Sección Uruguaya

XVII JORNADAS NACIONALES DE DERECHO DE SEGUROS

LA APORTACIÓN DEL USO MASIVO DE DATOS (BIG DATA) Y DE LA CADENA DE BLOQUES (BLOCKCHAIN) a la cadena de valor del seguro.

Joaquín Alarcón Fidalgo

Abogado, Miembro del Consejo Directivo de SEAIDA

Presidente del Grupo Internacional de Trabajo de NT de AIDA

ÍNDICE

Hablar de Big Data (BD) y de Blockchain (BC) está de moda. Todo el mundo habla del fenómeno, a veces, con cierta confusión, pero es algo que,

después de la nanotecnología, va a cambiar, de manera definitiva, nuestro enfoque asegurador, como lo está haciendo en otros sectores.

La analogía con la nanotecnología es un tópico frecuente; en esta el principio es que cuando se alcanza el nivel nano (la milmillonésima parte de un metro) las propiedades físico-químicas de los materiales se modifican muchas veces; se pueden dar, por ejemplo, metales más flexibles o cerámicas que se expanden.

Por el contrario, cuando aumentamos la cantidad de los datos que analizamos, podemos hacer cosas que no era posible con una cantidad menor; mediante el análisis de grandes conjuntos de datos podemos identificar correlaciones y predecir eventos futuros. El sistema BC puede revolucionar aún más el sector asegurador mediante, por ejemplo, los contratos inteligentes.

Este nuevo escenario en el que se ve inmerso el seguro nos lleva a plantearnos determinadas cuestiones relacionadas con la mecánica B D y BC y con sus repercusiones concretas en el sector asegurador.

A. BIG DATA

1. Qué son

Un dato es un representación simbólica (numérica, alfabética, algorítmica) de un atributo o variable cuantitativa o cualitativamente; describe hechos empíricos, sucesos y entidades, es el elemento primario, la mínima unidad de información, siendo irrelevante por sí solo. **La información**, en cambio, es un conjunto de datos procesados que tienen significado y se pueden utilizar para diferentes tareas.

Big Data, macrodatos, datos masivos, datos a gran escala, megadatos son **denominaciones** que se refieren al almacenamiento de grandes cantidades de datos y a los procedimientos usados para encontrar patrones repetitivos dentro de esos datos.

Los BD son datos en cantidades demasiado grandes, o que se mueven muy rápido para las bases de datos convencionales que no los pueden ni procesar, ni almacenar, ni analizar.

BD no se refiere a alguna cantidad específica de datos, se utiliza cuando hablamos en términos de petabytes (1.000.000.000.000.000) y exabytes (1.000.000.000.000.000.000).

2. Características

Los BD se suelen delimitar por cinco características o rasgos que empiezan por V: volumen (la enorme cantidad de datos generados cada segundo); velocidad (la rapidez a la que son generados nuevos datos y circulan por todas partes); variedad (los diferentes tipos de datos que podemos usar ahora); veracidad (la confianza y fiabilidad de los datos) y valor (nuestra capacidad de convertir nuestros datos en valor).

3.Tipos

3.1. Datos estructurados: tienen bien definidos su longitud y formato, como las fechas, los números o las cadenas de caracteres. Se almacenan en tablas, es decir en filas y columnas. Un ejemplo: las bases de datos relacionales y las hojas de cálculo

3.2. **Datos no estructurados**: su formato es tal y como fueron recolectados. No tienen un formato específico, no siendo posible desgranar su información a tipos básicos de datos, tienen un formato que no puede ser fácilmente indexado en tablas relacionales para el análisis. Ejemplos: PDF, documentos multimedia, emails o documentos de texto

3.3. **Datos semiestructurados:** no se ajustan a un esquema fijo**,** ni se limitan a campos determinados, sin embargo contienen marcadores para separar los distintos elementos, es información poco regular para ser gestionada de forma estándar. Ejemplo: documentos xml, los blogs o los sensores que emplean estos tipos de datos**.**

4 Personal y herramientas

Han surgido nuevos perfiles de **profesionales** como el data scientist (a caballo entre programador, economista y matemático) que aportan una nueva función de estadística y análisis de datos. La analítica digital es una disciplina relativamente joven. La labor del analista de datos es analizar

los datos, cuantitativa y cualitativamente, del entorno digital con la finalidad de extraer la información preparada para la toma de decisiones.

Existen muchas **herramientas** para tratar con los BD, algunas de las más conocidas son Hadoop, NoSGL, Cassandra, Business Intelligence, Machine Learning, MapReduce .

5. Procesos

5.1. Procedencia: los datos pueden ser **generados** por personas (emails, WhatsApp, tuitear), transacciones de datos, E-marketing y web, Machine to Machine, Biométrica.

Grandes cantidades de información proceden de diversas **fuentes** (ciudadanos, Administración Pública, redes sociales, sensores de tráfico, estaciones meteorológicas, los coches que circulan por una carretera ....)

Cada vez que realizamos una llamada desde un teléfono móvil, navegamos por Internet, descargamos una aplicación o mandamos una foto por el ciberespacio dejamos un rastro que es sumamente valioso.

5.2. Extracción: la recolección de datos es una de las disciplinas que más ha variado en menos tiempo. Cada vez tenemos más datos públicos en cantidades ingentes y dispositivos extendidos por toda la tierra emitiendo, procesando y recogiendo datos de las más diversas actividades. Hay varias empresas especializadas en recogida de datos mediante diversos programas que añaden algo de inteligencia, con lo que los números recolectados son coherentes y homogéneos para poder realizar los procesos posteriores Un ejemplo serían las arañas de un buscador de noticias.

5.3. Almacenamiento: el gran volumen de datos exige un almacenamiento escalable; muchas empresas tienen archivados sus datos, pero no saben cómo procesarlos.

Las **plataformas ETL** (Extract, Transform and Load) tienen la finalidad de extraer los datos de las diferentes fuentes y sistemas para luego hacer las correspondientes transformaciones (conversiones de datos, limpieza de datos sucios, cambios de formato) para finalmente cargar los datos en la base de datos o Data Warehouse especificada. Un ejemplo de plataforma es la Pentaho Data Integration, y su aplicación Spoon.

Existen cuatro grandes bases de datos de almacenamiento: Key Value, Documental, en rafo, Orientado a Columnas

5.4. Análisis: revela la información oculta en el almacenamiento en un tiempo razonable, cosa que no pueden hacer los estudios de mercado estático. Como la mayoría de los datos no están estructurados, el reto es filtrar solo aquellos que sean relevantes, estructurarlos y hacerlos útiles.

El análisis de datos **tradicional** es predefinido y, además, lento. Si se produce un incremento de volumen y una variedad de origen, solo da una información limitada, ya que solo se pueden analizar terabytes de datos estructurados y agrupados.

De ahí la necesidad de aplicar una analítica específica para BD. El punto clave es el análisis de los datos mediante su valoración y la combinación de sus distintas fuentes

Hay soluciones como el Apache Hadoop, es un marco de código abierto para el procesamiento, almacenamiento y análisis de grandes volúmenes, utilizado por Amazon, Facebook, Google, IBM, Intel Research ...

6. Ámbitos

- en el ámbito **empresarial,** las **redes sociales** se utilizan para dar a conocer la actividad, cruzar los datos de un candidato a trabajar, ver su perfil social y profesional en segundos, creación de listas de posibles candidatos según el perfil profesional necesario

- en c**onsumo**: se usa la minería de datos masiva cruzando los patrones de compra de un usuario con los datos de compra de otros, creando con ello anuncios personalizados y boletines de compra de aquello que el usuario quiere en ese momento

-en **deportes,** por ejemplo**,** análisis de los partidos de futbol para el entrenamiento y tomas de decisión. El **Sistema Amisco** que registra los movimiento de los jugadores, los envía a una central donde se hace un análisis masivo de los datos

- en **salud** o medicina, proporcionando una información fiable y pública para abastecer a la población de las medidas preventivas necesarias en caso de pandemias

- en **defensa y seguridad** en escenarios como la vigilancia y seguridad de fronteras, lucha contra el terrorismo y crimen organizado, contra el fraude, seguridad ciudadana etc.)

