الجمهورية العربية السورية

جامـــــعة دمـــــشق

كليَّـــــة الحقوق

قسم القانون التجاري

عقد التّأمين ضد مخاطر الانترنت

(دراسة تحليلية لبعض مخاطر استخدام الشابكة)

رسالة مقدمة لنيل درجة الماجستير في القانون التجاري

إعداد الطالبة

زينب خضور

إشراف الدكتورة

حنان مليكه

الأستاذ المساعد في قسم القانون التّجاري في كليّة الحقوق

العام الدراسي

2021 – 2020

بسم الله الرحمن الرحيم

(وعلمك ما لم تكن تعلم وكان فضل الله عليك عظيماً)

الآية رقم 113 من سورة النساء

صدق الله العظيم

الإهـــــداء

إلى اليد الخضراء التي ما ملّت يوماً من العطاء...

إلى كلمةٍ كبيرةٍ كالكون ونقيّةٍ كالصِّدق...

والدي الحبيب

إلى أعزّ وأغلى وأطيب قلب...

إلى مَن تظلُّ كلمات دعائها تميمة الفرح الدَّائم لخطواتي...

والدتي الحنونة

إلى رفاق البسمة والدَّمعة والفرحة والحلم...

سندي وعزوتي...

إخوتي الأحباء

إلى مَن رافقت خطواتهم خطواتي

وصنعتُ معهم أجمل سنواتي الدّراسيّة

أصدقائي الأعزاء

لكم جميعاً أهدي هذه الرّسالة المتواضعة التي أعلّق عليها آمالي، وبها أكون قد اجتزت شطراً جديداً من حياتي.

شـــكر وتقـــدير

إرادتنا تصنع مستقبلنا، فما الغد سوى تجسيدٌ لعملنا وجهدنا اليوم، فتمرّ وتمضي السنوات فلا ندري بها إلّا ونحن على مفارق الطرق، فنجد بُداً من أن نسعد بما تحقّق أو بما انقضت همومه، وهكذا مرّت هذه المرحلة من حياتي، فلن أنسى ما حييت سنوات قضيتها في كنف كليَّة الحقوق بفرحها وتعبها.

شكراً لهذا البناء العظيم الذي احتوانا هذه السّنين كلّها.

شكراً لمن كانت لهم اليد الطولى في أن نصل إلى ما وصلنا إليه، فأتقدّم بشكرٍ إلى دكاترتنا الذين نعتزّ بهم، وإنّ اليراع ليعجز عن إيفائهم حقّهم بالكلمات.

شكراً لجهود عمادة كليّة الحقوق وأعضاء الهيئة التّدريسيّة فيها جميعهم، وعلى رأسهم السيد العميد الأستاذ الدكتور هيثم الطاس.

وأخصُّ بالشكر الدكتورة حنان مليكه التي شرفتني بإشرافها على بحثي وجهدي الذي بذلته لإنجاز هذه الرسالة فكانت نِعم المرشد والمعلّم.

كما لا يسعني إلَّا أن أتقدَّم بالشُّكر إلى الأساتذةِ أعضاء لجنة المناقشة؛ لقبولهم الموافقة على تحكيم رسالتي. فلكم منِّي أسمى آيات الشُّكر وجزيل التَّقدير.

والشُّكر موصولٌ إلى أساتذة قسم القانون التّجاريّ جميعهم.

ولكم أيهّا السّادة المربّون نقف بإجلالٍ وإكبارٍ لما زودتمونا به من فيض معرفتكم وخبراتكم، فلكم منّا كلّ الحبّ والتّقدير ونعدكم أن نسير على خطاكم، وأن نقدّس العلم الذي أخذناه منكم وأن نحاول منحه لغيرنا.

ولا يسعني إلّا أن أتذكر كلَّ مَن كانوا عوناً وسنداً لي، وأن أقدّم لهم الشّكر والامتنان على ما قدّموه من وقوفهم جانبي، ودعمي بما يملكونه من خبرةٍ ومعرفةٍ لمساعدتي في التطلّع إلى المستقبل بعيونٍ ملؤها الأمل.

مع محبتي: زينب خضور

قائمة المحتويات

المُلخَّص

تُشكّل مخاطر الإنترنت اليوم الهاجس الأكبر لأيّ فردٍ وكيانٍ؛ نظراً لكونها أمراً غير متوقع، وغير قابل لتحديد مداه وأثره، وذلك بسبب الاستخدام الهائل للإنترنت في مناحي الحياة كافّة. فلا توجد شركة لا تستخدم الإنترنت في أعمالها بدءاً من تخزين المعلومات حتى إجراء المعاملات الإلكترونية، والدّفع الإلكترونيّ، ويرافق هذا الاستخدام مخاطرُ كبيرةٌ نتيجة إمكانيّة سرقة المعلومات المخزّنة، وبيعها لشركاتٍ منافسةٍ، وتعطيل المواقع الإلكترونية المستخدمة، وغير ذلك من المخاطر ممَّا يؤثّر بشكلٍ كبيرٍ على مسار العمل الإلكترونيّ. ونتيجةً لذلك لجأت الشّركات لحماية نفسها من هذه المخاطر إلى شركات التّأمين ضدّ مخاطر الإنترنت، وذلك من أجل الحصول على تغطيةٍ تأمينيّةٍ للمخاطر التي قد تتعرّض لها، في مقابل دفع أقساطٍ تحدّدها شركات التّأمين. ويعد عقد التّأمين ضدّ مخاطر الإنترنت عقداً جديداً ينتمي إلى غيره من طائفة عقود التّأمين، ولكنّه في الوقت ذاته متميّز عن سواه نتيجة الخصائص الإلكترونية التي تسبغه بسمةٍ فريدةٍ من نوعها. وعليه سيُدرس عقد التّأمين ضدّ مخاطر الإنترنت عبر فصلين اثنين، يُفرَد الأوّل منهما للحديث عن ماهيّة عقد التّأمين ضدّ مخاطر الإنترنت وماهيّة هذا المخاطر، في حين يُفرَد الفصل الثاني للحديث عن الالتزامات النّاشئة عن هذا العقد.

الكلمات الرّئيسة: مخاطر الإنترنت، التّأمين ضدّ مخاطر الإنترنت، تغطية تأمينيّة، أقساط التّأمين.

Key words: internet risks, cyber insurance, insurance coverage, insurance premiums.

4التعريفات والمصطلحات المعتمدة:

من التعريفات ذات الأهمية في موضوع التّأمين ضد مخاطر الإنترنت:

-التّأمين: وهو عقدٌ تلتزم بموجبه شركة التأمين بأن تؤدي مبلغاً من المال إلى المؤمَّن له عند وقوع الخطر المؤمن منه أو حصول الحادث المتوقع، وذلك مقابل أقساط يدفعها المؤمَّن له وفق الاتفاق الحاصل بين الطرفين.

-التّأمين ضد مخاطر الإنترنت: هو عقدٌ يبرمه المؤمَّن له من أجل حماية نفسه من المخاطر الناشئة عن استخدام الإنترنت في أعماله، ويلتزم بموجبها بدفع أقساطٍ وأداء التزاماتٍ معينةٍ تفرضها عليه شركة التأمين التي تلتزم في المقابل بدفع مبالغ مالية لتغطية الأضرار الحاصلة وحماية المؤمَّن له بصورة سابقة ولاحقة لوقوع الخطر المؤمّن منه.

-المؤمَّن له: هو شخص معرّض لخطر من مخاطر الإنترنت، يلجأ إلى شركة تأمين لتقوم نيابة عنه بتحمل الخسائر التي قد تلحق به نتيجة تحقق الخطر المؤمّن منه مقابل أن يدفع لها قسطاً محدداً.

-مخاطر الإنترنت: وهي مخاطرُ تظهر بصورة غير مادية محدثة نتائجَ غير مادية ناجمة عن استخدام شبكة الإنترنت، كالابتزاز الإلكترونيّ والدخول غير المشروع إلى الأنظمة والبيانات.

-الإنترنت: شبكة دوليّة للمعلومات تتيح للمستخدمين الكثير من الميزات، كالبريد الإلكترونيّ والاتصال الصوتي والمرئي ونقل الملفات والمعلومات إلى أي مكانٍ في العالم.

-التغطيّة التأمينية: وهي الالتزام الملقى على عاتق شركة التأمين بموجب العقد المبرم مع المؤمَّن له، وتلتزم بموجبه بأن تدفع له مبلغاً يعادل الضرر اللاحق به، كما تلتزم بأن تقدم له خدمات عينية سابقة لمرحلة وقوع الخطر، كالتدريب وتقديم برامج الحماية وغيرها.

–القسط: وهو مبلغ ماليّ معين يلتزم المؤمَّن له بأن يدفعه إلى شركة التأمين على دفعات شهرية أو سنوية حسب الحال.

المُقدِّمة:

تشغل المخاطر فِكْرَ العديد من الأفراد في مراحل حياتهم كافَّة، وتأخذ فكرة حماية أنفسهم من هذه المخاطر حيّزاً كبيراً من تفكيرهم حول الوسائل الممكنة لوضع حدٍّ لها، ويختلف الكثيرون في هذه الوسائل، فمنهم مَن يذهب إلى تحصين نفسه ضدَّ المخاطر عبر اتخاذ إجراءاتٍ معيّنةٍ تبدو في رأيهم الوسيلة المُثلى للحماية، في حين يذهب غيرهم إلى أنَّ الوسيلة الفضلى هي تحويل المخاطر إلى مؤسَّسةٍ أخرى لتحملها نيابةً عن الفرد المُهدّد بها، ويطلق على هذه الوسيلة مصطلح التّأمين، والذي يتضمَّن إدخال طرفٍ ثانٍ ليعوّض الشَّخص المُعرَّض للخطر عن الخسائر التي تلحق به عند تحقُّق المخاطر المؤمَّن منها. وقد أخذ التّأمين منذ بدايته وقتاً طويلاً حتى وصل إلى التطور المتمثِّل الآن، وتاريخياً ظهر التّأمين لأول مرَّةٍ في عمليَّات النقل البحريّ (التّأمين البحري)؛ إذ أخذ شكل التّأمين على الأشياء وكانت آنذاك البضائع المنقولة من المخاطر البحريّة، وتمّ ذلك على يد لويدز لندن Lloyds of London، ومن ثمّ في عام 1666 حصل حريقٌ ضخمٌ في لندن كان الشّعلة الأولى لإنشاء وثائق تأمينٍ ضدّ الحريق، ومن ثمّ بدأت تتوالى وثائق التّأمين البريّة بأشكالٍ مختلفةٍ كالتّأمين على الحياة، وضدّ الحوادث، والسّرقة، وكلَّما زادت الحياة تطوّراً وتعقيداً كان التّأمين مواكباً لهذا التطوّر[1].

ومع بزوغ الثّورة التكنولوجيّة وما أفرزته من تطوّرٍ كبيرٍ في وسائل الاتصال والتّعاقد عن بعد، دخلت مخاطرُ جديدةٌ مختلفةٌ عن المخاطر التي تخافها المؤسّسات والأفراد على السّواء وهي مخاطر الإنترنت، إذ بات التعاقد يتمّ عن طريق الإنترنت، كما أنّ الخلافات بين الأفراد باتت تأخذ شكل القدح والذمّ الإلكترونيّ على مواقع التواصل الاجتماعيّ، كذلك عمليّة تسديد الدّيون وتحويل الأموال تتم إلكترونيّاً عبر الشّبكة، وأصبحت تتّخذ الشّركات من الإنترنت سجلاً لأسماء عملائها. ومع الاعتماد الكبير على شبكة الإنترنت في نواحي الحياة كافّة ظهر المجرمون الإلكترونيون الذين يتّخذون من الإنترنت ساحةً لمعاركهم الافتراضية، وأصحبت الشّركات والأفراد

[1] مكناس، جمال الدين، وعاشور، محمد سامر، (2018)، التّأمين، دمشق: سورية، منشورات الجامعة الافتراضية السورية، ص3.

عرضةً لهجماتٍ إلكترونيّةٍ بهدف سرقة المعلومات المُخزّنة أو العبث فيها وتدميرها، إذ باتت بنوك المعلومات الإلكترونيّة اليوم الكنز الثمين للمجرمين والتي تستقطبهم مدفوعين بدوافعَ متعدّدةٍ للقيام بهجماتٍ لكشف خصوصيَّة الأفراد وسرقة معلوماتهم للإتجار بها. وفي ظلّ هذه الفوضى الإلكترونية كان لا بدَّ من وضع حدٍّ لإيقاف انتشارها، إذ كان القانون في المرصاد كما هو الحال دائماً، وبدأت الدول تضع تشريعاتٍ لتجريم هذه الأفعال وهو ما حذاه المشرّع السّوريّ عبر إصدار قانون تنظيم التواصل على الشّبكة ومكافحة الجريمة المعلوماتية[2]، والذي جرّم بموجبه بعض الأفعال الإلكترونية كإرسال البريد المزعج، والدخول غير المشروع إلى منظومة معلوماتيّة، وهجمات حجب الخدمة[3]، وعلى هذا الدرب سار العديد من المشرّعين. ولكن ذلك حقيقةً لم يفلح في وضع حدٍّ للهجمات الإلكترونيَّة، بل استمرَّ المجرمون في العبث بالإنترنت، ويشجّعهم على ذلك سهولة ارتكاب الجرائم الإلكترونيّة وإمكانيّة التخفّي، ولذلك بُحِث عن وسيلةٍ أخرى لحماية المتضرّرين من هذه الأفعال، فوقع الاختيار على التّأمين، ودُرِست إمكانية الاستفادة من خدمات التّأمين في هذا المجال، وقد بدأت أولى إرهاصات التّأمين ضدّ مخاطر الإنترنت في سبعينيات القرن العشرين على شكل بعض التّغطيات المحدودة للقرصنة الإلكترونيَّة لتغطية خسائر البيانات، والتي تُشكِّل ضرراً غيرَ ماديٍّ؛ نظراً لأنَّ الوثائق العامة آنذاك وإن كانت تغطّي الخطر الإلكترونيّ إلَّا أنَّها تتطلَّب ضرراً ماديّاً ليتمّ التّعويض، وهو ما سبّب رفض العديد من الوثائق؛ لأنَّ الأضرار الحاصلة أخذت شكلاً إلكترونيّاً لم يكن مغطّىً في ذلك الوقت[4]، وقد قُدّمت تغطيّة مخاطر الإنترنت أيضاً عبر تقديم تغطياتٍ إضافيةٍ في وثائق التّأمين التقليدية التي كانت تأخذ شكل وثائق تغطية الفشل والإهمال التقني، أو وثائق المسؤوليّة التّجاريّة العامّة، أو وثائق انقطاع الأعمال[5]، لكن وللصّعوبات التي واجهت هذه التّغطية، وعدم ملاءمتها الواقع الافتراضيّ، والمخاطر التي تحيط بالشركات اندفعت شركات التّأمين لتقديم خدماتٍ أكثر ملاءمةً، ففي أواخر التسعينيات وعلى وجه التحديد في عام 1998 تم تقديم أول وثائق التّأمين ضد

---

[2] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم (17) لعام 2012.

[3] المواد (2-10-17) من القانون المذكور.

[4] Kesan J. P., Yurcik, W., & Majuca, R., (2006). The Evolution of Cyber insurance, computer science, ArXiv, p4.

[5] Camillo, M., (2017). cyber risk and the changing role of insurance, v2, journal of cyber policy, p1.

القرصنة من شركةٍ تقنيّةٍ، وقد تعاونت في ذلك مع شركات تأمين لتوفّر للعملاء خدماتٍ تقنيّةً وتغطية الطرف الأول من أجل الوصول إلى إدارة شاملة للمخاطر التي يتعرض العملاء لها[6]، وكانت هذه الوثائق البداية الخجولة لعالم التّأمين ضد مخاطر الإنترنت، ولكن ما تبع أحداث 11 أيلول من هجماتٍ إلكترونيةٍ عبر نشر الفيروسات، وهجمات حجب الخدمة، وسرقة الهُويّات، والتصيد ضدّ الشّركات الأمريكيّة عزّز الحاجة لوجود وثائق أكثر فعاليّة، إذ إنّه بحسب الإحصائيات فإنَّ 90% من الشّركات والوكالات تعرّضت لخرقٍ أمنيٍّ، ما دفع المشرّعين إلى محاولة وضع حدٍّ لهذه الهجمات عبر فرض عقوباتٍ وواجباتٍ على الشّركات الضّحيّة، وهو ما دفع إلى إنشاء وثائق أكثر دقّةً بالتعامل مع مخاطر الإنترنت نظراً لما ينتاب هذه المخاطر من اختلافاتٍ عن المخاطر التّقليديّة من حيث كونها تأخذ شكلاً غير ملموس، وتؤدّي إلى أضرارٍ افتراضيّةٍ، وكثيراً ما كانت الوثائق التّقليديّة لا تغطّيها كما ذُكر سابقاً، وبدأت شركات التّأمين مثل شركات Marsh, American International Group (aig),Lloyds of London, Zurich, تقدم وثائق تأمين تغطي الطرف الثالث (وكانت تمثل التغطية الجديدة في ذلك الوقت)، إضافةً للطّرف الأوّل الذي تمّت تغطيته بموجب وثائق القرصنة الأولى، وهكذا ساهمت الأحداث الأمنيّة الإلكترونيّة وتطوّر القوانين في دفع عجلة التّأمين ضدّ مخاطر الإنترنت حتى أخذ الشّكل المعروف عنه اليوم[7].

إشكاليّة البحث:

تتمحور هذه الإشكاليّة في بيان مدى الاختلاف بين عقد التّأمين ضدّ مخاطر الإنترنت وغيره من عقود التّأمين المعروفة، وتحديد أوجه الاختلاف إن وُجدت وصولاً إلى تخصيصه بأحكامٍ ناظمةٍ له. وتتفرّع عن هذه الإشكاليّة تساؤلاتٌ عدةٌ هي:

- ما التّعريف الأمثل لعقد التّأمين ضد مخاطر الإنترنت؟
- ما الطّبيعة القانونيّة لعقد التّأمين ضدّ مخاطر الإنترنت؟

---

[6] Kesan J. P., Yurcik, W., & Majuca, R., (2006)., p4.

[7] Camillo, M., (2017)., p1-2.

- مدى قابليّة القواعد القانونيّة الموجودة لتطبيقها على عقد التّأمين ضد مخاطر الإنترنت؟
- ما المشكلات التي يواجهها هذا العقد والحلول المبتكرة لوضع حدٍ لها؟
- ما المفهوم الأشمل لمخاطر الإنترنت التي يغطّيها هذا العقد؟
- كيف تصدّت شركات التّأمين لهذه المخاطر، وما الصعوبات التي ترافق تغطيتها؟

أهميّة البحث:

إنّ لكلَ بحثٍ قانونيٍ أهمية وأسباب تدفع الباحث إلى اختياره موضوعاً لبحثه، من أجل الخروج من هذا البحث بنتائجَ وتوصياتٍ، عبر معالجة المشكلات التي تعتريه وإيضاح وسائل الحل، وحيث أنه تتمثل أهمية بحث التّأمين ضد مخاطر الإنترنت في:

1- تسليط الضّوء على هذا العقد الجديد الذي أفرزه العالم الإلكترونيّ الذي نعيش فيه، وذلك بهدف إزالة أيّ غموضٍ يعتريه.

2- إيضاح أهم صور مخاطر الإنترنت التي باتت اليومَ الشغلَ الشاغل لجميع الأفراد والمؤسسات على السواء نظراً لطبيعتها ولانتشارها الواسع.

3- بيان انعكاس طبيعة عقد التأمين ضد مخاطر الإنترنت المميزة على طبيعة الالتزامات التي يرتبها العقد.

4- تمكين الأشخاص من الإفادة من التأمين ضد مخاطر الإنترنت في ظلّ التطوّر التكنولوجيّ والتّقنيّ الذي فرض مخاطرَ جديدةٍ تستوجب تغطيتها من أجل الوصول إلى الاستفادة القصوى من الفضاء الإلكترونيّ.

محددات البحث:

تبحث هذه الدراسة في عقد التّأمين ضد مخاطر الإنترنت، الذي بات اليوم يشقّ طريقه بصورةٍ أكثر استقلاليّة عن غيره من صور التّأمين، وأصبح منتشراً في غالب دول العالم، لذلك ليس هنالك ما يمنع من أن يتم تعميم النتائج والتوصيات التي يصل إليها البحث في سوريا وغيرها من الدول العربيّة.

أهداف البحث:

تكمن أهداف البحث بشكلٍ رئيسٍ في التعريف بمفهوم عقد التّأمين ضد مخاطر الإنترنت الذي لا يزال يشكّل حتى الآن مفهوماً غامضاً للكثير من العاملين في مجال التّأمين وللعملاء على حدٍ سواء، نتيجة لاتصاله الوثيق بمخاطر لا يزال إلى يومنا هذا يختلف الشراح في طبيعتها، وهو ما أثار بعض المشكلات والصعوبات في التعامل، وفي ترتيب الالتزامات القانونية الناشئة عن العقد، في مسعىً للوصول إلى نتائجَ وتوصيّاتٍ قابلةٍ للتطبيق من قبل صناع التّأمين من أجل تخطي العقبات التي تواجههم.

معوّقات البحث:

لا بد من وجود صعوباتٍ تواجه الباحث أثناء دراسته لأيّ بحثٍ علمي أو قانوني، لاسيما عندما يكون البحث جديداً غير مطروق، وعليه تتمثل أهم المعوقات في الآتي:

- غياب التّنظيم التّشريعيّ لعقد التّأمين ضدّ مخاطر الإنترنت على مستوى دول العالم؛ نظراً لحداثته في المقام الأوّل ولإمكانية الاستفادة من نصوص التّأمين التّقليديّ الواردة في القوانين المدنيّة.
- ندرة الدّراسات العربيّة المتعلّقة بهذا الموضوع؛ ما استدعى الباحث إلى الاستعانة بالدّراسات الأجنبيّة.
- صعوبة الحصول على اجتهاداتٍ قضائيّةٍ متعلقة في صميم هذا العقد، بالإضافة إلى عدم وجود شركات تأمين محلية تقدم تغطيةً لمخاطر الإنترنت، وبالتالي عدم وجود منازعات أمام القضاء قد تغني عمل الباحث، وإن أمكن الاستعانة ببعض القضايا الأجنبية.

الدراسات السابقة:

من الدراسات ذات الصلة بموضوع البحث:

– دراسة الناصري، أسنر خالد (2019)، دراسة **بعنوان المسؤوليّة المدنية عن انتهاك الخصوصيّة على مواقع التواصل الاجتماعيّ**، دار النهضة العربيّة للنشر والتوزيع، مصر.

هدفت هذه الدراسة إلى تحديد المخاطر التي تحيط بالأفراد المستخدمين لمواقع التواصل الاجتماعيّ، لاسيما في ظل الانتشار الواسع لهذه المواقع، واستخدامها من قبل فئاتٍ عمريّةٍ متعددةٍ، وعدم وجود تنظيمٍ قانونيّ لها، وعرّج الباحث في دراسته على موضوع التّأمين ضد مخاطر الإنترنت من حيث إمكانيّة استخدامه كأحد الوسائل لمواجهة مخاطر مواقع التواصل. وبذلك تختلف هذه الدراسة عن دراستي لكونها لم تتعمق في موضوع التّأمين ضد مخاطر الإنترنت كافة بل تحدثت عن أحد صور هذه المخاطر.

–دراسة إبراهيم، حسام (2019)، دراسة بعنوان **التطور التكنولوجي وقطاع التأمين مالنا وما علينا**، بحث مقدم إلى مؤتمر العقبة، الأردن.

لقد تحدثت هذه الدراسة عن إمكانيّة الاستفادة من التكنولوجيا في قطاع التأمين لما يمكن أن يحقّقه من مزايا تسويقية أفضل لشركات التأمين والعملاء، ومن ثم بادر الباحث بالحديث عن الجرائم الإلكترونيّة والتأمين ضد الأخطار الإلكترونيّة عبر إبراز دور شركات التّأمين العاملة في هذا المجال، وأشكال التغطيّة المقدّمة من جانبها، وقد ركزت هذه الدراسة على فكرة الالتزامات الناشئة عن العقد (التغطيّة) دون الحديث عن مفهوم هذا العقد بشكلٍ مفصّلٍ.

– دراسة Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk, Journal of Cyberecurity.

لقد ركزت هذه الدراسة في إطار عقد التّأمين ضد مخاطر الإنترنت على المشكلات التي تواجه شركات التّأمين أثناء قيامها بحساب الأقساط واجبة الدفع من قبل المؤمَّن لهم، لما يعترض هذا الحساب من صعوباتٍ نتيجة عدم وجود إحصائيات دقيقة للمخاطر، وقلة المعلومات المتعلقة بها، وطبيعة المخاطر المتغيرة، وغيرها من عواملَ تضع الشركات في حيرةٍ من أمرها، وبذلك تختلف عما درسته لكونها قد ركزت على أحد آثار عقد التأمين ضد مخاطر الإنترنت.

منهج البحث:

وفي سبيل الإحاطة بموضوع البحث سيتم اتباع المنهج التحليليّ والوصفيّ في آنٍ معاً، من خلال إيراد النصوص الناظمة لعقد التأمين الواردة في القانون المدني السوري وغيره من القوانين وملاحظة مدى إمكانيّة الاستفادة منه في عقد التّأمين ضد مخاطر الإنترنت الذي لم يُفرد له أحكام خاصة به، وتحليل هذه النصوص للوصول إلى نتائجَ وتوصيّاتٍ تخدم البحث.

مكونات البحث:

لدراسة مفردات البحث، قُسِّم إلى:

الفصل الأول: الإطار الموضوعي لعقد التّأمين ضدّ مخاطر الإنترنت

المبحث الأول: ماهيّة عقد التّأمين ضدّ مخاطر الإنترنت

المطلب الأول: تعريف عقد التأمين ضد مخاطر الإنترنت وتقييمه

الفرع الأول: تعريف عقد التأمين ضد مخاطر الإنترنت

الفرع الثاني: تقييم عقد التأمين ضد مخاطر الإنترنت

المطلب الثاني: أركان عقد التأمين ضد مخاطر الإنترنت وطبيعته القانونية

الفرع الأول: الأركان التي تحكم عقد التأمين ضد مخاطر الإنترنت

الفرع الثاني: الطبيعة القانونية لعقد التأمين ضد مخاطر الإنترنت

المبحث الثّاني: ماهيّة مخاطر الإنترنت

المطلب الأول: مفهوم مخاطر الإنترنت

الفرع الأول: تعريف مخاطر الإنترنت وطبيعتها القانونية

الفرع الثاني: خصائص مخاطر الإنترنت وأنواعها

المطلب الثاني: دوافع مخاطر الإنترنت وصورها

الفرع الأول: دوافع مخاطر الإنترنت وطرق الاستفادة من البيانات المسروقة

الفرع الثاني: صور مخاطر الإنترنت وبعض الهجمات الإلكترونية تاريخياً

الفصل الثّاني: آثار عقد التّأمين ضدّ مخاطر الإنترنت

المبحث الأوّل: التزامات شركة التّأمين

المطلب الأول: التغطية التأمينية واستثناءاتها في عقد التأمين ضد مخاطر الإنترنت

الفرع الأول: أشكال التغطية التأمينية

الفرع الثاني: الاستثناءات من التغطية التأمينية

المطلب الثاني: آلية التغطية التأمينية في عقد التأمين ضد مخاطر الإنترنت

الفرع الأول: دفع مبالغ التأمين في عقد التأمين ضد مخاطر الإنترنت

الفرع الثاني: تحديد مبالغ التأمين ومدة الالتزام في عقد التأمين ضد مخاطر الإنترنت

المبحث الثّاني: التزامات المؤمَّن له

المطلب الأول: التزام المؤمَّن له بدفع الأقساط التأمينية

الفرع الأول: دفع قسط التأمين والآثار المترتبة على الإخلال به

الفرع الثاني: العوامل المتعلقة بتحديد قسط التأمين ضد مخاطر الإنترنت

المطلب الثاني: التزام المؤمَّن له بالإعلام وبواجب العناية

الفرع الأول: التزام المؤمَّن له بإعلام شركة التأمين

الفرع الثاني: التزام المؤمَّن له بواجب العناية والتقيد بتعليمات شركة التأمين

الفصل الأوَّل

الإطارُ الموضوعيُّ لعقد التّأمين ضدّ مخاطر الإنترنت

تحيط المخاطر بالحياة التجاريّة في كلِّ مكانٍ من هذا العالم، وتتنوّع صور المخاطر التي تواجهها القطاعات المختلفة بحسب البيئة التي تعمل فيها، فقد كانتِ المخاطر أغلبها ذات صورة ماديّة تنتج ضرراً ماديّاً، لكن مع تطور التكنولوجيا باتت المخاطر تأخذ شكلاً غيرَ محسوسٍ وتؤدي إلى نتائجَ مختلفةٍ عمَّا كانت تخلّفه المخاطر المادية تبعاً لتغير الشيء الذي يقع عليه الخطر الإلكتروني. وأمام هذه المخاوف من تطور مخاطر الإنترنت على نحوٍ لا يمكن معه للمؤسسات مواجهتها بمفردها، كان السبيل إلى إنتاج وثائق تأمين ضد مخاطر الإنترنت هو الطريق الأمثل لوضع حدٍّ لما تسببه هذه المخاطر من خسائرَ هائلةٍ. وباتت تطفو على السطح عقود التّأمين ضد مخاطر الإنترنت كأحد الحلول المستحدثة لمواجهة مخاطر الإنترنت في وقتٍ أصبحت فيه هذه المخاطر أحد أبرز أسباب الخسائر اللاحقة بالمؤسّسات كافَّة حول العالم وفي أيّ مجال دون حصرٍ، إذ إنّها تُشكِّل هاجساً مخيفاً نتيجة سرعة وسهولة انتشارها، وإمكانيّة تحقيقها ضرراً كبيراً دونما قدرةٍ على التتبع. وفي سبيل إيضاح الأفكار المذكورة سيتم إفراد هذا الفصل لإعطاء أكبر قدر ممكن من المعلومات عن عقد التّأمين ضد مخاطر الإنترنت في مبحثين اثنين، يدرس الأول ماهية هذا العقد، في حين يدرس الثاني ماهية مخاطر الإنترنت.

المبحث الأوَّل

ماهية عقد التّأمين ضد مخاطر الإنترنت

يُعدّ عقد التّأمين ضد مخاطر الإنترنت من أكثر عقود التّأمين رواجاً إلى جانب غيره من صور التّأمين الأخرى، كالتّأمين على الحياة، والتّأمين الإلزامي على السيارات. فلا يمكن لشركةٍ أن تكمل مسيرتها المهنيّة والعمليّة إلا عبر الاستعانة بعقود التّأمين التي تتولى تعويضها عند حصول مخاطر الإنترنت المؤمَّن منها، والتي بشكلٍ أو آخرَ لا سبيل للهرب منها، إذ إنّ المخاطر في تطوّرٍ مستمرٍّ، ويرافق ذلك انتعاشٌ كبيرٌ في سوق التّأمين ضد مخاطر الإنترنت الذي بات يشغل الآن حجماً كبيراً من سوق التّأمين حول العالم. حيث باتت العديد من الشركات تلجأ إليه بعد العديد من الأحداث الإلكترونية التي أودت بشركاتٍ أخرى إلى حافة الإفلاس. **وعليه في سبيل الإحاطة بماهية هذا العقد وتسليط الضوء عليه من أجل فهمه بشكلٍ أكبر لتمييزه عن غيره من عقود التّأمين، فقد قُسِّم هذا المبحث إلى مطلبين، يُفرد الأول منهما للحديث عن تعريف عقد التّأمين ضد مخاطر الإنترنت وتقييمه، ويُفرد الثاني للحديث عن أركان العقد وطبيعته القانونية.**

المطلب الأوَّل

تعريف عقد التّأمين ضد مخاطر الإنترنت وتقييمه

بات عقد التّأمين ضد مخاطر الإنترنت يتربع عرش عقود التّأمين السائدة؛ نتيجةً لكثرة المخاطر الإلكترونية التي تواجهها الشركات والكيانات الاقتصادية المختلفة، بل وحتى الأفراد أنفسهم، ويبدو من تتابع الأحداث أنَّ هذا التّأمين قد ظهر منذ ما يقارب ثلاثة عقود أو أقلّ بقليل. والحقيقة أنَّ أهميّة عقد التّأمين ضد مخاطر الإنترنت تنبع ممَّا يؤدّيه من دورٍ كبيرٍ في زيادة الأمن الإلكترونيّ، وبث الطمأنينة في نفوس أصحاب الأعمال الإلكترونيّة ضد مخاطر الإنترنت، وتشجيعهم على الانخراط أكثر فأكثر في التجارة الإلكترونية، وعليه يُفرد هذا المطلب لبيان تعريف عقد التّأمين ضد مخاطر الإنترنت (الفرع الأول)، ومن ثمّ تقييمه لبيان مزاياه، وخصائصه، والمشكلات التي تعترضه (الفرع الثاني).

الفرع الأوَّل

تعريف عقد التّأمين ضد مخاطر الإنترنت

ينتمي عقد التّأمين ضد مخاطر الإنترنت إلى طائفة عقود التّأمين ذاتها، إذ يتفق معها بهدفها من حيث تعزيز الأمان والثقة وتخفيف الأضرار الحاصلة عند تحقق الخطر.

ولا يمكن البدء بتعريف عقد التّأمين ضد مخاطر الإنترنت قبل تناول تعريف عقد التّأمين التقليدي _ إن جاز القول_ على ما جاء تعريفه لدى القوانين والفقه.

أولاً: تعريف عقد التّأمين التّقليديّ

نتناول في هذا المجال بعض التعاريف التشريعيّة، ومن ثمّ نتناول ما جاء به الفقه في تعريف التّأمين.

1-التعريف التشريعي:

على أنَّ عمل القوانين لا يتضمّن صياغة التعاريف، فالأمر كما هو معلوم من عمل الفقه، لكن مع ذلك فإنّ بعض التشريعات ذهبت إلى وضعٍ مفهومٍ محدَّدٍ لعقد التّأمين.

فالبداية من القانون المدنيّ السّوريّ؛ حيث ورد تعريف التّأمين ضمن الأحكام العامة للتأمين على أنَّه: "عقدٌ يلتزم المؤمن بمقتضاه أن يؤدّي إلى المؤمَّن له أو إلى المستفيد الذي اشترط التّأمين لصالحه (لمصلحته) مبلغاً من المال، أو إيراداً مرتباً، أو أي عوضٍ ماليٍّ آخر في حالة وقوع الحادث، أو تحقيق الخطر المبين بالعقد، وذلك لقاء قسط أو أيّ دفعة ماليّة أخرى يؤدّيها المؤمَّن له للمؤمن[8]"، ويطابق هذا التعريف التعاريف الواردة في المادة (920) من القانون المدني الأردني[9]، والمادة (747) مدني مصري[10].

وعرّف المشرّع اللبناني عقد التّأمين في تقنين الموجبات والعقود تحت عنوان عقد الضمان على أنّه: "عقدٌ بمقتضاه يلتزم شخصٌ يقال له الضامن بعض الموجبات عند نزول بعض الطوارئ بشخص المضمون أو أموالهم مقابل دفع بدل يسمى القسط أو الفريضة[11]."

وتبرز من التّعاريف السّابقة العناصر القانونية لعقد التّأمين والآثار الناتجة عنه، من حيث وجود طرفين للعقد هما شركة التّأمين، والمؤمَّن له، وإمكانية وجود طرف ثالث خارج عن العقد هو المستفيد، ينتفع المؤمَّن له أو المستفيد من العقد في التّقليل من الأضرار التي تصيبه نتيجة تحقّق خطر معيّن مؤمَّن ضده، في حين تستفيد شركة التّأمين من الفروقات بين المبلغ المدفوع (التعويض) والأقساط المؤدّاة في تشكيل هامشٍ من الرّبح، لا سيّما إذا ما عرفنا أنَّ هذا النوع من العقود غالباً ما يكون تجارياً يقوم على الرّبح، وينشئ العقد التزاماتٍ على عاتق أطرافه بدفع المؤمَّن له للأقساط المحدّدة ودفع شركة التّأمين لمبلغ التّأمين الذي حدّده المشرّع السّوريّ على شكل مبلغ يُدفع إمَّا مرّة واحدة في دفعة واحدة، أو إيراد مترتّب مدى الحياة، أو لمدّة معيّنة وفق أوقاتٍ معيّنةٍ

---

[8] المادة (713) من القانون المدني السوري رقم 84 لعام 1949.

[9] المادة (920) من القانون المدني الأردني رقم 43 لعام 1976.

[10] المادة (747) من القانون المدني المصري رقم 131 لعام 1948.

[11] المادة (950) من قانون الموجبات والعقود اللبناني رقم 0 لعام 1932.

حسب العقد المبرم بين الطّرفين، في حين يُعاب على هذه التعاريف خلوّها من بيان الأسس الفنية للتأمين بعيداً عن صفته القانونية.

أمَّا في فرنسا فلا يوجد حتى الآن تعريف قانونيّ لعقد التّأمين[12].

2-التَّعريف الفقهيّ:

بينما اهتمّتِ التعاريف التشريعيّة معظمها بالأسس القانونيّة للتّأمين، فانكبّ الفقه على دراسة الأسس الفنية للتّأمين.

وقد عرّف جانبٌ من الفقه التّأمين بأنّه: "نظامٌ يهدف إلى حماية الأفراد والمنشآت على السّواء من الخسائر الماديّة اللاحقة بهم نتيجة تحقّق خطر غير مؤكّد الحدوث في المستقبل عبر نقل عبء تحمّل الخطر إلى مؤمّن يلتزم بالتّعويض مقابل قسط معين[13]." ويلحظ على هذا التعريف تركيزه على الهدف من التّأمين وهو التعويض من الخطر المحتمل، مع الإشارة إلى بعض عناصر التّأمين الأخرى كالقسط والخطر غير المحقّق.

كما جاء في تعريفٍ فقهيّ آخرَ بأنّه: "عمليّةٌ فنيّةٌ تزاولها هيئاتٌ منظّمةٌ تكون مهمّتها جمع أكبر عدد ممكن من الأخطار المتشابهة وتحمّل تبعتها عن طريق المقاصة وفقاً لقوانين الإحصاء، ومن مستلزمات ذلك حصول المؤمَّن له أو من ناب عنه على العوض المالي عند تحقّق الخطر المعيّن مقابل التزامه بدفع أقساط معينة[14]".

---

[12] https://www.uk.practicallaw.thomsonreuters.com/9-501-3248?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

تاريخ الزيارة: 22\4\2020، الساعة 2:30 p.m.

[13] عبد ربه، إبراهيم علي إبراهيم. (2006). مبادئ التأمين، مصر، الدار الجامعية، ص64، 66.

[14] عرفة، محمد علي. 1949، شرح القانون المدني الجديد في التأمين، ص11، مشار إليه لدى: حسين، محمد عبد الظاهر. (1995) عقد التأمين مشروعيته آثاره إنهاؤه، القاهرة: مصر، دار النهضة العربية، ص11.

ويركّز التّعريف السّابق على عناصر التّأمين بشكلٍ أفضل من سابقه، فهو أشار إلى شركة التّأمين الّذي تمثّله الهيئات المنظّمة، وطريقة تحمّل الأخطار ونوع هذه الأخطار وطريقة تحويلها عبر المقاصة، دون إغفال ذكر القسط ومبلغ التّأمين واجبَي الدّفع من شركة التّأمين والمؤمَّن له.

ومن الفقه الأمريكيّ مَنْ عرّفه على أنَّه: "وسيلةٌ اجتماعيّةٌ لإحلال التأكّد محلّ عدم التأكّد في مجال تجميع الأخطار، وقد يكون التّأمين عمليّةً تجاريّةً، وقد تكون شركة التّأمين هيئةً حكوميّةً أو خاصّةً، ويستخدم في مجاله الأساليب الإحصائية[15]." لكن ما هو ملاحظٌ في كلّ ما سبق من تعاريفَ إغفال كلّ الفقهاء السّابقين لعنصر المصلحة التّأمينيّة، وهو أحد وسائل تمييز هذا العقد عن عقد المقامرة على سبيل المثال.

ولا شكّ أنّ التّعاريف تتعدّد وتختلف من فقيهٍ لآخر؛ نظراً لتركيز كلّ منهم على عنصرٍ معيّنٍ وإبرازه دون غيره من العناصر، فلا يمكننا الوصول إلى التّعريف الفقهيّ الشّامل ولكن بعد مراجعة تعريف الفقيه الفرنسي هيمار يمكن القول إنّه الأفضل والأكثر شمولاً لدى الفقه في فرنسا ومصر على السّواء فعرّفه على أنَّه: "عقدٌ بموجبه يحصل أحد المتعاقدين وهو المؤمَّن له في نظير مقابل يدفعه على تعهد يدفعه له أو للغير إذا تحقق خطر معيّن المتعاقد الآخر وهو المؤمّن الذي يُدخل في عهدته مجموعة من الأخطار التي يجري فيما بينها مقاصة طبقاً لقوانين الإحصاء[16]."

ويثير عقد التّأمين إشكاليَّة تشابهه مع القمار، حيث يعرَّف القمار على أنَّه: "مراهناتٌ يقوم بها أفرادٌ بدفع مبلغٍ معيّنٍ من أجل الحصول على ربح أو خسارة بناءً على معيار الحظّ والنّصيب دون أيّ أسسٍ موضوعيّة أخرى[17]". ولكن لا شكّ أنّ الفرق واضحٌ بين التّأمين والقمار، ولا مجال للخلط بينهما للأسباب الآتية:

---

[15] أحمد، ممدوح حمزة، وعبد الحميد، ناهد. (2003). إدارة الخطر والتأمين، (د.ن.)، ص242.

[16] السنهوري، عبد الرزاق أحمد. (1964). عقود الغرر وعقد التأمين، مج:2، بيروت: لبنان، دار إحياء التراث العربي، ص 1090، وأيضاً لدى: أحمد، (2003)، ص242.

[17] فلاح، عز الدين، (2008). التأمين مبادئه وأنواعه، ط:1، عمان: الأردن، دار أسامة للنشر والتوزيع، ص18.

أ_ يدفع المقامر مبالغ من المال من أجل اصطناع خطرٍ وهميٍّ ليس له وجود لولا فعل المقامر نفسه، فهو يبني كلّ عمله على الحظ والمقامرة، فقد يدفع مبلغاً قليلاً ويربح أموالاً كثيرةً، ولكن على المقلب الآخر فقد يخسر كلّ ما يملك في لحظةٍ واحدةٍ.

والفيصل هنا للتفريق هو أنّ عمليّة خلق الخطر في القمار من صنع المقامر نفسه، أمّا لو عدنا إلى الهدف الرّئيس من التّأمين فهو حماية الشخص وممتلكاته من الأخطار المُحدِقة به والتي تحصل خارج إرادته، بل وحتى لو حاول أن يحيد عنها فهي ستصيبه لا محالة دون أن يكون له دورٌ في إنشائها.

ب_ القمار هو أحد أسباب الإثراء، فإن فاز المقامر قد كسب أكثر ما كان يملكه، ولكن قد يخسر أكثر ممّا يملك أيضاً. أمّا التّأمين فلا يمكن النّظر إليه من هذه الناحية، فالمؤمَّن له إمّا أن يحصل على تعويضٍ يساوي خسارته، أو قيمة الشّي المؤمّن عليه، أو مبلغ التّأمين لا أكثر من ذلك[18].

بل إنّ ذلك مكرَّسٌ بنصوصٍ قانونيّةٍ من أجل القضاء على شبهة القمار ولإبعاد المتعاقدين عن إمكانيّة تحويل العقد إلى أحد وسائل الكسب غير المشروع، فقد نصّ المشرّع السّوريّ في المادة (717) من القانون المدنيّ على أنّه (لا يلتزم المؤمن في تعويض المؤمَّن له إلّا عن الضّرر الناتج عن وقوع الخطر المؤمّن منه بشرط ألّا يجاوز ذلك قيمة التّأمين).

ج_ يُعدُّ من شروط الخطر القابل للتغطية التّأمينيّة أن يكون احتمالياً، وغيرَ إراديّ؛ أي لا يد للمؤمّن له بحصوله، وإلّا لما استحقَّ التّعويض حسب العقد، كما أنّه يشترط أن يكون للمؤمّن له مصلحةٌ مشروعةٌ من هذا العقد ليتفادى الضّرر الحاصل من تحقّق هذا الخطر، وهو ما ذهب إليه المشرّع السّوريّ في المادة (715) فاعتبر محلّ التّأمين هو كلّ مصلحةٍ اقتصاديّةٍ مشروعةٍ تعود على المؤمَّن له من عدم وقوع خطرٍ معيّنٍ، أمَّا الخطر في القمار فهو من صنع المقامر نفسه.

---

[18] المرجع السابق، ص18-19، كما يراجع أيضاً الرّابط التالي:
https://www.insurance4arab.com/2014/03/blog-post_288.html?m=0
تاريخ الزيارة 2020\1\5، الساعة 5.30 p.m.

د_ لا يكون التّأمين على الأصول إلّا بأقل من قيمتها الحقيقية، فالتّأمين في حقيقته هو تشاركٌ بين شركة تأمين ومؤمَّن له في تحمّل الخطر، فلا يقع العبء كاملاً على المؤمّن في دفع المبلغ، بل يُترَك جزءٌ من هامش الخسارة ليتحمّله المؤمَّن له كونه الشّخص الأساسيّ الذي أصابه الخطر، وهنا تحديداً ينجح المؤمّن في تفادي مشكلة الخطر المتعمّد بأن يحصل الخطر بإرادة المؤمَّن له نفسه من أجل الحصول على التّعويض.

وبعد إيراد تعاريف التّأمين التّقليديّ التّشريعيّة والفقهيّة وتمييزه عن القمار يمكن الوصول إلى تعريفٍ مستمدٍّ من التّعاريف المتعدّدة للتّأمين على أنّه: "عقد يلتزم بمقتضاه المؤمّن بدفع مبلغ متّفق عليه مسبقاً لمصلحة المؤمَّن له أو المستفيد عند تحقّق خطر معيّن غير إرادي عبر عمليّة المقاصة بين مجموعة الأخطار التي يتحمّلها المؤمّن وباستخدام عمليّات إحصائيّة للأخطار المغطّاة وتعاون المؤمنين والمؤمَّن لهم في تحمّل الخسارة."

ثانياً: تعريف عقد التّأمين ضدّ مخاطر الإنترنت

ما يزال التّأمين ضدّ مخاطر الإنترنت مفهوماً جديداً في عالم التّأمين رغم مرور ما يقارب ثلاثة عقود على ابتكاره؛ لذلك لا يوجد حتى الآن تعريف تشريعيّ لهذا المفهوم، وإن كان وضع التّعاريف ليس من عمل القانون. وهنا يظهر عمل الباحثين وشركات التّأمين الذين انكبّوا على وضعِ تعريفٍ لهذا النّوع من التّأمين.

ويطلق على التّأمين ضدّ مخاطر الإنترنت مصطلح التّأمين السيبراني –cyber insurance– انطلاقاً من طبيعة الأخطار السيبرانية التي يغطّيها هذا التّأمين، وتشتقّ كلمة السيبرانية من كلمة سايبر cyber في اللّغة الإنكليزيّة وهي مصطلحٌ درج استخدامه لوصف الفضاء الذي يضمّ الشّبكات المحوسبة وشبكات الاتصال والمعلومات وأنظمة التحكّم عن بعد[19]، ولمّا كان التّأمين ضدّ مخاطر الإنترنت مرتبطاً بهذه الشّبكات والفضاء الإلكترونيّ فالتصق هذا المصطلح به وأصبح مرادفاً له.

[19] https://www.ar.wikipedia.org/wiki/%D8%B3%D8%A7%D9%8A%D8%A8%D8%B1

تاريخ الزيارة 20\4\2020، الساعة 11p.m.

وتتعدّد التّعاريف الفقهيّة التي ساقها المؤلّفون لوصف عقد التّأمين باختلاف وجهات النّظر، فاعتمد بعضها على معيار التّغطيات التّأمينيّة أو معيار البيئة التي يعمل فيها، وتراوحت التّعاريف بين تعاريف شارحة لصور هذه التّغطيات وأخرى تتحدّث عن بيئة العمل الإلكترونيّة على النّحو الآتي:

1-معيارٌ شارحٌ لصور التَّغطيات:

أطلق بعض الفقه على عقد التّأمين ضدّ مخاطر الإنترنت مصطلح (تأمين المسؤوليّة الإلكترونيّة) فعرّفوه بأنّه: "تغطية المخاطر المرتبطة بخرق البيانات؛ أي التدمير أو الفقدان أو التّعديل غير المقصود أو غير القانوني للبيانات، والكشف غير المصرّح به للبيانات، والدّخول إلى بياناتٍ شخصيّةٍ مخزّنةٍ أو معالجة في نظام معين لدى الشركة[20]." بيّن هذا التّعريف بعض صور الأخطار الإلكترونيّة الأكثر شيوعاً وهي الخرق والدخول غير المصرّح به.

واتّجه رأيٌ آخر لتعريفه إلى أنّه: "عقود تأمين مخصّصة لتغطية الخسارة نتيجة سرقة البيانات أو الأصول المعلوماتية، بالإضافة إلى تغطية خسائر أصول الشّبكات والمعلومات، وقد تصل التغطية إلى إعلام عملاء المؤمَّن له (الطرف الثالث) وتعويض المسؤوليّة والابتزاز الإلكتروني[21]."

وأبرز التّعريف السّابق أحد آثار عقد التّأمين ضد مخاطر الإنترت المتجسّد بواجب المؤمَّن له إعلام عملائه عند حصول أحد الخروقات، وهنا يعمل التّأمين على تغطية النّفقات النّاتجة عن هذا الواجب.

وأطلق بعض الفقه مصطلح (عقد التّأمين المعلوماتي) على عقد التّأمين ضدّ مخاطر الإنترنت وعرّفه على النّحو الآتي: "عقد مُبرم بين شركة متخصّصة في تأمين الأنظمة المعلوماتيّة ومالك النّظام

[20] Hibberd, G. (2014). The Rise of Cyber Liability Insurance, Rotterdam: Netherlands, Elsevier Inc, p 222-223.

[21] Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management–a modeling approach, semantic scholar, p23.

المعلوماتي، يكون الغرض منه حماية هذا النّظام من أيّ اختراقٍ أو فيرسة، وذلك طيلة المدّة المحدّدة للعقد[22]."

وكما هو واضح أنّ هذا التّعريف بالإضافة إلى أنّه ذكر بعض صور الأخطار الإلكترونية (الخرق ونشر الفيروسات)، فقد ذكر أيضاً أطراف العقد وهم مالكو الأنظمة المعلوماتيّة التي تعمل عبر الإنترنت وشركات التّأمين المتخصّصة في هذا النّوع من الأعمال.

في حين ذهب اتّجاهٌ آخرُ من الفقه إلى تعريف عقد التّأمين ضد مخاطر الإنترنت على النّحو الآتي: "عقود التّأمين المُصمّمة لتسوية مشكلات المسؤوليّة وخسارة الممتلكات وسرقتها، وتلف البيانات، وفقدان الدّخل النّاشئ عن انقطاع الشّبكة وفشل الكمبيوتر، بالإضافة إلى التّلاعب بموقع الويب والابتزاز الإلكترونيّ[23]"، ويُلاحظ في هذا التّعريف ذكر بعض نتائج الأخطار الإلكترونيّة مثل فقدان الدّخل والمسؤوليّة النّاشئة عن الخطر تجاه الغير (الطّرف الثّالث).

-معيار متعلّق ببيئة العمل الإلكترونيّة:

يتعلّق هذا المعيار بتعاريفَ أكثر عموميّةً، لم تبدِ الاهتمام بالبحث عن صور الأخطار الإلكترونيّة أو التّغطيات التّأمينيّة، ومن هذه التّعاريف:

عرّفت وكالة أمن المعلومات والشبكات الأوروبية (إنيسا) عقد التّأمين ضد مخاطر الإنترنت بأنّه: "طائفةٌ من عقود التّأمين التي تهدف إلى تغطية نطاق واسع من المشكلات المتعلقة بأخطار الفضاء الإلكتروني[24]." وقد اعتمد هذا التعريف على المكان الذي تقع فيه الأخطار تاركاً المجال مفتوحاً أمام صور هذه الأخطار من أجل توسيع نطاق التّغطيات التّأمينيّة.

---

[22] Raphael Peuchot, Rudiments juridiques à l'usage des clients de prestations d'intrusion informatique, Lamy Lexel, 26 mars 2002.

مشار إليه لدى: الناصري، أسنر خالد. (2019). المسؤولية المدنية عبر انتهاك الخصوصية عبر مواقع التواصل الاجتماعي- دراسة مقارنة، ط:1، القاهرة: مصر، دار النهضة العربية للنشر والتوزيع، ص 193.

[23] http://www.betterley.com

تاريخ الزيارة 2020\1\10 الساعة 9p.m.

[24] Incentives and barriers of the cyber insurance market in Europe, (2012) ENISA, p8.

بينما اتّجه تعريفٌ ثانٍ إلى أنّ: "عقد التّأمين هو حلٌّ يحرّكه السّوق ليحسّن استقرار القطّاع الخاص في مواجهة الأخطار الإلكترونيّة (السّيبرانيّة)[25]."

ويُنتقد هذا التّعريف لجهة اقتصاره على القطاع الخاص دون ذكر القطاع العام معه، مع أنّ المخاطر الإلكترونيَّة تضرب القطّاعين في آنٍ معاً، ولعلَّ القطاعات العامة تُصاب بضررٍ أكبرَ من غيرها من القطّاعات الخاصة نظراً لكون هذه الجهات تملك سجلّات بيانات أكبر من غيرها، ممَّا يوسّع نطاق الخسائر التي تصيبها.

في حين ذهب اتّجاهٌ ثالثٌ من الفقه إلى تعريف التّأمين على أنَّه:" تأمينٌ يهدف إلى حماية الشّركات والمؤسّسات، بل وحتّى الأفراد الطّبيعيين المستخدمين لشبكة الإنترنت من المخاطر المتعلّقة باستخدام الشّبكة المذكورة، ويمكن بصورةٍ أشمل القول إنّه تغطيةٌ لأخطارٍ متعلّقةٍ بالبنية التّحتيّة لتكنولوجيا المعلومات وأنشطتها[26]."

ويتميّز هذا التّعريف بإدخاله الأفراد ضمن نطاق التّغطيّة التّأمينيّة، فخرق البيانات وانتهاك الخصوصيّة يصيب الأفراد الطّبيعيين والاعتباريين على السّواء تاركاً آثاراً ماليّةً ومعنويّةً كبيرةً، بالإضافة إلى توسيع نطاق الأخطار المغطّاة.

كما ارتأى جانبٌ من الفقه الكندي وصف عقد التّأمين ضدّ مخاطر الإنترنت بأنّه: " مجموعةٌ من المنتجات والخدمات التي يعمل على تقديمها مزودو خدمات تأمين محليّون وعالميّون لمواجهة المخاطر الإلكترونية[27]."

كما ويعرّف التّأمين ضد مخاطر الإنترنت انطلاقاً من كونه عقد تأمين ضدّ المسؤولية السيبرانية بكونه عقداً تشتريه الكيانات الاقتصاديّة لتقليل الأخطار الماليّة المترابطة مع القيام بالأعمال عبر الشبكة

---

[25] Aburish, N., Fixler, A., & Dr. Hsieh, M. (2019).The Role of Cyber Insurance in Securing the Private Sector, Washington, DC: United States Of America, center on cyber and technology innovation, p1.

[26] إبراهيم، حسام. (2019). التطور التكنولوجي وقطاع التأمين ما لنا وما علينا، بحث مقدم إلى المؤتمر الدولي السابع للتأمين (مؤتمر العقبة)، الأردن، ص 22.

[27] An introduction to cyber insurance understanding the Canadian ecosystem, (2019) the conference board of Canada, p4.

(أونلاين)، حيث يدفع المؤمَّن له أقساطاً دوريّةً شهريّةً أو ربعيّةً مقابل تحويل بعض المخاطر إلى المؤمّن[28].

يبرز التعريف آثار هذا العقد من حيث واجب دفع الأقساط والالتزام بالتغطية.

وعليه يُتوصّل إلى **تعريف لعقد التّأمين ضدّ مخاطر الإنترنت بعد معاينة هذه التعاريف، بأنّه:**

عقدٌ يُبرم بين شركة تأمين ومؤمَّن له، تلتزم من خلاله شركة التّأمين بتغطية المؤمَّن له ضدّ كلّ أو بعض الأخطار التي تصيبه نتيجة لاستخدام الإنترنت بما تشمله من تغطية للطّرف الأوّل (المؤمَّن له) لما يصيبه من أضرار، أو للأضرار التي تصيب الطّرف الثّالث أي المسؤوليّة النّاشئة عن الأخطار المذكورة، ويلتزم المؤمَّن له في المقابل بدفع أقساطٍ محدّدةٍ في العقد والقيام بالواجبات التي تفرضها عليه شركة التّأمين لضمان حسن تنفيذ العقد.

وتبرز هذه التّعاريف أوجه اختلاف وتميّز عقد التّأمين ضدّ مخاطر الإنترنت لناحية اختلاف الشّيء المؤمّن عليه، واختلاف الخطر المؤمّن ضدّه، واختلاف صور التّغطيات التّأمينيّة على النّحو الذي سيتمّ تفصيله لاحقاً.

ويتبادر إلى الأذهان تساؤلٌ حول مدى إلزاميّة التّأمين ضدّ مخاطر الإنترنت بالنّسبة للشّركات الكبيرة أو حتّى الصّغيرة والمتوسّطة خاصةً إذا ما عرفنا أنّ آثار الهجمات الإلكترونيّة عليها قد تكون مدمّرةً وتوصلها إلى الإفلاس في أحيانٍ كثيرةٍ؟

والحقيقة كما نعلم أنّ القانون بطابعه الإلزاميّ وبما يفرضه من مؤيّداتٍ يتّجه نحو إلزام الأفراد بالقيام بواجباتٍ معيّنةٍ من أجل تحقيق مصلحة المجتمع، فعلى سبيل المثال:

أ-ضرورة التّأمين الإلزاميّ على المركبات، وهو ما اتّجه إليه المشرّع السّوريّ في قانون السير[29] وذلك نتيجةً لكثرة حوادث السّير الحاصلة والأضرار التي تصيب مالك السيّارة والغير على السّواء، فعند حصول حادث

---

[28] https://www.searchsecurity.techtarget.com/definition/cybersecurity-insurance-cybersecurity-liability-insurance

تاريخ الزيارة:2020\1\10, الساعة 6p.m.

[29] المادة 37 من المرسوم التشريعي رقم 11 لعام 2008 المعدل لقانون السير والمركبات رقم 31 لعام 2004 تنص على: (لا يجوز تسجيل أو ترخيص أي مركبة أو تجديد الترخيص إلا بعد تقديم عقد تأمين لدى إحدى شركات التأمين المسجلة في الجمهورية العربية السورية لممارسة أعمال تأمين المركبات، لتغطية المسؤولية المدنية عن الأضرار المادية والجسدية التي تلحق بالغير والناجمة عن استخدام تلك المركبة.)

كهذا تلتزم شركة التّأمين بتعويض المضرور وتخفيف عبء دفع مبالغَ طائلة عن عاتق المالك. فلو أُخِذ التّأمين الإلزاميّ على السيّارات كمثالٍ لإلزاميّة التّأمين، نجد أنّ المشرّع لم يتدخّل في هذا النّطاق إلّا بعد أن لاحظ كثرةً في الحوادث المتكرّرة والأضرار الحاصلة للأشخاص وحالات التهرّب العدّة من أصحاب الحوادث، فكان ذلك إحدى محاولات المشرّع لإعطاء كلّ ذي حقٍّ حقّه.

ب_ كما أنّ التّأمين الصّحيّ الإلزاميّ الذي فرضه القانون بالتّعاون بين ربّ العمل والعامل هو نتيجةً لما يتكبّده العاملون من أعباءٍ كثيرة في أثناء أعمالهم، وما قد يصابون به من أضرار في أثنائها، ومحاولة تهرّب أرباب عملهم من تغطية هذه الأضرار، مما ذهب بالقانون إلى الوقوف إلى صفّ العمّال وإنصافهم بأن ألقى جزءاً من هذه المسؤوليّة على عاتق أرباب عملهم عبر إلزامهم بإبرام عقد تأمينٍ صحيٍّ لصالح عمّالهم، وذلك في قانون الضمان الصحي، الذي أكد على إحداث هيئة عامة للضمان الصحي مهمتها تأمين معالجة المنتفعين ورعايتهم طبيا في حال المرض والحوادث والحمل والولادة[30].

وبالعودة إلى التّأمين ضدّ مخاطر الإنترنت، فلا يوجد حتى الآن أيّ قانونٍ يُلزم المتعاملين عبر شبكات الإنترنت –أفراداً كانوا أم مؤسّسات– بأن يبرموا عقود تأمينٍ لممتلكاتهم غير الماديّة كالبرمجيّات والبيانات، أو ضدّ المسؤوليّة النّاشئة عن حالات الخروقات والقرصنة وغيرها من هذه المخاطر.

لكن من خلال تتبّع الأخطار الإلكترونيّة التي تحصل يومياً حول العالم، يمكن القول إنّ إمكانية اتّجاه القانون نحو إلزاميّة التّأمين السيبراني تغدو مسألة وقت فحسب للأسباب الآتية:

أ_ إنّ الأخطار الإلكترونيّة باتت في قمّة الأخطار التي تواجهها الأعمال اليوم، نظراً لاعتماد هذه الأعمال على الإنترنت في تسيير أعمالها، وخاصّةً أنّ عملاءها قد يكونون أجانب وفي غير دولةٍ فلا يكون لهم إلّا الوسائل الإلكترونيّة لمتابعة أعمالهم.

ب_ انتشار الجرائم الإلكترونيّة بصورةٍ غير مسبوقة مسبّبة خسائرَ ماليّةً فادحةً تعجز شركاتٌ بأسرها عن تعويضها، وما يرافق هذه الجرائم من صعوبة ملاحقة المجرمين وفقاً لأحكام القوانين ونظراً لمجهوليّة مكان تواجدهم وصعوبات تحديد القوانين الواجبة التطبيق.

---

[30] قانون الضمان الصحي رقم 1 لعام 1979.

ج_ حالات تهرب الشركات من دفع التعويضات المستحقة للمتضررين من الجرائم المذكورة؛ لأنّ حجم البيانات المخترقة كبيرٌ جداً ويصل لمئات آلاف المستخدمين مع تعويضات بملايين الدولارات، بالإضافة إلى النفقات التي تتكبّدها الشّركات لمعالجة آثار هذه الجرائم وما تستغرقه من وقتٍ أيضاً.

د_ عدم إمكانية تفادي هذه الأخطار فهي ستقع ولو تأخّرت وبرغم محاولات منع وقوعها.

هـ_ التّأمين إحدى وسائل إدارة المخاطر التي تعمل على تخفيف حدة الأخطار عند وقوعها عبر تحويل الخطر إلى طرفٍ ثالثٍ؛ أي شركة التّأمين التي ستتولّى الدّفع نيابةً عن الشّركات المصابة إلى عملائها المتضرّرين أو تعمل على تعويض الفرد المتضرّر من فقدان بياناته الشّخصيّة (على سبيل المثال)، كما أنّ كثيراً من الشّركات في أمريكا وأوروبا لجأت إلى التّأمين السيبراني ممّا انعكس إيجاباً على انتعاش السّوق وتوسّعه المستمرّ.

وعليه ولهذه الأسباب المذكورة آنفاً كلّها يمكن تبرير إمكانيّة إضفاء الطّابع الإلزاميّ على التّأمين السيبراني من أجل وضع حدٍّ لهذه المشكلات جميعها التي يعانيها مستخدمو الإنترنت اليوم.

ويمكن بعد تعريف عقد التّأمين ضدّ مخاطر الإنترنت العمل على تقييمه في الفرع الثّاني عبر ذكر الدّوافع، والخصائص، ومن ثمّ المشكلات التي تواجه هذا النّوع من عقود التّأمين.

