Seguros ante los *cyber risks*

Elikah de Santana y França Santhiago[*]

Resumen

El avance tecnológico ha generado enormes progresos y cambios en la vida de las personas, las empresas y los gobiernos en general. La globalización y la diseminación de ordenadores y de Internet han permitido que cada vez más personas, organismos públicos y empresas dependan de los recursos de la automatización y la integración. El robo, la adulteración, el secuestro de información, la extorsión virtual, el robo de identidad, entre tantos otros, son crímenes que causan daño tanto a empresas como a particulares. Muchos de ellos todavía no han sido enfrentados por la ley. Ante tantas amenazas, el número de empresas que contratan seguros sigue siendo muy pequeño ante el rápido y constante crecimiento de los perjuicios que ese tipo de delito puede causar. Se sabe que anticiparse al problema sigue siendo la mejor salida para asegurar los datos personales y corporativos y que, como no existe una forma de eliminar la ocurrencia de los crímenes, se hace necesaria la adquisición urgente de soluciones de seguros que atenúen los daños causados por ellos. La cobertura ofrecida por un seguro contra delitos cibernéticos debe considerar los diversos tipos de daños posibles, desde los patrimoniales, incluyendo robos de datos y de dinero, hasta los casos de responsabilidad de la empresa asegurada debido a la divulgación indebida

* Magíster en Base de Datos por la Universidade Federal de Pernambuco (UFPE), Brasil, curso de Derecho de la Faculdade Estácio em Natal/RN, Brasil. El artículo fue presentado como trabajo final de la disciplina Consumidores de Seguros dictada por el profesor Dr. Waldo Sobrino en el programa de doctorado de la Universidad de Buenos Aires (UBA). Funcionaria Pública Federal; elikahfranca@gmail.com.

de informaciones de sus clientes, empleados y productos. En cambio, las aseguradoras exigen que las empresas hagan altas inversiones en *hardware*, *software*, programas antivirus actualizados y en personal altamente calificado para monitorear, identificar y eliminar ataques a sus redes internas y para controlar los accesos a Internet.

Palabras claves: Seguros, cibercrímenes, Derecho Penal, Derecho del Consumidor.

Cyber Risk Insurance

Abstract

The technological advance has generated enormous progress and changes in the lives of people, companies and governments in general. The globalization and dissemination of computers and the Internet has allowed more and more people, public bodies and companies to depend on the resources of automation and integration. Theft, adulteration, the kidnapping of information, virtual extortion, identity theft among many others are crimes that cause damage to both companies and individuals. Many of them have not yet been faced by law. And even in the face of so many threats, the number of companies that hire insurance is still very small in the face of the rapid and constant growth of the damages that this type of crime can cause. It is known that anticipating the problem is still the best way to ensure personal and corporate data and that, there being no way to eliminate the occurrence of crimes requires the urgent acquisition of insurance solutions that mitigate the damage caused by them. The coverage offered by insurance against cybercrime should consider the various types of possible damage, from patrimonial, including data theft and money theft, to cases of liability of the insured company due to the undue disclosure of information from their clients, employees and products. Instead, insurers demand that companies make high investments in hardware, software, updated antivirus programs and highly qualified personnel to monitor, identify and eliminate attacks to their internal networks and to control access to the Internet.

Keywords: Insurance, Cyber Crimes, Criminal Law, Consumer Law.

I. Introducción

La sociedad posmoderna ha pasado por un gran cambio debido a la globalización y a la diseminación de ordenadores y de Internet. Vivimos en una era de información y de avance tecnológico. El mundo se está volviendo cada vez más virtual y atractivo. La Internet es hoy un fenómeno mundial de utilidad pública. Además, acortó distancias, llevó productos y servicios a lugares nunca antes imaginados. Gracias a Internet, la comunicación es instantánea, las personas anónimas se convirtieron en celebridades. Es como si existiera otro mundo donde los conceptos de distancia y de materia hubieran sido remodelados. Hoy tenemos empresas que solo existen en el mundo de bits y bytes, donde las personas cambian de identidad virtual como si fuera un simple accesorio que se utiliza según el estado de ánimo y la situación. El bitcoin, una de las tantas monedas virtuales, solo existe en el mundo digital, en un mundo conectado. La llamada aldea virtual no tiene fronteras, pero necesita límites. Es en ese ambiente de anonimato, de situaciones efímeras, de gran velocidad, que personas que antes nunca habían pensado en cometer delitos se sienten libres para transgredir, para experimentar nuevas emociones, para actuar con curiosidad. En los primeros años, cuando ese nuevo ambiente se expandió, se percibió que no había derecho material, ninguna ley especial que contemplara esas nuevas situaciones.

Segundo Emeline Piva Pinheiro no se puede dejar de observar que:

> (...) es justamente en este ambiente libre y totalmente sin fronteras que se ha desarrollado una nueva modalidad de crímenes, una criminalidad virtual, desarrollada por agentes que se aprovechan de la posibilidad de anonimato y de la ausencia de reglas en la red mundial de computadoras.[1]

Entre los varios delitos que ya se han identificado hay que tratar con robo, adulteración, secuestro de informaciones, extorsión virtual, robo

1. Pinheiro, Emeline Piva. *Crimes virtuais: Uma análise da criminalidade informática e da resposta estatal*, 2003, 34 p. Monografia (Graduação em Direito). Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2006. Disponible en: http://www.egov.ufsc.br/portal/sites/default/files/emeline.pdf. Acceso: 15/03/ 2018. p. 8.

de identidad, entre tantos otros crímenes que causan daños a empresas y a particulares, y que aún no han sido enfrentados por la ley. Son acciones que pueden ocurrir con cualquier dispositivo conectado a la red mundial de computadoras, a Internet. Para tratar con este nuevo mundo, para reducir los daños causados por esos crímenes, las aseguradoras se modernizaron. Ahora se ofrecen nuevas modalidades de seguros.