- en el sector de **la distribución y el financiero** son los primeros que han adoptado el sistema de BD, pero también las **aseguradoras y Administración Pública**

-en el **periodismo de investigación**: el sistema BD ayuda al periodista a encontrar información, pero también a captar lectores y satisfacer la demanda

- en la **ciudad inteligente** (Smart City): entorno urbano sostenible, lleno de conexiones inalámbricas para los vecinos, células que gestionan los riesgos en los parques, sistemas de transporte conectados a los móviles, edificios que gestionan su propia energía, la casa conectada etc.

- en la **predicción de comportamientos:** en los servicios de atención al cliente se aplican, por ejemplo, modelos predictivos con los que se puede determinar el número de llamadas que recibirá para organizar el servicioya que en un call center existe una alta fluctuación en el volumen de llamadas del cliente

7. Internet de las Cosas (IdC)

Es una infraestructura global interconectada, que enlaza objetos físicos y virtuales a través de la explotación de la captura de datos y las capacidades de comunicación. Consigue que los objetos cotidianos sean inteligentes las 24 horas del día gracias a la velocidad en la que se procesan los datos y la conexión desde cualquier lugar.

Existe una íntima conexión entre BD e IdC; se ha dicho que los BD son el alimento de la sociedad de la información, como el petróleo, mientras que el IdC es el ecosistema donde se recoge, procesa y circula esa información, formada por todo tipo de máquinas y objetos (cámaras de seguridad, termostatos inteligentes, smartwaches, frigoríficos, dispositivos médicos o deportivos con sensores o disponibilidad para ejecutar acciones).

8**. Las dificultades más habituales**

- El **colapso tecnológico** en el transporte de datos. La actual crisis del **espectro de frecuencias**: las redes inalámbricas actuales no son capaces de

soportar la enorme cantidad de datos esperada, en las frecuencias de radio no hay espacio libre para una futura expansión. Los problemas también se sitúan en la gestión de la recolección y almacenamiento, búsqueda, compartición, análisis y visualización.

- La **conectividad j**uega un papel esencial, especialmente en aquellas aplicaciones que requieren un análisis más complejo de datos de fuentes variadas. Hoy no está disponible una conectividad "ubicua". Necesidad de acceso gratuito a Internet.

-Los **límites de procesamiento** han ido creciendo a lo largo del tiempo; se produce el fenómeno de que los científicos encuentran límites en el análisis debido a la gran cantidad de datos en ciertas áreas (genómica, investigaciones relacionadas con procesos biológicos y ambientales etc), límites que también afectan a los motores de búsqueda en internet. La ausencia de un software común, formatos de datos estándares y protocolos de conectividad suponen hoy en día un freno al desarrollo.

-Los requisitos de seguridad que garanticen la **privacidad de las personas** y un buen uso de los datos que no conduzcan a prácticas discriminatorias

-La **energía**. Lo que funciona en determinadas circunstancias no lo hace en otras. La sensorización de objetos en zonas remotas obliga a utilizar baterías de mayor duración y redes válidas.

- Las correlaciones arbitrarias

En bases de datos muy grandes aparecen siempre correlaciones arbitrarias, no debidas necesariamente a la naturaleza de los datos, sino solo a su cantidad. Cuando los estadísticos hablan de la correlación de Pearson entre dos variables se refieren a una buena o mala relación lineal entre ellas . Sin embargo, la causalidad hace referencia a que un suceso constituya el resultado de otro. Causalidad siempre implica correlación, pero la correlación no necesariamente implica causalidad. Hay que tener en cuenta que en conjuntos de datos amplios siempre es posible encontrar correlaciones casi perfectas entre variables disparatadas (por ejemplo, los divorcios en Maine y el consumo per cápita de margarina en USA o bien el gasto en USA en I+D y los suicidios por ahorcamiento, estrangulamiento o asfixia).

9. El escenario actual

El modelo actual de negocio de una empresa, basado solo en sus datos internos, está **desfasado**, pues hoy los datos externos superan con creces los internos; procedencias diversas, la mayoría datos no estructurados.

Pero la realidad actual es que muy pocas empresas saben extraer el verdadero valor de los datos. Se dice que solo un 4 % lo hace; el 43 % de las empresas europeas y norteamericanas obtienen muy poco beneficio tangible de esa información y el 23 % no saca ningún beneficio de la misma .

B. ASPECTOS RELEVANTES PARA EL SEGURO

1. Perspectiva general

1.1. Un activo muy valioso

Los BD son un valioso activo para el sector asegurador pero llevan aparejada la necesidad de hacer frente a formatos de datos diferentes, competencia técnica, medios y uso innovativo de BD orientado al cliente; pueden consolidar la información y los procesos y una más rápida identificación de la información relevante para encontrar conexiones ocultas mediante la inteligencia artificial, mejorar la interacción con el cliente, dar mayor relevancia a la experiencia de este, reducir los gastos, mejorar los procesos de tramitación de siniestros, reducir el fraude y fortalecer la suscripción y la gerencia de riesgos **.**

Todo ello mediante los nuevos conceptos relacionados con BD como el análisis inteligente, la suscripción predictiva, la suscripción en base a estilos de vida y patrones de consumo, la economía conductista o del comportamiento.

1.2. Cambio de paradigma

La mayor aportación del BD al sector asegurador consiste en que induce a un **cambio de paradigma,** dentro del cual los actuales productos de seguros tienen que ser modificados. La idea básica es que la industria aseguradora abandone su lógica centrada en el producto para poner al cliente en el centro.

En el futuro la cuenta de resultados no debería ser más por áreas de negocio sino por cliente, gracias a las herramientas de gestión del conocimiento del cliente. La segmentación se realizará entonces por **nichos de riesgo**,

gracias al conocimiento del cliente y a la huella digital que el mismo va dejando; el riesgo del cliente deberá ser gestionado en su conjunto, pasando del paradigma del producto/póliza a la integridad del cliente

1.3. La tramitación de siniestros

La tramitación del siniestro es el proceso que mayor carga emocional tiene en la relación entre cliente y aseguradora. 1 de cada 3 clientes citan como la causa más importante del abandono de la aseguradora la deficiente gestión del siniestro.

La gestión de siniestros futura tendrá que profundizar en los aspectos más emocionales para mejorar la experiencia del cliente, transformar la organización hacia un modelo preventivo, en el que el cliente sea consciente de la importancia de anticiparse a la ocurrencia del siniestro, mejorando con ello su calidad de vida.

Dentro de este ámbito se podrían activar sistemas analíticos predictivos para detectar posibles casos de fraude en tiempo real, implantación de aplicaciones móviles para dar aviso del siniestro in situ y consultar posteriormente su estado de tramitación, ingeniería de control de siniestros en tiempo real, tramitación de siniestros flexible y fácil, etc.

. En el seguro de salud, la experiencia y satisfacción del cliente puede ser influenciada positivamente por BD, al igual que en los programas de gestión de la enfermedad. BD pueden ayudar a la aseguradora a considerar qué características de la conducta pueden conducir a siniestros relevantes, a enseñar cómo se pueden medir y cómo encontrar incentivos para evitarlos.

1.4. La gerencia de riesgos

Las oportunidades en el análisis de los riesgos que proporcionan los BD están siendo ampliamente apreciadas por los **gerentes de riesgos** en lo referente a la detección temprana de nuevos riesgos, perfiles de riesgo, control de exposiciones y, finalmente, cuantificación del riesgo.