الفرع الثاني

تقييم عقد التّأمين ضد مخاطر الإنترنت

وتعاني الشّركات في أثناء قيامها بعملها عبر الإنترنت من بعض المضايقات التي يقوم بها مجرمون يتّخذون من الفضاء الإلكترونيّ مقرّاً لأعمالهم التّخريبيّة، فيخترقون حواسيب العمل ويسرقون البيانات ويبتزون الشركات لدفع مبالغَ باهظة الثّمن. ولأجل ذلك باتت الشركات تلجأ إلى التّأمين ضد مخاطر الإنترنت في محاولةٍ منها لإدارة هذه المخاطر، وهذا هو حال الأفراد الذين يقومون بأنشطتهم إلكترونيّاً، ولعقد التّأمين ضد مخاطر الإنترنت سماتٌ تميّزه عن غيره من العقود، وتبرز صفاته الفريدة، ولكنّه كأيّ عقدٍ جديدٍ في بداية طريقه ما يزال يعاني من مشكلاتٍ تجعله يتعثَّر في طريقه نحو التبنّي الواسع من شركات التّأمين، وعليه نبيّن في هذا الفرع

دوافع عقد التّأمين ضد مخاطر الإنترنت (أولاً)، ثمّ ننتقل لبيان خصائصه (ثانياً)، والمشكلات التي تعترضه (ثالثاً).

أولاً: دوافع عقد التّأمين ضدّ مخاطر الإنترنت:

حيث تندفع الشّركات تحت وطأة المخاطر التي تواجهها إلى العمل على الحدّ من آثار الخطر عبر وسائل إدارة الخطر المعروفة التي تتراوح بين منع الخطر، الاحتفاظ بالخطر، التّأمين الذّاتيّ، وتحويل الخطر. ولمّا كان الخطر بطبيعته غير متوقّع ومتغيّر بشكلٍ كبيرٍ فلا يمكن الوصول إلى منعه بشكلٍ كاملٍ، بل يعدّ ذلك مستحيلاً، أمّا الاحتفاظ بالخطر ومتابعة العمل فهو لخطرٌ أكبر، فقد يؤدّي ذلك إلى إفلاس الشّركات وانهيار سلسلةٍ من الشّركات بسبب ذلك، في حين أنّ التّأمين الذاتيّ هو ما تتّبعه كثيرٌ من الشركات عبر تكوين إدارة محافظَ ذاتيّةٍ للخطر لتتعامل عند حدوث الكارثة، ومع ذلك فهي قد لا تكفي، فلا يبقى أمام المؤسّسات الاقتصاديّة إلّا تحويل الخطر إلى طرفٍ ثالثٍ ليتحمّل تبعة الأخطار مع المؤمَّن لهم.

وهذا هو حال عقد التّأمين ضدّ مخاطر الإنترنت الذي بات يؤدّي دوراً كبيراً في ظلّ تعاظم الأخطار الإلكترونيّة واتّساع سوق العمل الإلكتروني، فبات مقصد كثيرٍ من الشّركات، وذلك لأسبابٍ كثيرةٍ سيتمّ بيانها وفق الآتي:

1- كثرة المخاطر الإلكترونيّة وتعدّدها، حيث يذهب باحثون إلى أنّه من المستحيل جعل الإنترنت آمناً بالكامل، وتُعزى هذه الاستحالة إلى التطوّر الكبير والسّريع في البرمجيّات الضّارّة والفيروسات والبريد المضلّل، ممّا يجعل من الصعوبة والتّكلفة العالية التوصل إلى نظامٍ آمنٍ من الأخطار كلّها، كما أنّ الإنترنت هو عالمٌ مترابطٌ ومتبادلٌ بحيث إنّ الخطر الذي يصيب مستخدماً لا يؤثّر عليه وحده بل يمتدُّ ويصل لمستخدمين عديدين غير قابلين للحصر، فإطلاق فايروس على شكل رابط في أحد المواقع لا يقتصر خطره على شخص واحد لكون الموقع مفتوح للعامّة، إذ يصيب كلّ شخص يضغط على الرابط[31].

[31] Baras, J. S., Katz, j., & Altman, E. (2011) Decision and game theory for security second international conference, game sec, Berlin, Germany, Springer, p132.

2-وثائق التّأمين العاديّة لا تغطّي الأخطار الإلكترونيّة، ذلك أنّ أكثر المؤسّسات تشتري وثائق تأمين تقليديّة كوثيقة تأمين العمل الشّخصيّ والوثيقة التّجاريّة العامّة ووثيقة انقطاع العمل ظنّاً أنّ هذه الوثائق قد تحميها من الأخطار الإلكترونيّة، لكنّ الحقيقة أنّ نزاعاتٍ عدّة قد نشبت بين مؤمّنين ومؤمّن لهم عند حدوث اختراقاتٍ إلكترونيّة، ورفض المؤمّنين دفع التّعويضات اللّازمة؛ إذ إنّ هذه الوثائق تغطّي المخاطر التّقليديّة التي تظهر في شكلٍ ماديٍّ محسوسٍ وإن كان لها نتائج غير ماديّة، بينما الأضرار الإلكترونيّة تأخذ شكلاً غيرَ ماديٍّ، وهنا ثار النّزاع حول تحديد ما يعدّ مادياً وغير ماديّ، فضلاً عن أنّ بعض الشّركات كانت تستثني المخاطر الإلكترونيّة بشكلٍ صريحٍ من التّغطية[32].

3-التّعويض الجزائيّ للأخطار الإلكترونيّة يرتبط بكون الفعل جريمةً إلكترونيّةً؛ نظراً لضيق النّصّ الجزائيّ غير القابل للقياس، أمّا خارج النّص الجزائيّ فلا تجريم ولا تعويض جزائيّ، وإن وُجِد التجريم فأغلبيّة الجرائم تكون عالميّةً؛ أي من خارج النِّطاق المحلّيّ، والمجرمون غير قابلين للتتبع فيخسر المضرور مبالغَ كبيرةً دون إمكانيّة محاكمة المجرمين، وهنا برز التّأمين ضدَّ مخاطر الإنترنت كوسيلةٍ للتَّعويض عن الأضرار الحاصلة.

4-توفير حمايةٍ واقيّةٍ قبل الحوادث عبر المراقبة الدَّائمة لأنظمة العميل، وتحديد مواطن الضَّعف، وتوفير الدَّعم للموجودات الحالية[33]، ولهذه المراقبة دورٌ كبيرٌ في تقليل إمكانيّة التّعرّض للأخطار والخسائر الواقعة حال حصوله، فالتّأمين ضدّ المخاطر الإلكترونيّة يوفّر مراقبة النّظام من قبل خبير على مدار السّاعة، ويمكّن شركة التّأمين من اتّخاذ خطواتٍ سريعةٍ ضدّ كلّ تهديد[34].

5-زيادة الأمان عبر شبكة الإنترنت؛ إذ يعزّز التّأمين ضد مخاطر الإنترنت الأمن الذاتي للمؤمَّن له، فحتّى تقبل شركة التّأمين التّغطية فإنّها تشترط على المؤمَّن له تبنّي مستوى معيّن من الأمن عبر الشَّبكة كجدران

---

[32] Kesan J. p. & Others, (2005). cyber insurance as a market based solution to the problem of cyber security- a case study, workshop on economics information security (WEIS), p5.

[33] Cyber insurance: a reference guide, institute for development and research in banking technology. (2017). reserve bank of India, p10.

[34] Kesan J. p. & Others, (2005), p11.

حماية ومضادات فيروسات من إصدارٍ معيّنٍ؛ وذلك من أجل العمل على تخفيض معدل إصابة المؤمَّن له بالخطر وتقليل حجم الخسائر.

لذلك يعمل المؤمَّن له على تبنّي أفضل الممارسات في سبيل الحصول على موافقة شركة التّأمين، كما أنَّ زيادة معدل الأمن الذاتي يعني مخاطر أقلّ وخسائرَ أقل، وذلك يعمل على تخفيض قيمة الأقساط التي سيدفعها؛ لأنَّ نظامه المستخدم سيكون أكثر أماناً[35].

6- يحقّق التّأمين ضدّ مخاطر الإنترنت مصلحة المؤمَّن له في حماية ممتلكاته المعلوماتيّة وسمعته التّجاريّة من أخطار الإنترنت، كذلك شركات التّأمين التي تسعى لتحقيق الرّبح تستفيد من التّأمين عبر الانخراط السّريع في سوق التّأمين، والعمل على توزيع الأخطار بين شركات تأمين متعددة وتقييم وتحليل الأخطار بدقّةٍ، وصياغة أقساطٍ متناسبةٍ تغطّي الخطر وهامش الرّبح بشكلٍ يحقّق مصلحة طرفي العقد، في حين لو أنّ الخطر قد تمّ تقييمه بشكلٍ غير دقيقٍ لأدّى ذلك إلى كارثةٍ تصيب شركة التّأمين والمؤمَّن له على السواء[36].

ثانياً: خصائص عقد التّأمين ضدّ مخاطر الإنترنت:

يتّسم عقد التّأمين ضدّ مخاطر الإنترنت بعددٍ من الخصائص التي تميّزه عن غيره من العقود، والمستمدّة من الخصائص العامّة لعقود التّأمين، وذلك بما يتّفق والطّبيعة الخاصّة لهذا النّوع من عقود التّأمين:

1-عقد رضائي:

الرضائيّة في العقود هي اتّجاه إرادة الأطراف بكلّ حريّةٍ نحو الالتزام بأداءٍ معيّنٍ دون التوقّف على شكلٍ أو عملٍ عينيٍّ؛ أي مجرّد تطابق الإيجاب والقبول، وخلاف العقد الرّضائيّ هو العقد الشّكليّ الذي يتوقّف انعقاده على توفّر شكل محدّد بحيث إنّ تخلّفه يعني بطلان العقد. ويُعدّ عقد التّأمين ضدّ مخاطر الإنترنت عقداً رضائيّاً لعدم استلزام وجود شكل معيّن لانعقاده، أمَّا الكتابة التي يتطلّبها العقد فلا تجعل منه عقداً شكلياً، إذ إنّ العقد انعقد عند تطابق الإيجاب والقبول، وتقتصر الكتابة على كونها وسيلة إثباتٍ ليس إلّا، كما هو حال وثيقة

[35] Clinton, L. (n.d.). Cyber-Insurance Metrics and Impact on Cyber-Security, Internet Security Alliance, Online paper, p1.

[36] Kesan J. P., Yurcik, W., & Majuca, R., (2006), p2.

التّأمين فهي تفسّر العقد وتوضّح شروطه. كما أنّ إلزام المؤمَّن له بدفع القسط الأول لا ينفي عنه صفة الرّضائيّة، بل يقتصر الأمر على بيان آثار العقد فقط[37].

2-عقدٌ ملزمٌ لجانبين:

وهو ما يُسمّى بتبادليّة الالتزامات، فسبب التزام الطّرف الأوّل هو سبب التزام الطّرف الثّاني، وتنشأ هذه الالتزامات من لحظة إتمام العقد بتطابق الإيجاب والقبول، ويلتزم المؤمَّن له بدفع الأقساط المترتبة عليه والإبلاغ عن الخطر طوال مدّة العقد حال حصوله أو حصول تغيّر عليه، في حين تلتزم شركة التّأمين بدفع المبلغ المتّفق عليه في عقد التّأمين. **وفي نطاق عقد التّأمين ضدّ مخاطر الإنترنت** تلتزم شركات التّأمين أيضاً بالإضافة إلى تقديم المساعدة والاستجابة الدّائمة طوال مدّة العقد للمؤمّن له، بتقديم الاستشارات له في مرحلةٍ ما قبل تحقّق الحادث، وفي حال حصول الخطر (الحادث المؤمّن ضدّه) فإنّها تلتزم بالإضافة إلى دفع مبلغ التّأمين بالعمل على استرجاع البيانات المخترقة، ودفع الفدية في حالات الابتزاز الإلكترونيّ، ودفع نفقات التّقاضي والغرامات المفروضة، بالإضافة إلى واجب تعويض الغير (الطّرف الثّالث) المتضرّر من الخرق، ناهيك عن وضع فريقٍ كاملٍ من الاستشاريّين المتخصّصين في الاستجابة السّريعة لحوادث الخرق في خدمة المؤمَّن له في محاولةٍ لتخفيف آثار الخرق، وذلك بحسب الاتفاق بين شركة التأمين والمؤمَّن له إذ قد يقتصر على بعض هذه الخدمات، والتزام المؤمَّن له بالدفع غالباً ما يبدأ منذ اللحظة الأولى للإبرام، في حين أنّ المؤمّن يبقى ساكناً حتى حصول الخرق ليقوم بالتزاماته، إذ يمكن القول إنّ التزام المؤمَّن له مؤكّدٌ، أمّا التزام شركة التّأمين احتماليٌّ معلّقٌ على شرط حصول الخرق (الخطر)[38]، ويبقى هذا الالتزام قائماً ما دام العقد صحيحاً، بحيث لا يحقّ لأحدهما الانفكاك عن التزامه دون رضا الطّرف الآخر[39]، مع مراعاة الاستثناءات الواردة في الوثيقة، **ويبرز في هذه الالتزامات مدى اتّساع تغطية شركات تأمين مخاطر الإنترنت عن غيره من عقود التّأمين.**

---

[37] حسين، (1995)، ص 61-62، والخفاجي، منعم. (2014)، مدخل لدراسة التأمين، ط:1، (د.ن.)، ص17.

[38] سيد، سالم رشدي. (2015). التأمين المبادئ والأسس والنظريات، ط:1، عمان: الأردن، دار الراية للنشر والتوزيع، ص65-64.

[39] القره داغي، علي محيي الدين. (2010). التأمين الإسلامي دراسة فقهية تأصيلية مقارنة بالتأمين التجاري مع التطبيقات العملية، ط:1، بيروت: لبنان، دار البشائر للطباعة والنشر والتوزيع، ص 14.

3-عقد احتماليّ:

تقوم الاحتماليّة في عقد التّأمين ضدّ مخاطر الإنترنت على حدثٍ غير محقّق الوقوع، فالخطر وإن كان محدداً بدقّةٍ إلّا أنّه غير معروف تاريخ الوقوع، إذ إنّ العقد معلّقٌ على حدثٍ سيقع في المستقبل على نحوٍ غير مؤكّدٍ، فلا يعرف المؤمَّن أو المؤمَّن له مقدار ما سيأخذه ويدفعه أيّ منهما تبعاً لتاريخ تحقّق الخطر، فقد يمضي العقد وينتهي دون تحقّق الخطر المؤمّن ضده؛ أي أنّ الاحتماليّة المقصودة هنا هي فقط احتمالية وقوع الخطر، أمّا الالتزامات فهي ثابتةٌ بموجب العقد وملزمةٌ لجانبيه طوال مدة العقد.

4-عقد زمني:

يُعدّ عقد التّأمين ضدّ مخاطر الإنترنت عقداً زمنياً مستمراً لمدّةٍ معيّنةٍ محدّدةٍ في العقد بالمقارنة مع العقد الفوريّ الّذي ينتهي في لحظته بتنفيذ أطرافه لالتزاماتهم في ذات اللحظة[40]، إذ إنّ الزمن عنصرٌ جوهريٌّ في العقد المستمرّ فيلتزم أطرافه بالتزاماتٍ متكرّرةٍ طوال مدّة العقد. حيث يلتزم المؤمَّن له بدفع الأقساط طوال مدّة العقد وبإعلام المؤمّن في حال حصول الخطر أو حصول أيّ تغيّر عليه، **وفي نطاق خصوصية التّأمين ضد مخاطر الإنترنت** يلتزم المؤمَّن له بحماية أنظمته وحواسيبه من الأخطار الإلكترونيّة، فهو ملزمٌ بأن يعمل على تحديث أنظمة الحماية التي يستعملها لتتوافق مع ما تطلبه شركة التّأمين منه، كما أنّه ملزمٌ بعدم القيام بأيّ فعلٍ من شأنه أن يسهّل تحقّق الخطر، كالضغط على روابطَ مشبوهةٍ أو الدخول إلى مواقعَ غير آمنةٍ أو استخدام نسخ منتهيّة الصلاحية من برامج مكافحة الفيروسات، أمّا شركة التّأمين فهي ملزمةٌ طوال مدّة العقد بأن تتحمّل تبعة الأخطار التي أُمِّن عليها في العقد وتلتزم بدفع الأقساط والنفقات المترتبة حال حصول الخطر، فالالتزام الأساسي لشركة التّأمين ولو لم يتحقق الخطر هو أن تبقى مسؤولةً في حال حصول الخطر خلال المدّة المحدّدة. وينتج عن كون العقد مستمراً أنّ إبطال العقد أو فسخه يكون فقط للمستقبل دون أن يؤثّر على ما رتّبه من آثارٍ في الماضي، فما دفعه المؤمَّن له لا يمكن ردّه؛ وذلك لأنّه مقابلٌ لما تحمّلته شركة التّأمين من تبعة احتماليّة حصول الخطر في ذلك الوقت، وتقتصر آثار الفسخ من تاريخ حصول الفسخ فقط[41].

---

[40] حسين، (1995)، ص 60- 61.

[41] عبيد، أسامة. (2016). استراتيجيات التأمين المفهوم والأهداف، ط:1، عمان: الأردن، دار أمجد للنشر والتوزيع، ص74.

5- عقد معاوضة:

حيث يحصل كلّ طرفٍ على منفعةٍ تقابل ما يؤدّيه للآخر، فتلتزم شركة التّأمين بتحمّل عبء الخطر ودفع المبلغ المتّفق عليه في مقابل حصولها على قسطٍ دوريٍّ يلتزم بدفعه المؤمَّن له، ولكن قد يجتمع عقد المعاوضة مع التبرع في حال وجود مستفيد هو طرفٌ ثالثٌ إلى جانب شركة التّأمين والمؤمَّن له، إذ تلتزم شركة التّأمين بدفع التعويض له ويلتزم المؤمَّن له بدفع الأقساط للمؤمّن دون أيّ التزامٍ من جانب المستفيد[42].

6-عقد إذعان:

ساد الرّأي على أنّ عقد التّأمين هو عقد إذعانٍ؛ نظراً للمركز القوي الذي تشغله شركات التّأمين في هذا العقد، فالأخيرة تضع شروطها ولا يكون للمؤمَّن له إلّا الموافقة عليها أو رفضها جملةً مع هامشٍ صغيرٍ من إمكانية المناقشة[43]، **وتظهر خاصيّة الإذعان في ظلّ التّأمين ضدّ مخاطر الإنترنت أيضاً**، ففي ظلّ المخاطر الإلكترونيّة والمخاوف من الآثار الجسيمة لها التي تكلّف الشّركات يومياً ملايين الدولارات لا يبقى أمام المؤمَّن له إلّا الانصياع لما تفرضه عليه شركة التّأمين من التزاماتٍ، لا سيّما إذا ما علمنا بارتفاع الأقساط ونقص شركات التّأمين التي تقدّم خدمات التّأمين ضدّ مخاطر الإنترنت، حيث يبقى المؤمَّن له الطّرف الضّعيف، لا سيّما في ظلّ الظّروف الصّعبة التي يعانيها سوق التّأمين ضدّ مخاطر الإنترنت. وبالرغم من هذه الرأي إلا أن الرأي أميل إلى نفي صفة الإذعان عن هذا العقد نظراً لوجود أكثر من شركة تأمين، بالإضافة إلى إمكانيّة مناقشة الشروط، ناهيك عن عدم إلزاميته حتى الآن. وعموماً قد تدخّل المشرّع السّوريّ كغيره من المشرّعين في محاولةٍ منه لرفع الإجحاف بحق المؤمَّن له فقضى ببطلان بعض الشروط فيما لو تضمنها عقد التّأمين، وورد ذلك في المادة 716 من القانون المدني السوري[44]، كما يعمل القضاء على تفسير الغموض في عقد التّأمين لمصلحة الطّرف المذعن

---

[42] حسين، (1995)، ص61.

[43] الخفاجي، (2014)، ص18.

[44] يقع باطلاً ما يرد في وثيقة التّأمين من الشروط الآتية:

1 . الشرط الذي يقضي بسقوط الحق بالتّأمين بسبب مخالفة القوانين والأنظمة، إلا إذا انطوت هذه المخالفة على جناية أو جنحة قصدية.

2 . الشرط الذي يقضي بسقوط حق المؤمَّن له بسبب تأخره في إعلان الحادث المؤمن منه إلى السلطات، وفي تقديم المستندات، إذا تبين من الظروف أن التأخر كان لعذر مقبول.

3 . كل شرط مطبوع لم يبرز بشكل ظاهر وكان متعلقاً بحالة من الأحوال التي تؤدي إلى البطلان أو السقوط.

4 . شرط التحكيم إذا ورد في الوثيقة بين شروطها العامة المطبوعة، لا في صورة اتفاق خاص منفصل عن الشروط العامة.

وهو المؤمَّن له كما هو معمول به في القواعد العامة لعقود الإذعان، وعلى ذلك جاء بأحد اجتهادات محكمة النقض المصريّة من أنّ الغموض أو الشّكّ في عبارات عقد التّأمين يُفسَّر لمصلحة المؤمَّن له[45].

7-عقد تجاري:

قد يكون عقد التّأمين مدنياً أو تجارياً تبعاً لصفة المتعاقدين، فهو تجاريٌّ بالنسبة لشركة التّأمين التي تتّخذ شكل شركةٍ مساهمةٍ مغفّلةٍ تهدف إلى تحقيق الربح، أمّا المؤمَّن له فقد يكون مدنياً كما لو أمّن شخص على حياته أو تجارياً كما لو أمّنت شركة على مصانعها ضدّ الحريق أو على بضائعها من التلف[46].

أمّا في نطاق عقد التّأمين ضد مخاطر الإنترنت، فإنّ المؤمّن بالتأكيد هو شركة تأمينٍ تجاريّةٍ تهدف إلى الرّبح، أمّا المؤمَّن له فهو غالباً شركاتٌ عملاقةٌ تخزّن بيانات عملائها إلكترونياً وهي غالباً ما تكون شركات تجارية، لذلك يوصف العقد في معظم الحالات بأنّه تجاريٌّ بالنسبة لطرفيه في نطاق عقد التّأمين ضد مخاطر الإنترنت.

8-عقد حسن النية:

يُعدّ حسن النية المبدأ الأساسيّ الذي يحكم العقود كلّها، إلّا أنّه في نطاق التّأمين ضد مخاطر الإنترنت يؤدّي دوراً رئيساً في إبرام العقد وضمان استمراره وتنفيذه على أكمل وجه. فشركة التّأمين تعتمد في قبولها التّأمين على ما يدليه المؤمَّن له عن صفات الخطر عند إبرام العقد من حيث شدّته ومدى إمكانية حدوثه، وكما يستمرّ هذا الالتزام طوال مدةّ العقد في حال حصول أيّ تغيير في الخطر المؤمّن ضده، بحيث إنّ سكوت المؤمَّن له عن هذا الإخبار أو إخفاءه لمعلوماتٍ جوهريّةٍ يؤثر في الخطر المؤمن ضده وقد يخوّل شركة التأمين فسخ العقد لما ما يمكن اعتباره غشاً في حقها من جانب المؤمَّن له[47]. كما يقوم التزام حسن النية من جانب شركة التّأمين، نظراً لجهل المؤمَّن له الأسس الفنية للتأمين التي تقوم عليها عملية الإحصاء وتحديد الأقساط والتي

---

5 . كل شرط تعسفي آخر يتبين أنه لم يكن لمخالفته أثر في وقوع الحادث المؤمن منه.

[45] https://www.cc.gov.eg/judgment_single?id=111307435&ja=164593

تاريخ الزيارة: 4\5\2021، الساعة: 9:42 p.m.

[46] سيد، (2015)، ص66.

[47] حسين، (1995)، ص65- 66.

يفترض علم شركة التأمين بها[48]. **و في نطاق التّأمين ضد مخاطر الإنترنت** يقوم هذا المبدأ بشكل أكبر وأكثر أهميةً وذلك لصفة الخطر الإلكتروني الذي يحيط بأنظمة وبرمجيات وحواسيب المؤمَّن له، ومن غيره أكثر دراية بمدى حماية شبكاته ومدى إمكانية اختراقها، ولا سيما أنّه يقع عليه واجب الإجابة عن عشرات الأسئلة الأمنية التي يطرحها عليه المؤمن قبل الموافقة على التّأمين، ففي حال لم يلتزم المصداقية في الإخبار عن تعرضه لعملية اختراق في وقتٍ سابقٍ أو وجود موظّفين من داخل الشركة يسرّبون معلوماتها أو يبتزّونها إلكترونياً ، فهو سيكون الخاسر الأكبر؛ لأنّ ذلك يخوّل المؤمّن الامتناع عن القيام بواجباته المحدّدة حسب العقد المبرم.

10-عقد تحويل للأخطار:

إذ يلجأ المؤمَّن له إلى شركة تأمين لتتحمّل بالنيابة عنه الأخطار التي قد يتعرّض لها أثناء قيامه بعمله؛ لأنّ هذه الأخطار قد تكون كبيرةً وكارثيّةً ومتكرّرةً بصورةٍ تخرج عن قدرة المؤمَّن له على تحملها. وتظهر أهميّة هذا العقد وتزيد في نطاق المخاطر الإلكترونية؛ لكونها غير قابلة للتفادي رغم وسائل الحماية كلّها التي قد يتّبعها المؤمَّن له، ولما تسبّبه له من خسائرَ كبيرةٍ.

11-عقد تقليدي أو إلكتروني:

قد يكون عقد التّأمين ضدّ مخاطر الإنترنت عقداً يبرم بطريقةٍ تقليديّةٍ عن طريق التواصل المباشر بين شركة التّأمين والمؤمَّن له، كما هو حال التّأمين التقليدي الذي كان و ما يزال يبرم حتى يومنا هذا، إذ قد يُبرِم العقد بصورةٍ مباشرةٍ بين شركة التّأمين والمؤمَّن له أو بين المؤمَّن له ووسيط التّأمين، وذلك عن طريق تقديم طلبٍ من المؤمَّن له يبدي فيه رغبته بالحصول على تأمين من شركةٍ معيّنةٍ، ويتم التفاوض بين الأطراف من أجل تحديد الأقساط وكتابة وثيقة التّأمين التي تحدّد شروط التّأمين ومدّته وكيفيّة تنفيذه من حيث دفع الأقساط والمبالغ المؤمّنة، وإن كان ذلك لا يمنع من استعمال وسيلةٍ إلكترونيّةٍ كدفع الأقساط عبر تحويلاتٍ إلكترونيّةٍ أو دفع مبلغ التّأمين بالطّريقة ذاتها. وقد يكون العقد إلكترونياً بحتاً عبر استعمال الوسائل الإلكترونيّة في مراحل انعقاده وتنفيذه كلّها، فيتمّ تقديم طلب التّأمين عبر التواصل مع الشّركة على البريد الإلكتروني الرّسميّ عبر

[48] سيد، (2015)، ص66.

موقعها الإلكترونيّ، وتتمّ عمليّة التّفاوض عبر الوسائل ذاتها، وترسل الأسئلة الأمنيّة من أجل التعرّف على طبيعة المال محلّ التّأمين والخطر المحيط به واحتماليته وغيرها من أسئلةٍ يحتاج المؤمّن لمعرفتها من أجل تحديد الأقساط، وبعد ذلك تتمّ موافقة المؤمّن على التّأمين وكتابة وثيقة التّأمين والقيام بالتزامات الأطراف إلكترونياً دون الحاجة لحضورٍ ماديٍّ للأطراف.

والسّائد حالياً هو استخدام الوسائل الإلكترونية والتقليدية معاً في إبرام العقد دون اقتصار على أيٍّ منهما دون الأخرى، فيرسل المؤمَّن له طلباً للتأمين إلى شركة التّأمين عبر البريد الإلكتروني، وبالتالي تتولّى شركة التّأمين بدورها زيارة موقع الشركة طالبة التّأمين من أجل الاطلاع على الأجهزة المستخدمة في العمل، والتأكّد من صدق بيانات المؤمَّن له التي أدلى بها، ثم تُبرم وثيقة التّأمين التي قد تُرسل ورقيّاً أو عبر الإنترنت ليبدأ بعدها عقد التّأمين بالسّريان وترتيب آثاره، إذ يتمّ إعلام شركة التأمين بالبيانات الضرورية عبر البريد الإلكتروني، أو حتى عبر مواقع التواصل الاجتماعي الرسمية للشركة، أو عبر الهاتف، وتُدفع الأقساط المترتبة على المؤمَّن له باستخدام الوسائل الإلكترونية كالدفع الإلكتروني أو باستخدام الدفع التقليدي للأموال، في حين تقوم شركة التّأمين بواجباتها كمراقبة أنظمة المؤمَّن له والاستجابة السّريعة لحوادث الخرق الحاصلة ودفعها مبالغ التّأمين المترتبة عليها حسب الطّريقة المتّفق عليها.

ثالثاً: مشكلات سوق التّأمين ضد مخاطر الإنترنت:

ما يزال التّأمين ضدّ مخاطر الإنترنت يتعثّر في طريقه نحو الوصول باتجاه الفهم الكامل والدقيق للمشكلات المحيطة به والحلول المقترحة، ومن المشكلات التي تعترضه:

1-قلّة المعلومات المتعلّقة بالأخطار المغطّاة:

يعتمد التّأمين على المعلومات الدّقيقة من أجل قياس الخطر ومدى إمكانية حدوثه والآثار التي يخلّفها وراءه، ولمّا كان التّأمين ضد مخاطر الإنترنت يتعامل مع الأخطار عبر الشبكة فإنّ ذلك يُصعِّب المهمّة أكثر على شركات التّأمين؛ نظراً لقلّة المعلومات الإحصائيّة وعدم دقّتها حول حجم الخطر المحيط بالمؤمَّن له ما يؤدّي إلى ظهور مشكلتين هما الاختيار السّلبيّ والخطأ المتعمّد (سيتمّ تفصيلهما لاحقاً)، كما أنّ عدم دقّة

المعلومات الإحصائيّة يؤثّر على تحديد ما الخطر المؤمّن منه بشكلٍ دقيقٍ؛ أي تحديد التغطية التّأمينية، وذلك بسبب التطور السريع في صور المخاطر، ممّا يثير غموضاً وسوء فَهْمٍ في تحديد التّغطية التّأمينيّة مع ظهور مخاطرَ جديدةٍ قد لا تكون مغطّاةً بوثيقة التّأمين، إذ إنّ التغطيات لم تعد تقتصر على إعادة بناء الأنظمة المعلوماتية المخرّبة، بل تعدّتها إلى دفع الغرامات والعقوبات المفروضة نتيجةً لانتهاك قوانين الخصوصيّة المعلوماتية نتيجة خرق البيانات[49]. ويُعزى سبب نقص المعلومات إلى أنّ كثيراً من الشّركات لا تبلّغ عن حصول خرقٍ لأنظمتها خوفاً من تضرّر سمعتها التّجاريّة وفقدان زبائنها، بالإضافة إلى أنَّ كثيراً من الحوادث لا تُكتشف في الوقت نفسه وقد تستغرق أياماً وأحياناً أشهراً حتى يُكشَف عنها، فلا يمكن معرفة مدى تكرار هذه الحوادث أو نفقاتها.

2-نقص شركات التّأمين:

إنَّ عدد الشركات المنخرطة في تقديم وثائق التّأمين ضد مخاطر الإنترنت ما يزال قليلاً، نظراً لقلّة المعلومات حول الدّعاوى المرتبطة بالأمن الإلكترونيّ، ونقص المعلومات المتعلقة بالنفقات المرتبطة بالأخطار الإلكترونية، ممّا يجعل شركات التّأمين حذرةً في تقديم وثائق تأمين ضد مخاطر الإنترنت[50].

3-نقص معيدي التّأمين[51]:

لا يمكن لشركات التّأمين أن تتطوّر دون مساعدةٍ من شركات إعادة التّأمين[52]، وما يزال سوق إعادة التّأمين ضد مخاطر الإنترنت ضعيفاً مقارنةً بأسواق إعادة التّأمين التّقليديّة؛ نظراً لما ذكر سابقاً من قلة المعلومات حول حجم الأخطار ونفقاتها ونطاق التغطيات وما يتبعه ذلك من نقص شركات التّأمين.

---

[49] Incentives and barriers of the cyber insurance market in Europe, (2012), p19-20.

[50] Ibid, p19.

[51] يعرف معيد التّأمين بأنه شركة تأمين ثانوية تتولى تغطية الأخطار التي تتعرض لها شركات التّأمين الأصلية، عبر عقد يبرم بينهما (بين شركة التّأمين الأصلية الشركة المتنازلة وشركة التّأمين الثانوية معيد التّأمين)، يتم بموجبه نقل بعض أو كل الأخطار التي تتعرض لها الشركة الأصلية إلى المعيد، مقابل دفع الطرف الأول مبلغ يسمى قسط إعادة التّأمين، ويلتزم مقابلها المعيدون بتعويض الشركة المتنازلة عن الأضرار التي تلحقها جراء عقد التّأمين الأول بينها وبين المؤمَّن له، مشارٌ إليه على الموقع الإلكتروني:
https://www.saudire.net/index.php/ar/reinsurance-market-ar/reinsurance-industry-2
تاريخ الزيارة: 5\5\2021، الساعة 8:30 p.m.

[52] Ibraheem K. (2008). risk costs and benefits of cyber insurance in Nigerian banks, p12.

4-الخوف من الإعصار الإلكترونيّ:

يُعرَّف الإعصار الإلكترونيّ على أنّه: "كارثةٌ كبيرةٌ تُنشئ عدداً كبيراً من الدعاوى"، وينشأ الإعصار نتيجة كون أنظمة الحواسيب مترابطةً بشكلٍ يجعل احتمال إصابة عددٍ كبيرٍ من الأنظمة بخطرٍ معيّنٍ في الوقت ذاته أمراً محتملاً، ما يدفع شركات التّأمين إلى رفع أقساط التّأمين في محاولةٍ منها لتوقُّع أسوأ الاحتمالات والتصدّي لها، كما تتردد بعض شركات التّأمين نتيجة لهذا الأمر من فكرة دخول عالم التّأمين ضد مخاطر الإنترنت خوفاً من إفلاسها في حال انهالت الدعاوى عليها قبل اكتمال تشكيل محافظ التّأمين اللازمة[53].

5-كان المؤمّنون حذرينَ في دخولهم سوق التّأمين ضد مخاطر الإنترنت؛ لأنّ الخطر الإلكتروني صعب التّسعير، ولم يكن من السّهل عليهم تكوين محافظَ لإدارة الأخطار، وينتج عن ذلك أنّ المؤمَّن لهم كانوا يتحمّلون الجزء الأكبر من المخاطر التي يتعرّضون لها، فبينما يتحمّل المؤمّن حوالي 10% فقط من الخسائر يضطرّ المؤمَّن لهم إلى تغطية باقي النفقات من أموالهم الخاصّة، بل حتى في حالات الإعصار الإلكترونيّ لم تزد نسبة تحمّل المؤمّنين للخسائر عن 20%[54]، فبينما تحصل شركات التّأمين على أقساطٍ سنويّةٍ بملايين الدولارات، فإنّها تدفع تعويضاتٍ للمؤمّن لهم بما يعادل مئات آلاف الدولارات فقط.

6-تغطّي **بعض** وثائق التّأمين ضدّ مخاطر الإنترنت انقطاع الأعمال الحاصل فقط في أثناء الهجوم الفعليّ، أمّا عن المرحلة اللّاحقة للهجوم (أي عند زوال الخطر ولكن بقاء الشبكة غير قابلة للوصول إليها) فإنّ ذلك غير مغطّى في بعض الحالات، كما لو أنّ قرصاناً إلكترونيّاً قد حجز بيانات شركة لمدّة أسبوع ثمّ دُفعت الفدية، لكنّ الشركة والمستهلكين كانوا ما يزالون غير قادرين على الوصول إلى بياناتها، فإنّ التّأمين سيغطّي فترة الأسبوع فقط دون غيرها، هنا تقع مشكلة مفادها أنّ النفقات في مرحلة استعادة الوصول للبيانات، وخسارة

---

53 Clinton, (n.d), p2-3.

54 Coburn, A., Leverett, E., & Woo, G. (2018). Solving Cyber Risk Protecting Your Company and Society, New York: United States Of America, Wiley.p274.

السمعة، وخسارة المستهلكين الحاصلة ضمن هذه الفترة غير المغطاة تكون مكلفة للشركات، ونتيجة سوء الفهم تظن الشركات أنها ستكون مغطّاةً بالتّأمين[55].

7-عدم وجود دعمٍ حكوميٍّ لقطاع التّأمين ضد مخاطر الإنترنت خاصةً في ظل كل ما يعانيه السوق من تعثرات في طريقه وهو في أمسّ الحاجة لتدخلٍ حكوميّ مساعد له.

8-عدم إمكان التنبؤ بالحوادث قبل وقوعها، ذلك أنّه وبشكلٍ نموذجيٍّ فإن المؤمّنين يستخدمون أحداث الماضي كبيانات للتنبؤ بالمستقبل، **أمّا في نطاق التّأمين ضد مخاطر الإنترنت** فذلك غير ممكن؛ لأنّه وكما يقول أحد كبار موظفي مجموعة التّأمين زيوريخ فلا يوجد في مخاطر الإنترنت حادثان متشابهان[56].

9-صعوبة تسعير وثائق التّأمين: إنّ كلّ ما سبق وقِيل من صعوباتٍ يواجهها سوق التّأمين تتمثل نتيجته في صعوبة تسعير الوثائق، إذ إنّه من أجل الوصول إلى تسعيرٍ دقيقٍ عادلٍ فلا بدّ من الحصول على المعلومات بشكلٍ كاملٍ حول الخطر المؤمّن ضدّه كاحتماليّة حصوله، والخسائر المالية التي يخلّفها، وعدد الأشخاص المعرّضين لهذا الخطر في آنٍ واحدٍ، بالإضافة إلى وجود سوق إعادة تأمين لمساعدة شركات التّأمين الأوليّة في تغطيتها للمؤمّن لهم. ولمّا كان الوصول إلى التسعير الدقيق صعباً في الوقت الحالي؛ نظراً لكون السوق التّأميني ما يزال جديداً في هذا النطاق، فتلجأ شركات التّأمين إلى نموذج الأسئلة التي تقدمها لطالبي التّأمين من أجل الإجابة عنها للتعرف إلى طبيعة الخطر المؤمّن ضدّه، وتتعدّد هذه الأسئلة في محاولةٍ لتغطيةٍ أكبر قدر ممكن من المعلومات كالنظام الأمني للشركة، فيما إذا حصلت خروقات سابقة، وطبيعة البيانات المخزنة، وحجمها ومدى أهميتها، وغير ذلك من الأسئلة.

---

[55] Lindsey, N. (2019). Businesses Are Finding Out That Cyber Insurance Coverage Might Not Be What They Thought, available at: https://www.cpomagazine.com/cyber-security/businesses-are-finding-out-that-cyber-insurance-coverage-might-not-be-what-they-thought

تاريخ الزيارة: 24\4\2020، الساعة 10.30 p.m.

[56] Wolff, J. (2018). Cyber insurance Tackles the Wildly Unpredictable World of Hacks, available at: **https://www.wired.com/story/cyberinsurance-tackles-the-wildly-unpredictable-world-of-hacks/**

تاريخ الزيارة: 24\4\2020، الساعة 11:30 p.m.

وعليه فإنّ عقد التّأمين ضد مخاطر الإنترنت هو عقدٌ مبرم بين مؤمّن له وشركة تأمين من أجل تغطية مخاطر بيئة العمل الإلكترونية التي باتت الشركات والأفراد يعانون منها نتيجةً لكثرة هذه المخاطر وتعددها، وهو ما يدفع هؤلاء إلى التمسك بحبل التّأمين من أجل المحافظة على أعمالهم ضمن طوفان الهجمات السيبرانية التي تحيط بهم، ويتميز هذا العقد بسماتٍ عدّةٍ جعلته متميّزاً عن غيره، وتعترضه مشكلات عدّة في ضوء المخاطر المحيطة به، والتي ستبدو أكثر وضوحاً عند دراسة أركان هذا العقد، وطبيعته القانونية.

المطلب الثّاني

أركان عقد التّأمين ضد مخاطر الإنترنت وطبيعته القانونية

عندما يخاف الفرد أو الشّركة من مخاطر الإنترنت التي قد تواجه أيّاً منهما في أثناء القيام بعمله عبر الإنترنت يلجأ إلى شركات تأمينٍ لإبرام عقود تأمينٍ ضدّ هذه المخاطر، والتي تقوم على أركانٍ عامّةٍ وخاصّةٍ ينبغي توفّرها حتى تنعقد صحيحةً منتجةً لآثارها القانونية. ولمّا كان عقد التّأمين ضد مخاطر الإنترنت من العقود الحديثة التي أفرزتها الثورة التقنية في قطاع المعلومات كان لا بدَّ من دراسة الطّبيعة القانونيّة لهذا العقد لتحديد النّوع الّذي ينتمي إليه وما ينطوي عليه ذلك من تحديدٍ للقواعد القانونية المنطبقة عليه. وعليه سيقسم هذا المطلب إلى فرعٍ أوّل، محوره الأركان التي تحكم العقد، وفرعٍ ثانٍ حول الطبيعة القانونية لعقد التّأمين ضد مخاطر الإنترنت.

الفرع الأوّل

الأركان التي تحكم عقد التّأمين ضد مخاطر الإنترنت

يتكون عقد التّأمين ضد مخاطر الإنترنت كغيره من العقود من أركانٍ عامّةٍ تساهم في إنشائه وإدخاله حيّز التنفيذ كالرّضا، والمحلّ، والسبب، وأركان خاصّة لهذا العقد تميّزه عن غيره من العقود.

أولاً: الأركان العامّة لعقد التّأمين ضدّ مخاطر الإنترنت:

يقوم عقد التّأمين ضد مخاطر الإنترنت كغيره من العقود على أركانٍ عامةٍ نبيّنها وفقاً للآتي:

1-الرّضا: يُعدُّ عقد التّأمين ضدّ مخاطر الإنترنت من العقود الرّضائيّة والتي تنعقد بمجرد تطابق الإيجاب مع القبول دون الحاجة إلى أيّ إجراءٍ آخر، وعادةً يصدر الإيجاب من طالب التّأمين ويأتي القبول من جانب شركة التّأمين مطابقاً لما ورد في العرض، فإن كان مغايراً لما ورد كان إيجاباً جديداً بحاجة لقبول من طالب التّأمين[57]. ويجب أن يكون الرّضا صحيحاً لا يشوبه أيّ عيبٍ من عيوب الرضا كالإكراه والتدليس والغلط، وتسري في حكمه القواعد العامة في العقود، وفيما يخصّ الكتابة التي تتمّ في وثيقة التّأمين فهي ليست إلّا وسيلة إثبات. وقد يصدر الرضا بوسيلةٍ تقليديّةٍ أو إلكترونيّةٍ، فقد يأتي العميل بصورةٍ تقليديّةٍ إلى الشركة ويملأ طلب التّأمين، أو يدخل إلى الموقع الإلكتروني للشركة ويملأ الطلب عبر الإنترنت، ويرسله إلى البريد الإلكترونيّ، ومن ثمّ يأتي ردّ المؤمّن إمّا بالإبلاغ شخصياً للمؤمَّن له بالموافقة، أو بالردّ عبر البريد الإلكترونيّ، وهنا نكون أمام كتابةٍ إلكترونيّةٍ يُلزم منحها القوة القانونية من أجل صحّة إبرام العقد، لذلك يثير استخدام الوسائل الإلكترونيّة مشكلات عدّة حول تحديد مفهوم الإيجاب والقبول الإلكتروني وتحديد زمان ومكان انعقاد العقد، بالإضافة إلى الحجيّة القانونيّة للمحرّرات الإلكترونيّة، وهو ما عالجه المشرّع السّوريّ في قانون التّوقيع الإلكترونيّ وخدمات الشّبكة، وقانون المعاملات الإلكترونيّة حيث أعطى حجيةً للكتابة الإلكترونية ضمن شروط محددة بوجود توقيعٍ إلكترونيٍّ مصدّقٍ، كما جعل الوسائل الإلكترونية وسيلةً مقبولةً قانوناً لإبداء الإيجاب والقبول[58].

2-أطراف العقد: يدور عقد التّأمين ضد مخاطر الإنترنت حول ثلاثة مصطلحات في نطاق الأطراف: شركة التّأمين، والمؤمَّن له، والمستفيد، فشركة التّأمين هي شركةٌ تقليديّةٌ أو إلكترونيّةٌ (تعمل عبر الفضاء الإلكتروني في تقديم خدماتها) تتولّى تحمّل تبعة المخاطر التي قد تحدث لشخصٍ آخرَ، وتتولّى تعويضه عند تحقّق تلك المخاطر مقابل أن تحصل على أقساطٍ محدّدةٍ، وتتّخذ شكل شركةٍ مساهمةٍ في الغالب، فقد حصرت

---

[57] عبد ربه، (2006)، ص66.

[58] لمزيد من التفصيل يمكن مراجعة المواد (2-3) من قانون التوقيع الإلكتروني وخدمات الشبكة السوري رقم 4 لعام 2009, والفصل الثاني حتى الفصل الرابع (المواد من المادة 2 حتى المادة 14) من قانون المعاملات الإلكترونية السوري رقم 3 لعام 2014.

معظم التّشريعات أعمال التّأمين بالشركات المساهمة دون غيرها؛ نظراً لخطورتها وحاجتها لرأسمالٍ ضخمٍ، وعلى سبيل المثال يمنع قانون الشركات السوري الشركات محدودة المسؤولية من تولّي أعمال التّأمين بصراحة نصّ المادة 56 الفقرة 8. أمّا المؤمَّن له غالباً ما تكون الشركات هي التي تتولى تخزين البيانات عبر الإنترنت (إلكترونيّاً) ومتابعة أعمالها إلكترونيّاً لحماية نفسها ضد المخاطر التي تهددها عبر الفضاء الإلكترونيّ، ولا شيء يمنع من أن يكون المؤمَّن له شخصاً طبيعيّاً يسعى لحماية نفسه من هذه المخاطر، كما لو كان عمله يتطلب دخولاً إلى الإنترنت ويخشى على جهازه الحاسبي من القرصنة أو السرقة أو إتلاف بياناته في معرض ابتزازٍ إلكترونيٍ، وعلى سبيل المثال تقدم شركة GAI تغطيةً تأمينيّةً للشّركات كلّها التي تستخدم الإنترنت، والتي تحتلُّ حيّزاً على المواقع الإلكترونيّة، أو أحد مواقع التّواصل الاجتماعيّ، بالإضافة إلى المؤسسات التي تقبل الدفع الإلكتروني، والتي تخزن البيانات الشخصية والتي تقدم أجهزةً ذكيةً لموظفيها[59]. في حين يشغل المستفيد الطرف الثالث في عقد التّأمين، وهو الشخص الذي يستحق مبلغ التعويض عند تحقق الخطر المؤمّن منه في العقد الذي يبرمه المؤمَّن له مع شركة التّأمين لمصلحة المستفيد، كما لو أخطأ موظّفٌ في شركةٍ للرّعاية الصّحيّة التي تخزّن آلاف العناوين، والأسماء، والبيانات لعملاءَ لديه ممّا أدّى إلى كشف خصوصية هذه البيانات، فتقوم مسؤوليّة هذه الشركة عن خطأ موظفها ويستوجب ذلك تعويض العملاء الذين كشفت خصوصيّتهم، فإذا ما كان لدى هذه الشركة تأمين ضد المخاطر الإلكترونيّة فتكون شركة التّأمين ملزمةً بأن تعوّض هؤلاء العملاء الذين يشغلون محل المستفيد في هذا العقد. وفيما يتعلق بالأهلية اللازمة لإبرام العقد فما دمنا أمام شركات تبرم هذه العقود (شركات التّأمين بالإضافة إلى المؤمَّن له إذا كان شركة أو مؤسسة) فتكون أهليتهم مفترضة لإبرام العقود طالما اكتسبوا شخصيّة اعتباريّة صحيحة، وما دام التّأمين يقع في إطار غرضهم ولحماية أنفسهم ضد مخاطر الإنترنت، أمَّا لو كان المؤمَّن له شخصاً طبيعيّاً فتكفي أهلية الإدارة؛ وذلك لأنّ التّأمين يقع ضمن أعمال الإدارة، فلا يشترط فيه كمال الأهلية ببلوغ سن الرشد، بل يكفي فيه أن يكون صبياً مأذوناً له بإدارة أمواله، وعندها يكون

[59] https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage

تاريخ الزيارة: 4\5\2021، الساعة 11 p.m.

العقد صحيحاً، أمّا لو لم يكن مأذوناً له بالإدارة لكان العقد قابلاً للإبطال لمصلحته ما لم يجزه الولي أو الصبي بعد بلوغه سن الرشد أو المحكمة بحسب الأحوال[60]، وعلى هذا نص القانون المدني السوري من أنّ أهلية الإدارة تكفي لإبرام عقد التّأمين إذا ما كان الصبي البالغ 15 عاماً مأذوناً له[61]، كما يجوز للصبي البالغ 13 عاماً أن يتولى إدارة أمواله التي كسبها من ماله الخاص وحينا يعد كامل الأهلية فيما يخص هذه التصرفات[62].

3-محل العقد: ويختلف العديد من الفقهاء في تحديد محل عقد التّأمين ضد مخاطر الإنترنت بين القول إنّه الالتزامات التي ينشئها العقد من حيث التعويض والقسط[63]، ويتّجه آخرون إلى أنّ المحل في التّأمين هو الخطر المؤمن ضده والذي يخشى منه[64]، وقد يكون المحل هو الشيء الذي ينصب عليه التّأمين، كالسيارة المؤمَّن عليها ضد الحريق في حال التّأمين ضد الحريق[65].

ولكن إذا كانت الالتزامات هي آثار العقد، فهل يمكن القول بأنّها المحل أيضاً، وهو ما يخلط بين محل العقد ومحل الالتزام؟ كما أنّ الخطر وهو أحد أركان العقد الخاصة لا يمكن أن يجمع بين كونه محلّ العقد وركناً خاصاً فيه. وتتباين التشريعات أيضاً في تحديد محل التّأمين، فمنها ما ذهب إلى اعتبار المصلحة محلّ التّأمين كحال المشرّع السّوريّ الّذي ذهب إلى أنّه يكون محلاً للتّأمين كلّ مصلحة اقتصادية مشروعة تعود على الشخص بمجرد عدم تحقق الخطر[66]، ويتوافق ذلك مع المشرع المصري[67] والفرنسي[68] أيضاً، في حين ذهب التشريع العراقي إلى جواز أن يكون محلاً للتأمين كل شيء مشروع يعود على الشخص بالنفع من عدم وقوع

---

[60] حسين، (1995)، ص 68.

[61] وفي ذلك تنص **المادة 112 (**1. إذا كان الصبي مميزاً كانت تصرفاته المالية صحيحة متى كانت نافعة نفعاً محضاً، وباطلة متى كانت ضارة ضرراً محضاً.2 . أما التصرفات المالية الدائرة بين النفع والضرر، فتكون قابلة للإبطال لمصلحة القاصر. ويزول حق التمسك بالإبطال إذا أجاز القاصر التصرف بعد بلوغه سن الرشد، أو إذا صدرت الإجازة من وليه، أو من المحكمة، بحسب الأحوال وفقاً للقانون، وتنص **المادة 113 (**إذا بلغ الصبي المميز الخامسة عشرة من عمره، وأذن له في تسلم أمواله لإدارتها، أو تسلمها بحكم القانون، كانت أعمال الإدارة الصادرة منه صحيحة في الحدود التي رسمها القانون.) من القانون المدني السوري رقم 84 لعام 1949.

[62] المادة (169) من قانون الأحوال الشخصية السوري رقم 59 لعام 1953.

[63] فلاح، (2008)، ص16.

[64] حسين، (1995)، ص94.

[65] الخفاجي، (2014)، ص15.

[66] المادة (715) من القانون المدني السوري رقم 84 لعام 1949.

[67] المادة (794) من القانون المدني المصري رقم 131 لعام 1948.

[68] المادة (33) من قانون التّأمين الفرنسي لعام 1930.

خطر معين[69]، ويتفق الباحث مع الرأي الأخير، ويمكن تبرير ذلك أنّ المؤمَّن له يبرم التّأمين ليحمي أشياء معيّنةً بذاتها من أخطار محدّدة، فالشّيء المؤمّن عليه هو وعاء التّأمين وليس الخطر أو المصلحة، **ولذلك فالأكثر منطقيّةً اعتبار الشّيء المؤمّن عليه محلّ التّأمين**، وفي التّأمين ضد مخاطر الإنترنت يعدّ الشّيء المؤمّن عليه البيانات التي يحتفظ بها المؤمَّن له، والبرمجيات والأنظمة التي يستخدمها، والحواسيب والمواقع الإلكترونية التي تستضيف متاجره الإلكترونية، ولا بدّ في هذا المجال من تسليط الضوء على ما يُراد بالبيانات الإلكترونية والأنظمة وغيرها، فيمكن تعريف البيانات على أنها: "معطيات أولية خام ترتبط بقطاع أو نشاط معين[70]" وتتخذ هذه البيانات شكلاً معنوياً غير ملموس، وفي السياق القانوني تناول المشرّع السوري في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية تعاريف للمصطلحات السابقة، فعرَّف المعلومات بأنّها: "العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابلاً للإدراك مرتبطاً بسياق محدد"، ويراد بالبرمجيات الحاسبية سلسلة متّسقة من التعليمات المرمّزة التي يمكن تنفيذها على جهاز حاسوبي بغية تمكينه من أداء الوظائف والتطبيقات المطلوبة، أمّا المنظومة المعلوماتية فهي: "مجموعةٌ متّسقةٌ من الأجهزة والبرمجيات الحاسبية والمعدات الملحقة بها"، في حين يُعرَّف الحاسب بأنّه: "جهازٌ يستخدم التِّقانات الإلكترونية أو الكهرطيسية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها"[71]. وتتصف التعريفات السابقة بأنها واسعةٌ وتضمّ في نطاقها عدداً لا حصر له من المعلومات.

4-**سبب العقد:** وسبب العقد هو الباعث على التعاقد، وهو الدافع، فبينما يهدف المؤمَّن له إلى تحقيق الأمان وحماية شركته وأمواله من المخاطر التي تحيط بأعماله عبر الإنترنت، تهدف شركات التّأمين إلى تحقيق الربح من الأقساط المحصلة من المؤمَّن لهم وتقديم خدماتها التأمينيّة.

---

[69] المادة (984) من القانون المدني العراقي رقم 40 لعام 1951.

[70] المومني، نهلا عبد القادر. (2010). الجرائم المعلوماتية، ط:2، عمان: الأردن، دار الثقافة للنشر والتوزيع، ص102.

[71] المادة (1) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم 17 لعام 2012.

ثانياً: الأركان الخاصة لعقد التّأمين ضد مخاطر الإنترنت:

ينفرد عقد التّأمين ببعض الأركان التي تميّزه عن غيره من العقود وتعطيه الصبغة الفريدة، وهذه الأركان هي: القسط، مبلغ التّأمين، مدّة التّأمين، والخطر المؤمّن ضدّه.

1-القسط: ويعرَّف على أنّه: "مقابلٌ ماليٌّ يلتزم المؤمَّن له بدفعه للمؤمّن مقابل أن يتحمّل الأخير تعويضه عن الضّرر عند تحقّق الخطر[72]"، وعلى الرّغم من اشتراط القسط بين عقود التّأمين كلّها إلّا أنّ له خصوصيّة في هذا العقد على وجه التّحديد، وعليه يتمّ حساب الأقساط في التّأمين ضدّ مخاطر الإنترنت عبر عمليّاتٍ إحصائيّةٍ للخطر المؤمّن ضدّه كاحتماليّة حصول الخطر وشدّته وحجم الآثار التي يخلّفها والخسارة اللاحقة بالمؤمَّن له. والجدير بالذّكر أنّ تاريخ شركة التّأمين في تغطية الخطر الإلكترونيّ يؤدّي دوراً مهماً في تحديد الأقساط؛ نظراً للخبرة القليلة التي قد تملكها في هذا الإطار، والخوف من الخسائر التي قد تلحقها في حال عدم التحديد بشكلٍ دقيقٍ، وعند إتمام هذه العمليّات تتحدّد الأقساط. وتختلف الأقساط من سنةٍ لأخرى تبعاً لتغير الظروف المحيطة بالأخطار المؤمّنة، وتُعدّ الأقساط هي الوسيلة التي يعتمدها المؤمّن في تكوين المحفظة التي تلزمه لمواجهة التزاماته في التّعويض عن الخسائر؛ ولذلك ينبغي تشغيل هذه الأقساط بالصورة الأمثل[73]، وتُعدُّ عملية حساب القسط في ظلّ التّأمين ضدّ مخاطر الإنترنت عمليّةً شاقّةً حتى تاريخ اليوم؛ بسبب قلّة المعلومات حول المخاطر الإلكترونية، ونقص شركات التّأمين وفق ما ذكر سابقاً في مشكلات التّأمين.

2-مبلغ التّأمين: ويعرَّف مبلغ التّأمين على أنّه: "العوض المالي الذي يلتزم المؤمّن بدفعه للمؤمّن له عند تحقق الخطر المؤمّن ضدّه والمساوي لمقدار الضرر الحاصل[74]"، ويعتبر مبلغ التّأمين هو الحد الأعلى الذي يمكن أن تدفعه شركات التّأمين، ولا شيء يمنع من أن يكون مبلغ التعويض المدفوع أقل من مبلغ التّأمين ما دام

---

[72] آل الشيخ، محمد بن حسن بن عبد العزيز. (2011). عقد التأمين التجاري للتعويض عن الضرر حقيقته وحكمه، عدد:8، بحث منشور في مجلة الجمعية الفقهية السعودية، ص 278، وأيضاً: عبد ربه، (2006)، ص78.

[73] خالد، خطيب. (2011). الأسس النظرية والتنظيمية للتأمين التقليدي في الجزائر ندوة حول مؤسسات التأمين التكافلي والتأمين التقليدي بين الأسس النظرية والتجربة التطبيقية، جامعة وهران، الجزائر، ص 25- 26.

[74] آل الشيخ، (2011)، ص 278.

مساوياً للضّرر. ويتّبع في حساب المبلغ عمليّاتٍ إحصائيّةً مشابهةً لعمليّات حساب القسط فيؤخذ بالحسبان القسط المحدّد، وهامش الرّبح، والفوائد، وإمكانيّة وجود معيد للتّأمين، والذي قد يرفع سقف مبلغ التّأمين إذ يُشعِر ذلك شركة التّأمين بأمانٍ أكبر ممّا لو كان ستدفع المبلغ لوحدها. ويتمّ الاتفاق على تقديم مبلغ التّأمين إمّا تقليديّاً بالدّفع التّقليديّ للأموال (التسليم التقليدي)، أو إلكترونيّاً عبر التّحويل المصرفيّ الإلكترونيّ، أو الشيكات الإلكترونية، أو غيرها ممّا يتّفق عليه الطّرفان.

3-مدّة التّأمين: وكما قيل سابقاً من أنّ عقد التّأمين ضدّ مخاطر التّأمين عقدٌ زمنيٌّ، فهو يعقد ليغطّي مدّةً معيّنةً يتمّ الاتّفاق عليها بين شركة التّأمين والمؤمَّن له، وغالباً ما يبدأ السّريان بتاريخ دفع أوّل قسطٍ من أقساط التّأمين، ويبقى المؤمَّن له مغطّى بالتّأمين طوال مدة السريان، فإذا تحقق الخطر خلال المدة استحقّ التعويض. وتظهر مشكلة تحديد حصول الخطر في نطاق التّأمين ضد مخاطر الإنترنت؛ لأنَّ الخطر قد يحصل ولا يُكتشف إلّا بعد مدّة قد تكون أسبوعاً أو أكثر، وقد تمتدّ إلى شهرٍ، إذ يذهب بعض الخبراء إلى القول إنّ الهجوم الإلكترونيّ قد يستغرق مدّة 120يوماً حتى يكتشف[75]؟ ففي هذه الحالة ما دمنا داخل مدّة السريان فلا خوف على المؤمَّن له، ولكن تكمن المشكلة إذا انتهى العقد قبل الانتباه إلى الخطر، ففي هذه الحالة ما دام الخطر قد حدث خلال السريان فتلتزم شركة التّأمين بتعويض المؤمَّن له عن الخسارة ولكن يجب على المؤمَّن له أن يثبت حصول الخطر خلال مدّة السّريان وهو أمرٌ صعبٌ ولكنَّه يظلّ ممكناً.

4-الخطر المؤمّن ضدّه: ويعرَّف الخطر بصفةٍ عامّةٍ بأنّه: "الحادث الاحتمالي المؤمّن منه والمحدّد في العقد كالسرقة والحريق[76]" ولا يختلف مفهوم الخطر الإلكتروني عن الأخطار التقليدية التي يؤمّن منها عادةً من حيث صفة الاحتمالية، لكن شكل أخطار الإنترنت هو المختلف، فهي لا تأخذ طابعاً مادياً بل إنّها غير ملموسة تتمّ عبر الشبكة العنكبوتيّة دون ترك أيّ أثرٍ ماديٍّ عليها ولذلك تصعب ملاحظة حصولها. ويمكن تعريف الخطر الإلكتروني بأنه: "أي حادث ناشئ عن استخدام البيانات الإلكترونية ونقلها، بما في ذلك الوسائل التقنية مثل

---

[75] Camillo (2017), p3.

[76] آل الشيخ، (2011)، ص278.

الإنترنت وشبكات الاتصالات، الأضرار المادية التي يمكن أن تحدث بسبب استخدام البيانات أو الأنظمة الإلكترونية أو الاعتماد عليها أو الهجوم الإلكتروني، الاحتيال نتيجة سوء استخدام البيانات، وأي مسؤولية ناشئة عن استخدام البيانات وتخزينها ونقلها، وتوافر وسلامة وسرية المعلومات الإلكترونية سواء كانت تتعلق بالأفراد والشركات والحكومات[77]".

وبيَّن التعريف السابق السبب الرئيس للمخاطر الإلكترونيّة ألا وهو استخدام البيانات الإلكترونيّة، كما أنّه تعرّض لبعض أشكال هذه المخاطر. ويمكن أن تأخذ هذه الخسارة العديد من الأشكال من مخترقٍ يستنزف حساباً مصرفياً إلى موظّف يعرض بياناتٍ خاصّة لزوار الموقع عن طريق الخطأ. كما أنّ المخاطر الإلكترونية التي يعالجها التّأمين ضد مخاطر الإنترنت تقتصر على البيئة الإلكترونية ولا تتخذ شكلاً ملموساً ويتم الخطر كلّه عبر الشبكة والأنظمة الإلكترونية فحسب، وعلاوةً على ذلك ينتج آثاراً إلكترونيّةً، وبكلّ الأحوال ومهما اختلفت الأخطار فإنّ هناك شروطاً يجب أن تتّصف بها لكي تقبل التّأمين وهي: 1-أن يكون الخطر محتمل الوقوع فلا نكون أمام عقد تأمين إذا ما كان الخطر مؤكّد الوقوع فتنتفي عنه صفة الاحتمالية ولا يجوز أن يكون الخطر مستحيلاً أيضاً فينتفي الخطر نفسه وينعدم العقد. ومفهوم الاحتمالية في هذا العقد يعني عدم التأكد من إمكانية حصوله فلا ندري على وجه اليقين هل يحصل أم لا، فمفهوم الاحتماليّة في الخطر بشكل عام يُعدُّ أساسياً في عقد التّأمين ويترتّب على انعدامه الاختلال في شروط الخطر وبالتّالي زوال الخطر وبطلان العقد.

2-ألّا يكون الخطر إرادياً: يجب ألّا يكون تحقّق الخطر بعملٍ إراديٍّ من جانب المؤمَّن له أو المؤمّن _وإن كان غير متوقّع تحقّق الخطر من جانب المؤمّن؛ لأنّه سيسعى في الأحوال كلّها إلى عدم تحقّق الخطر وعندها يصبح عدم التحقّق مؤكّداً _وهذا لا يجوز_ وإذا ما كان الخطر متوقّفاً على محض إرادة المؤمَّن له انتفت الاحتمالية فيصبح الخطر مؤكداً، وبالتّالي يبطل العقد. ويشترط إذن أن يكون الخطر عرضياً؛ أي يحصل من تلقاء نفسه دون تدخّلٍ إراديٍّ من جانب المستفيد، إذ إنّ التّأمين لا يغطّي الأخطار المتعمّدة ومبرّره انتفاء صفة

[77] https://www.thecroforum.org/2018/02/21/supporting-on-going-capture-and-sharing-of-digital-event-data/ تاريخ الزيارة: 8\5\2020، الساعة 9 p.m.

الاحتمالية والغرر التي تشكّل جوهر التّأمين[78] ولهذا تصدّى المشرّع لذلك وقضى بعدم التزام المؤمّن تجاه المؤمَّن له بحال تسبّب الأخير بتحقّق الخطر غشاً أو تعمّداً منه ولو اتّفق على غيره[79]، فالنّصّ المذكور من النظام العام وجاء بصفةٍ عامّةٍ مطلقةٍ في نطاق التّأمين التّقليديّ في القانون المدنيّ، **وهو يطبق على التّأمين ضد مخاطر الإنترنت**؛ لأنّ المطلق يجري على إطلاقه ولأنّ المبادئ العامّة في التّأمين التقليدي تنطبق على التّأمين ضد مخاطر الإنترنت.

