Los tratamientos singulares de datos personales por parte de entidades aseguradoras, sus distribuidores y agencias de suscripción

Rafael Fernández
Counsel de Pérez-Llorca
DEPARTAMENTO DE SEGUROS Y REASEGUROS

Jesús Almarcha
Abogado de Pérez-Llorca
DEPARTAMENTO DE SEGUROS Y REASEGUROS

Andrea Sánchez
Abogada de Pérez-Llorca
DEPARTAMENTO DE PROPIEDAD INTELECTUAL, INDUSTRIAL Y TECNOLOGÍA

Índice/

Resumen: En este trabajo analizamos el tratamiento de datos personales por los distintos sujetos participantes en el sector asegurador, tanto desde un punto de vista técnico como práctico, así como las distintas técnicas y herramientas de las que hacen uso para obtener el mayor valor añadido posible de ese bien tan preciado: el dato.

Abstract: In this paper, we analyse the processing of personal data by the different parties involved in the insurance sector, both from a technical and practical point of view, as well as the different techniques and tools they use to obtain the greatest possible benefit from this valuable asset: the data.

Palabras clave: Datos personales, contrato de seguro, agencia de seguros, corredor de seguros, agencias de suscripción, colaborador externo, distribución de seguros, mediador de seguros complementarios, *call center*, *big data*, internet de las cosas, *blockchain*.

Keywords: Personal data, insurance contract, insurance agency, insurance broker, underwriting agencies, external partner, insurance distribution, supplementary insurance intermediary, call centre, big data, Internet of Things, blockchain.

Los tratamientos singulares de datos personales por parte de entidades aseguradoras, sus distribuidores y agencias de suscripción

I. Introducción

Los datos tienen una importancia crucial para el sector asegurador. En efecto, ya desde el inicio de la negociación de un contrato de seguro los datos del asegurado se tienen en cuenta, no sólo como base de los cálculos actuariales para concretar la cuantía de potenciales coberturas en caso de siniestro, sino también para estimar la probabilidad de que tenga lugar un determinado siniestro y, por tanto, determinar las condiciones y el precio del seguro. Y este traslado o comunicación de datos tiene especial trascendencia precisamente en el marco del deber de declaración del riesgo recogido en el artículo 10 de la Ley de Contrato de Seguro.

Igualmente, para la efectiva celebración del contrato de seguro, se ha de tener acceso a los datos personales del potencial cliente y otras categorías especiales de datos (información acerca de su salud, o datos biométricos, por ejemplo) y, una vez celebrado el mismo, estos datos deberán tratarse a lo largo de la vida del contrato. Es más, teniendo en cuenta que una pluralidad de entidades suele intervenir en la actividad aseguradora (mediadores, agencias de suscripción, etc.), una gran cantidad de sujetos tendrán acceso a datos personales durante la vigencia del contrato, no ya solo los relacionados con el cliente, sino incluso los de potenciales beneficiaros en caso de acaecimiento de un siniestro.

Realizamos en este artículo una aproximación a las implicaciones que el tratamiento de datos personales tiene para estos sujetos intervinientes durante la vida del seguro, para, posteriormente, analizar cuáles son los ámbitos en los que mayores desafíos está planteando esta temática.

II. La posición de la entidad aseguradora, los mediadores y las agencias de suscripción en el tratamiento de datos personales

Una de las principales cuestiones a las que tienen que enfrentarse las entidades aseguradoras y demás sujetos intervinientes en la cadena de distribución es la que se refiere a la licitud del tratamiento de datos personales.

El actual escenario regulatorio establecido por la normativa de distribución de seguros, cuya base en nuestro ordenamiento jurídico descansa en el Real Decreto ley 3/2020, de 4 de febrero[1] ("**RDL 3/2020**"), tiene un impacto especial en el tratamiento de los datos personales. Si bien los sujetos intervinientes siguen siendo similares a los de la anterior normativa de mediación de seguros, el hecho de introducir a las entidades aseguradoras como distribuidores de seguros permite confeccionar un esquema sobre la posición de cada figura en el marco

1 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.

del tratamiento de datos personales. En efecto, los artículos 203 y 204 del RDL 3/2020 marcan la pauta a seguir en cuanto a los roles que los distribuidores de seguros y demás partes implicadas tendrán en el tratamiento de los datos personales[2]. Así, el artículo 203 del RDL 3/2020 establece que:

a) Los agentes de seguros y los operadores de banca-seguros tendrán la condición de encargados del tratamiento de la entidad aseguradora con la que hubieran celebrado el correspondiente contrato de agencia.

b) Los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos.

c) Los colaboradores externos que realicen actividades de distribución por cuenta de los mediadores de seguros tendrán la condición de encargados del tratamiento de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil.

Conviene igualmente recordar que el artículo 99 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras ("**LOSSEAR**") establece el marco en virtud del cual las entidades aseguradoras podrán tratar los datos de tomadores, asegurados, beneficiarios o terceros perjudicados.

2 Vid. sobre las diferentes figuras implicadas en la distribución de seguros, VEIGA COPO, A. B.: "Clases de distribuidores de seguros" en BATALLER GRAU. J. y QUINTÁNS EIRAS, M. R. (dirs.): *La distribución de seguros privados*, Marcial Pons, 2019, pp. 107 a 147, y PEÑAS MOYANO, M. J.: "Los mediadores y sus colaboradores. Las relaciones con la clientela y la entidad aseguradora", *Revista Española de Seguros*, núm. 185-186, 2021.

1. La entidad aseguradora

Las entidades aseguradoras tienen la consideración de responsables del tratamiento, esto es, quienes deciden sobre el tratamiento de los datos personales, determinando los fines y los medios de dicho tratamiento, y debiendo aplicar medidas técnicas y organizativas para, en atención al riesgo que implica el tratamiento de los datos personales, cumplir y ser capaz de demostrar el cumplimiento con la normativa de protección de datos.

Por este motivo, entre otras obligaciones, deben mantener un registro de actividades del tratamiento[3] en el que se recoja la información prevista en el artículo 30 del 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 y por el que se deroga la Directiva 95/46/CE ("**RGPD**"). Se trata de un documento de carácter interno quedeberá estar a disposición de la Agencia Española de Protección de Datos cuando lo solicite.

En lo que se refiere a la conservación de datos personales, el artículo 203.3 del RDL 3/2020 establece la prohibición para las entidades aseguradoras de conservar los datos que les sean facilitados por los mediadores de seguros que no se deriven de la celebración de un contrato de seguro, salvo que exista una base

3 Este registro debe contener la siguiente información: nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del delegado de protección de datos; fines del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales; categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales, incluidos los que estén en terceros países y las organizaciones internacionales; en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias del artículo 49 del RGPD, las garantías adecuadas; cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

legitimadora conforme al artículo 6 del RGPD y el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("**LOPDGDD**"). De ello se deduce que la entidad aseguradora sí puede conservar los datos recibidos de un mediador de seguros cuando dichos datos deriven de la celebración de un contrato de seguro. Sin embargo, este derecho de conservación no resulta ilimitado, sino que el artículo 99.9 de la LOSSEAR viene a restringirlo, al establecer que la entidad aseguradora deberá proceder, en el plazo de diez días, a la cancelación de los datos que les hubieran sido facilitados con anterioridad a la celebración de un contrato, si este no llega a celebrarse, salvo que se cuente con el consentimiento específico del interesado, consentimiento que habrá de ser expreso, cuando se refieran a datos sobre su salud.

