني من دون تأخير، كحدوث خرق للبيانات الشخصية للعملاء، ويقدم الإخطار وفقاً لأحكام اللائحة العامة لحماية البيانات إلى الجهات المعنية

(١) محمد حسين منصور، مصدر سابق، ص١١٦.

(٢) باسم محمد صالح، مصدر سابق، ص٢٧٣.

(٣) عمار ياسر رشيد، مصدر سابق، ص ٧٤ وص١٠٣.

بقضايا الأمن السيبراني والتي أطلقت عليها تسمية (السلطات الإشرافية)[١] خلال موعد اقصاه (٧٢) ساعة من تاريخ العلم اذا كان ذلك ممكناً ، مع وصف طبيعة الخطر السيبراني والعدد التقريبي للمتضررين منه مع وصف النتائج المحتملة للخطر، وفي حال التأخر عن المدة المسموح بها قانوناً للإخطار يلتزم المؤمن له بإثبات وجود سبب لتأخير الإخطار[٢].

٣. إلتزام المؤمن له بتخفيف أثر المخاطر السيبرانية:

فبالإضافة للإلتزامات السابقة سيتعين على الشركة التجارية (المؤمن لها) ان تتخذ ما بوسعها من الإجراءات التقنية والإدارية اللازمة لإيقاف الخطر السيبراني في أسرع وقت ممكن، و ان تعمل على تخفيف الآثار المترتبة على وقوعه وحصر الضرر في اضيق نطاق وانقاذ ما يمكن انقاذه من الشيء المؤمن عليه، وهذا الإلتزام هو إلتزام قانوني حيث فرضت اللائحة العامة لحماية البيانات هذا الإلتزام على عاتق الشركات التجارية وكان الغرض الاساسي من النص على هذا الإلتزام في اللائحة هو التشديد على حماية البيانات الشخصية للعملاء حتى بعد تحقق الخطر السيبراني حيث أن تحققه لا يلغي الإلتزام الأصيل للشركات التجارية بالمحافظة على سرية بيانات عملائها[٣]. ويتفرع عن هذا الإلتزام التزامين فرعيين هما: الإلتزام المتابعة والإلتزام بالإعلان والإسترجاع، **والإلتزام بالمتابعة** يعني اتخاذ المؤمن له لجميع التدابير اللازمة لتتبع النتائج الضارة للخطر السيبراني المتحقق بعد اكتشاف تحققه كإكتشافه لإصابة أحد البرامج الشائعة بالفيروسات بعد أن طرحها للتداول، أما الإلتزام بالإعلان والاسترجاع يتمثل بإبلاغ العميل بوجود عيب في البرنامج مما يستدعي إستعادة المنتج لغرض فحصه وإصلاحه أو حتى سحبه من السوق[٤].

---

(١) ويقصد بالسلطة الاشرافية كل سلطة عامة تنشئها الدولة للإشراف على الأمن السيبراني. انظر المادة (٤/ف ٢١) من اللائحة العامة لحماية البيانات(GDPR).

وقد منحت اللائحة للسلطة الاشرافية في المادة (٥٨ /ف١) من اللائحة صلاحية اصدار التوبيخ إلى كل طرف مسؤول عن معالجة بيانات الغير على اثر انتهاكها لأحكام هذه اللائحة، كما ان لتلك السلطة الحق في فرض قيود مؤقته أو نهائية تتضمن فرض الحظر على المعالجة ولها ان تأمر بتصحيح ومحو البيانات الشخصية أو تقييد عملية معالجة البيانات واخطار المستفيدين الذين تم الكشف عن بياناتهم الشخصية بتلك الاجراءات

(٢) المادة (٣٣) من اللائحة العامة لحماية البيانات (GDPR) لسنة ٢٠١٦.

(٣)المواد (٢٥) و (٣٢) و (٣٣) من اللائحة العامة لحماية البيانات (GDPR).

(٤) طارق عفيفي صادق، مصدر سابق، ص ٣٥٧.

ثانياً: إلتزامات شركة التأمين بعد تحقق الخطر السيبراني

١. **الإلتزام بإصلاح الشيء المؤمن عليه واعادته إلى حالته وقت انعقاد العقد:** إن الاثر المترتب على تحقق الخطر السيبراني هو تعويض الضرر الذي لحق بالشركة التجارية المؤمن لها، ويختلف ذلك حسب نوع الخطر المؤمن منه ، ففي حالة التأمين على البيانات الإلكترونية ستلتزم شركة التأمين بوقف الهجوم أو تسرب البيانات والتأكد من أن ابعاد مسبب الضرر عن نظام معلومات الشركة مما يتطلب تدخلاً مكلفاً من الخبراء والذين هم من خارج الشركة في الغالب[١] ، كما تلتزم شركات التأمين من المخاطر السيبرانية بإصلاح نظام التشغيل أو الحواسيب أو الاعطال البرمجية عند تحقق الخطر السيبراني المؤمن منه من قبل الشركة التجارية (المؤمن لها) والغرض من هذا الإلتزام هو تفادي الغش الذي قد يصدرمن المؤمن له إذا ما قام بإصلاحه فيذكر سعر تكلفة الإصلاح أعلى من المبلغ الفعلي المدفوع[٢]. وهذا الإلتزام يؤدي للقول بوجوب توافر حداً كافياً من الخبرة في هذا المجال الأمر الذي يلزم شركات التأمين من المخاطر السيبرانية بتدريب كوادرها الإدارية والفنية للتعامل مع المخاطر السيبرانية المتحققة لإكتشاف حجم الخطر و مدى إمكانية تعديه للغير[٣].

٢. **الإلتزام بدفع التكاليف:** ويقصد به أن شركة التأمين من المخاطر السيبرانية ستكون ملزمة تجاه الشركة التجارية المؤمن لها بدفع تكاليف الإخطار بوقوع الخطر السيبراني المؤمن منه، والنفقات المعقولة والضرورية لخبراء تكنولوجيا المعلومات والتي تتكبدها الشركة التجارية، بالإضافة للتكاليف الضرورية التي يتكبدها المؤمن له للحفاظ على السمعة التجارية لمنع وتقليل آثار الخطر السيبراني المؤمن منه على سمعة الشركة التجارية بشرط استحصال المؤمن له لموافقة خطية مسبقة من شركة التأمين[٤].

---

(١) قضية (EMOI Servs LLC ضد Owners Ins.Co Slip Opinion) / المحكمة العليا في أوهايو / قرار رقم ٤٦٤٩-أوهايو -٢٠٢٢ في ٢٧ ديسمبر ٢٠٢٢ منشور على الموقع الرسمي للمحكمة:
https://www.hinshawlaw.com/newsroom-updates-ohio-supreme-court-no-coverage-ransomware-physical-damage-limitation.html تاريخ الزيارة ٢٠٢٣/٢/١٣ الساعة ٥:٠٠م.

(٢) بولحية سمية، النظام القانوني لعقد التأمين على المركبات في التشريع الجزائري، رسالة ماجستير مقدمة إلى جامعة العربي بن مهيدي ام البواقي /كلية الحقوق والعلوم السياسية، ٢٠١١، ص ٨٠.

(٣) طارق عفيفي صادق، مصدر سابق، ص٦٨.

(4) Tsohou A Diamantopoulos V, Gritzalis S, Lambrinoudakis C, op. cit, p742.

٣. **الإلتزام بدفع مبلغ التأمين من المخاطر السيبرانية:** متى ما تحقق الخطر أو حل أجل العقد أصبح التعويض أو المبلغ المستحق بمقتضى عقد التأمين واجب الأداء[١]. ومبلغ التأمين هو المبلغ الذي يلتزم به المؤمن عند وقوع الخطر المؤمن منه إلى المؤمن له أو المستفيد، وهذا الالتزام هو المقابل لأداء المؤمن له (الشركة التجارية) بدفع القسط ويتناسب معه طردياً حيث كلما ارتفع قسط التأمين ارتفع مبلغه المستحق الدفع للمؤمن له[٢]. فتلتزم شركة التأمين من المخاطر السيبرانية بإلتزام تقليدي تجاه الشركة التجارية طالبة التأمين ويتمثل ذلك بتعويض الشركة التجارية المؤمن لها من الخطر السيبراني عن الضرر الناشئ من وقوع الخطر المؤمن منه شرط أن لا يتجاوز التعويض لقيمة التأمين الواردة في العقد[٣]. فيكون مبلغ التأمين بما يقابل مبلغ الخسارة الحقيقية التي لحقت بالشركة التجارية المؤمن لها من تحقق الخطر السيبراني المؤمن منه، بحيث تلتزم شركة التأمين من المخاطر السيبرانية بحدود المبلغ الوارد في وثيقة التأمين حتى لا يكون التعويض سبباً لافتقار المؤمن أو إثراء المؤمن له، وكما هو الحال في جميع عقود التأمين فإن التزام المؤمن بالتعويض وتحمل نفقات التقاضي والدفاع يكون رهناً بتوافر شروط معينة:

١- تحقق الخطر المؤمن منه وتضرر محل عقد التأمين.

٢- وجود علاقة سببية بين الخطر المؤمن منه والضر الناشئ عنه

٣- أن لا يكون الخطر المؤمن منه قد تحقق بفعل الشركة التجارية طالبة التأمين عمداً أو بالتواطؤ مع محدث الضرر

٤- أن لا تكون الأضرار الواقعة قد حدثت للشركة المؤمن لها بسبب مخاطر مستثناة في العقد. أو تسبب في وقوعها خطر غير مشمول بالتغطية التأمينية.

٥- أن يكون المؤمن قد التزم بكافة الشروط التعاقدية مع شركة التأمين و بذل العناية اللازمة في المحافظة على الشيء المؤمن عليه وان لا تشتمل المطالبة على دفوع صحيحة للمؤمن [٤].

ومبلغ التأمين – أو ما يسمى بعهدة المؤمن أو العوض المالي أو عوض التأمين أو أداء المؤمن – هو الأداء المالي الذي يدفعه المؤمن للمؤمن له أو المستفيد عند تحقق الخطر المؤمن منه

---

(١) المادة (٩٨٨) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

(٢) ابي الفضل هاني بن فتحي، التأمين: أنواعه المعاصرة، ط١، دار العصماء، دمشق، ٢٠٠٩، ص٥٩.

(٣) وفقاً للمادة (٩٨٩) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

(٤) شذى عبد جمعة موسى، مصدر سابق، ص٢٣٤.

في مقابل القسط الذي يدفعه المؤمن له، ويكون مبلغ التأمين متناسباً مع القسط فكلما زاد القسط زادت قيمة التأمين وقد تلتزم شركة التأمين بدفع مبلغ التأمين بصورة مالية دفعة واحدة أو على شكل دفعات شهرية أو قد يكون مبلغ التأمين اي عوض مالي آخر(١). ويكون إلتزام المؤمن بأداء مبلغ التأمين عبارة عن إلتزام إحتمالي إذ لا يكون واجب الأداء إلا إذا تحقق الخطر المؤمن منه ، حيث إن تحقق الخطر هو ركن أساسي لإلتزام المؤمن وليس مجرد شرط في العقد، وبما أن المؤمن له يلتزم بإخطار المؤمن بوقوع الخطر المؤمن منه وعند توافر البيانات والمستندات التي تسمح لشركة التأمين بالتثبت من صحة هذه البيانات والتي يطمئن لها المؤمن ولا يحدث تنازع فيها فمن واجب شركة التأمين أداء التزامها الرئيسي والمتمثل بالضمان المتفق عليه وفي أجلٍ معقول(٢).

ويختلف مبلغ التأمين الذي يلتزم المؤمن بدفعه بإختلاف نوع التأمين، ففي التأمين على الاشخاص يكون مبلغ التأمين محدد بالقيمة المتفق عليها مسبقاً مع المؤمن له في وثيقة التأمين دون النظر لحجم الضرر الناجم عن تحقق الخطر، أما في التأمين عن الأضرار فإن التعويض يكون بحدود ما أصاب الشركة التجارية المؤمن لها من ضرر شرط أن لا تتجأوز قيمة هذا الضرر لقيمة مبلغ التأمين المتفق عليه في الوثيقة والذي يعتبر الحد الأعلى لإلتزام المؤمن(٣). يتمثل التعويض في التأمين عن الأضرار بما أصاب الشيء المؤمن عليه من هلاك أو تلف إذا كان التأمين هو التأمين على الأشياء، أما إذا كان تأمين من المسؤولية فإن الضرر يكون بقيمة ما يتكبده المؤمن له من خسائر بسبب رجوع المضرور عليه. أما بالنسبة للتأمين عن المخاطر السيبرانية فلا يوجد نص تشريعي يحدد قيمة التعويض الواجب دفعه مما دفع البعض للقول بإمكانية تطبيق القواعد الخاصة بالتأمين على الأشياء لتحديد المبلغ الواجب دفعه عند تحقق الخطر السيبراني المؤمن منه والتي تغطي قيمة الأضرار المباشرة فقط،إلا أن الخطر السيبراني بسبب طبيعته الخاصة لا ينحصر اثره بالضرر المباشر فقط(٤)، فغالباً ما يضاف إليها الأضرار غير المباشرة والتي يصعب حسابها

(١) بولحية سمية، مصدر سابق، ص ٨٠.

(٢) وقد أورد المشرع العراقي استثناء على هذا الاصل عند التأمين من المسؤولية حيث ان التزام المؤمن بالضمان لا ينتج اثره الا حين مطالبة المتضرر للمستفيد من عقد التأمين بعد وقوع الخطر الذي نجمت عنه هذه المسؤولية. للمزيد انظر: ثروت عبد الحميد، العقود المدنية المسماة، الكتاب الثالث، الاحكام العامة في عقد التأمين، بلا سنة نشر، ص ٦٣ وما بعدها. والمادة (١٠٠٤) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥٩.

(٣) سنا مازن فالح، مصدر سابق، ص٧٥.

(٤) عمار ياسر رشيد، مصدر سابق، ص ١١٠.

والإحاطة بها وتقديرها مقارنة بالأضرار المباشرة، حيث يصعب على القضاة وخبراء التأمين تقديرها بالمال لتحديد مبلغ التعويض المستحق عنها. فلعل أسهل الخسائر تقديراً هي تلك التي تنتج عن تلف المكونات المادية للنظام المعلوماتي في الشركة التجارية، كأجهزة الحاسوب وغيرها(١).

ويلتزم المؤمن بتعويض المستفيد عن الضرر الذي نشأ بسبب وقوع الخطر المؤمن منه شرط أن لا يتجاوز التعويض لقيمة التأمين المتفق عليها في العقد(٢)، ذلك أن المبدأ الأساسي الذي يكمن وراء التأمين بجميع أنواعه من أجل تجنب التخمينات المبالغة للتعويضات التأمينية عند حدوث الخسارة إعادة الشركة التجارية إلى الحالة التي كان عليها قبل وقوع الخطر المؤمن منه، لذا فأن أي إثراء للمؤمن لهم من التغطية على حساب شركة التأمين من المخاطر السيبرانية سيكون غير قانوني(٣).

ويُثار التساؤل في نطاق التأمين من المخاطر السيبرانية عن مدى إمكانية تطبيق القواعد الخاصة بالتأمين ضد الأضرار والمتعلقة بالتأمين على الاشياء ومدى فاعليتها في تغطية الضرر الناشئ عن تحقق الخطر السيبراني؟

يذهب البعض إلى أن القواعد التي تحدد قيمة التعويض عند تحقق الخطر في عقد التأمين على الاشياء لا تكفي لتحقيق الغاية من عقد التأمين من المخاطر السيبرانية حيث أنها تغطي الخسارة المباشرة فقط بينما يؤدي وقوع الخطر السيبراني إلى تكبد خسائر غير مباشرة هائلة بسب طبيعته الخاصة مما يستوجب إنفاق المضرور لمبالغ طائلة لتفادي إمتداد الخطر السيبراني ومساسها لباقي الاجهزة والبيانات و انقاذ ما تبقى منها أو حمايتها إلا أنه لا مجال لشمول الاخطار الالكترونية غير المباشرة دون وجود اتفاق مسبق بين طرفي العقد(٤) ، في حين يرى البعض الآخر أن الخسارة المترتبة على الخطر السيبراني هي خسارة عامة وتكون على نوعين: خسارة مالية أو الربح الفائت للمضرور، أو ان تكون خسارة معنوية تصيب الشخص بسمعته وكرامته أو بحقوقه المعنوية على ملكيته الفكرية(٥).

---

(١) طارق عفيفي صادق، مصدر سابق، ص٣١٦.

(٢) انظر: المادة (٩٨٩) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

(3) Gaspard Ferey, Nicolas Grorod, Simon Leguil, L'assurance des risques cyber, Mémoire de fin de formation du Corps des mines, Année de soutenance, 2017, P14.

(٤) عمار ياسر رشيد، مصدر سابق، ص١١٠.

(٥) اسراء فهمي ناجي، مصدر سابق، ص٢١.

وفي إعتقادنا أن التأمين من المخاطر السيبرانية من الممكن أن يندرج تحت غطاء التأمين عن الأضرار. فالتأمين من الأضرار هو تأمين ضد المخاطر التي يترتب على تحققها ضرراً بالذمة المالية للمؤمن له لا شخصه[١] كالتأمين من الحريق والتأمين من السرقة ويكون إما تأميناً على الأشياء حيث يهدف إلى تأمين المؤمن له من أي ضرر مباشر يصيب ماله، أو يكون تأميناً من المسؤولية حيث يهدف إلى تأمين الشركة التجارية من الرجوع عليها من قبل الغير بأحد دعاوى المسؤولية المدنية، ويعتبر الضرر في هذا النوع من التأمين ضرراً غير مباشر، فهو ضرر ينشئ بسبب دين في ذمة المؤمن له عند تحق مسؤوليته العقدية أو التقصيرية و يلتزم المؤمن بتعويض الضرر الناشئ عن وقوع الخطر على أن لا يتجاوز ذلك لقيمة التأمين على عكس التأمين على الأشخاص الذي يسوده مبدأ إنعدام صفه التعويض[٢].

ويمكن التمييز بين نوعين رئيسيين للأضرار الناشئة عن المخاطر السيبرانية حيث يتمثل النوع الأول بما يسمى بأضرار الأداء والتي يتم التعويض فيها عن الأضرار المادية وما يترتب عليها من خسائر وتتعلق بتدمير الممتلكات المرتبطة بالفضاء السيبراني ومنها إتلاف بيانات الحاسوب والإحتيال الحاسوبي وأعمال القرصنة الالكترونية ، ويمكن في هذا النوع من الأضرار الأخذ بالتعويض العيني وإعادة الحال إلى ما كانت عليه قبل وقوع الضرر الناجم من الخطر السيبراني المؤمن منه، ويكون ذلك بحسب طبيعة الممتلكات التي وقع عليها الخطر كإصلاح النظام الذي تم اختراقه أو إستعادة البيانات التي تم محوها وفي هذا النوع من الأضرار يجب على المؤمن له تحديد ما يعتبر من ضمن الممتلكات أولاً من ثم اثبات وقوع الخطر وحجم الخسائر المادية ثانياً. أما النوع الثاني من الأضرار فتتمثل بأضرار النشر كالضرر الناجم عن انتهاك الخصوصية ونشر البيانات السرية والأضرار التي تطول محتوى الملكية الفكرية الرقمية والتي تم تنظيم حمايتها بقوانين خاصة أما تلك التي لم يتم تنظيمها بقانون فيمكن تطبيق القواعد القانونية التقليدية عليها، فمثلاً تتمتع محتويات المواقع الإلكترونية وفقاً لمكتب الولايات المتحدة لبراءات الاختراع والعلامات التجارية (UPSTO) بذات منزلة براءات الإختراع وحقوق المؤلفين وبالتالي تخضع للقواعد القانونية المقررة لحقوق المؤلف والعلامات التجارية ذاتها للتشابه بينها وبالتالي يمكن حمايتها بذات القواعد

(١) هيثم حامد المصاروة، المنتقى في شرح عقد التأمين، ط١، اثراء للنشر والتوزيع، عمان، ٢٠١٠، ص٧٠.

(٢) عبد الرزاق السنهوري، مصدر سابق، ص ١٠٩٧.

القانونية[١]. وبالرغم من إنعدام النص التشريعي للضرر الواجب التعويض عنه في عقد التأمين من المخاطر السيبرانية، نجد أن أبرز القرارات القضائية قد استقرت على إمكانية التعويض عن الخسارة المادية المباشرة فقط عند تحقق الخطر السيبراني المؤمن منه ومثال على ذلك القضيتين أدناه:

١- أصدرت المحكمة العليا في أوهايو أهم القرارات المتعلقة بالتغطية من المخاطر السيبرانية لسنة ٢٠٢٢ في قضية (EMOI Servs LLC)، ضد (Owners Ins.Co Slip Opinion) [٢] حيث قضت بأن هجوم الفدية لم يتسبب بخسارة مادية مباشرة أو ضرر للبرنامج لذا فلا يمكن مطالبة شركة التأمين بتغطية تلك الخسائر لذا نقضت المحكمة العليا قرار محكمة الاستئناف واصدرت حكماً مستعجلاً للمحكمة الابتدائية لصالح شكة التأمين على اساس مخالفة حامل الوثيقة للعقد وادعاءات سوء النية. حيث تعرضت شركة (EMOI Servs) وهي شركة مختصة في برامج الكمبيوتر للمكاتب الطبية لهجوم برمجيات الفدية في سبتمبر ٢٠١٩ حيث تمكن متسلل مجهول و بشكل غير قانوني من الوصول لأنظمة الكمبيوتر الخاصة بها بالإضافة للملفات المشفرة وأنظمة قواعد البيانات الخاصة بالشركة وعند فتح ملف في كمبيوتر الشركة ظهرت مذكرة فدية تعلم الشركة بأن ملفاتها قد تم تشفيرها ولا يمكن إعادتها وفك تشفيرها إلا بدفع فدية والتي هي ثلاث عملات بتكوين[٣]، وعندما دفعت الشركة مبلغ الفدية والذي يقدر آنذاك ب ٣٥٠٠٠ الف دولار عادت معظم الملفات لوضعها بعد فك تشفيرها، ورفضت شركة التأمين تغطية الخسارة كونها استثنت عمليات التهديد والابتزاز من التغطية وادعت بأن هجوم الفدية لم يلحق بخسارة مادية مباشرة للشركة وانما نصت الوثيقة على ان شركة التأمين ستغطي الخسارة المادية المباشرة التي لحقت بالمعدات الالكترونية التي تمتلكها الشركة التجارية المؤمن لها أو التي تم تأجيرها أو التي تكون تحت سيطرتها. ومن ثم قررت المحكمة أن

(١) شذى عبد جمعة موسى، مصدر سابق، ص ١٦٩ وما بعدها.

(٢) قضية (EMOI Servs LLC ضد Owners Ins.Co Slip Opinion) سابقة الذكر.

(٣) وهي عملة رقمية افتراضية ليس لها كيان مادي ملموس أو وجود فيزيائي تم انتاجها بواسطة برامج حاسوبية ولا تخضه لسيطرة البنك المركزي أو لسيطرة جهة رسمية اخرى في العديد من الدول ويتم بيعها وشرائها عبر الانترنت وتمثل نسبة ٥٠ بالمائة من سوق العملة الرقمية المشفرة، وظهرت بقيمة 0.0001 دولار عند طرحها أول مرة ووصلت إلى 17608دولار، ومعروض البيتكوين محدود حول العلم حيث بلغ سقف اصداره 21 مليون وحدة حول العالم فقط مجزئة إلى 100 مليون ساتوشي اي جزء، ويخفض اصدارها كل اربع سنوات حفاظاً على عنصر الندرة ومن المقرر ان يتوقف اصدارها في العام 2140. للمزيد انظر:
عبد الجبار بن علي، النقود المشفرة "بتكوين ومشتقاتها "بحث في حقيقتها وتخريج احكامها الفقهية"، مجلة الشهاب /جامعة الشهيد حمه خضر الوادي، المجلد (٥)، العدد (٢)، ٢٠١٩، ص٢٨٤.

هجوم الفدية قد عرض البيانات للخطر إلا أنه لم يتسبب بضرراً مادياً مباشراً للوسائط المشمولة بالتغطية بحيث يستوجب شمولها بالتغطية التأمينية كون البرنامج عنصر غير ملموس ولا يمكن أن يتعرض لخسارة مادية مباشرة.

٢- المتتبع للأحكام القضائية في الولايات المتحدة الأمريكية يجد ان محكمة الاستئناف الأمريكية في ميسيسيبي/ الدائرة الخامسة قد وضعت مبدأ عام يحدد شروط تعويض المؤمن له عن الخطر السيبراني المتحقق وذلك في قضية شركة (MSH) المصنعة لمعدن السيليكون ضد شركة (AXIS) للتأمين، والصادر في ٢٠٢٠/٢/٢١ (والتي سبق ان تطرقنا اليها الفصل السابق)، طلبت الشركة الأولى تفسير بنود عقد التأمين من المخاطر السيبرانية والذي أبرمته مع الشركة الثانية، بالإضافة لطلب الحصول على مبلغ التأمين منها بسبب تحقق الخطر المؤمن منه بموجب بند الإحتيال، فقد قررت المحكمة أن أحقية المؤمن له في التعويض حال تحقق الخطر المؤمن منه مرهون بشروط معينة، فتكون شركة التأمين من المخاطر السيبرانية ملزمة بدفع التعويض الذي يقابل الخسارة اللاحقة بممتلكات الشركة التجارية المؤمن لها شرط ان يكون الضرر اللاحق بتلك الممتلكات و الناجم عن تحقق الخطر السيبراني ضرراً مباشراً على ان يكون المؤمن له حسن النية ومعيار حسن النية وفقاً للقرار القضائي اعلاه يتمثل بوقوع الخطر السيبراني المؤمن منه دون علم الشركة التجارية المؤمن لها أو من غير موافقتها. لأن شركات التأمين غالباً ما تحاول التخلص من التزاماتها من خلال قطع العلاقة السببية بين الخطر السيبراني المتحقق وبين الضرر الناشئ عنه حيث ادعت شركة التأمين في القضية اعلاه ان علاقة السببية قد انقطعت بسبب عدم وجود ضرر مادي مباشر في نظام الكمبيوتر، وبالتالي لا يمكن للشركة المؤمن لها الاستفادة من التغطية التأمينية كون الخطر السيبراني قد تحقق نتيجة اتخاذ اجراء ايجابي من قبلها مع امكانية الاستفادة من مبلغ التغطية وفق بند الهندسة الإجتماعية[١].

نستنتج من القرارين شروط التعويض عن الخطر السيبراني وهي:

١- وجود علاقة سببية بين الخطر السيبراني والخسارة اللاحقة بالشركة التجارية

(1) United States Court of Appeals Fifth Circuit, (Mississippi Silicon Holdings, L.L.C. vs. Axis Insurance Company) No. 20-60215/ FILED February 4, 2021 Lyle W. Cayce Clerk https://www.hinshawlaw.com/assets/htmldocuments/Alerts/5th%20Circuit%20MSH.pdf date of visit 13/2/2023 5:00pm.

٢- أن يكون الضرر الناتج عن الخطر السيبراني هو ضرراً مباشراً ويعني ان يكون الخطر السيبراني قد تسبب مباشرة بالضرر الحاصل للشركة المؤمن لها.

٣- أن تكون الشركة التجارية المؤمن لها (حسنة النية) أي أن الخطر السيبراني تحقق دون أي تدخل من موظفي الشركة العمدي وإلا سقط حقة بالمطالبة بمبلغ التأمين.

٤- أن يكون الضرر مادي فلا يمكن التأمين ضد الضرر المعنوي (كالقلق النفسي المصاحب لعملية الإحتيال).

وبإعتقادنا أنه كان الأولى بالمحكمة أن تقرر التعويض عن الكسب الفائت وليس فقط الخسارة اللاحقة، فأحد أهم نتائج الخطر السيبراني هو الضرر المعنوي الكبير الذي يخلفه بالشركة التجارية بسبب فقدان سمعتها التجارية وفقدان ثقة العملاء، الأمر الذي يؤدي إلى خسائر فادحة بالشركة بسبب توقف العملاء الحاليين لتعاملهم معها، وتجنب التعامل معها من القبل العملاء المستقبليين وهذا الضرر أكبر بكثير من الخسارة المادية الفعلية اللاحقة بالمؤمن له.

ويرى البعض في هذا الصدد بان التفسير الدقيق لإحتساب الأضرار المطلوب التعويض عنها من مبلغ التأمين يتطلب قدر كبير من الشروط والبنود المفصلة في وثيقة التأمين من المخاطر السيبرانية ومع ذلك لا تزال الإشكالية في الواقع العملي بخصوص ان بعض الأضرار السيبرانية لا يمكن اثباتها بموضوعية، كما هو الحال في انتهاك البيانات السرية للشركة التجارية مثلاً، حيث يجب ان تكون هنالك خسارة لاحقة من الممكن اثباتها بصورة مادية ملموسة مع وجود رابطة سببية مباشرة بين الضرر الواقع على الشركة وبين انتهاك الخصوصية والسرية، وبما ان الضرر الناشئ عن المخاطر السيبرانية هو غالباً خطر غير ملموس أو (معنوي) فلا يمكن تحديد كمية الضرر الحاصل للشركة التجارية نتيجة تحقق الخطر السيبراني المؤمن ضده بصورة جيدة، كما ان تحقق الخطر السيبراني وتراكم الأضرار يثير مشاكل في اثباتها ايضاً حيث ان اثبات قيمة الضرر الناجم عن انتهاك الخصوصية مثلاً بصورة مادية قد يكون في غاية الصعوبة[١].

وقد يثور التساؤل عن سبب لجوء الشركات التجارية إلى التأمين من المخاطر السيبرانية و الإلتزام بدفع اقساط مرهقة نسبياً مقارنة بالقسط المدفوع لشركات التأمين التقليدية خصوصاً وان بعض الأضرار الناجمة عن المخاطر السيبرانية بالإمكان تغطيتها بموجب الوثائق التقليدية؟ والإجابة على ذلك تكمن في ان وثيقة التأمين تغطي الأضرار التي تصيب الممتلكات التجارية كالخسائر التشغيلية

(١) صدام فيصل كوكز، مصدر سابق، ص١٣٨.

الناجمة عن خلل بأجهزة الحاسوب على إعتبارها من الممتلكات المادية للشركة، ولكن هذه الوثائق التقليدية تنحصر فيها التغطية للأضرار اللاحقة بالممتلكات المادية فقط دون تغطية الأضرار الناتجة عن خلل غير مادي في هذه الممتلكات لذا يكون التعويض محصوراً بإصلاح هذه الممتلكات المادية دون التعويض عن الأضرار غير المادية التي لحقت بتلك الممتلكات كإتلاف البيانات أو فقدها(١).

والسبب الأخر هو ان وثائق التأمين التقليدية تعوض الشركة التجارية عن الضرر المباشر فقط والذي يتمثل في الغالب بتعويض محدود مقارنة بالخسائر غير المباشرة الناتجة عن انخفاض نشاط الشركة بسبب الخطر السيبراني، ناهيك عن الغرامات الادارية المفروضة على الشركة التجارية نتيجة افتقارها لأمن نظام المعلومات عند معالجة البيانات، بالإضافة إلى عدم امكانية تغطية الضرر الناجم عن اخلال الشركة التجارية بعلاقتها التعاقدية مع الغير(٢). مما جعل الشركات التجارية تلجأ لإبرام عقد التأمين من المخاطر السيبرانية نظراً لكونه يقرر تعويضات أكبر من تلك المقررة في عقود التأمين التقليدية.

فنجد ان بعض المحاكم استثنت الخسائر السيبرانية من شمولها بتغطية وثائق التأمين من المسؤولية المدنية، فهذه الوثائق التقليدية تغطي فقط الخسارة الحاصلة في الممتلكات المادية للشركة التجارية، ولا يمكن ان تغطي بصورة مباشرة الضرر الحاصل بالمعلومات أو البيانات أو البرامج تكون على شكل غير ملموس، مثال على ذلك قرار محكمة الاستئناف الامريكية/ الدائرة الثامنة في قضية *Eyeblaster* ضد *Federal Ins.* فقد رفع احد عملاء الشركة المؤمن لها (*Eyeblaster*) دعوى يطالب فيها بالتعويض عن الضرر اللاحق بجهاز الحاسوب الخاص به والذي زعم أن جهاز الكمبيوتر الخاص به أصبح غير صالح للعمل بعد أن قام بزيارة موقع المؤمن له الإلكتروني حيث تضرر الجهاز بعد ان فتح المدعي اعلانات منبثقة موجودة على الموقع الإلكتروني للشركة المؤمن لها مما تسبب في حدوث اعطال تقنية في الجهاز الذي كان يحتوي على بيانات تتعلق بالضرائب تقدر بآلاف، قررت المحكمة عدم امكانية التعويض عن الضرر الحاصل في جهاز الحاسوب كونه ضرر غير مادي وخارج نطاق التغطية السيبرانية للمؤمن له كون بند وثيقة التأمين يغطي المسؤولية

(1) Pierre-Grégoire Marly, L'assurance du risque cyber, Colloque de l'Université du Mans du 5 décembre 2018 sur les nouvelles technologies et les mutations des assurances، Dalloz IP/IT 2019 p.603.

(2) Gaspard Ferey, Nicolas Grorod, Simon Leguil, op.cit, P33.

عن "الضرر المادي للممتلكات المادية"، وخلصت المحكمة إلى ان البيانات والمعلومات هي ممتلكات غير مادية وغير ملموسة فقررت عدم شمولها بالتغطية [١].

نستنتج مما سبق إن ما يميز التأمين من المخاطر السيبرانية عن التأمين التقليدي هو ان الأخير لا يغطي سوى الخسارة المادية للممتلكات و الناجمة عن مخاطر محددة كالحريق أو الزلال مثلاً، ولا يغطي قيمة الممتلكات غير المادية كالبيانات السرية أو البرامج مثلاً[٢]، فالتأمين على الممتلكات الإلكترونية عند تأمين الملكية التجارية التقليدية لن يغطي سوى الخسارة التي حدثت بسبب تخريب أو تحطيم في الأجهزة الإلكترونية والتي هي شرط لإستحقاق التعويض النقدي ولا يغطي الضرر غير المادي الحاصل للممتلكات كفقدان البيانات وقرصنة العملات الرقمية. ويجب تبني مفهوم واسع للأضرار المادية فالضرر المادي لا يقتصر على التدمير المادي أو الضرر الذي يصيب برامج الحاسوب وانما يمكن ان يشمل فقدان الوصول لتلك البرامج و خسارة الاستخدام وعدم التمكن من اداء الوظائف[٣].

كما يتميز التأمين من المخاطر السيبرانية عن التأمين التقليدي بالاضافة لقدرته على تغطية الأضرار المادية الحاصلة في الممتلكات الالكترونية المؤمن عليها بقدرته على تغطية الأضرار غير المادية والناتجة عن اخطار غير مادية فيمكن تغطية الخسائر التشغيلية الناجمة عن الأضرار التي لحقت بنظام الحاسوب للشركة التجارية المؤمن لها والتي تسبب بإبطاء عمل تلك الأنظمة أو تدهورها أو منع الوصول للبيانات في أجهزة الحاسوب التابعة للشركة[٤].

وتجدر الاشارة إلى ان التعويض عن الخسائر التشغيلية وانقطاع الاعمال بصفتها اضراراً غير مادية بدأ بالظهور بشكل خجول في عقود التأمين في الوقت الحالي اما الأضرار المستقبلية المتكبدة

(1) United States Court of Appeals, Eighth Circuit (EYEBLASTER, INC.، Plaintiff-Appellant, v. FEDERAL INSURANCE COMPANY) Date published: Jul 23, 2010.
https://casetext.com/case/eyeblaster-inc-v-federal-ins-co
date of visit 23/3/2023 7:30 pm.

(٢) البيانات السرية ليست بالضرورة ان تكون بيانات شخصية وانما تشمل كل البيانات المحفوظة في نظام الكمبيوتر الخاص بالمؤمن له والذي يلتزم بالمحافظة عليها وفقاً لإلتزام قانوني أو تعاقدي. للمزيد انظر:
Tsohou A, Diamantopoulou V, Gritzalis S, Lambrinoudakis C, op.cit, p741.

