

**UNIVERSIDAD EXTERNADO DE COLOMBIA**

**FACULTAD DE DERECHO**

**MAESTRÍA EN DERECHO PRIVADO, PERSONA Y SOCIEDAD CON  
ÉNFASIS EN CONTRATACIÓN CONTEMPORÁNEA**

<b>Rector:</b>	<b>Dr. Juan Carlos Henao</b>
<b>Secretaria General: Dra.</b>	<b>Martha Hinestrosa Rey</b>
<b>Decana Facultad de Derecho:</b>	<b>Dra. Adriana Zapata Giraldo</b>
<b>Director de Departamento de Derecho Civil:</b>	<b>Dr. Felipe Navia Arroyo</b>
<b>Director de Tesis:</b>	<b>Dr. Luis Carlos Sánchez Hernández</b>
<b>Presidente de Tesis:</b>	<b>Dr. Felipe Navia Arroyo</b>
<b>Examinador:</b>	

**FELIPE ANDRÉS CASTILLO DÍAZ**

**Contrato de seguro para riesgos cibernéticos: análisis de la cobertura de  
responsabilidad civil por violación de datos personales**

**Bogotá D.C.  
2.020**

## Contenido

1. RIESGOS CIBERNÉTICOS: CONTEXTO, TIPOS Y TAXONOMÍA DEL CONTRATO DE SEGURO DE RIESGOS CIBERNÉTICOS .....	4
1.1. El contexto de los riesgos cibernéticos.....	4
1.2. Tipología de riesgos cibernéticos.....	6
1.3. Taxonomía del contrato seguro de riesgos cibernéticos.....	9
1.4. Partes del contrato de seguro de daños patrimoniales que amparan riesgos cibernéticos.....	12
1.5. Beneficiarios en el contrato de seguro de daños patrimoniales que amparan riesgos cibernéticos: .....	14
2. RESPONSABILIDAD POR VIOLACIÓN DEL <i>HABEAS DATA</i> .....	15
2.1. Derecho fundamental de <i>habeas data</i> . .....	15
2.2. Problemática de la reclamación por violación del <i>habeas data</i> .....	19
2.3. ¿Cobertura para daños extrapatrimoniales? .....	21
3. COBERTURA PARA PROTECCIÓN DE DATOS PERSONALES QUE OFRECE EL SECTOR ASEGURADOR EN COLOMBIA.....	26
3.1. Análisis Comparativo de Pólizas del Sector Asegurador en Colombia.....	26
3.2. Condiciones para el aseguramiento de riesgos cibernéticos.....	27
CONCLUSIONES .....	28
BIBLIOGRAFÍA.....	29
ANEXO A. ANÁLISIS DE TENDENCIAS INVESTIGATIVAS ASOCIADAS A LOS CIBERSEGUROS .....	33
ANEXO B. ANÁLISIS DE PÓLIZAS DE RIESGOS CIBERNÉTICOS EN COLOMBIA .....	42

# Contrato de seguro para riesgos cibernéticos: análisis de la cobertura de responsabilidad civil por violación de datos personales

Cyber risks insurance: analysis of liability coverage for privacy violation

**Autor: Felipe Andrés Castillo Díaz<sup>1</sup>**

Director: Dr. Luis Carlos Sánchez Hernández

**RESUMEN.** En el contexto internacional, los riesgos cibernéticos han venido creciendo de manera significativa por cuenta de las nuevas tecnologías. Conforme a ello, la industria aseguradora ha construido un contrato de seguro para enfrentar las amenazas que supone la incorporación de diferentes empresas en el ciberespacio. A pesar de la relevancia de este tipo de contratos, se encuentra que el estudio de este tema aún es incipiente y fragmentado y que se requieren más estudios con el fin de determinar su viabilidad como mecanismo de transferencia del riesgo. En consecuencia, esta investigación tiene como propósito profundizar en el entendimiento del contexto de esta materia, abordar su proyección en relación con el *habeas data* y con los daños cubiertos; y, finalmente, analizar la cobertura de protección de datos personales en el sector asegurador de Colombia.

**PALABRAS CLAVE:** Contrato de Seguro, Riesgos Cibernéticos, Responsabilidad Civil, *Habeas Data*, Daños Extrapatrimoniales.

**ABSTRACT.** In the world today, there exists an increase of cyber risks as new technologies are introduced. As such, the insurance industry is incorporating a cyber risk policy for those companies seeking protection in the cyber world. Despite the relevance of these types of contracts push, the study indicates that we are still at its infancy with a fragmented view. Therefore, there is a need to continue the study to determine viable mechanism to manage this kind of risk. The research aims to deepen the understanding and context of this subject and address its relationship with privacy laws, damages, others effects. Finally, an analysis will be made on the coverage of civil liability for the violation of privacy in the Colombian insurance sector.

**KEYWORDS:** Insurance Policy, Cyber Risks, Liability, Privacy, Non-economic Losses.

**SUMARIO.** Introducción. 1. Riesgos cibernéticos: contexto, tipos y taxonomía del contrato de seguro de riesgos cibernéticos. 2. Responsabilidad por violación del *habeas*

---

<sup>1</sup> Abogado [Universidad Autónoma de Bucaramanga]. Especialista en Seguros y Seguridad Social [Universidad de la Sabana]. Estudiante de la Maestría en Derecho Privado, Persona y Sociedad con énfasis en Contratación Contemporánea [Universidad Externado de Colombia].

*data*. 3. El contrato de riesgos cibernéticos en Colombia y su cobertura de datos personales. Conclusiones y Referencias.

## INTRODUCCIÓN

En el año 2.004, en una entrevista concedida por el filósofo Italiano, GIORGIO AGAMBEN, al *German Law Journal*, se le inquirió sobre el incremento en la regulación en materia cibernética y su relación con la sensación de seguridad que tenían los ciudadanos, para utilizar los dispositivos asociados a este ámbito denominado ciberespacio. En torno a esta dicotomía, el filósofo expresó que en el campo cibernético es perfectamente viable la coexistencia de dos elementos, a saber: por un lado, la anomía y el desorden, y de otro lado, la existencia al máximo de regulación sobre la materia<sup>2</sup>.

Bajo este contexto, es posible afirmar que el ciberespacio es una esfera que captura la tensión en la era contemporánea entre dos elementos que confluyen en él y, por lo tanto, habrá lugar a la protección de los ciudadanos frente a las amenazas que surgen en la interacción en este medio. Es así, como las empresas enfrentan diferentes amenazas y vulnerabilidades en su infraestructura informática, que generan daños propios y responsabilidad civil frente a terceros. La posibilidad de que estas amenazas ocurran se denominan riesgos cibernéticos.

El estudio de los riesgos cibernéticos se considera un campo de conocimiento creciente, desde la perspectiva teórica y práctica, justificado en los impactos que trae consigo la ocurrencia de estos incidentes para las organizaciones en términos de pérdidas económicas relacionadas con su reputación y pérdida de mercado<sup>3</sup>. La relevancia del tema se explica desde la perspectiva práctica en relación con el incremento de ataques cibernéticos, donde tan sólo en un informe realizado por Cibercrimen *ThreatMetrix*, se identificó a América Latina como un foco para el fraude en la creación de cuentas, con alrededor del 20% del volumen total frente a un promedio de la industria del 12,2%.<sup>4</sup>; y que, según lo afirma ELING<sup>5</sup>, el futuro de los modelos de negocio implicará el incremento en la generación de riesgos cibernéticos. Sin embargo, a pesar de la relevancia de la temática, aún se encuentra la necesidad de abordar estudios desde la perspectiva jurídica que se orienten a analizar el contrato de seguro como mecanismo de transferencia de los riesgos cibernéticos, evidenciando que los pocos estudios publicados sobre el tema tienen la característica de abordar múltiples metodologías<sup>6</sup>, dificultando su comparabilidad y fragmentando el campo de conocimiento.

En la práctica, se evidencia que las organizaciones presentan retos asociados a la preparación para administrar de manera adecuada los riesgos inherentes a sus transacciones en el ciberespacio, acompañados de un desconocimiento de las leyes de privacidad de los

---

<sup>2</sup> RAULFF, U., 2004. *An Interview with Giorgio Agamben*. *German Law Journal*, vol. 5, no. 5, pp. 609–614. DOI 10.1017/S2071832200012724.

<sup>3</sup> MAROTTA, Angelica, et al. Cyber-insurance survey. *Computer Science Review*, 2017, vol. 24, p. 35-61.

<sup>4</sup> Informe de amenaza de Cibercrimen de Metrix: una entrevista (noviembre de 2019); disponible en <https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/>.

<sup>5</sup> ELING, Martin. *Cyber risk and cyber risk insurance: status quo and future research*. 2018, p. 39

<sup>6</sup> *Ibíd.*

datos personales<sup>7</sup> y de la asimetría de la información que existe entre las organizaciones y el mercado asegurador, donde se presenta tanto desconocimiento de las coberturas que ofertan los contratos de seguro, como desconocimiento frente a los comportamientos y riesgos que afrontan las diferentes industrias. Al respecto, se destaca que a pesar de que esta problemática ha sido abordada con especial profundidad en Estados Unidos, en Japón y en algunos países de Europa; en Latinoamérica y específicamente en Colombia, se encuentra que la literatura sobre el tema aún es incipiente<sup>8</sup>. Haciéndose necesario, establecer criterios de evaluación para facilitar la incorporación del mecanismo del contrato de seguro en la estrategia de protección patrimonial de las organizaciones y en general de los ciudadanos.

Considerando los planteamientos anteriores, esta investigación tiene como objetivo responder a la siguiente pregunta de investigación: ¿Cuáles son las condiciones del Contrato de Seguro en el ámbito de la Responsabilidad Civil, en materia de riesgos cibernéticos, que garantizan una reparación integral de los daños sufridos por los beneficiarios?, para dar respuesta a este cuestionamiento, se seguirán tres objetivos de investigación: i) se profundizará en el entendimiento de los riesgos cibernéticos y en la identificación de sus tipos; ii) se profundizará en la responsabilidad por violación del *habeas data*; y por último, iii) se analizará la cobertura para protección de datos personales que ofrece el sector asegurador en Colombia.

---

<sup>7</sup> TALESH, Shauhin A. *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers” for Businesses*. *Law & Social Inquiry*, 2018, vol. 43, no 2, p. 417-440.

<sup>8</sup> SOBRINO, Waldo. *Cyber Risk Insurance Law (New Developments Upon May 12, 2017 Global Cyber-Attack)*. *Revista Ibero-Latinoamericana de Seguros*, 2017, vol. 26, no 47.

# 1. RIESGOS CIBERNÉTICOS: CONTEXTO, TIPOS Y TAXONOMÍA DEL CONTRATO DE SEGURO DE RIESGOS CIBERNÉTICOS

## 1.1. El contexto de los riesgos cibernéticos

Al realizar una aproximación al concepto de riesgos cibernéticos (Ver Anexo A), debemos advertir que no hay un concepto unívoco de todos los incidentes de seguridad que lo constituyen, ni tampoco es el propósito de este escrito definir cada uno de ellos. Sin embargo, siguiendo los ámbitos en donde se materializan, según KOSSEF<sup>9</sup>, podemos simplificar que los riesgos cibernéticos se enmarcan dentro de la categoría de ciberseguridad y, en términos generales, los mismos se relacionan con los siguientes ámbitos:

- Regulación de Ciberseguridad<sup>10</sup>.
- Leyes Anti – Hacking<sup>11</sup>.
- Vigilancia y control de las entidades gubernamentales<sup>12</sup>.
- Protección de datos personales<sup>13</sup>.

Conceptualizado sus ámbitos de aplicación y para el propósito de abordar el tópico de investigación, podemos decir que en materia de riesgos cibernéticos las organizaciones enfrentan diferentes amenazas a la seguridad de su información, entre las que se encuentran:

- **Evento de seguridad de la información:** “presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad”<sup>14</sup>.

---

<sup>9</sup> KOSSEFF, Jeff. *Cybersecurity law*. John Wiley & Sons, 2017.

<sup>10</sup> En Colombia mediante el CONPES No. 3701 de 14 de julio de 2011, el Consejo Nacional de Política Económica y Social, del Departamento Nacional de Planeación se adoptaron, a saber: “LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA”, disponible en <https://www.mintic.gov.co/portal/604/w3-article-3510.html>.

<sup>11</sup> Ver Ley 1273 de 2009 “por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

<sup>12</sup> En Colombia el Ministerio de Defensa creó el COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), el cual está conformando por un equipo de personas dedicadas a la gestión de incidente con el objetivo de mitigar el riesgo y dar respuesta a incidentes de tipo cibernético.

<sup>13</sup> Según la Ley 1581 de 2012, en su artículo 21, la Superintendencia de Industria y Comercio en materia de datos personales cuenta con la facultad, entre otras, a saber: “Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.”

<sup>14</sup> Definición tomada de ISO/IEC 27000:2009, citada en la Guía Técnica Colombiana, GTC- ISO27035, expedida por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), página 3.

- **Incidente de seguridad:** “evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información”<sup>15</sup>.
- **Ataques cibernéticos:** entre los ataques más frecuentes se encuentran la denegación de servicio (estos ataques se realizan con frecuencia por medio de *botnets*, un grupo de robots de software (códigos maliciosos) que funcionan en forma autónoma y automática) y hacen que un sistema, servicio o red dejen de operar a su capacidad prevista; acceso no autorizado (ataques por desbordamiento de búfer para obtener acceso a un objetivo privilegiado a un objetivo (por ejemplo administrador del sistema); códigos maliciosos identifican un programa o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, destrucción de información y recursos, correo de basura, etcétera<sup>16</sup>.
- **Recolección de información:** en términos generales, la categoría de incidentes de recolección de información incluye las actividades asociadas con la identificación de objetivos potenciales y la comprensión de los servicios que funcionan en dichos objetivos, por ejemplo, el escaneo de los puertos de red disponibles en un sistema para identificar los servicios relacionados (por ejemplo, correo electrónico, FTP, Web, etc.) y la versión del software de estos servicios<sup>17</sup>.

Este estudio no se detendrá en la significación y tipificación de cada uno de los riesgos antes enunciados, por cuanto esta materia escapa a la órbita del derecho y pertenece a otros campos de investigación como la ciberseguridad y la ingeniería de sistemas. Desde la perspectiva jurídica, lo que sí resulta relevante es comprender, en el campo práctico, cómo los empresarios enfrentan amenazas a la seguridad de su información, siendo una prioridad la protección de sus activos de información, según su nivel de exposición o vulnerabilidad, pues éstos son agentes generadores de responsabilidad civil y, por consiguiente, llamados a responder integralmente a las presuntas víctimas con ocasión de los siniestros que estén amparados debidamente en un contrato de seguro. Por ello es relevante fijar un marco de referencia, determinando el riesgo asegurable como uno de los elementos esenciales para la existencia del contrato de seguro de acuerdo con la legislación colombiana, al tenor del artículo 1045 del Código de Comercio<sup>18</sup>.

Para ilustrar con mayor claridad la relevancia de la asegurabilidad del riesgo en materia de ciberseguros, podemos referirnos al caso de Target<sup>19</sup>, cuya ocurrencia pone en evidencia la fuga de información generada en una de las cadenas de supermercado más grandes de los Estados Unidos<sup>20</sup>, cuando un grupo de hackers denominado *Rescator* logró, a través de los

<sup>15</sup> *Ibíd.*

<sup>16</sup> *Ibíd.*, ver anexo informativo B.

