ddoctrinaa

La protección de datos en el ámbito del seguro

Ana Isabel Caballero Ferrer
Abogada

SUMARIO

I. OBJETO, FINALIDAD Y MEDIOS DEL ESTUDIO

La realidad, en el mundo actual ampliamente informatizado en el que nos movemos, es que no somos conscientes del valor de nuestros datos personales y del creciente riesgo que supone el uso inconsentido de los mismos por terceros ajenos a su titular. Ya lo advirtió nuestro Tribunal Constitucional al indicar *"(..) Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin (...)"*[1]

Nuestro legislador constitucional fue pionero en la defensa y protección de datos personales al otorgar rango de derecho fundamental el derecho al honor, a la intimidad personal y a la propia imagen en el artículo 18 de nuestra Carta Magna. Más aún, con un carácter visionario y previsor, nuestra Constitución ya advertía del auge de la informática y de las consecuencias que, en el ámbito de este derecho fundamental, se podría acarrear si no se protegiesen debidamente los datos personales.[2]

Así, como un medio para preservar y garantizar el derecho fundamental al honor y la intimidad personal y familiar, el artículo 18.4 de la CE promulga el derecho a la protección de datos personales: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

Nuestro Tribunal Constitucional, en sentencia del Pleno núm. 292/2000 de 30 de noviembre de 2000 se encargar de y explicar la función, objeto y contenido del derecho a la protección de datos y diferenciarlo del derecho a la intimidad del art. 18.1 de la CE: *"(...) Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 C.E. debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 C.E.), bien regulando su ejercicio (art. 53.1 C.E.). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.*(...)"

Así, en palabras de nuestro Tribunal Constitucional, la función del derecho a la protección de datos es *"(...) garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, F.J. 5; 144/1999, F.J. 8; 98/2000, de 10 de abril, F.J. 5; 115/2000, de 10 de mayo, F.J. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. (....)"*

Más de 45 años después de la entrada en vigor de nuestra Constitución, el avance de la informática ha experimentado un auge quizá inimaginable para el legislador constitucional,

1 Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000.

2 Sentencia del Pleno del TC num.292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000.

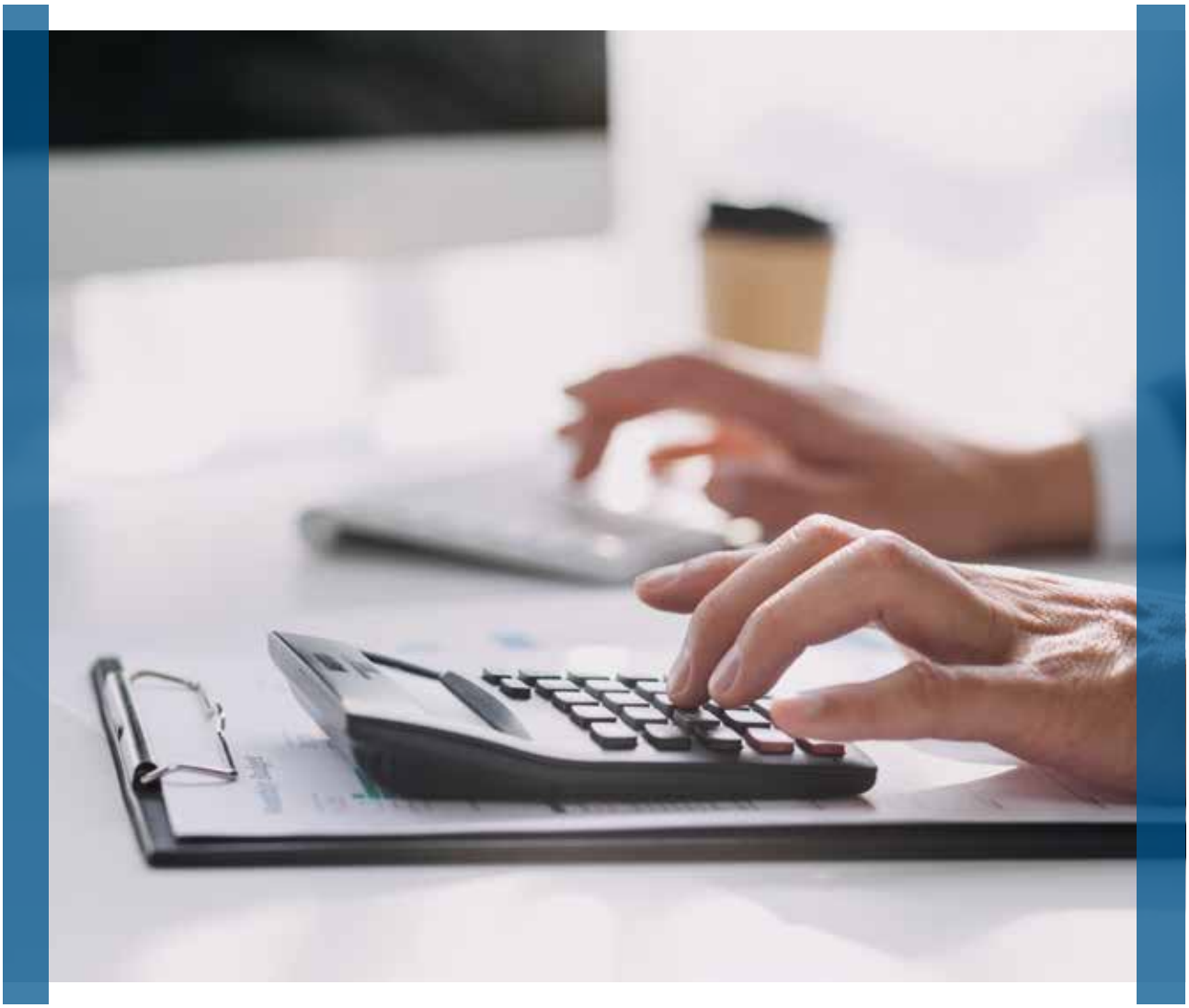
"(...) Ahora bien, con la inclusión del vigente art. 18.4 C.E. el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, F.J. 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 C.E. y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 C.E. no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.(...)"

pero sentó las bases normativas para que nuestro legislador pudiera proteger sobradamente el derecho a la protección de datos (primero con la LORTAD, posteriormente con la LOPD y actualmente con la LOPDGDD)

Basta echar un vistazo a la Memoria 2023 publicada por la Agencia Española de Protección de Datos[3] (la de 2024 aún no se ha publicado) para darse cuenta del auge de reclamaciones y, por ende, de sanciones que ha impuesto la citada Autoridad en el 2023, batiendo su record con un total de 22.348 reclamaciones, lo que supone un 43% más que las reclamaciones recibidas en el año anterior. Por áreas de actividad y procedimientos sancionadores, destaca-

3 Sentencia del Pleno del Tribunal Constitucional núm. 290/2000, de 30 de noviembre de 2000.Competencia sobre derechos fundamentales y la Agencia de Protección de Datos.

"(...) En efecto, al dar cumplimiento al mandato contenido en el art. 18.4 C.E., el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, como se determina en los apartados 2 a 5 del art. 17 L.O.R.T.A.D., no ha querido sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental. Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la L.O.R.T.A.D. le atribuye y, en su caso, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos (art. 17.1), las que provocarán la posterior actuación de este órgano. Por lo que cabe estimar que existe una correspondencia entre las funciones y potestades que la L.O.R.T.A.D. ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones. Pues es este carácter tuitivo o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada.(...)"



mos la Publicidad (spam email/SMS) con 28 procedimientos sancionadores, Contratación fraudulenta con 27 procedimientos sancionadores, Asuntos laborales con 18, Publicidad (excepto spam) con 14 y brechas de seguridad con 14 procedimientos sancionadores.

Traducido al ámbito asegurador, la confluencia, tratamiento y transmisión de datos personales es bastante elevada lo que obliga, por un lado a extremar una cautela para poder dar cumplimiento al derecho fundamental de protección de datos personales (artículo 18.4 C.E) pero, por otro, permite al sector asegurador rentabilizar el conocimiento de dichos datos desde un punto de vista empresarial.

La Agencia Forward analiza en un artículo publicado en Marzo de 2024[4] el análisis de datos para el sector asegurador indicando al respecto: *"Los avances en la disponibilidad de datos y la tecnología son los principales impulsores de la escala y la velocidad con la que las empresas pueden utilizar el análisis de datos en su beneficio en la actualidad."* previniendo fraudes mediante el uso de la IA (inteligencia artificial) y el análisis de enlace de datos, rentabilizando la utilización del marketing, y análisis predictivo *"identificando riesgos y adaptando las ofertas de manera más eficiente".*

El sector asegurador tiene acceso y tratamiento de un amplio espectro de datos personales, en la mayoría de las ocasiones con la consideración de categorías especiales de datos (artículo 9 del RGPD), lo que nos lleva a concluir que el cumplimiento por el sector asegurador del tratamiento de datos personales ha de ser más exigente. A tal efecto, las compañías aseguradoras *"se han puesto las pilas"* publicando códigos de conducta[5] y creando organismos de supervisión a fin de garantizar el derecho a la protección de datos de los interesados. Por su parte, el legislador ha promulgado una amplia normativa sectorial que regula esta materia y que tendremos ocasión de analizar y referenciar ampliamente en este artículo.[6]

En el ámbito del seguro, el tratamiento de datos personales va más allá de la mera contratación. Así, las historias clínicas son necesarias para cualquier compañía aseguradora a raíz de un accidente de tráfico a fin de conocer los antecedentes médico-sanitarios que pudieran influir a la postre en la valoración médica derivada de cualquier siniestro. También son objeto de solicitud y aportación en procesos judiciales.

Por ello, haremos una especial parada en el tratamiento de datos personales de salud, en su consideración como dato sensible especialmente protegido tanto por la legislación europea (RGPD) como nacional (LOPDGDD, Ley de Mediación de Seguros y Reaseguros Privados, Ley de Ordenación, Supervisión y Solvencia de las entidades aseguradoras y reaseguradoras y LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico).

Por tanto, el objeto y finalidad de este artículo es realizar un recorrido lo más extenso y detallado posible, por todos los campos del ámbito del seguro en el que aparezca un tratamiento de datos personales, tratando de ofrecer una visión pragmática desde el plano normativo, jurisprudencial y doctrinal en la materia

4 AGENCIA FORWARD. *"Tendencias de 2024 en análisis de datos para seguros"* 1 de marzo de 2024

5 UNESPA. "Código de Conducta regulador del tratamiento de datos personales en los sistemas comunes de información del sector asegurador" de 12 de Abril de 2022. Aprobado por la AEPD en resolución dictada en Expediente Nº CC/0012/2019.

6 -Reglamento Delegado (UE) 2015/35 de la Comisión, de 10 de octubre de 2014 por el que se completa la Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II).

-Reglamento (UE) nº 1286/2014 del Parlamento Europeo y del Consejo, de 26 de noviembre de 2014, sobre los documentos de datos fundamentales relativos a los productos de inversión minorista vinculados y los productos de inversión basados en seguros.

-Directiva (UE) 2016/97 de 20 de enero de 2016 sobre la distribución de seguros.

-Reglamento Delegado (UE) 2017/2358 de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de control y gobernanza de los productos aplicables a las empresas de seguros y los distribuidores de seguros.

-Reglamento Delegado (UE) 2017/2359 de la Comisión, de 21 de septiembre de 2017, por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de información y las normas de conducta aplicables a la distribución de productos de inversión basados en seguros.

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

-Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

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

-Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor.

-Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados.

-Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI-CE)

sin olvidar los informes y resoluciones de las autoridades en protección de datos (Agencia Española de Protección de Datos y Supervisor Europeo de Protección de Datos).

II. BREVE INTRODUCCIÓN AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

2.1 Conceptos

Nuestro RGPD define en su artículo 4 los datos personales como *"Toda información sobre una persona física identificada o identificable ("el interesado"). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

No debe llevarnos al equívoco pensar que los datos personales se limitan al nombre y apellidos de una persona o una fotografía, el concepto se extiende a toda información sobre una persona física identificada o identificable por datos como pueden ser la matrícula de un vehículo o los datos que aparecen en una dirección IP.[7]

El sujeto protegido es una persona física (salvo datos tratados en el ámbito doméstico), excluyéndose a las personas jurídicas[8] y personas fallecidas[9] (estas últimas solo para el Reglamento Europeo de Protección de Datos pues según el Dictamen 4/2007 del Grupo de Trabajo del artículo 29[10] los fallecidos dejan de tener la consideración de personas físicas para el Derecho Civil) pues en cambio, en el marco competencial de los Estados Miembros, nuestra LOPDGDD sí regula el tratamiento de datos de personas fallecidas en su artículo 3.

Para que sea objeto de regulación, no basta con la existencia de datos personales sino que es necesario que exista tratamiento de datos personales pues, en palabras de TRONCOSO REIGADA, el riesgo se produce cuando se tratan datos personales.

El tratamiento de datos personales es definido en el artículo 4 del RGPD como *"Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."*

Además, existen tratamientos específicos como los de la elaboración de perfiles[11] para los que el Reglamento Europeo plantea obligaciones adicionales como, por ejemplo, realizar evaluaciones de impacto.

Trasladado al ámbito asegurador, el tratamiento de datos personales se produce no solo por las compañías aseguradoras al recibir datos del interesado e incorporarlos a su base de datos con fines contractuales, sino también por parte de las Fuerzas y Cuerpos de Seguridad del Estado que intervienen en la elaboración de un Atestado por accidente de circulación o por los servicios sanitarios que atienden a todos los implicados en un siniestro de circulación. Incluso hay tratamiento de datos por los peritos que elaboran informes derivados de siniestros o por los servicios de grúa.

Todo ello hace que, de forma indispensable, sea objeto de análisis en este artículo no sólo el tratamiento de datos por los responsables y encargados del mismo, sino también la cesión de datos entre los distintos agentes que hemos

7 Informe Jurídico de la AEPD 327/2003 sobre el carácter de dato personal en la dirección IP

8 Considerando 14 RGPD: *"(...) El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto."*

9 Considerando 27 RGPD: *"El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas."*

10 El Grupo de Trabajo del artículo 29, creado por la Directiva 95/46/CE, fue un órgano consultivo independiente formado por las autoridades nacionales en materia de protección de datos, el Supervisor Europeo en protección de datos y la Comisión Europea. Con el RGPD este organismo ha sido sustituido por el Comité Europeo de Protección de Datos, pero sus informes siguen teniendo actual relevancia

11 Art. 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"*

mencionado, siempre que se realice sobre una base de legitimación, como vamos a tener ocasión de detallar en este estudio.

A modo de ejemplo podemos citar los Informes de la AEPD 0411/2010 o 2009/0006 que versan sobre la consulta planteada en relación a la cesión de datos personales relativos a accidentes de tráfico a las compañías aseguradoras o abogados defensores de los implicados en ellos.

Es indispensable en este punto citar los principios generales que deben cumplirse en todo tratamiento de datos personales y que contiene el artículo 5 del RGPD:

Licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad.

2.2 Origen del Derecho a la Protección de Datos

La Declaración de Derechos Humanos de 10 de Diciembre de 1948 proclama en su artículo 12 que *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."* Así lo hacen también el Pacto Internacional de Derechos Civiles y Políticos de 16 de diciembre de 1966 en su artículo 17[12] o el Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950 en su artículo 8[13].

Más recientemente nos encontramos con el Convenio 108 del Consejo de Europa el 28 de enero de 1981[14] actualizado mediante el denominado Convenio 108 Plus (convenio 223 de 18-05-2018 del Comité de Ministros del Consejo de Europa).

Deberían pasar unos años para que se promulgara la Carta de Derechos fundamentales de la Unión Europea de fecha 7 de diciembre de 2000[15] en la que ya se menciona de forma al derecho a la protección de datos de carácter personal.

La regulación normativa europea en materia de protección de datos comenzó con la Directiva 95/46/CE de 24 de octubre de 1995 (que estuvo vigente en España desde el 13 de diciembre de 1998) y que fue derogada por el actual Reglamento (UE) 2016/679 de 27 de abril de 2016, el cual entró en vigor en España tras una prolongada vacatio legis el día 25 de mayo de 2018.

En el ámbito nacional, la protección de datos arranca con la Constitución Española de 1978. Habría que esperar hasta la LO 5/1992 de regulación del tratamiento automatizado de datos de carácter personal. Tras la adopción de la Directiva 95/46/CE por España fue necesario su trasposición al ordenamiento jurídico español mediante la LO 15/1999 de protección de datos de carácter personal (LOPD) y su reglamento de desarrollo aprobado mediante RD 1720/2007. Ambos textos normativos han sido prácticamente derogados en su totalidad por la LO 3/2018 de 5 de diciembre de protección de datos personales y garantía de derechos digitales.

