SEGURO DE RIESGOS CIBERNÉTICOS: ENFOQUE Y PERSPECTIVAS EN LA NUEVA NORMALIDAD [1]

CYBER RISK INSURANCE: APPROACH AND PERSPECTIVES ON THE NEW NORMALITY

Por *Hugo Fabián Pérez Carretta* [(*)]

Resumen: La llegada de la cuarta revolución industrial, el constante desarrollo de las tecnologías de Información y Comunicación (TICs) y el contexto de pandemia, han transformado drásticamente la vida digital, generando una nueva categoría de riesgo: el cibernético. Las ciberamenazas, -intromisión de terceros, daño en sistemas informáticos, filtración de información, robo y pérdida de datos, ciberextorsión y fraudes- acompañadas de tecnologías disruptivas, exigen una herramienta que contribuya a mesurar tales contingencias: un seguro cibernético, como mecanismo de respuesta indispensable. Este tipo de seguro abarca los elementos esenciales de los seguros tradicionales y también otros que lo distinguen y que en este trabajo se indagan en distintas fuentes con el propósito de reflexionar sobre sus significaciones, alcances, limitaciones y aplicabilidad. Conjuntamente, se analizan las coberturas disponibles para empresas y se cuestiona la factibilidad de su implementación en el ámbito de la Seguridad Nacional. Asimismo, se estudian la criptomoneda, la Justicia electrónica y la Inteligencia Artificial como riesgos asegurables, enfatizando en esta última.

Palabras claves: Seguro cibernético - Riesgos empresariales - Seguridad nacional - Criptoseguros - Inteligencia artificial asegurable

Abstract: The arrival of the fourth industrial revolution, the constant development of Information and Communication Technologies (ICTs) and the pandemic context have drastically transformed digital life, generating a new category of risk: cyber risk. Cyber threats -third-party intrusion, damage to computer systems, information leakage, data theft and loss, cyber extortion and fraud- accompanied by disruptive technologies, call for a tool that helps to measure such contingencies: cyber insurance, as an indispensable response mechanism. This type of insurance encompasses the essential elements of traditional insurance as well as others that distinguish it, which are explored in this paper in different sources with the purpose of reflecting on their meanings, scope, limitations and applicability. Together, the coverage available for companies is analyzed and the feasibility of its implementation in the field of National Security is questioned. Likewise,

[1] Artículo recibido el 3 de abril de 2021 y aprobado para su publicación el 23 de mayo de 2021.

[(*)] Abogado, Universidad Nacional de Córdoba. Diplomado en Cibercrimen y Evidencia Digital, Univ. Champagnat Mendoza. Diplomado en Derecho Digital, Acción Jurídica Córdoba. Miembro de la Asociación de Derecho Informático Argentina- ADIAr. Miembro de ICANN At-Large Staff. Especialista en Seguros de Riesgos Cibernéticos. Perito Judicial Informático, UTN Bs.As. Propietario de INFO&IUS "Red Social de Informática y Derecho". Contacto estudioperezcarretta@gmail.com

cryptocurrency, e-Justice and Artificial Intelligence are studied as insurable risks, with emphasis on the latter.

Keywords: Cyber insurance - Business risks - National security - Crypto insurance - Insurable artificial intelligence

DOI http://dx.doi.org/10.22529/rfd.2021(7)04

Introducción

El contexto de pandemia sanitaria de covid propagó también un nuevo tipo de virus de naturaleza tecnológica: el del ciberterrorismo, basado en ataques *online* a empresas y sistemas estatales especialmente vulnerables y sensibles durante esta crisis: laboratorios, centros hospitalarios, de investigación científica, como así también a redes de infraestructuras y de suministros de servicios públicos esenciales.

La actualización y capacitación constante a través de guías e informes nacionales e internacionales, delimitan el curso de las buenas prácticas en cuestiones de seguridad de la información. En su Panorama de amenazas ENISA[2] -Threat Landscape (ETL) de la Agencia de la Unión Europea para la Ciberseguridad identifica y evalúa las principales amenazas cibernéticas del período enero/2019 – abril/ 2020 brindando un total de 22 informes y un mapeo del panorama de amenazas en el escenario de covid. Según se observó los ciberdelincuentes mejoran sus capacidades, atacando de manera más rápida y eficaz.

La gestión de riesgos es un conjunto de actividades coordinadas para dirigir y controlar una organización[3] que demanda una permanente actualización en materia de ciberdelito y ciberseguridad a través de la problematización e indagación en un campo incipiente y novedoso por ser escasa la literatura científica actual.

Y en este sentido, reflexionar acerca del alcance y limitaciones del seguro de riesgos cibernéticos; analizar su aplicabilidad en otras dimensiones o planos: micro y macro empresas, Seguridad Nacional, criptomonedas e inteligencia artificial, con énfasis en esta última, son los dos objetivos generales de este

[2] http://www.debatesiesa.com/liderar-en-la-cuarta-revolucion-industrial/, 26/05/2020.
[3] Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica. Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. MAGERIT – versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Secretaría General Técnica*, Madrid, 2012.

trabajo. Mientras que, indagar sobre riesgos cibernéticos a partir de datos estadísticos, artículos, guías, reportes, legislación nacional y resignificarlos epistemológicamente, son sus dos objetivos específicos.