<sup>17</sup> *Ibíd.*

<sup>18</sup> Artículo 1045: Son elementos esenciales del contrato de seguro: 1) El interés asegurable; **2) El riesgo asegurable**; 3) La prima o precio del seguro, y 4) La obligación condicional del asegurador. En defecto de cualquiera de estos elementos, **el contrato de seguro no producirá efecto alguno.** (La negrilla es nuestra).

<sup>19</sup> Existen otros casos que han sido relevantes para el estudio de riesgos cibernéticos, por ejemplo, el caso de las consolas de *Play Station*. BAILEY, Liam. *Mitigating moral hazard in cyber-risk insurance*. JL & Cyber Warfare, 2014, vol. 3, p. 1.

<sup>20</sup> COBURN, Andrew; LEVERETT, Eireann; WOO, Gordon. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2018. Páginas 3 - 7

permisos que tenía un proveedor autorizado, vulnerar la seguridad de sus sistemas informáticos, generando de esta forma miles de reclamaciones ante sus clientes y entidades financieras. Reclamaciones explicadas en que, debido a fallas en los protocolos de seguridad, se permitió el robo de información bancaria, lo que a la postre se tradujo en un siniestro cuantificado en 200 millones de dólares americanos relacionados con pérdidas económicas, reputacionales y de mercado.

Conforme a lo anterior, consideramos que es necesaria la aproximación del empresario a este tipo de incidentes de seguridad de la información, para que, una vez conocida su exposición a los mismos, defina una adecuada administración del riesgo a efectos de controlarlo o mitigarlo. De esta forma, cobra relevancia adentrarnos en el campo de uno de los mecanismos que ha diseñado el sector asegurador para transferir los riesgos de este estilo, identificando su oportunidad, idoneidad y garantía.

Como lo veremos a continuación, y para efectos prácticos de este estudio, haremos mención a la tipología de los riesgos que están inmersos en las pólizas de responsabilidad civil por riesgos cibernéticos.

## **1.2. Tipología de riesgos cibernéticos.**

Sea lo primero profundizar en la razón por la cual la industria aseguradora ha ido generando un contrato específico y especial para amparar los riesgos cibernéticos, y no ha señalado que los mismos son susceptibles de cobertura a través de un contrato de responsabilidad civil general, basado en la cobertura general de predios, labores y operaciones<sup>21</sup>.

Sobre el particular, consideramos que el sector asegurador no ha sido ajeno al influjo que ejerce la tecnología en los modelos de negocio, conduciendo a un análisis de determinadas políticas de prevención tendientes a evitar o mitigar los efectos de los incidentes de seguridad en campos como la medicina<sup>22</sup> o el sector financiero<sup>23</sup>, entre otros. En ese sentido, si pudiéramos llamarlo así, se ha ido especializando en la construcción de clausulados de condiciones generales diseñados para la protección del expediente clínico electrónico o del aseguramiento de los canales de pagos virtuales que utilizan las diferentes entidades financieras.

Una de las razones que podría influir en esta construcción propia y autónoma, puede estar referida a normas técnicas de auditoría para el desarrollo de una actividad especializada, susceptible de ser vulnerada. Es el caso, por ejemplo, de la construcción de la “Norma PCI

---

<sup>21</sup> Según la definición de Colombia compra eficiente: Bajo este amparo se otorga cobertura a los daños que se le causen a terceros como consecuencia de la actividad del contratista por: i) la posesión, el uso y el mantenimiento de los predios en los que ejecuta el contrato, ii) las labores y operaciones del contratista relativas a la ejecución del contrato. Disponible en línea: <https://www.colombiacompra.gov.co/content/en-que-consiste-el-amparocobertura-de-predios-labores-y-operaciones>. Fecha de consulta: 16/09/2019.

<sup>22</sup> SIGNORINO, Andrea Barbat. Visión Jurídica sobre privacidad, confidencialidad y protección en el expediente clínico electrónico. IV congreso de nuevas tecnologías La influencia de internet, genética y nanotecnología en la medicina y el seguro. Universidad Externado de Colombia, 2015.

<sup>23</sup> PAZ, Antonio. “La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico”, Revista de Derecho Privado, Universidad Externado de Colombia, n. ° 35, julio-diciembre de 2018, 261-289.

– DSS<sup>24</sup>, establecida como estándar internacional para prevenir la ocurrencia de fraudes relacionados con tarjetas de crédito.

Otra razón que podría servir para la edificación de un ámbito propio de estas pólizas, está vinculado a la necesidad de que el tomador de la póliza profundice en las coberturas que requiere según el tipo de riesgo que desea asegurar. Así, por ejemplo, si el empresario realiza encuestas para fines comerciales o electorales, procurará que sus bases de datos estén debidamente protegidas frente a las brechas o fugas de los datos de las personas que son encuestadas dentro del giro ordinario de su negocio, para un período determinado y con una finalidad específica<sup>25</sup>.

En términos generales, se puede indicar que el sector asegurador ha diseñado coberturas especializadas en proteger los intereses y costos directos que tendría que asumir el empresario en caso de ver afectado su patrimonio. Estas coberturas abarcan: las notificaciones que debe realizar al público en general cuando sufra un ataque cibernético conforme a su política de privacidad, la auditoría forense para determinar las causas del siniestro, el manejo económico de las crisis, el restablecimiento de sus sistemas operativos, entre otras pérdidas económicas relativas al lucro cesante y daño emergente, como consecuencia de la interrupción de su negocio.

La literatura ha entendido que los riesgos anteriormente descritos pueden clasificarse como de primera persona, entendidos como aquellos daños y perjuicios que son causados directamente al patrimonio del empresario. No obstante, y paralelo a ello, surgen otro tipo de daños que afectan a terceros, referidos esencialmente a las violaciones de privacidad, robo de la identidad personal con fines de fraudes electrónicos, derechos de autor y propiedad industrial (secretos empresariales, patentes, obras literarias), entre otros. Estos últimos han sido denominados daños sufridos por terceros, los cuáles se traducen en la posibilidad de que el empresario sea llamado a juicio de responsabilidad frente a terceros, como consecuencia de las reclamaciones elevadas por las víctimas.

Ante la diversidad de riesgos que han de ubicarse dentro de la especialidad de cibernéticos y con el fin de clasificarlos para introducirlos en las pólizas, conviene mencionar la metodología que ha sido propuesta por el *Chief Risk Officers Forum*<sup>26</sup> (*CRO Forum*), según la cual, para aproximarse a la taxonomía de estos riesgos, es necesario entender el proceso de su formación, basado en dos etapas, a saber: (i) lo que interesa para la suscripción del seguro; (ii) lo necesario para la emisión del seguro. En el primer ámbito, debe identificarse el incidente cibernético, el tipo de evento, las causas que dieron origen a su ocurrencia y su actor. Esto permitirá al asegurador, en la etapa subsiguiente, determinar el tipo de impacto, su descubrimiento, cobertura y reclamación. El resultado de lo descrito, será lo que se

---

<sup>24</sup> Sus siglas en Inglés “*Payment Card Industry Data Security Standards*”.

<sup>25</sup> Estos ámbitos sin desconocer los riesgos que genera el comercio electrónico. Para mayor información: “Pero lo cierto es que tal sentimiento de desconfianza parece justificarse en un ambiente de inseguridad informática, donde aparecen constantes fenómenos como la fuga de información, la suplantación de identidad y la publicidad engañosa, entre otras.”. PEÑA, Daniel Peña Valenzuela. *La protección del consumidor en el comercio electrónico*. ROJAS, Carmen Ligia Valderrama (ed.). *Perspectivas del derecho del consumo*. U. Externado de Colombia, 2013, página 466.

<sup>26</sup> CRO FORUM, 2014. *The cyber risk challenge and the role of insurance*, p. 23. DOI: <https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf>.

conoce en el mundo asegurador como riesgo asegurable, susceptible de ser transferido por el tomador de la póliza.

En ese mismo sentido, *CRO Forum* ha efectuado un extenso análisis para codificar<sup>27</sup> los riesgos cibernéticos, agrupándolos en cuatro categorías principales, sobre las cuáles se pueden dar los siguientes ejemplos:

**a. Mal funcionamiento del sistema:** ocurre cuando un hacker toma el control de un computador del sistema o la red y a través de ese canal lleva a cabo actividades ilícitas en contra de un tercero. Esto puede ser ejecutado a través de un *DoS* o un *Botnet*, según lo hemos expuesto en el acápite que antecede. Este evento se denomina en Inglés como “*Inadvertent disruption of third-party system*”.

**b. Confidencialidad de datos:** un sujeto (compañía o persona) detecta que los datos de otra persona están siendo almacenados o procesados por fuera de su sistema o red (perímetro). Por ejemplo, percibe que los datos personales del tercero están siendo vendidos, tratados o expuestos en la *Deep web*. Este tipo de incidente se denomina “*Theft of third party data*”.

**c. Integridad y disponibilidad de los datos:** un sujeto (compañía o persona) detecta que los datos de otra persona están siendo almacenados o procesados tergiversados. Usualmente es difícil detectar los cambios porque son pequeños y puede tardarse mucho tiempo en la detección de los cambios. Este tipo de incidente se denomina en Inglés “*Corruption of third party data*”.

**d. Actividad maliciosa:** un *hacker* inicia una transferencia de dinero haciendo mal uso de unas credenciales y actuando como el sujeto (víctima) en un sistema determinado. Normalmente esta conducta es denominada “Cyber Fraud” o “Cyber theft”.

Descrito, *a grosso modo*, las categorías que agrupan a cada uno de los riesgos cibernéticos, conviene centrarnos, para los efectos de la presente investigación, en aquellos incidentes de seguridad relacionados con los daños y perjuicios causados a terceros, para determinar si aquellos tienen derecho a reclamar una indemnización por parte del asegurador en caso de que se configuren siniestros atribuidos al tomador - asegurado, con ocasión de un evento que altere las condiciones de seguridad y permita la fuga de información de sus bases de datos.

Corolario de lo anterior y antes de abordar el siguiente acápite, cuyo contenido se ocupará de analizar la incorporación de los impactos de estos riesgos en el contrato de seguro, debe desarrollarse unas condiciones de asegurabilidad, tendiente a definir una adecuada transferencia de riesgos.

Para ello, el *National Institute of Standards and Technology Cybersecurity Framework* (“*NIST framework*”) ha diseñado una guía que contiene los parámetros necesarios para definir las evaluaciones y mejoras en los sistemas y redes cibernéticas que las

---

<sup>27</sup> CRO FORUM, 2016. *CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk, Annex – Detailed cyber incident type and descriptions*. p. 25.

organizaciones deben realizar para protegerse frente a los riesgos cibernéticos. Con ello se busca que el empresario sea capaz de desarrollar posibles escenarios y así identifique las posibles amenazas y vulnerabilidades que tiene su infraestructura informática. Basado en lo anterior, la propuesta del ente mencionado, ha considerado que en las empresas privadas deben implementar su sistema de ciberseguridad contemplando un marco de referencia que desarrolle la identificación, la protección, la detección, la respuesta y la recuperación<sup>28</sup>.

Sin pretender desarrollar cada una de las etapas mencionadas, es importante indicar que para el contrato de seguro estas etapas tendrán que ser analizadas en dos momentos esenciales. El primero está referido a la suscripción del contrato de seguro, en el cual habrá de tenerse en cuenta si la empresa tiene políticas y prácticas seguras en el tratamiento de datos personales, tarjetas de créditos y general sus activos informáticos y, en caso de tenerlos implementados, observar con detenimiento su exposición al riesgo, basado en la modelación de posibles escenarios para conocer el monto estimado de sus pérdidas económicas y así pueda suscribir el seguro. Esta fase impone, sin duda, una carga al empresario *ex ante* de la celebración del contrato.

De otro lado, conviene que el empresario efectúe un análisis con base en unos deberes *post siniestrales*, es decir, adentrándose en las etapas de respuesta y recuperación, allí juega un rol capital la capacidad que tiene el empresario para hacer frente y superar el impacto de un ataque cibernético. En estas fases se exige de él una implementación adecuada de los planes de emergencia frente a la contingencia, logrando de esta manera detener la propagación y las consecuencias negativas del evento de ciberseguridad, además de identificar en el menor tiempo posible las causas que dieron origen al ataque para solucionarlas, protegerse de nuevos ataques similares y dando aviso oportuno a su asegurador, para detener el crecimiento de sus pérdidas económicas, notificaciones a las víctimas y, en fin, todas las medidas tendientes a recuperar sus sistemas y redes de infraestructura.

### **1.3. Taxonomía del contrato seguro de riesgos cibernéticos**

Según lo dispuesto por la clasificación que realiza el Código de Comercio colombiano en el artículo 1082, podríamos señalar que el contrato de seguros asociado al cubrimiento de riesgos cibernéticos se subsume dentro de la categoría de seguros de daños patrimoniales, específicamente en la materia relacionada con el ramo de la responsabilidad civil.

De acuerdo con lo anterior, y siguiendo al tratadista ORDÓÑEZ<sup>29</sup>, es necesario advertir que “cuando se trate de seguros patrimoniales, el valor asegurado no se da en estricto sentido con referencia a un valor real del interés asegurado; viene a representar simplemente una suma de dinero hipotética que representa el máximo compromiso del asegurador frente a una eventual pérdida económica del asegurado en caso de siniestro, bajo la forma del nacimiento de una deuda o la desaparición de un ingreso, o ambos”.

---

<sup>28</sup> EGAN, R., CARTAGENA, S., MOHAMED, R., GOSRANI, V., GREWAL, J., ACHARYYA, M., DEE, A., BAJAJ, R., JAEGER, V.-J., KATZ, D., MEGHEN, P., SILLEY, M., NASSER-PROBERT, S., PIKINSKA, J., RUBIN, R. and ANG, K., 2019. *Cyber operational risk scenarios for insurance companies*. *British Actuarial Journal*, vol. 24, pp. e6. DOI 10.1017/S1357321718000284.

<sup>29</sup> ORDÓÑEZ, A. *Estudios de seguros*. Universidad Externado de Colombia, 2012, “El carácter indemnizatorio del seguro de daños”, página 186.

Esta característica de los seguros de daños patrimoniales en materia de responsabilidad civil, trae consigo dos dificultades para el tomador de la póliza de *Cyber-Risk*, a saber:

a) Considerando que el ciberespacio podría tomar rumbos inesperados y desconocidos, el momento originario de la celebración del contrato de seguro, podría estar rodeado de unas circunstancias particulares, pero durante la vigencia de la póliza con ocasión de la identificación de un nuevo riesgo, la ejecución podría traer incidentes que no están bajo la cobertura del seguro, o que estando en su cobertura, el valor asegurado sea insuficiente frente al valor real del potencial riesgo. Por tal motivo, resulta de cardinal relevancia que el tomador del seguro, aun habiendo suscrito el contrato de riesgos cibernéticos, mantenga una constante revisión de los riesgos de su empresa, pudiendo mantener una dialéctica con el asegurador, para garantizar una transferencia adecuada del riesgo.

