ISSN 0123-1154 (IMPRESO)
ISSN 2500-7556 (EN LÍNEA)

CONTRATO DE SEGURO. LA OBLIGACIÓN DE INFORMACIÓN Y AGRAVACIÓN DEL RIESGO CIBERNÉTICO

INSURANCE CONTRACT. DISCLOSURE OBLIGATION AND AGGRAVATION OF CYBER RISKS

ADILSON JOSÉ CAMPOY[*]
MARCIO ALEXANDRE MALFATTI[**]
MICHELLE SAMPAIO LOPES MALFATTI[***]
THAÍS DE CÁSSIA RUMSTAIN[****]

Fecha de recepción: 30 de abril 2020
Fecha de aceptación 15 mayo 2019
Disponible en línea: 30 de junio 2020

Para citar este artículo/To cite this article

Campoy, Adilson José; Malfaltti, Marcio Alexandre; Malfatti, Michelle Sampaio Lopes & Rumstain, Thaís de Cássia. *Contrato de seguro-La obligación de información y agravación del riesgo cibernético,* 52 Rev.Ibero-Latinoam.Seguros, 131-144 (2020). https://doi.org/10.11144/Javeriana.ris52.csoi

Doi: 10.11144/Javeriana.ris52.csoi

[*] Licenciado en Derecho de la Universidade Braz Cubas, en Mogi das Cruzes-SP, Especialista en Derecho de Seguros de la Universidade Nova Lisboa, Especialista en Derecho de Seguros de la Universidad de Salamanca. Abogado, socio fundador de Pimentel e Associados Advocacia, y miembro del Consejo AIDA-Asociación Internacional de Derecho de Seguros-Sección Brasileña. Contacto: adilson@pimentel.com.br.

[**] Socio de Pimentel e Associados Advocacia, Especialista en Derecho de Seguros de la Universidad de Salamanca y en Derecho de Seguros de la Universidade Nova Lisboa. Con postgrado en procedimiento civil de la Universidade Paulista. Profesor de gestión de litigios y soluciones alternativas de resolución de conflictos en el MBA de la FIA. Profesor de Procedimiento Civil en el MBA en Derecho de Seguros de la Escuela Nacional de Seguros de Brasil, actualmente es vicepresidente del Grupo de Trabajo de Seguros de Crédito y Depósito de CILA. Contacto: marcio@pimentel.com.br.

[***] Data Private Officer–DPO en Banco PAN. MBA en Administración de Empresas de la Fundação Getúlio Vargas São Paulo–FGV. Especialista en Derecho Digital del Instituto de Educación e Investigación–INSPER. Extensión de seguridad cibernética en el Instituto de Tecnología de Massachusetts–MIT. Graduada de la Universidade Presbiteriana Mackenzie en Análisis de Sistemas. Contacto: michellesl@msn.com.

[****] Máster en derecho y estudios sobre resolución consensuada de conflictos en contratos de seguros. Profesor invitado en la Facultad CESUSC, sobre Seguro de Responsabilidad Civil y Seguro Obligatorio. Postgrado en Derecho de Seguros y Profesor de Derecho Procesal Civil y Civil. Miembro de la Comisión de Derecho de Seguros OAB/ SC. Gerente legal de la firma de abogados Pimentel e Associados Advocacia. Contacto: thais.rumstain@pimentel.com.br y thaisrumstain@gmail.com.

RESUMEN

Brasil tiene leyes muy recientes que regulan el flujo de información que proporciona la tecnología, con reglas y consecuencias para aquellos que no cumplen, ya sea en el ámbito civil o penal. Sin embargo, el escenario mundial apunta a un aumento en el número de ataques cibernéticos y eso coloca a Brasil en una posición prominente en la vulnerabilidad a estos ataques.

A partir de ahí, sigue la reflexión sobre el empeoramiento del riesgo en los contratos de seguro de responsabilidad y protección de datos cibernéticos y el deber de información inherente a todos los contratos de seguro.

Palabras clave: Contrato de Seguro, Seguro de Responsabilidad Cibernética, Agravación, Deber de Información, Pandemia.

ABSTRACT

Brazil has very recent laws that regulate the flow of information that technology provides, with rules and consequences for those who fail to comply, whether in the civil or criminal field. However, the world scenario points to an increase in the number of cyber attacks and that puts Brazil in a prominent position in vulnerability to these attacks. Based on that, there is a reflection on the worsening of risk in cyber data protection and liability insurance contracts and the duty of information inherent in all insurance contracts.

Keywords: Insurance contract, Cyber Liability Insurance, Worsening, Duty of Information, Pandemic.