BD pueden ser efectivos proporcionando información sobre riesgos difíciles de cuantificar y que requieren una vigilancia permanente como son

los riesgos relacionados con la reputación; ayudan también a rellenar las lagunas existentes en el conocimiento de determinados riesgos.

Estas posibilidades vienen condicionadas por una política efectiva de gestión de datos. Para ello es necesario emplear métodos modernos de análisis de datos. Ejemplos de nuevos modelos estadísticos son los procesos para la reducción dimensional, que hacen posible de varios cientos de informaciones calcular unos pocos parámetros que tengan la mayor parte de la información. Lo mismo rige para los modernos métodos de regresión o las redes neuronales que nos permiten, con el análisis de las relaciones, explicar acontecimientos individuales del pasado y también prever los del futuro.

1.5. La incipiente e incompleta regulación

Un tema aún no resuelto del todo es la **regulación de los BD** en cuanto a la exposición que los mismos puedan suponer para la esfera privada. En este contexto, la fiabilidad y la calidad de los datos externos es un elemento decisivo a la hora de evitar conclusiones equivocadas. No podemos olvidar que los BD son algo diferente al resto de los datos dada su heterogeneidad, variedad de fuentes, parcialidad o imparcialidad de su recolección o utilización de los denominados lagos de datos.

Las predicciones derivadas de BD en una aseguradora se enfrentan a escenarios un tanto conflictivos como pueden ser la asimetría informatíva, el deber de declaración del riesgo o el deber de respuesta a iniciativa del asegurador (cuestionario).

En el deber de declaración, las cuestiones son sobre la forma del cuestionario predeterminado, ausencia de cuestionario o cuestionario defectuoso así como las relacionadas con la agravación o disminución del riesgo.

Todo esto es importante pues los BD proporcionan informaciones no previstas en la ley, informaciones que pueden ir más allá de la misma.

La conclusión es que al no tener un marco regulatorio bien definido, que nos permita asumir los retos del BD, estamos en una especie de limbo de consecuencias imprevisibles.

Sin embargo, la ESA (Autoridades Europeas de Supervisión),en un informe aparecido el 15 de mayo de 2018, opina que existen ya un número considerable de requerimientos legales referentes a la protección de datos, seguridad cibernética y protección del consumidor, tendentes a mitigar muchos de los riesgos derivados de BD. Junto al Reglamento General de Protección de Datos, que veremos en el punto siguiente, podemos tener en cuenta, a efectos regulatorios, las siguientes Directivas:

- Directiva (EC) 2002/58/EC relativa al procesamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas (Directive on privacy and electronic communications). Arts. 26 y 13.

-Directiva 2016/1148/EC sobre la seguridad en la red y sistemas de información (art. 14).

- Directiva 2005/29/EC referente a las prácticas comerciales ilícitas (art. 5).

-Directiva 2002/65/EC referente a la comercialización de servicios financieros a distancia (arts. 9 y 10).

1.6. El Reglamento (UE) 2016/679, de 27 de abril de 2016

El Reglamento, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, señala diversos aspectos que afectan a los BD.

Aún sin mencionar expresamente la palabra Big Data, se deben considerar como afectados directamente; por ejemplo, ya en la E.de M. se habla de que la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales en los que la **magnitud** de recogida e intercambio ha aumentado significativamente.

El Reglamento se refiere únicamente a las personas físicas, no regulando el tratamiento de datos personales referidos a las personas jurídicas. Tampoco se aplica a los datos personales de las personas fallecidas. Como la protección de las personas físicas debe ser tecnológicamente neutra, la protección se aplica tanto al tratamiento automatizado como a su tratamiento manual.

Los principios de protección se aplican a toda la información relativa a una persona física identificada o identificable. Se introduce explícitamente el

concepto de seudonimización, pero sin excluir ninguna otra medida para la protección.

Los datos personales son toda información sobre la persona física identificada o identificable, en el sentido de que se pueda determinar su identidad, directa o indirectamente, como, por ejemplo, mediante un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Se establecen una serie de **principios** respecto al tratamiento (licitud, lealtad y transparencia, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación, integridad y confidencialidad). El responsable del tratamiento tiene una responsabilidad proactiva, ya que es responsable del tratamiento y debe ser capaz de demostrarlo.

Con carácter general, se **prohíbe (art. 9.1)** el tratamiento de todos aquellos datos reveladores de origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, datos genéticos o biométricos dirigidos a identificar inequívocamente a una persona, física, así como datos relativos a la salud, vida sexual o orientación sexual. Sin embargo, existen varias **excepciones** a esta regla en el **art. 9.2** (consentimiento del interesado, necesidad de tratamiento para el cumplimiento de las obligaciones y ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito laboral, de la seguridad y protección social, protección de intereses vitales del interesado en caso de incapacidad, datos personales hechos públicos por el interesado, necesidad de tratamiento para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia, fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos).

- **art. 5.1**.: los datos a tratar deben ser adecuados, exactos y actualizados. Los inexactos deben ser suprimidos o rectificados

- **art. 6.1**: el tratamiento tiene realizarse con el consentimiento del interesado para uno o varios fines

- **art. 22:** " todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

- el **art. 15** fija el derecho del interesado a obtener confirmación de si se están tratando o no sus datos personales, especialmente la información sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles citados en el art. 22, información que debe ser significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento para el interesado.

El Reglamento establece también un **derecho** de acceso del interesado, el derecho de rectificación y supresión (el derecho al olvido), derecho a la limitación del tratamiento, , derecho a la portabilidad de los datos etc.

Interesante e indudablemente referido, aunque de manera indirecta, a los BD, es la introducción de un sistema de **evaluación de impacto** cuando sea probable que un determinado tipo de tratamiento, en particular si **utiliza nuevas tecnologías**, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Otra novedad es la introducción de la figura del **delegado de protección de dato**s.

Finalmente, la persona que sufra daños y perjuicios materiales o inmateriales como consecuencia de la infracción del Reglamento tendrá derecho a recibir del responsable o encargado del tratamiento una **indemnización** de los datos y perjuicios sufridos.

La aplicación del Reglamento es a partir del 25 de mayo de 2018.

España se anticipó al Reglamento Comunitario mediante la trasposición, el 15 de julio de 2015, al ordenamiento español de la Directiva Europea-Solvencia II. Esta norma supone una forma de aplicar el contenido del art. 9.2 del Reglamento comunitario. No se sabe si será derogada o modificada, al ser el Reglamento de aplicación directa.

En dicha norma, el **art. 99,** bajo la denominación de " Protección de datos de carácter personal" se dictan reglas específicas para el sector del seguro y reaseguro en materia de tratamiento y protección de datos personales,

siempre teniendo presente el marco de la Ley de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal. La norma no menciona expresamente el concepto BD, pero, al igual que en el Reglamento antes citado, en cuyo texto previo se inspiró, se podría entender, al hablar de "datos", que incluye a todos, sean grandes o pequeños.

La citada norma parece ser que atribuye plena libertad de uso por la aseguradora de los BD en su poder relativos a los tomadores, asegurados, beneficiarios o terceros perjudicados con el fin de o bien garantizar el pleno desenvolvimiento del contrato de seguro o bien garantizar el cumplimiento de las obligaciones establecidas en la propia ley, sin necesidad de su consentimiento.

Las entidades pueden tratar sin consentimiento del interesado los datos relacionados con su salud para la determinación de la asistencia sanitaria, determinación de la indemnización, abono a los prestadores de la asistencia y reintegro de estos gastos al asegurado o beneficiarios.

Las aseguradoras pueden también establecer pools o ficheros comunes de datos de carácter personal para la liquidación de los siniestros y la colaboración estadístico-actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora.