También se aprobaron diversas leyes sectoriales que comenzaron a regular discretamente el derecho a la protección de datos tales como la Ley 11/1998 General de Telecomunicaciones (derogada por la Ley 32/2003 que a su vez está derogada por la actual Ley 9/2014 General de Telecomunicaciones), la Ley 34/2002 de Servicios de la Sociedad de la Información, la Ley 59/2003 de firma electrónica, la ley 10/2020 de prevención del blanqueo de capitales y de la financiación del terrorismo, la Ley 4/1997 que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado, la ley 41/2002 regu-

12 Art 17.1. *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

13 Art. 8:*" 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

14 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981.

15 Art. 8 de la CDFUE: *"Protección de datos de carácter personal. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. El respeto de estas normas estará sujeto al control de una autoridad independiente."*

ladora de la autonomía del paciente, la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas, la Ley 56/2007 de medidas de impulso de la sociedad de la información, la Ley 9/2017 de contratos del sector público, o la LOPJ en su reforma de 2015.

En cuanto a las comunidades autónomas, hasta la presente sólo cuatro han regulado normativamente la protección de datos: Andalucía (Ley 1/2014 de Transparencia Pública de Andalucía), Madrid (Ley8/2001 de protección de datos que ha sido derogada por la Agencia de Protección de Datos de Madrid), País Vasco (ley 2/2004 que creó la Agencia Vasca de Protección de Datos) y Cataluña (Ley 32/2010 que creó la autoridad catalana de protección de datos).

2.3 Regulación del derecho a la protección de datos en el sector asegurador

En el marco de la atribución de competencias que realiza el RGPD al derecho de la Unión o de los Estados Miembros para regular de forma más específica el tratamiento de datos personales basado en el cumplimiento de obligaciones legales, nos encontramos con los siguientes textos legislativos en el ámbito asegurador:

- Reglamento Delegado (UE) 2015/35 de la Comisión, de 10 de octubre de 2014, por el que se completa la Directiva 2009/138/CE, así como los reglamentos comunitarios de ejecución de solvencia II.

- Reglamento (UE) 1286/2014, de 26 de noviembre de 2014, sobre los documentos de datos fundamentales relativos a los productos de inversión minorista vinculados y los productos de inversión basados en productos de seguros.

- Reglamento Delegado (UE) 2017/2358, de 21 de septiembre por el que se completa la Directiva 2016/97 en lo que respecta a los requisitos de control y gobernanza de productos de seguros.

- Reglamento Delegado (UE) 2017/2359 de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de información y las normas de conducta aplicables a la distribución de productos de inversión basados en seguros.

- Directiva UE 2016/97 sobre la distribución de seguros.

Por su parte, entre la normativa del Estado español destacamos los siguientes cuerpos legales:

- Ley 50/1980, de 8 de octubre, de Contrato de Seguro (En adelante "LCS").

- Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (en adelante "LOSSEAR").

- Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de entidades aseguradoras y reaseguradoras (en adelante "RDOSSEAR").

- Real Decreto Legislativo 8/2004, por el que se aprueba el texto refundido de la ley de responsabilidad civil y seguro en la circulación de vehículos a motor (en adelante "TRLRCSCVH ").

- Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros.

- Ley 20/2015, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

III. CATEGORÍAS ESPECIALES DE DATOS PERSONALES. DATOS SENSIBLES. ESPECIAL TRATAMIENTO Y PROTECCIÓN

3.1 Concepto

El artículo 9.1 del RGPD[16] considera datos sensibles aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física y prohíbe su tratamiento salvo que

16 Art. 9.1 RGPD *"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física."*

confluyan determinadas circunstancias que nos encargaremos de analizar.

Por su parte, nuestra LOPDGDD trata esta categoría especial de datos personales en su Título II[17], y más concretamente en su artículo 9[18], el cual establece una reserva especial para que, en el ámbito de la salud, el tratamiento esté amparado no solo en el RGPD sino en una norma con rango de ley que refuerce la seguridad y confidencialidad de datos sensibles relativos a la salud en el ámbito de la asistencia sanitaria o en la ejecución de un contrato de seguro.

El objeto de estudio de este apartado va a ser la protección y tratamiento de datos sensibles no sólo desde la perspectiva de la asistencia médico-sanitaria (y especial detenimiento en la historia clínica) sino también desde la perspectiva de la ejecución del contrato de seguro.

3.2 Prohibición genérica de tratamiento de datos personales sensibles. Excepciones

Empezaremos diciendo que los datos de salud, al tratarse de datos sensibles, son protegidos impidiéndose con carácter general su tratamiento por el art. 9.1 del RGPD, salvo que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD:

-Consentimiento explícito del interesado salvo que el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.

-Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del Derecho laboral y de la seguridad y protección social.

-Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

-Que el tratamiento sea efectuado por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

- Que el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos.

-Que el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

-Que el tratamiento sea necesario por razones de un interés público esencial

-Que el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los siste-

17 En la Exposición de motivos de la LOPDGDD se indica lo siguiente: *"(...) En relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos(....)"*

18 LOPDGDD. ***Artículo 9. Categorías especiales de datos.***

"1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte."

mas y servicios de asistencia sanitaria y social.

-Que el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública,

-Que el tratamiento sea necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

El art. 9.4 del RGPD establece una reserva para que los Estados miembros puedan mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos personales sensibles.

3.3 Clasificación de datos sensibles. Especial referencia a los datos relativos a la salud, datos genéticos y datos biométricos

De todos los datos personales sensibles enumerados en el artículo 9 del RGPD, van a ser objeto de análisis en este apartado los datos relativos a la salud, los datos genéticos y los datos biométricos ya que los mismos, como vamos a tener ocasión de exponer, guardan especial incidencia con el ámbito del sector de seguros.

a) Datos relativos a la salud.

El artículo 4 del RGPD, en su apartado 15, define los datos relativos a la salud como *"datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"*. Por su parte, el considerando 35 del RGPD[19] establece una definición y enumeración de datos personales relativos a la salud, determinando que por datos de salud deben considerarse no solo aquellos que den información sobre el estado de salud física o mental pasado, presente o futuro del interesado sino además toda información recogida a efectos de la formalización o prestación de asistencia sanitaria de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo.

Entre la enumeración de datos personales de salud el RGPD incluye pruebas o exámenes incluida la procedente de datos genéticos y muestras biológicas, información relativa a enfermedad, discapacidad, historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado.

19 Considerando 35 RGPD: " *Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ( ); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro."*

Los datos de salud deben ser conceptuados en sentido amplio, extendiéndose a aquellos datos de carácter tanto físico como psíquico, de personas tanto vivas como fallecidas. Se extienden también a datos relativos al consumo de alcohol o de drogas o datos de salud que incidan en el alta o baja laboral.

Por su parte la AEPD define datos de salud[20] como *"los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud". También son datos de salud los datos genéticos que son aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.*

Por tanto, los datos personales existentes en bases de datos sanitarias son de dos tipos: los que identifican a la persona, tales como nombre y apellidos, dirección, teléfono, DNI, número de tarjeta sanitaria, etc...; y toda la información acerca de su estado de salud, tales como pruebas diagnósticas, cirugías, medicamentos, antecedentes familiares, etc."

Es decir, son datos relativos a la salud no solo los datos que identifican a una persona (Nombre, apellidos, número de afiliación sanitaria, etc) sino los relativos a la salud de esta (pruebas diagnósticas, intervenciones quirúrgicas, antecedentes de salud, etc).

En palabras de la Sociedad española de Salud Pública y Administración Sanitaria (SESPAS) *"los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por otros puede menoscabar el desarrollo de la personalidad, como lo son la orientación sexual, el padecimiento de enfermedades psiquiátricas o de transmisión sexual, embarazos interrumpidos, fertilidad, ser alcohólico o ex-alcohólico, drogadicto, determinadas discapacidades, portador de VIH, etc. Su tratamiento puede provocar que el responsable o un tercero que ha accedido a los datos vulnere derechos fundamentales del titular de los datos,particularmente, el derecho a la no discriminación. De ahí que los datos de salud disfruten de un estatuto jurídico particular dada su calificación como categoría especial de dato."*

Antes de la entrada en vigor del RGPD (Mayo 2018), en nuestro país ya se encargaban de proteger los datos personales relativos a la salud de los pacientes, entre otras, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP), la Ley 16/2002, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud (LCCSNS), la Ley 14/2007, de 3 de julio, de Investigación biomédica (LIB), la Ley 33/2011, de 4 de octubre, General de Salud Pública (LGSP), o el Real Decreto 1090/2015, de 4 de diciembre, que aprueba el reglamento de ensayos clínicos con medicamentos, así como diversas leyes autonómicas.

También la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD), que fue sustituida por la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) hacía una mención especial a los datos de salud en sus artículos 7 y 8.

Sin embargo, existía una notable falta de armonía entre la Ley básica de autonomía del paciente (LBAP) y la derogada LOPD de 1999. En palabras de Juan Luis Beltrán Aguirre, Fernando José García López y Carmen Navarro Sánchez: *"Conviene significar la falta de armonía entre ambas. La primera contempla una relación clínica en la que el protagonismo lo tiene la continuada información, oral o escrita, al paciente y la recopilación y tratamiento de la información obtenida en aras de la mejor asistencia posible. La segunda sitúa la información obtenida sobre la salud de las personas en el nivel máximo de discreción y protección1. En cuanto a la protección de los datos de salud, ambas leyes se hacen remisiones mutuas, lo que ha generado lagunas en su regulación. La literal aplicación de ambas leyes en ocasiones puede llevar a actos irregulares según la ley desde la que se analiza el acto en cuestión.".*

La incidencia de los datos de salud en el sector de seguros es bastante elocuente. Sólo en el ámbito de la contratación, los datos relativos a la salud que deben manejarse para contratar un seguro relativo a la salud (Seguro sanitario, seguro de vida, etc) hace que las entidades aseguradoras deban extremar las medidas de precaución en su calidad de datos sensibles de especial protección. No en vano, tal y como indica la *AEPD "De acuerdo con los últimos datos del segundo semestre de 2021, el 15% de las notificaciones de brechas recibidas en la Agencia las realizaron responsables del tratamiento*

20 "Guía para pacientes y usuarios de la sanidad" AEPD, Noviembre de 2019.

cuyo sector de actividad principal es el asistencial en el ámbito de la salud."[21]

En palabras de DE MIGUEL SÁNCHEZ "(...) Es *ineludible la necesidad de disponer de una ley específica sobre protección de datos personales relativos a la salud; ley que, por ende, se enmarcaría en la normativa del sector sanitario*".

La Sociedad Española de Salud Pública y Administración Sanitaria también se hace eco de esta cuestión al señalar que: *"Hoy es opinión generalizada que lo más operativo es elaborar una ley estatal para la protección de los datos personales de salud, que complemente el RGPD y sustituya a las disposiciones contenidas en la todavía vigente LOPD, en la LBAP, y en el resto de legislación sanitaria estatal (...)"*

b) Datos genéticos.

Los datos genéticos se encuentran incluidos dentro de los datos de salud y revelan características físicas, incluso étnicas, que los conforman como datos especialmente protegidos.

El art. 4.13 del RGPD define los datos genéticos como aquellos datos personales *"(...) relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona(...)"* encargándose de precisar el considerando 34 de dicho cuerpo legal qué tipo de análisis extraen la muestra biológica "(...) *en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.(...)".*

Según Jesús Jiménez López, Director del Consejo de Transparencia y Protección de Datos de Andalucía España, *"se incluyen dentro del concepto de datos genéticos tanto los inicialmente adquiridos antes del nacimiento como los adquiridos durante la vida de una persona o de su familia genética".*

La información genética comporta aspectos muy positivos como información científica, médica y personal tanto actual no solo del titular de la muestra, sino también de los familiares consanguíneos incluso fallecidos, pero también puede suponer una injerencia a las libertades fundamentales y al respeto de la dignidad humana.[22]

El Consejo de Europa ya estableció en el año 2015 que los datos genéticos solo pueden permitirse de forma excepcional, por ejemplo para prohibir daños graves a la salud del interesado o de terceros. Se indicaba igualmente que tanto los datos genéticos como los relativos a la salud de las personas precisan la adopción de medidas técnicas y organizativas precisas para conseguir un acceso restringido a dichos datos.

Es por ello que los datos genéticos deben ser tratados con unas limitaciones y solo con unas finalidades legítimas de tratamiento, que son:

- Diagnóstico y asistencia sanitaria.

- Investigación científica

- Medicina forense y procedimientos civiles o penales u otras actuaciones legales.[23] En este caso, la base de tratamiento debe ser o bien el consentimiento del interesado o bien el interés público sustancial (Art. 9.2.g del RGPD y Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policiales sobre identificadores obtenidos a partir del ADN.

- Consentimiento del interesado para la realización de pruebas y exámenes genéticos con fines de atención médica con el fin de

21 https://www.aepd.es/areas-de-actuacion/salud/brechas-de-datos-personales-en-el-sector-de-la-salud

22 ALVAREZ GONZALEZ (2017. p. 26)," *la garantía de los derechos fundamentales se asienta en la capacidad de la persona de determinar el grado y alcance de la utilización de su información genética. La posibilidad de perfilado genético, y su utilización, se ha incrementado como consecuencia de una mayor capacidad tecnológica, en cuando a cantidad de datos tratados, no solo genéticos, respecto de los cuales se extraen inferencias, por los algoritmos empleados, en su caso integrando sistemas de inteligencia artificial, y por la capacidad de computación. El perfilado, la predicción de comportamientos, también sobre el estado y evolución de la salud de las personas, se anudan a consecuencias que necesariamente han de afectarles."*

23 Art. 12 de la Convención para la salvaguardia del patrimonio cultural inmaterial UNESCO 03/11/2003, relativo a la Recolección de muestras biológicas con fines de medicina forense o como parte de procedimientos civiles o penales u otras actuaciones legales dispone: *"Cuando se recolecten datos genéticos humanos o datos proteómicos humanos con fines de medicina forense o como parte de procedimientos civiles o penales u otras actuaciones legales, comprendidas las pruebas de determinación de parentesco, la extracción de muestras biológicas, in vivo o post mortem, sólo debería efectuarse de conformidad con el derecho interno, compatible con el derecho internacional relativo a los derechos humanos"*

preservar y garantizar el derecho de autodeterminación.[24]

- No discriminación y prohibición de estigmatización. En el ámbito asegurador, por poner un ejemplo, por cuanto por determinadas características genéticas, en una contratación de seguro de salud podría tener relevancia en la determinación de las primas.

c) Datos biométricos.

- El art. 4.14 del RGPD considera como datos biométricos aquellos datos personales dirigidos a identificar de manera unívoca a una persona *"(...) obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (...)"* Otros ejemplos pueden ser los modelos retinales, estructuras venosas, estructuras óseas o geometría de la mano. Pero, insistimos, solo tienen la consideración de categoría especial aquellos datos biométricos que permitan identificar de forma unívoca a una persona.

Las fotografías solo son consideradas como dato biométrico[25] cuando sean tratadas por medios específicos que permitan la identificación o autenticación unívoca de una persona.

La especial protección, como dato sensible, que le otorga el RGPD se basa en palabras de la AEPD en que " *Los tratamientos que incluyen operaciones con datos biométricos se pueden emplear con muchas finalidades: prueba de vida, identificación, autenticación, seguimiento, perfilado, decisiones automáticas, etc. Las operaciones biométricas pueden emplear distintas técnicas, algunas de forma simultánea, y, a su vez, una misma técnica se puede implementar de formas diferentes. Las operaciones con datos biométricos en un tratamiento concreto tendrán un grado distinto de intrusión e impacto en la privacidad de los individuos que dependerá de la técnica empleada, pero también de la propia definición del tratamiento, su naturaleza, el ámbito o alcance en el que se va a desarrollar, su contexto y, en especial, los fines que se persiguen. Por lo tanto, la evaluación de impacto de las operaciones biométricas se ha de realizar en el marco de un tratamiento y con relación a sus fines últimos."*

La AEPD analiza en su Guía *"Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos"* [26] algunos de los criterios que pueden ser útiles para incluir las operaciones biométricas en el marco de un tratamiento, así como el ámbito o alcance del tratamiento, etc.

En cualquiera de los casos se debe atender al principio de minimización de tratamiento de este tipo de datos personales. Así, *"si el tratamiento tiene como consecuencias efectos jurídicos en el interesado o le afecta significativamente y el resultado de la operación biométrica, el art.22 del RGPD establece prohibiciones y garantías adicionales, entre ellas la posible intervención humana cualificada."*

La AEPD se ha encargado de analizar este tipo de datos personales en varios informes como el número 10318/2019 del Gabinete Jurídico de la AEPD en respuesta a una consulta sobre la licitud de sistemas de reconocimiento facial en los servicios de videovigilancia de empresas seguridad privada, el Informe 36/2020 que versa sobre la utilización del reconocimiento facial para realizar exámenes o el Informe 368/2006 que se encargó de analizar la proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio.