SUMARIO

1. Introducción. 2. Breves consideraciones sobre seguro de responsabilidad cibernética y cláusulas contractuales. 3. Derecho de información y agravación de riesgo. 3.1. Agravación deliberada en riesgos cibernéticos. 3.2. Agravación por hecho o acto de terceros en riesgos cibernéticos. 4. Conclusión. 5. Referencias.

1. INTRODUCCIÓN

Los ataques cibernéticos no son un tema nuevo y son más comunes de lo que se piensa. En una encuesta realizada por la Organización de Estados Americanos (OEA), en 2015, Brasil ocupó el tercer lugar en ataques cibernéticos (11%), detrás de Estados Unidos (15%) y China (51%). En 2019, el gasto mundial en productos y servicios de seguridad cibernética fue del orden de US $ 124 mil[1] millones y, en el primer trimestre de 2020, Brasil ya estaba en la segunda posición en pérdidas financieras debido a los ataques cibernéticos, llegando al orden de $ 20 mil millones[2].

En el informe de riesgo global, presentado por el Foro Económico Mundial (FEM), publicado en enero de 2020, los riesgos cibernéticos a gran escala combinados con los problemas derivados de los avances tecnológicos afectarán a más del 74% de las empresas, lo que representará pérdidas en el orden de los EE. UU. $ 3 billones[3], destacando la importancia del tema en la economía mundial.

Lo poco que se ha dicho es suficiente para intuir la importancia del contrato de seguro en esta atmósfera en la que, por un lado, la sociedad depende cada vez más de la tecnología y, por otro lado, los ataques maliciosos en los datos de terceros son cotidianos y más sofisticados con el tiempo.

En vista de esta situación, a responsabilidad de la custodia, a cualquier título, de la información de terceros, gana una relevancia que anteriormente no entendíamos, o incluso no existía.

En nuestro país, en los últimos tiempos, se ha instituido el "Marco Civil de Internet" y la Ley General de Protección de Datos, aún en vacacio legis, para regular este flujo de información que proporciona la tecnología, con reglas y consecuencias para aquellos que no cumplan con ellas. En el ámbito penal, fue importante la promulgación de la Ley N° 12.737 / 2012, que penaliza los delitos informáticos.

Pero, si estas leyes recientes servirán como base para delimitar el alcance del contrato de seguro relacionado con la cobertura de los riesgos cibernéticos, debe decirse que se prevé cierta dificultad. En efecto, nuestro Código Civil, la norma principal que regula el contrato de seguro, ha estado en vigor desde enero de 2003, durante 17 años. Y su promulgación tuvo como base un proyecto presentado en los años 70, hace medio siglo.

De ahí la dificultad que tenemos de lidiar con la obligación de información en los seguros sobre riesgos cibernéticos.

El análisis del tema debe tener en cuenta las leyes recientes que, aunque no son normas de principios, abordan cuestiones subyacentes a la discusión sobre el contrato de seguro,

[1] Disponible en https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. Acesso em 13.05.2020.

[2] Investigación realizada por la Unión Internacional de Telecomunicaciones (UIT), un órgano de las Naciones Unidas (ONU) y disponible en: https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-taques-ciberneticos-aponta-audiencia Acesso em 14.05.2020.

[3] Disponible en https://www.weforum.org/reports/the-global-risks-report-2020. Acesso em 13.05.2020.

como la Ley N° 12.965, de 23 de abril de 2014, llamada "Ley del Marco Civil de Internet, N° 13.709 de / 14 de agosto de 2018, conocida como la "Ley General de Protección de Datos" (LGPD) y la Resolución N ° 4658, del Banco Central, las dos primeras normas ya mencionadas, marcos legales desde el que comienza el análisis del contrato de seguro vinculado a la protección de datos y la responsabilidad cibernética.

El riesgo se materializa, por ejemplo, en relación de las declaraciones precontractuales, que permitirán al asegurador evaluar si está interesado en garantizar el riesgo propuesto y a qué tasa de prima; se evaluará también la posible agravación de ese riesgo y el cumplimiento de la información de las partes contratantes.

Considerando el espacio reducido para formular nuestras consideraciones simples, nos limitaremos a tratar con información relacionada con el agravamiento del riesgo, evidentemente considerando el tratamiento que nuestra legislación dedica al tema.

2. BREVES CONSIDERACIONES SOBRE SEGURO DE RESPONSABILIDAD CIBERNÉTICA Y CLÁUSULAS CONTRACTUALES

El seguro de responsabilidad cibernética tiene como objetivo proteger la responsabilidad de las compañías aseguradas que, por cualquier razón y de cualquier forma, mantienen información de terceros, por el pago de las pérdidas reclamadas por estos terceros como resultado de ciberataques externos[4] o no[5].