II. Crímenes cibernéticos, delitos informáticos

Son muchos los daños causados por ataques cibernéticos y que crecen año tras año. Sin embargo, pocas empresas se preocupan por la seguridad contra este tipo de ataques. Es un hecho que, cuanto más conexiones a Internet, mayor es la vulnerabilidad de los sistemas empresariales que controlan los activos. Hoy, los gobiernos ya reconocen en los *cybercrimes* una amenaza a la economía, lo que requiere la adopción de prácticas y tecnologías de combate a las amenazas.[2]

La principal característica del entorno virtual es que, una vez disponibles en la red, la información se puede copiar varias veces. Así, aunque su original se mantiene, deja de ser único, "es prácticamente imposible medir la extensión del daño, no hay control de tirada y ni siquiera sabe cuántas veces ese contenido se ha duplicado, a menos que se programe el contenido para tanto".[3] Esto significa que cuando sea necesario evaluar el perjuicio causado por las invasiones, no hay que dejar de considerar que habrá copias no autorizadas que siempre estarán disponibles. Así, por más que una empresa entre con acción contra un sitio de búsqueda, esas copias no autorizadas pueden nunca dejar de existir.

En su libro sobre redes sociales y tecnologías, Tomeo enumera los argumentos usados por los sitios de búsqueda cuando esos se defienden de acciones que apuntan a responsabilizarlos por las informaciones enviadas en Internet.

2. "Gastos com seguros contra ciberataques somam cerca de US$ 2 bi." [S.l.]: Revista Apólice, [02/02/2017]. Disponible en: http://www.revistaapolice.com.br/2017/02/gastos- com- seguros- contra-ciberataques/. Acceso: 30/01/2018.

3. Pinheiro, Patrícia Peck. *Direito Digital*. 6ª ed. São Paulo: Saraiva, 2016, p. 205.

> El hecho de solicitar judicialmente la eliminación de los resultados de búsqueda a un buscador nunca solucionará el problema, pues el contenido difamatorio seguirá existiendo en el servidor donde se encuentra alojado el sitio *web* y en consecuencia seguirá estando visible en la red y será accesible por otros buscadores o por medio de enlaces (*links)* existentes en otras páginas de usuarios, ciberbitácoras, foros, redes sociales, e incluso hasta en cadena de correos electrónicos.[4]

Y, finalizando ese argumento, el autor aclara que la forma de solucionar el problema sería remover el contenido del servidor en el que está almacenado. Esto es porque, además de ser posible que ya se haya copiado, el sitio de búsqueda no es el responsable del almacenamiento, solo indica el camino a través del cual se puede encontrar la información.

Para Sydow, "buena parte de los delitos perpetrados tienen como responsables usuarios con alguna relación laboral con los blancos de ataque".[5] Si se tiene en cuenta esta afirmación, esto explica por qué las empresas necesitan adoptar rutinas de seguridad tales como intercambios periódicos de contraseñas, tener siempre registros de operaciones actualizadas, además de un control riguroso de acceso a los sistemas, entre otras tantas medidas que pueden y deben ser observadas. En general, los colaboradores, afirma Sydow (2015: 144), "a veces buscan venganza de sus empleadores, meros perjuicios o incluso beneficios y ventajas por conocer las debilidades de la empresa".

La especialista en el área del Derecho Digital en Brasil, Pinheiro (2016: 144) confirma la necesidad de controlar el acceso a los sistemas informatizados. "La Internet funciona como una red orgánica en la que los responsables de los puertos de entrada y de salida tienen cómo autorizar el acceso, restringirlo, identificar al usuario en su base de datos, entre otras informaciones."

Sin embargo, no son solo empleados y exempleados que amenazan la seguridad de la información almacenada en sistemas empresariales, Sydow (2015: 115) apunta a otra cuestión que afirma que:

4. Tomeo, Fernando. *Redes sociales y tecnología 2.0*. 2ª ed. Buenos Aires:Astrea, 2014, p. 16.

5. Sydow, Spencer Toth. *Crimes informáticos e suas vítimas*. 2ª ed. São Paulo: Saraiva, 2015. p. 143.

> También es una práctica bastante común en las redes informáticas la inducción de víctimas futuras y eventuales a instalar archivos que generan fallas de seguridad o crean verdaderas puertas de acceso libre en los dispositivos ajenos. Una vez instalados estos códigos maliciosos, el delincuente puede ingresar al sistema.

Las personas que navegan sin cuidado o que abren archivos de procedencia desconocida muchas veces no tienen noción de cuánto están siendo cebos para criminales. "El usuario atacado no sabe de dónde viene el ataque, quién lo ataca, por qué lo ataca, lo que quiere y ni siquiera sabe si hubo o no modificación o estrago en su sistema." (Sydow, 2015: 49).

Al contrario de lo que sucede en el mundo real, donde la víctima se ve ante la amenaza, en el mundo virtual,

> A veces, el usuario ni siquiera percibe que su aparato ha sufrido una violación de privacidad, ya que la instalación de un programa hace que haya una verdadera entrada oculta, de acceso libre y desimpedido, que se conoce en la jerga informática como puerta de los fondos o *backdoor*. Ninguna violencia ha habido, sino un ardid (Sydow, 2015: 115).