---

24 La Recomendación núm. 92 del Comité de Ministros a los estados miembros Pruebas y exámenes genéticos con fines de atención médica, de 10 de febrero de 1992, se habla del principio de autodeterminación indicando al respecto: *"La prestación de servicios genéticos deberá basarse en el respeto al principio de la autodeterminación de las personas interesadas. Por este motivo, cualquier prueba genética, incluso cuando se ofrezca de manera sistemática, deberá estar sujeta al consentimiento expreso, libre e informado de la misma. b. Estará sujeta a especiales medidas de salvaguardia la realización de pruebas a las siguientes categorías de personas: — Menores de edad. — Personas que sufran trastornos mentales. — Adultos que se encuentren bajo tutela limitada. La realización de pruebas a dichas personas con fines de diagnóstico únicamente se permitirá cuando ello sea necesario para su propia salud o si la información fuese absolutamente necesaria para diagnosticar la existencia de una enfermedad genética en familiares. Será necesario el consentimiento de la persona que vaya a ser sometida a la prueba, salvo cuando la legislación nacional disponga otra cosa"*

25 *.Considerando 51 del RGPD: "(...) El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando* el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

26 "Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos" AEPD 26 de Julio de 2022. https://www.aepd.es/prensa-y-comunicacion/blog/datos-biometricos-evaluacion-perspectiva-proteccion-datos

También la AEPD ha emitido una Guía relativa a la Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial.

3.4 Especial referencia a la Historia Clínica

Toda la información personal y de salud de una persona constituye la denominada *"Historia clínica"* y está regulada en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LAP), la cual la define como *"El conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".*

Como dato personal sensible, en cuanto que contiene datos relativos a la salud, está especialmente protegido por el RGPD, permitiéndose su tratamiento y cesión solo en los casos determinados en el artículo 9.2 RGPD como tuvimos ocasión de analizar anteriormente.

En palabras de LÓPEZ Y GARCÍA DE LA SERRANA, *"La exigibilidad del consentimiento de los pacientes para el tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el denunciado pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o su comunicación a la contraparte, puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho."*[27]

De todos los accesos permitidos, destaca la del cumplimiento de obligación de prestación de la debida asistencia sanitaria (Apartados 3 y 2 h). Pero aún así, la historia clínica permitiría el acceso a miles de profesionales sanitarios, en el caso de las historias clínicas electrónicas, si no se adoptaran las debidas cautelas.[28]

Ello entronca con el deber de confidencialidad (artículo 5.1.f) del RGPD y art. 5 de la LOPDGDD y el deber de secreto profesional (artículo 5.2 LOPDGDD) como uno de los principios esenciales en la relación entre profesionales sanitarios y pacientes. Así lo señalan el artículo 9.3 del RGPD, el artículo 10.3 la Ley 14/1986, de 25 de abril, General de Sanidad y los artículos 7.1 y 16.6 de la LAP.

---

27 LÓPEZ Y GARCIA DE LA SERRANA, JAVIER. "Compatibilidad entre el derecho de defensa y la protección de datos" 8º Congreso Jurídico de la Abogacía Malagueña 18 y 19 de octubre de 2012

Compatibilidad entre el derecho de defensa y la protección de datos

28 En palabras de la profesora Andrea Casanova Asencio, *"la historia clínica electrónica ha sido vista como una herramienta que asegura una mayor protección de los datos que la historia clínica en papel, por imponer la necesidad de identificación para el acceso y la trazabilidad de los mismos"* . Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias INDRET, Barcelona 2019

Para TRONCOSO REIGADA, "la mejor manera de velar por la seguridad de los datos clínicos es su traslado a soportes informáticos" (TRONCOSO REIGADA, 2006, pp. 84, 85, 137, 142).

Este deber de confidencialidad se extiende a toda persona que tenga acceso a los datos contenidos en las historias clínicas, (no solo por tanto de aquellas profesiones sujetas al deber de secreto profesional), tal y como dispone el artículo 2.7 LAP.

La Ley 41/2002 de autonomía del paciente garantiza en su artículo 7.1 que nadie pueda acceder a los datos referentes a la salud de las personas sin la debida autorización amparada por la Ley. A tal efecto, dicha autorización legal se encuentra en el artículo 16 de dicho cuerpo legal el cual determina las finalidades que justifican el acceso a la historia clínica.

Pues bien, entre las finalidades recogidas por el artículo 16 LAP se destacan, como las más frecuentes y comunes, la finalidad asistencial (art. 16.1); el acceso con fines de investigación, docencia, epidemiología, de salud pública, o judicial (art. 16.3).

A) Acceso a la historia clínica con finalidad asistencial.

Es la finalidad más común por cuanto la historia clínica aparece como elemento necesario e inherente al tratamiento médico, pues así lo indica el Informe SESPAS de 2017.[29]

El acceso con finalidad asistencial es considerado para numerosos autores como un principio: el de vinculación asistencial, el cual unido al principio de proporcionalidad, marcan las pautas de porqué y en qué medida pueden acceder los profesionales sanitarios a las historias clínicas de sus pacientes.[30]

Este acceso a la historia clínica del paciente se configura a su vez como un deber del personal sanitario, garantizado por el artículo 16.2 LAP, quien está obligado a acceder a dichos datos para prestar su servicio adecuadamente y, a su vez, desde la vertiente del paciente, se corresponde con su deber de facilitar sus datos sanitarios de manera veraz (art. 2.5 LAP).

Sin embargo, el acceso debe realizarse con pleno respeto a los principios de minimización de datos, veracidad y exactitud, limitación del tratamiento y proporcionalidad. Existen multitud de resoluciones judiciales con pronunciamientos condenatorios respecto del acceso extralimitado a la historia clínica por parte de distintos profesionales de la salud, de las que extraemos la sentencia del TSJ de Navarra, Sala de lo Contencioso-Administrativo, de fecha 08/02/2012 en la que se condena al Servicio Navarro de Salud al haberse registrado 2.825 accesos a la historia clínica de una paciente por parte de 417 usuarios integrados en 55 servicios. También destacamos en la jurisdicción civil la sentencia del Tribunal Supremo, Sala 1ª, de fecha 27/01/1997 (Roj 452/1997) que condena al centro sanitario por haberse producido quiebras de seguridad al haber dejado desatendida la documentación clínica de un paciente, que pasó a mano de terceros ajenos al servicio sanitario.

Es en la jurisdicción penal donde más pronunciamientos condenatorios existen por delito de revelación de secretos en sentencias como las del Tribunal Supremo, Sala 2ª, de fecha 04/04/2001 (RJ 2001/2016), o la sentencia de la misma sala de fecha 18/10/2012 (RJ 2012/1437) llamativa por condenar a un personal del cuerpo de gestión de un hospital por acceder a más de 5.000 historias clínicas sin justificación, o la sentencia del Tribunal Supremo, Sala 2ª también, de 03/02/2016 (Roj 185/2016) que condena a un facultativo por acceder hasta en 171 ocasiones a las historias clínicas de su ex pareja y de la familia de ésta.

B) Acceso a la historia clínica con fines judiciales.

El artículo 118 de la Constitución Española señala que *"Es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos"*

Por su parte, como hemos visto, el art. 9.2.f) RGPD permite el tratamiento de datos personales sensibles, como son los datos de salud, cuando los tribunales actúen en ejercicio de su función judicial.

Ahora bien, el artículo 16.3 de la LAP limita el acceso a los datos personales que sean estrictamente necesarios para los fines específicos en cada caso. Además, remarca que no se predica la anonimización a los *"supuestos de la autoridad judicial en los que se considere im-*

29 *"Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGDP "* Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS) 2017

30 GALLEGO RIESTRA y RIAÑO GALÁN señalan que *"Los numerosos motivos que justifican la legitimidad para entrar en una historia clínica se pueden resumir en dos principios: el de vinculación asistencial y el de proporcionalidad, marcando entre ambos quién, cuándo y hasta dónde se puede acceder"*

"Tiene el paciente derecho a saber quienes y porqué han accedido a su historia clínica? " 2012, pp. 86, 87.

prescindible la unificación de datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente".

En palabras de LÓPEZ Y GARCÍA DE LA *SERRANA "lo recomendable sería aportar al juzgado solicitante aquellos datos de la historia clínica relacionados con el proceso de que se trate, haciendo notar que se ampliará la información en caso de que la autoridad judicial así lo determine. Si la solicitud efectivamente se refiriera a la historia clínica completa, como se dice en la consulta, habría dos alternativas, o enviarla efectivamente advirtiendo a la autoridad judicial que el envío del historial clínico completo puede contener anotaciones confidenciales del paciente, quedando a criterio de la autoridad judicial su utilización en el procedimiento, o por el contrario solicitar del juzgado información adicional que permita determinar qué partes de dicha historia serían necesarias para el procedimiento."*

C) Acceso a la historia clínica por compañías aseguradoras.

Como tendremos ocasión de analizar en el siguiente expositivo, las entidades aseguradoras en el marco del cumplimiento de sus obligaciones legales dispuestas en la Ley 50/1980 de Contrato de Seguro de las que destacamos la de abono de indemnización finalizado el proceso de investigación y peritación (y en su caso el proceso judicial) deben tener acceso a las historias de los pacientes.

En este contexto, la aseguradora debe conocer datos de salud incluidos en la historia clínica, pero la norma solo permite un acceso indirecto respetando, eso sí, el principio de minimización de datos por lo que no se podrán ceder más datos que aquellos que resulten adecuados, pertinentes y no excesivos para determinar el importe de la asistencia sanitaria a satisfacer por la aseguradora en virtud de un contrato de seguro.

La AEPD ha analizado la cesión de datos por centros sanitarios a compañías de seguros en supuestos de accidentes de tráfico en el Informe 526/2003 de la AEPD, precisando que no es necesario el consentimiento del interesado en estos supuestos por entender que la base de legitimación se encuentra en el cumplimiento de la obligación legal de las aseguradoras del pago de la asistencia sanitaria prestada, al amparo de lo dispuesto en los artículos 16.3 y 83 de la Ley 14/1986, de 25 de abril, General de Sanidad, pero precisando dos matices de notable importancia: a) solo se pueden ceder los datos imprescindibles para la facturación, y b) no se prejuzga el criterio que deba seguirse en el caso de centros privados.

Sin embargo, no se puede tener acceso a la historia clínica para el cumplimiento de la obligación de las aseguradoras de estar dotados de provisiones técnicas para poder atender indemnizaciones, tal y como obliga la Ley 30/95 de Ordenación y Supervisión de Seguros privados. Así lo indica la AEPD en su Informe 449/2004 por entender que las provisiones técnicas se dotan con base en cálculos actuariales, sin que sea precisa cada acto médico de un siniestro ni dicha información deba encontrarse en la Dirección General de Seguros, por lo que en este supuesto sí será preciso el consentimiento del interesado sin que quepa ninguna otra base de legitimación.

D) Acceso a la historia clínica de pacientes fallecidos.

Los datos personales de pacientes fallecidos quedan al margen de la protección del RGPD de manera expresa el Considerando 27[31], y con fines de archivo y con fines de investigación histórica en los considerandos 158[32] y 160[33].

Por el contrario, nuestra LOPDGDD sí regula de manera específica el tratamiento de datos personales de personas fallecidas en su artículo 3 en determinados supuestos, entre los que se encuentra el derecho de acceso, y, en su caso, su rectificación o supresión, a ejercitar por personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos, salvo que exista oposición expresa del interesado fallecido a ello.

En cualquiera de los casos, la base de legitimación debe ser el interés legítimo que obliga-

31 Considerando 27 del RGPD: *"El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas."*

32 Considerando 158 del RGPD: *"El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe ser de aplicación a personas fallecidas."*

33 Considerando 160 del RGPD: *"El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas."*

damente debe acreditarse por aquellas personas o instituciones recogidas en el art. 3 de la LOPDGDD, denegándose a pesar de ello dichas facultades cuando exista una disposición normativa pese a existir interés legítimo[34].

Se ha de contextualizar estas disposiciones normativas con lo dispuesto por la LAP en su artículo 18.4 el cual dispone que *"Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes.*

No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros".

34 La Audiencia Nacional, en sentencia dictada por la Sala de lo Contencioso-Administrativo, Sección primera, en recurso 1443/2020 que interpuso el Instituto Social de la Marina contra la Agencia Española de Protección de Datos denegó el acceso por parte de una hija a la vida laboral de su padre pues, si bien se acreditó la consanguinidad, no se fundamentó el interés personal y directo que exige la normativa de la Seguridad Social.

Y ello, en aplicación del párrafo segundo del art. 3.2 de la LOPDGDD: "Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

Por tanto, esta debe ser la hoja de ruta a seguir cuando deba permitirse a disposición de familiares y allegados la historia clínica.

IV. TRATAMIENTO DE DATOS PERSONALES EN SINIESTROS DE CIRCULACIÓN

Cuando tiene lugar un siniestro vial confluyen un gran trasiego de datos personales en los que tienen intervención un número elevado de agentes que tratan datos personales de forma directa o mediante cesión. Muchos de los datos personales de los que disponen las compañías aseguradoras ya han sido objeto de tratamiento previo al suscribir la póliza de seguro. En el momento de un accidente de circulación, la aseguradora debe conocer el nombre y apellidos, dirección, tfno y número de póliza. También precisa conocer detalles del vehículo tales como la matrícula. Las aseguradoras deben ser prudentes y tratar solo los datos personales que sean estrictamente necesarios cumpliendo los principios de minimización, limitación de la finalidad, confidencialidad y responsabilidad proactiva (tratamiento desde el diseño y por defecto).

Pero también las entidades aseguradoras comunican datos personales a los gruistas y/o servicios de taxi para desplazar a los accidentados. Por su parte, los servicios de bomberos y las fuerzas y cuerpos de seguridad del Estado tratan datos personales a la hora de elaborar las oportunas diligencias instructoras.

En definitiva, los agentes implicados en un siniestro de circulación realizan un tratamiento

de datos bien directo mediante los datos personales que son comunicados directamente por el implicado o bien mediante cesión por parte de algún agente de los mencionados, lo que implica necesariamente que el tratamiento se ampare en una de las bases de legitimación reguladas en el RGPD.

La ley 3/2018 de 5 de Diciembre, de Protección de Datos Personales (LOPDGDD) establece en su disposición adicional décima que los responsables de tratamiento pueden comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento del afectado o cuenten con una base de legitimación tal como interés legítimo que prevalezca sobre los derechos o intereses de los afectados.

En este apartado vamos a tratar de analizar y exponer los distintos agentes que tratan datos personales en un accidente de circulación, su posible cesión a otros agentes, y las bases de legitimación que amparan su tratamiento en los supuestos en los que no existe el consentimiento del interesado.

4.1 Tratamiento de datos personales contenidos en Atestados e Informes Periciales. Especial referencia a la cesión de datos personales a entidades aseguradoras y letrados de los implicados/perjudicados en el siniestro

La antigua y derogada Ley 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal definía la cesión de datos como *"Toda revelación de datos efectuada a persona distinta del interesado".*

La cuestión no es baladí pues existen numerosa jurisprudencia, incluso penal, en supuestos en los que se ceden datos personales sin consentimiento del interesado y sin estar amparado en el cumplimiento de obligaciones contractuales o amparadas en norma con rango de ley, de la que citamos la sentencia num. 615/2022 dictada por la Audiencia Provincial de Valencia con fecha 30/11/2022 en procedimiento abreviado 72/2022 por un delito de revelación de secretos o la dictada por el Tribunal Supremo (Sala de lo Penal) de 22 de octubre de 2021 en recurso de casación 4846/2019.

La AEPD en los Informes 0549/2008 y 0078/2009 desarrollan ampliamente esta cuestión al resolver, entre otras cuestiones, una consulta sobre cesión por parte de la Policía Local de datos personales de implicados en accidentes de circulación al resto de las partes afectadas por dichos accidentes.

Ya aventuraba la AEPD en dichos Informes que *"el artículo 11.1 de la Ley* (se refiere a la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal), *establece que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado", quedando exceptuado el consentimiento en aquellos casos en que así lo prevea una Ley.*

Del tenor de dichos preceptos parece desprenderse que sólo será lícita la cesión de los datos personales de los individuos implicados en un accidente de circulación cuando exista previo consentimiento del interesado o una disposición con rango de Ley así lo prevea.

No obstante, en el supuesto objeto de consulta, si el resto de las personas implicadas en un accidente lo que solicitan es una copia del atestado policial sobre las circunstancias e implicaciones del mismo, entendemos que resultarán de aplicación los principios contenidos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, para el derecho de acceso por parte de quién ostente la condición de interesados en los términos indicados en la propia Ley, a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos."

A) Cesión de datos a las aseguradoras.

La AEPD, en el Informe de 04/03/2009, ya se encargó de analizar los motivos y argumentos, y por ende las bases de legitimación, para que las aseguradoras puedan recabar datos personales de terceros perjudicados ajenos a su asegurado sin que sea preciso el consentimiento del tercero perjudicado implicado en el siniestro.