1.Concepto y caracteres distintivos del riesgo cibernético

El riesgo asegurable**,** de acuerdo con del manual Principios Técnicos del Seguro[4] es la posibilidad de sufrir una pérdida o un daño; es una eventualidad, algo que tiene la posibilidad de suceder, un acontecimiento incierto que, de ocurrir, traerá como consecuencia un desequilibrio económico para la persona o entidad que lo sufre. Pero, si reviste el carácter de "cibernético", se amplia e intensifica el factor riesgo y las consecuencias, debido a la imprudencia, negligencia y/o impericia en la gestión de ciberseguridad y manejo de datos.

En la actualidad se advierte una resignificación en el concepto tradicional de *riesgo,* del cual se infiere que, "riesgo cibernético" es todo aquel que exponga a individuos, entidades públicas y privadas al peligro de sufrir daños sobre activos digitales, reputación online, marca comercial, fraude cometido por robo de información, e incluso daño físico, producto del uso de información y medios electrónicos, por *sucesos (inesperados o no deseados) con consecuencias, en detrimento de la seguridad del sistema de información*[5].

Los seguros tradicionales poseen características esenciales y privativas respecto del riesgo asegurable que debe ser: incierto, aleatorio, posible, concreto, de lícito interés, fortuito, de contenido económico y extraño a la voluntad de las partes. A diferencia del riesgo tradicional, el cibernético además de incierto, es eventual, porque está sujeto a un acontecimiento impreciso, prácticamente impredecible; asimismo es aleatorio y de alcance ilimitado, en el sentido de que

[4] FAPASA. *Principios Técnicos del Seguro*. Bs As: Centro de Capacitación Federal, 2019, p.24.
[5] Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica. Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. MAGERIT – versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Secretaría General Técnica*, Madrid, 2012.

desconoce límites geográficos, culturales, económicos y puede tomar como víctima tanto a particulares como entidades públicas o privadas.

Profundizando, el riesgo cibernético es posible, porque aun cuando se realiza toda diligencia necesaria para que no ocurra la potencialidad dañosa, la afectación a bienes o personas está siempre latente. También es relativamente previsible, debido a que en la actualidad se sabe que con solo navegar en Internet existen ciertos riesgos implícitos que implican un peligro inminente, actual o futuro para usuarios de internet e intranet; lo que lleva a tomar recaudos y a ser diligentes al exponer o manipular datos personales o secretos comerciales.

A su vez, el riesgo cibernético es concreto; el daño ocasionado por el mismo a la víctima se puede valorar cuantitativa y cualitativamente, generalmente deriva de actos considerados ilícitos para el derecho interno e internacional; está vinculado a un lícito interés, el estado debe poner los medios y los recursos para su protección; puede afectar derechos de contenido patrimonial propios o de tercero e incluso es extensivo a los de contenido moral o extrapatrimonial; se desarrolla en entorno online y offline; es dinámico, debido a que las técnicas de ataque están en constante evolución; es complejo, por estar compuesto de muchos y variados aspectos; y finalmente, puede desencadenar consecuencias legales desfavorables para quien es víctima de un incidente de seguridad informática, y lo convierte en responsable por su acción u omisión incluso frente a terceros.

2.Contrato de Seguro de Riesgos Cibernéticos

2.1 Objeto, consentimiento, actividades, cobertura y suma asegurada.

El material consultado de las tres aseguradoras sobre la oferta de paquetes de seguro de riesgos cibernéticos en Argentina, permite inferir elementos comunes y distinguir rubros a los que dan cobertura, que continuación se exponen brevemente.

El artículo 2 de la Ley de Seguros Nº 17.418[6], establece que el contrato de seguro puede tener como objeto toda clase de riesgos siempre que exista interés asegurable, salvo prohibición expresa de la ley, extremos claramente presentes en este moderno esquema de riesgo cibernético. Como todo contrato, el de seguro de riesgos cibernéticos, requiere el consentimiento de las partes al suscribirlo.

Las partes interesadas en protegerse de estos siniestros abarcan: administradores, directivos o socios, responsable de seguridad, director de cumplimiento o de asesoría jurídica interna de la sociedad, empleados de empresas o pymes; también el Estado en algunas de sus reparticiones y particulares, aunque en menor medida.

Las condiciones contractuales de las coberturas otorgadas tienen limitaciones o restricciones que se estipulan en el clausulado de cada póliza en particular. Las aseguradoras consultadas focalizan su interés en las pymes, eje de la oferta de diferentes paquetes de seguros.

Cabe aclarar que existen actividades económicas que por el carácter del riesgo pueden ser asegurables y no asegurables.