Las aseguradoras que formen parte de un grupo pueden intercambiar, sin necesidad de consentimiento, los datos de carácter personal necesarios para el cumplimiento de las obligaciones de supervisión establecidas en la ley, comunicar al reaseguro, sin consentimiento del tomador, asegurado, beneficiario o tercero perjudicado, los datos estrictamente necesarios para la celebración del contrato de reaseguro

2. Incidencia en algunas modalidades de seguros

En general, todos los ramos del seguro están afectados por la nueva constelación de los BD; su utilización será transformativa, proporcionando mayores servicios de prevención de riesgos o productos hechos a medida del cliente. El concepto de predictibilidad alcanza su máxima expresión.

2.1.La selección- suscripción del riesgo y la tramitación del siniestro mediante la predictibilidad

Tradicionalmente el punto de incidencia ha sido la denominada condición primaria, lo que supone, por ejemplo, en los seguros relacionados con Vida y salud, que las tarifas se modifican teniendo en cuenta la gravedad del padecimiento y el alcance y duración del tratamiento, añadiendo el efecto mortalidad y la tendencia que se detecta en edades avanzadas; se crea una reserva para la antiselección; la idea central es aceptar, posponer o rechazar. En otros seguros se ha acudido al **análisis del histórico** de incidencias para recalcular la prima o establecer deducibles adecuados.

La analítica de datos está abriendo un gran potencial para el sector asegurador; este puede ampliar su campo de visión en el proceso de toma de decisiones, adecuando las mismas al caso específico y cliente. Ello conlleva una mejora en la selección y retención del cliente. Los usos posibles del empleo de BD son, además de la selección y retención del cliente mediante la valoración del riesgo, el ajuste de siniestros; en este ámbito se pueden reducir gastos y suprimir tiempos muertos; se puede pre-aceptar la solicitud de una persona y reducir el número de preguntas, simplificando con ello el proceso de suscripción.

No obstante, es conveniente evitar un exceso de optimismo sobre los resultados de la analítica predictiva, pues no todas las decisiones obtenidas pueden ser, de manera concluyente, hechas en base solo a probabilidades calculadas, por ejemplo si la decisión lleva a la aplicación de una exclusión, a un recargo de prima o a una denegación del siniestro.

Predecir con sentido supone tener bien estructurados **tres pilares básicos**: los sistemas, la capacidad analítica y los datos.

En cuanto a los **sistemas**, hoy tenemos excelentes con capacidades enormes de análisis. Pero el problema es cómo la aseguradora implementa los mismos en una infraestructura ya existente. Por ello puede ser recomendable acudir al outsourcing, es decir externalizar.

La **capacidad analítica**, mediante los correspondientes analistas de datos, es necesaria para elegir tanto el método adecuado a las necesidades del caso concreto como a la tecnología necesaria. A la hora de implementar las decisiones sugeridas es conveniente involucrar también a expertos actuariales y en valoración de riesgos, especialistas médicos y ajustadores de siniestros, todos ellos necesarios para validar los resultados del análisis y fijar las repercusiones en los procedimientos y en el negocio en general.

Los **datos** que se quieren analizar deben ser definidos. Información valiosa puede y suele estar contenida en lo propios archivos de la aseguradora, pero no suelen estar bien estructurados para su evaluación a fin de obtener una predicción válida. Una vez recogidos y evaluados los datos internos, se puede pasar a los datos externos para tener la imagen adecuada de los factores que influencian el comportamiento del cliente y la producción de los siniestros. Es obvio que aquí se precisan gestores profesionales de datos.

En el campo de la ciencia actuarial, aplicada al seguro de vida, se están implantando nuevos modelos que miden con mucha precisión el fenómeno de la mortalidad. En estos modelos, la suscripción predictiva incorpora variables como la información personal (edad, género, ocupación), información socio-demográfica (población urbana o rural, tamaño de la población), estilo de vida- ocio, estado de salud personal y familiar, solvencia crediticia, información disponible en las redes sociales.

Esta metodología toma como base información personal y externa de hábitos de comportamiento, siendo una aproximación a la medida del envejecimiento humano desde el desgaste biológico del organismo, es decir, la **edad biológica** y no la cronológica.

2.2. **En el seguro de daños** la observación sistemática con métodos estadísticos de los ríos de información mundiales puede ser una excelente ayuda para conocer tempranamente siniestros o daños potenciales relevantes. Esta información se puede comparar con la propia cartera y nos ofrece un sistema preventivo anticipado que nos permite actuaciones que disminuyen el daño futuro.

- BD puede apoyar, entre otros, la suscripción de riesgos de **pérdida de beneficios** por interrupción o paralización del negocio**,** analizando, por ejemplo, las cadenas de suministro, teniendo en cuenta los efectos que producen los cambios en empresas globales. Para ello, se utilizan las informaciones libres en Internet, datos no estructurados, se detectan aquellas que sean relevantes, se analizan y se comparan con los propios datos.

- Lo mismo rige para los suministradores de servicios cloud, donde existe un gran riesgo de cúmulo si un ofertante falla o bien es hakeado.

- Igualmente en la industria de gas y petróleo o en la farmacéutica, el asegurador no tiene siempre claro las corrientes de suministro y su valor. Con un buen sistema de BD se podría mejorar considerablemente la suscripción en selección de riesgo, control de participaciones, primas y control de cúmulos, evitando siniestros de negocio no rentable.

Existen ya varios **ejemplos** que demuestran cómo las herramientas BD pueden ser utilizadas para agrupar la información. Uno de ellos es que la monitorización automática de 7.000 canales digitales de noticias, con un volumen diario de 250 gigabytes, hace posible que los siniestros de incendios en GB y en USA queden registrados más rápida y económicamente. La comparación de estos datos con los datos en las carteras permite una mejor identificación de pautas de riesgo, lo que permite una utilización más rápida y efectiva de la gerencia de siniestros.

2.3. En el seguro de automóviles

I d C anticipa lo que va a fallar en los vehículos (coches, aviones, barcos o trenes). Los sensores aportan información sobre el entorno y obstáculos al y en software de los vehículos, evitan colisiones; asistentes de voz, cartografía digital avanzada, sensores y cámaras facilitan la conducción de coches.

La llegada de **coche conectado**, autónomo es, tanto técnicamente como desde el punto de vista legislativo, otro de los grandes retos. Si se piensa que más del 90 % de las muertes en carretera es producida por errores humanos, podemos darnos cuenta de la importancia del tema. También con ello se pretende reducir los atascos y la contaminación, pero es preciso un nuevo diseño de carreteras aptas para dichos vehículos, aparcamientos y normas de circulación. La seguridad es una de las obsesiones al respecto. Se busca hoy el coche o,o: cero emisiones y cero accidentes; para ello los vehículos son equipados con múltiples cámaras, radares y escáneres láser que posibilitan la identificación de otros vehículos objetos y personas para evitar cualquier accidente. Todo ello solo es posible gracias al BD/ I d C

En los c**oches sin conductor** existe una borrosa vía media de la automatización donde los fabricantes todavía obligan a los conductores humanos a prestar atención; no siempre está claro dónde cae la línea que separa al ser humano de la máquina.

La segmentación de riesgo en el automóvil se ha hecho tradicionalmente basada en datos relacionados con la persona (datos demográficos, comportamiento, experiencia, sexo hasta hace poco etc.) y con el vehículo (potencia, velocidad). BD permite ampliar la base de conocimiento con datos valiosos. La información obtenida de comportamientos del conductor permite, por ejemplo, obtener una efectiva prevención del fraude, dando, a su vez, la base para dar servicios útiles y precios competitivos. Estos datos están, sin embargo, sometidos al control de la privacidad.

