Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

MÁSTER DE ACCESO A LA ABOGACÍA

TRABAJO FIN DE MÁSTER

LA DIGITALIZACIÓN DEL SEGURO

Alumno: Miguel Suárez González

Convocatoria: Ordinaria primer semestre.

Tutora: María Luisa Muñoz Paredes.

Resumen

La implementación de la tecnología en prácticamente todas las actividades de nuestra vida ha posibilitado la recolección de grandes cantidades de datos, lo que a su vez ha propiciado cambios en muchas de las actividades económicas, donde el sector seguros no es una excepción. La actividad aseguradora, que desde sus inicios se ha basado en el tratamiento de datos para hacer estimaciones, se ha visto plenamente reformada. La Inteligencia Artificial, el Cloud Computing o el Internet de las cosas son tecnologías que se han comenzado a utilizar durante las distintas fases de la cadena de valor del negocio asegurador, desde el desarrollo del producto, hasta los servicios de postventa y asistencia, pasando por la contratación de servicios o la gestión de reclamaciones. Sin embargo, este desarrollo tecnológico trae consigo algunos peligros que no pueden pasar inadvertidos. Es tarea de las sociedades ofrecer respuestas normativas que garanticen que el desarrollo tecnológico tenga lugar con pleno respeto a los derechos de las personas y entidades. Todas estas son cuestiones que exponen en el presente trabajo.

Abstract

The implementation of technology in virtually all of our lives activities has made it possible to collect large amounts of data, which in turn has led to changes in many economic activities, where the insurance sector is no exception. The insurance activity, which has been based on data processing to make estimates since its inception, has been completely reformed. Artificial Intelligence, Cloud Computing or the Internet of Things are technologies that have begun to be used during the different phases of the insurance business value chain, from product development to after-sales and assistance services, through recruitment phases or the management of claims. However, this technological development entails some dangers that cannot go unnoticed. It is the task of societies to offer regulatory responses that guarantee that technological development takes place with full respect to individuals and entities rights. All these issues are analyzed in this paper.

Abreviaturas y acrónimos.

AAVV ..... Autores varios
AEPD ..... Agencia Española de Protección de Datos
ART ..... Artículo
CEPD ..... Comité Europeo de Protección de Datos
EEUU ..... Estados Unidos
EIOPA ..... European Insurance and Occupational Pensions Authority
ENISA ..... European Union Agency for Cybersecurity
IA ..... Inteligencia Artificial
IaaS ..... Insurance as a service
IoT ..... Internet of Things
LCS ..... Ley del Contrato de Seguro
LOPD ..... Ley Orgánica de Protección de Datos
ML ..... Machine Learning
NÚM ..... Número
PÁG ..... Página
RGPD ..... Reglamento General de Protección de datos
SIDA ..... Síndrome de la Inmunodeficiencia adquirida
SS ..... Siguientes
TIC ..... Tecnologías de la Información y la Comunicación
UE. ..... Unión Europea.
UNESCO ..... United Nations Educational, Scientific and Cultural Organization
VTC ..... Vehículos de transporte con conductor

ÍNDICE

1. INTRODUCCIÓN. EL PODER DE LOS DATOS

En los últimos años se ha vivido y se está viviendo una transformación en la gran mayoría de actividades económicas, propiciadas por el desarrollo de nuevas tecnologías que hacen los procesos productivos más eficientes, ágiles y rentables. El sector de los seguros no es una excepción y prueba de ello son los cambios que las compañías aseguradoras están introduciendo en sus modelos de negocio (aunque tal vez con menor agilidad que en otras actividades económicas menos sujetas a control administrativo). El conocimiento es poder y los datos aportan conocimiento. La utilización por parte de todos los agentes económicos de nuevas tecnologías ha propiciado la recolección de ingentes cantidades de datos que hasta el momento eran inaccesibles o que, aun siéndolo, eran sencillamente ignoradas por no ser posible extraer su valor al no tener ni conocimientos ni capacidad para su tratamiento[1].

Las bases de datos han existido siempre (desde que el ser humano ha tenido capacidad para retener y contrastar información) pues no son más que conjuntos de información que se agrupan o estructuran y que permiten obtener conocimiento acerca de distintos factores para su análisis y contraste. Lo que ha cambiado y lo que les da cada vez mayor relevancia son las fuentes de las que provienen esos datos y las técnicas que utilizamos para su gestión y análisis. Si bien antiguamente el contenido de las bases de datos se extraía de forma manual, por no decir artesanal (como ocurría por ejemplo en los registros que en el campo se hacían sobre las cosechas de cada año) y su análisis era efectuado por personas, quedando por tanto limitado por las rudimentarias técnicas del momento o como mucho por la destreza mental de cada persona, con el desarrollo de las TIC la obtención de datos cada vez resulta más simple, rápida y precisa. En la actualidad todos los dispositivos electrónicos utilizados en nuestro día a día (un smartphone, un pc, un smartwatch) generan un rastro de todas las operaciones efectuadas con él (si entramos en una web, si realizamos una compra, si nos hemos desplazado…, incluso el modo en el que nos hemos desplazado; a pie, en coche, en transporte público etc.) lo que supone que existan nuevas fuentes de datos capaces de aportar mucha información de manera automática. Esto unido al hecho de que contemos con técnicas que permiten someter dichos datos a cálculos para obtener resultados concretos en periodos muy cortos de tiempo, incluso

[1] La Comisión Europea informa de que el volumen de datos producidos en el mundo está incrementándose constantemente, estimando que mientras que en el año 2018 se producían 33 zettabytes anuales de información, la previsión para el año 2025 alcanza los 175 zettabytes. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones. Una Estrategia Europea de Datos. Bruselas, 19.2.2020*. Pág.2.
Más información en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=ES

en tiempo real, permite situar a los datos en el centro de las decisiones empresariales y por tanto, en el centro de la actividad económica, "la economía del dato" de la que como ya hemos dicho, el sector asegurador no resulta inmune.

Los abogados, como profesionales que pueden desempeñar su trabajo en el ámbito asegurador, han de conocer perfectamente las tecnologías ya utilizadas en la actualidad en este sector, así como los riesgos y problemas que plantean. De lo contrario, no tendrán capacidad para defender los derechos tanto de las entidades de seguro como de los asegurados, pues con la digitalización del seguro se plantean retos jurídicos que hasta el momento no se han tenido que afrontar, como se expone en el presente trabajo.

2. TECNOLOGÍAS QUE PERMITEN EXTRAER VALOR DE LOS DATOS.

Las nuevas tecnologías que nos permiten obtener valor de los datos son, entre otras:

2.1. La inteligencia artificial (IA) y Machine Learning[2].

El término **inteligencia artificial** es un concepto amplio que engloba distintas herramientas basadas en datos y técnicas de computación. A grandes rasgos y de manera aproximada, se puede definir como sistemas diseñados para la resolución de problemas mediante métodos que tradicionalmente han sido asociados a la inteligencia humana tales como el aprendizaje, la resolución de problemas y el reconocimiento de patrones[3] o en general cualquier tarea para la que hasta el momento era necesaria la aportación humana.

Machine learning **o aprendizaje automático[4]** es una de las tecnologías que integran la inteligencia artificial y que puede ser definida como un conjunto de técnicas que permiten que un algoritmo (un conjunto ordenado de operaciones) pueda modificar su propio comportamiento (las operaciones a realizar) en base a los datos que ostenta o en base a los resultados ya obtenidos mediante el reconocimiento de patrones y que posibilita obtener un resultado óptimo. Estas técnicas pueden ser de aprendizaje supervisado, en las que el resultado al que se pretende llegar ya es conocido y que por tanto sirven para "entrenar" a la máquina hasta que obtenga el resultado deseado o bien pueden ser de aprendizaje no supervisado en los que no se define ningún objetivo que se pretenda alcanzar, sino que sólo se aportan valores de entrada, sin etiquetar, que son analizados, agrupados y de los que se buscan patrones sin que

[2] Artificial intelligence: How does it work, why does it matter, and what can we do about it? Servicio de Estudios del Parlamento Europeo 2020. Pág. 1 y ss. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf

[3] https://aws.amazon.com/es/machine-learning/what-is-ai/

[4] https://es.wikipedia.org/wiki/Aprendizaje_autom%C3%A1tico

exista un resultado concreto al que se deba llegar. Con este último modelo se consigue inferir unos resultados de los datos de entrada que no eran conocidos hasta el momento.

Una de las técnicas utilizadas para ejecutar estos aprendizajes automáticos es la de las redes neuronales artificiales que, explicadas de forma simple, son conjuntos de unidades de procesamiento[5] (funciones matemáticas) autónomas que intercambian información y resultados entre sí, funcionando por tanto en red, emulando así la manera de actuar del cerebro humano (de ahí su nombre). No obstante, su implementación según EIOPA[6] todavía es limitada en la industria aseguradora, pues aunque el 55% de las firmas aseguradoras reconoce que las tendrá que utilizar en los próximos tres años, sólo el 30% lo están haciendo ya. Cada unidad, llamada neurona artificial, está dotada de diferentes capas: la capa de entrada, formada por canales por los que se introduce la información (sea proveniente del exterior o de otras unidades), la capa oculta, formada por una o varias funciones matemáticas que permite procesar dicha información y la capa de salida que sirve como enlace con el resto de neuronas o con el exterior y por la cual se exponen los resultados obtenidos. Que la información sea procesada por las funciones matemáticas de la capa oculta puede causar problemas en relación con la transparencia en el tratamiento de datos, como veremos más adelante. Como adelanto, se puede afirmar que en términos de precisión, transparencia y explicabilidad, debido a la opacidad en el funcionamiento de la capa oculta, puede ser difícil explicar la relación causal existente entre las entradas de información y las salidas del modelo.

2.2. Cloud computing:

El *Cloud computing* o computación en la nube no es una tecnología basada esencialmente en datos, pero desempeña también un papel fundamental en la digitalización de las empresas. Consiste en la utilización de servicios de computación y almacenamiento deslocalizados través de internet[7], es decir, en el uso de servidores remotos en red que hace posible el aprovechamiento de la capacidad de cómputo de servidores distintos a los propios del usuario para almacenar, administrar o en general procesar información de manera que no es necesario que el usuario posea una gran infraestructura para tener gran capacidad de computación. Sin

[5] Para saber más sobre redes neuronales: https://www.ibm.com/docs/es/spss-modeler/saas?topic=networks-neural-model
[6] Big Data analytics in motor and health insurance: A thematic review.. EIOPA. Pág. 15.
[7] Cloud computing. An overview of economic and policy issues. Servicio de Estudios del Parlamento Europeo 2016. Pág. 3 y ss. Disponible en: https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf

embargo, esto también plantea problemas respecto al tratamiento de datos personales, como veremos más adelante.

2.3. Internet de las cosas:

Se trata de una tecnología que auxilia al resto de las descritas, pues es la que posibilita la recolecta de información del mundo físico y la traslada al mundo *online* sin necesidad de intervención humana, lo que a su vez permite contar con la información suficiente como para construir bases de datos que puedan ser tratadas con posterioridad por el resto de herramientas de Big data. Está conformada por todos aquellos dispositivos (sensores, radares, contadores…) capaces de transferir y recibir datos en red, aportando información sobre fenómenos del mundo *offline* de forma automatizada, sin que la recolecta de información dependa de la actuación de alguna persona[8].

Esta tecnología permite obtener una cantidad de información mayor y más precisa sobre fenómenos del mundo *offline*. Por ejemplo, permite conocer las pautas de comportamiento de una persona a través de la monitorización de sus hábitos con una pulsera de actividad, permite conocer las condiciones de temperatura y humedad de un determinado lugar en tiempo real, o conocer el nivel de uso que se hace de algún objeto en cada momento.

El Internet de las cosas (Internet of things, IoT) posee gran variedad de aplicaciones empresariales, donde el sector seguros no es una excepción. Disponer de mayor cantidad de información, así como de información más precisa, aporta beneficios a la industria aseguradora, como se estudia en los siguientes apartados del presente trabajo. El Internet de las cosas permite obtener en tiempo real datos sobre los objetos asegurados, lo que a su vez posibilita reducir riesgos, prevenir siniestros o mitigar sus consecuencias de forma inmediata[9], bien sea mediante la activación de mecanismos automatizados que eviten o calmen, por ejemplo, un incendio, o bien porque en base a la información que aporta el internet de las cosas se active alguna alarma o señal que permite a las personas actuar contra un siniestro, por ejemplo, llamando a un servicio de emergencias.

Un ejemplo real del uso de Internet de las cosas por compañías aseguradoras lo encontramos en la compañía estadounidense Church Mutual[10]. Esta compañía instala sensores de temperatura y fugas de agua en los inmuebles asegurados (es un seguro pensado para inmuebles

[8] Para saber más sobre el internet de las cosas: https://es.wikipedia.org/wiki/Internet_de_las_cosas
[9] The Geneva Association. From Risk Transfer to Risk Prevention. *How the Internet of Things is reshaping business models in insurance.* Pág. 8 y ss.
[10] Este seguro se encuentra disponible en la web de la compañía: https://www.churchmutual.com/sensors/

que generalmente están vacíos). Así, los sensores pueden detectar situaciones de riesgo como congelamiento de tuberías o fugas de agua. En base a los datos captados por los sensores, se generan alertas que se envían al cliente para que pueda responder. Si este no responde, la compañía avisa automáticamente a los servicios de emergencia. El objetivo se basa en comprender la dinámica de los riesgos en tiempo real y poder actuar en consecuencia de forma inmediata.

3. USO DE LAS TECNOLOGÍAS BASADAS EN DATOS EN LAS DISTINTAS FASES DE LA CADENA DE VALOR DEL NEGOCIO ASEGURADOR.

Las tecnologías mencionadas ayudan a las empresas a mejorar sus procesos productivos aportando agilidad y precisión, incrementando la eficiencia y velocidad en la toma de decisiones y reduciendo los costes operacionales[11]. En el caso concreto de las compañías aseguradoras, estas tecnologías se utilizan en prácticamente todas fases de la cadena de valor de su negocio[12].

3.1 Desarrollo del producto.

Las herramientas de Big Data Analytics son utilizadas desde la primera fase del negocio de las aseguradoras, esto es, al diseñar los productos que posteriormente lanzarán al mercado. Estas técnicas permiten a las compañías entender mejor las necesidades y las características de sus clientes lo que hace posible desarrollar productos y servicios más personalizados[13]. Las aseguradoras (y cualquier empresa) ahora tienen la capacidad de identificar patrones subyacentes en las conductas de sus clientes, lo que les permite detectar necesidades específicas a partir de las cuales es posible lanzar al mercado nuevos productos diseñados estratégicamente para satisfacer esas necesidades concretas. Un claro ejemplo son los **seguros basados en el uso**[14], estos productos se basan en los datos provenientes del Internet de las cosas, que miden tanto el comportamiento del cliente como su entorno a través de sensores instalados en los dispositivos y utensilios que aquél utiliza.

En virtud de datos como, por ejemplo, el número de kilómetros conducidos al año, el tipo de vías recorridas, la velocidad media, la franja horaria, la actitud en la conducción etc., en el caso de los seguros de motor, o de los pasos caminados cada día, las calorías quemadas, la calidad del sueño, presión arterial..., en el caso de los seguros de vida, es posible ofrecer al

[11] Big Data analytics in motor and health insurance: A thematic review. Big Data Analytics in Motor and Health Insurance: a thematic review. EIOPA. Pág. 18.
[12] The Geneva Association. Big Data, Big Impact. Asia Insurance Review, Julio 2016.
[13] CAPIELLO, A. Technology and the insurance industry. Palgrave Pivot. 2018. Pág. 31
[14] BOOBIER, T: *Analytics for Insurance*. Wiley. 2016. Pág. 155 y ss.

cliente un seguro que cubra únicamente los riesgos a los que con mayor probabilidad se puede exponer, lo que a su vez permite reducir el coste del seguro, pagando únicamente por las coberturas que necesita.

Los seguros basados en el uso son uno de los desarrollos más extendidos de la utilización de la tecnología de los datos en el sector asegurador[15]. Tradicionalmente las políticas de tarificación de las que dependen las primas de seguro se han basado en variables respecto de las que se ha demostrado que existe una relación directa con una mayor, o menor, siniestralidad y que han permitido clasificar a los asegurados en grandes grupos de riesgo. Por ejemplo, el género, la edad, los años de experiencia en la conducción, el tipo de vehículo, el estado de salud de la persona, sus hábitos diarios, entre otras, son factores que tradicionalmente se han tenido en cuenta para la determinación de los precios. Así, las técnicas de fijación de primas se han venido clasificando en dos grandes grupos[16]. Por un lado, las técnicas de tarificación *a priori*, que se aplican cuando una aseguradora no dispone de información previa sobre un potencial asegurado, en las que la compañía aseguradora establece una tarifa atendiendo al historial de siniestralidad de personas con un perfil similar que ya son clientes de la compañía. Por ejemplo, a los conductores jóvenes que les suelen ofrecer tarifas más elevadas, aún sin conocer sus hábitos de conducción, en base a la idea (a veces falsa) de que los jóvenes poseen mayores cifras de siniestralidad. Por otro lado, existen las técnicas de tarifación *a posteriori*, que se aplican cuando una compañía ya posee información sobre el asegurado (como el número de siniestros declarados hasta el momento).