(٣) صدام فيصل كوكز، مصدر سابق، ص١٤٩.

(4) Pierre-Grégoire Marly, op.cit, p 2.

بسبب فقدان سرية البيانات بسبب خلل بنظام الحاسوب في الشركة التجارية فهي غير مشمولة بالتغطية التأمينية في الوقت الحاضر(١).

ويثور التساؤل عن مدى امكانية رفض شركة التأمين من المخاطر السيبرانية عن تعويض الشركات التجارية المؤمن لها على الرغم من تحقق الخطر السيبراني المؤمن منه في وثيقة التأمين؟ في اعتقادنا – من خلال استقراء عدد من القرارات القضائية بهذا الصدد – نجد انه لا يمكن ان يترتب أي اثر قانوني على مجرد وقوع الخطر السيبراني المؤمن منه في بعض الأحيان، فلا يعتبر فيها مجرد تحقق الخطر شرطاً لإستحقاق الشركة التجارية للتعويض، ففي احدى اكبر النزاعات القضائية المتعلقة بإستحقاق التعويض بموجب عقد التأمين من المخاطر السيبرانية عن انتهاك البيانات، قررت المحكمة العليا في الولايات المتحدة الأمريكية/ ولاية كونيتيكت في قضية (Fed Inc.) ضد (Mgmt) لعام ٢٠١٥، ان شركة التأمين الفيدرالية غير ملزمة قانونياً بتغطية الضرر الناتج عن ضياع اشرطة الكمبيوتر الخاص بالشركة التجارية المدعية حتى وان احتوت على بيانات سرية اذا ما تم العثور عليها من قبل شخص ما عند عدم وجود دليل قانوني حول تمكن الشخص من الاطلاع على تلك البيانات السرية حيث ان شرط "النشر" قد تخلف في الواقعة المعروضة امام القضاء لذا لا تكون شركة التأمين من المخاطر السيبرانية ملزمة بأي تعويض تجاه الشركة التجارية المؤمن لها(٢).

وبالمقابل نجد ان قضية (portal Health care) ضد (LLC) لعام ٢٠١٦ والتي تتعلق بالنزاع حول تعويض المتضررين من قبل حامل وثيقة التأمين، حيث تمت اقامة دعوى جماعية متعلقة بالأمن السيبراني حيث زعم المدعين ان الشركة التجارية حاملة الوثيقة فشلت في تأمين خادمها مما جعل السجلات الطبية متاحة للمستخدمين غير المصرح لهم عبر الانترنت حيث قررت المحكمة الابتدائية ان جعل السجلات الطبية السرية متاحة للغير يشكل نشراً لتلك البيانات وبالتالي على شركة التأمين الالزام بدفع التغطية(٣).

---

(١) نعني بنظام الحاسوب جميع الادوات والعمليات التي تسمح للشركة بتخزين البيانات غير المادية أو تبادلها أو معالجتها. للمزيد من التفاصيل انظر:

Gaspard Ferey, Nicolas Grorod, Simon Leguil, op.cit, p17, 25.

(2) Mgmt Inc. v. Fed. Ins. Co, 115 A.3d 458، 317 Conn. 46 (Conn. 2015). https://casetext.com/case/recall-total-info-mgmt-inc-v-fed-ins-co-1
date of visit 23/3/2023 9:30 pm

(3) Mc Dermott Will and Emery, Courts Approach To Cyber Insurance Continues to Evolve, the national law review, Volume (XIII)، Number (331), 2023, p45.

مع الاخذ بنظر الاعتبار ان سياسات التغطية من المخاطر السيبرانية تستبعد تغطية الضرر الحاصل نتيجة فشل المؤمن له في منع وقوع الخطر الحاصل لشركته التجارية كعدم اتخاذه لتدابير احتياطية تسمح بإستعادة البيانات عند فقدانها كإجراء نسخ احتياط للبيانات، أو عند استخدامه لبرامج غير محمية قانوناً أو فشل الشركة في تأمين الحواسيب الخاصة بها(١).

ويتصور عدم إمكانية حصول الشركة التجارية على التعويض بالرغم من وقوع الخطر السيبراني المؤمن منه في حال تم النص في وثيقة التأمين على ذلك. فبعض عقود التأمين من المخاطر السيبرانية تشترط لإستحقاق المؤمن له التعويض عن نشر بياناته التي تم التأمين عليها " ان وثيقة التأمين تؤمن من نشر بيانات حامل الوثيقة حصراً وليس بيانات الغير "، فعلى الرغم من حدوث خرق للسرية وتحقق الخطر السيبراني ونشر المعلومات الواردة في المواقع الإلكترونية الخاصة بالشركة التجارية إلا ان شركة التأمين تكون غير ملزمة بدفع مبلغ التغطية نظراً لكون المعلومات التي تم نشرها هي معلومات العملاء و ليست معلومات الشركة التجارية(٢).

الفرع الثاني

إلتزامات أطراف العقد تجاه الغير بعد تحقق الخطر السيبراني

ان تحقق الخطر السيبراني المؤمن منه يتسبب بخسائر مالية كبيرة للشركات التجارية وعملائها وموردیها فقد يستغرق الأمر أعوام عديدة لبناء سمعة تجارية ودقائق قليلة من الخطر السيبراني لتدميرها(٣) وتقدر هذه الخسائر بملايين الدولارات سنوياً بسبب سرقة بياناتهم المخزنة الكترونياً أو عدم قدرة الأنظمة على العمل وغيرها. مما يؤدي لفقدان الاستقرار المالي نتيجة لتدهور قيمة الأسهم وانعدام الثقة لدى العملاء نتيجة لحدوث اضطرابات كبيرة في النظام المالي والاقتصادي للشركة، مما يهدد استمرار وتنافسية قطاع التجارة، فالمخاطر السيبرانية عادةً ما تكون كارثية ومدمرة لجميع الأطراف على الرغم من اختلاف آلية تنفيذ تلك المخاطر و الوسط الذي تحققت فيه والاستراتيجية المتتبعة في تدارك تلك المخاطر(٤).

(1) Pierre-Grégoire Marly،op.cit, p 2.
(2) Mc Dermott Will and Emery, op. cit, p45.
(3) Ganbayar Uuganbayar،op.cit, p1.
(٤) دراعو عز الدين، الاثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي، مجلة التكامل الاقتصادي، جامعة محمد بن احمد وهران، المجلد (١٠) العدد (٢)، ٢٠٢٢، ص ١١٩.

وتعتمد شركة التأمين على مجموعة متنوعة من خيارات التغطية المتعلقة بالمخاطر السيبرانية المؤمن منها، أهمها تغطية الأضرار الناشئة عن الخطر السيبراني الذي أصاب الغير، أو ما تسمى ب (مطالبات الطرف الثالث) في العديد من عقود شركات التأمين من المخاطر السيبرانية، وتنشئ عن الضرر الذي يلحق بالشركات أوالاشخاص الآخرين الذين اصابهم ضرر من الخطر السيبراني حيث تتضمن تغطية الغير الحماية من الخسائر أو الأضرار التي تقع على هذا الطرف وعادة ما يتضمن التقاضي وتكاليف الاخطار وادارة الازمات وقد تتجاوز قيمة اصول الغير قيمة الطرف الأول (المؤمن له) مما يؤدي إلى نتيجة مفادها ان الضرر الحاصل للغير قد يفوق الأضرار الحاصلة للطرف الأول كما هو الحال في الشركات الصغيرة والمتوسطة والتي تمتلك اصول محدودة نسبياً و لكنها في ذات الوقت تسبب ضرر كبير للغير عند وقوعها ضحية لإحدى المخاطر السيبرانية[1].

وفي اعتقادنا حتى وان لم يكن هناك دليل على ان الخطر السيبراني قد تحقق نتيجة فعل ضار لم تكن لارادة الشركة سبب في تحققه الا ان العملاء سيفقدون الثقة بالشركة وسيبحثون عن حلول بديلة لتعويض خسائرهم وقد يباشرون بالإجراءات القانونية التي تستمر لعدة اشهر للحصول على تعويض عن الأضرار التي لحقت بهم نتيجة فقدان السرية وانقطاع الخدمة وتكاليف التشغيل الإضافية، فحجم الخسائر اللاحقة بالغير يكون كبيراً في اطار التأمين من المخاطر السبيبرانية نتيجة تعدد المضرورين بالاضافة إلى ارتفاع مبلغ التعويضات والتكاليف القانونية المتكبدة، مقارنة بباقي انواع التأمينات.

ويمكن إجمال الإلتزامات المترتبة على أطراف عقد التأمين من المخاطر السيبرانية تجاه الغير بما يلي:

١. **إخطار الشركة المؤمن لها للغير عند تحقق الخطر السيبراني:** فإذا ادى تحقق الخطر السيبراني إلى الحاق الضرر بسرية البيانات المتعلقة بأطراف أخرى خارج نطاق عقد التأمين من المخاطر السيبرانية (الغير) سيتعين على الشركة التجارية |– المؤمن له – ابلاغ الأطراف المعنية بوقوع ضرر على بياناتهم الشخصية الموجودة لديها، والغاية من هذا الإلتزام هي لكي يتم تحديد الاشخاص

(1) Florian Schütz, Florian Rampold, Andre Kalisch, Kristin Masuch, Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis, Procedia Computer Science, Volume(219), 2023, p523.

المتضررين من وقوع الخطر المؤمن منه، وهي عملية مكلفة في هذا النوع من التأمين بسبب تضرر عدد كبير من الاشخاص الذي قد يصعب احصائه أو يصعب تعويضهم عن فقدانهم لتلك البيانات كون الأضرار الواقعه عليها من الصعوبة بمكان ان يتم تقديرها بالمال في حال تعذر استعادتها بالرغم من تحمل شركة التأمن لتكاليف هذا الإخطار(١).

ويقع على عاتق الشركة التجارية المؤمن لها ضد المخاطر السيبرانية عبء اثبات تحقق الخطر المؤمن منه على الرغم من ان هذا الاثبات قد يكون صعباً(٢). وفي إعتقادنا ان عملية اثبات وقوع المخاطر السيبرانية والتي تعتبر مخاطر غير مادية (غير ملموسة) تقع في فضاء سيبراني غير مادي وقد تتسبب بأضرار يصعب اثباتها بسبب طبيعتها الخاصة سوف تشكل عبئاً ثقيلاً على الشركات التجارية المؤمن لها وعلى وجه الخصوص الشركات التجارية الصغيرة والمتوسطة.

٢. **تحمل شركة التأمين من المخاطر السيبرانية لتكاليف إخطار (الغير):** حيث تلتزم شركة التأمين بتحمل تكاليف إخطار ضحايا المخاطر السيبرانية في حالة حدوث خرق لأمن البيانات و انظمة المعلومات للشركات التي تقوم بمعالجة البيانات، وتكاليف الإخطار التي تتكبدها شركات التأمين يمكن أن تكون ضخمة كونها تشمل التكاليف المتعلقة بتعيين خبراء خارجيين مختصين بالأمن السيبراني لإخطار المتضررين عبر البريد الالكتروني كما يمكن أن تشمل تكاليف إستعادة بيانات و رسائل البريد الالكتروني الخاصة بالعملاء(٣).

٣. **تعويض شركة التأمين من المخاطر السيبرانية الخسائر اللاحقة بالغير:** حيث تكون شركة التأمين من المخاطر السيبرانية ملزمة بتعويض الخسارة اللاحقة بالغير نتيجة تحقق الخطر السيبراني الذي أصاب المؤمن له مثل نقل الفيروسات للغير، مما تسبب بعدم قدرتهم على الوصول إلى نظام المؤمن له بسبب رفض الخدمة، فيترتب على تحق الخطر السيبراني تعويض الغير عن الأضرار المادية التي تسبب بها كتلف أجهزة الحاسب الآلي نتيجة الإصابة بالفيروس، بالإضافة للأضرار غير المادية (غير الملموسة) اللاحقة كتعويض الغير عن فقدان بياناته الإلكترونية الموجودة في الحاسب الآلي المصاب بالفيروس(٤). مثال على ذلك: اذا ما تم اختراق أنظمة التشغيل في ميناء بحري ما واستطاع المهاجم الوصول إلى جزء من نظام المعلومات في الميناء والتحكم في الرافعة

(1) Gaspard Ferey, Nicolas Grorod, Simon Leguil, op.cit, p23.

(٢) عبد الرزاق السنهوري، مصدر سابق، ص١٣٤٣.

(3) Pierre-Grégoire Marly, op.cit, p 4.

(4) Gaspard Ferey, Nicolas Grorod, Simon Leguil, op.cit, p40.

المؤتمته جزئياً اثناء رفع حاويات احد العملاء مما ادى إلى سقوطها على السفينة التي كانت تقل الحاوية وإصابة اثنين من افراد الطاقم اصابات جسدية وتدمير محرك لطائرة مشحونة في هذه الحاوية، مما دفع بالناقلين الأخرين إلى تحويل مسار سفنهم عن المسار القصير المعتاد والذي يؤدي إلى تأخيرها عن موعد تسليم البضاعة لعملائهم، فيمكن للغير المتمثل بكل شخص بإستثناء المؤمن والمؤمن له (الميناء البحري) في عقد التأمين من المخاطر السيبرانية ان يرفع عدة دعاوى قضائية على الميناء (المؤمن له) كالمطالبة بتعويض الأضرار التي لحقت بموظفي الشاحن المصابين واصلاح سفينته، بالإضافة إلى مطالبه الشاحن بالتعويض عن الخسائر التشغيلية الناتجة عن الخطر السيبراني ودعوى تعويض صاحب الطائرة المحمولة الموجودة داخل الحاوية بسبب حدوث عطل في محركها نتيجة تأثرها بالسقوط من الرافعة، فضلاً عن مطالبة اصحاب الحاويات الأخرى للميناء بتعويضهم عن التكاليف التشغيلية الإضافية المتكبدة نتيجة لتجميد بضائعهم أو تحويل مسارها أو انخفاض الاقبال على التعاقد معهم بسبب الخلل التقني في الرافعة التابعة للميناء مع تحميل الأخير لمصاريف الدعاوى ولجميع التكاليف القانونية المتكبدة لإصلاح الرافعة والمصاريف اللازمة لإدارة الازمة من قبل خبراء الكمبيوتر[1].

وقد يتم التساؤل عن مدى التزام شركة التأمين من المخاطر السيبرانية بالتعويض عن الأضرار التي تلحق بالأطراف المتعاقدة مع الشركة التجارية المؤمن لها والتي لحقها ضرر بسبب وقوع الخطر السيبراني، فهل تشمل التغطية تعويض الأطراف المتعاقدة مع المؤمن له نتيجة تأثر تلك الاطراف بالخطر السيبراني الذي لحق بالمؤمن له كنتيجة حتمية لتحقق الخطر، ام ان شركات التأمين غير مسؤولة قانوناً عن تعويض تلك الاطراف؟

ان الاجابة على هذا التساؤل نجده في اتجاه القضاء بصورة عامة إلى استبعاد مسؤولية شركات التأمين عن تعويض الأضرار الناتجة عن الخطر السيبراني المؤمن منه والذي اصاب الاطراف التي ترتبط مع الشركة المؤمن لها بعلاقة تعاقدية، فلا تلتزم شركات التأمين من المخاطر السيبرانية بالتعويض عن المسؤولية الناشئة عن الإخلال بالالتزامات التعاقدية بين المؤمن له والغير، ففي قرار لمحكمة الاستئناف الامريكية/ الدائرة الثامنة في قضية (*PF*

(1) Gaspard Ferey, Nicolas Grorod, Simon Leguil, op.cit, p18, p31.

Chang's China Bistro)، ضد(.Federal Insurance co) لسنة ٢٠١٦[1] اشترت سلسلة المطاعم (*PF Chang's China*) وثيقة تأمين من المخاطر السيبرانية من شركة التأمين الفيدرالية (*Federal Insurance Co.*) حيث تغطي الوثيقة "الخسارة المباشرة تحقق والخسارة اللاحقة الناتجة عن انتهاكات الأمن السيبراني والمسؤولية المدنية". كان لدى (PF Chang's) عقد مع مقدم خدمة تابع لجهة خارجية لمعالجة معاملات بطاقات الائتمان الخاصة بها، والتي تعاقدت بدورها مع شركة (MasterCard). تعرضت(PF Chang's) لخطر سيبراني نتج عنه خرق للبيانات في العام ٢٠١٤ عندما حصل قراصنة الكمبيوتر ونشروا على الإنترنت تقريبًا ٦٠٠٠٠ رقم بطاقة ائتمان تخص عملاء المؤمن له نتيجة لذلك، تكبدت MasterCard رسوماً وغرامات وأرسلتها إلى مقدم الخدمة وفقًا للعقد المبرم بينهما، والذي قام بنفي مسؤوليته وتحميلها للمؤمن له وفقًا للاتفاقية المبرمة بين PF Chang's وبين شركة التأمين، ونتيجة لذلك طلبت سلسلة المطاعم الحصول على تعويض من شركة التأمين ومع ذلك، رأت المحكمة أن المؤمن عندما رفض التغطية كان موقفه صحيح من الناحية القانونية على أساس استثناء الوثيقة "للالتزامات التعاقدية التي تقع على عاتق المؤمن له مع الغير على الرغم من ان المؤمن له كان لديه وقت التعاقد مع المؤمن "توقع معقول" بأن شركة التأمين الخاصة به ستغطي الأضرار الناجمة عن خرق البيانات مع الرسوم الناتجة المستحقة للغير، لكن لم تجد المحكمة أي شيء في وثيقة التأمين يشير إلى أن PF Chang's اتفقت مع المؤمن على ضمان تغطية هذه الرسوم.

وفي اعتقادنا ان قرار المحكمة كان صائباً حين استثنى الإلتزامات التعاقدية بين المؤمن له والغير من الشمول بالتغطية، ولم تكترت المحكمة في قرارها إلى نية المؤمن له، كون النوايا كامنة في النفس ومن الصعوبة إثباتها من جانب، ومن الجانب الأخر فإن الإلتزام بحرفية بعض بنود عقد التأمين من المخاطر السيبرانية يؤدي إلى استقرار المعاملات ويجنب النزاعات.

لذا فإن الغير الذي هو في علاقة تعاقدية مع المؤمن له ان يرفع دعوى قضائية ضده للمطالبة بالتعويض عن الضرر الناتج من وقوع الخطر السيبراني نتيجة اخلال المؤمن له

(1) P.F. Chang's China Bistro Inc. v. Fed. Ins. Co.، No. CV-15-01322-PHX-SMM (D. Ariz. May. 26, 2016)
https://casetext.com/case/pf-changs-china-bistro-inc-v-fed-ins-co
date of visit 6/5/2024 3:00am.

بإلتزاماته العقدية وفقاً لقواعد القانون المدني ففي حالة وجود علاقة تعاقدية بين منصة الانترنت التابعة للشركة التجارية المؤمن لها و بين العملاء، فإن العميل الذي تعرض لخطر سيبراني نتيجة استخدامه للمنصة بإمكانه مطالبة المؤمن له بالتعويض عن اخلالها بواجب تقديم مستوى الامان السيبراني الموعود به مما ادى إلى حدوث ضرر فعلي مادي أو حتى معنوي كالضرر الذي يصيب سمعة العميل التجارية. ويمكن استبعاد المسؤولية عن المؤمن له اذا ما اثبت عدم ارتكابه اي خطأ ادى لوقوع الخطر أو ان العقد تضمن شرط الاخلاء من المسؤولية أو في حالة ان الخطر قد تحقق بسبب العميل كعدم محافظته على كلمة المرور الخاصة ببريده الالكتروني أو في حالة السبب الاجنبي كالقوة القاهرة أو الحادث المفاجئ أو خطأ المضرور كوجود فيروسات في جهاز العميل أو بسبب فعل أو خطأ الغير كالابتزاز الالكتروني أو قضايا الفدية[١] وفي حال تم الأضرار بشخص ما نتيجة وقوع الخطر السيبراني ولم يكن يرتبط مع المؤمن له بعلاقه تعاقدية هنا تكون مسؤولية الشركة التجارية المؤمن لها هي تقصيرية وفقاً للقواعد العامة في القانون المدني.

بالإضافة إلى أن وثائق التأمين من المخاطر السيبرانية لا تغطي بشكل كاف جميع المخاطر السيبرانية وانما تحتوي على تغطيات اساسية مثل تغطية المصاريف المتكبدة نتيجة اختراق البيانات حيث تغطي تكاليف الاستجابة القياسية للخطر السيبراني والاستعانة بمحامين فضلاً عن اخطار العملاء بإختراق بياناتهم، كما تغطي عقود التأمين تكاليف الدفاع وتسوية الدعاوى الجماعية والدعاوى المقامة من قبل الغير والدعاوى التنظيمية كالغرامات المدنية والتسويات وتغطية الارباح المفقودة الناتجة عن اغلاق الشبكة[٢].

وبدخول اللائحة العامة للبيانات (GDPR) حيز التنفيذ في مايو ٢٠١٨ تم فرض التزامات جديدة على الشركات المسؤولة عن معالجة البيانات ففي حال سرقة تلك البيانات التابعة لشخص ثالث أو تلفها في حال حدوث انتهاك في مجال الامن السيبراني وتحقق الخطر المؤمن منه ستقع على الشركة غرامات مالية بموجب هذه اللائحة وفي الجانب الآخر فأنه لا يمكن للشركة التجارية ان تؤمن من خطر تلك العقوبات المالية لدى شركات التأمين

(١) محمد سعيد اسماعيل، مصدر سابق، ص ٢١٥.

(2) Florian Schütz, Florian Rampold, Andre Kalisch, Kristin Masuchop. Cit, p52.

السيبراني حيث انه من غير الممكن ان تشمل شركة التأمين تلك الغرامات المالية بالتغطية السيبرانية[١].

وبينت المادة (٨٣) من اللائحة الشروط العامة لفرض الغرامات الادارية على منتهكي احكام اللائحة حيث تقرر فرض غرامات ادارية من قبل السلطات الاشرافية في الدول المشمولة بأحكامها على المخالفين حيث قررت الفقرة الثانية من تلك المادة تباين فرض هذه الغرامات تبعاً لكل حالة على حدا مع الأخذ بنظر الاعتبار عدة عوامل منها طبيعة الإنتهاك وخطورته وعدد الاشخاص المعنيين بالبيانات المتأثرة ومستوى الضرر الذي لحق بهم وهل ان الإنتهاك ناتج عن عمد ام اهمال المعنيين ومدى صحة الاجراءات المتخذة من قبل معالج البيانات أو وحدة التحكم للتخفيف من حدة الضرر الذي تعرض له الافراد ودرجة التدابير الفنية والتنظيمية المتخذة من قبل المخالفين ومدى وجود انتهاكات سابقة من عدمها ودرجة التعاون مع السلطات الاشرافية للتخفيف من حدة الضرر الناجم عن الخطر والتخفيف من اثاره المحتملة وهل تم الاخطار عن تحقق الخطر للسلطات المعنية ام لا والطريقة التي تم الاخطار بها ومدى التزامهم بمدونات السلوك المعتمدة[٢] وقد تصل الغرامة إلى عشرة مليون يورو عند مخالفة كل من يقوم بمعالجة البيانات بإلتزاماته بينما تقرر اللائحة فرض غرامة مالية تصل إلى عشرين مليون يورو أو في حالة وجود تعهد تصل الغرامة إلى نسبة ٤ بالمائة من اجمالي قيمة التداول السنوية في السنة المالية السابقة عند مخالفة الاطراف للمبادئ الاساسية لمعالجة البيانات الخاصة بالعملاء أو انتهاك حقوق اصحاب البيانات أو نقل البيانات الشخصية للعملاء إلى بلد اخر أو منظمة دولية أو اي التزام اخر تقرره قوانين الدول الاعضاء[٣].

---

(١) وفقاً للتقرير الصادر عن اللجنة القانونية العليا في مركز باريس المالي ٢٠٢٢ بعنوان (القابلية للتأمين من المخاطر السيبرانية):

RAPPORT SUR L'ASSURABILITÉ, DES RISQUES CYBER, du Haut Comité Juridique, du Haut Comité Juridique 2022, p5.

https://www.banque-france.fr/system/files/2023-10/rapport_45_f.pdf

date of visit 6/5/2024 7:00pm

(٢) المادة (٨٣ /ف٢) من اللائحة العامة لحماية البيانات GDPR لسنة ٢٠١٦.

(٣) المادة (٨٣ /ف/ك/ج١) من اللائحة العامة لحماية البيانات GDPR لسنة ٢٠١٦.

ونتسائل حول مدى امكانية تعويض الغير نتيجة الضرر المعنوي الذي اصابهم نتيجة وقوع الخطر السيبراني المؤمن منه، فهل يجوز التعويض عن الضرر المعنوي كالقلق والضيق الذي اصابهم دون ان يكون هناك ضرر مالي ام لا؟

للإجابة على هذا التساؤل ونظراً لانعدام التشريعات المتخصصة في مجال التأمين السيبراني، لذا يمكن القول باللجوء إلى الأحكام الواردة في اللائحة العامة لحماية البيانات (GDPR) حيث نصت المادة (٨٢) من اللائحة على امكانية تعويض اي شخص عن الضرر المالي وغير المالي نتيجة انتهاك الاحكام الواردة للائحة من قبل معالجي البيانات كالمؤمن والمؤمن له. اي ان اللائحة قررت أحقية تعويض الغير عن الضرر المعنوي الذي أصابه نتيجة تحقق الخطر السيبراني.

وقد كان للمحكمة العليا في انكلترا في قضية (**Rolfe & Ors v Veale**) لسنة٢٠٢١[(١)] دور واضح في تحديد ماهية الضرر المعنوي الذي بالإمكان التعويض عنه وشروطه، وفحواها ان المدعى عليه وهو شركة محاماة قد أرسل بريد إلكتروني يتضمن بيانات شخصية، إلى مستلم بشكل غير مقصود بسبب خطأ مطبعي. وتضمنت هذه البيانات عناوين العملاء (الغير) وبعض البيانات المالية الخاصة بهم، ولكنها لم تتضمن معلومات الحساب المصرفي للمدعين أو تفاصيل الاتصال بهم. وقد أبلغ المستلم المدعى عليه على الفور بذلك الخطأ. لذلك، طلب المدعى عليه من المستلم حذف البريد الإلكتروني وتم ذلك على الفور. رفع العملاء دعوى التعويض عن خرق البيانات، ودعوى للحصول على تعويضات عن الضرر المعنوي الذي أصابهم نتيجة لذلك الخطأ. وعبروا عن الضرر المعنوي بأنهم "فقدوا النوم وهم قلقون بشأن العواقب المحتملة لخرق البيانات وأنه جعلهم يشعرون بالمرض" و"الخوف من المجهول." ونظرت المحكمة العليا في طبيعة المعلومات التي تم الكشف عنها، والخطوات المتخذة لتصحيح خرق البيانات، والدليل على أي خسارة أو ضرر ناتج عن الخطر السيبراني ووجدت أن الادعاء "مبالغ فيه بوضوح" وغير قابل للتصديق. ولاحظت المحكمة أيضًا، ان هذا الانتهاك يعتبرتافه ولا يستحق التعويض عنه. وحكمت

(1) England and Wales High Court (Queen's Bench Division) Decisions, (Rolfe & Ors v Veale Wasbrough Vizards LLP), [2021] EWHC 2809 (QB) (07 September 2021) https://www.bailii.org/ew/cases/EWHC/QB/2021/2809.html
date of visit 6/5/2024 7:30pm

المحكمة لصالح المدعى عليه – شركة المحاماة– ومنحته ١١٠٠٠ جنيه إسترليني كتكاليف للدعوى كنوع من التعويض، وهو ما يزيد عن التكاليف التي تحكم بدفعها المحكمة من الطرف الخاسر في الدعوى، لتعكس طبيعة المبالغة والمضاربة في إدعاء المدعين وعدم وجود اثبات على وجود الضرر المعنوي وان الضرر المعنوي الحقيقي هو ذلك الضرر المؤثر على الصحة البدنية والعقلية.

ونستنتج من قرار المحكمة ان خرق البيانات اذا كان غير مقصود و تقني دون وجود نية متعمدة للخرق، وان البيانات التي تم الكشف عنها ليست بيانات من فئة خاصة على النحو المحدد في اللائحة العامة لحماية البيانات وقانون حماية البيانات لعام ٢٠١٨، أو انها ليست بيانات شخصية أو حساسة من المحتمل أن تُستخدم في الاحتيال، وان الخطوات التي اتخذها المؤمن له سريعة، وبالتالي يتم التخفيف من مخاطر إساءة الاستخدام؛ بالإضافة لعدم تقديم المدعي أدلة كافية لإثبات الضرر المعنوي والذي يجب ان يتجاوز مجرد القلق والخوف من المجهول، فلا مجال للتعويض عن الضرر المعنوي.

كما نستنتج مما سبق النهج الصارم للمحكمة في التعامل مع دعاوى التعويض الشائعة بشكل متزايد والمتعلقة بخرق البيانات التي تستند إلى مجرد الضيق والقلق دون وجود دليل لتأثير الخطر السيبراني على الصحة البدنية أو العقلية للمدعي. وهذا يخالف نص المادة (٨٢) من اللائحة العامة لحماية البيانات والذي اجاز لأي شخص ان يطالب بالتعويض عن جميع الأضرار المادية والمعنوية. وربما كان السبب في عدم تطبيق النص في اعتقادنا هو عدم وجود معيار يحدد ماهية الضرر المعنوي الواجب التعويض عنه مما جعل القضاء يستخدم صلاحيته وسلطته التقديرية لتقرير مدى احقية الغير المتضرر بالتعويض عن الضرر اللاحق بسبب تحقق الخطر السيبراني من عدمها.

وبالنظر لأهمية اللائحة العامة لحماية البيانات (GDPR) النافذة سنة ٢٠١٨ واعتبار بنودها السند القانوني للعديد من الأحكام القضائية الحديثة المتخصصة في مجال عقود التأمين من المخاطر السيبرانية، سيبدو من المهم التساؤل عن موقف القضاء من تعويض الغير عن الخطر السيبراني قبل تاريخ نفاذ اللائحة وهل أقر تعويض الغير عن تحقق الخطر السيبراني ام لا؟

نجد الإجابة عن التساؤل أعلاه في قضية (Warren) ضد شركة (DSG Retail Limited)[1]، (DSG) هي شركة تجارية تدير متاجر إلكترونية مثل Curry's PC World و Dixons Travel، وبين عامي ٢٠١٧ و٢٠١٨، تعرضت أنظمة (DSG) لخطر سيبراني وهو قيام مهاجمين متطورين قاموا بتثبيت برامج ضارة على ما يقرب من ٦٠٠٠ نقطة بيع في المتاجر، وتمكنوا من الوصول إلى البيانات الشخصية للعديد من العملاء التابعين للشركة، بما في ذلك الأسماء والعناوين وأرقام الهواتف وأعياد الميلاد وعناوين البريد الإلكتروني .ادعى دارين لي وارن، أحد عملاء (Curry's PC World)، الذي أن بياناته الشخصية تعرضت للاختراق أثناء الهجوم .وقد رفع دعوى على أساس فردي وليس جماعي ضد حكومة دبي الذكية مستنداً إلى: خرق مبدأ أمن البيانات في قانون حماية البيانات لعام ١٩٩٨(**DPA**) [٢] وإساءة استخدام البيانات، خرق الواجب القانوني والإهمال، والمطالبة بتعويضات قدرها ٥٠٠٠ جنيه إسترليني. تقدمت (DSG) بطلب إلى المحكمة للحصول على حكم مستعجل أو أمر بشطب كل من هذه المطالبات بصرف النظر عن المطالبة بانتهاك الواجب القانوني الناجم عن الانتهاك المزعوم للواجب القانوني بحماية البيانات.

وافقت المحكمة العليا في المملكة المتحدة على طلب المدعي، معتبرة أن هذه الدعاوى تتطلب نوعًا من الفعل الإيجابي من قبل الشركة التجارية المدعى عليها مثل الكشف عن المعلومات للغير . حتى تتمكن الشركة التجارية من الحصول على مبلغ التأمين وفقاً لعقد التأمين من المخاطر السيبرانية.

---

(1) Warren v. DSG Retail Limited [2021] EWHC 2168 QB.
https://www.jdsupra.com/legalnews/warren-v-dsg-retail-ltd-shifting-the-1199275/
date of visit 30/11/2024 7:00pm

(٢) سبق وان تم تشريعه من قبل برلمان المملكة المتحدة، وهو قانون يهدف إلى حماية البيانات الشخصية المخزنة على أجهزة الكمبيوتر أو في نظام حفظ الملفات الورقية المنظم .وقد سنت أحكامه من توجيه حماية البيانات للاتحاد الأوروبي (EU) لعام ١٩٩٥ بشأن حماية البيانات ومعالجتها وحركتها. وقد حل محله قانون حماية البيانات لعام ٢٠١٨ (DPA 2018) في ٢٣ مايو ٢٠١٨. ويكمل قانون حماية البيانات ٢٠١٨ اللائحة العامة لحماية البيانات في الاتحاد الأوروبي(GDPR) ، والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨. ينظم قانون حماية البيانات جمع وتخزين وحفظ البيانات. استخدام البيانات الشخصية بشكل أكثر صرامة.

https://www.dpalaw.co.uk/about

تاريخ الزيارة ٢٠٢٣/٨/٢ الساعة ١:٠٠ ص.

والحقيقة ان شركة (DSG) ضحية لهجوم إجرامي من طرف ثالث ولم تنشر المعلومات الشخصية للمدعي. وحاول المدعي الإدعاء بأن الشركة التجارية المدعى عليها قد فشلت في الحفاظ على أمان البيانات ومنع وقوع الهجوم كان بمثابة النشر لكن المحكمة العليا رفضت هذه الحجة واقرت بأن دعاوى الخصوصية والسرية تتطلب فعلًا إيجابيًا من قبل الشركة التجارية وتم رفض جميع المطالبات، باستثناء دعوى المطالبة بانتهاك الواجب القانوني للشركة لحماية بيانات العملاء. كما تم تغريم الشركة التجارية بمبلغ ٥٠٠٠٠٠ جنيه إسترليني وهو الحد الأقصى بموجب قانون DPA (1998).

نستنتج مما سبق أن شركة (DSG) لن تتمكن من مطالبة شركة التأمين بمبلغ التأمين وفق بند انتهاك البيانات كون البيانات لم يتم نشرها ولم تصل إلى حيازة المجرمين نتيجة السلوك الإيجابي للمؤمن له، والذي كان حسن النية، مع الأخذ بنظر الاعتبار إمكانية حصول المدعى عليه على مبلغ التأمين وفق بند التأمين ضد الغرامات غير الجزائية كون المحكمة العليا في المملكة المتحدة قد فرضت الغرامة الناتجة عن دعوى المطالبة بانتهاك الواجب القانوني بحماية بيانات العملاء.

وفي إعتقادنا ان القرار أعلاه سيكون بمثابة سابقة قضائية في مجال عقود التأمين من المخاطر السيبرانية حيث سيؤدي إلى رد العديد من دعاوى التعويض التي يقيمها الغير ضد الشركات التجارية المؤمن لها من المخاطر السيبرانية من جهة، وإلى رد دعاوى المؤمن لهم ضد شركات التأمين للحصول على مبلغ التأمين بحجة سرقة البيانات مالم يتوفر شرط النشر. كما أكد القرار على أهمية الواجب القانوني العام المفروض على الشركات التجارية تجاه عملائها والمتمثل بتوفير الحماية الكافية لبيانات العملاء وإلا سيتكبدون مبلغ الغرامة المالية المقرر قانوناً.

علماً ان مبلغ الغرامات المفروضة بموجب اللائحة العامة لحماية البيانات (GDPR) اعلى بكثير من تلك المفروضة في قانون (DPA 1998) حيث تصل إلى ٢٠ مليون يورو، أو ٤ في المائة من اجمالي قيمة التداول السنوية في السنة المالية السابقة ايهما أعلى[١].