No hacerlo, además de defraudar los intereses del asegurado frente a una eventual reclamación, configura un incumplimiento al artículo 1060 del Código de Comercio, donde se establece la obligación de conservar el estado del riesgo y notificación de cambios, so pena de la terminación automática del contrato de seguro.

b) Otra característica que debe analizarse para la contratación de este seguro, es el cálculo del valor asegurado, por cuanto son contratos que no se vinculan con un bien determinado, como ocurriría con el contrato de daños reales, el tomador de la póliza debe estimar correctamente su máximo potencial de pérdidas, basado, por ejemplo, en un estudio probabilístico que permita identificar cuál sería su pérdida máxima probable<sup>30</sup>.

De otro lado, es oportuno señalar que un elemento común a las pólizas de riesgos cibernéticos, son las cláusulas denominadas *claims made*, cuyo contenido encuentran sustento en el artículo 4º de la Ley 389 de 1997<sup>31,32</sup>. Debe indicarse que los contratos de responsabilidad civil, que incluyen dentro de su texto este tipo de cláusulas, en el fondo modifican el siniestro por la ocurrencia del riesgo asegurado, al momento en el que se verifica la existencia de una reclamación, debiendo esta última ser formulada durante la vigencia de la póliza o dentro del plazo de extensión, según sea previsto en el contrato de seguro.

---

<sup>30</sup> Revista: Gerencia de Riesgos y Seguros. *Estimación de Pérdidas Máximas por siniestros. Utilidad para asegurados industriales*. Número. 115 - 2.013. Disponible en línea <http://www.mapfre.com/fundacion/html/revistas/gerencia/n115/docs/Estudio3.pdf>. Fecha de la consulta 15.09.2019.

<sup>31</sup> “Expedida la Ley 389 de 1997, que permite la estipulación legal de las denominadas Cláusulas *Claims Made*, las pólizas actualmente colocadas en el mercado, cubren los siniestros ocurridos durante la vigencia, siempre y cuando se reclamen como máximo dentro de los dos años posteriores a la expiración de la misma”. Ver: RODAS, F. ¿Es necesaria en Colombia la estipulación legal de un seguro obligatorio de responsabilidad civil que cubra el ejercicio de la actividad médica?. Responsabilidad Civil y del Estado, Tomo III/Ediciones 15 - 19, 2003, Responsabilidad Civil y del Estado N° 18. Instituto Colombiano de Responsabilidad Civil y del Estado, Pág. 494.

<sup>32</sup> Es importante diferenciar el tipo de cláusula *Claims Made* al respecto Andrés Villegas y Sergio Villegas señalan: “Siniestro como la reclamación (teoría de *claims made*) en cualquiera de sus modalidades, por ejemplo: *claims made* puro sin periodo de retroactividad, *claims made* puro con periodo de retroactividad, *claims made* con reporte durante el periodo de vigencia, *claims made* con cobertura especial a futuro para hechos notificados, *claims made* con periodo especial para notificaciones, sistema mixto entre ocurrencia y *claims made*, entre otras”. Ver: VILLEGAS, A. y VILLEGAS, S. La vía ejecutiva en el seguro de responsabilidad civil. Responsabilidad Civil y del Estado, Tomo V/Ediciones 25 - 28, 2003, Responsabilidad Civil y del Estado N° 25. Instituto Colombiano de Responsabilidad Civil y del Estado, Pág. 204.

Lo anterior, podría generar complicaciones en el asegurado, en relación con la expectativa de su indemnización, por cuanto éste podría tardarse en conocer las causas que ocasionaron el incidente de seguridad informática y, por tanto, quedar sin cobertura por la expiración de la póliza<sup>33</sup>.

Por otro lado, es relevante indicar que según el artículo 1099 del Código de Comercio no es posible que en caso de que el asegurador asuma el pago de los siniestros derivados de los incidentes de seguridad, debidamente amparados en la póliza, pueda éste subrogarse para reclamar en contra del tomador asegurado lo pagado, pues dentro de los seguros de daños en lo relativo a la responsabilidad civil, no es procedente la figura mencionada, salvo que se demuestre que el tomador asegurado actuó con culpa grave o dolo en el acaecimiento del hecho ilícito del siniestro generador de la responsabilidad<sup>34</sup>. En consecuencia, si el asegurador demuestra que la pérdida de información o vulneración a las bases de datos se produjo con complicidad del tomador asegurado, dicha cláusula de no subrogación no será aplicada al caso concreto, otorgándole a la aseguradora la posibilidad de perseguir al tomador asegurado, para que responda por daños y perjuicios causados a terceros.

Otra hipótesis que daría lugar a la acción subrogatoria del asegurador se refiere al hecho en que pueda identificar los responsables del ataque cibernético, es decir, descubra a los *hackers* o responsables de determinado delito cibernético, pues para este caso, una vez haya pagado la indemnización del seguro podrá repetir lo pagado en contra de los responsables del hecho ilícito.

Finalmente, es importante destacar que el contrato de seguro es un contrato de adhesión<sup>35</sup>, lo cual supone que el asegurador, en su condición de emisor de la póliza, ha sido quién ha predispuesto el contenido de las cláusulas del contrato, sin lugar a que el tomador intervenga en su definición. Además de esta característica, es necesario señalar que la adhesión está referida a la rigidez en las estipulaciones contractuales y la generalidad, máxime en el mundo asegurador, en donde la celebración del contrato, únicamente le corresponde al tomador – asegurado, diligenciar una declaración de asegurabilidad, un formulario y otros documento requeridos, pero su discrecionalidad se encuentra restringida y, por tanto, no cuenta con la posibilidad de modificar las condiciones generales del seguro.

---

<sup>33</sup> La Corte Suprema de Justicia de Colombia, al examinar la citada disposición, en la Sentencia CSJ SC, 18 dic. 2013, Magistrado Ponente, Ruth Marina Díaz Rueda, rad. 2000-01098-01, comentó: De conformidad con dicho precepto, pueden presentarse las siguientes situaciones: a.-) Que coincidan dentro de la vigencia tanto el hecho dañoso, como la reclamación de la víctima al asegurado o la aseguradora. b.-) Que el hecho dañoso sea anterior a la vigencia, pero el reclamo se presente dentro de ésta. c.-) Que se cubran sucesos acaecidos durante la vigencia, pero el reclamo se haga por fuera de la misma, en un plazo preestablecido para notificaciones. El primer caso es connatural al convenio, pero los otros dos requieren de pactos expresos, claramente delimitados, cuya interpretación exige del fallador un examen estricto y restringido, que impida extender los amparos a riesgos no cubiertos o dejar por fuera aquellos que sí lo están.

<sup>34</sup> ZORNOSA, Hilda Esperanza. *El Seguro de Responsabilidad Civil Su evolución Normativa y Jurisprudencial en Colombia*. Revista Ibero-Latinoamericana de seguros, 2011, vol. 20, no 35, páginas 132 y ss.

<sup>35</sup> LORENZETTI, citando López Cabana al respecto ha expuesto: que los contratos de adhesión reflejan las siguientes reglas: la necesidad de evitar condiciones generales “sorpresivas”, exigiendo que el no predisponente las conozca de manera efectiva si se hallan en instrumento separado; en caso de ambigüedad, la interpretación en contra del predisponente. LORENZETTI, Ricardo Luís. *Tratado de los contratos*. Tomo I. Página 45.

Con ello, debe prestarse especial atención a que en las condiciones generales no incluyan cláusulas abusivas o sorprendidas que suelen restringir los derechos del tomador – asegurado, tal como sería el caso de aquellas cláusulas que le impongan el deber al asegurado de demostrar el siniestro de determinada manera (tarifa)<sup>36</sup> o aquellas en las que el asegurador se reserva el derecho de revisar las condiciones de aseguramiento del siniestro, una vez ha ocurrido el mismo, entre otros ejemplos.

#### **1.4. Partes del contrato de seguro de daños patrimoniales que amparan riesgos cibernéticos.**

Para referirnos en los capítulos subsiguientes a la responsabilidad por la violación del derecho fundamental del *habeas data* y su asegurabilidad, es necesario detenernos en las partes y sus principales obligaciones del contrato patrimonial de responsabilidad civil.

En primer término, quien diseña y ofrece este tipo de pólizas en materia de riesgos cibernéticos y, por consiguiente, asume los riesgos, es denominado asegurador<sup>37</sup>, quien para ofrecer al público general este producto financiero, debe contar con una autorización previa por parte de Superintendencia Financiera<sup>38</sup>. Así, para el ejercicio de su objeto social, el asegurador, esencialmente, debe acreditar el respaldo patrimonial para pagar los siniestros, entre otros requisitos. Lo anterior, denota el interés público que tiene el Estado en la intervención de la actividad aseguradora, al punto que, para la emisión y colocación de estas pólizas en el mercado, exige la aprobación previa del clausulado de condiciones generales por parte de Superintendencia Financiera.

La obligación principal que asume el asegurador al momento de suscribir el contrato de seguro, consiste en reconocer al asegurado una indemnización por la ocurrencia de un siniestro debidamente amparado en la póliza. Igualmente, surgen otro tipo de obligaciones como lo son entregar al tomador, con fines probatorios, la póliza dentro de los quince días siguientes a la celebración del negocio y devolver al asegurado la prima no devengada cuando el contrato se termina, entre otros.

Es importante resaltar que al tenor del artículo 1110 del Código de Comercio, el asegurador tiene la facultad para pagar la indemnización no sólo en dinero, sino que también podrá indemnizar el siniestro reparando o reconstruyendo a su elección. Esta facultad del asegurador contempla una noción en sentido amplio del pago, pues permite al deudor responder por los siniestros a su cargo no solamente pagando en dinero, sino que, en determinado momento, le permite decidir indemnizar con el cumplimiento *in natura* de un contrato, o reconstruyendo el objeto que sufrió el daño.

---

<sup>36</sup> Al respecto la Corte Suprema de Justicia ha señalado: “En este sentido, la calificación de abusiva, leonina o vejatoria -entre otras denominaciones más enderezadas a relieves el resquebrajamiento o erosión de la justicia contractual- de una cláusula que, como la aquí colacionada, impone al asegurado o beneficiario la carga de probar su derecho de una manera específica -o tarifaria-, limitando por esta vía indebidamente los diversos medios de prueba a su disposición, en contra de la preceptiva legal imperante, responde, preponderantemente, al hecho de que ella socava el equilibrio prestacional que, en línea de principio, debe existir en todo contrato...”. CSJ, S. Civil, Sentencia del 2 de febrero de 2001, M.P. Carlos Ignacio Jaramillo Jaramillo.

<sup>37</sup> Artículo 1037 del Código de Comercio: “el asegurador es la persona jurídica que debidamente autorizada por la ley asume el riesgo”.

<sup>38</sup> Artículos 53 numeral 2) decreto 663 de 1.993 y 1º de la Ley 1510 de 1.999.6

La elección que reconoce la ley al asegurador, de decidir sin intervención del tomador o asegurado, ha sido cuestionada por la doctrina<sup>39</sup>, en materia de contratación Estatal, pues con ocasión de la reforma a dicho régimen, la entidad estatal puede exigir el cumplimiento del contrato al asegurador, cuando éste no cuenta con un objeto social que le permita ejecutar actividades relacionadas con una obra pública. No obstante, en materia de pólizas de riesgos cibernéticos, nos parece apropiado destacar esta facultad, pues bien podría el asegurador pagar los siniestros derivados del seguro a través de una investigación forense, la reparación de un sistema operativo de la víctima, entre otras opciones que podrían contribuir con la indemnización. En nuestra opinión, siempre será necesario precisar que las actividades accesorias, como sería la del caso de contratar una firma especializada para reparar un sistema informático, deben ser valoradas como un medio legítimo, para que, en el fondo, se repare los daños causados al asegurado o beneficio de la póliza.

Ahora bien, en el otro extremo de la relación contractual está el tomador de la póliza, quién decide, al momento de celebrar el contrato de seguro, transferir sus riesgos o los de un tercero. Para el caso de nuestra investigación, no sería otra persona distinta que el empresario, pues es él quien tiene interés en proteger su patrimonio, frente a posibles riesgos que involucra el tratamiento de datos personales de terceros en el ciberespacio. Podría advertirse que este sujeto conoce su actividad económica, y tiene no sólo el interés de transferir sus riesgos a un tercero, sino que también conoce a qué riesgos se encuentra expuesto su negocio y cómo se debe administrar en su sistema la ocurrencia de incidentes de seguridad.

En ese sentido, las obligaciones que emergen para este sujeto desde el campo del derecho comercial se encuentran relacionadas con los deberes de información – declarar sinceramente el estado del riesgo – y declarar su modificación en caso de agravación, así como asumir el pago de la prima, a cuya remuneración tiene derecho el asegurador, por la labor de asumir los riesgos. Vale la pena aclarar que el tomador puede ostentar al mismo tiempo otros dos roles el de asegurado y beneficiario del seguro. En ese sentido, ZORNOZA ha expuesto que: “En los seguros de daños casi siempre el titular del interés asegurable concluye el contrato y comparece, de manera directa o través de representante, tomador, asegurado y beneficiario son uno solo”<sup>40</sup>.

Por su parte, el asegurado es quién soporta los riesgos y puede ver afectado su patrimonio con ocasión de un siniestro, debidamente amparado en el contrato de seguro. Es decir, quien tiene el interés asegurable. Así mismo, sumadas a las obligaciones que hemos señalado, también el asegurado tiene deberes<sup>41</sup> que nacen después de ocurrido el siniestro, tales como 1097 y numeral 2 del artículo 1128 del Código de Comercio, según las cuales, no le es dable al asegurado renunciar en cualquier momento a los derechos que tenga contra

---

<sup>39</sup> ZORNOZA, Hilda Esperanza (ed.). *Escritos sobre riesgos y seguros*. U. Externado de Colombia, 2012. “*Las partes en el contrato de seguro*”, página 652, señala: “Pero, con ocasión a la reforma al régimen estatal, la doctrina discute si ahora la entidad estatal puede exigir del asegurador la continuación de la obra”.

<sup>40</sup> *Ibidem*.

<sup>41</sup> JARAMILLO, C. Derecho privado: estudios y escritos de derecho patrimonial: “Derecho de Obligaciones”. Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, 2013, Pág. 104. Grupo Editorial Ibáñez. Bogotá, Colombia. La doctrina ha dado a estas obligaciones la figura jurídica de carga, señalando así que el asegurado debe: “... abstenerse de realizar ciertas y determinadas conductas como la relativa a no gravar el estado del riesgo o a no efectuar transacción alguna con la víctima o sus derecho habientes en los seguros de responsabilidad civil extracontractual, sin perjuicio de la autorización del asegurador”

terceros responsables del siniestro o afrontar el proceso contra orden expresa del asegurador, respectivamente.

Por último, encontramos al beneficiario quien es la persona legitimada para reclamar o demandar del asegurador el pago de la indemnización. Al respecto, el mismo autor que hemos citado anteriormente, señala que: “En los seguros de daños no es frecuente encontrar beneficiarios distintos del mismo asegurado, pero bien puede ocurrir en el seguro de automóviles, en el de sustracción, o en los incendios y de manera general cuando las entidades financieras o las personas naturales conceden créditos para la adquisición de bienes muebles e inmuebles<sup>42</sup>”.

### **1.5. Beneficiarios en el contrato de seguro de daños patrimoniales que amparan riesgos cibernéticos:**

Para el caso de las pólizas de riesgos cibernéticos, cobra relevancia el rol del tercero como beneficiario, pues normalmente en las bases de datos del empresario se realiza el tratamiento de sus datos personales, siendo estos clientes, proveedores, empleados y demás personas que intervienen en su actividad económica. Por ello, podemos advertir que pueden existir terceros diferentes al tomador y asegurado, quienes podrían eventualmente reclamar al asegurado el pago de una indemnización por la vulneración a sus datos personales.