Sin embargo, estas técnicas de tarificación (sobre todo las *a priori*) no permiten crear perfiles de riesgo que sea ajusten fielmente a la realidad, sino que generan perfiles basados estimaciones que no necesariamente se han de corresponder con el riesgo real asegurado (con la consecuente pérdida de competitividad en el mercado en los casos en que se exige una prima mayor de lo necesario, o la obtención de unos ingresos insuficientes en los casos en que se oferta una prima inferior a la que se corresponde con el riesgo real). Si además tenemos presente el hecho de que la competencia en el mercado es cada vez mayor y que los asegurados cada vez tienen un mejor conocimiento de su riesgo, se hace patente la necesidad de las aseguradoras de

[15] Un ejemplo de seguros basados en el uso son el que ofrece la compañía Hello Auto. Esta compañía ofrece dos seguros cuya prima depende o de la distancia recorrida o del modo de conducción. Para ello, instala un dispositivo en los coches de sus asegurados que le permite rastrear la conducción de los mismos. Disponible en: https://helloauto.com/seguros

[16] ALCAÑIZ ZANÓN, M., AYUSO GUTIERREZ, M., PÉREZ MARÍN, A.M: *El seguro basado en el uso*. Fundación Mapfre. Área de seguro y previsión social. 2014. Pág. 8 y ss.

innovar y reaccionar al respecto[17]. De todo lo expuesto, una de las consecuencias ha sido el desarrollo de los seguros basados en el uso, cuya idea fundamental radica en ofrecer cobertura para el riesgo específico y concreto al que se expone el asegurado en función del uso que el asegurado le dé a un bien o de su comportamiento, evitando destinar recursos de más para la cobertura de riesgos a los que realmente no se enfrenta un asegurado. Por ejemplo, en los seguros de motor, parece sensato cuestionar[18] el hecho de que una persona que habitualmente conduce por carreteras nacionales pague la misma prima que otra que sólo conduce en el ámbito urbano, o que aquel que sólo conduce por la noche pague lo mismo que otro que conduce por el día, o a hora punta..., ya que su exposición al riesgo no es la misma.

El desarrollo de estos seguros se asienta sobre un cambio respecto a la información que la compañía aseguradora posee acerca del asegurado. Mientras que tradicionalmente la compañía únicamente conocía los datos que el cliente le proporcionaba en una etapa precontractual[19], en la actualidad, en virtud de dispositivos telemáticos (ya sean dispositivos instalados en los coches, o en aparatos que portamos día a día las personas), las compañías son capaces de obtener datos que les permitan realizar un seguimiento del riesgo frente al que ofrecen cobertura. Esto genera diversas ventajas, además de una mayor individualización del producto, lo que implica un ajuste de las primas en función del riesgo real asegurado (al menos en teoría), permite reducir el riesgo al situar al asegurado en una posición en la que le conviene actuar activamente para prevenir el riesgo, abandonando la posición de cobertura pasiva de los riesgos[20].

Así mismo, una subespecie de los seguros basados en el uso son los seguros *on-demand*[21] (bajo demanda). Lo que caracteriza principalmente a estos seguros es la adaptación de las coberturas a las necesidades del cliente en cada momento[22]. En los seguros *on-demand* es posible la activación o desactivación de la cobertura aseguradora directamente por el asegurado, lo que dota al cliente de un poder de decisión sobre los supuestos en los que actuará

[17] CAPIELLO, A. *Technology and the insurance industry*. Palgrave Pivot. 2018. Pág. 8 y ss.
[18] El seguro basado en el uso. Fundación Mapfre. Área de seguro y previsión social. Pág. 10.
[19] MUÑOZ PAREDES, M.L., "Seguros usage-based: luces y sombras". AAVV, *Seguro de personas e inteligencia artificial*. 1ª ed., abril 2022, pág 4.
[20] MUÑOZ PAREDES, M.L., "Seguros usage-based: luces y sombras". *Seguro de personas e inteligencia artificial*, pág 21.
[21] Un ejemplo de seguro on-demand es el lanzado en 2018 por Zurich Seguros llamado *Zurich Klinc*. Se trata de un seguro para dispositivos portátiles (smartphones, ordenadores portátiles, tablets, etc.) que permite activar o desactivar su cobertura mediante el marcado de las casillas "On" u "Off" en una App. Disponible en: https://www.zurich.es/klinc
[22] Pérez-Llorca. Seguros on-demand en España. Nota Jurídica. Septiembre 2020. Disponible en: https://www.perezllorca.com/wp-content/uploads/2020/09/nota-juridica-seguros-on-demand-en-espana.pdf

la cobertura aseguradora (dentro, claro está, del marco contractual previamente estipulado). Así, con estos seguros se garantiza que el cliente únicamente pague por el tiempo que el cliente requiera, con la disminución de costes que esto supone.

No obstante, no todo lo que deriva de estos seguros son ventajas, también existen inconvenientes. Entre ellos, los más preocupantes pueden ser los siguientes. En primer lugar, el que señala María Luisa Muñoz Paredes[23], que se presenta al asegurado en caso de que las ventajas asociadas a la prevención del riesgo por su parte se configuren como una oferta promocional de la aseguradora, sin que dichas ventajas formen parte del contenido del contrato de seguro, y por tanto, sin fuerza obligacional. Si dichos beneficios se configuran de esta manera, el asegurado no los podrá exigir en caso de que consiga reducir su riesgo, sin perjuicio de que haga uso de la facultad que le otorga el artículo 13 de la Ley del Contrato de Seguro que le permite exigir una revisión de la prima en el momento de renovar la póliza. Otro inconveniente que también anuncia María Luisa Muñoz Paredes es la posibilidad de aumento de la prima por parte de las aseguradoras ante una agravación del riesgo. En estos nuevos seguros, las aseguradoras pueden conocer, mediante el seguimiento del riesgo real en cada momento, si este se ha incrementado sin necesidad de que sea el asegurado el que se lo comunique, lo que les permitirá incrementar las primas en su caso, práctica que no es contraria a lo establecido en los artículos 11 y 12 de la LCS (que permiten la modificación del contrato por el asegurador en caso de agravación del riesgo), sino que además podría considerarse como una aplicación de los mismos y que puede conducir incluso hasta la rescisión del contrato, cuestión que se examina más adelante.

Además, para poder ofrecer seguros a medida es necesario monitorear los hábitos y costumbres del cliente, acumulando datos de aspectos muy sensibles de las personas, que también pueden ser utilizados para finalidades distintas a aquellas para las que fueron recolectados.

El monitoreo directo de los hábitos de los asegurados es un fenómeno que puede entrar en directa contradicción con la normativa de protección de datos personales[24]. En concreto,

[23] MUÑOZ PAREDES, M.L., "Seguros usage-based: luces y sombras". *Seguro de personas e inteligencia artificial*, pág. 10 y ss.

[24] 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, a nivel europeo, y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, respecto a nuestra legislación nacional.

puede suponer, además de un ataque general a la privacidad[25] de los usuarios, una vulneración del principio de minimización de datos, que exige que sólo se recolecten los datos estrictamente necesarios para alcanzar los propósitos perseguidos con el tratamiento de datos, así como de otros principios, como tendremos ocasión de analizar más adelante.

También existen otros riesgos asociados a los seguros basados en el uso. Por ejemplo, ante un siniestro no previsto por las herramientas de Big Data, es posible que el cliente se quede sin cobertura aseguradora pese a que cuenta con un seguro teóricamente diseñado de forma específica para él. En este caso, no se podrá exigir responsabilidad (contractual) a la compañía aseguradora, pues el riesgo no está cubierto por la póliza. No obstante, se podrá discutir si la compañía sigue siendo responsable del siniestro en virtud de una suerte de "*culpa in vigilando*" por no haber señalado al asegurado todos los riesgos a los verdaderamente se enfrentaba, pese a que el deber de análisis del riesgo recaería sobre la compañía.

3.2. Fijación de primas.

Otra utilidad de las herramientas de Big Data en el negocio de los seguros, muy relacionada con la anterior, es la de la fijación de las primas. El Big Data permite conocer con mucho detalle una gran cantidad de aspectos del mercado, identificando con mayor precisión el riesgo a asegurar[26], lo que permite ajustar al máximo los precios que pagan los consumidores, incluso diseñando precios individualizados[27], todo ello con la finalidad de que las aseguradoras sean lo más competitivas posibles. No obstante, esto plantea una serie de cuestiones que deben ser tratadas:

3.2.1. Prácticas de optimización de precios.

Una costumbre cada vez más extendida en el sector asegurador, tal y como señala EIOPA[28], es la llamada "optimización de precios"[29] que consiste en cobrar diferentes cantidades a grupos de clientes que son similares en términos de riesgos y costes de servicio, para alcanzar así ciertos objetivos empresariales. Con estas prácticas las aseguradoras actúan basándose en factores comerciales ajenos al servicio contratado, tratando de forma distinta y situando en posición de

[25] RODRÍGUEZ-PARDO, J.M: "Aspectos éticos del tratamiento de los datos personales". *Revista Actuarios*, Nº 40. 2017. Pág. 15
[26] O´NEIL, C: *Armas de destrucción matemática*. Crown Books, 2016, Pág. 258
[27] MUÑOZ PAREDES, M.L.: "Sobre la individualización del riesgo: Elaboración de perfiles y desprotección del asegurado". *Derecho y Nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020, Pág. 590 y ss.
[28] Big Data analytics in motor and health insurance: A thematic review. EIOPA. Pág 38.
[29] Consumer Trends Report 2021. EIOPA. Pág. 25 y ss.

desventaja a unos consumidores frente a otros, pese a que como hemos dicho, son iguales en términos de riesgo y costes.

3.2.1.1. Factores ajenos al riesgo: sensibilidad de los clientes al precio.

Uno de estos factores ajenos al riesgo es la sensibilidad de los clientes al precio, así como la propensión de estos de cambiarse de compañía en favor de aquella que sea más barata. Para captar al mayor número de clientes posible, las firmas ofrecen precios muy competitivos a los clientes más sensibles al precio a cambio de subir las tarifas a aquellos otros menos propensos a cambiarse de compañía, todo ello gracias a un análisis individual de los datos que tienen las compañías de cada uno de sus asegurados. Los primeros resultan plenamente beneficiados, sin embargo, los segundos son los perjudicados. Esta conducta puede constituir una práctica desleal prohibida por nuestra Ley de Competencia Desleal (art. 16: trato discriminatorio del consumidor en materia de precios), todo dependerá de que se pruebe si esta diferencia de precios depende de algo más que de motivos comerciales.

Las prácticas de optimización de precios han despertado la atención de los reguladores[30]. Se comenta el potencial trato injusto para algunos grupos de consumidores que pueden ocasionar tales prácticas de optimización, sobre todo en los grupos de consumidores más vulnerables (personas mayores, de bajos ingresos, con poca formación...) y es que, por muy útiles que puedan resultar estas técnicas desde un punto de vista empresarial, los poderes públicos han de velar porque exista un mercado justo en igualdad de condiciones, sin olvidar claro está el principio de libertad que rige en nuestra economía.

De la misma manera, el creciente uso de técnicas de "*micro-zoning"*, consistentes en identificar y segmentar a clientes por pequeñas áreas geográficas en función de las características de la zona, creando nichos de mercado grupales, pero al mismo tiempo muy específicos[31], puede perjudicar a las personas que viven en zonas más pobres a la hora de conseguir, por ejemplo, el seguro obligatorio de coche, lo que a su vez reforzará la existencia de la desigualdad[32]. Esto pone de manifiesto que, si bien las tecnologías del dato pueden ser muy útiles y que por tanto no se puede renunciar a ellas, su utilización debe ir acompañada de medidas que disminuyan las posibles consecuencias negativas que impliquen.

---

[30] En diversos estados de EEUU se han regulado las prácticas de optimización de precios. Para consultar las medidas adoptadas en los diferentes territorios: "The use of Price optimization in insurance ratemaking". Janet Kaminski Leduc, Senior Legislative Attorney. *Oficina de investigaciones legislativas de los Estados Unidos*. Disponible en: https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm

[31] MCGURK, B: *Data profiling and insurance law*. HART PUBLISHING. 2020. Pág. 64.

[32] O´NEIL, C: Armas de destrucción matemática.2016. Pág. 343 y ss.

En este sentido, como reseña María Luisa Muñoz Paredes[33], se debe tener presente que nuestro ordenamiento jurídico otorga libertad a las entidades aseguradoras para fijar sus precios, aunque tal libertad no es absoluta. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras en su artículo 94.1 establece que las tarifas de primas se habrán de fundamentar en bases técnicas e información estadística y que habrán de ser suficientes, según hipótesis actuariales razonables, para permitir a la entidad aseguradora satisfacer el conjunto de las obligaciones derivadas de los contratos de seguro. Por tanto, la propia ley reconoce que no es posible fijar primas que no permitan cubrir los costes asociados a los riesgos cubiertos (se trata por tanto de una excepción al régimen general previsto en el artículo 14 de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, el cual, desde su reforma en el año 2018, permite la venta a pérdida siempre y cuando tal práctica no se repute desleal). Además, se indica que no podrán establecerse diferencias de trato entre mujeres y hombres, cuando las mismas consideren el género como factor de cálculo (salvo en los contratos de seguro vinculados a una relación laboral, cuando la diferencia de trato esté justificada por razones actuariales). Por tanto, aun utilizando técnicas de Big Data para la fijación de precios, las empresas aseguradoras habrán de cuidar que las tarifas sean suficientes para cubrir los costes asociados a los riesgos cubiertos y que el género no sea un factor determinante en los resultados de sus algoritmos, factor que se habrá de tener en cuenta en la fase de diseño del algoritmo.

Bajo estos presupuestos, la propia ley, en el segundo párrafo del citado artículo, reconoce expresamente que las tarifas de primas responderán al régimen de libertad de competencia en el mercado. De la misma manera, en su artículo 95.1 se expresa que las tarifas de primas no estarán sujetas a autorización administrativa, sin perjuicio de su posible ulterior control por la Dirección General de Seguros y Fondos de Pensiones.

3.3. Ventas y distribución.

A través del Big Data las aseguradoras pueden segmentar a sus clientes basándose en datos como su estado civil, el número de personas aseguradas por unidad familiar, su geolocalización etc. Los resultados de estos análisis permiten perfilar a cada cliente para hacerle llegar campañas de marketing personalizadas.

[33] MUÑOZ PAREDES, M.L: "Big data y discriminación de los asegurados". *II Congresso Internacional de Direito do Seguro*. AAVV. Pág. 378 y ss.

Algunas firmas aseguradoras ya utilizan técnicas de machine learning[34] para implementar la estrategia "*próxima mejor acción*"[35], que consiste en la evaluación de todos los datos de los que disponen de un cliente (su comportamiento pasado, sus acciones recientes, sus necesidades...) para contemplar todos los posibles productos de su interés y en base a ello, a través de la toma de decisiones automatizada del machine learning, elegir el servicio que más le pueda interesar, haciéndole llegar el mensaje correcto, en el momento exacto y en el canal adecuado, aumentando así las posibilidades de que lo contrate.

3.3.1. Clasificación y segmentación de clientes.

La prima que los clientes pagan por sus pólizas de seguro depende de una serie de factores de clasificación fijados por las compañías durante los procesos de contratación. Por lo general son utilizados para medir el riesgo y la probabilidad de que el individuo realice una reclamación o sufra un siniestro, aunque como ya hemos visto, en ocasiones también se tienen en cuenta elementos puramente comerciales. Es importante destacar que los factores de clasificación pueden ser parte de la propiedad industrial de las aseguradoras.

3.3.1.1. Factores de clasificación.

Los factores de clasificación más utilizados en los seguros de motor son: la edad del conductor, el kilometraje recorrido, el uso, la potencia, el modelo o el valor del vehículo, los años de tenencia del permiso de circulación, el tipo de cobertura, el comportamiento al volante, código postal, ocupación, riesgo crediticio, entre otros.