(١) وفقاً للمادة (٨٣) من اللائحة العامة لحماية البيانات (GDPR) النافذة سنة ٢٠١٨.

المبحث الثاني

تحديات التأمين من المخاطر السيبرانية

على الرغم من كون التأمين من المخاطر السيبرانية وسيلة مميزة تلجأ لها بعض الشركات التجارية لتغطية الخسائر و النفقات الناتجة عن تلك المخاطر، إلا أن هذا النوع من التأمين لا يزال يواجه العديد من التحديات والمعوقات التي تعرقل نموه وتطوره مقارنة بالتأمين من المخاطر التقليدية[1]. ويمكن تصنيف هذه التحديات بصورة عامة إلى فئتين رئيسيتين: تحديات فنية وتحديات قانونية. وكل من هذه التحديات قد واجهها التأمين من المخاطر السيبرانية في جانب معين، لذا سنقسم هذا المبحث لمطلبين، نخصص الأول للتحديات الفنية للتأمين من المخاطر السيبرانية، أما المطلب الثاني فسنخصصه لبحث التحديات القانونية للتأمين من المخاطر السيبرانية.

المطلب الأول

التحديات الفنية للتأمين من المخاطر السيبرانية

يواجه التأمين من المخاطر السيبرانية العديد من التحديات التي تقلل من إعتماد الشركات التجارية لهذا النوع من التأمين وتحد من تطوره، فحداثة هذا النوع من التأمين وإختلافه عن صور التأمين التقليدية المعروفة منذ تاريخ طويل، أفرز العديد من المشاكل الفنية والعملية التي واجهتها شركات التأمين عند طرحها لوثائق التأمين من المخاطر السيبرانية. وإن ما يميز هذه المعوقات الفنية هو إرتباط كل منها بالأخرى كمحصلة نهائية أثناء البحث فيها، وسنتطرق في هذا المطلب إلى أبرز التحديات الفنية التي واجهها هذا النوع من التأمين والتي كانت محل نقاش العديد من الباحثين في هذا المجال، وتتمثل ب: صعوبة تسعير تغطية التأمين من المخاطر السيبرانية، و التخوف من التأمين من المخاطر السيبرانية، التي سنتناولها بالبحث تباعاً.

(1) Andrew Granato, Andy Polacek, The growth and challenges of cyber insurance, the federal reserve bank essays on issues of Chicago no. 426، 2019, p 1.

الفرع الأول

صعوبة تسعير تغطية التأمين من المخاطر السيبرانية

تدير شركات التأمين بشكلٍ عام المخاطر عن طريق تحديد أسعار التأمين _ أي تحديد المبلغ الواجب دفعه من قبل العملاء كقسط للتأمين _ والاستثمار في الأصول، ومن خلال هذه الكيفية تضمن قدرتها على الدفع لحاملي الوثائق عند المطالبة في المستقبل عند تحقق الخطر المؤمن منه، حيث تقوم بدورها بتقدير إحتمالية وقوع الأحداث وسلوك حامل الوثيقة عن طريق إستخدام مجموعة كبيرة من البيانات التي تم تجميعها على مدار سنوات عديدة، ووجود هذا الكم الهائل من السجلات التاريخية والبيانات اللازمة لتقدير المخاطر المراد إدراجها في وثائق التأمين الخاصة بها يسهل من عملها، على العكس من المخاطر التي تفتقر إلى مثل هذه النوع البيانات بسبب حداثتها أو عدم الإبلاغ عن حدوثها من الأساس[١] ، وبالتزامن مع بدء ظهور سوق التأمين من المخاطر السيبرانية، قامت شركات التأمين بتحسين سياستها التأمينية، إلا أنه لا تزال هناك جملة من التحديات التي تجعل من الصعب عليها كتابة وتسعير عقود التأمين من المخاطر السيبرانية، وذلك بسبب محدودية سجل الخسائر[٢] والذي سيؤدي بدوره إلى صعوبة تحديد أقساط التأمين، على عكس الأنماط التقليدية من التأمين كالتأمين على المركبات، حيث يوجد تاريخ طويل وسجل وافر من البيانات التي تتعلق بالخطر والأضرار الناجمة عن تحققه والذي يساعد على معرفة احتمالية تعرض سائق المركبة لحادث معين مما يسهل على شركات التأمين بالمقابل إمكانية تحديدها للأقساط التأمينية لغرض تغطية الخسائر المتوقعة. علماً أن السجلات الخاصة بالبيانات المتعلقة بالحوادث السيبرانية تكاد تكون نادرة، ويعتقد البعض أنه حتى وإن وجدت مثل هذه السجلات فهي قد تكون عديمة الفائدة في وقت ما بسبب التطور السريع للخطر السيبراني[٣].

(1) Zain Mohey-Deen, Richard J. Rosen, The risks of pricing new insurance products: The case of long-term care, the federal reserve bank essays on issues of Chicago, no. 397, 2018 p1.

(2) Henry R K Skeoch, Christos Ioannidis، The barriers to sustainable risk transfer in the cyber-insurance market, Journal of Cybersecurity, Volume 10, Issue 1, 2024, p2.

(٣) صدام فيصل كوكز، مصدر سابق، ص١٥٦.

ونتيجةً لعدم وجود سجلات إحصائية للحوادث السيبرانية التي قد سبق و أن تضررت منها الشركات التجارية في وقت ما، فإنه سيتحتم على شركة التأمين – إذا ما رغبت في إضافة وثائق تأمين من نوع آخر كوثيقة التأمين من المخاطر السيبرانية بصورة مبدأيه – التكهن بجميع التكاليف المستقبلية المتوقعة لهذا النوع من المخاطر لغرض توفير التغطية التأمينية من المخاطر السيبرانية لجميع الشركات التجارية الراغبة بالتأمين منها، ويمكن الإستعانة في تقدير تكاليف التغطية من المخاطر السيبرانية بعدد من الوسائل التي تم من خلالها تقدير سعر تغطية بعض المخاطر التقليدية، والتي غالباً تكون مختلفة عن طبيعة المخاطر السيبرانية وخصوصيتها كخطر مؤمن منه(١).

لقد أدى عدم إفصاح الشركات التجارية التي سبق وأن تعرضت للمخاطر السيبرانية عن البيانات الخاصة بهذه المخاطر وما خلفته من أضرار مادية ومعنوية إلى تفاقم مشكلة ندرة البيانات وعرقلة التعرف على الطريقة الدقيقة لتقدير خسائر المخاطر السيبرانية لكي يتم وضع سجل خاص بها، الأمر الذي أدى إلى إرتفاع أسعار التأمين و محدودية التغطية، على الرغم من إلزام بعض الدول للشركات التجارية التي سبق وأن تعرضت لخطر سيبراني بضرورة الإفصاح عنه، كما هو الحال عليه في المملكة المتحدة حيث تم وضع عدد من القوانين واللوائح المتخصصة لتعزيز عملية صيانة الأمن السيبراني بحيث يمكن للشركات تبادل البيانات لغرض إدارة المخاطر السيبرانية والإستفادة من التعاون الوثيق مع بعضها البعض كما ألزمتها بضرورة الإبلاغ عن هذا النوع من المخاطر حال تحققها نظراً لمساسها بالأمن القومي(٢)، لكن وحتى وإن ألزم القانون بالإفصاح عن هذه المخاطر السيبرانية فإننا نكون أمام مشكلتين رئيسيتين:

الأولى هي أن بعض القوانين قد تستثني من هذا الإلزام حالة الخرق الذي يؤثر على عدد قليل من الأفراد، فعلى سبيل المثال لا تكون الشركة التجارية ملزمة بالإفصاح عن الخطر السيبراني عند حدوث

(1) Zain Mohey-Deen, Richard J. Rosen, op.cit, p3.

(٢) على الرغم من عدم وجود قانون وطني أساسي شامل للأمن السيبراني في المملكة المتحدة، إلا أن هناك أربعة مخططات تشريعية مهمة تحكم الأمن السيبراني وخصوصية البيانات وحماية البيانات فيها مثل: قانون حماية البيانات لعام ٢٠١٨ (DPA) و اللائحة العامة لحماية البيانات في المملكة المتحدة لعام ٢٠٢١ UK_GDPR و لوائح أمن الشبكات والمعلومات لعام ٢٠١٨ (NIS) و قانون اساءة استخدام الكمبيوتر لسنة ١٩٩٠. للمزيد انظر:

Yueshan He, "Cyber Risk Insurance Pricing Based on Optimized Insured Strategy. A research paper presented to the University of Waterloo in partial fulfillment of the requirement for the degree of Master of Mathematics in Computational Mathematics" (2016), p42.

خرق بسيط للبيانات بحيث يمتد أثره على عدد قليل من الافراد ، أو أن الشركة لم يصل لعلمها تعرضها لخطر سيبراني من الاساس، وهذا بدوره يؤثر على العمليات الاحصائية التي يتم من خلالها تحديد أسعار التأمين على عكس الحوادث التي تطال الآلاف أو الملايين من الأفراد. **أما المشكلة الاخرى** ؛ فوصفها البعض بتحيز القوانين أي أن القوانين ذات الصلة ألزمت الشركات التجارية بضرورة الإفصاح عن مخاطر سيبرانية معينة دون أخرى، كما هو الحال في الولايات المتحدة ،حيث تبنت معظم الولايات قوانين تطالب الشركات بالإبلاغ عن المخاطر السيبرانية المتعلقة بخرق البيانات دون تلك التي تتعلق بإنتهاك الخصوصية أو الحوادث الامنية السيبرانية الأخرى(١).

أما بالنسبة للدول التي لا تلزم الشركات التجارية بالإبلاغ عن تعرضها لجريمة سيبرانية، فإن إمكانية إحصاء بيانات الخسائر لغرض التوصل إلى إستنتاج تكلفة أسعار التأمين تكون ضئيلة، فمن بين جميع الحوادث السيبرانية سيتم وصول البعض منها لعلم الجمهور وذلك إما عن طريق إفصاح الشركة المتعرضة للخطر بذاتها عن تعرضها لخطر سيبراني بصورة مباشرة ، أو عن طريق تداول بياناتها المالية علناً والتي يتبين منها صرف جزء من الأرباح لشركات الأمن السيبراني أو دفع تعويضات للمتضررين، أو قد تتم معرفة تعرض الشركة للخطر من خلال طرف ثالث يقوم بالإبلاغ عن تحقق الخطر(٢).

ومن هنا يكمن التحدي في تسعير التأمين من المخاطر السيبرانية، فقد يؤدي التسعير الخاطئ له على أسس من إفتراضات إما خاطئة أو متفائلة إلى حد ما، إلى نتائج وخيمة على شركات التأمين قد تنتهي بإفلاسها(٣).

ومن هذا المنطلق ستكون شركة التأمين أمام احتمالين:

الأول هو أن تحدد أسعاراً عالية جداً نتيجة عدم يقينها بالخسائر المحتملة بالمستقبل نظراً لإنعدام وجود سجل خسائر بسبب طبيعة الخطر السيبراني المترابطة والمتغيرة ، فتنعكس حالة عدم اليقين هذه على الأقساط فترفعها ، وهذا ما يؤدي إلى وصف عقد التأمين من المخاطر السيبرانية بأنه عقد يكتنفه الغموض وعدم اليقين من قبل شركات التأمين ذاتها الأمر الذي يؤدي إلى عدم قدرتها على إبرام

(1) Sasha Romanosky, Examining the costs and causes of cyber incidents, op. cit. p123.
(2) Sasha Romanosky, Ibid. , p122.
(3) Andrew Granato, Andy Polacek, op.cit, p4.

العديد من عقود التأمين وبالتالي يؤدي إلى بطئ نمو سوق التأمين من المخاطر السيبرانية[١]، أما بالنسبة **للإحتمال الثاني** هو أن تحدد شركة التأمين أسعاراً منخفضة للغاية نتيجة صعوبة تقدير الخسائر المتوقعة ووضع حدود أكبر للتغطية مقارنة بما يطمح إليه العملاء مما يجعل الشركة في موقف محرج نتيجة عدم قدرتها على دفع المطالبات المستحقة لحاملي وثيقة التأمين مما يقودها للإفلاس، كأن يكون الحد الأدنى للتعويض هو ٥٠٠ مليون دولار على الرغم من أن معظم شركات التأمين الكبرى بالكاد تستطيع تأمين ٣٠٠ مليون دولار، فكيف الحال بالنسبة لشركات التأمين الصغيرة[٢].

وهذا مشابه لما حدث لشركة (**Penn Treaty Network America Insurance**) والتي كانت تعد إحدى أكبر شركات التأمين في الولايات المتحدة الأمريكية، و سبق وأن أبرمت عدد من عقود التأمين من المخاطر السيبرانية مع بعض الشركات التجارية، ووضعت للشركات التجارية أسعاراً منخفضةً عما يتوجب أن يكون عليه في الواقع التأمين من تلك المخاطر، وكان ذلك نتيجة التكهنات غير الصحيحة وقلة الخبرة في هذا النوع الجديد من عقود التأمين فضلاً عن وجود بينات إكتوارية محدودة عن الخطر السيبراني، كما كانت الأقساط طويلة الأمد حتى ٥٠ عاماً في المستقبل، مما جعله السبب الرئيس للإضرار بربحيتها وإفلاسها ومن ثم تصفيتها في مارس ٢٠١٧[٣].

والسؤال الذي يثار بهذا الصدد هو كيف سيتم معالجة قضية مفصلية وإشكالية مثل تسعير التأمين من المخاطر السيبرانية؟ هل من الممكن ان يتم ذلك وفق الآلية ذاتها المعمول بها في تحديد أقساط التأمين من المخاطر التقليدية، ام ان التأمين من المخاطر السيبرانية يحتاج لأن ينفرد بآلية تسعير خاصة به؟

بالرجوع لمؤتمر (**CYBER RISK INSIGHTS**)[٤] لعام ٢٠١٩ نجد أن شركات التأمين والوسطاء قد أشاروا إلى أن إستخدام الأسس الفنية المستندة للتحليل الإكتواري السليم والنماذج

(1) 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, p16.

(٢) نشرة الاتحاد المصري للتأمين "الهجمات الالكترونية (السيبرانية) والتأمين"، مصدر سابق.

(3) Zain Mohey-Deen, Richard J. Rosen, op. cit, p5.

(٤) هو مؤتمر عقد في نيويورك في العام ٢٠١٩ تحت عنوان "قياس المخاطر السيبرانية ونمذجتها وإدارتها" ببرنامج مدته يوم واحد، و يعتبر حدثًا رئيسيًا في مجال المخاطر السيبرانية. ويتضمن مؤتمر التأمين متعدد المسارات أهم المواضيع بما في ذلك إدارة المخاطر السيبرانية، وتطوير القضايا في مجال التأمين من المخاطر السيبرانية وإلقاء=

الإحتمالية _ والتي كانت تستخدم في تسعير عقود التأمين من المخاطر التقليدية _ وتطبيقها على هذا النوع من التأمين لا يمثل سوى إستثناء من الأصل العام، حيث أن تحديد أقساط التأمين من المخاطر السيبرانية يعتمد بشكل كبير على أسعار السوق والتي تقوم على أساس المنافسة لا التحليل، كما هو الحال في عقود التأمين الأخرى. لذا لا يزال تسعير التأمين وفق أسس فنية أو علمية موثوقة بعيد المنال نظراً للطبيعة المتطورة للمخاطر السيبرانية(١) . فضلاً عن ذلك فإن أقساط التأمين تتناسب طردياً مع ضعف الشركة الأمني، فكلما كانت الشركة المؤمن لها ضعيفة ومعرضة للمخاطر السيبرانية كلما ادى ذلك لزيادة القسط التأميني والعكس صحيح. لذا فأن معالجة مشكلة إرتفاع أسعار التأمين تكمن في معالجة هذا الضعف من خلال إستثمار الشركات التجارية في مجال نظام أمن المعلومات ، بل إن بعض الباحثين يقترح على شركات التأمين إجراء خصم على أسعار التأمين لتحفيز عملائها وتقليل القسط الذي يثقل كاهل الشركات طالبة التأمين ، وعلى وجه الخصوص تلك التي تمتلك نظام أمني عالي وتؤدي حماية ذاتية أفضل(٢).

وتحاول شركات التأمين المتخصصة بالتأمين من المخاطر السيبرانية الإعتماد على عدد من العوامل غير المباشرة لغرض تسعير عقود التأمين بما يتلائم وطبيعة الخطر السيبراني المتغيرة ، وذلك من خلال الرجوع إلى تقديرات السوق لتكلفة الهجمات السيبرانية ، أو عمل إستبيانات خاصة لتحديد المخاطر التي من الممكن التأمين منها، أو أن تعتمد شركة التأمين على التسعيرة السائدة في السوق والتي وضعتها شركات التأمين الأخرى لخطر سيبراني مماثل(٣). لكن غالباً ما تغفل هذه الشركات عن الأخذ بنظر الإعتبار عند تحديد معادلة تسعير التأمين إحتمالية تأثرها بالأنواع المتطورة من المخاطر السيبرانية على المدى الطويل كالفيروسات و برامج الفدية وبرامج القرصنة التي تؤدي إلى انتهاك البيانات والخصوصية والهندسة الاجتماعية(٤).

=نظرة ثاقبة على "الجانب المظلم" للويب – مع التركيز على الأشخاص الذين يقفون وراء أحدث الجرائم السيبرانية. كما ناقش المؤتمر التوقعات الحالية والمستقبلية لسوق التأمين من المخاطر السيبرانية، وإمكانية العمل على الشمول والمساواة في ذلك السوق. للمزيد انظر:

https://www.advisenltd.com/2019-cyber-risk-insights-conference-new-york/

تاريخ الزيارة ٢٠٢٣/٩/١٧ الساعة ٨:٠٠ ص.

(1) Julie Bernard, op.cit, p14.
(2) Yueshan He, op.cit, p26.
(3) Andrew Granato, Andy Polacek, op.cit, p6.
(4) Julie Bernard, Ibid., p12.

وبغض النظر عن التحدي المتمثل بتسعير أقساط التأمين من المخاطر السيبرانية فإن شركات التأمين بإمكانها أن تعتمد في تسعير الأقساط على أحد هذه العوامل[١]:

١- الإعتماد على المصادر الخارجية للتسعير كالمنظمات المتخصصة.

٢- تقدير أو تخمين القسط الواجب دفعة.

٣- الإعتماد على تسعيرة المنافسين، حيث أن بعض الشركات إعتمدت على أسعار منافسيها في تحديد قسط التأمين، فبالرغم من أن هذه الممارسة قد تبدو غريبة إلا أنها أصبحت أمراً شائعاً لدى العديد من شركات التأمين.

٤- إستفادة شركة التأمين نفسها من تجاربها السابقة، حيث تميل شركات التأمين إلى هذا الاسلوب عند وثوقها بخبرتها بدرجة كافية، فشركة التأمين التي تتمتع بخبرة كافية في مجال التجارة الالكترونية والتأمين على الإنترنت والخصوصية وتأمين مسؤولية الشركات، سيكون من السهل عليها تحديد قسط التأمين مقارنة بالشركات حديثة النشأة، حيث تستخدم خبرتها للفهم العميق للأسعار التنافسية وردود الأفعال لتحديد معادلة الأسعارالمناسبة.

٥- الإعتماد على الأقساط المذكورة في عقود التأمين التقليدية الأخرى.

وتجدر الإشارة إلى أنه قد ظهرت في الآونة الاخيرة منظمات تأخذ على عاتقها مهمة تجميع البيانات التي تتعلق بالمخاطر السيبرانية كتجميع البيانات المتعلقة بالخسائر الناجمة عن هذه المخاطر والتكلفة الناشئة عنها والمسؤولية الناشئة عن خطأ موظفي الشركة التجارية المؤمن لها والمطالبات المتعلقة بالشركة المؤمن لها نفسها والمطالبات المتعلقة بالغير. ومهمة هذه المنظمات هي تجميع البيانات أعلاه ومن ثم بيعها على شركات التأمين ليتم على أساسها تقدير كلفة التغطية التأمينية وتحديد أسعار القسط الواجب دفعه من قبل الشركات التجارية الراغبة بالتأمين، وتعد منظمة (**Advisen**) من المنظمات الربحية[٢] الرائدة في هذا المجال ومقرها الولايات المتحدة، وتتجاوز قاعدة

(1) Sasha Romanosky and others، Content analysis of cyber insurance policies: how do carriers price cyber risk?, Journal of Cyber security, Volume (5), Issue (1), 2019, p12.

(٢) وهذا لا يعني انه لا توجد منظمات غير ربحية تقوم بهذه المهمة، ومن هذه المنظمات الرابطة الوطنية لمفوضي التأمين (NAIC)، حيث طورت نظام سجلات الكتروني يسمى (SERFF) من اجل تسهيل تقديم ومراجعة واعتماد ايداعات المنتجات بين المنظمين وشركات التأمين وكذلك الاستثناءات واستبيانات التقييم الذاتي المقدمة للعملاء للتعرف على وضعهم الامني والمعادلات التي على اساسها تم تحديد الاسعار، وتكمن الفائدة لمثل هكذا منظمات هو التنسيق في المعلومات بين الدول المختلفة، بالإضافة لكونها مصدر اعلام للجمهور، كما انها توفر فرصة فريدة لفحص كيفية فهم=

البيانات الخاصة بها و المتعلقة بالخسائر السيبرانية (٣٠٠٠٠٠) ملاحظة تم جمعها من قبل فريق متخصص من المحللين في هذا المجال والذين يستخدمون مجوعة شاملة من استراتيجيات البحث من أجل العثور على هذه البيانات وتصنيفها على وجه التحديد، والمصادر الرئيسية لهذه البيانات تتمثل بجميع المصادر المتاحة للجمهور والتي يمكن الحصول عليها من حكومة الولايات والحكومة الفيدرالية والوكالات ومراكز خدمات المعلومات القانونية المتخصصة ومراكز تبادل لمعلومات المتعلقة بخرق البيانات عبر الإنترنت و المواقع الإخبارية المحلية والوطنية..الخ[١].

وقد تحتاج شركات التأمين من المخاطر السيبرانية لكي يتم تحديد القسط بشكل دقيق إلى التعرف على مدى تعرض الشركة التجارية طالبة التأمين إلى هذه المخاطر السيبرانية، ويتم ذلك من خلال إلزام الشركة بالإفصاح عن المخاطر التي تعرضت لها والطرق التي تبنتها للحفاظ على نظام الكتروني آمن في العمل بالإضافة إلى تحديد كمية الدعم التقني والبشري الممكن توفيره في حال تحقق الخطر[٢].

وفي جميع الأحوال، يمكن وصف المخاطر السيبرانية بأنها مخاطر فوضوية– إذا جاز التعبير – مقارنة بالمخاطر التقليدية، حيث إنه من غير الممكن تقديرها من خلال الاعتماد على البيانات

=شركات التأمين للمخاطر وتسعيرها وعلى وجه التحديد فهم ماهية الضوابط التي يتم اخذها بنظر الاعتبار حساب الاسعار للمزيد انظر:

Sasha Romanosky and others، Content analysis of cyber insurance policies: how do carriers price cyber risk?, op.cit, p2,3.

(1) Sasha Romanosky, Examining the costs and causes of cyber incidents ,op .cit, p12.

(٢) وتم النص على ذلك في العديد من وثائق التأمين من المخاطر السيبرانية، للاطلاع على الوثائق أنظر:

(AXIS) Cyber ransomeware Supplement Application, No. 1012729 10 20:
https://www.euclidspecialty.com/wp-content/uploads/2021/05/AXIS_Ransomware_App-2021-1.pdf

(QBE) Cyber Response Insurance Policy, Danmark:
https://qbe.dk/media/8241/qbe-cyber-response.pdf

(MSIG Insurance) cyber risk Application:
MSIG Insurance (Vietnam) Company Limited، CYBER INSURANCE POLICY
https://www.msig.com.vn/sites/default/files/downloads/CYBER_INSURANCE_0.pdf

(HSB) cyber risk Application:
https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf
date of visit 13/5/2024 12:00 pm.

التاريخية فقط حتى وإن تم جمعها بصورة صحيحة، كونه لا يوجد ضابط محدد لتقييم هذه المخاطر في المستقبل كونها مخاطر متطورة ومتغيرة، وبالتالي لا يمكن نمذجتها بسهولة. لذا فإن الحل الأمثل لتقييم هذه المخاطر السيبرانية قد يكون بالإستناد إلى أحكام الخبراء في مجال التأمين السيبراني أو الامن السيبراني. وعلى الرغم من أن هذا الحل قد يكون هو الأنسب من بين الحلول السابقة إلا أنه لا يخلو من مثالب، حيث إن عامل الخطأ في تقدير الخطر لدى الخبراء لا يزال موجوداً، نتيجةً لإختلاف الخبراء فيما بينهم حول الآراء والخلفيات بسبب إختلاف درجة معرفة كل منهم، فلا يوجد تقييم معتدل لهذه الاخطار فإما ان يبالغون في تقدير الخطر أو انهم يقللون من قيمته، مما ينعكس سلباً على صحة توقع سعر وثيقة التأمين من المخاطر السيبرانية(١).

وتجدر الاشارة إلى أن المشرع العراقي قد ألزم شركات التأمين بالتعامل مع الخبراء المسجلين لدى ديوان التأمين حصراً وفقاً لقانون تنظيم اعمال التأمين رقم ١٠ لسنة ٢٠٠٥ واستناداً للفقرة أولاً من المادة (٧٧) منه نجد ان المشرع العراقي قد حضر مزاولة اعمال خبير الكشف وتقدير الأضرار بأستثناء المسجلين منهم في سجل الديوان مع الاخذ بنظر الإعتبار إمكانية الاستعانة بالخبراء غير المسجلين في الحالات التي تستوجب خبرة فنية خاصة عند استحصال الموافقة التحريرية من رئيس الديوان وفقاً للفقرة الثانية من المادة السابقة، وكذلك الأمر بالنسبة لخبراء رياضيات التأمين الاكتواريين حيث يحظر القانون مزاولتهم لأعمالهم كخبراء تأمين إلا بعد الحصول على ترخيص من ديوان التأمين ووفقاً للأسس والشروط التي يحددها رئيس الديوان وذلك وفقاً للمادة ٧٨/ أولاً من القانون ذاته.

ويمكن القول بصورة عامة بإن الخبراء متفقين على أنه – بغض النظر عن نوع الخطر المطلوب التأمين منه – سواء أكان خطر تقليدي ام لا، فسوف تتحكم ثلاثة معايير في تحديد الشركة لقسط التأمين، وهي عدم المبالغة، والكفاية. والتمييزية. ويقصد **بعدم المبالغة** أن لا تكون الاقساط مسعرة بصورة مبالغ فيها أو غير معقولة، اما **الكفاية** فيقصد بها ان تكون الأسعار مرتفعة بصورة تكفي لدعم الاعمال التجارية لشركة التأمين، أما **التمييزية** فتعني أن أي فرق أو تمييز في تحديد قسط التأمين لشركة تجارية معينة يجب أن يتناسب مع حجم المخاطر السيبرانية المتوقع تحققها(٢).

(1) Michael Krisper, op.cit, p7.

(2) Sasha Romanosky and others، Content analysis of cyber insurance policies: how do carriers price cyber risk?, op.cit, p 12.

الفرع الثاني

التخوف من التأمين من المخاطر السيبرانية

بالرغم من حاجة الشركات التجارية على إختلاف أنواعها للتأمين من المخاطر السيبرانية في الوقت الحالي بسبب إزدياد سعة ونطاق المخاطر المنتشرة عبر الفضاء السيبراني، وعلى وجه الخصوص الشركات المعتمدة على الإنترنت كوسيلة لتسهيل أداء نشاطها التجاري سواء كانت شركة كبيرة او متوسطة او حتى صغيرة، حيث ان ٦٠ بالمائة من المخاطر السيبرانية تأتي من داخل المؤسسة من موظفين و عملاء و موردين أو حتى الزائرين ومزودي الخدمة أو المتدربين، حيث يمكن لهؤلاء الإطلاع على أسرار الشركة التجارية والمالية والتكنولوجية بسهولة أكثر من غيرهم المهاجمين الخارجيين وبغض النظر عن أهدافهم كالحصول على عقود مشاريع أو بيانات الاسهم أو البيانات المحاسبية للشركة (١).

فالضرر السيبراني يمكن أن يمتد وينتشر بسرعة هائلة مخلفاً العديد من الأضرار المادية وغير المادية للشركة بحد ذاتها ولعملائها على وجه العموم، لذا يمكننا تشبيه المخاطر السيبرانية بالسلسة التي يكون من الصعب إيقافها، فقد لا يكلف مهاجمة شركة تجارية سوى ثواني معدودة لتخلف أضراراً كبيرة يصعب تقديرها في أغلب الأحيان. وفي إعتقادنا أنه من الناحية النظرية لابدّ لكل شركة تجارية تمارس نشاطها في الفضاء السيبراني أن تبادر بالتأمين ضد هذه المخاطر، إلا أنه من الناحية العملية لا يزال معدل لجوء الشركات التجارية للتأمين من المخاطر السيبرانية منخفضاً وينمو ببطئ شديد، وهذا النمو البطيء لم يأت من فراغ وإنما يرجع لأسباب عديدة يراها البعض مقنعة لتبرير هذا الإحجام عن إبرام عقود التأمين من هذه المخاطر الجديدة. فقد تحجم الشركات التجارية عن التأمين من المخاطر السيبرانية لسبب رئيسي هو عدم قدرتها على تحمل التكاليف الباهظة لهذا النوع من عقود التأمين بسبب ارتفاع أقساطه، حيث يبحث مديرو الشركات التجارية في الغالب عن أساليب واطئة الكلفة لتجنب الاضرار الناشئة عن العمل في الفضاء السيبراني، فهم يترددون في دفع أقساط عالية للحماية من المخاطر السيبرانية بهدف التقليل من الميزانية المخصصة لإدارة المخاطر. ومن ثم قد يلجؤون لحل بديل لتدارك هذه المخاطر كالتعاقد مع مختصين في مجال الامن السيبراني لتجنب

(١) بغداد شامبي، مصدر سابق، ص٢٧٩.

اللجوء إلى عقود التأمين من المخاطر السيبرانية ذات الاقساط باهظة والتي تتطلب ميزانية أكبر[١] حيث تشكل قلة أعداد الشركات التي تقدم على التأمين من المخاطر السيبرانية أحد أبرز أسباب إرتفاع الأسعار، و بالمقابل فإن أقساط التأمين من المخاطر السيبرانية تتناسب طردياً مع حجم هذه المخاطر فكلما تصاعدت وتيرة الجرائم السيبرانية كلما إرتفع سعر قسط التأمين منها[٢].

وعدّ أصحاب الشركات التجارية أن تكلفة هذا النوع من التأمين هو نوع من الترف ولا يمثل ضرورة ملحة، حيث وجد البعض أن اقساط التأمين من المخاطر السيبرانية أخذت بالارتفاع منذ الربع الثالث من العام ٢٠١٩ مما دفع الشركات إلى اللجوء إلى حلول بديلة أخرى تناسبهم كاللجوء إلى عقود التأمين تقليدية العامة غير المتخصصة في تغطية المخاطر السيبرانية والتي تؤدي الغرض ذاته من التأمين وبأقساط منخفضة _ مقابل عدم التأمين بعقود متخصصة ضد المخاطر السيبرانية _ كأن تقوم الشركات التجارية بالتأمين من الأضرار المادية والتأمين من الجريمة و التأمين من المسؤولية العامة[٣]. لكن النتائج تشير إلى أن المخاوف العامة المتعلقة بإرتفاع تكلفة التأمين من المخاطر السيبرانية بسبب المعدلات المتزايدة للإنتهاكات والدعاوى القانونية، ماهي إلا مخاوف مبالغ فيها حيث توصل المختصين في هذا المجال إلى أن هذه المخاوف العامة تتعارض مع واقع سوق التأمين، فأسعار التغطية السيبرانية تكون مساوية تقريباً للميزانية السنوية لأمن تكنولوجيا المعلومات للشركة التي ليس لديها تغطية تأمينية، وهذا لا يمثل سوى (0.4) بالمائة من ايرادات الشركة السنوية، وقد جرت محاولات لتحفيز الشركات على إعتماد إجراءات الأمن السيبراني كما حصل في الولايات المتحدة الأمريكية في العام ٢٠١٣ حيث وقع رئيس الولايات المتحدة على أمر تنفيذي للمساعدة في تأمين البنى التحتية الحيوية للدولة من الهجمات السيبرانية [٤] ، وعلى ضوء ذلك وجه المعهد الوطني للمعايير والتكنولوجيا **(NIST)** إطار عمل طوعي غير ملزم للشركات التجارية لغرض إختيار أفضل شركة من ناحية ممارسات الأمن السيبراني، لأجل تحفيز الشركات لتحسين ممارساتها الأمنية وتقليل المخاطر السيبرانية[٥].

(1) Yueshan He, op. cit p3.

(2) Chiaradonna، S., & Lanchier, N, Exact Insurance Premiums for Cyber Risk of Small and Medium-Sized Enterprises. Mathematical Modelling of Natural Phenomena journal,vol. (17), Article (40), (2022), p1.

(3) Julie Bernard, op. cit, p7.

(4) Sasha Romanosky, Examining the costs and causes of cyber incidents، op. cit, p122.

(5) Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Matthew Fallon, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication NIST SP 800-161r1،2022, p234.

ويثور التساؤل عن الجدوى من هذه الممارسات الطوعية طالما أنها غير ملزمة، حيث أن عنصر الإلزام ضروري لتحفيز الشركات على متابعة العمل بهذه الممارسات الأمنية لذا نعتقد بضرورة تشريع قانون يلزم الشركات التجارية بتخصيص جزء من الميزانية لتفعيل وتطوير الأمن السيبراني للشركة كتدبير وقائي يقلل من الأضرار الوخيمة التي تسببها هذه المخاطر للشركات وخصوصاً المتوسطة والصغيرة منها ، ولا نعني بما سبق بإلزام الشركات التجارية بالتأمين من المخاطر السيبرانية حيث أن بعض الدول لا تزال في مرتبة متأخرة نوعاً ما من ناحية فهم ماهية هذا الخطر التأميني وتبعاته الوخيمة، فقد لا توجد عقود تغطي المخاطر السيبرانية للشركات من الأساس كما هو الحال في العراق، حيث تكتسح التغطيات التأمينية التقليدية سوق التأمين العراقي ولا وجود لعقود التأمين من المخاطر السيبرانية إلى وقتنا الحالي، على الرغم من تزايد الوعي بهذه المخاطر وإلتفات المختصين في مجال التأمين لضرورة تطوير هذا النوع من عقود التأمين. لذا قد يكون مهماً في الوقت الحالي بالنسبة لبعض الدول كالعراق مثلاً أن يتم إصدار قانون يلزم الشركات بإتخاذ تدابير الأمن السيبراني الضرورية كمرحلة أولى،ومن ثم إلزامها بالتأمين من المخاطر السيبرانية كمرحلة ثانية بعد أن تنضج فكرة التأمين من المخاطر السيبرانية فيه.

ومن الأسباب الأخرى التي دعت إلى إنخفاض الطلب على التأمين من المخاطر السيبرانية هو أن كل خطر سيبراني يتم الإبلاغ عنه نتيجةً لفشل النظام أو خرق البيانات يؤدي إلى خسارة مالية كبيرة أو فقدان السمعة فيزداد تخوف العملاء من إبرام عقود التأمين من المخاطر السيبرانية، بسبب إعتقادهم بأن عقود التأمين من المخاطر السيبرانية الحالية لا تغطي جميع الأضرار الناجمة عن المخاطر السيبرانية بشكل كافٍ[1] كما إن شروط العقد قد تكون صارمة، أي أنها تحتوي على بنود مقيدة للغاية، فتقيد من حرية الشركات التجارية وتضيق الخناق عليها نتيجة خصوصية شروط هذا العقد، ومن أمثلة هذه الشروط ان ينص العقد على ضرورة تعاقد الشركة التجارية المؤمن لها مع شركة أمن سيبراني للمحافظة على أمن الشركة التجارية وهذا بدوره يمثل تكلفة إضافية تثقل من كاهل الشركة خصوصاً ذات الميزانية المتواضعة. كما قد يؤدي غموض لغة عقود التأمين من المخاطر السيبرانية إلى تخوف الشركات التجارية من التأمين من المخاطر السيبرانية. وقد يكون سبب تباطؤ نموه هو الحدود المنخفضة للتغطية، بينما تفضل الشركات التجارية أن تغطي عقود التأمين من

(1) Biener, C., Eling, M., Wirfs, J. Insurability of Cyber Risk: An Empirical Analysis. Geneva Pap Risk Insur Issues Pract 40, 2015, p131.