3-أن يكون الخطر مشروعاً: حيث يشترط ألّا يكون الخطر المؤمّن ضدّه مخالفاً للنّظام والآداب العامّة، وهو يخضع لأحكام القانون المدنيّ الذي يوجب أن يكون العقد مشروعاً، ووفقاً للقواعد العامة في التّأمين لا يجوز التّأمين من مخاطر المطالبة بالغرامة الماليّة التي تحكم على الشّخص بدفعها، كما لا يجوز التّأمين أيضاً على الإتجار بالمخدرات على سبيل المثال[80]. وهذا وفقاً للقواعد العامة، وهو ينطبق على التّأمين ضد مخاطر الإنترنت؛ نظراً لكونه عقداً يخضع للقواعد العامّة ذاتها في القانون المدني، ولكن توجد شركات عدّة تقدم تغطيات ضدّ الغرامات الماليّة التي تُحكم بها الشّركات نتيجة لخرق خصوصيتها، أو نتيجة لإهمالها إعلام عملائها بحصول خرق، وهو ما يتنافى مع قوانين الخصوصيّة التي تحكم سريّة المعلومات والتي توجب الإعلام خلال مدّةٍ معيّنةٍ، وتعاقب الشّركات على إهمالها حماية بياناتها بصورةٍ صحيحةٍ، ولذلك تلجأ الكثير من الشّركات إلى شركات التّأمين لحماية نفسها ضدّ هذه الغرامات والعقوبات، **وهو أمرٌ لا يلحظ في التّأمين التقليدي وإن كان أمراً مشروعاً وسائداً في التّأمين ضد مخاطر الإنترنت.**

ويتوجّب بعد بيان الأركان العامّة والخاصة التي يقوم عليها عقد التّأمين ضد مخاطر الإنترنت البحث في الطبيعة القانونية لهذا العقد في الفرع الآتي.

---

[78] عبد ربه، (2006)، ص85- 86، وأيضاً، عبيد، (2016)، ص101.

[79] المادة (734) من القانون المدني السوري رقم 84 لعام 1949.

[80] عبيد، (2016)، ص105- 106.

الفرع الثّاني

الطَّبيعة القانونيَّة لعقدِ التّأمين ضدَّ مخاطر الإنترنت

يبدو من الأهميّة بمكان بعد التعرّف على أركان العقد إلقاء الضّوء على الطّبيعة القانونيّة لعقد التّأمين ضدّ مخاطر الإنترنت، إذ إنّ تحديد طبيعة عقدٍ ما يعني معرفة القواعد القانونيّة المنطبقة على هذا العقد. وستُدرس الطبيعة القانونية لعقد التّأمين ضد مخاطر الإنترنت وفقاً للآتي:

أولاً: عقد التّأمين ضدّ مخاطر الإنترنت عقد تأمينٍ تجاريٍّ يستهدف تحقيق الربح:

يعرّف التّأمين التّجاريّ بأنّه: "التّأمين ذو القسط المحدّد ويقوم على هدف تحقيق الربح وتقوم به عادةً شركات التّأمين المساهمة[81]، وفيه تتعهّد شركة التّأمين بأن تضمن الأخطار المحدّدة في عقد التّأمين مقابل التزام المؤمَّن له بدفع أقساطٍ محدّدةٍ ثابتة[82]". ويتميّز التّأمين التجاري بالآتي: 1- تعداد أطرافه من حيث وجود مؤمّن هو شركة تأمين مساهمة ومؤمَّن له شخص طبيعي أو اعتباري عام أو خاص على السواء.

2- ثبات القسط التّأمينيّ؛ إذ إنّ القسط الواجب الدّفع من قبل المؤمَّن له يبقى ثابتاً طوال مدّة العقد، ولا يمكن لأيٍّ من الطرفين إحداث أيّ تعديل عليه زيادة أو نقصان ما دامت العوامل المؤثّرة في الخطر لم تتغيّر[83]، كما أنّ الأقساط تحدّد بشكلٍ مسبقٍ في العقد دون انتظار حصول الخطر، بل حتى لو لم يتحقّق الخطر.

3- التحديد المسبق لمبلغ التّأمين الذي تدفعه شركات التّأمين، وتظهر أهمية هذا الأمر في أنّ الشركات غالباً ما تتبع في تحديد مبالغ التعويض بالنظر إلى رأس مالها وميزانيتها وحجمها المالي وعدد المؤمنين الذين لديهم الإمكانية نفسها للتعرّض للأخطار في وقت واحد، ذلك من أجل تفادي إفلاس الشركات بحال عدم تحديد مبالغ التّأمين، إذ قد تكون الخسائر كبيرةً وتفوق قدرة المؤمنين على تحملها[84].

---

[81] عبد ربه، (2006)، ص56.

[82] عبده، عيسى. (1978). التأمين بين الحل والتحريم، ط:1، (د.ن.)، ص27.

[83] عبيد، (2016)، ص24.

[84] حسين، (1995)، ص 25- 26.

4-الصفة التجارية لهذا النوع تبرز من خلال تغليب الربح على تحقيق الأمان، إذ إنّ الربح الصافي يبرز عبر المقاصة بين الأقساط المدفوعة من المؤمَّن لهم ومبالغ التغطية، وغالباً ما تكون الأقساط أعلى من التغطية من أجل الحفاظ على هامش الربح الذي تسعى إليه شركات التّأمين التجارية[85]، بالإضافة إلى عدم التضامن بين المؤمَّن لهم، فتدخل الأقساط المدفوعة في ذمة الشركة المالية وتغدو ملكاً لها وكل ما يحصل عليه المؤمَّن له هو مبلغ التّأمين عند تحقّق الخطر والّذي قد يقلّ عن قيمة الأقساط وليس له حينها حقّ المطالبة باستعادة أيٍّ من أمواله المدفوعة[86].

في حين يقوم التّأمين التعاوني على أساس عدم تحقيق الربح، بل توفير تغطية تأمينيّة للمؤمّن لهم بأقلّ تكلفة ممكنة، ويمارس هذا التّأمين هيئاتُ تأمينٍ تعاونيّةٍ أو جمعيّات تأمين[87]. ويطلق على التّأمين التعاوني مصطلح التّأمين التبادلي، ويعرّفه بعض الفقه على أنّه: "مجموعةٌ من الأشخاص المحاطين بأخطارٍ مشتركةٍ ينتظمون في جمعيّةٍ معيّنةٍ من أجل التّأمين على أخطارهم، إذ لا تهدف هذه الجمعيّة إلى تحقيق الرّبح، بل للحصول على خدماتٍ تأمينيّةٍ بأقلّ تكلفةٍ ممكنةٍ"[88]. ويتّسم هذا التّأمين بالسّمات الآتية: 1- يجمع العضو بين صفتي شركة التّأمين والمؤمَّن له معاً، حيث يؤمّن الأفراد على الأخطار التي تهدّد كلاً منهم لدى الآخر، وفي حال حلّ الخطر بأحدهم كان مؤمَّناً له وباتت الجماعة هي شركة التّأمين وتعوّضه عن ذلك، وهنا يبرز الاختلاف بينه وبين التّأمين التّجاري باتّحاد صفة شركة التّأمين والمؤمَّن لهم بذات الجماعة وليس بجهة مستقلة[89].

2-عدم تحقيق الرّبح، إذ لا يهدف إلى كسب الأموال، بل العمل على تفتيت الأخطار التي تهدّد الجماعة ككل وتوزيعها فيما بينهم فحسب[90]، ولذلك تبرز التضامنيّة بين أعضاء الجماعة في تغطية المخاطر،

---

[85] عبيد، (2016)، ص24.

[86] حسين، (1995)، ص26.

[87] عبد ربه، (2006)، ص56.

[88] بابكر أحمد، عثمان. (1997). قطاع التأمين في السودان تقويم تجربة التحول من نظام التأمين التقليدي إلى التأمين الإسلامي، ط:1، جدة: السعودية، البنك الإسلامي للتنمية، ص19.

[89] عبيد، (2016)، ص21- 22.

[90] عبده، (1978)، ص27.

فكلٌّ منهم ملزمٌ بأن يغطّي الآخر الذي حلّ الخطر به، وإذا ما كانت التّغطيات لا تكفي لمقابلة الخطر الحاصل فيلزم كلّ عضو ملزم بأن يدفع زيادةً تناسب حصّته التي اشترك فيها[91].

3-عدم ثبات القسط التّأميني؛ لأنّ المبالغ المدفوعة قابلةٌ للتغيير دائماً؛ إذا ما كانت الخسائر المتحققة تزيد عن الاشتراكات المدفوعة، لذلك لا يمكن معرفة مقدار المبلغ الواجب دفعه منذ البداية على عكس الحال في التّأمين التجاري الذي يحدد قسطه بدقّةٍ ودون قابليّةٍ للتّغيير الفجائي[92]، وهو ما يميّز التّأمين التّعاوني عن نظيره التّجاريّ بانخفاض أقساطه التي يزال منها هامش الربح الذي تسعى الشركات إلى تحقيقه.

ويمكن القول فيما يتعلّق بالطّبيعة القانونيّة لعقد التّأمين ضدّ مخاطر الإنترنت إنّه من العقود التّجاريّة التي تقوم بها شركات التّأمين بقصد تحقيق الربح في المقام الأول، ويتميّز بثبات القسط التّأميني المدفوع ما لم يطرأ أيّ تغييرٍ في طبيعة الخطر الإلكترونيّ المؤمّن عليه.

ثانياً: عقد التّأمين ضد مخاطر الإنترنت عقدُ تأمينٍ خاصٍّ فرديٍّ اختياريٍّ:

ويطلق على التّأمين الخاص التّأمين الفردي أيضاً، وهو يهدف إلى حماية مصلحةٍ خاصّةٍ فرديّةٍ، فلكلّ مَن يهدّده خطرٌ معيّنٌ الحقّ بأن يلجأ إلى شركة تأمين لتحمل معه هذا الخطر[93]، فالدافع نحو التّأمين الخاص هو المصلحة الشخصية البحتة دون النظر إلى المصالح العامة لبقية الأفراد، ولذلك يلجأ المؤمَّن له إلى شركات تأمين تهدف إلى الربح ويتحمّل القسط كاملاً بنفسه[94]. ويعد هذا التّأمين تأميناً اختيارياً يلجأ إليه الفرد بنفسه دون أيّ إلزامٍ قانونيٍّ.

في حين يقوم التّأمين الاجتماعي على أهدافٍ اجتماعيّةٍ تغلب عليها مصلحة المجموع أكثر من المصلحة الفردية، وهو لا يهدف إلى تحقيق الربح كما هو حال التّأمين التجاري، بل يغلب عليه تحقيق مصالح

---

[91] حسين، (1995)، ص27، وأيضاً بابكر أحمد، (1997)، ص19.

[92] المرجع السابق، ص19.

[93] عبيد، (2016)، ص37.

[94] عبده، (1978)، ص28.

الطّبقات الفقيرة المعرّضة لأخطار غير قادرة على مواجهتها[95]. وتتميّز أقساط التّأمين الاجتماعيّ بانخفاضها مقارنةً بالتّأمين الخاص على سبيل المثال؛ لأنّها تهدف إلى تحقيق هدفٍ اجتماعيٍّ بحتٍ، فيتشارك في دفع الأقساط المؤمَّن له وربّ العمل خصوصاً إذا ما عرفنا أنّ الأخطار المغطّاة في هذا التّأمين مرتبطةٌ بأعمالٍ معيّنةٍ محيطةٍ بالعاملين فيها، وحيث إنّهم لا يستطيعون تحمل أعباء التّأمين لوحدهم فيتشاركونها سويةً[96]. ويعرَّف بعض الفقه التّأمين الاجتماعي على أنّه: "تأمين الأشخاص الذين يعتمدون في كسب عيشهم على بعض الأخطار التي تقعدهم عاجزين عن العمل كالمرض والشيخوخة والبطالة[97]"، وتبرز أهمية هذا النوع في تحقيقه الأمان للعاملين في أثناء انقطاعهم عن عملهم نتيجةً لإصابةٍ معيّنةٍ أو طردهم من العمل أو عدم قدرتهم على العمل لإصابتهم بعجزٍ ما. كما يُعدّ هذا التّأمين إجباريّاً تلتزم به الدّولة أو تلزم مواطنيها بالاكتتاب عليه لتحقيق مصلحةٍ اجتماعيّةٍ، كالتّأمين الإجباريّ على حوادث السيّارات، كما ذهب إليه المشرّع السّوريّ في قانون السير، إذ أوجب إبرام عقود التّأمين لتغطية المسؤولية المدنية الناشئة عن الأضرار الجسديّة والماديّة التي تسببها المركبة أثناء استعمالها[98].

وتكمن الفوارق بين التّأمين الخاص والاجتماعيّ في الهدف، وطريقة دفع الأقساط، فبينما يرمي التّأمين الفردي إلى حماية مصلحة خاصة يحددها الفرد بنفسه، يذهب التّأمين الاجتماعي إلى حماية مصالح مجموعة من الأفراد معرّضين لنوعٍ معيّنٍ من المخاطر كالمرض، والعجز، والشيخوخة، وحيث إنّ المؤمَّن له الفردي يتحمل القسط كاملاً فتغلب الصفة التشاركية على التّأمين الاجتماعي.

وفي إطار عقد التّأمين ضد مخاطر الإنترنت، ينتمي التّأمين ضد مخاطر الإنترنت إلى طائفة التّأمين الخاص، نظراً لكونه يحمي مصالح فرديّةً خاصّةً، ويلجأ إليه المؤمَّن لهم من أجل حماية شبكاتهم المعلوماتية، وتغطية مسؤولياتهم المدنية بصرف النظر عن أيّ هدفٍ آخر، كما يُعدّ عقد تأمينٍ اختياريٍّ فلا

---

[95] عبد ربه، (2006)، ص56.

[96] حسين، (1995)، ص30.

[97] عبده، (1978)، ص28.

[98] المادة (186) من قانون السير والمركبات السوري رقم 31 لعام 2004.

يوجد أيُّ مؤيّدٍ يُلزم مستخدمي الشبكات المعلوماتية وشركات تخزين البيانات بأن تلجأ إلى التّأمين حتى الآن، بل إنها تلجأ إليه رغبةً في تحميل طرف ثالث الأخطار التي تتعرّض لها في سياق أعمالها عبر الإنترنت وتغطية المسؤولية المدنية التي تنشأ عنها.

ثالثاً: عقد التّأمين ضدّ مخاطر الإنترنت من طائفة عقود التّأمين من الأضرار:

يُعرَّف التّأمين على الأشخاص على أنّه: "تأمينٌ يرمي عن طريقه المؤمَّن له إلى حماية شخصه ونفسه من مخاطرَ معيّنةٍ كوصوله إلى عمرٍ معيّنٍ أو إصابته بمرضٍ معيّنٍ أو وفاته، ويلتزم بدفع أقساط معيّنةٍ مقابل التزام المؤمَّن له بدفع مبلغ التّأمين عند حصول الخطر المؤمّن منه[99]". وعليه فإنّه يشمل أنواع التّأمين التي يكون محلّها الشّخص نفسه والمخاطر التي تصيب جسم الإنسان كالمخاطر التي تصيب الإنسان في وجوده أو صحّته أو سلامة أعضائه، والحقيقة أنّه لا يقتصر هذا التّأمين فقط على الأحداث المؤلمة التي تأتي بالخسائر على المؤمَّن لهم، بل تمتدّ إلى الأحداث السعيدة كالزواج وإنجاب الأولاد أو التخرج[100].

وتتعدّد أنواع التّأمين على الأشخاص تبعاً لتعدّد الأخطار المؤمّن ضدّها، فهنالك تأمين المرض، ويكون الخطر المؤمَّن منه هو المرض، في حين يوجد تأمين البطالة والخطر المؤمَّن منه هو البطالة، وتأمين الإصابات والخطر هو الإصابات في بعض أجزاء الجسم، في حين يوجد تأمين الوفاة الذي يغطّي الوفاة[101]، وكذلك تأمين الزواج الذي يدفع عند الزواج في عمر معيّن، بالإضافة إلى تأمين المهر[102]، وتأمين الإنجاب في حال حصول الحدث في عمر معيّنٍ محدّدٍ مسبقاً. ويتميّز التّأمين على الأشخاص بعددٍ من الصّفات، نبيّنها وفقاً للآتي:

---

[99] زهرة، البشير. (1997). التأمين البري دراسة تحليلية وشرح لعقود التأمين، تونس، دار بو سلامة للطباعة والنشر، ص317.

[100] حسين، (1995)، ص30- 31.

[101] عبد ربه، (2006)، ص58.

[102] عبيد، (2016)، ص33.

1-ليس له صفة تعويضيّة؛ إذ لا يشترط حصول الضّرر من أجل دفع مبلغ التّأمين ولا إثبات وقوع الضرر من عدمه نتيجة لذلك، بل يستحق المبلغ بوقوع ضرر أو لا[103]، وينتج عن هذه الصفة حريّة الأطراف في تعيين مبلغ التّأمين بصرف النّظر عن الضّرر الحاصل للمؤمّن له، وإمكانيّة إبرام المؤمَّن له عقود عدّة تغطّي الخطر نفسه لدى شركات تأمين عدّة والحصول على مبالغ التّأمين كلّها دون النظر إلى مقدار الضرر الذي حلَّ بالمؤمَّن له، ويجب على شركة التّأمين دفع مبلغ التّأمين كلّه دون أن يكون له الاحتجاج بقاعدة النسبية.

2-عدم حلول شركة التّأمين محلّ المؤمَّن له في الرّجوع على الغير بالحقوق التي للمؤمَّن له عليه؛ لأنّ حقَّ الرجوع على الغير مختصٌّ بالمؤمَّن له وحده ولا ينتقل إلى شركة التّأمين، فلا يحقّ لها مقاضاة الغير؛ لأنَّ دفع شركة التّأمين لمبلغ التّأمين يقابل أقساط التّأمين التي دفعها المؤمَّن له، وليس نتيجة الضَّرر الحاصل من عمل الغير للمؤمّن له، بالإضافة إلى أنّ الغير يجب عليه دفع التعويضات التي يلزم بها نتيجة فعله، وليس له حقّ طلب المقاصة مع مبلغ التّأمين[104]. ويذهب بعض الفقه إلى تكييفه نتيجةً لهذه الخصائص على أنّه وعدٌ بدفع مبلغٍ معيّنٍ وليس عقد تعويض[105].

أمَّا التّأمين من الأضرار فيضمن هذا النوع من التّأمين للمؤمّن له كلّ المخاطر التي تصيب عناصر ذمّته الماليّة فتؤثّر عليها نقصاناً، ويعرَّف التّأمين ضد الأضرار على أنَّه: "عقد تأمين ضدّ نتائج الحوادث التي تصيب الفرد وتسبب ضرراً لأمواله ويهدف إلى تعويض الخسائر الحاصلة له[106]". وعلى خلاف التّأمين على الأشخاص يكون الخطر المؤمّن منه متعلّقاً بمال الشّخص المؤمَّن له لا شخصه، وينقسم التّأمين من الأضرار إلى تأمين على الأشياء وتأمين ضد المسؤولية، ويُطلق على التّأمين على الأشياء مفهوم التّأمين على الأموال أو الممتلكات، وينصبّ التّأمين هنا على أموالٍ منقولةٍ أو غير منقولة، بمعنى أنّ محلّ التّأمين هنا هو المال وليس الإنسان، في حين أنّ محل التّأمين في التّأمين ضدّ المسؤولية هو المسؤوليّة النّاشئة على عاتق

---

[103] المرجع السابق، ص33.

[104] زهرة، (1997)، ص 319- 320.

[105] القره داغي، (2010)، ص69.

[106] زهرة، (1997)، ص131.

المؤمَّن له[107]. ومن بعض صور هذا النّوع من التّأمين: تأمين السّرقة، تأمين الحريق، التّأمين البحري، تأمين المسؤولية المدنية، تأمين المسؤولية المهنية...، وتتمثّل خصائص التّأمين من الأضرار في الآتي:

1-الصّفة التّعويضيّة: إذ إنّ عقد التّأمين من الأضرار عقدٌ ذو صفةٍ تعويضيّةٍ يهدف إلى تعويض المؤمَّن له عن الضّرر الذي يحصل له نتيجة تحقّق الخطر المؤمّن منه في حدود هذا الضّرر، حيث إنّ التّعويض (مبلغ التّأمين) يكون بمقدار الضّرر الحاصل للمؤمَّن له، وينتج عن هذه الخصّيصة نتائج عدّة أهمّها:

أ- صعوبة تحديد مبلغ التّأمين مقدماً؛ نظراً للارتباط بين الضرر والتعويض، ولكن ذلك لا يمنع شركات التّأمين من تحديد حدٍّ أقصى لمبلغ التّأمين المحدّد في العقد، ويحصل المؤمَّن له عند وقوع الضّرر على جزءٍ منه يتناسب مع مقدار خسارته ودون أن يتجاوز الحدّ الأعلى.

ب-تطبيق مبدأ عدم إثراء المؤمَّن له على حساب المؤمّن، فلا يجوز أن يكون المؤمَّن له في مركز أفضل بعد تحقّق الخطر ممّا كان عليه سابقاً، ولذلك يكون التزام المؤمّن محدوداً بقيمة الخسارة فقط، فالمؤمَّن له ليس له الحقّ في تقاضي أيّ تعويض يزيد عن مقدار الضّرر الذي حصل له ولو كان لديه تأمينٌ لدى أكثر من شركة تأمين، فهو إمّا أن يأخذ تعويضاً من إحدى الشركات أو تتقاسم الشركات مبلغ التعويض فيما بينها بحسب نسبة مساهمة كلّ منها، ولا شيء يمنع من تقاضي تعويضٍ أقلّ من قيمة الضّرر ما دام يتساوى مع مبلغ التّأمين، وعبر هذه القيود على دفع التعويض يمكن التوصل إلى القضاء على خشية تعمّد تحقيق الخطر المؤمّن منه عن طريق إتلاف المال المؤمّن عليه والحصول على مبلغ تأمين يفوق قيمة الضّرر في حال كان مبلغ التّأمين يفوق قيمة الضّرر، وكما يمكن الوصول إلى هذه النتيجة عبر تحميل المؤمَّن له نسبة من الخسارة مع شركات التّأمين بمعنى أنّ تغطية الشّركة لا يشترط أن تكون كاملةً لكلّ الخسارة، بل قد تشترط إشراك المؤمَّن له في ذلك، وتأخذ صور هذا التّحميل إحدى الصّور الثّلاثة، وهي إمّا أن يتحمّل المؤمَّن له جزءاً من التعويض أو أن يتحمل مبلغاً معيناً مسبقاً أو أن يتحمّل تخفيضاً محدّداً مسبقاً من مبلغ التّأمين المستحقّ.

---

[107] الخفاجي، (2014)، ص 37- 38.

ج–كما أنّ الصّفة التّعويضيّة تفيد في التّخفيف من مخاوف المضاربة عبر تعدد المؤمنين والعمل على إتلاف المال المؤمّن عليه، فلو لم يوجد المبدأ التّعويضي لاستحقّ المؤمَّن له المبالغ التّأمينيّة كافّة، وهو ما يغريه بتحقيق الخطر بنفسه[108]، وأيضاً يتفرّع عن الصّفة التعويضية حريّة المؤمَّن له في تحديد صور المخاطر التي يشملها التّأمين، وينبثق عن ذلك تعدّد وثائق التّأمين بتعدّد المخاطر المؤمّن وتعدّد محلّات التّأمين، وعليه يمكن إبرام أكثر من عقد تأمين على محلٍّ واحدٍ، كما لو أمّن مالك عقار ومستأجره على العقار ذاته وهذا شيءٌ مقبولٌ وشائعٌ، كما ينطبق على التّأمين ضد المسؤولية –وهو أحد نوعَي التّأمين على الأشياء– قواعد الاشتراط لمصلحة الغير نظراً لوجود أطرافٍ ثلاثة هم شركة التّأمين والمؤمَّن له والمستفيد الذي سيدفع له المؤمّن مبلغ التّأمين عند وقوع الخطر[109].

2–مبدأ المصلحة: للمؤمَّن له أو المستفيد مصلحةٌ في عدم تحقّق الخطر المؤمّن منه، ويطلق مفهوم المصلحة على كلّ قيمةٍ اقتصاديّةٍ مشروعةٍ يُخشى عليها من التلف أو الهلاك نتيجة تحقق الخطر المؤمّن منه[110]. ونصَّ المشرّع السّوريّ على مبدأ المصلحة في القانون المدنيّ بقوله: يكون محلاً للتّأمين كلّ مصلحةٍ اقتصاديةٍ مشروعةٍ تعود على الشّخص من عدم تحقّق خطر معين[111]، وتكون هذه المصلحة للمالك ولكلّ مَن له حقٌّ عينيٌّ، كالدّائن المرتهن، ولمن له حقٌّ شخصيٌّ، فلكلّ هؤلاء مصلحةٌ بعدم تحقّق الخطر وضياع مصالحهم مع ضياع الشّيء المؤمّن عليه، ويشترط في هذه المصلحة أن تكون مشروعةً غير مخالفةٍ للنّظام العام وإلّا بطل العقد.

ويعدُّ عقد التّأمين ضدّ مخاطر الإنترنت أحد صور التّأمين من الأضرار؛ نظراً لكونه يغطي الخسائر التي تصيب الذمّة المالية للمؤمَّن له نتيجة مخاطر الإنترنت، بالإضافة إلى أنّ محلّ التّأمين هو البيانات الإلكترونيّة، والأنظمة التشغيليّة، وغيرها من وسائل العمل الإلكترونيّ ـوالتي تعود في غالب الأحيان لملكية

---

[108] زهرة، (1997)، ص132– 133..

[109] حسين، (1995)، ص41 وما يليها.

[110] القره داغي، (2010)، ص80.

[111] المادة (715) من القانون المدني السوري رقم 84 لعام 1949.

المؤمَّن له_ فيغطّي هذا التّأمين الأضرار التي تصيب ذمّة المؤمَّن له الماليّة نتيجة التعدّي على الأنظمة والحواسيب التي يعمل عبرها، وكشف البيانات المخزنة، وسرقة الأموال الإلكترونيّة، وأعمال الاحتيال الإلكتروني وانقطاع العمل نتيجةً لأيّ هجومٍ إلكترونيٍّ، كما يغطّي المسؤوليّة التي تقع على عاتق المؤمَّن له تجاه الغير نتيجة الأخطار السّابقة، وما تخلّفها من نفقاتٍ كالدّعاوى التي يرفعها الغير الذي كُشِفت خصوصيّته، والعميل الّذي سرقت أمواله نتيجة اختراق خوادم المصرف المودع لديه الأموال، والغرامات والتّعويضات التي يحكم للغير بها ويلزم المؤمَّن له بدفعها فتتحمّل شركة التّأمين ذلك نيابةً عنه، وبذلك لا يمكن إدخال هذا التّأمين تحت طائفة تأمين الأشخاص؛ لأنَّه لا يحمي الشخص المؤمَّن له أو نفسه أو غيره ممّا سبق ذكره، إنمّا يحمي ممتلكاته الإلكترونيّة التي تعود بملكيتها للمؤمَّن له.

رابعاً: إنّ عقد التّأمين ضدّ مخاطر الإنترنت يمثّل أحد صور الاشتراط لمصلحة الغير، وذلك عندما يكون تأميناً ضدّ المسؤوليّة، إذ إنّه عقدٌ يُبرم بين المؤمَّن له (المتعهّد) وشركة التّأمين (المشترط) الذي يلتزم بدفع مبلغٍ معيّنٍ هو مبلغ التّعويض لطرفٍ ثالثٍ (المستفيد) لا علاقة له بالعقد المبرم بين الطّرفين نتيجة الضّرر الذي لحقه عند تحقّق الخطر المؤمّن ضدّه، ومصلحة المؤمَّن له في ذلك ألّا يضطرَّ في لحظةٍ ما لدفع مبالغَ طائلةٍ كتعويضاتٍ للمتضرّرين من الحوادث الإلكترونية، كما أنّ المستفيدين ليسوا مُحدّدين في لحظة العقد ذاتها باسمهم الكامل، بل قابلين للتّحديد عند حصول الخطر.

ويستخلص مما سبق أنّ عقد التّأمين ضدّ مخاطر الإنترنت ينشأ بالأركان ذاتها التي يحتاجها أيّ عقدٍ حتى يبرم صحيحاً من رضا وأهليّة وسبب ومحلّ للعقد ولكن مع إسباغ الصفة الإلكترونيّة الناشئة عن طبيعة المخاطر التي تجعله فريداً من نوعه، فنحن أمام محلٍّ للعقد (البيانات والأنظمة) يختلف بطبيعته كليّاً عن المحل الذي يحميه العقد التقليدي، كما أنّ العقد بحاجة إلى أركانٍ خاصّةٍ للإبرام ناشئةٍ عن الطبيعة المختلفة التي يتميّز بها هذا العقد والهدف الذي يرمي إليه، كأخطار الإنترنت والتي بدورها تختلف عن المخاطر التقليديّة. ونتيجةً للبيئة الإلكترونيّة التي توجد فيها تلك المخاطر الإلكترونيّة فإنّها تؤثّر على الطّبيعة

القانونيّة للعقد والقواعد القانونيّة التي تحكم هذا العقد، فهو عقد تأمينٍ تجاريٍّ وخاصٍّ ضدّ الأضرار، وهو أحد أشكال الاشتراط لمصلحة الغير.

ولا ريب أنّ عقد التّأمين ضدّ مخاطر الإنترنت يدور وجوداً وعدماً مع المخاطر الإلكترونيّة، فهي من أهم الأركان التي يقوم عليها هذا العقد؛ لذلك لا بدَّ من الإضاءة بشكلٍ موسّعٍ على ماهيَّة هذه المخاطر في المبحث الثاني.

المبحث الثَّاني

ماهيَّة مخاطر الإنترنت

لم تعد المخاطر التي تواجه الأفراد والشركات في أعمالهم تقتصر على المخاطر التقليديّة كالحريق والسّرقة الماديّة، بل تطوّرت نتيجة التطوّر التّقنيّ الحاصل ووسائل التواصل الحديثة وربط كلّ الأعمال عبر شبكة الإنترنت، وأصبحت تأخذ شكلاً مختلفاً عمّا عهدته الشركات في الأيام السابقة. وتشكّل مخاطر الإنترنت اليوم إحدى الهواجس التي يتخوّف منها الأفراد والشركات التي تستخدم الإنترنت في أعمالها ولا سيّما في ظلِّ تنامي هذه المخاطر وانتشارها الكبير لتشمل مختلف القطّاعات وحجم الخسائر التي تسبّبها سنويّاً بمختلف القطاعات، إذ بات الإنترنت أحد وسائل ارتكاب الجرائم عبر الشبكة وتحوَّل إلى سلاحٍ مؤذٍ بيد المجرمين الإلكترونيين الذين جعلوا الفضاء الإلكترونيّ مسرحاً لجرائم افتراضيّة. وعليه لا بدَّ من محاولة فَهْم مخاطر الإنترنت عبر التعرّف إلى مفهوم هذه المخاطر في المطلب الأوّل، ودوافع وصور مخاطر الإنترنت في المطلب الثّاني.

المطلب الأوَّل

مفهوم مخاطر الإنترنت

تتربَّع مخاطر الإنترنت عالميّاً على رأس قائمة المخاطر التي تتعرَّض لها الشّركات بمختلف أنواعها وقطّاعاتها، وبات الشّغل الشّاغل للشّركات كيفية تأمين نفسها ضدّ هذه المخاطر، خاصّة أنَّه لا يمكن الإفلات منها مع اتّساع العمل الإلكترونيّ وسهولة عمليّة الاختراقات. وتغدو عمليّة تحديد مفهوم هذه المخاطر ذات أهميّة لتفريقها عن المخاطر الأخرى، وعليه سيتمّ البحث في تعريف هذه المخاطر (الفرع الأوّل)، ومن ثمّ دراسة خصائصها لتمييزها عن سواها من المخاطر (الفرع الثّاني).

الفرع الأوَّل

تعريف مخاطر الإنترنت وطبيعتها القانونيَّة

تغدو عمليّة وضع تعريفٍ لأيّ مفهومٍ صعبةً للغاية لا سيّما أنّ القانون في كثيرٍ من الأحيان لا يتطرّق إلى هذا الجانب تاركاً الأمر للفقه الذي يتولّى زمام المبادرة شارحاً المصطلحات وموضّحاً المعاني.

أوّلاً: تعريف مخاطر الإنترنت:

باتت مخاطر الإنترنت مصطلحاً واسعاً متداولاً عبر المواقع الإلكترونية ولا يكاد يمرّ يوم دون سماع أخبارٍ عن هجومٍ إلكترونيٍّ على موقع شركةٍ معيَّنةٍ هنا وهناك. ويتكوّن مفهوم مخاطر الإنترنت من مفهومينِ رئيسينِ يتشاركان فينتجان مخاطر الإنترنت، فلا بدَّ من توضيح هذه المفاهيم وصولاً إلى تحديد مفهوم مخاطر الإنترنت.

1-المخاطر: وتنبثق كلمة المخاطر من مصطلح الخطر، وقد سبق تناول مفهوم الخطر عند الحديث عن أركان العقد، فهو الحادث احتماليّ الحصول، ويعرَّف الخطر بأنّه: "حالة عدم التأكّد الممكن قياسه، وبذلك يُعدُّ الخطر هو الحالات القابلة للقياس والحسابات الإحصائيّة، أمّا عداه فهو ليس بخطرٍ بل لا يعدو أن يكون

مجرّد شكٍّ لا يرقى إلى مرحلة الخطر[112]"، كما عرَّفه اتجاه آخر بأنَّه: "عدم التأكّد الموضوعيّ فيما يتعلّق بتحقّق حادثٍ غير مرغوبٍ فيه[113]" وقد أضاف هذا التّعريف صفة الرَّغبة في تجنّب الخطر وعدم تحقّقه. والحقيقة مهما تعدّدت تعاريف الخطر وهي كثيرةٌ، لكنّها كلّها تشدّد على فكرة الاحتماليّة وعدم إمكانيّة التّحقّق من حصول الخطر، وبأنّه حادثٌ لا يرغب الشّخص في تحقّقه.

2-الإنترنت: يُعدُّ الإنترنت تقنيةً حديثةً أحدثت ثورةً في عالم الاتصالات ويتيح الإنترنت لمستخدمه بالتّواصل مع أشخاص حول العالم والوصول إلى المعلومات عبر الحواسيب التي ترتبط ببعضها البعض، ولفظ الإنترنت ليس عربياً بل هو تعريب لكلمة Internet التي تعود في أصلها إلى اللغة الإنكليزية، وتقسم هذه الكلمة إلى مقطعين هما inter والتي تعني (ما بين) و net اختصاراً لكلمة network أي الشَّبكة، وبالتالي عند دمج هاتين الكلمتين يتوصّل إلى تعريف الإنترنت بأنَّها: "شبكة الشّبكات أو الشّبكة البينيّة أو نظام يصل بين شبكاتٍ مستقلّةٍ عن بعضها"، وتعرف أيضاً بأنّها: "شبكةٌ دوليّةٌ للمعلومات تتفاهم باستخدام بروتوكولات وبتعاون فيما بينها لصالح مستخدميها، وتتيح لهم كثيرٌ من الميّزات كالبريد الإلكترونيّ والاتّصال الصّوتيّ والمرئيّ وإقامة مؤتمرات عبر الفيديو وقوائم بيانات وملفات متاحة لنقلها واستخدامها شخصياً[114]".

كما يعرَّف بأنّه: "شبكة حواسيب آليّةٍ مرتبطةٍ ببعضها عن طريق خطوط الهاتف أو الأقمار الصّناعيّة، والّتي تتيح لمشاركيها الاطّلاع على المعلومات التي يتبادلونها عبر الشّبكة، بالإضافة إلى تبادل الرسائل والوثائق[115] ". كما يعرّفه آخرون بأنَّه: "شبكة حواسيب دوليّة تربط شبكات وحواسيبَ أخرى من الجامعات والشركات وغيرها[116]"، وهو طريقٌ سريعٌ ومعروفٌ وشاملٌ للمعلومات قادرٌ على توفير الوصول الفوري تقريباً إلى

---

[112] أبو السعود، علي. (د. ت.) مبادئ الخطر والتأمين، (د. ن.)، ص 2- 3.

[113] المرجع السابق، ص3.

[114] https://www.ar.wikipedia.org/wiki/%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA

تاريخ الزيارة: 10\5\2020, الساعة 9:20 p.m.

[115] سلطان العلماء، محمد عبد الرحيم. (2003). جرائم الإنترنت والاحتساب عليها، مج: 18، عدد: 36، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، ص22.

[116] Ibraheem (2008), p4.

مخزنٍ كبيرٍ من المعلومات يمتدّ عبر العالم[117]". ومهما تعدّدت تعاريف الإنترنت فكلّها لا تخرج عن كونها شبكةَ حواسب ممتدّة عبر العالم، متّصلة ببعضها بخطوط هاتفيّةٍ أو أقمارٍ صناعيّةٍ وتسهم في توفير كلّ ما يحتاجه الفرد في حياته من معلوماتٍ بسهولةٍ ويسرٍ.

وفيما يتعلّق بمفهوم مخاطر الإنترنت، فهو يقوم على حدثٍ احتماليٍّ يهدّد شبكات الإنترنت حول العالم، وما يزال حتى الآن وضع تعريف محدّد للخطر الإلكتروني من أهم التحديات التي تواجه الخبراء، وشركات التّأمين، والشركات التي تواجهها هذه المخاطر؛ نظراً لصعوبة تحديد حجم الخطر الإلكتروني وطبيعته، وتحديد الأصول المستهدفة بهذا الخطر، إذ تبدو النقطة الأولى لتحديد الأخطار التي قد تواجهها الشّركة عبر تحديد الأصول التي تملكها والمعلومات المخزّنة لديها. وفي إطار التّعاريف التي سِيقت لمفهوم مخاطر الإنترنت، والتي يُطلق عليها المخاطر الإلكترونيّة أيضاً أو المخاطر السيبرانيّة _ كونها ترتبط بالفضاء السيبراني_[118] من عرَّفها على أنَّها: "مجموعةٌ من مصادر الخطر التي تؤثّر على أصول المعلومات والتكنولوجيا التي تملكها شركةٌ معيّنةٌ ومن هذه الأخطار سرقة الهويات، وكشف معلوماتٍ حسّاسة، وانقطاع العمل[119]". ويفرّق البعض بين تعريفٍ ضيّقٍ وتعريفٍ واسعٍ لمخاطر الإنترنت بناءً على أشكال هذه المخاطر، ففي التعريف الضيّق يقال: إنّه "الخطر المرتبط بحوادثَ إلكترونيّةٍ خبيثةٍ تسبّب انقطاعاً في العمل وخسائر ماليّة كاستغلال بعض المهاجمين الإلكترونيين والموظفين من داخل الشركة لنقاط ضعف مستويات الأمان في الشركة واقتحامهم لقواعد بياناتها وجمع معلومات العملاء كبطاقات الائتمان والبطاقات التعريفية[120]، ويقوم هذا التعريف على تحديد سبب الخطر وهو البرمجيّات

---

[117] Forsythe, S., Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping, v56, Elsevier: Netherlands, Journal of Business Research, p868

[118] يقصد بالفضاء السيبراني المجال المادي وغير المادي الذي يتكون من عناصر هي الحواسيب، والشبكات، والبرمجيات، وحوسبة المعلومات، والمحتوى، ومعطيات النقل، والتحكم، ومستخدمو كل هذه العناصر، مشار إليه على الموقع الإلكتروني:
https://www.ar.wikipedia.org/wiki/%D9%81%D8%B6%D8%A7%D8%A1_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

تاريخ الزيارة: 5\5\2021، الساعة 6:30 p.m.

[119] Biener, C., Eling, M., Wirf, J. H. (2015). insurability of cyber risk: an empirical analysis, working papers on risk management and insurance, no. 151, St.Gallen: Switzerland, institute of insurance economics., p3.

[120] Mukhopadhyay, A., & others. (2013). Cyber-risk decision models: To insure IT or not, v56, decision support systems, p1.

الخبيثة، ونتيجتها في انقطاع العمل والخسائر الماليّة؛ ولذلك ضيّق هذا التعريف من نطاق المخاطر الإلكترونية، والحقيقة أنّها أوسع من ذلك؛ لأنّ أشكالها غير حصريّة وتتجدّد كلّ يومٍ، وبهذا الصّدد يُطلق على مخاطر الإنترنت مصطلح الهجوم السيبرانيّ، ويعرَّف بأنَّه: "استغلالٌ متعمّدٌ لأنظمة الكمبيوتر والشّبكات والشّركات المعتمدة على التكنولوجيا عبر برمجيّاتٍ ضارّةٍ لتعديل البيانات مسبّبةً عواقبَ مدمّرة[121]". في حين ذهب التّعريف الواسع إلى أنّ الخطر الإلكترونيّ هو: "خطر أمنٍ معلوماتيٍّ أو أيّ خطرٍ ناشئٍ عن فشل أنظمة المعلومات[122]"، ولم يحدّد التّعريف السّابق شكل هذا الخطر، بل ذهب إلى أنّه أيّ فشلٍ في النظام أو أخطار أمن معلوماتي، وترك الباب مفتوحاً أمام أشكالٍ مختلفةٍ من الأخطار، وهو ما يوسّع نطاق المخاطر، ويعرَّف أيضاً في هذا النطاق على أنّه: "أيّ خطر مرتبط بخسارةٍ ماليّةٍ، انقطاع عمل، أو ضرر لسمعة منظمةٍ ما نتيجة حادثٍ سلبيٍّ أثَّر على معلومات الشّركة أو أنظمة معلوماتها[123]"، كما يُراد بالخطر الإلكترونيّ أيضاً أنَّه يتضمَّن أخطاراً معيَّنةً تتعلَّق أو ترتبط باستخدام الحواسيب أو تقنيّة المعلومات أو الواقع الافتراضي[124]، ويتميّز هذا التَّعريف بكونه أوسع من سابقه. وفي أحد التعاريف الموجزة عن مخاطر الإنترنت تبيّن أنّها: "أيّ مخاطر مرتبطة بالخسارة المالية أو الاضطراب أو الضرر الذي يلحق بسمعة المنظمة من الفشل أو الاستخدام غير المصرّح به أو الاستخدام الخاطئ لأنظمة المعلومات الخاصّة به"، وتشمل الأمثلة على المخاطر السيبرانية التي يتعرّض لها النشاط التجاري الجرائم الإلكترونية، والإرهاب السيبراني، والخسارة العرضيّة للبيانات السريّة، فضلاً عن المسؤوليّة عن نشاط الشّركة عبر الإنترنت. وهذه الأمثلة على سبيل المثال لا الحصر والباب مفتوحٌ أمام أمثلةٍ أخرى تبعاً للتطوّر المستمرّ في الإنترنت، ولتوضيح الأمر بطريقةٍ أخرى، فإنَّ المخاطر السيبرانيَّة هي التكرار والحجم

---

[121] https://www.phoenixnap.com/blog/cyber-security-attack-types

تاريخ الزيارة: 10\5\2020, الساعة 10:30p.m.

[122] Böhme, R., Kataria, G., (2003). Models and Measures for Correlation in Cyber-Insurance, Working Paper, Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK, p1.

[123] https://www.cyber-risk.com.au/

تاريخ الزيارة: 10\5\2020, الساعة 12a.m.

[124] Cyber risk explained: what they are, what they could cost, and how to protect against them (2013), Marsh, available at:
https://www.marsh.com/se/en/services/cyber-risk.html

تاريخ الزيارة: 10\5\2020, الساعة 12a.m.

المحتمل للخسارة المستقبليّة التي تتعلق بأنظمة معلومات المنظمة والأصول المرتبطة بها، سواء المادية أو المعلوماتية[125].

والحقيقة أنّه مهما حاول الفقه وضع تعريفٍ لمخاطر الإنترنت إلّا أنها ما تزال مهمّةً صعبةً؛ وذلك لأنّ المفهوم يتّسع كلَّ يومٍ مع دخول أشكالٍ جديدةٍ من التقنيات المعلوماتيّة، ولتعدّد أشكال المخاطر التي تواجهها الشّركات اليوم، لذلك كثيراً ما تكون التّعاريف ضيقةً محدّدةً في شكل خطرٍ معيّنٍ أو تكون واسعةً عامّةً لشكل الخطر الإلكتروني.

ثانياً: الطبيعة القانونية لمخاطر الإنترنت:

ويخرج عن نطاق مخاطر الإنترنت المخاطر التقليدية وإن كانت تؤثّر على شبكة المعلومات أو الأنظمة، كما لو أدّى حريقٌ ما في شركةٍ إلى فقدان معلوماتها أو أدت سرقة حاسب موظّفٍ إلى كشف بيانات الشركة لكن لا تندرج هذه الأخطار في نطاق مخاطر الإنترنت؛ لأنّها وإن أحدثت نتيجةً إلكترونيةً إلّا أنّ الخطر لم يكن إلكترونيّاً أبداً، لذلك يخرج عن نطاق المخاطر الإلكترونيّة أو مخاطر الإنترنت المخاطر التّقليديّة كالحريق والسّرقة والعواصف والكوارث الطّبيعيّة أو الخطأ المادّيّ لشخصٍ أو لموظّفٍ، ويمكن القول إنّ **معيار الخطر الإلكترونيّ هو أن يكون سببه إلكترونيّاً ناشئاً عن التعامل عبر الإنترنت**، كحوادث الاختراق لخوادم الشركة أو الدخول غير المصرّح به أو احتجاز موقع الشّركة لساعاتٍ من أجل فديةٍ، ناهيك عن حوادث التشهير وتشويه السمعة المرتكبة، ففي كلّ هذه الأمثلة كان السبب إلكترونياً؛ ولذلك عُدَّ خطراً إلكترونيّاً عدا عن كونه ينتج آثاراً إلكترونيّةً، وفي هذا جوهر الفرق في شكل الأخطار بين هذا العقد وغيره من عقود التّأمين، ولذلك تستثني كثيرٌ من شركات التأمين ضد مخاطر الإنترنت هذه المخاطر التقليديّة من تغطيتها.

---

[125] Cyber Risk – Enlightenment through information risk management, available at: https://www.pwc.com.au/consulting/security-cyber-assets/cyber-risk.html

تاريخ الزيارة: 11\5\2020, الساعة 1p.m.

وتتعدّد أسباب مخاطر الإنترنت بحسب نوايا المهاجم وأصول الخطر، فتقسم إلى مخاطرَ داخليّةٍ عمديّةٍ أو غير مقصودةٍ، ويُراد بها أفعال السّرقة والتّخريب الإلكترونيّ الحاصلة من موظّفٍ داخل الشّركة أو بنتيجة إهمال الموظّف، ومخاطر خارجيّة عمديّة أو غير مقصودة؛ أي الاعتداء العمديّ من قبل مهاجم من خارج الشّركة كاختراق قواعد البيانات الخاصّة بها أو هجمات إنكار الخدمة وإغلاق المواقع، وقد تكون هذه المخاطر غير مقصودة، أي بنتيجة خطأ في النّظام المستخدم يؤثّر على إمكانيّة الوصول[126].

وبات الإنترنت اليوم سلاحاً بين الدّول تشهره على أعدائها وتحوّلت الحرب من حربٍ تقليديّةٍ وقودها الأسلحة إلى حربٍ إلكترونيّةٍ تتمّ كلّها عبر شبكة الإنترنت وقودها خبراء المعلوماتية الذين يتولّون قيادة هذه الحرب نيابةً عن بلادهم، وأُطلِق على هذه الحرب (حرب المعلومات)، ومضمارها هو الفضاء السيبرانيّ، ومقومات نجاح الطّرف أو هزيمته هو مقدار تقدّمه تقنياً وحيازته لأقوى العقول وأكثرها خبرةً على المستوى المعلوماتيّ، ويُراد بحرب المعلومات: "استخدام نظم المعلومات من أجل استخدام أو تدمير أو تخريب أو تعطيل معلومات الخصم وعملياته المبنيّة على المعلومات ونظمٍ معلوماتيّةٍ وشبكات الحواسيب لديه"[127]. ويقسِّم البعض حرب المعلومات إلى حربٍ شخصيّةٍ وحربٍ بين مؤسّساتٍ وحربٍ عالميّةٍ، ويُقصَد بالحرب العالمية الحرب التي تنشب بين دولٍ مختلفةٍ من أجل سرقة أسرارها وتوجيه تلك المعلومات ضدّها، كحوادث التجسّس على الدّول كنظام التجسس إيشلون أو إيكيلون الذي أنشئ إبان الحرب الباردة باتفاق الولايات المتحدة الأمريكيّة وبريطانيا ونيوزيلندا وأستراليا وكندا واستمرّ حتى الآن، وهو يستطيع جمع ما يزيد على 100 مليون اتّصال شهرياً حول العالم والتنصّت عليها واستخدام المعلومات التي تجمعها وفك شيفرات بعض الرموز، وكلّ ذلك في سبيل خدمة أهدافٍ تجسسيّةٍ لغاياتٍ صناعيّةٍ وتجاريّةٍ وعسكريّةٍ وتحت ذريعة مكافحة الإرهاب والجريمة والمخدرات[128].

---

[126] https://www.finder.com.au/cyber-risk#1

تاريخ الزيارة: 8\5\2020، الساعة 10.p.m.

[127] الحمود، عبد الله بن ناصر. (2006). وسائل الإعلام المعاصرة والإرهاب المعلوماتي، دورة تدريبية تقيمها جامعة نايف الأمنية في مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، المغرب، ص62.

[128] https://www.arab-army.com/t84615-topic

تاريخ الزيارة: 11\5\2020, الساعة 6.p.m.

و الواقع أنّ حرب المعلومات هذه وفق بعض الفقه لا يقتصر نطاقها على الدّول فحسب، إنّما تضمّ أيضاً الشّركات التي تعمل على استغلال الإنترنت من أجل القضاء على منافسيها، وترويج سلعها، وزيادة سمعتها وشهرتها التجارية، ويدخل هذا العمل ضمن إطار المنافسة غير الشّريفة، ويمكن أن يكون ضمن سياسة الإقصاء التي تقوم على تعطيل قوى الشّركة المنافسة عبر اختراق أنظمة الشّركات وسرقة معلوماتها وتدميرها أو استخدامها من قبل الشّركة المهاجمة، وقد يندرج ذلك ضمن سرقة الأسرار التّجاريّة، كما قد يتمّ الأمر عبر التّشهير بشركةٍ ما من قبل منافستها عبر الإنترنت من أجل إخراج هذه الشّركة من المنافسة[129].

وخلاصة القول: ينصبّ محلّ هذه المخاطر على أشياءَ متعدّدةٍ، منها البرمجيات، والبيانات، والأنظمة والحواسيب، وغيرها، كما لو كان المسروق هو وحداتٌ نقديّةٌ إلكترونيّةٌ من حسابٍ مصرفيٍّ، كما وينصبُّ أيضاً على حقِّ الخصوصيَّة في صورةٍ أوسع، فالبيانات المخترقة تمثّل معلوماتٍ شخصيّةً حول العميل متضمّنةً اسمه وتاريخ الولادة ومعلومات صحيّة وماليّة تبعاً لصفة الشركة التي تخزّن هذه المعلومات، وهي معلوماتٌ يفترض أن تبقى سريّةً وألّا يطّلع عليها إلّا أصحاب الاختصاص في الشّركة لتعلّقها بحقٍّ شخصيٍّ للعميل، ولذلك فإنَّ الخرق وسرقة هذه البيانات هو اعتداءٌ على حقِّ الخصوصيَّة قبل كونه سرقة بياناتٍ أو معلومات شركةٍ معيّنةٍ، كما قد يكون محلّ الخطر حقوق الملكيّة الفكريّة، كحقِّ المؤلّف وحقوق الملحّن والموزّع وغيره على سبيل المثال، فقد تمتلك شركة إنتاج أو منصّة عرضٍ معيّنةٍ حقوق العرض الحصريّة لفيلم ما، وعندها تتمّ قرصنة الموقع الإلكتروني لها وسرقة هذا الفيلم وعرضه بالمجّان للعامة دون أخذ إذن الشّركة في أحد أكثر أشكال انتهاك حقوق الملكية الفكرية شيوعاً. ويمكن القول: إنّ **طبيعة المعلومات والبيانات المخزّنة** عبارةٌ عن معلوماتٍ قابلةٍ للنّقل والحيازة عبر وسائلَ إلكترونيّةٍ كالبريد الإلكتروني أو وسائلَ ماديّةٍ كالأقراص الصّلبة، وهي ذات قيمةٍ اقتصاديّةٍ بذاتها تفوق قيمة الأشياء الماديّة، وتظهر فقط بمظهرٍ معنويٍّ، وعليه يمكن اعتبارها مالاً معنوياً، وكما يمكن الاستناد إلى نصّ المادة (83) من القانون المدنيّ السّوريّ الذي ذهب إلى أنَّ كلَّ شيءٍ غير خارجٍ عن التعامل بطبيعته أو بحكم القانون يصحّ أن يكون محلاً للحقوق الماليّة، وهو خير دليلٍ على إضفاء صفة المال على هذه

[129] الحمود، (2006)، ص63.

البيانات، فالشّرط الوحيد لعدّ الشّيء مالاً هو ألّا يكون الشّيء غير قابلٍ للتّعامل فقط. ولا بدَّ من دراسة خصائص هذه المخاطر وأنواعها بعد تحديد تعريف مخاطر الإنترنت وطبيعته القانونيّة.

الفرع الثّاني

خصائص مخاطر الإنترنت وأنواعها

تتَّسم مخاطر الإنترنت عن غيرها من المخاطر بصفاتٍ تعطيها ميزةً مستقلّةً، وتنبع في أساسها من الصّبغة الإلكترونيّة المحيطة بها، ويتمّ تقسيم المخاطر بناءً على معاييرَ عدَّةٍ إلى أنواعٍ عدّة، سيتمّ دراستها فيما سيأتي.

أولاً: خصائص مخاطر الإنترنت:

تتميّز مخاطر الإنترنت بصفاتٍ عدّةٍ نابعةٍ من طبيعتها الإلكترونيّة، نذكر منها[130]:

1-مخاطر إلكترونيّة: إنَّ الصّفة الأساسيّة لهذه المخاطر هو طبيعتها الإلكترونيّة النّاشئة عن طبيعة العمل عبر الإنترنت، فهذه المخاطر لا يمكن أن تتجسّد بصورةٍ ماديّةٍ تقليديّةٍ، إذ لا يستطيع الشّخص أن يرى الفايروس في حاسوبه بالعين المجرّدة أو أن يلمسه، إنّما هي عبارةٌ عن رموزٍ وشيفراتٍ لا يعرفها إلّا المختصّون، ولكنَّ النتائج التي تسبّبها هذه المخاطر تتنوّع بين ماديّةٍ وإلكترونيّة، فبينما يسبّب ذلك تضرّر الأنظمة التي يستخدمها المضرور وتوقّفها عن العمل في بعض الأحيان، وكذلك خسارة المعلومات التي يخزّنها والتي اتُّفِق على أنَّها أموالٌ معنويّةٌ، بالإضافة إلى خسارة المصداقيّة والسّمعة، إلَّا أنَّ ذلك لا يعني أنَّ النتائج لا تظهر بصورةٍ ماديّةٍ عبر الخسارات التي تلحق بالذمَّة الماليَّة للشَّخص المضرور، كما أنَّ الضَّرر قد يلحق أعطالاً بحاسبه غير قابلة للإصلاح، وبالتَّالي لا بدَّ من استبداله بحاسبٍ جديد، وأيضاً كساد المنتجات التي قد تتولَّى الشَّركات بيعها نتيجة فقدان الثّقة من الزبون.

---

[130] Ruan, K. (2019). Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics, Rotterdam: Netherlands, Academic Press Elsevier, P 160.

2-مخاطر افتراضيَّة: فهي لا تظهر للشَّخص المضرور بصورةٍ ماديّةٍ يمكن لمسها، وإنَّما هي ممارساتٌ تتمّ عبر الواقع الافتراضيّ (الشبكات)؛ ولذلك قد تظلّ لفترةٍ طويلةٍ غير مكتشفةٍ تعمل على تخريب الحاسب وتدمير المعلومات دون ترك أيّ أثرٍ ماديٍّ، وعليه هي بحاجة لجهدٍ كبيرٍ من أجل اكتشافها، ثمّ تحديد سبب هذا الخطر ومحاولة معالجته.

3-نطاق مخاطر الإنترنت غير محدّد: من حيث المبدأ يصيب الخطر الأفراد والمؤسّسات والشّركات عامّة أو خاصّة كانت، أمَّا مخاطر الإنترنت فهي بصفةٍ عامّةٍ لا تُصيب شخصاً بنفسه، وإنّما تتعدّد الأنظمة المصابة بالفايروس الذي يخترق أنظمةً عدّة في آنٍ واحدٍ، وقد يصل عددها إلى عشرات الأنظمة التي تنهار في الوقت ذاته نتيجة لفايروس يصيب نظاماً في المرحلة الأولى، لكنّه سرعان ما ينتقل إلى أنظمةٍ كثيرةٍ عن طريق نسخ نفسه وانتقاله مع الملفّات المرسلة من النّظام المصاب، كما أنّ إصابة أحد أنظمة التشغيل بعطلٍ يعني إصابة كلّ الحواسيب العاملة بهذا النّظام بالعطل ذاته، عوضاً عن أنّ كثيراً من المخاطر تنطوي على اختراق وسرقة بيانات، وبالتالي لمّا كان محلّ الخطر معلوماتٍ فإنَّ ذلك سيصعب مهمّة تحديد نطاق الخطر؛ لأنَّ الخرق غالباً ما ينطوي على ملايين البيانات التي تخزّنها كلّ شركةٍ، وبالتَّالي كنتيجةٍ لما ذُكِر يكون من الصّعب حساب الخسائر والأضرار في وقتٍ قصيرٍ، بل يأخذ ذلك وقتاً طويل خصوصاً إذا ما قِيل أنَّ الكشف عنه لا يتمّ فوراً، إذ لا يمكن ملاحظته إلّا بعد فترةٍ.

4-مجهوليّة مرتكبي المخاطر: فالشّخص المضرور لا يمكنه معرفة المجرم الذي تلاعب بحاسبه ما يجعله غير قادرٍ على مقاضاته، ذلك أنَّ هذا المجرم في كثيرٍ من الأحيان قد يكون بعيداً عن ضحيّته آلاف الكيلومترات _بل إنَّه قد يكون في قارّةٍ أخرى_ يرتكب جريمته من وراء الحاسب مستخدماً شيفرات يعرفها ويستغلّها في سرقة معلومات الشّركات ليبتزّهم مقابل عدم بيعها في السّوق السّوداء؛ لذلك كثيراً ما تُسجَّل هذه القضايا ضدّ مجهول لعدم معرفة المتسبّب لها، بل إنّ التحقيقات قد لا تُفضي إلى معرفة نقطة البداية؛ أي ما هو أوّل حاسبٍ مخترَقٍ (الضحيّة الأولى)؛ لذلك لا يوجد شخصٌ لتحمّل المسؤوليّة القانونيّة عن أفعاله.

5-مخاطر الإنترنت تمتدّ إلى ما هو أبعد من مجرّد بياناتٍ تُسرَق وحواسيب تُدمَّر، فهي تجعل الشّركات الضحيّة لهذه الأفعال مسؤولةً قانوناً أمام عملائها عن الإخفاق في حماية خصوصيّة معلوماتهم، ما يعني غرامات باهظة تُفرض عليهم، وسمعة وقدرة تسويقيّة فاشلة، وهو ما قد يؤدّي بها لإعلان إفلاسها.

6-سرعة التغيّر: تُعدّ مخاطر الإنترنت سريعة التطور؛ إذ إنّها تغيّر استراتيجيّة هجماتها بسرعةٍ وباستمرارٍ، فالتطوّرات التقنيّة تتيح هجماتٍ إلكترونيّةً جديدةً على أشكالٍ مختلفةٍ من التكنولوجيا الحديثة، كإنترنت الأشياء وخدمات الحوسبة السّحابيّة إلى الذّكاء الاصطناعيّ. **ويُعدُّ هذا التطوّر أحد التّحديات المستمرّة التي تواجه عمليّات التّأمين ضدّ مخاطر الإنترنت؛ نظراً لعدم القدرة على معرفة المخاطر بصورةٍ دقيقةٍ، وهو ما ينعكس على تقييم الأصول وتقدير الخسائر ونقص البيانات**[131].

7-ارتباط مخاطر الإنترنت ببعضها: وهو كما ذكر سابقاً أنّ الحواسيب والشبكات اليوم عبارة عن أنظمةٍ متّصلةٍ ببعضها بعضاً والخلل في أيٍّ منها يؤدّي لعطلٍ على الشبكة ككل؛ لذلك فالهجوم الذي يصيب أيّ شبكةٍ يمتدّ إلى غيره على نحوٍ غير قابلٍ للتوقّف، وهو أحد السمات التي تجعل الخطر الإلكترونيَّ منفرداً بطبيعته.

ثانياً: أنواع مخاطر الإنترنت:

ويمكن البحث في إطار الخصائص عن بعض أنواع مخاطر الإنترنت التي ساقها بعض الفقه، والتي تختلف تبعاً لمعاييرَ متعددةٍ:

1- تبعاً لمستويات المخاطر: يذهب بعض الفقه إلى أنّه يندرج تحت مسمّى مخاطر الإنترنت أشكالٌ مختلفةٌ من المخاطر، ويتم تحديد نوع المخاطر حسب مستويات المخاطر التي تُبنى على أساس البعد الذي يظهره الخطر[132]:

---

[131] ibid, p77.

[132] Grzebiela, T. (2002). Insurability of Electronic Commerce Risks, Proceedings of the 35th Hawaii International Conference on System Sciences, Germany, Institute for Computer Sciences and Social Studies, p2.

أ–مستوى الخطر الفني: ويُظهِر المخاطر من منظورٍ تقنيّ، إذ يقوم على تفحّص نماذج المهاجمين الإلكترونيين عبر تقييم ودراسة آليّات الحماية التي يتبعها الفرد المتضرّر مقابل قياس نقاط قوّة وقدرات المهاجم، وبمعنىً آخر تُوضع وسائل الحماية في مقابل قدرات المهاجمين، ويضمّ هذا المستوى هجمات القراصنة والفيروسات، بالإضافة إلى هجمات إنكار الخدمة.

ب–مستوى الخطر الفرديّ: ويضمّ في مقدّمة هذا الخطر خرق الخصوصيّة وسرقة الهويات، ويضم هذا المستوى بُعدَين؛ الأول منهما الفرد الذي قد تنتهك خصوصيته عبر إساءة استعمال المعلومات الشخصيّة ومحاولة بناء ملف تعريفٍ شخصيٍّ باستخدام المعلومات المسروقة، وإمكانية استخدامه بالانتحال وسرقة الأموال، والثاني هو الخطر الذي يصيب الشركات أيضاً عبر التلاعب بمعلوماتها أو سرقتها، وتضم هذه المعلومات بيانات عملائها أو أسرارها التجارية، والتي تمّثل عناصر القوة لدى الشركة وأحد أسباب بقائها وقدرتها على المنافسة.

ج–مستوى الخطر الاقتصادي: يحدّد هذا المستوى الآثار الاقتصاديّة التي تنعكس بشكلٍ مباشرٍ في خسارة المبيعات نتيجة الخطر الإلكتروني، أو بشكلٍ غير مباشر فيما يسمى فقدان الصورة والسمعة، والحقيقة أنّ السمعة هي معيار تكوين الرّبح والخسارة؛ لذلك فإنَّ انخفاض مستويات المبيعات يعني تدهور الصورة التي صنعتها الشّركة لنفسها.

د–مستوى الخطر المجتمعيّ: ويوضّح هذا المستوى البعد المجتمعي الذي ينشأ من تقنيات المعلومات والاتصالات والإنترنت، ويضمّ هذا البعد الإرهاب الإلكترونيّ وحرب المعلومات والتجسّس الصّناعيّ وغيره من المخاطر التي تلقي بظلالها على المجتمع ككلّ، وتؤثّر فيه ككتلةٍ واحدةٍ، فحرب المعلومات تهدف إلى تدمير الأنظمة المعلوماتيّة على مستوى البلاد ككلّ على سبيل المثال.