Según EIOPA[36], la mayoría de las aseguradoras afirma que en los últimos tres años no ha habido cambios en los factores de clasificación utilizados. Sin embargo, cerca de un tercio de las compañías de seguro de motor reconoce que, si bien los factores siguen siendo los mismos, su uso se ha incrementado en torno a un 25% (lo que puede ser consecuencia de la implementación de nuevas tecnologías). Así mismo, las firmas creen que en los próximos tres años su uso se incrementará otro 25%. Por lo que se refiere al sector de los seguros de vida, este se muestra más conservador, ya que la mayoría de las firmas reconoce que no se han variado los factores de clasificación tenidos en cuenta, ni variarán en los próximos años.

[34] Big Data analytics in motor and health insurance: A thematic review. EIOPA. Pág. 21
[35] Para saber más sobre la estrategia "siguiente mejor acción": https://www.tibco.com/es/reference-center/what-is-next-best action#:~:text=La%20siguiente%20mejor%20acci%C3%B3n%20es,el%20proceso%20de%20ventas%20personalizado.
[36] Big Data analytics in motor and health insurance: A thematic review. EIOPA. Pág 34

Por lo que se refiere a los seguros de salud, los factores de clasificación más habituales son: la condición médica al momento de suscripción de la póliza, la edad, el comportamiento habitual del individuo, el historial de reclamaciones, el tabaquismo, el consumo de alcohol, la actividad diaria, la profesión, el salario, la educación, el código postal...

La utilización de datos provenientes del Internet de las cosas puede hacer que las aseguradoras formulen a sus clientes preguntas más precisas en el cuestionario al que se refiere el artículo 10 de la Ley del Contrato de Seguro. Si el cuestionario es más preciso, las compañías tendrán un mayor control de los riesgos asegurados, reduciendo las posibilidades de que existan riesgos no declarados por los clientes, pues como se deduce dicho precepto, los clientes sólo están obligados a declarar aquellos riesgos por los que se les pregunte.

3.4. Gestión de reclamaciones

En la actualidad, un gran número de firmas ya utilizan Big Data para la gestión de las reclamaciones de sus clientes. Se utiliza el análisis masivo de datos para predecir las características de las reclamaciones y optimizar su tratamiento. Por ejemplo, se identifican patrones que sirven para clasificar a las reclamaciones según su complejidad o su riesgo de fraude y así de determina de forma ágil qué equipo debe ser responsable de su gestión.

Dos métodos de Big Data que permiten una mejor detección y mitigación del fraude son el análisis de texto y el análisis de redes sociales[37]. Las herramientas de Big Data permiten analizar datos no estructurados[38] como informes y entrevistas de asegurados. Así, por ejemplo, si se entrevista a varias personas acerca de reclamaciones que aparentemente no están relacionadas y sin embargo, todas contestan de la misma manera, las herramientas de Big Data podrían identificar patrones que muestren indicios de tratarse de una reclamación fraudulenta. También podría utilizarse el Big Data para identificar, en virtud de las redes sociales, relaciones

[37] Big Data and Regulation in the Insurance Industry. Lawrence S. Powell, PhD Executive Director Alabama Center for Insurance Information and Research University of Alabama. SSRN. Pág. 7. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2951306

[38] Los datos no estructurados son información que no tiene una estructura interna identificable. Es un conglomerado desorganizado de diferentes objetos. Más información en: https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/articles/diferencia-entre-datos-estructurados-y-no-estructurados.html y en https://www.netapp.com/es/data-storage/unstructured-data/what-is-unstructured-data/#:~:text=No%20estructurado%20significa%20simplemente%20que,predefinidos%20por%20modelos%20de%20datos.

entre personas con reclamaciones similares. Dicho análisis de las redes cada vez es más usado por las aseguradoras para controlar los fraudes[39].

Otro ejemplo actual de cómo se utilizan los datos para gestionar reclamaciones se da en el uso que se hace de los datos provenientes del internet de las cosas (sensores en los coches, smartphones, radares...) para estimar la gravedad de un accidente. En función de la mayor o menor gravedad, las reclamaciones son dirigidas al departamento de siniestros de la empresa o directamente al servicio de emergencias.

La prevención del fraude es uno de los objetivos principales de las aseguradoras. Con el apoyo de técnicas de Big Data es posible identificar aquellos supuestos en los que el siniestro tuvo lugar de forma intencionada o aquellos casos en los que se expone una idea equivocada del incidente para exonerarse de culpa (pese a que son conductas tipificadas en nuestro Código Penal como fraude). Según la Federación Europea de Entidades Aseguradoras, los fraudes son un 10% de las reclamaciones de los clientes[40].

En este sentido, la mayoría de aseguradoras utilizan ya herramientas de puntuación de los siniestros basadas en algoritmos de Machine Learning para encontrar patrones de fraude en base a ciertas características (localización del siniestro, periodo de tiempo desde que se contrata el seguro hasta que tiene lugar el siniestro, número previo de reclamaciones del tomador de la póliza...). En base a dichos factores se otorga una puntuación de fraude (cuanta mayor puntuación, mayor probabilidad de fraude). Estas técnicas se combinan con otras basadas también en Inteligencia Artificial que permiten analizar la veracidad de facturas o imágenes del siniestro, determinando si los daños y los costes se encuentran dentro del rango predefinido como adecuado o si por el contrario presentan indicios de fraude.

Evidentemente, aunque son innegables las ventajas que estas técnicas presentan, también existen riesgos asociados a ellas. Un reto que se presenta es determinar quién es responsable de que la Inteligencia Artificial cometa un error en la detección del fraude, considerando como fraudulento un supuesto que no lo es o si se considera de menor gravedad un accidente relevante, derivándolo a un departamento de la empresa que no es el adecuado. En estos supuestos se provoca un perjuicio al asegurado que en ningún caso tiene la obligación de soportar y que, de cualquier manera, el responsable está obligado a resarcir ex artículo 1902 de nuestro Código Civil.

[39] Sobre el uso de redes sociales para detectar el fraude, se exponen varios casos en la siguiente web: https://www.inese.es/el-uso-de-las-redes-sociales-para-prevenir-el-fraude-en-materia-de-seguros/
[40] Big Data analytics in motor and health insurance: A thematic review. EIOPA. Pág. 26

Además, el deseo de las aseguradoras de obtener cuantos más datos sea posible para distinguir un siniestro fraudulento de uno veraz, puede desembocar en una presión[41] por parte de estas entidades hacia los asegurados para obtener determinados datos que pueden ser comprometidos. Parece necesario establecer garantías normativas para que dicha presión sobre los asegurados no sea excesiva.

Por otro lado, en caso de que no haya sospechas de fraude es posible incluso que las compañías paguen directamente la indemnización pactada sin necesidad de ningún trámite adicional. Para ello será necesario que la IA sea capaz de revisar el clausulado del contrato de seguro (mediante técnicas de procesamiento de lenguaje natural[42] o, en la medida de lo posible, con el clausulado del contrato redactado en algún lenguaje de programación[43]). En tal caso, si se constata que se cumplen determinadas condiciones previamente pactadas, un software podría ejecutar automáticamente las contraprestaciones a las que se obligaron las partes (por ejemplo, el abono de una indemnización), lo que constituye lo que muchos llaman un Smart Contract[44] (contrato inteligente), que no deja de ser un código informático que recoge los acuerdos a los que han llegado dos partes y que posibilita la ejecución automática de las prestaciones a las que cada parte se ha obligado. No obstante, en este sentido debemos tener presente las limitaciones de estos instrumentos[45], pues muchas de las palabras clave que se utilizan en la contratación entre dos personas no pueden ser traducidas a código de programación[46].

3.5. Servicios postventa y asistencia.

Por lo que se refiere a la fase de postventa, las compañías aseguradoras también utilizan la Inteligencia Artificial como aliada para gestionar su trabajo[47]. Por ejemplo, algunas firmas han introducido respuestas automáticas en los *call centres* o han implementado servicios

[41] BOOBIER, T: Analytics for Insurance. Pág 58.
[42] Como puede ser GPT-3, para saber más: https://es.wikipedia.org/wiki/GPT-3
[43] Entre ellos, destacan Python, Java o C/C++ entre otros.
[44] Para saber más sobre Smart Contracts: TUR FAÚNDEZ, C.E: *Smart contracts: Análisis jurídico (Derecho de las nuevas tecnologías.* Editorial Reus, 2018.
[45] VEIGA COPO, A.B: *Seguro y tecnología. El impacto de la digitalización en el contrato de seguro*. Civitas Thomsom Reuters. 2020, pág. 183 y ss.
[46] Se debe tener presente que la "traducción" de las condiciones del contrato de seguro a algún lenguaje de programación (código informático) es una cuestión prácticamente imposible, toda vez que el lenguaje jurídico que integra el contrato de seguro no puede ser transcrito a lenguaje de código (al menos en la actualidad). A lo sumo, se podrían transcribir ciertas estipulaciones de carácter condicional que hagan posible que un software ejecute las prestaciones a las que se obligan las partes (por ejemplo, que en caso de que la temperatura de una habitación supera determinados grados, se avise al servicio de bomberos o, por ejemplo, que si no se ha comunicado ningún siniestro en determinado tiempo, se reduzca la prima a pagar por el asegurado), pero no parece posible una traducción íntegra de los contratos de seguro a lenguaje de código.
[47] Big Data analytics in motor and health insurance: A thematic review. EIOPA. Pág. 22 y ss.

robotizados en la evaluación de la calidad. A través del Machine Learning las compañías analizan las interacciones de los clientes con las herramientas mencionadas para desarrollar comunicaciones más simples, rápidas y significativas.

También se está generalizando la utilización de asistentes virtuales o *chatbots*. Estas son aplicaciones capaces de mantener conversaciones como un humano vía voz o texto y que presentan ventajas tanto para las firmas, pues incrementan la eficiencia del servicio y la reducción de costes operacionales, como para los clientes, pues se trata de aplicaciones que posibilitan un servicio postventa permanente a cualquier hora y cualquier día del año.

Una vez vistas las aplicaciones que tienen las nuevas tecnologías en las distintas fases de la cadena de valor del negocio de los seguros, debemos analizar otros aspectos relevantes del uso de estas técnicas que, sin duda, deberán ser tratados desde el punto de vista normativo.

4. PROBLEMAS DEL ANÁLISIS MASIVO DE DATOS EN EL SECTOR SEGUROS.

Los algoritmos son instrumentos útiles, eficaces y potentes que permiten obtener resultados que sin ellos sería prácticamente imposible alcanzar (por ejemplo, detección de patrones ocultos, realización de predicciones, resolución de problemas complejos en cortos periodos de tiempo, entre otros). No obstante, no son instrumentos perfectos, pues tanto en su diseño como en su utilización, se puede incurrir en errores que hagan que los resultados obtenidos no sean acertados. Pasamos a exponer algunos de los peligros que conllevan.

4.1. Discriminaciones y tratos injustificados.

Generalmente las aseguradoras a la hora de diseñar productos y fijar precios, siguen clasificando a los potenciales clientes en grupos grandes y homogéneos de personas en función de características grupales y comunes de colectivos[48] (por ejemplo, el código postal o la renta familiar), lo que supone una segmentación de los clientes, pero no una verdadera individualización. Esta no individualización conlleva un trato igual para situaciones que, aun con características comunes, son desiguales, pese a que probablemente se proyecten en el

[48] Sobre formas de discriminación directa e indirecta de los asegurados, consultar: MCGURK, B: *Data profiling and insurance law*. Pág 68 y ss.

mercado como servicios personalizados[49]. El problema no reside en ofrecer los mismos productos a distintos clientes, sino en ofrecer productos que aparentemente son a medida, pese a que realmente van dirigidos a clientes con características distintas. Aunque para algunos integrantes del grupo esto sea beneficioso, para otros puede ser perjudicial pues adquirirán productos que realmente no se ajustan a sus necesidades, pese a su creencia de que son los adecuados para ellos.

Este problema puede ser mayor si es justificado y camuflado por la utilización de métodos estadísticos que le dan "un aire artificioso de imparcialidad científica"[50]. El hecho de utilizar métodos analíticos que, al menos en apariencia, son rigurosos y precisos, dota de cierta opacidad a la manera en que los clientes (en su mayoría consumidores) son clasificados, lo que implica que quepa la posibilidad de que se produzca una manipulación del mercado sin que los consumidores se enteren siquiera[51].

Es evidente que renunciar a las ventajas que aporta el análisis masivo de datos supone un retroceso en el desarrollo social y económico, pero a su vez, delegar en los algoritmos, como instrumentos complejos y poco inteligibles, todas o gran parte de las decisiones que afectan a los consumidores supone un retroceso en cuanto a protección de los consumidores se refiere, pues resulta mucho más complejo defenderse de decisiones que no se sabe cómo se han tomado. La solución puede pasar por exigir a las aseguradoras una explicación de la manera en que se encuadra a cada cliente en un grupo u otro y de las razones por las que se les ofrecen unos servicios u otros.

Además, también se debe tener presente que no toda diferencia de trato debe ser considerada discriminación. Así, como indica María Luisa Muñoz Paredes[52]., se debe distinguir entre diferenciación en materia de precios y discriminación. Por ejemplo, la Ley del Contrato de Seguro, en sus disposiciones adicionales cuarta y quinta, prohíbe la diferenciación de trato a personas con discapacidad y a personas portadoras de SIDA/VIH. Sin embargo, en caso de

[49] Por ejemplo, la aseguradora Reale Seguros presenta los "seguros a medida", por contraposición a los "seguros paquetizados", como productos diseñados específicamente para cada cliente mediante la recogida de datos y la detección de sus patrones de comportamiento, gracias al uso de Big data.
Esta publicidad cada vez es más frecuente en el mercado del seguro, por lo que resulta necesario garantizar que la misma sea veraz, y no una mera estrategia de marketing. Más información acerca de los "seguros a medida" de Reale en: https://blog.reale.es/seguros-a-medida-que-son-por-que-y-cuando-contratarlos/

[50] O´NEIL, C: *Armas de destrucción matemática*, 2016, pág 256.

[51] Tal práctica podría producir un incremento de los precios o márgenes comerciales que constituya una intervención en el mercado tipificada como infracción por el artículo 47.1 f) del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

[52] MUÑOZ PAREDES, M.L: "Big data y discriminación de los asegurados". *II Congresso Internacional de Direito do Seguro.* AAVV. Pág 380 y ss.

que tal diferencia de trato se encuentre fundada en causas justificadas, proporcionadas y razonables, que se hallen documentadas previa y objetivamente, la misma será lícita. Por tanto, en virtud de estas disposiciones, resultaría legítimo ofrecer un precio distinto a personas con discapacidad o VIH si se trata de un seguro de salud o de vida y tales circunstancias influyen en el riesgo asegurable.

Distinto al problema de la discriminación en materia de precios es el problema del incremento del número de personas inasegurables (personas con un nivel de riesgo elevado a las que las entidades aseguradoras no ofrecen cobertura). Este aumento no constituye una discriminación como tal, como señala María Luisa Muñoz Paredes[53], sino que se trata de una consecuencia natural derivada de la capacidad actual de las aseguradoras de medir el riesgo individual con mayor precisión y fijar el precio de forma proporcional. No obstante, el hecho de que sea una consecuencia natural no implica que ésta sea deseable, sino que incluso debería ser una cuestión a tratar activamente para paliar sus efectos. Pese a ello, no es una discriminación pues tal efecto deriva de exigir a cada persona un precio que se ajuste a su nivel de riesgo, siempre y cuando la medición de riesgos se haga conforme a criterios objetivos. Así, se abandonaría la dinámica típica del seguro que propicia que algunas personas paguen una prima más alta de la que le corresponde para compensar el nivel de riesgo que asumen las aseguradoras ofreciendo cobertura a otras personas más riesgosas (las ahora inasegurables). Por ello, como indica la citada autora, habrá insolidaridad, pero no discriminación. Además, no se trata de una consecuencia inevitable, pues el incremento del número de inasegurables puede frenarse si, midiendo el riesgo real de cada individuo, las aseguradoras ofrecen productos con coberturas más sencillas, pero con condiciones más asequibles.

Con todo, se pone de manifiesto la existencia de dos modelos de seguros, los individualistas, en los que cada asegurado paga según su nivel de riesgo real, y los modelos mutualistas[54], en los que personas con menor nivel de riesgo contribuyen a la financiación de las coberturas de aquellos con mayor riesgo. Corresponde ahora a cada persona determinar qué modelo considera preferible (pues ninguno es mejor que el otro), aunque parece que la digitalización nos conduce hacia el modelo individualista. Al mismo tiempo, se debe tener

[53] MUÑOZ PAREDES, M.L: "Big data y discriminación de los asegurados". *II Congresso Internacional de Direito do Seguro.* AAVV. Pág 371 y ss.