En Colombia, con la reforma que trajo consigo la Ley 45 de 1990, se reconoció que el seguro de responsabilidad civil puede ser a favor de un tercero, es decir, que tiene como propósito el resarcimiento de la víctima, por lo cual ésta es titular de una indemnización, en caso de que demuestre a ocurrencia del daño y su cuantificación, según lo previsto en el artículo 1077 del Código de Comercio.

En este último punto, es donde cobra especial relevancia referirnos a lo que atañe con la violación de la privacidad, o infracciones relacionadas con la protección de datos personales, pues es allí donde el empresario, puede ver afectado su patrimonio, en la medida que su infraestructura tecnológica sufra incidentes de seguridad.

---

<sup>42</sup> Ibídem.

## 2. RESPONSABILIDAD POR VIOLACIÓN DEL *HABEAS DATA*

Teniendo una aproximación al mundo de los riesgos cibernéticos y su importancia desde la perspectiva del sector asegurador, es indispensable abordar los puntos de conexión que la temática encuentra con el derecho fundamental de *habeas data*. Esto por cuanto de allí, se pueden extraer criterios que están ligados al derecho de seguros, específicamente en lo que tiene que ver con la ocurrencia del daño y su cuantificación.

### 2.1. Derecho fundamental de *habeas data*.

La consagración constitucional del derecho fundamental de *habeas data*, encuentra su fundamento en el artículo 15 de nuestra Constitución Política<sup>43</sup>. Allí se consagra la especial protección que recibe la privacidad de las personas en cuanto a sus datos personales, incluyendo dentro de este ámbito el derecho que tienen a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

El desarrollo de esta prerrogativa constitucional estuvo soportada inicialmente por la jurisprudencia emanada de la Corte Constitucional<sup>44</sup>, en donde reconoció que la actividad asociada a los bancos de datos deben tener siempre un sujeto activo y un sujeto pasivo, refiriéndose este último al administrador de la base de datos, en quién recae la adecuada utilización de los sistemas informáticos para la conservación, uso y circulación de datos personales, es decir, aquella persona natural o jurídica que para efectos de nuestra investigación, tendría interés en contratar la póliza de riesgos cibernéticos.

Así mismo, es oportuno señalar que el tratadista UPEGUI menciona que el “proceso de administración de información personal debe respetar los derechos fundamentales de los sujetos concernidos por esta; que tanto la finalidad que persiga tanto la base de datos, como el proceso de administración debe ser clara y delimitada y que el proceso de administración de información personal debe estar justificado mediante la superación de juicio de relevancia y de pertinencia en función de la finalidad de la base de datos y del proceso de su administración”<sup>45</sup>.

La afirmación anteriormente descrita, trae consigo elementos que sirven para la protección de datos personales de las personas naturales o jurídicas. Con claridad destaca que el procesamiento de datos no debe vulnerar derechos fundamentales, es decir, no puede erosionar aquellas garantías como la intimidad de las personas, atentar contra su honra o buen nombre y, por consiguiente, el proceso de administración de datos personales se puede considerar que no es una actividad libre. Al contrario, el tratamiento de datos

---

<sup>43</sup> Constitución Política de Colombia, artículo 15) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

<sup>44</sup> Ver Corte Constitucional de Colombia. Sentencia SU-082/95.

<sup>45</sup> UPEGUI, Juan Carlos. Universidad Externado, 2008. *Habeas data: fundamentos, naturaleza y régimen*”. P. 397.

personales está regulado y, en consecuencia, su vigilancia y control hace que el encargado o responsable de llevar a cabo esta actividad, deba enmarcarse dentro de una parámetros claramente establecidos y delimitados, debiendo contar siempre con la autorización y el consentimiento del titular de los derechos personales.

Luego, es dable afirmar que cualquier incumplimiento por parte de la persona que realiza el procesamiento de datos personales, dará lugar a la responsabilidad de este frente al ilícito, debiendo reparar al titular conforme a derecho. Así, pues, que el responsable del tratamiento de datos tiene una obligación respecto del proceso de administración, consistente en mantener la disponibilidad, integridad y confidencialidad de la información que reposa en su base de datos.

En Colombia, a partir del año 2012 la consagración normativa de este derecho fundamental, recibió un impulso extraordinario con la expedición de la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario Decreto 1377 de 2013. Bajo este marco legal, el legislador y el ejecutivo fijaron los parámetros para regular el tratamiento de datos personales, y su protección por parte del Estado.

En concreto, vale la pena transcribir lo expuesto por la Honorable Corte Constitucional, sobre las características que reúnen los datos personales. En la sentencia C- 748 de 2011, señaló lo siguiente: “En efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales- son las siguientes: “i) estar referido a aspectos exclusivos y propios de una persona natural, ii) *permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.*” (Cursiva fuera del texto original).

Este planteamiento de la Corte Constitucional, es fundamental puesto que hace énfasis en que los datos personales asociados en conjunto son susceptibles de identificar personas, lo cual, en un ejercicio de análisis de información por parte del empresario, le permitirá conocer sus preferencias personales a partir del análisis de conductas de los consumidores, lo que a la postre se traduce para el comerciante en explorar nuevos mercados, diseñar nuevos productos y en general, valerse de los datos personales para conseguir ventajas en su actividad económica.

Otro aspecto significativo que se encuentran dentro de las características de la protección de este derecho de rango constitucional consiste en que autoriza a terceros para obtener datos personales de las personas, pero que dicho tratamiento de manera alguna constituya la traslación de un derecho de propiedad en favor del tercero, pues el titular en ejercicio del derecho fundamental puede pedir al tercero su actualización, restringir su uso, o eliminarlo de determinada base de datos. Importante resulta ver como la Corporación Judicial en comento, resalta que la propiedad de los datos personales está en cabeza de su titular, así se obtengan por acto ilícito, pues como lo observamos al comienzo del presente escrito, la mayoría de los riesgos cibernéticos son susceptibles de configurar conductas punibles que

no sólo interesan al campo del derecho privado, sino que su comisión se enfoca en el ámbito del derecho penal.

Con ello, es indudable que la Corte Constitucional, como lo dijo en otra oportunidad<sup>46</sup>, busca que las víctimas de ataques cibernéticos tengan una tutela efectiva de sus derechos vulnerados, aun legitimando su reclamación por la vía de la acción de tutela. Ante este nuevo marco legal sobre la tutela que recibe el tratamiento de datos personales, los empresarios que se sirven de aquellos para el desarrollo de su actividad económica, han tenido que sopesar su nivel de exposición, y ver comprometida su responsabilidad frente a sus víctimas.

Valdría la pena preguntarse sobre la extraterritorialidad que supone el Internet<sup>47</sup>, respecto de la competencia de autoridades administrativas para adelantar y sancionar este tipo de conductas. Lo anterior por cuanto el Internet, y específicamente las redes sociales, son un fenómeno a nivel internacional, donde en la mayoría de los casos las personas que administran estas plataformas tienen su domicilio en Colombia, sino que son constituidos y su funcionamiento se rige bajo los parámetros de leyes foráneas.

Al principio de la expedición de la Ley Estatutaria 1581 de 2012, la Superintendencia de Industria y Comercio se refirió sobre su competencia para investigar las conductas que acaecen en redes sociales, y se refieren a las personas jurídicas extranjeras, en el sentido de que carecía de competencia para investigarlas. No obstante, mediante concepto 14-218349-4-0, rectificó su posición de no competencia, para en su lugar, señalar que sí cuenta con facultades para investigar los actos que ocurren en redes sociales<sup>48</sup>, y que son susceptibles de control en materia de datos personales.

De otro lado, el tratamiento de datos personales no es una materia exclusiva de Colombia, sino que las normativas sobre el tratamiento estos datos se caracterizan por tener un enfoque internacional y ser armonizadas<sup>49</sup>. Con base en ello, es posible afirmar que, al tratarse de un derecho de connotación universal, su protección es susceptible de ser amparada por la vía del ordenamiento interno, o de manera internacional.

---

<sup>46</sup> Ver Corte Constitucional de Colombia. Sentencia C-1147/01, Magistrado Ponente: Manuel José Cepeda Espinosa, en la cual señaló: En Internet puede haber una realidad virtual, pero ello no significa que los derechos, en dicho contexto, también lo sean. Por el contrario, no son virtuales: se trata de garantías expresas por cuyo goce efectivo en el llamado “ciberespacio” también debe velar el juez constitucional.

<sup>47</sup> REMOLINA, Nelson y otros. Editorial Temis, 2018. *“De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil. Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información”*. Al respecto señala: “Las TIC – tecnologías de la información y la comunicación -, por su parte, no solo son consideradas el “símbolo emblemático de la cultura contemporánea” sino que ha contribuido a la “datificación” de la sociedad contemporánea y a la consolidación del dato personal como el bien más apetecido de la economía digital”.

<sup>48</sup> Concepto 14-218349-4-0, según el cual, la Superintendencia de Industria y Comercio, señaló: En otras palabras, la SIC se encuentra completamente facultada para garantizar el tratamiento de datos personales de los colombianos que, a través de las redes sociales en internet compartan información personal; todo en observancia de los principios, derechos, garantías y procedimientos establecidos por la Ley 1581 de 2012.

<sup>49</sup> Ibidem, cit. 34, página 46.

Múltiples son las regulaciones que existen para la protección de los datos personales. Sin embargo, para los efectos de nuestra investigación, fijaremos nuestra atención en las directrices que la Superintendencia de Industria y Comercio ha emitido en relación con el principio de responsabilidad demostrada (*Accountability*), según el cual, una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos personales<sup>50</sup>.

Este principio se encuentra estructurado en el artículo 26 de Decreto 1377 de 2013, según el cual, el responsable del tratamiento de datos personales debe probar ante la Superintendencia de Industria y Comercio que cumple con estándares mínimos para prevenir las posibles vulneraciones a los datos personales que se encuentran en sus bases de datos. En consecuencia, se observa que el Legislador colombiano, y su respectivo Ente regulador, procuran por que la protección a los datos se haga de una manera efectiva y real, pudiéndose, en todo momento, ejercer sanciones administrativas en contra de las entidades públicas o privadas que incumplan con las obligaciones previstas en el marco legal.

En este aspecto, es fundamental preguntarse si el Estado lo que pretende a través de la regulación de los datos personales, además de intervenir en el control y vigilancia sobre las bases de datos, impone al responsable del tratamiento una carga de probar que cumplió con los parámetros indicados para proteger a la víctima de determinado incidente de seguridad<sup>51</sup>. Nos parece que, sin decirlo de manera expresa, todas las obligaciones que se establecen para el responsable del tratamiento de los datos personales, hacen que sea éste el llamado a demostrar ante el juez que siguió las medidas idóneas y conducentes para prevenir la fuga de información. Consideramos que, en este punto, el legislador colombiano tomó una postura similar a la prevista en el artículo 2050 del Código Civil italiano, en cuyo contenido la víctima no necesita probar un comportamiento incorrecto en relación con el tratamiento de sus datos personales, ni identificar al sujeto autor del ilícito<sup>52</sup>.

Es así como el tratamiento de datos personales prevé una suscripción de un acuerdo entre el responsable del tratamiento y el titular de la información, en donde incumbe al responsable del tratamiento de los datos personales probar su diligencia en la custodia de la información, basado para ello en la presunción general de culpa por incumplimiento de un contrato que se encuentra en el inciso 3º del artículo 1604 del Código Civil.

---

<sup>50</sup> Superintendencia de Industria y Comercio, "Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*), 2015, disponible en: <https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada> [consultado el 05 de octubre de 2019].

<sup>51</sup> LORENZETTI, al respecto ha expuesto: "En la concepción de la responsabilidad como deuda, todo el peso recae sobre la víctima, que debe probar la causa fuente de la obligación del deudor. Se le exige que ponga en marcha el sistema, que acredite la existencia de una acción antijurídica culpable. En el enfoque actual, hay un principio *favor victimae* que tiende a aliviar su carga. LORENZETTI, Ricardo Luís. *El sistema de la responsabilidad civil: ¿una deuda de responsabilidad, un crédito de indemnización o una relación jurídica*. Boletín de la Facultad de Derecho. Universidad Nacional de Educación a Distancia. Madrid, 2002, p. 269-308.

<sup>52</sup> VISINTINI, Giovanna. *¿Qué es la responsabilidad civil? Fundamentos de la disciplina de los hechos ilícitos y del incumplimiento contractual*. U. Externado de Colombia, 2015, página 116.

Con lo anterior, no estamos afirmando que el tratamiento de datos personales deba ser considerado como una actividad peligrosa, sino que más bien la teleología que persigue el legislador colombiano, consiste en que el empresario como responsable de este tratamiento sea quien deba asumir la prueba de su diligencia y cuidado del tratamiento de datos personales.

Corolario de lo expuesto, podemos señalar que el derecho fundamental de *habeas data* encuentra protección desde el ámbito sancionatorio administrativo del Estado a través de la Superintendencia de Industria y Comercio, y también es susceptible de protección directa por la vía de acción de tutela por tratarse de un derecho fundamental autónomo<sup>53</sup>. Sin embargo, sería útil analizar su proyección en el campo de la responsabilidad civil con el propósito de dilucidar qué protección recibe desde este ámbito.

En ese sentido, se destaca el Reglamento 2016/679 del 27 de abril de 2016 el cual ha precisado que ‘el sujeto de datos’ tiene derecho a exigir una compensación del controlador o procesador de datos cuando este por incumplimiento a las obligaciones que ha adquirido conforme a ese reglamento, ha causado un daño material inmaterial<sup>54</sup>.

Esta norma Europea hace eco en nuestra investigación, pues no sólo se refiere a la responsabilidad administrativa derivadas de multa o sanciones por un indebido procesamiento de datos ante las autoridades de supervisión, sino que consagra expresamente el derecho del sujeto de datos, el cual en Colombia conocemos como titular de exigir una compensación frente al responsable del tratamiento, además de consagrar varias previsiones tendientes a la seguridad de los datos, notificaciones en caso de incidentes de ciberseguridad, así como el restablecimiento de la información y el derecho al olvido, entre otras garantías favorables al sujeto de datos.

## **2.2. Problemática de la reclamación por violación del *habeas data***

La vulneración del *habeas data* en el campo de la responsabilidad, supone el estudio del daño, como primer elemento de la responsabilidad. Como punto de partida podríamos advertir que en materia de seguros es bien interesante la aproximación a este elemento, porque según el artículo 1077 del Código Comercio, la víctima debe demostrar al asegurador la ocurrencia del daño y su cuantía.

---

<sup>53</sup> Corte Constitucional de Colombia., Sentencia T-176A de 2014, acción de tutela instaurada por Robinson Blanco Parra, contra Transporte Humadea S. A., Defencarga y Colfecar. Derechos fundamentales invocados: trabajo, *habeas data*, mínimo vital (M. P. Jorge Ignacio Pretelt Chaljub), 25 marzo 2014: “El reconocimiento del derecho fundamental autónomo al *habeas data*, busca la protección de los datos personales en un universo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad, entre otros. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto conlleva una serie de garantías diferenciadas, cuya protección es directamente reclamable por medio de la acción de tutela, sin perjuicio del principio de subsidiariedad que rige la procedencia de la acción”

<sup>54</sup> Regulation (EU) 2016/679: Article 82. “Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.”