El referido plazo de diez días no parece acomodarse con el deber de mantener una oferta o proposición de seguro durante un plazo mínimo de quince días, tal como exige el artículo 6 de la Ley de Contrato de Seguro. Así, cabría plantearse hasta qué punto la entidad aseguradora puede compatibilizar dicho deber con el tratamiento de datos personales pasados los diez días iniciales que concede el artículo 99.9 de la LOSSEAR, máxime teniendo en cuenta que la proposición de seguro le vincula y puede ocurrir que el cliente la acepte entre el décimo y el decimoquinto día.

Entendemos que la incoherencia normativa habría que resolverse interpretando que la exégesis de dicho artículo 99.9 de la LOSSEAR es que el tratamiento de datos personales finalice, en todo caso, a los diez días de que se produzca la finalización de cualquier actividad comercial. De este modo, el cómputo del plazo de los diez días no comenzaría el día en que los datos fueron transmitidos por el mediador a la entidad aseguradora, sino el día en que la proposición de seguro (en caso de hacerse) pierde su vigencia o vigor, es decir, desde que deja de ser vinculante para la entidad aseguradora. Ello, a su vez, permitiría plazos superiores a los quince días para la aceptación de estas proposiciones de seguros, que son plenamente válidos por ser más beneficiosos para el asegurado en virtud del artículo 2 de la Ley de Contrato de Seguro.

Si el contrato llega a celebrarse, la entidad aseguradora podrá conservar los datos con base en el interés legítimo que dimana del artículo 99.1 de la LOSSEAR[4], incluso si no contase con el consentimiento del cliente.

Además, cuando la entidad aseguradora forme parte de un grupo, el artículo 99.3 de la LOSSEAR establece que no será necesario que cuente con el consentimiento del interesado para el tratamiento con fines de cumplimiento de las obligaciones de supervisión de seguros, si bien no podrán tratarse con cualquier otra finalidad sin el consentimiento específico del interesado. Las sociedades del grupo involucradas deberán considerarse en este ámbito y exclusivamente para dicha finalidad supervisora como corresponsables del tratamiento, por lo cual deberán actuar conjuntamente durante el tratamiento de dichos datos.

4 "Las entidades aseguradoras podrán tratar los datos de los tomadores, asegurados, beneficiarios o terceros perjudicados, así como de sus derechohabientes sin necesidad de contar con su consentimiento a los solos efectos de garantizar el pleno desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo".

El tratamiento de los datos de las personas antes indicadas para cualquier finalidad distinta de las especificadas en el párrafo anterior deberá contar con el consentimiento específico de los interesados."

2. Los agentes de seguros y los operadores de banca-seguros

Los agentes de seguros y los operadores de banca-seguros ("**OBS**") tendrán la consideración de encargados del tratamiento dada su dependencia de las entidades aseguradoras. La principal diferencia con el responsable del tratamiento es que el encargado de tratamiento se limita a tratar los datos personales por cuenta del responsable, sin intervenir en la toma de decisiones sobre el tratamiento de los datos personales, salvo en el caso de que el responsable de tratamiento lo haya delegado por cuestiones meramente técnicas y organizativas.

En este punto, conviene recordar la doble sanción de 50.000 euros impuesta por la Agencia Española de Protección de Datos ("**AEPD**") a una entidad aseguradora y al OBS en su Resolución de 18 de abril del 2018 (JUR 2018\79262). El supuesto se enmarcaba en la suscripción del seguro de daños sobre el inmueble hipotecado del interesado, obligación que venía impuesta en la escritura de compraventa con subrogación de hipoteca. El OBS comunicó los datos a la entidad aseguradora para la contratación del seguro en nombre del cliente, sin que tuviera su consentimiento, motivo por el que fue sancionado. Además, la entidad aseguradora, como responsable del tratamiento, también fue sancionada por utilizar los datos para la contratación del seguro sin que estuviera legitimada para ello, actuación que fue calificada de no diligente.

Por tanto, las entidades aseguradoras, consideradas responsables del tratamiento, serán las primeras en velar por el correcto tratamiento de los datos personales. estableciendo no sólo cláusulas específicas y precisas en el contrato de agencia, sino asegurándose de contar con legitimación suficiente para efectuar el tratamiento a título personal.

En concreto, el contrato de agencia deberá recoger las precisiones del artículo 28.3 del RGPD[5], así como si el agente va a celebrar contratos mercantiles con colaboradores externos. En este sentido, el mismo apartado 2 del artículo 28 del RGPD recuerda que el encargado del tratamiento no podrá recurrir a otro encargado sin la autorización escrita del responsable.

---

5 "El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

3. Los corredores de seguros y los corredores de reaseguros

Conforme al artículo 203.1b del RDL 3/2020, los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos. El elemento de independencia frente a las entidades aseguradoras es característico y diferenciador del régimen establecido en este ámbito para los agentes, elemento que ha sido trasladado también al ámbito del tratamiento de datos personales. En efecto, la autonomía de la que gozan los corredores de seguros y reaseguros les hace dignos del estatus de responsables, lo cual les convierte indirectamente, en poseedores de una información valiosa desde el punto de vista comercial.

En tales circunstancias, la entidad aseguradora que reciba los datos del corredor de seguros, tendrá la condición de responsable del tratamiento respecto de los datos específicos para prestar los servicios de seguros, mientras que el corredor de seguros será responsable para sus finalidades de gestión propias, produciéndose entre ellos una comunicación de datos que debe ser consentida por el interesado. Dicha comunicación, por lo general, vendrá regulada en las propias cartas de condiciones suscritas entre las entidades aseguradoras y los corredores de seguros, mediante cláusulas específicas que garanticen las condiciones bajo las cuales se permite el tratamiento y transmisión de los datos y, además, protegiéndose en todo caso las posiciones comerciales de ambas partes.

4. Los colaboradores externos

Un colaborador externo es una persona física o jurídica que está vinculada a un mediador de seguros mediante un contrato mercantil, en virtud del cual colabora con este en la distribución de productos de seguros. No estamos, por tanto, ante un mediador de seguros, sino ante quien realiza actividades de distribución de

---

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros."

seguros por cuenta de un mediador. En contraposición con la antigua figura de los auxiliares externos, que se encontraba bastante limitada, entendemos que el actual artículo 137 del RDL 3/2020 viene a seguir la línea expansiva de la capacidad de actuación de los colaboradores externos, de manera que su condición de no mediadores no les impedirá que de facto realicen la actividad de distribución en sentido puro, aunque no de forma independiente.

Los colaboradores externos tendrán siempre la condición de encargados del tratamiento de los mediadores de seguros con los que hubieran suscrito el correspondiente contrato mercantil, pues tal es el régimen previsto para ellos por el artículo 203.1c del RDL 3/2020. Sólo podrán tratar los datos para el desarrollo de la actividad de distribución de seguros por cuenta de los mediadores, por lo que cabe aquí recordar que los colaboradores externos, no pueden prestar servicios para las entidades aseguradoras.

Al igual que ocurre entre los agentes y las entidades aseguradoras, los contratos mercantiles entre los colaboradores externos y los mediadores deben recoger los extremos previstos en el artículo 28.3 del RGPD.

5. Los mediadores de seguros complementarios

Los mediadores de seguros complementarios son mediadores de seguros distintos de una entidad de crédito o una empresa de servicios de inversión que, a cambio de una remuneración, realizan la actividad de distribución de seguros con carácter complementario, siempre y cuando su actividad profesional principal sea distinta a la distribución de seguros y solo distribuyan determinados productos de seguros que sean complementarios de un bien o servicio. Como regla general, están sometidos al mismo régimen que los mediadores, salvo en determinadas circunstancias establecida en el artículo 130.2 del RDL 3/2020[6].