[54] A su vez, entre los seguros mutualistas, podríamos diferenciar entre los seguros solidarios y los seguros mutualistas propiamente dichos. La diferencia entre ambos, en términos generales, reside en que los seguros solidarios están proporcionados por las autoridades públicas, sin tener en cuenta el perfil de riesgo de cada persona y con el objetivo de lograr una distribución del riesgo para garantizar una cobertura más universal, mientras que los seguros mutualistas se basan en un análisis individual del riesgo por las aseguradoras privadas en el mercado. *Vid*. McGURK, B: *Data profiling and insurance law*. 2020. Pág. 62 y ss.

presente que las aseguradoras son empresas con ánimo de lucro, diseñadas para obtener beneficios, siendo razonable por ello que les interese exigir a cada asegurado un precio que se adecúe a su nivel de riesgo real.

4.2. Fallos y sesgos en algoritmos.

Como defiende Cathy O´Neil en su libro "Armas de destrucción matemática", los modelos de análisis de datos no pueden ser nunca perfectos, pues no es posible recoger completamente todos y cada uno de los factores de la vida real, sino que son una simplificación de la realidad en base a las ideas, preferencias y creencias de sus creadores[55]. Estos introducen en el modelo aquellas variables que consideran más importantes y prescinden de aquellas otras a las que otorgan menos relevancia, por lo que, los modelos arrastran sesgos, creencias y tendencias de quienes los crean.

En este mismo sentido se pronuncia EIOPA[56], defendiendo que en los algoritmos de aprendizaje automático supervisado (según declara el mismo organismo, el 90 % de todos los sistemas de IA utilizados hasta la fecha) se etiquetan ciertas variables o conjuntos de datos conforme a juicios humanos que podrían reflejar prejuicios de la persona que etiquetó los datos (por ejemplo, los evaluadores de siniestros que etiquetan una reclamación como fraudulenta o no). Dado que esas etiquetas sirven como verdad básica, cualquier sesgo en los datos usados para entrenar el modelo, sea accidental o intencional, se reproducirá y se reflejará en la salida del sistema.

Por lo tanto, aunque se trate de instrumentos basados en cálculos matemáticos, no son plenamente objetivos y neutrales, sino que poseen intrínsecamente las influencias de sus diseñadores. Además, tales modelos necesitan ser actualizados constantemente introduciendo nuevas variables que surgen en la realidad.

Esto no quiere decir que los algoritmos sean instrumentos poco deseables, perpetuadores de sesgos y prácticas discriminatorias propias de las personas, pues simplemente son instrumentos conformados por una serie de operaciones lógico-matemáticas a los que se les aplican unos datos. Lo que se pretende reseñar es que, a pesar de que son instrumentos muy deseables, no son perfectos y sus resultados no deben ser mitificados.

[55] O´NEIL, C: *Armas de destrucción matemática*. 2016, Pág 32.
[56] Artificial Intelligence Governance Principles: towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector", EIOPA, 2021, pág. 28 y ss

Por esta razón defiende EIOPA[57] la importancia de hacer esfuerzos para monitorear y mitigar o eliminar los sesgos en los datos de entrenamiento y prueba de los modelos, evitando que estos sesgos se reproduzcan en los resultados de los sistemas de Inteligencia Artificial.

Otro aspecto que se debe cuidar en la utilización de algoritmos es la calidad de los datos con los que funcionan. Un algoritmo es capaz de obtener resultados imposibles para la mente humana, pero dichos resultados dependen directamente de los datos que "alimentan" al algoritmo. Por tanto, no sólo se debe cuidar el diseño de los algoritmos, sino también "la materia prima" con la que funcionan. Si la información con la que trabaja el algoritmo está sesgada o es errónea, el algoritmo puede reproducir ese sesgo o error en sus resultados, actuando como fuerza multiplicadora de dichos sesgos o errores. Surge así la necesidad de que las bases de datos en virtud de las cuales funcionan los algoritmos sean controladas, al menos en cuanto a su veracidad, para evitar ese efecto amplificador de sesgos y errores no deseable[58].

Otra cuestión fundamental es si las aseguradoras deberían estar vetadas o no a la hora de recoger información sobre el riesgo de un cliente[59]. Es claro el hecho de que los datos que se utilicen para analizar y clasificar a los clientes han de ser veraces, precisos y auténticos. Sin embargo, existen factores que, aunque objetivamente pueden aumentar el riesgo de una persona (y que, por tanto, su concurrencia justificaría el encarecimiento de la prima) es posible que no dependan de la voluntad del sujeto (por ejemplo, una discapacidad). Parece que lo justo es que las personas sólo paguen el precio de aquellos factores que, influyendo en su riesgo, dependan de su voluntad. Esta hipótesis implica que existan datos que, a pesar de influir en el nivel de riesgo de una persona, no deban ser utilizados por las empresas. La cuestión no es sencilla, pues la concurrencia de factores que incrementan el riesgo relativo a una persona puede hacer que el ofrecimiento de cobertura a la misma sea antieconómico para las empresas. Por esta razón, resulta necesario que los poderes públicos sean los que determinen cuáles son los datos que pueden, y sobre todo los que no pueden, ser utilizados por las aseguradoras, aunque, como ya hemos dicho, una diferencia de trato por razones objetivas y justificadas es válida y no supone, en principio, una discriminación.

[57] Artificial Intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector", EIOPA, 2021, pág 22.
[58]CAMPIONE, R: "Humaquinismo. Una panorámica sobre el ser humano, la robótica y la inteligencia artificial", *Derecho y nuevas tecnologías,* AAVV. Civitas Thomsom Reuters. 2020, Pág. 65.
[59] MCGURK, B: Data profiling and insurance law. 2020, pág. 75.

4.3. Transparencia en los algoritmos.

Muy conexo con el problema de los fallos y sesgos en algoritmos se encuentra el problema de la transparencia. En el proceso de contratación de un seguro, de forma previa, tiene lugar una evaluación de los riesgos que se pretender asegurar y que posibilita la determinación de la prima a pagar.

Cuando en ese análisis del riesgo se utilizan algoritmos (que analizan y combinan multitud de factores sobre el objeto a asegurar) resulta necesario que el cliente tenga la posibilidad de obtener información transparente e inteligible sobre los criterios que se han utilizado para determinar su nivel de riesgo. Sería importante que se reconozca expresamente (bien sea a nivel normativo o a nivel contractual) el derecho del asegurado a conocer el funcionamiento, la lógica y los criterios utilizados por el algoritmo para evaluar su riesgo y determinar su prima, y a hacerlo de una forma simple, accesible y clara, pues de nada serviría que el cliente conozca los criterios técnicos (estadísticos, probabilísticos, computacionales...) en los que se basa la decisión del algoritmo si no están adaptados a un lenguaje que el cliente medio pueda comprender. Esta es la única manera que posibilita que cualquier cliente se pueda defender frente a decisiones de la IA que le resulten perjudiciales. Además, este enfoque posibilita el control de los criterios utilizados, pues de lo contrario sería imposible conocer si, por ejemplo, se utilizan criterios discriminatorios o arbitrarios prohibidos por nuestro ordenamiento jurídico.

En este sentido se ha pronunciado la UNESCO en su *Recomendación sobre la ética de la Inteligencia Artificial*[60], que tiene por objetivo proporcionar un marco universal de valores, principios y acciones para orientar a los Estados en la formulación de sus leyes, políticas u otros instrumentos relativos a la IA y orientar las acciones de las instituciones públicas y empresas del sector privado a fin de asegurar la incorporación de la ética en todas las etapas del ciclo de vida de los sistemas de IA, entre otros.

4.3.1. Principios de transparencia y explicabilidad.

La UNESCO señala que la falta de transparencia de los sistemas de Inteligencia Artificial "*podría mermar la posibilidad de impugnar eficazmente las decisiones basadas en resultados producidos por los sistemas de IA".* No obstante, es consciente de la necesidad de

[60] Recomendación sobre la ética de la inteligencia artificial. UNESCO. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa/PDF/380455spa.pdf.multi

"*encontrar un equilibrio entre la transparencia y la explicabilidad y otros principios como la privacidad, la seguridad y la protección".*

Además, reconoce el derecho de las personas a estar plenamente informadas de los supuestos en los que una decisión se basa en algoritmos de IA, afirmando que "*deberían tener la oportunidad de solicitar explicaciones e información al actor de la IA*", apuntando, por añadidura, que "*las personas deberían poder conocer los motivos por los que se ha tomado una decisión* (en base a la IA) *que afecta a sus derechos, y tener la posibilidad de presentar alegaciones*".

Declara, por otra parte, que la transparencia debe permitir a las personas comprender cómo se implementa cada etapa de un sistema de IA, así como proporcionar información sobre los factores que influyen en una predicción o decisión específica.

Por lo que se refiere al principio de explicabilidad[61], este "*supone hacer inteligibles los resultados de los sistemas de IA y facilitar información sobre ellos. La explicabilidad de los sistemas de IA también se refiere a la inteligibilidad de la entrada, salida y funcionamiento de cada componente algorítmico y la forma en que contribuye a los resultados de los sistemas...Los actores de la IA deberían comprometerse a velar por que los algoritmos desarrollados sean explicables".*

Llegados a este punto, se debe ser consciente del reto que supone tal principio de exigibilidad y de cuáles son sus límites. Los algoritmos, en muchas ocasiones, son verdaderamente complejos, con miles de variables y funciones (cajas negras). Si bien es fácil entender la función final de un algoritmo, puede ser muy difícil comprender y explicar cómo se llegó al resultado obtenido[62]. Además, los resultados del algoritmo no dependen sólo de la arquitectura del modelo, sino que, por ejemplo, en el Machine Learning los resultados dependen de los datos de los que aprende el algoritmo, si los datos están sesgados, el resultado también estará sesgado, como ya se ha advertido.

[61] La Comisión Europea también hace referencia al principio de explicabilidad en su informe "Directrices Éticas para una IA fiable". Según el Organismo Europeo, en los sistemas de IA "es preciso comunicar abiertamente las capacidades y finalidad de los sistemas de IA y las decisiones deben poder explicarse – en la medida de lo posible- a las partes que se vean afectadas. Sin esta información, no es posible impugnar adecuadamente una decisión. No siempre resulta posible explicar por qué un modelo ha generado un resultado. Esos casos, que se denominan algoritmos de "caja negra" requieren especial atención…" Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019, Pág. 16, disponible en: https://data.europa.eu/doi/10.2759/14078

[62] https://www.deeplearning.ai/the-batch/issue-146/

También sobre esta cuestión se pronuncia EIOPA[63], reconociendo que las empresas de seguros deben esforzarse por utilizar modelos de IA explicables. Sin embargo, el organismo europeo es consciente de la dificultad de esta tarea, reconociendo que ciertos sistemas de IA pueden considerarse "cajas negras" cuando la lógica de los resultados o predicciones de los sistemas son difíciles de explicar (sobre todo los que tienen capacidad para aprender autónomamente). Por ello, el organismo supervisor propone que las aseguradoras, en ciertos casos, combinen la explicabilidad de sus modelos con otras medidas de gobernanza que garanticen la responsabilidad de las empresas y la existencia de mecanismos de reparación del daño causado a cada cliente, como pueden ser un mayor nivel de supervisión humana y una mejor gestión de los datos a lo largo del ciclo de vida del modelo de IA.

Ambos principios (transparencia y explicabilidad) están ligados al principio de rendición de cuentas, al que también hace referencia la UNESCO, cuando afirma que "*las acciones basadas de alguna manera en un sistema de IA siempre deberían ser atribuibles, en última instancia, a los actores de la IA".* Además, la falta de transparencia y explicabilidad podría comprometer la auditabilidad del sistema, pues se reducen las posibilidades de identificar las circunstancias en las que el modelo puede proporcionar predicciones incorrectas.

4.4. La opacidad de los algoritmos y el problema de la indefensión.

La opacidad de los modelos genera desconfianza por parte del cliente, provocando el rechazo decisiones que serían aceptables si se entendiera cómo o por qué se han tomado. Un ejemplo que evidencia esto es el expuesto por Cathy O'Neil[64]: "*Si un acomodador nos dice al llegar a un concierto al aire libre que no podemos sentarnos en las diez primeras filas de asientos, puede que pensemos que eso es inaceptable. Sin embargo, si nos explica que las diez primeras filas están reservadas para personas en silla de ruedas, nos parecería perfectamente lógico*". La transparencia importa y marca la diferencia.

Los asegurados han de poder conocer qué datos posee una aseguradora sobre ellos y, lo que es más importante, debe tener la posibilidad de saber y comprender cómo se han utilizado para la toma de decisiones que le puedan afectar. La complejidad de los métodos de análisis de datos crea un "efecto de caja negra", es decir, una aparente opacidad que hace muy difícil

[63]Artificial Intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector", EIOPA, 2021, pág. 40 y ss.
[64] O´NEIL, C: Armas de destrucción matemática.2016, Pág 46.

comprender los procedimientos y resultados de las técnicas de análisis masivo de datos. El hecho de que los asegurados no tengan la capacidad de rastrear los procesos y motivos que se han tenido en cuenta para tomar una decisión que les perjudica, los sitúa en una inevitable posición de indefensión. Si los algoritmos operan de una manera que no permite conocer por qué las primas de un asegurado son altas, este no podrá identificar los comportamientos que debe cambiar o mejorar para reducir su prima[65].

Pese a que la solución ideal es que los usuarios tengan la capacidad de conocer cómo y por qué se les encuadra en un grupo u otro de clientes, la cuestión no es sencilla, pues muchas empresas defenderán que los criterios y la lógica de sus algoritmos forma parte de su propiedad intelectual o industrial y que, por tanto, no tiene por qué ser divulgada.

Surge por tanto un conflicto entre el derecho de las personas a conocer los criterios por los cuales se les clasifica en un grupo u otro de clientes (y que resulta imprescindible para defenderse frente a decisiones arbitrarias y/o perjudiciales) y el derecho de las empresas a salvaguardar su propiedad industrial o intelectual, algo que por otro lado es completamente legítimo y lógico.

4.5. La protección legal de los algoritmos.

La posibilidad de proteger a un algoritmo mediante alguna forma de propiedad intelectual o similar es una cuestión compleja, con argumentos a favor y en contra[66]:

La Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador, en su considerando 11, establece que "*las ideas y principios implícitos en los elementos del programa* (de ordenador), *incluidas las de sus interfaces, no pueden acogerse a la protección de los derechos de autor con arreglo a la presente Directiva",* así como que "*en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están protegidos con arreglo a la presente Directiv*a", lo que excluye expresamente a los algoritmos de dicha protección. Se establece también que "d*e acuerdo con la legislación y jurisprudencia de los Estados miembros y los convenios internacionales en la materia, la expresión de dichas ideas y principios debe protegerse mediante derechos de autor*".

[65] MCGURK, B: Data profiling and insurance law. 2020. Pág 56.
[66]Sobre la protección legal de los algoritmos: https://www.garrigues.com/es_ES/garrigues-digital/proteger-algoritmos-big-data-economia-digital y https://www.expansion.com/economia-digital/innovacion/2016/04/17/5706510c46163fa5648b45a6.html y https://ecija.com/algoritmo-software-donde-reside-propiedad-intelectual/

En nuestra legislación nacional, el artículo 96.4 del Real Decreto Legislativo 1/1996 por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual establece que "*No estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces"*. Es preciso determinar qué se entiende por ideas y principios de un programa de ordenador, si esta expresión incluyera los criterios en base a los que un algoritmo clasifica a un cliente, es probable que dicha parte del algoritmo no esté protegida por derechos de propiedad intelectual.

Si se quisiera proteger a los algoritmos como patentes, tanto el Convenio de Munich sobre concesión de Patentes Europeas, como nuestra Ley 24/2015 de Patentes, establecen que no se considerarán invenciones "*los métodos matemáticos*" ni "*los planes, reglas y métodos para (…) actividades económico-comerciales, así como los programas de ordenadores*", por lo que tampoco parece posible proteger a los algoritmos como patentes.