Los datos obtenidos telemáticamente son recogidos por una serie de empresas que operan entre el asegurado y aseguradora, lo que supone para esta un plus de riesgo como coordinadora. BD proporciona una información variada que sirve a ambas partes: una serie de dispositivos pueden recoger datos sobre la conducta del conductor respecto a la aceleración, frenado, la forma de tomar las curvas etc., comparando estos datos con las señales de tráfico, tipo de carretera y pavimento. Todos estos datos pueden servir al conductor para ver cómo conduce realmente y ,a la vez, pueden influir el precio a la baja.

2.4. En el seguro de enfermedad/salud

Predecir lo que va a pasar es lo que se busca al aplicar la tecnología BD, que está aterrizando en el sector sanitario. Nuevos ámbitos de actuación los podemos constatar en el campo de la tramitación de siniestros, promoción de la salud, valoración del riesgo, desarrollo de productos y optimización de procesos.

Por lo tanto, las posibilidades del BD en el ámbito de salud son varias, por ejemplo, predicción de hospitalizaciones por patologías basándose en factores ambientales, poblacionales, identificación de pacientes de alto riesgo, análisis del estado de salud de una población o territorio, seguimiento de tendencias, efectividad de medicamentos y seguimiento de efectos adversos o evaluación de servicios sanitarios. Indudablemente, no podemos olvidar que detrás de todos esos datos hay personas cuya privacidad es necesario garantizar.

Del BD sanitario merece la pena reseñar el programa denominado **Real World Data**. Este refleja la atención real que reciben los pacientes reales en un contexto determinado y los resultados clínicos obtenidos, que no son necesariamente iguales a los obtenidos en los ensayos clínicos. El sistema

RWD recoge los beneficios y efectos adversos de las decisiones médicas en la práctica habitual con millones de pacientes. Se recogen una serie de datos (estudios observacionales de registro, historias clínicas electrónicas, ensayos clínicos pragmáticos) que sirven para identificar anticipadamente a pacientes crónicos en riesgo de descompensación e incluirlos en programas específicos de atención, ayuda a la toma de decisiones clínicas en tiempo real, reducción de la variabilidad en la práctica médica et. Es decir, el nuevo modelo RWD pretende hacer una gestión proactiva del cuidado.

En los **hospitales** hay un equipamiento sofisticado pero no ha habido **ninguna revolución** en la manera como nos ocupamos de la atención sanitaria. Aquí los wearables desempeñarán un papel clave. Estos dispositivos, colocados en el cuerpo del paciente, pueden monitorizar sus constantes vitales y enviar esa información en tiempo real a los médicos. Con ellos se podrán monitorizar patrones de comportamiento en una persona depresiva, por ejemplo. Si no se encuentra bien, estará más tiempo en cama, no saldrá de casa, no estará ocupado... ser capaces de comprender eso puede permitir que los profesionales médicos intervengan a tiempo Pero el riesgo de ser hackeados puede alcanzar su máxima expresión en la industria médica. En 2015 se robaron 100 millones de informes médicos.

El individuo porta cada vez más sensores que incorporan y emiten información continuamente, el móvil es el principal, pero la propia ropa está empezando a incorporar sensores o añadidos que realizan funciones concretas; hay camisetas que se iluminan a la velocidad de los latidos del corazón, otras muestran con su color los índices de contaminación del entorno. La tecnología de identificación por radiofrecuencia (RFID) permite reconocer de forma automática cualquier objeto, animal o persona gracias a la información contenida en etiquetas electrónicas (tags) que llevan.

- En la **tramitación de siniestros,** uno de los temas candentes es el reconocimiento de los estafadores. Los sistemas clásicos regulares de control médico permiten una tramitación de los siniestros automatizada en tiempo real y con exámenes de bajo costo, pero estos sistemas tienen un mantenimiento costoso y pueden reconocer parcialmente solo comportamientos sistemáticos y solo mediante el estudio de muchas facturas. Estos sistemas pueden ser completados mediante comportamientos analíticos que puntúan cada nuevo siniestro con una

probabilidad de engaño o abuso. Según el valor del punto (score) otorgado, se decide si se pasa o no el caso al departamento encargado de la estafa en el seguro.

- Programas de gestión de la enfermedad: en Europa, diversas aseguradoras ofrecen al cliente un servicio que consiste en un programa de gestión de la enfermedad; con él se pretende optimizar la elección del paciente y medir el resultado. En enfermedades tan populares como la diabetes o dolor de espalda se ofrecen estos programas de salud con mayor frecuencia, con el fin de elevar la calidad de cuidado del paciente, pero también ahorrar gastos al asegurador. Las medidas del programa van más allá de la cobertura clásica de salud, pudiendo incluir aspectos tales como el nivel educativo, actividad física, vigilancia médica del paciente con la finalidad de apoyar un estilo de vida más sano etc.

Cada fase del programa, desde su diseño y ejecución hasta la valoración del resultado, es mejorado considerablemente con la utilización de BD. En el diseño, la aseguradora tiene acceso directo, por la póliza o por los siniestros, a determinados factores de riesgo (edad, diagnósticos, servicios médicos utilizados etc.) pero normalmente no se captan importantes factores como son la información sobre la conducta. Estos factores obtenidos de dispositivos o medios sociales pueden servir para una segmentación del riesgo, aunque en determinados países la legislación no lo permite. Los procesos de identificación y segmentación tienen que ser apoyados por técnicas analíticas tales como modelos de predicción individual de costes para los pacientes o bien mediante algoritmos que identifiquen grupos homogéneos de pacientes. La fase de evaluación se centra en el ahorro de costes y en la mejora del paciente adscrito al programa. Pero una medición solvente de estos factores depende de la disponibilidad de un grupo válido con el que se pueda comparar. El reto es identificar un subgrupo que sea tan parecido al grupo de participantes teniendo en cuenta todos los factores de riesgo.

C. BLOCKCHAIN O LA CADENA DE BLOQUES

1. Qué es

Es un **registro compartido**, replicado en múltiples ubicaciones, actualizado mediante un consenso distribuido, con acceso de todo el mundo o unos pocos, inmutable, indeleble y auditable. Fiable y confiable. Muy

rápido, Coste muy pequeño, pues se puede acceder a él con un equipamiento convencional (un simple ordenador).

De manera simplificada, podemos decir que es un medio de almacenamiento digital, mantenido descentralizadamente por numerosos participantes, en el cual las transacciones, empaquetadas en bloques, pueden ser almacenadas seguramente y libres de manipulaciones. Es un registro, en principio, incorruptible, permanente y que no puede ser modificado por ningún miembro de la red.

Plantea cuestiones técnicas y jurídicas interesantes, al quedar cualquier activo registrado en una especie de libro de contabilidad indeleble, en un registro permanente que no puede ser modificado por ningún miembro de la red.

2. Funcionamiento. La función hash

La transacción **se inicia** cuando alguien envía datos a otra parte. Estos datos se refieren no solo a criptomonedas, sino que pueden ser contratos, escrituras o títulos de propiedad, información médica o datos personales, contratos inteligentes, pólizas de seguros y, en general, archivo de documentos (notarías en línea, registros de la propiedad ..).

Las nuevas entradas están sometidas a reglas estrictas y requieren el consenso de la mayoría de los usuarios. Como los usuarios del BC como un todo garantizan que el registro está siempre actualizado, no hay necesidad de que otras autoridades certifiquen que es correcto. Ello supone que los intermediarios y los representantes o apoderados tales como abogados, notarios y peritos tendrán un papel más reducido que en la actualidad, papel que asume la criptología, sobre la base de que se crea en el BC un registro de toda la información relevante a prueba de manipulaciones.

La transacción se **difunde** en una red P2P de ordenadores que gestionan la cadena de bloques, denominados nodos; son miles de ordenadores repartidos por todo el mundo.