Los mediadores de seguros complementarios que se encuentren sujetos al cumplimiento del RDL 3/2020 deberán acogerse a cualquiera de los regímenes previstos para el resto de mediadores de seguros (artículo 134.2 del RDL 3/2020). Por tanto, tendrán la consideración de responsables o encargados del tratamiento en función de si optan por el régimen de los corredores de seguros o el de los agentes. En la práctica, lo más habitual será que tengan la condición de encargados del tratamiento en tanto que preferirán optar por el régimen de agencias de seguro.

Respecto a los mediadores de seguros complementarios exentos del cumplimiento del RDL 3/2020, es decir, a los que se refiere el artículo 130.2 del mismo cuerpo legal, quedarán liberados del régimen recogido en los artículos 203 y 204 del RDL 3/2020, de manera que las prohibiciones o limitaciones en ellos previstos podrán obviarse. No obstante, en la medida en la que estos mediadores acceden y tratan datos personales, quedarán sujetos al régimen general recogido en el RGPD y la LOPDGDD.

6 "El título I no se aplicará a los mediadores de seguros complementarios que ejerzan actividades de distribución de seguros cuando concurran todas las circunstancias siguientes:

a) Que el seguro sea complementario del bien o del servicio suministrado por algún proveedor, cuando dicho seguro cubra:

1.º El riesgo de avería, pérdida o daño del bien o la no utilización del servicio suministrado por dicho proveedor, o

2.º los daños al equipaje o la pérdida de este y demás riesgos relacionados con el viaje contratado con dicho proveedor; y

b) que el prorrateo anual del importe de la prima abonada por el producto de seguro no supere los 600 euros, o que el importe de la prima abonada por persona no supere los 200 euros, cuando la duración del servicio a que se refiere la letra a) sea inferior o igual a tres meses."

6. Las agencias de suscripción

Una agencia de suscripción es una persona jurídica que cuenta con un contrato de apoderamiento con una o varias entidades aseguradoras, y que le faculta para la suscripción de riesgos en nombre y por cuenta de aquella o aquellas. Por tanto, actúa suscribiendo riesgos en representación de una entidad aseguradora o reaseguradora, de modo que no tiene la condición de mediador de seguros y sus operaciones no se consideran como actividades de mediación de seguros.

Al no tener la condición de distribuidores de seguros, las agencias de suscripción no se encuentran sujetas a las normas previstas en el RDL 3/2020. En principio, si bien ostentan la posición de mandatarias de las entidades aseguradoras a las que representan (artículo 60 de la LOSSEAR), pues son prácticamente una extensión de ellas, cabría entender que las agencias de suscripción actúan en calidad de encargados del tratamiento de los datos titularidad de las aseguradoras. Por tanto, en el contrato mercantil deberían también recogerse los extremos del artículo 28.3 del RGPD.

Sin embargo, estas agencias de suscripción también podrían actuar como responsables del tratamiento en función del nivel de autonomía que tengan a la hora de tratar los datos. Así, para el supuesto de que la agencia decida sobre los medios y fines del tratamiento de los datos y este vaya más allá de lo solicitado por parte de la entidad aseguradora, persiguiéndose finalidades propias, podrá considerarse como responsable del tratamiento o, incluso, cabría la posibilidad de que la relación entre la entidad aseguradora y la de la agencia de suscripción sea de co-responsables del tratamiento.

III. La legitimidad para el tratamiento lícito de datos personales de todas las partes involucradas durante el ciclo de vida de un contrato de seguro

La actual normativa de protección de datos, encabezada por el RGPD, recoge como regla general que el tratamiento de los datos personales debe descansar sobre cualquiera de las bases legitimadoras, entre las que se encuentra el consentimiento del interesado, que debe ser expreso e inequívoco, por contraposición con tácito o implícito, tal como ha recogido el artículo 6 de la LOPDGDD. Sin embargo, en el sector asegurador, dada la enorme magnitud del dato personal como pivote de la relación entre el cliente y el resto de partes intervinientes, se han desarrollado normas específicas que vienen a matizar o flexibilizar aquella regla general de la necesidad del consentimiento del interesado, legitimando a los operadores sectoriales a dicho tratamiento sin que el interesado deba pronunciarse.

Tal y como se ha indicado anteriormente, en el caso de las entidades aseguradoras, el artículo 99.1 de la LOSSEAR establece que pueden tratar los datos de los tomadores, asegurados, beneficiarios o terceros perjudicados, así como de sus

derechohabientes, sin necesidad de contar con su consentimiento, todo ello con el objeto de garantizar el desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en dicha ley y en las disposiciones de desarrollo. Podemos afirmar que esta fundamentación del tratamiento se encontraría en sintonía con el artículo 6 del RGPD y el artículo 8 de la LOPDGDD.

La Guía para el tratamiento de los datos personales por aseguradoras de la Unión Española de Entidades Aseguradoras y Reaseguradoras[7] ("**UNESPA**") recoge un listado de tipos de tratamientos de datos en este ámbito:

- "**Tratamiento de datos fundado en el contrato de seguro o en la aplicación de medidas contractuales o precontractuales**: no se requiere el consentimiento del interesado al estar sustentado en la ejecución del contrato, en el interés legítimo y en la base legal que le otorga la legislación aseguradora, salvo que se trate de tratamientos de datos de salud que no estén fundados en una habilitación legal.

- **Tratamiento de datos con fines de publicidad y marketing propio a clientes de la entidad sobre productos similares**: no se requiere el consentimiento del interesado al ser una acción sustentada en el interés legítimo de la entidad aseguradora. Son productos similares los productos de seguros de vida o de no vida que se adecúen al perfil del cliente.

- **Tratamiento de datos relacionados con la actividad aseguradora**: no requieren el consentimiento explícito al ser tratamientos fundados en el cumplimiento de obligaciones legales o en habilitaciones legales."

Si bien la guía constituye autorregulación sectorial, lo cierto es que su contenido es realmente útil por cuanto para su confección se contó con la colaboración de la AEPD, de modo que dicho contenido se encuentra respaldado por esta institución.

A los anteriores supuestos de tratamiento de datos, también podemos añadir el tratamiento de datos para su comunicación a las autoridades judiciales. En este caso, la legitimación vendría dada por el artículo 6.1.c) del RGPD y el artículo 8 de la LOPDGDD. La reciente Sentencia de la Audiencia Nacional (Sala de lo Contencioso administrativo, Sección Primera) de 30 de abril del 2021 [JUR 2021\191856] precisamente ha avalado la comunicación hecha por una entidad aseguradora a un juzgado de los datos relativos a una póliza de un ex directivo de una entidad de crédito. La peculiaridad, además, reside en que el juzgado no había requerido la aportación de esos datos, sino que fue la entidad aseguradora la que lo hizo motu proprio al ver una noticia en la prensa.

Sin embargo, una vez finalizado el contrato de seguro, la entidad aseguradora no puede tratar los datos del cliente. En este sentido, la Resolución de la AEPD de

7 UNESPA: "Guía para el tratamiento de los datos personales por las entidades aseguradoras", de 7 de febrero de 2019.

14 de mayo del 2021 [JUR 2021\273159] impuso una sanción de 30.000 euros a una entidad aseguradora que, debido a un error informático involuntario, pasó el recibo de una póliza a la cuenta bancaria de un antiguo cliente.