المخاطر السيبرانية حدوداً أعلى بالكيفية التي تجعلها تغطي جميع التكاليف التي من الممكن أن تتكبدها تلك الشركات فيما لو تعرضت لأحد المخاطر السيبرانية[١] ، كذلك قد يعود سبب تخوف إبرام عقود التأمين من المخاطر السيبرانية إلى عدم وجود المعرفة والوعي الكافي بهذه المخاطر[٢]، أو الاستخفاف بالأضرار التي قد تلحق بالشركة التجارية إذا ما أصابها هذا الخطر. وعلى الرغم من رفع تصنيف هذه المخاطر من المرتبة الخامسة عشرة في العام ٢٠١٣ إلى المرتبة الخامسة في العام ٢٠٢٢ إلا أن عدد كبير من الشركات لا تزال غير واعية لماهية التأمين من المخاطر السيبرانية حيث إن بعض الإستطلاعات وجدت أن(٢١) بالمائة من الشركات التجارية في أوربا تعرف ماهية التأمين السيبراني مقابل (٧٩) بالمائة من الشركات لا تعي تماماً ما تعنيه المخاطر السيبرانية[٣].

وفي إعتقادنا أن عامل الخوف هو سلاح ذو حدّين، فمن جهة قد يدفع الشركات لإبرام عقود التأمين من المخاطر السيبرانية لحماية نفسها من الأضرار الوخيمة لهذه المخاطر ومن جهة اخرى قد يكون سبباً في احجام الشركات عن هذا النوع من التأمين لحداثته وعدم معرفه ماهيته وارتفاع تكلفته. ولحل هذه الاشكالية نعتقد بضرورة تفعيل دور وسطاء التأمين في مضاعفه الوقت والجهد لتثقيف الشركات التجارية وتعريفها بماهية هذا النوع من التأمين وإعلامهم بمدى أهميته كمصدر أمان للشركة وعملائها على حد سواء كونه يجنب الشركة العديد من المطالبات التي ستثقل من كاهلها في أحسن الظروف أو قد تعرضها للإفلاس في أسوأ الإحتمالات.

من الجدير بالذكر أن عامل الخبرة يلعب دور رئيسي في هذا الصدد، فالشركات التي سبق وأن تعرضت لأحد المخاطر السيبرانية غالباً ما تسارع إلى التأمين من المخاطر السيبرانية بسبب تخوفها من تكرار التعرض لتلك المخاطر السيبرانية، على عكس الشركات الحديثة التأسيس التي لم يسبق لها ان تتعرض لتهديد سيبراني، فكلما زادت خبرة المؤمن له زادت إحتمالية تأمينه من المخاطر السيبرانية كنوع من رد الفعل للمخاطر التي تعرض لها في السابق. فإذا كانت شركات التأمين تطمح لنمو سريع في السوق فإنه يتوجب أن تنشر الوعي في الشركات التجارية لأهمية التأمين من المخاطر السيبرانية بصورة مستقلة، وأن تتجنب العقود التقليدية التي قد تغطي المخاطر السيبرانية بصورة ضمنية أوعامة،

(1) Julie Bernard, op. cit, p7.
(2) Chiaradonna, S., & Lanchier, N, op. cit، p1.
(3) Daniel Woods, Andrew Simpson, Policy measures and cyber insurance: a framework, Journal of Cyber Policy Volume(2), Issue (2), 2017, p214.

ويجب عليها أن تثبت للعملاء المستقبليين أنه يمكن لهذه العقود المتخصصة بحد ذاتها أن تسد الفجوات التي غفلت عن تغطيتها عقود التأمين التقليدية[١].

وعلى الرغم من إقدام شركات التأمين لتغطية نوع جديد من المخاطروهو التأمين من المخاطر السيبرانية و الذي يعتبر بمثابة أمر مربح لها إلى حدٍ ما؛ بسبب أن هذه المخاطر لا تستثني احداً فهي من الممكن أن تصيب جميع الشركات التجارية التي تجري تعاملاتها من خلال الفضاء السيبراني، حيث يمكن أن تقع في أي زمان ومكان دون إستثناء شركة عن غيرها، مما يؤدي إلى توسيع قاعدة العملاء مقارنة بعقود التأمين التقليدية، لكن هذه الميزة في الوقت ذاته قد تؤثر بصورة سلبية على إزدياد تخوف العملاء من نشاط شركات التأمين التي تؤمن من المخاطر السيبرانية حيث أن شركات التأمين معرضة لذات المخاطر التي يفكر العملاء التأمين ضدها، فشركة التأمين أيضاً تمارس نشاطها في الفضاء السيبراني لديها كم هائل من البيانات الخاصة بعملائها مما يجعلها فريسة سهلة من قبل المهاجمين، مما ينعكس سلباً على نمو سوق التأمين من المخاطر السيبرانية ويقلل من إقبال الشركات التجارية على شراء التغطية[٢].

وبصورة عامة تتمتع المخاطر التقليدية بصفة رئيسية مميزة ألا وهي **(الإستقلالية)** ، حيث يجب أن تكون المخاطر المؤمن عليها على درجة معينة من الإستقلالية بصورة تتيح لشركات التأمين السيطرة على الآثار المترتبة على تحققها، أما بالنسبة للمخاطر السيبرانية فتمتاز بصفة التبعية والارتباط[٣]، وهذه الصفة تجعل من عملية التأمين برمتها غير مستقرة مما يشكل تحدياً لشركات التأمين لطرح هكذا تغطيات، فشركة التأمين من المخاطر السيبرانية لن تكون قادرة على أن تغطي جميع هذه الخسائر المتزامنة، حيث أن الخطر السيبراني من الممكن أن يكون خطراً **(كارثياً)** ، وهذا يتنافى مع أساسيات التأمين، والتي تشترط أن يكون الخطر غير كارثي للتأمين ضده، فحادثة سيبرانية واحدة قد تتزامن بصورة متسلسلة بين أكثر من نظام تشغيل لشركة تجارية واحدة لتحدث كارثة تصعب تغطيتها من قبل

(1) Julie Bernard, Ibid. , p10-16.

(2) 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, p379.

(٣) ويمكن تعريف المخاطر المرتبطة بأنها تلك المخاطر التي يمكن ان تؤثر في الوقت ذاته على عدد غير محدد من العملاء، للمزيد انظر:

Eling, M. Schnell, W., "What do we know about cyber risk and cyber risk insurance?", Journal of Risk Finance, Vol. (17) No. (5), 2016, p477.

شركات التأمين بسبب تجاوزها احتياطات الشركة المالية المقدرة مسبقاً فيؤدي ذلك لإفلاسها خصوصاً عند تعدي الخسائر الناتجة عن الخطر حدود الشركة المالية كالإضرار بالغير و الإصابة بضرر ثانوي كالإساءة للسمعة التجارية مثلاً[١]، مما يصعب المهمة على شركات التأمين بسبب هذه الطبيعة الخاصة للخطر و النتائج الوخيمة التي يخلفها والتي يصعب التنبؤ بها بسبب سرعة إنتشاره وعدم وجود معلومات كافية بشأنه حيث من الممكن أن يضرب العشرات من الشركات التجارية في وقت واحد بسبب طبيعة الوسط الذي ينتشر من خلاله الخطر بين أكثر من عميل وخلال ثواني معدودة مما يلزم شركة التأمين إلى دفع المطالبات لحاملي وثائقها دفعة واحدة[٢] ، لذا نستنتج أن المخاطر السيبرانية بصفتها مخاطر مرتبطة لا تقلل من كفاءة عملية التأمين أو تجعلها مستحيلة، بل أن هذا النوع من المخاطر يصعب من عملية التأمين عنه بشكل عام[٣].

وبناء عليه، نجد أن من أبرز التحديات التي تواجهها شركات التأمين هو إحتمالية الفشل المتتالي الناتج عن طبيعة الخطر السيبراني المؤمن منه، مثال على ذلك إستغلال المتسللين لثغرات أمنية في حواسيب شركة تجارية يؤدي بدوره لحصولهم على كلمات المرور لأجهزة أخرى موجودة في فروع الشركة المنتشرة حول العالم مما يؤدي إلى إنتقال الخطر السيبراني من الشركة الأم إلى فروعها ثم إلى بيانات عملائها الأمر الذي يتسبب بخسائر كبيرة تقدر بمليارات الدولارات مع إمكانية تكرار حدوث الخطر مرة أخرى خلال ثواني معدودة مما يخلف نتائج أسوأ في المرة المقبلة على عكس فكرة المخاطر التقليدية حيث أن تكرار حدوث الخطر بهذه الوتيرة السريعة يكاد يكون معدوماً[٤].

ومع ذلك فأن شركات التأمين من المخاطر السيبرانية يمكن لها من مواجهة التحدي المتمثل بتتابع أو ترابط الأخطار السيبرانية من خلال إتخاذها لتدابير تقلل من عملية الترابط هذه، كأن تتنوع في إختيار عملائها بصورة تكفل عدم وجود إرتباط فيما بينهم فيما لو تحقق الخطر السيبراني فتقل المطالبات التي ستثقل من كاهل شركة التأمين فيما لو كان الضرر متعدياً لأكثر من عميل كأن تتنوع في إختيار العملاء لأكثر من بلد، كما يمكن التقليل من الصفة التبعية للخطر السيبراني من خلال التنويع في إستخدام أنظمة التشغيل بحيث أن الضرر الذي يصيب أحد العملاء على نظام تشغيل

(1) Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, Ibid, p380.

(٢) محمد سعيد اسماعيل، مصدر سابق، ص٢٢٣.

(3) Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, op. cit, p 12.

(4) Andrew Granato, Andy Polacek، op. cit, p3.

معين قد لا يصيب عميل آخر يعمل في نظام تشغيل ثانٍ، أو أن تمتنع عن تغطية المخاطر التي تجدها مؤثرة على درجة ملائتها وسيولتها لكن قد يتكون لدى شركة التأمين انطباع خاطئ حول خطر سيبراني ما فتقوم بإستثنائه من بنود التغطية معتقدة أنه خطر مترابط لا يمكنها تحمل تكلفته(١). بالإضافة لما سبق فإن ما يعيق تطور هذه الشركات هو أن الأخطار السيبرانية هي مخاطر معقدة فمن الصعوبة فهمها أو وضع معايير لها وحجم خسائرها التي تفوق طاقة شركات التأمين مثل الأعطال المنتشرة على نطاق واسع في البنى التحتية الحيوية أو الشبكات وفي مثل هذه المخاطر تكون بعض الدول داعمة للمتضررين من الشركات التجارية وتقدم رعاية خاصة لهذه الحوادث الكارثية كتلك المقدمة لمحاربة الإرهاب(٢).

كما تتميز الحوادث السيبرانية بالتباين الإقليمي حيث تتركز هذه الحوادث في أماكن معينة بصورة أكبر من أماكن اخرى، فعلى سبيل المثال نجد أن الولايات المتحدة وأمريكا الشمالية وروسيا كانت من أكثر الدول إنفاقاً على الحماية السيبرانية على العكس مما هو عليه الحال في إفريقيا نظراً لوجود ارتباط بين مستوى الدخل وكمية الخسارة اللاحقة بسبب المخاطر السيبرانية وهذا لا نجده في المخاطر التقليدية التي لا يوجد فيها مثل هذا التباين(٣).

إن التأمين من المخاطر السيبرانية يحمي الشركات التجارية من مخاطر الفشل المتتالي ولابدّ للمختصين أن يأخذوا بنظر الإعتبار إحتمالية 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

(1) Yogesh Malhotra Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis December 7, 2017, p 5.

(2) **Juraj Sikra_Karen V. Renaud_Daniel R. Thomas**، UK Cybercrime, Victims and Reporting: A Systematic Review،**commonwealth cybercrime journal volume (1), issue** (1), 2023, p7.

(3) Yueshan He "Cyber Risk Insurance Pricing Based on Optimized Insured Strategy. A research paper presented to the University of Waterloo in partial fulfillment of the requirement for the degree of Master of Mathematics in Computational Mathematics" (2016) p3.

السنوات الماضية حاولت شركات التأمين توضيح نطاق تغطيتها القياسية وهل تتضمن التأمين ضد المخاطر السيبرانية كنوع من التغطية الصامتة[١] 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[٢]، 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 كبيراُ من العناية من قبل شركات التأمين في أثناء كتابة عقودها، حيث يجب أن تأخذ بنظر الإعتبار 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[٣].

المطلب الثاني

التحديات القانونية للتأمين من المخاطر السيبرانية

واجه سوق التأمين من المخاطر السيبرانية بالإضافة إلى التحديات الفنية التي أعاقت تطوره والتي تمت مناقشتها في المطلب السابق، تحديات من نوع آخر، وهي التحديات القانونية، فلا تزال فكرة التأمين من المخاطر السيبرانية مجهولة في العديد من دول العالم، ولا توجد نصوص قانونية كافية تنظم عقود التأمين من المخاطر السيبرانية، حيث لا تزال فكرة تشريع قانون التأمين من المخاطر السيبرانية بعيده، مما يؤدي إلى نتيجة مفادها تطبيق القواعد العامة للتأمين، وبما أن الخطر السيبراني ذي طبيعة خاصة تختلف عما هو موجود في التأمين التقليدي برز لدينا تحدي رئيسي وهو عدم وجود قواعد قانونية متخصصة بالتأمين ضد المخاطر السيبرانية، بالاضافة إلى أن طبيعة عقود التأمين من

(١) يقصد بالتغطية الصامتة حالة عدم ذكر المخاطر السيبرانية بصورة واضحة وصريحة ضمن المخاطر الواردة في عقد التأمين من المخاطر السيبرانية، انظر:

Julie Bernard, op. cit, p16.

(2) Julie Bernard, Ibid, p16.

(3) Yogesh Malhotra, Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis December 7, (2017) p 6.

هذا الخطر نوعاً ما معقدة وغير منمذجة ويكتنفها الغموض، فلا توجد نماذج وصيغ ثابتة لهذه العقود، فتختلف العقود من شركة إلى اخرى ومن خطر إلى آخر. عليه سوف نقسم هذا المطلب إلى فرعين نتناول في الأول **إنعدام القوانين الخاصة بالتأمين من المخاطر السيبرانية**، أما الفرع الثاني سنتناول فيه **صعوبة صياغة عقود التأمين من المخاطر السيبرانية.**

الفرع الأول

إنعدام القوانين الخاصة بالتأمين من المخاطر السيبرانية

تثير منازعات التأمين من المخاطر السيبرانية تحدياً بارزاً على المستوى القانوني حيث أنها تكلف الأطراف مبالغ باهظة بسبب إتساع حجم الأضرار الناشئة عن هذه المخاطر وصعوبة تلافيها حيث أن الأضرار التي قد تتكبدها الشركة التجارية نتيجة هذا الخطر يفوق بأضعاف حجم الأضرار للأخطار التقليدية ، ومن ناحية أخرى فإن إثارة النزاعات المتعلقة بهذا النوع من التأمين أمام القضاء أمر مكلف وفي غاية التعقيد نظراً لإنعدام القواعد القانونية المتخصصة، مما يؤدي بالشركات التجارية المتوسطة والصغيرة على وجه الخصوص بالتنازل عن مطالباتها بدلاً من الخوض في صراعات غير محمودة العواقب(١).

وعلى الرغم من إختلاف نطاق تغطية التأمين من المخاطر السيبرانية عن نطاق عقود التأمين التقليدية، إلا أنه لم يتم وضع قواعد قانونية خاصة بمنازعات التأمين من المخاطر السيبرانية(٢)، ومن الناحية القانونية يشكل إنعدام وجود قانون خاص بالتأمين من المخاطر السيبرانية تحدياً لا يستهان به،فعلى المشرع ان يعالج هذا النوع الجديد من عقود التأمين، وذلك من خلال إصدار قانون خاص بها. وبالمقابل يتحتم على الشركات التي تغطي المخاطر السيبرانية أن تأخذ بنظر الإعتبار هذه اللوائح والقوانين في جوهرها عند ممارسة نشاطها التجاري (٣). لا سيما وأن الأحكام العامة لعقد التأمين تكاد تكون غير كافية لسد هذا الفراغ التشريعي. فهي لا تضع سوى الخطوط العريضة لعقد التأمين وهي

(1) Franke Ulrik 0p. cit, p5.

(٢) شذى عبد جمعة موسى، مصدر سابق، ص١٥٩.

(3) Bahaa Eltahawy, Duong Dang. Understanding Cyberprivacy: Context، Concept, and Issues, 17th International Conference on Wirtschaftsinformatik (WI22) At: Nuremberg, Germany, 2022, p7.

عاجزة عن تنظيم التفاصيل الدقيقة والمؤثرة في مجال التأمين من المخاطر السيبرانية، فالقوانين الحالية في إعتقادنا لا تجيب عن أغلب التساؤلات التي تمت إثارتها في هذا البحث.

لذلك نرى أن تشريع قانون خاص بعقد التأمين من المخاطر السيبرانية، من شأنه إزالة الغموض الذي يكتنف هذا العقد، إبتداءاً من تعريف المخاطر السيبرانية وتحديد طبيعة المخاطر التي يمكن شمولها بالتغطية التأمينية ومن ثم تحديد آلية تسعير هذه التغطية، وإنتهاءً بالمسؤولية المدنية لشركات تأمين من حيث مطالبات الشركات التجارية المؤمن لها ومطالبات الغير، بل وحتى الغرامات المفروضة عند إنتهاك أحكام هذا القانون من قبل أطراف العقد. ويمكن في هذا الإطار الإستعانة بالسوابق القضائية والأعراف المهنية وآراء الخبراء والمختصين في مجال الأمن السيبراني، فضلاً عن الاستعانة بتجارب بعض الدول في مجال حماية البيانات والخصوصية، من أجل تعزيز الوعي بهذا النوع من التأمين، فتشريع هكذا قانون في العراق أمر تفرضه الضرورة العملية نظراً للتطورات التكنولوجية المستخدمة في مجال التجارة الإلكترونية من قبل الشركات التجارية بسبب إزدياد المخاطر السيبرانية وسهولة إنتشارها وإزدياد الوعي بآثار هذه المخاطر. لا سيما وأن المشرع العراقي يحاول جاهداً مسايرة الإتجاهات التشريعية الحديثة في مجالات الأمن السيبراني والتوقيع الإلكتروني والمعاملات الإلكترونية والجرائم المعلوماتية، حيث يمكن القول بأن المشرع العراقي قد وضع الأساس لتمهيد عملية تشريع قوانين تتعلق بالفضاء السيبراني و التأمين من المخاطر السيبرانية، فبالإضافة إلى تشريع قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (٧٨) لسنة ٢٠١٢، قد تم إعداد إستراتيجية الأمن السيبراني العراقي لسنة ٢٠٢٢والتي تأخذ على عاتقها رسم السياسة السيبرانية للدولة، حيث أفصحت هذه الاستراتيجية عن نية المشرع العراقي في مراجعة وتحسين القوانين السيبرانية ذات الصلة، بالإضافة إلى تشريع قوانين سيبرانية جديدة كقانون الخصوصية وقانون أمن الإتصالات والمعلومات، بهدف تعزيز الوعي القانوني والإرتقاء بمستوى التشريعات في الدول المتطورة، مع تأكيد الإستراتيجية على إنسجام هذه التشريعات وإعتبارها تكميلية للقوانين والإتفاقيات والمعاهدات الدولية، مما يدلل على رغبة المشرع العراقي في تشريع قوانين ذات نصوص موحدة مع الدول الاخرى[١].

(١) هي استراتيجية صادرة عن مستشارية الامن الوطني وتعالج التعرض الوطني للمخاطر السيبرانية في مجالات الجريمة الالكترونية والارهاب الالكتروني وتأخ على عاتقها اجراء التدابير المضادة من اجل تأمين وحماية الفضاء السيبراني الوطني وركزت الاستراتيجية على الاطار التشريعي والتنظيمي في مجالات الامن السيبراني وشددت على ضرورة التعاون الدولي في هذا المجال، كما اكدت على ضرورة حماية البنى التحتية الرقمية بالإضافة الى اشراك اصحاب المصلحة الوطنيين والدوليين من اجل التصدي للهجمات السيبرانية، وتضمنت العديد من المعالجات في هذا=

فوجود مثل هذه القواعد الخاصة بهذا المجال يعد وسيلة فعالة للردع القانوني امام كل من تسول له نفسه التعدي على حقوق الغير وخصوصاً الطرف الضعيف في العقد الا وهو المؤمن له حيث ستتمكن الشركات التجارية المؤمنة من المخاطر السيبرانية ان تذهب إلى ابعد الحدود لتحمي حقوقها الناشئة عن العقد واستحصالها كافة المطالبات بغض النظر عن قوة ونفوذ الطرف الاخر اي شركة التأمين(١).

وفي إعتقادنا أن إنعدام التنظيم التشريعي للتأمين من المخاطر السيبرانية يعدّ أبرز العوامل التي تتخوف منها الشركات التجارية، فقد تتردد في شراء تغطية تأمينية خارج إطار التنظيم القانوني للدولة، حيث تبحث هذه الشركات في الغالب عن حماية قانونية واضحة، بعيدة كل البعد عن غموض موقف المشرع تجاه عقود التأمين ضد المخاطر السيبرانية، خصوصاً وأنها نوعاً ما مكلفة حيث ستقوم الشركات التجارية طالبة التأمين بدفع أقساط مرتفعة وعلى مدى سنوات قد تكون طويلة، فلا تجد هذه الشركات الأمان القانوني في عملية التأمين من المخاطر السيبرانية، حيث لا يزال سوق هذا النوع من التأمين في بدايته، فتنفرد شركات التأمين بوضع أحكامه وضوابطه وإستثناءاته لتكون الطرف القوي في العقد خصوصاً مع إنعدام الأسس الثابتة في تحديد أسعار التأمين سواء من الناحية الفنية او القانونية.

ومن الجدير بالذكر أنه أصبح هناك إدراك متزايد بأن مخاطر العالم الإفتراضي لا تتناسب بالضرورة مع نطاق العديد من التغطيات من فئات التأمين التقليدية وبالتالي برزت الحاجة لوضع نظام قانوني خاص في مجال تأمين المخاطر السيبرانية(٢). وعلى الصعيد العام فأن تشريع قوانين التأمين السيبراني والخصوصية هو مفتاح لحماية الخصوصية الالكترونية وضمانة ضرورية لعمل شركات

=الاطار من الناحية التشريعية كضرورة العمل على طرح مسودات قوانين ذات صلة بالفضاء السيبراني والتركيز على زيادة الوعي بهذه المخاطر وبأثارها على مستوى الامن القومي، وبناء قدرات الباحثين في هذا المجال واضافة المناهج والتخصصات في مجال الامن السيبراني، وتعزيز القدرات القانونية في مجال التحقيق والاثبات في القضايا المتعلقة بالمعلوماتية. انظر موقع الهيئة الرسمي:

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

تاريخ الزيارة ٢٠٢٣/٥/١٢ الساعة ٤:٤٠م.

(١) صدام فيصل كوكز، مصدر سابق، ص١٧٣.

(2) Mark Camillo, Cyber risk and the changing role of insurance, Journal of Cyber Policy, vol. (2), issue (1), 2017, p54.

التأمين وللعملاء على حد سواء، ولهذه اللحظة لا يوجد إطار قانوني شامل ومشترك فيما يخص التأمين من المخاطر السيبرانية بحيث يكون لدى المعنيين وعي قانوني بالمسؤوليات والحقوق المترتبة عليهم خصوصاً أن هذا التأمين يتطلب كشف العديد من البيانات الشخصية للعملاء ، فشركات التأمين تطلب في الغالب الكشف عن بيانات أكثر من مما تحتاجه فعلاً، مما قد يخلف ممارسات خاطئة من قبل شركات التأمين أبرزها إنتهاكات الخصوصية[١] . ومما لا شك فيه فأن وجود قوانين خاصة في هذا المجال سيكون له أثر إيجابي من خلال إجبار الشركات على الحفاظ على خصوصية عملائها وبخلافه سيتحتم عليها دفع غرامات مالية كبيرة في حالة عدم إلتزامها بهذه المعايير[٢]، حيث أثبتت الدراسات أن سن القوانين المتعلقة بالجوانب السيبرانية يلعب دوراُ حيوياً في بناء الثقة في المعاملات التجارية الحديثة. خصوصاً أن هذه الاخطار محل البحث تمتاز بأنها سهلة الوقوع من الناحية الفنية وصعبة الإثبات من الناحية القانونية ، لذا لا بد من أن تتوفر الحماية القانونية لهذا النوع من التأمين كما توفرت الحماية للأنواع التقليدية منه[٣]، ومن ثم فإنه من الضروري أن تحدد القوانين والأنظمة ما هو مسموح وما هو غير مسموح في إطار التأمين ضد المخاطر السيبرانية بالإضافة إلى تحديد حقوق والتزامات الطرفين مع الأخذ بنظر الإعتبار نطاق تطبيق هذا القانون وتحديد جهات رقابية متخصصة في هذا المجال كما أن عدم كفاية القواعد العامة سيؤدي إلى إطلاق العنان للسلطة التقديرية للقاضي والتي قد يكون الضحية فيها هو العميل أو الشركة التجارية المؤمن لها[٤]، فضلاُ عن أن تشريع هكذا قانون يساعد في تقليل الأضرار المادية المكلفة للغاية في مجال إنتهاك البيانات والتي قد تطال الشركات التجارية بسهولة كون تشريع هذا القانون يعزز ثقافة الامن السيبراني مما يزيد الوعي لديها بضرورة أخذ الحيطة والحذر لتأمين الوسط الذي تمارس نشاطها من خلاله[٥].

---

(1) Bahaa Eltahawy, op.cit, p8.

(٢) نجد ان المادة (٨٣) من اللائحة الأوروبية العامة لحماية البيانات (GDPR) قد نصت على فرض الغرامات على كل شخص يخالف الأحكام الواردة في بنود اللائحة.

(3) Bahaa Eltahawy, Duong Dang. Understanding Cyberprivacy: Context, Concept, and Issues, 17th International Conference on Wirtschaftsinformatik (WI22) At: Nuremberg, Germany, (2022), p8.

(٤) صدام فيصل كوكز، مصدر سابق، ص ٢٣٣.

(5) Bahaa Eltahawy, Ibid, p13.

ومن الممكن أن يؤدي تنفيذ اللائحة العامة لحماية البيانات إلى زيادة الإقبال على عقود التأمين من المخاطرالسيبرانية. إلا أن التأثير حتى الآن يعتبر متواضعاً بعض الشيء بالنسبة للشركات التجارية المتوسطة والصغيرة، إلا ان هذه اللائحة أو أي تنظيم قانوني يتعلق بالمخاطر السيبرانية سيعمل أولاً وقبل كل شيء على كسر الجمود لمخاطبة الشركات التجارية حول المخاطر السيبرانية التي تحيط بالبيئة التجارية في الوقت الحالي، وكنتيجة لذلك سيتم إدخال التأمين من المخاطر السيبرانية، كما من المتوقع ان تؤثر اللائحة أيضاً على السوق، حيث أن الشركات التي تمتثل للقوانين المتعلقة بالأمن السيبراني وحماية البيانات ستكون مرتبطة بمخاطر سيبرانية أقل من غيرها، مما يؤدي بالتالي إلى تخفيف الأعباء والمسؤوليات التي من المتوقع أن تتحملها شركات التأمين من المخاطر السيبرانية[١].

وتجدر الإشارة إلى أن الاجراءات المتبعة في حل نزاعات التأمين ضد المخاطر السيبرانية تختلف عن تلك المتبعة في حل نزاعات التأمين التقليدية من ناحيتين رئيسيتين: الأولى هي أن نزاعات التأمين محل البحث تتطلب توفر خبرة تقنية وقانونية من نوع خاص يجب توافرها لدى المعنيين في الدعاوى الناشئة عن هذا العقد، كما أن تكاليف الدفاع مرتفعة نسبياً مقارنة بتكاليف دفاع عقود التأمين التقليدية بالإضافة إلى أن حجم الخسائر كبير مما يتطلب خبرة كافية لإحتسابها بدقة ومن ثم التعويض عنها. اما الناحية الأخرى فهي ان منازعات التأمين ضد المخاطر السيبرانية غالبا ما تتطلب مختصين في مجال القانون الدولي الخاص نظراً لإن احتمالية وجود تنازع في الاختصاص القانوني والقضائي واردة في هذا النوع من التأمين[٢].

وإزاء عدم وجود قانون خاص بالتأمين من المخاطر السيبرانية في العراق يثار التساؤل حول نطاق تطبيق اللائحة العامة لحماية البيانات (GDPR) على عقد التأمين من المخاطر السيبرانية؟ فهل يمكن أن تطبق في العراق أو في الدول الأخرى خارج الإتحاد الأوروبي أم أن تطبيقها ينحصر بدول الإتحاد الأوروبي؟

للإجابة على هذا التساؤل يتحتم علينا الرجوع إلى نصوص اللائحة، فقد أشارت المادة (٢) منها إلى عدم قابلية نصوص اللائحة للتطبيق على اي نشاط يقع خارج نطاق الاتحاد الأوروبي كقاعدة

(1) Even Langfeldt Friberg op.cit p70.
(2) Franke Ulrik, Meland Per Håkon, op.cit, p5.

عامة وأكدت على ذلك المادة (٩٩) حيث قررت إلزامية هذه اللائحة وقابليتها للتطبيق المباشر على جميع الدول الأعضاء إعتباراً من ٢٥ مايو ٢٠١٨، لكن نجد أن المادة (٣) قد حددت النطاق الاقليمي للائحة حيث أشارت إلى الزامية تطبيق أحكامها عند معالجة البيانات الشخصية أو التحكم بها من قبل أي مؤسسة تمارس نشاطها في الإتحاد الاوروبي بغض النظر عما إذا كانت المعالجة تمت في داخل الإتحاد أو في دولة أخرى خارج الإتحاد، كما تنطبق على المؤسسات التي تتعامل بالبيانات التي يتعلق موضوعها بالإتحاد الأوروبي حتى وإن كانت المؤسسة خارج الإتحاد، كما تنطبق أحكام اللائحة على معالجة البيانات الشخصية من قبل المؤسسات غير المنصوص عليها في الإتحاد الأوروبي لكن عملية المعالجة تمت في مكان ينطبق فيه قانون أحد الدول الأعضاء بموجب قواعد القانون الدولي العام. وهذا يعني أن اللائحة تطبق على جميع المواطنين الأوروبيين بغض النظر عن مكان تواجدهم، كما أنها تطبق على أي جهة أو مؤسسة تتعامل أو تتحكم ببيانات مواطنين أوروبيين، أو أي جهة تقع خارج الإتحاد الأوروبي لكنها تعالج البيانات الشخصية داخل الإتحاد الاوروبي.

ولذلك نعتقد أن نطاق تطبيق اللائحة وفقاً للنصوص أعلاه هو نطاق واسع ومرن، بسبب صياغة نصوص اللائحة التي تحتمل أكثر من تأويل، فمن الممكن تطبيق أحكامها على أي شركة تؤمن من المخاطر السيبرانية في أي دولة كانت، طالما أن مركز نشاطها في الإتحاد الأوروبي أو أنها تتعامل في بيانات شخصية تتعلق بالإتحاد الأوروبي _ مع الأخذ بنظر الإعتبار عدم وجود معيار يحدد مدى صلة البيانات الشخصية التي تعالجها شركات التأمين بالاتحاد الاوروبي أو ان عملائها في الاتحاد الاوروبي أو أن عملية معالجة البيانات تتم في الإتحاد الإوروبي.

ومع ذلك نعتقد أن العديد من الدول قد بادرت بمحاولات لتشريع القوانين المتعلقة بالأمن السيبراني وحماية الخصوصية وحماية الملكية الفكرية الرقمية وصدور اللائحة العامة لحماية البيانات وأن هذه المحاولات هي دليل على النقص التشريعي وعدم كفاية القواعد العامة التقليدية للتأمين لأن تحكم عقود التأمين من المخاطر السيبرانية والحاجة لوجود تنظيم قانوني متكامل للتأمين من المخاطر السيبرانية.

الأمر الذي دفع البعض إلى القول بضرورة التدخل الحكومي بسوق التأمين من المخاطر السيبرانية، من خلال الشراكة بين القطاعين العام والخاص، و هذا التدخل له ما يبرره بسبب إخفاق هذا التأمين في تحقيق التوقعات، فقد تتدخل الحكومات عند نضوج السوق وتراكم البيانات الإكتوارية

كجهة إعادة تأمين ، مع الأخذ بنظر الإعتبار إرتباط تواتر وشدة الخسائر على قطاع الأعمال ونوع التهديد السيبراني بإنتهاكات البيانات والكشف غير المصرح به عن البيانات، و ممارسات الإبتزاز السيبراني والتصيد والإنتحال وممارسات الهندسة الاجتماعية(١).

وتجدر الإشارة إلى أن وجود تشريعات خاصة بعقود التأمين من المخاطر السيبرانية من شأنها أن تؤدي إلى نمو هائل في السوق ورفع الطلب للتأمين من هذا النوع الجديد من المخاطر، فوجود تشريعات تنظم التكلفة المالية للمخاطر السيبرانية يمثل أحد عوامل زيادة الطلب على التأمين كما هو الحال في كاليفورنيا حيث تم تشريع قانون خاص بالإخطار الإلزامي عن خرق البيانات في العام ٢٠٠٣(٢)، والذي أدى إلى تشجيع الشركات التجارية الطلب المبكر على التأمين من مخاطر الإنترنت، وتؤدي اللائحة العامة لحماية البيانات دوراً مهما في زيادة نمو سوق التأمين السيبراني كونها تتضمن الإلتزام بالإخطار بالخرق في غضون (٢٤) ساعة حيثما كان ممكناً ، وفرضت العقوبات والغرامات عند عدم تنفيذ هذا الالتزام، إلا أن تأثير اللائحة على نمو السوق قد لا يرقى إلى مستوى التوقعات كون الغرامات والعقوبات غير قابلة للتأمين فالتكلفة المالية للمخاطر السيبرانية يجب أن تكون قابلة للتأمين لكي يقابلها زيادة الطلب على التأمين(٣). بالإضافة لما سبق يمكن أن تساهم الحكومات في نمو سوق التأمين من خلال تشريع قانون يلزم المؤسسات الحكومية بالتأمين من المخاطر السيبرانية أو من خلال إلزام الشركات بالتأمين من هذا النوع من المخاطر لتكون له الأفضلية بالعقود الحكومية. وقد تمارس الحكومات دوراً أقوى ، فقد تجعل التأمين من المخاطر السيبرانية الزامياً من خلال تشريع قانون يلزم المعنيين من الأفراد والشركات بالتأمين من تلك المخاطر، كما هو الحال في بعض المخاطر التقليدية كالتأمين من حوادث السيارات الذي يكون إلزامياً في بعض البلدان؛ لكن عملية تشريع قانون إلزامي للتأمين من المخاطر السيبرانية ليس بالأمر السهل، فمن شأنه أن يزيد العبء ويثقل كاهل شركات التأمين والعملاء على حد سواء فقد لا يتمكنون من تحمل تكاليفه الباهظة(٤).

(1) Pavel V Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, Stefan Trück The nature of losses from cyber-related events: risk categories and business sectors, Journal of Cybersecurity, Volume(9), Issue (1), 2023, p3.

(2) Data Security Breach Reporting / State of California NO. S.B. 1386،signed into law September 25, 2002, Effective July 1, 2003.