Cada nodo dispone de un procedimiento para comprobar la validez de la transacción. Alcanzado el consenso en la red, los algoritmos empaquetan en un bloque la transacción junto a otras recientes. El propio programa crea entonces una huella digital del nuevo bloque codificando sus datos

mediante una función hash y dos elementos más: la huella digital del bloque anterior y un número aleatorio de uso único (nonce). A continuación, ciertos nodos, apodados **mineros**, ejecutan una serie de cálculos que, por ensayo o error, intentan resolver un problema matemático arbitrario, también definido por la red. Quien primero completa esta prueba de trabajo y halla la solución "extrae" ese bloque, obteniendo una recompensa. La minería está hoy dominada por equipos gigantescos, por lo que la posibilidad de que un nodo aislado resuelva un bloque es aproximadamente de uno entre ocho millones.

Pero esta minería basada en pruebas de trabajo requiere mucha energía por lo que otras cadenas de bloques prescinden de ella, utilizando, en su lugar, una red de nodos "validadores", los cuales certifican las transacciones mediante un proceso denominado "prueba de participación", que consume poca electricidad al no precisar cálculos complejos.

La estructura de datos subyacente, como cadena de bloques, está en una serie de bloques codificados secuencialmente, que se actualizan de manera consensuada mediante diversos mecanismos de autentificación que garantizan la fiabilidad y seguridad. Las transacciones entre usuarios (P2P) se efectúan directamente entre ellos, sin una autoridad central y sin la ayuda de intermediarios.

Después de esta **validación** del bloque, por uno de los sistemas previstos, este se añade a la cadena con una huella digital en la que también se codifican las huellas validadas de los bloques previos. La modificación de un solo bit en cualquier parte de la cadena altera la huella digital de ese bloque concreto y las de los posteriores.

Función resumen (función hash): es un método criptográfico; la función hash condensa cualquier cantidad de datos en una cadena alfanumérica de longitud fija, generando con ello una **huella digital** de los datos de partida; si uno solo de sus bits se modifica, el resultado de aplicar la función hash es completamente distinto, con lo que se detectan errores o manipulaciones en los datos originales. Interesante es que el método es unidireccional; los datos iniciales no pueden recuperarse a partir de la huella digital. En resumen:

-criptografía asimétrica, se emplean dos claves (pública y privada) donde una sirve para cifrar y la otra para descifrar. Función criptográfica

irreversible, pues no permite recuperar el texto aislado. Obtenido el resumen, no se puede obtener el texto.

- función matemática que transforma un número (por ejemplo, una transacción digital), posiblemente muy grande, en otro más pequeño denominado resumen o huella digital.

- su resultado (llamado resumen o huella digital) es un número de tamaño predeterminado, muy pequeño y rápido de obtener. Es prácticamente imposible obtener dos números que tengan el mismo resumen.

- BB DD, confidencial, detección de errores durante las transmisiones, firma digital, sellado de tiempo, antivirus etc.

- diversos mecanismos de consenso que difieren según el registro sea público o privado y con modalidad de bloques " con permiso y sin permiso".

3. Posibles fallos

Se suele hablar de diversas posibilidades de penetrar en el armazón de una cadena de bloques:

- la primera sería la del 51 %: para dinamitar el mecanismo de consenso de la cadena de bloques, los atacantes tendrían que controlar la mayoría de los nodos, lo que permitiría decidir qué bloques se extraen y cómo

-la segunda se refiere a un posible error humano (mala administración- caso Mt.Gox-, pérdida de la contraseña)

- la tercera está relacionada con la explosión de datos, que en sí es la consecuencia natural del buen funcionamiento del sistema. Como cada nuevo bloque revalida todos los anteriores, cada nodo de validación necesita una copia de la última versión de la cadena completa para procesar cada nueva transacción, lo que conduce a que el método se hace inmanejable; en realidad, solo los ordenadores de alto rendimiento serán capaces en el futuro de soportar la carga, lo que va en contra del principio básico de disponer de un libro de contabilidad o archivo distribuido

- la cuarta está relacionada con la mala fe y los fallos de seguridad. Un individuo corriente no puede utilizar directamente ninguna cadena de bloques; para ello el individuo dispone de aplicaciones que hacen uso de la

cadena subyacente, de una u otra forma. En esta capa de aplicación es donde puede presentarse una enorme confusión y, frecuentemente, una absoluta mala fe. Un ejemplo son las carteras de criptodivisas donde e cometieron enormes fallos de seguridad en sus aplicaciones, que llevaron a pirateos notorios. Por eso es de la opinión común que usar cualquier aplicación diseñada por un tercero para guardar archivos digitales basados en cadenas de bloques sigue siendo una propuesta altamente insegura

- finalmente, tenemos el reto de **transparencia**: se estudia la creación de sistemas informáticos que constituyan una red de confianza, que permita el registro y la reproducción de transacciones y contratos entre las diversas partes pero sin exponer los datos reservados y respetando la privacidad.

4. Peculiaridades jurídicas

-La pregunta clave es cómo se **regula** un sistema descentralizado. Una cadena de bloques es en realidad una regulación, es decir, un sistema de normas impuestas matemáticamente sobre lo que puede hacerse y lo que no con una base de datos; la regulación es definida y aplicada por un código fuente en vez de por un gobierno o un banco central o una autoridad de control centralizada. Pero en un sistema descentralizado no hay ningún lugar concreto al que ligar la regulación.

-El sistema BC implica un derecho de **control compartido** que, al hacer desaparecer el contrato original, dificulta considerablemente presentar una pretensión o derecho controvertidos ante un juez. El sistema está diseñado para la gestión de elementos duraderos. Como los bloques están sometidos a la función hash, es muy difícil hacer aparecer un documento en un proceso o arbitraje. Esto supone revitalizar el principio de la **buena fe**: todas las partes firman el acto de pasar de un eslabón a otro. Como el BC no puede retroceder, la pregunta es si no sería posible crear un árbitro que intervenga, mediante la introducción de la cláusula correspondiente.

-En el sistema BC tenemos su código (normas de funcionamiento) y el contrato que se incorpora a la cadena; en esta nos encontramos con un archivo que actúa conforme al protocolo BC, distribuido entre varios participantes, archivo que viene a completar el código que está previo al contrato. El código es la frontera del BC.

- Hay una serie de aspectos en el contrato de seguro que quedan fuera pues no son parte del código como es la agravación del riesgo etc.

Luego la diferencia con lo que había antes sería en que tenemos la incorporación del contrato de seguro al código BC y un derecho de control compartido, pues no hay persona/autoridad que certifique o tercero de confianza.

También es un problema, por ejemplo en Vida, el derecho de desestimiento, puesto que en el contrato incorporado a un bloque no es posible dar marcha atrás.

También en el derecho de información, hay una serie de elementos que no se pueden encajar en el Blockchain, pues cualquier acción que se toma está irrevocablemente documentada en el sistema.

1.5. Los contratos inteligentes

Los BC pueden almacenar también los denominados contratos inteligentes (smart contracts), que pueden ser configurados de manera que se ejecuten automáticamente. Las principales ventajas son que las transacciones no necesitan ser ejecutadas y confirmadas por un organismo centralizado solvente y que un mecanismo especial de encriptación asegura que los datos no pueden ser manipulados después del hecho.

Los "**smart contracts**", creados en los 90, fueron definidos como un protocolo basado en la computadora para la ejecución automática de las cláusulas de un contrato. Un contrato inteligente se elabora mediante un código informático para estructurar, verificar y ejecutar un pacto entre las partes, pacto que se ejecutará automáticamente, de acuerdo a los términos establecidos en el mismo. La ventaja frente a un contrato tradicional es, por ejemplo, no dejar el cumplimiento de sus condiciones al arbitrio de uno de los contratan.