Y así, se indica que las entidades aseguradoras, con el fin de satisfacer las pertinentes indemnizaciones que pudieran derivarse de la suscripción y vigencia de un seguro de responsabilidad civil en el ámbito de la circulación de vehículos a motor, tienen la obligación de realizar las investigaciones y peritaciones precisas tanto de la existencia del siniestro como de la

valoración de los daños que hubieran podido producirse, pues así lo dispone el artículo 18 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro.[35]

Y ello, como decimos, pues es obligación contractual del asegurador la de indemnizar a un tercero los daños y perjuicios causados por un hecho objeto de cobertura en el contrato de seguro del que sea civilmente responsable el asegurado. Pero es que, además, el tercero perjudicado en el siniestro (ajeno por tanto a la relación contractual entre asegurador y asegurado) tiene reservada la acción directa contra la entidad aseguradora para exigirle el cumplimiento de la obligación de indemnizarle los daños y perjuicios que le ha ocasionado el asegurado de aquella, pues así lo dispone el art. 76 de la ley 50/1980, de 8 de octubre, de Contrato de Seguro.

El asegurador debe, además, realizar unas provisiones técnicas con el fin de disponer de recursos económicos tendentes a abonar la indemnización correspondiente, por lo que el desconocimiento de los datos relativos al siniestro pudiera dificultar el cumplimiento de su obligación de resarcimiento.

Además de ello, las aseguradoras tienen otras obligaciones establecidas por disposiciones normativas entre las que se encuentran la llevanza de un libro de siniestros, entre cuyos datos se deberán incluir los del perjudicado y los daños sufridos por este debidamente probados[36] y están sometidas a supervisión y control financiero por el Ministerio de Economía[37].

Dicha información podrá ser requerida por la Dirección General de Seguros y Fondos de Pensiones, pues se le atribuye dicha potestad supervisora por el Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados y la negativa a facilitar dichos datos personales a dicha corporación puede conllevar sanciones administrativas.

Esta cuestión la abordó ampliamente el doctor D. JAVIER LÓPEZ GARCÍA DE LA SERRANA en el año 2012 en el 8ª Congreso Jurídico de la Abogacía Malagueña quien analiza tanto la normativa como la base de legitimación que permite a las aseguradoras recabar los datos personales existentes en atestados policiales. En base a ello, el Dr.López y García de la Serrana concluye que *" Teniendo en cuenta que, como consecuencia de la producción del siniestro, se genera una relación jurídica entre la compañía aseguradora del causante del daño y el perjudicado, de la que, de una parte, resulta la obligación de aquélla de pagar la indemnización derivada de los daños causados por el siniestro y de otra, otorga al perjudicado una acción directa contra la compañía aseguradora para exigir el pago de dicha indemnización, las cesiones de datos objeto de consulta resultan igualmente amparadas por lo previsto en el artículo 11.2.c) de la LOPD.".*

Todo lo expuesto lleva a concluir que la base de legitimación para que las aseguradoras tengan acceso a los datos personales de terceros perjudicados insertos que constan en los atestados policiales e Informes Periciales es el interés legítimo, el cumplimiento de sus obligaciones contractuales de provisiones técnicas, obligación de abono de indemnización al tercero perjudicado y el cumplimiento de normas con rango de ley (artículos 18 y 76 de la Ley 50/1980 LCS y artículo 7 del TRLSCVH).

El proyecto de Ley de modificación del TRLSCVH[38] que ha creado un Título V dedicado a la protección de datos personales (del que haremos un amplio desglose en otro apartado de este artículo) otorga a las entidades aseguradoras en el recién creado artículo 146, apartado 3, la potestad de recabar los datos personales contenidos en Informes Periciales y Atestados *"que resulten necesarios, proporcionales e idó-*

35 Art. 18 Ley 50/1980, de 8 de octubre, de Contrato de Seguro: "El asegurador está obligado a satisfacer la indemnización al término de las investigaciones y peritaciones necesarias para establecer la existencia del siniestro y, en su caso, el importe de los daños que resulten del mismo. En cualquier supuesto, el asegurador deberá efectuar, dentro de los cuarenta días, a partir de la recepción de la declaración del siniestro, el pago del importe mínimo de lo que el asegurador pueda deber, según las circunstancias por él conocidas(..)"

36 Artículo 65 del Real Decreto 2486/1998, de 20 de noviembre por el que se aprueba el Reglamento de Ordenación y Supervisión de los Seguros Privados.

37 Articulo 71.2 del Real Decreto 2486/1998, de 20 de noviembre por el que se aprueba el Reglamento de Ordenación y Supervisión de los Seguros Privados, indica que *"(...) el control financiero consistirá, en particular, en la comprobación del conjunto de actividades de la entidad aseguradora, del estado de solvencia y de la constitución de provisiones técnicas(..)"*

38 Proyecto de Ley de 7 de Junio de 2024por la que se modifican el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, y la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras..

neos para la determinación de la indemnización" y únicamente para las finalidades indicadas en el apartado 2 de dicho artículo, esto es: para cumplir con las obligaciones derivadas del contrato de seguro y, en su caso, cuantificar el importe de la indemnización correspondiente al mismo, y para elaborar la propuesta de indemnización o la respuesta motivada prevista en el artículo 7.2 del citado TRLRCSCVH.

B) Cesión de datos contenidos en atestados a letrados de los implicados.

Habida cuenta los letrados de los implicados son, a priori, terceros ajenos al siniestro y a la relación contractual que vincula a su cliente con la aseguradora, debe analizarse qué base de legitimación permite a los abogados solicitar datos personales de otros implicados en accidentes de circulación que consten en atestados policiales para poder entablar las oportunas acciones judiciales en defensa de sus clientes, pues hemos de partir de la base de que los letrados carecen del consentimiento de los implicados en el siniestro que no sean sus clientes.

Volvemos a traer a colación al Doctor LÓPÉZ Y GARCÍA DE LA SERRANA en su ponencia de la Abogacía malagueña[39], el cual analiza pormenorizadamente la base de legitimación que permite a los letrados tener acceso a datos personales contenidos en el atestado, siendo la misma el cumplimiento de una norma con rango de ley, mejor dicho dos, cuales son el artículo 76 de la ley 50/1980 de 8 de Octubre, de Contrato de Seguro y el art. 7.1 del TRLRCSCVH: El ejercicio de acción directa por parte del perjudicado o sus herederos para exigirle el cumplimiento de su obligación de indemnización.

Así las cosas, para que el perjudicado en un siniestro de circulación y/o su letrado puedan entablar las correspondientes acciones extrajudiciales y judiciales para ser resarcido de los daños personales y materiales sufridos con ocasión del siniestro es preciso que conozca y tenga acceso al atestado.

Por ello, como tendremos ocasión de analizar posteriormente en el apartado VI, el proyecto de ley de reforma del TRRCSCVH dispone en el recién creado artículo 146 que las entidades aseguradoras podrán poner a disposición de los abogados que representen a los lesionados en accidentes de tráfico, plataformas seguras de intercambio de información que garantizarán en todo momento, la trazabilidad de las reclamaciones y el cumplimiento de la normativa en materia de protección de datos personales.

C) Qué datos personales contenidos en atestados pueden comunicarse a aseguradoras o letrados.

Debemos traer a colación en este punto la LO 7/2021 de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como la existencia del denominado fichero SIDENPOL (Sistema de denuncias policiales) por lo que la Unidad de planificación estratégica y coordinación de la Policía Nacional ha implementado un procedimiento para articular los derechos de los interesados en materia de protección de datos (acceso al fichero, rectificación, cancelación, entre otros muchos).

Ahora bien ¿Se deben facilitar todos los datos contenidos en el atestado? Ya avanzamos con anterioridad que el tratamiento de datos contenidos en atestados debe respetar los principios de limitación de la finalidad del tratamiento (art. 5.1b), de minimización de datos (Art 5.1.c) y de limitación del plazo de conservación (art 5.1.e) de manera que solo deben facilitarse aquellos datos personales que sean necesarios para la finalidad para la que van a ser cedidos.

En el caso de las aseguradoras, como hemos expuesto, para cumplir sus obligaciones legales (adelanto de indemnización, respuesta motivada, y pago de indemnización) y contractuales (provisiones técnicas, llevanza de libro de siniestros, indemnización a tercero perjudicado etc) y en el caso de los letrados para el ejercicio de las correspondientes acciones judiciales tendentes a resarcir los daños y perjuicios a su cliente derivados del siniestro de circulación.

Eso sí, el resto de datos personales que no sean necesarios para la finalidad para la que han sido cedidos deberán estar debidamente anonimizados a fin de preservar el derecho constitucional de protección de datos personales del artículo 18.4 de la Constitución Española.

La cuestión es ampliamente desarrollada por la AEPD en el citado Informe 2010/411 del cual extraemos y hacemos expresa mención, por su importancia, al criterio que sigue la Agencia respecto del vehículo de transmisión y recepción de dicha información, considerándo-

39 LÓPEZ GARCÍA DE LA SERRANA, Javier. 8º Congreso de la Abogacía malagueña. 18 y 19 de Octubre de 2012.

se como el más apropiado el correo electrónico en aplicación de lo dispuesto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos[40].

Con respecto a la comunicación de datos personales por vía telefónica, el citado Informe de la AEPD previene que dicho medio pudiera ser ilícito ya que no permite contrastar con veracidad la identidad de la persona que solicita los datos y la base de legitimación que le ampara, indicando al respecto que, si se opta por dicho medio de comunicación debe cerciorarse previamente de que *" el sistema utilizado para acreditar la identidad de la persona que llama impida que terceras personas no autorizadas puedan acceder a la información referida al afectado, procedimientos que normalmente exigen la existencia de una clave de acceso como mecanismo de identificación del interesado.*

En el presente supuesto, habrá que estar igualmente a si el Organismo en el que presta servicios el consultante ha habilitado, con carácter general, un procedimiento de acreditación que permita, con la utilización de las claves que se establezcan y guardando las debidas medidas de seguridad, facilitar datos personales por esta vía."

4.2 Tratamiento de datos personales por parte de Servicios de emergencia.

Los servicios telefónicos de emergencia (el conocido como 112), en el momento en que son conocedores de un accidente de tráfico, a fin de desplegar los oportunos dispositivos, precisan conocer una serie de datos personales que, o bien pueden ser directamente facilitados por el propio afectado en el accidente, o bien son recabados directamente por dicho Servicio de Emergencia mediante solicitud de cesión de datos dirigida a otros organismos, instituciones o administraciones, o bien son facilitados por diversas aplicaciones técnicas como sistemas de localización o geolocalización.

¿Estamos en presencia de datos personales cuando hablamos de datos de localización? Nuestra AEPD ya se ha pronunciado en varias ocasiones al respecto en informes como el de 17 de abril de 2006 o informe 438/2015, que se remitían a la anterior LOPD 1999.

Por dato de localización debe entenderse *"Cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público"*[41]

El Grupo de Trabajo del Artículo 29 (GT 29)[42], ya advertía del *"aumento exponencial en el uso de los datos de localización vía satélite, que en la actualidad pueden ser muy precisos y valiosos, especialmente por lo que se refiere a la asistencia a personas en apuros"* y a *"la difusión sin precedentes de la telefonía móvil, merced a la cual cada usuario lleva siempre un dispositivo mediante el cual se le puede localizar".*

Por ello, la Directiva 2002/58/CE de 12 de julio de 2002, establecía en su artículo 9.2 la obligación de recabar el consentimiento de los usuarios o abonados antes de proceder al tratamiento de los datos de localización necesarios para prestar un servicio con valor añadido y de informar a los usuarios o abonados de las con-

40 Artículo 27 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los *ciudadanos a los Servicios Públicos: "1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.*

2. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso,emitirse y recabarse por medios electrónicos.

3. Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del 2. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.

4. Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas."

41 Artículo 2 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en la redacción dada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009

42 El Grupo de Trabajo del Artículo 29 (GT 29) es un organismo consultivo independiente que fue creado por la Directiva 95/46/CE (anterior al RGPD) que estaba integrado por las autoridades de protección de datos de los Estados miembros de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea (con funciones de Secretariado).

diciones de dicho tratamiento.[43] Dicho artículo establecía además la salvaguarda de que el interesado tenga siempre el control y disposición de sus datos pudiendo limitar, restringir, e incluso oponerse al acceso en un determinado siniestro o momento.

En España, en aplicación de dicha normativa, nos encontramos con Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuyo artículo 48.2 c) indica:

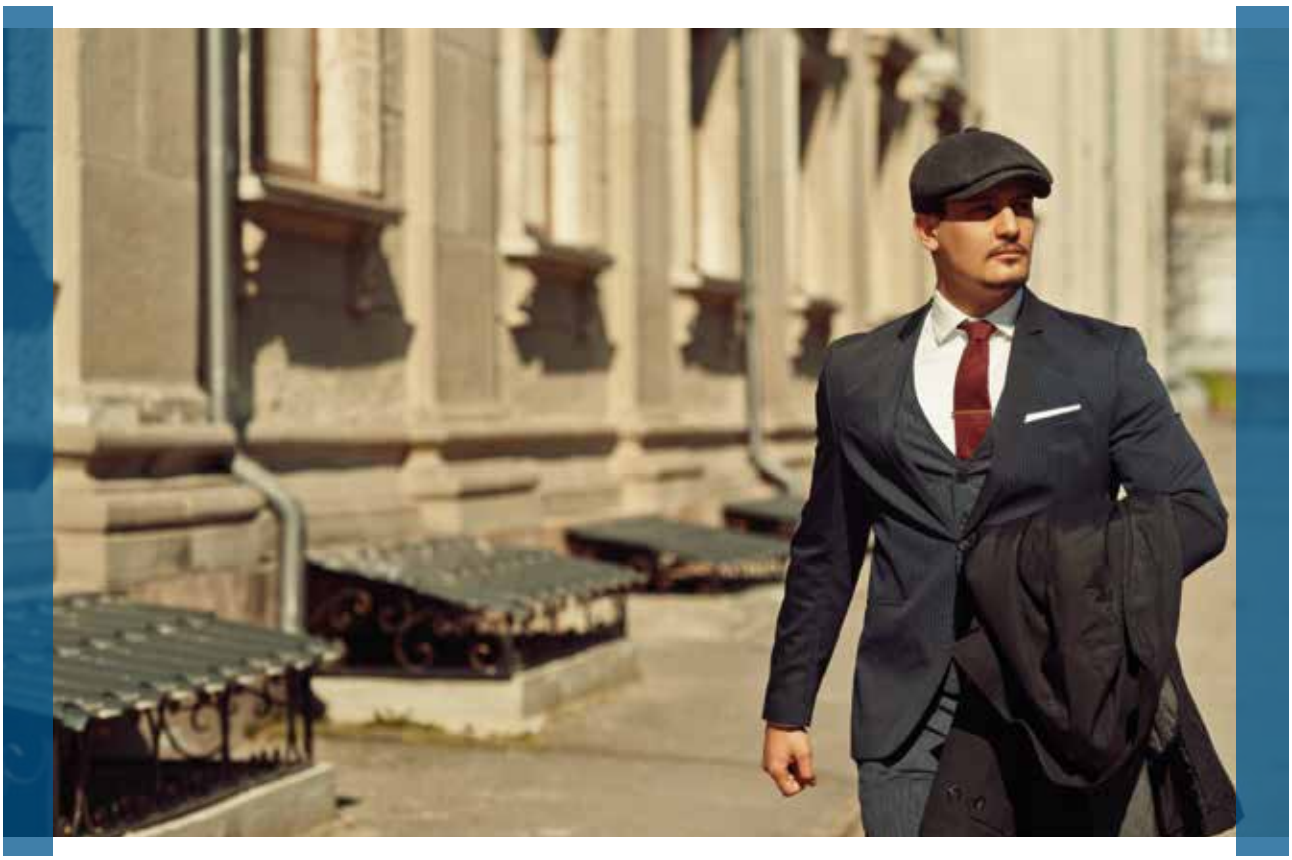
"Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico"

En este recorrido por la normativa europea también debemos hacer mención a una Directiva, la 2018/1972, de 11 de Diciembre, del Parlamento Europeo y del Consejo, por la que se es-

43 Artículo 9.2 del 2002/58/CE de 12 de julio de 2002:*"1. En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas decomunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico."*



tablece el Código Europeo de Comunicaciones Electrónicas, la cual ya establecía en su artículo 109.6 la obligación de los estados miembros de poner a disposición de los servicios de emergencias la ubicación de red y la localización del dispositivo móvil.[44]

Por su parte, nuestro ordenamiento jurídico también establece la obligación de facilitar a los servicios de emergencia los datos de localización, si bien no prima el consentimiento del interesado sino la protección del interés vital del implicado en un siniestro de circulación, siendo por tanto la base de legitimación del tratamiento del dato de localización la letra d) del artículo 6.1. del RGPD: Cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, tal y como acertadamente señala el considerando 46 del RGPD.[45]

En la prevalencia y salvaguarda de los intereses vitales de un implicado en accidente de circulación, el art. 47.1.m) de la Ley 9/2014 de 9 de mayo de Telecomunicaciones, impide que el usuario pueda ejercer su derecho a la no identificación de su línea cuando se trate de llamadas de emergencia o llamadas a organismos que presten servicios de llamadas de urgencia determinados normativamente y su art. 48.1.c) prevé la misma limitación respecto de otros datos de localización distintos a los datos de tráfico.