(3) Mark Camillo, op.cit, p57.

(4) Daniel Woods, Andrew Simpson, op.cit, p214.

ونتفق مع عدم جعل التأمين من المخاطر السيبرانية إلزامياً على جميع الشركات التجارية، فالشركات الصغيرة والمتوسطة هي المتضرر الأول من ذلك؛ لأن أسعار التأمين الباهظة قد تشكل عائق رئيسي أمامها، أما الشركات الكبيرة فقد تضرر هي الأخرى من التأمين الإلزامي حيث إن حجم الشركة الكبير يجعلُ الأمر معقداً من ناحية توفير البيانات المطلوبة للتعاقد والإمتثال لإجراءات ما قبل التعاقد المكلفة نسبياً كإتخاذ وسائل وإحتياطات الأمن السيبراني، لذا يمكن أن يكون الحل الأقرب للواقعية هو تشريع قانون خاص بذلك يلزم أشخاص محددين بوجوب التأمين ضد المخاطر السيبرانية كالمؤسسات الحكومية أو الشركات المختلطة أو المصارف. فالغالب أن هذه الأطراف هي الأكثر حاجة للتأمين من المخاطر السيبرانية لكبر حجمها ولتماسها مع الامن القومي كون الدولة طرف فيها كما أنها قادرة على تحمل تكلفة هذا النوع من التأمين.

الفرع الثاني

صعوبة صياغة عقود التأمين من المخاطر السيبرانية

إنّ السمة المميزة لعقود التأمين من المخاطر السيبرانية هي (التعقيد)؛ لأن صياغة بنود هذا العقد مقارنة بعقود التأمين من المخاطر التقليدية تعتبر أكثر طولاً وتعقيداً[1] ،و يعدّ من ضمن التحديات التي تواجهها شركات التأمين الراغبة بالتعامل في عقود التأمين من المخاطر السيبرانية هو إنشاء نماذج هذه العقود التي سيتم من خلالها وضع الإطار العام لطبيعة التغطية و تحديد نطاقها لكي يتم من خلالها معرفة حقوق وواجبات كلا الطرفين حين إبرام التعاقد، وهو أمر بالغ الدقة، حيث أن العقد يمثل أساس العلاقة القانونية بين أطرافه ، فالقاعدة العامة هي أن العقد شريعة المتعاقدين خصوصاً أن هذا النوع من العقود لم يتم تنظيمه بشكل خاص من قبل المشرعين حيث سيكون العقد بمثابة القانون الذي يتحتم على طرفيه السير وفق أحكامه، وهذا الأمر يمثل تحدياً له ثقله من الناحية القانونية في إعتقادنا، لا سيما و أن هذا النوع من التأمين كما ذكرنا جديد من نوعه، فلا توجد خبرة قانونية كافية لدى المختصين في شركات التأمين لكتابة هكذا عقود غير تقليدية ، كما أن قلة توفر نماذج لعقود التأمين من المخاطر السيبرانية يزيدُ الأمر صعوبةً.

(1) Tsohou A, Diamantopoulou V, Gritzalis S, Lambrinoudakis op.cit, p743.

فكل شركة تأمين تتخذ نهجها الخاص عند إعداد نماذج العقود ، حيث يختلف تفسير المصطلحات القانونية الواردة في العقد بين شركة وأخرى بالإضافة إلى تضمين العقود بعدد من الإستثناءات مما يصعب من مهمة الشركات الصغيرة والمتوسطة – غير المطلعة نسبياً – في إتخاذ قرار الحصول على تغطية تأمينية مناسبة لها، فقد تبدو التغطية التأمينية متشابهة للوهلة الأولى لكن عند التدقيق عن كثب نجد إختلافات كثيرة بين شركات التأمين من حيث السعر و مدى التغطية والخصومات والإمتيازات إن وجدت، الأمر الذي يستوجب من شركات التأمين من المخاطر السيبرانية توخي الدقة في صياغة بنود العقد(١)، حيث أن فهم ما تتضمنه عقود التأمين من حدود للتغطية هو أمر ضروري بالنسبة للشركات التجارية حيث تساعد اللغة الواضحة للعقد الخالية من التعقيد إلى تحفيز العملاء في إتخاذ قرارهم بالتأمين من المخاطر السيبرانية خصوصاً أن هذا القرار ذي تبعات مالية كبيرة، فعلى شركات التأمين أن تأخذ بنظر الإعتبار عند عمل نماذج التغطية الخاصة بالتأمين من المخاطر السيبرانية الطبيعة العالمية لهذا التأمين، لأن كتابة شركة التأمين لهذه العقود تتطلب منها التركيز على كلا الصعيدين الوطني والدولي المتصل بالعقد ليتم تحديد الضوابط التي تحكمه بصورة دقيقة، على عكس عقود التأمين التقليدية التي قد لا تحتاج في الغالب إلى وجود هذا الأمر عند كتابة عقودها(٢).

لقد تأثرت شركات التأمين من المخاطر السيبرانية عند صياغتها لعقود التأمين بطبيعة تلك المخاطر، مما أدى إلى وجود حالة عدم يقين قانوني أثرت على على كتابة عقود التأمين من جوانب متعددة:

الجانب الأول هو وجود حالة عدم يقين قانوني لدى العملاء حول ما إذا كانت شركة التأمين ستغطي بعض الأضرار الناجمة عن الخطر السيبراني الذي لحق بالشركة التجارية المؤمن لها أم لا مثل إنخفاض قيمة العلامة التجارية أو السهم أو زيادة تدقيق الراغبين بالإستثمار في الشركة المعنية أو إنخفاض الإيرادات أو فقدان ثقة العملاء. **الجانب الثاني** هو وجود حالة عدم يقين قانوني من قبل شركات التأمين ذاتها حيث يفتقر التأمين من المخاطر السيبرانية إلى وجود السوابق القضائية التي تسهم في زيادة وعيها حول سياسات السوق، وحل التساؤلات التي قد تساعد هذه الشركات عند كتابة

(1) Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, op.cit, p 400 .
(2) Florian Schütz, Florian Rampold, Andre Kalisch, Kristin Masuch, op.cit, p522.

عقودها، فعلى سبيل المثال لا تزال المحاكم مترددة فيما يتعلق بخروقات البيانات، على الرغم من أن سرقة البيانات يعد ضرر ناجم عن خطر سيبراني إلا أن القضاء منقسم حول ما إذا كان ضحايا سرقة البيانات لا يمتلكون الصفة في الدعوى في حالة عدم وجود إحتيال أو سرقة فعلية للبيانات، في حين تتجه محاكم أخرى إلى وجود الصفة في رفع الدعوى بمجرد وجود خطر إساءة استخدام البيانات الناتج عن الخرق. وتبرز أهمية عدم اليقين القانوني لدى شركات التأمين السيبراني بشأن قضايا خرق البيانات لأنه يؤثر بصورة مباشرة على إحتمالية دفع مطالبات جديدة للمتضررين من الخرق مما يستتبع تأثير هذه المطالبات على عملية تسعير الأقساط التأمينية(١).

وفي ضوء ما تقدم؛ قد ينتج عدم اليقين تجاه شركات التأمين بسبب عملها وفق أحكام السوق غير المعتمدة قانوناً، حيث أن هناك تمييز بين تنظيم التأمين في السوق المعتمد والسوق غير المعتمد، حيث يجب على شركات التأمين أن تلتزم بالعمل وفق المعمول به بالأسواق المعتمدة أو المقبولة قانوناً، وأن تلتزم بتقديم عقودها إلى لجان التأمين الحكومية والإلتزام بجميع القوانين واللوائح للحصول على ترخيص بالعمل. لكن قد يحدث أن تتجاهل شركة التأمين هذه الإلتزامات والقيود القانونية التي يفرضها مفوضو التأمين وأن تلجأ إلى بيع التأمين في سوق غير معتمدة من قبل الدولة يطلق عليها إسم (خطوط التأمين الزائدة او الفائضة) ووجد المختصون في مجال التأمين من المخاطر السيبرانية أن هنالك العديد من الشركات التي تعمل في هكذا سوق غير مصرح به، حيث قدرت (NAIC)(٢) ان (1.8) مليون دولار من الأقساط السنوية المدفوعة لشركات التأمين تمت في هذه الاسواق غير المعترف بها قانوناً(٣).

وعلى كل حال فإن وجود حالة عدم اليقين القانوني يؤدي إلى نتيجة ذات أثر عكسي على شركات التأمين، حيث يؤدي بها إلى زيادة أسعار التأمين بسبب إفتقارها إلى المعلومات والبيانات

(1) Andrew Granato, Andy Polacek, op. cit, p 4.

(٢) توفر الرابطة الوطنية لمفوضي التأمين (NAIC) الخبرة والبيانات والتحليلات لمفوضي التأمين لتنظيم الصناعة بشكل فعال وحماية المستهلكين. تأسست في عام ١٨٧١، وهي منظمة وضع المعايير الأمريكية يحكمها كبار منظمي التأمين من ٥٠ ولاية، ومقاطعة كولومبيا، وخمسة أقاليم أمريكية لتنسيق تنظيم شركات التأمين متعددة الدول انظر:
https://content.naic.org/about
تاريخ الزيارة ٢٠٢٣/٥/١ الساعة ١٢:٠٠م.

(3) Sasha Romanosky and others, Content analysis of cyber insurance policies: how do carriers price cyber risk?, op. cit, p 3.

المتعلقة بالمخاطر السيبرانية المحدثة بصورة مستمرة و التي تحتاجها عند كتابة عقودها، فلا تستطيع تقديم تغطية تأمينية ضد المخاطر السيبرانية التي قد تواجه الشركات التجارية و بأسعار معقولة إذا كانت البيانات المتعلقة بالخطر المؤمن منه قليلة مما يؤدي إلى عدم وجود منافسين في السوق كون شركات التأمين من المخاطر السيبرانية لا تزال قليلة ولا تخلق جواً من المنافسة يفضي إلى خفض التكلفة في السوق(١).

وقد تؤدي قلة الخبرة القانونية في مجال كتابة عقود التأمين السيبراني إلى خسارة شركة التأمين، بسبب التسرع في كتابة بنود العقد، فقد تغفل شركة التأمين النص على ضرورة بذل عناية أمنية معينة بعد إبرام العقد بينها وبين الشركة التجارية مما يؤدي إلى ممارسة الاخيرة لسوك احتيالي يتمثل ببذل عناية أقل في مجال الأمن السيبراني الخاص بها كونها قد سبق وأن أمنت على الاضرار الناجمة عن المخاطر السيبراني في حال تعرضها لهجمات سيبرانية، فمراقبة شركة التأمين للعميل أمر مكلف وغير مستساغ لدى العملاء، لذلك لابد لشركة التأمين أن تتدارك هذا الإحتمال من خلال النص على درجة العناية الواجب إتباعها في مجال الأمن السيبراني من قبل الشركة التجارية الراغبة بالتأمين(٢).

ويشكّل إنعدام اللغة الموحدة لعقود التأمين من المخاطر السيبرانية وغموض بنود العقد وعدم إتفاق شركات التأمين غالباً على ما تغطية من مخاطر، عاملاً مساعداً في بطئ تطور سوق التأمين السيبراني حيث يؤدي ذلك إلى حصول إختلاف في الآثار المترتبة على تحقق الخطر من شركة إلى أخرى، مما من يزيد صعوبة كتابة عقود تأمين من المخاطر السيبرانية بصيغة موحدة في المستقبل(٣).

ولا تزال شركات التأمين بصورة عامة غير مستقرة على ما يجب إستبعاده من الخسائر وهذا بدوره يؤدي إلى عدم وجود تناسق بين عقود شركات التأمين من المخاطر السيبرانية المختلفة وحدوث نزاعات قضائية عديدة، فعقود التأمين من المخاطر السيبرانية تتضمن بصورة عامة الخسائر التي سيتم تغطيتها من قبل شركة التأمين بالإضافة إلى الخسائر المستبعدة. ووجد الباحثون في هذا المجال أن الخسائر المغطاة قد لا تشكل تحدياً في عقود التأمين مقارنة بالإستثناءات الواردة فيها، حيث إن أغلب

(١) محمد سعيد اسماعيل، مصدر سابق، ص ٢٢٤.

(٢) محمد سعيد اسماعيل، مصدر سابق، ص٢٢٤.

(3) Sasha Romanosky and others, Content analysis of cyber insurance policies: how do carriers price cyber risk?, op. cit, p 1.

عقود التأمين متفقة على الخسائر التي تتم تغطيتها بموجب عقودها بينما كان التنوع واضح في الخسائر غير المغطاة بين شركة وأخرى(١).

و فضلاً عما سبق ذكره ، قد يؤدي غموض لغة عقود التأمين من المخاطر السيبرانية إلى تردد الشركات التجارية في شراء تغطية تأمينية تناسبها الأمر الذي يؤدي إلى عدم حصول العملاء على التعويضات نتيجة لصياغة بنود العقد بطريقة غامضة تمكن شركات التأمين في الغالب من التنصل من إلتزاماتها تجاه العميل(٢).

وفي إعتقادنا أن هذا الغموض في لغة عقود التأمين من المخاطر السيبرانية قد تتعمد وجوده البعض من شركات التأمين، فغالباً ما يتم إستغلال الشركات التجارية طالبة التأمين وإيهامها من خلال أسلوب صياغة بنود العقد بإمكانية شمول عدد معين من المخاطر السيبرانية بالتغطية، فيتم التعاقد على هذا الأساس بسبب أن العميل كان يعتقد انها تندرج ضمن التغطية نتيجة قلة خبرته في هذا المجال ليتفاجئ بعد تحقق الخطر السيبراني بعدم إمكانية إستحصال مبلغ التأمين كون الخطر السيبراني المتحقق غير منصوص عليه بصورة صريحة في بنود العقد.

---

(١) مثال على ذلك قامت شركة Mondelez International – الشركة متعددة الجنسيات للأغذية والمشروبات – بتسوية الدعوى القضائية ضد شركة التأمين التابعة لها Zurich American Insurance Company بسبب مزاعم= =بأن زيورخ رفضت تغطية نفقات Mondelez التي تزيد عن ١٠٠ مليون دولار بعد التعطيل. هجوم إلكتروني من برمجيات الفدية عانى منه في عام ٢٠١٧. ففي يونيو ٢٠١٧، أصبحت Mondelez ضحية لهجوم NotPetya ransomware عندما أصبح حوالي ١٧٠٠ من خوادمها و ٢٤٠٠٠ من أجهزة الكمبيوتر المحمولة الخاصة بها غير قابلة للاستخدام من قبل البرامج الضارة. بالإضافة إلى فقدان الأجهزة، عانت الشركة أيضًا من اضطرابات في قنوات التوريد والتوزيع، وفقدان ثقة العملاء بسبب الطلبات التي لم يتم الوفاء بها، وحتى سرقة بيانات الاعتماد من عدة مستخدمين. ومع ذلك، أشارت شركة التأمين التابعة لشركة Mondelez في زيورخ في عام ٢٠١٨ إلى أنه سيتم رفض تغطية أكثر من ١٠٠ مليون دولار من نفقات التعافي من الهجمات الإلكترونية بسبب بند استثناء الحرب، حيث يشتبه بشدة في أن NotPetya هي حملة فدية برعاية الدولة من روسيا. أدى ذلك إلى قيام شركة الأغذية العملاقة بمقاضاة شركة التأمين للمطالبة بالإعفاء من انتهاكاتها للالتزامات التعاقدية، وادعاء أن زيورخ أخفقت في الوفاء بوعودها. وتم اعتبار القضية منذ ذلك الحين كمثال على الفجوة المحتملة في السياسات السيبرانية. انظر:

Case No. 2018-L-11008 (Ill. Cir. Ct. Oct. 27، 2022)
https://www.scribd.com/document/397265756/Mondelez-Zurich
date of visit 23/12/2023 7:00pm.

(2) Julie Bernard, op. cit, p7.

وعلى كل حال نعتقد أن التباين الكبير في عقود التأمين من المخاطر السيبرانية ينعكس سلباً على نمو سوقه، حيث أن الشركات التجارية قد تفضل عدم شراء تغطية تأمين من المخاطر السيبرانية لشركة تأمين معينة إعتقاداً منه انها تستبعد تغطية ذات المخاطر التي إستثنتها شركة أخرى من أحكام العقد مما يؤدي إلى فوات المنفعة للعديد من الشركات. لذا نعتقد أن عدم إتفاق الشركات على نماذج موحدة أو ذات عوامل مشتركة على الأقل يؤدي إلى انفرادها بتسعير منتاجاتها التأمينية والمبالغة في تحديد أقساطها لعدم وجود ضابط محدد أو عرف مهني ثابت يحكم هذه العقود. فالطرف المتضرر هنا بالدرجة الأساس هي الشركة التجارية طالبة التأمين، والتي قد تكون غير قادرة على تحمل تكلفة هذا التأمين أو شروط المؤمن، فهي أمام خيارين لا ثالث لهما، إما أن تذعن لبنود العقد المجحفة أو أن تبقى بلا تأمين فتتحمل الخسارة بمفردها.

ومن المعوقات التي تواجه نمو سوق التأمين من المخاطر السيبرانية كذلك هو وضع شركات التأمين ضمن بنود العقد العديد من الشروط الصارمة للتعاقد مع الشركات التجارية طالبة التأمين مما قد يشكل عائقاً أمام رغبة هؤلاء العملاء بالإقدام على شراء تغطية التأمين من المخاطر السيرانية، حيث يجدون صعوبة حقيقة في الحصول على مطالباتهم عند تحقق الخطر المؤمن منه، مما يثير حفيظتهم عن مدى جدوى هذا التأمين وهل سيكون كافياً لتدارك نتائج الخطر السيبراني أم لا. ومن شأن هذه التساؤلات أن تعيق نمو سوق التأمين محل البحث على المدى القصير على أقل تقدير، كما أن من شأن هذه الاحكام والشروط الصارمة في العقد أن تؤدي إلى منازعات قضائية عديدة بين شركات التأمين وعملائها، أو اللجوء إلى اتخاذ اجراءات رقابية صارمة بحقهم من قبل الجهات الرقابية المختصة في الدولة[1].

وتجدر الإشارة إلى أن الطبيعة السريعة والمتغيرة للخطر السيبراني المؤمن منه، تعدّ معوقاً أساسياً عند كتابة عقود التأمين المتخصصة، حيث أنه من المهم أن تحتوي عقود التأمين من المخاطر السيبرانية على بنود تغطية دقيقة للغاية من أجل ضمان الأمن القانوني وتجنب التفسير الخاطئ. وفي الوقت نفسه، يمكن لصياغة هذه العقود والإستثناءات المتعددة الواردة فيها أن تحد من قابلية تطبيق بنود التأمين. ولا تزال العقود المعروضة في سوق التأمين من المخاطر السيبرانية تنحرف عن المستوى المطلوب مقارنةً بعقود التأمين التقليدية حيث أن الاولى لها سقف منخفض نسبياً بالنسبة للمطالبات

(1) Henry R K Skeoch, Christos Ioannidis, op. cit, p3.

الناتجة عن الحوادث السيبرانية فلا يزال هناك مطالبات كثيرة للمؤمن له تم استبعادها في العقد و عليه تحملها وحده[١].

ويشدد القضاء فيما يتعلق بعقود التأمين من المخاطر السيبرانية على أهمية العقود ذات اللغة الواضحة والتغطيات الملائمة حيث يمكن أن يساعد وجود عقود تأمين سيبراني بصيغة ثابتة على تقليل النزاعات مما يوفر الوقت والجهد على جميع الأطراف سواء أكانوا المتعاقدين ام الغير ام السلطات القضائية ، لكن في الوقت ذاته لا ننكر فوائد العقود التي يتم تصميمها لكل عميل على حدىً، حيث تتصف بالمرونة التي تجاري طبيعة الخطر المتغيرة وحجم الشركة التجارية طالبة التأمين و طبيعة نشاطها ضمن الفضاء السيبراني ومدى إلتزامها بمتطلبات الأمن السيبراني، مما يؤدي إلى جعل اقساط التأمين تتلائم ومستوى الأمن السيبراني في الشركة التجارية ونتيجة لذلك سنجد أن علاقة القسط بمستوى الامن هي علاقة عكسية، فكلما قلت إجراءات الأمان المتخذة كلما زاد القسط[٢].

وفي إعتقادنا أن عقود التأمين من المخاطر السيبرانية سواء أكانت تحتوي على بنود ثابتة تطبق على جميع العملاء دون استثناء، ام كانت عقود ذات بنود مرنة – بحيث يتم تخصيص العقد لشركة تجارية طالبة التأمين دون الشركات الاخرى– لها مميزات وعيوب ، فالقول بضرورة أن تعمم جميع نماذج العقود على جميع العملاء ودفعهم ذات القسط بغض النظر عن حجم الشركة العميلة أو موظفيها او كم البيانات التي تتعامل به هو أمر مجافي للعدالة ، فعلى الرغم من سهولة العمل بهذه العقود بالنسبة لشركات التأمين بسبب توفيرها الوقت والجهد اللازمين للحصول على البيانات الخاصة بكل عميل على حدىً، إلا انها تبطئ من نمو سوق التأمين السيبراني؛ بسبب عزوف الكثير من الشركات التجارية الصغيرة والمتوسطة عن شراء تغطيات التأمين من المخاطر السيبرانية بسبب عدم قدرتها على توفير قيمة القسط . أما بالنسبة للعقود المرنة والتي تنفرد فيها كل شركة تجارية طالبة تأمين عن غيرها، هو أمر لا يخلو من الصعوبة، ويستنزف جهد ووقت شركة التأمين على الرغم من أنها تحدد أسعار القسط بما يتلائم مع حجم العميل ونشاطه في السوق.

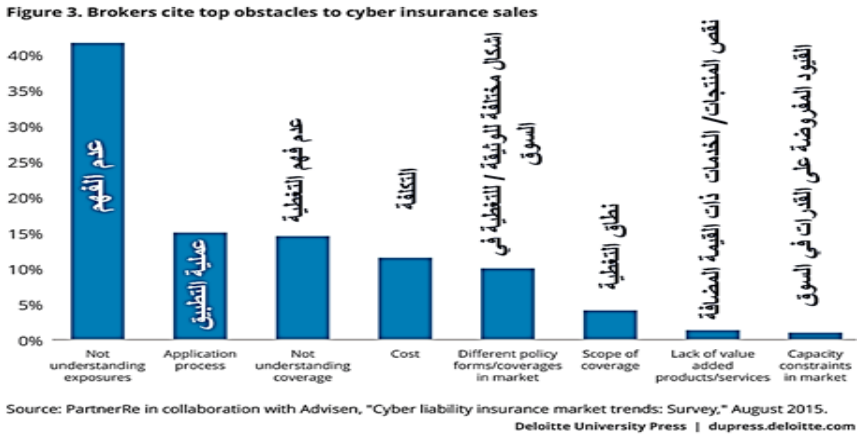
لذا نعتقد أن جمع شركة التأمين بين هذين النوعين من العقود يمثل حلاً سليماً للحصول على مزايا الطريقتين والتخلص من عيوبهما في الوقت ذاته، حيث يمكن لشركة التأمين أن تضع نماذج

(١) بغداد شامبي، مصدر سابق، ص٢٥٦.

(2) Bob de Waard, Bernold Nieuwesteeg, Louis Visscher, op.cit, p22.

عقود ثابتة لكل فئة محددة من الشركات، فعلى سبيل المثال تقوم شركة التأمين بتصنيف عملائها بطريقة تؤدي إلى شمول كل فئة منهم بنموذج عقد ذي بنود ثابته تتشابه مع الشركات التي هي من ذات التصنيف، فقد يكون التصنيف بناء على حجم الموظفين أو طبيعة النشاط أو حجم رأس المال أو مدى الإعتماد الكلي أو الجزئي على العمل في الفضاء السيبراني..الخ.

ولا تزال التغطية من المخاطر السيبرانية المتاحة في سوق التأمين بعيده عن النموذجية، نتيجة لإجراءات التعاقد المعقدة والتي تستهلك وقتاً طويلاً، كما توجد مجموعات متميزة من عقود التأمين من هذا النوع من المخاطر إلا أنها تختلف من ناحية المصطلحات والشروط من شركة تأمين لأخرى ومن وثيقة لأخرى من قبل الشركة ذاتها مما يستدعي الإهتمام الدقيق بالعقود وإعادة النظر فيها لإستبعاد المثالب سالفة الذكر[1].



(عدم فهم المخاطرالسيبرانية) ٤٠% ، (صعوبة التطبيق العملي) ١٦% ، (عدم فهم التغطية) ١٧% ، (إرتفاع التكلفة) ١٠%، (إنعدام وجود نماذج موحدة للتأمين) ٩% ، (عدم تحديد نطاق التغطية)٥% ، (نقص الخدمات السيبرانية) ٢% ، (القيود المفروضة على قدرة الشركة)١%

(رسم بياني يوضح تحديات نمو سوق التأمين من المخاطر السيبرانية)

(1) Franke Ulrik, Meland Per Håkon, op.cit, p3.

الخاتمة

الخاتمة

توصلنا من خلال البحث في موضوع الحماية التأمينية للشركات التجارية من المخاطر السيبرانية إلى جملة من الإستنتاجات والمقترحات وعلى النحو الآتي:

أولاً: الإستنتاجات

١- الخطر السيبراني هو خطر غير مادي أو (غير ملموس) يصيب أنظمة تشغيل الشركات التجارية التي تمارس أعمالها في الفضاء السيبراني، ويلحق اضراراً مادية ومعنوية قد تتعدى حدود الدولة التي وقع فيها الضرر. ويتميز بالحداثة مقارنة بأنواع المخاطر التقليدية المراد التأمين منها كونه أحد آثار التطور التكنولوجي في الوقت الحاضر.

٢- لا يوجد لحد الآن تعريف تشريعي أو قضائي له، على الرغم من وجود بعض المحاولات من الفقه القانوني لتعريفه بصورة تحدد معالمه وتزيل الغموض الذي يكتنفه، لا سيما و أن مصطلح السيبرانية هو مصطلح غربي ولا يوجد ما يقابله في اللغة العربية الفصحى لذا تم تعريبه ودرج إستخدامه في جميع المحافل الدولية والتشريعات القانونية ذات الصلة.

٣- يعدّ مصطلح الخطر السيبراني شاملاً لكل من الجريمة السيبرانية والهجمة السيبرانية، على الرغم من وجود إختلاف جوهري في مفهوم المصطلحين الآخيرين، فالجريمة السيبرانية تقع على الأفراد وتهدف لتحقيق غايات شخصية، أما الهجمة السيبراني فتتجه ضد الدولة لتحقيق غايات غالباً ما تكون سياسية أو إقتصادية.

٤- للخطر السيبراني أنواع عديدة ومتطورة إلا أن أكثرها إنتشارًا في الواقع العملي هي: خطر الفيروسات والقرصنة الإلكترونية وبرامج الفدية والهندسة الاجتماعية وسرقة البيانات. ولهذه المخاطر عواقب مدمرة للشركة التجارية، فبغض النظر عن الإلتزامات المالية المترتبة على عاتق الشركة التجارية نتيجة لإنتهاك معايير الأمن السيبراني والذي يؤدي لسرقة بياناتها أو تعطيل نظام التشغيل فيها مثلاً بسبب أحد هذه المخاطر السيبرانية، فإن لهذه المخاطر آثار وخيمة على السمعة التجارية لهذه الشركات مما يسبب فقدان ثقة العملاء.

٥- إن الخطر في عقد التأمين من المخاطر السيبرانية له خصوصية مقارنةً بباقي أنواع المخاطر في عقود التأمين التقليدية، فالخسارة اللاحقة بالشركات التجارية (المؤمن لها) نتيجة تعرضها لأحد المخاطر السيبرانية يضاهي الخسارة الناجمة عن الكوارث الطبيعية لذا فهو (خطر كارثي) ذي طبيعة (مترابطة) يحقق ضرراً (غير ملموساً) يصعب تقييمه عادةً.

٦- ليس كل خطر سيبراني هو خطر قابل للتأمين منه، فغالباً ما تتضمن وثيقة التأمين أنواع محددة من المخاطر التي من الممكن للشركات التجارية التأمين منها في حين تستثني أخطاراً أخرى من عملية التأمين كهجمات الفدية والحروب السيبرانية، وغالباً ما يقتصر الخطر السيبراني الممكن التأمين منه بتلك الاخطار التي تصيب المكونات غير الملموسة لأنظمة تشغيل الشركة التجارية مع إمكانية التأمين على المكونات المادية للنظام. إلا أن شركات التأمين وفي ظل غياب التشريعات المنظمة للتأمين من المخاطر السيبرانية تنفرد في تحديد المخاطر السيبرانية التي يمكن التأمين منها، وتلك التي لا يمكن التأمين منها.

٧- تتميز عقود التأمين من المخاطر السيبرانية عن باقي عقود التأمين التقليدية بكونها معقدة من الناحية الفنية و مرتفعة الاقساط نسبياً و تتطلب شروطاً محدده تسبق عملية التأمين فلا يمكن لشركة التأمين من الخاطر السيبرانية قبول طلب التغطية المقدم من قبل شركة تجارية ما لم يتمتع نظام تشغيل هذه الشركة بمستوى محدد من الأمن السيبراني كما ان مرحلة التعاقد تتضمن الابقاء على إجراءات الأمن السيبراني هذه والتشديد منها كلما كانت الشركة التجارية المؤمنة معرضة للمخاطر السيبرانية بصورة أكبر مما هو عليه في مرحلة قبل التعاقد.

٨- تتسم عقود التأمين من المخاطر السيبرانية بالغموض، كما تحتوي على مصطلحات واسعة ومرنة نظراً لحداثة الأخطار المؤمن منها، مما يتيح سهولة التنصل من الإلتزامات التعاقدية بحجة غموض المصطلحات الواردة ضمن بنود العقد، فالشك يفسر دائماً لمصلحة المدين بالإلتزام.

٩- إن عقود التأمين من المخاطر السيبرانية لا تستوجب بالضرورة أن يتم إبرامها من قبل شركات متخصصة بالتأمين من المخاطر السيبرانية، بل إن بإمكان جميع شركات التأمين بصورة عامة أن تطرح هذا النوع من الوثائق سواء من خلال تغطية خاصة بالمخاطر السيبرانية أو من خلال تغطية عامة لجميع المخاطر كوثيقة التأمين من المسؤولية المدنية.

١٠- قد يختلط مصطلح التأمين من المخاطر السيبرانية مع مصطلحات قانونية أخرى كمصطلحي التأمين الإلكتروني والأمن السيبراني لوجود بعض التشابه بينهم، ولكن الحقيقة أن عقد التأمين الإلكتروني ما هو إلا عقد تأمين يتم بوسائل إلكترونية – أي غير ورقية – وفقا لما يتطلبه قانون التوقيع الالكتروني والمعاملات الالكترونية من شروط. أما الأمن السيبراني هو إجراءات أمنية متخذه من قبل الأفراد والشركات للحماية والتقليل من أضرار المخاطر السيبرانية.

١١- يترتب على إنعقاد عقد التأمين من المخاطر السيبرانية جملة من الالتزامات المترتبة على أطرافه، قسم منها ينشأ في ذمتهم عند انعقاد العقد وقبل تحقق الخطر السيبراني كالإلتزام بأتخاذ إجراءات الأمن السيبراني طيلة فترة العقد، والإلتزام بالإفصاح عن بعض البيانات الشخصية والمالية الخاصة بالشركة المؤمن لها وموظفيها وعملائها. والقسم الآخر من هذه الإلتزامات ينشأ بعد تحقق الخطر كالإلتزام بالإعلام عن تحقق الخطر السيبراني، والإلتزام بإبلاغ الجهات المختصة في الدولة بوقوع الخطر وبخلافه ستكون الشركة التجارية ملزمة بدفع غرامات مالية.

١٢- يفرض عقد التأمين من المخاطر السيبرانية إلتزامات مالية تجاه الغير أكثر شدة مما هو عليه الحال في التأمين من المخاطر الأخرى فالضرر الناجم عن المخاطر السيبرانية يخلف في الغالب أضراراً جسيمة للعملاء وغير العملاء تكاد تفوق الأضرار التي تصيب الشركة التجارية المؤمن لها.

١٣- تلتزم شركات التأمين من المخاطر السيبرانية بالتعويض عن الضرر المادي المباشر فقط ، أما بالنسبة للأضرار المعنوية والأضرار غير المباشرة فلا يمكن التعويض عنها ، وهذا مشابه للقواعد العامة في عقود التأمين التقليدية، فلا تلتزم شركة التأمين من المخاطر السيبرانية بتعويض الغير عن الإلتزامات التعاقدية الناشئة بينه وبين الشركة التجارية المؤمن لها والتي لم يتمكن المؤمن له من الوفاء بها بسبب تحقق الخطر السيبراني المؤمن منه، أما بالنسبة للضرر المعنوي الناجم عن الخطر السيبراني والذي يلحق بالشركة التجارية أو عملائها او الغير فلا يزال القضاء متردداً بوضع مبدأ عام لقبول التعويض عنها، على الرغم من إمكانية التعويض عن الضرر المعنوي وفقاُ للائحة الأوروبية لحماية البيانات (GDPR) لسنة ٢٠١٦.

١٤- صعوبة تقدير قسط و مبلغ التأمين عند إبرام عقد التأمين من المخاطر السيبرانية نظراً للطبيعة المتغير والمتطورة للخطر السيبراني مما يسبب صعوبة تقييم هذه المخاطر أو نمذجتها، لا سيما وأن الخطر السيبراني قد يلحق الضرر بممتلكات غير ملموسة كما هو الحال عند تقدير التعويض عن سرقة البيانات أو نشرها أو سرقة الملكية الفكرية الرقمية أو فقدان السمعة التجارية..الخ.

١٥- لا تزال الأحكام القضائية المتعلقة بالتأمين بالمخاطر السيبرانية مترددة في مدى إمكانية إعتبار البيانات الخاصة بالشركات التجارية من ضمن الممتلكات المادية للشركة أم لا، لكن المشرع العراقي قد حسم الامر في قانون التوقيع الالكتروني والمعاملات الإلكترونية حين أعطى البيانات قيمة مادية وبالتالي إمكانية السماح بتقديرها ماليا والتعويض عنها. كما أن الاحكام القضائية الخاصة بالتأمين من

مخاطر الفدية لا تزال مترددة في مدى قابلية التأمين منها وبالتالي تعويض الشركات التجارية عن قيمة الفدية المدفوعة للمهاجمين من عدمها.

١٦- يفرز التعامل في عقود التأمين من المخاطر السيبرانية العديد من الإشكاليات الفنية بالدرجة الأساس والتي أعاقت عمل شركات التأمين من المخاطر السيبرانية، كإنعدام وجود سجل بيانات للخسائر التي الحقتها هذه المخاطر في المؤمن لهم والغير، وتخوف الشركات من التأمين من المخاطر السيبرانية، مما صعب من مهمة وضع أسعار التأمين من المخاطر السيبرانية وبالتالي إمكانية فشل عملية التأمين برمتها مما يعرض العديد من شركات التأمين لخطر الإفلاس بسبب سوء تقدير الضرر الناجم عن الخطر السيبراني المؤمن منه.

١٧- يترتب على عقود التأمين السيبراني عدد من التحديات القانونية كإنعدام التنظيم التشريعي للمخاطر السيبراني بصورة عامة ولعقد التأمين من المخاطر السيبرانية بصورة خاصة، والصياغة المعقدة لعقود التأمين من المخاطر السيبرانية، الأمر الذي يؤدي الى وجود صعوبة في فهمها وبالتالي تخوف الشركات التجارية من أن تصبح طرفاً في هذه العقود.

١٨- لا تزال اللائحة العامة لحماية البيانات (GDPR) ولحد الآن اللائحة التنظيمية الوحيدة التي يعزى لها الفضل في التأثير المباشر والفعال في زيادة الوعي بين الشركات التجارية – بغض النظر عن كونها معنية بحماية البيانات الشخصية للمواطنين الأوروبيين – حيث كانت بمثابة نقلة تاريخية ساهمت في تعريف الشركات التجارية بالبيانات التي تحتاج لحمايتها من المخاطر السيبرانية المنتشرة في وقتنا الحاضر وكيفية حمايتها ووضع عقوبات الرادعة على كل شركة تنتهك بنود اللائحة، مما أدى بالشركات التجارية إلى أخذ مسؤولية الأمن السيبراني في أنظمتها على محمل الجد.