وبعد البحث في هذا النوع يمكن القول إنّ هذه الأخطار ورغم هذه الأبعاد التي ترسمها _والتي قد يُعتقد أنّها منفردةٌ لوحدها بشكلٍ مستقلّ_ إلّا أنّ ذلك لا يغدو أن يكون عملاً أكاديميّاً بحتاً؛ لأنّ الأبعاد تظهر كمجموعةٍ واحدةٍ عند حصول هجومٍ إلكترونيٍّ على شركةٍ ما، فيبرز هذا الهجوم فشل الشّركة في حماية بياناتها، ويؤدّي إلى

كشف خصوصيّة الأفراد ونزول أسهمها في السّوق، وبالتّالي ترك حالة من الخوف لدى أفراد المجتمع من المخاطر الإلكترونيّة.

2-تبعاً لدور الفرد في تحقّق المخاطر[133]:

فالخطر الإلكترونيّ يُقسم إلى خطرٍ عمديّ، حيث يتمّ ارتكاب الفعل مع نيّة إحداث الضّرر كأفعال الاحتيال والسّرقة الإلكترونيّة وتخريب الشّبكات العمديّ، وخطرٍ غير مقصود يتحقّق نتيجة إهمالٍ أو خطأٍ كإهمال الموظّف ودخوله موقعاً مشبوهاً ممّا يؤدّي إلى إدخال الفيروسات إلى الحاسب، وخطرٍ ينطوي على عدم حسن التصرّف بالأجهزة الإلكترونيّة؛ نظراً لنقص المهارات التقنيّة المعلوماتيّة.

3-تبعاً لسبب المخاطر[134]: يُنسب خطر الإنترنت إلى فشل النّظم، فقد يكون سبب الخطر هو المعدّات الماديّة المستخدمة في الشّركة، فقد تُصاب بعطلٍ ما يُسهّل إصابتها بالأخطار كعدم الصّيانة الدّوريّة، وقد يكون السبب هو البرمجيّات (software)؛ أي أصول البرامج المستخدمة والتطبيقات وأنظمة التّشغيل نتيجة عدم تطبيق ممارسات الأمان المطلوبة من جدرانٍ ناريّةٍ، وكلمات مرورٍ، وقنواتٍ آمنةٍ للاتصال، والسبب الثالث قد يكون بسبب إخفاقٍ في الأنظمة في تقديم الأداء المتوقَّع منها.

4-تبعاً لطبيعة المخاطر[135]: فقد تحصل المخاطر بفعل حدثٍ خارجيٍّ مثل الكوارث سواء بتدخّلٍ بشريٍّ أم طبيعيٍّ، أو بالمشكلات القانونيّة نتيجةً لمخالفة أحد القوانين، أو بمشكلاتٍ عمليّةٍ نتيجة تغيّر بيئة عمل الشّركة أو اعتماد الشّركة على أطرافٍ خارجيّةٍ، **والحقيقة أنَّه لو كان سبب الخطر الإلكترونيّ كارثةً طبيعيّةً، فهو غير قابلٍ للتّأمين كما تذهب إليه كثيرٌ من شركات التّأمين ضدّ مخاطر الإنترنت.**

وفي ختام الحديث عن مفهوم مخاطر الإنترنت، يُتوصَّل إلى نتيجةٍ أنّ الخطر يُعدُّ إلكترونيّاً عندما يتمّ بوسيلةٍ إلكترونيّةٍ، ويصيب عناصرَ إلكترونيّةً، كالأنظمة والبيانات، وتتميّز بكونها مخاطرَ افتراضيّةً، وغير محدّدة، ومجهولة، وصعبة التتبّع، كما أنّ ارتكابها هو أمرٌ مقصودٌ وعملٌ يمتهنه المجرمون الإلكترونيون

---

[133] Biener, C., Eling, M., Wirf, J. H. (2015). P5.

[134] Ibid, P5.

[135] Ibid, P5.

حول العالم؛ لسهولة عمليّات الاختراق، ورغبةً بالإضرار بالشّركات، إذ إنّ خسائرها كبيرةٌ وباهظةٌ ممّا يؤدّي لإفلاس الشّركات المتضرّرة. وبعد التوصُّل لتحديد تعريفٍ معيّنٍ لخطر الإنترنت والبحث في أحكامه الأخرى، يُنتقل في المطلب الثاني للبحث في دوافع مخاطر الإنترنت الأكثر شيوعاً من أجل الإضاءة عليها وبيانها، ومن ثمّ بيان صور هذه المخاطر.

المطلب الثّاني

دوافع مخاطر الإنترنت وصورها

والدوافع هي الأسباب التي قد تُغري مهاجمي الإنترنت لارتكاب الهجمات الإلكترونيّة، وتمثّل الغاية التي تبرّر الأفعال الإجراميَّة التي يرتكبها المخترقون الإلكترونيّون حول العالم (الفرع الأوّل)، وتتعدّد صور مخاطر الإنترنت تبعاً للوسائل التي يستخدمها المجرمون الإلكترونيون (الفرع الثاني).

الفرع الأوَّل

دوافع مخاطر الإنترنت وطرق الاستفادة من البيانات المسروقة

تُعدُّ الدَّوافع الأسباب التي تقف وراء مخاطر الإنترنت، فلا بدَّ من وجود دوافعَ شخصيّةً أو اقتصاديّةً تحرّك المجرمين الإلكترونيين، وتغريهم بارتكاب هذه الأفعال الإجراميَّة لأجل الاستفادة ممَّا يحصلون عليها من بياناتٍ ومعلوماتٍ شخصيّةٍ وماليّةٍ وغيرها، ممَّا يمكن بيعه في السّوق السّوداء.

أولاً: دوافع مخاطر الإنترنت:

وهذه الدّوافع هي مثار تساؤلٍ لدى الجميع، فالشّركات تتساءل لِمَ قد تكون هدفاً للمخترقين، ولماذا قد يرتكب الأشخاص هجماتٍ إلكترونيةً؟

في الواقع توجد أسبابٌ كثيرةٌ وراء ارتكاب الأفعال الإجراميَّة عبر الإنترنت ومنها:

1-البداية مع الشّركات التي تقوم الآن بأعمالها كلّها، وتخزّن بياناتها عبر الحواسب أو عبر رفع بعض ملفّاتها على غوغل درايف، فهذه الشّركات تغري المهاجمين بسرقة بياناتها من أجل بيعها للطّرف المنافس مثلاً، ويتمّ تفصيل ذلك عند البحث في تحديد المستهدف في الهجمات الإلكترونيّة لاحقاً.

2-أمّا عن الدوافع التي تقف وراء ارتكاب المهاجمين لأفعالهم الإجراميّة عبر الإنترنت، فتتعدّد هذه الأسباب تبعاً لغاية المهاجم، وبالمجمل تُقسم إلى دوافعَ شخصيّةٍ واقتصاديّةٍ وسياسيّةٍ:

أ-دوافع شخصيّة: ويبرز هذا الدّافع لدى بعض المهاجمين الذين يهدفون إلى إثبات الذات في بعض الأحيان، وأحياناً أخرى لتنبيه الشّركات إلى بعض الثّغرات التي تنتاب أنظمتها. وغالباً ما يكون هؤلاء المخترقون

من صغار السن والذين يريدون أن يثبتوا لمجتمعهم ورفاقهم أنّهم قادرون على القيام بعمليات الاختراق دون أن يكون لديهم أيّ نيّةٍ إجراميّةٍ إلّا تحقيق الشهرة والتباهي بقدراتهم الخاصة، أو قد يكونون مجرّد أشخاصٍ غايتهم توجيه النّظر إليهم من قبل بعض الشّركات الرّائدة، عبر تعطيل أنظمتهم لبضع ساعاتٍ أو اختراق نظامهم دون القيام بأيّ عملٍ آخر من أجل لفت نظر الشركة نحو بعض الثغرات التي يجب تلافيها، وعن طريق ذلك قد يكسب هؤلاء فرصة العمل لدى هذه الشركة. وبعيداً عن هؤلاء قد تكون بعض الأفعال مرتكبةً من أشخاصٍ عامّةٍ يستغلّون الإنترنت من أجل توجيه الإساءة نحو شخصٍ ما بدافعٍ تشهيريٍّ فقط، كارتكاب أعمال التشهير والنقد الموجّهة نحو شركةٍ ما من أجل تقليب الرّأي العام ضدّها، أو قد يكون هدف الهجوم الإلكترونيّ ما يسمّى بتحقيق العدالة الاجتماعية، فيما إذا كانتِ المؤسّساتُ المهاجمةُ تمارس ممارساتٍ ضدّ العدالة الاجتماعيّة في نظر المهاجم، أو تملك معلوماتٍ حيال هذا الموضوع، ويرى المهاجم وجوب فضحها للعامّة، كاختراق مواقع الوزارات أو المجالس النيابية أو المفاعلات النّوويّة كردٍّ فعلٍ من الأفراد لممارسات دولةٍ ما تجاه دولتهم، كاختراق قراصنة إيرانيين لموقع مكتبة الإيداع الفيدرالية الأمريكيّة مطلع الشّهر الأول من عام 2020 في تهديدٍ موجّهٍ للحكومة الأمريكيّة على أنّه مجرّد مثالٍ صغيرٍ على قدرتهم على الاختراق عبر الإنترنت وكردٍّ على سياسة أمريكا تجاه إيران[136].

ب–دوافع اقتصادية: وهذه الدوافع قد توجد لدى الأفراد المخترقين أو الشركات أيضاً، فالأفراد غالباً ما يشكّلون جماعاتٍ إجراميّةٍ تكون غايتها ارتكاب أفعال القرصنة، أو الاختراق والابتزاز لغاياتٍ ماليّةٍ؛ أي أنَّ هذه الجماعات باتت تمتهن هذه الأفعال من أجل الحصول على رزقها، فتقومُ مثلاً بتشفير بيانات الشّركة وتطلب فديةً من أجل إطلاق سراحها، وإلّا فنشر البيانات على الإنترنت سيكون الخيار الآخر. وقد تكون هذه الجماعات تابعةً لبعض الشرّكات؛ إذ ترتكب عمليّات الاختراق من أجل سرقة البيانات التي تملكها الشّركات المنافسة والاعتداء على حقوق الملكيّة الفكريّة والصّناعيّة وغيرها من أشكال المخاطر، فتقوم الشّركات بتوظيف بعض المخترقين

[136] https://www.arageek.com/tech/%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%85%D9%88%D9%82%D8%B9-%D8%A3%D9%85%D8%B1%D9%8A%D9%83%D9%8A

تاريخ الزيارة: 29\5\2020, الساعة 5:15 p.m.

لديها للتجسّس على منافسيها والوصول إلى بياناتهم وأسرارهم التّجاريّة وفضحها من أجل هزّ ثقة عملائها وإخراجها من السوق. والدوافع لدى الطّرفين هنا هي جني المال فقط بطرقٍ غير مشروعة، وعادةً ما يكون مرتكبو هذه العمليات من خبراء المعلوماتية الذين يسخّرون قدراتهم في ارتكاب الجرائم الإلكترونيّة.

ج–دوافع سياسيَّة: وكما قيل سابقاً إنّ الدول تحاول استخدام الإنترنت كوسيلةٍ للسيطرة على غيرها من الدّول، كارتكاب أفعال التجسّس أو اختراق بعض شبكات البنية التحتية في ظلِّ حربٍ قائمةٍ بين الدّول من أجل إضعافها وتشتيتها، بالإضافة إلى بعض الدوافع الاقتصادية التي تدفع الدّول إلى انتهاك خصوصيّة بعض الدّول من أجل سرقة معلوماتٍ عسكريّةٍ أو اقتصاديّةٍ أو صناعيّةٍ. ومن الأمثلة على ذلك ما قامت به مجموعةٌ من القراصنة الصينيين التابعين للحكومة الصينية في مطلع عام 2020 من اختراق أجهزة حواسيب تابعةٍ لمتعاقدٍ مع البحرية الأمريكيّة وسرقة ما يقارب 614 غيغابايت من البيانات الحسّاسة حول الحرب في البحار ومعلوماتٍ أخرى تتعلّق بتطوير صواريخَ مضادّةٍ للسّفن من مخطّطاتٍ للبحرية الأمريكيّة[137].

ثانياً: الاستفادة من البيانات المسروقة:

عندما تكون السرقة الهدف الرّئيس للاختراق، تُعدّ كلمات المرور والمعلومات الشّخصيّة وأرقام بطاقات الائتمان الكنز المسروق والبطاقة الرّابحة في يد المُخترقين، ولكن كيف يمكن لهم أن يستفيدوا منها؟ أو بشكلٍ آخر ما وسائلهم لوضع هذه المسروقات موضع التّنفيذ والاستغلال؟

يوجد في نطاق سرقة قواعد البيانات ما يُسمَّى **بهجوم تكديس البيانات**، ويُراد بهذا الهجوم أن يقوم المخترق بتحميل قواعد البيانات والمعلومات التي تحوي على أكبر عددٍ ممكنٍ من أسماء المستخدمين، وكلمات المرور الخاصة بهم، وبطاقات ائتمانهم، ومن ثمّ إدخالها في أداة اختراقٍ مؤتمتةٍ لاختبارها على مجموعةٍ واسعةٍ من مواقع الويب والتّطبيقات المحمولة، وكلَّما زاد عدد كلمات المرور كلَّما زادت احتماليَّة العثور على كلمة مرور الصّحيّة. وبعبارةٍ أخرى، يعني ذلك أنَّ القواعد المسروقة بكلِّ ما فيها تُوضَع على أدواتٍ تقوم تلقائياً بالعمل على تجربة هذه الكلمات المسروقة على مواقع الإنترنت جميعها، كاستخدامها على مواقع المحادثة، أو التجارة

---

[137] https://www.dw.com/ar/

تاريخ الزيارة: 29\5\2020, الساعة 6:10 p.m.

الإلكترونيّة، أو تطبيقات السّياقة، والمغزى أنَّ كثيراً من الأفراد يستخدمون كلمة المرور نفسها على حساباتٍ متعدّدةٍ في تطبيقاتٍ مختلفةٍ، كاستخدام البريد الإلكتروني وكلمة السرّ ذاتهما على موقع فيسبوك، وفي غوغل، وفي أحد الحسابات البنكية مثلاً، فعند الحصول على أحد كلمات المرور ستكون نسبة الوصول إلى حسابات المستخدم على مواقعَ أخرى كبيرةً، وبالتَّالي ستزداد قواعد البيانات التي سيملكها المخترق. ومع أنّ المبدأ هذا قد يبدو صعباً ربّما، لكنّه السائد في كثيرٍ من الاختراقات حول العالم، فبين كلّ مليون محاولة اختراق توجد 30 ألف محاولة ناجحة، وإنّ 90% من محاولات تسجيل الدخول على مواقع التجارة الإلكترونية كانت من هجمات تكديس البيانات، وليس من المتسوّقين شخصيّاً، ويليها مواقع خدمات الطّيران، ومن ثمّ المواقع البنكيّة، إذ تخسر المصارف حوالي 1،7 مليار دولار سنوياً من هذه الهجمات، وعلى سبيل المثال: يمكن الاستفادة من هذه البيانات المسروقة بالقيام بعمليّات احتيالٍ عبر الإنترنت، فيظهر المخترق بصفة المستخدم الشرعي ويقوم بالشراء عبر الإنترنت من أحد المواقع، ثمّ يتفاجأ المستخدم بالفواتير التي تصله، أو قد تستخدم البيانات من أجل القيام بعمليّات تحويلٍ بنكيةٍ احتياليةٍ إلى حساباتٍ تتبع للمخترق، أو تزوير أحد بطاقات الدّفع واستخدامها من قبل المخترق بدلاً عن المستخدم في دفع فواتيره، ويمكن استخدام المعلومات الشّخصيّة في تزوير جوازات سفرٍ، أو بطاقات شخصيّةٍ، أو الدّخول على حساب تويتر باسم المستخدم الضّحيّة والتّغريد نيابةً عنه، وهذه الأمثلة كلّها تحصل في الواقع العمليّ، وتتعدّد إلى مجالٍ لا حصرَ له[138].

ولا يختار كل المخترقين استخدام البيانات هذه لدوافع شخصية بحتة _إن جاز القول_ بل يقوم بعضهم _وفي سبيل الإضرار بشكل أكبر بالشركة_ بعملية بيع هذه البيانات على الإنترنت، فيعرضها على مواقع الإنترنت بأثمانٍ بخسةٍ مقارنةً بأهمية المعلومات، ولا سيما مساسها بالحياة الشخصية للعملاء، وحق الخصوصية الذي تحميه القوانين حول العالم. ولا يخفى على أحد مقدار الضرر الذي يجلبونه للشركة عبر بيع قواعد بياناتها على الإنترنت، لأن ذلك من شأنه أن يهزَّ ثقة عملائها بها نتيجة لعدم حسن تعاملها مع المعلومات، وعدم تحديث وسائل أمانها، وهو ما يعرّضها لكثيرٍ من الدعاوى القضائيّة نتيجة المسؤوليّة العقديّة والتقصيريّة التي قد

---

[138] https://www.aitnews.com

تاريخ الزيارة: 29\5\2020, الساعة 10:15 p.m.

تترتب، عدا عن الغرامات والعقوبات التي تفرضها عليها السلطات القضائية، ولا سيما إذا ما ظهر تقصير أو إهمال من جانبها، ناهيك عن الخسائر المادية التي قد تتكبدها الشركات من أجل استرجاع البيانات المسروقة، حيث يجب الاستعانة بخبراء لتصحيح الخلل، وإعادة بناء الأنظمة المخترقة. و أما عن ثمن هذه البيانات فهو سعرٌ صادمٌ، إذ تتحدث بعض التقارير عن بيع الهويات الرقمية بأكملها بمبلغ 50 دولاراً، وتضم هذه الهويات بيانات حسابات مواقع التواصل الاجتماعي، وتفاصيل مصرفية، وخدمات عن بعد، ومواقع ألعاب إلكترونية، والتي بدورها تخزن أرقام بطاقات الائتمان[139]، وربما تكون البيانات البنكية الأغلى سعراً بين كل البيانات، فحسب إحدى مواقع الويب المظلم في 2018 وصل سعر بيانات موقع paypal إلى 710 دولاراً؛ نظراً لأهميّة هذا الموقع وخصوصيّته، في حين قد تُباع بيانات حساب فيسبوك ب 5 دولارات فقط، أمّا حساب gmail فقد يُباع بدولار![140]. وفي أحد الحوادث عن بيع البيانات، ما حصل مع شركة زوم المخصّصة لاتصالات الفيديو في نيسان 2020 من عمليّات تسريب بيانات أكثر من 500 ألف مستخدمٍ عبر هجمات تكديس البيانات، ومن ثمّ بيعها على أحد منصّات القراصنة مقابل نصف بنس لكلِّ بيانٍ منها، فاشترت الشّركة حوالي 530 ألف بيان مقابل 0،002 دولاراً لكلٍّ منها، كما أنَّ بعضها قد وُزِّع بالمجّان، وتضمّ البيانات عناوينَ بريدٍ إلكترونيٍ، وكلمات مرور، وشفراتٍ، وغيرها[141]. والحقيقة أنّ الأمر يتجاوز كونه مجرّد تجارة بهذه البيانات إلى كونه فضيحةً حقيقيّةً تلاحق الشّركات المستهدفة، فليس بالسّهل عليها تلقّي وتبرير هذا الحادث أمام مستخدميها.

وكما يظهر سؤالٌ آخرُ هنا هو تحديد مَن المستهدف بأخطار الإنترنت؟

تظنّ العديد من الشّركات أنّها بمنأىً عن الأخطار الإلكترونيَّة، وهذا ما يُعدّ أحد أكبر الأخطاء التي قد ترتكبها الشركات بحقِّ نفسها، إذ تضع نفسها وسط المخاطر دون أن تعدّ الحماية اللازمة لمواجهتها. وبحسب إحصائياتٍ أُقيمت بين عامي 2014-2018 تبيّن أنَّ أكثر القطّاعات المتضرّرة من الاختراقات هي: قطاع

---

[139] https://www.aawsat.com

تاريخ الزيارة: 29\5\2020, الساعة 11:30 p.m.

[140] https://www.youm7.com

تاريخ الزيارة: 29\5\2020, الساعة 11:45 p.m.

[141] https://www.al-ain.com/article/zoom-scandal-600-users-sale-hacker-forum

تاريخ الزيارة: 29\5\2020, الساعة 11:55p.m.

الأعمال (المشاريع التجاريّة)، والقطاع الطبيّ (المنظّمات الطّبيّة والصّحيّة)، يليها القطّاع الماليّ والمصرفيّ، وأخيراً القطّاع الحكوميّ، والعسكريّ.

1- يمثّل قطّاع الأعمال فئةً واسعة النّطاق لا سيّما أنّها تضمّ التّجارة الإلكترونيّة بالمعنى الواسع وقطاع التّجزئة، وتتعرّض هذه الشّركات للتّهديد نتيجة البيانات الماليّة والشّخصيّة التي تخزّنها وتعالجها. وقد تعتقد بعض الشركات الصغيرة أنّها غير مستهدفة، لكنَّ الحقيقة تثبت عكس ذلك لا سيّما أنّ الإحصائيات تقول إنَّ حوالي 14 مليون شركة صغيرة قد تعرّضت لخروقاتٍ خلال العام 2017، ولكنّ المشكلة في أنّ هذه الشركات لا تملك المقدرة اللازمة لحماية نفسها، بخلاف الشركات المتوسطة والكبيرة التي تملك البنية التّحتيّة لإيقاف الهجمات الإلكترونية.

2-في حين يعد قطاع الرّعاية الصّحيّة والطّبيّة هدفاً آخرَ للمجرمين الإلكترونيين؛ لما تملكه منظّمات الرّعاية من بنوك بيانات خاصّة لسجلّات الرّعاية الطّبيّة الإلكترونيّة بما فيها من معلوماتٍ ماليّةٍ وشخصيّةٍ مثل المشافي، وما تملكه من معلوماتٍ حسّاسةٍ سريّةٍ عن المرضى لديهم، ومن أمثلة الهجمات تدمير فايروس لعمليات خدمة الصّحّة البريطانيّة والتّأثير سلباً على صحّة المرضى.

3-ما يتعلّق بالقطّاع المصرفيّ، فهو شديد الوضوح كهدفٍ للمخترقين؛ لما يملكه من أموالٍ قابلةٍ للسّرقة عبر التّحويلات الإلكترونيَّة، بالإضافة إلى المعلومات الشَّخصيَّة للعملاء، والتي قد تُسرَق وتُستَغلّ في ابتزاز الشّركة لعدم نشرها أو بيعها أو استخدامها في أعمال الانتحال، ورغم اعتقاد الشركات أنّها تلتزم بخططٍ للأمن السيبرانيّ، لكنَّ الحقيقة تُثبت عكس ذلك؛ إذ إنَّ واحدةً من كلِّ ثلاث شركات تُخترق بنجاح.

4-وفيما يتعلّق بالقطّاع الحكوميّ وما يحتويه من معلوماتٍ على قدرٍ عالٍ من السّريّة والأهميّة فلا يُستغرَب أن يكون من أحد القطّاعات المستهدفة، والحقيقة أنَّ الهجمات الإلكترونيَّة قد ترتكب من قبل دولٍ بغيةَ التجسّس على أعدائها والتّأثير عليهم، مثل الاعتداء على الأنظمة العسكريّة بما يُهدّد أمنها، وقد يهدف المجرم الإلكتروني إلى الحصول على معلوماتٍ سريّةٍ من أجل ابتزاز الحكومات لعدم الإدلاء بها للعامّة.

5-ولا يغيب عن الذّكر المؤسّسات التّعليميّة التي تتعرّض للهجوم وسرقة أبحاثها في اعتداءٍ إلكترونيٍّ على حقوق الملكيّة الفكريّة للباحثين، بالإضافة إلى المعلومات الشّخصيّة للطلّاب والموظّفين، وقد تعرّض التّعليم العالي بحسب إحصائياتٍ بين عامي 2005-2015 إلى 539 خرقاً بما يقرب حوالي 13 مليون سجلٍّ مفقودٍ أو مخترقٍ.

6-قطّاع الطّاقة والمرافق العامة: تُعدّ أحد الأهداف الاستراتيجيّة للمجرمين الإلكترونيين عبر اختراق شبكات البنية التحتية كالنّقل أو الطّاقة الكهربائيّة بما ينعكس سلباً على المواطنين ويهدّد حياتهم، كما لو تمّ تعطيل أحد مرافق الطّاقة النووية، وهو ما قد يُهدِّد بانفجارها أو قطع الكهرباء عن مدينةٍ ما[142].

7-قطّاع تكنولوجيا المعلومات أيضاً: يُعدّ أحد القطّاعات المستهدفة، فمقدّمو خدمات التّخزين السّحابي ومطوّرو برامج الأمان ومزوّدو خدمات الإنترنت يشكّلون أحد أهداف المخترقين؛ نظراً لما يخزّنونه من معلوماتٍ حسّاسةٍ على حواسيبهم وأنظمتهم، فالهدف المباشر للاختراقات هو الوصول إلى عمليّات وبيانات الشّركات، أمّا الهدف غير المباشر فهم المشتركون في قطّاع الاتّصالات من أجل التّحكّم بهم وانتحال صفتهم.

8-القطّاع القانونيّ عرضةٌ للهجمات الإلكترونية؛ وذلك لحجم المعلومات الحسّاسة التي تُخزَّن لدى الشّركات القانونيّة والمحاكم في ظلِّ العمل عبر الإنترنت، والاتّجاه نحو التَّخزين الإلكترونيّ للبيانات.

9-بيانات الموارد البشريَّة وقطّاع التّوظيف؛ حيث يجد المنتهكون طرقهم الخاصّة في الوصول إلى الشّركات عبر اختراق نظام الموارد البشريّة لديها، فيمكن عبرها الوصول إلى أسماء الموظّفين والعناوين وتفاصيل البنك، وهو لا يؤثّر فقط على الأفراد، بل على أجزاءٍ أخرى من العمل، إذ يفتح الباب نحو اختراقاتٍ أوسع، وبهذا الاختراق تُترك عقود التّوظيف والبيانات الحسّاسة كتأشيرات السّفر _على سبيل المثال_ مكشوفةً للقراصنة لتُستغلّ على النّحو الّذي يجلب لهم المال.

---

[142] https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks/

تاريخ الزيارة: 13\5\2020، الساعة 10:45 p.m.

10-القطّاع الصّناعيّ كصناعة السيّارات والإلكترونيّات وغيرها، فلطالما كان هدفاً ذا قيمةٍ بالنِّسبة للمخترقين؛ نظراً لما لحقوق الملكيّة الفكريّة، والصّناعيّة، والأسرار التّجاريّة التي تحويها أنظمة هذه القطّاعات من قيمةٍ ثمينةٍ تجعلها هدفاً للاستغلال والبيع للمنافسين[143].

والحقيقة بعد ذكر هؤلاء المستهدفين يُتوصَّل إلى نتيجةٍ أن لا قطاع اليوم في أمانٍ من مخاطر الإنترنت، وكلّ الشّركات صغيرةً أو كبيرةً عامّةً أو خاصّةً عرضةٌ للاختراقات والبرامج الضّارّة؛ لأنَّ الاتجاه نحو أتمتة الأعمال كلّها، وازدياد إدخال الحاسب إلى القطّاعات جميعها بات أمراً لا مهرب منه، ولذلك لا بدّ من الانتباه أكثر نحو المحافظة على الأمن المعلوماتيّ الذي يتطلّب من الشّركات كلّها تحديث كلمات مرورها، والمحافظة على جدرانها النارية، وأنظمة الأمان المستخدمة، بالإضافة إلى الالتزام بالقوانين التي توجب اتخاذ إجراءاتٍ من أجل الحفاظ على الخصوصيّة في محاولةٍ لإيقاف تمدّد مخاطر الإنترنت أو على أقلّ تقدير تقليص أضرارها.

الفرع الثَّاني

صور مخاطر الإنترنت وبعض الهجمات الإلكترونيَّة تاريخيَّاً

تتعدَّد الصّور التي تتّخذها مخاطر الإنترنت تبعاً لنوع الوسيلة المستخدمة في تنفيذ الخطر أو الهدف منه، فهنالك الكثير من المخاطر التي تصيب الأفراد عبر الإنترنت، كمخاطر الابتزاز الإلكترونيّ، والقرصنة الإلكترونيّة، وتعود هذه الهجمات الإلكترونيّة قدماً إلى القرن الماضي وما زالت تتطوّر حتى يومنا هذا.

أوّلاً: صور مخاطر الإنترنت: ويُذكر من هذه الصّور الآتي:

1- البرمجيّات الخبيثة: ويُشار إلى هذه البرمجيّات باللُّغة الإنكليزيَّة باسم MALWARE ويمكن تعريف البرمجيَّات الخبيثة على أنَّها: "برامج ضارّة يتمّ تضمينها أو إدراجها عمداً في نظام الحاسب لأغراضٍ ضارّةٍ دون رضا المالك لأهدافٍ متعدّدةٍ كعرقلة عمل الحاسب أو جمع معلوماتٍ حسّاسةٍ من قواعد البيانات أو الوصول لأنظمة الكمبيوتر الخاصّة"، وهي برامج تصعب إزالتها خصوصاً أنَّها تتكاثر وتتمدَّد، ويتراوح الأذى الذي تسبّبه

[143] https://www.ifsecglobal.com/cyber-security/which-sectors-are-most-vulnerable-to-cyber-attacks/ تاريخ الزيارة: 13\5\2020، الساعة 11:45p.m.

بين أذىً بسيطٍ كالإزعاج للمستخدم عبر النَّوافذ التي تنبثق إلى أذىً شديدٍ غير قابلٍ للإصلاح عبر إعادة تهيئة القرص الصّلب، وبالتَّالي محو البيانات المخزَّنة عليه[144]، وتتَّخذ هذه البرمجيات صوراً عدّة، مثل الفايروسات، وأحصنة طروادة، والقنابل والدّيدان.

2- الابتزاز الإلكترونيّ: والابتزاز فعلٌ قديمٌ يُمارس من قِبل أشخاصٍ بهدف الحصول على مالٍ أو لأسبابٍ أخرى عبر التَّهديد بفضح الأسرار الشَّخصيَّة، ويُطبَّق على الأفراد والشّركات على السّواء، ويُشار إلى الابتزاز الإلكترونيّ بمصطلح (هجمات الفدية) ويُراد بها أنَّها إحدى أشكال البرامج الضّارّة التي تدخل على شركةٍ ما وتقوم بمنع الوصول إلى أنظمة الشّركة (تشفير البيانات) حتى تُدفَع الفدية وإعطاء رمز فكّ التّشفير، ومن المعلوم أنّ الشركات تخزّن ملايين المعلومات لا سيّما في إطار أعمال المصارف مثلاً، إذ إنّ سرقة معلوماتها وتعاملاتها تعني فضح السّريّة المصرفيّة التي يقوم عليها العمل المصرفيّ، وعمليّة الابتزاز كي تتمّ بحاجةٍ إلى اختراقٍ سابقٍ من قبل المهاجم من أجل السّيطرة على النّظام، وهو ما يحدث بإحدى البرمجيّات الخبيثة، فيُتحَّكم بالحواسيب ويهدد بتدمير البيانات أو نشرها عبر الإنترنت؛ أي أنّ الابتزاز هنا ليس موجّهاً نحو كشف المعلومات فحسب، بل قد يكون التهديد بتعديلها أو محوها بشكلٍ كاملٍ أو بيعها إلى جهةٍ منافسةٍ أو عبر الإنترنت المظلم، ونتيجةً لذلك تجد الشّركات نفسها مضطرّةً إلى دفع الفدية التي يطلبها المهاجمون من أجل ترك النظام[145].

3- مشاكل البريد الإلكترونيّ: تتعدّد هذه المشاكل ولا يمكن إحصاؤها، لكنّها في الغالب تضمّ إغراق البريد الإلكتروني والتّصيّد وهجمات إنكار الخدمة، ويُراد بالإغراق أنَّه: "إرسال كميّة كبيرة من البريد غير المطلوب للمستخدمين متضمّناً إعلاناتٍ تجاريّةً إلى أشخاصٍ ليس بينهم وبين المرسل أيّ علاقة[146]"، ويعرَّف على أنَّه: "إرسال عشرات الرّسائل عبر البريد الإلكترونيّ لشخصٍ ما أو للعديد من المستخدمين[147]"، وأبرز الأضرار التي يسبّبها الإغراق تأثيره على وظيفة البريد الإلكتروني؛ إذ يؤدّي إلى إعاقة حركة البريد وإضعافه

---

[144] https://www.en.wikipedia.org/wiki/Malware

تاريخ الزيارة: 17\5\2020، الساعة 10:50 p.m.

[145] بانقا، علم الدين. (2019). مخاطر الهجمات الإلكترونية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، عدد: 63، دراسات تنموية في المعهد العربي للتخطيط، ص 10.

[146] غنام، شريف محمد. (2008). التنظيم القانوني للإعلانات التجارية عبر شبكة الإنترنت، مصر، دار الجامعة الجديدة، ص86.

[147] داود، حسن طاهر. (2000). جرائم نظم المعلومات، ط:1، الرياض: السعودية، أكاديمية نايف العربية للعلوم الأمنية، ص93.

نتيجةً لتراكم الرّسائل غير المرغوب فيها، وتأثيره على ذاكرة الكمبيوتر بإشغال مساحةٍ من التَّخزين، وانقطاع خدمة البريد الإلكتروني نتيجة ملء منافذ الاتصال وقوائم الانتظار الخاصّة بهم أمام الزبائن، والتّكاليف اللازمة للاتصال واستقبال هذه الرسائل، بالإضافة إلى أنّ هذه الرسائل تشكّل اعتداءً على خصوصيّة الأفراد عبر اختراق بريدهم الإلكتروني وإزعاجهم برسائلَ غير مرغوبةٍ، وعاقبَ المشرّع السّوريّ على الإغراق؛ فنصَّت المادة 20 من قانون التَّواصل على الشَّبكة ومكافحة الجريمة المعلوماتيَّة السّوريّ[148] على فرض غرامةٍ بين العشرين والمئة ألف ليرة سوريّة على إرسال البريد الواغل إن لم يستطع إيقاف وصوله أو كان إيقاف وصوله يرتبط بتحمُّل المتلقّي نفقاتٍ إضافيّةً، في حين تُعرَّف هجمات إنكار الخدمة بأنّها: "إغراق الخوادم بآلاف أو ملايين الطّلبات للحصول على المعلومات"، كما لو تمّ إرسال ملايين الرسائل عبر البريد الإلكتروني بهجومٍ منظّمٍ في وقتٍ واحدٍ، ممَّا يزيد عن قدرة القرص الصلب أو قواعد المعلومات على حمله فيصيبها بالشّلل التام[149]. ويهدف الهجوم إلى جعل العميل أو الزائر غير قادر على الوصول إلى الموقع الذي يريده (جعل الموقع غير متاحٍ مؤقتاً)، وتتم عملية التعطيل دون الحاجة إلى اختراق الموقع المستهدف، بل بمجرد الإغراق، وتبدو خطورة هذا الهجوم في أنَّه لا يصيب موقعاً وحده، بل يُهدّد شبكة الإنترنت ككلّ؛ لأنّ كلّ موقعٍ يحجز جزءاً من حزمة البيانات على شبكة الإنترنت؛ ولذلك قد يسبّب تعطيل شبكة الإنترنت حول العالم نتيجة الضَّغط عليها.

4- القرصنة الإلكترونيّة: وهي وسيلةٌ غير شرعيّةٍ للدخول إلى الأنظمة واستخدامها دون إذنٍ من المالك أو المستخدم الشّرعيّ، ويبدو مفهوم القرصنة مفهوماً واسعاً؛ إذ يدخل تحت نطاقه أعمال الدخول غير المصرّح به وما يستتبعه ذلك من إفشاء الأسرار والمعلومات، وسرقة حقوق الملكيّة الفكريّة، واستخدام هذه البيانات في الأغراض غير المشروعة، وتنطوي القرصنة على الدخول والاطّلاع غير المشروع على البيانات، وقد عاقب المشرّع السّوريّ في قانون التّواصل على الشّبكة بالغرامة من عشرين إلى مئة ألف ليرة سورية على الدخول قصداً إلى جهازٍ حاسوبيٍّ أو منظومةٍ معلوماتيّةٍ أو موقعٍ إلكترونيٍّ على الإنترنت دون أن يكون له الحقّ أو يملك

---

[148] قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم (17) لعام 2012.

[149] قطب، محمد علي. (2010). الجرائم المعلوماتية وطرق مواجهتها، ج:2، البحرين، الأكاديمية الملكية للشرطة، ص8.

الصّلاحيّة أو التّصريح بالقيام بذلك مع تشديد العقوبة في حال وجود نيّة بالنّسخ أو الإلغاء أو الاستخدام أو الإفشاء[150].

ويمكن للمخترق استخدام البيانات المسروقة في القيام بعمليّات احتيالٍ أو استخدام الجهاز المخترق نفسه كمنصّةٍ للقيام بهجوماتٍ على حواسيبَ أخرى، وتُسرَق المعلومات مثلاً من أجل بيعها إلى شركةٍ منافسةٍ أو في السّوق السّوداء، أو قد يتمّ حجز البيانات وتعطيل الخدمات كوسيلةٍ لدفع الفدية، وإلّا سيتمّ إفشاؤها، كما قد يكون الاختراق بوّابةً من أجل القيام بأعمال تخريب المعلومات وإتلافها، كتدمير قواعد البيانات أو إصابة الأنظمة بفايروساتٍ تؤدّي لإتلافها بشكلٍ كاملٍ أو بشكلٍ جزئيٍّ، أو القيام بإدخال تعديلاتٍ وتغييراتٍ في المعلومات المخزّنة ما يعود بالضّرر على الشَّركة.

ثانياً: بعض الهجمات الإلكترونيَّة تاريخيّاً:

هناك من يعتقد أنَّ مخاطر الإنترنت التي تواجهها الشّركات اليوم حديثة العهد، وأنّها وليدة القرن الحادي والعشرين، ولكنَّ الحقيقة غير ذلك، ويمكن توضيحها عبر عرض بعض الهجمات التاريخية على شبكات وأنظمة الشركات حول العالم[151]:

1-التّلاعب الإلكترونيّ: في عام 1970 وعلى مدار 3 سنوات قام أحد كبار الصّرافين في أحد فروع بنك UNION DIME SAVINGS بالتلاعب بنظام الحاسب في البنك، وقام بسرقة حوالي مليون ونصف المليون دولار من حسابات مئات العملاء.

2-تصميم بوب توماس لفايروس (كريبر) الذي أصاب بعض أنظمة ARPANET [152]، بالإضافة إلى تجربته على أنظمةٍ أخرى مملوكةٍ لمنظّماتٍ أخرى.

---

[150] المادة (15) من قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم (17) لعام 2012.

[151] Akhgar, B., Staniforth, A., & Bosco, B. (2014). Cyber Crime and Cyber Terrorism Investigator's Handbook, Rotterdam: Netherlands, Elsevier Inc, p20.

[152] وهي وكالة مشاريع البحوث المتقدمة الكاملة وشبكة كمبيوتر تجريبية كانت رائدة الإنترنت. حيث قامت وكالة مشاريع البحث المتقدم (ARPA)، وتعدّ ذراعاً لوزارة الدفاع الأمريكية، بتمويل تطوير شبكة وكالة مشاريع الأبحاث المتقدمة (ARPANET) في أواخر الستينيات (1969)، غرضه الأولي ربط أجهزة الكمبيوتر في مؤسسات الأبحاث الممولة من البنتاغون عبر خطوط الهاتف، مشار إليه على الموقع الإلكتروني:

3 –في أوائل عام 1977، سرق مخترقون خلال عطلة نهاية الأسبوع المئات من أشرطة الحاسب الأصليّة ونسخها الاحتياطيّة من مركز الحاسب والتخزين الاحتياطي لشركة صناعةٍ كيميائيةٍ تسمّى (ICI)، فحاول المخترقون ابتزاز الشّركة وطلب فدية 275،000 جنيه إسترليني، وقد قيل بعد هذه الحادثة إنّ عصراً جديداً من الإجرام قد بدأ.

4–في 2 نوفمبر 1988 أطلق روبرت موريس أوّل دودةٍ حاسوبيّةٍ على الإنترنت، إذ هاجمت آلاف الحواسيب التي تستخدم نظام تشغيل UNIX، قدّر عددها ب 6 آلاف جهاز، يرتبط معها 60 ألف نظام عبر الإنترنت، وسببت أضراراً بالغةً نتيجة تعطيل العمل، فهي لم تسبب إتلاف المعلومات فحسب بل أوقفت الأنظمة عن العمل، وكلّفت خسائرَ حوالي مئة مليون دولار من أجل الإصلاح وإعادة التشغيل للأنظمة المستهدفة[153]. وفي عام 1990، أُدين موريس بموجب قانون الاحتيال وإساءة استخدام الكمبيوتر لعام 1986، وقد حُكم عليه بالسجن لمدّة ثلاث سنوات تحت المراقبة و400 ساعة من خدمة المجتمع وغرامة قدرها 10000 دولار أمريكي.

5– في عام 1994، أجرى قراصنةٌ مجموعةً من التّحويلات المصرفيّة قُدِّرت ب 40 تحويلاً وبلغ مجموعها أكثر من 10 ملايين دولار أمريكي من مصرف (CITY BANK) إلى مجموعةٍ من الحسابات المصرفية في فنلندا، وروسيا، وألمانيا، وهولندا، والولايات المتّحدة، وسويسرا، وغيرها، ولحسن الحظّ تمكّن المصرف من استرداد الأموال جميعها باستثناء 400 ألف دولار.

6– في عام 1995، جرت أولى محاولات التّصيّد، ويعدّ التّصيّد إحدى وسائل الاحتيال الإلكترونيّ الأكثر شيوعاً[154].

---

https://www.marefa.org/%D8%A3%D8%B1%D9%BE%D8%A7%D9%86%D8%AA

تاريخ الزيارة: 5\5\2021، الساعة 7:45 p.m.

[153] الحسيناوي، علي جبار. (2018). جرائم الحاسب والإنترنت، عمان: الأردن، دار اليازودي للنشر والتوزيع، ص2.

[154] ويعرّف التصيد على أنّه "محاولة احتيالية للحصول على معلوماتٍ سريّةٍ من مستخدم بريدٍ إلكتروني، وتكون الرسائل المزيّفة مرسلة من مواقعَ مزيّفةٍ مقلّدةٍ للمواقع الشرعية الحقيقية، أو مزودي خدمات الإنترنت، بحيث ينخدع بها المبعوث إليه وتطلب منه الكشف عن معلومات حساسة ككلمات المرور، ومعلومات بطاقات الائتمان، وبطاقات التعريف الشخصي وغيره"، مشار إليه على الموقع الإلكتروني:
https://www.youm7.com/story/2019/10/7/5-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82%D8%A7%D8%AA-

7- في عام 1997، أُنشئ مسرح الاعتصامات الإلكترونيّة (EDT) في المكسيك، وقد أُنشِئ هذا المسرح لإيجاد نسخةٍ إلكترونيّةٍ من الاعتصامات على الإنترنت، ويضمّ هذا المسرح مجموعةً من النّشطاء السّياسيّين الذين يتّخذون هذه المنصّة كوسيلةٍ للتّعبير عن رأيهم بعيداً عن العنف. وفي 10 أبريل 1998، تمّ استخدام أداة Floodnet الخاصّة بهم من قبل المتظاهرين من العديد من الدول للقيام بهجمات إنكار الخدمة على الموقع الإلكتروني لرئيس المكسيك، ولاحقًا في البيت الأبيض، حيث اعتمدوا على نسخ عنوان URL لفتراتٍ قصيرةٍ متعددةٍ بشكلٍ متكررٍ ممّا سبّب بطئاً في الموقع ومن ثمّ تعطيله.

8- في عام 2005 أُخترِق نظام تكييف الهواء لمركز الحاسب في أحد البنوك الأوروبيّة عمداً، ممَّا أدَّى إلى زيادة درجة حرارة غرفة الكمبيوتر ببطءٍ، وبالتالي تسبّب في إيقاف تشغيل خدمات نظام الحاسب جميعها.

9- في عام 2006، بدأت شبكة الأعمال الرّوسيّة (RBN) أعمالها[155]، وبعد فترةٍ وجيزةٍ من بدايتها كانت RBN نقطةً مركزيّةً لتقديم أدوات وخدمات الجرائم الإلكترونية للرسائل غير المرغوب فيها والتصيد الاحتيالي وأحصنة طروادة.

وتطول القائمة في تعداد نماذج مخاطر الإنترنت، وإن كانتِ الحوادث المذكورة مجرّد أمثلة على المخاطر الإلكترونيّة التي تتعرّض لها الشّركات منذ أواخر القرن العشرين، وبالتالي فإنّ الهجمات الإلكترونيّة الآن ليست إلّا امتداداً للأفعال الإجرامية القديمة، ولكنَّها أكثر شراسةً تبعاً للتطور التكنولوجي الهائل رغم محاولات الأمان كلّها التي تتّبعها الشركات.

%D8%A3%D9%85%D9%86%D9%8A%D8%A9-%D8%AD%D8%AF%D9%8A%D8%AB%D8%A9-%D8%AA%D9%87%D8%AF%D8%AF-%D9%85%D8%B3%D8%AA%D8%AE%D8%AF%D9%85%D9%89-%D8%A7%D9%84%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9/4447681

تاريخ الزيارة: 5\5\2021، الساعة 8 p.m.

[155] RBN هي شبكة الأعمال الروسية التي بدأت عملها في 2006 كشبكة أعمال مشروعة، لكن سرعان ما تغير ذلك وبدأت تتجه نحو تبني الأعمال الإجرامية الإلكترونية، فتعد كشركة مستضيفة للأعمال غير القانونية كالتصيد، والبريد المزعج، وهجمات إنكار الخدمة، وسرقة الهويات الشخصية مقابل إعادة بيعها، وتوزيع البرمجيات الخبيثة، وتأخذ مقابل هذه الهجمات حوالي ال600 دولار شهرياً، مشار إليه على الموقع الإلكتروني:

https://www.en.wikipedia.org/wiki/Russian_Business_Network

تاريخ الزيارة: 16\5\2020، الساعة 12:15a.m.

وبعد دراسة الدوافع ووسائل استغلال البيانات المسروقة، والاطلاع على أمثلة الهجمات الإلكترونيّة في التاريخ، يدور التساؤل الآتي حول النتائج التي تلحقها مخاطر الإنترنت بالشّركات المستهدفة، لا سيّما أنّ كلّ المخاطر غالباً ما تُسبّب عمليّة إفشاءٍ غير مشروعٍ للبيانات المخزّنة؟

فعندما يقوم المجرم ببيع المعلومات على شبكة الإنترنت فهو لا يهدف فقط إلى كسب الأموال، بل إلى الإضرار بالشركات وتحميلها خسائرَ كبيرةً، وتُقسم هذه الخسائر إلى مباشرة وغير مباشرة[156]:

1-الخسائر المباشرة: وهي التي تصيب الشركة بشكلٍ مباشرٍ نتيجةً لأخطار الإنترنت، ورغم تعدّد أشكال الخسائر نتيجةً لتعدّد المخاطر، لكن في الغالب تنتج الخسائر الآتية:

أ- تكاليف الاستجابة للخروقات، يتضمّن ذلك الاستعانة بخبراء أمن معلومات وتكنولوجيا داخليين من الشّركة نفسها أو خارجيين لتحديد سبب الخطر؛ أي لتحديد ما الذي حصل بالضبط، وإعادة الوضع إلى ما كان عليه، وما يستلزمه ذلك من شراء معدّاتٍ، وأنظمةٍ أمنيّةٍ جديدةٍ لسدِّ الثّغرات.

ب- نفقات تعويض الأفراد المتضرّرين من الاختراقات بما فيها تكاليف الإخطار للعملاء الذين تمّ إفشاء معلوماتهم الشّخصيّة، وإدارة الاستفسارات، وتقديم الدّعم اللازم، وخدمات مراقبة الائتمان، وأيّ نفقاتٍ أخرى يستلزم دفعها من الشّركة لعملائها.

ج-النفقات القضائيّة بشقّيها سواء ما كان منها غرامات تفرضها القوانين نتيجةً لانتهاك الخصوصيّة المعلوماتية، أو الدّعاوى القضائيّة التي تُرفَع على الشّركة بسبب الخرق، وما ينتج عنها من نفقات تسويةٍ، أو خسارة هذه الدّعوى ووجوب دفع التّعويضات والغرامات.

د-الخسارة النّاتجة عن سرقة الأصول الماليّة من العملات، والتّحويلات، والأنظمة المتضرّرة من الخرق، بالإضافة إلى الإيرادات المفقودة نتيجة تعطّل العمل، كما لو استمرَّ حجب الخدمة لساعاتٍ عدّة أو أيّامٍ، ما يسبّب ساعاتٍ ضائعةً وإيراداً فائتاً.

---

[156] Coburn, A., Leverett, E., & Woo, G. (2018). p 8-9-10.

2-الخسائر غير المباشرة: قد تكون الخسائر غير المباشرة أكثر ضرراً وأشدّ على الشركات من خسائرها المباشرة، وتتمحور هذه الخسائر بصفةٍ عامةٍ حول تضرّر سمعة الشّركة نتيجة حوادث الخرق، وينتج عنها ما يلي:

أ-فقدان ثقة العملاء ونقل أعمالهم إلى شركاتٍ أخرى، إذ إنّه حوالي 31% من المستهلكين قد توقّفوا عن العمل مع الشّركة المخترقة.

ب-استقالة كبار المديرين في الشّركة المسؤولين عن ضعف الأنظمة الأمنيّة، والثّغرات المسبّبة لنجاح الخروقات لتفادي المسؤولية القانونية الواقعة عليهم، وهو ما حصل مع بنك بنغلادش في عام 2016 عندما تمّ اختراقه وسرقة حوالي 80 مليون دولار، ما سبّب استقالة حاكم المصرف نتيجة لذلك.

ج-تراجع إيرادات الشّركة وخسارة فرص الأعمال، فثلث الشّركات التي عانت من اختراقاتٍ شهدت فقدان أرباح، وبعض الشّركات كانت خسائرها تزيد عن 20 % من أرباحها السنوية _وهو معدّلٌ مرتفعٌ_ إذ إنّ الشّركة لا تكون قادرةً بوضعها الحالي على المنافسة وهي تسعى لإخراج نفسها من مأزق الخروقات والخسائر الهائلة، بالإضافة إلى انخفاض قيمة أسهمها في الأسواق الماليّة، ففي بعض الأمثلة شهدت الشّركة انخفاض 5% من أسعار أسهمها بعد تعرّضها لخرقٍ ما، كما أنّ حالات الخروقات تؤدّي إلى خسارة حقوق الملكية الفكريّة التي تملكها الشّركة، وهو ما يؤدّي إلى تهديد بقائها في السّوق والقدرة على المنافسة.

د-إفلاس الشّركة، وهو ما قد يحصل كنتيجةٍ نهائيّةٍ لما يلحق بالشّركة من خسائرَ جمّةٍ نتيجة الخروقات، فالنّفقات التي تلزم بدفعها لإصلاح الأمور المخترقة، وتعويض العملاء، وما يلحقه الضّرر بسمعة الشّركة وتوابعه، كلّها أسباب تجتمع لوضع حدٍّ في كثيرٍ من الأحيان لحياة الشّركة وتؤدّي إلى إغلاقها.

وفي ختام هذا المطلب يتبيّن أنّ المخاطر وعلى تعدّدها فإنّها تشترك في هدفٍ واحدٍ هو الكشف عن البيانات المحفوظة في الأنظمة المخترقة، والعمل على سرقتها أو تعديلها أو تدميرها أو حجزها للضّغط على الشّركة المالكة لدفع فديةٍ باهظةٍ، وكما أنَّ البرمجيَّات الخبيثة هي خطّ الهجوم الأوّل في كلِّ الاختراقات، والتّصدّي لهذه البرمجيات لا يكون إلّا عبر الحِيطة واستخدام برامج مكافحة البرامج الضارة والجدران النارية.

كما أنّ البريد الإلكتروني بات أحد الوسائل التي يتّخذها المجرمون لتنفيذ جرائمهم الإلكترونيّة، حيث يستخدم لعمليات الاحتيال الإلكترونيّ وإحداث أعطالٍ في المواقع وإيقافها عن العمل، أمَّا القرصنة الإلكترونيَّة من دخولٍ واطّلاعٍ غير مشروعٍ فيشكّل الخطر الأكبر الذي تخشاه الشّركات نتيجة ما يسبّبه من أضرارٍ كبيرةٍ لا تُحصى. وبعد التعرّف إلى مفهوم عقد التّأمين ضدّ مخاطر الإنترنت واستيضاح مخاطره لا بدّ وأن يُنتقل في الفصل الثاني للحديث عن الالتزامات التي ينشئها عقد التّأمين ضد مخاطر الإنترنت على طرفيه من واجب التّغطية التّأمينيّة، ودفع أقساط التّأمين.

الفصل الثَّاني

آثار عقد التّأمين ضدّ مخاطر الإنترنت

تكمن النتيجة الحقيقيّة لأيّ عقدٍ في أيّ نظامٍ قانونيٍّ حول العالم فيما يكرّسه من آثارٍ قانونيّةٍ على أطرافه، وتنقسم هذه الآثار إلى حقوقٍ والتزاماتٍ، فما هو حقٌّ لطرفٍ يُشكِّل التزاماً على الطَّرف الآخر، ولا يختلف الأمر فيما يتعلَّق بعقد التّأمين ضدّ مخاطر الإنترنت، فلكونه ينتمي إلى طائفة العقود الملزمة لجانبينِ وعقود المعاوضة فيرتّب العقد التزاماً على جانب كلِّ طرفٍ تجاه الآخر، وبالتالي تكون الآثار متبادلةً بين الطّرفين. وكما ذُكِر سابقاً من أنَّ الهدف الحقيقيَّ لعقد التّأمين بالنّسبة للمؤمَّن له هو الحصول على مأمنٍ من المخاطر المحيطة به، في حين تهدف شركة التّأمين (المؤمِّن) إلى تحقيق الرّبح من تحصيل الأقساط، ويُشكِّل هذان الهدفان الحقّ في عقد التّأمين ضد مخاطر الإنترنت، أمّا الالتزامات فهي تتراوح بين واجب حماية المؤمَّن له عند حصول الخطر أو قبله، ودفع الأقساط وبذل العناية الكافية من قبل المؤمَّن له من أجل تمكين شركة التّأمين من القيام بواجبها. وغالباً ما تقتصر آثار العقد على أطرافه وفقاً لمبدأ نسبيّة العقود، لكن لذلك المبدأ استثناءٌ بإمكانيّة مدّ هذه الآثار كحقٍّ فقط دون التزامٍ إلى الغير، ويتبيّن ذلك في حالة التّأمين من المسؤولية عند امتداد التغطية التّأمينيّة إلى أشخاصٍ غرباءَ عن العقد هم المتضرّرون من حادثة الهجوم الإلكتروني (دون أن يكونوا طرفاً بالعقد لكن المؤمَّن له أراد تغطية مسؤوليته تجاههم). وعليه وفي سبيل الإحاطة الكاملة بآثار عقد التّأمين ضد مخاطر الإنترنت سيُقسَّم هذا الفصل إلى مبحثينِ، يبحث الأوَّل التزامات شركة التّأمين، بينما يبحث الثَّاني التزامات المؤمَّن له.

المبحث الأوَّل

التزامات شركة التّأمين

بعد نشوء عقد التّأمين ضد مخاطر الإنترنت صحيحاً متمّماً لأركانه القانونيّة، تظهر الآثار القانونية من حقوقٍ والتزاماتٍ مختلفةٍ على عاتق الأطراف. ويُشكِّل كلّ حقٍّ التزاماً على الطرف الآخر، وفيما يتعلّق بشركة التّأمين فلها الحقّ الكامل بتقاضي أقساط التّأمين المتّفق عليها، والحق بالحصول على المعلومات الكاملة حول الخطر المؤمَّن منه قبل وأثناء العقد، ولمّا كانت هذه الحقوق التزاماتٍ على عاتق المؤمَّن له فستُدرَس في المبحث الثاني وفقاً لانعكاس طبيعة عقد التّأمين ضد مخاطر الإنترنت عليها. أمّا عن الالتزامات التي يوجبها العقد على شركة التّأمين فهي دفع مبالغ التّأمين عند تحقّق الخطر المؤمّن ضدّه، وما يميّز هذا التّأمين أنَّ الالتزامات لا تقتصر على مجرّد دفع مبلغ تأمينٍ، بل هي تغطية تأمينيّةٌ سابقةٌ لوقوع الخطر ولاحقة له، إذ ينطوي العقد على مرحلةٍ هدفها تجنّب حصول الخطر ومرحلةٍ لاحقةٍ لوقوعه لمحاولة إصلاح ما نشأ من أضرارٍ، واستعادة ما تمَّ إفشاؤه، فالتّغطية التّأمينيّة إحدى أبرز مزايا التّأمين ضد مخاطر الإنترنت. ويمارس هذا النوع من التّأمين عشرات الشركات حول العالم، إذ باتت صناعةً رابحةً لكثيرٍ منها فتنتفع بأقساطٍ عاليةٍ ومبالغ تأمين قليلة، ويثير هذا التّأمين العديد من النّزاعات بسبب الغموض الحاصل في عددٍ من عقود التّأمين حول إمكانيّة تأمين الأضرار التي لحقت بأنظمة المؤمَّن لهم وبياناتهم نتيجة لمخاطر الإنترنت بموجب وثائق التّأمين المشتراة من قبلهم، وستتمّ دراسة التزام شركة التّأمين في تغطية المؤمَّن لهم وفق مطلبينِ، حيث سيُبحث في التغطية التّأمينية واستثناءاتها في المطلب الأول، ثمّ نتعرّض لآليّة التّغطية التّأمينيّة في المطلب الثاني.

المطلب الأوَّل

التَّغطيّة التّأمينيَّة واستثناءاتها في عقد التّأمين ضدَّ مخاطر الإنترنت

يكمن الدور الرّئيس لشركات التّأمين في التغطيّة التّأمينيّة التي تقدّمها لعملائها، فكما ذُكِر في أنَّ التغطية لا تقتصر على عمليّة دفع مبلغ التّأمين كما هو الحال في باقي عقود التّأمين، بل تضمّ التغطيات عمليّات مراقبةٍ سابقةٍ لحصول الخطر من أجل تجنّب حصوله في المرتبة الأولى كعمليّات المراقبة للأنظمة والحواسيب، وفي حال حصول الخطر فستُعوّض الأضرار وتُصلَح الأعطال وتُستردّ البيانات المسروقة، وتُدفَع الغرامات القضائية، وغيرها من التغطيات التي تلتزم شركة التّأمين بها، ولكن لا يُعوّض عن كلّ خطر، فهنالك بعض المخاطر التي تخرج عن نطاق التغطية؛ لأنَّها من طبيعةٍ غير إلكترونيَّةٍ، أو تنطوي على إهمال، أو غيره من المخاطر التي تُستثنى، ونتحدّث في هذا المطلب عن أشكال التَّغطية التّأمينية في الفرع الأوّل، والاستثناءات من التَّغطية في الفرع الثاني.

الفرع الأوّل

أشكال التّغطية التّأمينيّة

تحصل التغطية التّأمينية عبر تقديم الخدمات التّأمينيّة من قبل شركات التّأمين عندما حدوث الخطر المؤمّن ضدّه أو قبل حدوثه، وتنقسم هذه التّغطيات وفقاً لثلاثة معايير من حيث الطرف المتضرر (أوّلاً)، ومن حيث وقت التغطية (ثانياً)، ومن حيث كيفية التغطية (ثالثاً).

أوّلاً: أشكال التّغطية من حيث الطّرف المتضرّر:

يقوم هذا المعيار على تحديد الشّخص المضرور الذي سيُدفَع له التّأمين، إذ إنّ بعض الوثائق تكون لتغطية الأضرار الحاصلة عند تحقّق الخطر، وبعضها يغطّي المسؤوليّة المدنيّة الناشئة عن الخطر.

1-تغطية الطّرف الأول، وتُعرَّف بأنَّها: "تغطية الخسائر الحاصلة بشكلٍ مباشرٍ للمؤمّن له، كنفقات خدمات استرجاع البيانات أو نفقات إعلام الأفراد المتضرّرين[157]"، وجاء هذا التّعريف عامّاً غير محدّدٍ، في حين عرّفها آخرون بأنَّها: "الوثيقة التي توفّر الحماية للأصول المملوكة من قبل الشركة المؤمَّن لها ضدّ كلّ الأخطار الإلكترونيّة، كحالات اختراق معلومات وبيانات الشركة، وهجمات حجب الخدمة، والابتزاز الإلكتروني، وأضرار السمعة[158]". ويُشار إلى تغطية الطّرف الأوّل بشكلٍ مختصرٍ على أنَّها الحماية التي توفّرها الوثيقة للمؤمّن له نفسه دون أيّ إشارةٍ إلى طرفٍ محميٍّ آخر، كالفرد الذي كُشفت معلوماته، أو العميل الذي سُرقت أمواله، ففي حالات الهجمات الإلكترونية كلّها هناك طرفان خاسران هما المؤسّسة المنتهكة أنظمتها، والفرد صاحب البيانات المكشوفة، وفي نطاق تغطية الطرف الأول لا يُغطَّى سوى صاحب الشّركة المتضرّرة من الهجمات الإلكترونيّة؛ ولذلك إذا ما اقتصر التّأمين على هذه التغطية فهو لن يكون مناسباً للشركات؛ لأنّ الاضرار كما ذُكِر لا تتوقف عند حدِّ الشّركة، بل تتعدّاها إلى الأفراد المسروقة بياناتهم وأموالهم، ويجب على الشّركة أن تقوم بتعويضهم نظراً لقيام مسؤوليّتها المدنيّة تجاههم.

2- ولذلك ظهر ما يسمّى بتغطية الطرف الثالث التي تهدف إلى تغطية نفقات الدفاع في الدعاوى، والتسويات، والغرامات، والأحكام التي تفرض على المؤمَّن له كنتيجةٍ لأعمال خرق بيانات الطّرف الثالث (العميل)، وقيام مسؤولية المؤمَّن له تجاه ذلك[159]، وتُعرَّف هذه التغطية بأنَّها: "الوثيقة التي تؤمّن الحماية لمعلومات الأفراد المستهلكين التي تحفظها الشركة لديها، والتي يفترض أن تبقيها بأمان، كحادث كشف بيانات العملاء نتيجة عملية اختراق، ما يفرض على الشركة دفع تعويضاتٍ لهم، والدفاع عن نفسها في المحاكم ضدّ الدعاوى القضائية التي يقيمها هؤلاء عليها[160]". فتغطية الطّرف الثّالث تغطّي كلاً من الشّركة المخترقة والفرد الذي تعرّضت بياناته للاختراق.

---

157 Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk, v5, Oxford: UK, Journal of Cybersecurity, p 5

158 Akhgar, B., Staniforth, A., & Bosco, B. (2014). p 223.

159 Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). P 6.

160 Akhgar, B., Staniforth, A., & Bosco, B. (2014), p 224.

ومهما قِيل في أشكال التّغطية بين تغطية طرفٍ أوّلٍ وثالثٍ فلا تخلو وثيقةٌ من الجمع بين هاتين التّغطيتين؛ لأنَّ كليهما مكمّلٌ للآخر، فلا تُقبل وثيقةٌ تغطّي أضرار تدمير البيانات على سبيل المثال دون أن تقوم بتعويض العملاء المتضرّرين من هذا الفعل، كما لا يمكن القول بأنّ الوثيقة لا تغطّي الغرامات التي سيحكم بها على الشركة المخترقة، وإن كان لا شيء يمنع قانوناً من ذلك لكن واقعياً يبقى الأمر مستبعداً.

ثانياً: أشكال التّغطية من حيث وقت التّغطية:

تبقى شركة التّأمين ملتزمةً بتغطية المؤمَّن له طوال مدّة العقد ما دام المؤمَّن له يدفع الأقساط، وفي إطار عقد التّأمين ضدّ مخاطر الإنترنت لا يقوم التزام التغطية التّأمينيّة عند حصول الخطر المؤمّن ضدّه فحسب، بل تلتزم شركة التّأمين بتغطية المؤمَّن له حتى قبل حصول الخطر عبر القيام بأفعالٍ عدّة.