Estas pólizas no se limitan a cubrir la responsabilidad de la compañía asegurada[6], sino también a los riesgos que la afectan directa y exclusivamente. Los riesgos cubiertos por estos contratos se dividen en "riesgos propios", que son, reiteramos, riesgos que afectan directa y exclusivamente a la compañía asegurada, y los riesgos de responsabilidad civil por daños causados a terceros, llamados "riesgos de tercera parte". Ambos riesgos pueden materializarse como resultado de un solo ataque cibernético o un solo fallo del sistema.

Los riesgos cubiertos por el contrato de seguro pueden estar relacionados con activos tangibles o intangibles. No existe una definición única de lo que serían los activos tangibles e intangibles, aunque puede decirse que los tangibles, serían elementos materiales, del patrimonio físico.

[4] Los riesgos externos pueden provenir de piratas informáticos, que modifican el software y el hardware de la computadora, cambian la funcionalidad existente o malware y ransomware, software ilícito que se infiltra en los sistemas y puede causar daños al sistema o robar información.

[5] Por ejemplo, los actos nocivos realizados por los empleados que pueden resultar del robo de información y / o la pérdida o eliminación incorrecta de computadoras o medios portátiles, incluido el hardware.

[6] Es importante tener en cuenta que nuestra legislación no se refiere a la figura del "tomador", sino única y exclusivamente a la figura del "asegurado". Esto no quiere decir que, aquí, no hay contratos de seguro firmados en nombre de otros, en cuyo caso el titular de los intereses, por lo tanto, asegurado, no es el contratista

En cuanto a los intangibles, Malone y Edvinsson (1997) los clasifican como aquellos que no tienen existencia física, pero que aún tienen valor para las empresas. Bontis, N.; Dragonetti; (1999) los definen como cualquier factor que contribuye a los procesos que generan valor para las empresas. En un sentido similar, Lev, B (2001) define los activos intangibles por sus principales fuerzas impulsoras, como la investigación, el desarrollo, la publicidad, la tecnología de la información y las prácticas de recursos humanos. Aunque los activos intangibles no se incluyen en los informes contables, tienen valor económico para las empresas (Schnorrenberger, 2005, pp. 52-53). Por lo tanto, la imagen de la sociedad y sus directores, marcas, patentes, derechos de autor, por ejemplo, serían activos intangibles.

Sin embargo, identificar los riesgos que afecten los activos intangibles para asegurarlos no es una tarea simple, sino un desafío para las compañías contratantes y las compañías de seguros, quienes tomarán los riesgos que creen que pueden suscribir, y es esencial mapearlos y medir la pérdida que pueden producir estos riesgos. Las pérdidas físicas, relacionadas con muebles, bienes raíces, inventario, dinero, por ejemplo, que son activos tangibles, se identifican, miden y valoran más fácilmente.

Los activos intangibles se incluyen en el concepto de "cosa", sujeto a la cobertura del seguro, según lo establecido en el Art. 757 del Código Civil brasileño, "el asegurador está obligado, tras el pago de la prima, a garantizar el interés legítimo del asegurado, en relación con la persona o la cosa, contra riesgos predeterminados".

En resumen, las pólizas comercializadas en Brasil garantizan la cobertura de pérdidas derivadas de: I) Violación real o presunta de información personal; II) Violación de la información corporativa; III) Violación de información personal de un tercero por parte del responsable del procesamiento y la recopilación de datos en nombre de la empresa prestataria; IV) Acto, error u omisión en la protección y seguridad de los datos; V) Costos de defensa relacionados con el reclamo; VI) Honorarios, costos y gastos con la investigación administrativa relacionada con un reclamo; VII) Costos y gastos razonables para mitigar el daño a la reputación y la imagen personal y profesional de los directores del prestatario, como consecuencia de uno de los riesgos cubiertos por la póliza; VIII) Costos para mitigar la reputación de la empresa prestataria; IX) Gastos de mitigación de emergencia o tarifas de mitigación.

Las pólizas también prevén exclusiones específicas para cada cobertura, ya que no es posible ofrecer cobertura general y sin restricciones, sino solo a los riesgos expresamente asumidos en la póliza y, en general, las pérdidas derivadas de: I) Acto, error u omisión que produce una ganancia de un beneficio o ventaja a la cual el asegurado no tiene derecho; II) Acto ilícito intencional o falta grave que cometa el asegurado o con su colusión o tolerancia, incluyendo deshonestidad, fraude y violación criminal de la ley o regulación; III) Competencia desleal, de conformidad con las normas legales que rigen el tema; IV) Caños materiales, como resultado de la pérdida o destrucción de propiedades tangibles, excepto por la pérdida del uso de datos; V) Daño corporal, a menos que el daño moral resulte de una violación por parte de la compañía asegurada de las reglas de protección de datos; VI) Quiebra, insolvencia, acuerdo o liquidación del asegurado y de las empresas vinculadas directa o indirectamente al asegurado; VII) Daños resultantes de actos de guerra, terrorismo, disturbios, huelgas