Por otro lado, en cuanto a los mediadores de seguros:

- **Los agentes de seguros y OBS**: estos mediadores de seguros, en tanto que ostentan la condición de encargados del tratamiento, deberán tratar los datos conforme se estipule en el contrato de agencia con las entidades aseguradoras. Además, los OBS tienen prohibido utilizar los datos personales para fines propios de su objeto social sin obtener el consentimiento previo del cliente.

  Por tanto, el tratamiento durante la vigencia del contrato de seguro dependerá del alcance acordado con la entidad aseguradora en cuestión, si bien lo habitual será que se ciña a lo dispuesto en el artículo 28.3 del RGPD.

- **Los corredores de seguros**: dado que son responsables del tratamiento, están sometidos a un régimen más exigente que los demás mediadores de seguros. En concreto, durante la vida del contrato el corredor de seguros estará legitimado en similares términos que una entidad aseguradora, es decir, deberá basar el tratamiento en alguno de los supuestos del artículo 6.1 del RGPD.

Cuando finalice el contrato de seguro en el que el corredor haya mediado, este deberá cancelar los datos del interesado (salvo que tenga su consentimiento para otros fines o para la celebración de un nuevo contrato de seguro). Hemos de considerar que este escenario también es trasladable al supuesto en el que se insta el cambio de posición mediadora por parte del interesado, pese a que el contrato de seguro mediado por el corredor siga vigente con otro mediador de seguros distinto.

IV. La grabación de llamadas en los centros de atención al cliente (*call centers* o *contact centers*) de las entidades aseguradoras

Una de los escenarios más problemáticos para las entidades aseguradoras es el del tratamiento de datos personales a través de sus *call centers*. Estos centros de atención al cliente, por su configuración, suelen tratarse los datos para multitud de propósitos, tales como la resolución de dudas sobre contratos de seguro ya suscritos, la contratación u oferta de un nuevo seguro, la grabación de llamadas con motivo de calidad, etc. Y, en el caso específico de la grabación de llamadas, el Tribunal Supremo ha establecido que la grabación de la voz asociada a otros datos, o su puesta a disposición de otras personas que pueden identificar a quien pertenece, ha de considerarse un dato de carácter personal sujeto a la normativa de protección de datos[8].

8 Sentencias del Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección Tercera) núm.815/2020, de 18 de junio (Rec. 1074/2019) y núms. 839/2020, 840/2020 y 853/2020, de 22 de junio (Recs. 2134/2019, 4958/2019 y 1745/2019)

Partiendo de tal premisa, es importante entender cuál es el propósito de la grabación y, por tanto, del tratamiento de los datos personales. Así, habrá que diferenciar los casos en los que se pretenda gestionar la relación contractual por teléfono (por ejemplo, resolución de dudas relacionadas con el contrato) o si se quiere llevar a cabo un control de calidad por parte de la empresa.

La grabación de la llamada con motivo de calidad no se encuentra amparado por el tratamiento en aras del cumplimiento de una obligación legal recogido en el artículo 8 de la LOPDGDD ni tampoco en el artículo 99.1 de la LOSSEAR, por lo que debería recabarse el consentimiento del cliente o amparar la grabación en algún otro interés legítimo de los previstos en el artículo 6.1 del RGPD.

Respecto a la prestación del consentimiento por el interesado, debe consistir en una conducta activa mediante la que exprese su voluntad de consentir el tratamiento del que se trate. Por ejemplo, la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda) de 11 de noviembre del 2020 (Asunto C-61/19) dictaminó que el consentimiento prestado por el consumidor en el momento de firma de un contrato ha de ser una expresión de voluntad palmaria y plenamente informada, especialmente cuando tal circunstancia se refiere al tratamiento de datos de carácter personal, no reconociéndose como lícita la utilización de casillas previamente marcadas por el responsable del tratamiento. Si bien el supuesto tratado por el TJUE se refiere a casillas pre-marcadas, la interpretación puede trasladarse a otros casos o ámbitos en los que el consentimiento del interesado se obtiene mediante una actitud pasiva.

Así ocurre con la práctica consistente en informar sólo de que "la llamada puede ser grabada…", donde el consentimiento, en caso de estar recabándose, se prestaría de forma tácita y no sería acorde a la actual normativa de protección de datos.

Mismo criterio hemos de mantener respecto a la práctica consistente en la implantación de una locución en la que se indique al interesado que, en caso de que no quiera que se grabe su llamada, pulse un número concreto, pues no se exige una actitud positiva del interesado para prestar su consentimiento, sino que se parte de un consentimiento "pre establecido", tácito, para cuyo no consentimiento se exige una actitud activa del interesado marcando el número, lo cual es precisamente contrario a lo que el RGPD pretende.

Con todo, debe destacarse que sólo cuando el interesado no sea un cliente (salvo que sea un tercero perjudicado) será necesario recabar el consentimiento, pues si el interesado ya tiene una vinculación contractual o precontractual con la entidad aseguradora y el tratamiento estuviera relacionado con las obligaciones legales o con la propia gestión del contrato, dicho tratamiento estaría amparado por lo dispuesto en el artículo 99.1 de la LOSSEAR y el artículo 8 de la LOPDGDD. Siempre teniendo en cuenta que la finalidad perseguida con la grabación de las llamadas no exceda el mantenimiento de la relación contractual.

Una posibilidad práctica para evitar o reducir el riesgo legal en el tratamiento de datos por parte de estos centros podría consistir en preguntar inicialmente a la persona si se encuentra entre los sujetos previstos en el artículo 99.1 de la LOSSEAR (tomador, asegurado, beneficiario, tercero perjudicado o derechohabiente), de modo que, en caso de que no lo sea, se recabe el consentimiento para proceder a grabar la llamada. Acto seguido, y con independencia de que la persona se encuentre entre los sujetos previstos en el artículo 99.1 de la LOSSEAR, se deberá proceder a informar sobre el tratamiento de los datos y demás obligaciones de información de primera capa, así como de la posibilidad de consultar la información adicional de segunda capa en el sitio web de la entidad aseguradora. Adicionalmente, para el caso de que el interesado exija recibir la información adicional de segunda capa también telefónicamente, la entidad deberá desarrollar un mecanismo que garantice su transmisión telefónica complementaria, todo ello tal como prevé la meritada Guía para el tratamiento de los datos personales por aseguradoras de UNESPA.

V. Límites y obligaciones para el perfilado de personas (*profiling*) por las entidades aseguradoras –¿En qué medida es compatible el uso de la analítica de big data para perfilar el riesgo con el GDPR?

Dentro del sector asegurador es frecuente que las aseguradoras lleven a cabo actividades relacionadas con la elaboración de perfiles de sus clientes y potenciales clientes. La principal finalidad que persiguen es analizar a los mismos para realizar una tarificación de las pólizas lo más adecuada posible y también, en una segunda instancia, para diseñar y comercializar otros productos adecuados al perfil de los clientes.

La elaboración de perfiles o *profiling* adquiere por tanto una especial relevancia y el RGPD lo regula de manera expresa tanto en su artículo 4[9], como en su artículo 22[10]. En este sentido, el referido artículo 4 se centra en la elaboración de perfiles clásica o general, cuyos elementos fundamentales son[11]:

- El tratamiento de los datos debe hacerse primordialmente de manera automatizada, pero debe existir también participación humana;
- Debe llevarse a cabo respecto a datos personales; y
- El objetivo principal es evaluar aspectos personales sobre una persona física. No se trata de recabar información conocida del individuo, sino de evaluar esa información conocida para posteriormente analizarla y hacer predicciones sobre la misma.