1-التّغطية التّأمينيّة قبل وقوع الخطر المؤمّن ضدّه: تهدف هذه التّغطية إلى محاولة الحدّ من التّعرّض للهجمات الإلكترونيّة خلال فترة التّأمين، أو الحدّ من آثار الهجمات الإلكترونيّة عند حدوثها، وتقدّم هذه التغطية كخدماتٍ إضافيّةٍ مع الوثائق التّأمينية، ويُشار لها بخدمات ما قبل الخرق أو خدمات التّخفيف من المخاطر، وتقدم هذه الخدمات إمّا شركات التّأمين نفسها أو بالاشتراك مع مقدّمي خدمات أمن المعلومات، ومستشاري إدارة المخاطر، كعمليات تقييم المخاطر التي تهدّد الشركة طالبة التّأمين، وفحص الضعف عبر تحديد مدى إمكانية التعرّض للحوادث الإلكترونية، واختبار الاختراق، بالإضافة إلى خدمات التخفيف من المخاطر كعمليّات تحديد التهديدات المحتملة، والإنذار المبكّر، وتقنيات الحماية المتخصّصة، وخطوط المساعدة على مدار السّاعة من أجل الإجابة عن أيّ استفسارٍ من قبل الشّركة المؤمَّن لها، ناهيك عن عمليّات تدريب الموظّفين من أجل محاولة عدم الوقوع في مصيدة الثّغرات الأمنيّة؛ لأنَّ أغلب الهجمات الإلكترونية تتمّ نتيجة إهمال الموظّف، أو نتيجة عدم معرفته بما يجب القيام به كفتحه رسالةً ملغومةً ممّا يمهّد الطّريق لدخول الفايروسات مثلاً[161]. وبالرّغم من كلّ هذه الخدمات المقدّمة من قبل شركات التّأمين، إلّا أنّها قد لا تتمكّن من صدِّ الهجمات الإلكترونيّة، وبالتّالي يبقى المؤمَّن له معرّضاً لخطر إصابته بأخطار الإنترنت، وعندها يتمّ تقديم التّغطية التّأمينيّة لما بعد وقوع الخطر.

[161] enhancing the role of insurance in cyber risk management (2017). Paris; France, OECD publishing, p 75.

وفي إحدى الخدمات التي تقدّمها شركة CHUBB للتّأمين ضدّ مخاطر الإنترنت التّواصل مع فريقٍ لهندسة المخاطر المخصّص لمساعدة الشركات المؤمّن لهم في تقييم تعرضهم للمخاطر على نحوٍ دقيقٍ[162]، كما يتم تدريب الموظفين من أجل تفادي عمليات التصيد الاحتياليّ بغية تلافي عمليات الاحتيال[163].

ب–التّغطية التّأمينيّة بعد وقوع الخطر المؤمّن ضدّه: لا تتم هذه التغطية إلّا بعد حصول الخطر ووقوع ضررٍ للمؤمَّن له منه، فكما ذُكِر سابقاً في حال حصل الخطر لكن دون وقوع أيّ ضررٍ فلا يكون للمؤمَّن له أيّ حقّ في الحصول على مبلغ التّأمين؛ بسبب انعدام المصلحة، ولكن في الحالة التي يتحقّق فيها الخطر ويخلّف وراءه خسائرَ لا بدّ عندها من دفع مبلغ التعويض من قبل شركة التّأمين المساوي لحجم الخسارة الحاصلة وما فاته من كسب نتيجة هذه الهجمات الإلكترونيّة وبما لا يتجاوز حدود عقد التأمين. **وتجدر الإشارة إلى أنّ التّأمين ضدّ مخاطر الإنترنت لا يتوقّف عند دفع مبالغ التّأمين فقط، بل يقدّم خدماتٍ متنوّعةً انطلاقاً من طبيعة العمل الإلكترونيّ _وإن كانت كلّ هذه الخدمات تكلّف شركات التّأمين أموالاً لكنها تتخذ شكلاً عينياّ_** فعلى سبيل المثال الخدمات المقدّمة لمحاولة تقليل آثار مخاطر الإنترنت عند وقوعها تضمّ خدمات التّحقيق من أجل تحديد مصدر الخرق، وتقديم المساعدة القانونيّة لإدارة المتطلّبات القانونيّة والمسؤولية المحتملة، وتقديم خدمات إخطار العملاء عند حصول الخرق، ومراقبة الائتمان، وحماية الهويّة لدعم العملاء المسروقة بياناتهم، والتواصل مع شركات علاقاتٍ عامةٍ من أجل تقليل أضرار السمعة نتيجة الحوادث الإلكترونية[164]. ويوفّر أيضاً الاستعانة بخبراءَ متخصّصين لمحاولة استرداد البيانات المسروقة أو المتلفة، وإصلاح أعطال الأجهزة، ومحاولة استعادة النّظام وإعادته إلى وضعه الطّبيعيّ ما قبل الخرق، عدا عن عمليّات دفع تكاليف الفدية من أجل فكّ تشفير البيانات في عمليّات الابتزاز الإلكترونيّ، ودفع الغرامات التي تفرضها قوانين حماية البيانات الشّخصيّة التي

[162] SME cyber claims are on increase understand your business exposure (n.d). CHUBB, P 10.

[163] Ibid, P 7.

[164] enhancing the role of insurance in cyber risk management (2017). P 75.

تعاقب المؤسّسات على خرق خصوصيّتها، ومحاولة شركات التّأمين القيام بصلحٍ وديٍّ فيما بين الشّركة المخترقة وعملائها، بالإضافة إلى دفع تكاليف الدعاوى القضائيّة والسّير فيها حتى فصلها[165].

ويُخلص للقول إنَّ نوعي التّغطية يتم تضمينهما في الوثائق التّأمينية على الأغلب؛ لأنَّ الخدمات المقدَّمة قبل وبعد حصول الخطر تكمّل بعضها وتصبُّ في بوتقة التَّخفيف من آثار مخاطر الإنترنت، ومهما قِيل في محاولة الفصل بين الأشكال المختلفة للتَّغطية يبقى الفصل نظريّاً؛ لأنَّ أغلب الوثائق التّأمينيَّة تضمُّ كلَّ هذه الأشكال، فتغطّي الطّرفين الأوَّل والثَّالث قبل حصول الخطر وبعده من أجل محاولة تغطية أكبر قدر ممكنٍ من الخسائر بما يلائم حاجة العملاء. كما يفرّق بعض الفقه بين الوثائق المغطية للأفراد وبين وثائق الشّركات من ناحية التّغطية المقدّمة وذلك لطبيعة الأخطار التي تهدّد كلَّ طرفٍ على حدة، فالتَّغطية المقدَّمة للأفراد تركّز على إساءة استخدام البيانات التي يستخدمها الأفراد على الإنترنت، كإساءة استخدام بطاقات الائتمان، وإصابة الحواسيب بالبرمجيّات الخبيثة، بالإضافة إلى عمليّات الاحتيال الإلكترونيّ كعدم تسليم البضاعة المشتراة عبر الإنترنت، وأفعال التنمّر الإلكتروني، وتُعدّ هذه الأخطار أكثرها شيوعاً في إصابة الأفراد، أمّا تغطية الشركات والتي تستهدف في المقام الأول الشركات صغيرة ومتوسطة الحجم فتركّز أيضاً على إساءة استخدام البيانات لا سيّما الماليَّة منها، والبرمجيَّات الخبيثة، وأعمال الابتزاز الإلكتروني، وتقدم تعويضاتٍ عن الخسائر، وفقدان الدّخل، وخدمات التحقيق والإعلام على ما ذُكر سابقاً في الأشكال السّابقة[166].

ثالثاً: أشكال التّغطية من حيث كيفيّة التّغطية:

على الرغم من أنَّ عقد التّأمين ضدَّ مخاطر الإنترنت يشترك مع أنواع التّأمين الأخرى في فكرة التَّعويض النَّقديّ، إلَّا أنَّ طريقة تطبيق هذا التَّعويض هي ما تميّزه عن سواه من عقود التّأمين، لكون هذا التعويض يضم خدماتٍ عينيةٍ (أداءات معيّنة تلتزم بها شركات التّأمين)، وهذا ما سنفصّله وفقاً للآتي:

---

[165] Ruef, M. (2017). Cyber insurance- benefits and uses, SCIP, P 1.

[166] Ibid, p 1

يضمّ التَّعويض النّقديّ الطّرف الأوّل (الشّركة المتضرّرة نفسها) والطّرف الثّالث (الغير وهو العميل الذي كُشِفت بياناته أو سُرِقت أمواله أو تعطَّلت أعماله نتيجة الهجمات الإلكترونيَّة المحدَّدة في العقد).

ومن صور التّعويض النّقديّ الذي يدخل في نطاق تغطية الطَّرف الأوَّل:

أ–تلتزم شركة التأمين بأن تعوّض المؤمَّن له عن الخسائر التي تلحق به نتيجة أعمال الخرق وتدمير البيانات أو الدّخول غير المصرّح به، ويكون هذا التعويض متناسباً مع حجم الخسارة وضمن حدود مبلغ التّأمين، ويتمّ دفع هذه النّفقات من أجل تعويض خسارة دخل الشّركة نتيجة توقّف أعمالها كانقطاع خدمتها عن زبائنها لوقتٍ طويلٍ (انهيار الشبكة)، وعدم القيام بالتّعاملات عبر الإنترنت كالمعتاد، كما تعوض المؤمَّن له عن النّفقات التي يصرّفها من أجل استعادة نظامه وبياناته، كالنفقات التي تُدفع من قِبل المؤمَّن له لاستبدال الأصول الرّقميّة التي تمّ تعطيلها، أو تدميرها، أو إتلافها نتيجة هجومٍ إلكترونيٍ معيّنٍ، أو استرداد هذه البيانات، أو إعادة إنشائها، أو الوصول إلى هذه البيانات والأصول عبر النسخ الاحتياطية أو النسخ الأصلية المحفوظة في مكانٍ آخر، أو جمع وإعادة إنشاء هذه البيانات الإلكترونيّة من مصادرَ أخرى لإعادتها إلى الحالة التي كانت عليها قبل سرقتها، أو تدميرها، أو تعديلها، إذ تُعدّ عمليّة نسخ البيانات احتياطياً في أماكنَ آمنةٍ من أهمّ الإجراءات التي يتوجّب القيام بها من قبل المؤمَّن له من أجل تقليل نسبة الضّرر الذي سيصيبه في حالة الهجوم الإلكتروني[167]، بالإضافة إلى ذلك تقوم شركة التّأمين بتعويض الشركة المؤمَّن لها عن نفقات تحسين الأجهزة والأنظمة المستخدمة، وترقية نسخ الحماية المستخدمة إلى نسخةٍ أكثرَ أماناً، بشرط أن يكون ذلك ضرورياً وفعّالاً لمنع تكرار أيّ هجومٍ إلكترونيٍ آخر طوال مدّة العقد.

ب–نفقات التّحقيق الجنائيّ: إذ إنّه في هجمات الخرق الأمنيّ أو غيرها من الهجمات الإلكترونيّة، كحجب الخدمة أو قطع الأعمال، لا بدّ عندها من فحص الحواسيب والأنظمة التّابعة للمؤمَّن له من أجل التأكّد من عدم وجود برامجَ ضارّةٍ أخرى، فكم يبدو هذا التحقيق ذا أهميّة لا سيّما في حالات سرقة المعلومات

[167] Purchasers' Guide to Cyber Insurance Products. (2016). United States of America, financial services sector coordinating council for critical infrastructure protection and homeland security, p7.

الشّخصيّة، إذ يتمّ عندها أيضاً التأكّد من حصول الخرق وأسبابه (أي الثّغرات التي أدّت إلى حصول هجومٍ أو محاولة هجومٍ من أجل محاولة سدّها وتلافيها في المرّات القادمة). وعندها تتمّ الاستعانة بخدمات خبراء الحاسب، إذ ستدفع شركات التّأمين النّفقات اللّازمة من أجل الاستعانة بخبراء أمنيين للحاسب يتمّ اختيارهم من قبل المؤمَّن له بالتعاون مع مجموعات الاستجابة لخدمات الخرق التي يوفّرها عقد التّأمين، وذلك من مجموعة خبراء الأمن المعتمدين من جانب شركة التّأمين والذين توفّرهم للمؤمّن لهم[168].

ج–نفقات إعلام المتضرّرين من الهجوم الإلكترونيّ، والغرامات التي يُحكم بها على المؤمَّن له نتيجة تهاونه في القيام بواجب الإعلام، أو التأخُّر في القيام بذلك؛ لذلك تقوم شركة التّأمين بتعويض المؤمَّن له عن هذه النفقات والغرامات.

د–خدمات العلاقات العامّة التي توفّرها شركة التّأمين للمؤمّن له: والّتي تضمّ نفقات الحصول على الدّعم والمشورة من مستشاري العلاقات العامَّة، أو مستشاري إدارة الأزمات من أجل التَّخفيف من أضرار السّمعة التي تلحق بالشّركة وأفرادها نتيجة الهجمات الإلكترونية، كرئيس مجلس الإدارة والموظفين فيها الذين توجّه إليهم أصابع الاتهام عند كلّ خرقٍ أمنيٍّ كنتيجةٍ لإهمالهم في حماية الأنظمة، ويدخل أيضاً في ذلك تكاليف الإعلان أو العروض الترويجيّة الخاصّة التي تسوّقها الشّركة المؤمَّن لها لنفسها[169].

هـ– نفقات الفدية التي تُدفع لوقف أعمال الابتزاز الإلكترونيّ، وهجمات حجب الخدمة، وقطع الأعمال التي قد تستمرُّ لساعاتٍ، والتي قد تسبّب تدمير البيانات وتعطيل الأنظمة إن لم تُدفع؛ ولهذا غالباً ما تدُفع هذه الفدية في محاولةٍ لفكِّ تشفير البيانات. ولكن قد تطلب كثيرٌ من شركات التأمين من عملائها إن وقعوا ضحيّةً لهذه الجريمة عدم الدّفع قبل إبلاغها؛ لأنّ شركة التّأمين قد تدخل طرفاً وسيطاً بين المبتزّين والشركة المخترقة، وقد تطلب مساعدة خبراء معلوماتيين من أجل محاولة تحرير البيانات أو تعطيل الأجهزة لوقف تمدّد المهاجمين،

---

[168] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019), p6,7.

[169] Ibid, p7.

ويضمّ التعويض نفقات الاستعانة بمفاوضٍ من أجل تسليم أمور التفاوض مع الحاجزين أو نفقات أيّ دفعاتٍ أو تحويلاتٍ أو أملاكٍ يتم التخلّي عنها كفديةٍ من أجل فكّ حجز البيانات والأنظمة[170].

وفي السياق ذاته، يدعم اليوروبول ومكتب التحقيقات الفيدرالية عدم دفع الفدية في حال كانت أقلّ من تكاليف التّأمين السيبراني، كما يشجّع على وجوب القيام بالنسخ الاحتياطي في أماكن خارج الموقع والشبكة من أجل زيادة الأمان، لكن هنالك بعض الحالات لا يمكن فيها إلّا دفع الفدية كأفضل خيارٍ أخيرٍ؛ لذلك يُدعم مقدّمو خدمات الاستجابة بمحافظ البتكوين[171]، وفي إحدى الأمثلة التي واجهت شركة chubb لخدمات التّأمين ضدّ مخاطر الإنترنت، تعرّض أحد المؤمَّن لهم لهجوم ابتزازٍ إلكترونيٍّ نتيجة قيام موظّف بالضغط على رابطٍ مشبوهٍ أدّى إلى تنزيل برنامج ضارٍّ على سيرفرات الشركة، وتشفير البيانات المخزنة، ومن ثمّ ظهرت رسالةٌ على الحاسب تطالب بدفع 10 آلاف دولار بعملة البتكوين خلال 48 ساعة مقابل فكّ التشفير، فما كان من الشركة إلا أن اتّصلت بالخط الساخن للاستجابة للحوادث لدى chubb، فسارع مدير الاستجابة للحوادث إلى إحضار محقّقين متخصّصين للتأكّد من صحّة التهديد، وإمكانية عدم دفع الفدية، وقُدِّرت تكاليف الاستجابة للحوادث والتي تضمّ التحقيقات من أجل تحديد مصدر البرنامج الضارّ، وتأثيره على النّظام، وحساب حجم الضّرر، ورسوم الاستشارات ومدير الاستجابة بـ31 ألف دولار، في حين بلغت تكاليف إدارة الابتزاز الإلكتروني، والتي تتعلق بمعالجة تهديدات الابتزاز، أو دفع مبلغ الفدية بالإضافة إلى نفقات مستشار تكنولوجيا المعلومات لتحديد إمكانية النسخ الاحتياطي إلى 14 ألف دولار، في حين أُنفِقَ حوالي 15 ألف دولار من أجل استعادة الملفات المسروقة أو المُخرَّبة. في حين تعرض شركةAIG[172] إمكانية دفع الفدية بالعملات الرّقميّة، وهو الأمر الأهم في تأمين مخاطر الإنترنت؛ لأنّ المبتزّين دائماً ما يطلبون الفدية بالعملات الرّقميّة؛ نظراً لعدم إمكانيّة تتبعها[173].

---

[170] Ibid, p5.

[171] Cyber claims examples, an aid to evaluating if you have adequate insurance in place (n.d). Chubb, p3.

[172] American International Group

[173] What's Inside Cyberedge (n.d). AIG, P8 To 17.

و–نفقات المحامين والمستشارين القانونيين التي تُدفَع لإنهاء الدّعاوى، أو التّصالح مع المتضرّرين (الصّلح الودّيّ)، أو اللّجوء إلى التّحكيم وتسوية الوضع.

ز–خدمات المراقبة: ولا يشترط أن تقدّم هذه الخدمات من قبل شركة التّأمين نفسها، بل قد يكون هناك تعاونٌ بين شركات التّأمين وشركات الأمن السيبراني من أجل تقديم هذه الخدمات، وتضمّ هذه الخدمات مرحلتَي ما قبل حصول الخطر المؤمّن ضدّه وما بعده، إذ إنّه قبل تحقّق الخطر تُقدَّم خدمات الدعم الفني من جانب شركة التّأمين للحواسيب الشّخصيّة للمؤمَّن له لحلّ المشاكل التّقنيّة التي تواجهها في أثناء فترة سريان الوثيقة، ويتوجّب تقديم رقم تعريف المؤمَّن له، ورقم الحساب المصرفي، ورقم الهاتف، وعنوان البريد الإلكتروني، من أجل توفير خدمة المراقبة المستمرّة على الإنترنت من أجل تتبّع النّشاطات الضارة[174]، أمّا بعد تحقّق الخطر فتتوفّر خدمات مراقبة الائتمان للحسابات المخترقة لدى المؤمَّن له فتُقدّم المراقبة على الفور بعد الخرق، وكشف البيانات حيث يتم إرسال تحذير مبكّرٍ عن التغيرات في الحساب والاستجابة لذلك فوراً (فتعدّ الساعات الأربعة والعشرين الأولى الأهمّ عند الاستجابة للحوادث)، وأيضاً تسمح خدمة المراقبة باكتشاف محاولات سرقة الهويات مبكّراً في محاولةٍ للتصدّي لمحاولات الاحتيال عبر الإنترنت باستخدام حساباتٍ مسروقةٍ[175]، كما تُراقَب عادةً السجلّات الائتمانيّة للأفراد المخترقة حساباتهم لمدّة عامٍ للكشف عن أيّ نشاطٍ مُريبٍ أو غير مصرَّحٍ به، ويتم الوصول المنتظم إلى هذا السجلّ، وإرسال تنبيهات عند حصول تغييراتٍ مهمّةٍ في السجل، وتعد شركة KROLL من أهمّ المزوّدين العالميين الرّائدين لخدمات الأمن السيبراني[176]. كما يُضاف إلى خدمات المراقبة تقديم تدريبٍ لموظّفي الشركة المؤمَّن لها؛ لما له من أهميّةٍ للطّرفين في محاولة تجنّب حصول خروقاتٍ أو تهديدٍ للأمن في البداية، والاستجابة بشكلٍ سريعٍ وفعّالٍ عند حصول الخرق من أجل الحفاظ على الخسائر والأضرار الحاصلة عند أقلّ حدٍ ممكنٍ.

---

[174] الناصري، (2019)، ص206.

[175] https://www.thebalance.com/best-credit-monitoring-services-4164937

تاريخ الزيارة: 17\6\2020، الساعة 8:30 p.m.

[176] https://www.irmi.com/term/insurance-definitions/credit-monitoring

تاريخ الزيارة: 17\6\2020، الساعة 8:40 p.m.

ح–تقدّم شركة AXA في سنغافورا تغطياتٍ للمؤمَّن له ولعائلته من الأضرار التي تصيبه من استعمال الإنترنت عن الأضرار الحاصلة للسمعة الإلكترونيّة، ونزاعات التجارة الإلكترونيّة، ففي حال نشر أحد الأشخاص منشوراً مسيئاً عن المؤمَّن له، تُخصّص شركة AXA متخصّصينَ من أجل إزالة المحتوى المسيء، بشرط أن يُقدَّم تقريراً للشرطة خلال 24 ساعةً تاليةً لاكتشاف المنشور، أمَّا عن نزاعات التجارة الإلكترونيّة فيغطّي التّأمين عمليات الشراء عبر الإنترنت عند عدم تسليم المشتريات أو تسليمها تالفةً أو مخالفةً لما اتُّفِق عليه عبر الموقع الإلكترونيّ، فهنا يكون لشركة التّأمين الخيار بين بأن تعوّض المؤمَّن له نقداً أو تقوم بإصلاح العنصر المشترى أو تستبدله بآخرَ جديدٍ.

ز–تقدّم شركة AXA سنغافورا أيضاً تغطيةً لانتهاك حقوق الملكيّة الفكريّة والتنمّر الإلكترونيّ، ففي أحد الأمثلة العمليّة التي تسردها الشركة، التقط شخصان صورةً فوتوغرافيةً لهما، وتفاجأا فيما بعد بهذه الصورة على أحد مواقع الإنترنت، وكانا يملكان وثيقة تأمينٍ ضدّ مخاطر الإنترنت من AXA فطلبت شركة التّأمين من النّاشر إزالة هذه الصورة، وعند عدم الرضوخ لهذا الطلب اتُّخِذت الإجراءات القانونيّة بحقِّه، وفي مثالٍ آخرَ تعرَّضت إحدى المؤمَّن لهم للتنمر بسبب صورها على تطبيق إنستغرام، فقامت شركة تأمينها بإرسال تحذيراتٍ إلى هؤلاء الأشخاص، ومن ثمّ تمّ التعامل معهم بشكلٍ قانونيٍّ[177].

أما عن صور التعويض النقدي الذي يدخل في نطاق تغطية الطَّرف الثَّالث والتي تمثِّل تغطية المسؤوليَّة المدنيَّة للمؤمَّن له فهو على نحو الآتي:

أ–تعويض المتضرّرين نتيجة أعمال الاحتيال والخداع عبر الشّبكة وعبر الهاتف التي تُمارس على عملاء الشركة المؤمَّن لها، والتي تسبب تحويل مبالغَ طائلةٍ من هذه الشّركة نتيجة الأعمال المذكورة، أو سرقة أسهم من الشركة فتُعوَّض هذه المبالغ للشّركة المخدوعة من قبل شركة التّأمين بعد أن يتم دفعها من الشركة للمتضررين، وقد يتمّ الدفع بشكلٍ فوريٍّ من قبل شركة التّأمين لصالح المتضرّرين، كما يُعاد إصدار بطاقات دفعٍ

[177] https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf
تاريخ الزيارة: 29\6\2020، الساعة 3 P.m.

جديدةٍ لصالح المستهلكين على نفقة المؤمَّن له. وبالإضافة إلى هذه النفقات المذكورة يتم تغطية أي نفقاتٍ أخرى قد يُتّفق عليها في عقد التّأمين، كنفقات انتهاك الخصوصيَّة التي قد ترتكبها الشركة نفسها تجاه الغير وتسبب قيام الدعاوى ضدها[178].

ب-خدمات الدّعم الفني للعملاء: عند إرسال إخطارات خرقٍ ما إلى حسابات العملاء لدى الشّركة المخترقة يبدأ الخوف والقلق لديهم ممّا سيحصل ببياناتهم، وما يمكن أن يسبّبه ذلك لهم من مشكلاتٍ ماليّةٍ، وقانونيّةٍ، لذلك يبادرون إلى الاتصال بالشّركة لمحاولة فَهم ما حصل، وعليه يُنشئ عقد التّأمين ما يُسمَّى بمركز خدمة العملاء الذي يديره موظّفون مختصّون، وخبراء قانونيّون، ومعلوماتيّون للرّدّ على استفسارات العملاء بسرعةٍ ومهنيّةٍ كاملةٍ، إذ يتم إعطاؤهم الإجابات والوسائل الوقائية اللازمة للتعامل مع مشكلات سرقة الهوية المحتمل، والاحتيالات الإلكترونيّة لمحاولة تقليل آثاره المالية والقانونية من الاستخدام غير المصرّح به للبيانات والحسابات المسروقة[179].

ج- الغرامات التي يحكم بها على الشّركة نتيجة أعمال التقاضي والدعاوى التي يرفعها المتضرّرون على الشركة المخترقة، وتتبنّى شركة GAI[180] مفهوماً واسعاً للدّعاوى فيدخل في نطاقها المطالبات الكتابيّة، أو الحلول البديلة كالوساطة، والتّحكيم، واتفاقيّة المهلة التي تعطي طرفَي الدّعوى مهلةً للحوار الهادئ لمحاولة تجنّب تكاليف التقاضي[181].

د-يغطّي التّأمين الغرامات التي تفرضها قوانين حماية البيانات حول العالم على الشركات والتعويضات التي تلزم بدفعها، وهو ما يطلق عليه مسؤولية أمن الشبكة، ومسؤولية الخصوصيّة أيضاً، إذ تقوم هذه المسؤولية نتيجة الفشل في الحماية، والتسبب في الخرق، وإفشاء السرية أو نتيجة نقل الفايروسات والبرمجيات الضارة من

---

[178] Cyber, Security and Privacy Protection Insurance, Policy Wording, (n.d). Zurich insurance, p3,4.

[179] https://www.kroll.com/en/services/cyber-risk/remediate-and-restore/data-breach-call-center-services

تاريخ الزيارة: 17\6\2020، الساعة 9:30 p.m.

[180] شركة Great American Insurance

[181] https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage

تاريخ الزيارة: 27\6\2020، الساعة 9:30 p.m.

قبل الشركة نفسها نحو عملائها وما يلحقه ذلك من ضررٍ لهم. ومن بين أشهر قوانين حماية الخصوصيّة قانون حماية البيانات العامّة GDPR في دول الاتّحاد الأوروبيّ، والذي دخل حيّز النّفاد في العام 2016، والذي يطلب من كلّ معالجي البيانات، ومقدّمي الخدمات عبر الإنترنت الذين يخزّنون بيانات الأفراد لديهم اتّخاذ إجراءاتٍ صارمةٍ لمنع انتهاك الخصوصيّة وفق ما يحدّده هذا النظام، ويجب على المعالج أن ينفّذ تدابيرَ تقنيّةً وتنظيميّةً يضعها النّظام مع وجوب إعادة مراجعتها كلَّ فترةٍ لضمان مناسبتها للوضع الراهن، وإذا ما قامت الشركة المعالجة بانتهاك هذه الإجراءات، وعرّضت بيانات الأفراد للخطر، يحقّ لهم المطالبة بتعويضاتٍ كاملةٍ عن هذا الضّرر[182]، وعندها تعوّض شركة التّأمين هؤلاء الأفراد نيابةً عن الشّركة الملزمة بذلك، وتوفّر عليهم عناء مواجهة خصمٍ مفلسٍ أو ذي رأسمالٍ غير كافٍ للجميع، **وهو ما يعد أهمّ ميّزات هذا التّأمين**، وفي هذا الإطار تعمد أغلب شركات التّأمين ضدّ مخاطر الإنترنت إلى تغطية الغرامات التي تلتزم الشركات بدفعها نتيجة خرقها لقانون حماية البيانات، وهو ما تقدمه شركة زيوريخ ضمن تغطيتها لمخاطر الإنترنت، إذا ما ارتكب المؤمَّن له أحد أفعال الخرق للقانون المذكور أو لأيٍّ من قوانين حماية البيانات والخصوصيّة النافذ خلال فترة سريان وثيقة التّأمين[183].

هـ-تغطية المسؤوليّة عن وسائل الإعلام الرّقميّة: يغطّي التّأمين تكاليف الانتهاك، والمسؤوليّة النّاشئة عن النّشر عبر مواقع الإنترنت، والبريد الإلكترونيّ، وغيرها من الوسائل الإلكترونيّة الحاصلة بغير نية عمديّة لإحداث ضرر أي بمحض الخطأ[184]، وفي هذا السياق تقدم شركة AIG هذه التغطية، ففي حال خرقت إحدى الشّركات المؤمَّن لها إحدى العلامات التجارية لشركةٍ ما عبر تسويقها على أنَّها عائدةٌ لها عبر أحد مواقع

---

[182] https://www.gdpr-info.eu/

تاريخ الزيارة: 13\6\2020، الساعة 11:10 p.m.

[183] https://www.zurichna.com/knowledge/topics/cyber

تاريخ الزيارة: 28\5\2020، الساعة 11:20 p.m.

[184] Ibraheem K. (2008), p 9.

التواصل، أو عبر موقعها الرّسميّ على الإنترنت، أو عبر الإعلان الإلكترونيّ، وقامت الشّركة المنتهكَة حقوقها بمقاضاة الشّركة المؤمَّن لها فإنَّ شركة التّأمين تغطّي هذه التَّكاليف[185].

وبصورةٍ عامَّةٍ في إطار تغطية الطَّرف الثَّالث، فهي تغطّي المسؤوليَّات التي تقوم على عاتق المؤمَّن له نتيجة هجماتٍ إلكترونيّةٍ مع ما تسبّبه من خسائرَ للعملاء. **وبعيداً عن ذلك فقد يتضمَّن عقد التّأمين ضدَّ مخاطر الإنترنت تغطيةً مختلفةً من نوعها** كتغطية المكافأة التي تدفع من جانب شركة التّأمين إلى مخبر معلوماتٍ سريّةٍ موثوقةٍ تؤدّي إلى إدانة الشخص المسؤول عن الهجوم الإلكتروني، فتقدّم معظم شركات التّأمين هذه التغطية، وعلى سبيل المثال تقدّم شركة زيوريخ تعويضاً عن المكافأة التي يعرضها المؤمَّن له للأشخاص الذين يدلون بمعلوماتٍ قد تؤدي إلى إدانة المجرمين الإلكترونيين، وتشترط شركة التّأمين لدفع هذا التعويض أن تُدفَع المكافأة في أثناء فترة سريان وثيقة التّأمين، وأن يحصل المؤمَّن له على موافقة شركة التّأمين قبل عرض هذه المكافأة[186].

وعلى نحوٍ مغايرٍ لا يمكن تغطية كافة المخاطر، فهناك أخطار تؤدّي إلى خسائرَ إلكترونيّةٍ فعليّةٍ لكنّها تخرج عن التغطيّة التّأمينية عموماً؛ نظراً لوجود ظروفٍ تحيط بها تُخرجها عن نطاق التّأمين، وهو مدار دراسة الفرع الثانيّ.

الفرع الثاني

الاستثناءات من التّغطية التّأمينيّة

تتعدَّد صور هذه الاستثناءات تبعاً لأسبابٍ مختلفةٍ، منها ما هو ناشئٌ عن طبيعة الخطر، أو نتيجة لتدخّل أحد أطراف عقد التّأمين في حصولها، وغير ذلك من أسبابٍ ستُبيَّن فيما يلي:

---

[185] What's inside cyberedge, (n.d). AIG, p8 to17.

[186] https://www.zurichna.com/knowledge/topics/cyber

تاريخ الزيارة: 28\5\2020، الساعة 1130 p.m.

أولاً–الإصابات الجسديَّة والأضرار الماديَّة: لا تُغطَّى الأضرار التي تلحق بالأفراد نتيجة مخاطر الإنترنت كالإصابات أو حصول وفاةٍ لأحدٍ ما؛ لأنَّ هذه المخاطر مغطّاةٌ بموجب وثائق التّأمين على الأشخاص التي تؤمّن على المرض والإصابة، كما لو أُصيب المدير التنفيذيّ لشركةٍ ما بمرضٍ ما نتيجة حصول خرقٍ لأنظمة شركته، أو تعرّض أحدٍ ما لضيقٍ نتيجة ابتزازه في بياناته، فلا يتمّ التعويض عنها. وعلى الرغم من ذلك تتّجه شركة زيوريخ إلى خلاف هذا المبدأ، وتقدّم تغطيتها للألم الجسديّ أو النفسيّ الذي يصيب المؤمَّن له نتيجة الخطر الإلكترونيَ[187]، ويميل الرأي إلى عكس هذه التغطية لكونها أنتجت آثاراً شخصيّةً وهو ما لا يتمّ تغطيته في عموم عقود التأمين من الأضرار ومنها التّأمين ضد مخاطر الإنترنت بل تتم تغطيتها على نحوٍ مخصّصٍ في عقود التأمين على الأشخاص. وفي السّياق نفسه لا تُغطَّى الأضرار الماديّة التي يتسبَّب فيها أيُّ خطرٍ إلكترونيٍّ، كما أنَّ الحريق والرياح والكوارث الطَّبيعيَّة التي تؤدّي إلى حصول خللٍ ما في الأنظمة لا يتمُّ تغطيته؛ لأنَّها ليست من منشأٍ إلكترونيٍّ، كما أنَّ الأعطال هذه تُغطَّى بوثائق التّأمين التّقليديّة كوثيقة التّأمين التّجاريّة العامّة، بالإضافة إلى أنَّ الخسائر الحاصلة نتيجة أعطال الكهرباء، وأعطال الاتصالات اللاسلكية أو الأقمار الصّناعيّة، وفشل البنية التحتية لا يتم تغطيتها[188].

ثانياً–الأخطار المتعمّدة: لا يتمّ عادةً تأمين الأخطار المتعمّدة كما هو الحال في وثائق التّأمين كلّها؛ نظراً لما تقوله القاعدة الفقهية (مَن استعجل الشَّيء قبل أوانه عُوقِب بحرمانه)، ولذلك درءاً لمحاولة قيام المؤمَّن له بتعمّد افتعال الخطر بنفسه، كقيام أحد موظّفيه بالدخول إلى أحد المواقع غير الآمنة مع علمه بخطورة ذلك من أجل تدمير بياناته ببرنامجٍ ضارٍّ ما، والحصول بسببه على مبلغ التّعويض؛ لأنَّه يعاني من أزمةٍ ما وبحاجةٍ للمال فلا سبيل له إلَّا افتعال ذلك، لذلك وإذا ما تحقّق هذا الأمر جاز لشركة التّأمين أن تدفع بعدم استحقاق المؤمَّن له لمبلغ التّعويض، وعلى المؤمَّن له في هذه الأحوال إثبات حقه بمبلغ التأمين عبر إيراد دلائل لتنفي عنه شبهة تحقيق الخطر بصورةٍ متعمدةٍ وفقاً لقاعدة البينة على من ادّعى . كما يُستند في ذلك إلى القانون المدنيّ

---

[187] Cyber, Security and Privacy Protection Insurance, Policy Wording (n.d). p3 to 10.

[188] Kesan J. p. & Others, (2005). P 10. Also Cyber insurance: a reference guide, institute for development and research in banking technology. (2017), p 7.

السّوريّ الذي أتاح للمؤمّن أن يتحلّل من واجبه بدفع مبلغ التّعويض إذا ما ساهم المؤمَّن له في تحقّق الخطر غشّاً أو تعمّداً منه ولو اتّفق على خلاف ذلك[189]، إذ إنّ هذا النّصّ عينُ الصّواب، فلا يجوز أن تتحمّل شركة التّأمين عبء مخاطر لم تكن لتحصل لولا التدخل العمديّ للمؤمَّن له وطمعه، **وينطبق هذا النص على التّأمين ضد مخاطر الإنترنت.**

ثالثاً- المطالبات السّابقة لعقد التّأمين: لا تُسأل شركة التّأمين عن الأضرار الحاصلة قبل انعقاد عقد التّأمين؛ لأنَّ مسؤوليّتها عن التّغطية تبدأ من لحظة إبرام العقد، أمّا ما قبله فلا مسؤوليَّة عليها ولا يمكن للمؤمَّن له أو لعملائه المتضرّرين من الخرق السّابق مطالبة شركة التّأمين بدفع التعويضات.

رابعاً- استبعاد الأجهزة المحمولة: وينطوي هذا الاستثناء على أنَّ الأجهزة المحمولة قد تكون أكثر عرضةً للسّرقة؛ كونها غير متّصلةٍ بشيءٍ آخر، كما أنَّها خفيفة الوزن ويمكن حملها في أيّ مكانٍ، ففي حال كان الموظّف يحمل حاسبه المحمول خارجاً، وتعرّض للسّرقة فإنّ الكثير من شركات التّأمين ترفض التّغطية؛ لأنّ احتمال حصول الخرق سيكون كبيراً لكون السارق بات يملك الملفّات كلّها التي يحتويها الجهاز المسروق، وغالباً ما سيقوم بتسريبها، كما أنَّ حالات السرقة هذه لا تكون عشوائيّةً، بل مدروسة بدقّةٍ من أجل عمليات ابتزاز الشركة، وتجنّباً لقيام مسؤولية شركة التّأمين تستثني هذا الخطر. ويرى بعض المحلّلين وجوب طلب المؤمَّن لهم من شركة التّأمين إدخال هذه الأجهزة ضمن التغطية التّأمينية ما دامتِ البيانات مشفّرةً فلا يمكن فكّ تشفيرها بسهولةٍ، وإذا ما حصل الخرق رغم ذلك فلا بدّ من إدخاله ضمن المخاطر المغطّاة كالدخول غير المصرّح به، وما قِيل عن الحواسيب المحمولة يمكن أن ينطبق على الأجهزة المحمولة كلّها كالهواتف الذكيّة، والفلاشات(usb)، وغيرها[190]. كما يدعم ويبرر هذا الاستثناء أنّ القوانين بحدّ ذاتها تعاقب الشركات على سرقة أجهزتها المحمولة إذا لم تقم بتأمين الحماية الكافية لهذه الأجهزة لمنع تسرّب البيانات التي تحتويها، ويتمّ بناءً على ذلك فرض غراماتٍ باهظةٍ من أجل محاولة الضّغط على الشّركات لتحسين الأنظمة اللازمة لإدارة مخاطر

---

[189] المادة (734) من القانون المدني السوري رقم 84 لعام 1949.

[190] https://www.irmi.com/term/insurance-definitions/laptop-exclusion

تاريخ الزيارة: 18\6\2020، الساعة 10:55..p.m

المعلومات التي قد تتعرّض لها، إذ فرضت إحدى السلطات الماليّة البريطانيّة غرامةً على إحدى الشركات نتيجة سرقة الحاسب العائد لأحد موظّفيها وإفشاء المعلومات التي يحتويها[191]، وفي هذا الإطار تقدّم شركة GAI تغطيةً للأجهزة المحمولة غير المشفّرة بحال تمّ خرقها نتيجة عمليّة سرقة، وذلك على خلاف الاستثناء السائد[192].

خامساً- الفشل والإهمال: تستثني شركة التّأمين عادةً من تغطيتها التّأمينية فشل المؤمَّن لهم في تحسين أنظمتهم التي يستخدمونها وعدم القيام بتحسين بيئة الأمن الإلكترونيّ _إن لم تكن هذه الخدمات مقدّمة من جانب شركة التأمين_ فلا يعير المؤمَّن لهم الاهتمام الكافي لأهميّة تحديث الأنظمة المستخدمة، وبرامج مكافحة الفيروسات والتجسّس فيتركون أجهزتهم عرضةً للاختراق لا سيّما إذا ما كان هنالك عيوبٌ وثغراتٌ في أنظمتهم الحاليّة، بالإضافة إلى أنَّ البرامج الضّارّة يتمّ تطويرها باستمرارٍ لمقاومة أنواع الأنظمة، وهو ما يبرز أهميّة تحديث مستويات الأمان للبقاء في بيئةٍ إلكترونيّةٍ آمنةٍ، ولذلك تستبعد شركات التّأمين التّغطية في هذه الأحوال؛ لأنّها نابعةٌ من فشل المؤمَّن لهم، إضافةً لكونها تخالف التزام المؤمَّن له بالتقيد بتعليمات شركة التأمين وبذل عناية كافية. كما أنَّ الخلل في برامج الحاسب نتيجة أخطاء البرمجة لا يتمّ تغطيتها أيضاً، لأنّه من المفترض أن تكون واضحةً للمؤمَّن له، وهذا الأمر يقع على عاتق المختص بالبرمجة، وليس على عاتق شركة التّأمين[193]، كما يدخل في إطار الفشل والإهمال عدم قيام المؤمَّن لهم بتشفير بياناتهم وجعلها متاحةً للجميع، ما يُسهّل عمليّة كشف هذه المعلومات، وكذلك قيام المؤمَّن له وتابعيه بالدخول إلى مواقعَ غير آمنةٍ مع علمهم بذلك وعدم الاكتراث له، ممّا يسهّل عملية إصابة الأنظمة بالبرامج الضارة؛ لأنّ هذه المواقع غالباً ما تكون مواقعَ اصطيادٍ مليئةٍ بالبرامج الخبيثة، فضلاً عن إهمال المؤمَّن له الكشف عن حصول عمليّة خرقٍ لأنظمته وتسريبٍ لبياناته المخزّنة في حال كان على علمٍ بذلك لِمَا ينطوي عليه من غشٍّ لشركة التّأمين والعميل في آنٍ معاً، ويزيد من الأضرار الحاصلة نتيجة لعدم علم العميل بذلك ولعدم قدرة شركة التأمين على تقديم خدمات الاستجابة

---

[191] Financial Services Authority. (2012). Annual Report, p 27.

[192] https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage

تاريخ الزيارة: 28\6\2020، الساعة 9:30 p.m.

[193] Kesan J. p. & Others, (2005). P 15.

للحوادث، وقد يبرّر المؤمَّن له ذلك من خوفه من الفضيحة التي قد تلاحقه نتيجة لعمليّة الخرق، وما ينتج عنه من ضررٍ لسمعته التجارية[194]. وعلى الرّغم من شيوع هذا الاستثناء، فإنّ شركة chubb تختار أن تقدّم تغطيةً عن المسؤوليّة النّاشئة عن عدم الحفاظ على سريّة البيانات، مع أنّ هذا قد ينمّ عن إهمالٍ من جانب المؤمَّن له، كما تقدّم الشّركة تغطيةً لخسارة انقطاع العمل نتيجة خطأ برمجة أو أخطاء بشريّة أو نتيجة فشل في أمان الشركات[195].

سادساً- البيانات التي تُحفَظ من جهة غير المؤمَّن له: تستثني وثائق التّأمين البيانات التي يقوم المؤمَّن له بتخزينها لدى موردٍ خارجيٍّ في حال اُختِرقت أنظمته وكُشِفت البيانات المحفوظة، ويبدو ذلك منطقياً؛ لأنّ العقد التّأميني قد تمّ بين شركة التّأمين والمؤمَّن له، ولم تكن الجهة الخارجيّة (مزوّد خدمات التخزين) طرفاً في هذا العقد، وبهذه الحالة لا بدّ للمؤمَّن له من التأكّد من أنّ المخزّنين الآخرين يملكون وثائق تأمينهم الخاصّة للتّغطية بحال الخروقات[196]، كما أنّ الأعطال التي تُصيب الأنظمة الخارجة عن إدارة المؤمَّن له لا تدخل في التّغطية، كفقدان السّيطرة على نظامٍ تابعٍ لمزوّد خدمات الإنترنت الذي يشترك فيه المؤمَّن له.

سابعاً- أعمال الحرب والإرهاب: كثيراً ما تستبعد وثائق التّأمين المخاطر التي تصيب الشّركات نتيجة أعمال الحرب الإلكترونيَّة التي تندلع بين الدّول، أو أعمال الإرهاب الإلكتروني التي ترتكبها جماعاتٌ إرهابيّةٌ تهدف من وراء ذلك إلى تحقيق أهدافها الدّنيئة، كما لو أعلن المخترقون عن أنفسهم كجماعاتٍ تتبع جهاتٍ رسميّةً في دولةٍ ما، أو تنظيماتٍ إرهابيّةً ما تظهر وقت نشوب الحرب بين الدول المعنية، وتقوم بممارسة أعمال الخرق والدخول غير المصرّح به إلى الشّركات والمؤسّسات الموجودة في البلد المعني بالهجوم، وتنشر البيانات المسروقة كأحد أساليب الحرب أو الإرهاب، وهنا يمكن لشركة التّأمين أن تتحلّل من التزامها بدفع التّعويض للمؤمَّن له، ولسبب رئيسٍ هو أنّ الخطر هذا قد يكون عامّاً وكبيراً في وقتٍ واحدٍ يخرج عن قدرة شركة التّأمين على تغطيته،

---

[194] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). P 7.

[195] https://www.chubb.com/uk-en/business/by-category-cyber-enterprise-risk-management.aspx تاريخ الزيارة: 24\6\2020، الساعة 11 .p.m.

[196] Purchasers' Guide to Cyber Insurance Products. (2016). P 14.

ويمكن تضييق نطاق هذا الاستثناء عبر تحديد دولٍ معيّنةٍ قد تكون هنالك حرب لها مع دولة المؤمَّن له، فعندها يستبعد الدفع وفي أحوالٍ أخرى يمكن التّعويض[197]. ومن أبرز الأمثلة على استثناء الحرب من وثائق التّأمين ضدّ مخاطر الإنترنت ما حصل مع شركة موندیلیز المؤمَّن لها وشركة زيوريخ للتأمين، وسيُشرَح ذلك لاحقاً، ولكن على عكس الاستثناء المذكور فإنَّ شركة GAI تقدم في وثائق تأمينها ضدّ مخاطر الإنترنت تغطيةً لمخاطر الحرب والإرهاب الإلكتروني[198].

ثامناً– القيام بالأعمال الإجراميَّة: ويضمّ مفهوم الأعمال الإجراميَّة أعمالاً كثيرةً، فتدخل في نطاقها الأعمال المخالفة للقانون كارتكاب الجرائم الإلكترونيّة، والأفعال الاحتياليّة التي تمارسها الشّركات تجاه الغير في محاولةٍ لكسب الأموال، وأفعال السرقة الإلكترونية وانتهاك الخصوصية التي تقوم بها تجاه منافسيها، وهو ما يُشكِّل عمليّة جمع البيانات بشكلٍ غير قانونيٍّ أو غير مصرّح به، مثل سرقة العلامات التّجاريّة التي تملكها الشّركات المنافسة، أو القيام بإطلاق شائعاتٍ تهدف إلى الإضرار بسمعة المنافس، والانتهاكات المتعمدة للقوانين، والممارسات التّجاريّة غير العادلة التي تضمّ أعمال المنافسة غير المشروعة والاحتكار، وانتهاك براءات الاختراع والإفصاح عن الأسرار التّجاريّة، وقيام المؤمَّن له بنقل البرامج الضّارّة المبرمجة أو المعدّلة من قبل صاحب الوثيقة لما يشكّله ذلك من أعمالٍ غير قانونيّةٍ؛ ولأنَّ المؤمَّن له كان يهدف إلى إلحاق الضَّرر بغيره[199].

تاسعاً– تستثني شركة تأمين AXA من وثائق تغطية أعمال الاحتيال الإلكتروني عمليّة **سحب النّقود من ماكينات الصرّاف الآلي**؛ لأنَّ عمليّة السّحب تتمّ بطريقةٍ تقليديةٍ[200].

وقد تضع بعض شركات التّأمين استثناءً للتّغطية في حال دُمّرت أو حُجِزت البيانات من قبل الحكومات والدول، وهذه الاستثناءات المذكورة هي الأكثر شيوعاً بين شركات التّأمين، وقد تضع شركات تأمينٍ

---

[197] Ibid, p 12-13.

[198] https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage

تاريخ الزيارة: 28\6\2020، الساعة 11:30.p.m

[199] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). P 7.

[200] https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf

تاريخ الزيارة:19\ 9\ 2020، الساعة 10:30 p.m.

أخرى استثناءاتٍ مختلفةً تبعاً لطبيعة أعمال المؤمَّن له، كما قد ترفض بعض شركات التّأمين تغطية أعمال تدريب الموظفين، وقد لا تتم تغطية بعض المطالبات المقدّمة من جانب الحكومات أيضاً، كما لو فُرِضت غرامةٌ على المؤمَّن له فلا يُدفَع التعويض عنها من جانب شركة التّأمين، ومهما قيل تبقى عمليّة تحديد التغطيات والاستثناءات عمليةً تعاقديّةً صِرفةً عائدةً لإرادة المتعاقدين وحسب الحاجة، وحيث أنَّه يبدو من المفيد بعد التّعرّف على التّغطيّة التّأمينية تبيان آليّة هذه التّغطيّة في المطلب الثانيّ.

المطلب الثَّاني

آليّة التّغطيّة التّأمينية في عقد التّأمين ضد مخاطر الإنترنت

تلتزم شركة التّأمين بتقديم التّغطية التّأمينيَّة في أثناء فترة عقد التّأمين المُبرم بينها وبين المؤمَّن له ما دام الأخير ملتزماً بأداء أقساط التّأمين المتَّفق عليها، وحيث أن عملية التغطية التّأمينية تنطوي على الخدمات المقدمة من شركة التّأمين من حيث دفع مبالغ التعويض عند حصول الخطر المؤمن منه، ومعرفة المدة التي يبقى هذا الالتزام قائماً على عاتق شركة التّأمين، وعليه سيُقسم هذا المطلب إلى فرعين، في الأوّل منهما يتناول دفع مبالغ التعويض، وفي الثانيّ تحديد قيمة المبالغ ومدة الالتزام.

الفرع الأوّل

دفع مبالغ التعويض في عقد التّأمين ضد مخاطر الإنترنت

تنطوي عملية دفع مبالغ التعويض على تحديد الطريقة المتبعة في الدفع، وعن تاريخ الدفع الذي تلتزم به شركة التّأمين ضد مخاطر الإنترنت.

أولاً: أمَّا عن طريقة دفع مبالغ التَّعويض فهي قد تكون تقليديَّةً تتمّ عبر الوسائل التَّقليديَّة ليُدفَع مبلغ التّأمين من جانب شركة التّأمين إلى المؤمَّن له، أو إلى المستفيد منه في حال كان تأميناً ضدّ المسؤوليّة، ويُدفع هذا المبلغ في مكان عمل شركة التّأمين استناداً لقاعدة الدين مطلوب وليس محمول. **وتكمن الصّعوبة هنا في**

حال كانت شركة التّأمين أو المؤمَّن له شركةً إلكترونيّةً لا وجود لها على الواقع، وهو إن كان احتمالاً لكنّه واردٌ، فهذه الشّركات يُفترض ألّا يكون لها مكان عملٍ على الأرض، ففي هذه الحالة كيف سيُدفع مبلغ التّأمين؟

يبدو من الواضح أنَّه لا بدَّ من اتّباع الوسائل الإلكترونيَّة في الدّفع، كالتّحويلات المصرفيّة الإلكترونيّة، والتي ستُستخدم أيضاً لدفع الأقساط من جانب المؤمَّن له، فإن كانت شركة التّأمين شركةً إلكترونيّةً فيفترض ألّا يوجد لها مكانٌ ماديٌّ ليذهب إليه المؤمَّن له، لذلك لا بدّ من الوسيلة الإلكترونية. كما أنَّ هذه الوسائل لا تقتصر على حالة الشركات الإلكترونية، بل يمكن استخدامها مع كون الطّرفين شركاتٍ تقليديّةً بحتةً؛ لأنّها الوسيلة الأسهل والأكثر رواجاً، فيتمّ الدفع بأيّ وسيلةٍ إلكترونيةٍ يتّفق عليها الأطراف. والسائد حالياً ونظراً لانتشار عمليات الدفع الإلكتروني، مع الاتجاه الواسع نحو التخلي عن التعامل النقدي التقليديّ هو اتّباع وسائل الدفع الإلكتروني، عبر التحويل الإلكترونيّ من حساب المؤمَّن له إلى حساب شركة التّأمين بصورةٍ مباشرةٍ وسريعةٍ وفعّالةٍ.

ثانياً: وعن تاريخ الدّفع فهو بعد مدّةٍ محدّدةٍ من الإخطار الذي يرسله المؤمَّن له إلى شركة التّأمين إشعاراً بحصول الخطر المؤمّن ضدّه، كما أنَّ شركة التّأمين تضمن المخاطر كلّها التي تنتج عن خطأ المؤمَّن له نفسه وأخطاء تابعيه. **والحقيقة في إطار عقد التّأمين ضدّ مخاطر الإنترنت وخصوصيته** إذا ما كان المؤمَّن له شركةً تمارس الأعمال الإلكترونيّة، فهذه الشركة لا يمكن لها التعبير عن إرادتها بنفسها، بل لا بدّ لها من نائبٍ يعبّر عن إرادتها وفقاً للقانون المدنيّ السّوريّ[201]، فإذا وقع الخطأُ من أيّ من هؤلاء الممثّلين للشّخص الاعتباريّ فيُعدّ كما لو أنَّه وقع منه نفسه (ولا يمكن القول إنّه وقع من تابعيه؛ لأنّهم ممثّلون لإرادته)، ويمكن التّدليل على ذلك في أنّ القوانين الجزائيّة تقوم بمساءلة الشّركات والمؤسّسات عن الأفعال التي يرتكبها ممثّلوها باسمها وتعتبر كما لو أنّها قامت بها بنفسها[202]، أمّا عن أخطاء الموظّفين لدى المؤمَّن له فتضمنها شركة التّأمين أيضاً؛ لأنّهم

---

[201] المادة (55) من القانون المدني السوري رقم 84 لعام 1949.

[202] والأكثر من ذلك أنّه لو كان المؤمَّن له شركة مساهمة فلا تخضع علاقة مجلس الإدارة بالشركة لعقد العمل، وهو ما ينفي أيضاً مسؤولية المتبوع عن أعمال تابعه (علاقة التبعية)، انظر المادة (16) من قانون الشركات السوري رقم (29) لعام 2011.

تابعون للمؤمَّن له ، وإذا كان المؤمَّن له فرداً يدير عمله عبر الإنترنت فيمكن اتّخاذ نظريّة مسؤوليّة المتبوع عن أعمال التّابع كمبدأٍ لضمان شركة التّأمين لأعمال التّابعين للمؤمَّن له.

ولكن قد تخلُّ شركة التّأمين بواجبها التّأميني، فلا تقوم بدفع مبلغ التعويض عند تحقّق الخطر المؤمَّن ضدّه رغم عدم وجود أيّ سببٍ يبرّر تعنّتها في القيام بالتزامها. فيكون أمام المؤمَّن له خيارات عدّة، ولا ريب أنّ أهمّها لا سيّما في لحظة تحقّق الخطر هو الطّلب من القضاء إجبار شركة التّأمين على تنفيذ التزامها بدفع مبلغ التّأمين، وما دام الالتزام ينطوي على دفع مبلغٍ ماليٍّ فهو قابلٌ للتنفيذ دائماً، إذ أن اللجوء إلى القضاء هو الخيار الأول للمؤمَّن له، فإذا ما كان الخطر من ضمن قائمة المخاطر المغطاة، فيكون للقضاء أن يلزم شركة التّأمين بهذا الأداء، وأن يفرض عليها غرامةً نتيجة لتخلفها عن واجبها المطلوب منها، مادام المؤمَّن له قد أدى واجباته على أتم وجهٍ وهو الهدف الأبرز من هذا العقد.

ولكن في حال لم يرد المؤمَّن له اللجوء إلى الخيار القضائي وطلب التنفيذ، نظراً لأن التّأمين في الوقت المطلوب لم يعد مجدياً، أو لأن مبلغ التّأمين لا يكفي لتعويضه عمّا أصابه من ضررٍ، فيحقّ له طلب فسخ العقد تبعاً للقواعد العامة في العقود التي تعطي لأحد الأطراف الحقّ في طلب فسخ العقد في حال امتناع الطّرف الآخر عن أداء التزاماته، بشرط أن يكون الأوّل قد أدّى التزاماته الكاملة، وفي هذا لا يختلف التّأمين ضد مخاطر الإنترنت عن غيره من عقود التّأمين، نظراً لكونه عقد كسائر العقود، وذلك مع احتفاظه بحق التعويض عن الضرر الحاصل نتيجة عدم أداء شركة التّأمين لواجبها بالتغطية التّأمينية.

وقد يُتّفق على الفسخ تلقائياً دون إخطار عند الامتناع عن الدّفع، أو قضائياً بحكمٍ قضائيٍّ، ويُحدّد ذلك في الوثيقة، كما يحقّ للمؤمَّن له طلب التّعويض بالإضافة إلى الفسخ نتيجةً للأضرار التي تلحقه جرّاء تملّص شركة التّأمين من واجبها بالدّفع. **وفي إطار عقد التّأمين ضد مخاطر الإنترنت لايبدو من المنطق طلب فسخ العقد نظراً لأن كل الأقساط المدفوعة لن تعادل قيمة الضرر عند وقوعه، بل إنه ليس من مصلحة المؤمَّن له طلب الفسخ والتعويض لأنه ومهما بلغت قيمة التعويض فلن تعادل مقدار الضرر اللاحق به، لذلك فإن هذا المبدأ غير قابل للتطبيق في نطاق تأمين مخاطر الإنترنت.**

ويدور تساؤلٌ، حيث ينطوي التّأمين ضدّ مخاطر الإنترنت على دفع أقساطٍ تقابل تعويضاً بعد حصول الخطر، وتقابل أيضاً الخدمات التي تقدّمها شركة التّأمين لعميلها كخدمات المراقبة التي تحمي من انتهاكات الهويّة أو خدمات تدريب الموظّفين أو خدمات تحسين الأنظمة، فكيف ستُردُّ هذه الخدمات من جانب المؤمَّن له في حال فُسِخ العقد؟

الحقيقة أنّ هذه الخدمات لا تُردّ، لأنَّ عقد التّأمين ضدّ مخاطر الإنترنت من العقود المستمرة والتي يكون فيها الفسخ للمستقبل فقط، ولا يؤثّر على ما تمّ سابقاً في مرحلة سريان العقد، كما أنَّ هذه الخدمات (ما كان منها قبل تحقّق الخطر أو بعده) قُدِّمت مقابل الأقساط المدفوعة، وعليه لا يُردّ أيُّ قسطٍ أو خدمةٍ من جانب أيٍّ من الطرفين، فما حصل في الماضي صحيحاً يبقى منشئاً لآثاره القانونيّة كلّها، ويقتصر الفسخ على المستقبل، فيتوقّف دفع الأقساط وتقديم الخدمات وتحمّل أعباء المخاطر المحتملة، وذلك استناداً إلى القواعد العامة في العقود التي تحكم العقود المستمرة والتي تجعل انتهاء هذه العقود يتمّ بأثرٍ مباشرٍ دون أيّ تأثيرٍ على ما تمَّ سابقاً.

الفرع الثاني

تحديد مبالغ التّأمين ومدة الالتزام في عقد التّأمين ضد مخاطر الإنترنت

تغدو عملية تحديد مبالغ التّأمين عمليّةً معقدّةً بالنسبة لشركات التّأمين، وتلتزم هذه الشركات بتقديم تغطيتها التأمينيّة طيلة المدة المتّفق عليها.

أولاً: وفي نطاق تحديد مبالغ التّأمين فإنَّ هذه العمليّة تتمّ بالاتفاق بين الطَّرفين، مع الأخذ بالحسبان صعوبة تحديد المبالغ؛ نظراً لطبيعة مخاطر الإنترنت، حيث أن التّأمين ضد مخاطر الإنترنت يتعامل مع أخطارٍ إلكترونيّةٍ، أي أخطارٍ غير ماديّةٍ وغير ملموسةٍ تتطور بسرعة كبيرة، وتزداد حدتها بشكل أكبر من أن تجاريها شركات التّأمين، ولمّا كان الهجوم الإلكترونيّ يسبب خسائرَ كبيرةً يصعب إحصاؤها، لأن الخسائر لا تقتصر على سرقة بيانات، أو تعطيل أنظمة، وإنّما تمتد إلى إلحاق الأذى بسمعة الشركات وهي عناصرٌ معنويّةٌ لا تقاس بسهولة، لذلك كله تواجه شركات التّأمين صعوباتٍ في تحديد مبلغ التعويض الواجب دفعه، ومن قبله في تحديد

مبلغ التّأمين عند إبرام العقد، وعلى ما ذُكر يُحلّل الخطر من حيث حجمه، وأهميّته، وآثاره، ومدى احتمال حصوله، وطبيعة العمل، وغيرها من أسئلةٍ تحاول شركة التّأمين الحصول على أجوبةٍ عنها لتحديد المبلغ، بالإضافة إلى الربح والفائدة التي يجنيها، ورأس المال الذي يملكه، والأقساط التي سيدفعها المؤمَّن له، ومدّة التّغطية، ومدى الأمن الإلكترونيّ المطبق، كلّها عوامل لا بدّ من أخذها بعين الاعتبار من أجل الوصول إلى تحديد مبلغ التّأمين ضدّ مخاطر الإنترنت، وهو الحدُّ الأعلى للتّعويض الذي سيدفع ليتوافق مع حاجة المؤمَّن له وإمكانيّة شركة التّأمين، حيث أنّه يُطبَّق على عملية تحديد مبلغ التّأمين **مبدأ التعويض**، نظراً لكون عقد التّأمين ضدّ مخاطر الإنترنت عقد تأمينٍ من الأضرار، ومقتضى هذا المبدأ وجوب تساوي قيمة مبلغ التّعويض مع الخسارة الحاصلة، فلا يزيد عنه بغية عدم إثراء المؤمَّن له على حساب شركات التّأمين، وإن كان يمكن أن يقل التّعويض عن إجمالي مبلغ التّأمين[203].

وعلى سبيل المثال: تقدّم شركة GAI تغطياتٍ تصل لحدود 10 ملايين دولار مقابل أقساط حدّها الأدنى تبدأ ب500 دولار[204]، في حين تقدم شركة AXA سنغافورة تغطيةً بمبالغ تصل ل50 ألف دولار سنغافوري[205]، وقد تأتي صيغة التّغطية واسعةً ومبهمةً تثير بعض النّزاعات حول مدى وجوب دفع التّأمين، ما يدفع بالطّرفين إلى القضاء للتّوصّل إلى حلٍّ، ولا بدّ في هذا الإطار من تطبيق مبدأ التفسير الواسع للنّصّ من أجل محاولة الحصول على تغطيةٍ أوسعٍ، من أجل حماية المؤمَّن له الطرف الضعيف في هذا العقد لعدم وجود شركات تأمينٍ متعدّدةٍ تغطّي مخاطر الإنترنت، كما أنَّ قلّة وجود وسطاء التّأمين في هذا النّوع من التّأمين ترخي بظلالها على هذه الصّناعة؛ إذ يؤدّون دوراً واسعاً في محاولة إيجاد الوثيقة الأفضل للمؤمَّن لهم انطلاقاً من طبيعة أعمالهم، وتحليل المخاطر التي يتعرّضون لها، ولذلك في ظلِّ هذا النّقص قد يختار المؤمَّن لهم الوثيقة وحدهم، ما يوقعهم في خطأ اعتقاد أنّ هذا الخطر مغطّىً بالوثيقة المُشتراة؛ نظراً لفهمٍ خاطئٍ للنّصّ، ولهذه الأسباب المذكورة سابقاً

---

[203] عبد ربه، (2006)، ص101 وما يليها.

[204] https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage

تاريخ الزيارة: 30\6\2020، الساعة 8:30.p.m

[205] https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf

تاريخ الزيارة: 20\9\2020، الساعة 10:25 p.m.

كلّها لا بدّ من أن ينصف القضاء المؤمَّن لهم ويضمن لهم تغطيةً أوسعَ لحمايتهم من طمع شركات التّأمين ضدّ مخاطر الإنترنت. ولا ريب أنّ من أهمّ مبادى عقد التّأمين ضد مخاطر الإنترنت مبدأ الحلول الذي يقضي بحقّ شركة التّأمين بأن تعود على الغير الذي تسبّب في حصول الخطر المؤمّن ضدّه بالتّعويض عمَّا دُفِع للمؤمَّن له، **لكنّ التساؤل هنا أيضاً يتعلَّق بالصّعوبة التي تواجهها شركة التّأمين في تحديد الشّخص واجب الملاحقة؛** لأنَّ مخاطر الإنترنت يرتكبها مهاجمون إلكترونيون من أيّ دولةٍ في العالم عبر هجماتٍ متلاحقةٍ في أيّ وقتٍ، وقد تمتدُّ لساعاتٍ طويلةٍ ولعدم كشفهم تُتّبع وسائلُ تسمح ببقائهم متوارين عن الأنظار عبر إخفاء عناوين IP التي حصل منها الهجوم، وهو ما يسمح بعدم معرفة الدّولة مصدر الهجوم، بل أكثر من ذلك في أنّ بعض الهجمات تتمّ عبر قنواتٍ رسميّةٍ تتبع لدولةٍ ما، وهو ما يزيد الأمر تعقيداً على شركات التّأمين ضدَّ مخاطر الإنترنت لملاحقة المتسبّبين بالأضرار، وهذه المشكلة لا يمكن التغلّب عليها في الوقت الحالي، ولهذا غالباً ما يُحاوَل التقليل من أضرارها على شركات التّأمين عبر رفع قيمة الأقساط، وتقليل قيمة حدود مبالغ التّأمين، ووضع بعض القيود على التّغطيات، وتحليل المخاطر بشكلٍ جيّدٍ ودقيق.