En relación con las actividades económicas asegurables, la lista suele ser muy extensa y excede los objetivos de este trabajo, por lo tanto se citan las más destacadas según el nivel de riesgo:

Alto: agencias y organizadores de viajes, asistencia a turistas, inmobiliarias -compra y venta, arriendo, etc.-, educativas, academias, hoteleras; de sedes políticas, de servicios jurídicos y notariales, suministro de electricidad, gas y agua, venta de electrodomésticos, equipos eléctricos, electrónicos y sus accesorios.

[6]Ministerio de Justicia y Derechos Humanos. Presidencia de la Nación. *Ley de Seguros*. Bs As, Argentina,1967.

Medio: agencias de noticias y publicidad, empresas de encomiendas y transportadoras, imprentas, editoriales, organizaciones empresariales, profesionales y de empleadores; salas de cine y teatros.

Bajo: bibliotecas y museos, fabricación de equipos eléctricos y electrónicos, restaurantes, heladerías, cafeterías, salones de té y comidas rápidas.

Por último, son riesgos ´no asegurables´ las siguientes actividades: institución financiera, "*big four*", *"call center"*, cabinas telefónicas, telecomunicaciones, servicios informáticos, administración pública, casinos y juegos de azar, salas de internet, laboratorios clínicos y clínicas médicas, las que tienen ingresos mayores a USD 5.000.000 o su equivalente en Pesos Argentinos, las actividades que requieran más de 200 empleados; y por último, según la aseguradora, no tengan siniestralidad en los últimos tres años.

La cobertura se apoya en tres pilares, que con sutiles diferencias entre compañías son:

- Por daños propios: recuperación de información digital, interrupción de su actividad empresarial, extorsión cibernética, transacciones bancarias fraudulentas, gastos para proteger su reputación.
- Por daños a otros: responsabilidad por violación de información confidencial o datos personales, responsabilidad por software malicioso o virus informático, publicación en medios digitales, gastos de defensa-judiciales.
- Manejo de Crisis: gastos forenses, gastos de defensa, gastos sin previa autorización.

En cada caso, las aseguradoras se encargan de suministrar los medios técnicos (asistencia calificada), económicos (pago o reembolso de gastos o perjuicios ocasionados) y legales (asistencia letrada en caso de demandas por daños), para contrarrestar la contingencia sufrida, el siniestro o incidente de seguridad siempre que estén *razonablemente* a su alcance y permita restablecer

la situación a su estado anterior a la brevedad posible y dentro de los parámetros contractuales.

Entonces, ¿qué no estaría cubierto? Multas o sanciones pecuniarias, administrativas o de cualquier naturaleza, y daños punitivos o ejemplarizantes, lesiones personales, muerte o enfermedades, trastornos emocionales ocasionados a terceros; deterioro, destrucción o pérdida de bienes tangibles; interrupción global del servicio de internet; incumplimiento de obligaciones contractuales excepto la derivada de la seguridad de la información; responsabilidad profesional; daños ocasionados por terceros contratados por su proveedor de servicio.

Respecto de la suma asegurada, ¿qué criterios se aplican? Las compañías se vieron en el problema de elegir un criterio que permita establecer un valor a los activos tangibles e intangibles puestos en riesgo; ya que su mensura puede verse teñida de subjetividades por parte del contratante. Para ello, las aseguradoras, establecieron cotizadores -la mayoría online- mediante los cuales, potenciales clientes pueden tomar de referencia un importe que finalmente verán reflejado en el valor asegurado para cada caso, en la póliza.

Los ítems para cotizar son: en primer término, el tipo actividad económica, a la que las aseguradoras le otorgan un nivel de riesgo alto, medio, bajo; o no asegurable. Luego, la suma asegurada y deducible, ambos en dólares; en tercer término, los ingresos del asegurado también en dólares, para evitar calcular en base a moneda que pueda devaluar como el peso, y que puede oscilar en la suma escalonada de 0 a 100.000 dólares, en un primer tramo, y hasta los 5.000.000 de dólares anuales como máximo, según la compañía aseguradora.

Posteriormente, el interesado además de completar el cotizador con sus datos, manifiesta sus ingresos, en forma equivalente a una declaración jurada, para poder calcular la prima[7]. Por su parte, la aseguradora determina una prima

[7]Es el precio del seguro y representa la contraprestación del riesgo asumido por el asegurador, entendido como el estricto valor del riesgo más los gastos y beneficios de gestión de la empresa aseguradora.

técnica a partir de la información brindada por el interesado, le aplica gastos de explotación y producción para obtener la prima total, a la vez que le aplica recargos financieros e impuestos para obtener el premio anual dividiéndolo en diez meses o cuotas, lo que el asegurado finalmente deberá pagar en cada mes.

Por último, existen dos modalidades en la oferta de estos seguros: una, la misma empresa de seguros ofrece pólizas propias; y otra, mediante operaciones de "fronting"; es decir, la empresa de seguros local contrata con su asegurado y al mismo tiempo reasegura la mayor parte o el total del riesgo con otra compañía del extranjero, especializada en este tipo de seguros; cuestión no menos importante si se toma en cuenta el principio de la responsabilidad solidaria, en caso de accionar contra la compañía aseguradora y la reaseguradora, por incumplimiento total o defectuoso de los términos de contratación.