y rebeliones; VIII) Pérdidas resultantes de problemas de infraestructura basados en fallas mecánicas, eléctricas, fallas de los sistemas de telecomunicaciones o de transmisión por satélite y fallas de seguridad del sistema informático por debajo de los estándares razonables de seguridad de la industria; IX) Pérdidas derivadas de transacciones financieras a través de transferencias electrónicas; X) daños resultantes de la infracción de los derechos de propiedad intelectual, incluidas las patentes y los secretos comerciales; XI) Responsabilidades contractuales; XII) Pasivos laborales y XIII) Reclamaciones de valores.

Además de las exclusiones de cobertura, las pólizas también abordan la hipótesis de pérdida del derecho a indemnización, en las cuales el asegurado continuará obligado a pagar la prima. Son: I) incumplimiento de las obligaciones acordadas en el contrato de seguro–hipótesis de incumplimiento contractual -; II) prácticas de actos ilícitos para obtener beneficios del contrato; III) cuando el asegurado hace declaraciones inexactas, por sí mismo o por su representante, u omite circunstancias que pueden influir en la aceptación de la propuesta o el valor de la prima, tal como está previsto en el Art. 766 del Código Civil brasileño:

> "Art. 766. Si el asegurado, por sí mismo o por su representante, hace declaraciones inexactas u omite circunstancias que pueden influir en la aceptación de la propuesta o la tasa de la prima, perderá el derecho a la garantía, además de estar obligado a la prima vencida".

Además, al reproducir las disposiciones del Código Civil brasileño, las pólizas estipulan que el tomador del seguro perderá el derecho a compensación cuando: I) Agrave intencionalmente el riesgo objeto del contrato[7]; II) No denuncie un reclamo a la aseguradora, tan pronto como se dé cuenta y no tome medidas inmediatas para mitigar sus consecuencias[8]; y III) No informe inmediatamente a la aseguradora, tan pronto como sepa, cualquier hecho que pueda agravar el riesgo cubierto, bajo pena perder el derecho a una indemnización, si se demuestra que él / ella guardó silencio de mala fe[9].

Los términos de los contratos de seguro de responsabilidad y protección de datos cibernéticos imponen un deber de buena fe en las declaraciones del asegurado, como en cualquier contrato de seguro. Esta disposición contractual refleja la más estricta buena fe, aplicable a todos los contratos de seguro, de conformidad con el Art. 765 del Código Civil brasileño:

---

[7] Art. 768, CCB: El asegurado perderá el derecho a la garantía si agrava intencionalmente el riesgo objeto del contrato.

[8] Art. 771, CCB: Bajo pena de perder el derecho a indemnización, el asegurado informará el reclamo al asegurador, tan pronto como él / ella lo sepa, y tomará medidas inmediatas para mitigar las consecuencias.

[9] Art. 769, CCB: El asegurado está obligado a informar al asegurador, tan pronto como lo sepa, cualquier incidente que pueda agravar significativamente el riesgo cubierto, bajo pena de perder el derecho a la garantía, si demuestra que guardó silencio de mala fe.

1° El asegurador, siempre que lo haga dentro de los quince días siguientes a la recepción del aviso de agravamiento del riesgo sin culpa del asegurado, puede informarle, por escrito, de su decisión de rescindir el contrato.

2° La resolución solo entrará en vigencia treinta días después de la notificación, y la aseguradora deberá devolver la diferencia de la prima.

"Art. 765. El asegurado y el asegurador están obligados a mantener, en la conclusión y ejecución del contrato, la más estricta buena fe y veracidad, tanto con respecto al objeto como a las circunstancias y declaraciones relacionadas con el mismo".

3. DERECHO DE INFORMACIÓN Y AGRAVACIÓN DE RIESGO[10]

El empeoramiento del riesgo se produce cuando las probabilidades de ocurrencia del accidente aumentan deliberadamente o no generando un desequilibrio considerable en la relación contractual y, en consecuencia, en todo el sistema de fondos mutuos del seguros.

En cuanto al tema de la agravación, es necesario diferenciar las dos especies legalmente previstas en nuestro país: la regulada por el Art. 768 y la regulada por el Art. 769 del Código Civil brasileño.

El área de aplicación de ambos dispositivos es, por supuesto, diferente: en el primero, el agravamiento surge de un acto consciente del asegurado, que lo practica a pesar de que aumenta el riesgo de que ocurra un accidente o, aun así, proporciona condiciones para que las consecuencias de un reclamo sean más dañinas de lo que podrían ser; en el segundo, el agravamiento ocurre debido a un hecho no relacionado con su, pero, igualmente, con su conocimiento.