وفي حال قيام شركة التّأمين بواجبها في التغطيّة التّأمينيّة، فإن القانون قد أعطاها الحقّ بالحلول محلّ المؤمَّن له في كل الحقوق التي يكتسبها الأخير تجاه الغير الذي تسبب في الضرر، وهو ما يُسمّى **بمبدأ الحلول،** ويهدف إلى عدم حصول المؤمَّن له على أكثر من تعويضٍ عن الضرر المتّحقق حتى لا يتّحول عقد التّأمين ضد مخاطر الإنترنت إلى مصدر ربحٍ غير مشروعٍ، فعند حصول الخطر تدفع شركة التّأمين مبلغ التّأمين الذي يتطابق مع مقدار الخسارة الحاصلة ومن ثم تحلُّ مكان المؤمَّن له في كل الحقوق والواجبات التي يملكها تجاه الغير المتسبّب في الضرر ويتولّى مطالبة الغير بكل حقوق المؤمَّن له، ولكن تقتصر هذه المطالبة على ما دفعه كمبلغ تعويضٍ مع الفائدة فقط وإن زادت الخسارة عن مقدار التّأمين، فيبقى للمؤمَّن له الحق في الرجوع بنفسه على الغير كما أنه لا يجوز أن تعود شركة التّأمين على الغير إلا بعد دفع التعويض عبر إبراز إيصالٍ يُثبت

ذلك[206]، وعلى هذا سار المشرع السوريّ عندما تحدّث عن التّأمين على الحريق حول حق شركة التّأمين بالحلول قانوناً بأخذ التعويض الذي يُحكم به للمؤمَّن له على من تسبّب بحصول الحريق[207].

ثانياً: أما عن تحديد المدة التي تبقى فيها شركة التّأمين ملتزمة بأداء مبلغ التّأمين، فهي تبقى مستمرةً طوال الفترة المتّفق عليها في وثيقة التّأمين، ما دام المؤمَّن له مستمراً بأداء الأقساط وغيرها من الالتزامات التي تفرضها عليه شركة التّأمين، وليس له أن يمتنع عن دفع مبلغ التّعويض عند حصول الخطر إلّا في حال كان الخطر الحاصل داخلاً ضمن أحد الاستثناءات المذكورة سابقاً. وفي حال تم إنهاء وثيقة التّأمين لأيّ سببٍ آخرَ غير سبب عدم دفع الأقساط كحالة انتهاء الوثيقة وعدم تجديدها، فإنّ شركة زيوريخ للتّأمين تقدّم تمديداً تلقائيّاً للتّغطية لمدة 90 يوماً بعد انتهاء فترة التّأمين فيما يتعلق بأيّ مطالبةٍ يتم تقديمها لأول مرة ضد المؤمَّن له، وتمّ إبلاغ شركة التّأمين عنها كتابيّاً خلال فترة 90 يوماً (فترة الإبلاغ الممتدة تلقائيّاً)، ولكن فقط فيما يتعلق بأيّ فعلٍ غير مشروعٍ يُرتكب في أثناء فترة التّأمين وقبل الانتهاء، ولا يتم دفع أيّ قسطٍ إضافيٍّ مقابل فترة إعداد التّقارير التلقائيّة الممتدة[208].

وكما أنّه في حال أُلغيت الوثيقة أو لم تجدّد أو استُبدِلت بأخرى فيمكن أن تكون فترة التبليغ الممتدّة متاحةً للمطالبات والدّعاوى التي تُجرى لأوّل مرّةٍ خلال فترة سريان الوثيقة، أو في أثناء فترة الإبلاغ، كما قد يطلب أن تكون التّغطية عامّةً لكلِّ أنحاء العالم (وثيقة شاملة) دون تحديد مكانٍ معيّنٍ ليحصل فيه الهجوم أو تُقام فيه الدعوى، وهو ما يُطلق عليه عدم إقليميّة التّغطية فلا يشترط أن تكون البيانات المخزّنة أو الأنظمة المتضرّرة موجودةً في مكانٍ معيّنٍ ليُدفَع التعويض، في حين قد تتضمّن بعض الوثائق شرط الإقليمية لمحاولة حصر الأضرار، ولتتناسب مع قدرة شركة التّأمين على الدفع، فلا تنهال عليها المطالبات من كلّ أنحاء العالم[209]، وهو

---

[206] العمري، شريف محمد، عطا، محمد محمد. (2012). الأصول العلمية والعملية للخطر والتأمين، ط:1، (د.ن.)، ص 111..

[207] المادة (737) من القانون المدني السوري رقم (84) لعام 1949.

[208] https://www.zurichna.com/knowledge/topics/cyber

تاريخ الزيارة: 2020\5\28، الساعة 10:30 p.m.

[209] Cyber insurance: a reference guide, (n.d), p 7.

ما تقدّمه شركة chubb في تغطيتها العالميّة للمؤمَّن له في أيّ مكانٍ يحصل فيه الخطر الإلكترونيّ[210]، **ويظهر في هذه الشروط أحد ميّزات هذا النوع من التّأمين لناحية تغطيته الشّاملة وعدم إقليميّته.** وإجمالاً فإنَّ الوثائق التّأمينيّة هي نتاج التّعاون بين شركة التّأمين والمؤمَّن له من أجل تحديد مقدار التغطية بما يناسب المخاطر التي قد يتعرّض لها المؤمَّن له، وبما يتناسب مع رأسمال شركة التّأمين، وقدرتها على الدّفع، وتُحدّد مدّة الوثيقة في العقد، ويمكن عند نهايتها إعادة تجديدها لعامٍ آخرَ، وقد تُعدّل التغطيات السّابقة وتُضاف مخاطرُ جديدةٌ.

كما أن بعض شركات التّأمين تمنع المؤمَّن لهم من أن يتّصرفوا بوثيقة التّأمين لأحدٍ آخرَ سواهم، ومن هذه الشركات شركة رأس الخيمة الإماراتيّة (راك)، والتي لم تجز التنازل عن هذه الوثيقة إلا بموافقةٍ خطيّةٍ مسبقةٍ منها، وذلك نظراً لطبيعة العقد الذي يقوم على حسن النية، وعلى طبيعة عمل المؤمَّن له، والمخاطر المحيطة به، والعوامل التي تسهّل حصول الخطر، وإمكانية اتخاذ إبرام العقد من قبل مؤمّنٍ له أول كوسيلة احتيال لنقله إلى المؤمَّن له الآخر، والذي قد لا تقبل شركة التّأمين تغطيته، نظراً لضعف أنظمته الأمنيّة، أو لوجود سوابق حوادثٍ إلكترونيّةٍ[211].

وفي ختام هذا المطلب لا بدَّ من لمحةٍ سريعةٍ عن وضع التّأمين ضد مخاطر الإنترنت في المنطقة العربيَّة، فهي ما تزال بعيدةً إلى حدٍّ ما عن التّغطيات السيبرانيّة، إذ إنّه حتى الآن ما يزال موضوع التّأمين ضدّ مخاطر الإنترنت قيد الدّراسة والمناقشة والتوصيات فقط، دون وجود شركاتٍ تقدّم تغطيةً سيبرانيّةً إلّا بشكلٍ خجولٍ جداً. ومن بين التوصيات ما أصدره الاتّحاد المصريّ للتّأمين من ضرورة توفير التّغطيات للهجمات الإلكترونيّة، لا سيّما في ظلِّ جائحة كورونا التي أجبرت الموظّفين في مصرَ على العمل من منازلهم، وما نتج عن ذلك من ازدياد الهجمات الإلكترونيّة عبر إرسال رسائلَ على البريد الإلكترونيّ مرفقةٍ بروابطَ تحتوي على برامج ضارّةٍ تعمل على خرق وتدمير البيانات، وأوصى الاتّحاد بالقيام بتسويق الوثائق الإلكترونيّة في أثناء الفترة المقبلة، وتخصيص الموارد اللّازمة لتحديد وإدارة المخاطر، ومحو الأميّة الرّقميّة داخل بيئة العمل، بسبب تصنيف

---

[210] https://www.chubb.com/hk-en/business/cyber-insurance.html

تاريخ الزيارة: 15\6\2020، الساعة 11 p.m.

[211] Simply Cyber Policy Terms & Conditions (2018). RAK insurance, v1, p19.

المخاطر الإلكترونية كثاني أكبر خطرٍ ستواجهه الشركات العالميّة في العقد المقبل[212]. في حين أكَّد خبراءُ في التّأمين أنّ سوقاً واعدةً للتّأمين ضدّ مخاطر الإنترنت بدأت تتشكَّل ملامحها في دول الخليج العربيّ، ولا سيَّما في الإمارات في ظلِّ انتشار المخاطر الإلكترونيَّة على نطاقٍ واسعٍ، وما تسبّبه من أضرارٍ وخسائرَ كبيرةٍ، بالإضافة إلى بدء انتشار أجهزة إنترنت الأشياء، وغياب برمجيّات الحماية، إذ يشير أحد خبراء التّأمين إلى أنَّه يُعاب على سوق التّأمين ضدّ المخاطر السيبرانيَّة في الإمارات محدوديّته؛ لغياب الوعي بهذه المنتجات والأخطار واعتبار الشّركات في معظمها هذه التّغطية مجرّد عبءٍ ماليٍّ، رغم أنّ البنوك والشركات المالية والاستثمارية بالإضافة إلى الشركات في قطاع الصّناعة هي أكثر الشّركات عرضةً للمخاطر السيبرانية[213]. أمّا في سورية فبدأت هيئة الإشراف على التّأمين عبر ورشة عمل _في النصف الثاني من العام 2019_ مناقشتها بخصوص تأمين مخاطر الجرائم الإلكترونيّة، عبر تحليل عيّناتٍ من الجرائم الإلكترونيَّة، وقانون مكافحة هذه الجرائم، والحلول التّقنيّة لها، وتوصّلت الورشة إلى التّوصية بتشكيل لجنةٍ فنيّةٍ بالتعاون بين هيئة الإشراف على التّأمين وشركات التّأمين جميعها والهيئة الوطنية لخدمات الشبكة ومهمّتها دراسة إمكانيّة إصدار عقود تأمينيّة لتغطية أخطار الجرائم الإلكترونية[214].

أمَّا عن الوضع في شرق آسيا كالصّين واليابان على سبيل المثال _بما أنّه ذُكِر الوضع في سنغافورا سابقاً_ يبدو أنَّ عجلة التّأمين ضدّ مخاطر الإنترنت قد بدأت تعمل الآن بعد سلسلةٍ من الهجمات الإلكترونيَّة، والخسائر الكبيرة، وبدء تطبيق قوانين حماية الخصوصية والبيانات، ما أدَّى إلى تسارع وتيرة تبنّي وثائق التّأمين ضدَّ مخاطر الإنترنت، ففي **الصين** دخل قانون خصوصية البيانات حيّز التنفيذ في حزيران 2017، وفرض على الشركات العاملة هناك التزاماتٍ فيما يخصُّ الأمن السيبراني، ممَّا جعلها تفكّر بجديَّةٍ أكثر بشأن المسؤوليّات التي ستواجهها عندما تتعرّض لبرامجَ ضارّةٍ أو خرقٍ للبيانات، وتضمن الالتزامات واجبة الاتباع من جانب مزوّدي

---

[212] https://www.alborsaanews.com/2020/04/20/1322824

تاريخ الزيارة: 3\7\2020، الساعة 9 p.m.

[213] https://www.albayan.ae/economy/capital-markets/2019-03-28-1.3522036

تاريخ الزيارة: 3\7\2020، الساعة 9:50 p.m.

[214] https://www.nans.gov.sy/ar/article/workshop_entitled_%22insurance_of_the_dang

تاريخ الزيارة: 3\7\2020، الساعة 11:30 p.m.

المنتجات الإلكترونية، وخدمات الشبكة، ومشغّلي الشبكات، وقواعد حماية المعلومات الشخصيّة، إذ مُنع مشغلو الشبكات من الكشف عن المعلومات الشخصية التي يجمعونها أو التلاعب بها، كما مُنع على أيّ مؤسسة أو فردٍ الحصول على المعلومات بطرقٍ غير مشروعةٍ أو بيعها بطرقٍ مماثلةٍ، مع وجوب اتّباع وسائل حماية فنيّة وتقنيّة لضمان أمن المعلومات التي يجمعها، وفي حال حصول تسريب للبيانات لا بدَّ من اتّخاذ تدابيرَ علاجيّةٍ، وإخطار المستخدمين والإدارة المختصة في الوقت المناسب. وفي المحصلة يضع القانون الجديد بوضوح أساساً قانونياً قوياً لتطوير التّأمين السيبراني في الصين _بالإضافة إلى تواتر الهجمات الإلكترونية، ورغبة الشركات بحماية نفسها من التبعات القانونيّة_ كما حدث بالفعل في دولٍ أخرى، كالولايات المتّحدة، والتي أسهم إدخال قوانين حماية البيانات في التطوّر السّريع لسوق التّأمين السيبراني. ويبدو أنّ التّأمين السيبراني الشامل بات متاحاً في الصين من جانب شركات التّأمين الأجنبية، والتي تقدّم تغطيةً لخسائر الطّرف الأوّل، وتعويض الطّرف الثالث. وبمقارنة سوق التّأمين ضدّ مخاطر الإنترنت في الصين مع شمال أمريكا وأوروبا يبدو أنّ الصين ما تزال في مرحلةٍ مبكّرةٍ من التطوّر، فالتّأمين السيبراني متاحٌ في الصّين منذ بضع سنواتٍ فقط وإلى الآن لا توجد خبراتٌ كثيرةٌ في نطاق الخسائر السيبرانيّة للاعتماد عليها، كما أنّ عدد الحوادث المُبلَّغ عنها أقلّ بكثير من العدد الحاصل[215].

أمّا عن اليابان، فلم يكن يوجد لدى شركات التّأمين اليابانيَّة الأصليّة التي تقدم خدمات تأمين على الأشياء تأميناً متخصّصاً ضدّ المخاطر السيبرانيّة، بمعنىً آخر أنّ التّأمين السيبراني في اليابان له طبيعةٌ مشابهةٌ للتّأمين على الممتلكات، والتّأمين ضدّ المسؤولية التّقليديّة، وإلى جانب ذلك لم تُوجد قضيّةٌ رائدةٌ يمكن فيها لأيّ محكمةٍ اتّخاذ قرارٍ بشأن عقد التّأمين ضد مخاطر الإنترنت في اليابان حتى وقتٍ قريبٍ[216]. ومن ثمّ سُنَّ قانون حماية المعلومات الشّخصيّة في عام 2003 ودخل حيّز التّنفيذ في 2005، وبعد ذلك بدأت شركات التّأمين ببيع وثيقة التّأمين لحماية المعلومات الشّخصيّة للشّركات في حال تسرّبت نتيجة الهجمات السيبرانية من بين أمورٍ

---

[215] Wang, F. (2017). Cyber Insurance Ready For Take-Off In China, Shanghai: China, p 2 To 4.

[216] Marano, P., Rokas, I., & Kochenburger, P. (2016) The "Dematerialized" Insurance Distance Selling And Cyber Risks From An International Perspective, Berlin: Germany, Springer, p 201-202.

أخرى. إذ تتمّ تغطية تسريب المعلومات الشخصية التي تخزّنها الشركة ضمن تأمين المسؤوليّة للطّرف الثّالث كاتّفاقٍ خاصّ مدرجٍ في وثيقة تأمين المسؤوليّة العامة، في حين يغطّى الضّرر عن انقطاع أعمال الخادم أو الحاسب ضمن تغطية الطّرف الأوّل في وثيقة التّأمين الشّاملة للحاسب، وقُدِّمت هذه التّغطيات بدايةً من شركة (Tokio Marine & Nichido Fire Insurance) في عام 2012. في حين طرحت الشركة المذكورة في عام 2015 وثيقة تأمين ضد مخاطر الإنترنت شاملةً على نطاق واسع للمؤسسات التجارية والتي تغطّي تكاليف إدارة الأزمات من قبل الشركات والتعويضات عند تقديم مطالبة نتيجة تسريب المعلومات مع نفقات النزاعات[217].

وصفوة القول بعد معاينة التغطيّة التّأمينيّة لمخاطر الإنترنت واستثناءاتها وآليّة التغطيّة التأمينيّة، إنّ هذه التّغطية هي أبرز سمات هذا النّوع من التّأمين وجوهر الفرق بينه وبين غيره من الأنواع، فهي على النّحو الذي ذُكِر تقدّم الحماية المطلوبة للمؤمَّن له خلال فترةٍ سابقة لحصول الخطر، ويعدّ من أبرز إيجابيات التّأمين ضد مخاطر الإنترنت، كما يلحظ أنّ أغلب التّغطيات كانت تندرج تحت نطاق التغطيات للأعمال كالشّركات والمؤسسات أو ما يمكن القول إنّه تغطيةٌ للشخصيات الاعتباريّة في نطاق أعمالها عبر الإنترنت، حتى إنّ المواقع الإلكترونية لشركات التّأمين تدرج هذا النوع من التّأمين تحت مسمى تأمين الأعمال (businesses)، في حين يقتصر تأمين الأفراد على تأمينات الصّحّة، والسّفر، والبطالة، وتأمين السّيّارات، وغيرها. وما يعزّز ذلك أنّ المخاطر المغطّاة مثل هجمات الفيروسات، أو الحرمان من الخدمة، أو قطع الأعمال، تتوجّه في المقدّمة نحو الأعمال التّجاريّة والمشروعات حول العالم، إذ لا نرى كثيراً من المخترقين الذين يقومون بحجب خدمة الإنترنت عن مستخدمٍ ما بشكلٍ شخصيٍّ؛ ولذلك تتوجّه هذه التغطيات بصورتها المباشرة نحو هؤلاء الأشخاص الاعتباريين لحمايتها من التّبعات المترتّبة على حصول هذه المخاطر. لكن هل يعني ذلك أنّ هذه التغطيات لا تمسّ مستخدمي الإنترنت الذين يتلقّون خدماتهم الإلكترونيّة من الشّركة المخترقة؛ أي أنّها تحمي الشّركات بصورةٍ خالصةٍ؟ حيث يبدو أنّ التّغطيات الإلكترونيّة تتوجّه بشكلٍ غير مباشرٍ إلى عملاء الشركات المخترقة عبر تغطية المسؤوليّة عند حصول الخطر الإلكتروني، فالعميل الذي سُرِقت بياناته جديرٌ بالحماية أيضاً في نطاق التغطيات

[217] Ibid, p 206.

الإلكترونية التي تشتريها الشركة المخّزنة معلوماته. وبذلك نجد أنّ التغطية التّأمينية ضدّ مخاطر الإنترنت تحاول في بداية طريقها حماية الشّركات والأفراد على حدّ سواء نوعاً ما، وإن كان الأفراد في مجتمع الإنترنت يرغبون أكثر بوجود وثائقَ تحميهم ضدّ الجرائم التي تمسّ اعتبارهم الشّخصيّ، كالقدح والذّمّ الإلكتروني، وانتهاك الحياة الخاصّة عبر الإنترنت، بالإضافة إلى دخول إنترنت الأشياء حياةَ الكثير من المستخدمين، وما أفرزه هذا الأمر الجديد من مخاطرَ إلكترونيّةٍ، ويُلاحظ هنا وفي هذا المجال قلّة _إن لم تكن ندرة_ وجود تغطية لهذه المخاطر حتى الآن، وإن كان المستقبل حالياً مفتوحاً أمام شركات التّأمين لتطوير الوثائق ضدّ مخاطر الإنترنت لجهة مدّها نحو حماية الأفراد على مستوىً شخصيٍّ فرديٍّ غير عمليٍّ بحت. كما يُثار بعض الانتقاد تجاه هذه التغطية من حيث كونها لا تغطّي في معظمها مخاطر التّصيّد، والتي تحيط بالمؤسّسات والشّركات كلّها، وتشكّل أحد أبرز وأعظم المخاطر التي تكبّدهم الخسائر الفادحة، ولربّما يفسّر اعتزال العديد من شركات التّأمين عن تغطية التصيد؛ لرغبتها الشديدة في التخلص من دفع بعض المبالغ للمؤمَّن لهم، بالإضافة إلى محاولاتها الحثيثة بتوسيع الإعفاءات وتضييق التغطيات لتوفير مبالغ التّأمين.

ويبدو من المفيد بعد بيان واجبات شركة التّأمين في عقد التّأمين ضدّ مخاطر الإنترنت الانتقال في المبحث الثّاني للحديث عن واجبات المؤمَّن له في نطاق هذا العقد.

المبحث الثّاني

التزامات المؤمَّن له

يرتّب عقد التّأمين ضدّ مخاطر الإنترنت **التزاماتٍ** على عاتق المؤمَّن له في مقابل الحقوق التي يحصل عليها، إذ تتبدّى هذه الحقوق في حصوله على مبلغ التعويض عند حصول الخطر، بالإضافة إلى مبالغ التعويض للغير عن الضّرر الحاصل لهم، ناهيك عن خدمات المراقبة والتحسينات التي يتلقّاها المؤمَّن له في سبيل الحفاظ على أمنه الإلكترونيّ، في حين تترتب هذه الالتزامات بدفع الأقساط التي تُحدّد بناءً على مقتضياتٍ معيّنةٍ لتكون متناسبةً مع إمكانيّات المؤمَّن له، وحدود الخطر، وقدرة المؤمّن على الدّفع كي لا يقع في خطر الإفلاس. وتعدّ عمليّة تحديد الأقساط مسألةً صعبةً للغاية في نطاق مخاطر الإنترنت خلافاً لغيره من أنواع التّأمين، وذلك نظراً لما يحيط هذه المسألة من غموضٍ، ونقصٍ بالمعلومات ما ينعكس سلباً على القسط، أمَّا عن الالتزام الآخر الذي يلتزم به المؤمَّن له _فهو وانطلاقاً من مبدأ حسن النيّة الذي ينطبق على أنواع التّأمينات كلّها_ يبدو لزاماً عليه أن يُطلع شركة التّأمين على المعلومات كلّها التي يعلم بها، والتي تتعلّق بمحلّ التّأمين، والخطر المؤمَّن ضدّه لما يسبّبه إخفاؤها من ضررٍ لشركة التّأمين قد يكلّفها الكثير، وقد يكون بإمكانها تفادي تفاقم الأضرار فيما لو أُخبِرت بالأمر، وهو ما قد ينعكس على المؤمَّن له ويحرمه من الحصول على التّعويض. وبناءً عليه سيُقسَّم هذا المبحث إلى مطلبينِ، يتناول الأوَّل التزام المؤمَّن له بدفع الأقساط التّأمينيّة، في حين يتمحور المطلب الثَّاني حول واجب الإعلام والعناية.

المطلب الأوَّل

التزام المؤمَّن له بدفع الأقساط التّأمينيَّة

بحسب القواعد العامَّة في عقود التّأمين يلتزم المؤمَّن له بدفع قسطٍ تأمينيٍّ لشركة التّأمين مقابل حصوله على التغطية التّأمينية كما ذكر سابقاً، والحقيقة أنّه في إطار عقد التّأمين ضد مخاطر الإنترنت لا يختلف الأمر كثيراً، فيلتزم المؤمَّن له أيضاً بدفع القسط وفق الأصول المتفق عليها مع شركة التّأمين. لكن عندما كان تحديد مقدار القسط في التّأمين ضد مخاطر الإنترنت يرتبط بعواملَ كثيرةٍ وأهمّها العوامل المتعلّقة بالخطر، فكان لزاماً أن يُدرس دفع القسط والآثار المترتّبة على الإخلال به في الفرع الأول، ومن ثمّ الانتقال إلى دراسة العوامل المتعلّقة بتحديد مقدار القسط في الفرع الثّاني.

الفرع الأوَّل

دفع قسط التّأمين والآثار المترتّبة على الإخلال به

يؤدّي القسط دوراً مميزاً في إطار عقود التّأمين، فهو أحد خصائصها ومميّزاتها عن غيرها من العقود، كما قد يُنظَر إليه على أنَّه ثمنٌ للتّأمين ومقابلٌ لتحمّل المخاطر. ويلتزم المؤمَّن له بمجرد إبرام العقد من حيث المبدأ بدفع القسط وفقاً للاتّفاق مع شركة التّأمين، وفي حال نكل المؤمَّن له عن هذا الالتزام، فقد حدّد القانون جزاءاتٍ معيّنةً يمكن لشركة التّأمين اللجوء إليها للوصول إلى حقّه.

أوّلاً: وجوب دفع قسط التّأمين:

ويُعرَّف القسط على أنَّه: "المقابل الماليّ الذي يدفعه المؤمَّن له إلى شركة التّأمين في مقابل الحصول على التّغطية التّأمينيّة للأخطار المؤمَّن ضدّها، وهو مقابلٌ مرتبطٌ بالخطر ومتغيرٌ نسبةً لتغيّر الخطر[218]"، وفي تحديد القسط جاء القانون المدني السوري على ذكر أنّ القسط لا بدّ أن يكون مبلغاً مالياً، فلا

[218] مكناس، (2018)، ص111.

يمكن القبول بالعمل مثلاً كقسطٍ تأمينيٍ، إذ أوجبَ دفع قسطٍ أو دفعةٍ ماليّةٍ أخرى يؤدّيها المؤمَن له لشركة التّأمين[219] ويمكن قبول الشّيكات أو الأسناد التّجاريّة كطريقةٍ تحلّ مقام الدفع الفوري. وكما جاء ذكره أعلاه في أنّ الملتزم بدفع قسط التّأمين هو المؤمَّن له حتى لو أُبرم العقد عن طريق ممثّلٍ له، إذ إنّ حدود الوكالة تقف عند إبرام العقد دون التزامه بدفع الأقساط والتي يلتزم المؤمَّن له وحده بدفعها، وقد يكون المؤمَّن له غير المستفيد من عقد التّأمين، وبالرّغم من ذلك فإنّ المؤمَّن له هو مَن يدفع القسط، في حين أنّ المستفيد ينتفع بتغطية شركة التّأمين فقط[220]، **وفي نطاق عقد التّأمين ضدّ مخاطر الإنترنت** ينطبق المبدأ العام في دفع الأقساط في عقود التّأمين على المؤمَّن له، بالرغم من كونه عقد تأمين من الأضرار والذي يضم التّأمين من المسؤولية الناشئة عن المخاطر الإلكترونية. وقد يحصل ألّا يتمكّن المؤمَّن له من دفع القسط لأحد الأسباب، كما لو انحلّت الشركة المؤمَّن لها أو أُشهِر إفلاسها، فالحقيقة أنّ الحل يكمن في فسخ العقد نظراً لعدم إمكانية الاستمرار بالالتزام لغياب أحد أطرافه، أمّا لو أُنتِقل الشّيء المؤمَّن عليه إلى شخصٍ آخرَ كما لو باع المؤمَّن له البرمجيّات والأنظمة التي يملكها إلى شركةٍ أخرى فلا شيء يمنع من انتقال التّأمين إلى الشّركة الجديدة، وكلّ ذلك وفقاً لاتّفاق الأطراف _أي بموافقة شركة التأمين_ مع الإبقاء على إمكانيّة فسخ العقد. وفي هذا المجال نبيّن النّقاط الآتية:

1-أمّا عن **تاريخ بداية دفع الأقساط**، فكما ذكرنا أنّ الأمر يقوم على اتّفاق الأطراف، ولكن غالباً ما يتمّ طلب دفع القسط مقدّماً كي تتمكّن شركة التّأمين من تكوين محفظة التّأمين التي تساعدها على تغطية المخاطر، ودفع مبالغ التّأمين في حال حصول الخطر على وجه السّرعة في بداية العقد، وقد تُدفَع الأقساط دفعةً واحدةً أو على أقساطٍ دوريّةٍ بحسب المتفق عليه[221]، **وهو السّائد في عقد التّأمين ضد مخاطر الإنترنت**؛ لأنّ العقد يستمرُّ لمدّةٍ زمنيّةٍ معيّنةٍ (غالباً سنة)، لذلك ولدفع الضيق عن المؤمَّن له وحماية لشركة التّأمين تُقسّم هذه الأقساط على دفعاتٍ.

---

[219] المادة (713) من القانون المدني السوري رقم (84) لعام 1949.

[220] مكناس، (2018)، ص112.

[221] المرجع السابق، ص113.

لكن _وعلى خلاف ذلك_ **ذهبت شركةAXA في سنغافورا إلى وجوب دفع إجماليّ أقساط عقد التّأمين ضد مخاطر الإنترنت كاملةً ودفعةً واحدةً قبل بدء سريان التّأمين وإلّا لن تُقدّم التغطية**[222].

وتتم عمليّة إشعار المؤمَّن له بوجوب دفع القسط برسالةٍ إلكترونيّةٍ عبر القنوات المتّفق عليها، كالبريد الإلكتروني، أو الاتصال الهاتفي من أجل تذكير المؤمَّن له بالدفع والقيام بما يجب عندما يمتنع عن القيام بالتزامه.

2- وعن **مكان دفع القسط**، فإنّه وبالرّغم من مبدأ (الدّين مطلوب وليس محمولاً) والذي يقضي بانتقال الدّائن (شركة التّأمين) إلى موطن المَدين (المؤمَّن له) من أجل تحصيل الأقساط، وبالرّغم من القواعد العامّة في العقود التي تقضي بوجوب الوفاء في موطن المؤمَّن له في حال غياب الاتفاق على مكان الوفاء بالقسط، **فإنّ هذينِ المبدأينِ غير معمولٍ بهما في عقد التّأمين ضدّ مخاطر الإنترنت**؛ لأنّ المبدأ الأكثر شيوعاً هو قدوم المؤمَّن له إلى مقرّ شركة التّأمين أو أيّ فرعٍ لها وقيامه بدفع القسط، وذلك بحسب العرف الجاري في نطاق التأمين ضد مخاطر الإنترنت على خلاف المبدأ السائد[223]، وفي حال كانت شركة التّأمين إلكترونيّةً دون وجود مكانٍ ماديٍّ لها _ إن وجد هذا الافتراض في الواقع _ عندها يبدو أمر تحديد المكان صعباً للغاية كونها موجودةً فقط على الإنترنت، ما ينعكس أيضاً على كيفية الدفع ويجبر المؤمَّن له على سلوك طريقة الدفع الإلكتروني عبر التحويلات المصرفية الإلكترونية، وعلى سبيل المثال تقدم شركة رأس الخيمة للتأمين خدماتها التّأمينية إلكترونياً للأفراد والمؤسسات عبر تطبيق الشركة على الأجهزة المحمولة، أو عبر الموقع الإلكتروني للشركة على الإنترنت، حيث يتم الدخول إلى التطبيق أو الموقع، ومن ثم الإجابة عن بعض الأسئلة التي تطرحها الشركة حول العمل

---

[222] https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf
تاريخ الزيارة: 2020\9\20، الساعة 10:25 p.m.

[223] https://www.almerja.com/reading.php?idm=115645
تاريخ الزيارة: 2020\9\17، الساعة 12:20 a.m.

وطبيعة التغطية المرادة (عادة تكون 5 أسئلة مفتاحية فقط للإجابة)، ومن ثم يتم الدفع إلكترونياً، وما هي إلا بضع دقائق وتكون الوثيقة جاهزة[224].

3-وعن **كيفية دفع الأقساط**، لا سيّما في ظلِّ انتشار وسائل الدفع الإلكتروني، فالخيار متروكٌ للطرفين ليختارا الوسيلة التي تناسبهما، فيمكن للمؤمَّن له اشتراط دفع القسط نقداً لدى الشركة إن لم يكن له حسابٌ مصرفيٌ مثلاً، وقد يُدفَع بوساطة حوالةٍ بريديةٍ تقليديةٍ، أو بوساطة الشيكات، وهنا يكون الدفع معلقاً شريطة صرف المبلغ نقداً من جانب المصرف، ناهيك عن إمكانية الدفع عبر أجهزة الصراف الآلي للبنوك المتعاقدة مع شركة التّأمين، كما هو حال **شركة أليانز** في مصر، إذ بدأت الشركة تتعاقد مع بنوكٍ وشركاتٍ متخصصةٍ لتحصيل الأقساط من أجل تسهيل الأمر على العملاء، كما قد تستفيد شركات التّأمين من الدفع بالطرق الإلكترونية كالتحويل الإلكتروني للأموال، ومثالاً على ذلك الشركة السابقة التي تتيح لعملائها دفع أقساط تأمينهم عبر تطبيقٍ للشركة على الأجهزة الذكية للعملاء، كما يمكن خصم قيمة الأقساط من بطاقات الائتمان الخاصة بهم، أو بطاقات ماستر كارد على الموقع الرسمي للشركة[225]، وهذه الطرق متّبعةٌ في معظم أنواع التّأمين بما فيها التّأمين ضد مخاطر الإنترنت.

وتتّضح أهمية أمر الدفع الإلكتروني في حالة إبرام التّأمين من جانب شركة إلكترونية، فهنا لا بدّ من استخدام الإنترنت لإتمام عملية الدفع، ويُطرح تساؤلٌ حول مدى إمكانية الاستفادة من العملات الرقمية كالبتكوين[226] في عمليات دفع الأقساط؟ وذلك في ظلّ الجدل الكبير حول إضفاء الحجية عليها، لكنّ المؤكّد أنّها

---

[224] https://www.rakinsurance.com

تاريخ الزيارة:6\5\2021، الساعة 8:45 p.m.

[225] https://www.allianz.com.eg/ar_EG/customer-care/premium-payment-methods.html

تاريخ الزيارة: 17\9\2020، الساعة 10:50 p.m.

[226] يعد البتكوين شبكة دفع إلكترونية جديدة تعتمد على النقود الإلكترونية بشكل كامل، وهي غير مركزية بل يتم إدارتها من قبل المستخدمين دون وسطاء، وتعد العملة النقدية الخاصة بالإنترنت، مشارٌ إليه على الموقع الإلكتروني:

https://www.bitcoin.org/ar/faq#general

تاريخ الزيارة: 1\5\2021، الساعة 11 p.m.

ستجد لذلك سبيلاً لا سيّما في ظلّ تعاظم سوق العملات الرقمية، وانتشارها الواسع، والاتجاه العالمي الكبير نحو الأتمتة، وإدخال الإنترنت والذكاء الاصطناعي في مجالات الحياة الواسعة.

4-إثبات عملية الدفع، حيث إنّه عند إتمام الدفع يُسلّم المؤمَّن له إيصالاً بالمبلغ المسدّد، أو يُرسَل إشعارٌ إلكترونيٌّ إلى بريده الإلكتروني، أو هاتفه المعتمد من أجل إثبات عملية دفع القسط، ولأنّ عقد التّأمين ضد مخاطر الإنترنت ينتمي إلى طائفة العقود التجارية حيث يمكن إثبات عملية الدفع بوسائل الإثبات كلّها وفقاً لمبدأ حرية الإثبات في المواد التجارية، إلّا أنّ الأكثر شيوعاً هو اللجوء إلى الكتابة من أجل الإثبات؛ نظراً لكونها الدليل الأقوى في الإثبات، وعلى هذا الرأي استقرّ المشرّع السّوريّ في قانون التجارة البحريّة في الباب المتعلّق بالتّأمين البحريّ فلم يُجز إثبات عقد التّأمين البحري إلّا بالكتابة[227]، ويمكن للشركات في ظلّ انتشار الكتابة الإلكترونية الاستفادة منها في تنظيم عقود التّأمين في الوقت الذي أعطاها المشرّعون حول العالم القوّة الثبوتيّة للكتابة التّقليديّة وباتت تحلّ محلّها في عالم الإنترنت[228].

5-أمّا عن تحديد **مبلغ القسط**، فالأمر يتعلّق بالخطر من حيث جسامته، واحتماليته، وغيرها من العوامل التي تتولّى شركة التّأمين التحقّق منها، **وفي نطاق عقد التّأمين ضد مخاطر الإنترنت يبدو تحديد الخطر أكثر صعوبةً من غيره من صور التّأمين؛ نظراً لحداثة عهده، وقلة المعلومات المتعلقة بالخطر الإلكتروني ما**

---

[227] المادة (355) من قانون التجارة البحرية السوري رقم 46 لعام 2006.

[228] أعطى التشريع السوري حجيّةً للكتابة الإلكترونية في المادة 2 من قانون المعاملات الإلكترونية رقم 3 لعام 2014، حيث نص على أنه (مع مراعاة الحجية المقررة قانوناً للتوقيع الإلكتروني المصدق يكون للكتابة الإلكترونية الحجية المقررة قانوناً للكتابة الورقية ويكون لتبادل المعلومات إلكترونياً عن طريق الفاكس أو البريد الإلكتروني أو أي وسيلة إلكترونية أخرى حجية القرائن القضائية أو مبدأ الثبوت بالكتابة)، في حين تنص المادة 2 من قانون التوقيع الإلكتروني وخدمات الشبكة على (للتوقيع الإلكتروني المصدق، المدرج على وثيقة إلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للأدلة الكتابية في أحكام قانون البينات، إذا روعي في إنشائه وإتمامه الأحكام المنصوص عليها في هذا القانون، والنواظم والضوابط التي يصدرها الوزير، بناء على قرار من مجلس إدارة الهيئة، المنصوص على إحداثها في الفصل الثالث من هذا القانون.

ب- للصورة المنسوخة على الورق من الوثيقة الإلكترونية الحجية ذاتها في الإثبات المقررة لهذه الوثيقة، بالقدر الذي تكون فيها مطابقة للأصل، ما دامت الوثيقة الإلكترونية والتوقيع الإلكتروني المصدق المدرج عليها موجودة على الحامل الإلكتروني الذي أُخذت عنه الصورة المنسوخة.

ج- تطبق في شأن إثبات صحة الوثائق الإلكترونية الرسمية والعادية والتواقيع الإلكترونية فيما لم يرد بشأنه نص في هذا القانون، وفي النواظم والضوابط التي يصدرها الوزير، بناء على قرار من مجلس إدارة الهيئة، الأحكام المنصوص عليها في قانون البينات).

ينعكس سلباً على عملية القسط، (وسيتم إفراد الفرع الثاني لدراسة العوامل المتعلقة بتحديد الأقساط في التّأمين ضد مخاطر الإنترنت).

ويُثار تساؤلٌ فيما لو حصل الخطر المؤمَّن منه في أثناء فترة التّأمين، فهل يعني ذلك إمكانية إنهاء العقد وتوقف المؤمَّن له عن دفع الأقساط؟

للإجابة عن التساؤل السابق، نبيّن أنّ عقد التّأمين إنَّما ينتهي لأسبابٍ معينةٍ هي: انتهاء مدّة العقد، أو فسخه، أو زوال الخطر المؤمّن منه، أو التقادم، وبحصول الخطر ضمن مدة السريان فلا يمكن إنهاؤه ما دامت مدته لم تنتهِ، أما عن حالات الفسخ فهو جزاءٌ لعدم قيام أحد الأطراف بالتزامه أو في حالات عدم القدرة على إتمام العقد لأسباب معينة كالتصفية أو الإعسار أو الإفلاس، وهذا السبب أيضاً لا يتوفّر في حالة تحقق الخطر، أمّا عن سبب زوال الخطر المؤمَّن، فالزوال المقصود به هنا الزوال الكليّ للخطر؛ أي أنّ الخطر لن يتحقّق في المستقبل؛ لأنّ الشّيء المؤمّن عليه قد زال، أو لأنّ الخطر بحد ذاته انتفى، كما لو أمّن الشخص على نفسه في أثناء رحلةٍ جويّةٍ ما، وأُلغيت هذه الرحلة فالخطر هنا زالَ ولا مجال لإكمال العقد، أمّا لو كان الزّوال مؤقتاً فيوقف العقد لمدّةٍ معيّنةٍ ويُستأنف بعدها، **ولو أُريد تطبيق هذا السّبب على التّأمين ضدّ مخاطر الإنترنت،** فالحقيقة ونظراً لطبيعة مخاطر الإنترنت من حيث كونها غير محدّدةٍ بشكلٍ معيّنٍ، وممكنة الحدوث في أيّ لحظةٍ لانتشارها الواسع، فلا يمكن القول بانتفاء الخطر المؤمّن منه إلّا في حال كان الخطر محدداً على وجه الدقة، وقابلاً لأن يزول أو بسبب زوال الشّيء المؤمّن عليه مثلاً، كمحو البيانات المؤمّن عليها من نظام عمل المؤمَّن له بإرادته الكاملة، وعليه لا يبقى محلّ لحصول الخطر المؤمّن ضدّه فيما لو كان العقد معقوداً لتأمين هذه البيانات التي أُزيلت فحينها يمكن إنهاء العقد، **وبعد بيان هذه الأسباب وحيث إنّه لا ينطبق أيٌّ منها على حالة حصول الخطر إبّان سريان العقد (ما لم ينطبق أي منها على حدة)، فالمبدأ أنّ العقد يبقى سارياً ويلتزم الطرفان بإكمال هذا العقد حتى النهاية ولوقت حصول أيّ سببٍ ينهي هذا العقد، إذ إنّ المؤمَّن له أبرم هذا العقد من أجل ضمان سلامة بياناته، وأنظمته، وإنّ حصول الخطر في أثناء السّريان لا يعني إنهاء العقد، ولذلك تلتزم شركة التّأمين بتغطية المؤمَّن له في كلِّ مرّةٍ يحصل فيها الخطر الإلكتروني ما دام داخلاً في**

التّغطية، وضمن مدّة السّريان، وما دامتِ المبالغ المدفوعة لتعويض المؤمَّن له ضمن مبلغ التّأمين الإجمالي المتّفق عليه (لأنّ مبلغ التّأمين هو الحدّ الأقصى لتغطية المؤمَّن له)، ولكن هذه التغطيات المستمرة تقلّص من إجمالي مبلغ التّأمين وقد تؤدّي في النهاية إلى استنفاذه؛ نظراً لأنّ مخاطر الإنترنت جسيمةٌ، وباهظة الثّمن، ولذلك لا بدّ من الانتباه إلى هذه النقطة من جانب الطّرفين، وإذا ما حصل ذلك فلا بدّ من إبرام عقدٍ جديدٍ أو تعديل العقد الأصليّ من أجل زيادة مبلغ التّأمين.

ثانياً: الآثار المترتّبة على عدم دفع الأقساط:

لمّا كان عقد التّأمين ضدّ مخاطر الإنترنت من عقود المعاوضة الملزمة لجانبين، فإنّ امتناع المؤمَّن له عن دفع القسط يدفع بشركة التّأمين إلى اتّخاذ إجراءاتٍ عدّة في محاولةٍ منها لردع المؤمَّن له عن هذا الامتناع وحثّه على تنفيذ التزامه، وهذه الإجراءات مأخوذة في جلّها عن القواعد العامة لعقود التّأمين. ومن بين الإجراءات التي يمكن اتخاذها من جانب شركة التّأمين الآتي:

1-امتناع شركة التّأمين عن أداء واجبها المقابل: فكما ذُكِر أنّ شركة التّأمين تلتزم بتغطية المؤمَّن له عند حصول الخطر، لكن ذلك مشروطٌ بأن يقوم الطرف الثاني بأداء ما يفرضه عليه القانون من التزاماتٍ، وأوّلها دفع الأقساط، فإن لم يقم المؤمَّن له بذلك الواجب فإنّ ذلك يخوّل شركة التّأمين التمسك بحقّها بالامتناع عن تغطية المؤمَّن له، وذلك مثلاً فيما لو حصل الخطر المؤمّن منه، (أُختِرق موقع المؤمَّن له) في أثناء فترة توقّفه عن الدّفع فتُعدّ شركة التّأمين في حلٍّ من التزامها بالتّغطية، ويمكن الاستناد في هذا إلى القانون المدنيّ السّوريّ الذي أرسى القاعدة العامة في العقود الملزمة لجانبين؛ من أنّه إذا كانتِ الالتزامات المتقابلة مستحقّة الوفاء جاز لكلٍّ من المتعاقدين أن يمتنع عن تنفيذ التزامه إذا لم ينفّذ المتعاقد الآخر ما التزم به[229]، **ويمكن التمسّك بهذه القاعدة من قبل شركات التّأمين ضدّ مخاطر الإنترنت؛** لأنّ ما ينطبق على العقود كافّة ينطبق على هذا العقد، مع الانتباه إلى وجوب أن تقوم شركة التأمين بإعذار المؤمّن له بدفع الأقساط المستحقة وإثبات هذا الامتناع، أو إقامة دعوى قضائية للمطالبة بالفسخ.

---

[229] المادة (162) من القانون المدني السوري رقم 84 لعام 1949.

2-الإعذار: ومعناه أن ترسل شركة التّأمين إشعاراً إلى المؤمَّن له تبلغه بوجوب دفعه الأقساط المستحقّة عليه، والغالب أن يشتمل الإعذار على معلوماتٍ معيّنةٍ منها، مبلغ القسط، وتاريخ استحقاقه، ومن ثمّ ذكر هدفه من وراء هذا الإعذار وهو المطالبة بالدفع، وتحديد النتائج المترتبة على التخلف عن هذا الواجب، كالوقف والفسخ حسب الحال[230]. ولم يأتِ القانون المدني السوري على ذكر الإعذار في نصوصٍ خاصّةٍ بعقود التّأمين عندما جاء الحديث على عقد التّأمين في المواد 713 وما بعد، ويُعزى ذلك لذكره الإعذار في نطاق حديثه العام عن التنفيذ بطريق التعويض، عندما ذكر كيفيّة الإعذار بوساطة الكاتب بالعدل أو بما يحلّ مقام الإنذار (كاستدعاء الدّعوى ولو رُفعت إلى محكمةٍ غير مختصّةٍ) أو عن طريق المراسلات بالبريد[231]. وعليه يبدو الأمر كما لو كان الحلّ متروكاً لرغبة شركات التّأمين فإن أرادت طبّقت هذا النص العام، وإن لم تُرد تجاهلته وقامت بفسخ العقد دون إعذار بالدّفع حتى، وبحسب مختصين فإنّ الواقع العمليَّ يكشف أنّ كثيراً من شركات التّأمين تلجأ إلى هذا الأمر، وتقوم بفسخ عقد التّأمين لعلة عدم دفع الأقساط ودونما أيّ إعذارٍ للمؤمَّن له بوجوب دفع الأقساط، وكأنما تتّخذ شركات التّأمين من إهمال بعض المؤمَّن لهم ذريعةً للتملّص من التزاماتها. وفي سبيل محاولة التشريعات سدّ الباب على التحايل ودرء الخطر عن المؤمَّن لهم، ذهب بعض المشرّعين إلى وجوب الإعذار بنصوصٍ خاصّةٍ بالتّأمين في تأكيدٍ منهم على أهميّة هذا الإجراء، ومن هذه التشريعات التشريع اللبناني، والفرنسي[232]، وقانون التجارة البحرية السّوريّ الذي أفرد نصوصاً خاصّةً بعقود التّأمين البحريّ، إذ أوجب إعذار المؤمَّن له بدفع الأقساط مع تهديده بإمكانية إيقاف العمل بعقد التّأمين، أو فسخ العقد، وقد اتّخذ المشرّع موقفاً صائباً بإلزام شركة التّأمين بالإعذار مرّةً أخرى (إعذار بالفسخ) بعد الإعذار الأوّل قبل أن يُفسَخ العقد إذا توانى المؤمَّن له عن دفع الأقساط والمصاريف، ولا يحدث الوقف أو الفسخ إلّا بعد انقضاء خمسة عشر يوماً على الإعذار الأوّل بالوفاء[233]. أمّا عن التشريع الفرنسي والذي تمّ اقتباسه في القانون اللبناني أيضاً، فقد نصّ على أنّه في أحوال

---

[230] مكناس، (2018)، ص119.

[231] المادة (220) من القانون المدني السوري رقم 84 لعام 1949.

[232] http://www.arab-ency.com.sy/law/detail/163444

تاريخ الزيارة: 2020\9\18، الساعة 11:30 p.m.

[233] المادة (365) من قانون التجارة البحرية السوري رقم 46 لعام 2006.

امتناع المؤمَّن له عن دفع الأقساط كاملةً أو جزئيةً فلا بدّ من إرسال إعذارٍ إلى المؤمَّن له بعد عشرة أيّام من تاريخ استحقاق القسط، وهنا في حال استمرار التوقّف عن الدّفع، يُعدّ عقد التّأمين موقوفاً بعد انقضاء ثلاثين يوماً على الإعذار المرسَل (الإيقاف يتمّ حكماً بمجرّد مرور مدّة الثلاثين يوماً دونما حاجةٍ إلى أيّ إجراءٍ آخر) ويُعدّ الدّين محمولاً هنا، وفي حال لم يُستردّ فيمكن لشركة التّأمين بعد مرور عشرة أيّام على انقضاء الثلاثين يوماً المذكورة فسخ العقد (دونما حاجة أيضاً لأيّ إجراءٍ)[234]. وهنا يظهر اختلاف التّشريع السّوريّ الذي استلزم إعذاراً آخرَ ليُفسخ العقد، في حرصٍ أكبرَ على مصلحة المؤمَّن له، بينما أعطى التشريع الفرنسي الحق بالفسخ لمجرّد مرور مدّةٍ معيّنةٍ، وهنا يظهر التشدّد لناحية تحقيق مصلحة شركة التّأمين. والحقيقة أنّ الرّأي أميل إلى الاتجاه الفرنسيّ؛ لأنّ الدّين كان مستحقّاً ولا يمكن القول بعدم معرفة المؤمَّن له بوجوب الدّفع، بالإضافة إلى أنَّ شركة التّأمين بعد أن أدّت واجبها بالإعذار بالدّفع والتهديد بالوقف لا تكون قد تركت مجالاً للادعاء من جانب المؤمَّن له بعدم علمه بواجب الوفاء بالقسط.

وبالعودة إلى عقد التّأمين ضدّ مخاطر الإنترنت، ولأنَّ التّشريعات لم تفرد له أحكاماً خاصةً حتى الآن فالموضوع إذن عائد لاتّفاق الأطراف، ولا شيء يمنع شركات التّأمين العاملة في هذا المجال من الاستفادة من النّصوص المذكورة في حماية حقوقها في تحصيل الأقساط، إذ غالباً ما تُحدّد مواعيد الوفاء بالأقساط وطُرق التّبليغ باتّفاق الطّرفين، وحينها يمكن لشركة التّأمين أن تقوم بإعذار المؤمَّن له بالوفاء، وأن تمارس حقّها بالوقف والفسخ في حال عدم الالتزام، ويمكن ترجيح الرَّأي الفرنسيّ في إمكانيّة الفسخ بعد الإعذار بالدّفع دونما حاجةٍ لإجراءٍ آخرَ وتطبيقه على تأمين مخاطر الإنترنت، لا سيّما وأنّ هذه المخاطر باتت متعلّقةً بنقرةٍ واحدةٍ على الحاسب من قِبل المخترق الذي بوسعه تدمير أنظمة المؤمَّن له، ولذلك تستوجب هذه المخاطر الدّقيقة سرعةً أكبرَ من جانب المؤمَّن له نفسه في حماية بياناته وأنظمته عبر دفع الأقساط لشركة التّأمين من أجل تأمين الحماية التّأمينيّة له، ولدفع الحرج عنه عند حدوث الخطر في مدّة وقف عقد التّأمين، إذ إنّ شركة التّأمين في حلٍّ من

[234] مكناس، (2018)، ص118.

التزاماتها في هذه المدة، لكن في أثناء مدّة الإعذار وقبل حصول الوقف تبقى شركة التّأمين ملتزمةً بالتّغطية التّأمينيَّة.

3-وقف التّأمين: في حال أُرسِل الإعذار وسرت المدّة المحدّدة لقيام المؤمَّن له بدفع قسط التّأمين، فعندها يعد عقد التّأمين موقوفاً لجهة التزامات شركة التّأمين دون الحاجة إلى أيّ إجراءٍ، وفي حال حصل الخرق الإلكتروني أو الهجمات بالفايروسات على شبكة المؤمَّن له في هذه المدّة فلا تلتزم شركة التّأمين تجاه عميلها بأيّ تغطيةٍ، بل إنّها تنفكّ حتى تجاه الأشخاص المتضررين من هذه الهجمات (عملاء المؤمَّن له)، وتحتجّ تجاههم بتعسّف المؤمَّن له في دفع أقساطه، ويبقى هذا العقد موقوفاً حتى يقوم المؤمَّن له بدفع ما يترتّب عليه من أقساطٍ ومصاريفَ أخرى، كفوائد التأخير ونفقات الإعذار، ومن اليوم التالي للدفع يعود عقد التّأمين إلى السريان كعهده السابق، لكن التغطية تكون للمدّة التالية على الدفع، أمّا ما كان قد حصل في أثناء الوقف فلا يعوَّض، وهذا الوقف لا يؤثّر في التزام المؤمَّن له بوجوب دفع القسط في مدّة الوقف[235].

4-فسخ العقد: إذا مرّتِ المدة المحددة في الإعذار ودخل عقد التّأمين في مرحلة الوقف، ثمّ مرّت هذه المدّة أيضاً دون دفعٍ، يكون من حقّ شركة التّأمين طلب فسخ العقد، ولا يعدّ فسخاً قضائياً؛ إذ إنه لا حاجة لدعوى قضائيّة، وليس قانونياً أيضاً، إنّما يتم عبر رسالةٍ توجّهها شركة التّأمين إلى المؤمَّن له تعبّر له بموجبها عن رغبتها بفسخ العقد لعلّة عدم دفع الأقساط[236]، وعليه يتمّ إنهاء العقد بين الطّرفين. لكن لشركة التّأمين _بالإضافة إلى ما سبق_ الحقّ في مطالبة القضاء إلزام المؤمَّن له بدفع الأقساط المستحقّة عليه كلّها حتى تاريخ الفسخ مع المصروفات كافّة التي تكبّدتها شركة التّأمين، ناهيك عن طلب التعويض عن الفسخ[237]، ولا يخفى على أحدٍ حقّ شركة التّأمين بطلب التنفيذ العينيّ رغم وصولها إلى مرحلة الفسخ، فيحقُّ لشركة التّأمين وبالرّغم من كلّ هذا التعنت من جانب المؤمَّن له وبدلاً عن الفسخ تقديم طلب قضائي لإجبار المؤمَّن له على

---

[235] المرجع السابق، ص120، 121.

[236] زهرة، (1997)، 106.

[237] مكناس، (2018)، ص122.

دفع ما يستحقّ عليه من أقساط ومصروفات وتعويضٍ لجبر العطل والضّرر الحاصل، وذلك وفقاً للقواعد العامة في العقود عن طريق التنفيذ العيني وفق ما حدّده المشرّع في المادّة (204) من القانون المدنيّ السّوريّ.

وخلاصة القول، وفي هذه الجزاءات المذكورة جميعها بأن لا شيء يمنع شركات التّأمين ضد مخاطر الإنترنت من الاستعانة بها في سبيل الحصول على حقّها في القسط من المؤمَّن له ما دامت هذه الجزاءات مكرّسةً بنصوصٍ قانونيّةٍ صريحةٍ، وما دامت قابلةً للتّطبيق على تأمين مخاطر الإنترنت. وإذا أمكن الاستعانة ببعض النّماذج التي توردها شركات التّأمين عن أشكال تغطيتها التّأمينيّة لمخاطر الإنترنت كونها تمثّل _في الكثير من الأحيان_ القواعد التي تُتّبع من جانبهم عند إبرامهم عقود التّأمين، ذكرت شركة رأس الخيمة في نموذجٍ للتأمين ضد مخاطر الإنترنت نصاً أعطت بموجبه لنفسها الحقّ في إلغاء الوثيقة التّأمينيّة في حال الامتناع عن سداد قسط التّأمين، وذلك بعد انتهاء فترة إنذارٍ لا تقلُّ عن 30 يوماً[238] (لا شيء يمنع أن تزيد المدّة، ولكن لا يجوز أن تقلّ عن ذلك)، كما قدّمت شركة فيلادلفيا للتأمين نموذجاً عن تأمين مخاطر الإنترنت، وذهبت إلى إمكانية إلغاء العقد المبرم لعلّة عدم دفع الأقساط بموجب إخطارٍ كتابيٍّ إلى المؤمَّن له مفاده أنَّه وبمرور عشرة أيّام (على الأقل إن لم تُزاد هذه المدّة في الإخطار) تاليةٍ لهذا الإعذار سيدخل إلغاء العقد حيّز النفاد، ومن هذا التاريخ تنتهي مدة الوثيقة[239].

[238] Simply Cyber Policy Terms & Conditions (2018). P 19.

[239] Cyber security liability coverage form (n.d). Philadelphia indemnity insurance company, p 21.

الفرع الثّاني

العوامل المتعلّقة بتحديد قسط التّأمين ضدّ مخاطر الإنترنت

على الرَّغم من التّشابه في بعض القواعد العامّة للأقساط بين هذا العقد وسائر عقود التّأمين، لكن تثير عمليّة تحديد قسط التّأمين ضدّ مخاطر الإنترنت مصاعبَ كثيرةً، إذ يرتبط هذا القسط بعواملَ جمّةً لا سيّما بالمخاطر التي يتمّ التّأمين منها، ويبدو أنّ المستفيد الأكبر من عملية التحديد هو المؤمَّن له؛ لأنّه يبيّن مقدار ما سيُدفع من جانبه، وبالتّالي مقدار الدَّين الذي سيترتّب عليه، كما أنّه يُحدّد على أساس القسط المدفوع مبلغ التّأمين الذي سيدفعه المؤمّن عند وقوع الخطر، وهذه العوامل متغيّرةٌ بحسب كلّ حالةٍ، وحسب كلّ طالب تأمينٍ، وعليه سنبيّن هذه العوامل تباعاً.

أولاً: تحديد قسط التّأمين تبعاً لمخاطر الإنترنت:

لكلِّ شركة تأمينٍ وسيلة تسعيرٍ خاصّةٍ بها لوثائق التّأمين ضدّ مخاطر الإنترنت بحسب الشّركات التي تشتريها بناءً على معاييرَ معينةٍ، مثل الولايات القضائية التي تعمل فيها، حجم الشّركة، وأنشطتها، ليعكس ذلك نوع المخاطر التي تحيط بالشركة، والأقساط التي تريدها مقابل تقديم التغطية التّأمينية[240]، لذلك وفي أشكال التّأمين جميعها وعلى اختلافها ينظر المؤمَّن في البداية إلى نوع الخطر المراد التّأمين ضدّه؛ لأنّه الهدف الأوّل الذي يدفع بطالب التّأمين إلى شركات التّأمين في محاولةٍ منه لدرء الخسائر عن نفسه وماله، وتعتمد قطّاعات التّأمين النّاضجة على قواعد بياناتٍ تاريخيّةٍ ضخمةٍ ونماذجَ صُقِلت على نطاق سنوات عدّة[241]. وبالنّظر إلى مخاطر شركة الأمن السيبراني، فهي مزيجٌ من قيمة حقوق ملكيّتها الفكريّة، ومدى احتماليّة تعرّض القطاع الذي تنتمي إليه الشركة طالبة التّأمين لمخاطر الإنترنت، بالإضافة إلى خصائص أنظمة حواسيب الشّركة، وفي حين يظلّ أوّل عاملين خارج إرادة شركة التّأمين؛ أي لا تتمكّن من إدارتها على نحوٍ مثاليٍّ؛ لأنّها متعلّقةٌ بظروفٍ

---

[240] Coburn, A., Leverett, E., & Woo, G. (2018). P 258.

[241] Oliver Ralph, "Cyber Attacks: The Risks of Pricing Digital Cover," Financial Times (UK), March 19, 2018, referred to by: Aburish, N., Fixler, A., & Dr. Hsieh, M. (2019). The Role of Cyber Insurance in Securing the Private Sector, Washington, DC: United States of America, center on cyber and technology innovation, p 6.

خارجيّةٍ لا يمكن التنبّؤ بحصولها، ويُنظَر إلى العامل الثّالث على أنَّه أحد الوسائل التي تعتمدها شركات التّأمين كعلاجٍ لتحسين بيئة الأمن الإلكترونيّ وتوفير أقساطٍ قليلةٍ كلَّما زادت نسبة الأمان[242]. والحقيقة فيما يخصُّ هذه المخاطر وكما ذكر سابقاً ورغم مرور ما يقارب ثلاثة عقودٍ على الانتشار الواسع لها، إلَّا أنَّ المشكلة كلّها تكمن في عدم وجود سجلّاتٍ وأرقامٍ حقيقيّةٍ تحدّد مقدارها، بالإضافة إلى قلّة المعلومات عن التّأمين على هذه المخاطر، وقلّة التّجارب، والدّعاوى القضائيّة في نطاق التّأمين عليها، ولذلك يعاني قطّاع التّأمين ضدّ مخاطر الإنترنت في ظلِّ هذا النّقص ومحدوديّة البيانات من صعوبةٍ في التّسعير، وينطبق ذلك على شركة التّأمين؛ إذ إنّها غير قادرة على تحديد المخاطر بالنسبة لطالب التّأمين، كما أنّ الأخير غير قادرٍ على تقييم مخاطره وحده، ما ينعكس سلباً على التسعير عبر رفع الأقساط لتغطيّة المخاوف، ويضاف إلى ذلك أنّ مخاطر الإنترنت لا تنحصر في مكانٍ ما، أو نظامٍ ما، بل تنتشر على رقعةٍ كبيرةٍ في العالم في كثيرٍ من الأحيان، وتصيب أنظمةً عدّةً في آنٍ معاً ما يصعب عمليّة حصر الأضرار على شركة التّأمين، ويعكس ذلك صعوبة تحديد القسط بصورةٍ عامّةٍ[243].

1-احتماليّة حصول الخطر وجسامته: وتهدف عملية تقييم مخاطر الإنترنت إلى التعرّف إلى احتمالية حصول الخطر، ودرجته، وجسامته فبناءً على هذه المعلومات التي يحصل عليها المؤمن تُحدّد الأقساط، ويُطلق عليها عملية قياس التعرض للمخاطر، والذي يتم بموجبه تحديد مقدار المخاطر المرتبطة بكلّ وثيقة، ومن ثمّ إمكانية تحديد القسط، ويفترض بهذا القياس التأكد من مدى تكرار وخطورة المطالبات المتعلّقة بالخطر المراد تأمينه، فعلى سبيل المثال: لو كان طالب التّأمين شركةً مزوّدةً لخدمات الإنترنت فهذه الشركة تستخدم الإنترنت بمعدّلٍ عالٍ من أجل تقديم خدماتها إلى المستهلكين العملاء، وهذا الاستخدام الكبير يخلق فرصاً أكبرَ لإمكانيّة إلحاق الضّرر بموقعها الإلكترونيّ، وقائمة بياناتها بسبب القراصنة والاختراقات والهجمات الفيروسية[244]، ولذلك يكون القسط بالنسبة لها أعلى من مستخدم إنترنت عادي، أو من شركةٍ صغيرةٍ تمارس بعض الأعمال عبر

---

[242] Ibid, p 6.

[243] Ibid, p 7.

[244] Mukhopadhyay, A., Debashis S., Chakrabarti B, Ambuj M., & Asok P. (2005). Insurance for cyber-risk: A Utility Model, V32, NO1, Decision, P 166.

الإنترنت، وترغب بتأمين أعمالها. ومن بين عوامل الخطر التي يمكن أخذها في الاعتبار عند قياس وحساب الخطر[245]:

أ–عدد الساعات التي يقضيها المؤمَّن له على الإنترنت ويقوم فيها بالمعاملات الإلكترونية.

ب–مدى احتمالية وسهولة اختراق المواقع التي يديرها المؤمَّن له وتكلفة إصلاحها.

ج–احتمالية تعرّض أجهزة مزوّدي خدمات الإنترنت والمستهلكين على السواء للمخاطر، ويُراد بذلك الضّعف الذي تعاني منه أجهزتهم، كإمكانيّة اختراق الراوتر؛ أيّ جهاز إيصال الإنترنت إليهم.

د–مخاطر الهجمات الفيروسية.

هـ–مخاطر تعطل الأجهزة والبرمجيات والمعدات الصلبة التي تُستعمَل كالأقراص الصلبة.

و–المواقع التي يتصفّحها ويزورها المؤمَّن له المستخدم.