3.Riesgos cibernéticos en el escenario empresarial

El proceso de digitalización es la causa de transformaciones a gran escala en múltiples aspectos de negocios, proporcionando oportunidades incomparables para la creación y captura de valor, al tiempo que representa una fuente importante de riesgo[8].

Frente a nuevos riegos, se puede analizar cómo se ve afectada una empresa si recibe un ciberataque; y en tal sentido, se puede decir -sin ser excluyentes- que la afectación inmediata se relaciona con la pérdida de ingresos como consecuencia de la interrupción de la actividad, la pérdida de información empresarial sensible, lesiones a su reputación y a la confianza de sus clientes. Sin dejar de mencionar, sanciones de entes de control como inhabilitaciones,

[8] En la jerga de seguros, el riesgo es el peligro de sufrir daños patrimoniales; puede referirse a un daño
material o pérdida de la posesión de un bien, a la aparición de una deuda involuntaria, a la desaparición
o disminución de ingresos. A estos riesgos se suman los relacionados con la duración de la vida humana
y los gastos incurridos para su conservación en caso de enfermedad o accidente.

suspensiones de licencias para operar en la actividad y reclamos o demandas por daños provocados a terceros producto de un ciberataque.

El costo de pérdidas derivadas de un ataque o falla cibernética varían de un caso a otro y de país a país. Por ejemplo, en Estados Unidos, este costo asciende a 5 billones de dólares anuales, mientras que en Australia suma poco más de la mitad, 2.9 billones de dólares.

Pese a las pérdidas millonarias registradas anualmente, sin embargo, un aspecto irreparable como consecuencia de un daño cibernético es la reputación de la empresa afectada, especialmente si se gestionan datos de identidad de terceros que pueden verse vulnerados; razón por la cual, además de contar con protocolos internos de prevención, es importante adquirir un seguro que brinde protección ante este tipo de amenazas y sus distintas repercusiones.

No solo hay una pérdida patrimonial por gastos de abogados, perjuicios generados a terceros, costos de reemplazo de la información o sistemas y la utilidad no percibida por interrupción del negocio; sino también, honorarios de expertos por manejo de crisis.

Por todas las razones explicitadas anteriormente, es oportuno citar la Guía de Ciberataques de Instituto Nacional de Ciberseguridad[9], Oficina de Seguridad Internauta (OSI) de España, que los diferencia entre ataques de los que pueden ser víctimas personas físicas y jurídicas, categorizándolos más exhaustivamente en: ataques a contraseñas, ataques por ingeniería social (phising, vishing, smishing, spam, fraude online); ataques a conexiones (redes wifi falsas, ip-web-email-dns spoofing, snifing, man in the middle, ataques a cookies) y ataques por malware (virus, anuncios maliciosos, spyware, falsos antivirus, troyanos como keyloggers y ransomware, apps móviles maliciosas). La lista no es excluyente pero claramente demanda una verdadera toma de conciencia en materia de prevención de posibles ataques, dada la diversidad y complejidad de los mismos.

9 Ministerio de Asuntos Económicos y Transformación Digital. Guía de Ciberataques. Madrid, España: Instituto Nacional de Ciberseguridad, 2020.

3.1 ¿Existen recomendaciones a la hora de establecer defensas?

Los portales especializados en ciberseguridad recomiendan la micro segmentación, es decir, construir pequeños muros alrededor de la información que no puede perderse; además de incorporar servicios de análisis de datos para detectar infracciones y protegerlo, diseñar equipos de piratería ética para encontrar y eliminar vulnerabilidades complejas en toda la organización. Así mismo, las empresas deben considerar otras medidas para mejorar la seguridad, como el uso de análisis de *big data*, piratería de equipos o computación cuántica, a estos procedimientos se le puede adicionar el seguro de riesgos cibernético a fin de robustecer y de alguna manera garantizar la continuidad funcional de la pyme.

A modo de corolario de este apartado, se tiene en cuenta los datos proporcionados por la "Encuesta de Percepción del Riesgo Cibernético 2019": 1,500 empresas a nivel global, 531 en Latinoamérica, en un 73% clasifica el riesgo cibernético como una de sus cinco principales preocupaciones, en comparación con el 47% del año 2017. Una de cada cinco organizaciones lo considera su riesgo principal. El 27% de las empresas en Latinoamérica desconfían totalmente de su capacidad para responder a un evento cibernético[10].

Según la mencionada encuesta, en Latinoamérica crece el número de empresas que cuentan con un seguro cibernético, aunque la región todavía está lejos de la media global (29% vs 47%). En el caso de las grandes empresas, el porcentaje de penetración del seguro cibernético crece hasta el 40%.