Esto sucede porque el usuario, en la gran mayoría de las veces, desconoce que los delincuentes actúan en el mundo virtual a través del envío de mensajes, vídeos, fotos y de tantas otras formas. Con ello, atraen su atención para que se adjunten comandos ocultos que se instalan en la máquina del destinatario con el objetivo de ejecutar, en determinado momento y según alguna condición, programas no autorizados. Pinheiro (2016, p. 145) señala que "el aumento de la seguridad en Internet depende directamente de un comportamiento colectivo y cooperativo de los propios internautas".

Los delitos cibernéticos pueden definirse como son presentados por Pinheiro (2003, p. 16) según la cual

> (...) el crimen virtual es cualquier acción típica, antijurídica y culpable cometida contra o por la utilización de procesamiento automático de datos o su transmisión en que un ordenador conectado a la red mundial de computadoras –Internet– sea el instrumento o el objeto del delito.

No hay consenso en cuanto a qué crímenes deben ser tipificados como tal. Sydow (2015: 297) enumera algunas acciones que representan la ocurrencia de crímenes virtuales que objetivan devastar el dispositivo de computadora de otro para obtener, adulterar o destruir datos o informaciones sin autorización del propietario del dispositivo o para instalar vulnerabilidades que favorezcan la obtención de una ventaja ilegal.

Algunos de estos delitos ya ocurrían antes de la existencia de Internet pero se volvieron potencialmente más nocivos debido a la rapidez del procesamiento electrónico de datos y al hecho de que el criminal puede estar en el anonimato cuando los comete.

Pinheiro (2003: 21) agrupa los crímenes por tipo y presenta otra lista de crímenes que también pueden ocurrir en Internet, son ellos:

> Los crímenes de lavado de dinero y las invasiones de privacidad, las fluctuaciones en los sitios oficiales del gobierno, el vandalismo, el sabotaje, los crímenes contra la paz pública, la piratería en general, el espionaje, las lesiones a los derechos humanos (terrorismo, crímenes de odio, racismo, etcétera), la destrucción de información, juegos ilegales, falsificación del sello o señal pública, falsedad ideológica, modificación o alteración no autorizada de sistemas de información, violación del secreto funcional, fraude en competencia pública, entre otros innumerables.

Como se puede observar, la lista es bastante extensa y no es fácilmente agotadora. La Internet, como se puede comprobar en estos casos, es usada como un instrumento, un medio para cometer delitos.

El objetivo no siempre es la destrucción de contenido almacenado en el ordenador objetivo, se puede querer cometer, por ejemplo, crímenes contra el honor, contra la dignidad de la persona humana, crimen fiscal. Es importante hacer que el lector vea la amplitud de riesgos inherentes al uso del ambiente virtual a los cuales las personas, empresas y gobiernos están expuestos. Estos últimos ya reconocen la amenaza económica representada por el cibercrimen y muchos ya están tomando una serie de medidas, que incluyen la adopción de mejores prácticas y tecnologías de combate a las amenazas.[6]

6. "Gastos com seguros contra ciberataques somam cerca de US$ 2 bi. [S.l.]"en Revista

III. Ataques cibernéticos en Brasil y en el mundo

Igrejas, en un artículo en la revista *Apólice*, afirma que "Brasil es el país que más recibe ataques cibernéticos en América Latina y está entre las primeras posiciones en el ranking mundial"[7]. Esto se debe al hecho de que Internet y las nuevas tecnologías han cambiado la forma en que las empresas realizan sus operaciones, principalmente en cuanto al almacenamiento y el intercambio de información. Esta evolución ha aumentado la eficiencia empresarial, pero ha traído una mayor vulnerabilidad en relación con la información sensible, los datos registrados de los usuarios, financieros y de gestión.

Las cifras llegan a ser espeluznantes, en un artículo publicado por L.S. en la Revista *Ap*ólice se tiene que "Solo el año pasado, 978 millones de personas fueron víctimas de *cybercrimes* en todo el mundo. En Brasil, 62 millones de víctimas, aproximadamente el 60% de toda la población en línea activa en el país".[8]

Y más, se afirma que:

> Brasil es uno de los países que más tiempo lleva para lidiar con un ataque después de que ocurre. De acuerdo con el informe Norton CyberSecurity Insights 2017, a Brasil le lleva 33,9 horas para resolver un cyberataque. El promedio general global es de 23,6 horas. Otros países como Japón (5,6 horas), Estados Unidos (19,8 horas) y Reino Unido (33,9 horas) suelen actuar más rápidamente.[9]

Segundo Pinheiro (2003: 14), "al lado de los beneficios que surgieron con la diseminación de las computadoras y del acceso a Internet, surgieron crímenes y criminales especializados en el lenguaje informático".

Apólice, [02/02/2017]. Disponible en: http://www.revistaapolice.com.br/2017/02/gastos- com- seguros- contra-ciberataques/. Acceso: 30/01/2018.

7. Igrejas, Álvaro. "Risco cibernético: Ele pode atacar a sua empresa". Maio-2017. Disponible en: https://www.revistaapolice.com.br/2017/05/risco-cibernetico-pode-atacar-empresa/. Acceso: 5/03/2018.