Por su parte, el artículo 22 habla exclusivamente de decisiones automatizadas, cuya principal característica es que, en la toma de las mismas, no existe

9 Artículo 4.4 RGPD. «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

10 Artículo 22 RGPD. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado.

11 Directrices sobre las decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679.

intervención humana. Los elementos fundamentales de la toma de estas decisiones son los siguientes:

- Pueden basarse en cualquier tipo de información (datos obtenidos directamente por el interesado (por ejemplo, a través de un formulario), datos observados (por ejemplo, a través de cookies o aplicaciones móviles) y datos derivados (por ejemplo, datos obtenidos a través de un perfil pre-existente de dicha persona); y

- No implica necesariamente que se lleven a cabo con elaboración de perfiles.

Antes de llevar a cabo cualquier tratamiento de datos personales, las aseguradoras deben determinar claramente las finalidades que buscan y en función de ello, elegir la base legitimadora adecuada. De todas las bases legitimadoras que ofrece el RGPD[12], para la elaboración de perfiles general pueden tener cabida las siguientes:

- **Consentimiento**: El consentimiento es aquella manifestación de voluntad libre, específica, informada e inequívoca, por la que el interesado acepta el tratamiento de datos personales que le concierne. Para que el consentimiento sea válido, las aseguradoras deben informar adecuadamente acerca del tratamiento que se va a realizar y deben solicitar el consentimiento de una manera expresa, por ejemplo, a través de una casilla diferenciada del resto de tratamientos que la aseguradora necesita realizar.

- **Contrato**: La necesidad contractual debe interpretarse de una manera estricta y no debe contemplar situaciones en las que el tratamiento no sea realmente necesario para la ejecución del contrato[13]. En el tema específico del *profiling*, se entiende como discutible utilizar esta legitimación, ya que no puede decirse que el *profiling* sea necesario para el correcto desarrollo del contrato de seguros, al existir medios más tradicionales y menos intrusivos.

- **Interés legítimo**: Es conveniente recordar que el interés legítimo no es un concepto nuevo creado a partir de la entrada en vigor del RGPD, puesto que la Directiva 95/46/CE ya lo recogía y el Comité Europeo de Protección de Datos, antiguo Grupo de Trabajo del Artículo 29, ("**CEPD**"), de hecho, desarrolló un dictamen[14] para intentar aportar cierta claridad sobre el concepto y su utilización. Los responsables del tratamiento tienden a pensar que un interés legítimo puede ser cualquiera, siempre y cuando no contravenga la normativa vigente. Sin embargo, el interés legítimo recogido por el RGPD va más allá y para considerarse válido, además de ser lícito, tiene que estar articulado con claridad suficiente y debe representar un interés real y actual. Una

12 Artículo 6 RGPD: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

13 Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE: Además, el hecho de que el tratamiento de algunos datos esté cubierto por un contrato no quiere decir automáticamente que el tratamiento sea necesario para su ejecución. Por ejemplo, el artículo 7, letra b), no es un fundamento jurídico apropiado para elaborar un perfil de los gustos y las opciones de estilo de vida del usuario, basado en su recorrido por un sitio web y en los artículos adquiridos. Ello se debe a que el responsable del tratamiento de los datos no ha sido contratado para elaborar perfiles, sino para entregar bienes y ofrecer servicios concretos, por ejemplo. Incluso si estas actividades de tratamiento se mencionan de manera específica en la letra pequeña del contrato, este hecho por sí solo no las convierte en «necesarias» para la ejecución del contrato.

14 Íbidem.

vez determinado que el interés de las aseguradoras es legítimo según los estándares del RGPD, será necesario llevar a cabo un análisis en profundidad y una ponderación entre el citado interés legítimo del responsable y los intereses, derechos y libertades fundamentales de los interesados (el "***Balancing Test***"). El principal inconveniente de la utilización de esta base legitimadora es que ni el RGPD ni la LOPDGDD desarrollan o establecen los requisitos a tener en cuenta al llevar a cabo el citado *Balancing Test*; ambos textos normativos únicamente recalcan la necesidad de llevar a cabo una evaluación meticulosa, sin más especificación.

Si nos centramos en la toma de decisiones automatizadas, tendrían cabida el consentimiento, la necesidad contractual y el cumplimiento de una obligación legal. El artículo 22 es muy claro y de la lectura del mismo se desprende una prohibición general de llevar a cabo este tipo de tratamientos salvo que la toma de decisiones automatizada (i) sea necesaria para la ejecución de un acuerdo; (ii) esté autorizada expresamente por una ley; y (iii) esté basada en el consentimiento explícito del interesado. Teniendo en cuenta lo anterior, se entiende que las entidades aseguradoras están facultadas para realizar este tipo de tratamientos. No obstante, como límites a este tratamiento de datos personales de sus clientes y potenciales clientes, las entidades aseguradoras deben llevar a cabo estas actividades teniendo en cuenta los principios rectores del RGPD. Concretamente:

- **Principio de licitud, lealtad y transparencia**. Los datos personales deben tratarse de manera lícita, leal y transparente.

  El cumplimiento de este principio implica que antes de llevarse a cabo la elaboración de su perfil, el cliente o potencial cliente debe ser informado explícitamente sobre esta actividad. En el caso de la toma de decisiones automatizadas, además se deberá informar también acerca de la lógica aplicada en la elaboración de las mismas.

- **Principio de limitación de la finalidad**. Los datos personales deben ser recogidos para finalidades determinadas, explícitas y legítimas y no deben ser tratados ulteriormente de manera incompatible con dichos fines.

  La elaboración de perfiles suele basarse en datos que fueron recabados originalmente para otra finalidad. El cumplimiento de este principio implica analizar las finalidades originales y determinar si esta nueva finalidad es compatible con las primeras, y en caso de no ser así encontrar la base legitimadora adecuada.

- **Principio de minimización del dato**. Los datos personales tratados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que han sido recabados.

El cumplimiento de este principio implica tratar y conservar únicamente los datos necesarios para realizar la elaboración de perfil deseada, no siendo posible un tratamiento masivo e ilimitado de los datos relativos a la persona en cuestión.

- **Principio de exactitud**. Los datos tratados deben ser exactos y en caso de que estos no lo sean, deberán ser modificados.

  El cumplimiento de este principio es de vital importancia en la elaboración de perfiles ya que, si no se recaban datos exactos y veraces, cualquier perfil y/o decisión que se tome posteriormente puede sean inadecuados. Es decir, la empresa aseguradora debe velar, durante todo el proceso de la elaboración de perfiles, de que los datos recabados sean veraces y estén actualizados. Y para ello deberá implementar cualesquiera medidas capaces de garantizar de forma continua la precisión y exactitud de los datos tratados.

- **Principio de limitación del plazo de conservación**. Los datos personales deben ser tratados únicamente durante el periodo de tiempo que sea necesario para poder conseguir los fines del tratamiento para los que fueron recabados. No obstante, estos datos podrán ser tratados durante periodos más largos de tiempo cuando se vayan a tratar con fines de archivo en aras del interés público, fines de investigación científica o histórica y fines estadísticos.

  El cumplimiento de este principio implica tratar y almacenar los datos únicamente durante el periodo de tiempo en que sea estrictamente necesario y de forma proporcional a la finalidad del tratamiento.
  El cumplimiento de este principio puede suponer un reto para las empresas aseguradoras, ya que con el desarrollo del tratamiento masivo de datos (*big data*) y la Inteligencia Artificial, los algoritmos utilizados en la elaboración de perfiles están diseñados precisamente para procesar grandes cantidades de información, independientemente de si son realmente necesarios para el análisis concreto o no, decisión a la que se llega precisamente durante el procesamiento de los datos.