4. Seguro de riesgos cibernéticos para la Seguridad Nacional: su viabilidad.

En Argentina, los principales problemas de seguridad informática a nivel estatal evidenciados a través de información mediática, son: falta de control del tráfico de datos, redes inseguras, utilización de emails personales y/o gratuitos en la organización, códigos inseguros, servidores desactualizados, inexistencia de

[10] https://www.microsoft.com/security/blog/2019/09/18/marsh-microsoft-2019-global-cyber-risk-perception-survey-results/, 18/09/2019.

backups y de políticas de recomposición en caso de eventos que lesionen su normal desenvolvimiento (*disaster recovery)*.

Las fuerzas de seguridad han sufrido diferentes ataques en estos últimos cinco años: desde el *deface* -cambio estético en las portadas de sitios web- del que fue objeto Gendarmería, Ejército y Policía Federal Argentina, y la filtración de datos de agentes que puso en riesgo sus vidas (causa denominada Gorra Leaks), hasta diversos casos de *phishing* que permitieron el acceso a cuentas de correo del Ministerio de Seguridad o bien a la cuenta de Twitter de Patricia Bullrich, la entonces Ministra de esa cartera; y más recientemente el ataque *ransomware* a Migraciones donde se filtró información sensible del Estado[11], son todos hechos que claramente ponen en riesgo la integridad y seguridad del país y de sus ciudadanos.

En tal sentido, el Rastreador de Operaciones Cibernéticas (*cyber operation trakers*) del programa de Política Digital y Ciberespacial, una base de datos de los incidentes públicos patrocinados por estados, informa que sólo en 2019 hubo un total de setenta y seis ciberoperaciones contra países, en su mayoría actos de espionaje[12].

Por lo hasta aquí expuesto, cabe preguntarse: ¿Cuán viable es un seguro de riesgos cibernéticos para la Seguridad Nacional? ¿El Estado posee mecanismos y procedimientos que garanticen la ciberseguridad? ¿Los perjuicios por negligencia estatal o sus dependientes ocasionados al ciudadano, tendrían cobertura?

Ensayar una respuesta a estos interrogantes demanda diferenciar primeramente ciberseguridad de ciberdefensa. Al hablar de ciberseguridad, se referencia acciones básicas que desarrolla una entidad pública o privada para proteger prospectivamente de forma sistemática y sistémica los activos de información crítica que se encuentran distribuidos en toda su infraestructura y

[11] https://www.pagina12.com.ar/290338-hackers-atacaron-la-direccion-nacional-de-migraciones, 07/09/2020.
[12] https://www.cfr.org/cyber-operations, 07/09/2020.

que tienen directa incidencia con su operatividad funcional. En cambio, la ciberdefensa además de prevenir ataques como hace la ciberseguridad, da respuesta a los mismos mediante nuevos ataques, con el propósito de salvaguardar la seguridad.

La Unión Internacional de Telecomunicaciones (ITU) establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: construcción de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional[13].

A modo de conclusión de este apartado, es lógico pensar que no están dentro de las facultades de ninguna empresa aseguradora -privada- la posibilidad de auditar o verificar por sí sola que se cumplan los requisitos o condiciones como los que aconseja la ITU, excluyendo de su potestad aquellas cuestiones inherentes a la soberanía del Estado, ya que éste último es el encargado y el responsable de garantizar la seguridad interna e internacional.

En esta línea de pensamiento se considera que el camino a seguir por parte del Estado es diseñar su propio fondo o destinar presupuesto para su protección; esto es, asegurarse a sí mismo para hacer frente a las contingencias propias de los riesgos cibernéticos y adecuarse a los estándares internacionales de ciberseguridad para una correcta implementación de herramientas destinadas a la ciberdefensa.

En la "Declaración internacional: cifrado de extremo a extremo y seguridad pública" del Departamento de Justicia de los Estados Unidos[14], se cuestiona la afirmación de que la seguridad pública no puede protegerse sin comprometer la privacidad o la seguridad cibernética; y por otra parte, los

[13] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, 07/09/2020.
[14] https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety, 11/10/2020.

organismos signatarios se comprometen a trabajar con la industria para desarrollar propuestas razonables, que permitan a las empresas de tecnología y los gobiernos proteger al público y su privacidad, defender la seguridad cibernética y los derechos humanos, apoyando la innovación tecnológica.

También los estados signatarios apelan a empresas de tecnología a que trabajen con los gobiernos para enfocarse en soluciones razonables y técnicamente factibles. Si bien, la Declaración no lo dice, es razonable pensar que para lograr tales objetivos haya que contemplar un seguro de riesgos cibernéticos a cargo de organismos públicos.

5. Criptomonedas como valor asegurable.

La Ley 27.430 incorporó como hecho imponible del Impuesto a las Ganancias a las operaciones realizadas con criptomonedas; decisión no menos importante a la hora de definir la naturaleza jurídica de las mismas, y de cuestionar si actualmente es viable un criptoseguro. Profundizando, cabe diferenciar dos corrientes impositivas: una, que le reconoce a las criptomonedas el mismo tratamiento que las monedas de curso legal; y otra, que las equipara a operaciones realizadas con bienes activos financieros y bienes inmateriales, entre otros.