Si una parte quería incumplir el contrato, por ejemplo, suspender el pago de un plazo de la compra de un coche, el smart contract podía cerrar automáticamente las ventanillas del vehículo o inmobilizar su arranque. Todo ello sin una autoridad que intermediara. Existen varios prototipos. Por ejemplo, el seguro para retraso de los vuelos. El asegurado puede pagar la prima predefinida al contrato inteligente. Si el vuelo se retrasa, el contrato ordena un pago al pasajero después de haber analizado la llegada

de los aviones. La suscripción y la gestión del siniestro están completamente automatizadas.

Nos encontramos, pues, con una serie de **problemas** relacionados con**:**

- la redacción, modificación e interpretación de las cláusulas, escritas en lenguaje digital, implica una estrecha colaboración entre juristas y programadores

- garantizar la adecuación y exactitud de las instrucciones contenidas en el contrato, al ser automática su ejecución

- la ley y jurisdicción aplicables, dado que el contrato inteligente se registra, verifica, ejecuta y se almacena en millones de ordenadores a la vez

- la protección de datos en el entorno BC que, como hemos dicho, ofrece gran transparencia y puede descubrir datos protegidos.

- cuestiones de forma (si el código es el contrato): en general, principio de libertad de forma, pero problemas de comprensibilidad etc. o la determinación del daño después del siniestro o la determinación de obligaciones; cómo se obtiene e incorpora la información externa, las modificaciones o los errores del código

- el principio de que el contrato es autoejecutable, sin intervención humana y sin posibilidad de suspender la ejecución

- el derecho de desestimiento, el (re)cálculo de la prima, declaración, la suplantación de la figura del juez.

6. Blockchain Insurance Initiative B3i

La tecnología BC tiene también el potencial para ser una nueva forma de intercambio de datos entre aseguradoras y reaseguradoras, siendo posible, al menos en teoría, y con la ayuda de los smart contracts, gestionar totalmente los contratos de seguro y reaseguro utilizando la misma. Ello supondría para el seguro, que muchos procesos serían más directos y transparentes y las transacciones entre tomadores del seguro, aseguradores y reaseguradores serían más rápidas; el consumidor tendría tiempos de procesos más reducidos, ajustes de siniestros más rápidos y primas más

bajas; también se reduciría considerablemente el trabajo administrativo de los participantes para asegurar la consistencia y ejecución de las pólizas.

Aseguradores y reaseguradores están tratando de crear una herramienta viable para transformar el sector asegurador mediante un registro compartido y transparente de la información relacionada con los contratos de seguro y reaseguro. Esta iniciativa parte de que se podrían obtener una serie de ventajas relacionadas con una sola versión de la verdad compartida, una gestión de los contratos más eficiente, mejora de la eficiencia del capital y, como indicado, menos administración y más protección del consumidor.

No obstante, los promotores de la iniciativa se encuentran en esta fase experimental con diversos riesgos y restricciones, debidos a la mecánica del BC, referentes a la privacidad, a la capacidad de aumentar el número de contratos procesados o al procesamiento de contratos mucho más complejos, a una tecnología inmadura, a la insuficiencia de estándares e, incluso a la necesidad de gestionar los cambios de forma activa.

D. OBSERVACIONES AL SEGURO CIBERNÉTICO Y AL USO DE ALGORITMOS

Los riesgos cibernéticos son considerados, en general, como una fuente primaria de preocupaciones tanto para los consumidores como para los operadores del mercado, dado que el tratamiento de los datos puede ser una materia altamente sensitiva y el impacto de los fallos en la seguridad cibernética puede tener graves consecuencias. BD/ BC incrementan indudablemente la exposición debido, entre otros, a la extracción de los datos de fuentes diversas o a la práctica de acuerdos IT, incluyendo el almacenamiento o el outsourcing en la nube.

La sociedad de la información, con su técnica, trae no solo ventajas sino también riesgos: los hackers pueden entrar, sin mayores problemas, en ordenadores, móviles, tabletas, fotocopiadoras etc. obteniendo los datos contenidos y utilizándolos indebidamente. Estos ataques ocasionan la pérdida de datos confidenciales, de secretos de la empresa objeto de la agresión, infecciones del hard- y del software, paralización del negocio y pérdida de imagen, que suponen pérdidas económicas considerables. Los empresarios alemanes consideran que la realización del riesgo cibernético (

paralización de instalaciones, espionaje y utilización ilícita de datos) supone hoy el máximo riesgo para sus empresas.

Los ataques a los sistemas informáticos pueden ser tanto internos (del propio personal de la empresa) como externos (hackers, empresas de la competencia, servicios secretos etc).

Estos supuestos no están lo suficientemente cubiertos por los seguros habituales que los incluyen solo parcialmente. Así, en los seguros de daños (incendios, corriente débil, maquinaria) el siniestro está cubierto únicamente cuando se produce un daño material, cuando las cosas son dañadas o deterioradas. Es decir, un daño material implica un deterioro de la sustancia del objeto asegurado que disminuye su valor o su utilización. Pero los ataques cibernéticos, por lo general, no ocasionan un deterioro, destrucción o desaparición o pérdida de un objeto físico; incluso los seguros del software, más especializados, no cubren con frecuencia la pérdida, modificación o no disponibilidad de datos o programas ocasionados por software contaminado, por ejemplo, por virus, gusanos o troyanos.

La configuración de la cobertura para los ciberriesgos es muy variada, pues se tiene que adaptar a la necesidad individual. Una definición de lo que es un cibersiniestro se refiere a un daño comprobable por primera vez como ocurrido durante la vigencia de la póliza, aunque la póliza extiende la cobertura en aquellos casos donde el daño no pudo ser comprobado antes de la terminación de la póliza. El daño tiene que ser causado por una violación de la seguridad de la información, es decir, tiene que existir una relación de causalidad entre la infracción de un deber y el daño ocasionado.

Esa violación de la seguridad de la información tiene, sin embargo, que ser ocasionada por determinados acontecimientos enumerados taxativamente, en concreto por ataques a los datos electrónicos o a los sistemas de procesamiento de los mismos del asegurado, acceso ilícito a los datos electrónicos o instalaciones, acción u omisión que infringe la legislación de protección de datos, software contaminado que ocasiona la pérdida de los datos o instalaciones etc. Es decir, la cobertura contiene elementos del seguro clásico de responsabilidad civil con una cobertura tanto de responsabilidad civil como de daños propios para el riesgo de interrupción

de la explotación y para los gastos necesarios para la recuperación de los datos o supresión del software contaminado.

Es adecuado citar aquí, aun brevemente, que la utilización de **algoritmos,** como herramienta imprescindible en las tecnologías expuestas, afecta y condiciona directamente esta modalidad de seguro, así como otras, si bien dicha afectación, en especial desde la perspectiva de la responsabilidad civil, no recibe aún la consideración que merece.

BD/BC y algoritmos están claramente relacionados, estos forman parte fundamental del proceso; un algoritmo es un conjunto ordenado y finito de operaciones que permite hallar la solución a un problema; facilita una automatización de tareas, procesos y decisiones, con funciones como priorizar, clasificar, asociar (grado de similitud) y filtrar.

Mediante la combinación de todas las variables de predicción se pueden construir algoritmos o modelos que clasifiquen a cada cliente de peor a mejor , en términos de probabilidad de otorgarle una tarifa estándar al momento de la solicitud. Los modelos predictivos se utilizan hoy en día en diferentes ámbitos.

Algo tan abstracto y matemático plantea problemas de delimitación de la responsabilidad derivada de la utilización de los mismos; en función de dónde esté situado el problema, se puede fijar la responsabilidad.

Entre las aplicaciones específicas actuales en el sector asegurador nos encontramos, por ejemplo, con aquellas dedicadas a averiguar el envejecimiento y estado de salud a partir del reconocimiento facial (Lapetus), al reconocimiento mediante drones de zonas de cultivo para su aseguramiento (Aerobotics) y a detección de fraudes, gestión de reclamaciones etc.