ز–انتماء المؤمَّن له إلى دولةٍ في حالة حربٍ مع دولةٍ أخرى لإمكانية حصول هجماتٍ إلكترونيّة في إطار الحرب القائمة.

ح–القطّاع الذي ينتمي إليه المؤمَّن له، ويُراد بذلك مدى إمكانية وجود شركات منافسة له قد تريد الإطاحة به عبر خرق مواقعه وتعطيل أعماله.

خ–احتمالية حصول الإعصار الإلكتروني[246].

وفي النتيجة فإنّ هذه العوامل كلّها تُسهم في إمكانية حصول الخطر المؤمَّن ضده؛ نظراً لإمكانيّة حصول الاختراق من أيّ مكانٍ يُزار أو عبر أيّ وسيلةٍ تُستخدم، وعليه تعمل شركات التّأمين على تقييم احتمالية وقوع هذه المخاطر، عبر تنظيم عوامل التعرض للخطر، وتقدير احتمالية الخسارة القصوى التي قد تتعرّض لها

---

[245] Ibid, p 167.

[246] سبق الحديث عن هذا المفهوم في الفصل الأول في الصفحة 28.

شركة التّأمين، وعبر تفاعل هذين العنصرين تتحدّد قابلية شركات التّأمين لتحمل المخاطر، وبالتالي مدى قدرتها على دفع مبالغ التّأمين بكلِّ سهولةٍ وأمانٍ.

وعلى النحو المقابل لعوامل الخطر يدخل في حساب القسط أيضاً العوامل المتعلقة بالتّأمين ضد مخاطر الإنترنت، ولمزيد من التوضيح لهذه العوامل يُذكَر الآتي:

أ–نوع التغطية (تغطية طرف أول أو هي تغطية شاملة): ويبدو هذا العامل ذا أهميّة، فوفقاً لشركات التّأمين فإنّ المؤمَّن له صاحب الوثيقة الأشمل سيميل إلى كونه أكثر إهمالاً من صاحب تغطية الطرف الأول فقط؛ لأنّ أيّ ضررٍ يصيب الغير سيؤدّي به إلى دفع مبالغَ جسيمةٍ للمتضرّرين، ولذلك لن ينتبه صاحب الوثيقة الأشمل إلى خطواته عبر الإنترنت ؛ لأنّه يرى في هذا التّأمين وسيلةً للتخلّص من مسؤوليته تجاه الغير بادّعائه أنّ شركة التّأمين ملزمةٌ بالدّفع، على الرغم من أنه بحال طولب بالتعويض عن الضرر الحاصل نتيجة تحقق أي خطر من أخطار الإنترنت فلن يستطيع الامتناع عن الدفع استناداً لوجود عقد تأمين، نظراً لكونه الملتزم الأول تجاه عملائه ولكونه ملتزم مع شركة التأمين بالتضامن تجاه الغير. ولذلك إذا ما كان المؤمَّن له حاملاً وثيقة تغطيةٍ للطّرف الأول، فبالتّأكيد القسط سيكون أقلّ ممّا لو كانتِ التّغطية شاملةً؛ لأنّ شركة التّأمين تتحمّل مخاطرَ أكبر ونفقاتٍ أكثر.

ب–الغرض من الاستخدام: ويرتبط هذا العامل بطبيعة استخدام المؤمَّن له الإنترنت، فيختلف الأمر فيما لو كان يستخدمها من أجل أعمالٍ شخصيةٍ، كالتصفح العادي والقيام ببعض عمليات الشراء، أو أنّ هذا الاستخدام من قبل شركة تدير أعمالها عبر الإنترنت، كالمصارف التي تجري حوالاتٍ إلكترونيةً، وأعمال إنشاء حسابات عبر الإنترنت، ويبدو أنّ هذا العامل مرتبطٌ بناحيةٍ أخرى بعامل الخطر السّابق، كعدد السّاعات التي تُقضى على الإنترنت، ومخاطر الهجمات الفيروسيّة؛ لأنّ هذين العاملين مرتبطان تناسبياً ببعضهما، فكلّما زاد استخدام المؤمَّن له واعتماده على الإنترنت زادت احتماليّة حصول الهجمات الفيروسية، وبالتّالي زادت مخاطر الاختراقات، وعليه كلّما زاد هذان العاملان زاد القسط تباعاً؛ لأنّ التصفّح الأكبر يعني مخاطر أكبر، واحتماليّة مديونيّة شركة التّأمين لعميلها ستكبر، ولتحمي نفسها تعمل على زيادة القسط.

ج–عامل عُمر المستخدم: ويرتبط هذا العامل أيضاً بعامل المواقع التي تزداد زيارتها من جانب المؤمَّن له، فإذا ما كنّا أمام مراهقٍ يستخدم الإنترنت بالتأكيد ستكون اهتماماته مختلفةً عن شركةٍ تجاريةٍ أو عن شخصٍ بالغٍ، ولربما استخدم المراهق الإنترنت برعونةٍ أكبرَ، وسبّب لنفسه متاعبَ أكبر، ولكانت احتماليّة المخاطر أعلى.

د–قيمة محتويات موقع الويب ومدى أهميّة إيراداته بالنّسبة للمؤسّسة ككلّ: ويعتبر هذا العامل مهمّاً بالنسبة للمؤسسات التي تمارس المعاملات التجارية عبر الإنترنت؛ لأنّها تستفيد بشكلٍ كبيرٍ من مواقع الويب، وقواعد البيانات الموجودة على الإنترنت، فخطر تعرّض هذه الشّركات لمخاطر الإنترنت كبيرٌ جداً، ويرخي بظلاله على هذه المواقع والقواعد، والتي إن شُفِّرت مثلاً في هجمات الفدية ستُدفع مبالغ طائلة من أجل فكّ التشفير، وهو ما ستلتزم به شركة التّأمين، ولذلك غالباً ما ترفع شركات التّأمين الأقساط من أجل تحديد مبلغ تأمين يتناسب والخطر المُحدق بعملائها[247].

وهذه العوامل التي ذُكِرت تُشكِّل أمثلةً على ما يُوضَع في حسبان شركات التّأمين ضدّ مخاطر الإنترنت عند تحديد الأقساط؛ لأنّ أيّ شركةٍ لا ترغب بأن تخسر أو تصل إلى هاوية الإفلاس من أجل عملائها، وبالمقابل لا تودّ تقديم وثائق تأمين لا تغطّي حاجة عملائها ومخاوفهم من المخاطر المحيطة بهم، ولذلك هنالك العديد من العوامل التي يُحسب لها عند القيام بعمليّة التّحديد، وغالباً ما يُحصَل عليها عبر الأسئلة التي تُقدَّم من جانب شركة التّأمين إلى المؤمَّن له (ستُذكر في المطلب الثاني).

2–مدى تأثير المخاطر: يدخل في نطاق تقييم مخاطر الإنترنت دراسة مدى تأثير هذه المخاطر على الشركة المستهدفة؛ أي مدى شدّة هذه المخاطر، وقوّتها، واستمراريّتها؛ لأنَّ كلَّ ذلك ينعكس على سعر الأقساط، فآثار المخاطر تكون قصيرة الأجل عندما تتعامل مع فقدان القدرة على العمل نتيجةً للخروقات، وتكاليف إصلاح ماُ خرِّب بسبب الهجمات الإلكترونية، وتكاليف الاستفادة من خدمات الإعلام للتواصل مع العملاء والمستهلكين، أمّا عن الآثار طويلة الأجل التي تسبّبها هذه المخاطر، فهي تتراوح بين مخاطر فقدان العملاء وتحولهم إلى شركاتٍ منافسةٍ، وعدم قدرة الشركة المستهدفة على جذب مستهلكين جددٍ نتيجة لانهيار سمعتها التجارية وصورتها

[247] Mukhopadhyay, A., Debashis S., Chakrabarti B, Ambuj M., & Asok P. (2005). P 167.

أمامهم، وما يرتّبه ذلك من فقدان الثّقة، ويُضاف إلى ذلك إمكانية حصول الشركات المنافسة على الأسرار التجارية الخاصّة بالشركة المستهدفة[248]، وعليه عندما يطلب المؤمَّن له تغطية المخاطر طويلة الأجل غالباً ما ترفع شركة التّأمين القسط عليه؛ لأنّها تزيد من التزامها بالدّفع تجاه المؤمَّن له ما يدفعها ذلك إلى إنفاق مبالغَ أكثر في سبيل محاولة إصلاح ما خُرِّب نتيجة الخروقات؛ لأنّ هذه الآثار تحتاج إلى وقتٍ ليس بقصيرٍ، ومبالغَ طائلةٍ لإعادة السمعة، والقدرة على المنافسة، بينما لو كان الأمر يقتصر على عمليّة إعادة إصلاح الأجهزة التي تخرّبت أو استعادة البيانات التي سُرِقت فلن يرتفع القسط على نحوٍ كبيرٍ مقارنةً بما سبق.

3-مبدأ الخطر المتبادل: كما يُنظَر عند تقييم مخاطر الإنترنت إلى مبدأ الخطر المتبادل أو الخطر المترابط بين العملاء المستخدمين للإنترنت _**وهو ما يرخي بظلاله على طبيعة التّأمين ضد مخاطر الإنترنت ويعطيه ميزةً مختلفةً عن غيره من أنواع التّأمين_**، فاختراق البريد الإلكتروني لعميلٍ ما يسهّل عملية اختراق حسابات عميلٍ آخر، كما أنَّ الهجمات على مزوّدي الخدمات السحابية قد يؤدّي لانقطاع الخدمة لدى عددٍ كبيرٍ من الشركات التي تستفيد من خدمات هؤلاء المزوّدين. وبسبب هذا الخطر المتبادل فإنَّ حالة الأمن السيبرانيّ لا تعتمد على الجهود الخاصّة لأيّ شركةٍ، بل على التّعاون بين الشّركات العاملة جميعها في فضاء الإنترنت[249]، و بحسب بعض الدّراسات يُعتبَر الخطر المتبادل سيفاً ذا حدين، فقد يكون أحد وسائل تحفيز المؤمَّن له على تبنّي أفضل الممارسات الصحيحة لتحسين واقع أمنه الإلكتروني، أو قد يكون التّأمين الإلكتروني أحد الوسائل التي تدفع المؤمَّن له إلى إهمال أمنه الإلكتروني، ولكن هذا أو ذاك سوف ينعكس على تسعير الأقساط، فكلّما اهتمَّت الشّركة بأمنها وحافظت على أعمالها انخفض القسط؛ نظراً لانخفاض احتماليّة حصول المخاطر المتبادلة، ولذلك يرتبط هذا الخطر بالقسط بشكلٍ حتميٍّ[250]، وفي الأحوال كلّها تشكّل عملية تقييم المخاطر الأساس في إتمام عملية التّأمين بحدِّ ذاتها؛ لأنّ أغلب شركات التّأمين تفضّل طالبي التّأمين ذوي المخاطر الأقلّ احتماليّةً والأقل كلفةً لتقديم تغطيةٍ تأمينيةٍ لهم.

---

[248] Ruan, K. (2019). P 80.

[249] Khalil, M., Naghizadeh, P., & Liu, M. (2017). Embracing Risk Dependency in Designing Cyber-Insurance Contracts, Fifty-Fifth Annual Allerton Conference, Illinois: USA, P 926.

[250] Ibid, p 926.

ثانياً: تحديد القسط تبعاً لمبلغ التّأمين:

يُنظَر إلى مبلغ التّأمين على أنَّه الالتزام الرَّئيس لشركة التّأمين، والذي يجب عليها دفعه عند حصول الخطر المؤمّن منه، وإنّ تحديد مبلغ التّأمين يرتبط في أساسه بعواملَ عدّةٍ منها مدى ملاءة الشّركة؛ أي رأسمالها، وموجوداتها، وصافي الرّبح الذي تحقّقه كلَّ سنةٍ، ومدى قدرتها على دفع مبالغ التغطية لمؤمّنٍ لهم عديدين في الوقت ذاته دون أن يؤدّي ذلك إلى تهديد وجودها، فكلّما كانت الشركة مليئةً وذات علاقاتٍ أكبرَ ومتعاونةً مع معيدي التّأمين، كلَّما كانت أكبر قدرةً على التّأمين لعددٍ أكبر من المؤمَّن لهم ولنطاقٍ أوسع من المخاطر، كما يرتبط تحديد المبلغ بالمخاطر التي تلتزم بتغطيتها بحسب نوع الخدمات التي تقدّمها، والحديث هنا عن تأمين مخاطر الإنترنت، فهذه المخاطر بما تتّصف به من صفاتٍ وخصائصَ تُؤخذ بعين الاعتبار عند تحديد مبلغ التّأمين، فالكثير من المخاطر الأكثر شيوعاً والتي قد تكلّف الشّركات المستهدفة نسباً أكبر من الخسائر قد تضع شركات التّأمين قيوداً على تغطيتها، أو تضع استثناءً على تغطيتها لمحاولة تقليص مبلغ التّأمين.

كما يدخل في حساب مبلغ التّأمين هامش الرّبح المتوقَّع من جرّاء الأعمال التّأمينية التي تمارسها، ويدخل في هذا الحساب أيضاً المصاريف التي تتكبّدها شركات التّأمين لإبرام هذا العقد، والعمولة التي تُدفَع لشركات إعادة التّأمين من أجل الحصول على تغطيتها الإضافيّة لشركات التّأمين الأوليّة.

كما ويُؤخذ في الحسبان عند تحديد مبلغ التّأمين لا سيّما عند التّعامل مع مخاطر الإنترنت أنَّ هذه المخاطر تنصبُّ على أشياء غير ماديّةٍ، كالبيانات، والمعلومات، والأنظمة التي قد تتعطّل دون استعادة؛ ولذلك عندها لا بدَّ من استبدالها عبر تثبيت أنظمةٍ جديدةٍ نيابةً عن المتضرّرة _مع وجوب الانتباه إلى القيمة الفعليَّة لهذه الأنظمة عند حصول الخطر، والتي قد تتغيَّر عمَّا كانت عليه عند شرائها في البداية_ كما أنَّ هذه البيانات بحاجةٍ لاسترجاعها، مع الانتباه إلى ما يكلّفه ذلك من الاستعانة بخدمات خبراءَ مختصّين، عداك عن التزام بعض شركات التّأمين بعمليات المراقبة للأنظمة المحميّة، وتدريب موظّفي المؤمَّن لهم (على النحو الذي ذُكِر عند الحديث عن التغطية التّأمينية السابقة لحصول الخطر)، ولذلك فإنَّ عملية التّأمين ضد مخاطر الإنترنت تكلّف شركة التّأمين كثيراً من المال، وينعكس ذلك على مبلغ التّأمين الذي تحاول شركة التّأمين زيادته ليتحمّل كلّ

النفقات، ويُلحَظ ذلك أيضاً على القسط الذي يتناسب طرداً مع مبلغ التّأمين، فكلّما كان مبلغ التّأمين أكبر زاد القسط ليغطّي الحاجة والعكس صحيح، وفي النهاية بتضافر هذه العوامل جميعها يُحدّد مبلغ التّأمين الذي يرتكز عليه تحديد الأقساط التي يتوجّب على المؤمَّن له دفعها لشركة التّأمين؛ إذ إنَّ هذه الأقساط ما هي إلَّا انعكاسٌ لمبلغ التّأمين.

ثالثاً: تحديد القسط تبعاً لقيمة الشَّيء المؤمَّن عليه:

حيث ينطوي التّأمين على تعويض المؤمَّن له عن الخسائر التي تلحق بالأصول المملوكة له نتيجة مخاطر الإنترنت. وتحديد قيمة الشّيء المؤمّن عليه في نطاق مخاطر الإنترنت ما يزال أمراً صعباً، فهو ليس بعقارٍ أو سيارةٍ تُثمّن في السوق، بل كثيراً ما تكون السّمعة التجارية هي المؤمَّن عليه، بالإضافة إلى حماية المعلومات العائدة للمؤمَّن له، والأنظمة التي يستخدمها، والجدران النارية التي يحمي بها حواسيبه، بمعنى أنّ ما يُحمَى ليس شيئاً مادياً (على النحو الذي توضّح مسبقاً)، بل هو حقوقٌ معنويةٌ تنطوي على سمعةٍ تجاريةٍ، وحقوق ملكيةٍ فكريةٍ كالأسرار التجارية التي تكتشف في حال حصول خرقٍ لأنظمة المؤمَّن له، بالإضافة إلى فقد ثقة المستهلكين بالشّركة التي يتعاملون معها (على أنَّ هذه المخاطر مثلاً تُنتج في كثيرٍ من الأحيان ضرراً مادياً يتمثّل بهلاك القرص الصّلب، أو دفع مبالغَ نقديّة للإصلاح أو انقطاع الأعمال)، وغير ذلك من الخسائر التي سبق الحديث عنها. وفي خضمّ كلّ ذلك يصعُب على شركة التّأمين عمليّة تحديد قيمة الأشياء المؤمَّن عليها؛ لأنَّ السمعة والثقة ليست أموراً يمكن تثمينها في السوق بسهولةٍ، بل هي نتاج تعبٍ وجهدٍ كبيرينِ ووقتٍ أكبر، وعليه تنطوي مشكلة صعوبة تحديد قيمة الأشياء المؤمّن عليها عند عمليّة تحديد القسط.

وبعد دراسة أهم العوامل المؤثرة في تحديد قسط التّأمين، يتدارك إلى الذهن تساؤلٌ حول كيفيّة حلّ هذه المعضلة لا سيّما في ظلّ انتشار التّأمين على مخاطر الإنترنت على نطاقٍ واسعٍ، وبالنظر إلى الصعوبات التي تحيط بكلّ عاملٍ على حدة؟؟

الحقيقة وبحسب دراساتٍ أُقيمت على حوالي 200 وثيقة تأمين على الإنترنت، فقد ثبت أنّ مقدّمي خدمات التّأمين غالباً ما يعتمدون في التسعير على أسعار المنافسين، وعلى مقارناتٍ مع أنواع التّأمين الأخرى، وعلى التّخمينات! وتحذّر وكالة فيتش من أنّ بعض شركات التّأمين التي تقدم خدمات التّأمين ضد مخاطر الإنترنت ليست لديها الخبرة الكافية في الاكتتاب في نطاق مخاطر الإنترنت، وفي بعض الحالات اعترفت بعض الشركات بأنّها لا تملك معلوماتٍ تاريخيةً موثوقةً يمكن بناءً عليها تقديم توقّعاتٍ واستنتاجاتٍ حقيقيةٍ حول توقعات الخسائر[251]. وعلى سبيل المثال: قد يُقدّم تخفيضٌ للأقساط بناءً على كون طالب التّأمين متعاقداً مع مزوّد خدمات أمن معيّن من جانب شركة التّأمين، فحاملو وثائق شركة لويدز للتّأمين يحصلون على تخفيض 10% من الأقساط إذا ما استخدموا برمجيات الأمان التي تقدّمها شركةTRIPWIRE[252].

في الواقع، يثير هذا الكلام بعض المخاوف من أنّ سوق التّأمين ضدّ مخاطر الإنترنت ما يزال حتى الآن يعاني من عدم الدّقّة في التسعير، وعدم الدقة في معرفة المخاطر، وهو ما ينعكس سلباً على المؤمَّن له الذي قد ينصدم بمبالغ تأمينٍ لا تكفي لتغطية مخاطره كلّها، نتيجة لعدم القدرة على الدراسة الدقيقة لما يمكن أن يتعرّض له من مخاطرَ في أثناء عمله، ورغم دفعه أقساطاً قد تعتبر عاليةً بالنّسبة له؛ نظراً لأنَّ شركات التّأمين تُقدّر الأقساط بصورةٍ عشوائيّةٍ بحسب ما سبق من أنَّ التّسعير يتمّ على تخميناتٍ وبمقارناتٍ معينةٍ، رغم أنّ أوجه المقارنة قد لا تكون صحيحةً بسبب اختلاف طبيعة الأعمال المؤمّنة، والمخاطر المؤمّن ضدّها، والأشياء محلّ التّأمين عن باقي أنواع التّأمين الأخرى لأسبابٍ طال شرحها سابقاً، وبالرّغم من أنّ الطرق المذكورة قد لا تفيد على نحوٍ صحيحٍ مئةً في المئة في خدمة المؤمَّن لهم، لكن يبدو أنّ ذلك هو المسار الأوّل الذي تتبعه شركات

---

[251] Aburish, N., Fixler, A., & Dr. Hsieh, M. (2019). P 7-8.

[252] Kesan J. p. & Others, (2005). P 14.

التّأمين في تلمّس طريقها نحو الوصول إلى أقساطٍ أكثر دقةً، نتيجةً للنّقص الحاصل في المعلومات، ولحداثة هذا النوع من التّأمين على أمل الوصول في الأيام القادمة إلى ما يرمي إليه المؤمَّن له وشركة التّأمين على حدٍّ سواء.

وفي سبيل الإضاءة أكثر على بعض النزاعات القضائيّة الحاصلة بين المؤمَّن لهم وشركات التّأمين سنعرض بعض الأمثلة القضائيّة:

1- في عام 2017، تعرّضت شركة موندليز للصناعات الغذائية لهجوم سيبرانيّ عبر برامج خبيثةٍ ممَّا كان يعرف وقتها بفايروس notpetya، وتم الدخول إلى خادمينِ في منطقتينِ مختلفتينِ، ومن ثمّ حصل بعدها الانتشار، وتسبّب الهجوم بسرقة معلومات العديد من العملاء، وأدّى إلى توقّف 1700 خادم و24 ألف حاسوبٍ عن العمل لمدّةٍ معيّنةٍ، وتكبّدت الشركة نتيجةً لهذا الهجوم حوالي 100 مليون دولار أمريكيّ نتيجة أضرار الممتلكات والأعطال الحاصلة وعدم القدرة على تقديم الخدمات للمستهلكين، وكانت الشّركة في تلك الأثناء تملك وثيقة تأمين ضدّ كلّ الأضرار (لم تملك وثيقة تأمين ضدّ مخاطر الإنترنت على وجه الخصوص)، وتقدّم هذه الوثيقة التغطية للخسائر المادية اللاحقة بالبيانات، والبرمجيات، والأنظمة نتيجة تدخل البرامج الخبيثة، بالإضافة إلى تغطية النفقات والخسائر الحاصلة نتيجة انقطاع العمل بسبب فشل أنظمة المؤمَّن له في العمل. وعند حصول هذا الهجوم طلبت موندليز من شركة تأمينها زيورخ أن تقدم لها التعويض، فرفضت الشركة ذلك استناداً على أحد الاستثناءات الواردة في الوثيقة، وهي استثناء الخسائر الناشئة من أعمال الحرب من قبل أيّ دولةٍ أو وكيلٍ لها أو قوّاتٍ تابعةٍ لها، ويُشار إلى أنّ هجوم فايروس notpetya يعود في أصله إلى روسيا، وعندها ادّعت موندليز على شركة زيورخ بوصفها أساءت استعمال هذا الاستثناء بصورةٍ غير مبرّرةٍ، وفسّرتِ النّص ليتلاءم ومصالحها دون أيّ أساسٍ قانونيٍّ، لا سيّما إذا ما عرفنا أنّ زيوريخ بعد رفضها الدفع بعثت برسالةٍ تبدي فيها رغبتها بالدفع والتراجع عن الرّفض، لكن بعد مماطلةٍ كبيرةٍ في الوقت لم تدفع، فكان الإصرار لدى موندليز على رفع الأمر إلى القضاء[253]، ولم يُتوصَّل إلى معرفة رأي القضاء في هذه القضيّة، لكن كان السّؤال الأبرز بحسب

[253] https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf

تاريخ الزيارة: 30\11\2020، الساعة 11:30. p.m

بعض الفقه حول تفسير استثناء الحرب الموجود في الوثيقة لناحية إمكانية اتساعه ليضمّ الهجوم الإلكتروني من جانب الدولة، بمعنىً آخر أنّ زيوريخ لمّا وضعت هذا الاستثناء لم يكن يخطر في بالها إمكانية تطبيقه على الهجوم الإلكتروني، بل غالباً كان يستخدم في الحرب التقليدية، وكان الدفع بهذا الاستثناء سابقةً تحصل لأوّل مرّةٍ، ولكونه قد يخدم مصالح شركة التّأمين في هذه القضية فقد توسّع استخدامه لناحية رفض التغطية، وهو ما يخالف المبدأ الذي يقول بتوسيع التفسير لنصوص الوثيقة لناحية توسيع التغطية لا تضييقها[254].

2–في حادثة أخرى، بدأت القصة حينما اشترت شركة P.F. Chang's China Bistro وثيقة تأمين ضد مخاطر الإنترنت من شركة federal insurance في عام 2014، وبحسب الشركة فإنّ هذه الوثيقة تقدّم حلاً مرناً للتأمين لأصحاب الأعمال الإلكترونيّة، فتقدم تغطيةً للخسائر المباشرة والمسؤولية القانونية والخسائر الناشئة عن حوادث خرق الأمن الإلكتروني، وقد صُنِّفت الشركة العميلة على أنّها ذات خطر عالٍ؛ لأنّها تُجري أكثر من 6 مليون معاملة تحويل سنوياً، وتتعلق هذه المعاملات بالبطاقات الائتمانية للعملاء، وعليه كان خطر سرقة الهويات عالٍ جداً لدى هذه الشركة، ولأنَّ شركة مثلها بضخامة أعمالها لا يمكنها إدارة التعاملات بالبطاقات لوحدها فقد لجأت إلى شركة أخرى bank of America merchants services لتدير لها هذه التعاملات بالتعاون مع المصارف المصدرة للبطاقات، وبناءً على ذلك أُعطيت هذه الشركة المعلومات المتعلقة بالعملاء أصحاب البطاقات الائتمانية. وبموجب الاتفاقية المعقودة بين الطّرفين تلتزم شركة chang بتعويضٍ bams عن الرّسوم والغرامات والعقوبات التي قد تُفرض على الأخيرة من جهة المصارف المصدّرة التي تتعامل معها نتيجةً لأيّ حادثة خرق بيانات. ولاحقاً في العام 2014 علمت chang أنّ خرقاً أمنياً لبياناتها قد حصل فسرقت ونشرت معلومات عن حوالي 60 ألف بطاقةٍ ائتمانيّةٍ، فأبلغت على الفور شركة تأمينها التي قدّمت تعويضاً يعادل مليون و700 ألف دولار. وفي أيّار عام 2015 طلب البنك المصدر master card من bams بالتعويض عمّا تكبّده من مبالغَ لإعلام الأفراد المتضرّرين من هذا الخرق، وتكاليف إعادة إصدار بطاقات جديدة،

[254] Justine Ferland, (2019). Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case, v35, Elsevier: UK, Computer Law & Security Review, P 371.

وعندها طلبت bams من chang أن تدفع لها المبالغ المطلوبة بموجب الاتفاقية الموقّعة بينهما وتمّ الدفع، فيما بعد طلبت chang من شركة تأمينها أن تعوّضها عمّا دفعته، لكن قُوبِل هذا الطلب بالرفض من قبل الأخيرة مدّعيةً أن طلب التعويض من جانب bams لا يدخل ضمن التَّغطية التي تقدّمها نيابةً عن عميلها المؤمَّن له للضَّرر الحاصل للآخرين؛ نظراً لأنَّ البيانات المسروقة لم تكن داخلةً في ملكيّة bams ليمكن القول بحصول ضررٍ لخصوصيّتها، وعليه فلن تقوم بتعويض المؤمَّن له عمَّا دفعه لbams ، ووافقت المحكمة شركة التّأمين وقضت بعدم أحقيّة المؤمَّن له بأيّ مبلغ تعويضٍ عمَّا دفعه لbams لعدم وجود أيّ خرقٍ للخصوصيَّة يُشكِّل أساساً لادّعاءٍ قانونيٍّ ضدّ chang، كما طلبت chang من شركة تأمينها أن تعوّضها عن نفقات الاتصال بالزبائن التي دُفِعت عن طريق ماستر كارد، وذهبت المحكمة إلى جانب المؤمَّن له بأحقيّة أخذه التّعويض عن هذه المبالغ؛ لأنَّه ومن حيث المبدأ الملتزمُ الأساسيُّ بهذا الواجب وإن قام شخصٌ آخر بفعله نيابةً عنه(على الرّغم من معارضة شركة التّأمين لدفع هذا التعويض)، كما أنَّ شركة التّأمين رفضت دفع مطالباتٍ أخرى من جانب chang نتيجة التزاماتها التعاقديّة مع bams ؛ لوجود استثناءٍ يعفي شركة التّأمين من التّغطية للالتزامات التّعاقديّة ما بين المؤمَّن له وطرفٍ ثالثٍ خارج الوثيقة، ووافقت المحكمة على رأي شركة التّأمين ورفضت طلب المؤمَّن له بالتغطية[255]. وعليه يمكن القول إنَّ شركة chang لم تحقّق المطلوب بالكامل من وثيقة التّأمين التي تملكها، كما أنّ لجوءها إلى القضاء لم ينصفها، وانتهى الأمر بخسارتها لدعواها ضد شركة تأمينها.

3- تعرّضت شركة medidata وهي شركة معلوماتٍ تقدّم خدماتٍ برمجيّةً في القطّاع الصّحيّ، لاختراقٍ عبر مخترقٍ تلاعب برسائل البريد الإلكترونيّ الوارد للشّركة ليظهر أمام الموظّفين بمظهرٍ رئيس الشّركة، وطلب منهم تحويل مالٍ إلى حسابه بحجّة أنّه يقوم بصفقةٍ ماليّةٍ وبحاجةٍ للمال، وقد دُبِّر الأمر ليظهر كما لو أنّه بُعِث من الرّئيس الحقيقيّ للشّركة، وعليه فقد تحوّل إليه، من ثمّ طلب تحويلاً ثانياً، وعندها شكّ أحد الموظّفين بالأمر، فتحدّث مع الرّئيس الحقيقيّ للشّركة يسأله عن الأمر، وحينها كُشفت الخدعة بأنّه لم يطلب أيَّ شيءٍ ولم

[255] يمكن قراءة القضية كاملةً على الرابط الآتي:
https://www.locktoncyberriskupdateblog.com/wp-content/uploads/sites/6/2016/06/PF-Changs-China-Bistro-Inc-v-Federal-Insurance-Company.pdf
تاريخ الزيارة: 1\12\2020، الساعة 11:30 p.m .

يبعث أيَّ رسالةٍ، وبذلك علمت الشركة أنَّها قد وقعت ضحيةً لاحتيالٍ إلكترونيٍ بمبلغ يعادل 4 ملايين دولار. فطلبت الشركة من شركة تأمينها federal insurance والتي كانت تحمل وثيقةً لاحتيال الحاسب ولتحويل الأموال والسّرقة، وتغطّي وثيقة الاحتيال خسارة الأموال والممتلكات والأسهم النّاشئة عن احتيال الحاسب من قبل طرفٍ ثالثٍ، ويُعرَّف الاحتيال بحسب الوثيقة على أنّه الأخذ غير القانوني أو الاحتيال على الأموال والممتلكات والأسهم النّاشئ عن خرق الحاسب، والذي يضم الدخول أو التغيير الاحتيالي للبيانات في الحاسب. أمَّا وثيقة تغطية تحويل الأموال فكانت تغطّي السرقة الناشئة عن تحويل الأموال الاحتياليّ من طرفٍ ثالثٍ، وعليه فقد رفضت شركة التّأمين التغطية بحجّة أنّ التحويل حصل بشكلٍ إراديٍّ من جانب الموظّفين التّابعين للشركة، ولم يكن هناك أيّ دخولٍ احتياليٍّ، أو تحويل احتيالي من جانب طرفٍ ثالثٍ، كما أنَّه لم يكن هنالك أيّ تغييرٍ احتياليٍّ على البيانات المخزَّنة، وذلك تمسّكاً من شركة التّأمين بحرفيّة نصّ الوثيقة، وعليه رُفِع النّزاع إلى المحكمة التي قضت أنّ الاحتيال في هذه القضيّة موجودٌ، ولا يشترط أن يتمّ الدخول والتغيير في البيانات، أو أن يتمّ التحويل من جانب المخترق نفسه، بل يكفي أن يكون العمل الاحتيالي الممارس هو ما دفع إلى وقوع السرقة والتحويل الإلكتروني (وهو ما رأته المحكمة متوفراً؛ لأنّ الموظفين قاموا بالتحويل كنتيجةٍ رئيسةٍ لرسائل انتحال الشخصية المرسلة إليهم)، وبذلك فإنّ القرصنة والاحتيال بحسب المحكمة تحدث بوسائلَ عدّة من ضمنها خداع المؤمَّن له لدفعه للتحويل، فقُبِلَ ادّعاء المؤمَّن له وإلزام شركة التّأمين بدفع التعويض عن الخسائر الحاصلة[256]. والجدير بالذكر أنّ هذه الواقعة تتشابه إلى حدٍّ كبيرٍ مع ما حصل مع شركة اكوا ستار (سيتم ذكر القضية لاحقاً)، لكنَّ المحكمة في القضية الأخيرة انتهت إلى عدم التغطية على عكس ما حصل في هذه القضية، وهو ما يفتح الباب واسعاً أمام فكرة التفسير المتباين للوثائق بحسب رأي كل محكمة على حدة.

[256] يمكن قراءة القضية كاملة على الرابط الآتي:
https://www.scholar.google.com/scholar_case?case=10203829454376203918&q=Medidata+Solutions+Inc.+v.+Federal+Insurance+Co.&hl=en&as_sdt=2006
تاريخ الزيارة: 2\12\2020، الساعة 11:40 p.m.

وفي الختام، يبدو أنَّ عمليَّة دفع الأقساط ما تزال عمليّةً شاقّةً على المؤمَّن لهم، وشركات التّأمين على السّواء في عقد التّأمين ضدّ مخاطر الإنترنت، وعليه بعد دراسة القسط لا بدَّ من الانتقال لدراسة الالتزام الآخر على عاتق المؤمَّن له، وهو واجب الإعلام والعناية في المطلب الآتي.

المطلب الثّاني

التزام المؤمَّن له بالإعلام وبواجب العناية

لا يقتصر التزام المؤمَّن له في عقد التّأمين ضدّ مخاطر الإنترنت على دفع أقساط التّأمين فقط، بل إنّ العقد ينطوي على التزاماتٍ إضافيّةٍ من أجل الوصول إلى التّطبيق الأمثل، والهدف المُراد من إبرام عقد التّأمين. وتنطوي هذه الالتزامات على واجب الإعلام أو الإخطار من جانب المؤمَّن له، ويشترك هذا الالتزام بين أنواع التّأمين كلّها، إذ يتوجّب على المؤمَّن له إخطار شركة التّأمين بكلّ الحوادث الحاصلة، بما قد يؤثّر سلباً على سير العمليّة التّأمينيّة، كما يُضاف إلى ذلك واجب المؤمَّن له بذل العناية الكافية من أجل محاولة تجنب حصول الخطر، مع تعهّده بالالتزام بما تصدّره إليه شركة التّأمين من تعليماتٍ من أجل السّلامة الإلكترونيّة. وعليه يُقسم هذا المطلب إلى فرعينِ يتناول الأوّل التزام الإعلام، في حين يتضمّن الثاني التزام القيام بالعناية المطلوبة.

الفرع الأول

التزام المؤمَّن له بإعلام شركة التّأمين

يقع على عاتق المؤمَّن له واجب إخبار شركة التّأمين بكلِّ الحوادث الحاصلة في أثناء فترة سريان عقد التّأمين بما يمكن أن يؤثّر على الخطر المؤمَّن منه، ويجعل وقوعه أكثر احتماليّةً، وهذا الالتزام في عقد التّأمين ضد مخاطر الإنترنت يعود في أصله إلى فكرة التّأمين بشكلها العام من حيث قيامها على افتراض حسن النية من جانب المؤمَّن له، والذي يلتزم بتقديم المعلومات الصحيحة حول الخطر المؤمن منه، والشيء محل التّأمين من أجل تكوين صورةٍ حقيقيةٍ من جانب شركة التّأمين تساعدها على تحديد مبلغ التّأمين والأقساط واجبة الدفع.

أولاً: مضمون الالتزام بالإعلام:

لم يأتِ المشرّع السّوريّ في القانون المدنيّ على ذكر هذا الواجب بصورةٍ صريحةٍ، أمّا قانون التجارة البحرية فقد جاء في تفصيل التزام المؤمَّن له بالإعلام، إذ أوجب على المؤمَّن له أن يعطي شركة التّأمين بياناً صحيحاً عند التعاقد بالظروف التي يعلم بها، ومن شأنها أن تمكّن شركة التّأمين من تقدير الأخطار، بالإضافة إلى واجب المؤمَّن له إطلاع الشركة على ما يحصل من تغييراتٍ جوهريّةٍ تؤثّر على الأخطار في أثناء سريان العقد، يُضاف إلى ذلك إطلاع شركة التّأمين على أي حادثةٍ من شأنها جعل المؤمَّن له مسؤولاً كي تؤدّي الشركة واجبها، والجزاء على مخالفة هذا الواجب يتراوح بين حقِّ الإبطال أو سقوط الحقّ في التّعويض (مبلغ التّأمين)[257]، ويبدو من هذه المادّة أنّ التزام الإعلام يظلُّ قائماً منذ اللّحظة التي تسبق سريان عقد التّأمين وحتّى نهايته، فهو التزامٌ مستمرٌ ويقوم على مراحل عدّة تبدأ منذ لحظة طلب التّأمين بوجوب الإفصاح عن طبيعة المخاطر، وما يحصل لاحقاً من تغييرات ولا تنتهي إلا بانتهاء العقد للأسباب التي ذكرت سابقاً، وتنطبق النصوص السابقة على معظم أنواع التّأمين بما فيها عقد التّأمين ضد مخاطر الإنترنت، إذ يبقى المؤمَّن له ملتزماً بإعلام شركة التّأمين بكل ما يعلمه من مخاطرَ تحيط بالشيء المؤمّن عليه، انطلاقاً من المبدأ العام في الإعلام، لكن لهذا الالتزام في العقد الذي يُدرَس أهميةٌ أكبر، وميزة مختلفة تعطيه اختلافاً عن غيره؛ لأنَّ المخاطر الإلكترونية ما تزال غير معروفة بشكلٍ تامٍ لشركة التّأمين للأسباب الواردة أعلاه من نقص المعلومات التاريخية، لذلك تعتمد شركة التّأمين في التقييم على ما تُخبر به من جانب طالب التّأمين، والذي يفترض به توخي الحذر وحسن النية عند الإعلام؛ لأنّ إخفاء بعض الحقائق عن طبيعة المخاطر التي ينوي التّأمين منها، وما يهدد أعماله قد يكون سبباً لامتناع شركة التّأمين عن دفع التعويض عند حصول الخطر، لا سيّما عندما تكون هذه المعلومات جوهريّةً كما لو أنَّه ذكر وجود جدران ناريّة لحماية أنظمته، وكان ذلك مخالفاً للواقع، أو لو أنكر وجود معلوماتٍ حسّاسةٍ شخصيّةٍ تتعلّق ببعض العملاء رغبةً منه بإخفاء ذلك لأسبابٍ معيّنةٍ، وعندما حصل الخطر تسرّبت، فهنا لا يمكن لوم شركة التّأمين لعدم دفعها مبلغ التّأمين؛ لأنّ المؤمَّن له لم يكن صادقاً في إفاداته.

---

[257] المواد (364 حتى 368) من قانون التجارة البحرية السوري رقم 46 لعام 2006.

والتزام المؤمَّن له بالإعلام يبدأ عند تقديم طلب التّأمين ضد مخاطر الإنترنت إلى شركة تأمينٍ معيّنةٍ مبدياً رغبته في الحصول على تغطية لأعماله، وعندها تقدّم الشّركة نماذجَ مطبوعةً تحتوي أسئلةً معينةً أمنيةً وتقنيةً ينبغي على طالب التّأمين أن يجيب عنها بصدقٍ من أجل تقييم المخاطر التي تحيط بالشَّيء المؤمَّن عليه، (بناءً على هذه الأسئلة تُقيَّم المخاطر، وتحدّد الأقساط، ولذلك يعد التزام الإعلام بصدق أساس عملية التّأمين). وتدور هذه الأسئلة والتي غالباً ما تُرسل على شكل استبيانٍ إلى طالب التّأمين عبر الإنترنت (حوالي 250 سؤال) حول فهم المخاطر الأمنيّة التي يعانيها، وما هي الحماية الإلكترونية (الميزانية المرصودة، البنية التحتية الأمنية، برامج الحماية من الفايروسات، إجراءات السلامة والفحص المستمرّ، الاستعانة بمصادر حماية خارجية) من أجل التحليل الشامل المادي والتقني للأمن والشبكات والإجراءات[258]. وقد تعتمد بعض شركات التّأمين في سبيل رغبتها التأكد من صحة المعلومات المقدمة من جانب طالب التّأمين على الاستعانة بإيراد نصوص القوانين التي تحكم عقود التّأمين لتذكير المؤمَّن لهم بأنَّ تقديم معلوماتٍ خاطئةٍ عن عمدٍ يعدّ جريمةً في بعض قوانين الولايات المتحدة الأمريكية، وهو ما يوفّر حافزاً كبيراً لدى طالبي التّأمين لتقديم معلوماتٍ صحيحةٍ عن المخاطر التي يتعرَّضون لها خوفاً من عقوبة السّجن[259]، في حين تشير معظم الشركات في النماذج المقدمة من جانبها إلى واجب الإفصاح، حيث تلزم شركة رأس الخيمة على سبيل المثال طالب التّأمين بأن يفصح عن أيّ معلوماتٍ يُعتقد أنّها قد تؤثّر على قرار الشركة بتقديم التغطية التّأمينية، ويتوجب عليه الإبلاغ عن هذه المعلومات تحت طائلة رفض طلب التغطية، بل إنّ هذا الواجب يظلّ قائماً في حال تجديد العقد أو تمديده أو تغييره أو إعادته، وفي حال لم يُعلم عن حصول أيّ تغييرٍ على المعلومات المذكورة تعتبر المعلومات المقدمة هي الأساس الذي تأخذ به شركة التّأمين، وقد تقرّر الشركة إلغاء العقد أو تخفيض قيمة التعويض في حال حصول الخطر، وفي حال كان الأمر منطوياً على احتيالٍ فقد يُلغى العقد كأنّه لم يكن (وهذا يعني خسارة الأقساط جميعها التي قد دُفِعت كجزاءٍ لمخالفة المؤمَّن له واجباته بالإعلام)[260]، كما تذهب شركة axa إلى تقرير هذه

---

[258] Kesan J. p. & Others, (2005). P 11.

[259] Ibid, p 12.

[260] Simply Cyber Policy Terms & Conditions. (2018). P 1.

الأحكام ذاتها، ففي حالُ قدّمت بيانات غير حقيقيّة وحصل الخطر يمكن لشركة التّأمين أن تقدم التغطية وفقاً لهذه البيانات الخاطئة، أو أن ترفض التغطية بكل بساطة، كما ينبغي على المؤمَّن له إعلام شركة التّأمين كتابةً في حال حصول أي تغييرٍ لدى المؤمَّن له يؤثّر على التغطية التّأمينية[261].

وتدور أغلب الأسئلة _ والتي تمثّل جوهر التزام المؤمَّن له بالإجابة عنها بصدق _ حول الخدمات المهنية المقدمة (المحتوى المقدم)، الأمن الإلكتروني، السياسة المتبعة من جانب طالب التّأمين بشأن أمن معلوماته، سياسة حذف العناصر المسيئة، السيرة الذاتية لكبار المسؤولين لا سيّما مديري تكنولوجيا المعلومات (ويبدو هذا الأمر على غايةٍ من الأهمية؛ لأنَّ كثيراً من الخروقات الإلكترونيّة يكون وراءها العاملون في الشركة برغبةٍ خفيّةٍ من المنافسين لتدمير الشركة عبر موظفيها أنفسهم؛ نظراً لأنّ الشكوك لا تدور حول هؤلاء في البداية)، كما قد يُستفسَر من طالب التّأمين عن البيانات المالية المدقّقة[262].

وبصورةٍ أكثر تفصيلاً تقسم هذه الأسئلة إلى شرائحَ يُتناول منها:

1-عمل المؤمَّن له ونشاطاته، مثل القطاع الذي ينتمي إليه، عدد الموظفين، تاريخ الهجمات الإلكترونية، حجم التجارة الإلكترونيّة، المواقع المملوكة له.

2-إدارة المخاطر وأمن المعلومات، كخطط الاستجابة للحوادث الإلكترونيّة، واستمرارية العمل، سياسة الخصوصية، إجراءات إنهاء عمل الموظفين، مدى توافق العمل مع القوانين التي تحمي البيانات والخصوصيّة.

3-البيانات والسجلات السرية مثل المعلومات الشخصية والصّحية والتجارية، معلومات بطاقات التسديد، الملكية الفكرية، حجم هذه المعلومات، مشاركتها مع أطراف ثالثة (كتخزينها لدى مقدم خدمات تخزين سحابي)، سياسة الاسترجاع، والتدمير، والتشفير، والحفظ.

---

[261] https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf

تاريخ الزيارة: 4\10\2020، الساعة 11:35 .p.m.

[262] Kesan J. p. & Others, (2005). P 11.

4-تكوين شبكة تكنولوجيا المعلومات، وتتضمن السؤال عن تكوين هذه الشبكة، حجمها، أنظمة التشغيل المستخدمة، معايير الأمان المتبعة، معرفة مقدمي خدمات البرامج والأنظمة، ومقدمي خدمات التخزين والخدمات الأخرى، الجدران النارية المستخدمة للحماية، أنظمة الحماية من الفيروسات وكشف التسلل إلى الشبكة، وإجراءات الوصول عن بعد، كلمات المرور المشفرة، التحقق من أمان الأجهزة الذكية المستخدمة[263].

وفي أغلب الأحيان لا تكتفي شركة التّأمين بطرح الأسئلة فقط، بل تقوم بجولاتٍ إلى مقرّ الشركة طالبة التّأمين للوقوف على الأعمال التي تتم إدارتها، والتحقق من صحة ما أُجيب عنه لتكوين فكرةٍ متكاملةٍ عن طالب التّأمين عن مدى ضعف وقوة بيئة الحماية للمعلومات المخزنة، إذ إنّ طريقة طرح الأسئلة عبارة عن تقييمٍ ذاتيٍ من قبل شخص طالب التّأمين قد تحتمل الصحة أو الكذب من جانبه لإخفاء بعض الحقائق، ولذلك لا يكتفى بذلك، ولا بدّ عندها من الوقوف على الشّيء المؤمَّن عليه، والمخاطر المحيطة به من قبل شركة التّأمين عبر الدخول إلى مقرّ طالب التّأمين من أجل فحص سلامة الأنظمة والأجهزة المستخدمة، وخدمات الأمان والحماية الموجودة، كما أنّ شركات التّأمين قد تلجأ إلى إجراء مكالماتٍ هاتفيةٍ مع طالبي التّأمين، وقد تقوم بلقاءاتٍ مع موظفي العميل المحتمل[264].

ونظراً لخصوصية تأمين مخاطر الإنترنت من حيث طبيعة المخاطر، وصعوبة التقييم والاكتتاب، كان لا بدّ من التوسّع في عملية طرح الأسئلة الأمنية والتقنية، ومحاولة التحقق بصورة أكثر دقةً، ممّا قيل. والجدير ذكره أنّ التزام الإعلام كما قيل سابقاً التزامٌ مستمرٌ كلّ مدة العقد، لذلك يجب على المؤمَّن له إعلام شركة التّأمين بحال حصول أي تغيير على المخاطر المؤمَّن ضدها أو الشيء المؤمَّن عليه من شأنه أن يجعل احتمالية تحقق المخاطر أكثر وقوعاً، كما لو شك المؤمَّن له بوجود فيروسات على أنظمة تشغيله نتيجة خطأ الموظف بالضغط على رابطٍ مشبوهٍ، أو حصلت بعض الانقطاعات في خدمته أو عملية حجبٍ لمواقعه الإلكترونيّة.

---

[263] Coburn, A., Leverett, E., & Woo, G. (2018). P 261-262.

[264] Luzwick, P. (2001) If Most of Your Revenue Is From E-Commerce, Then Cyber-Insurance Makes Sense, v2001, issue 3, computer fraud & security, P 17

ثانياً: الالتزام بالمطالبة:

و علاوةً على ما سبق ينبغي على المؤمَّن له إعلام شركة التّأمين عند حصول الحادث المؤمَّن منه، وأن يطالبها بدفع التعويض، ويقوم هذا الالتزام على واجب الإبلاغ عن الحادث الإلكتروني، والامتناع عن القيام بأي فعل قبل الحصول على ردٍّ من شركة التّأمين، ومطالبتها بأن تقوم بواجبها المتّفق عليه من تغطيةٍ للأضرار، وإصلاح ما تمّ تخريبه، وقد جعل المشرع السوري من الشّرط الذي يقضي بسقوط حقّ المؤمَّن له بسبب تأخره في إعلان الحادث المؤمّن منه إلى السلطات، أو في تقديم المستندات إذا تبين من الظروف أنّ التأخر كان لعذرٍ مقبولٍ، باطلاً[265]، ويُعلّل هذا الالتزام بأن هذا الحادث قد يؤدي إلى حصول مطالبةٍ قضائيّةٍ للمؤمَّن له من جانب عملائه المتضررين، وإن لم تكن شركة التّأمين على علم في الوقت اللازم فقد يؤدّي ذلك إلى خسائرَ كبيرةٍ بالنّسبة للمؤمَّن له، وشركة التّأمين على السّواء، كما قد لا يكون المؤمَّن له ميسور الحال في الوقت ذاته لدفع التّعويضات ما يهدّد بإشهار إفلاسه، ويُضاف إلى ذلك أنَّ كثيراً من المخاطر تحتاج إلى سرعةٍ كبيرةٍ في التّصدّي لها وإصلاحها حتى لا تترك آثاراً كبيرةً، وخسائرَ أكبرَ، لذلك ينبغي على المؤمَّن له عند اليقين بحصول الخطر المؤمّن منه أو الشكّ بوقوعه أن يبادر على الفور إلى إبلاغ شركة التّأمين، وفي كثيرٍ من الأحيان تقبل شركات التّأمين مطالبات المؤمَّن لهم في حال أبلغ عن حصول الحادث الإلكترونيّ في الوقت المناسب (قد تتراوح المدّة بين شهر وشهرين من تاريخ اكتشاف الحادث)[266].

ويمكن القول إنّ شركات التّأمين تستمدّ إلزاميّة هذا الإخبار من:

1- المبدأ العام في التّأمين وهو حسن النية والذي كما ذكر سابقاً يُوجب على المؤمَّن له الإعلام عن كلّ الحوادث الطارئة في أثناء فترة العقد بصدقٍ وبالسّرعة المطلوبة.

2-القوانين التي تحمي خصوصيّة البيانات الإلكترونيّة، فعلى سبيل المثال يفرض قانون حماية البيانات العامّة الأوروبي (gdpr) على المتحكّمين بالمعلومات (وهذا المفهوم واسع يشمل شركات التخزين السحابي،

[265] المادة (716-2) من القانون المدني السوري رقم 84 لعام 1949.

[266] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). P 10.

الشركات التي تعالج البيانات، الشركات التي تخزّن البيانات لديها لحاجات عملها كالمستشفيات أو البنوك مثلاً)، الإبلاغ عن خرق البيانات إلى السّلطات المختصّة خلال 72 ساعة، والجهات التي تخالف هذا النّصّ يمكن تغريمها حتى 4% من حجم مبيعات الشّركة العالميّ السّنويّ أو 20 مليون يورو أيّهما أكبر[267]، والحقيقة أنّ نصّاً كهذا يمكن أن يحقّق تقدّماً واسعاً في سبيل وضع الحدّ لحالات الإخفاء المتكرّر للحوادث الإلكترونيّة من جانب الشّركات المخترَقة، ويمهّد الطريق للحصول على قاعدة بياناتٍ أكبرَ عن المخاطر الإلكترونية. أمّا عن الولايات المتحدة الأمريكية فلا يوجد لديها تنظيم تشريعي فيدرالي واحد على مستوى الدّولة ككلّ لحماية خصوصية البيانات، بل إنّ التّشريعات الموجودة غالباً ما تكون صادرة عن ولايةٍ معيّنةٍ، إذ تبنّت أوهايو وساوث كارولينا وميتشيغان القانون النموذجيّ لأمن بيانات التّأمين المستندة إلى لوائح إدارة الخدمات الماليّة في نيويورك، والتي تستلزم الإبلاغ عن الحدث السيبراني خلال 72 ساعة إلى المنظمين، وتقديم إشعار للمستهلكين بطريقة معينة وفق جدول زمني محدد[268]. وعليه قد تساعد هذه النصوص على تدعيم فكرة التّأمين ضدّ مخاطر الإنترنت؛ لأنّ المؤمَّن له سيكون أمام أحد خيارين، إمّا أن يخبر المختصّين ويضم ذلك شركة تأمينه عن حصول الخطر الإلكتروني، أو أن يتجاهل هذا الواجب وعندها سيكون أمام مخالفةٍ قانونيّةٍ تستوجب دفع غراماتٍ باهظةٍ، وعندها يكون الخيار لشركة التّأمين بين أن تغطّي هذه النفقات أو تستثنيها؛ نظراً لأنّها قد تتضرّر من هذا الإخفاء إذا ما تفاقمت الأضرار النّاشئة عن الخطر الإلكترونيّ المتحقّق.

3-وجوب الإبلاغ عن المخاطر الحاصلة والمطالبة بالدفع؛ لأنّ شركة التّأمين ضد مخاطر الإنترنت توجب على المؤمَّن له فعل هذا الأمر، بل إنّها قد تتملّص من واجبها بالدّفع إن دُفِع التّعويض أو حصلت تسويةٌ مع المتضرّرين من جانب المؤمَّن له قبل الحصول على موافقتها[269].

---

[267] Monroe, M. f., Boer, M. (2019). cyber risk insurance update: advances in risk management, prioritizing prevention and protection, Washington, D.C: USA, institute of international finance, p 6.

[268] Ibid, p 6.

[269] https://www.nok6a.net/%d8%a7%d9%84%d8%aa%d8%a3%d9%85%d9%8a%d9%86-%d8%b6%d8%af-%d8%ad%d9%88%d8%a7%d8%af%d8%ab-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a/

تاريخ الزيارة: 10\10\2020، الساعة 9:20 p.m.

4-وختاماً يبدو أنّ هذا الالتزام هو جوهر التّأمين، فلولا الإعلام هذا لما قامت الحاجة إلى وجود تأمينٍ ضدّ مخاطر الإنترنت (أساس منطقي للعقد). **وعلى سبيل المثال ما أوردته شركة التّأمين الأمريكية hiscox** من وجوب قيام المؤمَّن له بإبلاغ شركة التّأمين على نحو فوريٍّ خلال مدّة سريان الوثيقة، أو خلال فترة 14 يوماً تالية لانتهاء العقد إذا ما تمّ العلم بحصول خطرٍ ما خلال الأيام السبعة السابقة لانتهاء الوثيقة، فإذا كان من شأن هذا الخطر أن يهدّد بحصول مطالبةٍ معيّنةٍ، أو خسارةٍ، أو مسؤوليةٍ تجاه طرفٍ ثالثٍ تحت طائلة عدم الدّفع في حال الإخلال بواجب المطالبة[270]. **وفي مثالٍ آخرَ ما قدّمته شركة American International Group** في أحد نماذج التّأمين ضدّ مخاطر الإنترنت (تغطية انقطاع الشبكة) عن واجب المؤمَّن له في أن يعلم شركة التّأمين خلال 90 يوماً تالية لاكتشاف أيّ خسارةٍ بوثيقةٍ مثبتةٍ، وموقّعةٍ، ومؤكّدةٍ للخسائر تتضمّن وصفاً كاملاً لهذه الخسائر والظروف المحيطة بها، ووقت ومكان وسبب الخسارة، مع حساب تفصيلي لمقدار الخسائر، والمستندات والوثائق جميعها التي تشكل جزءاً من وسائل الإثبات.[271] وتجدر الإشارة إلى واجب المؤمَّن له إخطار وحدات الاستجابة للطوارئ التي تحددها شركة التّأمين من أجل الاستنفار لأيّ حادثٍ إلكترونيٍّ أو شبهة حادثٍ، كما يعتبر هذا الإخطار إلى الوحدات المذكورة إخطاراً لشركة التّأمين، وينشئ كل آثار الإبلاغ إلى شركة التّأمين نفسها[272].

ثالثاً: المشكلات المتعلّقة بواجب الإعلام والمطالبة في إطار عقد التّأمين ضدّ مخاطر الإنترنت:

لا يقوم التزاما الإعلام والمطالبة دائماً على نحوٍ يسيرٍ وسلسٍ وبصدقٍ كما هو واجب؛ لأنّ كثيراً من المؤمَّن لهم قد يقومون بإخفاء كثيرٍ من البيانات لأسبابٍ شخصيّةٍ معيّنةٍ، أو يحاولون عدم الإبلاغ عن حصول

---

[270] Cyber and data insurance, policy wording, (n.d). hiscox, p12.

[271] https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf

تاريخ الزيارة: 2020\10\14، الساعة 9:30 p.m.

[272] https://www.nok6a.net/%d8%a7%d9%84%d8%aa%d8%a3%d9%85%d9%8a%d9%86-%d8%b6%d8%af-%d8%ad%d9%88%d8%a7%d8%af%d8%ab-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a/

تاريخ الزيارة: 2020\10\10، الساعة 9:30 p.m.

الخطر لاعتقادهم بقدرتهم على احتوائه، وعليه يصطدم هذان الالتزامان بعوائقَ هي: الخطأ المتعمّد، الاختيار الخاطئ، والارتباط المتبادل.

1-أمّا عن الخطأ المتعمّد، فهو بالمعنى العام تعمّد المؤمَّن له إيراد معلوماتٍ خاطئةٍ بخلاف الحقيقة، أو إخفاء معلوماتٍ مهمّةٍ من شأنها أن تؤثّر على مسار التّأمين، **وفي نطاق التّأمين ضد مخاطر الإنترنت** يُشار إليه أيضاً على أنّه فشل المؤمَّن له باتخاذ التّدابير المناسبة لتقليل احتمال الخسارة (كما لو تخاذل المؤمَّن له عن تحديث أنظمة الحماية، أو ترك مواقعه عرضةً للقرصنة دون اتخاذ أيّ إجراءٍ نظراً لوجود تأمينٍ لديه) أو عندما لا يكون المؤمَّن له قادراً على إثبات حصول الخطر بصورةٍ ذاتيّةٍ (وفق مجرى الأحداث الطبيعي) دون أي تدخّل منه[273]، كما قد تظهر هذه المشكلة عند تعمد المؤمَّن له إحداث الخطر المؤمّن منه لأخذ مبلغ التّأمين (قد تحصل فيما لو كان المؤمَّن له في ضائقةٍ ماديةٍ ما وتسبب بنفسه بحصول الخطر لأخذ تعويضٍ لفكّ ضائقته)[274]. ومهما قيل في وصف هذه المشكلة فأساسها يعود إلى الراحة التي يشعر بها المؤمَّن له من أنّ هنالك شخصاً آخرَ سيتحمّل عنه المسؤولية عند حصول الخطر الإلكتروني، لذلك يركن إلى الإهمال وعدم المبالاة حيال حصول المخاطر.

وتتجلّى هذه المشكلة كما ذكرنا سابقاً في صورٍ كالإهمال، أو إخفاء المعلومات، أو إيراد معلوماتٍ خاطئةٍ. أمّا عن الحلول التي قد تقدّم في هذا الإطار فأغلب شركات التّأمين تحاول تطبيق جزاءاتٍ معيّنةٍ كالتوقّف عن دفع مبالغ التّأمين، أو تخفيضها عند حصول الخطر المؤمّن ضدّه، وذلك بوضع نصوصٍ صريحةٍ في وثائق التّأمين تعفي نفسها من دفع التعويضات عند وقوع خطرٍ نتيجة وجود احتيالٍ من جانب المؤمَّن له بالكذب في البيانات المقدّمة من جانبه، أو وجود إهمالٍ في حماية نفسه من مخاطر الإنترنت، أو مماطلةٍ في الإبلاغ عن حصول الخطر، ويُضرب مثلاً لذلك شركة austbrokers professional services التي تقدّم في أحد نماذج التّأمين ضدّ مخاطر الإنترنت حقّها في رفض التّغطية أو تخفيضها في حال لم يلتزم بما

---

[273] Miaoui, Y., Boudriga, N. (2019). Enterprise security economics: A self-defense versus cyber-insurance dilemma, Applied Stochastic Models Business and Industry, p 13.

[274] Kesan J. p. & Others, (2005). P 11.

تمليه شركة التّأمين على المؤمَّن له من وجوب الإعلام الصّحيح عن المعلومات، أو ممارسة أحد أعمال الاحتيال على شركة التّأمين[275]. كما وقد تحاول شركة التّأمين بحماية نفسها منذ البداية عند إبرام العقد عبر رفع الأقساط بشكلٍ قد يتساوى مع المخاطر المؤمّن ضدّها، وبالنتيجة تضع في الحسبان إمكانيّة تخاذل المؤمَّن له في واجباته بالإعلام أو تأخّره في المطالبة، وكثيراً ما يعاني سوق التّأمين ضدّ مخاطر الإنترنت من ارتفاع الأقساط الكبير الذي يقابله عدم وجود مبالغ تغطيةٍ كافيةٍ للمخاطر[276].

2-أمّا عن مشكلة الاختيار الخاطئ، فلهذه المشكلة ارتباطٌ مع الخطأ المتعمّد، وتقوم على فكرة إخفاء المؤمَّن له المعلومات المتعلّقة بمخاطر الإنترنت المحيطة به عن شركة التّأمين من أجل محاولة الحصول على أقساطٍ منخفضةٍ[277]. وتُعزى إمكانيّة حصول هذه المشكلة إلى وجود طرفينِ غير متوافقينِ، فكما يُقال في العقود المثاليّة يكون الطّرفان على قدم المساواة من حيث علمهم بالمنتج المتعاقد عليه، أمّا في التّأمين ضدّ مخاطر الإنترنت فلا تكون شركة التّأمين عالمةً مسبقاً بالمخاطر المحيطة بطالب التّأمين بصورةٍ كاملةٍ وحقيقيةٍ، بل تعتمد في تقديم تغطيتها التّأمينيّة على ما يقدّمه لها طالب التّأمين من معلوماتٍ عن الخطر المؤمّن منه، والأشياء محلّ التّأمين، وعندها تحاول الشّركة توفير التّغطية بما يتناسب مع المعلومات، وهنا تبرز مشكلة الاختيار الخاطئ بحال وجود عدم دقّة في المعلومات من جانب طالب التّأمين، وبالتّالي عدم علم شركة التّأمين بمدى الخطورة المحيطة بطالب التّأمين فيما لو كان منخفض المخاطر أم مرتفع المخاطر، ولذلك تتبنّى شركات التّأمين بعض الحلول للتغلّب على هذه المشكلة عبر تقديم نوعين من عقود التّأمين، الأوّل منه يقدّم تغطيةً لشركاتٍ تتعرّض لمخاطرَ منخفضةٍ وهو منخفض الأقساط، أمّا الثّاني فهو للشّركات عالية المخاطر وعندها ترتفع الأقساط بالمقابل مع رفع مبالغ التّأمين (التعويض)[278].

---

[275] ACP Cyber Insurance Proposal Form (SME), (n.d). p 3.

[276] Ibid, p 11.

[277] Miaoui, Y., Boudriga, N. (2019). P 13.

[278] Kesan J. p. & Others, (2005). P 8.

3-أمّا عن المشكلة الثّالثة وهي الارتباط المتبادل، في عالم الإنترنت المترابط الخطر الحاصل على أحد الأنظمة لا بدّ وأن يلقي بظلاله على الأنظمة الأخرى، ولو كانت تابعةً لإدارةٍ أخرى في مكانٍ مختلفٍ من العالم، وذلك بسبب الأمن الإلكترونيّ المترابط، بحيث فيما لو هُوجِم أحد الأنظمة عبر اختراقها بوساطة فايروس فيمكن استخدام هذا النظام كمنصّةٍ للهجوم على أنظمةٍ أخرى، وهذه المشكلة تؤثّر بشكلٍ كبيرٍ على احتماليّة زيادة مخاطر الإنترنت المتوقّعة؛ لأنّ المؤمَّن له ورغم قيامه بالإعلام عمّا يصل إلى علمه من مخاطرَ يمكن أن تصيبه فلا يمكن أن يتوقّع إمكانيّة إصابته بعطلٍ ما نتيجة كونه من أحد القطاعات المتأثّرة بهجومٍ إلكترونيٍّ معيّنٍ.