8. "Brasil somou 62 milhões de vítimas de cybercrimes em 2017. [S.l.]" en Revista *Apólice*, 2018. Disponible: https://www.revistaapolice.com.br/2018/03/brasil-somou-62-milhoes-de-vitimas-de-cybercrimes-em-2017/. Acceso: 19/03/2018.

9. Ibídem.

El 12 de mayo de 2017, el mundo sufrió dos ataques cibernéticos de proporciones mundiales que alcanzaron a más de 200 mil empresas en 150 países. Uno de ellos fue resultado de la activación de un virus "*ransomware"*, un virus bautizado WannaCry que se extendió por Internet a través de un fallo de Windows.[10] A través de él, los criminales obtuvieron control de la red de las organizaciones y pasaron a exigir rescate mediante pago en bitcoins (moneda virtual) para desbloquear el acceso a archivos y el posterior retorno del funcionamiento del sistema operativo. Para recuperar su información era necesario pagar $ 1.300 (mil trescientos dólares) por máquina, según el artículo publicado por el sitio especializado Consultor Jurídico (CONJUR).[11]

En un artículo publicado en el diario *La Ley* el 5 de junio de 2017, el profesor Dr. Waldo Sobrino (Sobrino, 2017) llama tsunami tecnológico a los rápidos cambios por los que hemos pasado cuando afirma: "Y este verdadero *tsunami tecnológico* tiene consecuencias puntuales y específicas no solo en la vida diaria de nuestra sociedad, sino también en los diversos aspecto de los *riesgos y las responsabilidades legales*."[12]

A pesar de esto, "solo tres de cada diez empresas brasileñas reconocen amenazas cibernéticas como algo que puedan impactar sus actividades".[13] Esto es verificado por los números de contrataciones de seguros de esa naturaleza. En ese mismo reportaje, se destaca que "de acuerdo con Ernest & Young, las empresas compran seguro para proteger sus activos, pero contabilizando solo el 30% de los activos que son tangibles, pero dejan el 70% que son intangibles al riesgo".

10. Fuchs, Karin. "Riscos cibernéticos eminentes [S.l.]", Revista *Cobertura* 22/03/ 2017. p.1. Disponible en: http://www.revistacobertura.com.br/2017/07/21/riscos-ciberneticos-eminentes/. Acceso: 18/03/2018.

11. D'urso, Luiz Flávio Filizzola; D'urso, Luiz Augusto Filizzola. "Ataque cibernético mundial é a comprovação da insegurança na internet". 17/05/2017. Disponible en: https://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet. Acceso: 5/03/2018.

12. Sobrino, Waldo. "Los seguros de *cyber risk*". Diario *La Ley*, Año LXXXI N° 104, Publicado: 5/07/2017.

13. "Brasil precisa amadurecer quando o assunto é ciberataque. [S.l.]": Revista *Apólice*, 2017. Disponible en: http://www.revistaapolice.com.br/2017/05/brasil-precisa-amadurecer-ciberataque/. Acceso: 19/03/2018.

El artículo[14] presenta el entendimiento de Gustavo Galvão, superintendente de Financial Lines & Liability de Argo Seguros y miembro de la Comisión de Líneas Financieras de la Federación Nacional de Seguros Generales (Fenseg) que declara que el bajo número de contrataciones de seguros se debe

> (...) a la baja concientización sobre la importancia de la gestión de riesgos, al aún bajo conocimiento de los productos de seguros disponibles y al hecho de que el brasileño tiene un bajo nivel de cultura con relación a la protección y transferencia de riesgo a través de la contratación de seguros.

Estados Unidos es el mayor mercado de seguros cibernéticos donde el 20% de todas las organizaciones tienen seguros para riesgos cibernéticos. Por ser un país con gran riesgo de nuevos ataques, en Brasil hay una previsión de aumento en la contratación de seguros contra ataques cibernéticos. De acuerdo con el Centro de Investigación y Desarrollo en Telecomunicaciones (CPqD), mientras que en los últimos años hubo un incremento del 38% en los ataques cibernéticos en el mundo, en Brasil eso representó el 276%.[15]

Cuando se analiza la representatividad en las contrataciones del seguro cibernético por las industrias, se verifica que el sector de manufactura con el 63% y el de comunicación, medios y tecnología con el 41% son los que más los contratan.[16]

En términos de actividad comercial en Internet, Pinheiro (2016: 169) observa que "muchas tiendas virtuales todavía poseen vulnerabilidades bien básicas, que ya deberían haber sido sanadas y que pueden ser explotadas por cualquier adolescente malintencionado o incluso por una pandilla interesada en recoger datos de tarjeta de crédito". No existe norma que obligue a las empresas a comunicar la ocurrencia de invasiones o daños a sus datos. Muchas de ellas no hacen público los crímenes que sufrieron con temor de que sus activos pierdan valor comercial.

14. Ibídem.

15. Ibídem.

16. "Gastos com seguros contra ciberataques somam cerca de US$ 2 bi. [S.l.]": Revista *Apólice*, 02/02/2017. Disponible en: http://www.revistaapolice.com.br/2017/02/gastos- com- seguros- contra-ciberataques/. Acceso: 30/01/2018.

Como forma de evitar ataques, "lo ideal es tomar medidas preventivas, porque una serie de informaciones esenciales –y muchas veces valiosas– están disponibles en todo momento para los proveedores" (MDS Brasil).[17] Anticiparse al problema sigue siendo la mejor salida para asegurar los datos personales y corporativos.