El uso masivo de algoritmos plantea, sin embargo, diversos problemas para el seguro cibernético, relacionados con la opacidad, automatización de tareas, decisiones, ejercicio de derechos, multiplicación de efectos, aprendizaje/evolución incierta/inestabilidad que conllevan perspectivas jurídicas aun no enteramente previstas como son las prohibiciones o limitaciones sectoriales de los algoritmos, los efectos jurídicos de los procesos automatizados (Ver MIFID II, art. 12: negociación algorítmica), temas relacionados con la protección de los algoritmos (patentabilidad,

secreto industrial, derechos de autor). Ver art. 8 (5) UK Data Protection Act 1998, Sectión 7 (1) (d), su impacto en la competencia del mercado, la transformación de la naturaleza jurídica de la actividad etc.

Todo ello puede llevar a determinados escenarios donde el diseño, desarrollo o aplicación de un algoritmo puede generar responsabilidad. Ejemplos claros son las precondiciones discriminatorias, diseño inadecuado, aprendizaje con resultado discriminatorio, resultados discriminatorios, falsos positivos/falsos negativos.(Ver en este contexto lo citado en el punto 1.6. sobre las decisiones automatizadas o elaboración de perfiles).

Este escenario ha llevado a la ESA a recomendar incluir, entre las buenas prácticas de las instituciones financieras que utilizan BD, la monitorización periódica del funcionamiento de los procedimientos, algoritmos y metodologías de BD así como las herramientas para adaptarse a los desarrollos tecnológicos y a los nuevos riesgos emergentes.

Como hemos visto, tanto los BD como los BC no están exentos de riesgos que afectan a todas las personas involucradas en el tratamiento, distribución y uso de grandes masas de datos y de las cadenas de bloques. Es necesario proceder a una ampliación de las coberturas, si bien la parquedad legislativa reguladora puede ser, en estos momentos un obstáculo.

E. BIBLIOGRAFÍA CONSULTADA

ABI REPORT. " How Data makes Insurance Work better for You". *The Digital Insurer, 2016*

ACHENBACH, M. " Die Cyber-Versicherung- Überblick und Analyse." *Versicherungsrecht, nr. 24, 15.12. 2017*

ALARCÓN FIDALGO, J. y otros: " Boletín nr. 14 de junio de 2017 del Grupo de Trabajo NT, Prevención y Seguro*". Seaida, Sección Española de la Asociación Internacional de Derecho de Seguros, AIDA*

ARIZA RODRÍGUEZ, F." Transformación del sector asegurador en la era digital*". Boletín de la Mutualidad de la Abogacía, nr. 24 , septiembre 2017*

ARNOLDUSSEN, L. y HAUNER, W. " Innovative risk solutions using big data*". Munich Re, Coloquio en Baden -Baden, 24 de octubre de 2016*

BBVA. "Tendencias regulatorias financieras globales y retos para Pensiones y Seguros". *Documentos de Trabajo nr13/23, Madrid, julio de 2013*

BELDA REIG, I." La inteligencia artificial. De los circuitos al conocimiento". *2017, RBA Coleccionables, S.A.*

BENITO OSMA, F. " El contrato de seguro y las tecnologías aplicadas a la medicina y la salud". *En La influencia de internet, genética y nanotecnología en la medicina y en el seguro,* IV Congreso de Nuevas Tecnologías, Universidad Externado de Colombia, octubre de 2015

BOLETÍN OFICIAL DEL ESTADO. "Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras". *B.O.E. de 15 de julio de 2015*

CELAYA, J. "Blockchain y su impacto en el sector asegurador" *Semana del Seguro, Madrid, Febrero 2017*

CRO FORUM. "Big Data & Analytics: the algorithm of modern business". *2015, CRO Forum, Netherlands*

EUROPEAN SUPERVISORY AUTHORITIES (ESAs). "*Joint Commitee Final Report on Big Data",* 15 de marzo de 2018

EVERIS. " Tendencias y oportunidades en el sector asegurador en un entorno cambiante", *2014*

GARCÍA-ALSINA, M. "Big Data. Gestión y Explotación de grandes volúmenes de datos". *Editorial UOC, 2017, Barcelona*

ILLESCAS ORTIZ, R. "*Big data medicorum* y la nueva legislación española". *En La influencia de internet, genética y nanotecnología en la medicina y en el seguro,* IV Congreso de Nuevas Tecnologías, Universidad Externado de Colombia, octubre de 2015

LARA DI LAURO, E. "Impacto de los grandes datos y el análisis inteligente del seguro de vida y salud". *En La influencia de internet,*

genética y nanotecnología en la medicina y en el seguro, IV Congreso de Nuevas Tecnologías, Universidad Externado de Colombia, octubre de 2015

LIPTON, A. Y PENTLAND, A." Hacer saltar la banca", en *Investigación y Ciencia, Marzo 2018*

MARTÍN CANTERO, N. y VALVERDE, R. " Internet de las cosas. El mundo hiperconectado*". The Valley, Digital Business School, 2016, Grupo Unidad Editorial.*

MAYER-SCHÓNBERGER, V. y CUKIER, K. " Big data. La revolución de los datos masivos*". Turner Publicaciones, S.L., 2013, Madrid*

MIELENHAUSEN, A. " Blockchain. El potencial para impulsar eficiencias a través del sector (re)asegurador". *Semana del Seguro, Madrid, Febrero 2017*

MUNICH RE. " Business Analytics sorgt für Struktur im Umgang mit Big Data**".** *Info MR Health, 2014*

MUNICH RE. "Big Data- eine riesige Herausforderung". *Topics, 1/ 2015, Munich.*

MUNICH RE."Predictive Analytics- Making better decisions to gain the competitive edge". *Munich 2017*

NUÑEZ, I. "El profesional digital. Perfiles, cultura y modelos". *The Valley, Digital Business School, 2016, Edición Isabel Nuñez*

PAULUS, J. "El mundo que el Bitcoin ha forjado", ", en *Investigación y Ciencia, Marzo 2018*

PÉREZ IZQUIERDO, A.T. " Max PLANCK. La revolución de lo muy pequeño" .2012*, RBA Coleccionables, S.A.*

PESCADOR, D. " Analítica digital. Cómo medir su impacto en los negocios". *The Valley, Digital Business School, 2016, Edición Isabel Nuñez*

REVISTA ESPAÑOLA DE SEGUROS. " Insurtech: retos y desafíos de cara a la nueva distribución y contratación de seguros". *Nr. 169 de 2017*

SMOLENSKI, N." El impacto social de las cadenas de bloques", en *Investigación y Ciencia, Marzo 2018*

SOLANA, A. y ROCA, G. "Big Data para directivos". *2015, by Ediciones Urano, S.A.U., Barcelona*

SWISS RE. " Big data approaches to crop insurance in Asia". 2016, *Swiss Re Centre for Global Dialogue, Zurich*

SWISS RE. " Laws of large numbers. Using of big data in Asian insurance markets". 2016, *Swiss Re Centre for Global Dialogue, Zurich*

SWISS RE. " Cyber liability: Features of a data breach". 2016, *Swiss Re , Zurich*

TOURIÑO, A. "Derecho digital. De la protección de datos a la ciberseguridad". *The Valley, Digital Business School, 2016, Edición Isabel Nuñez*

UNESPA. "El libro blanco del seguro", *Madrid, 2015*

UNIÓN EUROPEA. " Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.." *Diario Oficial de la Unión Europea de 4.5.2016*

UNIÓN EUROPEA. " Building a European Data Economy". *Communication from the Commission ....., 10.1.2017*

VIVANCOS, D. " Big Data. Hacia la inteligencia artificial"". *The Valley, Digital Business School, 2016, Edición Isabel Nuñez*