En cualquier caso, la doctrina nacional y extranjera sobre el tema es unánime al afirmar que el instituto de agravación tiene como objetivo evitar que se rompa el equilibrio entre el riesgo asegurado y la prima recibida por el asegurador[11].

3.1. Agravación deliberada en riesgos cibernéticos

En el caso del Art. 768, si el asegurado, después de celebrar el contrato de seguro, cambia su operación haciéndola más susceptible a un ataque, y es consciente de ello, existe una pérdida del derecho a la protección asegurativa.

La transcripción de la ley mencionada vale nuevamente:

"Art. 768. El asegurado perderá el derecho a la garantía si agrava intencionalmente el riesgo objeto del contrato".

Se discute mucho sobre las hipótesis de aplicación de esta disposición que, si se admite, impone una consecuencia extrema al asegurado: la pérdida de la garantía (cobertura) que el contrato, en principio, ofrecía.

[10] (Art. 769, CC). Sabemos que la doctrina en general, incluida la patria, usa la expresión "agravación". Sin embargo, utilizamos el término "agravamiento" porque así es como se expresa nuestro Código Civil en el único momento en que se refiere expresamente al fenómeno.

[11] Schiavo, Carlos A. *Contrato de seguro. Reticencia y agravación del riesgo.* Buenos Aires: Hammurabi, 2006. p. 265.

Ya hemos visto, antes, las hipótesis en las cuales las cláusulas contractuales excluyen la garantía de riesgo para ciertas circunstancias. Estas exclusiones son lo que la doctrina define como la hipótesis de que no hay seguro, o lo que se llama "no seguro". En estas circunstancias, no hay pérdida del derecho a garantizar o a obtener cobertura, ya que este derecho nunca existió. Es un riesgo que la aseguradora nunca tuvo la intención de garantizar o asegurar y sobre el cual nunca cobró una prima, todo dentro del principio universal de que la aseguradora tiene el derecho de delimitar los riesgos que va a garantizar o asegurar.

De manera diferente, ocurre en el caso de un agravamiento del riesgo en el cual la acción –u omisión– de la persona asegurada conduce a la pérdida del derecho a la garantía asegurativa. Aquí, el riesgo estaba asegurado en el contrato, el derecho a una garantía que se pierde, sin embargo, por el comportamiento consciente del asegurado.

Para Andrea Signorino Barbat[12]:

Las alteraciones de riesgo que determinan su agravación no son equivalentes a riesgos no cubiertos. Los riesgos no cubiertos son delimitaciones del riesgo que se pactan al celebrar el contrato, son las circunstancias, especial y expresamente, determinadas en el contrato de seguros como causales de exclusión de cobertura y calificadas como riesgos no cubiertos, como circunstancias en cuyo contexto la ocurrencia del riesgo no se considera cubierto.

3.2. Agravación por hecho o acto de terceros en riesgos cibernéticos

Si, en la hipótesis del Art. 769, por acto o hecho de un tercero, el riesgo aumenta y el asegurado lo sabe, debe informar al asegurador. En el caso de la pandemia, no hay forma de alegar ignorancia sobre el empeoramiento de las amenazas, porque incluso si el asegurado no está monitoreando o no tiene un mecanismo para monitorear las amenazas a las que está expuesto, todo el mercado de seguridad comenzó a alertar y enviar boletines sobre los escenarios a que las empresas estuvieron expuestas a la hora de proporcionar trabajo remoto. Depende de la empresa interpretar estas amenazas y evaluar sus controles para medir su nueva exposición al riesgo.

Los datos publicados por Kaspersky, una empresa especializada en seguridad digital, indican que solo en Brasil, los intentos de estafas relacionadas con el secuestro de datos aumentaron un 350% en el primer trimestre y están directamente relacionados con la adopción de la oficina en casa debido a la pandemia, comportamiento que siente el mercado de ciberseguridad.

Art. 769, del Código Civil Brasileño:

Art. 769, CCB:

[12] Signorino Barbat. Andrea. *Estudios de Derecho de Seguros y Reaseguros – La Ley Uruguai*. Montevideo: Ituzaingó, 2016, p. 35.

"El asegurado está obligado a comunicar al asegurador, tan pronto como lo sepa, cualquier incidente que pueda agravar significativamente el riesgo cubierto, bajo pena de perder el derecho a la garantía, si demuestra que guardó silencio de mala fe.

1. El asegurador, siempre que lo haga dentro de los quince días siguientes a la recepción del aviso de agravación del riesgo sin culpa del asegurado, puede informarle, por escrito, de su decisión de rescindir el contrato.