IV. La protección jurídica contra *cybercrimes*

La inserción de código malintencionado o *malware*, según Sydow (2015:122), se hace mediante la inserción de programas "que violan el bien jurídico seguridad telemática y, con ello, indirectamente, pueden causar otros daños".

Segundo Tomeo (2014: 14), "al no existir reglas de juego claras (esto es, una legislación específica que establezca pautas concretas), las sentencias dictadas hasta el momento toman distintos caminos y arrojan resultados diversos para una problemática que se profundiza".

Cuando son llevadas a la jurisdicción estatal, las decisiones no suelen ser uniformes una vez que cada país tiene sus normas. Cuando hablamos de aspectos legales que tratan estos tipos de crímenes, es importante tener en cuenta que la mayor dificultad encontrada por los países es la transnacionalidad de su cometido. "El enfoque legal vinculado a los crímenes cibernéticos difiere de país a país de modo que una acción definida como criminal en un lugar puede no ser en otro. Al mismo tiempo, la incidencia de los crímenes difiere de un país a otro."[18]

En su artículo, Arocena destaca:

> Cuando se tenga por justificada la necesidad del derecho penal para el tratamiento de las cuestiones problemáticas que trae aparejadas la alta tecnología informática, resulta indispensable determinar

17. "Seguros contra ciberataques defendem e previnem patrimônio de empresas, clientes e fornecedores. [S.l.]": MDS Brasil, 2017. Disponible en: http://www.mdsinsure.com.br/seguros-contra-ciberataques-defendem-e-previnem-patrimonio-de-empresas-clientes-e-fornecedores/. Acceso: 21/03/2018.

18. Riscos Cibernéticos. [S.l.]: *Tudo Sobre Seguros*, 2017. Disponible en: http://www.tudosobreseguros.org.br/portal/pagina.php?l=741. Acceso: 20/03/2018.

> también si es imprescindible sancionar *nuevas reglas* del Derecho criminal enderezadas a dicha tarea.[19]

Para Sydow (2015: 86), "los bienes jurídicos ya protegidos y que son perjudicados por el uso de la tecnología no merecerán nuevo ropaje, por ya ser objeto de protección". Sin embargo, hay otra cuestión para tener en cuenta: las conductas. En su libro, él destaca que no solo ocurre con los bienes jurídicos, "las conductas practicadas merecen alternativas de agravamiento, ya que practicadas por medio facilitador y con alta capacidad lesiva y, más especialmente, por ser una tendencia de criminalidad." (Sydow, 2015: 86).

Se observa, por lo tanto, que para lidiar con esa nueva criminología, se hace necesario definir una forma de regulación legal de los delitos informáticos. En el artículo en que Arocena (2011: 298) analiza la Ley Nacional Nº 26.388, sancionada el 4 de junio de 2008, en la Argentina, presenta dos formas posibles de ser adoptadas con el fin de normalizar el tratamiento de los crímenes cibernéticos: sancionando una ley específica en complemento al ya existente Código Penal o realizando una reforma en el propio Código Penal, "ora agregando un nuevo título que contemple las nuevas ilicitudes no tipificadas, ora ubicando estas en los distintos títulos del digesto conforme los diversos bienes jurídicos que pretendan tutelarse". La primera solución especifica fue adoptada por Venezuela, Chile y Alemania; y la segunda, por Bolivia, Paraguay, España y Francia, por ejemplo.

En la Argentina, según Arocena (2011: 297), aún es posible encontrar ejemplos de las dos alternativas, aunque la normativa vigente haya decidido tratar de forma descentralizada en el Código Penal "incluyendo los distintos tipos legales en los diversos títulos del Libro Segundo del digesto, conforme los variados objetos jurídicos que se desea tutelar".

En Brasil, el Marco Civil de Internet[20] establece principios, garantías y deberes para el uso de Internet en Brasil, teniendo como fundamentos tres

19. Arocena, Gustavo. "La regulación de los delitos informáticos en el Código Penal Argentino: Introducción a la Ley Nacional Nº 26.388". *Revista Jurídica de la Facultad de Jurisprudencia de la Universidad Católica de Santiago de Guayaquil*, Guayaquil, v. 2011, n. 12, pp. 289-327, dez. 2011. Disponible en: http://www.revistajuridicaonline.com/2011/12/ la-regulacion-de-los-delitos-informaticos-en-el-codigo-penal-argentino/. Acceso: 05/03/2018. p. 291.

20. Véase en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

pilares principales: neutralidad de la red, privacidad de usuarios y libertad de expresión.[21] Esta legislación trajo una seguridad jurídica que antes los brasileños no tenían, al servir de base legal para el Poder Judicial en el juicio de proceso que versaran sobre problemáticas involucrando el ambiente virtual. De un lado están los gobiernos, dispuestos a adaptar la ley penal para normalizar la tipificación de los nuevos delitos y del otro, los profesionales del Derecho. Para Pinheiro (2016: 77) "Los nuevos profesionales del Derecho son los responsables de garantizar el derecho a la privacidad, la protección del derecho de autor, el derecho de imagen, la propiedad intelectual, los derechos de imagen, la seguridad de la información, los acuerdos de derechos de imagen, y asociaciones estratégicas, de los procesos contra *hackers* y mucho más".