La regulación normativa estatal de las llamadas telefónicas a servicios de emergencia se encuentra en el Real Decreto 903/1997, de 16 de junio, el cual regula el número telefónico 112, cuyo artículo 3.3 dispone: *"Asimismo, dichos operadores facilitarán la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas al número telefónico 112 (...) para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y persecución de delitos, la seguridad de la vida humana o razones de interés público".*

Por su parte, la Orden de 14 de octubre de 1999 sobre condiciones de suministro de información relevante para la prestación del servicio de atención de llamadas de urgencia a través del número 112 establece en su artículo 4[46] los requisitos para la cesión de esos datos de manera que, en cualquier caso, los datos que sean tratados o cedidos deberán cumplir los principios de limitación de tratamiento y de conservación de datos, lo que implica que serán eliminados cuando cumplan la finalidad para la que fueron tratados.

En nuestro país, las Administraciones que se encargan de gestionar el Servicio de Emergencias 112 ya han reclamado la utilización de la herramienta informática AML (Advance Mobile Location) que activa la ubicación del móvil del implicado en el siniestro vial.

En este punto, es aconsejable detenerse en un informe de la AEPD 2019/0039 que resuelve la licitud de tratamiento de los datos de localización de un implicado en siniestro vial mediante el empleo de la herramienta informática AML (Advance Mobile Location).

44 artículo 109.6 Reglamento 2018/1972, de 11 de Diciembre: *"Los Estados Miembros velarán por que la información relativa a la ubicación de las personas que efectúan llamadas se ponga a disposición del SAP más indicado inmediatamente tras el establecimiento de la comunicación de emergencia. Dicha información incluye los datos sobre ubicación de la red y, si están disponibles, los datos relativos a la localización del llamante procedentes del dispositivo móvil. Los Estados miembros garantizarán que el establecimiento y la transmisión de la información relativa a la localización del llamante sea gratuita para este último y para el PSAP con respecto a todas las comunicaciones de emergencia al número único europeo de emergencia "112" [...]*

45 Considerando 46 RGPD: *"El tratamiento de datos personales también debe considerarse lícito cuando*

sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente.

Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano"

46 *Artículo 4 Orden de 14 de octubre de 1999:" La cesión de datos personales referidos en el artículo 2 se entenderá amparada por la protección del interés vital del llamante, la seguridad pública y la protección del interesado o de los derechos y libertades de otras personas y quedará sometida a la legislación de protección de datos, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal y su normativa de desarrollo.*

Dicha cesión de datos será utilizada, de manera exclusiva, como soporte para una más efectiva prestación de los servicios de atención de llamadas de urgencia a través del número 112 y será responsabilidad de la entidad prestataria el adecuado uso de los mencionados datos.

Los datos sobre la ubicación geográfica de las estaciones bases de las redes públicas de telefonía móvil se utilizarán exclusivamente para la prestación del servicio de atención de llamadas de urgencia, no pudiéndose utilizar para otros fines ni cederse a terceros".

Tal y como se describe en dicho Informe por la AEPD *"AML es un mecanismo, ya desplegado en algunos países, por el que los centros de atención a llamadas de emergencia (servicios 112 y similares, conocidos como PSAP por su siglas en inglés) pueden recibir de forma automática información sobre la ubicación del llamante (cuando éste llama desde un teléfono móvil) con una precisión muy superior a la que puede obtenerse actualmente a través de la información que proporcionan los operadores de telefonía móvil, basada en la ubicación de la estación base desde la que se origina la llamada.*

AML es independiente del operador, ya que funciona sobre el teléfono móvil (directamente desde el sistema operativo, por lo que no requiere que el usuario descargue una app o realice una configuración previa). Cuando detecta que se está produciendo una llamada a un número de emergencias, AML activa la ubicación del móvil en alta precisión (típicamente obtenida a partir de redes WIFI o Bluetooth cercanas, o de un servicio GNSS, como GPS o Galileo) y genera un mensaje con las coordenadas de la ubicación. El mensaje (que puede ser un SMS, un mensaje de datos, o ambos) es enviado a un número y/ o una URL predefinidos para cada país. El servicio se puede configurar para que el mensaje sea reenviado cada cierto tiempo mientras la llamada de voz siga activa."

El citado Informe 2019/0039 la AEPD considera lícito el tratamiento de datos de localización de un implicado en accidente de tráfico mediante la herramienta AML, siendo su base de legitimación el art. 6.1.d) del RGPD, si bien conforme a la normativa española de trasposición de la Directiva (UE) 2018/1972 de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas, si bien la base de legitimación pudiera ampararse igualmente en el artículo 6.1c) del RGPD, (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento) y art. 6.1.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).

4.3 Tratamiento y cesión de datos personales por parte de la Comisión Nacional de los Mercados y la Competencia a Servicios de Emergencias para la prestación del servicio de llamadas de emergencia.

También sobre esta cuestión ha tenido ocasión de pronunciarse nuestra AEPD en varios informes, del que destacamos el Informe 2018/186, el cual se remite a los Informes de 6 de marzo de 2001 y de 23 de julio de 2002, para analizar la base de legitimación que permite que la Comisión Nacional de los Mercados y la Competencia pueda ceder datos personales a un ayuntamiento (que fue la entidad local que elevó consulta a la AEPD objeto del citado Informe) amparándose en la protección de intereses vitales del interesado o de otra persona física, por lo que se constituye como base de legitimación el apartado d) del artículo 6.1 del RGPD y el artículo 25.1 c) de la vigente Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

El citado Informe ahonda más la cuestión y se pronuncia en concreto sobre la cesión de directorio de números de abonados para la prestación de servicios de emergencia, remitiéndose para ello a la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, completada por el antes citado Real Decreto 903/1997, de 16 de junio que regula el acceso mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112, y en materia normativa autonómica de la Comunidad Autónoma de Andalucía, por la Ley 2/2002 de 11 de noviembre de Gestión de Emergencias en Andalucía.[47]

Por su parte, el apartado Sexto de la Circular 1/2013, de la Comisión del Mercado de las Telecomunicaciones, sobre el procedimiento de suministro y recepción de los datos de los abonados, establece las premisas sobre las que se pueden ceder datos de los abonados, de entre los que destacamos:

> "a. La información solicitada será tratada única y exclusivamente para la prestación del servicio y/o para la finalidad para la que fue entregada.
>
> b. Los datos de los abonados que hayan sido suministrados serán actualizados conforme a lo dispuesto en la presente Circular.
>
> c. Los servicios prestados por las entidades con derecho a obtener la información de los abonados deberán iniciarse en el plazo máximo de seis meses desde la resolución de la Comisión del Mercado de las Teleco-

47 Artículo 4.2 de la Ley 2/2002 de 11 de noviembre de Gestión de Emergencias en Andalucía: *"Los ciudadanos tienen derecho a recibir información relativa a los riesgos que puedan afectarles, las consecuencias de los mismos que sean previsibles y las medidas de autoprotección y conductas a seguir, en el marco de lo dispuesto en los planes de emergencia".*

municaciones otorgando el suministro, y se prestarán con las características, el contenido y en las condiciones previstas en la normativa específica que los regula."

4.4 Tratamiento y cesión de datos personales a familiares y allegados por parte de Servicios de Emergencia.

El informe 2019/0039 de la AEPD, del que ya hemos hablado con anterioridad, aborda esta cuestión posibilitando la cesión de determinados datos a familiares y allegados bajo el argumento y justificación de que *"pudieran existir situaciones de urgencia vital, considerando que los familiares o allegados pueden suministrar, en un primer momento de atención médica urgente, información que pudiera resultar esencial para la debida atención en el centro hospitalario de destino, por lo que el supuesto de hecho quedaría incardinado en el interés vital del afectado en esta cesión de los datos."*

Ahora bien, el principio de limitación del tratamiento (art 5 RGPD y el derecho a limitación del tratamiento que ostentan los interesados (art. 18 RGPD) solo permiten indicar determinados datos a los familiares o allegados que se encuentran especificados en el Apartado Decimoquinto 2) de la Orden CTE/711/2002, para la atención del servicio de llamada de urgencia (entre ellos, si el interviniente en un siniestro vial ha sido atendido por servicios sanitarios y el centro hospitalario al que haya sido trasladado). Cualquier otra información o dato personal pudiera ser considerado excesivo y, por tanto, no puede ser facilitado al familiar o allegado, con el objeto de cumplir el principio de minimización de datos personales y el de confidencialidad.

También se analiza esta cuestión en el Informe de la AEPD de 11 de noviembre de 2008 relativo a datos personales de pasajeros y tripulación sobre la base de que "*quienes realicen las actuaciones de salvamento, acceder de modo más rápido a los datos de salud que puedan resultar imprescindibles para llevar a cabo una adecuada atención sanitaria de las víctimas, dado que el acceso por el público en general a los datos de las víctimas, mortales o no, permitirá a aquellos familiares, allegados o profesionales de la medicina que tengan conocimiento de la existencia de determinados episodios del afectado que pudieran afectar a su curación, poner esas circunstancias en conocimiento de los servicios de emergencia para llevar a cabo una adecuada asistencia de los heridos*".

4.5 Tratamiento de datos personales de personas fallecidas.

Si bien, como estamos teniendo ocasión de analizar, hay multitud de datos personales que confluyen en la producción de un siniestro vial y que son objeto de tratamiento por diversos organismos, instituciones, entidades jurídicas en base a diversas bases de legitimación que hemos tenido ocasión de analizar, en el caso de personas fallecidas el tratamiento de datos personales puede analizarse desde diversos prismas: sector asegurador para pólizas de seguro de vida, seguro de salud o seguros sociales, sector sanitario para traslado del difunto, etc.

Hemos de comenzar indicando que, pese a tratarse de datos *"delicados"*, no tienen la categorización de datos sensibles ni por el RGPD ni por nuestra LOPDGDD.

Es más, son excluidos de manera general por el RGPD tal y como indica de manera expresa el Considerando 27[48], y con fines de archivo y con fines de investigación histórica en los considerandos 158[49] y 160[50].

Por el contrario, nuestra LOPDGDD sí regula de manera específica el tratamiento de datos personales de personas fallecidas en su artículo 3 en determinados supuestos:

Pueden solicitar el derecho de acceso, y, en su caso, su rectificación o supresión personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos, salvo que exista oposición expresa del interesado fallecido a ello.

En cualquier caso, la oposición del fallecido no surte efecto alguno respecto de los derechos de los herederos para acceder a datos personales de la persona fallecida en el ámbito patrimonial.

48 Considerando 27 del RGPD: *"El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas."*

49 Considerando 158 del RGPD: *"El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe ser de aplicación a personas fallecidas."*

50 Considerando 160 del RGPD: *"El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas."*

También podrán solicitar el acceso, y en su caso rectificación o supresión, a datos personales de una persona fallecida aquellas personas o instituciones a las que el fallecido hubiese designado expresamente.

En el caso de que el fallecido fuera menor de edad, los citados derechos pueden ejercitarse por sus padres, representantes legales o Ministerio Fiscal en el marco de las competencias atribuidas normativamente.

En caso de fallecimiento de personas con discapacidad, las facultades citadas podrán ejercerse no solo por las personas o institución antes indicadas sino además por quienes se hubieran designado judicialmente para el ejercicio de funciones de apoyo (curador, defensor judicial, etc).

En cualquiera de los casos, la base de legitimación que permita el ejercicio de los citados derechos de acceso, rectificación o supresión, debe ser el interés legítimo que obligadamente debe acreditarse por aquellas personas o instituciones recogidas en el art. 3 de la LOPDGDD, denegándose a pesar de ello dichas facultades cuando exista una disposición normativa pese a existir interés legítimo[51].

Hacemos una parada en este punto en el denominado *"testamento digital"* entendido por MORALEJO INVERNÓN, Nieves, como *"documento de últimas voluntades que nos permite dejar instrucciones sobre el destino de nuestros contenidos digitales en caso de fallecimiento"*[52] y *"derecho digital de los ciudadanos en virtud del cual determinados sujetos podrán acceder a los contenidos de los derechos digitales de las personas fallecidas que estuvieran siendo gestionados por prestadores de servicios de la sociedad de información"* y que es regulado en el artículo 96 de la LOPDGDD.

4.6 Tratamiento de Datos personales incluidos en el fichero FIVA (Fichero de Información de Vehículos Asegurados)

El denominado fichero FIVA es un fichero de carácter público, creado por el artículo 23.1 del Real Decreto 7/2.001, de 12 de enero, por el que se aprueba el ya derogado Reglamento sobre la responsabilidad civil y seguro en la circulación de vehículos de motor.

Dicho fichero se constituyó con la finalidad, tal y como dispone el artículo 27 de dicho cuerpo legal de *"Suministrar la información necesaria para que las personas implicadas en un accidente de circulación puedan averiguar a la mayor brevedad posible las circunstancias relativas a la entidad aseguradora que cubre la responsabilidad civil de cada uno de los vehículos implicados en el accidente y en facilitar el control de la obligación de asegurarse."*

El artículo 24 de dicho Real Decreto indicaba los datos que debían facilitar las compañías aseguradoras en el momento de suscripción de un contrato de seguro de responsabilidad civil de vehículos a motor*: "Matrícula, código identificativo de la marca y modelo del vehículo, fecha de inicio de la vigencia y fecha de finalización del período de seguro en curso, así como el tipo de contrato,todo ello de acuerdo con las especificaciones contenidas en la resolución de la Dirección General de Seguros y Fondos de Pensiones que a tal efecto se dicte."*

Por su parte, el Anexo del citado Real Decreto 7/2001, indica en su apartado 5º a quienes se puede ceder los datos contenidos en el fichero FIVA: implicados en accidentes de circulación, Ministerio del Interior, Ministerio Fiscal, y órganos judiciales.

En relación con la cesión de datos del fichero FIVA, el Informe 2009/78 dictado por la AEPD se remite a las Conclusiones y Recomendaciones del Plan de inspección de oficio al Consorcio de Compensación de Seguros, dictadas por el Director de la Agencia de Protección de Datos con fecha 23 de julio de 2.001, y más concretamente a la recomendación cuarta en la que se indica que *"De la normativa aplicable se desprende que el Consorcio sólo podrá facilitar datos personales incluidos en sus ficheros automatizados a personas físicas y entidades públicas y privadas, a los efectos del cumplimiento de la normativa sobre Tributos y Seguros, así*

51 La Audiencia Nacional, en sentencia dictada por la Sala de lo Contencioso-Administrativo, Sección primera, en recurso 1443/2020 que interpuso el Instituto Social de la Marina contra la Agencia Española de Protección de Datos denegó el acceso por parte de una hija a la vida laboral de su padre pues, si bien se acreditó la consanguinidad, no se fundamentó el interés personal y directo que exige la normativa de la Seguridad Social.

Y ello, en aplicación del párrafo segundo del art. 3.2 de la LOPDGDD: "Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

52 MORALEJO INVERNÓN, Nieves. *"El testamento digital en la nueva Ley Orgánica 3/2018 de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales"* ADC. Tomo LXXIII, 2020, fascículo I. Páginas 241-281.

como para facilitar el control de la obligación de asegurarse, todo ello de conformidad con lo dispuesto en el anterior apartado 1. 7". Dicho apartado 1. 7 de las Conclusiones de la Inspección de la Agencia de Protección de Datos, indicaba específicamente que: "Con respecto al Fichero Informativo de Vehículos Asegurados la finalidad de mismo es suministrar información por parte del Consorcio a las personas implicadas en un accidente de circulación referente a la entidad aseguradora que cubre la responsabilidad civil, según establece la Ley 30/1.995 y la Directiva 90/232/CEE."

V. TRATAMIENTO DE DATOS PERSONALES POR EL SECTOR ASEGURADOR

Como hemos tenido ocasión de analizar en anteriores expositivos de este texto, las compañías aseguradoras tratan datos personales que, o bien le han sido facilitados por el propio asegurado con el fin de concertar un contrato de seguro, o bien son recabados por las aseguradoras cuando tiene lugar un siniestro que pudiera ser objeto de cobertura por la póliza a fin de cumplir las obligaciones legales y contractuales.

También hemos tenido ocasión de analizar que no es posible el tratamiento de datos personales sin una base de legitimación que permita dicho tratamiento.

5.1 Bases de legitimación para el tratamiento de datos personales.

Las bases de legitimación para tratar datos personales se encuentran enumeradas en el artículo 6 del RGPD[53] y, a lo que el sector asegurador concierne, las bases de legitimación más comunes son el consentimiento del interesado, la ejecución del contrato de seguro y el cumplimiento de obligaciones legales del asegurador.

5.1.1 Tratamiento de datos personales basada en el consentimiento del interesado.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su artículo 4.11 define el consentimiento del interesado como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".*

Es preciso el consentimiento del interesado en los siguientes supuestos:

- Tratamientos de datos de salud que no estén amparados legalmente en la LOSSEAR, en el artículo 9.2. de la LOPDGDD o en cualesquiera otras leyes y que sean de obligado cumplimiento para las entidades aseguradoras.