- **Principio de integridad y confidencialidad**. Los datos personales deben ser tratados de una manera que garantice su seguridad, adoptando las medidas técnicas y organizativas que se adecuen a las categorías de datos personales y el tratamiento que se lleva a cabo.

  El cumplimiento de este principio podría resultar sencillo, ya que implica analizar las tecnologías internas utilizadas para la elaboración de los perfiles y los sistemas en los que se almacena la información y establecer las medidas de seguridad técnicas y organizativas adecuadas para los tratamientos que se realizan.

Es fundamental llevar a cabo este tipo de tratamientos de manera adecuada, ya que la elaboración de perfiles puede generar situaciones discriminatorias para el interesado e incluso verse afectados sus derechos, por ejemplo, mediante la denegación de servicios o productos específicos. Para garantizar que se implementan todas las garantías necesarias para eliminar o minimizar las potenciales consecuencias negativas que este tratamiento puede inferir sobre los interesados, se deberá realizar una evaluación de impacto sobre la privacidad de los datos antes de llevarlos a cabo.

Finalmente, huelga decir que el interesado podrá ejercitar los diferentes derechos que le asisten en materia de protección de datos, pudiendo retirar su consentimiento, limitar el tratamiento que se hace de sus datos u oponiéndose al mismo. El derecho a la protección de datos es un derecho fundamental, pero no es un derecho absoluto y no puede ejercitarse como tal.

Si bien el RGPD reconoce en sus artículos 12 a 22 una serie de derechos que cualquier interesado puede ejercitar en relación con el tratamiento que se hace de sus datos, el legislador ha querido también otorgar cierto poder de decisión sobre la ejecución de los mismos a los responsables del tratamiento. Habrá que atenerse a cada situación específica para ver qué prevalece, si el derecho del interesado o el derecho de la aseguradora a seguir llevando a cabo un tratamiento específico.

VI. Desafíos por la utilización de dispositivos (IoT - *Internet of Things*) y el tratamiento masivo de datos (*big data*) por el sector asegurador – No hay uniformidad en el sector asegurador en la aplicación de estas tecnologías

La inteligencia de datos o *big data* implica el tratamiento masivo de información, incluyendo la capacidad de recopilar y almacenar grandes cantidades de datos de diversas fuentes, para obtener una finalidad concreta utilizando la tecnología disponible. Por su parte, el "Internet de las Cosas" o *IoT* supone la conexión de diferentes objetos a Internet para el procesamiento de la información recolectada por dicho dispositivo, para la toma de decisiones de diferente índole.

Las grandes capacidades de computación y de almacenamiento de la información de los últimos años ha hecho que las empresas incrementen su deseo de recabar y tratar información para diferentes fines.

Analizar un mayor volumen de información implica la obtención y comprensión de información que antes no entendíamos ni éramos capaces de observar. Con el *big data* cualquier empresa es capaz de sacar un mayor beneficio de la información a la que acceden ya que a diferencia de lo que ocurre con las herramientas tradicionales, cuánta más información se obtiene, mayores combinaciones de datos se pueden realizar y más información nueva se puede descubrir.

Existen dos categorías de datos que se recogen con el *big data*[15]:

- Datos estructurados: constituyen toda aquella información que puede encontrarse de manera ordenada en una base de datos, lo que facilita su tratamiento por todo tipo de herramientas. En otras palabras, es información fácilmente accesible e identificable.

- Datos no estructurados: constituyen toda aquella información que no sigue una estructura clara, un conglomerado masivo y desordenado de datos, que en su conjunto no tiene valor.

La utilización de *big data* en el sector asegurador ofrece ventajas competitivas y supone un beneficio económico para aquellas que la utilizan, pudiendo ser más eficientes al contar con datos fiables y una visión más realista de los riesgos que pretenden cubrir. Concretamente, el desarrollo de la tecnología, y más concretamente la utilización del *big data*, permite a las aseguradoras cambiar su modelo tradicional de protección *ex post facto*, por un modelo de predicción *ex ante*. Obtener mejores modelos predictivos en la práctica puede implicar que una aseguradora sea capaz de seleccionar proactivamente a individuos de bajo riesgo que sus competidores no han sido capaces de identificar[16].

A pesar de que tanto el *IoT* como el *big data* ofrecen numerosas ventajas a las empresas, como las citadas anteriormente o también mejoras en la captación y fidelización de clientes y potenciales clientes, hay que poner de relieve que, con la utilización de ambas, se llevan a cabo tratamientos de datos (esencialmente personales) y, por tanto, hay que atender a la potencial confrontación que surge entre estas tecnologías y la protección de datos personales.

El objetivo de utilizar este tipo de tecnologías es tratar un gran volumen de información obteniendo el mayor beneficio posible. Tal y como se ha expuesto en el apartado IV, cualquier tratamiento de datos personales debe, entre otras muchas cosas, cumplir con los principios rectores del RGPD. Los principales desafíos a los que las entidades aseguradoras se enfrentan son los siguientes:

- **Posible colisión con el principio de minimización de los datos personales**. Si el RGPD obliga a recopilar y tratar únicamente aquellos datos estrictamente necesarios para conseguir la finalidad perseguida, el *big data* supone precisamente todo lo contrario: una recopilación masiva de información, independientemente de que esa información sea relevante o no para la finalidad perseguida.

  Para disminuir el riesgo de incumplir este principio, dentro de sus respectivos repositorios masivos de datos (denominados en el sector *data lake*), las entidades aseguradoras deben procurar analizar detenidamente la información y seleccionar sólo aquella que sea relevante para la finalidad perseguida.

15 GIL GONZÁLEZ, E., "*Big Data, privacidad y protección de datos. 2016*". XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos; páginas 21 a 24).

16 McGurk, B., "*Data Profiling and insurance law*", Hart Publishing 2019.

- **Posible colisión con el principio de exactitud de los datos personales**. Al obtenerse información de muy diversas fuentes, la utilización del *big data* no permite validar dichas fuentes ni comprobar que la información recabada es veraz, fiable y actualizada.

  El principal riesgo que existe para las entidades aseguradoras es utilizar información no contrastada o poco fiable como base para sus estrategias o sus análisis de mercado, ya que un tratamiento descuidado de esta información puede tener implicaciones devastadoras para sus intereses.

- **Posible colisión con el principio de confidencialidad e integridad de la información**. La información que se recaba, comparte y comunica en el *IoT* no está debidamente protegida mediante sistemas de cifrado y por tanto la hace muy vulnerable a sustracciones y accesos no autorizados, definidos como brechas de seguridad por el RGPD.

  Para evitar sufrir brechas de seguridad y las consiguientes sanciones administrativas interpuestas por la autoridad de control competente (la AEPD) es cardinal que las entidades aseguradoras implementen aquellas medidas técnicas y organizativas que garanticen la integridad de la información.

Teniendo en cuenta lo anterior, el principal riesgo ante el que nos encontramos es la elevada probabilidad de que los datos utilizados para llevar a cabo la elaboración de perfiles de los individuos sean inexactos y, por tanto, las predicciones y conclusiones sacadas no sean adecuadas, generando un grave perjuicio al interesado afectado. Es importante recordar que las predicciones sobre comportamientos futuros se basan únicamente en cuestiones de probabilidad, que no es una ciencia exacta.