Para estos fines resulta interesante hacer la distinción que trae HENAO<sup>55</sup> sobre el daño y el perjuicio, debido a que en los incidentes de seguridad podría presentarse la siguiente situación hipotética: supóngase que una cadena de supermercados realiza el tratamiento de datos personales de sus clientes y potenciales clientes con el propósito de segmentar el mercado y aumentar sus utilidades.

En desarrollo de estas actividades, es víctima de un ataque cibernético, trayendo como consecuencia la pérdida de información de sus bases de datos, lo cual provoca el fraude electrónico de algunos de sus clientes. Dentro de las personas que resultaron afectadas con este ataque, podría identificarse dos tipos de víctimas, a saber: el primer grupo, sufrió fraudes electrónicos a causa de que su información bancaria estaba registrada en la base de datos, conforme a ello hubo un detrimento en su patrimonio. En cambio, el segundo grupo de personas no tuvo lesión patrimonial, aunque su información también fue objeto de fraude, pues las medidas que tomó la cadena de supermercados, con posterioridad al incidente, evitaron que ocurrieran mayores pérdidas económicas. Sin embargo, a partir de los datos personales obtenidos por el agresor, se pudo conocer información sensible del segundo grupo, permitiendo de esta manera que, de manera no autorizada, se comunicara al público en general la información privada relacionada con el estado de salud de las personas, sus hábitos de alimentación, entre otros.

Bajo el contexto descrito, ¿podría considerarse que el segundo grupo, aunque su información fue filtrada de una manera no autorizada, hecho que puede generar daños extrapatrimoniales, no tendría derecho a reclamar a la cadena de supermercados o a su asegurador, pues no hubo un verdadero detrimento patrimonial, como en efecto si ocurrió con el primer grupo (pérdida de información bancaria)?;

Para tratar de dar una respuesta a los interrogantes planteados, es indispensable identificar que el daño o incidente de seguridad indemnizable será el hecho relacionado con la fuga de información por cuenta de un ataque cibernético, es decir, este será la causa, en cambio, el perjuicio será aquel detrimento que hubo como consecuencia del incidente de seguridad en las cuentas bancarias de los usuarios. En ambos casos, las personas que integran los grupos señalados son víctimas de un daño, en el sentido que sus datos personales están siendo utilizados, con fines distintos a su autorización, por personas extrañas a quien estaba autorizado para dicho propósito. Haciendo énfasis en la relación causa y efecto entre el daño y el perjuicio, no habría lugar a dudas que en ambos casos hay un daño.

La problemática se centra entonces, en conocer si dicho daño es objeto de resarcimiento, pues como ya lo advertimos las consecuencias para los dos grupos es distinta. Para el primer caso no habría duda de que al demostrar el perjuicio (detrimento en sus cuentas bancarias), el responsable del tratamiento de datos personales tendría que asumir la indemnización correspondiente, en la medida que la víctima logre demostrar, extrajudicial o judicialmente, que sufrió un detrimento patrimonial. Empero, para el caso de aquellas víctimas que sufrieron la fuga de información pero que no sufrieron un detrimento

---

<sup>55</sup> HENAO, Juan Carlos. El daño: análisis comparativo de la responsabilidad extracontractual del Estado en derecho colombiano y francés. Universidad Externado, 1998, página 76.

patrimonial concreto y cierto, valdría preguntarse si son susceptibles de recibir indemnización.

Para el primer grupo, es decir, aquellas personas que vieron menoscabado su patrimonio por las diferentes transacciones no autorizadas, se puede considerar que hubo unos perjuicios materiales que son susceptibles de ser reclamados a la cadena de supermercados y, en caso de que esta cadena se encuentre asegurada, la víctima tendría derecho a reclamar al asegurador. El *quantum* de dicha indemnización podría estimarse sobre el equivalente a la pérdida económica o transacción bancaria no autorizada. En contraste, y según un eventual criterio del asegurador, podría establecer que las víctimas del primer y segundo grupo que sufrieron perjuicios extrapatrimoniales, es decir, que no tuvieron menoscabo patrimonial, están desprovistas de la acción indemnizatoria. Dicho de otro modo, el asegurador podría, eventualmente esgrimir en su defensa, que no hay perjuicio indemnizable, que quizás hubo un daño, pero que al confrontar el mismo con la póliza de seguro no es susceptible de reclamación.

Con base en lo anterior, es cardinal analizar si la víctima que padeció por causa de un incidente de seguridad, daños psicológicos (estrés o angustia), mental o moral puede acudir a la acción directa en contra del asegurador, o si por el contrario el ordenamiento jurídico colombiano sobre este particular no prevé indemnización. Esto será objeto de análisis en el apartado subsecuente.

### **2.3. ¿Cobertura para daños extrapatrimoniales?**

En materia de derecho de seguros, se discute si la redacción del artículo 1127 del Código de Comercio, incluye la protección de los perjuicios inmateriales que haya sufrido la víctima, con ocasión de un siniestro. La anterior discusión surge por la manera en la cual se expresó la norma, puesto que “impone a cargo del asegurador la obligación de indemnizar los perjuicios patrimoniales que **cause** el asegurado con motivo de determinada responsabilidad en que incurra de acuerdo con la ley y tiene como propósito el resarcimiento de la víctima...”<sup>56</sup> (Negrilla fuera del texto original). Es decir, de una lectura simple se entendería que la norma excluye de protección los perjuicios inmateriales que sufran las víctimas.

No obstante la redacción de la norma actual, la Corte Suprema de Justicia – Sala de Casación Civil ha dicho con relación a su interpretación que, según la reforma introducida por la Ley 45 de 1.990, “quiso la ley procurar la tutela eficaz de los derechos del damnificado, pero nada más, de ahí que no existe razón válida para afirmar que desapareció la razón de ser del aseguramiento, cual es la de servir como garantía de la indemnidad

---

<sup>56</sup> El artículo 1127, en la redacción original del Código de Comercio definía el seguro de responsabilidad como aquél que «impone a cargo del asegurador la obligación de indemnizar los perjuicios patrimoniales que sufra el asegurado con motivo de determinada responsabilidad en que incurra de acuerdo con la ley. Son asegurables la responsabilidad contractual y la extracontractual, con la restricción indicada en el Artículo 1055» (subrayado propio).

patrimonial del asegurado, quien precisamente acude a dicha modalidad como medida para precaverse de las consecuencias de sus actos”<sup>57</sup>.

En armonía con la interpretación anterior, ha de entenderse, entonces, que si el clausulado de condiciones generales no dispone en absoluto sobre la cobertura o exclusión de los perjuicios inmateriales o extrapatrimoniales, los mismos son susceptibles de amparo bajo la filosofía del seguro de responsabilidad civil, cuyos efectos cumplen un doble propósito: (i) servir de mecanismo preventivo para proteger el patrimonio del asegurado, (ii) pero al mismo tiempo satisfacer la indemnización de la víctima, en una función reparadora.

Ha de destacarse la extrapatrimonialidad de los perjuicios para los fines de nuestra investigación pues, a más de las veces, la responsabilidad generada a partir de la violación de habeas data conduce indefectiblemente a la vulneración de otros intereses relacionados con la personalidad, salud e integridad de la víctima. De allí deriva la importancia de dos aspectos cruciales: (i) establecer la finalidad que tenía la información objeto del hecho ilícito; (ii) y el carácter del dato personal sustraído, filtrado sin autorización, puesto que si estamos en presencia de un dato cuya naturaleza sea pública, fácilmente podríamos argumentar que allí no habría responsabilidad.

A guisa de ejemplo, si se realiza el tratamiento no autorizado de una información genética de un donante, para fines distintos de la donación, como sería la hipótesis que dicha información fuese adquirida por una aseguradora para establecer la prima que debe cobrar en un seguro de vida, nos parece que allí nace la obligación de indemnizar al donante, como quiera que la información genética tiene un carácter eminentemente reservado, confidencial y sensible, cuya divulgación para fines diversos a los que el donante o titular de la información otorgó autorización, puede lesionar sus derechos fundamentales a la salud, al buen nombre o a su dignidad humana<sup>58</sup>.

En esta perspectiva, debemos referirnos a la incorporación y protección de los perjuicios extrapatrimoniales en el ordenamiento jurídico colombiano. Sea lo primero señalar que esta categoría no encuentra una consagración expresa en el Código de BELLO, por ello, la construcción de esta categoría jurídica se ha realizado a partir de la jurisprudencia<sup>59</sup> y la armonización del sistema jurídico a través del Código de Comercio de 1.971, cuyo artículo 1.006, expresó refiriéndose a las acciones del pasajero fallecido: “En uno u otro caso, si se demuestra, habrá lugar a la indemnización del daño moral”.

Con base en lo anterior, comenzó la edificación jurisprudencial sobre el daño moral, este perjuicio referido al dolor, la pesadumbre, perturbación de ánimo, el sufrimiento espiritual,

---

<sup>57</sup> Ver Sentencia de la Corte Suprema de Justicia, Sala de Casación Civil, SC20950-2017 de fecha 12 de diciembre de 2.017, Magistrado Ponente, Ariel Salazar Ramírez, Radicación n° 05001-31-03-005-2008-00497-01

<sup>58</sup> SANTAMARIA, Enrique. Contracts on Human Biological Samples: The European Prohibition of Financial Gain from the Human Body and its parts. ERCL 2017; 13 (2). De Gruyter, Páginas 197 - 213.

<sup>59</sup> Corte Suprema de Justicia—Sala de Casación— Bogotá, veintiuno de julio de mil novecientos veintidós. Magistrado ponente, doctor Tancredo Nannetti.

el pesar, la congoja, aflicción, sufrimiento, pena, angustia, zozobra, perturbación anímica, desolación, impotencia u otros signos expresivos<sup>60</sup>.

El desarrollo jurisprudencial en materia civil, ha conducido a la construcción de subcategorías para clasificar los perjuicios extrapatrimoniales, siendo pertinente destacar, a efectos de nuestra investigación, la relacionada con la vulneración a derechos fundamentales como lo son el buen nombre, la propia imagen, la libertad, la privacidad y la dignidad, que gozan de especial protección constitucional<sup>61</sup>.

Con base en lo anterior, podemos afirmar que los perjuicios extrapatrimoniales hoy gozan de protección en materia de responsabilidad civil y, por lo tanto, son susceptibles de ampararse por medio del contrato de seguro. Sin embargo, con base en lo anterior y para efectos de la celebración del contrato de seguro, interesa que el tomador de la póliza revise si en el clausulado de condiciones generales no hay una cláusula cuyo contenido excluya el amparo de los perjuicios extrapatrimoniales de las víctimas, pues en este caso, y en virtud de lo preceptuado en el artículo 1.056 del Código de Comercio, podría inferirse que el asegurador tienen la facultad de excluir expresamente el cubrimiento de esta categoría de daño. Razón por la cual, insistiremos en lo que ya hemos expuesto, que el tomador de la póliza debe revisar cuidadosamente el clausulado de condiciones generales, para allí atisbar que las exclusiones no dejen por fuera de la cobertura los perjuicios extrapatrimoniales.

Precisado lo anterior y de regreso al ejemplo que propusimos en el acápite que antecede, según el cual, si las víctimas de un ataque cibernético pueden o no reclamar perjuicios extrapatrimoniales al asegurador, basado en su angustia, zozobra o afectación mental sobre la exposición de sus datos personales de carácter confidencial y que gozan de reserva bancaria en la web, podemos afirmar que sí habrá lugar a proponer reclamaciones basados en la violación al derecho fundamental del habeas data, siempre y cuando la víctima este en la capacidad de demostrar el hecho ilícito (siniestro) y su cuantía.

Sin embargo y pese a la creación de esta tipología de daño extrapatrimonial por violación a derechos fundamentales como categoría autónoma, podríamos señalar que hay varias dificultades para que la víctima, en efecto, pueda acudir sin necesidad de un proceso judicial a la reparación del mismo. Lo anterior debido a que la categoría no cuenta con unos contornos bien definidos para su valoración y cuantificación, sino que, dicho concepto proviene de una construcción jurisprudencial realizada por los jueces en la jurisdicción contenciosa administrativa y civil<sup>62</sup>.

---

<sup>60</sup> Ob. Cit. 45.

<sup>61</sup> La Corte Suprema de Justicia - Sala de Casación Civil, se pronunció respecto de la clasificación de los perjuicios extrapatrimoniales, así: De ahí que el daño no patrimonial se puede presentar de varias maneras, a saber: i) mediante la lesión a un sentimiento interior y, por ende, subjetivo (daño moral); ii) como privación objetiva de la facultad de realizar actividades cotidianas tales como practicar deportes, escuchar música, asistir a espectáculos, viajar, leer, departir con los amigos o la familia, disfrutar el paisaje, tener relaciones íntimas, etc., (daño a la vida de relación); o, **iii) como vulneración a los derechos humanos fundamentales como el buen nombre, la propia imagen, la libertad, la privacidad y la dignidad, que gozan de especial protección constitucional.** (Subrayado es nuestro) Sentencia SC10297-2014 de fecha 05 de agosto de 2.014, Magistrado Ponente: Ariel Salazar Ramírez, Radicación: 11001-31-03-003-2003-00660-01.

<sup>62</sup> M'CAUSLAND, María Cecilia. *Equidad judicial y responsabilidad civil extracontractual*. Universidad Externado de Colombia, Bogotá, 2019. Página 439 – 440. Al respecto ha señalado: “El análisis de las

En ese sentido y habida consideración del auge de este tipo de riesgos, habría que cuestionarse sobre la posibilidad que tiene la víctima para reclamar, aun extrajudicialmente, perjuicios extrapatrimoniales, o si ésta tendría que esperar que un juez, haciendo uso excepcional del criterio de la equidad, profiriera una condena para que ampare sus derechos fundamentales, y como consecuencia de ello termine condenado al ofensor o asegurador para el reconocimiento de la obligación.

Para resolver la inquietud planteada, bastaría señalar que el artículo 1131 del Código de Comercio establece que “En el seguro de responsabilidad se entenderá ocurrido el siniestro en el momento en que acaezca **el hecho externo** imputable al asegurado...”, lo que quiere decir que no es necesario la intervención judicial para reconocer efectivamente una indemnización a la persona que se ha visto afectada por un ataque cibernético.

En nuestra opinión, consideramos que no se requiere de un contrato de transacción, un acta de conciliación extrajudicial o judicial o una sentencia, para que, en efecto, el asegurador pueda y deba reconocer la posible indemnización a una víctima de un ataque cibernético. Con ello, no estamos suponiendo que en todos los casos el asegurador deba, per se y sin necesidad de intervención judicial reconocer la indemnización, pues sabido es que la responsabilidad civil para generar la obligación a cargo del ofensor o agresor debe demostrar el daño, la culpa y el nexo causal, pudiendo éste, a través de un juicio de responsabilidad civil, demostrar una causa extraña como exoneración de su responsabilidad<sup>63</sup>.

Luego con lo que estamos señalando no pretendemos aducir que se desvirtúan los elementos que configuran la responsabilidad, sino que queremos expresar es que si, aun extrajudicialmente, se logra demostrar un hecho externo imputable al asegurado relacionado con un ataque cibernéticos, es posible colegir del mismo que se puede reconocer una indemnización a favor de la víctima.