Argentina, con algunas particularidades, se enrola en la segunda corriente que considera las criptomonedas como activos financieros, es decir, bienes. Cabe preguntarse aquí, si las criptomonedas son activos financieros o se la puede considerar solamente monedas. En respuesta a tal interrogante, en el informe del Comité de Interpretaciones de Normas Internacionales de Información Financiera (CINIIF) se dictaminó que las criptomonedas "no son dinero en efectivo ni un instrumento de patrimonio de otra entidad"[15]; lo que es lo mismo que, las posesiones de criptomonedas no son equivalentes a efectivo ni a activos financieros, sino que cumplen con la definición de un activo intangible.

15 https://www.criptonoticias.com/regulacion/criptomonedas-activos-intangibles-organismo-estandares-contabilidad/, 24/09/2019.

Haciendo un análisis de las coberturas que ofrecen las empresas aseguradoras, se puede afirmar que, en general, aseguran la pérdida por desaparición, destrucción o deterioro de dinero, caja fuerte, cheques al portador, u otros valores especificados en las condiciones de contratación para casos de robo, incendio, rayo o explosión. Por valores dichas empresas acuerdan en designar al "dinero nacional o extranjero, en billetes o monedas de oro, plata u otros metales, certificados de acciones, bonos, cupones, cheques, giros postales, estampillas y cualquier otra manifestación semejante de valores"[16]; pero, tangibles.

Claro está entonces que, considerar a las criptomonedas como activos intangibles (no financiero), ni dinero, ni manifestación de valor semejante, representa un revés con respecto al reconocimiento o estatus prospectivo de las mismas como monedas, y a su falta de previsión como objeto asegurable dentro del escenario de las nuevas tecnologías.

Quienes utilizan criptomonedas como medio transaccional, ya sea para ahorrar, invertir, o compra-venta, conocen los riesgos del entorno cibernético. Solo por ilustrar, los hackeos en plataformas online de numerosas empresas de *exchange*, provocaron la fuga de criptomonedas; mediante el *phishing* accedieron a billeteras de usuarios; robo de datos incluidas clave pública y privada de ´billeteras frías´, hasta el asalto a mano armada para obligar a la víctima a transferir desde su aplicación móvil las *criptodivisas* directamente usando el código QR mostrado -en persona- por su victimario.

Para concluir, es apropiado señalar que, la vida digital y en particular el comercio electrónico cómo se desarrolla en la actualidad, requieren de un mecanismo de respuesta a diferentes contingencias que puede plantear el uso de tecnologías disruptivas, las criptomonedas entre otras.

[16] ZURICH ARGENTINA, Compañía de Seguros S.A. *Póliza Integral de Comercio*. Cláusula Particular 18/501. Bs As, Argentina, 2020.

Las empresas aseguradoras deberán integrar y adaptar sus pólizas a estas nuevas necesidades para poder hacer frente de modo razonable a eventuales perjuicios; para tal fin deberán mínimamente especificar en forma expresa: qué se entendería por criptomonedas, cómo llevar un registro válido de las mismas, qué medidas de seguridad debería tomar su propietario, cuál sería la forma de diligenciar el siniestro (caso de robo, extravió de la wallet, etc.), formas y plazos para indemnizar y causales de exclusión de la cobertura.

6. Inteligencia artificial, Justicia electrónica y seguros

Actualmente convivimos con el auge de empresas que comenzaron a desarrollar soluciones -de la mano de abogados y tribunales- basadas en sistemas automatizados que permiten reemplazar aquellas tareas que requieren más tiempo. Las aplicaciones para Inteligencia Artificial (IA) son una de las principales soluciones, y tienen por finalidad predecir procesos y descubrir nuevos patrones.

La IA, así concebida, favorece la toma de decisiones autónomas dentro del ámbito judicial, minimiza procesos y tareas que requieren de mucho tiempo a jueces y abogados; también permite, reducir el papeleo, la burocracia, los gastos en tiempo y dinero de ciudadanos y funcionarios, y mejorar la gestión y administración pública.

Dos casos de éxito en la implementación de IA son China y Estonia. China, a través del llamado Tribunal de Internet de Pekín basado en IA, tiene la capacidad de “estudiar” casos anteriores y verificar la jurisprudencia en tiempo real para resolver litigios simples. En Estonia, siguiendo el esquema anterior, las partes presentan sus demandas y pruebas en formato digital, para que luego un juez de inteligencia artificial analice la documentación y emita sentencia, con la

aclaración de que si alguna de las partes disiente respecto del resultado, podrá presentar un recurso de apelación ante un juez[17].