- Tratamientos de marketing directo sobre productos de terceras entidades.

- Tratamientos de marketing directo dirigidos a personas que no son clientes de la entidad aseguradora. Para las comunicaciones comerciales por medios electrónicos habrá de estarse a lo dispuesto en el artículo 21 de la Ley 34/2002 se estará a lo establecido en el artículo 21 de la Ley (LSSI).[54]

53 Art. 6.1 del RGPD: *"El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

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 o para la aplicación a petición de este de medidas precontractuales.

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, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

54 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico: *"Art. 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que

Por el contrario, no es preciso el consentimiento del interesado:

- Tratamiento de datos en la ejecución del contrato de seguro, ya que la base de legitimación en este caso es la relación contractual, el interés legítimo y la legislación de seguros, 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 (aquí la base de legitimación es la relación contractual y el interés legítimo de la entidad aseguradora).

- Tratamiento de datos relacionados con la actividad aseguradora (la base de legitimación es el cumplimiento de obligaciones legales o habilitación legal)

- Tratamiento de datos para la prevención del fraude. (la base de legitimación es el interés público del Fondo Monetario Internacional).

Por su parte, la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, en su artículo 99 indica la no necesariedad de contar con el consentimiento del interesado en los siguientes supuestos:

1º) Para garantizar la ejecución del contrato de seguro y el cumplimiento de las obligaciones establecidas en dicha Ley o de su desarrollo legislativo.

2º) En el caso de datos de salud del interesado, para determinar la prestación de asistencia sanitaria o la indemnización que deba prestarse con cargo a la entidad de seguros, así como para abonar a los prestadores sanitarios o reintegrar al asegurado

inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección. "

aquellos gastos de asistencia sanitarios ocasionados en el ámbito de un contrato de seguro.

3º) Para el cumplimiento de las obligaciones de supervisión en el caso de grupo de entidades aseguradoras y reaseguradoras.

4º) Cuando deba comunicarse por las entidades aseguradoras a sus entidades reaseguradoras los datos que sean estrictamente necesarios para la celebración del contrato de reaseguro o para la realización de las operaciones con las que tengan relación tales como estudios estadísticos o actuariales, análisis de riesgos o investigaciones para sus clientes.

5.1.2. Tratamiento de datos personales basada en el cumplimiento de obligaciones legales de la entidad aseguradora.

Esta base de legitimación, prevista en el art. 6.1.c) del RGPD, tiene sustento en el considerando 40 del RGPD el cual dispone que *"Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato "*

Por su parte, el considerando 45 del RGPD reitera la necesidad de que, si la base de legitimación es el cumplimiento de una obligación legal, *"el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros".*

En base a ello, el art. 6.2 del RGPD establece la obligación de los Estados miembros de introducir disposiciones normativas específicas que regulen el tratamiento de datos personales del art. 6.1.c) del RGPD, *"fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.*

Por su parte, el art. 6.3 del RGPD vuelve a incidir en la necesidad de que *"La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento."*

5.1.3. Tratamiento de datos personales basada en el interés legítimo de la entidad aseguradora.

Tal y como señala la Guía para el tratamiento de los datos personales por las entidades aseguradoras publicada por la UNESPA[55] *"Las entidades aseguradoras deben verificar si existe interés legítimo y/o habilitación legal para el tratamiento de los datos que realizan o alguna otra base legitimadora del tratamiento como, por ejemplo, la ejecución del contrato de seguro, ya que, de otro modo, tendrán que obtener el consentimiento del interesado para tratar sus datos personales en los términos que establece el RGPD"*

Es decir, esta base de legitimación tiene un carácter residual, y debe ser objeto de ponderación pormenorizada por parte de la entidad aseguradora si pretende realizar un tratamiento de datos personales bajo esta base de legitimación.

Por ello, la UNESPA trae a colación el Dictamen 06/2014 que emitió el Grupo de Trabajo del artículo 29[56], el cual indica que el interés legítimo como base de legitimación, para poder ser pertinente debe cumplir los siguientes requisitos:

- licitud conforme a la legislación europea y nacional.

- Especificidad, es decir, estar articulado con la claridad suficiente

- Corresponder a un interés real del responsable del tratamiento.

5.2 Clasificación de datos personales que se tratan por las aseguradoras en cada una de las fases del contrato.

Antes de la formalización de un contrato de seguro, las aseguradoras deben recabar datos

55 UNESPA "Guía para el tratamiento de los datos personales por las entidades aseguradoras". 7 de Febrero de 2019

56 El Grupo de Trabajo del Artículo 29 (GT 29) fue creado por la Directiva 95/46/CE (que era la normativa anterior al actual RGPD), y es un órgano consultivo independiente formado por todas las Autoridades de Protección de Datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea – que realiza funciones de secretariado-.

personales del futuro asegurado fundamentalmente para analizar la viabilidad del riesgo y, en el ámbito de seguros de salud, los antecedentes de salud del asegurado.

La UNESPA, en su Guía de tratamiento de datos personales en el sector de seguros, analiza de manera pormenorizada esta cuestión en el ANEXO 1, indicando al respecto que los datos personales necesarios en la fase precontractual son los de:

- Valoración del riesgo: La entidad aseguradora requiere recabar del futuro tomador del seguro información que le permita valorar si el riesgo es o no asegurable (es lo que se conoce como declaración del riesgo). La declaración del riesgo tiene efectos durante toda la vida del contrato pues puede sufrir variaciones como agravación, exclusión, disminución del riesgo, falsedad, etc. Así lo disponen los artículos 10, 11, 12, 93 y 94 de la LCS.

- Tarificación: Las entidades deben calcular las tarifas en base al principio de suficiencia para satisfacer las obligaciones derivadas de los contratos y constituir las provisiones técnicas. Además, podrán establecer ficheros comunes para la selección y tarificación de riesgos. Así lo disponen los artículos 94 y 99.7 de la LOSSEAR.

- Test de idoneidad y conveniencia: En productos de inversión basado en seguros, el distribuidor debe recabar datos personales, estudios e información sobre la actividad profesional, conocimientos y experiencia en productos financieros, ingresos y patrimonio y sus objetivos de inversión, pues así lo dispone la Directiva de Distribución y Reglamento UE 1286/204,sin que sea preciso el consentimiento del tomador.

Por su parte, y respecto de los datos personales tratados en la fase precontractual la UNESPA señala en su Guía para el tratamiento de datos personales que *"Entre los datos que necesariamente deben incluirse en el contrato figuran los del tomador del seguro, el asegurado y el beneficiario, en su caso. Además, dependiendo del tipo de seguro pueden ser necesarios otros datos que también serían de carácter personal, alguno de ellos pudiendo hacer referencia a la salud, como podría ser la exclusión de enfermedades preexistentes que se incluyen en el contrato, el resultado de la valoración del riesgo como la existencia de cuestionarios o reconocimientos médicos"*

También debe contener información bancaria, información a efecto de comunicaciones,

La LOSSEAR reconoce la legitimidad de las entidades para el tratamiento de datos necesarios para el pleno desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en la legislación de seguros, pues tanto dicho cuerpo normativo como el RDOSSEAR obligan a las entidades aseguradoras a conservar la documentación contractual y técnica a disposición de la Dirección General de Seguros y Fondos de Pensiones (DGSFP) a incluir la información de ésta en el registro de siniestros que está a disposición de la DGSFP.

El RDOSSEAR obliga también a las entidades aseguradoras a llevar, entre otros, un registro de pólizas y suplementos emitidos que debe incluir los datos más significativos de cada póliza de seguro o suplemento en relación con sus elementos personales, características del riesgo cubierto y condiciones económicas del contrato.

También a llevar un registro de siniestros que debe incluir la póliza de la que procede cada siniestro, pagos o consignaciones posteriores, estimación de la provisión al comienzo y al cierre, fecha de la última valoración así como los pagos e importes recuperables de reaseguro.

5.3 Tratamiento de datos personales por las entidades aseguradoras, distribuidoras y agencias de suscripción.

No solo las entidades aseguradoras, como hemos visto, tratan datos personales del asegurado. También lo hacen otros agentes intervinientes en el marco del contrato de seguro y la responsabilidad de cada uno de ellos en el tratamiento de datos personales dependerá en gran medida del rol que cada uno de ellos ocupe.

A tal efecto, debemos remitirnos al RDL 3/2020 de 4 de febrero [57], en cuyo artículo 204 se analiza la situación de agentes de seguros, corredores de seguros respecto de las compañías aseguradoras.

a) Así, y respecto de agentes de seguros y operadores de banca-seguros, se establece una relación de dependencia de la entidad

57 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.

aseguradora en el marco del contrato de agencia de seguros pactado, de manera que solo podrán tratar datos personales en nombre y por cuenta de la entidad aseguradora (responsable del tratamiento) con la que hubieran celebrado el contrato, sin que puedan tomar decisiones sobre el tratamiento de los datos personales, salvo en el caso de que el responsable de tratamiento lo establezca así por motivos organizativos en el oportuno contrato de encargo de tratamiento.

A mayor abundamiento, dicha disposición normativa solo permite respecto de los operadores de banca-seguros tratar los datos relacionados con su actividad mediadora para fines propios de su objeto social sin contar con el consentimiento inequívoco y específico de los afectados.

Esto hace que estos agentes intervinientes aparezcan como encargados de tratamiento de datos personales bajo la batuta y dirección de la entidad aseguradora como responsable del tratamiento. Así lo dispone el art. 203 de dicho cuerpo legal.

b) Por el contrario, los corredores de seguros no dependen de la entidad aseguradora para tratar datos personales, debiendo regirse por alguna de las bases de legitimación reguladas en el artículo 6 del Reglamento (UE) 2016/679 de 27 de Abril (RGPD). Por ello, tienen la consideración de responsables del tratamiento.

Por ello, y para garantizar el cumplimiento de la normativa de protección de datos personales, una vez resuelto el contrato de seguro en cuya distribución hubiera intervenido un corredor de seguros o de reaseguros deberá proceder a la inmediata cancelación de datos personales, salvo que el interesado hubiera otorgado su consentimiento para otras finalidades.

No se permite la cesión de datos personales por parte del corredor de seguros o de reaseguros a otra entidad aseguradora salvo que medio el consentimiento del interesado

c) Existe la figura de los colaboradores externos, que realizan bajo la fórmula de un contrato mercantil, actuaciones de distribución por cuenta de agentes o corredores de seguros. En este caso tienen la consideración de encargados del tratamiento respecto de dichos mediadores de 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.

5.4 Código de conducta regulador del tratamiento de datos personales en los sistemas comunes del sector asegurador.

El Reglamento Europeo no ofrece una definición de código de conducta. Nos debemos remitir a la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, cuyo artículo 2 define el código de conducta como *"acuerdo o conjunto de normas no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro, en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código en relación con una o más prácticas comerciales o sectores económicos concretos."*

Lo que sí hace el RGPD [58]es recomendar la elaboración y suscripción de códigos de conducta para facilitar la aplicación efectiva del Reglamento y, sobre todo, para delimitar las obligaciones de responsables y encargados teniendo en cuenta que, en determinados sectores como el de seguros el tratamiento de datos personales ofrece unas características especiales como estamos teniendo ocasión de comprobar en este artículo.

Así el Considerando 81 del RGPD indica que *"la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable."*

En palabras del profesor D. Alberto Díaz-Romeral *"Los códigos de conducta pueden facilitar la aplicación de las normas jurídicas en la*

58 Considerando 98 del RGPD: *"Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.*

Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento."

medida en la que aporten orientaciones y claridad a los operadores jurídicos"[59]

En el marco de dicha recomendación, en el panorama nacional, UNESPA elaboró con fecha 5 de diciembre de 2019 el denominado "*Código de Conducta regulador del tratamiento de datos personales en los sistemas comunes del sector asegurador*" el cual fue aprobado por la AEPD mediante resolución dictada en Expediente núm. CC/0012/2019.

En dicha resolución la AEPD indica que *"En ese sentido, la finalidad de la valoración del riesgo asegurado y la oportunidad de llevar a cabo el aseguramiento solicitado, así como la cuantificación de la prima, son finalidades que presentan necesidades específicas en cuanto al tratamiento de datos personales en los Sistemas de Información creados para cumplirlas. El código define la finalidad de los tratamientos de datos de cada uno de los Sistemas de Información: la realización de una valoración técnica y objetiva del riesgo, así como la correcta aplicación de las tarifas de prima en l Sistema SIHSA y la prevención del fraude en los Sistemas SIAPTRI y SIPFSRD."*[60] y [61]

VI. ESPECIAL MENCIÓN A LA PROTECCIÓN DE DATOS PERSONALES

INCLUIDA LA REFORMA DEL TEXTO REFUNDIDO DE LA LEY SOBRE RESPONSABILIDAD CIVIL Y SEGURO DE LA CIRCULACIÓN DE VEHÍCULOS A MOTOR

Con fecha 7 de Junio de 2024 el Congreso aprobó el Proyecto de Ley por la que se modifican el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, y la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Entre sus disposiciones, se crea un título V al TRLRCSCVH dedicado a la protección de datos personales, cuya función es la de dotar de mayor seguridad jurídica a los datos personales tratados *"(...) por las entidades aseguradoras, el Consorcio de Compensación de Seguros y cualesquiera otras personas, entidades o Administraciones Públicas en el contexto de las previsiones de la presente ley(...)"* extendiendo la definición de entidades aseguradoras no solo al Consorcio de Compensación de Seguros sino también a OFESAUTO en su condición de organismo de indemnización.

El proyecto de Ley deja clara la sumisión normativa del TRLRCSCVM tanto al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y a la Ley 20/2015 de 14 de julio de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

El legislador ha querido dejar patente que la finalidad no es establecer un nuevo marco normativo de la protección de datos en el ámbito del sector de seguros sino tal y como establece la exposición de motivos *" el objetivo es aclarar la aplicación de tales normas explicitando las bases jurídicas para los distintos tratamientos de datos personales."*

El título V se articula sobre dos capítulos, el capítulo I denominado "Disposiciones Generales" que comprende los artículos 144 *(Normativa aplicable*), artículo 145 (*Tratamiento de datos personales en el marco de la celebración del contrato de seguro),* artículo 146 (*Tratamiento de los datos personales durante la vigencia del seguro y para la valoración, gestión y tramitación de siniestros) y el* artículo 147 *(Tratamiento de datos de salud en caso de siniestro)* y el capítulo II que regula los sis-

59 DIAZ-ROMERAL GÓMEZ, A. *"Los códigos de conducta en el Reglamento General de Protección de Datos"*en PIÑAR MAÑAS, J.L. *"Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad."* Ed. Reus. Madrid 2016.

60 El Sistema de Información de Pérdida Total, Robo e Incendio (SIAPTRI) tiene por objeto recoger información sobre siniestros del seguro del automóvil en los que se haya producido su pérdida total, ya sea por daños, incendio o robo.

Por su parte, el sistema de Información de Prevención del Fraude en Seguros del Ramo de Diversos (SIPFSRD) tiene por finalidad la prevención y detección del fraude, bien previniendo a la entidad aseguradora una vez emitida la póliza, bien detectando el fraude y cometido en los siniestros declarados en los ramos de Hogar, Comunidades y Comercios.

El sistema de Información Histórico de Seguros del Automóvil (SIHSA) permite el acceso a información de las pólizas del tomador y, si los hubiera, siniestros asociados a las mismas en el momento de suscribir un nuevo seguro de automóvil.

61 *TIREA (Tecnologías de la Información y Redes para las Entidades Aseguradoras S.A.) es una entidad que se encarga del tratamiento de los datos aportados por las Aseguradoras a los Sistemas SIHSA, SIAPTRI y SIPFSRD, así como de atender a las personas para el ejercicio de sus derechos de protección de datos reconocidos en el RGPD. Se formó en el 1997 con apoyo de UNESPA y más de 165 entidades aseguradoras que representaban el 80% de la facturación total del sector*

temas comunes de información (artículos 148 y 149)

6.1 Datos personales en el marco de la contratación de seguro.

El Proyecto de Ley del Texto Refundido sobre la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial dedica el nuevo artículo 145 a detallar los datos personales de los interesados que pueden recabar las entidades aseguradoras, haciendo especial hincapié en el cumplimiento de los principios de protección del RGPD en su tratamiento.

En este contexto, se considera que las entidades aseguradoras podrán recabar toda aquella información que resulte *"necesaria, idónea y proporcional para poder determinar y cuantificar el riesgo asegurado"* en consonancia con el principio de licitud, transparencia e idoneidad del RGPD.