Otro aspecto será, entonces, determinar la cuantificación de los perjuicios extrapatrimoniales porque, según lo que hemos señalado hasta ahora, esta determinación, en Colombia, se hace por vía jurisprudencial, variando las tipologías del daño según el criterio de cada jurisdicción existente y las categorías que hayan adoptado. Empero, aquí surge una propuesta innovadora que podría facilitar su reconocimiento por vía extrajudicial, como lo es la inclusión de tablas<sup>64</sup> que cuantifiquen los perjuicios extrapatrimoniales,

---

decisiones de la Corte Suprema de Justicia y del Consejo de Estado colombianos contienen la jurisprudencia reciente permite afirmar que estas situaciones desafortunadas parecen propiciarse con el reconocimiento de la violación de los derechos fundamentales como categoría autónoma daño reparable, dado que no se establecen criterios claros y coherentes para considerar su inclusión en la tipología del daño”.

<sup>63</sup> TAMAYO JARAMILLO, Javier. Tratado de responsabilidad civil, t. II, 3.a reimpr. Bogotá, Legis, 2008. Páginas - 14 - 15. Este autor refiriéndose a la teoría de causalidad adecuada ha expresado: “El juez considera que la *causa extraña* ha sido el hecho que normalmente ha producido el daño y, en consecuencia, el vínculo de causalidad debe romperse, de tal modo que el demandado no se considere jurídicamente como causante del daño”.

<sup>64</sup> KOTEICH, Milagros. *La reparación del daño como mecanismo de tutela de la persona. Del daño a la salud a los nuevos daños extrapatrimoniales*. U. Externado de Colombia, 2012, Página 57. Este autor con relación a las tablas de liquidación del daño a la salud que hace el Código de los seguros (*Codice delle*

incluyendo las mismas a través de del clausulado de condiciones generales, pues nada obsta para que las partes en virtud de la autonomía contractual que les asiste al momento de celebrar el contrato de seguro, puedan previamente acordar el valor de los perjuicios.

Finalmente, valdría la pena analizar la pertinencia de acudir a la vía legislativa para definir baremos objetivos que contribuyan a la determinación del daño extrapatrimonial, en lo relativo a la violación de datos personales. Para ello, en vía de ejemplo, podría señalarse parámetros como tiempo de exposición indebida de los datos en Internet, probabilidades de pérdidas según el número de ataques, peritajes basados en información comprobable y objetiva, entre otros<sup>65</sup>.

---

*Assicurazionni*, D.L. n.o. 209) se ha referido así: “Pero en realidad no toda la jurisprudencia ha quedado satisfecha con el texto, ..., al haber desconocido del llamado daño existencial, no fue fiel ni reconoció la autonomía de cada uno de los rubros de la trilogía de daños establecidas por las “sentencias gemelas” del 2003, a saber: daño moral subjetivo, daño biológico en sentido estricto y daño derivado de la lesión a (otros) intereses de rango constitucional inherentes a la persona.

<sup>65</sup> CABRERA, Karen y MONTENEGRO, Yamile., “La incorporación de los daños preestablecidos como criterio de determinación del daño en infracciones al derecho de autor en Colombia”, *Revista de Derecho Privado*, Universidad Externado de Colombia, n.º 37, julio-diciembre 2019, 155-182, doi: <https://doi.org/10.18601/01234366.n37.07>. En materia de infracciones a derechos de autor, las autoras han indicado, a saber: “La idea es que el juez al revisar los topes verifique que estos sean congruentes con la capacidad económica de un colombiano promedio, pero sobre todo con las condiciones económicas del infractor y el uso o finalidad del uso que se obtuvo con la infracción, pues imponer penas tan altas o desproporcionadas ocasionaría que no se pagaran las indemnizaciones que se ordenan, tal como ha sucedido en Estados Unidos y Canadá. **De todos modos, la labor del legislador será la de incorporar unos topes de cobros claros, pero será el juez quien tendrá la labor de procurar que las indemnizaciones no sean excesivas pero que de igual forma sí satisfagan las demandas de las víctimas.**” (El subrayado es nuestro)

### **3. COBERTURA PARA PROTECCIÓN DE DATOS PERSONALES QUE OFRECE EL SECTOR ASEGURADOR EN COLOMBIA.**

Con el ánimo de absolver nuestra pregunta de investigación, en virtud de la cual indagamos, a saber: ¿Cuáles son las condiciones del Contrato de Seguro de Responsabilidad Civil, en materia de riesgos cibernéticos, que garantizan una reparación integral de los daños sufridos por los beneficiarios?; a continuación nos proponemos a esbozar algunas condiciones que pueden contribuir a resolver dicho interrogante.

#### **3.1. Análisis Comparativo de Pólizas del Sector Asegurador en Colombia**

Para aproximarnos a las condiciones de asegurabilidad de los riesgos cibernéticos, es necesario realizar un análisis sobre la oferta que realiza el sector asegurador en Colombia. Para ello, se tomaron cinco pólizas que existen en el mercado y que hemos analizado desde la perspectiva de la cobertura de *habeas data* y sus posibles exclusiones, cuyos resultados se sintetizan en el **ANEXO B** del presente trabajo.

Podemos destacar de las pólizas objeto de estudio, que todas incluyen una cobertura relacionada con la protección de datos personales y, por consiguiente, amparan reclamaciones provenientes de las víctimas que se ven afectadas por la vulneración a las bases de datos de cuyo tratamiento es el asegurado. En ese mismo sentido, se puede apreciar en los clausulados analizados, que dichas pólizas no excluyen expresamente de la cobertura perjuicios extrapatrimoniales, lo cual según lo hemos visto dentro del capítulo anterior, es relevante para la víctima y garantiza una reparación integral.

Sin embargo, del análisis efectuado también se puede decir que existen exclusiones generalizadas que podrían menoscabar los derechos de las víctimas a ser indemnizadas, pues se refieren al no cubrimiento por parte del asegurador de la responsabilidad contractual y no otorgamiento de cobertura para las infracciones relacionadas con la propiedad industrial.

Estas exclusiones resultan desproporcionadas y desconocen el carácter de derecho fundamental del *habeas data*. Las razones que particularmente nos llevan a afirmar lo anterior, corresponde a que los datos personales, *per se*, no son lo que la víctima quiere amparar, sino que dichos datos generalmente tienen una utilidad o explotación y más allá del dato, se protege en sí, su uso no autorizado o indebido, es decir, el dato personal embebe información normalmente relacionada con patentes, o su uso se otorga en el marco de un contrato, como sería el caso de un contrato de prestación de servicio o de determinada consultoría.

En consecuencia, se propone que el dato personal sea valorado y susceptible de asegurar a través de una protección que no desconozca que los mismos son el eje que conduce información de diversa naturaleza, como lo sería en los ejemplos que dimos en este escrito, de naturaleza comercial para la explotación de un mercado, o información genética, o de una nueva patente para explotar, en fin, un sin número de casos que podrían suscitarse

alrededor de la responsabilidad contractual o de controversias relacionadas con la propiedad intelectual.

### 3.2. Condiciones para el aseguramiento de riesgos cibernéticos

Según lo expuesto, a continuación algunas condiciones que garantizan la utilidad del seguro de riesgos cibernéticos, viéndolo como una figura bifronte que, por una parte, aseguran la esfera del asegurado, protegiéndolo en su patrimonio<sup>66</sup>, y por otro lado, protege a terceros y los repara integralmente.

**1. Necesidad del seguro:** Desde la esfera del empresario, tomador y asegurado se debe perseguir como fin último del seguro amparar sus bases de datos, infraestructura tecnológica y demás elementos expuestos al Internet. Resulta significativo que el empresario que esté interesado en la contratación de este seguro, identifique claramente sus activos de información, para así poder integrar a su mecanismo de protección el contrato de seguro, y transferir de manera adecuada su exposición y cuantificación al momento de la ocurrencia del siniestro.

En virtud de lo anterior, si el asegurado pretende proteger su patrimonio frente a posibles ataques cibernéticos y su actividad económica se concentra en la explotación de una industria farmacéutica, tendrá que observar que no se excluyan expresamente las patentes, pues naturalmente su contenido de datos personales, puede estar expuesto a los denominados riesgos cibernéticos.

**2. Conexidad:** Es relevante para asegurar debidamente a los beneficiarios de las pólizas de riesgos cibernéticos, que los clausulados del asegurador no excluyan materias relacionadas con la propiedad industrial, daños a la salud, daños a la intimidad y al buen nombre de las personas, pues bien podemos señalar que del estudio efectuado a lo largo del presente escrito, encontramos que un ataque cibernético es susceptible que afectar varios derechos fundamentales que se contienen en un dato personal. Es decir, el dato personal puede asumir la vocación de ser un medio o conducto para el tratamiento de información diversa, que en su gran mayoría constituye datos sensibles relacionados con la privacidad e intimidad de la persona, o que puede contener información de carácter religiosa o de afinidad política, entre otros.

**3. Cuantificación del perjuicio extrapatrimonial:** Como lo expusimos, el ordenamiento jurídico colombiano no conoce la indemnización de perjuicios extrapatrimoniales sino por la vía de la intervención judicial, siendo necesario que el tomador de la póliza y el asegurador, en ejercicio del principio de autonomía dispositiva<sup>67</sup>, definan contornos claros

---

<sup>66</sup> BETTI. Emilio. *Teoría generale delle obbligazioni*, I (Milano: Giuffré, 1.953), 40 – 42. El autor señala, a saber: “la esencia de este contrato es precisamente la asunción de un riesgo que grava sobre la esfera jurídica del asegurado – de suerte que – la utilidad para el asegurado consiste cabalmente en quedar relevado de la ansiedad que le produce la incertidumbre acerca de su propio porvenir, en estar liberado de las preocupaciones que tal incertidumbre le genera.

<sup>67</sup> El Consejo de Estado, Sala de lo Contencioso Administrativo, sección tercera, subsección c, se pronunció así: “Ahora, pese al pre-diseño del texto contractual por parte de ECOPETROL, como el régimen contractual

y baremos que contribuyan a la cuantificación de los efectos nocivos que deriva un incidente de seguridad.

## CONCLUSIONES

En primer lugar, debe señalarse que las obligaciones que naturalmente se desprenden del contrato de seguro son obligaciones típicas de *praestere*, cuyo contenido encierra esa confianza, respaldo o garantía que acompaña al asegurado, según la cual le otorga tranquilidad porque realizó una adecuada transferencia de riesgos, que eventualmente pueden afectar su patrimonio y generarle la obligación de indemnizar.

De acuerdo con lo anterior, puede inferirse que el mercado asegurador, acoplándose a los riesgos contemporáneos, ha construido un mecanismo de transferencia de riesgos a favor de los empresarios que con ocasión del tratamiento de datos personales, pueden ser vulnerados por el fenómeno de los riesgos cibernéticos, lo cual supone que la dialéctica que debe existir entre el asegurador y tomador del seguro, fluya en ambiente de certeza, completitud y precisión, con el propósito de que la expectativa del acreedor – tomador y asegurado –, sea objeto de cobertura y tutela adecuada, pues de nada serviría que la transferencia de riesgos se haga de una manera exigua o sencillamente no se realice.

En segundo lugar, y viendo al seguro de responsabilidad civil para la gestión de riesgos cibernéticos desde el ámbito de las víctimas, hay que señalar que la incorporación de estas pólizas merece un estudio más profundo para indagar sobre la cobertura que ellas contiene en materia de vulneración a derechos fundamentales, pues como bien lo advertimos en este escrito, es posible colegir que a la fecha los perjuicios extrapatrimoniales sólo vienen siendo reconocidos a través de una intervención judicial, pero ello no obsta, para que las partes del contrato de seguro, en ejercicio de la autonomía dispositiva, puedan convenir parámetros o baremos que contribuyan a establecer la cuantificación de este tipo de perjuicios.

Por último, en nuestra opinión disentimos en torno a las exclusiones que los aseguradores vienen realizando en sus clausulados de condiciones generales, pues no están amparando la responsabilidad contractual o las controversias amparados con la propiedad intelectual, desconociendo, de esta manera, que los datos personales son vehículos para la transmisión de datos sensibles o privados, cuya manipulación indebida podría eventualmente afectar otros derechos fundamentales, o estar relacionados con otros ámbitos que también generan responsabilidad civil frente a terceros, tal como sería el caso de la filtración de unos datos personales sobre el estado de salud de las personas o sus enfermedades, con fines lucrativos y en contravía del consentimiento informado conferido por el titular de la información.

---

aplicable es el derecho privado, y especialmente al principio de la autonomía dispositiva, las partes están facultadas legalmente para: **modificar o ajustar algunos términos o elementos del contrato, cuando en su criterio las condiciones fácticas, técnicas y económicas así lo aconsejan, y en todo caso con aprobación del Ministerio de Minas y Energía.** (Subrayado nuestro). Sentencia radicado número: 19001-23-31-000-2007-00147-01 (41.783), de fecha 24 de agosto de 2.016, Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección C, Magistrado Ponente Jaime Orlando Santofimio Gamboa.

## BIBLIOGRAFÍA

### 1. Referencias:

BAILEY, Liam. Mitigating moral hazard in cyber-risk insurance. *JL & Cyber Warfare*, 2014, vol. 3, p. 1.

BETTI, Emilio. Teoría general de las obligaciones, I (Milano: Giuffrè, 1.953), 40 – 42.

CABRERA, Karen y MONTENEGRO, Yamile., “La incorporación de los daños preestablecidos como criterio de determinación del daño en infracciones al derecho de autor en Colombia”, *Revista de Derecho Privado, Universidad Externado de Colombia*, n.º 37, julio-diciembre 2019, 155-182, doi: <https://doi.org/10.18601/01234366.n37.07>

COBURN, Andrew; LEVERETT, Eireann; WOO, Gordon. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2018. Páginas 3 – 7

CRO FORUM, 2014. The cyber risk challenge and the role of insurance, p. 23. DOI: <https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf>.

CRO FORUM, 2016. CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk, Annex – Detailed cyber incident type and descriptions. p. 25.

ELING, Martin. Cyber risk and cyber risk insurance: status quo and future research. 2018, p. 39.

HENAO, Juan Carlos. El daño: análisis comparativo de la responsabilidad extracontractual del Estado en derecho colombiano y francés. Universidad Externado, 1998, página 76.

HINESTROSA, Fernando. Tratado de las obligaciones. Concepto, estructura, vicisitudes, I. Bogotá: Universidad Externado de Colombia, 2007, 262 – 263.

Informe de amenaza de Cibercrimen de Metrix: una entrevista (noviembre de 2019); disponible en <https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/>.

JARAMILLO, Carlos Ignacio. Derecho privado: estudios y escritos de derecho patrimonial: “Derecho de Obligaciones”. Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, 2013, Pág. 104. Grupo Editorial Ibáñez. Bogotá, Colombia.

KOTEICH, Milagros. *La reparación del daño como mecanismo de tutela de la persona. Del daño a la salud a los nuevos daños extrapatrimoniales*. U. Externado de Colombia, 2012, Página 57.

KOSSEFF, Jeff. *Cybersecurity law*. John Wiley & Sons, 2017.

LORENZETTI, Ricardo Luís. El sistema de la responsabilidad civil: ¿una deuda de responsabilidad, un crédito de indemnización o una relación jurídica. *Boletín de la Facultad de Derecho. Universidad Nacional de Educación a Distancia*. Madrid, 2002, p. 269-308.