La manera más factible de proteger a los algoritmos es considerarlos secretos empresariales, amparados por la Ley 1/2019, de secretos empresariales. Esta normativa no contiene ninguna exclusión relacionada con los programas informáticos o a métodos matemáticos, sin embargo, para que la misma sea aplicable, es necesario que la información o conocimiento que se quiera proteger sea secreto, tenga un valor empresarial y haya sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

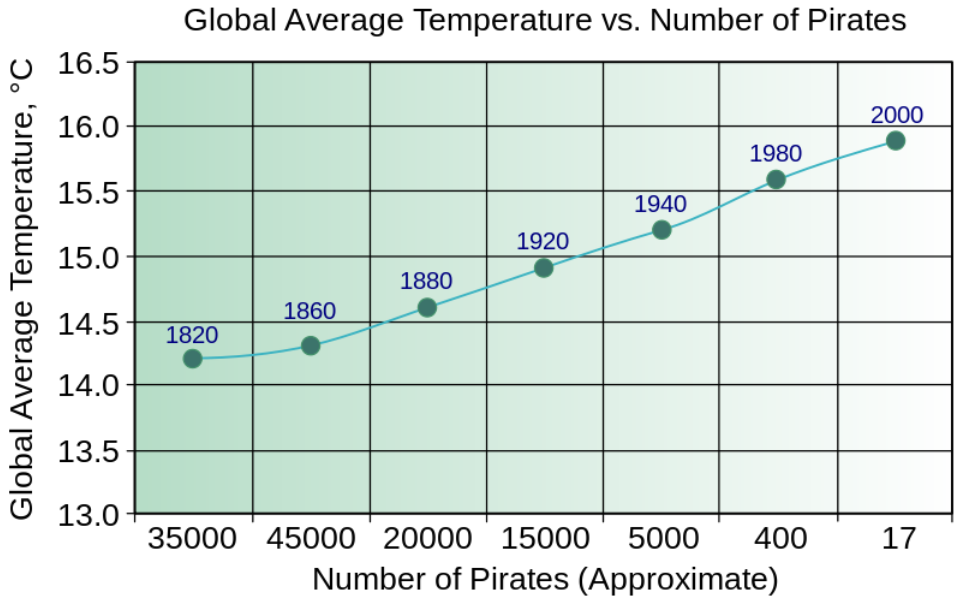
Si se exige que las aseguradoras hagan públicos los criterios o métodos en base a los cuales se clasifica a un cliente, es posible que no se cumpla con los requisitos necesarios para que resulte de aplicación la citada Ley 1/2019. Una solución para solventar este obstáculo puede ser la imposición de la obligación de respetar la confidencialidad de los algoritmos a aquellos asegurados que quieran conocer cómo se les ha clasificado por parte de un algoritmo, justificando dicha necesidad y limitando su utilización a las mera de defensa de sus intereses o mediante la divulgación únicamente de los criterios utilizados por los algoritmos para la clasificación de clientes, pero sin desvelar la composición del algoritmo en todos sus aspectos.

4.6. El problema de la correlación y el problema del contexto.

Es probable que los datos analizados por las compañías aseguradoras provengan de fuentes de terceros, con los que se produzcan cruces de información que pueden ocasionar la toma de decisiones de forma incorrecta. Eso da lugar a los problemas de correlación y contexto.

Se dice que con las técnicas de análisis masivo de datos se identifican correlaciones y no causas[67], es decir, con ellas se identifican patrones comunes de ciertos factores que permiten predecir determinados resultados, pero no se identifican las causas de dichos patrones[68]. En ese empeño de identificar patrones comunes tiene lugar el problema de la correlación. El análisis de datos basado en correlaciones posibilita cuantificar el grado en que se relacionan dos variables.

Un ejemplo que permite comprender el problema de la correlación es el que representa el siguiente gráfico[69]:



Este gráfico expresa la evolución de la temperatura media global y la evolución del número de piratas que han existido en los últimos doscientos años. A simple vista, se podría extraer como conclusión que cuantos más piratas hay en el mundo, menor es la temperatura media global. Sin embargo, aunque es cierto que en los últimos doscientos años la temperatura media global ha ascendido y el número de piratas ha descendido, resulta evidente que el aumento de la temperatura terrestre no se debe a la disminución del número de piratas.

Como vemos, la correlación no es suficiente para demostrar causalidad. Si existe alguna variable oculta de la cual dependen los datos observados, entonces correlación no implicaría causalidad. En el ejemplo anterior, la temperatura media global ha ido aumentando por diversos factores (aumento de la emisión de CO2, desforestación...), que no se tienen en cuenta en el

[67] MCGURK, B: Data profiling and insurance law. 2020. Pág. 54.
[68] https://keepcoding.io/blog/correlacion-estadistica-big-data/
[69] Gráfico y conclusiones extraídas de: https://www.gradiant.org/blog/claves-analisis-causal/

gráfico (variables ocultas), y lo mismo ocurre con la disminución del número de piratas, sin que se pueda afirmar la relación de causalidad entre la evolución de las dos variables.

Esto puede ocurrir en el sector asegurador con el uso de Big Data. Si al analizar el nivel de riesgo de un cliente se identifican patrones comunes con otras personas de riesgo más elevado es probable que se clasifique al cliente con un riesgo superior al que le corresponde (asociándolo con esas otras personas con las que comparte algún patrón común), con las consecuencias perjudiciales que para él conlleva.

Si las aseguradoras, y las empresas en general, al emplear técnicas de análisis masivo de datos utilizan correlaciones para tomar decisiones sobre sus clientes sin comprender las razones subyacentes de dichas correlaciones, tales decisiones podrían ser erróneas y generar daños a aquellos.

Por tanto, el análisis basado en correlaciones opera comparando a un cliente con otros clientes con los que comparte una misma característica, asociándolos con base en dicho factor común y tratándolos de la misma manera, a pesar de que por el resto de sus características se trate de clientes con un perfil distinto[70]. Por ejemplo, es posible que una compañía de seguros de motor identifique a un grupo de clientes por tener un riesgo crediticio alto, al haber incumplido todos ellos sus obligaciones de pago de algún crédito del pasado y que, sin embargo, su nivel de riesgo al volante sea distinto. Si a todas estas personas se las clasifica de la misma manera, atendiendo a dicho factor común (el alto riesgo crediticio), no se las clasificará según su riesgo real, lo que provocará que identifique a varios potenciales clientes como personas con un alto riesgo por haber incumplido sus obligaciones de pago de un crédito en el pasado, pese a que dicho factor no está relacionado con el riesgo a asegurar. Todos los clientes serán tratados como personas con alto riesgo, pese a que realmente no todas tienen el mismo riesgo al volante (aunque todas ellas sí lo puedan tener a la hora de devolver un crédito).

Tradicionalmente, las aseguradoras han segmentado a sus clientes atendiendo a factores de riesgo prestablecidos con técnicas actuariales, como su edad, su género... Sin embargo, gracias al desarrollo de nuevas tecnologías y al análisis masivo de datos, cada vez se utilizan más criterios, muchos de los cuales no están directamente relacionados con el riesgo a asegurar, por ejemplo, el uso de redes sociales o su historial de compras online[71]. El hecho de que existan factores comunes entre personas que utilizan mucho las redes sociales o que compran

[70] MCGURK, B: Data profiling and insurance law. 2020. Pág. 55
[71] MCGURK, B: Data profiling and insurance law. 2020. Pág. 55

determinados productos online y personas con un nivel de riesgo elevado, no implica que todos los que presenten dichas características presenten un riesgo objetivamente mayor.

En concreto, y aquí reside la mayor crítica en relación con el problema de la correlación, al segmentar a los asegurados de esta manera, en lugar de generar un perfil de riesgo individualizado, algunos asegurados pueden encontrarse con que sus primas están vinculadas a las de otros que realmente tiene un perfil distinto, pero con los que comparten alguna característica que puede no ser la causa de un riesgo.

Como conclusión cabe afirmar que, aunque es cierto que los datos masivos en ocasiones pueden ser la solución para identificar con mayor precisión el riesgo individual de cada asegurado, es necesario que los datos valorados sean los adecuados y que estos sean tratados mediante las técnicas apropiadas (lo que se garantiza si los modelos son transparentes, como se expuso con anterioridad), pues de lo contrario, cabe la posibilidad de que personas con distinto nivel de riesgo sean tratados de la misma manera (exigiéndoles por ejemplo el pago de primas idénticas) en base a que comparten ciertos factores comunes (ajenos al riesgo) con otras personas que sí tienen un mayor nivel de riesgo, y que por tanto, sí deberían pagar una prima mayor.

Además, existe e**l problema del contexto.** Aunque las aseguradoras utilicen datos y técnicas adecuadas para evaluar el riesgo de un asegurado, es necesario que dicha información sea interpretada en el contexto correcto, de lo contrario, las aseguradoras diseñarán patrones erróneos de los datos analizados. Por ejemplo, respecto a las reclamaciones contra los seguros por accidentes de tráfico, los datos sobre la velocidad de los conductores en el momento del siniestro deben ser contextualizados combinándolos con otros datos como el tráfico, el tiempo meteorológico o las condiciones de la carretera. Que el asegurado accidentado haya conducido a la velocidad adecuada puede no ser información suficiente para determinar o no su culpabilidad. Es necesario combinar todos aquellos datos que sean necesarios para entender la situación a analizar.

Cuantas más fuentes de datos se fusionen (trazado de las carreteras, datos meteorológicos, intensidad del tráfico...), mejor será la recreación del siniestro que realicen las aseguradoras, pero también se habrán de tomar mayores garantías para asegurar que se extraen las inferencias correctas de los datos, pues como se ha expuesto, unos datos mal interpretados provocarán la toma de decisiones equivocadas.

Por todo lo expuesto, se pone de manifiesto la necesidad que surge de regular los algoritmos por parte de los poderes públicos, algo que ya ha iniciado la Unión Europea en su Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, en cuya exposición de motivos 3.5 reconoce que "*El uso de la IA, con sus características particulares (p. ej., la opacidad, la complejidad, la dependencia de datos, el comportamiento autónomo) puede tener repercusiones negativas para múltiples derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»). La presente propuesta pretende garantizar un elevado nivel de protección para dichos derechos fundamentales*".

5. CAMBIOS EN EL MODELO DE NEGOCIO EN LA INDUSTRIA DEL SEGURO.

El sector asegurador ha comenzado a digitalizar la mayor parte de la cadena de valor de su negocio, en un intento de mejorar la calidad, incrementar la personalización de sus servicios, disminuir costes y aumentar la competitividad de las aseguradoras en el mercado, todo ello como consecuencia del desarrollo tecnológico y el cambio de hábitos de los asegurados.
Las plataformas digitales constituyen canales de comunicación directa con el cliente, reduciendo en ocasiones la necesidad de intermediarios como agentes y corredores[72].

Aquellos servicios que tienen un alto valor añadido, como el asesoramiento que proporcionan los intermediarios respecto a productos de gran complejidad, siguen siendo esenciales y no están siendo sustituidos por las plataformas digitales. Sin embargo, para otros servicios más sencillos, los clientes prefieren tomar decisiones por sí mismos de forma directa, sin que intervenga un tercero en sus decisiones.

Como se ha expuesto, la creciente recolección de datos ha permitido el desarrollo de nuevos productos de seguros, más personalizados basados en riesgos reales, en lugar de en estándares de riesgos[73] como se hacía hasta el momento.

Por otro lado, en los últimos años también ha tenido lugar una reducción del margen de beneficios de las aseguradoras como consecuencia de una regulación del sector cada vez más

[72] La transformación de las compañías de seguros en la era digital. Visión Deloitte, Marzo, 2017. Pág. 2
[73] CAPIELLO, A. Technology and the insurance industry, Pág. 8.

exigente y un aumento de la competencia debido a la entrada de nuevas empresas en el mercado (compañías insurtech, start-ups centradas en el negocio del seguro).

La posición del cliente respecto a las aseguradoras también ha cambiado. Ahora los asegurados tienen mayores posibilidades de conocer su nivel de exposición al riesgo (pues tienen mucha más información a su disposición), aumentando su capacidad e independencia para elegir cómo cubrir sus necesidades de seguro. Esto ubica a los clientes en una posición de cierto poder de dirección que hasta ahora nunca habían tenido, ya que se debían limitar a aceptar las opciones que las aseguradoras ofrecían, sin que pudieran negociar sus condiciones y más teniendo en cuenta que el mercado del seguro se caracteriza tradicionalmente por ser un mercado de información asimétrica, en el que una de las partes tiene más información sobre el objeto de negocio que la otra.

El sector asegurador está sufriendo una intensa reforma tecnológica. Pese a que las aseguradoras siempre han manejado una gran cantidad de datos para medir riesgos y fijar condiciones de pólizas, hoy en día, gracias al *Internet of things (IoT),* aquellas pueden analizar nuevos tipos de datos, con nuevas técnicas, posibilitando clasificar y segmentar a los clientes de mejor manera.

Además, el aumento de datos disponibles y la mejora de sus técnicas de procesamiento, permite no sólo que se analicen los riesgos de forma más precisa, si no que estos se puedan prever, anticipándose a los siniestros y mitigando sus consecuencias negativas.

5.1. La evolución de los seguros de salud. De la medicina curativa a la medicina preventiva.

En el ámbito de los seguros de salud, las coberturas tradicionales de asistencia médica (tratamientos posteriores a la enfermedad) son complementadas con nuevos servicios de prevención de riesgos[74]. En virtud de toda la información de la que se dispone sobre el estado de salud de un asegurado (horas de sueño, ritmo cardiaco, glucosa media, información genética...), las aseguradoras son capaces de anticiparse a futuras enfermedades, advirtiendo a los clientes de los riesgos que sufren y dándoles pautas para mejorar su salud. Ahora ya no sólo se cubren los tratamientos médicos que los asegurados necesiten, sino que se valora cómo debe actuar el asegurado para que mejore su salud anticipándose a los problemas. En este contexto se desarrolla lo que se conoce como Insurance as a Service (IaaS)[75], donde los seguros se configuran como un servicio de protección frente a riesgos cambiantes. A través del análisis

[74] RODRÍGUEZ-PARDO, J.M: "Big data en los seguros sobre personas". *Revista Actuarios,* Nº 40. 2017, Pág. 18 y ss.
[75] https://blogmapfre.com/seguros/insurance-service-el-seguro-como-suscripcion-un-servicio-de-proteccion/

masivo de datos se analizan los riesgos reales de cada momento, permitiendo que las coberturas varíen según los mismos y, de la misma forma, ajustando las primas en cada momento. La posibilidad de contratar cobertura frente a un riesgo cambiante es una cuestión que con merece especial atención.

5.2. La agravación del riesgo y la facultad de las aseguradoras de rescindir el contrato.

Como se ha expuesto anteriormente, gracias a la combinación de una gran cantidad de datos actualizados del asegurado, así como a la mejora en el poder de procesamiento de los mismos, es posible revalorar los riesgos asegurados de cada momento y recalcular las primas por intervalos de tiempo.

Resulta recomendable que este asunto sea fijado en el contrato detalladamente, sobre todo teniendo en cuenta que el artículo 12.2 de la Ley del Contrato de Seguro permite al asegurador rescindir el contrato comunicándolo por escrito al asegurado en el plazo de un mes a partir del día en que tuvo conocimiento de la agravación del riesgo. Sería conveniente fijar en el contrato con exactitud el nivel de agravación del riesgo hasta el que la compañía de seguros se compromete a brindar cobertura. De lo contrario, ante una excesiva agravación del riesgo, la compañía podría tener la posibilidad de extinguir el contrato en virtud de dicho artículo 12 (dejando al asegurado desprotegido de cobertura aseguradora ante un excesivo agravamiento del riesgo).

Esta recomendación de aclarar bien los límites de variación del riesgo que el asegurador se compromete a cubrir se hace puesto que el citado artículo fue redactado en base a la idea de que la agravación del riesgo debe ser comunicada por el asegurado y, sin embargo, en la actualidad las compañías aseguradoras tienen capacidad por sí mismas para conocer la agravación del riesgo (algo que probablemente no estaba en la mente del legislador en el momento de redacción del artículo). Tal vez sea necesaria una reforma del artículo 12 que contemple la capacidad de las aseguradoras de conocer por sí solas las variaciones del riesgo de los asegurados (gracias a las nuevas posibilidades de análisis masivo de datos) y que fije límites a su facultad de rescindir el contrato.

5.3. Nuevos nichos de mercado para el sector asegurador.

El desarrollo tecnológico no solo influye en la organización y el modus operandi de las aseguradoras, sino que también abre un nuevo campo de negocio para las mismas. A medida que la tecnología se implanta en la sociedad, surgen nuevos riesgos que también deben ser

asegurados. Un ejemplo de ello son los seguros contra ciberriesgos. La ciberseguridad cada día es más importante para las empresas y, las aseguradoras, conscientes de ello, han diseñado nuevos productos de seguro que cubren los daños sufridos por ciberataques, robo de datos, la paralización del negocio, como los seguros de ciberriesgo que ofrecen aseguradoras como Allianz[76] o Mapfre[77].

El Ciberriesgo es un problema que también es tratado por EIOPA. Este organismo, en su informe "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies", lo define como cualquier tipo de riesgo procedente del uso de datos electrónicos y su transmisión, así como del daño físico causado por incidentes de ciber seguridad por fraudes cometidos por el mal uso de datos o derivados del almacenamiento de datos, ya sean acerca de personas físicas, empresas o instituciones.

Esta definición puede ser clave para determinar el ámbito de cobertura que ofrecen estos seguros. El citado informe advierte que las compañías aseguradoras encuentran como una gran dificultad la falta de de similitud en el lenguaje de evaluación de riesgos cibernéticos y por ello, EIOPA propone[78] utilizar la taxonomía establecida por la Agencia de la Unión Europea para la Ciberseguridad[79] (ENISA), pero esta es una cuestión que necesita un gran consenso entre los operadores del mercado y que todavía no está plenamente resuelta.