2º La resolución solo entrará en vigencia treinta días después de la notificación y el asegurador deberá devolver la diferencia de la prima".

Entonces, mírese que aquí nos enfrentamos a un escenario en el que el riesgo, asegurado en el contrato, se incrementa por el hecho o el hecho de terceros, no necesariamente interesados en la existencia de este contrato, normalmente desinteresado[13].

Aquí, la agravación no será el resultado del comportamiento del asegurado, pero, habiendo sido consciente de esta agravación, debe informar al asegurador bajo pena de perder el derecho a la garantía[14].

En la doctrina autorizada de Andrea Signorini Barbat[15], es un agravante que se extiende con el tiempo y ocurre de manera impredecible cuando se firma el contrato. Además, considera innecesario el vínculo causal entre el agravamiento y la ocurrencia del siniestro[16].

Luiza Moreira Petersen[17] señala que la agravación debe ser relevante y superveniente a la formación del contrato, y también registra que debe ser impredecible.

¿Y cuál será el propósito de esta obligación de comunicar la agravación al asegurador? Darle la oportunidad, conociendo el nuevo riesgo, de cuantificarlo adecuadamente, evidentemente aumentando esa tasa, o, dentro de un período que el legislador considere apropiado, de rescindir el contrato dentro de los 30 (treinta) días a partir de la notificación de su intención al asegurado de hacerlo, devolviendo a este último la diferencia de la prima eventualmente no devengada.

Véase, entonces: el asegurado debe informar el incidente que aumenta el riesgo, sin su culpa, tan pronto como lo sepa[18]; el asegurador, una vez informado, puede, dentro de los próximos 15 (quince) días, informar al asegurado de su decisión de rescindir el contrato. Al hacerlo, debe garantizar el riesgo por otros 30 (treinta) días.

---

[13] Cabe señalar que el asegurado está obligado a informar un incidente que podría agravar el riesgo. Muchos, en nuestra opinión con bastante razón, entienden que este incidente no necesariamente debe ser el resultado del comportamiento de los demás. Puede deberse, por ejemplo, a causas naturales, si es culpa del asegurado.

[14] Para esta hipótesis, se requiere prueba de que el asegurado guarda silencio de mala fe, y el asegurador es responsable de esta prueba, un requisito que no está en armonía con la estructura del Código Civil, que se basa, entre otros, en el principio de buena fe, considerado en su cara objetiva.

[15] Op. Cit., pp. 32 ss.

[16] Op. Cit., pp. 45.

[17] Petersen, Luiza Moreira. *O risco no contrato de seguro.* São Paulo: Roncarati. 2018. p. 149.

[18] La expresión genera un gran revuelo debido a su vaguedad. Muchos creen que la ley debería haber fijado una fecha límite y no permitir que el intérprete lo haga en cada caso específico.

Es cierto que el mecanismo bajo análisis no admite expresamente la continuidad del contrato con la adecuación de la tasa de la prima, pero esta alternativa es obvia cuando la terminación del contrato se coloca como una opción para el asegurador. Ahora, si no necesariamente se necesita rescindir el contrato, significa decir que, en acuerdo con el asegurado, puede continuar con aquél, ajustándolo.

Lo que se pregunta es si, en el caso de los riesgos cibernéticos, esta posibilidad de rescindir el contrato, aún más en los plazos ajustados, no conducirá a la incertidumbre legal que afectará a la sociedad en su conjunto.

Cuando el artículo de ley en estudio le da al asegurado otros 30 (treinta) días de plazo después de ser informado de que el asegurador rescindirá el contrato, es porque tiene la intención de darle la oportunidad de buscar un nuevo asegurador, dispuesto a garantizar el riesgo rechazado por el primero.

Pero, admitamos la posibilidad de que este nuevo riesgo no sea aceptado por ninguna otra aseguradora y tendremos, entonces, terceros que contarán solo con la propia capacidad de la compañía asegurada para soportar las pérdidas que causa. En pocas palabras, será su propia aseguradora.

Es cierto que, en muchos otros segmentos, este daño puede ocurrir, pero los riesgos cibernéticos son algo que raya en lo inconmensurable, en términos de alcanzar los intereses de terceros.

También es cierto que, dada la inconmensurabilidad mencionada anteriormente, la existencia de un seguro puede no ser suficiente para garantizar el interés de terceros en caso de agotamiento rápido de su límite de garantía o indemnización, pero un asegurador especializado puede, durante todo el plazo del seguro y en cooperación con el titular de la póliza, promover una gestión de riesgos adecuada, para mitigarlos, para que estén sujetos a fijación de precios a medida que cambian.