Se percibe, por lo tanto, que los gobiernos se preocupan y se concientizan de los daños económicos, financieros y sociales que los crímenes cibernéticos causan en muchas organizaciones, en sus órganos y en las residencias de su pueblo hasta el punto de crear normas que castiguen a los responsables de los delitos. No hay todavía una forma de eliminar la ocurrencia de ataques, robos, extorsión, divulgación de datos privados, falsificaciones, entre tantos otros, aún más cuando el avance de la tecnología ha traído siempre nuevas formas de actuar, lo que exige la adquisición urgente de soluciones de seguros que atenúen los daños causados por ellos.

V. De los seguros contra cibercrímenes

El análisis de riesgos en un entorno virtual ya no es algo excepcional, no es algo solo imaginable en un futuro lejano, se trata de un riesgo a ser considerado no solo por grandes empresas, sino también en ambientes domésticos.

21. Savegnago, Jéssica Uliana; Woltmann, Angelita. *A regulamentação dos cibercrimes no Brasil: Uma análise jurídica dos "Três Pilares" norteadores do Marco Civil da Internet*. 2015. 17 p. Artículo científico (Anais do 3º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede)-Faculdades de Direito e Informática, UFSM-Universidade Federal de Santa Maria, Santa Maria / RS, 2015. Disponible en: http://coral.ufsm.br/congressodireito/anais/2015/6-10.pdf. Acceso: 5/03/2018. p. 7.

Las exposiciones ocurridas en el ambiente virtual (cyber) son multidisciplinares, lo que significa que cubren la seguridad en la red, los medios en línea, la propiedad intelectual y la privacidad.[22]

La cobertura ofrecida por un seguro de esta naturaleza debe considerar los diversos tipos de daños posibles, desde los daños patrimoniales, incluyendo los robos de datos y de dinero, que pueden llevar a extorsiones e interrupciones de acceso, hasta los casos de responsabilización de la empresa asegurada debido a la divulgación indebida de informaciones de sus clientes, empleados y productos. Se hace necesario, por lo tanto, que se considere "una solución para la transferencia y mitigación de esos riesgos a través del seguro de protección de datos y responsabilidad cibernética".[23]

En 2011, por la Deliberación N° 147, la Superintendencia de Seguros Privados (Susep) en Brasil, lanzó la Política de Seguridad de la Información y las Comunicaciones (Posic) que tiene como objetivo "instituir directrices estratégicas, responsabilidades y competencias, con el objetivo de asegurar integridad, confidencialidad, disponibilidad y autenticidad de los datos e informaciones de Susep, ya sean estáticos o en tránsito, contra amenazas que puedan comprometer sus activos, incluso su imagen institucional".[24]

Entre las varias coberturas posibles, el sitio Bolsa de Seguros presenta una lista de garantías que una empresa necesita contratar para permanecer en el ambiente cibernético con seguridad:

- Responsabilidad por la divulgación de datos privados y corporativos.
- Responsabilidad por empresas tercerizadas.

Costes de defensa.

Hechos, errores u omisiones que resulten en: contaminación por virus, denegación inadecuada de acceso, robo o robo de código de acceso, corrupción de datos almacenados, robo de *hardware* y violación en la seguridad de datos.

22. Bolsa de Seguros. Principais coberturas : https://www.bolsadeseguros.com.br/seguro-riscos-ciberneticos/

23. Ibídem.

24. "Riscos Cibernéticos. [S.l.]": *Tudo Sobre Seguros*, 2017. Disponible en: http://www.tudosobreseguros.org.br/portal/pagina.php?l=741. Acceso: 20/03/2018.

Gastos de publicidad.

Notificación y monitoreo (costos incurridos para la notificación de una violación de datos a los usuarios).

Beneficios Salarios del tomador del seguro (análisis caso por caso).

Perjuicio financiero del tomador del seguro.

Beneficios de terceros, entre otros.[25]

También la aseguradora AIG, en su sitio, ofrece un tipo de seguro denominado *cyber edge* que incluye las siguientes coberturas:

- Responsabilidad por Datos Personales y Corporativos.
- Responsabilidad por la seguridad de datos.
- Responsabilidad por Empresas Tercerizadas.
- Costos de Defensa.
- Sanciones administrativas.
- Restitución de imagen de la sociedad y personal.
- Notificación y Monitoreo.
- Datos Electrónicos.[26]

Entendiendo por responsabilidad por la seguridad de datos, en ese caso, aquella que resarza a la empresa contratante cuando ocurra cualquier acto, error u omisión que resulte en:

• Contaminación de datos de terceros por software no autorizado o código malicioso (virus).
• Negación de acceso inadecuado para el acceso de un tercero autorizado a los datos.
• Robo o robo de código de acceso en las instalaciones de la sociedad o vía sistema informático.
• Destrucción, modificación, corrupción y eliminación de datos almacenados en cualquier sistema informático.

25. Bolsa de Seguros. Principais coberturas : https://www.bolsadeseguros.com.br/seguro-riscos-ciberneticos/

26. "Cyber Edge. [S.l.]": AIG Seguros, 2018. Disponible en: https://www.aig.com.br/empresas/produtos/linhas-financeiras/cyber-edge#accordion-child_pr_cr_accordion_2. Acceso: 20/03/2018.

• Robo o robo físico de *hardware* de la empresa por un tercero.
• Divulgación de datos debido a una violación de seguridad de datos.

Además de estas coberturas, la empresa ofrece algunas cláusulas adicionales que buscan proteger al contratista contra extorsiones en Internet, contenido de medios e interrupción de red.