Dado que el análisis predictivo realizado principalmente a través del *big data* se fundamenta únicamente en una correlación entre diferente información recabada y un análisis realizado por algoritmos, existe el riesgo de catalogar a las personas en función de sus propensiones y no de sus acciones, pudiéndose generar así situaciones de discriminación y desigualdad.

Por tanto, si bien la utilización del *IoT* y el *big data* ofrecen ventajas competitivas muy atractivas, las entidades aseguradoras deben implementar protocolos internos que permitan (i) comprobar la veracidad y exactitud de la información; (ii) analizarla para descartar aquella información que no sea necesaria para las finalidades perseguidas; y (iii) asegurarla de potenciales accesos no autorizados.

VII. La utilización de sistemas inteligentes (Inteligencia Artificial) para la toma automatizada de decisiones por parte de entidades aseguradoras y de *blockchain* para la descentralización de la información.

1. Inteligencia artificial

A pesar de los innumerables avances tecnológicos de las últimas tres décadas, pocas tecnologías han levantado tanta expectación y augurios revolucionarios y disruptivos como la inteligencia artificial ("**IA**") y la *blockchain* o "cadena de bloques". Mientras la primera pretende conseguir que un sistema informático reemplace la inteligencia humana a través de la imitación de su razonamiento (incluso, con técnicas de aprendizaje con intervención humana –*machine learning*– o en las que la máquina es capaz de razonar por sí misma –*deep learning*–), la segunda se basa en una cadena de bloques a través de la cual los usuarios realizan transacciones de valor de manera descentralizada, con un mismo libro-registro igualmente distribuido, en donde se registran todas las transacciones y que es utilizado para dotar de confianza a todo el sistema[17].

En relación con la IA y el *machine learning*, en el sector asegurador es importante hablar de dos tipos de aprendizaje: el supervisado y el no supervisado:

- Supervisado: los algoritmos se desarrollan a partir de conjuntos de datos ya etiquetados. Son entrenados para ir avanzando mediante el suministro de datos con valores "correctos" ya asignados.

- No supervisado: los algoritmos no están entrenados y se les deja encontrar regularidades en los datos de entrada sin ninguna instrucción sobre lo que deben buscar.

Lo que hace que el *machine learning* sea potente es la capacidad de los algoritmos de cambiar su resultado en función de la experiencia.

El sector asegurador no ha ignorado estas nuevas tecnologías, con reseñables intentos de implementación dentro de sus procesos productivos, aunque, a pesar de la relativa longevidad de estas tecnologías[18], su actual estado primigenio y relativamente inmaduro, y aún más, como expondremos a continuación, sus desafíos jurídicos, están provocando que su implantación sea, en la actualidad, claramente testimonial.

La inteligencia artificial promete la toma de decisiones relativamente complejas por un sistema cibernético y sin intervención humana. Desde hace décadas existen multitud de sistemas informáticos que toman decisiones con cierto impacto exterior y sobre el ser humano (por ejemplo, un aparato médico que proporciona un medicamento cuando un paciente ha alcanzado un determinado umbral

17 Más información sobre el funcionamiento técnico de la *blockchain*, en Real Instituto Elcano http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari106-2019-alonsolecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomoneda (última revisión el 11 de octubre de 2021).

18 La Inteligencia Artificial fue formulada por primera vez en 1956 por el ingeniero informático John McCarthy. Por otro lado, los principios de la tecnología *blockchain* fue inicialmente desarrollada por Satoshi Nakamoto en 2008.

medible), si bien, la comunidad científica y los organismos de investigación públicos y privados pretenden una mayor automatización de tareas que, en el sector asegurador, podrían delegar en máquinas importantes procesos, incluyendo de atención al cliente, análisis y procesado de solicitudes o detección del fraude.

La Comisión Europea ha mostrado su preocupación ante la creciente utilización de sistemas basados en inteligencia artificial con gran capacidad de impacto en el ser humano, por ejemplo, por la opacidad de los algoritmos a la hora de tomar decisiones. Por este motivo, en abril de 2021, la Comisión Europea aprobó una propuesta de reglamento en materia de inteligencia artificial[19] (la "**Propuesta**") centrada en un sistema de gestión de riesgos, la cual establece determinados principios, derechos y límites que será de obligado cumplimiento para todas las empresas e instituciones que desarrollen o exploten sistemas inteligentes, con el objetivo general de alcanzar el respeto de unos estándares éticos y generar confianza en la tecnología.

Por su parte, la AEPD publicó en febrero de 2020 el documento "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción" (el "**Documento de la AEPD**"), en donde aborda las principales dudas que se plantean en el marco de protección de datos de carácter personal, y analiza los aspectos más relevantes en la relación entre Inteligencia Artificial y RGPD que deben ser tenidos en cuenta desde el diseño y en la implementación de tratamientos que incluyan inteligencia artificial. En el documento se presta atención especial, entre otras cuestiones, a la legitimación para el tratamiento, la información y transparencia, el ejercicio de derechos, las decisiones automatizadas, la exactitud, la minimización de datos, la evaluación de impacto y el análisis de la proporcionalidad del tratamiento.

Ambos documentos son una muestra de la preocupación existente por dar una respuesta adecuada a la regulación de los tratamientos de datos que incorporen componentes de inteligencia artificial.

Así, la Propuesta categoriza a los sistemas con inteligencia artificial según los riesgos que sus usos pudieran ocasionar, calificándolos como (i) riesgo inaceptable; (ii) riesgo alto; y (iii) riesgo bajo o mínimo. Entre los primeros se encuentran los usos descritos en el artículo 5 de la Propuesta, que están directamente prohibidas por tener "gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas[20]." Por otro lado, los sistemas de riesgo alto son aquellos que suponen un riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas, los cuales estarán permitidos, si bien el operador de dicho sistema con IA deberá cumplir determinados requisitos obligatorios y realizar una evaluación de la conformidad del sistema con la norma *ex ante*. Finalmente,

19 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, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=EN (última revisión el 11 de octubre de 2021).

20 Apartado 5.5.2 de la Exposición de Motivos de la Propuesta.

sobre los últimos, cuyos usos supone un riego bajo para la salud, seguridad o derechos de las personas, la Propuesta no establece medidas específicas, dada su inocuidad.

Por sus propias características, el sector asegurador será uno de los que, potencialmente, se vea más afectado por esta Propuesta si finalmente se aprueba en los términos planteados por la Comisión Europea. La posibilidad de denegar determinadas coberturas médicas con base en decisiones tomadas por un sistema de IA servirá enormemente para agilizar los procesos y optimizar los recursos de las compañías aseguradoras, pero pueden crear situaciones como las enumeradas anteriormente, que obligarán a hacer un análisis de riesgos previa a la utilización de IA y, además, a configurar y a operar ésta según en los términos de la Propuesta. Entre las obligaciones más representativas se encuentra la de informar convenientemente a los usuarios, de manera análoga a en materia de protección de datos personales; diseñar la herramienta con capacidad de registrar eventos automáticamente, para garantizar la trazabilidad de la toma de decisiones; o la preparación de documentación técnica, en donde se describa suficientemente el sistema y se demuestre que cumple con los límites y obligaciones de la Propuesta.