4. CONCLUSIÓN

Bajo el sistema brasileño, y ante un escenario de riesgo agravado, solo tenemos que establecer un sistema de declaraciones –obligatorio– para ambas partes en caso de agravamiento sin culpa por parte del asegurado y que puede resultar en la terminación del contrato.

Entendemos que las reglas establecidas por el artículo de ley que lo regulan, agravación sin culpa, pueden no ser suficientes, o incluso convenientes, para los intereses de la sociedad.

Se espera, entonces, que la doctrina y la jurisprudencia moderen, si esto es posible, la interpretación de la norma, antes de defender el nacimiento del seguro obligatorio para garantizar los riesgos cibernéticos.

Pero no se dude que puede surgir la idea.

Vale la pena comentar lo que estamos experimentando hoy, señalando la pandemia que ahora nos está atormentando.

No queremos, bueno es decirlo, relacionarlo, o sus efectos, con el fenómeno del aumento del riesgo. La agravación del riesgo, la que señalamos como resultado de la aplicación de la regla del Art. 769 del Código Civil brasileño, se aplica a un caso específico, circunscrito a la esfera de intereses existente entre un asegurador y un asegurado y relacionado con un contrato específico.

Nunca, tal como lo entendemos, podría ser posible, con base en el artículo antes mencionado, sostener la ausencia de cobertura para riesgos, cibernéticos o no, basados, vale la pena repetir, en riesgo agravado. En el caso, ni siquiera existe la obligación del asegurado de hacer ninguna comunicación al asegurador porque es un hecho público, declarado por la autoridad competente.

Pero, parece posible afirmar que, muchos riesgos, cibernéticos o no, aumentarán durante y después de esta pandemia: vale la pena repetir hasta el agotamiento, aquí no se trata de aplicar el fenómeno de agravación del riesgo, sino solo de reconocer que la sociedad puede verse obligada a vivir con mayores riesgos que los presentados en los últimos días.

La opción para la llamada oficina en el hogar crece, un sistema en el que los empleados prestan sus servicios no en la sede de las empresas que los contratan, sino directamente desde sus hogares.

La opción se justifica principalmente en el entorno de las grandes ciudades, donde el desplazamiento de personas entre sus hogares y la sede de sus empleadores representa un gasto financiero directo, el costo de dicho desplazamiento, e indirecto, el tiempo que consume el desplazamiento, esto, quizás, lo más significativo.

Pero este proceso se aceleró enormemente con la llegada de la pandemia. Como parte de las acciones de emergencia para poner a las empresas a trabajar sin contacto social, las empresas se vieron obligadas a implementar un sistema de trabajo de oficina en casa a gran escala, sin la posibilidad de una planificación previa en relación con los riesgos derivados de esta nueva realidad.

Sin embargo, a diferencia de lo que sucede cuando el trabajo se lleva a cabo dentro de la infraestructura de las empresas, que tienen herramientas de Firewall e Intrusion Prevention System (IPS) o Intrusion Detection System, por ejemplo, en trabajos remotos, los usuarios tienen menos mecanismos de protección, porque cuando usan su equipo personal son más susceptibles a los ataques cibernéticos al acceder a datos e información confidencial de las empresas.

En el escenario actual, hay una multiplicación de los ciberataques, según los estudios realizados por el WEF[19], debido a la mayor dependencia de las personas de una infraestructura digital asociada con el mayor tiempo de uso de herramientas digitales, así como

[19] Disponível em https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cyber security/. Acesso em 16.05.2020.

al hecho de que el cibercrimen explota el miedo e inseguridad humana, lo que lleva a los usuarios a ser más susceptibles al acceder a links y download baja seguridad.

Este es un escenario nuevo y adverso, que ha impuesto el aislamiento social y, en muchos lugares, medidas extremas como el bloqueo, lo que contribuye a una transformación digital acelerada de las empresas, no solo con la institución de la oficina en casa, sino también, con el uso de nuevas herramientas tecnológicas, para las cuales aún se desconocen las vulnerabilidades de seguridad cibernética, lo que hace que la protección de datos sea una tarea desafiante y urgente.

La llamada transformación digital ahora tiene una intensa experiencia y, una vez que se ha verificado su eficacia, puede resultar ser un camino sin retorno al mundo corporativo, que requiere que las empresas tengan planes e inversiones consistentes para crear entornos, procesos y personas capacitadas. También es irreversible la dependencia que las empresas tendrán de los Sistemas de Información (SI) y la Seguridad de la Información (SegInfo), en la gestión de sus actividades comerciales (Weske, 2007) y para mitigar los riesgos derivados de esta transformación digital.