El sitio *Tudo sobre Seguros*, especializado en seguros, previsión y capitalización, afirma que "Las pólizas cubren daños causados a bienes y valores del asegurado y/o daños causados a bienes y valores de terceros (responsabilidad civil)"[27] y que hay que tener en cuenta los tipos de riesgos a los que las empresas están expuestas ya que "existen coberturas para pérdidas debidas a fallas en la seguridad de sistemas de información, para pérdidas derivadas de procesos judiciales o administrativos vinculados a violaciones de leyes de privacidad o daños en servidores, para ganancias salientes en función de pérdidas de datos y para gastos de honorarios de consultores para amenizar daños a la reputación de la compañía".[28]

Las agencias de seguros, preocupadas por las pérdidas que pueden tener, requieren que las empresas contratistas de seguros demuestren cierta preocupación por los riesgos y que estén atentas a los peligros e implantar algunas protecciones básicas en sus sistemas de seguridad interna. En Brasil, solo grandes aseguradoras ofrecen pólizas contra *cyber risks*.

Para ofrecer ese tipo de seguro, se hace necesario un profundo estudio de los riesgos a los que cada tipo de empresa está expuesta. No existe una póliza única para todas las empresas, ya que diferentes empresas almacenan y gestionan diferentes tipos de información y ofrecen diferentes tipos de servicios en Internet.

En México, la aseguradora Chubb ofrece un producto para pequeñas y medianas empresas que se "aplica para cualquier empresa que mantenga datos personales y corporativos como pueden ser bancos, farmacias, clubes deportivos, hospitales, laboratorios, tiendas departamentales y escuelas"[29]

27. "Riscos Cibernéticos. [S.l.]": *Tudo Sobre Seguros*, 2017. Disponible en: http://www.tudosobreseguros.org.br/portal/pagina.php?l=741. Acceso: 20/03/2018.

28. Ibídem.

29. Cruz, Ariadna. *Un seguro contra ciberataques: Este producto garantiza que las empresas retomen sus operaciones*. 2017. Disponible en: http://www.eluniversal.com.mx/

pues, según Yadim Trujillo representante de la empresa, "el principal mercado que están identificando son las pequeñas y medianas empresas pues de acuerdo con la firma Symantec 40% de los ataques cibernéticos están dirigidos a este sector empresarial"[30].

VI. Conclusión

En un mundo globalizado y altamente conectado, el ordenador y sus sistemas se han vuelto imprescindibles para la vida en sociedad. Todo se hizo más rápido y las distancias disminuyeron. La forma en que las personas se relacionan entre sí y con las empresas y los gobiernos ha cambiado. Cambió el mundo, cambió la forma en que se realizan las transacciones comerciales y cómo se ofrecen los servicios. Se crearon nuevas formas de interacción. Y con todo ese cambio, los delitos también evolucionaron, impulsando a cada gobierno a legislar para inhibir ataques, invasiones y accesos no autorizados y también para castigar a los criminales.

Las nuevas formas de crímenes no se cometen con una sola víctima a la vez, ahora los crímenes son mucho más perjudiciales y afectan a varios países al mismo tiempo, lo que requiere integración y compartición de soluciones y de legislaciones. Hoy en día, muchas empresas tienen como prioridad la protección a sus bases de datos, contratando seguros que garanticen una rápida reparación de los daños ocurridos en la empresa y sus clientes. Como los ataques no cesan y afectan cada vez a más personas, es posible prever en un futuro próximo el incremento en la oferta de nuevos seguros.

Por otro lado, para hacer frente a esta nueva realidad, las aseguradoras necesitan estar atentas al desarrollo tecnológico para que sus contratos ofrezcan productos eficientes que abarquen el mayor número posible de daños que puedan ocurrir en cada ataque cibernético.

Las empresas contratantes, a su vez, necesitan evolucionar en sus sistemas de defensa y deben pensar en rutinas de seguridad internas más eficientes. Hoy en día, es necesario hacer altas inversiones en *hardware* y *software* y en programas antivirus actualizados, personal altamente calificado

articulo/techbit/2017/05/22/un-seguro-contra-ciberataques. Acceso: 20/03/2018.

30. Ibídem.

para monitorear, identificar y eliminar ataques a sus redes internas y para controlar los accesos a Internet.

Todavía hay muchos desafíos en el área de seguros en entornos virtuales. La red mundial de computadoras hizo surgir un nuevo concepto de vida: la vida virtual que trae y continuará trayendo muchas ventajas y, como otra cara de la misma moneda, genera una dependencia de todos a los sistemas electrónicos de información. Tal situación ya no se puede ignorar. Se requiere que se incrementen y protejan las rutinas de la vida digital.

En el futuro, con las nuevas herramientas de interacción, ¿será posible que existan empresas que sean totalmente digitales? ¿Cómo podremos protegerlas de ataques cibernéticos? ¿Cómo tratar los bitcoins, la nueva moneda utilizada para cobrar las extorsiones de los ataques de los *ransonwares*? ¿Cómo lidiar con ataques a la Internet de las cosas (IoT-*Internet of Things*) donde todos los aparatos electrónicos se conectan y pueden ser controlados a través de aparatos celulares o de tabletas?

Es destacable la premura de la actuación de los especialistas, tanto del Derecho y de la Informática, en el sentido de proponer soluciones técnico-jurídicas a fin de contribuir con los gobiernos que tienen como objetivo proteger a sus ciudadanos y sus empresas.