A las ventajas antes señaladas, se enfrentan las desventajas, que pueden tener los modelos de IA; una es la mala o inapropiada utilización, además de problemas de sesgo en los sistemas de reconocimiento facial que en muchos casos fueron portadas de diferentes sitios de noticia, y dio origen al estudio sobre la crisis de diversidad de la IA llevado a cabo por IA NOW, un grupo de investigación de la Universidad de Nueva York[18].

Sin embargo, la IA alcanzó un grado importante de avance y en la actualidad superó al ser humano en vista, comprensión lectora, lenguaje de signos, traducción, lectura de labios, entre otros procedimientos y habilidades, a punto tal que sistemas de IA que fueron entrenadas a partir del conocimiento humano, ahora enseñan a otras IA, hasta que estas últimas superan a su entrenador.

Luego, de una muy breve síntesis del estado actual de la IA cabe preguntarse sobre su responsabilidad civil, para concluir con su vinculación a los seguros que se vienen tratando. En Argentina no se dispone de normativa específica sobre responsabilidad por el uso de la IA, lo que lleva necesariamente a subsumirla en las normas y principios de derecho interno.

La IA se encuentra dentro de las tecnologías de "elevado riesgo de causar daños a otros", ya sea por actualizaciones defectuosas en productos destinados a la circulación, por pérdida o destrucción de datos personales de usuarios, fallas operativas, entre otras causas, y se la debe dotar tanto de una compensación por daños, -basada en la responsabilidad objetiva- como un seguro obligatorio, según aseveró el Expert Group on Liability and New Technologies.

En ese contexto, surgen inmediatamente cuestionamientos como: ¿quién responde por tales daños, la IA o su propietario? ¿Se la puede dotar de

[17] https://confilegal.com/20191013-china-y-estonia-desarrollan-jueces-virtuales-basados-en-inteligencia-artificial-para-resolver-demandas-de-cantidad, 13/10/2019.
[18] https://fortune.com/2019/04/23/artificial-intelligence-diversity-crisis, 13/10/2019

personería jurídica y un patrimonio propio? ¿Se les reconoce capacidad de obrar? ¿Pueden tener legitimación procesal propia? ¿Se las puede incautar, embargar o subastar para hacer frente a los daños ocasionados?

En la búsqueda de responder tales interrogantes, es factible ensayar algunas respuestas desde la perspectiva de la responsabilidad civil en el Código Civil y Comercial de la Nación (C.C.C.N). Al decir de Pizarro y Vallespinos, para determinar el concepto de daño es menester formular una distinción necesaria, por un lado daño en sentido amplio (conceptualizado en el artículo 1737) y daño resarcible (reglado bajo la impropia denominación indemnización en el artículo 1738 y en el artículo 1741).

El C.C.C.N, reconoce dos grandes tipologías de daño: patrimonial (o material) y extrapatrimonial (o moral). Daño patrimonial o económico es el menoscabo que experimenta el patrimonio de una persona, en sus elementos actuales, o en sus posibilidades normales, futuras y previsibles, a raíz del hecho generador. El daño patrimonial produce una merma en el patrimonio del damnificado, en tanto que, el daño extrapatrimonial o moral, se define como una minoración en la subjetividad de la persona humana, derivada de la lesión a un interés no patrimonial, es decir, una modificación no valiosa del espíritu, en el desenvolvimiento de su capacidad de entender, querer o sentir, consecuencia de una lesión a un interés no patrimonial[19].

Los artículos 1710 a 1713 incluido, del mencionado código incorporó el reconocimiento legislativo de la función preventiva en el Derecho de Daños, que brinda una herramienta legal específica para asegurar su efectividad a través de la denominada “acción preventiva” y cuyo fundamento se asienta en que antes del deber de reparación del daño, se debe evitar que ese daño ocurra; y que por lo tanto, el resorte del deber resarcitorio se accione únicamente cuando la prevención ha fracasado[20].

[19] PIZARRO, Ramón Daniel y VALLESPINOS, Carlos Gustavo. *Tratado de Responsabilidad Civil. Tomo 1. Parte General*. Ed. Rubizal-Culzoni, 2017, p. 131 y ss.
[20] *Código Civil y Comercial de la Nación*, 2015.

En la actualidad la función resarcitoria, plasmada en los artículos 1716 y ss. amplió la concepción de los efectos perjudiciales del hecho dañoso entre víctima y victimario, hacia la afectación plural de personas, con incidencia negativa en lo social, cultural y económico.

Según lo expuesto, la IA puede considerarse "cosa riesgosa", y en apoyo a tal postura se encuentra la Teoría del Riesgo Creado plasmada en el artículo 1757, que estipula la responsabilidad objetiva derivadas del riesgo o vicio de las cosas y de las actividades que sean riesgosas o peligrosas; y en el artículo 1758 al establecer los sujetos responsables en forma concurrentes del daño causado por las cosas, es decir, el dueño y el guardián.

Seguidamente se abordan los puntos de conexión de la Inteligencia Artificial (IA) con los seguros de riesgos cibernéticos que venimos tratando y su vinculación con el derecho de daños. El uso de sistemas de IA en drones, vehículos autónomos, cámaras de vigilancia, entre otros dispositivos tecnológicos, trae aparejado cierto riesgo propio del software incorporado a los mismos.