LORENZETTI, Ricardo Luís. *Tratado de los contratos*. Tomo I. Página 45.

M'CAUSLAND, María Cecilia. Equidad judicial y responsabilidad civil extracontractual. Universidad Externado de Colombia, Bogotá, 2019. Página 439 – 440.

MAROTTA, Angelica, et al. Cyber-insurance survey. Computer Science Review, 2017, vol. 24, p. 35-61.

ORDÓÑEZ, A. Estudios de seguros. Universidad Externado de Colombia, 2012, “El carácter indemnizatorio del seguro de daños”, página 186.

PAZ, Antonio. “La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico”, Revista de Derecho Privado, Universidad Externado de Colombia, n. ° 35, julio-diciembre de 2018, 261-289. doi: <https://doi.org/10.18601/01234366.n35.10>.

PEÑA, Daniel Peña Valenzuela. La protección del consumidor en el comercio electrónico. ROJAS, Carmen Ligia Valderrama (ed.). Perspectivas del derecho del consumo. U. Externado de Colombia, 2013, página 466.

REMOLINA, Nelson y otros. Editorial Temis, 2018. “De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil. Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información”

Revista: Gerencia de Riesgos y Seguros. Estimación de Pérdidas Máximas por siniestros. Utilidad para asegurados industriales. Número. 115 - 2.013.

RAULFF, Ulrich., 2004. An Interview with Giorgio Agamben. German Law Journal, vol. 5, no. 5, pp. 609–614. DOI 10.1017/S2071832200012724.

RODAS, Fernando, ¿Es necesaria en Colombia la estipulación legal de un seguro obligatorio de responsabilidad civil que cubra el ejercicio de la actividad médica? Responsabilidad Civil y del Estado, Tomo III/ Ediciones 15 - 19, 2003, Responsabilidad Civil y del Estado N° 18. Instituto Colombiano de Responsabilidad Civil y del Estado, Pág. 494.

SANTAMARIA, Enrique. *Contracts on Human Biological Samples: The European Prohibition of Financial Gain from the Human Body and its parts*. ERCL 2017; 13 (2). De Gruyter, Páginas 197 – 213.

SIGNORINO, Andrea Barbat. Visión Jurídica sobre privacidad, confidencialidad y protección en el expediente clínico electrónico. IV congreso de nuevas tecnologías La influencia de internet, genética y nanotecnología en la medicina y el seguro. Universidad Externado de Colombia, 2015.

SOBRINO, Waldo. Cyber Risk Insurance Law (New Developments Upon May 12, 2017 Global Cyber-Attack). Revista Ibero-Latinoamericana de Seguros, 2017, vol. 26, no 47.

TALESH, Shauhin A. Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers” for Businesses. Law & Social Inquiry, 2018, vol. 43, no 2, p. 417-440.

TAMAYO JARAMILLO, Javier. Tratado de responsabilidad civil, t. II, 3.a reimpr. Bogotá, Legis, 2008. Páginas - 14 – 15.

UPEGUI, Juan Carlos. Universidad Externado, 2008. Habeas data: fundamentos, naturaleza y régimen”. P. 397.

VISINTINI, Giovanna. ¿Qué es la responsabilidad civil? Fundamentos de la disciplina de los hechos ilícitos y del incumplimiento contractual. U. Externado de Colombia, 2015, página 116.

VILLEGAS, Andrés y VILLEGAS. Sergio. La vía ejecutiva en el seguro de responsabilidad civil. Responsabilidad Civil y del Estado, Tomo V/Ediciones 25 - 28, 2003, Responsabilidad Civil y del Estado N° 25. Instituto Colombiano de Responsabilidad Civil y del Estado, Pág. 204.

ZORNOSA, Hilda Esperanza. El Seguro de Responsabilidad Civil Su evolución Normativa y Jurisprudencial en Colombia. Revista Ibero-Latinoamericana de seguros, 2011, vol. 20, no 35, páginas 132 y ss.

ZORNOZA, Hilda Esperanza (ed.). Escritos sobre riesgos y seguros. U. Externado de Colombia, 2012. “Las partes en el contrato de seguro”, página 652

## **2. Documentos normativos:**

CONPES No. 3701 de 14 de julio de 2011, el Consejo Nacional de Política Económica y Social, del Departamento Nacional de Planeación se adoptaron, a saber: “LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA”. Constitución Política de Colombia

DECRETO 410 DE 1971, Código de Comercio.

GTC-ISO, Guía Técnica Colombiana. IEC 27035 (2012), Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.

LEY 1273 DE 2009, “por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”.

LEY 45 de 1990, “Por la cual se expiden normas en materia de intermediación financiera, se regula la actividad aseguradora, se conceden unas facultades y se dictan otras disposiciones.”

LEY 57 de 1887, Código Civil.

LEY ESTATUTARIA 1581 DE 2012, “por la cual se dictan disposiciones generales para la protección de datos personales”

Regulation (EU) 2016/679

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE COLOMBIA, Concepto 14-218349- -4-0 de 2014.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, "Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*), 2015.

### **3. Jurisprudencia:**

Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección C, Sentencia radicado número: 19001-23-31-000-2007-00147-01 (41.783), de fecha 24 de agosto de 2.016, Magistrado Ponente: Jaime Orlando Santofimio Gamboa.

Corte Constitucional de Colombia. Sentencia C-1147/01, Magistrado Ponente: Manuel José Cepeda Espinosa.

Corte Constitucional de Colombia. Sentencia SU-082/95, Magistrado Ponente: Jorge Arango Mejía.

Corte Constitucional de Colombia., Sentencia T-176A de 2014, acción de tutela instaurada por Robinson Blanco Parra, contra Transporte Humadea S. A., Defencarga y Colfecar. Derechos fundamentales invocados: trabajo, habeas data, mínimo vital (M. P. Jorge Ignacio Pretelt Chaljub).

Corte Suprema de Justicia – Sala de Casación Civil, CSJ SC, radicado: 2000-01098-01 18 dic. 2013, Magistrado Ponente, Ruth Marina Díaz Rueda.

Corte Suprema de Justicia – Sala de Casación Civil. Sentencia SC10297-2014 de fecha 05 de agosto de 2.014, Magistrado Ponente: Ariel Salazar Ramírez, Radicación: 11001-31-03-003-2003-00660-01.

Corte Suprema de Justicia - Sala de Casación, Sentencia. veintiuno de julio de mil novecientos veintidós, Magistrado ponente: doctor Tancredo Nannetti.

Corte Suprema de Justicia, Sala de Casación Civil, SC20950-2017 de fecha 12 de diciembre de 2.017, Magistrado Ponente, Ariel Salazar Ramírez, Radicación n° 05001-31-03-005-2008-00497-01

Corte Suprema de Justicia, Sala de Casación Civil, Sentencia del 2 de febrero de 2001, M.P. Carlos Ignacio Jaramillo Jaramillo

## ANEXO A. ANÁLISIS DE TENDENCIAS INVESTIGATIVAS ASOCIADAS A LOS CIBERSEGUROS

**I. Objetivo.** Identificar líneas de investigación futuras sobre ciberseguros a través de un análisis de tendencias investigativas asociadas al campo de conocimiento.

**II. Estructura metodológica.** La Vigilancia Tecnológica se entiende como un proceso organizado de observación y análisis del entorno, que implica el tratamiento, el reporte y la circulación interna de los hechos observados y su posterior utilización para la toma de decisiones<sup>68</sup>. Desde la perspectiva de ROUACH<sup>69</sup>, la vigilancia tecnológica permite desarrollar acciones que se anticipen a los cambios del entorno, aprovechando las oportunidades que se generan en diversos momentos del tiempo. En particular, el propósito de esta investigación fue identificar tendencias investigativas asociadas a los ciberseguros como punto de partida para la construcción de un estado del arte sobre el tema.

Para la realización del ejercicio de Vigilancia Tecnológica se utilizó como referente la propuesta metodológica establecida por PALOP, MARTÍNEZ, Y BEDOYA<sup>70</sup>, que integra a su vez los planteamientos propuestos por PALOP Y VICENTE<sup>71</sup>. La Figura 1 sintetiza, las tres fases y las siete etapas que se implementaron para consolidar el estudio.

La ecuación de búsqueda utilizada en la base de datos *Web of Science* se muestra en la Figura 2. Esta ecuación integra dos apartados, el primero, describe los tópicos asociados a los ciberseguros y el segundo describe la acotación del campo de conocimiento de interés para la investigación. Complementario a lo anterior, se procesó una ecuación de búsqueda genérica en la base de datos Lens.org, esta sólo incluyó los términos “*cyber insurance*” con el propósito de contar con una visión más amplia sobre el campo de conocimiento. Como resultado de la aplicación de la ecuación de búsqueda en la base de datos *Web of Science*, se generaron 88 resultados, al filtrar sólo artículos se generaron 76. En la base de datos Lens.org se generaron 844 resultados, al filtrar sólo artículos se generaron 484 documentos objeto de análisis.

Figura 1. Fases y etapas que conforman la estructura metodológica de la investigación

---

<sup>68</sup> PALOP, Fernando; VICENTE, José M. *Vigilancia tecnológica e inteligencia competitiva: su potencial para la empresa española*. Madrid: Cotec, 1999.

<sup>69</sup> ROUACH, Daniel. *La veille technologique et l'intelligence économique*. Presses universitaires de France, 2008.

<sup>70</sup> PALOP, F.; MARTÍNEZ, J. F.; BEDOYA, A. Guía metodológica de práctica de la vigilancia tecnológica e inteligencia competitiva. *Proyecto Piloto de Transferencia y Desarrollo de Capacidades Regionales en Vigilancia Tecnológica e Inteligencia Competitiva*. Valencia y Medellín, 2012, vol. 6.

<sup>71</sup> PALOP, Fernando; VICENTE, José M. *Vigilancia tecnológica e inteligencia competitiva: su potencial para la empresa española*. Madrid: Cotec, 1999.

<b>OBSERVAR</b>	<b>Búsqueda</b>	<ul style="list-style-type: none"> <li>Se definieron palabras clave asociadas al campo de conocimiento. Las palabras clave se establecieron a través de una revisión de literatura no estructurada y permitieron consolidar una ecuación de búsqueda estructurada.</li> </ul>
	<b>Captación</b>	<ul style="list-style-type: none"> <li>Para el ejercicio de Vigilancia Tecnológica, se utilizaron como fuentes de información la base de datos multidisciplinar Web of Science y la base de datos Lens.org.</li> </ul>
	<b>Difusión</b>	<ul style="list-style-type: none"> <li>Se diseñaron protocolos de filtrado en las bases de datos: por tipo de documento (solo artículos)</li> </ul>
<b>ANALIZAR</b>	<b>Tratamiento</b>	<ul style="list-style-type: none"> <li>La información derivada de las bases de datos se procesó utilizando el Software de Minería de Datos Vos Viewer y las herramientas analíticas de las propias bases de datos.</li> </ul>
	<b>Análisis</b>	<ul style="list-style-type: none"> <li>Se analizaron tres elementos: dinámica de publicación por país, instituciones más productivas y tendencias investigativas asociadas al campo de conocimiento.</li> </ul>
	<b>Validación</b>	<ul style="list-style-type: none"> <li>Los resultados del ejercicio de análisis se visualizaron en: mapa de publicaciones por país, mapa de instituciones más productivas y mapa de relevancia con temáticas asociadas al campo de conocimiento.</li> </ul>
<b>UTILIZAR</b>	<b>Explotación</b>	<ul style="list-style-type: none"> <li>Los principales resultados del ejercicio de vigilancia tecnológica se sintetizan en este documento.</li> </ul>

Fuente: Autor considerando como referente Palop, Martínez, y Bedoya; Palop y Vicente

Figura 2. Palabras Clave y Estructura de la Ecuación de búsqueda utilizada



### III. Resultados

#### 3.1 Dinámica de Publicación por país

La dinámica de publicación por país se estudió tanto para la base de datos *Web of Science* como para la Base de datos Lens.org. Los resultados se muestran en la Figura 3 y la Figura 4 respectivamente y evidencian como convergencia que el país con mayor interés en el campo de conocimiento es Estados Unidos, destacando un especial interés por el análisis de los riesgos cibernéticos y la toma de decisiones asociada al aseguramiento de estos

riesgos<sup>72</sup>. Igualmente, se ha profundizado en temas de políticas públicas y en el estudio de las leyes de políticas cibernéticas en el contexto de los contratos de seguro<sup>73</sup>. Complementario a lo anterior, se encontró que existe un creciente interés por profundizar en el análisis de los ciberataques y las vulnerabilidades que estos producen, entendiendo que estas complejidades sistémicas asociadas a la agregación de riesgos deberán ser medidas y supervisadas por las aseguradoras<sup>74</sup>.

Figura 3. Dinámica de Publicación por país *Web of Science*



Del ejercicio realizado se evidenció que, en el contexto latinoamericano, no se encuentran publicaciones que aborden esta temática, a excepción de 1 publicación de Brasil y 1 de Argentina (en *Web of Science*). La publicación brasilera realiza un análisis de investigaciones empíricas, estudiando temas asociados a la libertad de expresión, al derecho a la privacidad y al debido proceso de los usuarios de Internet<sup>75</sup>. La publicación argentina, se enfoca en el desarrollo de un marco conceptual técnico-probabilístico para abordar temas de seguridad cibernética<sup>76</sup>. Ninguna de las dos publicaciones profundiza en el objetivo y en el enfoque de esta investigación.

<sup>72</sup> DE SMIDT, Guido; BOTZEN, Wouter. Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 2018, vol. 43, no 2, p. 239-274.

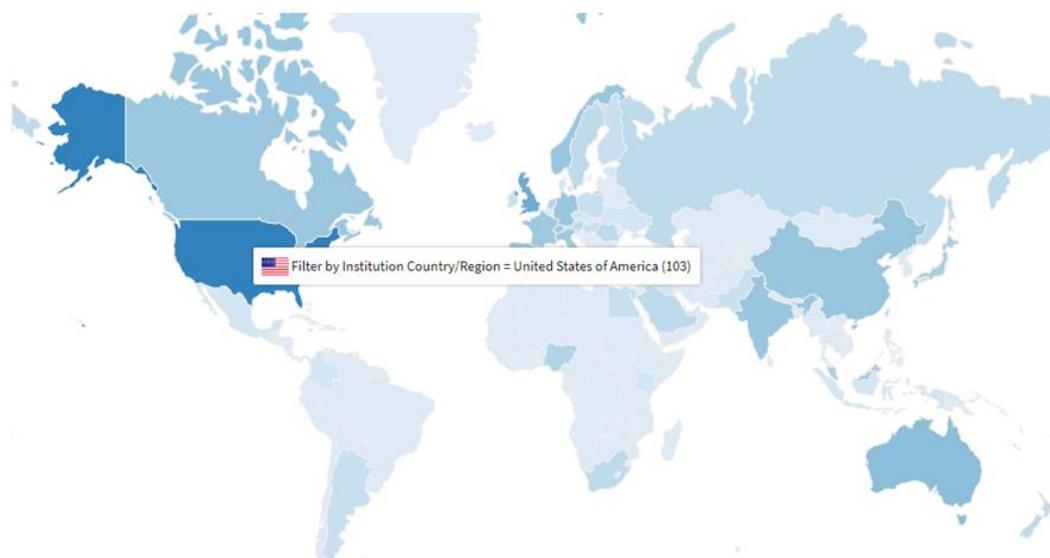
<sup>73</sup> HEATH, Brendan. Before the Breach: The Role of Cyber Insurance Incentivizing Data Security. *Geo. Wash. L. Rev.*, 2018, vol. 86, p. 1115.