١٩- لا يمكن لأي شركة تجارية تعمل ضمن الوسط السيبراني بغض النظر عن حجمها أو نوعها أن تكون بمعزل عن المخاطر السيبرانية، مهما إدعت إمتلاكها نظام أمني متكامل ضد المخاطر السيبرانية والسبب قد يعود للطبيعة المتطورة للخطر السيبراني وصعوبة السيطرة على آثاره وإن تفعيل دور الحماية التأمينية للشركات التجارية من المخاطر السيبرانية لا يعتبر مسألة إمتثال للقوانين والأنظمة بقدر ما هو وسيلة لضمان استمرارية الشركة التجارية وممارستها لنشاطها التجاري في وسط آمن ومستقر وبأقل خسائر ممكنة.

ثانياً: المقترحات:

١- نوصي المشرع العراقي بضرورة تفعيل الإستراتيجية الوطنية للأمن السيبراني والتي سبق وأن حددت إتجاهات و رؤية الأمن السيبراني في العراق، والمتمثلة بمجتمع آمن ومضمون ومرن وموثوق به يحمي الأصول والمصالح الوطنية ويعزز التفاعلات والمشاركة الإستباقية في الفضاء السيبراني بهدف تحقيق الرخاء الوطني بما يوفره من فرص ممتازة لتأمين وتنمية إقتصاد 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 الامن القومي في العراق والعالم، بإعتبار أن الفضاء السيبراني اصبح هو المجال الرابع بعد الارض والبحر والجو وفقاً للإستراتيجية الوطنية .

٢- نوصي المشرع العراقي بضرورة تشريع قانون للأمن السيبراني يحدد ماهية الخطر السيبراني وأنواعه وشروطه، مع الأخذ بنظر الإعتبار ضرورة التعريف بالإجراءات الواجبة الإتباع لتحقيق الأمن السيبراني وأن 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.

٣- 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 والردع اللازمة لحث الشركات التجارية على التعامل في بيئة تجارية آمنة.

٤- نوصي المشرع العراقي بعدم الإكتفاء 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 الإكتفاء بالقواعد العامة.

٥- من الضروري أن يوضح القانون ماهية عقد التأمين من المخاطر السيبرانية ويحدد شروطه بالإضافة لبيان المخاطر السيبرانية الممكن التأمين منها والأخرى المستثناة من العقد، مع ضرورة تحديد آلية التعاقد والتشديد على إلزام الشركات التجارية الكبيرة والمتوسطة والتي تتعامل بأساليب رقمية حديثة ضمن الفضاء السيبراني بالتأمين من المخاطر السيبرانية مما يجنب هذه الشركات خسائر مالية

ومعنوية هائلة، بالإضافة إلى تشجيع عمل هذه الشركات في بيئة رقمية آمنة من خلال منح حوافز للشركات المؤمنة من هذه المخاطر كإعفائها من الضرائب كلاً أو جزءاً أو منحها علامة معينة تميزها عن باقي الشركات التجارية مما يشجع العملاء للإقبال عليها.

٦- 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.

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

٨- نوصي بضرورة الأخذ بنظر الإعتبار التنسيق بين التشريعات الوطنية المقترحة مع التشريعات الدولية ذات الصلة والعمل على توحيد المصطلحات القانونية الواردة فيها قدر الامكان خصوصاً المصطلحات الحديثة منها لتجنب الوقوع في اشكالية الغموض التشريعي.

٩- نوصي بضرورة عمل ندوات علمية لطلبة الكليات وموظفي دوائر الدولة عن المخاطر السيبرانية وأضرارها وطرق التقليل منها والتثقيف عن أهمية التأمين من المخاطر السيبرانية للأطراف المعنية وهم الأشخاص الطبيعيين ودوائر الدولة والشركات التجارية على إختلاف أنواعها.

١٠- نوصي بضرورة إنشاء شركات متخصصة بالتأمين من المخاطر السيبرانية وإدراج هذا النوع من المخاطر ضمن فئات المخاطر القابلة للتأمين لدى شركات التأمين من المخاطر التقليدية على أقل تقدير بسبب إنعدام وجود شركة مختصة بالحماية التأمينية للشركات التجارية من المخاطر السيبرانية في العراق لحد الآن.

١١- العمل على ترسيخ ثقافة الأمن السيبراني والتأمين من المخاطر السيبرانية في الشركات التجارية كافة، وإلزامها على وضع سياسات وإرشادات أمنية كفيلة بتوضيح كيفية التعامل مع المخاطر السيبرانية في الشركات التجارية و وسيلة الحماية منها، مع التأكيد على إنشاء فرق متخصصة داخل كل شركة لمتابعة تنفيذ إجراءات الأمن السيبراني ومراقبة المخاطر السيبرانية والعمل على وضع آليات محددة للإستجابة لهذه المخاطر السيبرانية عند وقوعها والتأكيد على موظفي الشركة في كيفية التعامل مع المخاطر السيبرانية، وتوضيح إلتزاماتهم القانونية والمسؤوليات التي قد تترتب على خرق إجراءات الأمن السيبراني تجاه الشركة أو عملائها أو الغير.

المصادر والمراجع

المصادر والمراجع

أولاً: المعاجم اللغوية

١- إبراهيم أنيس وآخرون، المعجم الوسيط، ط٤، الناشر: مجمع اللغة العربية - مكتبة الشروق الدولية، القاهرة، ٢٠٠٤.

٢- أحمد مختار عمر، معجم اللغة العربية المعاصرة، المجلد الأول، ط١، عالم الكتب للنشر والتوزيع، القاهرة، ٢٠٠٨.

٣- محمد بن ابي بكر الرازي، مختار الصحاح، دار الكتاب العربي، بدون سنة نشر، بيروت.

٤- معجم المعاني الجامع.

٥- منير البعلبكي ورمزي منير، قاموس المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩.

ثانياً: الكتب

١- أبي الفضل هاني بن فتحي، التأمين: أنواعه المعاصرة، ط١، دار العصماء، دمشق، ٢٠٠٩.

٢- أحمد شرف الدين، أحكام التأمين، ط٣، القاهرة، ١٩٩١.

٣- أشرف وفا محمد، الوسيط في القانون الدولي الخاص، ط١، 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، ط١، دار الراية للنشر والتوزيع، عمان، ٢٠١٥.

٧- سلطان عبد الله محمود، عقود التجارة الإلكترونية والقانون الواجب التطبيق، ط١، 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، اتمتة التأمين والتأمين على مخاطر الفضاء الرقمي، دار الفكر الجامعي، الاسكندرية، ٢٠٢٣.

١٠- طارق عفيفي صادق، الخطر محل التأمين من المسؤولية في مجال المعلوماتية، ط١، دار الحكمة للطباعة والنشر والتوزيع، القاهرة،٢٠١٣.

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 الإلتزام 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، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣.

١٦- ماجد محمد سليمان، العقد الإلكتروني، ط١، 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، الخطر في 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.

٢٣- مصطفى كمال طه، التأمين البحري، الدار الجامعية للنشر والتوزيع، القاهرة، ١٩٩٢.

٢٤- نضال إسماعيل إبراهيم، أحكام عقود التجارة الإلكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥.

٢٥- هيثم حامد المصاروة، المنتقى في شرح عقد التأمين، ط١، اثراء للنشر والتوزيع، عمان، ٢٠١٠.

ثالثاً: الرسائل والأطاريح

١- بولحية سمية، النظام القانوني لعقد التأمين على المركبات في التشريع الجزائري، رسالة ماجستير مقدمة إلى جامعة العربي بن مهيدي ام البواقي /كلية الحقوق والعلوم السياسية، ٢٠١١.

٢- حنين جميل ابو حسين، الإطار القانوني لخدمات الامن السيبراني رسالة ماجستير مقدمة الى كلية الحقوق، جامعة الشرق الاوسط، ٢٠٢١.

٣- حيدر شكري فيصل، التامين على اعمال الإرهاب الالكتروني عابر الحدود – دراسة مقارنة، رسالة ماجستير مقدمة إلى معهد العلمين لدراسات العليا/ قسم القانون، ٢٠٢٣.

٤- زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير مقدمة الى كلية القانون/ جامعة الكوفة، ٢٠١٦.

٥- سنا مازن فالح، دور إعادة التأمين في ضمان حقوق المؤمن له في مواجهة المؤمن الأصلي، رسالة ماجستير مقدمة إلى كلية الحقوق/ جامعة الشرق الأوسط، عمان، ٢٠١١.

٦- صادق زغير محيسن، القواعد ذات التطبيق المباشر في القانون الدولي الخاص، رسالة ماجستير مقدمة الى كلية القانون / جامعة البصرة، ١٩٩٧.

٧- علي محمد الموسوي، المشاركة المباشرة في الهجمات السيبرانية، رسالة ماجستير مقدمة إلى كلية الحقوق /جامعة النهرين، ٢٠١٩.

٨- عمار ياسر رشيد، التأمين ضد مخاطر الالكترونية في التشريع الأردني، أطروحة دكتوراه مقدمة الى جامعة العلوم الاسلامية / كلية الدراسات العليا / قسم القانون المقارن، ٢٠٢١.

٩- لما عبد الله صادق، مجلس العقد الإلكتروني، رسالة ماجستير مقدمة إلى كلية الدراسات العليا / جامعة النجاح الوطنية، ٢٠٠٨.

١٠- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير مقدمة الى الجامعة الافتراضية السورية، ٢٠٢١.

رابعاً: البحوث

١- أحمد الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، الجامعة المصرية –الروسية، المجلد (٢٤)، العدد (٤) ٢٠٢٣.

٢- أحمد عطا حسين، وسائل حماية التجارة الالكترونية من المخاطر الهجمات السيبرانية، مجلة جامعة واسط للعلوم الإنسانية، مجلد (١٨) العدد (٥٢) لسنة ٢٠٢٢.

٣- أزهار محمود لهمود، القانون الواجب التطبيق في منازعات العقود الدولية، مجلة كلية القانون للعلوم القانونية والسياسية، مجلد (٩)، العدد (٣٤)، جامعة تكريت كلية الحقوق،٢٠٢٠.

٤- إسراء فهمي ناجي، التأمين ضد الأخطار الالكترونية مجلة رسالة الحقوق السنة الثالثة عشرة، العدد الأول جامعة كربلاء كلية القانون، ٢٠٢١.

٥- إسلام فوزي، الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، مجلد (٥٦)، العدد (٢)، ٢٠١٩.

٦- إسلام مصطفى جمعة، جريمة اختراق الامن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية، المجلد (١٢)، العدد (٣)، لسنة ٢٠٢٢.

٧- آمنة محمد منصور، تأثير الامن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية، مجلة الادارة والاقتصاد الجامعة المستنصرية، العدد (١٢٧) لسنة ٢٠٢١.

٨- أميرة عبد العظيم محمد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد (٣٥)، الجزء (٣)، ٢٠٢٠.

٩- بغداد شامبي، تأمين الخطر السيبراني، مجلة هيرودوت للعلوم الأنسانية والاجتماعية، المجلد (٧) العدد (٢٥)، ٢٠٢٣.

١٠- بن عميروش ريمة، عن خصوصية الجريمة المعلوماتية، مجلة الفقه القانوني والسياسي، المجلد (٢) العدد (٢) لسنة ٢٠٢١.

١١- بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الابحاث، المجلد الثاني، العدد (٥)، ٢٠١٦.

١٢- حازم حمد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، المجلة الجزائرية للعلوم القانونية والسياسية، مجلد (٥٧)، العدد (٥)، ٢٠٢٠.

١٣- حبيب عبيد مرزة العمارة وماهر محسن عبود الخيكاني، التنظيم القانوني للتأمين الالكتروني، مجلة جامعة بابل للعلوم الانسانية، مجلد (٢٦)، عدد (٨)، ٢٠١٨.

١٤- حزام فتيحة، الاحكام المتعلقة بخدمات التأمين الالكترونية، مجلة جامعة محمد بوقرة بومرداس، مجلد (١٤)، العدد (١)، ٢٠٢١.

١٥- حنان مليكه، عقد التأمين الالكتروني، مجلة جامعة دمشق للعلوم القانونية، العدد الاول المجلد (٢)، ٢٠٢٢.

١٦- حيدرة محمد وآخرون، الهجمات السيبرانية ومواجهتها في القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد (٤)، ٢٠١٧.

١٧- خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للابحاث ودراسة السياسات، سبتمبر ٢٠١٣.

١٨- دراعو عز الدين، الاثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي، مجلة التكامل الاقتصادي، جامعة محمد بن احمد وهران، المجلد (١٠) العدد (٢)، ٢٠٢٢.

١٩- درويش سعيد، الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة في ضوء احكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد (٥٤)، العدد (٥)، ٢٠١٧.

٢٠- دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي قراءة في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، المجلد (٨)، العدد (٠) عدد خاص، ٢٠٢٢.

٢١- رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد (١٥)، العدد (٢)، ٢٠١٨.

٢٢- رمضان عارف رمضان وأبو الحمد مصطفى صالح، استخدام المنهجية الرشيقة في تطوير اداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، مجلة البحوث المالية والتجارية، المجلد (٢٣)، العدد (٣)، ٢٠٢٢.

٢٣- روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد (٢٤) الشهر (٥) لسنة ٢٠٢٠.

٢٤- سلوى يوسف الأكيابي، مدى انطباق القانون الدولي الانساني على الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق، جامعة الزقازيق، المجلد (٣٥)، العدد (١٠١)، المجلد (٢)، ٢٠٢٣.

٢٥- سيف هادي، امل فاضل عنوز، الالتزام بالأدلاء ببيانات المتعلقة بالخطر، مجلة المنهل الاقتصادي المجلد (٤) العدد (٢)، ٢٠٢١.

٢٦- شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية مجلد (١٧)، العدد (١)، ٢٠٢٠،

٢٧- صلاح مهدي هادي وزيد محمد علي اسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، كلية العلوم السياسية جامعة النهرين، مجلة قضايا سياسية العدد (٦٢)، السنة (١٢)، ٢٠٢٠

٢٨- عبد الجبار بن علي، النقود المشفرة "بتكوين ومشتقاتها ": بحث في حقيقتها وتخريج احكامها الفقهية، مجلة الشهاب / جامعة الشهيد حمه خضر الوادي، المجلد (٥)، العدد (٢)، ٢٠١٩.

٢٩- عبد الحليم محمود شاهين، تقييم اقتصادي أولي لمخاطر البيت كوين، مجلة كلية الاقتصاد والعلوم السياسية، جامعة الاسكندرية، مجلد (٢٢)، العدد (٣)، ٢٠٢١.

٣٠- عبد الله عبد الكريم، الهجمات السيبرانية في ضوء القانون الدولي، المجلة المصرية للقانون الدولي، مجلد (٧٧)، العدد (٧٧)، ٢٠٢١.

٣١- علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط، العد (٦٣)، الكويت، ٢٠١٩.

٣٢- علي فاضل علي سليمان، حق الدفاع الشرعي عن الهجمات السيبرانية، مجلة جامعة تكريت للحقوق السنة (٤)، المجلد (٤)، العدد (٤)، الجزء الأول،٢٠٢٠.

٣٣- فاطمة سرير، رباحي احمد، فعالية تنميط البيانات الشخصية في تخصيص التجارة الالكترونية على ضوء اللائحة العامة رقم ٦٧٩لسنة ٢٠١٦ المتعلقة بحماية البيانات، مجلة الدراسات القانونية المقارنة، المجلد (٨)، العدد (٢)، ٢٠٢٢.

٣٤- قيصر بهاء، أشهر الهجمات السيبرانية، تقرير الفريق الوطني للاستجابة للإحداث السيرانية.

٣٥- محمد الدمرداش ابو التوح، متطلبات تنمية المهارات الرقمية للمنظم الاجتماعي للحد من هجمات الهندسة الاجتماعية، مجلة الخدمة الاجتماعية، المجلد (٧٦)، العدد (٢)، ٢٠٢٣.

٣٦- محمد سعد أحمد، دور التأمين في مواجهة المخاطر الناشئة عن الذكاء الاصطناعي وتكنولوجيا المعلومات، مجلة مصر المعاصرة، العدد (٥٤٣)، ٢٠٢١.

٣٧- محمد سعيد اسماعيل. التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المقترحة – دراسة في القانون القطري والمقارن، المجلة الدولية للقانون، المجلد (١٠)، العدد (٣)، (عدد خاص بمؤتمر القانون في مواجهة الازمات العالمية – الوسائل والتحديات)، كلية القانون، جامعة قطر،٢٠٢١.

٣٨- ناجي محمد اسامة الشاذلي الجوانب القانونية للحرب السيبرانية: دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، المجلد (٣٥)، العدد (١٠٣)، (ج٢)، ٢٠٢٣.

٣٩- نشرة الاتحاد المصري للتأمين، الهجمات الالكترونية (السيبرانية) والتأمين، العدد (٦٧)، ٢٠١٩.

٤٠- نشرة الاتحاد المصري للتأمين، مخاطر الهجمات الالكترونية في المؤسسات المالية، العدد (٢٤٥)، لسنة ٢٠٢٢.

٤١- ننسي أحمد فاروق، التزام المؤمن عليه بالإدلاء بالبيانات المتعلقة بالخطر وجزاء الإخلال به، مجلة البحوث القانونية والإقتصادية، المجلد (٥٤)، العدد (١)، ٢٠٢١.

٤٢- هاني محمد العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، المجلد (١١٤)، العدد (٥٤٩)، ٢٠٢٣.

٤٣- هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد (٢٤)، العدد (١)، الرقم المسلسل للعدد ٩٤، ٢٠٢٣.

٤٤- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الاحمر، مجلد (٩٤)، ٢٠١٢.

خامساً: القوانين

١- القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١.

٢- قانون اساءة استخدام الكمبيوتر لسنة ١٩٩٠/ المملكة المتحدة.

٣- قانون قابلية نقل التأمين الصحي والمساءلة الصادر عن الكونغرس في الولايات المتحدة لعام ١٩٩٦ (HIPAA).

٤- قانون الأونسترال النموذجي بشأن التجارة الالكترونية الصادر عن لجنة الامم المتحدة لقانون التجارة الدولية لسنة ١٩٩٦.

٥- التوجيه الأوروبي رقم (٩٧/٧) الصادر عن مجلس وبرلمان الاتحاد الأوروبي في ٢٠ مايو ١٩٩٧.

٦- قانون الإخطار الإلزامي عن خرق البيانات رقم S.B. 1386 / النافذ في ١ تموز / ٢٠٠٣ / ولاية كاليفورنيا.

٧- قانون حماية المعطيات الشخصية التونسي رقم (٦٣) لسنة ٢٠٠٤.

٨- قانون المصارف العراقي رقم (٩٤) لسنة ٢٠٠٤.

٩- قانون ديوان التأمين العراقي رقم (١٠) لسنة ٢٠٠٥.

١٠- القانون الاتحادي لدولة الامارات العربية المتحدة بشأن مكافحة جرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦.

١١- قانون مكافحة جرائم المعلوماتية السوداني رقم (١٤) لسنة ٢٠٠٧.

١٢- قانون المعاملات الالكترونية العماني رقم (٦٩) لسنة ٢٠٠٧.

١٣- قانون حماية المعطيات ذات الطابع الشخصي المغربي رقم (٠٩/٠٨) لسنة ٢٠٠٩.

١٤- القانون المؤقت لسنة ٢٠١٠ الخاص بجرائم انظمة المعلومات الأردني لسنة ٢٠١٠.

١٥- قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢.

١٦- قانون حماية خصوصية البيانات الشخصية القطري رقم (١٣) لسنة ٢٠١٦.

١٧- قانون حماية البيانات الصادر عن برلمان المملكة المتحدة لعام ٢٠١٨(DPA).

١٨- قانون الأمن السيبراني الأردني رقم (١٦) لسنة ٢٠١٩.

١٩- قانون حماية البيانات الشخصية الفيدرالي للإمارات العربية المتحدة رقم (٤٥) لسنة ٢٠٢١.

سادساً: اللوائح والأنظمة

١- نظام مكافحة الجرائم المعلوماتية السعودي لسنة المرقم (م/١٧) لسنة ٢٠٠٧.

٢- اللائحة الأوروبية العامة لحماية البيانات General Data Protection Regulation (GDPR) لسنة ٢٠١٦ والنافذة في ٢٥ مايو ٢٠١٨.

٣- لوائح أمن الشبكات والمعلومات في المملكة المتحدة لعام ٢٠١٨ NIS)).

٤- الضوابط الاساسية للامن السيبراني الصادرة عن الهيئة الوطنية للامن السيبراني السعودية لسنة ٢٠١٨.

٥- اللائحة العامة لحماية البيانات في المملكة المتحدة لعام ٢٠٢١(GDPR –UK)

٦- نظام حماية البيانات الشخصية السعودي المرقم (م/١٩)لسنة ٢٠٢١.

سابعاً: المصادر الأجنبية

1- Andrew Granato, Andy Polacek, The growth and challenges of cyber insurance, the federal reserve bank essays on issues of chicago, no. (426),2019.

2- Anna Cartwright, Edward Cartwright, EstherSolomon Edun, Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies, Computers & Security jornal, vol. (131) issue (3), 2023.

3- Assurance des risques cyber – Guide Pratique, club de la sécurité de l'information français (CLUSIF), 2018.

4- Assurance des risques cyber. Guide Pratique, club de la securite de l`information Franceais,. Janvier 2018.

5- Bahaa Eltahawy, Duong Dang. Understanding Cyberprivacy: Context, Concept, and Issues, 17th International Conference on Wirtschaftsinformatik (WI22) At: Nuremberg, Germany, (2022) .

6- Bc. Jan Linert Pojištění kybernetických rizik, VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE, Fakulta financí a účetnictví, 2019.

7- Biener, C., Eling, M., Wirfs, J. Insurability of Cyber Risk: An Empirical Analysis. Geneva Pap Risk Insur Issues Pract 40, 131–158 (2015).

8- 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).

9- Böhme, Rainer and Gaurav Kataria. "Models and Measures for Correlation in Cyber-Insurance." Workshop on the Economics of Information Security", University of Cambridge, UK, England, June 2006.

10- Cebula, J.J. and Young, L.RA, Taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN- 028, Software Engineering Institute, Carnegie Mellon University, (2010).

11- Chiaradonna, S., & Lanchier, N, Exact Insurance Premiums for Cyber Risk of Small and Medium-Sized Enterprises. Mathematical Modelling of Natural Phenomena journal, vol. 17, Article 40, (2022), p1.

12- chubb, Cyber Enterprise Risk, Terms and Conditions Management Insurance, 2016.

13- cyber risk for insurance, challenges and opportunities, Luxembourg: Publications Office of the European Union, 2019.

14- Daniel Woods, Andrew Simpson, Policy measures and cyber insurance: a framework, Journal of Cyber Policy Volume (2), Issue (2) 2017.

15- Danish Javeed, Man in the Middle Attacks: Analysis, Motivation and Prevention.

16- DOD Dictionary of Military and Associated Terms, 2021, p55.

17- Eling, M. Schnell, W., "What do we know about cyber risk and cyber risk insurance?", Journal of Risk Finance, Vol. 17 No. 5, pp. 474-491 (2016).

18- Even Langfeldt Friberg, The Cyber-Insurance Market in Norway: An Empirical Study of the Supply-side and a Small Sample of the Maritime Demand-side Master's thesis, TALLINN UNIVERSITY OF TECHNOLOGY School of Information Technologies, 2018

19- Even Langfeldt Friberg, The Cyber-Insurance Market in Norway: An Empirical Study of the Supply-side and a Small Sample of the Maritime Demand-side, Master's thesis, TALLINN UNIVERSITY OF TECHNOLOGY, School of Information Technologies, 2018.

20- Florian Schütz, Florian Rampold, Andre Kalisch, Kristin Masuch, Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis, Procedia Computer Science, Volume (219), 2023.

21- Franke Ulrik, Meland Per Håkon, Demand side expectations of cyber insurance, International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019.

22- Ganbayar Uuganbayar, Relation between cyber insurance and securety investments/controls,universita Degli studi Di Trento, PhD.Thesis,2021.

23- Gaspard Ferey, Nicolas Grorod, Simon Leguil. L'assurance des risques cyber, Mémoire de fin de formation, Sciences de l'Homme et Société, .2017

24- Grzegorz Strupczewski, Defining cyber risk, Safety Science, Volume 135, 2021, 105143, ISSN 0925-7535.

25- Henry R K Skeoch, Christos Ioannidis, The barriers to sustainable risk transfer in the cyber-insurance market, *Journal of Cybersecurity*, Volume 10, Issue 1, 2024.

26- International Journal of Computer Networks and Communications Security, vol. (8), No. (7),2020.

27- IRM, Cyber Risk. Resources for Practitioners The Institute of Risk Management ,2014 .

28- ISACA. The Risk IT framework, Information Systems Audit and Control Association, 2009

29- Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Matthew Fallon, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication NIST SP 800-161r1,2022.

30- Julie Bernard, Overcoming challenges to cyber insurance growth expanding standalone policy adoption among middle market businesses, A report from the Deloitte center for financial services,2020.

31- Juraj Sikra_Karen V. Renaud_Daniel R. Thomas, UK Cybercrime, Victims and Reporting: A Systematic Review, commonwealth cybercrime journal volume (1), issue (1),2023.

32- Kala, The Impact of Cyber Security on Business: How to Protect Your Business. Journal of Safety Science and Technology, vol. (13), No. (2), 2023.

33- kenneth s. Abraham, Daniel schwarcz, Courting disaster: the underappreciated risk of A Cyber insurance Catastrophe, Connecticut insurance law jornal vol. (27), issue (2), 2021.

34- L'assurance du risque cyber Colloque de l'Université du Mans du 5 décembre, 2018.

35- Mallik Avijit, Ahsan Abid, Shahadat Mhia, Tsou, Jia - Chi. Man – in – the - middle-attack: Understanding in simple words. International Journal of Data and Network Science, vol. (3), issue (2). (2019).

36- Mark Camillo, Cyber risk and the changing role of insurance, Journal of Cyber Policy, vol. (2), issue (1), (2017).

37- Mc Dermott Will and Emery, Courts Approach To Cyber Insurance Continues to Evolve, the national law review, Volume (XIII), issue (331), 2023.

38- Michael Krisper, Jürgen Dobaj, Georg Macher. Assessing Risk Estimations for Cyber-Security Using Expert Judgment, 27th European Conference, EuroSPI, Düsseldorf, Germany11Proceedings. (2020).

39- Mukhopadhyay, Arunabha, Chatterjee, Samir, Saha, Debashis, Mahanti, Ambuj, Sadhukhan, Samir K, Cyber-risk decision models: to insure IT or not? Decision Support Systems vol. (56), issue(1), 2013.

40- NIDA TARIQ, IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, vol. (23), issue (2), 2018.

41- Nieuwesteeg, B., Visscher, L., de Waard, B, The law & economics of cyber insurance contracts: a case study, European Review of Private Law, Volume 26, Issue 3, (2018).

42- NISTMinimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200, National Institute of Standards and Technology (NIST), Gaithersburg, MD,2006.

43- Okereafor, Kenneth, Impacts Of Cyber Attacks On Corporate Business Continuity: Fostering Cyber Security Consciousness In The Citizenry,1st National Cybersecurity and Cybercrime ConferenceAt: Abuja, (2008).

44- Pavel V Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, Stefan Trück, The nature of losses from cyber-related events: risk categories and business sectors, Journal of Cybersecurity, Volume (9), Issue (1), 2023.

45- Peters Gareth ،Shevchenko Pavel, Cohen Ruben ،Maurice Diane, Understanding Cyber Risk and Cyber InsuranceSSRN Electronic Journal. 10.219, 2017.

46- Philip Rawlings, Cyber Risk: Insuring the Digital Age, British Insurance Law Association Journal, volume 128, Paper No. 189/2015, Queen Mary School of Law Legal Studies Research, 2015.

47- Pierre-Grégoire Marly, L'assurance du risque cyber, Colloque de l'Université du Mans du 5 décembre 2018 sur les nouvelles technologies et les mutations des assurances, Dalloz IP/IT 2019.

48- Pojištění kybernetických rizik . Autor diplomové práce: Bc. Jan Linert. Vedoucí diplomové práce: prof. Ing. Eva Ducháčková VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. Fakulta financí a účetnictví, CSc. Rok obhajoby: 2019.

49- RAPPORT SUR L'ASSURABILITÉ, DES RISQUES CYBER, du Haut Comité Juridique, du Haut Comité Juridique 2022.

50- Refsdal, A., Solhaug, B., Stolen, K. Cyber-risk Managemen, Springer briefs in computer scince, 2015.

51- Samuel Tweneboah - Koduah, Samuel Tweneboah - Koduah, William J Buchanan Impact of Cyberattacks on Stock Performance: A Comparative Study, Information and Computer Security juornal, vol. (26), No. (3),2018.

52- Sasha Romanosky and others, Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cyber security, Volume (5), Issue (1), 2019.

53- Sasha Romanosky, Examining the costs and causes of cyber incidents, Journal of Cybersecurity, Volume 2, Issue 2, December 2016.

54- Shergunova E.A, The Electronic Insurance in the Context of Innovative Development of Digital Law in Russia, volume 138, 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020).

55- Shinichi Kamiya Jun-Koo Kang Jungmin Kim Andreas Milidonis René M. Stulz, WHAT IS THE IMPACT OF SUCCESSFUL CYBERATTACKS ON TARGET FIRMS? Working Paper NO. 24409, NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, 2018.

56- Simon Holtz, Patrick Dummermuth, Simon Künzler, Melanie Koller, Nadine Janser, CYBER RISK and INSURANCE UPDATED 3RD EDITION, (2021).

57- Sonakshi Kathuriya, Graphic Era, IMPACT OF CYBERSECURITY ON BUSINESS ENVIRONMENT, DE JURE NEXUS LAW JOURNAL, VOLUME 2 ISSUE 4, 2022.

58- Spencer, Be Smart about Insurance for the Smart Grid: Coverage for Losses from, Cyber Events—Part II,2017.

59- Steven Hadwin, Norton Rose Fulbright LLP and Jamie Monck-Mason,WillisTowers Watson, cyber INSURANCE:AOVERVIEW,UK,2020

60- sur les nouvelles technologies et les mutations des assurance

61- Torsten Grzebiela, Insurability of Electronic Commerce Risks, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

62- Tsohou A, Diamantopoulou V, Gritzalis S, Lambrinoudakis C. Cyber insurance: state of the art, trends and future directions, International Journal of Information Security, vol. (22), 2023.

63- Wiener, Norbert: Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

64- Yaniv Harel, Irad Ben Gal, and Yuval Elovici. Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. ACM Trans. Intell. Syst. Technol. vol. (8), issue (4), Article 49, July 2017.

65- Yogesh Malhotra, Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis December 7, (2017)

66- Yogesh Malhotra, PhD, Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics, MS Network and Computer Security Thesis On Model Risk Management of Statistical Probability Distributions in Cyber Insurance, Thesis Presented to the state university of NY.

67- Yueshan He, "Cyber Risk Insurance Pricing Based on Optimized Insured Strategy. A research paper presented to the University of Waterloo in partial fulfillment of the requirement for the degree of Master of Mathematics in Computational Mathematics" (2016).

68- Zain Mohey - Deen, Richard J. Rosen, The risks of pricing new insurance products: The case of long-term care, the federal reserve bank essays on issues of Chicago, no. 397, 2018.