Esta definición vuelve a incluirse en el art. 147.2 al establecer el mecanismo y protocolo de actuación en caso de producción de un siniestro al indicar que *"En caso de producirse un siniestro, las entidades aseguradoras tratarán como responsables del tratamiento todos los datos personales que resulten necesarios, idóneos y proporcionales para cumplir con las obligaciones derivadas del contrato de seguro y, en su caso, cuantificar el importe de la indemnización correspondiente al mismo y para elaborar la propuesta de indemnización o la respuesta motivada prevista en el artículo 7.2 de esta ley. "*

Es un cajón de sastre establecido del que, ya en su momento el Consejo General de Mediadores de España se quejó de su ambigüedad ante la Dirección General de Seguros formulando tres alegaciones al entonces Anteproyecto de Ley de modificación del TRLRCSCVH, centrados sobre todo en los datos de salud al suscribir una póliza, en caso de siniestro.

Una de las alegaciones versaba precisamente sobre la ambigüedad de la expresión *"información necesaria, idónea y proporcional"*, entendiendo que debía precisarse de una manera más explícita la información se refiere la citada expresión, debiendo indicarse igualmente la normativa y sanción aplicable en caso de extralimitación.

También el Consejo de Estado, en su Informe de 16 de mayo de 2024[62] de al Anteproyecto de Ley, ha cuestionado la falta de rigor conceptual señalando que sería conveniente precisar mejor qué debe entenderse por información *"necesaria, idónea y proporcional"*.

Por su parte, la Dirección General de Seguros y Fondos de Pensiones no ha sido demasiado explícito pues ha entendido que los datos personales a la hora de contratar un seguro deben ser únicamente los necesarios para la contratación del seguro de acuerdo con la normativa vigente, lo que no viene a dotar de mayor claridad a la cuestión.

El nuevo artículo 145 se encarga igualmente de precisar la finalidad del tratamiento, en cumplimiento del artículo 6.1 b) del RGPD, indicando que se debe circunscribir únicamente a cuantificar el riesgo asegurado a fin de elaborar la proposición de seguro, para lo cual podrán recabar y tratar la información que se contiene en los sistemas comunes de información[63] así como la información procedente de terceros, siempre que cuenten con base jurídica de legitimación conforme al Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre.

Por otro lado, el artículo 145 habla sobre el plazo de conservación de los datos personales en el caso de que, a pesar de existir una propuesta de seguro, este no se llegara a concertar, las entidades aseguradoras deberán proceder al bloqueo de los datos personales en los términos previstos en la LOPDGDD, no tratando los datos de los solicitantes para otros fines distintos a menos que cuenten con una base jurídica adecuada para ello, en cuyo caso podrán proseguir en el tratamiento únicamente para las finalidades respecto de las que exista dicha base jurídica.

62 Consejo de Estado. Informe al anteproyecto de Ley por la que se modifican el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, y la Ley 20/2015, de 14 de julio, de ordenación, Supervisión y solvencia de las entidades aseguradoras y reaseguradoras. 16 de Mayo de 2024

63 La UNESPA en su Código de Conducta regulador del Tratamiento de Datos Personales en los sistemas comunes de información del sector asegurador, de 12/04/2022, en su artículo 4.5 dispone que: *"Cuando proceda la supresión de los datos por no ser necesarios para los fines del tratamiento o por haber transcurrido los plazos de cancelación, pero el interesado solicite su conservación por necesitarlos para la formulación, el ejercicio o la defensa de reclamaciones. La limitación podrá ser temporal mientras se verifiquen las circunstancias alegadas por el interesado, pudiendo devenir definitivo si concurren las circunstancias para ello. En caso de satisfacción del derecho a la limitación al tratamiento, dichos datos serán conservados y tratados únicamente conforme a lo previsto en el apartado 2 del artículo 18 del RGPD.(...)"*

En este punto debemos hacer una parada y tratar de explicar la diferencia entre cancelación, bloqueo y supresión de datos personales. Para ello, debemos partir del principio general de limitación del plazo de conservación de datos personales contenido en artículo 5.1.e) del RGPD, el cual establece que los datos personales solo pueden conservarse durante el tiempo necesario para la finalidad que justificó su tratamiento.

Sin embargo, agotado ese plazo es posible que esos datos personales puedan ser requeridos por jueces y tribunales, Ministerio Fiscal o Administraciones Públicas competentes, en particular de las autoridades de protección de datos. Por ello, la cancelación de datos no conlleva el borrado y supresión definitiva de los mismos, sino que agotada la finalidad para la que fueron tratados se deberá proceder al bloqueo de los datos.

El gabinete jurídico de la AEPD, en su Informe 00148/2019 ya dejaba sentado que *"(...) existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.(...)"*[64]

Es decir, que si a pesar de la propuesta de seguro, la misma no culminara con la contratación de la pertinente póliza, se habría agotado la finalidad de tratamiento de los datos personales debiendo procederse a su cancelación mediante el bloqueo de los datos que deberán conservarse únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión, es decir, a la eliminación definitiva de estos.

El bloqueo debe ser de tal forma que sea imposible el acceso a los datos por parte del personal, limitado el acceso a los mismos únicamente a una persona de la empresa con la máxima atribución de funciones y responsabilidad, por ej el CEO.

La Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección 1.ª,en sentencia de 19 de junio de 2018 (recurso Núm: 936/2016) resolvió que los datos personales de un asegurado fueron tratados sin su consentimiento por una aseguradora desde el momento en que aquel manifestó su voluntad de no renovar la póliza por lo que a partir de ese momento cualquier tratamiento de datos derivados de tal póliza del seguro, no renovada, carecía del consentimiento de su titular. Por dicha actuación, ya la AEPD le impuso una sanción a dicha aseguradora.[65]

6.2 Tratamiento de los datos personales durante la vigencia del seguro y para la valoración, gestión y tramitación de siniestros.

El anteproyecto de Ley crea un nuevo artículo 146 al TRLRCSCVH para aclarar y precisar qué datos personales se deben tratar una vez concertado el contrato de seguro y durante la vida de este, haciendo especial mención a los datos personales tratados en caso de siniestro y más concretamente la finalidad y las bases de legitimación para dicho tratamiento.

La finalidad del tratamiento, como ya expuso la AEPD en su informe de Marzo de 2009, debe estar amparado exclusivamente en a) el cumplimiento de las obligaciones derivadas del contrato de seguro b) la cuantificación del importe de la indemnización correspondiente y c) la elaboración de la propuesta de indemnización o respuesta motivada del artículo 7.2 de dicho Texto Refundido.

En cuanto a la base de legitimación, precisa que debe ser necesariamente la indicada en el artículo 6.1c) RGPD: el cumplimiento de obliga-

64 Art. 32 Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:*" El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.*

Transcurrido ese plazo deberá procederse a la destrucción de los datos."

65 En el Procedimiento Sancionador Nº: PS/00079/2019 la Agencia Española de Protección de Datos sancionó a LINEA DIRECTA ASEGURADORA, S.A. por enviar comunicaciones comerciales sin haber otorgado el interesado su consentimiento para la recepción de correos electrónicos publicitarios.

ciones legales para las entidades aseguradoras dispuestas en los artículos 18 y 76 de la Ley 50/1980 LCS y artículo 7 del TRLSCVH.

Para dicha finalidad, sobre la misma base de legitimación, y en el marco de la facultad que confiere el art. 145 a las aseguradoras para pedir datos personales a los interesados, estas podrán tratar también los datos personales que sean facilitados por el perjudicado en su solicitud de indemnización, así como los obrantes en los informes periciales complementarios del artículo 7.2 de dicho Texto Refundido y los obrantes en Atestados.

A estos efectos, el artículo 146 precisa que las entidades aseguradoras y reaseguradoras tendrán la consideración de responsables del tratamiento de dichos datos personales, mientras que los terceros encargados de investigación, peritación y valoración de los daños tendrán la consideración de encargados de tratamiento, por lo que considera preciso suscribir un contrato de encargo de tratamiento[66] entre ambos que regule las obligaciones de responsable y encargado. (Art. 28.3 del RGPD).

Por último, el artículo 146 detalla el tratamiento de datos incluidos en la Declaración amistosa de accidente, o los derivados de la aplicación de Convenios de indemnización directa o de asistencia sanitaria para lesionados de tráfico. En este caso, el legislador se ha preocupado de que dicho tratamiento deba cumplir los principios de minimización, exactitud y limitación de finalidad (solo información necesaria, idónea y proporcional a)para el cálculo y valoración de la indemnización b)para elaboración de la oferta de indemnización y, c)para reparación de los daños) así como para la adopción de cuantas medidas sean necesarias para evitar brechas de seguridad en el tratamiento (principio de integridad y confidencialidad).[67]

5.3 Tratamiento de datos de salud en caso de siniestro.

El tratamiento de este tipo de datos, tiene la consideración de datos sensibles por el RGPD, son objeto de una protección especial que impide su tratamiento salvo que se encuentre amparado en alguno de los supuestos del artículo 9 del RGPD que ya hemos analizado anteriormente.

El Proyecto de Ley introduce un nuevo artículo 147 al TRLRCSVH que se encarga de aclarar que las bases de legitimación para el tratamiento de datos de salud en casos de siniestro son las del articulo 6.1c) del RGPD (cumplimiento de una obligación legal) y 9.2.f) del mismo cuerpo legal (cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial) como consecuencia de la acción directa reconocida al perjudicado por el artículo 7.1 del TRLRCSVH y, de ser necesario, para atender a su derecho a la indemnización, y en el artículo 99.1 de la Ley 20/2015, de 14 de julio[68]

66 Artículo 28.3 del RGPD: *"**3.** 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."* Dicha disposición normativa se encarga de detallar y enumerar lo que debe incluir el contrato de encargo de tratamiento.

67 Art. 5.1 del RGPD: *" 1. Los datos personales serán:*

a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia");

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad");

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos");

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ("exactitud");

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("limitación del plazo de conservación");

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").

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

Art. 99.3 *"El tratamiento de los datos se limitará en estos casos a aquellos que resulten imprescindibles para el abono de la indemnización o la prestación derivada del contrato de seguro. Los datos no podrán ser objeto de tratamiento para ninguna otra finalidad, sin perjuicio de las obligaciones de*

Debido a su catalogación de datos sensibles, este artículo 147 dota de mayor seguridad a los datos de salud relacionados con un siniestro, obligando a las aseguradoras a garantizar al perjudicado que la comunicación y transmisión de los datos se pueda llevar ejecutar de manera segura, y obliga a las entidades aseguradoras una vez recibida la documentación a establecer un sistema que proteja los datos de forma efectiva, teniendo en cuenta lo establecido en los artículos 25 y 32 del RGPD.

A estos efectos, las entidades aseguradoras podrán poner a disposición de los abogados que representen a los lesionados en accidentes de tráfico, plataformas seguras de intercambio de información que garantizarán en todo momento, la trazabilidad de las reclamaciones y el cumplimiento de la normativa en materia de protección de datos personales.

6.4 Sistemas comunes de información

El art. 148 de la Reforma de Ley permite a las aseguradoras en el marco de la obligación de las aseguradoras para expedir la certificación acreditativa de siniestros (Art. 2.7 TRLRCSCVM) y al amparo de lo dispuesto en el artículo 99.7 de la Ley 20/2015, de 14 de julio, sistemas comunes de información en los que se incorporen los datos relacionados con la siniestralidad de los vehículos. En este caso, el propio artículo señala que la base de legitimación será la indicada en el art. 6.1 c) del RGPD esto es el cumplimiento de obligaciones legales.

En aplicación del principio de minimización de datos y de limitación de la finalidad del tratamiento (art. 5 RGPD) dicho precepto señala que los datos que se recaben se limitarán únicamente al tomador, al contrato celebrado y la fecha y el alcance, personal o material, de los daños producidos e importe de la indemnización, así como los que se contuvieran en la certificación de antecedentes siniestrales regulada en el artículo 16 de la Directiva (UE) 2021/2118.

También, con respeto al principio de conservación de datos, se hace mención expresa a que los datos se circunscriben únicamente a los siniestros de los últimos cinco años por lo que, transcurrido dicho plazo, se deberán adoptar mecanismos seguros y automáticos para garantizar la supresión de los datos.

información establecidas en esta Ley"

Este mecanismo reforzado también será exigido a las aseguradoras para verificar la existencia de una solicitud de un interesado, incorporando, además de un dato personal que lo identifique, alguna otra información que sólo pudiera obrar en poder de aquél. Dicha exigencia persigue dotar de mayor seguridad a las entidades para evitar posibles brechas de seguridad en el tratamiento de datos personales por parte de personas distintas al interesado (*privacy by default and by design*).

También aclara que, en base al principio de limitación del tratamiento, las entidades solo podrán tratar los datos con la finalidad de gestión de la solicitud de aseguramiento, tarificación y valoración del riesgo asegurado y la cuantificación de la prima.

Por su parte, y en un ámbito más específico, el artículo 149 del Proyecto de Ley, permite establecer sistemas comunes de información *"para el cumplimiento de sus obligaciones legales de prevenir, impedir, identificar, detectar, informar y remediar conductas fraudulentas relativas a seguros",* conforme a lo dispuesto en los artículos 99.7 y 100 de la Ley 20/2015, de 14 de julio,

Se vuelve a introducir una expresión genérica, al igual que en el artículo 145, para referirse a los datos que deberán ser incluidos en los sistemas de información al indicar que deben ser *"los necesarios, idóneos y proporcionales para el cumplimiento de la finalidad a la que se refiere el apartado anterior"* si bien precisa y limita que deben ser datos referidos a perjudicados, sin incluir dato alguno referente a la salud.

Obliga a las entidades aseguradoras a actualizar los datos en cumplimiento del principio de exactitud.

En el apartado 4 se establece la finalidad de la consulta a estos sistemas, con el fin de evitar posibles interpretaciones e uso indebido de estos sistemas indicando al respecto que se consultarán con la finalidad de *"poder identificar situaciones de anomalía y de riesgo de fraude por parte del tomador, asegurado, beneficiario, titular del vehículo o perjudicado, a fin de poder valorar las solicitudes de suscripción de una póliza y, en su caso, la tarificación del riesgo, así como adoptar las decisiones que resulten necesarias en relación con la tramitación de un siniestro con posible riesgo de fraude."*

Se permite que se comunique la información de los sistemas de prevención del fraude

a las Fuerzas y Cuerpos de Seguridad, así como a los Órganos de las Administraciones Públicas de las que los mismos dependen para el ejercicio de sus funciones en la prevención y lucha contra el fraude y a la Dirección General de Tráfico pero no dice si debe hacerse mediante cesión de datos o acceso a dichos sistemas, lo cual hubiera sido más lógico.

Eso sí, precisa que la información debe ser específica *"ajustada a los datos que resulten precisos para la tramitación de un expediente determinado, sin que pueda tratarse de un acceso masivo o indiscriminado."* También a la Dirección General de Tráfico.

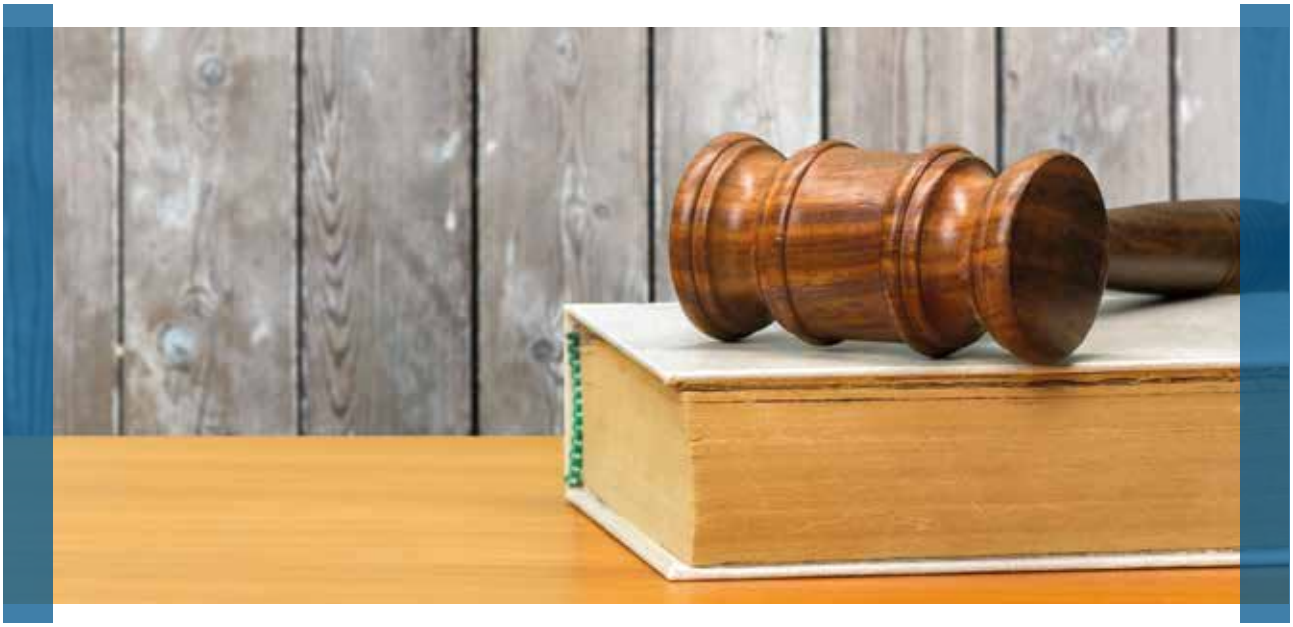
Por último, el artículo 150 se encarga de delimitar la cualidad de cada parte en estos sistemas comunes de información en su calidad de responsable del tratamiento (Sistema común de información), corresponsable del tratamiento (entidades aseguradoras) y/o encargado de tratamiento (En aquellos casos en los que se encargue la gestión del sistema a terceras entidades)[69]. También se permite a las asociaciones representativas de las entidades aseguradoras tratar los datos contenidos en los sistemas comunes de información para la realización de estudios técnicos y actuariales y la elaboración de estadísticas del sector asegurador, si bien no precisa en este supuesto la calidad en la que se tratarán los datos (corresponsable o encargado de tratamiento).