De acuerdo con Sêmola et al. (2003), el riesgo para las empresas será mayor cuanto más salgan las actividades desarrolladas del perímetro interno de las empresas, con un aumento en el uso de herramientas que facilitan los ataques e invasiones, asociado con un crecimiento exponencial en el intercambio de información por parte de los empleados.

Con el cambio en las relaciones laborales impuesto por la pandemia del Covid-19, algunas compañías estaban mejor preparadas para la implementación a gran escala de la oficina en casa y ya tenían la infraestructura adecuada, que solo requiere una expansión de esta infraestructura y / o enlaces de acceso a todos los empleados. Sin embargo, otras compañías se encontraron incapaces de hacer posible esa conectividad, permitiendo así el acceso a través de los dispositivos personales de los empleados con el objetivo de que las compañías no se vieran obligadas a detener las actividades por completo, lo que es extremadamente dañino.

Todas las empresas, con más o menos estructura, tuvieron que correr riesgos, cada una en su propio grado. Y, después de unos meses de pandemia, muchos vieron este modelo de trabajo como un viaje sin retorno, y ya se están preparando para una situación más duradera como resultado de un nuevo modelo de trabajo efectivo y productivo.

Después de la primera etapa, que se centró en mantener a las personas seguras y mantener los negocios en funcionamiento, en un segundo paso, las empresas comenzaron a mapear las vulnerabilidades y esbozar planes de acción, minimizando[20] los riesgos en la medida en que estén dispuestos a aceptarlos.

Independientemente del modelo adoptado, a corto o largo plazo, las empresas no pueden ignorar el hecho de que el riesgo actual es mayor que el riesgo al que estaban

[20] De acuerdo con la definición del Instituto Nacional de Estándares y Tecnología (NIST), el riesgo se traduce en la probabilidad de que una fuente de amenaza o una vulnerabilidad potencial cause un evento inesperado y resulte en un impacto adverso para la compañía. Disponible www.nist.gov. Acesso em 16.05.2020.

sujetas antes de la pandemia. Varios organismos de monitoreo en todo el mundo han indicado un aumento considerable en phishing[21] y fraude en este período.

Esto se combina con empleados poco capacitados, procesos frágiles y entornos tecnológicos defectuosos, formando un entorno perfecto para el fraude y el aumento exponencial del riesgo de ataques cibernéticos.

Hay, repetimos, ya muchas compañías que están muy bien preparadas para el uso del sistema llamado oficina en casa, con un sistema de seguridad cibernética muy cercano, si no idéntico, a lo que tenían en su propio entorno. Es evidente que, perpetuando la oficina en el hogar, incluso si esto no significa que todas las compañías lo elijan o lo elegirán de tal manera que abandonen por completo el modelo que hasta hace poco conocíamos, ciertamente habrá una mejora en los sistemas de seguridad. vinculado a los riesgos cibernéticos.

Pero incluso las grandes corporaciones tienen compañías más pequeñas que les prestan servicios, y es de esperar de estos proveedores que sea más difícil estar siempre, pari passu, protegidos frente el avance de los delitos cibernéticos.

5. REFERENCIAS

Bontis, N. *Assessing knowledge assets: a review of the models used to measure intelectual capital*. Working paper, Queen's Managemente Research Centre for Knowledge-Based Enterproses. 2000.

BRASIL. Lei 10.406, de 10 de janeiro de 2020. Código Civil, 2002, disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

BRASIL. Lei 12.737, de 30 de novembro de 2012, Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRASIL. Lei 12.965, de 23 de abril de 2014. Marco Civil da Internet, 2014, Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGDP), 2018, Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Edvinsson, L.; Malone, M. S.S. *Capital intelectual: descobrindo o valor real de sua empresa pela identificação de seus valores interiores*. São Paulo: Makron Books, 1998.

Lev, B. *Intangibles: management, seasurement and reporting.* Brookings Institution Press, Washington, D.C. 2001.

Petersen, Luiza Moreira. *O risco no contrato de seguro.* São Paulo: Roncarati. 2018.

Schiavo, Carlos A. *Contrato de seguro–Reticencia y agravación del riesgo.* Buenos Aires: Hammurabi, 2006.

[21] Es un tipo de fraude con el objetivo de "pescar" información de los usuarios, como datos personales o contraseñas, que generalmente llegan a través de mensajes de correo electrónico y redes sociales, y también pueden contaminar el dispositivo electrónico con un virus o un malware.

Schnorrenberger, D. *O alvorecer do capital intelectual.* Revista Brasileira de Contabilidade– RBC, N. 139: Janeiro-Fevereiro, 2003.

Signorino Barbat, Andrea. *Estudios de Derecho de Seguros y Reaseguros – La Ley Uruguay.* Montevideo: Ituzaingó, 2016.

Weske, M. *Concepts, Languages, Architectures.* V. 14. Springer, 2007.