سابعاً: القرارات القضائية

1. THE HIGH COURT OF JUSTICE, BUSINESS & PROPERTY COURTS OF ENGLAND AND WALES COMMERCIAL COURT (QBD) IN PRIVATE, CL-2019-000746, (reporting restrictions lifted and released for publication, 17 January 2020.
http://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html

2. WM Morrisons Supermarkets plc (Appellant) v Various Claimants (Respondent), Judgment date,01 Apr 2020, Neutral citation number, [2020] UKSC 12, Case ID
UKSC 2018/0213

https://www.mcgradyinsurance.com/news/supreme-court-employer-liability

3. Miss. Silicon Holdings v. Axis Ins. Co., No. 20-60215 (5th Cir. Feb. 4, 2021)
https://casetext.com/case/miss-silicon-holdings-llc-v-axis-ins-co-2

4. EMOI Servs LLC v. Owners Ins. Co Slip Opinion No. (4049) ohio 27/12/2022.

https://www.hinshawlaw.com/newsroom-updates-ohio-supreme-court-no-coverage-ransomware-physical-damage-limitation.html

5. United States Court of Appeals Fifth Circuit, (Mississippi Silicon Holdings, L.L.C. vs. Axis Insurance Company) No. 20-60215/ FILED February 4, 2021 Lyle W. Cayce Clerk
https://www.hinshawlaw.com/assets/htmldocuments/Alerts/5th%20Circuit%20MSH.pdf

6. United States Court of Appeals, Eighth Circuit
(EYEBLASTER, INC., Plaintiff-Appellant, v. FEDERAL INSURANCE COMPANY) Date published: Jul 23, 2010
https://casetext.com/case/eyeblaster-inc-v-federal-ins-co

7. England and Wales High Court (Queen's Bench Division) Decisions, (Rolfe & Ors v Veale Wasbrough Vizards LLP), [2021] EWHC 2809 (QB) (07 September 2021)
https://www.bailii.org/ew/cases/EWHC/QB/2021/2809.html

8. COLUMBIA CASUALTY COMPANY Plaintiff, v. COTTAGE HEALTH SYSTEM Defendant.
Court: United States District Court, Ninth Circuit, California, C.D. California
https://casetext.com/case/columbia-casualty-co-v-cottage-health-system

9. Landry's, Incorporated, as successor in interest to Landry's Management,,United States Court of Appeals, Fifth Circuit, Date published: Jul 21, 2021
https://casetext.com/case/landrys-inc-v-the-insurance-company-of-the-state-of-pennsylvania

10. Ernst & Haas Mgt. Co. v. Hiscox, Inc., 23 F.4th 1195 (9th Cir. 2022)
https://www.jdsupra.com/legalnews/commercial-crime-policy-covers-loss-/4840071

11. Warren v DSG Retail Limited [2021] EWHC 2168 (QB)
https://www.jdsupra.com/legalnews/warren-v-dsg-retail-ltd-shifting-the-1199275/

12. Mgmt., Inc. v. Fed. Ins. Co., 115 A.3d 458, 317 Conn. 46 (Conn. 2015).
https://casetext.com/case/recall-total-info-mgmt-inc-v-fed-ins-co-1
Date published: May 7, 201

https://www.insurancelaw.london/2017/03/aig-europe-limited-v-woodman-and-others-2017-uksc-18
13. MONDELEZ INTERNATIONAL, INC., Plaintiff, v. ZURICH AMERICAN INSURANCE COMPANY, DefendantCase No. 2018-L-11008 (Ill. Cir. Ct. Oct. 27, 2022)
https://www.scribd.com/document/397265756/Mondelez-Zurich
14. AIG Europe Limited vs Woodman (and others)/ 22 march / [2017] UKSC 18
https://www.supremecourt.uk/cases/uksc-2016-0100.html
15. *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM (D. Ariz. May. 26, 2016)
https://casetext.com/case/pf-changs-china-bistro-inc-v-fed-ins-co

ثامناً: المواقع الإلكترونية

1- https://www.dictionary.com/browse/cyber
2- استراتيجية الامن السيبراني العراقي الصادرة عن مستشارية الأمن الوطني:
https://www.itu.int/en/ITU-
3- الموقع الرسمي للهيئة الوطنية للأمن السيبراني السعودي:
https://nca.gov.sa
4- الموقع الرسمي للمركز الوطني للأمن السيبراني الأردني:
https://ncsc.jo/
5- مكتب الامم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، مسودة شباط و فبراير،٢٠١٣.
www.unodc.org/romena/en/cybercrime.html
6- الموقع الرسمي لمجلس الاستقرار المالي (Financial Stability Board)
www.fsb.org
7- الموقع الرسمي لـ(IAIS)الجمعية الدولية لمشرفي التأمين :
www.iaisweb.orgm
8- منظمة شنغهاي للتعاون (sco) :
http://eng.sectsco.org/cooperation/20170110/192193.html
9- الموقع الرسمي للإنسكوا: https://www.unescwa.org/ar/about
10- https://www.cdc.gov/phlp/publications/topic/hipaa.html
11- الموقع الرسمي لشركة وساطة التأمين:(GB&A)
Avoiding The Most Common Cyber Insurance Claim Denials report
https://www.gbainsurance.com/avoiding-cyber-claim-denials

12- https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard
13- chohen and co.,5 Cyber Liability Insurance Fundamentals for Your Business, July 09, 2021
https://www.cohencpa.com/knowledge-center/insights/july-2021/5-cyber-liability-insurance-fundamentals-for-your-business
14- الموقع الرسمي للمركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC)
https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
15- https://www.aecl.com/ar/security/cyber-security-1/
16- الموقع الرسمي لدليل الامتثال للائحة العامة لحماية البيانات
https://gdpr.eu
17- Stephen M. Foxman, Sample Contract Clauses, Esq
https://www.eckertseamans.com
18- https://kpmg.com/uk/en/home/services/products/cyber-risk-insights.html
19- : الموقع الرسمي لوكالة الاتحاد الاوروبي للامن السيبراني
https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering
20- CYBER INSURANCE: A guide for SMEs.
https://hamiltonleigh.com/cyber-insurance-a-guide-for-smes/
21- The Hartford steam Boiler Inspection and Insurance Company (HSB), cyber risk insurance Application,2019 :
https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf.
22- : وثيقة شركة أكسيس للتأمين
AXIS Cyber ansomeware Supplement Application,No. 1012729 10 20 :
https://www.euclidspecialty.com/wp-content/uploads/2021/05/AXIS_Ransomware_App-2021-1.pdf
23- : وثيقة شركة (كيو بي اي) للتأمين
QBE Cyber Response Insurance Policy,Danmark :
https://qbe.dk/media/8241/qbe-cyber-response.pdf
24-
: الموقع الرسمي للإتحاد الأوروبي

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31997L0007

26- https://www.advisenltd.com/2019-cyber-risk-insights-conference-new-york/

27-
وثيقة التأمين من المخاطر السيبرانية لشركة (TRAVELERS) الأمريكية لسنة ٢٠١٦ المنشورة على الموقع:

https://www.profunderwriters.com/wp-content/uploads/2018/04/TRAVELERS_CyberRisk-app-1100-ind-0116.pdf

28-
وثيقة التأمين من المخاطر السيبرانية لشركة (MSIG Insurance) الفيتنامية :
MSIG Insurance (Vietnam) Company Limited, CYBER INSURANCE POLICY

https://www.msig.com.vn/sites/default/files/downloads/CYBER_INSURANCE_0.pdf

٢٩- وثيقة تأمين من المخاطر السيبرانية لشركة : (HSB)
https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/HSB-Total-Cyber-Insurance-Application-2019.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/HSB-Total-Cyber-Insurance-Application-2019.pdf

الملاحق

(مجموعة من وثائق التأمين من المخاطر السيبرانية)

ملحق (١):

-1-

شركة Exis للتأمين/ Chicago رقم الهاتف 9000-678746

الرقم المجاني: 5435-866259

فاكس 67874 -9315

ملاحظة:

فيما يتعلق بتأمين المسؤولية بموجب هذه الوثيقة التي يتم من خلالها تقديم هذا الطلب. توفر وثيقة التأمين من المخاطر السيبرانية هذه ، تغطية كل المخاطر التي يتم تقديمها والإبلاغ عنها في هذه الوثيقة حصراً والمقدمة لأول مرة بصورة دعوى أو شكوى ضد المؤمن له خلال فترة التغطية أو أي فترة أخرى معمول بها ، والإبلاغ عنها إلى شركة التأمين كما هو منصوص عليه في قسم الإبلاغ عن المخاطر والأحداث السيبرانية علماً انه يتم تضمين تكاليف الدفاع ضمن حدود مبلغ التغطية والتي من الممكن أن تفوق حدود التأمين و تستنزف جميع مبلغ التغطية.

(يشير مصطلح مقدم الطلب بشكل فردي أو جماعي إلى المؤمن لهم وتعتبر جميع الإجابات مقدمة بالنيابة عنهم)

ملاحظة:

إن مجرد تقديم هذا الطلب لا يلزم مقدم الطلب بشراء التأمين ولا تلتزم شركة التأمين ببيع التأمين أو تقديمه بناء على أي شروط محددة مطلوبة.

- إذا ما تم إصدار الوثيقة فإن هذا الطلب والذي يجب أن يتضمن جميع الملحقات التكميلية والمواد والمعلومات المقدمة من قبل المؤمن لهم فسيتم إعتباره مرفقاً بالوثيقة و يشكل جزءاً منها.

-٢-

تعليمات

- يرجى الإجابة على جميع الأسئلة بشكل كامل و عدم ترك الفراغ والتحقق من الإجابات وفي حال كانت المساحة غير كافية للإجابة تابع الإجابة في صفحة فارغة ملحقة.

- يجب إكمال هذا الطلب وتأ ريخه و توقيعه من قبل الموظف المعتمد من قبل الكيان المحدد في القسم المعنون معلومات الطلب

ملحق برامج الفدية

إسم التطبيق:.....

العنوان البريدي:.....

هل يستخدم مقدم الطلب أي وسيلة لكشف التسلل ومنعه

نعم لا ☐ ☐

هل يستخدم مقدم الطلب وسيلة للكشف عن نقطة النهاية والاستجابة لها

نعم لا ☐ ☐

إذا ما كانت الإجابة بنعم هل يتم استخدام أي من الوسائل التالية؟ اختر كل ما ينطبق

Windows المدافع ☐

سيمانتك EDR ☐

سيلانس ☐

نقطة نهاية اللعبة ☐

شيء آخر ☐

- هل يستخدم مقدم الطلب برنامج Microsoft office 365

نعم..... لا.....

-٣-
إذا كانت الإجابة بنعم فهل يتم تنفيذ ما يلي:

- الحماية من التهديدات

نعم ..... لا.....

- مصادقة متعددة العوامل لجميع مستخدمي Microsoft office 365

نعم ..... لا.....

- هل المصادقة متعددة العوامل مطلوبة للوصول التالي:

المعلومات الحساسة

نعم..... لا.....

المعلومات و التطبيقات غير الهامة

نعم..... لا.....

الأجهزة الشخصية

نعم..... لا.....

الوصول عن بعد

نعم..... لا.....

- هل يستخدم مقدم الطلب الوسائل التالية:

DMARC.

نعم ..... لا.....

- هل يقوم مقدم الطلب بمراقبة وصول الشخص المسؤول للسلوك والأنشطة غير العادية بشكل فعال وأمن؟

نعم..... لا.....

- هل تم تمكين بروتوكول سطح المكتب RDP))

اذا كانت الإجابة بنعم هل تم تنفيذ ما يلي:

- الوصول إلى vpnفقط

-٤-

نعم _____ لا_____

- مصادقة متعددة العوامل

نعم _____لا_____

- مصيدة RDP

نعم .....لا.....

- هل تم تمكين المصادقة على مستوى الشبكة

نعم.....لا.....

تحديد أي شيء آخر

_____
_____
_____
_____

التدريب والتوعية:

- هل يجري مقدم الطلب تدريبا إلزامياً على أمن المعلومات السيبرانية والخصوصية للموظفين ذوي العلاقة سنوياً على الاقل؟

نعم ..... لا.....

إذا كانت الإجابة بنعم فما هو نوع التدريب؟

- ☐ حملات التصيد
- ☐ الامتثال للخصوصية التعامل مع البيانات
- ☐ الهندسة الاجتماعية
- ☐ الوعي الأمني للتهديد

-٥-

- هل يقوم وقدم طلب إجراء نسخ احتياطي للبيانات بصورة منتظمة؟

نعم.....لا.....

ما مدى تكرار عمل نسخة إحتياطية من المعلومات الهامة على ألاقل:

بشكل مستمر_____

يومياً_____

أسبوعياً_____

شهرياً_____

٢\١ سنوياً_____

سنوياً_____

كل أربع سنوات_____

- هل يستخدم مقدم الطلب أشرطة النسخ الاحتياطي المادية؟

نعم..... لا.....

- أين يتم تخزين نسخة الاحتياطية؟

في المبنى ذاته.....

في مركز بيانات ثانوي.....

على السحابة.....

تخزين خارج الموقع.....

تحديد شيء آخر.....

-٦-

هل تخضع النسخة الاحتياطية للتدابير التالية:

التشفير

نعم..... لا.....

مصادقة متعددة العوامل

نعم..... لا.....

فحص الفيروسات والبرامج الضارة

نعم..... لا.....

هل يتم تخزين بيانات النسخ الاحتياطي الفريدة بشكل منفصل عن بيانات النسخ الإحتياطي الأخرى للمستخدم؟

نعم..... لا.....

هل يستخدم مقدم الطلب الفصل المادي بطريقة تؤدي إلى تقليل احتمالية وقوع الخطر السيبراني الذي قد يؤثر على جميع البيانات الموجودة لدى المستخدم؟

نعم.....لا.....

ما مدى تكرار عمل النسخ الاحتياطي وتخزين البيانات خارج موقع مقدم الطلب

أسبوعي	
شهري	
سنوي	
أربع سنوات	

-٧-

كم مرة يتم إختبار إسترجاع النسخة الاحتياطية على الاقل؟

أسبوعي	
شهري	
سنوي	
أربع سنوات	

في حالة إنقطاع شبكة مقدم الطلب ما هو الهدف الزمن الذي يتم فيه إسترداد الأنظمة والتطبيقات والعمليات المهمة بعد الخطر السيبراني؟

_____ أقل من ثمان ساعات

_____من ثمانية إلى ١٢ ساعة

_____من١٢ الساعة إلى ٢٤ ساعة

_____من ٢٤ ساعة إلى ٤٨ ساعة

_____ أكثر من ٤٨ ساعة

في حالة عدم توفر المعلومات الهامة أو الأنظمة أو التطبيقات أو العمليات الأخرى ما المدة التي يتم استغراقها لقطع عمل مقدم الطلب بشكل مادي في الغالب؟

اقل من ساعة

من ساعة إلى ثمان ساعات

من ثمان ساعات إلى ١٢ ساعة

من ١٢ ساعة إلى ٢٤ ساعة

من ٢٤ إلى ٤٨ ساعة

-٨-

معلومات إضافية:

الإقرار والتوقيع:

- من خلال التوقيع على هذه الوثيقة يقر الموقع أدناه لمقدم الطلب و النائب عن جميع الأشخاص و الكيانات المقترحة للتغطية ب:

أولاً: البيانات والإجابات الواردة في هذا الطلب وجميع الملحقات المقدمة معه صحيحة ودقيقة وكاملة.

ثانياً:لم يتم تفويت او إخفاء اي حقائق أو مواد معلوماتية عن الخطر السيبراني المقترح التأمين منه.

ثالثاً:تعتبر هذه الإقرارات بمثابة حافز مادي لشركة التأمين لتقديم عرض التأمين.

رابعاً: سيتم إصدار أي وثيقة التأمين تصدرها شركة التأمين بالإعتماد على هذه الإقرارات.

خامساً: يجب على مقدم الطلب إبلاغ شركة التأمين على الفور بصورة كتابية بأي تغيير جوهري في أنشطة مقدم الطلب ومنتجاته.

سادساً:سيقوم مقدم الطلب بإبلاغ شركة التأمين على الفور كتابياً بأي تغيرات جوهرية تطرأ على الإجابات الواردة في هذا الطلب والتي تحدث أو يتم اكتشافها بين تاريخ هذا الطلب وتاريخ نفاذ الوثيقة المطلوبة.

سابعاً:يحتفظ المؤمن بالحق عند استلام أي إشعار من هذا القبيل في تعديل أو سحب أي مقترح للتأمين

تحذير

يرجى مراجعة بيان الإحتيال الحكومي الوارد في نهاية هذا الطلب:

(تنطبق على الولاية التي يقيم فيها مقدم الطلب)

أي شخص يقدم بقصد الإحتيال او يسهل من الإحتيال طلباً يحتوي على بيان كاذب أو خادع يعتبر مرتكب جريمة الإحتيال في التأمين.

-٩-

يجب أن يتم توقيع هذا الطلب من قبل الرئيس التنفيذي لمقدم الطلب أو الرئيس او كبير مسؤولي أمن المعلومات أو مسؤول تكنولوجيا أو مدير العمليات السيبرانية أو المدير المالي أو المستشار العام أو مدير المخاطر أو ما يعادلهم وظيفياً ما لم تصدر شركة التأمين تعليمات إلى مقدم الطلب بخلاف ذلك

الاسم:.....

التوقيع:.....

العنوان:.....

التاريخ:.....

بيان الإحتيال الحكومي

ولاية الاباما

أي شخص يقدم عن عمد مطالبة كاذبة أو احتيالية لدفع خسارة أو منفعة أو يقدم عن عمد معلومات كاذبة في طلب التأمين يعتبر مذنب بإرتكاب جريمة وقد يتعرض لغرامات تعويضية أو الحبس او السجن او أي مزيج منهما

ولاية أركنساس

أي شخص يقدم عن علم مطالبة كاذبة أو احتيالية لدفع خسارة أو منفعة أو يقدم عن علم معلومات كاذبة في طلب التأمين يعتبر مذنب بارتكاب جريمة و قد يتعرض للغرامات والحبس والسجن

ولاية كولورادو

من غير القانوني تقديم حقائق أو معلومات كاذبة أو غير كاملة أو مظللة عن عمد إلى شركة التأمين بغرض الإحتيال أو محاولة الإحتيال على الشركة وقد تشمل العقوبات السجن والغرامات والحرمان من التأمين و الأضرار المدنية و أي شركة تأمين او وكيل لشركة التأمين يقدم عن

-١٠-

عمد معلومات كاذبة أو غير كاملة أو مضللة إلى حامل الوثيقة بغرض الإحتيال أو محاولة الإحتيال عليه فيما يتعلق في تسوية أو مكافأة مستحقة الدفع من عائدات التأمين يجب إبلاغ قسم التأمين في كولورادو داخل إدارة الهيئة التنظيمية

مقاطعة كولومبيا

يعتبر تقديم معلومات كاذبة أو مضللة بغرض الإحتيال جريمة يعاقب عليها بالسجن أو الغرامات بالإضافة إلى ذلك يجوز لشركة التأمين رفض مزايا التأمين إذا قدم مقدم الطلب معلومات كاذبة تتعلق مادياً بحقوقه

فلوريدا

كل من قام عن علم وقصد الإضرار أو الإحتيال والخداع بأية ملفات او بيان دعوى او طلب يحتوي على بيانات مضللة او كاذبة او ناقصة يعتبر مرتكباً لجناية من الدرجة الثالثة

كانساس

" عملية التأمين الإحتيالية " تعني اي فعل يرتكبه اي شخص عن عمد وقصد بتقديم او التسبب بتقديم عن طريقه او عن طريق مساهم او وسيط او وكيل رسالة او بيان إلكتروني مكتوب او فاكس او شفهي او هاتفي كجزء من او لدعم طلب إصدار وثيقة تأمين شخصي او تجاري او المطالبة بدفع او أي منفعة أخرى بموجب الوثيقة والتي يعلم هذا الشخص أنها تحتوي على معلومات كاذبة مادياً فيما يتعلق بأي حقيقة جوهرية او اخفى بغرض التضليل معلومات تتعلق بأي حقيقة جوهرية

ولاية كنتاكي

أي شخص يقوم عن علم وقصد الإحتيال على شركة التأمين او أي شخص آخر من خلال تقديم طلب تأمين يحتوي على معلومات غير صحيحة جوهرياً او يخفي بغرض التضليل معلومات تتعلق بأي حقيقة جوهرية فإنه يرتكب عملاً تأمينياً إحتيالياً ويعد جريمة يحاسب عليها القانون

حتى نتمكن من رفض أي مطالبة على أساس البيانات الخاطئة أو المضللة او المحرفة أو الإغفالات او البيانات الكاذبة يجب علينا أن نبين ما يلي :

١- تكون المعلومات الخاطئة جوهرية بالنسبة للمحتوى الوثيقة

-١١-

٢- إعتمدنا على هذه المعلومات المغلوطة

٣-إذا كانت المعلومات المقدمة إما جوهرية بالنسبة للمخاطر السيبرانية التي تغطيها الوثيقة أو تم تقديمها بطريقة احتيالية.

بالنسبة للتعويضات يجب أن تكون البيانات الخاطئة أو الكاذبة او المحرفة او التي تم إخفاء لها من جانبك احتيالية أو معادية لمصالحنا.

الملحق (٢)

-١-

وثيقة التغطية ضد المخاطر السيبرانية لشركة travelers
للتأمين / شركة تأمين من الحوادث والضمان

للمسافرين الأمريكية

ملاحظة :

تنطبق جميع بنود التأمين من مسؤولية الغير التي تم تقديم الطلب عليها فقط على المطالبات بالتعويض المقدمة لأول مرة أو التي تعتبر مقدمة ضد المؤمن لهم خلال فترة التغطية أو أي فترة ممتدة وإذا كان ذلك منطبقاً سيتم تخفيض حد المسؤولية المتاحة لدفع الخسائر بمقدار المبالغ المتكبده كنفقات دفاع ،

- ليس على شركة التأمين أي التزام بالدفع عن أي طلبات ما لم يتم توفير تغطية للدفع عن تلك الطلبات على وجه التحديد والخصوص .

- يقصد بمقدم الطلب جميع الشركات أو المنظمات أو الكيانات الأخرى بما في ذلك الشركات التابعة المقترحة هذا التأمين .

معلومات عامة :

١. إسم مقدم الطلب:

٢. العنوان البريدي:

٣. الموقع الإلكتروني:

٤. المدينة:

المعلومات المالية :

١. هل لدى مقدم الطلب أي شركات تابعة او يملك اكثر من ٥٠% في المشاريع المشتركة ؟

نعم ..... لا.....

إذا كانت الإجابة بنعم يرجى إرفاق قائمة بالشركات التابعة المشاريع المشتركة

٢. إجمالي عدد الموظفين بدوام كامل أو جزئي بما في ذلك الموظف المؤجر أو الموسمي أو المؤقت:

....

-٢-

٣. إجمالي الأصول للسنة المالية المتوقعة:.....

٤. إجمالي الإيرادات للسنة المالية المتوقعة:.....

شروط التأمين المطلوبة /معلومات التأمين الحالية :

الخطر المؤمن منه	الحد المطلوب / بالدولار
مسؤولية أمن الشبكات والمعلومات	
مسؤولية الاتصالات والإعلام	
مصاريف الدفاع التنظيمية	
مصاريف فعاليات إدارة الأزمات بالدولار	
معالجة الخرق الأمني ونفقات الأخطار	
مصاريف برامج الكمبيوتر واستعادة البيانات الإلكترونية	
الإحتيال الإلكتروني	
الإحتيال في تحويل الاموال	
الإبتزاز في التجارة الإلكترونية	
إنقطاع الأعمال و النفقات الإضافية	

هل لدي مقدم الطلب وثيقة تغطية من المخاطر السيبرانية في الوقت الحالي؟

نعم..... لا.....

إذا كانت الإجابة بنعم متى تم شراء تلك التغطية لأول مرة؟

أمن الكمبيوتر والشبكات:

ما هو المنصب للشخص المسؤول عن أمن المعلومات (على سبيل المثال ضابط أمن)

إلى أي شخص داخل الشركة يقدم هذا الشخص تقاريره؟

_____

في ما يتعلق بأنظمة الكمبيوتر هل يمتلك مقدم الطلب ما يلي:

خطة التعافي من الكوارث ☐

نظام الكمبيوتر الثانوي أو الاحتياطي ☐

-٣-

خطة الاستجابة للحوادث الخاصة بعمليات اقتحام الشبكة وحوادث الفايروسات ☐

في حال وجود نظام ثانوي أو احتياطي كم تحتاج من الوقت قبل أن يصبح هذا النظام جاهز للعمل؟

.....

أي مما يلي موجودة مقدم طلب حاليا؟

تحديث برامج مكافحة الفيروسات النشطة ☐

برامج كشف التسلل ☐

إجراءات النسخ الاحتياطي للبيانات القيمة أو الحساسة ☐

إجراءات اختبار او تدقيق ضوابط الأمن السيبراني للشبكة ☐

سياسات وإجراءات شؤون الموظفين وإدارة البائعين

هل يتم تدريب الموظفين في ما يتعلق بالقضايا والإجراءات الأمنية السيبرانية

نعم ..... لا.....

هل يتم إنهاء الوصول إلى جهاز الكمبيوتر عندما يغادر الموظف الشركة

نعم ..... لا.....

هل تم تطبيق الإجراءات المتعلقة بإنشاء كلمات المرور و تحديثها دورياً

نعم ..... لا.....

هل يتم التعرف على الخلفيات الخاصة بموظفي الشركة المحتملين؟

نعم..... لا.....

هل يتعين على مقدمي الخدمات إظهار السياسات والإجراءات الأمنية كافة؟

نعم ..... لا.....

هل تتضمن العقود المبرمة مع مقدمي الخدمات اتفاقيات الحماية والتعويض؟

☐

نعم ..... لا.....

هل يستخدم مقدم الطلب حاليا مزود خدمة سحابية لإجراء الأنشطة التجارية؟

-٤-

نعم..... لا.....

امن المعلومات

- أي نوع من انواع البيانات يقوم مقدم الطلب بجمعها أو استخدامها أو تخزينها أو معالجتها أو نقلها أو الاحتفاظ بها كل جزء من بياناتها ويتعامل بها في أنشطته التجارية؟

بيانات الموظفين الشخصية.....

كلمات مرور بطاقات الدفع الخاصة بالعملاء .....

معلومات الحسابات المصرفية الخاصة بالعملاء.....

البريد الإلكتروني الخاص بالعملاء والموظفين ....

كلمات مرور نظام التشغيل .....

- ما هو الحد الأقصى لعدد الأفراد الذي يقوم مقدم الطلب بجمع وتخزين ومعالجة بياناتهم الشخصية؟

إذا كان ذلك ممكنا هل ان مقدم الطلب يتوافق في الوقت الحالي مع معايير امن بيانات صناعة بطاقة الدفع الإلكترونية (pci dss) ؟

نعم لا

- ما هو إجمالي عدد معاملات بطاقات الائتمان السنوية؟ .....
- إذا كان ذلك ممكن هل توافق مقدم الطلب مع قانون نقل التأمين الصحي والمسؤولية(HIPPA)؟
- هل يقوم مقدم الطلب بتشفير المعلومات الخاصة الحساسة؟

إذا كانت الإجابة بنعم حدد كل ما ينطبق:

البيانات الموجودة بالأجهزه المحموله مثل:

أجهزة الكمبيوتر المحموله

أجهزة المساعد الرقمي الشخصي

محركات أقراص USB وما إلى ذلك

معلومات الموقع و المحتوى

-٥-

هل لدى مقدم الطلب ورقة رسمية مكتوبة لإثبات الملكية الفكرية؟ نعم .... لا.....

هل تم فحص أي علامة تجارية تم الحصول عليها من الآخرين خلال السنوات الثلاث الماضية للتأكد من عدم من انتهاكها المحتوى المنشور عبر الموقع الإلكتروني لمقدم الطلب ؟

نعم..... لا.....

هل توجد إجراءات رسمية من أجل ما يلي:

تجنب نشر محتوى غير لائق او مخالف

نعم ..... لا.....

تحرير أو إزالة المحتوى المثير للجدل أو المسيء أو المخالف؟

نعم..... لا.....

الحصول على إذن الوالدين لجمع البيانات المتعلقة بالأطفال الذين يستخدمون الموقع؟

نعم ..... لا.....

الرد على الإدعاءات بأنه المحتوى تم إن شاء أو عرضها أو نشرها بواسطة مقدم الطلب أو بالنيابة عنه وهل يعتبر ذلك تشهيراً و انتهاكا لحقوق الخصوصية الخاصة ب بالطرف الثالث؟

نعم... لا .....

معلومات الخسائر

هل تلقيت أي شكاوى او دعوى قضائية في ما يتعلق بالخصوصية أو انتهاك المعلومات أو الأمن السيبراني لشبكة أو الكشف غير مصرح به عن انتهاك المحتوى؟

نعم لا

هل خضعت لأي إجراء حكومي أو تحقيق أو أمر استدعاء بخصوص أي انتهاك مزعوم القانون او لائحة تتعلق بالخصوصيه و امن المعلومات ؟

نعم لا

هل تم أخطار العملاء أو الغير بحادث خرق البيانات الذي يتعلق مقدم الطلب؟

نعم لا

هل تعرضت فعليا لمحاولة إبتزاز في ما يتعلق بالأنظمه الكمبيوتر الخاصة بك ؟

نعم..... لا.....

-٦-

هل أن مقدم الطلب أو أي شخص مقترح لهذا التأمين على علم بأي حقيقة أو ظرف أو موقف او حدث أو فعل يمكن أن يؤدي بشكل مباشر أو غير مباشر إلى رفع دعوى ضدهم بموجب وثيقة التأمين من المخاطر السيبرانية التي تقدم بها مقدم الطلب ؟

نعم ..... لا.....

إذا تمت الإجابة على أي سؤال بنعم يرجى على مقدم الطلب إرفاق التفاصيل الخاصة بكل شكوى أو دعوى أو حادث بما في ذلك إرفاق التفاصيل التي تتعلق بالتكاليف أو الخسائر او الأضرار المتكبدة و أية إجراءات تصحيحية لتجنب مثل هذه الإدعاءات في المستقبل و المبالغ المدفوعة بموجب أي وثيقة تأمين أخرى.

(فيما يتعلق بالمعلومات المطلوب الكشف عنها في الأسئلة أعلاه لن يوفر التأمين من المخاطر السيبرانية تغطية لأي دعوى تنشأ عن أي حقيقة او ظرف أو موقف او حدث أو فعل يعلم به المسؤول التنفيذي لمقدم الطلب قبل إصدار هذه الوثيقة ولا على أي شخص أو كيان كان على علم بهذه الحقيقة أو الظرف أو الموقف أو الحدث أو الفعل قبل إصدار هذه الوثيقة)

المرفقات المطلوبة

البيانات المالية الحالية أو السنوية التي تم تدقيقها. إذا كانت حدود المسؤولية عن أمن الشبكات والمعلومات تتجاوز ٣،٠٠٠،٠٠٠ دولار

إشعار التعويض:

للحصول على المعلومات الكافية حول كيفية قيام شركتنا بتعويض العملاء المستقلين او الوسطاء أو شركات التأمين الأخرى يرجى زيارة موقع الويب:

www. travellers.com

إذا كنت تفضل يمكنك الاتصال بالرقم المجاني التالي :

١٨٦٦٩٠٤٨٣٤٨

تحذيرات من الإحتيال

- أي شخص يقدم عمداً مطالبة كاذبة أو احتيالية لدفع خسارة أو منفعة أو يقدم على علم أو عمد معلومات كاذبة في طلب التأمين هذا يعتبر بمثابة جريمة وقد تخضع للغرامات والحبس .
- أي شخص يقوم على عمل وقسم خداعي شركة التأمين بتقديم بيان او طلب يحتوي على معلومات كاذبة او مضلله يعد مرتكب لجناية من الدرجة.

-٧-

(لا تتجاوز العقوبة المدنية ٥٠٠٠ دولار تنتهك من هذا القبيل)

قسم التوقيع

يصرح المفوض الموقع أدناه سواء كان الرئيس أم المدير التنفيذي او كبير مسؤولي الأمن السيبراني لمقدم الطلب انه حسب علمه و اعتقاده وبعد استفسار معقول فإن البيانات الواردة في هذا الطلب أو في طلب تجديد التأمين هي بيانات صحيحة وكاملة ويمكن الاعتماد عليها من قبل شركة التأمين وفي حال تغيير المعلومات الواردة في الطلب قبل ابدأ سريان تاريخ التغطية سيقوم مقدم الطلب بإخطار الشركة بهذه التغيرات ويجوز لشركة التأمين تعديل أو سحب أي عرض قائم كما أن الشركة مخولة بإجراء أي استفسار فيما يتعلق بالمعلومات الواردة بهذه الوثيقة

- إن التوقيع على هذا الطلب لا يلزم شركة التأمين بتقديم التأمين او مقدم الطلب بشراء التغطية

- تم الاتفاق على أن هذا الطلب بما في ذلك أي مرفقات او ملحقات يعتبر أساس التأمين

إسم الممثل المعتمد مطبوع

توقيع الممثل المعتمد الرئيس أو المدير التنفيذي أو رئيس قسم معلومات الأمن السيبراني أو ضابط الأمن لدى مقدم الطلب

التاريخ اليوم الشهر السنة : / /

توقيع الوكيل عن شركة التأمين

رقم الوكالة: .....

رقم الترخيص وتاريخ الترخيص :..... / /

ملاحظة إذا كنت تقدم هذه الوثيقة بصورة إلكترونية فقط قم بتطبيق توقيعك الالكتروني على هذا النموذج عن طريق التحقق من الرابط الإلكتروني ومن خلال القيام بذلك فإنك توافق على استخدامك للوحة

الخاصة بالمفاتيح أو الماوس أو أي جهاز اخر للتحقق من مربع التوقيع الإلكتروني و يعد توقيعك وقبولك و موافقتك كما لو كانت موقعه بالفعل بواسطتك كتابياً ولها ذات القوة في الاثبات .

-٨-

التوقيع و القبول الإلكتروني للممثل المعتمد

التوقيع و القبول الإلكتروني للمؤمن

الملحق (٣)

-١-

شركة هارتفورد للتأمين /هارتفورد، كونيتيكت

06102

(وثيقة التأمين من المخاطر السيبرانية)

- **(وفقاً لوثيقة تغطية المخاطر السيبرانية هذه سيتم تخفيض الحد الأعلى للمسؤولية لدفع التعويضات أو التسويات وقد يتم استنفاده بالمبالغ المتكبدة للدفاع القانوني).**
- **(لاحظ أيًضاً أن المبالغ المتكبدة للدفاع القانوني سيتم تطبيقها على المبلغ القابل للخصم وفقاً لهذه الوثيقة).**

- يرجى قراءة وثيقة تغطية المخاطرالسيبرانية بالكامل بعناية لتحديد الحقوق والواجبات ومايتم تغطيته وما لايتم تغطيته.
- يرجى ملئ البيانات أدناه من قبل المؤمن له:

إجمالي الإيرادات السنوية المتوقعة:.....

قائمة بجميع عناوين URL لموقع الويب:

.....

.....

.....

تاريخ تأسيس الشركة:.....

عدد الموظفين:.....

وصف الشركة:.....

القسم الأول –التغطية المطلوبة

تاريخ نفاذ التغطية المقترحة : .....

-٢-

- حدود المسؤولية المطلوبة:

٢٥٠،٠٠٠دولار

١٠٠٠٠٠دولار

٥٠٠٠٠٠دولار

١،٠٠٠،٠٠٠دولار

٢،٠٠٠،٠٠٠دولار

٥،٠٠٠،٠٠٠دولار

٣،٠٠٠،٠٠٠دولار

١٠،٠٠٠،٠٠٠دولار

- **القسم الثاني – معلومات عامة:**

- فترة السياسة المطلوبة: من ...../...../....إلى...../...../.....

- إسم مقدم الطلب وجميع الشركا ت التابعة:_____

- عنوان مقدم الطلب :_____

- المقر الرئيسي للشركة:_____

- العنوان البريدي لمقدم الطلب:_____

- صافي مصاريف التشغيل : _____

-إجمالي الإيرادا ت: من السلع أو الخدمات و العملاء عبر الإنترنت.....

-٣-

الرمز البريدي :-————————————

ملاحظة : لاتوجد معلومات إضافية ضرورية إذا كان الحد المطلوب للتأمين لايتجاوز ٥٠٠٠٠٠دولار.بخلاف ذلك،يرجى المتابعة.

القسم الثالث – معلومات الاكتتاب العامة ومعلومات الخسارة:

.١ هل تقوم بتشفير جميع أجهزتك المحمولة كأجهزة الكمبيوتر المحمولة، ومحركات الأقراص المحمولة، والهواتف المحمولة، وما إلى ذلك للحفاظ على سرية البيانات؟

.٢هل تستخدم برامج حماية محدثة من الفيروسات والبرامج الضارة كافة لأجهزة الكمبيوترالمكتبية وأجهزة الكمبيوترالمحمولة والخوادم وما إلى ذلك و جدران الحماية على جميع نقاط الوصول الداخلية لديك؟

.٣هل تقوم بتقييد صلاحيات الموظفين والمستخدمين الخارجيين للوصول الى أنظمة تكنولوجيا المعلومات والوصول إلى المعلومات الشخصية المعلومات للعملاء؟

.٤هل تقوم بإجراء نسخ احتياطية لبيانات الأعمال الهامة بشكل إسبوعي على الأقل ؟

.٥هل تعرضت، في أي وقت خلال الـ ٣٦شهراً الماضية، لخطر سيبراني كالقرصنة، التهكير، إصابة بالبرامج الضارة، احتيال، خرق للمعلومات الشخصية، ابتزاز إلكتروني وما إلى ذلك(كلفك أكثر من ١٠٠٠٠دولار أو واجهت دعوى قضائية أو نزاعاً قانوني آخر)مع طرف من أشخاص القانون الخاص أو وكالة حكومية نشأ عن خطر سيبراني؟

نعم..... لا لايوجد.....

٦. خلال ال ١٢ شهراً الماضية هل واجهت انت او احد موفري الخدمة السحابية لديك إنقطاعاً غير مخطط له يدوم أكثر من ساعتين (وهذا لا يشمل الفشل الناجم عن الهجوم السيبراني (الوصول غير المصرح به) اذا كانت الاجابة بنعم يرجى ارفاق التفاصيل.

_____

_____

_____

- **ملاحظة : لا توجد معلومات إضافية مطلوبة اذا كان الحد الاعلى للتغطية ١٠٠٠،٠٠٠ دولار يرجى التوقيع وادراج التاريخ مع الطلب .**

-٤-

القسم الرابع :الأجهزة والمعلومات وإدارة البائعين

١.ما عدد الأجهزة التالية لديك في الوقت الحالي:

الخوادم: .....

أجهزة الكمبيوتر المكتبية:.....

أجهزة الكمبيوتر المحمولة:.....

الهواتف المحمولة/ الأجهزة:.....

.٢ما هو عدد الأشخاص (الموظفين والعملاء وما إلى ذلك) الذين يقومون حاليا بتخزين أو الاحتفاظ بالمعلومات الخاصة بهم) سواء بنفسك أو باستخدام أطراف ثالثة ؟

.٣هل تقوم بمعالجة أوتخزين المعلومات الشخصية أو غيرها من المعلومات السرية للشركات الأخرى أو المنظمات؟

.٤لكل بائع يقوم بمعالجة أوتخزين المعلومات الشخصية لك، هل لديك عقد مكتوب او اتفاقية تجعل البائع مسؤولاً مالياًعن عواقب الهجوم السيبراني أو خرق البيانات؟ إذا لم تقم بإشراك أي من هؤلاءالبائعين، أجب بـ"نعم"

.٥ هل تطلب من مقدمي الخدمة وسائل الأمان الكافية؟

نعم ..... لا.....