Respecto a las coberturas que se ofrecen en estos seguros, las más comunes son las relativas a los perjuicios derivados de la interrupción del negocio y la restauración de los datos dañados. También es frecuente que se oferte cobertura frente a la ciber extorsión y apoyo legal para hacer frente a estos problemas. No obstante, este es un ámbito en el que los seguros a medida encajan plenamente, pues los riesgos cibernéticos a los que se enfrente una gran corporación pueden variar mucho respecto a los que debe afrontar una pequeña empresa.

Se debe tener en cuenta que estos seguros son productos que se encuentran en plena fase de desarrollo y que los riesgos que cubren están evolucionando permanentemente, por lo que resulta difícil realizar un modelaje del riesgo adecuado, lo que a su vez hace recomendable que las pólizas de ciberseguros sean actualizadas periódicamente, en las que se clarifique detalladamente los riesgos cubiertos en cada caso y en cada momento.

[76] https://www.allianz.es/seguros/especialidades/seguros-ciberataques.html
[77] https://www.mapfre.es/empresas/seguro-ciberriesgos/
[78] "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies", EIOPA. Pág. 6
[79] https://www.enisa.europa.eu/about-enisa/about/es

5.3.1. El problema de los riesgos cibernéticos silenciosos.

Un problema que se plantea para las aseguradoras es el de los riesgos silenciosos[80]. Estos son riesgos que pueden llegar a cubrirse por las pólizas de seguro tradicionales pese a que en el momento de su contratación no están diseñadas para hacerlo. Dado que la mayoría de coberturas que ofrecen las pólizas tradicionales están expuestas, directa o indirectamente, a ciberriesgos, los riesgos cibernéticos silenciosos se plantean como una cuestión que preocupa a las aseguradoras. Por ejemplo, es posible que debido a un fallo informático se origine una explosión en una fábrica y que esta genere un incendio, o que un fallo en el software de un coche provoque un accidente con heridos. Estas y otras muchas son situaciones en las que la exposición cibernética no está ni explícitamente incluida ni explícitamente excluida de la póliza de seguro. Se trate de un seguro contra incendios o un seguro de responsabilidad civil, estos seguros tienen un objeto predefinido, y en ningún momento se contempla la posibilidad de asumir un siniestro derivado de un evento cibernético. Sin embargo, a pesar de ello, parece que de las consecuencias de un incidente cibernético sí deberán responder las aseguradoras, haciendo frente así a pérdidas con las que no contaban y que no se han tenido en cuenta a la hora de fijar las condiciones de las pólizas y de las primas. Por lo expuesto, el nivel de comprensión del riesgo por parte de los aseguradores en la actualidad tiene que ser más preciso que nunca. De lo contrario, se verán obligados a hacer frente a pérdidas con las que no contaban.

No obstante, los ciberriesgos no sólo deben preocupar a las aseguradoras, sino también a los clientes, pues la mayoría de particulares, pequeñas empresas e instituciones no son conscientes de los ciberriesgos a los que están expuestos y, en caso de que las compañías aseguradoras comiencen a excluir expresamente esos riesgos de sus pólizas tradicionales, pueden verse desprovistos de protección[81].

Las empresas consultadas por EIOPA consideran que los agentes reguladores deberían establecer unas pautas para otorgar mayor seguridad y certeza al mercado de los ciberseguros, aunque sin requisitos demasiado exigentes que frenen el desarrollo del mismo.

Entre las medidas regulatorias que las empresas proponen se encuentran[82]: asegurar una tarificación adecuada, así como un seguimiento permanente de los riesgos, establecer cauces rápidos y eficaces para garantizar la notificación de incidentes y el intercambio de información

[80] "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies", EIOPA, pág. 14

[81] En este sentido, la compañía de seguros Zurich ha anunciado que dejará de asegurar los riesgos cibernéticos, convirtiéndolos en riesgos "no asegurables". Más información en: https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d

[82] "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies", EIOPA, pág. 25

entre empresas de diferentes industrias con el único fin de atender amenazas cibernéticas, para ello, proponen un sistema anónimo que permita el intercambio de información. También consideran necesario el desarrollo de prácticas regulatorias que permitan una mejor comprensión de los riesgos, la introducción de estándares mínimos de seguridad informática y de información sobre la misma, mejorar el nivel de conciencia y prudencia de los nuevos actores del mercado (insurtechs), la exigencia de requerimientos de capital adecuados para hacer frente a los riesgos de suscripción, establecer medidas para evitar el contagio en caso de ataques de software maliciosos, establecer medidas para asegurar una mayor claridad sobre la cobertura que se ofrece, entre otras.

5.4. La evolución del papel del corredor de seguros. El corredor de seguros como aliado del cliente.

Tradicionalmente la contratación de seguros ha tenido lugar a través de intermediarios como los corredores de seguros. Estos son los encargados de asesorar de forma independiente al cliente sobre cuál es el producto de seguro más conveniente para él[83]. Los corredores analizan la situación del asegurado, sus riesgos y sus necesidades, ofreciéndole diversas opciones y aconsejándole la más adecuada a su perfil, sobre todo en productos complejos sobre los que el cliente no puede decidir por sí solo.

Con la utilización del Big Data y el desarrollo de productos personalizados, esta tarea de asesoramiento debe evolucionar, asumiendo nuevas competencias.

Gracias a los nuevos canales de distribución y comunicación como son el internet[84] y los dispositivos portátiles, las relaciones entre clientes y aseguradores son cada vez más directas, los clientes disponen de mayor cantidad de información sobre los productos que se ofertan en el mercado, lo que propicia que sean ellos mismos los que decidan contratar un seguro directamente sin necesidad de un intermediario.

Las aseguradoras, a su vez, tienen mayores instrumentos para conocer al cliente, sin que sea imprescindible confiar en el conocimiento y opinión de los intermediarios (incluso, como se ha expuesto, pueden diseñar productos personalizados y ofrecerlos directamente a los potenciales clientes, sin intermediarios) [85]. En este contexto, los corredores de seguros deben

[83] LATORRE CHINER, N.: "La independencia del corredor de seguros", *La reforma del Derecho del seguro*, AAVV, Aranzadi Thomson Reuters, 2015. Pág. 575 y ss.
[84] MAS BADIA, M.D: "La contratación del seguro en internet", *La reforma del Derecho del seguro*, AAVV, Aranzadi Thomson Reuters, 2015. Pág. 179 y ss.
[85] APIELLO, A. Technology and the insurance industry. Pág. 15.

evolucionar y adaptar su misión a las nuevas circunstancias del mercado, pudiendo ocupar una posición fundamental en la relación entre cliente y asegurador.

El Real Decreto-Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, establece en su artículo 155 que los corredores de seguros ofrecen asesoramiento independiente basado en un análisis objetivo y personalizado a quienes demanden la cobertura de riesgos. Así mismo declara que los corredores de seguros deberán informar a quien trate de concertar el seguro sobre las condiciones del contrato que a su juicio conviene suscribir y ofrecer la cobertura que, de acuerdo a su criterio profesional, mejor se adapte a las necesidades de aquel.

Por tanto, es tarea de los corredores de seguros ofrecer un asesoramiento objetivo, profesional e imparcial, es decir, estos deben ser capaces de dar una opinión objetiva, desnuda de todo condicionante favorable a alguna entidad aseguradora[86]. Para ofrecer esa opinión, la ley impone un deber de análisis que hace que los corredores estén obligados a estudiar qué y cómo se debe asegurar el tomador, sin que se puedan limitar a seguir las instrucciones del cliente respecto a estos aspectos, sino que deben comprobar que las condiciones que se ofrecen en el mercado son adecuadas para el futuro asegurado.

Como se ha expuesto, el creciente uso de técnicas de análisis masivo de datos ha hecho que las aseguradoras sean capaces de analizar de forma más individualizada el riesgo de cada cliente, posibilitando la oferta de productos más personalizados. En este contexto, la tarea de los corredores de seguros debería evolucionar. Si los productos que se ofrecen en el mercado ya están diseñados a medida para cada asegurado, el papel del corredor pasa por verificar ese análisis del cliente hecho por la aseguradora, toda vez que la tarea del corredor de seguros no puede limitarse a una mera labor de comercialización de productos (como sí puede ocurrir con los agentes de seguros, cuya función principal es promover la contratación de productos de la o las compañías con las que trabaja).

Sería conveniente que los corredores sean capaces de analizar por sí mismos el riesgo real de cada cliente en virtud de dichas técnicas de análisis masivo de datos o, al menos, supervisar los análisis hechos por las compañías de seguros. Si los corredores, como profesionales independientes, conocen el verdadero nivel de riesgo de cada asegurado, pueden

[86] MUÑOZ PAREDES, J.M: *Los corredores de seguros*. Thomson Civitas, 2008, pág. 101.

informar a los clientes sobre su situación personal y aconsejarles sobre qué producto de los que las aseguradoras venden como personalizados es el más adecuado a sus necesidades, de lo contrario, su poder de asesoramiento se vería mermado, pues ni siquiera ellos serían capaces de distinguir la mejor de las distintas ofertas personalizadas que existan en el mercado.

Además, los corredores podrían servir como garantes de que las ofertas personalizadas que proponen las compañías a los clientes son las verdaderamente adecuadas para ellos, librando a los asegurados de ofertas que pese a ser venderse como personalizadas, realmente no lo son, protegiéndolos así de engaños y abusos por parte de las aseguradoras.

Por tanto, el corredor de seguros se convierte en un aliado del asegurado para conocer su nivel de riesgo real y garantizar que los productos que se le ofrecen sean los verdaderamente adecuados. La actividad de corretaje de seguros, lejos de convertirse en una actividad de intermediación prescindible, puede posicionarse como un aliado fundamental del asegurado para que este tenga un conocimiento real de su riesgo y de su posición en el mercado. Para ello, resultaría necesario que en un futuro los corredores de seguros tengan conocimientos en ciencia de datos, que sean capaces de entender los criterios y métodos en base a los que las aseguradoras clasifican a los clientes y sean capaces de explicar a sus clientes las decisiones de las empresas aseguradoras.

5.5. La economía colaborativa en el sector asegurador.

La economía colaborativa se está desarrollando en multitud de actividades económicas, entre ellas, el sector asegurador. Los **seguros Peer-to-peer**[87] o seguros entre iguales son un ejemplo de ello y están muy cerca del espíritu mutualista del que nacieron las entidades aseguradoras[88]. En virtud de este modelo de seguros, personas con las mismas necesidades y mismo nivel de riesgo se agrupan, formando una plataforma de economía colaborativa en la que realizan aportaciones individuales. En la mayoría de estas plataformas, las citadas aportaciones se dividen en dos partes, una destinada a pagar la cobertura de un seguro tradicional con el que la plataforma colabora y la otra parte se destina a la constitución de un fondo común. Con el dinero común, la plataforma se compromete a cubrir las reclamaciones

[87] Un ejemplo de plataforma de seguros peer to peer es FriendInsurance. Disponible en: https://www.friendsurance.com/
Otro ejemplo es la compañía Lemonade, que se configura a sí misma como una verdadera aseguradora digital. Disponible en: https://www.lemonade.com/fr/en/?f=1
[88] CAPIELLO, A. Technology and the insurance industry. Pág. 40 y ss.

que cualquiera de los integrantes del grupo realice (hasta un máximo acordado previamente). Así, si el fondo común resulta suficiente para cubrir las reclamaciones, no será necesario utilizar la cobertura ofrecida por la aseguradora tradicional, con la consiguiente reducción de la prima en el ejercicio siguiente. Además, si el fondo común no se agota, la aportación que se haga al mismo el año siguiente podrá ser menor, consiguiendo de esta manera también un ahorro de dinero a cada integrante del grupo. Además, ésta fórmula reduce el riesgo de fraude, pues el hecho de que sean los propios asegurados los que sufraguen las coberturas mediante la constitución de un fondo común, implica que ellos mismos sean los primeros interesados en que se produzca el menor número de siniestros posibles.

Se debe tener presente que estas plataformas no funcionan siempre como verdaderas entidades aseguradoras[89], sino que en ocasiones funcionan como plataformas de distribución de seguros, lo que origina dos problemas que reseña María Luisa Muñoz Paredes[90]. En primer lugar, estas plataformas escapan de la regulación de control administrativo a la que están sujetas las compañías aseguradoras tradicionales y, en segundo lugar, y como consecuencia del anterior problema, según las entidades de seguro tradicionales, la actividad de estas plataformas de economía colaborativa podría constituir una práctica de competencia desleal, pues para el desarrollo de su actividad se exigen requisitos menos estrictos. Se trata de una acusación similar a la que formuló en su momento el sector del taxi frente a los VTC.

No obstante, parece lógico pensar que, si sus actividades son distintas, su regulación no sea la misma. Así como que, si su actividad no es la misma, no debería entenderse como competencia desleal. La solución pasaría por imponer unos requisitos regulatorios similares a los que prevé la Ley 20/2015 de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras para aquellas plataformas que sí pretendan prestar servicios de seguro directamente y no para las plataformas que únicamente se dediquen a la intermediación de seguros.

6. BIG DATA, SEGUROS Y PROTECCIÓN DE DATOS.

Como se ha comentado, la utilización de técnicas de Big Data en todas las fases de la cadena de valor del negocio asegurador exige recolectar y tratar importantes cantidades de datos. En

[89] Sobre la calificación jurídica de los servicios prestados por las entidades de economía colaborativa: CAMPUZANO TOMÉ, H: "La entrada en escena de las plataformas colaborativas: ¿Prestadoras de servicios profesionales o empresas tecnológicas?", *Derecho y nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020, pág. 481 y ss.

[90] MUÑOZ PAREDES, M.L.: "La regulación de las plataformas de seguros P2P". *Almacén de Derecho*. https://almacendederecho.org/la-regulacion-las-plataformas-seguros-p2p

este contexto, cualquier tratamiento de datos debe hacerse con absoluto respeto a los derechos y garantías que establece nuestro ordenamiento (sean en defensa de la competencia en el mercado, en defensa de los consumidores, del orden y seguridad pública o de cualquier otra índole). Sin embargo, en caso de que los datos objeto de tratamiento sean de carácter personal se debe ser consciente de que las exigencias normativas se incrementan, pues se habrán de respetar tanto el 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 (RGPD), como nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD).

Tales normas resultan de aplicación cuando se traten datos de carácter personal, que son, como indica el artículo 4 del Reglamento, toda información sobre una persona física identificada o identificable. En este sentido, se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador. Esta definición puede resultar engañosa, pues como veremos, existen datos que aún sin referirse directamente a una persona, posibilitan su identificación, por lo que habrán de ser considerados dentro del ámbito de aplicación de tales normas.

Las citadas normativas establecen una amplia gama de principios y derechos que protegen tanto a las personas como a sus datos en un entorno digital. La Ley Orgánica 3/2018 pretende adaptar la anterior normativa española (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) al Reglamento Europeo (artículo 1.a de la citada Ley), por lo que se remite a él en muchos preceptos. Además, el legislador nacional ha querido ampliar la protección de las personas en el ámbito digital reconociendo lo que denomina "derechos digitales" (artículo 1.b)[91].

Con el presente trabajo no se pretende hacer una exposición amplia y detallada de los principios y derechos reconocidos en las citadas normas, sino que se pretende poner de manifiesto los riesgos inherentes al uso del Big data en el sector seguros cuando se utilizan datos personales.

Las citadas normas obligan a que los datos sean exactos y actualizados, a que se mantenga su confidencialidad y que su tratamiento sea legítimo, ya sea por mediar consentimiento del

[91] Una exposición sobre algunos de estos derechos digitales en: PALACIOS GONZÁLEZ, D: "Algunos derechos digitales en la Ley Orgánica de Protección de datos", *Derecho y nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020, Pág. 129 y ss.

afectado (norma general) o bien porque existan otros motivos que legitimen su tratamiento (tales como obligaciones legales, interés público o ejercicio de potestades públicas). Así mismo, el afectado por el tratamiento de datos tendrá derecho a acceder a sus datos y a exigir información transparente sobre el uso que se hace de ellos, la identidad de quien los trata, así como la finalidad del tratamiento. Tendrá derecho a rectificarlos, suprimirlos, portarlos a otro responsable de tratamiento u oponerse al mismo, entre otros.

En el mismo sentido, el artículo 79 de nuestra LOPD reconoce que, los derechos y libertades consagrados en la constitución y en los tratados y convenios internacionales en los que España es parte, son plenamente aplicables en internet. Bajo este presupuesto, reconoce un conjunto de derechos entre los que se encuentran el derecho a la neutralidad en internet, el derecho al acceso universal en Internet, a la seguridad digital, a la educación digital, a la rectificación en internet, entre otros, y que también deben ser tenidos en cuenta en cualquier interacción en red que se haga con el asegurado.