Bibliografía

Arocena, Gustavo. "La regulación de los delitos informáticos en el Código Penal Argentino: Introducción a la Ley Nacional Nº 26.388". *Revista Jurídica da Facultad de Jurisprudencia de la Universidad Católica de Santiago de Guayaquil*, Guayaquil, v. 2011, n. 12, pp. 289-327, dez. 2011. Disponible en: http://www.revistajuridicaonline.com/2011/12/la-regulacion-de-los-delitos-informaticos-en-el-codigo-penal-argentino/. Acceso: 05/03/2018.

Cruz, Ariadna. *Un seguro contra ciberataques: Este producto garantiza que las empresas retomen sus operaciones*. 2017. Disponible en:
http://www.eluniversal.com.mx/articulo/techbit/2017/05/22/un-seguro-contra-ciberataques. Acceso: 20/03/2018.

D'Urso, Luiz Flávio Filizzola; D'Urso, Luiz Augusto Filizzola. "Ataque cibernético mundial é a comprovação da insegurança na internet". 17/05/2017. Disponible en: https://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet. Acceso: 5/03/2018.

Fuchs, Karin. "Riscos cibernéticos eminentes". *Revista Cobertura*, [S.l.], 22/03/2017. p.1. Disponible en: http://www.revistacobertura.com.br/2017/07/21/riscos-ciberneticos-eminentes/. Acceso: 18/03/2018.

Igrejas, Álvaro. "Risco cibernético: Ele pode atacar a sua empresa". Maio-2017. Disponible en: https://www.revistaapolice.com.br/2017/05/risco-cibernetico-pode-atacar-empresa/. Acceso: 5/03/2018.

Pinheiro, Emeline Piva. *Crimes virtuais: Uma análise da criminalidade informática e da resposta estatal*. 2003. 34 p. Monografia (Graduação em Direito). Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2006. Disponible en: http://www.egov.ufsc.br/portal/sites/default/files/emeline.pdf. Acceso: 15/03/2018.

Pinheiro, Patrícia Peck. *Direito Digital*. 6ª ed. São Paulo: Saraiva, 2016, p. 781.

Prado, Bruno. "Segurança digital: O que aprendemos em 2017 e as tendências para 2018". *Revista Apólice*, [S.l.], 19 Federal jan. 2018. Artigos, p. 1. Disponible en: https://www.revistaapolice.com.br/2018/01/seguranca-digital-artigo/. Acceso: 20/02/ 2018.

Savegnago, Jéssica Uliana; Woltmann, Angelita. *A regulamentação dos cibercrimes no Brasil: Uma análise jurídica dos "Três Pilares" norteadores do Marco Civil da Internet*. 2015. 17 p. Artigo científico (Anais do 3º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede) - Faculdades de Direito e Informática, UFSM - Universidade de Santa Maria, Santa Maria / RS, 2015. Disponible en: http://coral.ufsm.br/congressodireito/anais/2015/6-10.pdf. Acceso: 5/03/2018.

Sobrino, Waldo. "Los seguros de *cyber risk*". Diario *La Ley*, Año LXXXI Nº 104, Publicado: 05/07/2017.

Sydow, Spencer Toth. *Crimes informáticos e suas vítimas*. 2ª ed. São Paulo: Saraiva, 2015.

Tomeo, Fernando. *Redes sociales y tecnología 2.0*. 2ª ed. Buenos Aires: Astrea, 2014.

"Gastos com seguros contra ciberataques somam cerca de US$ 2 bi. [S.l.]": *Revista Apólice*, 02/02/2017. Disponible en: http://www.revistaapolice.com.br/2017/02/gastos- com- seguros- contra-ciberataques/. Acceso: 30/01/2018.

"Riscos Cibernéticos. [S.l.]: Tudo Sobre Seguros", 2017. Disponible en: http://www.tudosobreseguros.org.br/portal/pagina.php?l=741. Acceso: 20/03/2018.

"Estudo aponta Brasil como segundo país que mais perdeu dinheiro com crimes cibernéticos em 2017. [S.l.]": *Revista Cobertura*, 2018. Disponible en: http://www.revistacobertura.com.br/2018/01/22/estudo-aponta-brasil-como-segundo-pais-que-mais-perdeu-dinheiro-com-crimes-ciberneticos-em-2017/. Acceso: 19/01/ 2018.

"Brasil somou 62 milhões de vítimas de cybercrimes em 2017. [S.l.]": *Revista Apólice*, 2018. Disponible en: https://www.revistaapolice.com.br/2018/03/brasil-somou-62-milhoes-de-vitimas-de-cybercrimes-em-2017/. Acceso: 19/03/2018.

"Brasil precisa amadurecer quando o assunto é ciberataque. [S.l.]": *Revista Apólice*, 2017. Disponible en: http://www.revistaapolice.com.br/2017/05/brasil-precisa-amadurecer-ciberataque/. Acceso: 19/03/2018.

"Seguros contra ciberataques defendem e previnem patrimônio de empresas, clientes e fornecedores. [S.l.]": MDS Brasil, 2017. Disponible en: http://www.mdsinsure.com.br/seguros-contra-ciberataques-defendem-e-previnem-patrimonio-de-empresas-clientes-e-fornecedores/. Acceso: 20/03/2018.

"Cyber Edge. [S.l.]": AIG Seguros, 2018. Disponible en: https://www.aig.com.br/empresas/produtos/linhas-financeiras/cyber-edge#accordion-child_pr_cr_accordion_2. Acceso: 20/03/ 2018.

Bolsa de Seguros-Principais coberturas : Disponible en: https://www.bolsadeseguros.com.br/seguro-riscos-ciberneticos/