Dicho de otro modo, la actualización del software tiene directa incidencia con el perfil de riesgo aplicado a una determinada tecnología: a menor actualización, mayor riesgo y potencialidad de daño, sobre todo en productos de tecnología digital que se han puesto en circulación.

> Los productos de tecnología digital están abiertos a extensiones de software, actualizaciones y enmiendas una vez que se han puesto en circulación. Cualquier cambio en el software del sistema puede afectar el comportamiento de todo el sistema o de componentes individuales o puede extender su funcionalidad. El software puede ser reparado, actualizado o revisado por el productor del sistema o por componentes individuales del sistema o por terceros, de una manera que pueda afectar la seguridad de estas tecnologías. Las actualizaciones suelen cerrar los agujeros de seguridad a través de

> correcciones, pero los nuevos códigos también agregan o eliminan características de manera que cambian el perfil de riesgo de estas tecnologías[21].

Entonces, ¿los daños ocasionados por la utilización de IA entran dentro de la categoría de riesgo cibernético asegurable? la respuesta es un rotundo sí, ya que como cualquier software –algoritmo- es vulnerable y puede ser adulterado o modificado con fines diferentes a los que fue creado, afectando su comportamiento o la seguridad de la tecnología aplicada. En el mismo sentido, cabe preguntarse, ¿es viable un seguro para IA cuya cobertura repose sobre los tres pilares -daño propio, daño a terceros y manejo de crisis- que se analiza al inicio del presente trabajo?, la respuesta también es afirmativa porque se cumplen las condiciones para otorgar cobertura y podría integrar los denominados riesgos cibernéticos asegurables.

En cuanto al objeto del contrato de seguro, la IA puede ser perfectamente objeto de ese contrato, pero dentro de una categoría autónoma, ya que no se la puede equiparar e incorporar plenamente a los seguros tradicionales, para lo cual será necesaria su incorporación a la lista de actividades económicas asegurables ya sea por su utilización, como fabricante de la IA, o como prestador de un servicio basado en la misma, al tiempo que requerirá asignarles un nivel de riesgo según cada caso en particular.

Los desafíos actuales deben encaminarse a dotar a la IA de un marco normativo específico, que establezca deberes y obligaciones a su dueño y guardián, la responsabilidad aplicable por su utilización, un sistema preventivo y resarcitorio propio, un registro detallado de libre acceso de estos sistemas que permita ser auditado en cualquier momento y un seguro obligatorio compatible con los riesgos cibernéticos que se han desarrollado.

[21] DANESI, Cecilia. C. "Inteligencia artificial y responsabilidad civil: un enfoque en materia de vehículos autónomos". Ed. Thomson Reuters, *Sup. Esp. Legal Tech*, AR/DOC/2374/2018, 2018, p.9.

Conclusiones

Según la "Guía para una adecuada gestión del riesgo cibernético" de Deloitte[22] las organizaciones públicas y privadas deberían poder responder seriamente los siguientes interrogantes: ¿demostramos la debida diligencia, propiedad, y la gestión efectiva del riesgo cibernético?, ¿cómo nuestro programa de riesgo cibernético y capacidades se alinean a los estándares de la industria y se pone a la par de nuestros competidores?, ¿tenemos una mentalidad cibernéticamente enfocada y una cultura de conciencia cibernética en toda la organización?, ¿qué hemos hecho para proteger a la organización contra riesgos cibernéticos de terceras partes?, ¿podemos contener daños rápidamente y movilizar diversos recursos de respuesta cuando un incidente cibernético ocurra?, ¿cómo evaluamos la efectividad del programa de riesgo cibernético de nuestra organización?.

Para atender tales interrogantes, cabe decir que será cada vez más necesario contar con un experto en ciberseguridad en las organizaciones para atender con premura los incidentes que se puedan provocar. El denominado *compliance*, es importante para identificar y clasificar los riesgos operativos y legales a los que se enfrentan empresas y entidades públicas, a fin de establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos. Dicho término además implica, adaptar recursos y funcionamiento de la empresa a los estándares, reglamentaciones, regulaciones y requerimientos vigentes dados por la organización política y legal del país donde se encuentra.

Finalmente adoptar medidas de "*criminal compliance*", en otras palabras, no sólo adecuar o readecuar la normativa de los seguros tradicionales a estos nuevos seguros de riesgos cibernéticos o su incorporación como categoría autónoma, sino también, a los estándares de normalización internacional desde

[22] Brinda servicios relacionados a organizaciones públicas y privadas de diversas industrias. Https://www2.deloitte.com/co/es/pages/risk/articles/gestionando-el-riesgo-cibernetico.html, 13/10/2019.

su contratación, para proteger la relación de consumo, de los datos personales e información comercial sensible, la prevención del cibercrimen y todo otro derecho esencial, en cuanto sea posible para satisfacer razonablemente las exigencias de su implementación.