Si bien la obligación de transmisión de datos personales a los sistemas comunes de información se encuentra amparada en estas disposiciones normativas analizadas, las entidades aseguradoras deberán informar al interesado, en cumplimiento de lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679 tanto de la comunicación como de la posibilidad de que se produzca un acceso posterior a los datos por otras entidades aseguradoras adheridas a los sistemas.

Por último, se permite a las entidades aseguradoras la adopción de códigos de conducta reguladores de los citados sistemas comunes de información.

En este sentido, y como ya hemos analizado en anterior expositivo, la UNESPA tiene aprobado el Código de Conducta denominado "*CÓDIGO DE CONDUCTA REGULADOR DEL TRATAMIENTO DE DATOS PERSONALES EN LOS SISTEMAS COMUNES DE INFORMACIÓN DEL SECTOR ASEGURADOR"* de fecha 12/04/2022 en el que se regula gran parte de estas disposiciones normativa.

69 *TIREA (Tecnologías de la Información y Redes para las Entidades Aseguradoras S.A.) es una entidad que se encarga del tratamiento de los datos aportados por las Aseguradoras a los Sistemas SIHSA, SIAPTRI y SIPFSRD, así como de atender a las personas para el ejercicio de sus derechos de protección de datos reconocidos en el RGPD. Se formó en el 1997 con apoyo de UNESPA y más de 165 entidades aseguradoras que representaban el 80% de la facturación total del sector*



Tal y como hemos avanzado, UNESPA ya tiene implantado el Sistema de Información de Pérdida Total, Robo e Incendio (SIAPTRI) el cual tiene por objeto recoger información sobre siniestros del seguro del automóvil en los que se haya producido su pérdida total, ya sea por daños, incendio o robo.

Y, por otro lado, el sistema de Información de Prevención del Fraude en Seguros del Ramo de Diversos (SIPFSRD) el cual tiene por objeto la prevención y detección del fraude, bien previniendo a la entidad aseguradora una vez emitida la póliza, bien detectando el fraude y cometido en los siniestros declarados en los ramos de Hogar, Comunidades y Comercios.

Por último, El sistema de Información Histórico de Seguros del Automóvil (SIHSA) permite el acceso a información de las pólizas del tomador y, si los hubiera, siniestros asociados a las mismas en el momento de suscribir un nuevo seguro de automóvil.

No obstante lo anterior, el resto de entidades aseguradoras no adheridas a UNESPA deberán implantar códigos de conducta y establecer los sistemas de información a que alude este título V del TRLRCSCVH, sin perjuicio de que todas las aseguradoras adapten lo ya publicado hasta la fecha a las disposiciones normativas citadas.

VII. CONCLUSIONES

Tras el trabajo realizado de análisis y estudio de la protección de datos en el ámbito del sector asegurador, podemos extraer las siguientes conclusiones:

- Resulta evidente la gran confluencia de datos personales en el marco de la contratación de cualquier seguro, desde la fase precontractual en la que se recaban datos personales que (en la gran mayoría de las ocasiones) son facilitados por el propio interesado, pasando por la suscripción del contrato de seguro de la que se derivan una serie de obligaciones normativas para la aseguradora que le obliga a tratar los datos personales bajo otras bases de legitimación como el cumplimiento de obligaciones legales o contractuales o el interés legítimo, y terminando en la ejecución del contrato de seguro en aquellos supuestos en que se produce un siniestro y la compañía aseguradora queda obligada a desplegar una ingente actividad tendente a ceder datos personales (gruistas, ambulancias, peritos, etc) pero también a recabarlos (a centros hospitalarios, fuerzas y cuerpos de seguridad del Estado, a los propios interesados o a familiares de estos, etc).

- En muchas de las ocasiones, los datos personales tratados por las compañías aseguradoras son datos que tienen la consideración de datos sensibles (entre ellos datos genéticos, datos biométricos, datos relativos a la salud, etc) lo que les dota de una especial protección por la normativa tanto europea como española que obliga a las entidades aseguradoras a adoptar medidas técnicas y organizativas para garantizar la integridad, disponibilidad y confidencialidad de los datos tratados (principio de seguridad) así como adoptar la diligencia debida y, en su caso, un análisis de riesgos (principio de responsabilidad proactiva) de tal modo que las aseguradoras en su faceta de responsables del tratamiento de los datos puedan demostrar, en caso de vulneración o brecha se seguridad, que el tratamiento se ajusta a la normativa de RGPD y LOPDGDD.

- En la ejecución del contrato de seguro, cuando se produce un siniestro, todos los agentes intervinientes en los mismos (fuerzas y cuerpos de seguridad del Estado, personal sanitario, servicios de emergencias, sistemas de geolocalización, servicios de bomberos) están obligados a tratar los datos personales de los perjudicados bajo el prisma de la normativa tanto europea como española en protección de datos.

- El legislador español fue sensible a la enorme interacción existente en el binomio datos personales-seguros y ha incluido variadas y numerosas disposiciones normativas en las diversas leyes en materia de seguros. En este artículo hemos profundizado en muchas de ellas como la Ley de Contrato de Seguro, el Texto Refundido sobre la Ley de responsabilidad civil y seguro en la circulación de vehículos a motor, la Ley de Autonomía del Paciente, o La ley de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, pero también hemos hablado de otros cuerpos legales como la Ley General de Telecomunicaciones o la Ley de la Sociedad de Servicios de la Información que tienen incidencia en la ejecución de un contrato de seguro.

- En contraposición a ello, la normativa europea en protección de datos es decir, el

RGPD apenas contiene referencias al ámbito del seguro; tan solo hace referencia a los datos relativos a la salud. Igual ocurre en nuestra LOPDGDD en la que solo encontramos una mención expresa en su artículo 9 al hablar de las categorías especiales de datos que obliga a regular normativamente requisitos adicionales para la seguridad y confidencialidad de esos datos en la ejecución de un contrato de un contrato de seguro.

- Todo ello ha hecho que haya tenido que ser la Agencia Española de Protección de Datos la que, entre sus numerosas funciones, se haya encargado de aclarar, interpretar, precisar y complementar la normativa de protección de datos en materia de seguros. Hemos analizado, en concreto, numerosos informes y resoluciones dictadas por la AEPD pero también guías publicadas por la AEPD en diversas materias relacionadas con el tratamiento de datos personales en el ámbito asegurador. Pero también la jurisprudencia se ha encargado de velar por el cumplimiento de la protección de datos y los derechos del interesado a fin de evitar quiebras de seguridad en su tratamiento y violaciones de este derecho fundamental constitucionalmente establecido.

- No podemos olvidar, y relegar a un segundo plano, que también han sido las propias entidades aseguradoras las que han tratado de velar por el cumplimiento de la protección de datos en todo momento, como por ejemplo la UNESPA publicando códigos de conducta para facilitar la aplicación normativa de protección de datos en el sector asegurador pero también para servir como elemento para demostrar el cumplimiento de las obligaciones por parte del responsable de tratamiento. También mediante el establecimiento de sistemas comunes de información para el cumplimiento de sus obligaciones legales tales como impedir conductas fraudulentas relativas a seguros.

- Todo ello se ha visto culminado con la redacción de un nuevo Título V dedicado a los datos personales que ha introducido el proyecto de ley para la reforma del Texto Refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, pues el legislador ha sido sensible al tratamiento especializado de datos personales que se lleva a cabo por el sector asegurador y del que ha tratado de servir de orientación y aclaración del tratamiento de protección de datos por dicho sector.

Este nuevo título V, en realidad, es la base vertebral de este texto pues regula con bastante precisión todo lo que hemos ido analizando en el artículo.

La dicción literal del articulado, bajo nuestro criterio, es bastante especializada en el ámbito de la protección de datos e incluye numerosa nomenclatura, conceptos, referencias y expresiones que nada tienen que ver con la responsabilidad civil y el seguro en la circulación de vehículos a motor, lo que pudiera llegar a dificultar la comprensión para los distintos operadores y sectores profesionales que aplican este texto normativo. Se lanza la idea de que sea la AEPD la que publique, una vez en vigor este título V, una guía explicativa que explique los distintos conceptos y expresiones utilizadas en dicho título V, al igual que ya hizo UNESPA al publicar la Guía de buenas prácticas para el tratamiento de datos personales por las entidades aseguradoras la cual, a nuestro juicio, es bastante clarificadora e incluye un exhaustivo análisis de las bases jurídicas que legitiman el tratamiento de datos personales para facilitar el cumplimiento de las obligaciones impuestas a las aseguradoras tanto por el RGPD como por la LOPDGDD.

- Por relevancia e incidencia práctica en la vida diaria, hemos hecho una especial parada en la historia clínica, materia que ha sido y es especialmente vigilada por los distintos operadores jurídicos a fin de dotarla de especial protección dado que contiene numerosos datos sensibles que pudieran ser objeto de accesos indebidos, extralimitados y no consentidos. Es en este ámbito donde mayores denuncias se han producido a la AEPD y también el ámbito donde mayores resoluciones judiciales y por la AEPD se han dictado y donde mayor número de sanciones y penas se han impuesto a profesionales de la sanidad.

VIII. GLOSARIO

- C.E: Constitución Española

- CE: Comunidad Europea

- DGSFP: Dirección General de Seguros y Fondos de Pensiones.

- IA: Inteligencia Artificial

- FIVA: Fichero Informativo de Vehículos Asegurados

- GT 29: Grupo de Trabajo del Artículo 29

- LAP: Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- LBAP: Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

- LCCSNS: Ley 16/2002, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud

- LCS: Ley 50/1980, de 8 de octubre, de Contrato de Seguro

- LGSP Ley 33/2011, de 4 de octubre, General de Salud Pública

- LIB: Ley 14/2007, de 3 de julio, de Investigación biomédica

- LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- LORTAD: Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automa-

tizado de los datos de carácter personal.

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

- LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico): Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- RGPD: 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 (Reglamento general de protección de datos).

- RDOSSEAR: Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de entidades aseguradoras y reaseguradoras.

- SESPAS: Sociedad Española de Salud Pública y Administración Sanitaria.

- SIAPTRI: Sistema de Información de Pérdida Total, Robo e Incendio.

- SIHSA: Sistema de Información Histórico de Seguros del Automóvil

- SIPFSRD: Sistema de Información de Prevención del Fraude en Seguros del Ramo de Diversos.

- TIREA: (Tecnologías de la Información y Redes para las Entidades Aseguradoras S.A.)

- TRLRSCVH: Texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor.

- UE: Unión Europea

IX. BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *"Guía para pacientes y usuarios de la Sanidad".* Madrid. Noviembre de 2019.

BATALLER GRAU. J. y QUINTÁNS EIRAS, M.R. La distribución de seguros privados. Ed. Marcial Pons 2019.

BELTRÁN AGUIRRE, J.L., GARCÍA LÓPEZ F.J y NAVARRO SÁNCHEZ, C. *"Protección de Datos Personales y Secreto Profesional en el ámbito de la salud. Una propuesta normativa de adaptación al RGPD".* Sociedad Española de Salud Pública y Administración Sanitaria. Noviembre de 2017.

CASANOVA ASENCIO, A.S: *"Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias."* Revista para el Análisis del Derecho. Barcelona, Abril 2019.

DE MIGUEL SÁNCHEZ, N., *"Principios de la protección de datos: datos especialmente protegidos. Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario"* en Comentario a la ley Orgánica de Protección de Datos de Carácter Personal, Civitas Ediciones, 2010, pp. 708-734.

DIAZ-ROMERAL GÓMEZ, A. "Los códigos de conducta en el Reglamento General de Protección de Datos"en PIÑAR MAÑAS, J.L. "Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad. Ed. Reus. Madrid 2016.

FERNÁNDEZ, R; ALMARCHA, J; SÁNCHEZ.A: *"Los tratamientos singulares de datos personales por parte de entidades aseguradoras, sus distribuidores y agencias de suscripción."* Revista jurídica Pérez LLorca 2021.

JIMÉNEZ LÓPEZ, JESÚS. *"Transparencia pública, genoma y datos genéticos"* Revista Española de la Transparencia Núm. 17. Año 2023

LÓPEZ Y GARCÍA DE LA SERRANA, J. *"Las reclamaciones por responsabilidad civil y la preservación de la protección de datos".* Revista Española de Seguros núm. 15, Julio-Diciembre 2019.

LÓPEZ Y GARCÍA DE LA SERRANA, J. *"La aplicación de la ley de protección de datos en relación con el artículo 32 de la LCS. Comentario a la Sentencia del Tribunal Supremo de 25-03-11",* Revista de Responsabilidad Civil, Circulación y Seguro num. 6 del año 47 (2011) Ed. INESE.

LÓPEZ Y GARCÍA DE LA SERRANA, J. *"Compatibilidad entre el Derecho de defensa y protección de datos".* Revista de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro. Núm. 42 .

2º Trimestre de 2012.

MORALEJO INVERNÓN, Nieves. *"El testamento digital en la nueva Ley Orgánica 3/2018 de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales"* ADC. Tomo LXXIII, 2020, fascículo I.

PEÑAS MOYANO, M. J.: *"Los mediadores y sus colaboradores. Las relaciones con la cliente-la y la entidad aseguradora",* Revista Española de Seguros, núm. 185-186, 2021.

PIÑAR MAÑAS, J.L."*Códigos de Conducta y espacio digital. Especial referencia a la protección de datos"* en REAL PÉREZ, A. Códigos de Conducta y actividad económica: una perspectiva jurídica. Marcial Pons, 2010.

TRONCOSO REIGADA, A (2010) *"La protección de datos personales. En busca del equilibrio".* Madrid. Editorial Tirant Lo Blanch.

UNESPA. *"Guía para el tratamiento de los datos personales por las entidades aseguradoras.".* Madrid, 2019.

VEIGA COPO, A. *"Tratado del contrato de seguro".* Ed. Civitas. Madrid 2023.

X. JURISPRUDENCIA Y DOCTRINA

a) Informes de la AEPD y dictámenes del Grupo de trabajo del artículo 29.

- Informe 327/2003
- Informe 0411/2010
- Informe 0006/2009
- Informe 526/2003
- Informe 449/2004
- Informe 0039/2009
- Informe 186/2018
- Informe 10318/2019
- Informe 36/2020
- Informe 368/2006
- Informe 0549/2008
- Informe 0078/2009
- Informe 2010/411
- Informe 2009/78
- Informe 438/2015
- Informe 0148/2019
- Dictamen 4/2007 del Grupo de Trabajo del artículo 29.
- Dictamen 06/2014 del Grupo de Trabajo del artículo 29

b) Sentencias.

- Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000.
- Sentencia del Pleno del Tribunal Constitucional núm. 290/2000, de 30 de noviembre de 2000.
- Sentencia del TSJ de Navarra, Sala de lo Contencioso-Administrativo, de fecha 08/02/2012
- Sentencia del Tribunal Supremo, Sala 1º, de fecha 27/01/1997 (Roj 452/1997)
- Sentencia del Tribunal Supremo, Sala 2º, de fecha 04/04/2001 (RJ 2001/2016)
- Sentencia del Tribunal Supremo, sala 2ª, de 18/10/2012 (RJ 2012/1437)
- Sentencia del Tribunal Supremo, Sala 2ª , 03/02/2016 (Roj 185/2016)
- Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección primera, recurso 1443/2020
- Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección 1.ª,de 19 de junio de 2018 (recurso Núm: 936/2016)
- Sentencia num. 615/2022 dictada por la Audiencia Provincial de Valencia con fecha 30/11/2022 en procedimiento abreviado 72/2022
- Sentencia del Tribunal Supremo (Sala de lo Penal) de 22 de octubre de 2021, recurso de casación 4846/2019.

c) Guías.

- "Guía para pacientes y usuarios de la sanidad" AEPD, Noviembre de 2019.

- *"Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos"* AEPD, 26 de julio de 2022. -https://www.aepd.es/areas-de-actuacion/salud/brechas-de-datos-personales-en-el-sector-de-la-salud

- Guía de buenas prácticas para el tratamiento de datos personales por las entidades aseguradoras. UNESPA.

- Guía de buenas prácticas de UNESPA sobre la aplicación del derecho al olvido oncológico a los seguros contratados antes de 30 de junio de 2023.

- "Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos" AEPD 26 de Julio de 2022.