- **القسم الخامس – السياسات الداخلية والامتثال وإدارة الخصوصية**

.١ هل لديك سياسة مكتوبة للخصوصية والأمان على مستوى الشركة؟

.٢هل لديك آلية معينة للاحتفاظ بالمستندات وإتلافها؟

. ٣ هل قمت بإجراءات أمان على شكل عقود مكتوبة تتطلب ما يلي :

أ-(التأكيد عبر الهاتف)أو عن طريق وسائل أخرى غير البريد الإلكتروني(مع المستفيد أو مقدم الطلب، على تفاصيل الدفع قبل إجراء الدفعات)بما في ذلك التحويلا ت البنكية وتحويلات)ACH التي تزيد قيمتها عن ١٠٠٠٠دولار؟

ب- أطراف داخلية متعددة لتأكيد التفويض قبل إجراء الدفعات (بما في ذلك التحويلات البنكية)ACH والتي تزيد قيمتها عن ١٠٠٠٠دولار؟

-٥-

.٤هل لدى كل مستخدم لنظامك حساب فردي منفصل؟

.٥ هل تمتلك عملية رسمية تضمن التحديد والتتبع والمراقبة (لإرجاع الخوادم وأجهزة الكمبيوتر المكتبية والمحمولة وغيرها من الأصول الرقمية إلى الخدمة بشكل صحيح و عملية رسمية تضمن الإزالة من الشبكة و الحذف من المخزون والمسح الآمن للبيانات الحساسة(لإزالة تلك الأصول من الخدمة بشكل صحيح؟

.٦إذا كنت تتعامل ببطاقات الدفع الخاصة بالائتمان والخصم، فهل تمتثل بطاقات الدفع لمعاييرالأمن السيبراني ؟ (إذاكنت لاتقبل بطاقات الدفع،أجب بـ"لاينطبق"

.٧إذا كنت تتعامل مع المعلومات الصحية، فهل تلتزم بقانون (HIPAA)وقانون ؟ (HITECH) إذا كنت لاتتعامل مع المعلوما ت الصحية، أجب ب "نعم"

.٨هل لديك مدير مسؤول عن أمن الشبكات او المعلومات أو أي موظف آخر مسؤول عن ا لمعلومات و أمن الأنظمة؟

.٩هل قمت بتحديد و تأمين المعلومات الشخصيةو غيرهامن المعلومات السرية للغاية التي أنت عليها مسؤول؟

- **القسم السادس – أمن الشبكة وإدارة الحوادث**

.١هل تقوم بتحديث وتصحيح أنظمة وتطبيقات تكنولوجيا المعلومات الهامة على أساس شهري على الأقل؟

.٢هل قمت بتنفيذ استخدام كلمات مرور طويلة ومعقدة أو منهجية أخرى آمنة للوصول إلى الحساب مثل التعريف متعدد العوامل أو التعريف الشامل؟

نعم ..... لا لايوجد.....

نعم ..... لا لايوجد.....

. ٣هل ان كافة الأنظمة التي يمكن الوصول إليها عبر الانترنت على سبيل المثال الويب وخوادم البريد الالكتروني ، داخل المنطقة المجردة من السلاح أو لدى مزود طرف ثالث من شبكتك الموثوقة؟

.....

٤. هل تستخدم أجهزة أوبرامج كشف التسلل أوتقوم بمراقبة شبكتك والتعرف عليها بطريقة؟

.....

-٦-

٥.هل تقدم تدريًبا توعويًا للموظفين فيما يتعلق بقضايا خصوصية البيانات و الأمن السيبراني) بمافي ذلك قضايا المسؤولية ا لقانونية و التصيد الإحتيالي ؟

.....

٦.هل تقوم بحذف الوصول إلى النظام والحسابات والحقوق المرتبطة بها بعد إنهاء خدمة المستخدمين (بما في ذلك الموظفين الدائميين والموظفين المؤقتين والمقاولين والبائعين)؟

.....

٧- هل تقوم بنفسك أو من خلال الاستعانة بمورد خارجي(بفحص انظمة التشغيل المهمة بانتظام من أجل الأمان للتعرف على نقاط الضعف ؟(قد تتضمن عمليات الفحص هذه اختبار الأمان والإختراق) .

.....

٨- إذاكنت تقوم بإجراء نسخ احتياطي لبيانات العملاء المهمة بشكل اسبوعي على الأقل ،فهل يتم تخزين النسخةالاحتياطية خارج الموقع في مكان آمن؟

.....

إذا لم تقم بعمل نسخة احتياطية لبيانات العملاء المهمةأسبوعًياعلى الأقل،فأجب بـ"غيرمتاح"

٩.إذاكنت تقوم بإجراء نسخ احتياطي لبيانات العملاء المهمة أسبوعًيا على الأقل،فهل تختبر استعادتك للبيانات حال فقدانها ؟

.....

اذا لم تقم بنسخ بياناتك مرة اسبوعياً على الأقل،فأجب بـ"غيرمتاح"

١٠.هل لديك خطة للتعافي من المخاطر السيبرانية ؟

نعم ..... لا.....

١١.هل لديك خطة للاستجابة للمخاطر السيبرانية كالهجمات السيبرانية و انتهاكات البيانات؟

نعم..... لا.....

.١٢هل لديك عملية لمراجعة جميع الإعلانات والمحتويات الأخرى قبل النشر؟

نعم..... لا.....

-٧-

إشعار لمقدمي الطلبات في الولايات: أي شخص يقوم عن علم،وبقصد الاحتيال أوخداعاً لشركة تأمين أو أي شخص آخر،بتقديم طلب للتأمين أوبيان مطالبة يحتوي على أي معلومات كاذبة من الناحية المادية ،أو يخفي لغرض معلومات مضللة عن أي حقيقةجوهرية،او يرتكب عملاً احتياليًا،مما يعدجريمة وقد يعرض هذا الشخص للعقوبات الجنائيةو المدنية.

إشعار لمقدمي الطلبات في كانساس: "قانون التأمين الاحتيالي"يعني أي فعل يرتكبه أي شخص، عن علم وبقصد الاحتيال، أويقدم أويتسبب في تقديمه أويستعد مع العلم أو الاعتقاد بأنه سيتم تقديمه إلى شركة التأمين أو بواسطتها، أو أي وكيل له، أي رسالة أوبيان مكتوب أو إلكتروني أو فاكسي أو مغناطيسي أوشفهي أو هاتفي كجزء من أو لدعم طلب لإصدار أوتصنيف وثيقة تأمين للأفراد أو التأمين التجاري، أو المطالبةبالدفع أو أي منفعة أخرى بموجبب وثيقة تأمين للتأمين التجاري أو الشخصي والتي يعلم هذا الشخص أنها تحتوي على معلومات كاذبة ماديًا في ما يتعلق بأي حقيقة جوهرية تتعلق بها؛ أو أخفى،بغرض التضليل، معلوما تتتعلق بأية حقيقة جو هرية تتعلق به.

إشعار لمقدمي الطلبات في كنتاكي ونيويورك وبنسلفانيا: أي شخص يقوم عن علم وبقصد الاحتيال على أي شركة تأمين أو أي شخص آخر بتقديم طلب للتأمين أوبيان مطالبة يحتوي على أي معلوما ت كاذبة ماديًا أويخفي لغرض التضليل معلومات أو أي تحريف متعمد أو إهمال أو إغفال أو إخفاء أوبيان غير صحيح لحقيقة جوهرية، في هذا الطلب أو غير ذلك،يجب أن يكون سبباً لإلغاء أي سند أو وثيقة صادرة.

بالنسبة للمتقدمين في ولايتي ماين وماريلاند فقط:يتم حذف كلمة "إلغاء" واستبدالهابكلمة "إنكار".

إشعار لمقدمي الطلبات:

يترتب على وجود أكثر من طلب تعويض عن نفس الضرر أو الخسارة جناية، ويعاقب عند الإدانة على كل مخالفة بغرامة لاتقل عن خمسة آلاف (٥٠٠٠) دولار ولا تزيد على عشرة آلاف (١٠٠٠٠) دولار، أو السجن لمدة محددة لمدة ثلاث سنوات، أو كلتا العقوبتين. وفي حالة وجود ظروف مشددة يجوز زيادة العقوبات المقررة على هذا النحو إلى مدة أقصاها خمس سنوات ،وفي حالة وجود ظروف مخففة يحوز تخفيضها إلى سنتين على الأقل .

-٨-

يرجى قراءة البيان التالي بعناية والتوقيع حيثما هو مبين:

- يقرّ المسؤول المفوض الموقع أدناه أو مالك أو مدير مقدم الطلب بأنه على علم بأن حد المسؤولية الوارد في جزء التغطية من المخاطر السيبرانية سيتم تخفيضه، وقد يتم استنفاده بالكامل، من خلال تكاليف الدفاع القانونية، وفي مثل هذا في هذه الحالة، لن تكون شركة التأمين مسؤولة عن تكاليف الدفاع القانونية أو عن مبلغ أي حكم أوتسوية إلى الحد الذي يتجاوز فيه حد مسؤولية جزء التغطية من المخاطر السيبرانية.

- يقرّ الموظف المفوض الموقع أدناه او المالك مدير مقدم الطلب بأنه على علم بأن تكاليف الدفاع القانونية التي يتم تكبدها سيتم تطبيقها على المبلغ القابل للخصم.

- يقرّ الموظف المفوض أو مالك أو مدير مقدم الطلب الموقع أدناه بأن المعلومات المقدمة في هذا الطلب كاملة وصحيحة وصحيحة.

- يوافق المسؤول المفوض أو المالك أو المدير الموقع أدناه على أنه إذا تغيرت المعلومات المقدمة في هذا الطلب بين تاريخ هذا الطلب وتاريخ نفاذ التأمين، فإن الموقع أدناه(ملزم بأن تكون المعلومات دقيقة وفقاً لتاريخ سريان التأمين، وإخطارشركة التأمين على الفور بهذه التغييرا ت، ويجوز لشركة التأمين سحب أوتعديل أي عروض أسعار و/أوتفويضات أو اتفاقيات ملزمة للتأمين).

- لمقدمي الطلبات في جورجيا فقط: أي تحريف أو إغفال أو إخفاء أوبيان غير صحيح لحقيقة جوهرية، في هذا الطلب أو غير ذلك،يعد سبباً لرفض التغطية وإلغاء أي سند أو وثيقةتأمين صادرة.

- لمقدمي الطلبات في لويزيانا فقط: أي تحريف أو إغفال أو إخفاء أوبيان غير صحيح لحقيقة جوهرية، في هذا الطلب أو غير ذلك،يعد سبباً لرفض أي مطالبة تتعلق بأي تحريف أو إغفال أوإخفاء أوبيان غيرصحيح أوإلغاء أي سندات أوبوليصة صادرة،بشرط أن تستمرالتغطيةللمطالبات المشروعة حتى يصبح الإلغاء ساري المفعول.

-٩-

التوقيع على هذا الطلب :

(لا يلزم مقدم الطلب أو المؤمن بإتمام التأمين، ولكن من المتفق عليه أن يكون هذا الطلب أساس العقد في حالة إصدار وثيقة التغطية من المخاطر السيبرانية).

إمضاء مقدم الطلب:.....

اسم مقدم الطلب و عنوانه:.....

التاريخ:.....

رقم الرخصة: ٦٩٥٢

ملاحظة : (يجب التوقيع من قبل المسؤول أو المالك أو المدير)

الملحق (٤)

وثيقة تأمين من المخاطر السيبرانية لشركة (QBE)

(بلجيكا)

ما هية هذا النوع من التأمين؟

- هذا التأمين يغطي المسؤولية القانونية لدفع التعويض الناشئ عن الخطر السيبراني والذي يتعلق بإصابة شخصية للمؤمن له او الغير أو يحدث أضرار في الممتلكات ناجمة عن الخطر أو فيما يتعلق بأعمال المؤمن له.

- ما الذي يدخل في نطاق التغطية ؟

- المسؤولية عن المخاطر السيبرانية و التعويض عن أي ضرر ناشئ عنه وتكاليف الدفاع التى يتم تقديمها لأول مرة ضد المؤمن له خلال فترة التغطية والتي تنشأ عن أي خطرسيبراني فعلي أو مزعوم يكون المؤمن له على علم به لأول مرة خلال فترة التغطية.
- مسؤولية وسائل الإعلام عبر الإنترنت: من خلال التعويض عن أي مطالبة إعلامية وتكاليف الدفاع التي تم تقديمها أولا ضد المؤمن له خلال فترة التغطية والتي علم بها المؤمن له لأول مرة خلال فترة التغطية.

- التعويض عن انقطاع الأعمال: التعويض عن فقدان دخل الأعمال الذي يتكبده المؤمن له خلال فترة الإعادة إلى وضعه السابق نتيجة لي فشل المؤمن له أو مزود الخدمة في الحماية ضد خرق الشبكة

- تكاليف إستعادة البيانات: التعويض عن التكاليف والمصاريف المتكبّدة في إصلاحها أو استبدال أو استعادة البيانات الإلكترونية والأجهزة المتضرر التي اكتشف المؤمن له فقدانها أو تلفها او تدميرها.

- الابتزاز السيبراني وتشمل التعويض عن نفقات الإبتزاز السيبراني الناشئة عن تهديد الإبتزاز السيبراني خلال فترة التغطية.

- التكاليف القانونية الناجمة عن خرق البيانات وتشمل التعويض عن النفقات القانونية و تكاليف الأخطار وخرق البيانات الناشئة عن الخطر السيبراني الفعلي أوالمشتبه بتحققه والذي يصبح المؤمن له على علم به لأول مرة خلال فترة التغطية.

-٢-

- تكاليف الطب الشرعي وتشمل التعويض عن تكاليف الطب الشرعي السيبراني التي يتكبدها مستشار الطب الشرعي نتيجة للمخاطر السيبرانية أو تهديد الابتزاز السيبراني الذي يصبح المؤمن له العلم به لأول مرة خلال فترة التغطية

- تكاليف العلاقات العامة: تعويض مستشار اللجنة العلاقات العامة ومستشار إدارة الأزمات لتجنب أو تخفيف أي ضرر كبير لأي من العلامات التجارية والعمليات التجارية للمؤمن له نتيجة للمخاطر السيبرانية التي يصبح المؤمن له على علم بها لأول مرة خلال فترة التغطية.

- مراقبة الائتمان أو تكاليف الهوية والعقوبات: التعويض عن تكلفة تقديم خدمات مراقبة الائتمان أو سرقة الهوية التي يتكبدها المؤمن عليه لمدة أقصاها ١٢ شهرا المتضررين من انتهاك الخصوصية الذي يعلم به المؤمن له لأول مرة خلال فترة التغطية

- التعويض عن تلك المبالغ التي يكون المؤمن له ملزماً قانونا بدفعها نتيجة انتهاك الخصوصية أو خرق قانون حماية البيانات لأي تكاليف قانونية وتحقيقية نتيجة لإجراء تنظيمي مدني أو عقوبة مدنية او غرامات مفروضة من جهة تنظيم حماية البيانات رد المؤمن له

- تكاليف (PCI DSS) وتشمل التعويض عن التكاليف التي تتكبدها الشركة المؤمن لها أثناء المطالبة بالتعويض وتكاليف الدفع المقدمة أولاً ضد المؤمن له من قبل كيان بطاقة الدفع أو الطرف الذي يكون المؤمن عليه مسؤولا امامه عن المطالبة الناشئة عن انتهاك الخصوصية خلال فترة

- تكاليف الطوارئ الموافقة بأثر رجعي على تكاليف الطب الشرعي والتكاليف القانونية لخرق البيانات والتكاليف الأخطار في خرق البيانات وتكاليف العلاقات العامة التي يتكبدها واحد أو أكثر من مستشاري اللجنة.

- مبلغ التأمين:

تخضع مسؤولية شركة كيو بي اي للتأمين لحد إجمالي شامل ولحدود مختلفة وحدود فرعيه مذكورة في جدول التغطية

- **الاستثناءات الواردة على التغطية والتي لا يمكن التأمين منها:**

- الإصابة الجسدية أو الخسارة جسدية أو تدمير أو إتلاف الممتلكات المادية

- المسؤولية الناشئة عن العمل

- المسؤولية الشخصية التي يتكبدها المؤمن عليه كونه المدير أو المسؤول

- المخاطر الناجمة عن الكوارث الطبيعية

- المخاطر النووية و الإشعاعية المؤينة

-٣-

- إنتهاك أي براءة الاختراع أو الاستخدام غير المصرح به للأسرار التجارية.

- خسائر التداول والتزامات المؤمن له.

- الإصابة الجسدية أو الضرر أو المطالبة أو الخسارة او المسؤولية أو النفقات أو تكاليف الدفاع الناجمة عن الحرب أو الإرهاب.

- خرق قوانين الضرائب أو المنافسة أو تقييد التجارة او تشريعات ولوائح مكافحة الاتجار أو الاتصالات غير المرغوب فيها.

- المطالبة بشكل مباشر أو غير مباشر بسبب تلوث أو المجالات الكهرومغناطيسية.

- إرجاع الرسوم أو العمولات.

- فشل مزود الإنترنت او الاتصالات أو الكهرباء أو أي مزوج مرفق عام آخر.

- البضائع والمنتجات التي تم بيعها أو تريدها أو إصلاحها أو تغييرها أو معالجتها أو تصنيعها أو تركيبها أو صيانتها من قبل المؤمن له أو نيابة عنه.

قيود التغطية

أولاً: لا تتحمل شركة كيو بي أي مسؤولية عن إجراء أي مدفوعات بموجب هذه الوثيقة بشكل مباشر أو غير مباشر لأي جهة.

ثانياً: تكاليف إصلاح أو استبدال أو استعادة نظام الكمبيوتر الخاص للمؤمن له إلى مستوى يتجاوز ما كان موجوداً قبل أي مطالبة أو خسارة.

ثالثاً: المطالبة المقدمة بشكل مباشر أو غير مباشر من قبل أو نيابة عن أي مؤمن له أو أحد الوالدين أو الشركة التابع للمؤمن له أو أي كيان يكون فيه المؤمن له أو مديره او شريكه او عضو في مصلحة تنفيذية أو مسؤولية أو لديه مساهمة او أي أموال أخرى.

رابعاً: تصرف غير آمين أو احتيال من جانب المؤمن له أو اي خرق متعمد او متهور من قبل المؤمن له لأي قانون او لائحة.

خامساً: حدوث الخطر السيبراني بأثر رجعي أو اختيار أي شركة تأمين أخرى تغطي نفس موضوع وثيقة التأمين السابقة.

سادسا: الإعلانات الكاذبة الممارسات التجارية الخادعة الناشئة عن محتوى الوسائط.

-٤-

سابعاً: الغرامات والعقوبات

ثامناً: إستخدام الألعاب او المقامرة او اليانصيب

تاسعاً: مصادرة أو استيلاء أو تدمير أو إتلاف نظام الكمبيوتر او معلومات التعريف الشخصية من قبل الحكومة.

عاشراً: التسعير غير دقيق للسلع أو المنتجات

أحد عشر: المؤمن له الذي يعمل بصفته وصياً او أمين أو مدير الهيئة التقاعد الخاصة بالمؤمن له او مشاركة الأرباح أو برنامج مزايا الموظفين.

اثني عشر: التغطية التي من شأنها أن تعرض البنك لأي عقوبة أو خطر أو تقييد بموجب قرارات الأمم المتحدة أو التجارة أو الاقتصاد أو العقوبات أو القوانين او اللوائح.

ثلاثة عشر: استخدام المؤمن له البرامج بشكل ينتهك أي حقوق ملكية فكرية لأي طرف.

ما هي إلتزاماتي كمقدم للطلب ؟

يجب عليك أن:

- تقوم بتقديم جميع مخاطرك عند إبرام هذا التأمين بما في ذلك الأفصاح بشكل شامل ودقيق عن ماهية المخاطر التي تتعرض لها الشركة المؤمن لها قبل الوثيقة و أثناء الوثيقة وبعدها.
- أخطارنا كتابياً بأي دعوى أو شكاوى قد تصبح دعوى في المستقبل بشرط أن تكون ضمن الفترة الزمنية المذكورة في التغطية. -
- عدم الإقرار بأي مسؤولية أو إلتزام أو تقديم عرض أو وعد أو عرض الدفع أو التعويض أو تحمل أي نفقات دون موافقة كتابيه من شركة التأمين كيو بي اي وتقديم كل هذه المعلومات والتعاون والمساعدة على إعادة توجيه جميع المستندات والمعلومات كما هو مطلوب من شركة كيو بي اي.
- قد تطلب شركة التأمين عدم حذف الأدلة والمعلومات المستندات الداعمة دون موافقة كتابيه مسبقة أو تدمير الممتلكات المتعلقة بالحدث أو خسارة أو دعوى قد تؤدي إلى دعوى.
- يلتزم المؤمن له بالدفاع عن المطالبة أو دعوى وذلك من من خلال القيام بكل ما تطلبه شركة كيو بي اي لتأمين الاسترداد و تقديم أي مساعدة وتعاون إلى الشركة المؤمنة قدر المستطاع

وأخبارنا بجميع التغيرات الجوهرية في النشاط التجاري المعلن أو المخاطر المؤمن منها إذا كانت تطلب تغطيتها بموجب هذا التأمين.

-٥-

- الالتزام بالشروط العامة واي شروط محددة تهدف إلى تقليل الخسارة الناجمة عن المخاطر السيبرانية المؤمن منها.

متى وكيف ادفع؟

يتم تحديد مدة دفع الأقساط تفاصيل الدفع الأخرى في الوثيقة و جدول الوثيقة.

أين يتم التغطية ؟

ما لم ينص على خلاف ذلك في الوثيقة ينطبق هذا التأمين على جميع أنحاء العالم

كيف ألغي العقد؟

يرجى التأكد من أنه الوثيقة مناسبة لمتطلبات حيث لا توجد حقوق إلغاء من جانبك. و يجوز لشركة كيو ب ياي إلغاء التأمين في حالة عدم دفع القسط

ما هي فترة التغطية ومتى؟

التأمين هو عقد سنوي مالم ينص على خلاف ذلك ويجوز تجديده في نهاية كل سنة ويتم ذكر تاريخ البداية تاريخ الانتهاء الوثيقة في الجدول.

اسم المؤمن له:

التوقيع:

ملحق (٥)

-١-

وثيقة التأمين من المخاطر السيبرانية لشركة نورثبريدج للتأمين / كندا

(من خلال استكمال هذا الطلب يكون مقدم الطلب قد تقدم بطلب الحصول على تأمين لدى شركة نورثبريدج للتأمين)

يرجى القراءة بعناية : (إذا تم إصدار وثيقة التأمين من المخاطر السيبرانية فإنها تغطي ما يتم المطالبة به والذي يتم تقديمه لأول مرة فقط وإبلاغ شركة التأمين به خلال فترة الوثيقة ، و سيؤدي دفع الخسارة والنفقات -إذا كان القانون يسمح بذلك- وخسارة الطرف الأول إلى تقليل حد المسؤولية).

- يجب الإجابة على جميع الأسئلة بشكل كامل وإذا لم تكن هناك إجابة فأكتب لا شي أو لا يوجد في المكان المخصص عندما تكون المساحة المتوفرة غير كافية للإجابة الكاملة يرجى استخدام أوراقاً منفصلة .

أ-معلومات عامة:

إسم مقدم الطلب :.....

العنوان البريدي : .....

سنة تأسيس العمل التجاري لمقدم الطلب :.....

يرجى وصف الأعمال التي يقوم بها مقدم الطلب:

.....

مقدم الطلب هو :

شركة ☐

مؤسسة ☐

شيء آخر ☐

يرجى تقديم عناوينURL العامة:.....

-٢-

هل يلتزم مقدم الطلب بالمتطلبات الأمنية الأساسية التالية :

- تشغيل برامج مكافحة الفيروسات بشكل مستمر وقبول كافة التحديثات التلقائية الخاصة بالموردين على أنظمة الكمبيوتر الخاصة بمقدم الطلب :

نعم ..... لا.....

- تمكين التصحيح التلقائي للبائعين البرامج و أنظمة التشغيل:

نعم. ..... لا.....

-اختبار دورات التصحيح ونشرها على مجموعات كبيرة من الخوادم وأجهزة الكمبيوتر المكتبية:

نعم ..... لا.....

-هل يستخدم مقدم الطلب تقنية جدار الحماية الحالية:

نعم ..... لا.....

-هل يوجد نظام ثابت للنسخ الاحتياطي واستعادة بيانات النظام :

نعم ..... لا.....

-إذا كانت الإجابة بنعم فهل يتم تطبيقه على جميع الأنظمة الخاضعة لسيطرة مقدم الطلب:

نعم ..... لا.....

-هل يستخدم مقدم الطلب برامج لكشف الخلل التقني في أنظمة التشغيل أو خدمات المراقبة الأخرى:

نعم ..... لا.....

-يرجى تقديم إجمالي الإيرادات الموحدة للسنة المالية الحالية و عدد الموظفين بما ذلك المتطوعين والمقاولين المستقلين حسب البلد:

.....

-٣-

(يرجى تحديد حد المخاطر السيبرانية/إجمالي مبلغ التأمين الذي يتطلب وهو مقدم الطلب):

٥٠٠،٠٠٠ دولار

١،٠٠٠،٠٠٠ دولار

٢،٠٠٠،٠٠٠ دولار

- يرجى تحديد المبلغ القابل للخصم المطلوب:

١٠٠٠ دولار

٥٠٠٠دولار

١٠،٠٠٠ دولار

- هل يحمل مقدم الطلب حاليا تأمين على أمن الإنترنت/الشبكات ومسؤولية الخصوصية:

نعم _____ لا_____

- هل يمتلك مقدم الطلب اكثر من ٥٠،٠٠٠ سجل معلومات شخصية بتنسيق ورقي او رقمي؟
(إذا كانت الإجابة بنعم كم ؟إذا كان الجواب لا من فضلك لا تُجب)

من ٥٠٠،٠٠١ دولار إلى ١،٠٠٠،٠٠٠ دولار

< ١٠،٠٠٠،٠٠٠ دولار

١٠،٠٠٠،٠٠٠ دولار>

ملاحظة : معلومات تحديد الهوية الشخصية هي معلومات تعريف شخصية يمكن استخدامها لتحديد هوية فرد واحد او الاتصال به أو تحديد موقعه ، على سبيل المثال رقم التأمين الاجتماعي و رخصة القيادة و تفاصيل الرعاية الصحية و تفاصيل بطاقة الائتمان للعملاء والموظفين.

ب-التغطية المخصصة

يتم إكمال القسم ب - ز فقط إذا كان مقدم الطلب يتطلب تغطية احادية او يتطلب حتى يزيد عن ١،٠٠٠،٠٠٠ دولار او لديه اكثر من ٥٠،٠٠٠ سجل او الإيرادات السنوية اكثر من ١٥،٠٠١ دولار وإلا انتقل إلى الأقسام الأخرى و اكملها.

هل يقبل مقدم الطلب معاملات بطاقة الدفع الإلكتروني ؟

نعم لا

-٤-

- إذا كانت الإجابة بنعم فهل إن مقدم الطلب متوافق مع مستوى PCI DSS المعني؟

نعم ..... لا.....

- إذا كانت الإجابة ب (لا) يرجى توضيح السبب ويرجى تقديم خطة العمل لمعالجة المتطلبات غير المتوافقة أو الامتثال للتاريخ الاخير.

-هل تتمتع جميع الشبكات اللاسلكية بوصول محمي؟

نعم ..... لا.....

-هل لدى مقدم الطلب إجراءات التحكم في الوصول إلى محرك تشفير لمنعها من التعرض غير المصرح به إلى البيانات الموجودة على جميع الاجهزة المحموله كمحركات الأقراص وأجهزة الكمبيوتر المحموله والهواتف الذكية وما إلى ذلك؟

نعم ..... لا.....

-هل جميع مهام الموظفين محددة بوضوح وتم منح الموظفين حقوقهم محددة كل امتيازات وكلمات المرور الفريدة لمعرف المستخدم والتي تتم مراجعتها والتحقق من صحتها بشكل دوري؟

نعم ..... لا .....

-هل تلقى جميع الموظفين تدريبا للتوعية من خطر التهديدات السيبرانية التي يمكن أن تؤدي إلى حدوث انتهاكات في نظام التشغيل ؟

نعم ..... لا.....

-هل يقوم مقدم الطلب بإنهاء جميع حسابات الوصول إلى الكمبيوتر وحسابات المستخدمين المرتبطة به على الفور كجزء من عملية الخروج عندما يغادر الموظف الشركة ؟

نعم ..... لا .....

- في حالة وقوع هجوم مثل برنامج الفيديو ما هو الوقت الذي يحتاج هو مقدم الطلب استعادة البيانات :

ثمانية إلى ١٢ الساعة.....

١٢ ساعة.....

١٤ الساعة.....

٤٨ ساعة.....

-٥-

أكثر من ذلك .....

-ما هي مخططات مقدم الطلب لتحقيق هدفه في استعادة المعلومات بعد برامج الفدية؟

.....

- هل لدى مقدم الطلب برنامج رسمي لإجراء اختبار اختراق أو تدقيق روابط أمن الشبكة سنويا؟

نعم لا

- هل لدى مقدم الطلب سياسة خصوصية موثقة بما في ذلك المبادئ التوجيهية للإبلاغ عن الانتهاك؟

(إذا كانت الإجابة بنعم)

- هل يتناول الإلتزامات الإقليمية لمقدم الطلب بموجب حماية الخصوصية والبيانات

نعم لا

-هل تتناول إلتزامات مقدم الطلب العالمية بموجب حماية الخصوصية والبيانات؟

نعم لا

هل يتضمن بيان المستخدمين حول كيفية إستخدام المعلومات التي تم جمعها و لأي أغراض؟

نعم لا

هل هناك إجراءات لتلبية طلبات العملاء المفصح عن معلوماتها الشخصية؟

نعم لا

هل تتم مراقبة الفترة التي من خلالها يتم الاحتفاظ ببيانات العميل وعمليات حذف هذه المعلومات في نهاية تلك المدة؟

نعم لا

هل هنالك إجراءات لحذف جميع البيانات الحساسة من الأنظمة والأجهزة الخاصة بالشركة؟

نعم لا

-٦-

ج- مقدم خدمات الانترنت

- هل يقوم مقدم الطلب بإجراء مراجعات منتظمة لمقدمي الخدمات والشركات الخارجية للتأكد من أنهم مستوفين المتطلبات مقدم الطلب لحماية المعلومات الموجودة تحت رعايتهم؟

نعم لا

هل يحصل مقدم الطلب على دليل المسؤولية السيبرانية لأمن الشبكة و الخصوصية أو تأمين التكنولوجيا والتشغيل من مقدمي الخدمات الخارجين؟

نعم لا

د-الوسائط المتعددة والملكية الفكرية:

هل تخضع جميع الأنشطة الإعلامية التي تواجه الجمهور للمراجعة القانونية قبل النشر؟

نعم لا

هل لدى مقدم الطلب إجراءات للتعديل او الإزالة او الرد على المخالف أو المحتوى غير اللائق او غير الدقيق بما في ذلك المحتوى موقع الويب او الوسائط الاجتماعية؟

نعم لا

ه-بيانات الضمان:

-هل واجه مقدم الطلب خلال السنوات الخمس الماضية خرقاً لأمن الشبكة أو فيروسات أو هجوماً برمجيات ضارة أو فقدان أو سرقة البيانات المادية أو الرقمية أو حادث قرصنة او لبرامج فيديو؟

نعم لا

-هل هناك أي حقائق أو ظروف ومواقف يمكن أن تؤدي إلى تقديم الدعوى ضد المؤمن له المشمول بهذه التغطية؟

نعم لا

-خلال السنوات الخمس الماضية هل تم تقديم أي خسارة أو دعوى ضد مقدم الطلب سواء كان مؤمن له أم لا في ما يتعلق بأي نوع من انواع التأمين المذكورة في هذا الطلب؟

نعم لا

-٧-

-هل سبق أن تم رفض مقدم الطلب أو عدم تجديده أو الغائه من قبل أي شركة التأمين من المخاطر السيبرانية ؟

نعم لا

- خلال السنوات الخمس الماضية هل تلقى مقدم الطلب شكوى بخصوص المحتوى المنشور عبر الإنترنت من قبل مقدم الطلب أو بالنيابة عنه؟

نعم لا

إذا كانت الإجابة بنعم على أي مما ورد عليه في القسميها يرجى تقديم التفاصيل الكاملة في ورقة منفصلة تتضمن :

تاريخ الدعوى

اسم المدعي

وصف الدعوى بما في ذلك الأضرار المزعومة

مبلغ التعويض النفقات المدفوعة

التدابير المتخذة لمنع المطالبات المماثلة

(دون المساس بأي حقوق لشركات التأمين يُفهم مقدم الطلب ويوافق على أنه في حالة وجود أي حقيقة أو ظرف او موقف سواء تم الكشف عنه أولاً في أعلاه فإن أي تعويض أو دعوى أو إجراء نشأ عن هذه الحقيقة أو الظرف فإنه سيتم استثناء ذلك من التغطية بموجب هذه الوثيقة.)

و- التصريحات :

- يعتبر هذا الطلب ومرفقاته أساس العقد في حال إصدار الوثيقة ويعتبر ملحقا بالوثيقة و يشكل جزء منها ويحق لشركة التأمين بموجب هذا إجراء أي تحقيق أو استفسار فيما يتعلق بهذا الطلب الذي تراه ضروريا ويسمح به القانون.

- لا يمكن الالتزام بالتغطية ما لم يتم استكمال نموذج الطلب هذا و توقيعها بالكامل والموقع أدناه لديه سلطة لإكمال تنفيذ هذا الطلب.

-٨-

ز- الأفصاح عن الخصوصية والموافقة عليها :

يقر الموقع أدناه نيابة عن المنظمة أو الشركة المؤمن لها أنه حصل على الموافقة اللازمة لجمع وإستخدام المعلومات و الأفصاح بها لشركة التأمين سواء كانت معلومات شخصية أو غيرها أو فيما يتعلق بأي معلومة وارده بهذا الطلب أو تجديد أو تغيير في التغطية لأغراض عرض وتوفير الخدمات لتلبية احتياجات الشركة المؤمن لها وتقييم المخاطر والإكتتاب فيها على أساس واضح وتحديد الأسعار لخدمات التأمين والتحقيق في الدعوى وتسويتها واكتشاف ومنع الإحتيال او الأنشطة غير القانونية الأخرى وتحليل نتائج الأعمال و تجميع الإحصائيات وتقديم التقارير إلى الكيانات التنظيمية والتصرف وفقا لما يقتضيه القانون او يسمح به.

توقيع مقدم الطلب :.....

العنوان :.....

إسم الشركة طالبة التأمين:.....

تاريخ توقيع الطلب :.....

Abstract:

Abstract:

Providing insurance protection for commercial companies against cyber risks is a modern and effective way to absorb financial losses resulting from a violation of the security of operating systems، since the insurance market in general tends to create many incentives to build more secure systems for those companies، but at the same time insurance is still one of Cyber risks are shrouded in a kind of ambiguity، due to the lack of specialized legislation for this type of insurance and the small number of companies that deal with this type of insurance coverage، which leads to hesitation and caution among commercial companies in general about purchasing insurance coverage against cyber risks، especially since these risks do not It is still not bound by a specific and clear standard، which leads clients who own commercial companies to not understand the nature of the risks contained in the terms of the cyber risk insurance contract. Insurance against cyber risks is also distinguished from insurance contracts against traditional risks by a number of requirements that may precede or accompany the stage of concluding the insurance contract، in addition to the higher premiums compared to the types of traditional insurance contracts due to the lack of historical data on this type of risk due to its recentness، which leads to the difficulty of evaluating this type. Risks or their modeling، which raises many questions about the nature of these risks، the legal implications resulting from their realization، and the question of the adequacy of the general insurance rules for their application to the insurance contract against cyber risks، in addition to the presence of a number of legal and technical challenges that have resulted from dealing with this new type of third-party risks. Concrete، which justified the need to study insurance protection for commercial companies from cyber risks.

The Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Maysan / College of Law

Postgraduate Studies /Private Law Department

Insurance protection for commercial companies from cyber risks

A Letter submitted by the student:

Amany Tammuz Abdul Rahman Al Khafajy

To:

Council of the College of Law / University of Maysan

As part of the requirements for obtaining a master's degree in private Law

supervised by:

ASST. Prof. Jaafar Kadhim Jabr

1446 AH **2024 AD**