6.1. Elaboración de perfiles y decisiones automatizadas.

Las técnicas de análisis masivo de datos utilizadas en el sector seguros no siempre tienen una fácil imbricación en las citadas normas. Algunos de los supuestos más conflictivos se dan, por ejemplo, cuando las empresas utilizan datos personales (tales como datos de salud, situación económica, preferencias y gustos personales...) para evaluar aspectos personales de un cliente con los que elaborar perfiles basados en deducciones estadísticas (para ofrecer, por ejemplo, unas coberturas de seguro u otras) o cuando se toman decisiones basadas en datos estadísticos sin que intervenga un ser humano (otorgando o denegando una cobertura únicamente en base a criterios matemáticos y de forma automatizada). De estas dos cuestiones se ocupó el Grupo de trabajo sobre protección de datos del artículo 29[92], elaborando unas directrices[93] que se han de tener en cuenta a la hora de implementar dichas prácticas.

El Reglamento europeo de protección de datos aborda específicamente estas cuestiones en su artículo 22, reconociendo que todo interesado tendrá derecho a no ser objeto de una decisión individualizada basada únicamente en el tratamiento automatizado (aunque con excepciones).

[92] El grupo de trabajo sobre protección de datos del artículo 29 es el grupo de trabajo europeo independiente, creado por la Comisión Europea, con funciones consultivas, que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018. Para más información: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es

[93] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento 2016/679. Grupo de trabajo sobre protección de datos del artículo 29. Disponible en https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

En las referidas directrices, se reconoce, como ya se ha expuesto en el presente trabajo, que la elaboración de perfiles puede llevar a predicciones inexactas, a la denegación de servicios y bienes y a una discriminación injustificada. Señala el referido documento que en los procedimientos de elaboración de perfiles se distinguen tres fases: recogida de datos, análisis y aplicación de las correlaciones obtenidas. Dichas prácticas no se encuentran prohibidas, pero es necesario que en todas las fases se respeten las previsiones normativas y que exista una base jurídica que legitime el tratamiento[94].

Los procesos de elaboración de perfiles suelen ser invisibles para los interesados, es decir, suelen realizarse sin que los afectados sean conscientes de que se está analizando su perfil. Este hecho contradice las exigencias del reglamento europeo de que los datos sean tratados de manera lícita, leal y transparente. El requisito de la licitud exige, como hemos indicado, que exista una base jurídica que legitime el tratamiento (el consentimiento, la existencia de necesidad para la ejecución de un contrato, la necesidad de cumplir una obligación legal o la existencia de razones de utilidad pública o interés social). El consentimiento como base jurídica del tratamiento plantea problemas cuando la elaboración de perfiles se basa en datos inferidos de otros datos y no en información facilitada directamente por el interesado. El Grupo de Trabajo[95] señala que los responsables del tratamiento deberán demostrar que los interesados entienden exactamente qué están consintiendo y que estos cuentan con suficiente información sobre el uso y las consecuencias del tratamiento para garantizar que el consentimiento constituya una elección informada, de lo contrario, podría darse un vicio en el mismo que lo anularía.

El requisito de la lealtad exige que a partir de los resultados de la elaboración de perfiles no se realicen prácticas contrarias a los intereses de los afectados. Por ejemplo, que no se ofrezcan productos demasiado arriesgados o costosos[96]. Se trata de una cuestión complicada, pues la lealtad no deja de ser un concepto jurídico indeterminado, por lo que parece probable que sean los tribunales los que deban determinar qué es y qué no es contrario a los intereses del afectado.

[94] El propio Reglamento Europeo contempla como bases jurídicas que legitiman el tratamiento automatizado: la necesidad de celebrar o ejecutar un contrato, la autorización del Derecho de la Unión Europea o de los Estados miembros o el consentimiento explícito del interesado.
a los efectos del Reglamento 2016/679. Pág 9
[95] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento 2016/679. Grupo de trabajo sobre protección de datos del artículo 29. Pág. 14
[96] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento 2016/679. Grupo de trabajo sobre protección de datos del artículo 29. Pág 11.

Por su parte, el requisito de la transparencia exige que exista la posibilidad para el interesado de obtener información concisa, transparente, inteligible y de fácil acceso sobre el tratamiento de sus datos personales, lo que obliga a las aseguradoras a tener preparados mecanismos para ofrecer dicha información a sus clientes o potenciales clientes.

Las Directrices señalan otro riesgo. Es posible que la elaboración de perfiles suponga la utilización de datos personales para otra finalidad distinta a la que justificó su recolección. Si bien esto no es una práctica completamente prohibida, sólo será lícita cuando se cumplan los requisitos establecidos en el artículo 6.4 del Reglamento Europeo y que, en resumen, exigen que el nuevo uso sea compatible con el fin para el que se recogieron, para lo que se tendrá en cuenta la relación entre los fines para los que se recogieron los datos y la nueva utilidad que se les pretende dar, el contexto en el que se recogieron los datos, que no se trate de categorías especiales de datos (salud, creencias religiosas, políticas, identidad sexual...), las consecuencias del nuevo uso de los datos y la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Así mismo, el Grupo de Trabajo señala que se debe tener presente la limitación del plazo de conservación impuesta por el artículo 5.1 e) del Reglamento, que exige que los datos no sean conservados más tiempo del necesario. Tal exigencia puede constituir un problema importante, pues la conservación de datos puede ser crucial para que los algoritmos de aprendizaje automático "aprendan" y mejoren sus resultados diariamente. Si pasado cierto tiempo resulta necesario eliminar determinados datos, es posible que el algoritmo de m*achine learning* pierda calidad en sus predicciones. No obstante, una posible solución pasa por la anonimización de tales datos.

De otro lado, la excepción del artículo 22.2 del Reglamento Europeo que posibilita la toma de decisiones basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado en caso de que sea necesaria para la celebración o ejecución de un contrato, puede constituir un motivo aducido por las compañías de seguros para escapar de las exigencias expuestas anteriormente. Por ello, el Grupo de Trabajo del artículo 29 se encarga de señalar[97] que compete a los responsables del tratamiento, esto es, a las entidades aseguradoras, el deber de demostrar que este tipo de tratamiento es necesario, sin que se pueda adoptar un método menos invasivo para la intimidad de los interesados, de lo

[97]Directrices sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento 2016/679. Grupo de trabajo sobre protección de datos del artículo 29. Pág 26.

contrario sí incurrirían en una vulneración de la normativa de protección de datos, que conlleva importantes sanciones económicas para los infractores.

6.2. Protección de datos en el contexto de los vehículos conectados.

El Comité Europeo de Protección de Datos[98] también ha elaborado unas directrices para la protección de datos personales en el contexto de los vehículos conectados. Si bien sus recomendaciones son similares a las efectuadas por el Grupo de Trabajo del artículo 29, señala riesgos específicos que merecen ser mencionados. En primer lugar, el Comité reconoce que los vehículos cada vez generan más datos que pueden considerarse datos personales[99]. Aunque se trate de datos relativos a aspectos técnicos y características del vehículo, se trata de datos que afectan al conductor o pasajeros del vehículo. Por ejemplo, los datos sobre el estilo de conducción, la distancia recorrida, el desgaste de las piezas del vehículo, los datos de localización etc., revelan información sobre los hábitos y costumbres de las personas. Pese a que se trata de datos relativos a circunstancias del vehículo, pueden estar tan individualizados que podrían permitir la identificación de sujetos. Por ejemplo, en función de la periodicidad con que una persona acuda a un lugar de culto, a un centro sanitario o a un local de ocio nocturno, podríamos conocer sus creencias religiosas, su estado de salud o incluso su identidad sexual[100]. Así, la monitorización de hábitos y comportamientos puede llegar a destruir la anonimidad de los datos (piénsese en la posibilidad de conocer el domicilio de una persona según el lugar donde aparque siempre el coche).

6.2.1. La calidad del consentimiento.

En ese sentido, el Comité señala la importancia de contar con un consentimiento del afectado de calidad[101]. Resalta que es posible que los conductores y pasajeros no estén siempre adecuadamente informados sobre el tratamiento de datos. Así, es necesario que se cumplan todos los elementos del consentimiento válido (libre, específico, informado y que constituya

[98] El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. Más información en: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_es#:~:text=El%20Comit%C3%A9%20Europeo%20de%20Protecci%C3%B3n,de%20datos%20de%20la%20UE

[99] Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad. CEPD. Pág. 4

[100] Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad. CEPD. Pág. 16

[101] Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad. CEPD. Pág. 13

una manifestación inequívoca del interesado), por ello, señala que debe prestarse por separado, para fines específicos, que no se podrá agrupar con el del contrato de compraventa o alquiler del vehículo y que deberá poder retirarse con la misma facilidad con la que se otorgó. De otra manera, el usuario podría no ser consciente del tratamiento de sus datos, impidiendo que exista un consentimiento informado, como exige la normativa. De la misma manera, se plantea un problema para obtener un consentimiento válido en el caso de usuarios de vehículos de segunda mano (que podrían estar afectados por el tratamiento que consintió el anterior propietario) o de vehículos de alquiler. El Comité menciona a los seguros basados en el uso[102] como unos tipos de seguros en los que resulta imprescindible el consentimiento válido del interesado, cumpliendo con todos los requisitos que hemos expuesto y afirmando además que es necesario que el tomador del seguro tenga la posibilidad de suscribir una póliza de seguro que no esté basada en el uso, de lo contrario, tal consentimiento nunca sería válido.

Otro aspecto que señala el Comité es el riesgo de la excesiva recogida de datos. Cada vez se implantan un mayor número de sensores en los vehículos, por lo que existe un riesgo muy alto de que los datos recogidos sean más de los necesarios para alcanzar los objetivos del tratamiento, lo que contradice el principio de minimización de los datos previsto tanto en el Reglamento Europeo como en nuestra Ley Orgánica y que además incrementa el riesgo de ataque cibernético, toda vez que el número de posibles canales por los que se podrían comprometer los datos personales aumenta, así como la propia seguridad de los ocupantes del vehículo.

Por lo expuesto, el Comité recomienda que, en caso de que se prevea la transmisión de datos personales fuera del vehículo, se valore, con carácter previo a su transmisión, la posibilidad de anonimizarlos[103]. Si los datos están adecuadamente anonimizados[104], de manera que no resulte posible identificar directa o indirectamente a las personas, las previsiones normativas de protección de datos personales ya no serán de aplicación, lo que también permitirá a las empresas seguir disfrutando de los beneficios de los vehículos conectados sin enfrentarse a posibles infracciones normativas, con sus consecuentes sanciones.

---

[102] Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad. CEPD. Pág. 27

[103] Para conocer más sobre técnicas de anonimización y su compatibilidad con la normativa de protección de datos personales, consultar el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo sobre protección de datos del artículo 29. Disponible en: https://www.aepd.es/es/documento/wp216-es.pdf

[104] Sobre anonimato y protección de datos personales leer: VILLAVERDE MENÉNDEZ, Á. I: "Libertad de expresión, anonimato y ciberespacio". *Derecho y nuevas tecnologías.* AAVV. Civitas Thomsom Reuters. 2020, Pág. 321 y ss.

6.3. Protección de datos y Cloud Computing.

Todos los procesos de digitalización en las distintas fases de la cadena de valor del negocio del seguro se llevan a cabo, en muchas ocasiones, con el apoyo de *cloud computing* o computación en la nube ya que, las aseguradoras, para el manejo de grandes cantidades de datos necesitan una infraestructura técnica e informática con la que generalmente no cuentan. Como ya expusimos, el *cloud computing* consiste en la utilización de recursos de procesamiento y almacenamiento de datos en remoto (en muchas ocasiones fuera del territorio nacional), es decir, en la utilización de servidores en red que no pertenecen a la entidad aseguradora, lo que implica que existan terceros que dispongan de datos de los asegurados. En estos procesos, se habrán de tener en cuenta las previsiones de la LOPD y RGPD y por ello, la Agencia Española de Protección de Datos ha elaborado unas guías[105] que pretenden orientar tanto a clientes como a prestadores de servicios en el uso de esta tecnología. Por lo expuesto, el presupuesto del que debemos partir es que la computación en la nube permite utilizar recursos de almacenamiento y procesamiento que se encuentran deslocalizados[106]. Este hecho implica, en el caso de las entidades de seguro, que la información acerca de los asegurados no se encuentre bajo la custodia de la propia compañía aseguradora, sino en los de una tercera persona (generalmente una empresa prestadora de servicios de cloud computing[107]), es decir, es posible que la propia entidad de seguros desconozca la localización precisa de su datos, sin tener el control directo sobre los mismos[108] (y por tanto, sin la posibilidad directa de acceso, borrado, portabilidad...). No obstante, esta externalización[109] no implica que la entidad de seguros esté exenta de responsabilidad desde el punto de vista de la protección de datos.

Así, en los modelos de cloud computing debemos distinguir entre varios actores. De un lado se encuentran los clientes, que son aquellas empresas y entidades que contratan el derecho a utilizar recursos de computación y tratamiento de datos ajenos (en nuestro caso, la entidad aseguradora), que pertenecen a otra entidad distinta y a la que llamaremos prestador de servicios. También existen otros agentes que participan en los procesos de cloud computing,

---

[105] Guía para clientes que contraten servicios de Cloud Computing. Agencia Española de Protección de datos., Consultar en: https://www.aepd.es/es/documento/guia-cloud-clientes.pdf
Orientaciones para prestadores de servicios de cloud computing. AEPD, Disponible en: https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf

[106] Big Data Analytics in motor and health insurance: a thematic review. EIOPA, Pág. 17

[107] Una de las principales empresas que se dedica a la prestación de servicios de computación en línea es Amazon Web Services (AWS), filial del gigante Amazon. Más información en: https://aws.amazon.com/es/

[108] Guía para clientes que contraten servicios de Cloud Computing. AEPD. Pág. 6

[109] Sobre la externalización de servicios en la nube consultar: VERCHER MOLL, J: "La externalización de las entidades de seguros y reaseguros a proveedores de servicios en la nube", *Transparencia y competitividad en el mercado asegurador, AAVV, Editorial Comares, 2021.* Pág. 327 y ss.

los socios o partners de los proveedores y que se encargan de proporcionar servicios adicionales en la nube (por ejemplo, ofreciendo un software que permite sacar más rendimiento a los recursos que ofrece el prestador).

Además, es posible que el proveedor de servicios de cloud computing no disponga de toda la infraestructura necesaria para prestar tales servicios, sino que subcontrate a terceros en función de la carga de trabajo que tenga[110](un socio). Así mismo, es posible que el subcontratista subcontrate a un nuevo socio parte de sus servicios, y así, formar una cadena de subcontrataciones que, al menos en teoría, no tendría por qué tener fin.

Por lo expuesto, la AEPD recuerda que, a la hora de elegir a un proveedor de servicios de cloud computing para su contratación, es necesario tener en cuenta la localización de los proveedores. La Agencia recomienda que se elija a países que se encuentren dentro del Espacio Económico Europeo o en territorios que protejan los datos personales de manera similar (de lo contrario, se trataría de una transferencia internacional de datos, sometida a las disposiciones del Título VI de nuestra LOPD). Además, no sólo se debería tener en cuenta el domicilio de las entidades, sino también el lugar donde físicamente se encuentran los servicios de computación y almacenamiento (tanto los propios como los subcontratados). De lo contrario, es posible que los derechos de los ciudadanos no puedan ejercitarse efectivamente.

De la misma manera, la Agencia advierte de que es necesario que el servicio de cloud sea transparente. Para ello, debe ser posible exigir información precisa de dónde, cuándo y quién ha procesado y almacenado los datos[111](tanto si lo ha hecho directamente el propio proveedor o si se ha subcontratado a un tercero), así como sobre en qué condiciones de seguridad se ha exigido.

Por lo expuesto, en la citada Guía se establecen unas garantías contractuales que es recomendable establecer en la contratación de servicios de cloud computing. En primer lugar, es imprescindible que el contrato entre el cliente (a los efectos de este trabajo, entidad aseguradora) y el prestador de servicios de cloud computing incorpore las garantías establecidas en el artículo 28 del Reglamento Europeo. En particular, sobre la entidad aseguradora, como cliente de servicios de cloud computing, recae una obligación legal de diligencia que se materializa en elegir "únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados", lo que se traduce, según la AEPD, en un abanico

[110] Guía para clientes que contraten servicios de Cloud Computing. AEPD. Pág. 9
[111] Guía para clientes que contraten servicios de Cloud Computing. AEPD. Pág. 10

de requerimientos de información al proveedor de los servicios de cloud computing y que tienen por finalidad conocer las garantías que este ofrece para proteger los datos personales tratados.