<sup>74</sup> CAMILLO, Mark. Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, 2017, vol. 2, no 1, p. 53-63.

<sup>75</sup> BELLI, Luca; VENTURINI, Jamila. Private ordering and the rise of terms of service as cyber-regulation. 2016.

<sup>76</sup> SHAKARIAN, Paulo, et al. Belief revision in structured probabilistic argumentation. *Annals of Mathematics and Artificial Intelligence*, 2016, vol. 78, no 3-4, p. 259-301.

Figura 4. Dinámica de Publicación por país Lens.org



### 3.2 Instituciones más productivas en el campo de conocimiento

Al analizar las instituciones más productivas en términos del número de publicaciones asociadas al campo de conocimiento en *Web of Science* (ver Figura 5), se identificó que en el primer lugar se encuentra *European University* de Ucrania, que cuenta con la Academia Ucraniana de Seguridad Cibernética, una organización pública establecida para promover el desarrollo de una red y un ecosistema de educación y entrenamiento de fuerzas productivas en el campo de la seguridad cibernética a través de asociaciones entre instituciones gubernamentales, la comunidad académica y la industria<sup>77</sup>. Otra de las organizaciones destacadas es el Departamento de Defensa de Estados Unidos, que ha orientado su investigación al análisis técnico de modelos de mitigación de riesgos cibernéticos y al desarrollo de modelos para evaluar estos riesgos integrando el análisis de comportamientos de los usuarios que intercambian información.

Al realizar el análisis en la base de datos Lens.org (Ver Figura 6) se encontró que la institución más productiva es la Universidad Tecnológica de Nanyang, universidad pública de Singapur, en convergencia con lo identificado en la base de datos Web of Science. Una de sus publicaciones destacadas, propone un modelo de ciberseguro con un enfoque en los servicios de asesoramiento de riesgos, el modelo cuantifica el efecto combinado de las inversiones en seguridad para abordar las amenazas y la vulnerabilidad cibernética<sup>78</sup>. Esta institución cuenta con el “*Cyber Security Research Centre*”<sup>79</sup> que orienta su investigación en cuatro áreas: aproximaciones a la ciberseguridad, detección de ataques, cibercrimen y análisis de seguridad y confiabilidad de los sistemas.

<sup>77</sup> <https://uacs.kiev.ua/about-academy/>

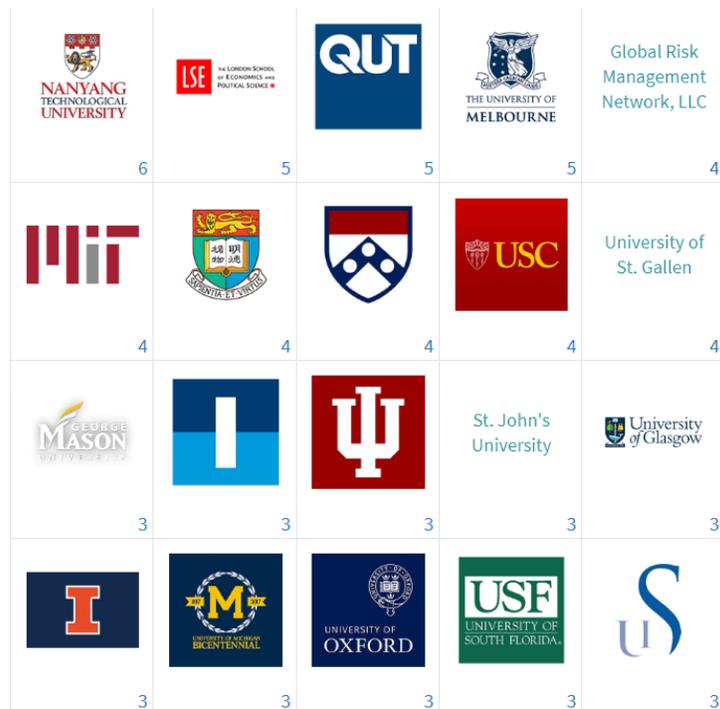
<sup>78</sup> WANG, Shaun. Integrated framework for information security investment and cyber insurance. Available at SSRN 2918674, 2017.

<sup>79</sup> <https://cysren.ntu.edu.sg/Pages/Home.aspx>

Figura 5. Instituciones más productivas Web of Science



Figura 6. Instituciones más productivas Lens.org

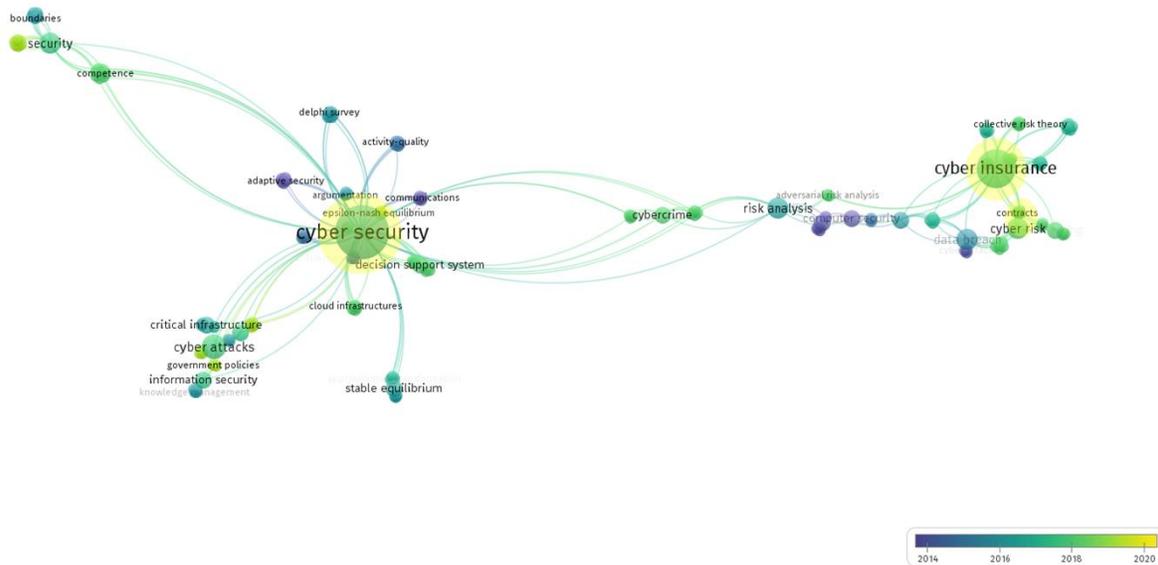


### 3.3 Tendencias Investigativas asociadas al campo de conocimiento

Al analizar las tendencias investigativas en la línea de tiempo, sobre el campo de conocimiento, se hizo evidente que en las publicaciones realizadas en la base de datos *Web of Science*, el interés investigativo inició en temáticas asociadas a los modelos de Ciberseguridad Adaptativos, que analizan comportamientos y eventos para protegerse y

adecuarse frente a las amenazas de ciberseguridad antes que estas ocurran, e implican una evaluación continua del riesgo<sup>80</sup>. Este interés ha ido evolucionando con el tiempo al análisis de riesgos, al estudio de ciberataques y a la investigación en diseños de infraestructura y de toma de decisiones para la gestión de la ciberseguridad. Adicional a lo anterior, se evidencia un interés particular por el análisis de políticas gubernamentales sobre crimen cibernético y una tendencia evidente del estudio de los ciber-riesgos y de su proyección en el contrato de seguro. Finalmente, se encontró que se muestra una tendencia al estudio de la protección de las reclamaciones frente al robo de datos (Ver Figura 6).

Figura 6. Tendencias Investigativas *Web of Science*



El análisis anterior, fue también realizado en la base de datos Lens.org, permitiendo identificar los principales campos de estudio asociados a los ciberseguros. Allí se hace evidente que la investigación se ha abordado con mayor énfasis desde la perspectiva económica, gubernamental, comercial, financiera, de relaciones públicas, de la gestión del riesgo y de la seguridad computacional. Sin embargo, se encontró que se presenta una tendencia investigativa creciente sobre el estudio de los ciberseguros desde la perspectiva legal, enfatizando en tópicos asociados a la responsabilidad civil, evidencia de ello, son los temas resaltados en la Figura 7.

<sup>80</sup> <https://www.forcepoint.com/es/cyber-edu/adaptive-security>



Como resultado del ejercicio de vigilancia tecnológica sobre el campo de conocimiento se concluye que países como Estados Unidos y algunos países europeos son líderes en la publicación de documentos científicos sobre las temáticas que involucran los riesgos cibernéticos, evidenciando de esta forma el reto de la investigación latinoamericana en desarrollar estudios que profundicen en el análisis de las coberturas, exclusiones y reclamaciones en materia de seguros asociados a los riesgos cibernéticos.

A partir del análisis de tendencias investigativas, se evidenció que en los últimos años se presenta una dinámica creciente de publicaciones orientadas a estudiar los incidentes relacionados con el robo de información que podrían involucrar la ingeniería social y comprometen la responsabilidad de las empresas susceptibles de recibir posibles reclamaciones por pérdidas de información que afecten la privacidad de sus clientes.

Finalmente, se identifica que el tema de los ciberseguros está relacionada con un universo multidisciplinar, en cuyo espectro confluyen áreas del conocimiento relacionadas con la economía, la ingeniería computacional, las finanzas, la administración y la legal. Se encuentra un reto investigativo relacionado con este último campo de conocimiento, entendiendo que se requiere profundizar en la regulación de la actividad cibernética. En particular, se hacen necesarios estudios orientados a estudiar como viabilizar la transferencia del riesgo a través de pólizas de seguros. En este contexto, se propone como relevante el estudio de la oferta del mercado asegurador en términos de protección frente a posibles siniestros derivados de la responsabilidad civil de las empresas aseguradas, analizando criterios como la causalidad, la espacialidad y la temporalidad, para generar así, propuestas teóricas y prácticas que permitan la asegurabilidad dentro de un esquema de ciberseguridad.

## **Referencias**

BELLI, Luca; VENTURINI, Jamila. *Private ordering and the rise of terms of service as cyber-regulation*. 2016.

CAMILLO, Mark. *Cyber risk and the changing role of insurance*. *Journal of Cyber Policy*, 2017, vol. 2, no 1, p. 53-63.

DE SMIDT, Guido; BOTZEN, Wouter. Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 2018, vol. 43, no 2, p. 239-274.

HEATH, Brendan. Before the Breach: The Role of Cyber Insurance Incentivizing Data Security. *Geo. Wash. L. Rev.*, 2018, vol. 86, p. 1115.

PALOP, F.; MARTÍNEZ, J. F.; BEDOYA, A. Guía metodológica de práctica de la vigilancia tecnológica e inteligencia competitiva. *Proyecto Piloto de Transferencia y Desarrollo de Capacidades Regionales en Vigilancia Tecnológica e Inteligencia Competitiva*. Valencia y Medellín, 2012, vol. 6.

PALOP, Fernando; VICENTE, José M. *Vigilancia tecnológica e inteligencia competitiva: su potencial para la empresa española*. Madrid: Cotec, 1999.

ROUACH, Daniel. *La veille technologique et l'intelligence économique*. Presses universitaires de France, 2008.

SHAKARIAN, Paulo, et al. Belief revision in structured probabilistic argumentation. *Annals of Mathematics and Artificial Intelligence*, 2016, vol. 78, no 3-4, p. 259-301.

WANG, Shaun. Integrated framework for information security investment and cyber insurance. *Available at SSRN 2918674*, 2017.

## ANEXO B. ANÁLISIS DE PÓLIZAS DE RIESGOS CIBERNÉTICOS EN COLOMBIA

A S E G U R A D O R	BERKLEY	MAPFRE COLOMBIA	LIBERTY	SURA	SBS
¿ I n c l u y e  a m p a r o s  r e l a c i o n a d o	<p>1. Seguridad y privacidad de la información.</p> <p>2. Reclamación de autoridad competente.</p> <p>3. Reclamaciones asociadas a tarjetas como medio de pago.</p>	<p>1. Violación de datos de carácter personal, incluyendo información sobre tarjetas de crédito o débito.</p> <p>2. Violación de derechos de confidencialidad.</p> <p>3. Incumplimiento de cualquier contrato escrito entre el Asegurado y un tercero a cargo del procesamiento y custodia de datos de tarjetas de crédito, incluyendo cualquier incumplimiento del PCI DSS (Payment Card Industry Data Security Standard)</p>	<p>1. Vulneración de los derechos de privacidad.</p> <p>2. Incumplimiento de cualquier deber legal o contractual de proteger la seguridad o confidencialidad.</p> <p>3. Transmisión de código malicioso desde la red del asegurado a la red de un tercero (excluyendo la de un tercero proveedor de servicios), o no evitar dicha transmisión.</p> <p>3. Infracción de copyright, nombre de dominio u otros derechos de propiedad intelectual (excluyendo patentes) del reclamante, Plagio, o reproducción o distribución no autorizada o cualquier alegación similar o equivalente formulada en la jurisdicción donde se presente la reclamación.</p>	<p>1. Responsabilidad por privacidad</p> <p>2. Responsabilidad por seguridad de la red</p> <p>3. Responsabilidad por contenidos electrónicos</p>	<p>1. Cualquier pérdida derivada de la violación de información personal, real o presunta (incluyendo el daño moral o la angustia emocional resultantes de la vulneración por parte de la sociedad de normas relativas a la protección de datos y al endoso de extensión opcional- contenidos multimedia- en caso de haber sido contratada.</p>

s c o n e l h a b e a s d a t a ?					
---	--	--	--	--	--

<p>¿ Q u é e x c l u s i o n e s  t i e n e  e n  r e l a c i ó n  c o n  e l  h a b e a s</p>	<p>1. Responsabilidad contractual. 2. Propiedad Intelectual. 3. Acuerdos de servicio de tarjetas de pago. 4. Competencia desleal y prácticas restrictivas de la competencia.</p>	<p>1. Responsabilidad contractual. 2. Responsabilidad por propiedad intelectual.</p>	<p>1. Responsabilidad asumida contractualmente por el asegurado, excepto en la medida que dicha responsabilidad hubiera existido incluso en ausencia de dicho contrato. Esta exclusión no será aplicable a un incumplimiento de la propia política de privacidad del asegurado. 2. Vulneración de derechos de propiedad intelectual o industrial de terceros</p>	<p>1. Reclamaciones relacionadas con la responsabilidad contractual. 2. Reclamaciones realizadas en desarrollo de una relación laboral. 3. Incumplimiento en los estándares de seguridad de las tarjetas de pago.</p>	<p>1. Propiedad intelectual cualquier infracción de cualquier derecho de propiedad intelectual, incluyendo marcas. 2. (i) Responsabilidad u obligación asumida bajo un contrato o Acuerdo que desconozca el deber de cuidado, de diligencia o de cualificación que es exigible; o (II) cualquier garantía u obligación de resultado, clausula penal o de indemnización predeterminada salvo que la responsabilidad hubiera correspondido al asegurado por ley en ausencia de dicha garantía, obligación o clausulas.</p>
--	--	--	--	---	--

<b>d a t a ?</b>					
----------------------------------	--	--	--	--	--