ومهما قِيل في شأن هذه المشكلات، ففي الأحوال كلّها ستنعكس على قيمة الأقساط انخفاضاً وارتفاعاً بحسب الجهد الذي يبذله المؤمَّن له في حماية أمواله، وأعماله من مخاطر الإنترنت، وبمقدار الصدق الذي يبديه عند الإعلام عن نوع المخاطر المُراد تأمينها، والإبلاغ عند حصول الخطر المؤمّن منه بحسب الطّرق المحدّدة، وبالمواعيد المعيّنة، ولا تنتهي التزامات المؤمَّن له عند هذا الحدّ، بل تتعدّاها إلى وجوب بذل عنايةٍ معتادةٍ تحدّدها شركة التّأمين في وثيقة التّأمين.

الفرع الثّاني

التزام المؤمَّن له بواجب العناية والتقيّد بتعليمات شركة التّأمين

تقع على عاتق المؤمَّن له التزاماتٌ تُضاف إلى واجبه بالإعلام والمطالبة، وتنطوي هذه الالتزامات على واجب بذل العناية والحرص الكافيين لمحاولة منع حصول الخطر المؤمّن ضدّه، والالتزام بما تصدره إليه شركة التّأمين من تعليماتٍ لمحاولة البقاء بمنأىً عن مخاطر الإنترنت من أجل الحصول على مبلغ التّأمين عند حصول الخطر.

أولاً: التزام المؤمَّن له ببذل العناية الكافية:

لا يعدو عقد التّأمين ضدّ مخاطر الإنترنت عن كونه عقداً ملزماً لجانبينِ، فكما تلتزم شركة التّأمين بدفع التعويض، يلتزم المؤمَّن له على المقلب الآخر ببذل جهدٍ كافٍ لحماية نفسه من مخاطر الإنترنت؛ لأنّ إبرام التّأمين لا يعفي المؤمَّن له من هذا الواجب وليس له أن يلقي عبأه أبداً على عاتق شركة التّأمين، رغم أنّ التّأمين قد يلزم الشركة بتدريب الموظّفين أو تقديم بعض نسخ برامج الحماية المطلوبة، لكن واجب العناية مطلوبٌ من المؤمَّن له؛ لأنّ الأشياء المؤمَّن عليها تقع تحت سيطرته وهو الأكثر قدرةً على تحديد كفاية الإجراءات المتّخذة للحماية. ولبيان ذلك يُضرب المثال الآتي: كما لو كان الشيء المؤمَّن عليه في عقد التّأمين ضد الحريق منزلاً، يلتزم المؤمَّن له بموجب العقد المبرم بتأمين حمايةٍ كافيةٍ لهذا المنزل عبر القيام بالإصلاحات اللازمة له لمنع حصول الحريق، كما لو شكّ بوجود تسريبٍ بالغاز فيتوجّب عليه أن يُصلح ذلك على الفور لمنع حصول حريقٍ، وكذلك ينطبق الأمر على عقد التّأمين ضد مخاطر الإنترنت، إذ ليس من المنطقي ترك الأمور تسير دون أي تدخل من جانب المؤمَّن له لوقف احتماليّة حصول الخطر، وعليه ينبغي على المؤمَّن له اتخاذ إجراءات تقنيّة وأمنيّة لمنع حصول الخطر المؤمَّن ضده، أو على أقل تقديرٍ تقليل قيمة الخسائر والأضرار الحاصلة بحال وقوعه. وينطوي واجب العناية على إجراءاتٍ عدّة منها تثبيت جدران نارية، والعمل على التحديث الدائم للأنظمة، واتباع مراحل معينة من الأمن الإلكترونيّ، وهذا ما سنوضّحه على النحو الآتي:

1-تثبيت الجدران النارية: باتت الجدران النارية في عالم الإنترنت شيئاً ضرورياً لا يمكن الاستغناء عنه، فالحكومات حول العالم، وخبراء المعلوماتية، ومقدمو خدمات الإنترنت، وبائعو ومصنعو الحواسيب ينصحون كل مستخدمٍ للإنترنت باستخدام جدارٍ ناريٍّ. ومن التعريفات التي قُدمت للجدران النارية على أنها: "عنصرٌ أو مجموعة عناصرٍ تقيّد الوصول بين شبكة محمية والإنترنت أو بين مجموعةٍ أخرى من الشبكات[279]"، كما يعرّفها بعض الفقه على أنّها: "مجموعةٌ من المكوّنات الموضوعة بين شبكتين لها خصائص تتجسّد بأنَّ كل البيانات الداخلة والخارجة من وإلى الشبكات ينبغي أن تمر عبر هذا الجدار، وأنَّ البيانات التي ستمر فقط هي

[279] Zwicky, E. D., Cooper, S., & Chapman, D. B. (2009). Building Internet Firewalls, California: USA, O'REILLY MEDIA, P 102.

المسموح بمرورها حسب تعريف سياسة الأمن المحلي، وأنَّ الجدار الناري بحدِّ نفسه محصّن ضد الاختراق[280]". ويجب تثبيت الجدار وتهيئته (تكوين الجدار في نظام معين) على نحوٍ صحيحٍ ليُستفاد من الحماية بالحد الأقصى، وعلاوةً على ذلك يجب الحفاظ على التحديث المستمر لهذا الجدار ليكون قادراً على مواكبة تطورات المخاطر الإلكترونيّة المحيطة جميعها.

وعليه تطلب شركة التّأمين من المؤمَّن له أن يقوم بتثبيت جدران نارية على أنظمته وأجهزته التي يستخدمها لدخول الإنترنت لحمايتها من محاولات الاختراق. وفي أحد الأمثلة على ذلك، تطلب شركة رأس الخيمة للتأمين من طالبي تأمين مخاطر الإنترنت جميعهم أن يقوموا بتنصيب الجدران النارية، والإبقاء على فعاليتها، وتحديثها كشرطٍ مسبقٍ لترتيب مسؤولية شركة التّأمين عند تحقق الخطر المؤمن منه، ويبرر ذلك بأنّ مخاطر الأعمال التجارية أكثر شدةً واحتماليةً من المستخدم العادي، وهو ما يستلزم درجة أمانٍ أكبر وجدراناً ناريّةً ذات فعاليّة أكثر، وقوة أكبر.

2-**القيام بالنسخ الاحتياطي للبيانات:** لما كانت البيانات والمعلومات (كالمعلومات المالية، المعلومات الشخصية للعملاء، الأسرار التجارية...) التي يستخدمها المؤمَّن له في أعماله يتم حفظها، وتخزينها، وتداولها عبر الإنترنت، لذلك فإنّ احتمال خسارتها عند حصول أيّ خرقٍ إلكترونيٍّ، كبيرٌ جداً، كما لو شُفّرت البيانات، وتدمّرت، أو تعدّلت لعدم دفع الفدية، أو سُرقت حواسيب الشركة وتدمرت أسرارها. وعليه إذا لم تضع الشركة خطةً للنسخ الاحتياطي لحفظ بياناتها في مكانٍ آمنٍ، فإنّ ذلك قد يعني خسارة هذه المعلومات للأبد، وتكبيد المؤمَّن له مبالغَ باهظةً من أجل تكوين قواعد بياناتٍ جديدةٍ، ناهيك عن تعويض المتضرّرين من هذا الفعل. ويُراد بالنّسخ الاحتياطيّ للبيانات إنشاء نسخ من البيانات يمكن استخدامها لاسترجاع الأصل عند حدوث خطرٍ إلكترونيٍّ يؤدي إلى فقدانها، أمّا عن النسخ الاحتياطية فهي نسخٌ عن الأصل تُحفَظ في مكانٍ آمنٍ بعيدٍ عن الأصل، ويمكن القيام بذلك عبر الاستعانة بوسائطَ خارجيّةٍ كقرصٍ صلبٍ خارجيٍّ، أو مقدمي خدمات التخزين السحابي، أو

[280] Cheswick, W. R., Bellovin, S. M., Rubin, A. D. (2003) Firewalls and Internet Security Repelling the Wily Hacker, Boston: USA, Addison- Wesley, p 12.

مقدمي خدمات النسخ الاحتياطي المتخصصين بهذه الأعمال (وهو الشائع لا سيّما في الشركات الكبرى التي تحتاج إلى مساحاتٍ كبيرةٍ من التخزين)، ومن أشهر هذه الشركات Carbonite و Jungle Disk ويمكن جدولة عمليات النسخ الاحتياطي بشكلٍ دوريٍ لمدةٍ معينةٍ، بحيث يتم النسخ بصورة تلقائية دون تدخل بشريٍّ من أجل محاولة التغلب على احتمالية نسيان الموظّف المسؤول عن النسخ القيام بمهمته، وكلّما زادت عمليّات النّسخ الاحتياطي زاد الأمان الإلكترونيّ، فمثلاً المعلومات الماليّة وقواعد البيانات وجهات الاتصال؛ ونظراً لأهميتها والتغير الطارئ عليها يومياً وكلّ ساعةٍ يُنصح بوجوب نسخها احتياطياً يومياً، أمّا العقود مثلاً فمعدّل تغيّرها شهريٌّ لذلك تنسخ احتياطياً كل شهر[281].

وفي الواقع العملي كثيراً ما تطلب شركات التّأمين من المؤمَّن لهم أن يقوموا بأعمال النسخ الاحتياطي الدوري للمعلومات التي يحفظونها في أنظمتهم، من أجل تقليل المخاطر التي تنتج عن عمليات الاختراق الإلكتروني، والحفاظ على نسخةٍ آمنةٍ من البيانات للعودة إليها عند الحاجة، وعلى سبيل المثال تطلب شركة التّأمين رأس الخيمة من المؤمَّن لهم القيام بالنسخ الاحتياطي للبيانات المهمة كل سبعة أيام على الأقل (يمكن القيام بالنسخ قبل هذه المدة)، وينبغي الاحتفاظ بالنسخ الاحتياطية في مكانٍ آمنٍ خارج الشّبكة (من أجل محاولة حمايتها من محاولات القرصنة مثلاً لدى مزوّد خدمات النسخ الاحتياطي)، وتعتبر شركة التّأمين هذا الواجب شرطاً مسبقاً لترتيب مسؤولية شركة التّأمين عند حصول الخطر المؤمن ضده[282]، و في مثالٍ آخر من شركة التّأمين Pohjola Insurance الفنلندية التي تقدّم خدمات التّأمين ضدّ مخاطر الإنترنت، فقد ألزمت المؤمَّن لهم بواجب القيام بالنسخ الاحتياطي الدوري عبر وضع جزاء عدم دفع مبلغ التّأمين في حال الإهمال، فهو لا يغطي الخسائر الناشئة عن إهمال هذا الواجب، ويوجب على المؤمَّن له التأكد من القيام بالنسخ الاحتياطي بشكل يومي

---

[281] https://www.baylor.edu/content/services/document.php/192120.pdf

تاريخ الزيارة: 14\10\2020، الساعة 10:30 p.m.

[282] Simply Cyber Policy Terms & Conditions, (2018). P 22.

للملفات جميعها التي تحدثت، مع واجب وضعها بشكلٍ منفصلٍ عن النسخ الأصليّة لضمان عدم حصول أيّ ضررٍ متزامنٍ بحال حصول ضررٍ للنّسخ الأصليّة[283].

3-تنصيب برامج مكافحة الفيروسات: باتت الفيروسات الورقة الرابحة التي يستخدمها القراصنة من أجل الدخول إلى الأنظمة والأجهزة دونما أي ملاحظة، وباتت مكافحة الفيروسات وغيرها من البرامج الخبيثة مدار اهتمام الشركات في أنحاء العالم كافّة؛ نظراً لما تخلّفه من خسائرَ كبيرةٍ وتهديدٍ حقيقيٍ للخصوصيّة، ولذلك كثيراً ما تسعى الشّركات إلى اقتناء برامج مكافحة الفيروسات والبرامج الضّارّة في محاولةٍ منها لحماية نفسها ضد احتمالية تعرّضها لأيّ خرقٍ. ويُراد ببرامج مكافحة الفيروسات البرامج التي تهدف إلى إنهاء وجود الفيروسات في النظام، والعمل على منع نسخ أو استلام ملفاتٍ مصابةٍ بالفيروسات في الوقت ذاته، ويشترط في هذه البرامج أن يكون مصادقاً عليها من جهةٍ ذات اختصاص في هذا المجال، وأن تكون من إنتاج شركاتٍ معروفةٍ في مجال مكافحة الفيروسات، كما ينبغي أن يتضمن هذا البرنامج القدرة على التعامل مع أنواع الفيروسات كافة، ويجب أن تكون الخدمة مقدمةً على مدار الساعة، وأن تكون البرامج قادرةً على محو الفيروسات دون التأثير على الملف المصاب، وختاماً لا بدّ أن تكون قابلةً للتحديث عبر الاتصال بالإنترنت[284].

وعليه ونظراً لأهمية هذه البرامج في تعزيز الأمن السيبراني وتقليل احتمالية حصول مخاطر الإنترنت، فإنّ شركات التّأمين تعتبر وجود هذه البرامج منصبةً ومحدثةً دائماً (يشترط التحديث الدائم فلا يقبل بمجرد وجود برنامج مكافحة فيروسات بإصدار قديم) شرطاً أساسيّاً لترتيب مسؤوليتها بدفع مبلغ التّأمين عند حصول الخطر المؤمَّن ضده، ولذلك فلن تقوم الشركة بدفع التعويض في حال وجد برنامج غير محدّث أو غير فعّال كما لو كانت النسخ المنصبة غير أصليةٍ[285].

---

[283] Cyberinsurance general terms and condition, (2019). pohjola insurance LTD, p 2.

[284] إسماعيل، محمد صادق. (2010). الحكومة الإلكترونية وتطبيقاتها في الدول العربية، ط:1، القاهرة: مصر، دار العربي للنشر والتوزيع، ص 124- 125.

[285] Cyberinsurance general terms and condition, (2019). P 2.

ولا شيء يمنع شركات التّأمين من الاتفاق على تقنياتٍ أخرى للحماية ضد مخاطر الإنترنت، مثل استخدام التشفير، وكلمات المرور القوية، وتقنيات حماية البريد الإلكتروني (عبر تحليل وتصفية الرسائل الواردة مثل رسائل التصيد وبريد الإغراق)، كما يمكن القيام باختبار الاختراق عبر القيام بمحاكاةٍ عمليّةٍ مشابهةٍ لعمليات الاختراق الواقعية لدراسة مدى قدرة التقنيات الموجودة لدى المؤمَّن له على التصدي في هذه الحالات، والكشف عن الثغرات، ونقاط الضعف، ومعالجتها[286].

وبصورةٍ عامةٍ يساعد القانون شركات التّأمين على الوصول إلى النتائج المثلى من تطبيق تقنيات الحماية، عبر وضع جزاءاتٍ قانونيّةٍ على الإهمال الحاصل من جانب المؤمَّن لهم في حماية أمن أعمالها السيبراني، ففي عام 2013 فرض مكتب مفوضي المعلومات في المملكة المتحدة غرامةً مقدارها 250 ألف جنيه إسترليني على شركة سوني (SONY) نتيجة خرقها الفاضح لتشريع حماية البيانات العامة بعد اختراق منصة Sony PlayStation في عام 2011، والتي كشفت بيانات ملايين المستخدمين بما تشمله من أسماء وعناوين، وعناوين بريدٍ إلكترونيٍّ، وكلمات سرٍ، وقد اعتبر المكتب هذا الاختراق انتهاكاً خطيراً مبرراً ذلك بضعف المعايير الأمنيّة الموضوعة من جانب الشركة لحماية بياناتها مقارنةً مع حجم وطبيعة هذه البيانات، فضلاً عن حجم الضرر الحاصل نتيجة هذا الإفشاء، وأشار المكتب إلى واجب معالج البيانات اتخاذ تدابيرَ وقائيّةٍ أكثر ملاءمةً لاحتماليّة وقوع خطرٍ إلكترونيٍّ على هذه المعلومات، كما لوحظ وجود نوعٍ مع المعايير المخففة كإجراءات الدفاع المطبقة عند حصول الهجوم، ومستوى تعقيد الهجوم، وإجراءات إخطار المستخدمين، والجهود المبذولة لاسترداد ما تم إفشاؤه، وتعاون الشركة مع المكتب، وإجراءات التصحيح المتخذة[287]. وفي السياق ذاته غرّمت هيئة الخدمات المالية في المملكة المتحدة شركة Nationwide Building Society بعدما تم سُرقِ أحد أجهزة حواسيبها المحمولة الخاص بأحد موظفيها، والذي يحتوي على بيانات عملائها السرية نتيجة فشلها في حماية خصوصية هذه البيانات بسبب عدم امتلاكها ضوابط، ومعاييرَ خاصةٍ لإدارة مخاطر أمن المعلومات[288]،

---

[286] الضوابط الأساسية للأمن السيبراني، (2018)، الهيئة الوطنية للأمن السيبراني، السعودية، ص20-23.

[287] Marano, P., Rokas, I., & Kochenburger, P. (2016). P 191.

[288] Ibid, p 192.

وفي الولايات المتحدة الأمريكية لا يختلف الأمر، فكثيراً من المؤسسات الحكومية تعمل على الاستفادة من قوانين الخصوصية الموجودة لحماية العملاء، إذ تم إصدار قانون Gramm–Leach–Bliley في عام 2000 لحماية البيانات المالية والشخصية للأفراد التي تحتفظ بها المؤسسات المالية، ويوجب هذا القانون على هذه المؤسسات إعطاء المستهلكين إشعارات خصوصية تشرح لهم الطريقة التي تشارك فيها هذه المعلومات لضمان عدم الوصول غير المصرّح به إلى سجلات العملاء، وعليه استفادت لجنة التجارة الفيدرالية من هذا القانون لاتخاذ إجراءاتٍ صارمةٍ ضد المؤسسات التي تخلق مخاطر غير ضرورية (أي يمكن تفاديها)، عبر السماح للموظفين أياً كانت رتبتهم بالوصول إلى السجلات، أو نتيجة الفشل في تشفير البيانات، أو حماية الوصول اللاسلكي (كما ذكر عبر الجدران النارية أو تقييد الوصول..)[289].

ممَّا سبق يُلاحظ مدى أهميّة وجوب الأخذ بهذه التقنيات وغيرها ممّا توصلت إليه التكنولوجيا من أجل وضع حدٍ للمخاطر الإلكترونيّة، أو على أقل تقدير تقليل نسبة التعرض لها، أو تقليل حجم الأضرار الحاصلة؛ لأنّ الكثير من مخاطر الإنترنت تحقّقت بسبب الإهمال الحاصل في حماية البيانات المخزنة، وكثيرٌ من الشركات وصلت إلى حدود الإفلاس؛ لأنها لم تبذل عنايةً كافيّةً في طريقة تواصلها مع الإنترنت، فعرّضت أنظمتها للخطر. وبعيداً عن التّأمين ضد مخاطر الإنترنت فلا بدّ من تشجيع الأخذ بهذه التقنيات من أجل الوصول إلى مرحلة الأمن السيبراني، وتحسين بيئة عمل الفضاء السيبراني، والذي بدوره ينعكس على المؤمَّن لهم وشركات التّأمين على حدٍ سواء، ويقلل نسبة المخاطر الإلكترونية والأقساط العالية، على الرغم من أنّ الكثير من الشركات تعتكف عن شراء برامج الحماية لغلاء أثمانها، أو لاعتقادهم بعدم احتماليّة الإصابة بمخاطر الإنترنت، ولكنَّها تبقى أفضل من حالة تعرض الشركة لخطرٍ إلكترونيٍ، والذي قد يطيح بسمعتها التجارية ويخرجها من المنافسة.

[289] Shackelford,S. (n.d). p 351.

ثانياً: التزام المؤمَّن له بالتقيد بتعليمات شركة التّأمين:

يلتزم المؤمَّن له باتباع ما تصدره إليه شركة التّأمين من تعليماتٍ وواجباتٍ من أجل الحفاظ على مستوى معيّنٍ من الأمن الإلكتروني في سبيل تحصين نفسه ضد حصول الخطر الإلكتروني المؤمَّن ضده، فإذا ما طلبت منه شركة التّأمين أن يحصل على نظام حمايةٍ من شركةٍ معينةٍ فيتوجب عليه الامتثال لذلك، وكذلك إذا ما طلبت منه تنصيب إصدارٍ معينٍ من برنامج تشغيل فينبغي القيام بذلك؛ لأنّ مخالفته قد تهدد بالامتناع عن دفع التعويض. ويعزى ذلك إلى أنَّ شركة التّأمين عندما تطلب من المؤمَّن له القيام بأمرٍ ما فهو ليس بطلبٍ عشوائيٍّ أو لمجرد الرغبة في تكليف المؤمَّن له فوق طاقته، بل إنّ ذلك نابع من حساباتٍ معينةٍ وفقاً لنوع المخاطر المحيطة واحتماليتها، وفق عملية قياس وتقييم المخاطر، ولذلك فلكل طالب تأمينٍ نوع معين من التعليمات الصادرة والتي تختلف عن غيره. فلو كانت شركة التّأمين أمام فردٍ عاديٍّ يتصفح الإنترنت، أو يمارس أعمالاً بسيطةً عبر الإنترنت فقد تطلب منه تنزيل برنامج حماية متوسط فحسب لمجرد حماية المتصفح المستخدم من الاختراق، بينما لو كانت الشركة أمام طالب تأمين كشركة تمارس التجارة عبر الإنترنت _والتي بطبيعة عملها تحفظ كلمات مرور عملائها مثلاً_ أو أمام مصرف يتلقى التحويلات الإلكترونية، أو مختبر صحي يحفظ بيانات عملائه لدى مزود تخزين سحابي، ففي هذه الأمثلة وغيرها من مشابهتها يكون خطر الاختراق أكبر ويكبر معه خطر تشويه السمعة، وكشف سرية بيانات العملاء، ولذلك تكون الأضرار في حال حصول الخطر أكبر. وعليه لا تكتفي شركات التّأمين فقط بأن تلزم عملاءها طالبي التّأمين بأن ينصبوا على أنظمتهم برنامج حماية، بل لا بد من التقيد بإجراءاتٍ أكثر صرامةً، ككلمات المرور القوية، وحماية مواقعها الإلكترونية بجدران نارية، وغيرها ممّا ذُكِر في هذا الفرع. ويلتزم المؤمَّن لهم في عقد التّأمين ضد مخاطر الإنترنت بالقيام بما تمليه عليهم شركة التّأمين انطلاقاً من كونه عقداً ملزماً لجانبين، وفي بعض الوثائق التّأمينية قد تمدّ شركة التّأمين يد العون للمؤمَّن لهم من أجل أداء هذه الواجبات، إذ قد تتضمن بعض الوثائق تغطية تكاليف تنصيب جدران نارية مثلاً، أو تكاليف التحديث المستمر، وفي المقابل يلتزم المؤمَّن لهم باتباع أوامر شركة التّأمين، إذ قد تمنعهم من الدخول إلى موقعٍ معيّنٍ، أو قد تحظر عليهم التعامل مع شركةٍ ما، أو تطلب منهم التعاون مع شركة أمنٍ معلوماتيٍّ

معينةٍ أيضاً، ولا يجوز لهم بأي حال مخالفة هذه التعليمات؛ لأنّها وفي أغلب الأحيان تكون قائمةً على معاييرَ محدّدةٍ من جانب شركة التّأمين.

وواجب العناية المطلوبة من المؤمَّن له هو عناية الرجل المعتاد، فكما كان يعتني ببياناته المخزنة وأنظمة عمله قبل أن يحصل على وثيقة التّأمين (إذا ما كانت برأي شركة التّأمين عنايةً كافيةً) فلا بدّ له أن يستمرّ في بذل هذه العناية، ولا يُقبل منه أن يستكين عن ذلك، أو يهمل حماية الأنظمة والبيانات بحجة وجود التّأمين، وقد سبق الحديث في إطار الاستثناءات من التّأمين من أنّ شركة التّأمين غالباً ما تعفي نفسها من الدفع في حال حصول الخطر المؤمن ضده نتيجة إهمال المؤمَّن له بذل ما يكفي من العناية المطلوبة؛ لأنه يخرق بنداً أساسياً من بنود التعاقد، وعليه لا بد من مجازاته على فعله، ويوضع هذا الإعفاء بصورة شرطٍ نموذجيٍّ من أنّ شركة التّأمين لن تقوم بتغطية المؤمَّن له في حال حصول الخطر نتيجة الفشل في التأكد من أنّ نظام الكمبيوتر كان محمياً بشكلٍ معقولٍ عبر الممارسات الأمنية التقنية وإجراءات الصيانة الدائمة للأنظمة التي تعادل أو تزيد عمّا ذُكِر من جانب المؤمَّن له عند الإجابة عن طلب التّأمين، والفشل في التنفيذ المستمر للإجراءات وضوابط المخاطر المحددة من جانب المؤمَّن له[290].

ويمكن القول إنّ التزامَي العناية والتقيد بتعليمات شركة التّأمين مرتبطان ببعضهما البعض؛ لأنّهما التزامان مستمران خلال فترة سريان الوثيقة، ولأنّ الإخلال بأيٍّ منهما قد يؤدّي إلى حصول الخطر المؤمّن ضدّه، وعليه لا يكفي مجرّد تنصيب برنامج حماية إذا ما كان المؤمَّن له يدخل إلى مواقعَ ممنوع عليه الدخول إليها، أو يقوم بترك بياناته عرضةً لدخول من لا عمل له بها، لأنّ ذلك يخرق واجب العناية المفترض.

ولدرء شبهة تدخل المؤمَّن له في حصول الخطر تلجأ شركة التّأمين إلى الطلب من المؤمَّن له أن يقدم دلائلَ تثبت أنّ الخطر المتحقّق لم يكن بأيّ حالٍ من الأحوال من صنعه عبر التأكيد على التزامه ببذل العناية

[290] https://www.gbainsurance.com/avoiding-cyber-claim-denials

تاريخ الزيارة: 2020\10\20، الساعة 10:30..p.m

وقيامه بكل ما تمليه عليه شركة التّأمين[291]، وعلى سبيل المثال على إهمال العناية الواجبة ما حصل مع شركة Cottage Health في عام 2014، إذ رُفعَت دعاوى جماعيّة عليها كلّفتها ما يقارب الثّلاثة ملايين دولار للتّسوية نتيجة نشرها وعن غير قصدٍ لمعلوماتٍ سريّةٍ خاصّةٍ بالعملاء، وبلغ عدد من أُفشيت معلوماتهم عشرات الآلاف، وقد حصل هذا الخرق على مراحل عدّة، فقد نشأ الخرق الأوّل نتيجة إزالة تقنيات الحماية الإلكترونيّة للبيانات من جانب أحد المتعاقدين مع الشّركة ما جعل أسماء المرضى، وعناوينهم، وتاريخهم الصحي، ومعلومات العلاج، وغيرها متاحةً لأي شخصٍ يصل إلى خادم الشّركة لتنزّل بكلّ سهولةٍ دون حاجةٍ لكلمة مرور مثلاً، أمّا عن الخرق الثّاني فقد حصل نتيجة خطأ موظّف وعندها تمّ الوصول إلى معلوماتٍ إلكترونيّةٍ لحوالي 11 ألف مريض، وعليه ادّعى قسم الخدمات الصحيّة والإنسانيّة الأمريكي أنّ الشركة قد فشلت في إجراء تحليلٍ دقيقٍ وشاملٍ للمخاطر المحيطة بالمعلومات الصّحيّة الشّخصيّة للأفراد التي تحتفظ بها الشّركة، كما فشلت باتّخاذ تدابيرَ أمنيّةٍ معقولةٍ لتحقيق الحماية الكافية لهذه المعلومات، والفشل في حصول الشركة على تأكيداتٍ خطيّةٍ من المقاول الذي تعاقدت معه بأنّه سيقوم بحذف بياناتها الإلكترونية المخزنة لديه، وعليه تُعتبر الشركة قد خرقت قانون التّأمين الصحي النافذ منذ عام 1996 في الولايات المتحدة الأمريكية (HIPPA)، وبرغم الخطأ البشري الحاصل بنشر المعلومات، إلا أنّ خرق الخصوصية يُعزى أيضاً إلى عدم وجود تقنيات حماية كافية، وعليه غُرّمت بدفع مبلغ 3 ملايين دولار بالإضافة إلى وضع خطةٍ من أجل تصحيح الوضع الحاصل[292]. ولذلك فإنَّه على الرغم من عدم وجود تأمينٍ للمخاطر الإلكترونيّة لدى هذه الشّركة عند حصول الخطر هذا، لكن ذلك يشير إلى أهميّة اتخاذ الإجراءات الأمنيّة اللازمة لمنع تحقّق المخاطر الإلكترونيّة بحال وجود تأمينٍ ضدّ مخاطر الإنترنت أو انتفائه، فضلاً عن أنّ المثال المذكور يظهر حجم الضرر الحاصل للمؤمَّن له بحال امتناع شركة التّأمين عن دفع التعويض نتيجة عدم بذل العناية الكافية من جانب الأول.

---

[291] Miaoui, Y., Boudriga, N. (2019). P 14.

[292] https://www.hhs.gov/sites/default/files/cottage-health-ra-cap.pdf

تاريخ الزيارة: 2020\10\21، الساعة 11:30 p.m.

وفي مثال آخر ما حصل مع شركة aqua star الأمريكيّة للمأكولات البحريّة، إذ قام موظّف من الشّركة بتحويل مئات آلاف الدولارات تقدّر بحوالي 700 ألف دولار إلى حساباتٍ مصرفيّةٍ خارج البلاد لاعتقاده الخاطئ أنّها تعود لأحد المزوّدين الذين يتعاملون معهم، وذلك نتيجة التّلاعب في رسائل البريد الإلكترونيّ لتظهر كأنّها من مرسلٍ مشروعٍ، وفي تفصيل الأمر أنّ مخترقاً استطاع الدخول إلى أنظمة عمل الشركة المتعاقد معها من جانب (اكوا ستار)، وعندها بدأ يراقب التعاملات والرسائل بين الشركتين، ومن ثم بدأ يرسل الرسائل الإلكترونية الاحتيالية المشابهة لرسائل الشركة الثانية، وعندها طلب من موظف (اكوا ستار) أن يغيّر معلومات الحساب المصرفي التابع للشركة المزوّدة، وطلب دفع مبلغ 713 ألف دولار، وهنا كانت الطامّة الكبرى عندما تمّ الاحتيال على الشركة وسرقة هذا المبلغ الكبير، ولحسن الحظ باعتقاد الشركة الضحيّة أنّها في ذلك الوقت كانت تملك وثيقة تأمين ضدّ مخاطر احتيال الكمبيوتر من شركة TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA والتي ظنَّت أنَّها ستغطّي عمليّة الاحتيال هذه، وعندها كانت الضربة الكبرى للضّحيّة بأنّ وثيقة تأمينها لا تغطّي المخاطر!

وحسب الشركة تُقدَّم التغطية للخسائر المباشرة للأموال والأسهم والممتلكات الناجمة عن احتيال الكمبيوتر، لكن الضّرر الحاصل هنا غير مغطّى؛ لأنّه لم يحصل نتيجة احتيال الكمبيوتر مباشرةً، وعندها أقامت (اكوا ستار) دعوى قضائيّة ضدّ شركة تأمينها، وانتهت حينها المحكمة إلى أنّ الفعل المرتكب يدخل تحت بند الاستثناءات، إذْ يمنع تغطية الخسائر المباشرة وغير المباشرة الناجمة عن إدخال البيانات الإلكترونية إذا كانت مرتبطةً بوصولٍ مصرّحٍ به إلى النّظام، وهنا حاول وكلاء (اكوا ستار) إثارة دفع أنّ التغطية تشمل أي خسارةٍ مباشرةٍ ناشئةٍ عن استخدام الكمبيوتر من أجل الاحتيال، لكن وكلاء شركة التّأمين دفعوا بأنّ هذه التغطية لا تنطبق لأنّ الموظّف المختصّ قد أدخل المعلومات الوهميّة إلى نظام شركته بنفسه، ولم يكن هناك أي وصولٍ غير مصرّح به إلى الشبكة (أي لا يوجد اختراق أو قرصنة أدت إلى تعديل البيانات)، وكان حكم الدّرجة الأولى موافقاً لادّعاءات شركة التّأمين، وعندها استأنفت (اكوا ستار) الحكم، وبالرّغم من ذلك حكمت محكمة الاستئناف

لمصلحة شركة التّأمين وقضت بأنّ التّغطية لا تنطبق على هذه الحالة[293]. وهذه القضية وسابقتها وغيرها يعطي خير مثالٍ لما ينبغي على الشركات القيام به من بذل عنايةٍ كافيةٍ، ووافيةٍ، ومناسبةٍ لما يحيط بها من مخاطر لكيلا تصل بها الأمور إلى خسارة الأموال والتّأمين على حدٍّ سواء، فبالرغم من أنّ شركة (اكوا ستار) قد أُحتِيل عليها عن طريق تغيير رقم الحساب المصرفي، لكن ربما كان يمكن تفادي حصول هذه الخسارة فيما لو عمل الموظف المسؤول على التواصل مع الشّركة للتحقّق من صحّة ما تم أُرسِل، وهنا يبرز عيب عدم بذل ما يكفي من عناية.

وضمن التزام التقيد بتعليمات شركة التّأمين، فإنّ الكثير من الشّركات المؤمّنة تطلب من عملائها المؤمَّن لهم أن يبلغوا شركة التّأمين قبل القيام بأيّ فعلٍ، كالدخول في تسوياتٍ أو صلحٍ أو تحمّل أيّ مسؤوليّةٍ من جانب المؤمَّن له دون الحصول على موافقةٍ خطيّةٍ مسبقةٍ من جانب شركة التّأمين، ولا يجوز إلغاء هذه الموافقة أو التّأخير فيها، ويُضاف إلى هذا الالتزام واجب تعاون المؤمَّن له ووكلاؤه مع شركة التّأمين في أعمال التحقيق عند حصول الخطر الإلكتروني. علماً أنّ جزاء مخالفة هذه الالتزامات هو عدم الدفع؛ لأنّ التقيّد بهذه الواجبات شرطٌ مسبقٌ لدفع التّعويض من جانب شركة التّأمين[294]، وذلك لأنَّ هذه التّسوية تسلب من شركة التّأمين فرصة الحصول على حكمٍ لمصلحة عميلها المؤمَّن له إذا ما قام الأخير بهذه التسوية بنفسه دون الرجوع إلى رأي شركة تأمينه، والتي قد تكون عالمةً بتفاصيل الأمور بشكلٍ أعمق. وختاماً، لا ريب أنّ هذه الالتزامات أساسيةٌ في كلِّ وثيقة تأمينٍ ضدَّ مخاطر الإنترنت؛ لأنَّها أساس العمل الصحيح من أجل الوصول إلى إعادة الأمور إلى نصابها، ولأنَّ العقد في أساسه يقوم على الالتزام المتبادل وحسن النية، ولا يمكن لأيّ طرفٍ أن ينجح بمفرده دون مساعدة الطرف الآخر.

---

[293] يمكن قراءة القضية كاملة على الرابط الآتي:

https://www.scholar.google.com/scholar_case?case=4637833847825659548&q=Aqua+Star+(USA)+Corp.+v.+Travelers+Casualty+and+Surety+Co.+of+America&hl=en&as_sdt=2006&as_vis=1

تاريخ الزيارة: 2020\10\22، الساعة 11:50 p.m.

[294] Simply Cyber Policy Terms & Conditions, (2018). P 18.

الخاتمة

حاول الباحث بعد إتمام هذا البحث الإضاءة بصورةٍ مفصّلةٍ على عقد التّأمين ضد مخاطر الإنترنت من الناحيتين التشريعيّة والعمليّة، فقد عُرض في الفصل الأول مفهوم عقد التّأمين ضد مخاطر الإنترنت عبر تحديد تعريفٍ لهذا العقد وبيان خصائصه وأطرافه وأركانه القانونيّة والمشكلات التي يعاني منها، وعبر دراسة مفهوم مخاطر الإنترنت من خلال تسليط الضوء على ما يُراد بهذه المخاطر وطبيعتها القانونية وتحديد صور هذه المخاطر، وما تلحقه من خسائرَ بضحاياها، مع الرجوع في الزمن إلى بدايات عصر الهجمات الإلكترونيّة. في حين تحدّث الفصل الثاني عن الالتزامات التي ينشئها هذا العقد على عاتق أطرافه، من حيث تحديد أشكال التّغطية التأمينية التي تقدمها شركة التأمين وصور الاستثناءات من هذه التغطية، وكيفيّة تقديم هذه التّغطية من حيث تحديد مبالغ التأمين وعرض بعض الأحكام القضائيّة من أجل إغناء البحث، ومن ثم العرض لالتزام المؤمَّن له لناحية التزامه بدفع قسط التأمين والآثار الناجمة عن الإخلال بهذا الواجب، مع بيان العوامل الداخلة في تحديد الأقساط، بالإضافة إلى واجب اتخاذ إجراءاتٍ معينةٍ ليحمي المؤمَّن له نفسه من مخاطر الإنترنت وفقاً لما تمليه عليه شركة التأمين كتثبيت جدران نارية والقيام بالنسخ الاحتياطيّ، والتزامه المستمر بواجب عناية الرجل المعتاد، والتزامه بإعلام شركة التأمين بحال حصول أي تغيّرٍ طارئٍ على الخطر المؤمّن منه وواجبه بمطالبة شركة التأمين عند حصول الخطر من أجل سداد مبالغ التأمين.

وفيما يلي عرض لأهم النتائج التي تم التوصّل إليها مع المقترحات بغية الوصول إلى الشكل الأمثل لهذا العقد:

أولاً: النتائج:

1-يرتبط التّأمين ضد مخاطر الإنترنت بالفضاء السيبراني والمخاطر الإلكترونيّة، ويُشار إليه على أنّه الحماية المقدّمة من جانب شركات التّأمين للمؤمّن لهم ضدّ مخاطر الإنترنت التي يتعرّضون لها في معرض عملهم عبر الشبكة.

2–يتّصف عقد التّأمين ضدّ مخاطر الإنترنت بكونه عقداً رضائياً ملزماً لجانبين؛ احتماليّ ومستمرّ، وقد يبدو إلكترونيّاً أو تقليديّاً، ويعد عقد تأمين ضد الأضرار؛ لأنّه يُعقد من أجل حماية الأصول الإلكترونيّة التي يملكها المؤمَّن له ولتغطية مسؤوليته المدنيّة تجاه عملائه في حالات الخطر الإلكتروني.

3–تتمثّل أهمّ المشكلات المرتبطة بعقد التّأمين ضدّ مخاطر الإنترنت في عدم دقّة المعلومات حول مخاطر الإنترنت، وتخوّف الشركات من الانخراط في هذا المجال، وارتفاع قيمة الأقساط، وقلّة وجود معيدي التّأمين، ما ينعكس سلباً على مبالغ التّأمين والأقساط.

4– ينبغي أن يكون الخطر في عقد التّأمين ضدّ مخاطر الإنترنت ذا منشأٍ إلكترونيٍّ بحتٍ، وأن يؤدّي إلى نتائجَ إلكترونيّة حتى يعد خطراً إلكترونياً لتفريقه عن المخاطر التقليديّة التي قد تصيب الأنظمة، وتقع هذه المخاطر على المعلومات المخزّنة لدى المؤمَّن له والتي تعد مالاً معنويّاً.

5– تعود مخاطر الإنترنت في التاريخ قدماً إلى سبعينيّات القرن الماضي، وتثبت الوقائع أن لا قطاع مهما كان بمنأىً عن هذه المخاطر، بل إنّ الأشخاص بمفردهم مستهدفون.

6–تمثّل البرمجيّات الخبيثة نقطة الضّعف الأولى التي يستغلّها المخترقون للتلاعب بالأنظمة المستهدفة، في حين تمثّل هجمات إنكار الخدمة والإغراق بالبريد العشوائي السبب الأكثر إزعاجاً للشّركات.

7–يستفيد من عقد التّأمين ضدّ مخاطر الإنترنت المؤمَّن لهم، بالإضافة إلى الطّرف الثالث (الغير) الذي يتم تغطيته عبر تغطية مسؤولية المؤمَّن لهم عن المخاطر الإلكترونية، ويقدم عقد التّأمين ضد مخاطر الإنترنت تغطيةً تأمينيّةً سابقةً على وقوع الخطر للحدِّ من وقوعه أو للتّخفيف من آثاره حال الوقوع، وخير مثلٍ لهذه التّغطية يتجسّد في تدريب الموظّفين، وعمليّات تقييم المخاطر، وتقديم الاستشارات وخدمات الحماية، وإعادة إصدار بطاقات الائتمان المسروقة وغيرها من التغطيات التّأمينيّة السّابقة للخطر.

8–يقدم عقد التّأمين ضد مخاطر الإنترنت في تغطيته التّأمينية خدمات تأمين العلاقات العامّة علاوةً على التّعويض النقدي؛ من أجل تحسين سمعة الشركة الضحيّة، بالإضافة إلى خدمات التحقيق الجنائي لمعرفة

ملابسات الحادث الإلكتروني وإعلام المتضررين من الهجوم الإلكتروني، ودفع نفقات الفدية في عمليات الابتزاز الإلكتروني.

9-إنّ فسخ عقد التّأمين ضدّ مخاطر الإنترنت لا يؤثر على الأقساط المدفوعة مسبقاً ولا يتمّ ردّ شيءٍ؛ لأنّها تُؤخذ مقابل عبءِ تحمُّل شركة التّأمين احتمال حصول الخطر، ومقابلاً للخدمات المقدّمة من جانبها لا سيّما أنّ العقد مستمرٌّ.

10-يبدأ التزام المؤمَّن له بدفع الأقساط بناءً على اتفاق الأطراف، وغالباً ما يكون الدفع مقدّماً لمواجهة حالات حصول الخطر الإلكتروني عند بدء العقد قبل تكوين محفظة التّأمين، ويؤثّر على تحديد القسط عواملُ كثيرةٌ تتعلّق بالخطر الإلكترونيّ خاصةً كاحتماليته وحجمه، ومنها ما يتعلق بطبيعة عمل المؤمَّن له، ومنها ما يرتبط بمبلغ التّأمين، وقيمة الشّيء المؤمّن عليه، وهو ما ينعكس على ارتفاع قيمة الأقساط.

11-يلتزم المؤمَّن له إلى جانب دفع الأقساط ببذل قدرٍ كافٍ من العناية في إدارة أعماله عبر الإنترنت، وبالقيام بكلّ ما تمليه عليه شركة التّأمين من واجباتٍ من شأنها أن تبقي المؤمَّن له في برِّ الأمان بعيداً عن مخاطر الإنترنت، ويلتزم بالإضافة إلى ذلك بواجب إعلام شركة التّأمين عن كلِّ حدثٍ من شأنه أن يؤثّر في احتمال حصول الخطر، وبالقيام بالمطالبة عند تحقّق الخطر المؤمّن ضدّه.

ثانياً: المقترحات:

1-العمل على توسيع قواعد المعلومات المتعلّقة بمخاطر الإنترنت والحوادث الإلكترونيّة السّابقة للاستفادة منها في تحديد المخاطر والعمل على تقديرها بشكلٍ صحيحٍ، ويحصل ذلك عبر الإفصاح والشّفافيّة من جانب الشّركات الضّحيّة عمّا تعرّضت له من خروقاتٍ أمنيّةٍ إلكترونيّةٍ.

2-التوجّه الحكوميّ على صعيد العالم لدعم قطّاع التّأمين ضدّ مخاطر الإنترنت انطلاقاً من أهميّة هذا القطّاع في ظلِّ العمل عبر الإنترنت، وذلك عبر إشراك شركات التّأمين العامّة في تقديم وثائق التّأمين ضدّ

مخاطر الإنترنت؛ لما سيعود ذلك بفوائدَ على القطاع برمّته؛ ولقدرة هذه الشّركات بمحافظ تأمينها على التّصدّي بصورةٍ أكثر فعاليّة لمخاطر الإنترنت.

3–العمل على تحسين بيئة العمل الإلكترونيّة وزيادة الأمن الإلكترونيّ، عبر الاستعانة بقوانين الخصوصيّة، وحماية البيانات التي لها بالغ الأثر في فرض حدٍّ معيّنٍ من الالتزامات والواجبات على الشركات، وهو ما يضع حداً كبيراً لمخاطر الإنترنت كونها تقلّل من نسبة الإهمال الحاصلة، كما أنّ هذه القوانين من شأنها أن تتّجه بالشّركات نحو شراء وثائق التّأمين ضدّ مخاطر الإنترنت رغبةً منها في التخلّص من مسؤوليّتها تجاه الغير عند حصول الخطر المؤمّن ضدّه.

4–زيادة حجم التغطية المقدّمة بموجب وثائق التّأمين ضدّ مخاطر الإنترنت لتغطّي بعض المخاطر الشّائعة والمستثناة، مثل مخاطر الحرب والإرهاب الإلكتروني؛ لأنّ هذا الاستثناء يفتح مجالاً واسعاً للتفسير، بالإضافة إلى توجّه الشّركات على نحوٍ أوسع لتأمين التغطية للأفراد الطبيعيين الذين يستخدمون الإنترنت بقدرٍ مماثلٍ لتأمين الشّركات.

5–على الصّعيد المحليّ، اتجاه شركات التّأمين المحليّة نحو تقديم وثائق لتغطية مخاطر الإنترنت، وتعدّ هذه الخطوة ضروريةً في الوقت الحالي لا سيّما في ظلِّ ازدياد الجرائم المرتكبة عبر الإنترنت والموجّهة نحو الأفراد رغم وجود قانون مكافحة الجرائم المعلوماتيّة.

قائمة المراجع:

أولاً: باللُّغة العربيَّة

1- الكتب:

1. أبو السعود، علي. (د.ت.). **مبادئ الخطر والتأمين**، (د.ن.)، ص 125.
2. أحمد، ممدوح حمزة، وعبد الحميد، ناهد. (2003). **إدارة الخطر والتأمين**، (د.ن.)، ص 515.
3. إسماعيل، محمد صادق. (2010). **الحكومة الإلكترونية وتطبيقاتها في الدول العربية**، ط:1، القاهرة: مصر، دار العربي للنشر والتوزيع، ص 269.
4. بابكر أحمد، عثمان. (1997). **قطاع التأمين في السودان تقويم تجربة التحول من نظام التأمين التقليدي إلى التأمين الإسلامي**، الطبعة الأولى، جدة: السعودية، البنك الإسلامي للتنمية، ص 116.
5. حسين، محمد عبد الظاهر. (1995). **عقد التأمين مشروعيته أثاره إنهاؤه**، القاهرة: مصر، دار النهضة العربية، ص 268.
6. الحسيناوي، علي جبار. (2018). **جرائم الحاسب والإنترنت**، عمان: الأردن، دار اليازوري للنشر والتوزيع، ص 165.
7. الخفاجي، منعم. (2014). **مدخل لدراسة التأمين**، ط:1، (د.ن.)، ص 124.
8. داود، حسن طاهر. (2000). **جرائم نظم المعلومات**، الطبعة الأولى، الرياض: السعودية، أكاديمية نايف العربية للعلوم الأمنية، ص 244.
9. زهرة، البشير. (1997). **التأمين البري دراسة تحليلية وشرح لعقود التأمين**، تونس: تونس، دار بو سلامة للطباعة والنشر، ص 420.
10. السنهوري، عبد الرزاق أحمد. (1964). **عقود الغرر وعقد التأمين**، مج:2، بيروت: لبنان، دار إحياء التراث العربي، ص 1722.
11. سيد، سالم رشدي. (2015). **التأمين المبادئ والأسس والنظريات**، ط:1، عمان: الأردن، دار الراية للنشر والتوزيع، ص 194.
12. عبد ربه، إبراهيم علي إبراهيم. (2006). **مبادئ التأمين**، مصر، الدار الجامعية، ص 405.
13. عبده، عيسى. (1978). **التأمين بين الحل والتحريم**، ط:1، (د.ن.)، ص 256.
14. عبيد، أسامة. (2016). **استراتيجيات التأمين المفهوم والأهداف**، ط:1، عمان: الأردن، دار أمجد للنشر والتوزيع، ص 184.
15. العمري، شريف محمد، عطا، محمد محمد. (2012). **الأصول العلمية والعملية للخطر والتأمين**، ط:1، (د.ن.)، ص 333.

16. غنام، شريف محمد. (2008). **التنظيم القانوني للإعلانات التجارية عبر شبكة الإنترنت**، مصر، دار الجامعة الجديدة، ص 223.
17. فلاح، عز الدين (2008). **التأمين مبادئه وأنواعه**، ط:1، عمان: الأردن، دار أسامة للنشر والتوزيع، ص 272.
18. القره داغي، علي محيي الدين. (2010). **التأمين الإسلامي دراسة فقهية تأصيلية مقارنة بالتأمين التجاري مع التطبيقات العملية**، ط:1، بيروت: لبنان، دار البشائر للطباعة والنشر والتوزيع، ص 712.
19. قطب، محمد علي. (2010). **الجرائم المعلوماتية وطرق مواجهتها**، ج:2، البحرين، الأكاديمية الملكية للشرطة، ص 15.
20. مكناس، جمال الدين، وعاشور، محمد سامر. (2018). **التأمين**، دمشق: سورية، منشورات الجامعة الافتراضية السورية، ص 231.
21. المومني، نهلا عبد القادر. (2010). **الجرائم المعلوماتية**، ط:2، عمان: الأردن، دار الثقافة للنشر والتوزيع، ص 239.
22. الناصري، أسنر خالد. (2019). **المسؤولية المدنية عبر انتهاك الخصوصية عبر مواقع التواصل الاجتماعي- دراسة مقارنة**، ط:1، القاهرة: مصر، دار النهضة العربية للنشر والتوزيع، ص 242.

2- الأبحاث والتقارير والندوات:

1. إبراهيم، حسام. (2019). **التطور التكنولوجي وقطاع التأمين ما لنا وما علينا**، بحث مقدم إلى المؤتمر الدولي السابع للتأمين (مؤتمر العقبة)، الأردن.
2. آل الشيخ، محمد بن حسن بن عبد العزيز. (2011). عقد التأمين التجاري للتعويض عن الضرر حقيقته وحكمه، عدد: 8، ص 255- 314، السعودية، بحث منشور في **مجلة الجمعية الفقهية السعودية**.
3. بانقا، علم الدين. (2019). **مخاطر الهجمات الإلكترونية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي**، عدد: 63، دراسات تنموية في المعهد العربي للتخطيط.
4. الحمود، عبد الله بن ناصر. (2006). **وسائل الإعلام المعاصرة والإرهاب المعلوماتي**، دورة تدريبية تقيمها جامعة نايف الأمنية في مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، المغرب.
5. خالد، خطيب. (2011). **الأسس النظرية والتنظيمية للتأمين التقليدي في الجزائر** ندوة حول مؤسسات التأمين التكافلي والتأمين التقليدي بين الأسس النظرية والتجربة التطبيقية، جامعة وهران، الجزائر.
6. سلطان العلماء، محمد عبد الرحيم. (2003). جرائم الإنترنت والاحتساب عليها، مج: 18، عدد: 36، ص 5- 58، السعودية، بحث منشور في **المجلة العربية للدراسات الأمنية والتدريب**.

3- المقالات:

- الضوابط الأساسية للأمن السيبراني، (2018)، **الهيئة الوطنية للأمن السيبراني**، السعودية.

4- القوانين:

أ- القوانين السورية:

- القانون المدني رقم 84 لعام 1949.

- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم 17 لعام 2012.

- قانون السير والمركبات رقم 31 لعام 2004.

- قانون التجارة البحرية رقم 46 لعام 2006.

- قانون الأحوال الشخصية رقم 59 لعام 1953.

- المرسوم التشريعي رقم 11 لعام 2008 المعدل لقانون السير والمركبات رقم 31 لعام 2004.

-قانون الضمان الصحي رقم 1 لعام 1979.

ب- القوانين العربية:

- القانون المدني المصري رقم 131 لعام 1948.

- القانون المدني الأردني رقم 43 لعام 1976.

- قانون الموجبات والعقود اللبناني رقم 0 لعام 1932.

ثانياً: باللغة الإنكليزية

1- books:

- Akhgar, B., Staniforth, A., & Bosco, B. (2014). **Cyber Crime and Cyber Terrorism Investigator's Handbook**, Rotterdam: Netherlands, Elsevier Inc, P 306.

- Baras, J. S., Katz, j., & Altman, E. (2011) **Decision and game theory for security,** second international conference, game sec, Berlin: Germany, Springer, p 270.

- Cheswick, W. R., Bellovin, S. M., Rubin, A. D. (2003) **Firewalls and Internet Security Repelling the Wily Hacker**, Boston: USA, Addison- Wesley, P 466.

- Coburn, A., Leverett, E., & Woo, G. (2018). **Solving Cyber Risk Protecting Your Company and Society**, New York: United States of America, Wiley, P 387.

- Hibberd, G. (2014). **The Rise of Cyber Liability Insurance,** Rotterdam: Netherlands, Elsevier Inc, p 10.

- Marano, P., Rokas, I., & Kochenburger, P. (2016) **The "Dematerialized" Insurance Distance Selling And Cyber Risks From An International Perspective**, Berlin: Germany, Springer, P 398.

- Ruan, K. (2019). **Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics**, Rotterdam: Netherlands, Academic Press Elsevier, P 186.

- Zwicky, E. D., Cooper, S., & Chapman, D. B. (2009). **Building Internet Firewalls**, California: USA, O'reilly Media, P 896.

2- articles:

- Camillo, M. (2017). cyber risk and the changing role of insurance, v2, P 53- 63, **journal of cyber policy**.

- Forsythe, S., Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping, v56, P 867- 875, Elsevier: Netherlands, **Journal of Business Research**.

- Justine Ferland. (2019). Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case, v35, P 369- 376, Elsevier: UK, **Computer Law & Security Review.**

- Luzwick, P. (2001) If Most of Your Revenue Is from E-Commerce, Then Cyber-Insurance Makes Sense, v2001, issue 3, **computer fraud & security**, P 2.

- Mukhopadhyay, A., Debashis S., Chakrabarti B, Ambuj M., & Asok P. (2005). Insurance for cyber-risk: A Utility Model, V32, NO1, P 154- 169, **Decision**.

- Mukhopadhyay, A., & others. (2013). Cyber-risk decision models: To insure IT or not, v56, P 11- 26, **decision support systems**.

- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk, v5, P1-19, Oxford: UK, **Journal of Cybersecurity**.

3- reports:

- Aburish, N., Fixler, A., & Dr. Hsieh, M. (2019). **The Role of Cyber Insurance in Securing the Private Sector**, Washington, DC: United States of America, center on cyber and technology innovation, p 10.

- ACP Cyber Insurance Proposal Form (SME). (n.d), P 7.

- **An introduction to cyber insurance understanding the Canadian ecosystem** (2019). the conference board of Canada, P 15.

- Bandyopadhyay, T. (2012). **Organizational adoption of cyber insurance instruments in IT security risk management–a modeling approach**, semantic scholar, p 7.

- Biener, C., Eling, M., Wirf, J. H. (2015). **insurability of cyber risk: an empirical analysis, working papers on risk management and insurance**, no. 151, St.Gallen: Switzerland, institute of insurance economics, P 32.

- Bohme, R., Kataria, G. (2003). **Models and Measures for Correlation in Cyber-Insurance**, Working Paper, Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK, p 26.

- Clinton, L. (n.d.). **Cyber-Insurance Metrics and Impact on Cyber-Security, Internet Security Alliance**, Online paper, p 8.

- Cyber and data insurance, policy wording, (n.d). hiscox, P 2.

- Cyber claims examples an aid to evaluating if you have adequate insurance in place, CHUBB, P 5.

- **Cyber insurance: a reference guide, institute for development and research in banking technology**. (2017). reserve bank of India, P 31.

- Cyberinsurance general terms and condition, (2019). pohjola insurance LTD, P 12.

- Cyber Risk – Enlightenment through information risk management, available at: https://www.pwc.com.au/consulting/security-cyber-assets/cyber-risk.html

تاريخ الزيارة: 11\5\2020، الساعة 1p.m.

- Cyber risk explained: what they are, what they could cost, and how to protect against them (2013). Marsh, available at: https://www.marsh.com/se/en/services/cyber-risk.html

تاريخ الزيارة: 10\5\2020، الساعة 12a.m.

- Cyber, Security and Privacy Protection Insurance, Policy Wording, Zurich insurance, p 35.

- Cyber security liability coverage form (n.d). Philadelphia indemnity insurance company, p 23.

- **enhancing the role of insurance in cyber risk management**. (2017). Paris: France, OECD publishing, p 142.

- Financial Services Authority. (2012). Annual Report, p 30.

- Grzebiela, T. (2002). **Insurability of Electronic Commerce Risks**, Proceedings of the 35th Hawaii International Conference on System Sciences, Germany, Institute for Computer Sciences and Social Studies, p 9.

- Ibraheem K. (2008). **Risk, costs and benefits of cyber insurance in Nigerian banks**, p 51.

- **Incentives and barriers of the cyber insurance market in Europe** (2012). ENISA, p 36.

- Kesan J. p. & Others, (2005). **cyber insurance as a market based solution to the problem of cyber security- a case study**, workshop on economics information security (WEIS), p 46.

- Kesan J. P., Yurcik, W., & Majuca, R., (2006). **The Evolution of Cyber insurance**, computer science, ArXiv, p 16.

- Khalil, M., Naghizadeh, P., & Liu, M. (2017). **Embracing Risk Dependency in Designing Cyber-Insurance Contracts**, Fifty-Fifth Annual Allerton Conference, Illinois: USA, p 926- 933.

- Lindsey, N. (2019). **Businesses Are Finding Out That Cyber Insurance Coverage Might Not Be What They Thought**, available at:

https://www.cpomagazine.com/cyber-security/businesses-are-finding-out-that-cyber-insurance-coverage-might-not-be-what-they-thought

تاريخ الزيارة: 24\4\2020, الساعة 10.30 p.m.

- Miaoui, Y., Boudriga, N. (2019). **Enterprise security economics: A self-defense versus cyber-insurance dilemma**, Applied Stochastic Models Business and Industry, p 31.

- Monroe, M. f., Boer, M. (2019). **cyber risk insurance update: advances in risk management, prioritizing prevention and protection**, Washington, D.C: USA, institute of international finance, P 11.

- **Purchasers' Guide to Cyber Insurance Products**. (2016). United States of America, financial services sector coordinating council for critical infrastructure protection and homeland security, p 26.

- Ruef, M. (2017). **Cyber insurance- benefits and uses**, SCIP, p 2.

- **Simply Cyber Policy Terms & Conditions** (2018). RAK insurance, v1, p 22.

- SME cyber claims are on increase understand your business exposure (n.d). CHUBB, p 5.

- Wang, F. (2017). **Cyber Insurance Ready For Take-Off In China**, Shanghai: China, p5.

- Wolff, J. (2018). **Cyberinsurance Tackles the Wildly Unpredictable World of Hacks**. available at: https://www.wired.com/story/cyberinsurance-tackles-the-wildly-unpredictable-world-of-hacks/

تاريخ الزيارة: 24\4\2020، الساعة 11:30 p.m.

4- websites:

- http://www.betterley.com

-https://www.searchsecurity.techtarget.com/definition/cybersecurity-insurance-cybersecurity-liability-insurance

-https://www.thecroforum.org/2018/02/21/supporting-on-going-capture-and-sharing-of-digital-event-data

- https://www.finder.com.au/cyber-risk#1

- https://www.nbins.com/blog/cyber-risk/what-is-cyber-risk-2/

_https://www.ar.wikipedia.org/wiki/%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA

- https://www.phoenixnap.com/blog/cyber-security-attack-types

- https://www.cyber-risk.com.au/

- https://www.arab-army.com/t84615-topic

_https://www.arageek.com/tech/%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%85%D9%88%D9%82%D8%B9
%D8%A3%D9%85%D8%B1%D9%8A%D9%83%D9%8A

- https://www.dw.com/ar/

-https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks/

-https://www.ifsecglobal.com/cyber-security/which-sectors-are-most-vulnerable-to-cyber-attacks/

- https://www.en.wikipedia.org/wiki/Russian_Business_Network

- https://www.aitnews.com
- https://www.aawsat.com
-https://www.youm7.com/story/2019/10/7/5-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82%D8%A7%D8%AA-%D8%A3%D9%85%D9%86%D9%8A%D8%A9-%D8%AD%D8%AF%D9%8A%D8%AB%D8%A9-%D8%AA%D9%87%D8%AF%D8%AF-%D9%85%D8%B3%D8%AA%D8%AE%D8%AF%D9%85%D9%89-%D8%A7%D9%84%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9/4447681
-https://www.al-ain.com/article/zoom-scandal-600-users-sale-hacker-forum
- https://www.en.wikipedia.org/wiki/Malware
-https://www.antivirus.comodo.com/blog/comodo-news/iloveyou-virus-and-its-removal/
-https://www.thebalance.com/best-credit-monitoring-services-4164937
-https://www.irmi.com/term/insurance-definitions/credit-monitoring
-https://www.kroll.com/en/services/cyber-risk/remediate-and-restore/data-breach-call-center-services
-https://www.gdpr-info.eu/
-https://www.irmi.com/term/insurance-definitions/laptop-exclusion
-https://www.greatamericaninsurancegroup.com/for-businesses/product-details/cyber-risk-insurance/primary-cyber-risk-coverage
-https://www.zurichna.com/knowledge/topics/cyber
-https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf
-https://www.alborsaanews.com/2020/04/20/1322824
- https://www.albayan.ae/economy/capital-markets/2019-03-28-1.3522036
-https://www.nans.gov.sy/ar/article/workshop_entitled_%22insurance_of_the_dang
-https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf
-https://www.almerja.com/reading.php?idm=115645
-https://www.allianz.com.eg/ar_EG/customer-care/premium-payment-methods.html
-http://www.arab-ency.com.sy/law/detail/163444

-https://www.axa.com.sg/pdf/our_solutions/cyber-risks/cyber-protector/cyberprotector.pdf

_https://www.nok6a.net/%d8%a7%d9%84%d8%aa%d8%a3%d9%85%d9%8a%d9%86-%d8%b6%d8%af-%d8%ad%d9%88%d8%a7%d8%af%d8%ab-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a/

-https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf

_https://www.nok6a.net/%d8%a7%d9%84%d8%aa%d8%a3%d9%85%d9%8a%d9%86-%d8%b6%d8%af-%d8%ad%d9%88%d8%a7%d8%af%d8%ab-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a/

-https://www.baylor.edu/content/services/document.php/192120.pdf

-https://www.gbainsurance.com/avoiding-cyber-claim-denials

-https://www.hhs.gov/sites/default/files/cottage-health-ra-cap.pdf

_https://www.scholar.google.com/scholar_case?case=4637833847825659548&q=Aqua+Star+(USA)+Corp.+v.+Travelers+Casualty+and+Surety+Co.+of+America&hl=en&as_sdt=2006&as_vis=1

-https://www.cc.gov.eg/judgment_single?id=111307435&ja=164593

https://www.ar.wikipedia.org/wiki/%D9%81%D8%B6%D8%A7%D8%A1%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

-https://www.marefa.org/%D8%A3%D8%B1%D9%BE%D8%A7%D9%86%D8%AA

Summary

The risks of the Internet today constitute the greatest concern of any individual and entity, given that it is something unexpected, and its extent and impact cannot be determined, due to the massive use of the Internet in all aspects of life. There is not any company does not use the Internet in its business, starting from storing information until conducting electronic transactions and electronic payment, and this use is accompanied by great risks as a result of the possibility of stealing stored information, selling it to competing companies, disrupting the used websites, and other risks, which greatly affect the course of Electronic work. As a result, companies resorted to protecting themselves from these risks to cyber insurance companies, in order to obtain insurance coverage for the risks that they may be exposed to, in exchange for paying premiums determined by the insurance companies. cyber insurance contract is a new contract that belongs to other insurance contracts, but at the same time it is distinguished from others due to the electronic characteristics that give it a unique characteristic. Accordingly, the insurance contract against Internet risks will be studied through two chapters, the first of which is devoted to talking about the nature of cyber insurance contract and what these risks are, while the second chapter is devoted to talking about the obligations arising from this contract.

Key words: internet risks, cyber insurance, insurance coverage, insurance premiums.

الكلمات الرئيسية: مخاطر الإنترنت، التّأمين ضد مخاطر الإنترنت، تغطية تأمينية، أقساط التّأمين.

Syrian Arab Republic

Damascus University

Faculty of Law

Commercial Law Department

CYBER INSURANCE CONTRACT

(An analytical study of some risks of using the internet)

A dissertation submitted in partial fulfillment of the requirements for the degree of Master in commercial law

By

Zienab Khaddour

Supervisor

Hanan Malikah

2020\2021