Además, la Agencia reconoce la existencia de dos grandes riesgos para la protección de datos que existen en el uso de servicios de cloud computing[112]. La falta de transparencia y la falta de control sobre las condiciones en que tiene lugar el servicio de cloud computing, ambos riesgos están conectados. Si el cliente (aseguradora) no tiene la oportunidad de conocer quién, cómo y dónde se lleva a cabo el tratamiento de datos (si no sabe, por ejemplo, si los datos están en poder del prestador de servicios o de un tercero subcontratado), difícilmente podrá evaluar los riesgos y exigir garantías específicas para controlar la seguridad de los datos. Por ello, es verdaderamente importante que el cliente cumpla con su deber de diligencia y elija un prestador de servicios de cloud computing que ofrezca garantías en materia de protección de datos, y más teniendo en cuenta que, aún externalizando el servicio de cloud computing, el cliente seguirá siendo responsable del tratamiento a los efectos del RGPD y la LOPD.

7. CONCLUSIONES

Por lo expuesto, resulta patente que no podemos permanecer inmóviles respecto al fenómeno de la digitalización del sector asegurador. Es necesario actuar proactivamente tomando medidas para garantizar que el desarrollo de la digitalización del sector seguros tenga lugar de forma segura y confiable. Este proceso, que es necesario para garantizar la competitividad del sector y que aporta múltiples beneficios, debe desarrollarse con pleno respeto a los derechos tanto de las entidades de seguro como de los clientes.

La implementación de las nuevas tecnologías (la inteligencia artificial y todas las tecnologías asociadas a ella) en cualquier sector de la economía, y más en sectores fuertemente regulados como el asegurador, debe hacerse con pleno control sobre sus consecuencias. Las sociedades tenemos derecho a controlar a la inteligencia artificial, y tenemos el deber de que la misma no se convierta en un instrumento ingobernable. Sin embargo, debemos ser conscientes de que ello exige un esfuerzo de adaptación y permanente aprendizaje por parte de sus usuarios.

El uso de técnicas de big data ha revolucionado el sector seguros. La gran cantidad de datos disponibles gracias al Internet de las cosas y la diversidad de los mismos, así como las nuevas herramientas que permiten su tratamiento, hace que los mecanismos tradicionales de análisis del riesgo se queden, en parte, obsoletos. Las entidades de seguro cada vez tienen mayor control del riesgo y mayor cantidad de información sobre el potencial cliente, lo que les permite

[112] Guía para clientes que contraten servicios de Cloud Computing. AEPD. Pág. 12.

desarrollar productos más personalizados, ofrecer una respuesta más rápida y acertada frente a un siniestro, evaluar las reclamaciones con mayor precisión e incluso anticiparse a los riesgos, minorarlos y prevenirlos. Sin embargo, se debe ser consciente de que la implementación del big data también acarrea peligros, principalmente para los asegurados. Los algoritmos y los datos utilizados por las compañías aseguradoras pueden perpetuar sesgos, generar discriminación o resultar inatacables (opacos) para los asegurados.

Así, resulta necesario adoptar respuestas normativas que garanticen el control del uso de las técnicas de big data por las entidades de seguro. La transparencia de los algoritmos de análisis de riesgo, la calidad de los datos con los que actúan, las fuentes de las que provienen y los fines para los que se usan son cuestiones que han de ser abordadas específicamente por los reguladores. La protección de datos personales también puede verse afectada por la digitalización del seguro, por lo que también se deben implementar medidas que garanticen el cumplimiento de la normativa tanto nacional como europea.

En definitiva, todas las fases de la cadena de valor del negocio asegurador se ven afectadas por el uso de nuevas tecnologías. La digitalización de la economía es un fenómeno imparable, para el que se debe estar preparado, asegurando que su desarrollo sea ordenado y controlado, pues, aunque el uso de la tecnología es deseable, el respeto a los derechos de las personas es preferible y nuestra misión pasa por garantizar que ambos sean compatibles.

BIBLIOGRAFÍA.

ALCAÑIZ ZANÓN, M., AYUSO GUTIERREZ, M., PÉREZ MARÍN, A.M: *El seguro basado en el uso*. Fundación Mapfre. Área de seguro y previsión social. 2014

BATALLER GRAU, J., QUINTANS EIRAS M.R., VEIGA COPO, A.: *La reforma del derecho del seguro*, Thomsom Reuters Aranzadi. 2015

BERNAD RÍOS, J. *Manual básico de seguros*, 2º ciclo, Volumen IV. Centro de estudios del Consejo General de los Colegios de Mediadores de Seguros Titulados. 1997.

Big Data and Regulation in the Insurance Industry. Lawrence S. Powell, PhD Executive Director Alabama Center for Insurance Information and Research University of Alabama. SSRN.

BOOBIER, T: *Analytics for Insurance*. Wiley. 2016.

CAMPIONE, R: "Humaquinismo. Una panorámica sobre el ser humano, la robótica y la inteligencia artificial", *Derecho y nuevas tecnologías,* AAVV. Civitas Thomsom Reuters. 2020.

CAMPUZANO TOMÉ, H: "La entrada en escena de las plataformas colaborativas: ¿Prestadoras de servicios profesionales o empresas tecnológicas?", *Derecho y nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020.

CAPIELLO, A. Technology and the insurance industry. Palgrave Pivot. 2018.

GUILLEN, M. Big Data en seguros. Revista índice. Abril 2016 *Ibero-Latinoamericana de Seguros*, 137-160 (2020). Disponible en: https://doi.org/10.11144/Javeriana.ris53.ntaa

IV CONGRESO DE LAS NUEVAS TECNOLOGÍASCongreso de nuevas tecnologías. La influencia de internet, genética y nanotecnología en la medicina y en el seguro. Universidad Externado de Colombia. AAVV. 2015.

La transformación de las compañías de seguros en la era digital. Visión Deloitte, Marzo, 2017.

LATORRE CHINER, N.: "La independencia del corredor de seguros", *La reforma del Derecho del seguro*, AAVV, Aranzadi Thomson Reuters, 2015.

MAS BADIA, M.D: "La contratación del seguro en internet", *La reforma del Derecho del seguro*, AAVV, Aranzadi Thomson Reuters, 2015.

MCGURK, B: *Data profiling and insurance law*. Hart publishing. 2020.

MUÑOZ PAREDES, J.M: *Los corredores de seguros*. Thomson Civitas, 2008.

MUÑOZ PAREDES, M.L. "''Big data'' y contrato de seguro: los datos generados por los asegurados y su utilización por los aseguradores". *La regulación de los algoritmos.* AAVV.

Thomsom Reuters Aranzadi. 2020.

MUÑOZ PAREDES, M.L., "Seguros usage-based: luces y sombras". AAVV, *Seguro de personas e inteligencia artificial*. 1ª ed., abril 2022.

MUÑOZ PAREDES, M.L.: "La regulación de las plataformas de seguros P2P". *Almacén de Derecho*. Disponible en: https://almacendederecho.org/la-regulacion-las-plataformas-seguros-p2p.

MUÑOZ PAREDES, M.L.: "Sobre la individualización del riesgo: Elaboración de perfiles y desprotección del asegurado". *Derecho y Nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020.

MUÑOZ PAREDES, M.L.; ¿Son ventajosos los seguros con monitorización del asegurado o de sus bienes? Almacén de Derecho. 1 de junio de 2021. Disponible en: https://almacendederecho.org/son-ventajosos-los-seguros-con-monitorizacion-del-asegurado-o-de-sus-bienes

MUÑOZ PAREDES, M.L: "Big data y discriminación de los asegurados". *II Congresso Internacional de Direito do Seguro*. AAVV.

O´NEIL, C: *Armas de destrucción matemática*. Crown Books, 2016.

ORTIZ DE ZÁRATE ALCARAZO, L. "Explicabilidad de la inteligencia artificial".

Eunomía. *Revista en Cultura de la Legalidad*, 2022. 328-344.

PADILLA-BARRETO, A.E., GUILLÉN M., BOLANCÉ, C,: "Big Data Analytics en seguros", *Revista del Instituto de Actuarios Españoles*, 4ª época, 23, 2017/1-19.

PALACIOS GONZÁLEZ, D: "Algunos derechos digitales en la Ley Orgánica de Protección de datos", *Derecho y nuevas tecnologías*. AAVV. Civitas Thomsom Reuters. 2020.

Pérez-Llorca. Seguros on-demand en España. Nota Jurídica. Septiembre 2020. Disponible en: https://www.perezllorca.com/wp-content/uploads/2020/09/nota-juridica-seguros-on-demand-en-espana.pdf

RODRÍGUEZ-PARDO, J.M: "Aspectos éticos del tratamiento de los datos personales". *Revista Actuarios*, Nº 40. 2017.

RODRÍGUEZ-PARDO, J.M: "Big data en los seguros sobre personas". *Revista Actuarios*, Nº 40. 2017.

The Geneva Association. From Risk Transfer to Risk Prevention. *How the Internet of Things is reshaping business models in insurance.*

TUR FAÚNDEZ, C.E: *Smart contracts: Análisis jurídico (Derecho de las nuevas tecnologías.* Editorial Reus, 2018.

VEIGA COPO, A.B: *Seguro y tecnología. El impacto de la digitalización en el contrato de seguro*. Civitas Thomsom Reuters. 2020.

VERCHER MOLL, J: "La externalización de las entidades de seguros y reaseguros a proveedores de servicios en la nube", *Transparencia y competitividad en el mercado asegurador, AAVV, Editorial Comares, 2021*. Pág. 327 y ss.

VILLAVERDE MENÉNDEZ, Á. I: "Libertad de expresión, anonimato y ciberespacio". *Derecho y nuevas tecnologías.* AAVV. Civitas Thomsom Reuters. 2020

YUDE LI. "The Application of Big Data in the Insurance Industrywith Potential Risks and Possible Solutions". *Advances in Economics, Business and Management Research*, volumen 656.

ZAPIOLA GUERRICO, M. "Las nuevas tecnologías en la actividad aseguradora", *53 Revista*

Normativa:

Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador

Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras

Ley 24/2015, de 24 de julio, de Patentes.

Ley 3/1991, de 10 de enero, de Competencia Desleal.

Ley 50/1980, de 8 de octubre, de Contrato de Seguro.

Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, respecto a nuestra legislación nacional.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

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, a nivel europeo.

Informes de instituciones:

Artificial Intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector", EIOPA, 2021

Artificial intelligence: How does it work, why does it matter, and what can we do about it? Servicio de Estudios del Parlamento Europeo 2020. Pág. 1 y ss. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf

Artificial intelligence: How does it work, why does it matter, and what can we do about it?. European Parlamentary Research Service. Philip Boucher

Big Data Analytics in Motor and Health Insurance. A thematic review. EIOPA.

Big Data and Insurance: Implications for Innovation, Competition and Privacy. Benno Keller, Special Advisor on Digital and Innovation, The Geneva Association.

Cloud computing. An overview of economic and policy issues. Servicio de Estudios del Parlamento Europeo 2016. Disponible en: https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf

Código de buenas prácticas en protección de datos para proyectos Big Data. AEPD. 2018

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019. Disponible en: https://data.europa.eu/doi/10.2759/14078

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las regiones. Una Estrategia Europea de Datos. Bruselas, 19.2.2020. Disponible en: en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=ES

Consumer Trends Report 2021. EIOPA.

Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo sobre protección de datos del artículo 29. Disponible en: https://www.aepd.es/es/documento/wp216-es.pdf

Dictamen 05/2014 sobre técnicas de anonimización. Grupo de Trabajo sobre protección de datos del artículo 29. 2014

Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad. CEPD.

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Grupo de trabajo sobre protección de datos del artículo 29. Disponible en https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

EIOPA letter to co-legislators on the Artificial Intelligence Act. EIOPA. 4 de julio de 2022.

EIOPA'S report on data quality in solvency II reporting. EIOPA. 2022

From Risk Transfer to Risk Prevention. How the internet of things is reshaping business models in insurance - The Geneva Association. Mayo 2021.

Guía para clientes que contraten servicios de cloud computing. AEPD. 2018

Guía para clientes que contraten servicios de Cloud Computing. Agencia Española de Protección de datos. Consultar en: https://www.aepd.es/es/documento/guia-cloud-clientes.pdf

Implicaciones jurídicas en el desarrollo y uso de sistemas de inteligencia artificial en el sector asegurador. Cuadernos de la Fundación Mapfre 232.

Las aplicaciones del Big Data en el ámbito asegurador y el tratamiento legal de sus datos. Cuadernos de la Fundación Mapfre. Alonso Ortega Giménez 229.

Obstáculos al desarrollo de la innovación y digitalización en el sector asegurador. UNESPA.

Orientaciones para prestadores de servicios de cloud computing. AEPD, Disponible en: https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf

Orientaciones para prestadores de servicios de cloud computing. AEPD. 2018

Technology and innovation in the insurance sector. OECD. 2017

The Geneva Association. Big Data, Big Impact. Asia Insurance Review, Julio 2016.

The use of price optimization in insurance ratemaking. Janet Kaminski Leduc, Senior Legislative Attorney. *Oficina de investigaciones legislativas de los Estados Unidos*. Disponible en: https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm

Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies", EIOPA.

Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. EIOPA 2018.

UNESCO. Recomendación sobre la ética de la inteligencia artificial. Disponible en:

https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa/PDF/380455spa.pdf.multi

Páginas web:

https://aws.amazon.com/es/machine-learning/what-is-ai/

https://es.wikipedia.org/wiki/Aprendizaje_autom%C3%A1tico

https://www.ibm.com/docs/es/spss-modeler/saas?topic=networks-neural-model

https://es.wikipedia.org/wiki/Internet_de_las_cosas

https://www.deeplearning.ai/the-batch/issue-146/

https://www.garrigues.com/es_ES/garrigues-digital/proteger-algoritmos-big-data-economia-digital

https://www.expansion.com/economiadigital/innovacion/2016/04/17/5706510c46163fa5648b45a6.html

https://ecija.com/algoritmo-software-donde-reside-propiedad-intelectual/

https://keepcoding.io/blog/correlacion-estadistica-big-data/

https://www.gradiant.org/blog/claves-analisis-causal/

https://blogmapfre.com/seguros/insurance-service-el-seguro-como-suscripcion-un-servicio-de-proteccion/

https://www.enisa.europa.eu/about-enisa/about/es

https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es

https://edpb.europa.eu/about-edpb/about-edpb/who-we are_es#:~:text=El%20Comit%C3%A9%20Europeo%20de%20Protecci%C3%B3n,de%20datos%20de%20la%20UE

https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/397768/las-estrategias-de-big-data-sector-seguros

https://www.avanzaprevision.com/lo-que-la-analitica-avanzada-puede-hacer-por-las-aseguradoras/

https://theobjective.com/further/mundo-ethos/2018-11-15/big-data-cathy-oneil/

https://decidesoluciones.es/algoritmia-matematica-para-hacer-la-vida-mas-facil-a-personas/

https://bigdatamagazine.es/paradojas-matematicas-demuestran-los-limites-de-la-ia

https://ibidat.es/event/from-big-data-to-great-value-and-the-value-of-data-science-research/

https://www.deeplearning.ai/the-batch/experts-debate-definitions-in-european-unions-ai-act/

¿Qué es y cómo funciona la inteligencia artificial? Canal de Youtube Derivando. https://www.youtube.com/watch?v=_tA5cinv0U8

https://concepto.de/dato-en-informatica/

https://www.oracle.com/es/artificial-intelligence/what-is-ai/

https://www.ibm.com/docs/es/spss-modeler/saas?topic=networks-neural-model

https://www.salesforce.com/mx/cloud-computing/

https://www.xataka.com/robotica-e-ia/las-redes-neuronales-que-son-y-por-que-estan-volviendo

https://presnolinera.wordpress.com/2022/04/23/la-insoportable-opacidad-del-algoritmo-a-proposito-aunque-no-solo-del-caso-bosco/

https://www.elnotario.es/opinion/9636-el-derecho-a-no-ser-gobernados-mediante-algoritmos-secretos

https://propintel.uexternado.edu.co/la-corte-suprema-de-los-estados-unidos-determina-que-las-ideas-abstractas-no-son-patentables-caso-alice-corporation-pty-ltd-vs-cls-bank-international-et-al/

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-recomendaciones-para-aquellos-que-realicen

https://www.aepd.es/es/documento/tratamientos-inteligencia-artificial-es.pdf

https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-iii-domotica

https://www.aepd.es/es/prensa-y-comunicacion/blog/vehiculos-conectados

https://www.rsprivacidad.es/estan-seguros-los-datos-en-la-nube-cloud-computing-y-proteccion-de-datos/