2. Tecnología *blockchain*

La Exposición de Motivos de la Propuesta afirma en varias ocasiones que uno de los objetivos finales de la misma es inspirar confianza en los ciudadanos y otros usuarios para que adopten soluciones basadas en la IA, confianza que es también el leitmotiv de la tecnología *blockchain* que, como adelantamos, no es una herramienta para la toma automatizada de decisiones, sino para el registro descentralizado de información y, cuando se une a un *smart legal contract*[21], la autoejecución de un contrato. Una cadena de bloques permitiría, en un plano teórico, descentralizar la responsabilidad del registro de información en un solo ente (por ejemplo, una empresa aseguradora) y, además, garantizar la ejecución automática de un contrato o de algún término de él, sin necesidad de intervención de las partes. En el sector asegurador permitiría, por ejemplo, que un asegurado cobrase automáticamente una indemnización contemplada en una póliza de seguros, ante una catástrofe natural como una riada, cuando el sistema, principalmente a través de sensores, registrase la misma. Esta tecnología promete transparencia, agilidad en la cobranza de indemnizaciones y, sobre todo, confianza por no depender todo el sistema de un ente centralizado, aunque plantea no menos retos jurídicos, precisamente de confidencialidad de la información registrada, cumplimiento de las obligaciones en materia de protección de datos personales, excesiva complejidad técnica o la imposibilidad de detener la ejecución de un *smart legal contract*, por existir alguna variable que inicialmente no fue contemplada. De hecho, a pesar de ser una tecnología con más de una década de existencia, su adopción por el sector asegurador es prácticamente testimonial, limitándose a pruebas de concepto que no se han materializado en casos de uso.

21 Un *smart legal contract* es un programa informático, desplegado en una *blockchain*, que permite la ejecución automática y autónoma de un contrato o de partes de este.

Así, la tecnología *blockchain* o "tecnología de contabilidad distribuida" (Distributed Ledger o DLT, por sus siglas en inglés), se popularizó en 2009 ligada a la figura del Bitcoin. Posteriormente, ha despertado gran interés en un buen número de sectores económicos, especialmente en el financiero y relacionados. Su potencial transformador de la figura de los intermediarios en las transacciones, así como la garantía de la exactitud e inalterabilidad de los contenidos de las transacciones o registros, puede llegar a mejorar la eficiencia en los procesos y disminuir los costes de determinadas transacciones para las entidades que adopten este tipo de tecnología.

El *blockchain* se define, a grandes rasgos, como un registro de operaciones único, organizado mediante nodos, que ha sido consensuado por las distintas partes implicadas y que no puede ser modificado salvo si todas ellas se ponen de acuerdo para hacerlo. Así, el nodo reúne copias exactas de diversas transacciones o registros, estando vinculado con el nodo inmediatamente anterior y el nodo siguiente, de manera que forma una cadena en la que el nodo tiene una posición es inamovible y un contenido inalterable. Es precisamente esta inalterabilidad la que tiene un mayor impacto en el mundo empresarial, ya que mejora la transparencia de las transacciones realizadas en la red y minimiza el riesgo de fraude[22]. En palabras de la doctrina "es una contabilidad pública entre pares que se mantiene mediante una red distribuida de ordenadores y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios"[23].

En el marco de los seguros, el *blockchain* presenta quizás su mayor potencial de desarrollo con los *smart legal contracts*, basados en tecnología *blockchain* y que, mediante un código informático, pueden ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin que resulte necesaria la intervención de una tercera persona o entidad que vele por su cumplimiento. Además, el contenido del contrato y toda la información que contiene se almacenan en un nodo, cuyos datos no se revelará salvo a las partes que lo firmaron, de no ser necesario.

Como se puede inferir, por tanto, una de las mayores ventajas de este tipo de contratos basados en *blockchain* es la posibilidad de acelerar todos los trámites que tienen lugar en la vida de un contrato de seguro, desde su contratación hasta las gestiones relacionadas con el acaecimiento del siniestro asegurado, lo que incluso puede implicar un beneficio al cliente, derivado de los posibles ahorros que le puedan suponer una reducción de las privas por este menor coste de los procesos internos para la aseguradora.

No obstante, a pesar de los beneficios que, a priori, presenta esta tecnología, se advierten algunos desafíos a los que habrá que hacer frente en relación con el obligado cumplimiento de las normas en materia de protección de datos personales. Así, por ejemplo, entre los aspectos más controvertidos, cabe destacar:

- Teniendo en cuenta que la cadena *blockchain* es una red, por definición, inmutable, se plantean dudas acerca de la posibilidad del ejercicio

22 Vid. "Blockchain (II): Conceptos básicos desde la protección de datos", publicado por la AEPD el 20 de noviembre de 2020.

23 MENDOZA ENRÍQUEZ, O.A., "Blockchain y protección de datos personales", *Revista Iberoamericana de Derecho Informático*, 2020.

de los derechos de supresión y el de rectificación. Incluso sería conveniente ver hasta qué punto los datos personales incorporados en *blockchain* deberían estar anonimizados.

- Dado que cada uno de los actores de la cadena *blockchain* actúa en plano de igualdad con el resto, es difícil determinar la posición que ocupa cada uno de estos actores, es decir, si son responsables de tratamiento) y, por tanto, cuáles son las obligaciones derivadas de su posición jurídica en relación con el tratamiento de datos personales que realicen o la base legitimadora en virtud de la cual realicen dicho tratamiento.

- La automatización de decisiones que deriva del uso de *smart contracts* parece entrar en conflicto con las previsiones del artículo 22 RGPD, que establece el derecho de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Por tanto, habrá que analizar si es posible que la tecnología *blockchain* permita adaptar estos contratos para que cumplan con esta exigencia derivada del RGPD.

- Al tratarse de una tecnología en la que no existen fronteras, los diversos actores implicados pueden estar radicados en diferentes lugares del planeta, lo que podría derivar en una transferencia internacional de datos que debería tener un marco regulatorio apropiado.

También en lo relativo a la protección de datos, la utilización de la tecnología *blockchain* por parte del sector asegurador exigirá, entre otros aspectos, garantizar el cumplimiento de las obligaciones establecidas en el RGPD, incluyendo en materia de confidencialidad de los datos, de limitación del tratamiento o de derechos de los interesados, cuando fuesen exigidos por estos, todo lo cual, *a priori*, entra en conflicto con la propia naturaleza de esta tecnología. Para salvarlo, la compañía de seguros tendrá que acudir al despliegue de redes privadas, dado que las características de estas redes facilitan el cumplimiento con la normativa de protección de datos, ya que, en la medida en que sus propietarios deciden quién puede participar en ella, resulta más fácil identificar el papel de cada sujeto interviniente en el tratamiento de los datos.

Igualmente deberán acudir, sobre todo, a la utilización de técnicas de anonimización, en los términos expuestos por la AEPD en las "Orientaciones y garantías en los procedimientos de anonimización de datos personales"[24].

24 Disponible en https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf (última revisión el 11 de octubre de 2021).

VIII. Conclusión

Tecnologías como la *blockchain*, la inteligencia de datos (*big data*), el *IoT* o la IA ofrecen incontables posibilidades a las empresas para ofrecer sus servicios de manera mucho más eficiente, personalizada y competitiva, si bien supone, en la mayoría de los casos, retos jurídicos en relación al tratamiento de los datos de los asegurados. No obstante, como hemos expuesto en este artículo, tanto la normativa general, desarrollada en el RGPD y en la LOPDGDD, como la especial en esta materia, concentrada en la LOSSEAR, exponen el marco jurídico que deberá respetar una compañía aseguradora cuando realice tratamientos singulares de datos, normativa que, junto con el futuro Reglamento de Inteligencia Artificial y las guías publicadas por la AEPD, ofrecerán directrices suficientes para poder llevar a cabo estos complejos tratamientos de datos personales con garantías y seguridad jurídica.